ON CODES OVER SOME NON-CHAIN EXTENSIONS OF Z_4

A THESIS

Submitted in partial fulfilment of the requirements for the award of the degree
of
DOCTOR OF PHILOSOPHY
in
MATHEMATICS

by

RAMAKRISHNA BANDI

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE-247667 (INDIA)
APRIL, 2016

INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis entitled "**ON CODES OVER SOME NON-CHAIN EXTENSIONS OF Z_4**" in partial fulfilment of the requirements for the award of the Degree of Doctor of Philosophy and submitted in the Department of Mathematics of the Indian Institute of Technology Roorkee, Roorkee is an authentic record of my own work carried out during the period from July, 2011 to April, 2016 under the supervision of Dr. Maheshanand, Associate Professor, Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee.

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

(RAMAKRISHNA BANDI)

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

(Maheshanand)
Supervisor

The Ph.D. Viva-Voce Examination of **Mr. Ramakrishna Bandi**, Research Scholar, has been held on 30/08/2016.

Chairman, SRC

External Examiner

This is to certify that the student has made all the corrections in the thesis.

Supervisor

Head of the Department

Date: August 30, 2016

Dedicated

to

My Parents

Abstract

Algebraic codes have been traditionally studied in the setting of vector spaces over finite fields. The study of codes over rings was initiated in early seventies [23,24,106,107,119,120, 132]. However, codes over rings got attention of researchers mainly after the breakthrough paper of Hammons et al. [58] in 1994, in which they have shown that some non-linear binary codes are actually the images of some linear codes over $\mathbb{Z}_4$ under the Gray map. The findings of this paper led to a lot of research in this area [19,25,30–32,35,56,67,89,135]. As a result, a large number of papers were produced studying codes over $\mathbb{Z}_4$. This quickly expanded to consider codes over $\mathbb{Z}_m$ and then onto other rings such as Galois rings and, in general, finite chain rings [3, 4, 21, 45, 49, 90, 96, 97, 130]. However, not much attention has been paid to codes over non-chain rings. Recently, finite polynomial rings such as $\mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$ [26, 124], $\mathbb{F}_2 + v\mathbb{F}_2$, $v^2 = v$ [140], $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, $u^2 = v^2 = 0$, $uv = vu$ [138], etc., have been considered as alphabets for studying codes. Some of these are non-chain rings. Recently, Yildiz and Karadeniz [139] have introduced a local non-chain ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$, and studied linear and self-dual codes over it. They have also got some good formally self-dual codes over this ring. The study of codes over finite rings has provided some codes with better parameters and such codes have also got some practical applications.

In this thesis, we have explored some families of codes over some non-chain extensions of $\mathbb{Z}_4$. In this context, we have introduced two new rings $\mathbb{Z}_4 + v\mathbb{Z}_4$, $v^2 = v$, and $\mathbb{Z}_4 + w\mathbb{Z}_4$, $w^2 = 2w$, and studied linear codes over them. Further, we have done an indepth study of cyclic and negacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. Finding a suitable metric for the codes over a given ring is an interesting problem. In view of this, we have studied codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ with respect to Lee and Gray metrics and also derived MacWillaims type identities for linear codes with respect to these metrics. A non-Hamming metric, namely, Rosenbloom-Tsfasman (RT) metric or the ρ metric has also been considered in this study, and linear codes over $\mathbb{Z}_4+v\mathbb{Z}_4$ with respect to this metric are studied. A MacWilliams type identity using Lee complete ρ-weight enumerator is presented. A transformation to obtain ρ-weight enumerator from Lee complete ρ-weight enumerator is provided.

Self-dual codes are an interesting class of codes and are closely related to design theory. The study of self-dual codes and their constructions is an important topic in coding theory. We have characterized self-dual codes over $\mathbb{Z}_4+v\mathbb{Z}_4$, $v^2=v$ and $\mathbb{Z}_4+w\mathbb{Z}_4$, $w^2=2w$ and presented some methods for constructing self-dual and self-orthogonal codes over $\mathbb{Z}_4+v\mathbb{Z}_4$ and $\mathbb{Z}_4+w\mathbb{Z}_4$. We have also briefly studied circulant codes and Type II codes over $\mathbb{Z}_4+w\mathbb{Z}_4$.

One of the most studied families of algebraic codes is the family of cyclic codes, which have a rich algebraic structure. Their structure over finite chain rings is now well known [45, 83, 84, 90]. However, they have not been well explored over local non-chain rings. We have studied cyclic codes over the non-chain ring $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$. First we have focused on cyclic codes of odd length n, and obtained their structure through the factorization of x^n-1 over $\mathbb{Z}_4+u\mathbb{Z}_4$. We have then considered cyclic codes of arbitrary lengths over $\mathbb{Z}_4+u\mathbb{Z}_4$ and presented their structure. In particular, all cyclic codes of length 2^k are classified. Using the structure of general form of cyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, we have obtained a minimal spanning set and a formula for the ranks of such codes. A necessary condition and a sufficient condition for cyclic codes to be free over $\mathbb{Z}_4+u\mathbb{Z}_4$ are obtained.

An important generalization of cyclic codes is negacyclic codes. We have characterized negacyclic codes of both odd and even lengths over $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$. The complete classification of negacyclic codes of length 2^k over $\mathbb{Z}_4+u\mathbb{Z}_4$ is given and their duals are determined in each case. All negacyclic codes $\mathcal{C}$ of length 2^k over this ring satisfying $\mathcal{C}\subset A(\mathcal{C})$ and $\mathcal{C}=A(\mathcal{C})$, where $A(\mathcal{C})$ is the annihilator of $\mathcal{C}$, are presented. Enumeration of codes of a particular type has been an interesting problem in coding theory. We have enumerated negacyclic codes of length 2^k over $\mathbb{Z}_4+u\mathbb{Z}_4$. This study has further been generalized to negacyclic codes arbitrary even length over $\mathbb{Z}_4+u\mathbb{Z}_4$. The classification of negacyclic codes led to some good $\mathbb{Z}_4$-codes via the Gray map.

Publications

Following are the publications produced during this research.

Journals:

- **Rama Krishna Bandi**, Maheshanand Bhaintwal and Nuh Aydin, "A mass formula for negacyclic codes of length 2^k and some good negacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$", *Cryptography and Communications* (Springer), DOI: 10.1007/s12095-015-0172-3.

- **Rama Krishna Bandi** and Maheshanand Bhaintwal, "Negacyclic codes of length 2^k over $\mathbb{Z}_4 + u\mathbb{Z}_4$", *International Journal of Computer Mathematics* (Taylor & Francis), DOI: 10.1080/00207160.2015.1112380.

- **Rama Krishna Bandi** and Maheshanand Bhaintwal, "A note on cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$", *Discrete Math. Algorithm. Appl.*, Vol. 08, No. 01, 1650017 (2016).

- **Rama Krishna Bandi** and Maheshanand Bhaintwal, "Self-dual codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$", *Discrete Math. Algorithm. Appl.*, Vol. 07, No. 02, 1550014 (2015).

Conferences:

- **Rama Krishna Bandi** and Maheshanand Bhaintwal, "Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$", *In Proc. The seventh International Workshop on Signal Design and its Applications in Communications (IWSDA'15)*, Indian Institute of Science Bangalore, Bengaluru, September 13–18, 2015, (Available on IEEE Explore).

- **Rama Krishna Bandi** and Maheshanand Bhaintwal, "Codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$", *In Proc. International Conference on Advances in Computing, Communications and Informatics (ICACCI-2014)*, Noida, India, September 24–27, pp 422–427 (2014) (Available on IEEE Explore).

- **Rama Krishna Bandi** and Maheshanand Bhaintwal, "Codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ with respect to Rosenbloom Tsfasman metric", *In Proc. International Conference on Advances in Computing, Communications and Informatics (ICACCI-2013)*, Mysore, India, August 22–25, pp 37–42 (2013) (Available on IEEE Explore).

Acknowledgements

It is a great pleasure and profound privilege to express my deepest gratitude to my research advisor Dr. Maheshanand who introduced me to the beautiful subject of coding theory, and without whose inestimable support this thesis would have been possible. He has been my mentor not only in research, but for many other things in life. My technical writing and presentation skills were essentially non-existent earlier, and I owe most of the improvement to the feedback and assistance provided by him.

I am also thankful to Prof. V. K. Katiyar, Head of the Department, and former Heads of the Department, Mathematics for providing the necessary facilities to carry out the research work. My sincere thanks must also go to Prof. Debhasis Ghosh, Department of Electrical and Communication Engineering, Dr. D. N. Pandey, and Prof. Kusum Deep, Chairman, DRC, Department of Mathematics, for sparing their valuable time in reviewing and critically examining my research progress throughout.

My deepest gratitude to Prof. Nuh Aydin, Department of Mathematics, Kenyon College, USA, for his support and guidance during the course of this study. The financial support from Ministry of Human Resource Development, India to carry out this work is thankfully acknowledged.

This acknowledgement would not be complete without thanking my father Mr. Babu Bandi, my mother Mrs. Sulochana Bandi and other family members for their constant support and encouragement. Nothing can compensate the sacrifices made by my best friend, my strength and my lovely wife Rama Devi Bandi. Without her this would not have been possible. Finally, I would also like to thank all my friends who directly or indirectly helped and made my stay at IIT Roorkee more memorable.

Rama Krishna Bandi

List of Figures

List of Tables

Contents

Chapter 1

Introduction

The exchange or communication of information from one person to another is an activity that is as old as mankind. The form of exchange of information is changing with time. In earlier days, people used to communicate information through agents, post cards, telegrams, etc., and in recent years, through telephones, fax, emails, wireless networks such as infrared, bluetooth, wifi, mobile phones, etc. Now, with the information era at hand, the need of communication is more pronounced than ever. As the world becomes more connected, there has been a dramatic increase in the volume of data that is being captured, stored, processed and transmitted as digital information. This has led to an increasing demand for efficient and reliable systems used in the transmission and storage of digital data. The efficient, reliable and secure transmission of information over noisy channels are basic requirements in digital communication and are challenging problems. Coding theory addresses the problem of reliable communication in noisy channels[1]. It is the study of error correcting codes over noisy communication channels and is concerned with developing codes that can detect and correct errors in a digital communication and for which efficient encoding and decoding algorithms exist. Error-correcting codes have become part of routine and are found in all walks of life - ranging from basic home and office appliances like telephones, compact disc players, computer hard disk drives to deep space communication. They are also now used in essentially all hardware-level implementations of smart and intelligent machines, such as scanners, optical devices, and telecom equipments. Apart from this, they are also used

[1] Security is the other concern which is dealt by cryptography.

in cryptography, construction of combinatorial designs, data compression, probabilistically checkable proofs, DNA computing, quantum computing, etc. Hence, in barely more than half a century, it has seen phenomenal growth. Though coding theory has its origins in an engineering problem, however, the subject has been developed by using more and more sophisticated mathematical techniques. Owing to richness of the subject, till date coding theory has been a flourishing subject that benefits from techniques developed in a wide variety of disciplines such as combinatorics, probability, algebra, geometry, number theory, engineering and computer science.

1.1 Coding Theory - Origin and Development

Coding theory originated with the seminal paper "A mathematical theory of communication" of Shannon in 1948 [108], in which he showed that, it is possible to transmit information through a noisy communication channel almost error free at any rate below the capacity of the channel. This fundamental and ground-breaking work signified the beginning of the twin disciplines Information Theory and Coding Theory. However, Shannon's theory is probabilistic rather than constructive. That is, it does not give any information how one can construct the codes that achieve the channel capacity.

At around the same time, his colleague at Bell Labs, Hamming was developing an error correcting scheme. He was frustrated with the computer that halts every time when it detects an error but could not correct it. While addressing the question that why the computer which could detect the errors was unable to correct them automatically, Hamming realized that the basic problem of error correction is to find strings over an alphabet that are in certain sense at a sufficiently large distance from each other. He introduced a famous class of single error correcting codes (named after him as Hamming codes) and defined a metric known as Hamming metric [57], for this purpose. This theory of Hamming is about the actual construction, encoding and decoding of codes and uses tools from areas such as combinatorics and algebra. Though, these codes did not achieve channel capacity as promised by Shannon, they were important as they showed a way to construct codes. In 1949, the first multple error correcting codes (in particular, a triple error correcting binary code [23, 12, 7] and a double error correcting ternary code [11, 6, 5]) were constructed by Golay in his single page research article "Notes on digital coding" [55]. In 1954, Reed and Muller introduced Reed-Muller codes (RM codes) [102] which have many algebraic and combinatorial properties. These were the first codes to be deployed in deep space communication (Mariner 9). Most of the research in coding theory since then is devoted to find good error correcting codes.

A major advance in this area came when Bose and Ray-Choudhuri [27], and Hocquenghem [60] independently found a large class of multiple error correcting codes called BCH Codes. Reed and Solomon [103] found a related class of codes for non-binary channels, named after them as Reed-Solomon (RS) codes which have many interesting properties. Inspired by this advance, many other families of codes have been discovered.

The error correcting capability of a code depends mainly on the minimum distance of the code. Also, for efficient transmission, a code needs to have large number of codewords. Therefore studying the metric and structural properties of a code becomes of paramount importance. Searching for the codes with good parameters is equally important. As a result, many families of codes have been introduced. Cyclic codes is one of the important class of those families. The study of cyclic codes began with two, 1957 and 1959 AFCRL reports by Prange [98,99]. Among all families of codes, cyclic codes are of great importance. This is mainly because they can be efficiently encoded and decoded. Besides this, they have many other interesting properties. Their rich algebraic and combinatorial structure made this class of error correcting codes one of the most prominent classes in coding theory. The well known codes BCH codes, RS codes, RM codes (Punctured), etc., are cyclic codes.

The area of coding theory which mainly uses algebraic tools for the analysis of codes is known as *algebraic coding*. Algebraic coding has become one of the most important and widely applied aspects of abstract algebra. Classically, algebraic codes have been mainly studied in the setting of vector of spaces over finite fields. The study of codes over rings was initiated by Blake in early seventies [23,24]. He first studied cyclic codes over $\mathbb{Z}_m$ using group algebra approach [23], and then he focused on linear codes over $\mathbb{Z}_{p^r}$ [24]. Blake's work was extended further by Spiegel [119, 120], followed by Shankar [107], in which she proposed a construction of BCH codes over integer residue rings using the polynomial approach.

Satyanarana [106] and Wasan [132] also studied codes over integer residue rings. However, the study of codes over rings got attention of researchers mainly after the breakthrough paper of Hammons et al. [58] in 1994, in which they have shown that some important families of non-linear binary codes (Kerdock and Preparata codes) with very good parameters are actually images of some linear codes over $\mathbb{Z}_4$, the ring of integers modulo 4, via a map, called the *Gray map*. The findings of this paper not only led to a new research in this area but also settled a long standing mystery behind the behavior of binary Kerdock and Preparata codes as formal duals of each other [81, Chapter 15]. Some other important papers on codes over $\mathbb{Z}_4$ produced during early nineties are [28, 35, 89].

The outcome of the paper by Hammons et al. [58] had an enormous effect on the coding theory community. People began to think of rings as an acceptable alphabet for coding theory. As a result, a number of papers were published and many properties of codes over some rings were established [19, 25, 30–32, 47, 56, 67, 90, 96, 130, 135]. Initially, a large number of papers were produced studying codes over $\mathbb{Z}_4$ [28, 125–127] but this quickly expanded to consider codes over $\mathbb{Z}_m$ and then to other rings such as Galois rings, finite chain rings, finite polynomial rings, etc [20, 101, 121]. A complete structure of cyclic codes of odd lengths over $\mathbb{Z}_4$ has been given by Pless and Qian in [96]. They have also studied cyclic self-dual codes over $\mathbb{Z}_4$ in [97]. This study has been later generalized to arbitrary ring of integers modulo p^s, p a prime, in [31, 67]. Gupta et al. [56] studied linear codes over $\mathbb{Z}_{2^s}$. Norton and Sălăgean [90], and Dinh and Permouth [45] studied cyclic over a more general setting of finite chain rings. Martínez and Rúa [83, 84] studied codes over finite chain rings in the multi-variable approach. In most of the study of cyclic codes, the length of the cyclic code is relatively prime to the characteristic of the ring. When the length of the code is not relatively prime to the characteristic of the ring, the corresponding cyclic codes are known as repeated root cyclic codes, and they have been well explored over finite fields [12, 33, 41, 44, 51, 87, 105, 109, 122, 128, 142] and also over some finite rings [3, 4, 10, 21, 28, 39, 42, 44, 49, 109, 118, 123, 125, 126] in the literature. The well known codes such as BCH codes, RM codes and RS codes have also been generalized to finite rings [18, 36, 37, 58, 63, 107]. The other families of codes constacyclic, quasi-cyclic codes, quasi-twisted codes, etc., have also been studied over finite rings [17, 38, 75–78].

This study has been carried further by introducing finite polynomial rings as alphabets, such as $\mathbb{F}_2+u\mathbb{F}_2$, $u^2=0$ [26,124], $\mathbb{F}_2+v\mathbb{F}_2$, $v^2=v$ [140], $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, $u^2=v^2=0$, $uv=vu$ [138], $\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p$, $v^3=v$ [79], $\frac{\mathbb{Z}_p[u]}{\langle u^k\rangle}$ [114], etc. The first among them was the ring $\mathbb{F}_2+u\mathbb{F}_2$, $u^2=0$ due to Bachoc [9], in which the ring was used in connections with modular lattices and coding theory. A further study of codes over $\mathbb{F}_2+u\mathbb{F}_2$ was done by Bonnecaze and Udaya in [26], in which they have not only studied cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$, but also got some very good codes over it.

There are interesting connections between $\mathbb{Z}_4$ and $\mathbb{F}_2+u\mathbb{F}_2$. For example, both are local rings of order 4 but of characteristics 4 and 2, respectively. The multiplicative structure of both is same but not the additive one[2]. The ring $\mathbb{F}_2+u\mathbb{F}_2$ has one non-zero non-unit as in $\mathbb{Z}_4$, namely u, and so a comparable Gray map was defined, where u acts 2. However, unlike the Gray map for $\mathbb{Z}_4$, this map is a linear map. The ring $\mathbb{F}_2+u\mathbb{F}_2$ is also used for the construction of optimal frequency hopping sequences [126], this can be considered as an immediate application. This inspired the researchers to introduce new similar ring structures to study codes over them. There is a large number of papers in recent past in this direction [5,6,43,68,117], and as a result some very good codes with parameters better than the existing codes with same length and minimum distance over finite fields have been obtained.

1.2 Motivation to our Investigations

In this section, we present the work that has motivated us to study codes over some non-chain extensions of $\mathbb{Z}_4$. We also present a survey of work that has been done in this direction.

Codes over $\mathbb{Z}_4$ have always remain a topic of special interest, in spite of codes over all the finite rings stated earlier, due to their connections with 4-phase sequences, lattices, design theory, cryptography, etc. Most of the work on codes over polynomial rings described in the previous section is confined to polynomial rings over finite fields. In view of this, recently, Yildiz and Karadeniz [139] have introduced a new ring structure $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$, and

[2] The additive structure of $\mathbb{F}_2+u\mathbb{F}_2$ is same as $\mathbb{F}_4$

studied linear and self-dual codes over it. They have also got some good formally self-dual codes over this ring. This motivated us to introduce two new ring structures $\mathbb{Z}_4 + v\mathbb{Z}_4$, $v^2 = v$ and $\mathbb{Z}_4 + w\mathbb{Z}_4$, $w^2 = 2w$, and to study some families of codes over them. Further, we have extensively studied cyclic and negacyclic codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$.

Given a finite ring, finding a suitable metric for the codes over the ring is always an interesting problem. Algebraic codes have been mostly studied using either Hamming metric or its other variants like generalized Hamming metric, Lee metric, Euclidean metric, homogeneous metric etc. Some non-Hamming metrics like rank metric, psuedo metric, poset metric, m-spotty metric, etc., have also been studied [29, 52, 53, 61, 64, 73, 133]. The Hamming metric and its other variants are well suited for channels in which channel noise generates equiprobable errors. However, not all real world channels are of that nature, especially when the possible errors form patterns of a specific shape. In such situations, a non-Hamming metric, called Rosenbloom-Tsfasman (RT) metric (also known as ρ-metric) is more appropriate, and is a generalization of the classical Hamming metric [82, 104, 116]. In the context of coding theory, the ρ-metric was first introduced by Rosenbloom and Tsfasman [104]. An interesting point to be noted here is that while studying codes with respect to RT metric, the ρ-weight enumerators of the duals of two linear codes with same ρ-weight enumerator may be different. This is not the case with Hamming weight enumerator.

Dougherty and Skriganov [50] have identified this problem and mentioned the need to search for more adequate definitions for weight enumerators. The problem has been resolved by them by considering orbits of a linear group preserving the ρ-weight (which is a method actually proposed by Skriganov in [115, Section 4.4]). Siap [111] addressed the same problem by defining the complete weight enumerator, which preserves the order of the entries of matrices. Siap [111] proved the MacWilliams identity for complete ρ-weight enumerator of a linear code in $\mathcal{M}_{m\times s}\langle\mathbb{F}_q\rangle$, and later he proved the same for linear codes in $\mathcal{M}_{m\times s}(R)$, where $R = \mathbb{F}_q[u]/\langle u^r - a\rangle$ with $a \in \mathbb{F}_q$ in [112]. Siap and Özen [113] further generalized this result to linear codes in $\mathcal{M}_{m\times s}(R)$, where R a finite commutative ring. With respect to the RT metric, Özen and Siap [91–93] studied the structure of linear codes in $\mathcal{M}_{m\times s}(R)$ when R is either a finite field or $\mathbb{F}_q[u]/\langle u^s\rangle$ or a Galois ring. Zhu and Xu [141] defined the *Lee complete* ρ-weight enumerator and the *exact complete* ρ-weight enumerator of a linear code in $\mathcal{M}_{m\times s}(\mathbb{Z}_4)$, and also derived the MacWilliams identity for each of these enumerators. This inspired us to study linear codes over $\mathbb{Z}_4+v\mathbb{Z}_4$, $v^2=v$. We have derived a MacWillaims type identity for linear codes over $\mathbb{Z}_4+v\mathbb{Z}_4$ with respect RT weight using an approach similar to that of [111]. Further, we have studied linear codes $\mathbb{Z}_4+v\mathbb{Z}_4$ with respect to Lee and Gray metrics and obtained MacWillaims identities with respect to these metrics.

Self-dual codes are an interesting class of codes as they often produce optimal codes and have many links to the other areas of mathematics such as lattices, t-designs, Hadamard matrices and quantum stabilizer codes. The search for self-dual codes with good parameters is an interesting problem in coding theory. Self-dual codes and their constructions over finite fields have been studied extensively [59, 69, 70, 72, 74]. Recently, several construction methods for self-dual codes over finite rings have also been proposed [71, 72]. Alfaro and Dhul-Qarnayn [6] proposed a more general method for constructing self-dual codes over $\frac{\mathbb{F}_q[u]}{\langle u^t\rangle}$ and over finite chain rings, through which one can obtain the self-dual codes obtained by methods proposed in [69–71]. As a result many new self-dual and formally self-dual codes are obtained. This motivated us to characterize self-dual codes over $\mathbb{Z}_4+v\mathbb{Z}_4$, $v^2=v$ and $\mathbb{Z}_4+w\mathbb{Z}_4$, $w^2=2w$. We have proposed a construction method for constructing self-orthogonal and self-dual codes over $\mathbb{Z}_4+v\mathbb{Z}_4$ and $\mathbb{Z}_4+w\mathbb{Z}_4$.

Cyclic codes are amongst the most studied algebraic codes. Their structure over finite chain rings is now well known [90]. As was stated earlier, there are a lot of papers in recent years on cyclic codes over different finite rings [5,26,43,68,96,110,114,138]. However, cyclic codes over local non-chain rings are not much explored. This led us to explore cyclic codes over the local non-chain ring $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$. We have explored cyclic codes and their structural properties over $\mathbb{Z}_4+u\mathbb{Z}_4$.

Another family of codes that we have considered in this thesis is negacyclic codes. Negacyclic codes were first introduced by Berkelamp [15]. Wolfmann [134] generalized negacyclic codes of odd lengths to $\mathbb{Z}_4$. Blackford [22] extended the results of [134] to negacyclic codes of even length over $\mathbb{Z}_4$, and determined all binary linear repeated root cyclic codes that are Gray images of quaternary codes. Dinh and Lopez-Permouth [45] studied negacyclic codes of odd length in the more general setting of finite chain rings, and also considered repeated root cyclic codes of length 2^s over $\mathbb{Z}_{2^m}$. The structure of negacyclic codes of length 2^s over Galois rings and their complete Hamming distances were discussed by Dinh in [39,40]. Constacylic codes of lengths 2^s and p^s over Galois extension of $\mathbb{F}_2+u\mathbb{F}_2$, $u^2=0$ and $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, $u^2=0$, respectively, have been studied by Dinh in [42, 43]. We have classified negacyclic codes of both odd and even lengths over $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$ and found some good $\mathbb{Z}_4$-codes via the Gray map.

Recently, few researchers have also worked on some non-chain ring extensions of $\mathbb{Z}_4$. The first among them was the paper by Yildiz and Aydin [136], in which they have obtained some new $\mathbb{Z}_4$-codes as Gray images of cyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$. Martínez et al. [86], have studied linear code over $\frac{\mathbb{Z}_4[x]}{\langle x^2-2x\rangle}$ and also considered quaternary RM codes in 2015. Luo and Udaya have studied self-dual cyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$ [80]. In 2016, Özen et al. [94] have discussed cyclic and constacyclic codes over $\frac{\mathbb{Z}_4[x]}{\langle x^2-1\rangle}$ and obtained few new $\mathbb{Z}_4$-codes via the Gray map. The ring $\frac{\mathbb{Z}_4[x]}{\langle x^2-1\rangle}$ is in fact isomorphic to $\frac{\mathbb{Z}_4[x]}{\langle x^2-2x\rangle}$. Gao et al. [54] have studied linear codes over $\mathbb{Z}_4+v\mathbb{Z}_4$, $v^2=v$ and generated many new $\mathbb{Z}_4$-codes (optimal in some cases) from the self-dual codes over $\mathbb{Z}_4+v\mathbb{Z}_4$.

Recently, in 2015, Martínez and Szabo [85] have classified all local rings of order 16 up to isomorphism. They have proved that there only seven local non-chain rings of order 16. Dougherty et al. [46] have studied linear codes over these seven local non-chain rings and have also given the form of a generator matrix of linear codes over these rings. They derived MacWilliams identities and also considered self-dual codes over them. The local non-chain rings $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$ and $\mathbb{Z}_4+w\mathbb{Z}_4$, $w^2=2w$, which we have used in this, are among them. This is the work that has been done so far on non-chain extensions of $\mathbb{Z}_4$.

1.3 Objective of the thesis and our contribution

Objective of the thesis: The objective of this thesis is to study codes over some non-chain extensions of $\mathbb{Z}_4$ such as $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$, $\mathbb{Z}_4+w\mathbb{Z}_4$, $w^2=2w$ and $\mathbb{Z}_4+v\mathbb{Z}_4$, $v^2=v$, and to explore their properties. By making use of their structural properties, we also aim to search for some optimal/good binary or $\mathbb{Z}_4$ codes.

Our contribution:

- We have introduced the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$, $v^2 = v$, and studied codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ with respect to Lee, Gray and RT metrics and also characterized the self-dual codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$.

- Introduced another ring $\mathbb{Z}_4 + w\mathbb{Z}_4$, $w^2 = 2w$, and studied self-codes over it. Proposed some construction methods for self-dual codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$.

- Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$, are well explored. We have presented the structure of cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and their generators. We have also obtained a minimal spanning set for such codes and determined their ranks.

- Characterized negacyclic codes of even lengths (in particular of length 2^k) over $\mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$, and obtained their duals. Also determined a mass formula for number of negacyclic codes of length 2^k over $\mathbb{Z}_4 + u\mathbb{Z}_4$.

- Using the classification of negacyclic codes and Magma Computational Algebra System, we have found some new $\mathbb{Z}_4$-codes via the Gray map.

1.3.1 Structure of the Thesis

The thesis is organized as follows.

Chapter 1 gives an introduction to coding theory and its development, and also its recent advances. The literature related to the topics discussed in the thesis are also covered here.

Chapter 2 covers most of the preliminaries which are required to understand the content of the thesis. We have given the literature review of the topics discussed in this chapter at appropriate places. Section 2.2 discusses some basic and known results of algebraic codes over finite fields including RT metric. In Section 2.3, we discuss some local rings and their properties. In particular, basic properties of Galois rings are discussed. We also briefly discuss linear and cyclic codes over $\mathbb{Z}_4$.

In **Chapter 3**, Section 3.2, we introduce the ring $\mathbb{Z}_4+v\mathbb{Z}_4$, $v^2 = v$ and define a Gray map. Section 3.3 discusses the study of linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$. MacWillaims type identities for codes over $\mathbb{Z}_4+v\mathbb{Z}_4$, with respect to Lee and Gray metrics, are obtained in Section 3.4, and with respect to RT metric, are obtained in Section 3.5. Some characterizations of self-dual codes over $\mathbb{Z}_4+v\mathbb{Z}_4$ are provided. Some constructions of self-dual and self-orthogonal. codes over $\mathbb{Z}_4+v\mathbb{Z}_4$ are given in Section 3.6.

Chapter 4 covers codes over the ring $\mathbb{Z}_4+w\mathbb{Z}_4$, $w^2=2w$. Section 4.2 introduces the ring and studies linear codes over the same. Some characterizations of self-dual codes over $\mathbb{Z}_4+w\mathbb{Z}_4$ are provided in Section 4.3. A new construction method for constructing self-dual codes over $\mathbb{Z}_4+w\mathbb{Z}_4$ is presented. Also, circulant self-dual codes are briefly discussed. In Section 4.4, Type II codes over $\mathbb{Z}_4+w\mathbb{Z}_4$ are briefly discussed.

In **Chapter 5**, we introduce the ring $\mathbb{Z}_4+u\mathbb{Z}_4$ and codes over it in Section 5.2. In Section 5.3, we describe the Galois ring extension of $\mathbb{Z}_4+u\mathbb{Z}_4$ and provide its ideal structure. In Section 5.4, we first consider cyclic codes of odd lengths and obtain their structure through the factorization of x^n-1, n an odd integer, over $\mathbb{Z}_4+u\mathbb{Z}_4$. Next, the general form of the generators of cyclic codes of arbitrary lengths over $\mathbb{Z}_4+u\mathbb{Z}_4$ is provided and the complete ideal structure of $\frac{(\mathbb{Z}_4+u\mathbb{Z}_4)[x]}{\langle x^{2^k}-1\rangle}$ is obtained. In Section 5.5, a minimal spanning set for cyclic codes of arbitrary length over $\mathbb{Z}_4+u\mathbb{Z}_4$ is obtained and formula for their ranks is determined. Also, we provide a necessary condition and a sufficient condition for principally generated cyclic codes to be free modules over $\mathbb{Z}_4+u\mathbb{Z}_4$.

Chapter 6 presents a study of negacyclic codes of both odd lengths and even lengths over $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$. In Section 6.2, we discuss negacyclic codes of odd lengths over $\mathbb{Z}_4+u\mathbb{Z}_4$ and thier properties. We classify negacyclic codes of length 2^k over $\mathbb{Z}_4+u\mathbb{Z}_4$ and derive a mass formula for the total number of negacyclic codes of length 2^k over $\mathbb{Z}_4+u\mathbb{Z}_4$ in Section 6.4. Further, in Section 6.5, we generalize the study of negacyclic codes of length 2^k to negacyclic codes of any even length over $\mathbb{Z}_4+u\mathbb{Z}_4$.

In **Chapter 7** Section 7.2, we obtain the duals of negacyclic codes of length 2^k over $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=0$, and classify all negacyclic codes $\mathcal{C}$ of length 2^k over $\mathbb{Z}_4+u\mathbb{Z}_4$ satisfying $\mathcal{C}\subset A(\mathcal{C})$ and $\mathcal{C}=A(\mathcal{C})$, where $A(\mathcal{C})$ is the annihilator of $\mathcal{C}$. Section 7.3 presents a mass formula for the number of negacyclic codes $\mathcal{C}$ of length 2^k over $\mathbb{Z}_4+u\mathbb{Z}_4$ satisfying $\mathcal{C}=A(\mathcal{C})$. In Section 7.4, we present some new $\mathbb{Z}_4$-linear codes which are obtained as the Gray images of negacyclic codes of length 2^k over $\mathbb{Z}_4+u\mathbb{Z}_4$ by a computer search using

Magma Computational Algebra System.

Finally in **Chapter 8**, we conclude the results, and give some suggestions and directions for further research on the families of codes studied in this thesis.

Chapter 2

Basic Concepts

2.1 Block Codes

Coding Theory deals with the problem of detecting and correcting errors caused by noise during transmission of information through a communication channel (or a date storage device). A typical communication system may be represented by the block diagram shown in Figure 2.1.

Consider a scenario that some information is to be transmitted from a source (S_1) to a sink (S_2) through a communication channel. In coding theory, we are not concerned about the source encoding. So we ignore the concerns of source coding, or in other, words presume that the information to be transmitted is already source coded. We are also not concerned about the modulation and demodulation in the construction of error correcting codes. Therefore the above communication system can be put in the form shown in Figure

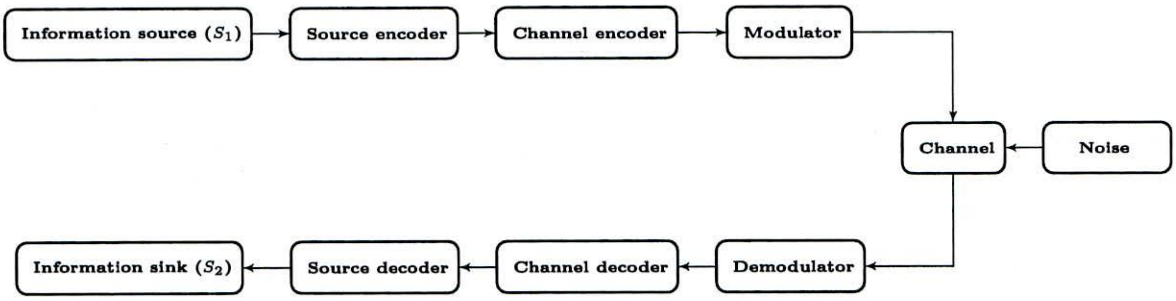

Figure 2.1: Block diagram of a communication system.

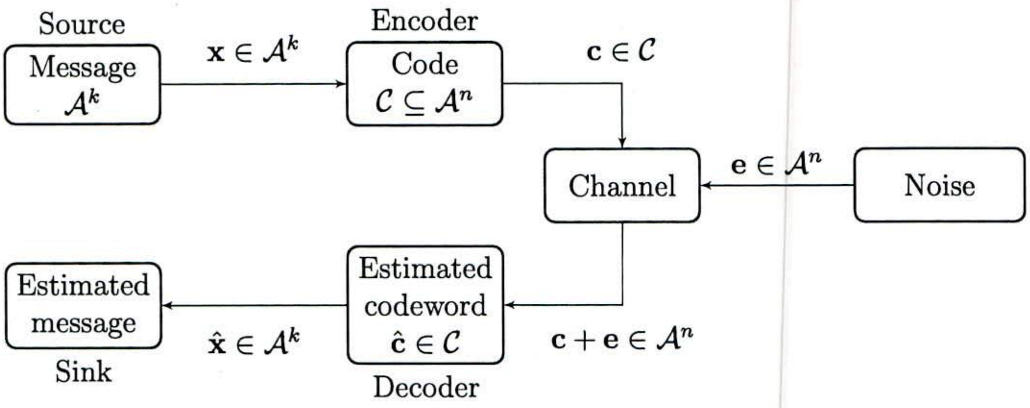
Source
Message
$\mathcal{A}^k$
$\mathbf{x} \in \mathcal{A}^k$
Encoder
Code
$\mathcal{C} \subseteq \mathcal{A}^n$
$\mathbf{c} \in \mathcal{C}$
Channel
$\mathbf{e} \in \mathcal{A}^n$
Noise
$\mathbf{c} + \mathbf{e} \in \mathcal{A}^n$
Estimated
codeword
$\hat{\mathbf{c}} \in \mathcal{C}$
Decoder
$\hat{\mathbf{x}} \in \mathcal{A}^k$
Estimated
message
Sink

Figure 2.2: Schematic diagram of a communication system.

2.2.

We consider the information transmitted through the channel as a sequence of symbols from some finite alphabet $\mathcal{A}$. Two structurally different codes that are commonly used for this purpose are *block codes* and *convolutional codes*. In this thesis we consider only block codes. To transmit the data through a communication channel using block codes, the information sequence is chopped into blocks of length k. These blocks of length k are called the message blocks. These message blocks are thus the elements of $\mathcal{A}^k$. If these messages blocks are directly transmitted through the noisy channel, it is impossible to determine whether the information received is error free. So the basic idea for error correction is to add some extra symbols to the message blocks so that even if the information is corrupted during transmission, the message is still be recovered. Thus redundancy is added to each message block so that its length becomes $n \geq k$. These new blocks of length n are called codewords, and the set of all such codewords is called a *block code*. Thus a block code $\mathcal{C}$ of length n is a subset of $\mathcal{A}^n$. The redundancy is added to message blocks based on proper rules and this process is called *encoding*, which is a bijective function from $\mathcal{A}^k$ to $\mathcal{C}$. We make another assumption that the codeword transmitted through the channel at a given point of time depends only upon the current message but not on the codewords previously transmitted. We say that an error has occurred during the transmission, if a codeword $c \in \mathcal{C}$ is transmitted and a word $x \in \mathcal{A}^n$ is received, and $x \neq c$. To correct the errors, it is assumed that errors at a fewer coordinate positions of a codeword are more likely than errors at a large number of coordinate positions. A distance function $d(.,.)$, called the *Hamming distance*, is defined on $\mathcal{A}^n$, to find the error correcting capability of a code.

Definition 2.1.1. *The Hamming distance $d(x,y)$ between any two words $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ of $\mathcal{A}^n$ is defined to be the number of coordinate positions at which x and y differ, i.e.,*

$$d(x,y) = |\{i \ : \ x_i \neq y_i\}| \ .$$

It is easy to see that d is a metric on $\mathcal{A}^n$. The *minimum Hamming distance* $d_H(\mathcal{C})$ of a code $\mathcal{C}$ is the smallest distance between any two of its distinct codewords, i.e.,

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

If a code has minimum distance d_H then it can detect up to $d_H - 1$ errors or correct up to $\lfloor \frac{d_H - 1}{2} \rfloor$ errors.

Another important parameter of a code is the *Hamming weight.*

Definition 2.1.2. *The Hamming weight $wt(c)$ of a codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ is the number of its nonzero coordinates, i.e.,*

$$wt(c) = |\{i \ : \ c_i \neq 0, c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}\}| \ .$$

The *minimum Hamming weight* of a code is the smallest weight of its nonzero codewords.

$$wt_H(c) = \min\{wt(c) \ : \ 0 \neq c \in \mathcal{C}\} \ .$$

For x, $y \in \mathcal{A}^n$, $d(x,y) = wt(x-y)$. The *rate* of code $\mathcal{C}$ is defined as $\frac{\log_{|\mathcal{A}|} |\mathcal{C}|}{n}$. For a good error correcting capability of a code, it needs to have a large minimum distance, and for the efficient transmission of information, the code should contain a large number of codewords. Hence for effective communication, the code $\mathcal{C}$ should have as large a cardinality as possible and minimum distance as large as possible. These are two conflicting aims. This leads us to the fundamental question of coding theory "What is the largest subset of $\mathcal{A}^n$ such that any two of its elements are at least d_H apart ?"

2.2 Codes over Finite Fields

2.2.1 Linear Codes

In classical coding theory, codes have been studied over finite fields. In fact, in most of the communication systems binary codes are being used. Block codes are mainly of two types, linear and non-linear. Though in some cases there are better non-linear codes than linear codes of same lengths, linear codes are used mostly in practice, because it is difficult to say much about the structure of a non-linear code, and linear codes are efficient to implement in practice. The well known codes such as Hamming codes, BCH codes, Reed Solomon codes, Reed Muller codes, Golay codes etc., are linear codes.

Let $\mathbb{F}_q$, $q = p^m$, p a prime and m a positive integer, be a finite field. A *linear code* $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$. If the $\mathbb{F}_q$-dimension of $\mathcal{C}$ is k, then we say that $\mathcal{C}$ is an $[n, k]$ linear code over $\mathbb{F}_q$. If an $[n, k]$ linear code has minimum distance d, then we say that $\mathcal{C}$ is an $[n, k, d]$ linear code. The rate of an $[n, k]$ linear code is k/n. For linear codes, the minimum weight and the minimum distance coincide. So, it is relatively easy to find the minimum distance of the code. This is one great advantages of using linear codes.

From linear algebra it is well known that any linear subspace of a finite dimensional space is completely determined by its basis. So any linear code of length n over $\mathbb{F}_q$ can be completely determined by its basis. A $k \times n$ matrix G, whose rows form a basis for $\mathcal{C}$ is called a *generator matrix* of $\mathcal{C}$. A message block $\overline{m} \in \mathbb{F}_q^k$ can be encoded into the corresponding codeword $c \in \mathbb{F}_q^n$ as

$$c = \overline{m}G\ .$$

A set of coordinate positions corresponding to any k linearly independent columns of G is called an *information set*. A linear code may have more than one generator matrix. However, if the first k coordinate positions form an information set, then the linear code $\mathcal{C}$ has a unique generator matrix G of the form $G = [I_k, A]$, where I_k is a $k \times k$ identity matrix and A is a $k \times (n-k)$ matrix, i.e., the first k columns of G are linearly independent. Such a generator matrix is said to be in standard form.

For any two elements $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ of $\mathbb{F}_q^n$, we define natural inner product x · y as,

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \ .$$

Two elements x, y of $\mathbb{F}_q$ are said to be *orthogonal* if $x \cdot y = 0$. If $\mathcal{C}$ is an $[n, k]$ linear code over $\mathbb{F}_q$, then the set of all vectors of $\mathbb{F}_q^n$ which are orthogonal to every codeword of $\mathcal{C}$ is called the *dual* of $\mathcal{C}$ and is denoted by $\mathcal{C}^{\perp}$, i.e.,

$$\mathcal{C}^{\perp} = \{x \in \mathbb{F}_q^n \mid x \cdot c = 0, \ \forall \ c \in \mathcal{C}\}$$

We know from linear algebra that $\mathcal{C}^{\perp}$ is a subspace of $\mathbb{F}_q^n$ of dimension $n-k$. Thus, $\mathcal{C}^{\perp}$ is an $[n, n-k]$ linear code over $\mathbb{F}_q$. A generator matrix H of $\mathcal{C}^{\perp}$ is called a parity check matrix of $\mathcal{C}$. Then it follows that $GH^T = 0$, where H^T is the transpose of H. If the generator matrix G of $\mathcal{C}$ is in standard form $G = [I_k, A]$, then it easy to deduce that $H = [-A^T, I_{n-k}]$. A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can also be described completely by its parity check matrix H, i.e.,

$$\mathcal{C} = \{c \in \mathbb{F}_q^n \mid Hc^T = 0\} \ .$$

This leads to an important theorem given below.

Theorem 2.2.1. *[61] Let $\mathcal{C}$ be a linear code with parity check matrix H. Then $\mathcal{C}$ has minimum distance d if and only if every $d-1$ columns of H are linearly independent.*

Further, if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, then $\mathcal{C}$ is called a *self-orthogonal code*, and if $\mathcal{C} = \mathcal{C}^{\perp}$, then $\mathcal{C}$ is called a *self-dual code.* If $\mathcal{C}$ is a self-dual code of length n, then n must be even and the dimension of $\mathcal{C}$ is $\frac{n}{2}$.

2.2.2 MacWilliams Identity

MacWilliams identity is one of the most celebrated results in coding theory, which shows that, for a given code, how to get the weight distribution of its dual. Let $\mathcal{C}$ be a code of length n over $\mathbb{F}_q$, and let A_i be the number of codewords of weight i. Then, the list A_i is called the *weight distribution* or *weight spectrum* of $\mathcal{C}$. Weight distribution of a code gives useful insights about the structure of the code. We call the polynomial

$$W_{\mathcal{C}}(x,\ y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

the weight enumerator of $\mathcal{C}$. This can also be written as

$$W_{\mathcal{C}}(x,\ y) = \sum_{c\in\mathcal{C}} x^{n-wt(c)} y^{wt(c)}$$

Theorem 2.2.2. *[81, Theorem 13][MacWilliams identity]*

$$W_{\mathcal{C}^\perp}(x,y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x+(q-1)y, x-y)\ .$$

2.2.3 Rosenbloom-Tsfasman Metric

In the classical coding scheme, codes are investigated with respect to the Hamming metric [81]. This metric is well suited for channels in which channel noise generates equiprobable errors. However, not all real world channels are of that nature, especially when the possible errors form patterns of a specific shape. In such situations, a non-Hamming metric, called Rosenbloom-Tsfasman (RT) metric, also known as ρ-metric, is more appropriate, and is a generalization of the classical Hamming metric [82, 104, 116].

In the context of coding theory, the ρ-metric was first introduced by Rosenbloom and Tsfasman [104]. In the context of the theory of uniform distributions, this metric was introduced by Martin and Stinson [82] and by Skriganov [115, 116]. We refer to [116] for further discussion on this topic.

The Rosenbloom-Tsfasmann (RT) metric is defined as follows:

Let $\mathcal{M}_{n\times s}(\mathbb{F}_q)$ denote the set of all matrices of order $n \times s$ over $\mathbb{F}_q$. For any $x = (x_1, x_2, \ldots, x_s) \in \mathcal{M}_{1\times s}(\mathbb{F}_q) = \mathbb{F}_q^s$. Define

$$w_N(x) = \begin{cases} \max\{i \mid x_i \neq 0, 1 \leq i \leq s\} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases} \tag{2.2.1}$$

The RT-distance or ρ-distance between $x = (x_1, x_2, \ldots, x_s)$, $y = (y_1, y_2, \ldots, y_s) \in \mathbb{F}_q^s$ is defined as $d_N(x,\ y) = w_N(x - y)$. If $X = [X_1, X_2, \ldots, X_n]^T \in \mathcal{M}_{n\times s}(\mathbb{F}_q)$ $(\equiv \mathbb{F}_q^{n\times s})$, where $X_j = (x_{j1}, x_{j2}, \ldots, x_{js}) \in \mathbb{F}_q^s$ denotes the j^{th} row of X, then the RT-weight and RT-distance in $\mathcal{M}_{n\times s}(\mathbb{F}_q)$ are defined respectively, as

$$w_N(X) = \sum_{j=1}^{n} w_N(X_j) \tag{2.2.2}$$

$$d_N(X,\ Y) = w_N(X - Y), \quad \forall\ X,\ Y \in \mathcal{M}_{n\times s}(\mathbb{F}_q)\ . \tag{2.2.3}$$

One can easily check that d_N is a metric on $\mathcal{M}_{n\times s}(\mathbb{F}_q)$. For $s = 1$, the RT metric is just the Hamming metric.

Example 2.2.3. *Let* $X = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 0 & 0 \end{bmatrix} \in \mathcal{M}_{n\times s}(\mathbb{F}_q)$. *Then* $w_N(P) = w_N((1,\ 0,\ 1)) + w_N((2,\ 0,\ 0)) = 3 + 1 = 4$. *If* $Y = (1,\ 2)^T$ *and* $w_N(Y) = 2 = w_H(Y)$.

The *minimum RT-weight* $w_N(\mathcal{C})$ and *minimum RT-distance* $d_N(\mathcal{C})$ of a code $\mathcal{C}$ are defined as follows:

$$\begin{aligned} w_N(\mathcal{C}) &= \min\{w_N(X) \mid X \in \mathcal{C},\ X \neq 0\} \\ d_N(\mathcal{C}) &= \min\{d_N(X,\ Y) \mid X, Y \in \mathcal{C},\ X \neq Y\}\,. \end{aligned} \tag{2.2.4}$$

It is easy to see that

$$w_H(X) \leq w_\rho(X) \leq s \times w_H(X) \tag{2.2.5}$$

MacWilliams Duality and Weight Enumerators in RT-metric

For a given linear code $\mathcal{C} \subseteq \mathcal{M}_{n\times s}(\mathbb{F}_q)$, the following set of non-negative integers

$$w_r(\mathcal{C}) = |\{X \in \mathcal{C} : w_N(X) = r\}|,\ 0 \leq r \leq ns \tag{2.2.6}$$

is called the ρ-weight (or RT-weight) spectrum of the code $\mathcal{C}$. The ρ-weight enumerator of $\mathcal{C}$ is defined as

$$W_{\mathcal{C}}(z) = \sum_{r=0}^{ns} w_r(\mathcal{C}) z^r = \sum_{X\in\mathcal{C}} z^{w_N(X)}. \tag{2.2.7}$$

Now we introduce an inner product on $\mathcal{M}_{n\times s}(\mathbb{F}_q)$. First, let $n = 1$, and $x = (x_1, x_2, \ldots, x_s)$ and $y = (y_1, y_2, \ldots, y_s)$ in $\mathcal{M}_{1\times s}(\mathbb{F}_q)$. Then the inner product of x, y is

$$\langle x,\ y\rangle = \langle y,\ x\rangle = \sum_{i=1}^{s} x_i y_{s-i+1}. \tag{2.2.8}$$

Now let $X = (X_1, X_2, \ldots, X_n)^T$ and $Y = (Y_1, Y_2, \ldots, Y_n)^T$ be two elements of $\mathcal{M}_{n\times s}(\mathbb{F}_q)$, $X_i, Y_i \in \mathcal{M}_{1\times s}(\mathbb{F}_q)$, $1 \le i \le n$. Then we define

$$\langle X,\ Y\rangle = \langle Y,\ X\rangle = \sum_{i=1}^{n} \langle X_i,\ Y_i\rangle. \tag{2.2.9}$$

Note that the inner product defined above is different from the usual inner product defined earlier. The choice of this inner product is due to the following reasons. First, it leads to the MacWilliams identities given in [50, Theorems 3.1 and 3.2], secondly, it was shown in [116, Theorem 4.1] that if C is a linear MDS code with respect to the RT-metric, then $C^{\perp}$ (given by this inner product) is also an MDS code. In general, this theorem fails for other choices of inner products. For a given linear code $\mathcal{C} \in \mathcal{M}_{n\times s}(\mathbb{F}_q)$, its dual code $\mathcal{C}^{\perp} \in \mathcal{M}_{n\times s}(\mathbb{F}_q)$ is defined by

$$\mathcal{C}^{\perp} = \{Y \in \mathcal{M}_{n\times s}(\mathbb{F}_q) : \langle Y,\ X\rangle = 0 \text{ for all } X \in \mathcal{C}\}. \tag{2.2.10}$$

It is obvious that $C^{\perp}$ is also a linear code, and $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

It is worth noting here that the duals of two codes $\mathcal{C}_1$, $\mathcal{C}_2$ may have different ρ-weight enumerators even if the ρ-weight enumerators of $\mathcal{C}_1$, $\mathcal{C}_2$ are same. This is not the case with Hamming weight enumerator. For example, consider two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $\mathcal{M}_{n\times s}(\mathbb{F}_2)$

$$\mathcal{C}_1 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \right\}, \text{ and } \mathcal{C}_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}. \tag{2.2.11}$$

Both codes have ρ-weight enumerator

$$W_{\mathcal{C}_1}(z) = W_{\mathcal{C}_2}(z) = 1 + z^2. \tag{2.2.12}$$

The dual codes $\mathcal{C}_1^{\perp}$ and $\mathcal{C}_2^{\perp}$ of $\mathcal{C}_1$, $\mathcal{C}_2$ are

$$\mathcal{C}_1^{\perp} = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \right\},$$

and

$$\mathcal{C}_2^{\perp} = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\},$$

respectively. The ρ-weight enumerators for $\mathcal{C}_1^{\perp}$ and $\mathcal{C}_2^{\perp}$ turn out to be different:

$$\begin{aligned} W_{\mathcal{C}_1^{\perp}}(z) &= 1 + 4z^4 + 2z + z^2 \\ W_{\mathcal{C}_2^{\perp}}(z) &= 1 + 2z^4 + z^3 + 3z^2 + z \end{aligned} \tag{2.2.13}$$

Thus, we observe that the ρ-weight enumerators (2.2.12) and (2.2.13) cannot be related by a MacWilliams type identity.

Dougherty and Skriganov [50] have identified this problem and mentioned the need to search for more adequate definition for weight enumerators in this setting. The problem has been resolved by them by considering orbits of a linear group preserving the ρ-weight (which is a method actually proposed by Skriganov in [115, Section 4.4]).

Siap [111] addressed the same problem by defining the complete weight enumerator, which preserves the order of the entries of the matrices. We have used the same approach to derive MacWilliams type identity over $\mathbb{Z}_4 + v\mathbb{Z}_4$, $v^2 = v$ in Chapter 3.

2.2.4 Cyclic Codes

A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is called a *cyclic code* if every left/right cyclic shift of every codeword of $\mathcal{C}$ is again a codeword in $\mathcal{C}$, i.e.,

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \implies (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}, \;\; \forall\, (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$$

To get an algebraic description, we associate to each codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ a polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]$. For codewords in $\mathcal{C}$, we use both polynomial and vector notations interchangeably. Then the cyclic shift of $c \in \mathcal{C}$ corresponds to $xc(x) \pmod{x^n - 1}$. This implies that $a(x)c(x) \in \mathcal{C}$ for any $a(x) \in \mathbb{F}_q[x]$. In polynomial presentation, the cyclic code $\mathcal{C}$ is an ideal of the quotient ring $R_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}$. The elements of R_n are residue classes $a(x) + \langle x^n - 1\rangle$, $a(x) \in \mathbb{F}_q[x]$, $\deg a(x) < n$. For convenience, we simply write $a(x)$ for the residue class $a(x) + \langle x^n - 1\rangle$ throughout this thesis. R_n is a principal ideal domain. Therefore, a cyclic code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a principal ideal of R_n. Thus there exists a unique monic polynomial $g(x)$ of smallest degree in $\mathcal{C} \neq 0$ such that $\mathcal{C} = \langle g(x)\rangle$, and such a $g(x)$ is called the *generator polynomial* of $\mathcal{C}$. If $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_{n-k}x^{n-k}$, $g_{n-k} \neq 0$, then $\mathcal{C}$ has dimension k and the set $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ is a basis for $\mathcal{C}$. Hence, a generator matrix for $\mathcal{C}$ is given by

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & \\ & & \ddots & \ddots & & \ddots & \\ 0 & & & g_0 & \cdots & & g_{n-k} \end{pmatrix} \longleftrightarrow \begin{pmatrix} g(x) & & & \\ & xg(x) & & \\ & & \ddots & \\ & & & x^{k-1}g(x) \end{pmatrix}$$

It is easy to show, by the division algorithm, that $g(x)$ divides $x^n - 1$. Therefore, the study of cyclic codes of length n over $\mathbb{F}_q$ depends on the factorization of $x^n - 1$ over $\mathbb{F}_q$. The polynomial $x^n - 1$ can have either repeated irreducible factors or distinct irreducible factors. In the literature, much attention has been given to the latter case, as they often produce codes with better parameters.

Distinct roots cyclic codes

In this section, we consider the code length n to be relatively prime to q. It is well known that $x^n - 1$ has distinct irreducible factors if and only if $(n,q) = 1$. We assume that $(n,q) = 1$ in the rest of this subsection.

Since $g(x)$ is a divisor of $x^n - 1$, there exist a monic polynomial $h(x) \in \mathbb{F}_q[x]$ of degree k such that $x^n - 1 = g(x)h(x)$. Then, $g(x)h(x) = 0$ in R_n. It follows immediately that $c(x) \in \mathcal{C}$ if and only if $c(x)h(x) = 0$ in R_n. Hence $\mathcal{C}$ can be determined simply by the polynomial $h(x)$. $h(x)$ is called the *check polynomial* of $\mathcal{C}$. The reciprocal polynomial $h^*(x) = x^k h(x^{-1})$ of $h(x)$ is a generator polynomial of the dual code $\mathcal{C}^\perp$. A generator matrix for $\mathcal{C}^\perp$, and hence a parity check matrix for $\mathcal{C}$, is given by

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & \\ & & \ddots & \ddots & & \ddots & \\ 0 & & & h_k & \cdots & & h0 \end{pmatrix}.$$

If $x^n - 1$ has t distinct irreducible factors over $\mathbb{F}_q$, then there are 2^t cyclic codes of length n over $\mathbb{F}_q$. Since the generator polynomial $g(x)$ of a cyclic code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a factor of $x^n - 1$, $\mathcal{C}$ can be specified by requiring that all polynomials (codewords) in $\mathcal{C}$ have certain nth roots of unity as zeros. Since $(n,q) = 1$, there exists a smallest extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$, which contains a primitive nth root of unity α. If $M_s(x)$ is the minimal polynomial of the nth root of unity α^s, then all the roots of $M_s(x)$ are $\alpha^i, i \in C_s$, where C_s is the q-cyclotomic coset mod n containing s. A q-cyclotomic coset modulo n containing s is a set defined as $\{s, qs, q^2 s, \ldots, q^{l-1}s\}$, where $s \equiv q^l s \pmod{n}$. Thus, the roots of any factor of $x^n - 1$ are contained in a union of q-cyclotomic cosets modulo n. Let $g(x)$ has roots $\{\alpha^i,\ i \in T\}$, where T is a union of q-cyclotomic cosets modulo n. Then

$$g(x) = lcm_{i \in T}\left(M_i(x)\right)\ ,$$

and $\mathcal{C}$ can be described as

$$\mathcal{C} = \{a(x) \in R_n \mid a(\alpha^i) = 0,\ i \in T\}\ .$$

T is called the *defining set* of $\mathcal{C}$, and the nth roots of unity $\{\alpha^i, \mid i \in T\}$, are called the *zeros* of $\mathcal{C}$.

Theorem 2.2.4 (BCH Bound). *If α is a primitive nth root of unity and the generator polynomial $g(x)$ of a cyclic code $\mathcal{C}$ of length n over $\mathbb{F}_q$ has the $\delta - 1$ consecutive powers $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ of α among its roots, then $d_H(\mathcal{C}) \geq \delta$.*

Repeated root cyclic codes

Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$. Assume that n is not relatively prime to q, i.e., $(n, q) \neq 1$. Then, for some odd integer m, $(x-1)^{p^k m} = (x^m - 1)^{p^k}$. So the generator polynomial of $\mathcal{C}$ will have repeated roots. Such codes are known as repeated root cyclic codes. Repeated root cyclic codes were first considered by Berman [16] in 1967 and then by Massey et. al [87], Falkner et. al [51], and Roth and Seroussi [105]. The concatenated construction of repeated root cyclic codes over finite fields was proved by Castangoli et. al [33] and Van Lint [128] independently in 1990. They also proved that the repeated root cyclic codes are asymptotically bad. However, they are optimal in some cases, and they use low complexity decoding algorithms. This motivated researchers to further investigate this class of codes (see [122] and [142] for more information). Recently, Dinh [41] has given the structure of cyclic codes of length p^s over $\mathbb{F}_q$ and also determined the Hamming weight distribution of such codes. Repeated root cyclic codes of different lengths such as lp^s, $p^n q$, etc., have also been studied [12, 44, 109].

Theorem 2.2.5. *[41, Theorem 6.2] q-ary cyclic codes of length p^s are precisely the ideals $\langle (x-1)^i \rangle$, $i = 0, 1, \ldots, p^s$, of the ring $\frac{\mathbb{F}_q[x]}{\langle x^{p^s} - 1 \rangle}$. If the cyclic code $\mathcal{C} = \langle (x-1)^i \rangle$ has $q^{(p^s - i)}$ codewords, then the dual of $\mathcal{C}$ is $\mathcal{C}^{\perp} = \langle (x-1)^{p^s - i} \rangle$, which contains q^i codewords.*

Theorem 2.2.6. *[41, Theorem 6.2] A q-ary cyclic code $\langle (x-1)^i \rangle$ of length p^s over $\mathbb{F}_q$ is self-orthogonal if and only if $\frac{p^s}{2} \leq i \leq p^s$. A self-dual q-ary cyclic code of length p^s over $\mathbb{F}_q$*

exists if and only if $p = 2$. The only self-dual 2^m-ary cyclic code of length 2^s over $\mathbb{F}_{2^m}$ is $\langle (x-1)^{2^{s}-1} \rangle$.

Theorem 2.2.7. *[41, Theorem 6.2] If $\mathcal{C} = \langle (x-1)^i \rangle$ is a q-ary cyclic code of length p^s over $\mathbb{F}_q$, then the Hamming distance $d_H(\mathcal{C})$ is determined by*

$$d_H(\mathcal{C}) = \begin{cases} 1, & \textit{if } i = 0, \\ \beta + 2, & \textit{if } \beta p^{s-1} + 1 \leq i \leq (\beta+1)p^{s-1}, \textit{where } 0 \leq \beta \leq p-2, \\ (t+1)p^k, & \textit{if } p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \leq i \leq p^s - p^{sk} + tp^{s-k-1}, \\ & \textit{where } 0 \leq t \leq p-1, 0 \leq k \leq s-1, \\ 0, & \textit{if } i = p^s. \end{cases}$$

2.2.5 Constacyclic Codes

Constacyclic codes are one of the important generalizations of cyclic codes. They were introduced by Berlekamp in [14], and have been studied in [11, 62, 65, 66, 109] , to mention a few.

In this section, we briefly describe constacyclic codes over finite fields. Let λ be a non-zero element of $\mathbb{F}_q$. We define a operator τ_λ on $\mathbb{F}_q^n$ as

$$\tau_\lambda(v_0, v_1, \ldots, v_{n-1}) = (\lambda v_{n-1}, v_0, \ldots, v_{n-2}),$$

where $(v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_q^n$. The operator τ_λ is called λ-constacyclic shift. A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is said to be a λ-*constacyclic* code if for every $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, the vector $(\lambda c_{n-1}, c_0, \ldots, c_{n-2})$ is also in $\mathcal{C}$. In other words, $\tau_\lambda(\mathcal{C}) = \mathcal{C}$. For $\lambda = 1$, a λ-costacyclic code is simply a cyclic code and for $\lambda = -1$, it is a *negacyclic code.*

In polynomial description, a λ-constacyclic code of length n over $\mathbb{F}_q$ is an ideal of $\frac{\mathbb{F}_q[x]}{\langle x^n - \lambda \rangle}$. The residue class ring $\frac{\mathbb{F}_q[x]}{\langle x^n - \lambda \rangle}$ is a principal ideal ring and hence a λ-constacyclic code of length n over $\mathbb{F}_q$ is a principal ideal of $\frac{\mathbb{F}_q[x]}{\langle x^n - \lambda \rangle}$. The other things are similar to the cyclic code case.

2.3 Codes over rings

All the rings considered in this thesis are finite commutative rings with identity.

Let R be a finite commutative ring with identity. A linear code $\mathcal{C}$ of length n over R is a R-submodule of the R-module R^n. Such a submodule need not be an R-free module. However, there exists a minimal set of generators for $\mathcal{C}$ over R, known as minimal spanning set for $\mathcal{C}$. A matrix G whose rows form a minimal spanning set of $\mathcal{C}$ is called a generator matrix for $\mathcal{C}$. Since $\mathcal{C}$ is in general not free, the rows of G may not be linearly independent over R. The minimum number of generators of $\mathcal{C}$ is called the *rank* of $\mathcal{C}$ and is denoted by rank $(\mathcal{C})$. The free rank of $\mathcal{C}$ is maximum of the ranks of R-free submodules of $\mathcal{C}$.

The Hamming weight and Hamming distance in R^n are defined similarly as in the case of finite fields. The usual inner product of two elements $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ of R^n is defined by

$$u \cdot v = \sum_{i=1}^{n} u_i v_i \ ,$$

where the multiplication is performed using the multiplication operation of R. The dual (strictly speaking, the *annihilator*) of a linear code $\mathcal{C}$ of length n over R is defined by

$$\mathcal{C}^{\perp} = \{v \in R^n \mid \ u \cdot v = 0, \ \forall \ u \in \mathcal{C}\} \ .$$

As usual, $\mathcal{C}$ is called *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ and *self-dual* if $\mathcal{C} = \mathcal{C}^{\perp}$. One important point to be noted here is that there does not exist any self-dual code of odd length over $\mathbb{F}_q$, but the same is not true over rings. For example, the linear code $\mathcal{C}$ of length 1 generated by 2 over $\mathbb{Z}_4$, i.e., $\mathcal{C} = \langle 2 \rangle$ is a self-dual code over $\mathbb{Z}_4$, as $2 \in \mathcal{C}^{\perp}$ and $|\mathcal{C}| = 2 = |\mathcal{C}^{\perp}|$.

The notion of cyclic and constacyclic codes discussed earlier over finite fields can be generalized to R. Thus, a linear code $\mathcal{C}$ over R is called a cyclic code if it is closed under the cyclic shifts of codewords. In polynomial representation, cyclic codes of length n over R are precisely the ideals of the residue class ring $\frac{R[x]}{\langle x^n - 1 \rangle}$. The factorization of $x^n - 1$ plays a vital role in studying cyclic codes over finite rings, as it does in the case of finite fields.

2.3.1 Local rings

Let R be a finite commutative ring with identity. An ideal of R is called a *maximal ideal* if it is not contained in any proper ideal of R. The intersection of all maximal ideals of R is called the *radical* of R and is denoted by Rad (R).

Definition 2.3.1. *A commutative ring with identity R is called a local ring if it has unique maximal ideal.*

Equivalently, R is called a local ring if $R/Rad(R)$ is a finite field. If R has more than one maximal ideal, then R is called a *semi-local ring*.

Theorem 2.3.2. *[88, Theorem V.1] Let R be a finite commutative rings with unity. Then the following are equivalent:*

1. *R is a local ring.*
2. *R has exactly one maximal ideal.*
3. *The non-units of R are contained in a proper ideal of R.*
4. *The non-units of R form an ideal of R.*
5. *For every $x \in R$, either x or $1 + x$ is a unit in R, where 1 is the unity in R.*
6. *The maximal ideal of R contains all non-units of R.*

Definition 2.3.3. *A finite commutative ring with identity is called a finite chain ring if its ideals form a finite chain under set theoretical inclusion.*

For example, finite fields, Galois rings and the ring of matrices $\left\{ \begin{bmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{bmatrix} : \quad a, b, c, d \ \in \mathbb{Z}_{p^r} \right\}$ are finite chain rings.

Theorem 2.3.4. *[45, Proposition 2.1] Let R be a finite commutative ring with unity. Then the following are equivalent:*

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

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

3. *R is a chain ring.*

Let R be a finite chain ring and M be its unique maximal ideal. Let γ be a fixed generator of M. If t is the nilpotency index of γ, then we have a chain ideals of R as

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

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

Theorem 2.3.5. *[45, Proposition 2.2] Let R be a finite commutative chain ring, with maximal ideal $M = \langle\gamma\rangle$, and let t be the nilpotency of γ. Then*

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

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

Definition 2.3.6. *A polynomial $f(x) \in R[x]$ is said to be a regular polynomial if $f(x)$ is not a zero divisor in $R[x]$.*

Theorem 2.3.7. *[88, Theorem XIII.2] Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \in R[x]$.*

1. *The following are equivalent:*

   (a) $f(x)$ is a unit,

   (b) $\overline{f}(x)$ is a unit,

   (c) a_0 is a unit and $a_1, \ldots, a_{n-1}$ are nilpotent.

2. *The following are equivalent:*

   (a) $f(x)$ is a nilpotent,

(b) $\overline{f}(x) = 0$,

(c) $a_0, a_1, \ldots, a_{n-1}$ *are nilpotent,*

(d) $f(x)$ *is a zero divisor,*

(e) there is a non-zero α *in* R *with* $\alpha f(x) = 0$.

3. *The following are equivalent:*

(a) $f(x)$ *is regular,*

(b) $\langle a_0, a_1, \ldots, a_{n-1}\rangle = R$,

(c) a_i *is a unit for some* i, $0 \leq i \leq n-1$,

(d) $\overline{f}(x) \neq 0$.

Thus an element $f(x) = f_0 + f_1x + \cdots + f_nx^n \in R[x]$ is regular if and only if f_i is a unit in R for some $i = 0, 1, \ldots, n$, if and only if, $\overline{f}(x) = \overline{f}_0 + \overline{f}_1x + \cdots + \overline{f}_nx^n \neq 0$ in $\overline{R}[x]$. In particular, a monic polynomial over R is a regular polynomial as its leading coefficient is a unit in R.

It is known that if $f(x)$ and $g(x)$ are two non-zero polynomials over R such that $f(x)g(x) \neq 0$, then deg $f(x)g(x) \leq$ deg $f(x)+$deg $g(x)$. If the leading coefficient of $f(x)$ or $g(x)$ is not a zero divisor in R, then $f(x)g(x) \neq 0$ and deg $f(x)g(x) =$ deg $f(x)+$deg $g(x)$. In particular, it holds for the monic polynomials over R. It follows from this discussion that a polynomial $f(x)$ over R with its leading coefficient a non-zero divisor in R cannot divide a non-zero polynomial of degree smaller than deg $f(x)$.

Theorem 2.3.8. *[88, Theorem XIII.6] If* $f(x)$ *is a regular polynomial in R[x]. Then there is a monic polynomial* $f^*(x)$ *with* $\overline{f}(x) = \overline{f}^*(x)$. *Furthermore there is a unit* $v(x)$ *in* $R[x]$ *such that* $f(x) = v(x)f^*(x)$.

The following version of the Euclidean algorithm holds true for polynomials over finite commutative local rings, which appears as an exercise (Exercise XIII.6) in [88, p. 273].

Theorem 2.3.9. *Let* $f(x)$ *and* $g(x)$ *be two polynomials in* $R[x]$. *If* $g(x)$ *is regular, then there exist polynomials* $q(x)$ *and* $r(x)$ *such that* $f(x) = g(x)q(x) + r(x)$, *deg* $r(x) <$ *deg* $g(x)$.

Proof. Since $g(x)$ is regular, by Theorem 2.3.8 there exists a monic polynomial $g^*(x) \in R[x]$ such that $g(x) = v(x)g^*(x)$, where $v(x)$ is a unit in $R[x]$.

Since $g^*(x)$ is monic, by division algorithm, there exists $q'(x)$ and $r(x)$ in $R[x]$ such that $f(x) = g^*(x)q'(x) + r(x)$, where deg $r(x) <$ deg $g^*(x)$. On multiplying both sides by $v(x)$, we get $v(x)f(x) = v(x)g^*(x)q'(x) + v(x)r(x)$, from which we get $f(x) = g(x)q(x) + r(x)$, where $q(x) = (v(x))^{-1}q'(x)$.

Since $g^*(x)$ is monic, so deg $g(x) \geq$ deg $g^*(x)$, as deg $g(x) =$ deg $v(x)+$ deg $g^*(x)$. From this follows that deg $r(x) <$ deg $g(x)$. ■

Let $f(x)$, $g(x)$ in $R[x]$. The polynomial $f(x)$ is called a divisor of $g(x)$ if $\langle g(x)\rangle \subseteq \langle f(x)\rangle$ and a proper divisor if $\langle g(x)\rangle \subset \langle f(x)\rangle$. A regular polynomial $f(x)$ is a proper divisor of $g(x)$ if and only if $f(x)$ is a divisor of $g(x)$ and $\overline{f}(x)$ is a proper divisor of $\overline{g}(x)$. The polynomial $f(x)$ is called an *associate* of $g(x)$, if there exists a unit $r(x) \in R[x]$ such that $f(x) = r(x)g(x)$. A non-zero, non-unit polynomial $f(x)$ is called *irreducible* if $f(x) = g(x)h(x)$, where $g(x)$, $h(x) \in R[x]$, then either $f(x)$ or $g(x)$ is a unit in $R[x]$. A polynomial is called *reducible* if it is not irreducible.

Definition 2.3.10. *Two polynomials $f(x), g(x) \in R[x]$ are said to be coprime if there exist $a(x), b(x) \in R[x]$ such that*

$$a(x)f(x) + b(x)g(x) = 1 \ , \tag{2.3.1}$$

or equivalently,

$$\langle f(x)\rangle + \langle g(x)\rangle = R \ .$$

Theorem 2.3.11. *If $f(x)$ and $g(x)$ are coprime over R if and only if $\overline{f}(x)$ and $\overline{g}(x)$ are coprime over $\overline{R}$.*

The Hensel's lemma guarantees that the factorization of polynomials into product of pairwise coprime polynomials in $\overline{R}[x]$ lift to such factorizations over R.

Theorem 2.3.12 (Hensel's Lemma). *[88, Theorem XIII.4] Let $f(x) \in R[x]$ and $\overline{f}(x) = g_1(x)g_2(x)\cdots g_r(x)$, where $g_1(x), g_2(x), \ldots, g_r(x)$ are pairwise coprime monic polynomials over $\overline{R}$. Then there exist pairwise coprime monic polynomials $f_1(x), f_2(x), \ldots, f_r(x)$ over R such that $f(x) = f_1(x)f_2(x)\cdots f_r(x)$ in $R[x]$ and $\overline{f}_i(x) = g_i(x)$, $i = 1, 2, \ldots, r$.*

The irreducible polynomials play a very important role in the study of extension fields. Approximately the same role is played by *basic irreducible* polynomials over local rings.

Definition 2.3.13. *A polynomial $f(x) \in R[x]$ is said to be basic irreducible if $\overline{f}(x)$ is irreducible in $\overline{R}[x]$, and basic primitive if $\overline{f}(x)$ is a primitive polynomial in $\overline{R}[x]$.*

Now we consider the factorization of a regular polynomial over R.

Definition 2.3.14. *A polynomial $f(x) \in R[x]$ is said to be a primary polynomial if $f(x) \mid g(x)h(x)$, for some $f(x), g(x) \in R[x]$, implies that $f(x) \mid g(x)$ or $f(x) \mid h(x)^n$ for some positive integer n.*

In other words, $f(x) \in R[x]$ is primary, if the ideal $\langle f(x) \rangle$ is a primary ideal of $R[x]$. It may be recalled that an ideal I of a commutative ring R' is primary if for any ideals A, B of R' such that $AB \subseteq I$, we have $A \subseteq I$ or $B^n \subseteq I$ for some positive integer n [7].

Furthermore, if $f(x) \in R[x]$ is a primary polynomial, then $\overline{f}(x) = ug(x)^n$, where $g(x)$ is an irreducible polynomial in $\overline{R}[x]$, u is a unit in $\overline{R}$, and n is a positive integer [88].

Theorem 2.3.15. *[88, Theorem XIII.11]] Let $f(x) \in R[x]$ be a regular polynomial. Then $f(x)$ factorizes uniquely, up to the order of factors and multiplication by units, into pairwise coprime primary polynomials over R.*

It follows from the above discussion that if $f(x) \in R[x]$ is a regular polynomial such that $\overline{f}(x)$ factorizes into distinct irreducible factors in $\overline{R}[x]$, then $f(x)$ factors uniquely into pairwise coprime basic irreducible polynomials over R.

Galois Rings

Galois rings are a special case of finite commutative local rings. Let $q = p^r$, p a prime and r a positive integer. To study codes over $\mathbb{Z}_q$, we very often require the extensions of $\mathbb{Z}_q$ containing primitive nth roots of unity. Galois rings provide such extensions for $\mathbb{Z}_q$.

In general, a Galois ring is defined as a finite commutative ring with identity 1 such that the set of its zero divisors together with the zero element 0 is a principal ideal $\langle p \rangle$ for some prime number p.

For any given positive integer m there exists a basic irreducible polynomial/basic primitive polynomial over $\mathbb{Z}_q$ [131]. A Galois ring of characteristic q is isomorphic to the quotient ring $\frac{\mathbb{Z}_q[x]}{\langle f(x)\rangle}$. So one can define a Galois ring as follows:

Definition 2.3.16. *If $f(x) \in \mathbb{Z}_q[x]$ is a monic basic irreducible polynomial of degree m, then the Galois ring of degree m over $\mathbb{Z}_q$ is the residue class ring $GR(q,m) = \frac{\mathbb{Z}_q[x]}{\langle f(x)\rangle}$.*

$\mathbb{Z}_q$ is a subring of the Galois ring $GR(q,m)$. $GR(q,m)$ has characteristic $q = p^r$ and the cardinality q^m. We have, $GR(q,1) = \mathbb{Z}_q$ and $GR(p,m) = \mathbb{F}_{p^m}$, the finite field of characteristic p with p^m elements. $\langle p^i\rangle$, $0 \leq i \leq r$ are ideals of $GR(q,m)$, and the ideal $\langle p\rangle$ contains all zero divisors $GR(q,m)$. All the ideals of $GR(q,m)$ form a chain under the set theoretical inclusion. Therefore $GR(q,m)$ is a local ring with the maximal ideal $\langle p\rangle$ (in fact, $GR(q,m)$ is a chain ring). The residue field of $GR(q,m)$ is $GR(q,m)/pGR(q,m) = \mathbb{F}_{p^m}$. If ξ is a root of $f(x)$, then $GR(q,m) = \mathbb{Z}_q[\xi]$. Each element of $c \in GR(q,m)$ can uniquely be expressed as

$$c = a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{m-1}\xi^{m-1},$$

which is called the additive representation of the elements of $GR(q,m)$. It is easy to see that $\{1, \xi, \xi^2, \ldots, \xi^{m-1}\}$ generates $GR(q,m)$ over $\mathbb{Z}_q$. Thus $GR(q,m)$ is a free module of rank m.

From [131, Theorem 13.9], there exists a primitive polynomial of degree m dividing $x^{p^m-1}-1$ over $\mathbb{Z}_q$. ξ is called a primitive root if it is a root of a unique monic basic primitive polynomial of degree m over $\mathbb{Z}_q$ and dividing $x^{p^m-1}-1$ in $\mathbb{Z}_q[x]$. Let $\mathcal{T} = \{0, 1, \xi, \ldots, \xi^{p^m-2}\}$. Then each element $x \in GR(q,m)$ can uniquely be expressed as

$$x = a_0 + a_1p + \cdots + a_{r-1}p^{r-1} \ ,$$

where $a_0, a_1, \ldots, a_{r-1} \in \mathcal{T}$. This representation is called the *p-adic* representation of the elements of $GR(q,m)$. An element $c = a_0 + a_1p + \cdots + a_{r-1}p^{r-1}$ is a unit in $GR(q,m)$ if and only if $a_0 \neq 0$. The set of all invertible elements of $GR(q,m)$ forms a cyclic group of order $(p^m-1)p^m$, which is a direct product of $\langle\alpha\rangle$ and ϵ, where $\langle\alpha\rangle$ is a cyclic group of order (p^m-1) and $\epsilon = \{1 + pb : b \in \mathcal{T}\}$. The map $^-$ gives a bijection from $\mathcal{T}$ to the residue field $\mathbb{F}_{p^m}$. Under this representation of the elements of $GR(q,m)$, the *Frobenius map* on $\mathcal{R}$ is defined by

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

f is an automorphism of $GR(q,m)$ that fixes $\mathbb{Z}_q$ and generates the group of automorphisms of $GR(q,m)$, which is a cyclic group of order m.

Example 2.3.17. *The polynomial $f(x) = x^4 + 4x^3 + 6x^2 + 3x + 1$ is a basic irreducible polynomial over $\mathbb{Z}_8$ as $\overline{f}(x) = x^4 + x + 1$ is an irreducible polynomial in $\mathbb{F}_2[x]$. Then the Galois extension $GR(8,4)$ of $\mathbb{Z}_8$ of degree 4 is the residue class ring $\frac{\mathbb{Z}_8[x]}{\langle f(x)\rangle}$. The elements of $GR(8,4)$ can uniquely be expressed as*

$$c = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 \ ,$$

where $a_0, a_1, a_2, a_3 \in \mathbb{Z}_8$, ξ is a root of $f(x)$.

Since $\overline{f}(x)$ is a primitive polynomial in $\mathbb{F}_2[x]$, $f(x)$ is a basic primitive polynomial in $\mathbb{Z}_8[x]$. So ξ is a primitive root. Let $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{14}\}$. Therefore each element of $GR(8,4)$ can uniquely be expressed as

$$c = b_0 + 2b_1 + 4b_2 + 8b_3 \ ,$$

where $b_0, b_1, b_2, b_3 \in \mathcal{T}$.

Theorem 2.3.18. *[31, 130] Let $q = p^r$, where r is a positive integer and $(n,q) = 1$. Let $g(x)$ be a divisor of $x^n - 1$ over $\mathbb{F}_p$. Then there exists a unique monic polynomial $f(x)$ in $\mathbb{Z}_q[x]$ such that $\overline{f}(x) = g(x)$ and $f(x) \mid (x^n - 1)$ in $\mathbb{Z}_q[x]$.*

The monic polynomial $f(x)$ in Theorem 2.3.18 is called the *Hensel lift* of the polynomial $g(x)$ to $\mathbb{Z}_q$.

For an odd positive integer n, the Hensel lift of an irreducible polynomial $f_2(x) \in \mathbb{Z}_2[x]$ dividing $x^n - 1$ to $\mathbb{Z}_4[x]$ can be obtained by the Graeffe's method [58, 129], described below. Let $f_2(x) = e(x) + o(x)$, where $e(x)$ contains only the even powers of x and $o(x)$ contains only the odd powers of x. Then $f(x)$ is obtained from the relation $f(x^2) = \pm\,(e(x)^2 - o(x)^2)$, where the sign ± is chosen in such a way that the coefficient of the highest power of x is 1. This is illustrated by the following example.

Example 2.3.19. *The polynomial* $g(x) = x^3+x+1$ *is an irreducible factor of* x^7-1 *over* $\mathbb{F}_2$. *For* $g(x)$, *we have,* $e(x) = 1$ *and* $o(x) = x^3+x$. *Therefore, if* $f(x)$ *is the Hensel lift of* $g(x)$ *to* $\mathbb{Z}_4[x]$, *then* $f(x^2) = ((x^3+x)^2 - (1)^2) = x^6+2x^4+x^2-1$, *and hence* $f(x) = x^3+2x^2+x-1$. $f(x)$ *is a divisor of* x^7-1 *in* $\mathbb{Z}_4[x]$.

More about Galois rings can be found in [34, 88, 100, 131].

2.3.2 Codes over $\mathbb{Z}_4$

Blake [23] initiated the study of codes over finite rings in early seventies, followed by the works of Speigel [119, 120] and Priti Shankar [107]. However, the study of codes over rings mainly got attention of researchers after the breakthrough paper of Hammons et al. [58] in 1994. There are many families of non-linear binary codes such as Kerdock, Preparata, Goethals, and Delsarte Goethals codes that have many more codewords than any known binary linear code of same length and minimum distance. Also, the Kerdock codes and the Preparata codes behave as duals of each other, just like linear codes. More precisely, the MacWilliams transform of the weight enumerator of one is the weight enumerator of the other. This mystery remained unsolved for several years until it was proved by Hammons et al. [58] that Kerdock, Preparata, Goethals, and Delsarte Goethals codes are in fact binary images of certain linear codes over $\mathbb{Z}_4$ under a map, called the *Gray map*, and Kerdock and Preparata codes (strictly speaking, a variant of Preparata codes [58]) are duals of each other as $\mathbb{Z}_4$ linear (cyclic) codes. The cyclic nature of Kerdock codes had already been shown by Nechaev [89]. In recent years, there has been a lot of investigation of codes over $\mathbb{Z}_4$ and many good binary codes have been obtained from codes over $\mathbb{Z}_4$ via the Gray map. Codes over $\mathbb{Z}_4$, also called the *quaternary codes*, are the most studied codes over finite rings.

A linear code of length n over $\mathbb{Z}_4$ is a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$. In particular, it is an additive subgroup of $\mathbb{Z}_4^n$. A generator matrix of a non-zero linear code C over $\mathbb{Z}_4$ is permutation-equivalent to a matrix of the form

$$\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{pmatrix},$$

where I_{k_1} and I_{k_2} are identity matrices of orders k_1 and k_2, respectively, A and C are $\mathbb{Z}_2$ matrices, and B is a $\mathbb{Z}_4$ matrix. $\mathcal{C}$ is an elementary abelian group of type $4^{k_1}2^{k_2}$, containing $2^{2k_1+k_2}$ codewords, and it is called a code of type $4^{k_1}2^{k_2}$. Further $\mathcal{C}$ is a free $\mathbb{Z}_4$-module if and only if $k_2 = 0$. The dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$ has the generator matrix

$$\begin{pmatrix} -B^T - C^T A^T & C^T & I_{n-k_1-k_2} \\ 2A^T & 2I_{k_2} & 0 \end{pmatrix},$$

where A^T denote the transpose of the matrix A. Further, $\mathcal{C}^{\perp}$ has the type $4^{n-k_1-k_2}2^{k_2}$ [58, 129].

For codes over $\mathbb{Z}_4$, several distance functions have been used. Lee and Euclidean distances are most important among them. The *Lee weight* of an element $a \in \mathbb{Z}_4$ is defined by

$$wt_L(a) = \min\{a, (4-a)\}.$$

Thus, the Lee weight of the elements $0, 1, 2$ and 3 of $\mathbb{Z}_4$ are $0, 1, 2$ and 1, respectively.

One of the main reasons for using Lee weight over $\mathbb{Z}_4$ is that, when $\mathbb{Z}_4$-codes are used in communication, the elements 0, 1, 2 and 3 are used to represent the signal points $i^0 = 1$, $i^1 = i$, $i^2 = -1$ and $i^3 = -i$, respectively (as shown in Figure 2.3). The distance between a, $b \in \mathbb{Z}_4$ is then defined as the half of the Euclidean distance between i^a and i^b, i.e.,

$$d_L(a,\ b) = \frac{1}{2}d_L^2(i^a,\ i^b)\ .$$

The Lee weight of an element $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_4^n$ is defined by

$$wt_L(\mathbf{a}) = \sum_{i=1}^{n} wt_L(a_i).$$

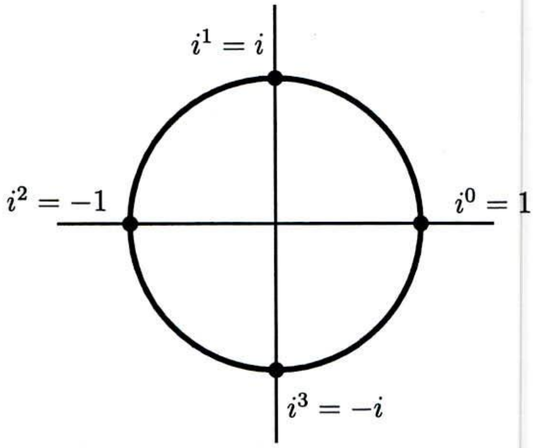

Figure 2.3: Representation of Signals as elements of $\mathbb{Z}_4$

The *Euclidean weight* of an element $a \in \mathbb{Z}_4$ is defined by

$$wt_E(a) = \min\{a^2, (m-a)^2\}.$$

The Euclidean weight of the elements $0, 1, 2$ and 3 of $\mathbb{Z}_4$ are $0, 1, 4$ and 1, respectively.

The Euclidean weight of an element $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_4^n$ is defined by

$$wt_E(\mathbf{a}) = \sum_{i=1}^{n} wt_E(a_i).$$

The Lee and Euclidean distances between two words $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_4^n$ are defined, respectively, by

$$d_L(\mathbf{x}, \mathbf{y}) wt_L(\mathbf{x} - \mathbf{y})$$

and

$$d_E(\mathbf{x}, \mathbf{y}) = wt_E(\mathbf{x} - \mathbf{y}) \ .$$

We can also see that $wt_L(\mathbf{x}) = n_1(\mathbf{x}) + 2n_2(\mathbf{x}) + n_3(\mathbf{x})$ and $wt_E(\mathbf{x}) = n_1(\mathbf{x}) + 4n_2(\mathbf{x}) + n_3(\mathbf{x})$, where $n_i(\mathbf{x})$ is the number of i's in $\mathbf{x}$ for $i = 1, 2, 3$.

The *Lee weight enumerator* and *Euclidean weight enumerator* of a $\mathbb{Z}_4$-code $\mathcal{C}$ of length n are defined as

$$Lee_{\mathcal{C}}(X, Y) = \sum_{c \in \mathcal{C}} X^{2n - wt_L(c)} Y^{wt_L(c)}$$

and

$$E_{\mathcal{C}}(X,Y) = \sum_{c \in \mathcal{C}} X^{4n - wt_L(c)} Y^{wt_L(c)},$$

respectively.

Using these facts one can derive the MacWilliams identities for both Lee and Euclidean weight enumerators of a linear code $\mathcal{C}$ over $\mathbb{Z}_4$, and are given in the following theorem.

Theorem 2.3.20. *[129, Theorem 2.4] Let $\mathcal{C}$ be a $\mathbb{Z}_4$-linear code of length n. Then*

$$Lee_{\mathcal{C}^\perp} = \frac{1}{\mathcal{C}} Lee_{\mathcal{C}}(X+Y,\ X-Y)$$

and

$$E_{\mathcal{C}^\perp} = \frac{1}{\mathcal{C}} E_{\mathcal{C}}(X+Y,\ X-Y)$$

Now we introduce an important map, called the *Gray map*, which establishes a relation between Quaternary codes and binary codes. This map opened doors to a new direction of research in coding theory. The map was introduced in the context of coding theory by Hammons et al. [58]. In communication systems employing quadrature phase-shift keying, the preferred assignment of two bits to the four possible phases is the one shown in Figure 2.4. In which adjacent phases differ by only one binary digit and the correspondence given as the following map:

Definition 2.3.21. *The map $\psi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ defined by $\psi(a+2b) = (b,\ a+b)$, where $a, b \in \mathbb{Z}_2$, is called the* Gray map, *i.e.,*

$$\begin{aligned} \psi(0) &= (0,0) \\ \psi(1) &= (0,1) \\ \psi(2) &= (1,1) \\ \psi(3) &= (1,0). \end{aligned}$$

This map is then extended componentwise to $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$. The map ψ is not a linear map, as $(1,1) = \psi(2) \neq \psi(1) + \psi(1) = (0,0)$. Therefore ϕ is also not a linear map. ϕ is a

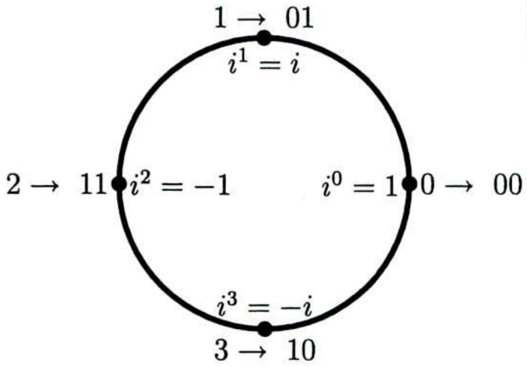

Figure 2.4: Gray amp

distance preserving map from $\mathbb{Z}_4^n$ with Lee distance to $\mathbb{Z}_2^{2n}$ with Hamming distance.

Since the Gray map ϕ is not a linear map, the Gray image $C = \phi(\mathcal{C})$ of a quaternary linear code $\mathcal{C}$ is in general not a linear code. Therefore, $\phi(\mathcal{C})$ need not have a dual. The $\mathbb{Z}_4$-*dual* of $\mathcal{C}$ is defined by $C_\perp = \phi(\mathcal{C}^\perp)$. We have the following diagram which need not be commutative

$$\begin{tikzcd}
\mathcal{C} \arrow[r, "\phi"] \arrow[d, "\text{dual}"'] & C & = & \phi(\mathcal{C}) \\
\mathcal{C}^\perp \arrow[r, "\phi"] & C_\perp & = & \phi(\mathcal{C}^\perp)
\end{tikzcd}$$

We have the following important results [58]:

1. C and $C_\perp$ are distance invariant.

2. The weight distributions of C and $C_\perp$ are MacWilliams transforms of each other.

A code $\mathcal{C}$ is called *distance invariant* if the Hamming weight distribution of its translates $c + \mathcal{C}$ is the same for all $c \in \mathcal{C}$ [81].

Definition 2.3.22. *A self-dual $\mathbb{Z}_4$-code $\mathcal{C}$ of length n is called a* Type II code *if the Euclidean weight of every codeword of $\mathcal{C}$ is a multiple of 8. Otherwise it is called a* Type I code.

Theorem 2.3.23. *[13, Proposition 3.4] A Type II code of length n over $\mathbb{Z}_4$ exists if and only if n is divisible by 8.*

Theorem 2.3.24. *[61, Theorem 12.5.1] Let $d_E(II)$ and $d_E(I)$ be the minimum Euclidean weights of a Type II code and a Type I code of length n, respectively, over $\mathbb{Z}_4$. Then*

$d_E(II) \leq 8\lfloor \frac{n}{24} \rfloor + 8$ and $d_E(I) \leq 8\lfloor \frac{n}{24} \rfloor + 8$ except when $n \equiv 23$ (mod 24), in which case $d_E(I) \leq 8\lfloor \frac{n}{24} \rfloor + 24$.

Codes satisfying the above bounds are said to be *Extremal Type II code* and *Extremal Type I code*, respectively. More about self-dual codes and Type II codes can be found in [61, 95].

2.3.3 Cyclic codes over $\mathbb{Z}_4$

As we have already seen in the beginning of this section that a cyclic code $\mathcal{C}$ of length n over $\mathbb{Z}_4$ is an ideal of $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$. Unlike over finite fields, the ring $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$ is not a unique factorization domain. For example, when $n = 4$, $x^4 - 1$ factorizes as $x^4 - 1 = (x-1)(x-1)(x^2+1) = (x-1)(x-1)(x^2+2x-1) = (x+1)(x+1)(x^2+2x-1)$ over $\mathbb{Z}_4$. Also a polynomial may have more number of roots than its degree. For example, all elements $1+2\alpha$, $\alpha \in GR(4,m)$ are roots of x^2-1 over $GR(4,m)$. Therefore one must be very careful when working on cyclic codes over $\mathbb{Z}_4$, and over rings in general. As was seen earlier, $x^n - 1$ exhibits distinct irreducible factors over $\mathbb{Z}_4$ only when n is odd. So throughout this subsection we assume that n is odd. The structure of the ideals of $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$ is well studied in [96]. A few important results are described below.

Theorem 2.3.25. *[96, Theorem 1] Let $x^n - 1 = f_1(x)f_2(x)\dots f_r(x)$ be the unique factorization of x^n-1 into pairwise coprime monic basic irreducible polynomials over $\mathbb{Z}_4$. Then every ideal of $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$ is the sum of the ideals $\langle \hat{f}_i(x)\rangle$ and $\langle 2\hat{f}_i(x)\rangle$, where $\hat{f}_i(x) = \frac{(x^n-1)}{f_i(x)}$, $1 \leq i \leq r$.*

Theorem 2.3.26. *[96, Theorem 2] Suppose $\mathcal{C}$ is a $\mathbb{Z}_4$-cyclic code of odd length n. Then there are unique, monic polynomials $f(x)$, $g(x)$, and $h(x)$ such that $\mathcal{C} = \langle f(x)h(x), 2f(x)g(x)\rangle$, where $f(x)g(x)h(x) = x^n - 1$, and $|\mathcal{C}| = 4^{deg\ g(x)}2^{deg\ h(x)}$. Further, when $h(x) = 1$, $\mathcal{C} = \langle f(x)\rangle$ and $|\mathcal{C}| = 4^{n-deg\ f(x)}$; and when $g(x) = 1$, $\mathcal{C} = \langle 2f(x)\rangle$ and $|\mathcal{C}| = 2^{n-deg\ f(x)}$.*

Corollary 2.3.27. *Assume that $x^n - 1$ is the product of r basic irreducible polynomials in $\mathbb{Z}_4[x]$. Then there are 3^r cyclic codes of length n over $\mathbb{Z}_4$.*

Theorem 2.3.28. *[96, Theorem 3] Let $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ and $b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}$ be two polynomials in $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$. Then $a(x)b(x) = 0$ if and only if $(a_0, a_1, \ldots, a_{n-1})$ is orthogonal to $(b_0, b_1, \ldots, b_{n-1})$ and its cyclic shifts.*

Let $f^*(x)$ denotes the reciprocal polynomial of $f(x) \in \mathbb{Z}_4[x]$. The following theorem gives duals of a cyclic codes of odd lengths over $\mathbb{Z}_4$

Theorem 2.3.29. *[96, Theorem 2] Let $\mathcal{C} = \langle f(x)h(x), 2f(x)g(x)\rangle$ be a $\mathbb{Z}_4$-cyclic code of odd length n, where $f(x)$, $g(x)$, and $h(x)$ are monic polynomials such that $f(x)g(x)h(x) = x^n - 1$, and $|\mathcal{C}| = 4^{deg\ g(x)}2^{deg\ h(x)}$. Then $\mathcal{C}^\perp = \langle g^*(x)h^*(x), 2g^*(x)f^*(x)\rangle$, and $|\mathcal{C}^\perp| = 4^{deg\ f(x)}2^{deg\ h(x)}$. Further, if $h(x) = 1$, then $\mathcal{C} = \langle f(x)\rangle$ and $\mathcal{C} = \langle g^*(x)\rangle$. If $g(x) = 1$, then $\mathcal{C} = \langle 2f(x)\rangle$ and $\mathcal{C}^\perp = \langle h^*(x), 2f^*(x)\rangle$.*

The following theorem gives self-dual cyclic codes of odd lengths over $\mathbb{Z}_4$

Theorem 2.3.30. *[97, Theorem 2] Let $\mathcal{C} = \langle f(x)h(x), 2f(x)g(x)\rangle$ be a $\mathbb{Z}_4$-cyclic code of odd length n, where $f(x)$, $g(x)$, and $h(x)$ are monic polynomials such that $f(x)g(x)h(x) = x^n - 1$, and $|\mathcal{C}| = 4^{deg\ g(x)}2^{deg\ h(x)}$. Then $\mathcal{C}$ is self-dual if and only if $f(x) = \alpha g^*(x)$ and $h(x) = \beta h^*(x)$, where α, β are units.*

Example 2.3.31. *[97, Exercise 721] The polynomial $x^7 - 1$ factorizes into the irreducible polynomials $x - 1$, $x^3 + x + 1$ and $x^3 + x^2 + 1$ over $\mathbb{Z}_2$. The Hensel lifts of these irreducible polynomials to $\mathbb{Z}_4$ are $g_1(x) = x - 1$, $g_2(x) = x^3 + 2x^2 + x - 1$ and $g_3(x) = x^3 - x^2 + 2x - 1$, respectively. Therefore there are 3^3 cyclic codes of length 7 over $\mathbb{Z}_4$. These codes, along with their duals, are listed in Table 2.1.*

More about cyclic codes of odd lengths over $\mathbb{Z}_4$ can be found in [61, 95, 129].

2.3.4 Cyclic codes of even lengths over $\mathbb{Z}_4$

When n is even, polynomials over $\mathbb{Z}_4$ do not factor into distinct basic irreducible polynomials, and so a cyclic code of even length over $\mathbb{Z}_4$ is a repeated root cyclic code. Also, when n is even, the polynomial $x^n - 1$ does not factorize uniquely over $\mathbb{Z}_4$. For example, $x^4 - 1 = (x-1)(x-1)(x^2+1) = (x-1)(x-1)(x^2+2x-1) = (x+1)(x+1)(x^2+2x-1)$ over

Table 2.1: $\mathbb{Z}_4$-cyclic codes of length 7

Code number	Generator polynomials	Type	Dual code
1	$g_2(x)g_3(x)$	4	6
2	$g_1(x)g_2(x)$	4^3	4
3	$g_1(x)g_3(x)$	4^3	5
4	$g_2(x)$	4^4	2
5	$g_3(x)$	4^4	3
6	$g_1(x)$	4^6	1
7	$2g_2(x)g_3(x)$	2	25
8	$2g_2(x)g_1(x)$	2^3	23
9	$2g_3(x)g_1(x)$	2^3	24
10	$2g_2(x)$	2^4	21
11	$2g_3(x)$	2^4	22
12	$2g_1(x)$	2^6	16
13	2	2^7	13 (self-dual)
14	$\langle g_2(x)g_3(x),\ 2g_2(x)g_1(x)\rangle$	$4\cdot 2^3$	19
15	$\langle g_2(x)g_3(x),\ 2g_3(x)g_1(x)\rangle$	$4\cdot 2^3$	20
16	$\langle g_2(x)g_3(x),\ 2g_1(x)\rangle$	$4\cdot 2^6$	12
17	$\langle g_2(x)g_1(x),\ 2g_2(x)g_3(x)\rangle$	$4^3\cdot 2$	17 (self-dual)
18	$\langle g_3(x)g_1(x),\ 2g_2(x)g_3(x)\rangle$	$4^3\cdot 2$	17 (self-dual)
19	$\langle g_2(x)g_1(x),\ 2g_3(x)g_1(x)\rangle$	$4^3\cdot 2^3$	14
20	$\langle g_1(x)g_3(x),\ 2g_2(x)g_1(x)\rangle$	$4^3\cdot 2^3$	15
21	$\langle g_1(x)g_2(x),\ 2g_3(x)\rangle$	$4^3\cdot 2^4$	10
22	$\langle g_1(x)g_3(x),\ 2g_2(x)\rangle$	$4^3\cdot 2^4$	11
23	$\langle g_2(x),\ 2g_3(x)g_1(x)\rangle$	$4^4\cdot 2^3$	8
24	$\langle g_3(x),\ 2g_2(x)g_1(x)\rangle$	$4^4\cdot 2^3$	9
25	$\langle g_1(x),\ 2g_2(x)g_3(x)\rangle$	$4^6\cdot 2$	7
26	0	4^0	27
27	1	4^7	26

$\mathbb{Z}_4$. But x^4-1 factors uniquely over $\mathbb{Z}_2$ as $x^4-1=(x-1)(x-1)(x-1)(x-1)$. Therefore the structure of irreducible factors of x^n-1 over $\mathbb{Z}_4$ is different from the factorization over $\mathbb{Z}_2$ for even n. Abualrub and Ohemke [3] have proved that cyclic codes of length 2^e over $\mathbb{Z}_4$ are not principally generated. They have given a structure of such codes in [4] and their duals in [2]. Blackford [21] has studied cyclic codes of length $2k$ over $\mathbb{Z}_4$ using discrete Fourier transform. Dougherty and Ling [49] have extended the results of [21] to cyclic codes of arbitrary even lengths over $\mathbb{Z}_4$. We present few important results which are required for latter purpose.

Lemma 2.3.32. *[4, Lemma 5, 6, 7] Let $n=2^k$, $k\geq 1$. Then $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$ is not a principal* *ideal ring. Furthermore, in* $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$*,*

1. $(x+1)^n = 2(x+1)^{\frac{n}{2}}$*,*

2. $x+1$ *is nilpotent of nilpotency* $\frac{3n}{2}$*,*

3. *an element* $f(x) = \sum_{j=0}^{n-1} a_j(x-1)^j$ *is a unit if and only if* a_0 *is a unit in* $\mathbb{Z}_4$*.*

A polynomial $f(x) = \sum_{i=0}^{n-1} a_i x^i$ in $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$ can uniquely be written as $f(x) = \sum_{i=0}^{n-1} a_i(x-1)^i$. If t is the smallest non-negative integer such that $a_t \neq 0$, then $f(x) = (x-1)^t h(x)$, where $h(x) \in \mathbb{Z}_4[x]$ and deg $h(x) \leq n-t-1$.

Theorem 2.3.33. *[4, Theorem 8, 9, 10] Let* I *be an ideal of* $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$*. Then* I *is one of the following:*

1. $\langle 2(x-1)^m\rangle$, $0 \leq m \leq n$,

2. $\langle (x-1)^s + 2(x-1)^t h(x)\rangle$, $0 \leq s \leq n-1$, *where* $h(x)$ *is either zero or a unit in* $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$*.*

3. $\langle (x-1)^s + 2(x-1)^t h(x),\ 2(x-1)^m\rangle$, $1 \leq s \leq n-1$, $0 \leq m \leq min\{s, n/2, n-s+t\}$, *where* $h(x)$ *is either zero or a unit in* $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$*.*

The reader is referred to [2–4, 21, 49] for more details cyclic codes of even lengths over $\mathbb{Z}_4$.

2.3.5 Negacyclic codes over $\mathbb{Z}_4$

Let λ be a unit in $\mathbb{Z}_4$. We recall the definition of λ-constacyclic codes. A linear code $\mathcal{C}$ of length n over $\mathbb{Z}_4$ is called a *λ-constacyclic code* if for every $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, $(\lambda c_{n-1}, c_0, \ldots, c_{n-2})$ is also in $\mathcal{C}$, i.e., $\mathcal{C}$ is closed under the λ-constacyclic shifts of codewords. When $\lambda = -1$, $\mathcal{C}$ is called a negacyclic code. Since λ is either 1 or -1 in $\mathbb{Z}_4$, so λ-constacyclic codes over $\mathbb{Z}_4$ are either cyclic codes or negacyclic codes over $\mathbb{Z}_4$. Just as in the case of finite fields, negacyclic codes of length n over $\mathbb{Z}_4$ are precisely the ideals of the residue class ring $\frac{\mathbb{Z}_4[x]}{\langle x^n+1\rangle}$.

When n is odd, there exists an isomorphism between $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$ and $\frac{\mathbb{Z}_4[x]}{\langle x^n+1\rangle}$. So, for each cyclic code of odd length over $\mathbb{Z}_4$, there is a negacyclic code of same length over $\mathbb{Z}_4$. However this is not the case when n is even. The structure of negacyclic codes of length 2^s over Galois rings and their complete Hamming distances were discussed by Dinh in [39, 40]. We present below the structure of the negacyclic codes of length 2^k over $\mathbb{Z}_4$, which is required in later chapters.

Theorem 2.3.34. *[39, Theorem 6.10] The negacyclic codes of length $n = 2^k$ over $\mathbb{Z}_4$ are precisely the ideals $\langle (x+1)^i \rangle$, $0 \le i \le 2n$, of $\frac{\mathbb{Z}_4[x]}{\langle x^n+1 \rangle}$. Moreover $|\langle (x+1)^i \rangle| = 2^{2n-i}$.*

Theorem 2.3.35. *[40, Theorem 4.4, 6.2, 7.2] Let $d_H(\mathcal{C})$, $d_L(\mathcal{C})$ and $d_E(\mathcal{C})$, respectively be the minimum Hamming, Lee and Euclidean distances of a negacyclic code $\mathcal{C} = \langle (x+1)^i \rangle$, $0 \le i \le 2n$, of length $n = 2^k$ over $\mathbb{Z}_4$. Then*

$$d_H(\mathcal{C}) = \begin{cases} 0, & \text{if } i = 2n \\ 1, & \text{if } 0 \le i \le n \\ 2, & \text{if } n+1 \le i \le n + \frac{n}{2} \\ 2^{r+1}, & \text{if } n+1+\sum_{j=1}^{r} 2^{k-j} \le i \le n + \sum_{j=1}^{r+1} 2^{k-j}, \text{ for some } 1 \le r \le k-1 \end{cases},$$

$$d_L(\mathcal{C}) = \begin{cases} 0, & \text{if } i = 2n \\ 1, & \text{if } i = 0 \\ 2, & \text{if } 1 \le i \le n \\ 4, & \text{if } n+1 \le i \le n + \frac{n}{2} \\ 2^{r+2}, & \text{if } n+1+\sum_{j=1}^{r} 2^{k-j} \le i \le n + \sum_{j=1}^{r+1} 2^{k-j}, \text{ for some } 1 \le r \le k-1 \end{cases}$$

and

$$d_E(\mathcal{C}) = \begin{cases} 0, & \textit{if}\ i = 2n \\ 1, & \textit{if}\ i = 0 \\ 2, & \textit{if}\ 1 \leq i \leq \frac{n}{2} \\ 4, & \textit{if}\ \frac{n}{2} + 1 \leq i \leq n \\ 8, & \textit{if}\ n + 1 \leq i \leq n + \frac{n}{2} \\ 2^{r+3}, & \textit{if}\ n + 1 + \sum\limits_{j=1}^{r} 2^{k-j} \leq i \leq n + \sum\limits_{j=1}^{r+1} 2^{k-j},\ \textit{for some}\ 1 \leq r \leq k-1. \end{cases}$$

Chapter 3

Codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$

3.1 Introduction

The work on codes over finite polynomial rings has shown that codes with better parameters (optimal in some cases) can be obtained over these rings and they have some practical importance [9, 26, 58, 138, 138]. It has already been noted that the codes over $\mathbb{Z}_4$ is a topic of special interest due to their connections with other areas of both mathematics and engineering. Initially, the work on codes over finite polynomial rings was confined to polynomial rings over finite fields. In [139], Yildiz and Karadeniz considered a new polynomial ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$, and studied linear and self-dual codes over it. They have constructed some good formally self-dual codes over this ring. Inspired by this, we have introduced another new ring of such type $R = \mathbb{Z}_4 + v\mathbb{Z}_4$, $v^2 = v$, in this chapter. This ring is a commutative semi-local principal ideal ring of characteristic 4 and size 16. We have introduced Lee weight and Gray weight for tuples over R. A Gray map on R is defined similarly as defined for $\mathbb{F}_2 + v\mathbb{F}_2$, $v^2 = v$ in [140]. Unlike the Gray map defined on $\mathbb{Z}_4$, the Gray map defined here is a linear map. We have obtained the MacWilliams identities for the Lee weight and Gray weight enumerators for codes over R. We have also considered RT metric and studied codes with respect to RT metric. Self-dual codes and their constructions over R have also been discussed.

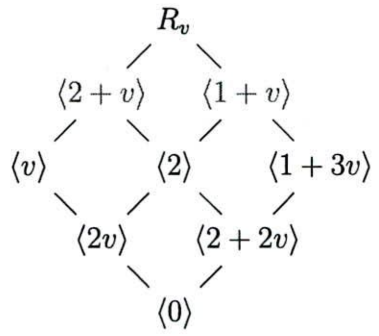

Figure 3.1: Lattice diagram of ideals of $\mathbb{Z}_4 + v\mathbb{Z}_4$

3.2 The ring $\mathbb{Z}_4 + v\mathbb{Z}_4$

Throughout this chapter, R denotes the ring $\mathbb{Z}_4 + v\mathbb{Z}_4 = \{a + vb \ : \ a, \ b \in \mathbb{Z}_4\}$, where $v^2 = v$. This ring is isomorphic to the polynomial ring $\frac{\mathbb{Z}_4[v]}{\langle v^2 - v \rangle}$. An element of R is a unit if and only if a is a unit and b is a non-unit, i.e., the units of R are $\{1, 3, 1+2v, 3+2v\}$. R is a principal ideal ring and has 7 non-trivial principal ideals:

$$\begin{aligned}
\langle 2v \rangle &= \{0, 2v\}, \\
\langle 2+2v \rangle &= \{0, 2+2v\}, \\
\langle 2 \rangle &= \{0, 2, 2v, 2+2v\}, \\
\langle v \rangle &= \{0, v, 2v, 3v\} = \langle 3v \rangle, \\
\langle 1+v \rangle &= \{0, 2, 2v, 1+v, 1+3v, 2+2v, 3+v, 3+3v\} = \langle 3+3v \rangle, \\
\langle 1+3v \rangle &= \{0, 1+3v, 2+2v, 3+v\} = \langle 3+v \rangle, \\
\langle 2+v \rangle &= \{0, 2, v, 2v, 3v, 2+v, 2+2v, 2+3v\} = \langle 2+3v \rangle \ .
\end{aligned}$$

Of these, $\langle 2+v \rangle$ and $\langle 1+v \rangle$ are maximal ideals. Thus R is a *semi-local ring.* Figure 3.1 represents the lattice diagram of the ideals of R.

It can easily be verified that the rings $\frac{R}{\langle 2+v \rangle}$ and $\frac{R}{\langle 1+v \rangle}$ are isomorphic to $\mathbb{Z}_2$. From the Chinese Remainder Theorem, it follows that $R = \langle 1+3v \rangle \oplus \langle v \rangle$. Therefore, an element $a + vb$ of R can be written as $a + vb = \alpha(1+3v) + \beta v$, where $\alpha, \ \beta \in \mathbb{Z}_4$. It follows from this that $\alpha = a$ and $\beta = a + b$, and so, $a + vb = a(1+3v) + (a+b)v$.

The main purpose of introducing R or its analogues in coding theory is to find some good $\mathbb{Z}_4$-codes. For this we need a Gray map which preserves the distances. We define the Gray map on R, which is same as the Gray map defined over the semi local ring $\mathbb{F}_2 + v\mathbb{F}_2$, $v^2 = v$ in [140]. For any $a + vb \in R$, the Gray map $\psi : R \to \mathbb{Z}_4^2$ is defined by

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

This map is then extended componentwise to $\phi : R^n \to \mathbb{Z}_4^{2n}$, so that for any $(x_1, x_2, \ldots, x_n) \in R^n$,

$$\phi(x_1, x_2, \ldots, x_n) = (a_1, a_2, \ldots, a_n, a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n),$$

where $x_i = a_i + vb_i$, $i = 1, 2, \ldots, n$. ϕ can easily be seen to be a $\mathbb{Z}_4$-module isomorphism.

We define the *Gray weight* of any $x \in R$ as the Hamming weight of its Gray image i.e., $wt_G(x) = wt_H(a,\ a + b)$. The Lee and Euclidean weights of any $x \in R$ are defined as the corresponding weights of its Gray image over $\mathbb{Z}_4$. That is, $wt_L(x) = wt_L(a,\ a + b)$ and $wt_E(x) = wt_E(a,\ a+b)$, where the Lee and Euclidean weights of $(a,\ a+b)$ are over $\mathbb{Z}_4$. The Hamming weight and distance of $x \in R^n$ are defined in the usual way. For any $x,\ y \in R^n$, the Hamming distance $d_H(x,\ y)$, the Gray distance $d_G(x,\ y)$, the Lee distance $d_L(x,\ y)$, and the Euclidean distance $d_E(x,\ y)$ between x and y are the corresponding weights of $x - y$, i.e., $d_G(x,\ y) = wt_G(x - y)$, $d_L(x,\ y) = wt_L(x - y)$ and $d_E(x,\ y) = wt_E(x - y)$. The different weights of elements of R are shown in Table 3.1.

3.3 Linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$

A linear code $\mathcal{C}$ of length n over R is an R-submodule of R^n. The *dual* of $\mathcal{C}$ is the code $\mathcal{C}^\perp := \{x \in R^n :\ x \cdot y = 0, \forall y \in \mathcal{C}\}$, where $x \cdot y$ denotes the usual inner product of x and y over R. Let A, B be two codes of length n over R. We define $A \otimes B = \{(a,\ b) :\ a \in A, b \in B\}$ and $A + B = \{a + b :\ a \in A, b \in B\}$.

Lemma 3.3.1. *The Gray map $\phi : R^n \to \mathbb{Z}_4^{2n}$ is linear and distance preserving.*

Proof. For any $x,\ y \in R^n$, it is easy to verify that $\phi(x+y) = \phi(x) + \phi(y)$ and $\phi(sx) = s\phi(x)$

Table 3.1: Weights of elements of $\mathbb{Z}_4 + v\mathbb{Z}_4$

Element x of R	**Gray image of x**	$wt_G(x)$	$wt_L(x)$	$wt_E(x)$
0	$(0,\ 0)$	0	0	0
1	$(1,\ 1)$	2	2	2
2	$(2,\ 2)$	2	4	8
3	$(3,\ 3)$	2	2	2
v	$(0,\ 1)$	1	1	1
$2v$	$(0,\ 2)$	1	2	4
$3v$	$(0,\ 3)$	1	1	1
$1+v$	$(1,\ 2)$	2	3	5
$1+2v$	$(1,\ 3)$	2	2	2
$1+3v$	$(1,\ 0)$	1	1	1
$2+v$	$(2,\ 3)$	2	3	5
$2+2v$	$(2,\ 0)$	1	2	4
$2+3v$	$(2,\ 1)$	2	3	5
$3+v$	$(3,\ 0)$	1	1	1
$3+2v$	$(3,\ 1)$	2	2	2
$3+3v$	$(3,\ 2)$	2	3	5

for any $s \in \mathbb{Z}_4$. So ϕ is linear.

From the definition of Lee weight in R,

$$\begin{aligned} d_L(x,\ y) &= wt_L(x-y) \\ &= wt_L(\phi(x-y)) \\ &= wt_L(\phi(x)-\phi(y)) \\ &= d_L(\phi(x),\ \phi(y)). \end{aligned}$$

Similarly, $d_G(x,\ y) = d_H(\phi(x),\ \phi(y))$ and $d_E(x,\ y) = d_E(\phi(x),\ \phi(y))$. Therefore ϕ is distance preserving. ■

It follows from the linearity of ϕ that, if $\mathcal{C}$ is a linear code of length n over R, then $\phi(\mathcal{C})$ is also a linear code of length $2n$ over $\mathbb{Z}_4$. Define $C_1 = \{a \in \mathbb{Z}_4^n :\ a + bv \in \mathcal{C}$ for some $b \in \mathbb{Z}_4^n\}$ and $C_2 = \{a+b \in \mathbb{Z}_4^n :\ a+bv \in \mathcal{C}$ for some $a \in \mathbb{Z}_4^n\}$. Obviously, $C_1,\ C_2$ are linear codes over $\mathbb{Z}_4$. The ring R is a Frobenius ring [135], and therefore $|\mathcal{C}||\mathcal{C}^{\perp}| = 16^n$ [135]. The following theorem is a generalization of [140, Theorem 3.1].

Theorem 3.3.2. *Let $\mathcal{C}$ be a linear code of length n over R. Then $\phi(\mathcal{C}) = C_1 \otimes C_2$ and $|\mathcal{C}| = |C_1||C_2|$.*

Proof. Since ϕ is bijective, for any $c' = (a_1, a_2, \dots, a_n, a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) \in \phi(\mathcal{C})$ there exists a $c = (c_1, c_2, \dots, c_n)$ in $\mathcal{C}$, where $c_i = a_i + b_i v$ such that $\phi(c) = c'$. Also from the definitions of C_1 and C_2, we obtain that $(a_1, a_2, \dots, a_n) \in C_1$, $(a_1+b_1, a_2+b_2, \dots, a_n+b_n) \in C_2$. Then it follows that $(a_1, a_2, \dots, a_n, a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) \in C_1 \otimes C_2$. Therefore, $\phi(\mathcal{C}) \subseteq C_1 \otimes C_2$.

On the other hand, for any $(a, b) \in C_1 \otimes C_2$, where $a = (a_1, a_2, \dots, a_n) \in C_1$, $b = (b_1, b_2, \dots, b_n) \in C_2$, there are $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$ in $\mathcal{C}$ such that $x = a + vs$ and $y = b + (1 + 3v)t$, where $s, t \in \mathbb{Z}_4^n$. Since $\mathcal{C}$ is linear, $x(1 + 3v) + yv = a + (3a + b)v \in \mathcal{C}$. Therefore, $\phi(a + (3a + b)v) = (a,\ b) \in \phi(\mathcal{C})$. This implies that, $C_1 \otimes C_2 \subseteq \phi(\mathcal{C})$. It follows then that $|\phi(\mathcal{C})| = |C_1 \otimes C_2| = |C_1||C_2|$. Since ϕ is bijective, $|\mathcal{C}| = |\phi(\mathcal{C})| = |C_1||C_2|$. ■

Corollary 3.3.3. *A linear code $\mathcal{C}$ over R can be expressed as $\mathcal{C} = (1 + 3v)C_1 \oplus vC_2$.*

Proof. Let $c = (c_1, c_2, \dots, c_n) \in \mathcal{C}$, where $c_i = a_i + b_i v$. Then $\phi(c) = (a,\ a + b)$, where $a = (a_1, a_2, \dots, a_n)$, $b = (b_1, b_2, \dots, b_n)$. This implies that $a \in C_1$ and $a + b \in C_2$ as $\phi(\mathcal{C}) = C_1 \otimes C_2$. Thus, $(1 + 3v)a + v(a + b) = a + bv = c \in (1 + 3v)C_1 \oplus vC_2$. Therefore, $\mathcal{C} \subseteq (1 + 3v)C_1 \oplus vC_2$.

For the reverse inclusion, let $x = (1 + 3v)a + vb \in (1 + 3v)C_1 \oplus vC_2$, where $a \in C_1$, $b \in C_2$. Then $\phi(x) = (a,\ b) \in C_1 \otimes C_2 = \phi(\mathcal{C})$. Since ϕ is bijective, so $x \in \mathcal{C}$. Therefore $(1 + 3v)C_1 \oplus vC_2 \subseteq \mathcal{C}$. Hence $\mathcal{C} = (1 + 3v)C_1 \oplus vC_2$. ■

Theorem 3.3.4. *Let $\mathcal{C}$ be a linear code of length n over R. Then $\phi(\mathcal{C}^\perp) = \phi(\mathcal{C})^\perp$.*

Proof. Let $\phi(c_1) \in \phi(\mathcal{C}^\perp)$, where $c_1 = a_1 + vb_1 \in \mathcal{C}^\perp$. Then $c_1 \cdot c_2 = 0$ for all $c_2 = a_2 + vb_2 \in \mathcal{C}$. This implies that $a_1 \cdot a_2 = 0$ and $a_1 \cdot b_2 + a_2 \cdot b_1 + b_1 \cdot b_2 = 0$. For any $c_2 \in \mathcal{C}$, $\phi(c_2) \in \phi(\mathcal{C})$ and $\phi(c_1) \cdot \phi(c_2) = (a_1,\ a_1 + b_1) \cdot (a_2,\ a_2 + b_2) = 2a_1 \cdot a_2 + (a_1 \cdot b_2 + a_2 \cdot b_1 + b_1 \cdot b_2) = 0$. So, $\phi(c_1) \in \phi(\mathcal{C})^\perp$. Therefore, $\phi(\mathcal{C}^\perp) \subseteq \phi(\mathcal{C})^\perp$.

On the other hand, since ϕ is a module isomorphism and the Gray image $\phi(\mathcal{C})$ of a code $\mathcal{C}$ is a $\mathbb{Z}_4$-code of length $2n$, $|\phi(\mathcal{C})^\perp| = \frac{4^{2n}}{|\phi(\mathcal{C})|} = \frac{16^n}{|\mathcal{C}|} = |\mathcal{C}^\perp| = |\phi(\mathcal{C}^\perp)|$. Hence $\phi(\mathcal{C}^\perp) = \phi(\mathcal{C})^\perp$.
■

Theorem 3.3.5. *Let $\mathcal{C}^\perp$ be the dual of a linear code $\mathcal{C} = (1+3v)C_1 \oplus vC_2$ of length n over R. Then $\mathcal{C}^\perp = (1+3v)C_1^\perp \oplus vC_2^\perp$, where $C_1^\perp$ and $C_2^\perp$ are duals of C_1 and C_2, respectively. Further $\phi(\mathcal{C}^\perp) = C_1^\perp \otimes C_2^\perp$.*

Proof. Let $c' = a' + vb' \in \mathcal{C}^\perp$. Then for any $c = a + vb \in \mathcal{C}$, we have $c' \cdot c = 0$. This implies that $aa' = 0$ and $ab' + a'b + bb' = 0$, which in turn implies that $(a+b)(a'+b') = 0$. Therefore $a' \in C_1^\perp$ and $a' + b' \in C_2^\perp$, as $c = a + vb \in \mathcal{C}$, $a \in C_1$ and $a + b \in C_2$. So $a'(1+3v) + (a'+b')v = a' + vb' = c' \in (1+3v)C_1^\perp \oplus vC_2^\perp$. Thus $\mathcal{C}^\perp \subseteq (1+3v)C_1^\perp \oplus vC_2^\perp$.

On the other hand, let $c' \in (1+3v)C_1^\perp \oplus vC_2^\perp$. Then $c' = (1+3v)a' + vb'$, where $a' \in C_1^\perp$ and $b' \in C_2^\perp$. This implies that $aa' = 0$ for all $a \in C_1$ and $bb' = 0$ for all $b \in C_2$. From Theorem 3.3.2, it follows that $(a,\ b) \in C_1 \otimes C_2 = \phi(\mathcal{C})$. Then there exists $c = (1+3v)a + vb \in \mathcal{C}$ such that $\phi(c) = (a,\ b)$. We can see now that $c \cdot c' = 0$. So $c' \in \mathcal{C}^\perp$. Therefore $(1+3v)C_1^\perp \oplus vC_2^\perp \subseteq \mathcal{C}^\perp$. Hence $\mathcal{C}^\perp = (1+3v)C_1^\perp \oplus vC_2^\perp$. Rest follows from Theorem 3.3.4. ■

Theorem 3.3.6. *Let d_L, d_G and d_E be the minimum Lee, Gray and Euclidean distances of a linear code $\mathcal{C}$ over R, respectively. Then $d_L = min\{d_L(C_1), d_L(C_2)\}, d_G = min\{d_H(C_1), d_H(C_2)\}$ and $d_E = min\{d_E(C_1), d_E(C_2)\}$, where C_1, C_2 are $\mathbb{Z}_4$-linear codes.*

Proof. Since ϕ is a distance preserving map, $d_L = d_L(\phi(\mathcal{C})) = d_L(C_1 \otimes C_2) = \min\{d_L(C_1), d_L(C_2)\}$. Similarly, $d_G = \min\{d_H(C_1), d_H(C_2)\}$ and $d_E = \min\{d_E(C_1), d_E(C_2)\}$.
■

3.4 The MacWilliams identities

Let the elements of R be represented as $R = \{a_1, a_2, \ldots, a_{16}\} = \{0, 1, 2, 3, v, 2v, 3v, 1+v, 1+2v, 1+3v, 2+v, 2+2v, 2+3v, 3+v, 3+2v, 3+3v\}$, where the order of elements is fixed.

Let I be a non-zero ideal of R. Define $\chi : I \to \mathbb{C}^*$ by

$$\chi(a+bv) = i^b,$$

where $\mathbb{C}^*$ is the multiplicative group of unit modulus complex numbers. χ is a non-trivial character of I, and hence we have $\sum\limits_{a\in I}\chi(a) = 0$.

Lemma 3.4.1. *Let $\mathcal{C}$ be a linear code of length n over R. Then for any $d \in R^n$,*

$$\sum_{c\in\mathcal{C}}\chi(c\cdot d) = \begin{cases} 0, & \text{if } d \notin \mathcal{C}^{\perp} \\ |\mathcal{C}|, & \text{if } d \in \mathcal{C}^{\perp}. \end{cases}$$

Proof. If $d \in \mathcal{C}^{\perp}$, then $c \cdot d = 0$. Since $\chi(0) = 1$, $\sum_{c\in\mathcal{C}}\chi(c\cdot d) = |\mathcal{C}|$. If $d \notin \mathcal{C}^{\perp}$, then $c \cdot d = \sum_{i=1}^{n} c_i d_i \neq 0$, where $c = (c_1, c_2, \ldots, c_n)$ and $d = (d_1, d_2, \ldots, d_n)$. Now,

$$\begin{aligned}\sum_{c\in\mathcal{C}}\chi(c\cdot d) &= \sum_{c\in\mathcal{C}}\chi\left(\sum_{i=1}^{n} c_i d_i\right)\\ &= \sum_{c\in\mathcal{C}}\prod_{i=1}^{n}\chi(c_i d_i)\\ &= \prod_{i=1}^{n}\sum_{c\in\mathcal{C}}\chi(c_i d_i) = 0,\end{aligned}$$

as for a fixed d_i, the set $\{c_i d_i \ : \ c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}\}$ forms an ideal of R, and there is at least one i for which $d_i \neq 0$, and for each such d_i we have $\sum_{c\in\mathcal{C}}\chi(c_i d_i) = 0$. Hence the result. ■

Theorem 3.4.2. *Let $\mathcal{C}$ be a linear code of length n over R and $\hat{f}(c) = \sum\limits_{d\in R^n}\chi(c\cdot d)f(d)$. Then $\sum\limits_{d\in\mathcal{C}^{\perp}} f(d) = \frac{1}{|\mathcal{C}|}\sum\limits_{c\in\mathcal{C}}\hat{f}(c)$.*

Proof. Since $\hat{f}(c) = \sum_{d \in R^n} \chi(c \cdot d) f(d)$,

$$\begin{aligned}
\sum_{c \in \mathcal{C}} \hat{f}(c) &= \sum_{c \in \mathcal{C}} \sum_{d \in R^n} \chi(c \cdot d) f(d) \\
&= \sum_{c \in \mathcal{C}} \sum_{d \in \mathcal{C}^\perp} \chi(c \cdot d) f(d) + \sum_{c \in \mathcal{C}} \sum_{d \in R^n - \mathcal{C}^\perp} \chi(c \cdot d) f(d) \\
&= \sum_{d \in \mathcal{C}^\perp} f(d) \sum_{c \in \mathcal{C}} \chi(c \cdot d) + \sum_{d \in R^n - \mathcal{C}^\perp} f(d) \sum_{c \in \mathcal{C}} \chi(c \cdot d) \\
&= |\mathcal{C}| \sum_{c \in \mathcal{C}^\perp} f(c) \ .
\end{aligned}$$

Hence the proof. ■

3.4.1 Complete Lee weight enumerator

The *complete Lee weight enumerator* (clwe) of a linear code $\mathcal{C}$ over R is defined as

$$clwe_{\mathcal{C}}(x_1, x_2, \ldots, x_{16}) = \sum_{c \in \mathcal{C}} x_1^{wt_{a_1}(c)} x_2^{wt_{a_2}(c)} \cdots \ x_{16}^{wt_{a_{16}}(c)},$$

where $wt_{a_i}(c)$ is the number of a_i's in c. This is a homogeneous polynomial in 16 variables $x_1, x_2, \ldots, x_{16}$ with total degree on each term being n, the length of $\mathcal{C}$. The Lee weight of each element of R and their corresponding variables are given in Table 3.2.

Theorem 3.4.3. *Let $\mathcal{C}$ be a linear code of length n over R. Then*

$$clwe_{\mathcal{C}^\perp}(x_1, x_2, \ldots, x_{16}) = \frac{1}{|\mathcal{C}|} clwe_{\mathcal{C}}(M \cdot (x_1, x_2, \ldots, x_{16})^T),$$

where M is an $|R| \times |R|$ matrix defined by $M(i,j) = (\chi(a_i a_j))$.

Proof. Let $f(x) = x_1^{wt_{a_1}(x)} x_2^{wt_{a_2}(x)} \cdots \ x_{16}^{wt_{a_{16}}(x)}$. From Theorem 3.4.2, we have

$$\begin{aligned}
\hat{f}(c) &= \sum_{d \in R^n} \chi(c \cdot d) f(d) \\
&= \sum_{d \in R^n} \chi(c \cdot d) x_1^{wt_{a_1}(d)} x_2^{wt_{a_2}(d)} \cdots \ x_{16}^{wt_{a_{16}}(d)} \ .
\end{aligned}$$

Table 3.2: Lee weight distribution of elements of $\mathbb{Z}_4 + v\mathbb{Z}_4$

Element x **of** R	**Lee weight** $wt_L(x)$	**corresponding variable**
0	0	x_1
1	2	x_2
2	4	x_3
3	2	x_4
v	1	x_5
$2v$	2	x_6
$3v$	1	x_7
$1+v$	3	x_8
$1+2v$	2	x_9
$1+3v$	1	x_{10}
$2+v$	3	x_{11}
$2+2v$	2	x_{12}
$2+3v$	3	x_{13}
$3+v$	1	x_{14}
$3+2v$	2	x_{15}
$3+3v$	3	x_{16}

For each $a \in R$, let $\delta_{a,d_i} = \begin{cases} 1 & \text{if } d_i = a \\ 0 & \text{otherwise} \end{cases}$. Then $wt_a(d) = \sum_{i=1}^{n} \delta_{a,d_i}$, and hence

$$\begin{aligned}
\hat{f}(c) &= \sum_{d\in R^n} \chi\left(\sum_{i=1}^{n} c_i d_i\right) \; x_1^{\sum_{i=1}^{n}\delta_{a_1,d_i}} x_2^{\sum_{i=1}^{n}\delta_{a_2,d_i}} \cdots \; x_{16}^{\sum_{i=1}^{n}\delta_{a_{16},d_i}} \\
&= \sum_{d\in R^n} \prod_{i=1}^{n} \chi(c_i d_i) x_1^{\delta_{a_1,d_i}} x_2^{\delta_{a_2,d_i}} \cdots \; x_{16}^{\delta_{a_{16},d_i}} \\
&= \prod_{i=1}^{n} \sum_{d_i\in R} \chi(c_i d_i) x_1^{\delta_{a_1,d_i}} x_2^{\delta_{a_2,d_i}} \cdots \; x_{16}^{\delta_{a_{16},d_i}} \\
&= \prod_{i=1}^{n} \sum_{j=1}^{16} \chi(c_i a_j) x_j \\
&= \prod_{i=1}^{16} \left(\sum_{j=1}^{16} \chi(a_i a_j) x_j\right)^{wt_{a_i}(c)} .
\end{aligned}$$

Now, from the definition of complete Lee weight enumerator (clwe), we get

$$\begin{aligned}
clwe_{\mathcal{C}^\perp}(x_1, x_2, \ldots, x_{16}) &= \sum_{c\in\mathcal{C}^\perp} x_1^{wt_{a_1}(c)} x_2^{wt_{a_2}(c)} \cdots\ x_{16}^{wt_{a_{16}}(c)} \\
&= \sum_{c\in\mathcal{C}^\perp} f(c) \\
&= \frac{1}{|\mathcal{C}|}\sum_{c\in\mathcal{C}} \hat{f}(c) \\
&= \frac{1}{|\mathcal{C}|}\sum_{c\in\mathcal{C}}\prod_{i=1}^{16}\left(\sum_{j=1}^{16}\chi(a_i a_j)x_j\right)^{wt_{a_i}(c)} \\
&= \frac{1}{|\mathcal{C}|}clwe_{\mathcal{C}}\left(\sum_{j=1}^{16}\chi(a_1a_j)x_j, \sum_{j=1}^{16}\chi(a_2a_j)x_j, \ldots, \sum_{j=1}^{16}\chi(a_{16}a_j)x_j\right) \\
&= \frac{1}{|\mathcal{C}|}clwe_{\mathcal{C}}(M\cdot(x_1, x_2, \ldots, x_{16})^T),
\end{aligned}$$

where $M = (\chi(a_ia_j))$ is a matrix of order 16 × 16. ■

Permutation equivalent codes have the same complete Lee weight enumerators but equivalent codes may have distinct weight enumerators. So the appropriate weight enumerator for studying equivalent codes is the *symmetrized Lee weight enumerator* (slwe) [129], defined as

$$slwe_{\mathcal{C}}(x, y, z, w, s) = clwe_{\mathcal{C}}(x, z, s, z, y, z, y, w, z, y, w, z, w, y, z, w),$$

where x represents the element of weight 0 (the element a_1), y represents the elements of weight 1 (the elements a_5, a_7, a_{10}, a_{14}), z represents the element of weight 2 (the elements $a_2, a_4, a_6, a_9, a_{12}, a_{15}$), w represents the elements of weight 3 (the elements $a_8, a_{11}, a_{13}, a_{16}$), and s represents the element of weight 4 (the element a_3), as shown in Table 3.3.

Therefore,

$$slwe_{\mathcal{C}}(x,\ y,\ z,\ w,\ s) = \sum_{c\in\mathcal{C}} x^{wt_0}y^{wt_1}z^{wt_2}w^{wt_3}s^{wt_4},$$

Table 3.3: Lee weights and their corresponding symmetric variables

$wt_L(x)$	**Elements of R**	**corresponding variables**	**symmetric variable**
0	0	x_1	x
1	$v,\ 3v,\ 1+3v,\ 3+v$	$x_5,\ x_7,\ x_{10},\ x_{14}$	y
2	$1,\ 3,\ 2v,\ 1+2v,\ 2+2v,\ 3+2v$	$x_2,\ x_4,\ x_6,\ x_9,\ x_{12},\ x_{15}$	z
3	$1+v,\ 2+v,\ 2+3v,\ 3+3v$	$x_8,\ x_{11},\ x_{13},\ x_{16}$	w
4	2	x_3	s

where

$$\begin{aligned}
wt_0 &= wt_{a_1}(c);\\
wt_1 &= wt_{a_5}(c) + wt_{a_7}(c) + wt_{a_{10}}(c) + wt_{a_{14}}(c);\\
wt_2 &= wt_{a_2}(c) + wt_{a_4}(c) + wt_{a_6}(c) + wt_{a_9}(c) + wt_{a_{12}}(c) + wt_{a_{15}}(c);\\
wt_3 &= wt_{a_8}(c) + wt_{a_{11}}(c) + wt_{a_{13}}(c) + wt_{a_{16}}(c);\\
wt_4 &= wt_{a_3}(c)\ .
\end{aligned} \tag{3.4.1}$$

Theorem 3.4.4. *Let C be a linear code of length n over R. Then* $slwe_{C^\perp}(x,\ y,\ z,\ w,\ s) = \frac{1}{|C|} slwe_C(x+4y+6z+4w+s,\ x-2y+2w-s,\ x-2z+s,\ x+2y-2w-s,\ x-4y+6z-4w+s)$.

Proof. The result follows from Theorem 3.4.3 and the definition of symmetrized Lee weight enumerator. ∎

The *Lee weight enumerator* (Lee_C) of a linear code C over R is defined as

$$\text{Lee}_C(x,\ y) = \sum_{c\in C} x^{4n-wt_L(c)} y^{wt_L(c)}\ .$$

Theorem 3.4.5. *Let C be a linear code of length n over R. Then*

$$Lee_C(x,\ y) = slwe_C(x^4,\ x^3y,\ x^2y^2,\ xy^3,\ y^4)\ .$$

Proof. Let $wt_L(c) = wt_1 + 2wt_2 + 3wt_3 + 4wt_4$, where wt_1, wt_2, wt_3, wt_4 are as in (3.4.1). Since $n = \sum_{i=1}^{16} wt_{a_i}(c) = wt_0+wt_1+wt_2+wt_3+wt_4$, so $4n-wt_L(c) = 4wt_0+3wt_1+2wt_2+wt_3$.

From the definition of Lee weight enumerator,

$$\begin{aligned}
\mathrm{Lee}_{\mathcal{C}}(x,\ y) &= \sum_{c\in\mathcal{C}} x^{4n-wt_L(c)} y^{wt_L(c)} \\
&= \sum_{c\in\mathcal{C}} x^{4wt_0+3wt_1+2wt_2+wt_3} y^{wt_1+2wt_2+3wt_3+4wt_4} \\
&= \sum_{c\in\mathcal{C}} x^{4wt_0}(x^3y)^{wt_1}(xy)^{2wt_2}(xy^3)^{wt_3} y^{4wt_4} \\
&= slwe_{\mathcal{C}}(x^4,\ x^3y,\ x^2y^2,\ xy^3,\ y^4)\ .
\end{aligned}$$

■

Theorem 3.4.6. *Let C be a linear code of length n over R. Then*

$$Lee_{\mathcal{C}^\perp}(x,\ y) = \frac{1}{|\mathcal{C}|} Lee_{\mathcal{C}}(x+y,\ x-y)\ .$$

Proof. From Theorems 3.4.5 and 3.4.4, we have

$$\begin{aligned}
\mathrm{Lee}_{\mathcal{C}^\perp}(x,\ y) &= \frac{1}{|\mathcal{C}|} slwe_{\mathcal{C}^\perp}\left(x^4+4x^3y+6x^2y^2+4xy^3+y^4,\ x^4+2x^3y-2xy^3-y^4,\right. \\
&\qquad \left. x^4-x^2y^2+y^4,\ x^4-2x^3y+2xy^3-y^4,\ x^4-4x^3y+6x^2y^2-4xy^3+y^4\right) \\
&= \frac{1}{|\mathcal{C}|} slwe_{\mathcal{C}^\perp}\left((x+y)^4,\ (x+y)^3(x-y),\ (x+y)^2(x-y)^2,\ (x+y)(x-y)^3,\right. \\
&\qquad \left.(x-y)^4\right) \\
&= \frac{1}{|\mathcal{C}|} \mathrm{Lee}_{\mathcal{C}}(x+y,\ \ x-y)\ .
\end{aligned}$$

■

3.4.2 Complete Gray weight enumerator

The *complete Gray weight enumerator* (cgwe) of a code is defined in the same way as the complete Lee weight enumerator, i.e.,

$$cgwe_{\mathcal{C}}(x_1, x_2, \ldots, x_{16}) = \sum_{c\in\mathcal{C}} x_1^{wt_{a_1}(c)} x_2^{wt_{a_2}(c)} \cdots\ x_{16}^{wt_{a_{16}}(c)},$$

where $wt_{a_i}(c)$ is the number of a_i's in c.

Theorem 3.4.3 holds for the complete Gray weight enumerator also, i.e.,

$$cgwe_{\mathcal{C}^{\perp}}(x_1, x_2, \ldots, x_{16}) = \tfrac{1}{|\mathcal{C}|} cgwe_{\mathcal{C}}(M \cdot (x_1, x_2, \ldots, x_{16})^T),$$

where M is the matrix defined in Theorem 3.4.3.

The *symmetrized Gray weight enumerator* (sgwe) of $\mathcal{C}$ is defined as

$$sgwe_{\mathcal{C}}(x,\ y,\ z) = cgwe_{\mathcal{C}}(x, z, z, z, y, y, y, z, z, y, z, y, z, y, z, z),$$

where x represents the element of weight 0 (the element a_1), y represents the elements of weight 1 (the elements $a_5, a_6, a_7, a_{10}, a_{12}, a_{14}$) and z represents the element of weight 2 (the elements $a_2, a_3, a_4, a_8, a_9, a_{11}, a_{13}, a_{15}, a_{16}$). Therefore, $sgwe_{\mathcal{C}}(x, y, z) = \sum\limits_{c \in \mathcal{C}} x^{wt_0} y^{wt_1} z^{wt_2}$, where

$$\begin{aligned}
wt_0 &= wt_{a_1}(c); \\
wt_1 &= wt_{a_5}(c) + wt_{a_6}(c) + wt_{a_7}(c) + wt_{a_{10}}(c) + wt_{a_{12}}(c) + wt_{a_{14}}(c); \qquad (3.4.2)\\
wt_2 &= wt_{a_2}(c) + wt_{a_3}(c) + wt_{a_4}(c) + wt_{a_8}(c) + wt_{a_9}(c) + wt_{a_{11}}(c) \\
&+ wt_{a_{13}}(c) + wt_{a_{15}}(c) + wt_{a_{16}}(c).
\end{aligned}$$

Theorem 3.4.7. *Let $\mathcal{C}$ be a linear code of length n over R. Then*

$$sgwe_{\mathcal{C}^{\perp}}(x,\ y,\ z) = \frac{1}{|\mathcal{C}|} sgwe_{\mathcal{C}}(x + 6y + 9z,\ x + 2y - 3z,\ x - 2y + z)\ .$$

Proof. The result follows from Theorem 3.4.3 and the definition of symmetrized Gray weight enumerator. ■

The *Gray weight enumerator* $(G_{\mathcal{C}})$ of a linear code $\mathcal{C}$ is defined as

$$G_{\mathcal{C}}(x,\ y) = \sum_{c \in \mathcal{C}} x^{2n - wt_G(c)} y^{wt_G(c)}\ .$$

Theorem 3.4.8. *Let $\mathcal{C}$ be a linear code of length n over R. Then*

$$G_{\mathcal{C}}(x,\ y) = sgwe_{\mathcal{C}}(x^2,\ xy,\ y^2)\ .$$

Proof. Let $wt_G(c) = wt_1 + 2wt_2$, where wt_1, wt_2 are as in (3.4.2). Since $n = \sum\limits_{i=1}^{16} a_i =$

$wt_0+wt_1+wt_2$, so $2n-wt_G(c) = 2wt_0+wt_1$. From the definition of Gray weight enumerator,

$$\begin{aligned} G_{\mathcal{C}}(x,\ y) &= \sum_{c\in\mathcal{C}} x^{2n-wt_G(c)}y^{wt_G(c)} \\ &= \sum_{c\in\mathcal{C}} x^{2wt_0+wt_1}y^{wt_1+2wt_2} \\ &= \sum_{c\in\mathcal{C}} x^{2wt_0}(xy)^{wt_1}y^{2wt_2} \\ &= sgwe_{\mathcal{C}}(x^2,\ xy,\ \ y^2)\ . \end{aligned}$$

■

Theorem 3.4.9. *Let $\mathcal{C}$ be a linear code of length n over R. Then*

$$G_{\mathcal{C}^\perp}(x,y) = \frac{1}{|\mathcal{C}|}G_{\mathcal{C}}(x+3y, x-y)\ .$$

Proof. From Theorems 3.4.8 and 3.4.7, we have

$$\begin{aligned} G_{\mathcal{C}^\perp}(x,\ y) &= \frac{1}{|\mathcal{C}|}sgwe_{\mathcal{C}^\perp}(x^2+6xy+3y^2,\ x^2+2xy-3y^2,\ x^2-2xy+y^2) \\ &= \frac{1}{|\mathcal{C}|}sgwe_{\mathcal{C}^\perp}((x+3y)^2,\ (x+3y)(x-y),\ (x-y)^2) \\ &= \frac{1}{|\mathcal{C}|}G_{\mathcal{C}}(x+3y,\ \ x-y) \end{aligned}$$

. ■

Corollary 3.4.10. *The Lee and Hamming weight enumerators of $\phi(\mathcal{C})$ over $\mathbb{Z}_4$ are same as the Lee and Gray weight enumerators of $\mathcal{C}$ over R.*

Examples

Example 3.4.11. *Let $\mathcal{C}$ be the linear code of length 2 over R generated by*

$$G = \begin{pmatrix} 1 & 3+2v \\ 0 & 2 \end{pmatrix}\ .$$

The Gray image of this code is a code of length 4 over $\mathbb{Z}_4$ and it is of type $4^2 2^2$. The Lee and Gray weight enumerators of $\mathcal{C}$ are

$$W_L(z) = 1 + 12z^2 + 39z^4 + 11z^6 + z^8$$

and

$$W_G(z) = 1 + 4z + 12z^2 + 24z^3 + 23z^4,$$

respectively.

Example 3.4.12. *The linear code $\mathcal{C}$ of length 4 over R generated by*

$$G = \begin{pmatrix} 1+3v & 1+v & 3+3v & 3+v \\ 2+2v & 2v & 0 & 2 \end{pmatrix}$$

is a self-orthogonal code of 32 codewords and its Gray image is also a self-orthogonal code of length 8 over $\mathbb{Z}_4$. The code $\mathcal{C}$ has all even Lee weight codewords and the minimum Lee weight of $\mathcal{C}$ is 4. The Lee and Gray weight enumerators of $\mathcal{C}$ are

$$W_L(z)1 + 3z^4 + 19z^8 + 9z^{12}$$

and

$$W_G(z) = 1 + 5z^2 + 12z^4 + 14z^6,$$

respectively.

Example 3.4.13. *The linear code $\mathcal{C}$ of length 4 over R generated by*

$$G = \begin{pmatrix} 1 & 3 & 3+2v & 1+2v \\ 0 & 2 & 0 & 2 \\ 2v & 0 & 0 & 2v \\ 2+2v & 2+2v & 0 & 0 \end{pmatrix}$$

is a self-dual code of 256 codewords and Lee weights of all code words are even. The Gray *image of $\mathcal{C}$ is also a self-dual code of length 8 over $\mathbb{Z}_4$. The Lee weight enumerator of $\mathcal{C}$ is*

$$W_L(z) = 1 + 28z^4 + 198z^8 + 28z^{12} + z^{16} .$$

3.5 Codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ with respect to Rosenbloom–Tsfasman metric

Let $\mathcal{M}_{n\times s}(R)$ be the set of all $n \times s$ matrices over R. Let $p = (p_0, p_1, \ldots, p_{s-1}) \in \mathcal{M}_{1\times s}(R)$. Then the RT weight ($\rho$-weight) of p is defined as [104]

$$w_N(p) = \begin{cases} max\{i : p_i \neq 0\} + 1, & p \neq 0 \\ 0, & p = 0 \end{cases} .$$

The ρ-distance between p and q is defined by

$$\rho(p, q) = w_N(p - q),$$

where $p, q \in \mathcal{M}_{1\times s}(R)$. The RT weight is then extended to $P = (P_1, P_2, \ldots, P_n)^T \in \mathcal{M}_{n\times s}(R)$ as $w_N(P) = \sum_{i=1}^{n} w_N(P_i)$, where $P_i = (p_{i,0}, p_{i,1}, \ldots, p_{i,s-1}) \in \mathcal{M}_{1\times s}(R)$, $1 \leq i \leq n$. The ρ-distance between P and Q is $\rho(P, Q) = w_N(P - Q)$, where $P, Q \in \mathcal{M}_{n\times s}(R)$. It can easily be shown that ρ is a metric on R, and for $s = 1$, the ρ-metric is just the usual Hamming metric.

A linear code $\mathcal{C}$ over R is an R-submodule of $\mathcal{M}_{n\times s}(R)$. The set of non-negative integers

$$w_r(\mathcal{C}) = |\{P \in \mathcal{C} : w_N(P) = r\}|,$$

where $0 \leq r \leq ns$, is called the *weight spectrum of* $\mathcal{C}$, and the ρ-*weight enumerator of* $\mathcal{C}$ is defined as [111]

$$W_{\mathcal{C}}(z) = \sum_{r=0}^{ns} w_r(\mathcal{C}) z^r = \sum_{P\in\mathcal{C}} z^{w_N(P)} .$$

Let $p = (p_0, p_1, \ldots, p_{s-1})$ and $q = (q_0, q_1, \ldots, q_{s-1}) \in \mathcal{M}_{1\times s}(R)$. Then the inner product of p and q is defined by

$$\langle p,\ q\rangle = \sum_{i=0}^{s-1} p_i q_{s-1-i}.$$

This is then extended to the inner product of P and Q as

$$\langle P,\ Q\rangle = \sum_{i=1}^{n} \langle P_i,\ Q_i\rangle = \sum_{i=1}^{n}\sum_{j=0}^{s-1} p_{i,j} q_{i,s-1-j},$$

where $P = (P_1, P_2, \ldots, P_n)^T, Q = (Q_1, Q_2, \ldots, Q_n)^T \in \mathcal{M}_{n\times s}(R)$ and $P_i = (p_{i,0}, p_{i,1}, \ldots, p_{i,s-1})$, $Q_i = (q_{i,0}, q_{i,1}, \ldots, q_{i,s-1}) \in \mathcal{M}_{1\times s}(R)$, $1 \le i \le n$. For $s = 1$, the inner product defined above becomes the usual inner product

$$\langle P, Q\rangle = \sum_{i=1}^{n} \langle P_i,\ Q_i\rangle = \sum_{i=1}^{n} p_{i,0} q_{i,0}\ .$$

The *dual* of the code $\mathcal{C}$ is defined by $\mathcal{C}^{\perp} := \{Q \in \mathcal{M}_{n\times s}(R) : \langle P, Q\rangle = 0, \forall P \in \mathcal{C}\}$. Clearly, $\mathcal{C}^{\perp}$ is also a linear code over $\mathcal{M}_{n\times s}(R)$.

It has been observed in [50] that even if the ρ-weight enumerators of two linear codes are the same, the ρ-weight enumerators of their duals need not be same.

Example 3.5.1. *Let* $\mathcal{C}_1 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2v & 0 \\ 2v & 0 \end{pmatrix} \right\}$, $\mathcal{C}_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2v \end{pmatrix} \right\}$ *be two linear codes over* $\mathcal{M}_{2\times 2}(R)$. *They have same ρ-weight enumerator* $1 + z^2$. *Let* $\mathcal{C}_1^{\perp}$, $\mathcal{C}_2^{\perp}$ *be the dual codes of* $\mathcal{C}_1$, $\mathcal{C}_2$, *respectively. Both* $\mathcal{C}_1^{\perp}$ *and* $\mathcal{C}_2^{\perp}$ *contain* $32,768$ *elements but their weight enumerators are different, namely,*

$$W_{\mathcal{C}_1^{\perp}}(z) = 1 + 30z + 449z^2 + 3360z^3 + 28928z^4,$$

$$W_{\mathcal{C}_2^{\perp}}(z) = 1 + 30z + 557z^2 + 5280z^3 + 26880z^4.$$

This problem has been resolved by considering the orbits of a linear group in [50]. The same problem has been addressed by Siap [111] in another way by defining the complete weight enumerator which preserves the order of the entries of the matrices.

A ring of $n \times s$ matrices over R can be identified with a ring of $n \times 1$ matrices having polynomial entries. We identify the set of all polynomials of degree at most $s-1$ over R with $\frac{R[x]}{\langle x^s \rangle}$. Define $\varphi : \mathcal{M}_{1\times s}(R) \to \frac{R[x]}{\langle x^s \rangle}$ by

$$\varphi(a_0, a_1, \dots, a_{s-1}) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{s-1}x^{s-1}.$$

This map is an R-module isomorphism and can be extended to $\Omega : \mathcal{M}_{n\times s}(R) \to \mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s \rangle}\right)$ by

$$\Omega\left((P_1, P_2, \dots, P_n)^T\right) = (P_1(x), P_1(x), \dots, P_n(x))^T,$$

where $P_i = (p_{i,0}, p_{i,1}, \dots, p_{i,s-1}) \in \mathcal{M}_{1\times s}(R)$ and $P_i(x) = p_{i,0} + p_{i,1}x + \cdots + p_{i,s-1}x^{s-1} \in \frac{R[x]}{\langle x^s \rangle}$, $1 \leq i \leq n$, A^T is the transpose of A.

Let $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{s-1}x^{s-1} \in \frac{R[x]}{\langle x^s \rangle}$. Let the l^{th} $(0 \leq l \leq s-1)$ coefficient a_l of $a(x)$ be denoted by $c_l(a(x))$. Then the inner product $\langle a,\ b\rangle$ becomes

$$\langle a(x),\ b(x)\rangle = c_{s-1}(a(x)b(x)).$$

This can be extended to the matrices $P,\ Q \in \mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s \rangle}\right)$, as

$$\langle P,\ Q\rangle = \sum_{i=1}^{n} \langle P_i(x),\ Q_i(x)\rangle.$$

This implies that

$$\langle P,\ Q\rangle = \sum_{i=1}^{n} c_{s-1}(P_i(x)Q_i(x)) = \sum_{i=1}^{n}\sum_{j=0}^{s-1} p_{i,j}q_{i,s-1-j}, \tag{3.5.1}$$

where $P = (P_1(x), P_2(x), \dots, P_n(x))^T$, $Q = (Q_1(x), Q_2(x), \dots, Q_n(x))^T$ and $P_i(x) = p_{i,0} + p_{i,1}x + \cdots + p_{i,s-1}x^{s-1}$, $Q_i(x) = q_{i,0} + q_{i,1}x + \cdots + q_{i,s-1}x^{s-1} \in \frac{R[x]}{\langle x^s \rangle}$, $1 \leq i \leq n$.

Let $\mathcal{C}$ be a linear code over $\mathcal{M}_{n\times s}(R)$, $P = (p_{ij})_{n\times s} \in \mathcal{C}$, where $1 \leq i \leq n$, $0 \leq j \leq s-1$ and $X_{ns} = (x_{1,0}, x_{1,1}, \dots, x_{1,s-1}, \dots, x_{n,0}, \dots, x_{n,s-1})$. We define the *complete ρ-weight* *enumerator* of $\mathcal{C}$ as

$$W_{\mathcal{C}}(X_{ns}) = \sum_{P\in\mathcal{C}} \left(x_{1,0}^{w(p_{1,0})} \cdots x_{1,s-1}^{w(p_{1,s-1})} \cdots x_{n,0}^{w(p_{n,0})} \cdots x_{n,s-1}^{w(p_{n,s-1})} \right),$$

which is a polynomial in ns variables.

3.5.1 Lee complete ρ-weight enumerator

Let $X_{ns} = (x_{1,0}, x_{1,1}, \ldots, x_{1,s-1}, \ldots, x_{n,0}, \ldots, x_{n,s-1})$ and $P = (p_{ij})_{n\times s}$, where $1 \leq i \leq n$, $0 \leq j \leq s-1$. We define the *Lee complete ρ-weight enumerator* of $\mathcal{C}$ over $\mathcal{M}_{n\times s}(R)$ as [141]

$$\mathrm{Lee}_{\mathcal{C}}(X_{ns}) = \sum_{P\in\mathcal{C}} \left(x_{1,0}^{w_L(p_{1,0})} \cdots x_{1,s-1}^{w_L(p_{1,s-1})} \cdots x_{n,0}^{w_L(p_{n,0})} \cdots x_{n,s-1}^{w_L(p_{n,s-1})} \right).$$

It is a polynomial in ns variables with total degree of each term being $4ns$. Note that, if we let $s = 1$ then the ρ-metric and inner products defined earlier are just the usual Hamming metric and usual inner products, respectively, and by arranging the subscripts we obtain the *complete Lee weight enumerator* of a code over R, discussed in Section 3.4.1.

One can obtain the ρ-weight enumerator from Lee complete ρ-weight enumerator by a proper transformation. Siap [111] has given a transformation to obtain ρ-weight enumerator from complete ρ-weight enumerator of a code. The transformation we propose here is a generalization of the transformation given in [111]. The transformations is as follows:

To obtain ρ-weight enumerator of code $\mathcal{C}$, replace

$$x_{1,0}^{w_L(p_{1,0})} \cdots x_{1,s-1}^{w_L(p_{1,s-1})} \cdots x_{n,0}^{w_L(p_{n,0})} \cdots x_{n,s-1}^{w_L(p_{n,s-1})} \qquad \text{by} \qquad z^N,$$

where $N = s\left\lceil \frac{wt_L(p_{i,s-1})}{4} \right\rceil + (s-1)\left\lceil \frac{wt_L(p_{i,s-2})}{4} \right\rceil \left(1 - \left\lceil \frac{wt_L(p_{i,s-1})}{4} \right\rceil\right) + (s-2)\left\lceil \frac{wt_L(p_{i,s-3})}{4} \right\rceil$ $\left(1 - \left\lceil \frac{wt_L(p_{i,s-2})}{4} \right\rceil\right)\left(1 - \left\lceil \frac{wt_L(p_{i,s-1})}{4} \right\rceil\right) + \cdots + \left\lceil \frac{wt_L(p_{i,0})}{4} \right\rceil \left(1 - \left\lceil \frac{wt_L(p_{i,1})}{4} \right\rceil\right)\left(1 - \left\lceil \frac{wt_L(p_{i,2})}{4} \right\rceil\right) \cdots$ $\left(1 - \left\lceil \frac{wt_L(p_{i,s-1})}{4} \right\rceil\right)$, and $\lceil . \rceil$ represents the least integer function.

Example 3.5.2. *Let* $\mathcal{C} = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2+2v & 0 \\ 2v & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 2v & 2v \end{pmatrix}, \begin{pmatrix} 2+2v & 0 \\ 2+2v & 0 \end{pmatrix} \right\}$

be a linear code over $\mathcal{M}_{2\times 2}(R)$. The Lee complete ρ-weight enumerator of $\mathcal{C}$ is

$$Lee_{\mathcal{C}}(X_{22}) = 1 \ + \ x_{10}^2 \ x_{20}^4 x_{21}^2 + \ x_{20}^2 x_{21}^2 \ + \ x_{10}^2 \ x_{20}^2 \ .$$

The ρ-weight enumerator of $\mathcal{C}$ is

$$W_{\mathcal{C}}(z) = 1 + 2z^2 + z^3,$$

which is obtained by the transformation

$$z^{2\left\lceil \frac{wt_L(a_{i1})}{4} \right\rceil + \left\lceil \frac{wt_L(a_{i0})}{4} \right\rceil \left(1 - \left\lceil \frac{wt_L(a_{i1})}{4} \right\rceil\right)},$$

where a_{ij} is the element in the i^{th} column and the j^{th} row in a codeword of $\mathcal{C}$, $i = 1, 2$ and $j = 0, 1$.

The following lemma is a generalization of Lemma 3.4.1 to the present setting.

Lemma 3.5.3. *Let $\mathcal{C}$ be a linear code over $\mathcal{M}_{n\times s}(R)$ and $P,\ Q \in \mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s\rangle}\right)$. Then*

$$\sum_{P\in\mathcal{C}} \chi(\langle P,\ Q\rangle) = \begin{cases} 0, & if\ Q \notin \mathcal{C}^{\perp} \\ |\mathcal{C}|, & if\ Q \in \mathcal{C}^{\perp} \end{cases}.$$

Proof. Let $P = (P_1(x), P_2(x), \ldots, P_n(x))^T$, $Q = (Q_1(x), Q_2(x), \ldots, Q_n(x))^T \in \mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s\rangle}\right)$, and $P_i(x) = (p_{i,0} + p_{i,1}x + \cdots + p_{i,s-1}x^{s-1})$, $Q_i(x) = (q_{i,0} + q_{i,1}x + \cdots + q_{i,s-1}x^{s-1}) \in \frac{R[x]}{\langle x^s\rangle}$, $1 \leq i \leq n$.

If $Q \in \mathcal{C}^{\perp}$, then $\langle P,\ Q\rangle = 0$. Since $\chi(0) = 1$, $\sum_{P\in\mathcal{C}} \chi(\langle P,\ Q\rangle) = |\mathcal{C}|$.

If $Q \notin \mathcal{C}^{\perp}$ then $\langle P,\ Q\rangle \neq 0$. From equation (3.5.1), we get that $\sum_{i=1}^{n} \sum_{j=0}^{s-1} p_{i,j} q_{i,s-1-j} \neq$

0. Now,

$$\begin{aligned}
\sum_{P\in\mathcal{C}} \chi(\langle P,\ Q\rangle) &= \sum_{P\in\mathcal{C}} \chi\left(\sum_{i=1}^{n}\sum_{j=0}^{s-1} p_{i,j}q_{i,s-1-j}\right)\\
&= \sum_{P\in\mathcal{C}} \prod_{i=1}^{n}\prod_{j=0}^{s-1} \chi(p_{i,j}q_{i,s-1-j})\\
&= \prod_{i=1}^{n}\prod_{j=0}^{s-1} \sum_{p_{i,j}\in R} \chi(p_{i,j}q_{i,s-1-j}) = 0,
\end{aligned}$$

as for any fixed $d \in R$, $cd \in R\ \forall c \in R$, and for each such d, $\sum_{c\in R} \chi(cd) = 0$. ■

Lemma 3.5.4. $\sum_{a\in R} \chi(ba)\ x^{w_L(a)} = (1+x)^{4-w_L(b)}(1-x)^{w_L(b)} \quad \forall\ b\ \in\ R$.

Proof.

$$\sum_{a\in R} \chi(ba)\ x^{w_L(a)} = \begin{cases} (1+x)^4 & \text{if } b = 0,\\ (1+x)^3(1-x) & \text{if } b = v,\ 3v,\ 1+3v,\ 3+v,\\ (1+x)^2(1-x)^2 & \text{if } b = 1,\ 3,\ 2v,\ 1+2v,\ 2+2v,\ 3+2v,\\ (1+x)(1-x)^3 & \text{if } b = 1+v,\ 2+v,\ 2+3v,\ 3+3v,\\ (1-x)^4 & \text{if } b = 2\ . \end{cases}$$

It follows that $\sum_{a\in R} \chi(ba)\ x^{w_L(a)} = (1+x)^{4-w_L(b)}(1-x)^{w_L(b)}$.

■

The following lemma is analogous to Lemma 3.5.4.

Lemma 3.5.5. $\sum_{a\in R} \chi(ba)\ x^{4-w_L(a)}y^{wt_L(a)} = (x+y)^{4-w_L(b)}(x-y)^{w_L(b)} \quad \forall\ b\ \in\ R$.

Proof.

$$\sum_{a\in R}\chi(ba)\ x^{4-w_L(a)}y^{wt_L(a)} = \begin{cases} (x+y)^4 & \text{if } \ b=0 \\ (x+y)^3(x-y) & \text{if } \ b=v,\ 3v,\ 1+3v,\ 3+v, \\ (x+y)^2(x-y)^2 & \text{if } \ b=1,\ 3,\ 2v,\ 1+2v,\ 2+2v,\ 3+2v, \\ (x+y)(x-y)^3 & \text{if } \ b=1+v,\ 2+v,\ 2+3v,\ 3+3v, \\ (x-y)^4 & \text{if } \ b=2 \end{cases}$$

$$= (x+y)^{4-w_L(b)}(x-y)^{w_L(b)}\ .$$

■

The following result is a generalization of Theorem 3.4.2 to the present setting.

Theorem 3.5.6. *Let $\mathcal{C}$ be a linear code over $\mathcal{M}_{n\times s}(R)$ and $f : \mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s\rangle}\right) \to \mathbb{C}[X_{ns}]$. Then $\sum_{Q\in\mathcal{C}^\perp} f(Q) = \frac{1}{|\mathcal{C}|}\sum_{P\in\mathcal{C}}\hat{f}(P)$, where $\hat{f}(P) = \sum_{Q\in\mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s\rangle}\right)}\chi(\langle P,\ Q\rangle)f(Q)$.*

Proof. Let $\hat{f}(P) = \sum_{Q\in\mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s\rangle}\right)}\chi(\langle P,Q\rangle)f(Q)$. Then

$$\begin{aligned} \sum_{P\in\mathcal{C}}\hat{f}(P) &= \sum_{P\in\mathcal{C}}\ \sum_{Q\in\mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s\rangle}\right)}\chi(\langle P,Q\rangle)f(Q) \\ &= \sum_{P\in\mathcal{C}}\sum_{Q\in\mathcal{C}^\perp}\chi(\langle P,Q\rangle)f(Q) + \sum_{P\in\mathcal{C}}\sum_{Q\notin\mathcal{C}^\perp}\chi(\langle P,Q\rangle)f(Q) \\ &= \sum_{Q\in\mathcal{C}^\perp} f(Q)\sum_{P\in\mathcal{C}}\chi(\langle P,Q\rangle) + \sum_{Q\notin\mathcal{C}^\perp} f(Q)\sum_{P\in\mathcal{C}}\chi(\langle P,Q\rangle) \\ &= |\mathcal{C}|\sum_{Q\in\mathcal{C}^\perp} f(Q)) + 0 \qquad \text{(from Lemma 3.5.3)} \end{aligned}$$

Therefore, $\sum_{Q\in\mathcal{C}^\perp} f(Q) = \frac{1}{|\mathcal{C}|}\sum_{P\in\mathcal{C}}\hat{f}(P)$. ■

Theorem 3.5.7. *Let $\mathcal{C}$ be a linear code over $\mathcal{M}_{n\times s}(R)$. Then*

$$\sum_{Q\in\mathcal{C}^\perp}\prod_{i=1}^{n}\prod_{j=0}^{s-1} x_{i,j}^{wt_L(q_{i,j})} = \frac{1}{|\mathcal{C}|}\left(\prod_{i=1}^{n}\prod_{j=0}^{s-1}(1+x_{i,j})^4\right)\sum_{P\in\mathcal{C}}\prod_{i=1}^{n}\prod_{j=0}^{s-1}\left(\frac{1-x_{i,j}}{1+x_{i,j}}\right)^{wt_L(p_{i,s-1-j})} .$$

Proof. Let $f(Q) = \prod_{i=1}^{n}\prod_{j=0}^{s-1} x_{i,j}^{wt_L(q_{i,j})}$. Then from Theorem 3.5.6, we have $\sum_{Q\in\mathcal{C}^\perp} f(Q) = \frac{1}{|\mathcal{C}|}\sum_{P\in\mathcal{C}} \hat{f}(P)$, where $\hat{f}(P) = \sum_{Q\in\mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s\rangle}\right)} \chi(\langle P, Q\rangle) f(Q)$. This implies that

$$\begin{aligned}
\hat{f}(P) &= \sum_{Q\in\mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s\rangle}\right)} \chi(\sum_{i=1}^{n}\sum_{j=0}^{s-1} p_{i,s-1,j}q_{i,j}) \prod_{i=1}^{n}\prod_{j=0}^{s-1} x_{i,j}^{wt_L(q_{i,j})} \\
&= \sum_{Q\in\mathcal{M}_{n\times 1}\left(\frac{R[x]}{\langle x^s\rangle}\right)} \prod_{i=1}^{n}\prod_{j=0}^{s-1} \chi(p_{i,s-1,j}q_{i,j}) x_{i,j}^{wt_L(q_{i,j})} \\
&= \prod_{i=1}^{n}\prod_{j=0}^{s-1} \sum_{q_{i,j}\in R} \chi(p_{i,s-1,j}q_{i,j}) x_{i,j}^{wt_L(q_{i,j})} \\
&= \prod_{i=1}^{n}\prod_{j=0}^{s-1} (1+x_{i,j})^{4-w_L(p_{i,s-1-j})}(1-x_{i,j})^{w_L(p_{i,s-1-j})}
\end{aligned}$$

Therefore,

$$\begin{aligned}
\sum_{Q\in\mathcal{C}^\perp} f(Q) &= \frac{1}{|\mathcal{C}|}\sum_{P\in\mathcal{C}}\prod_{i=1}^{n}\prod_{j=0}^{s-1}(1+x_{i,j})^{4-w_L(p_{i,s-1-j})}(1-x_{i,j})^{w_L(p_{i,s-1-j})} \\
&= \frac{1}{|\mathcal{C}|}\sum_{P\in\mathcal{C}}\prod_{i=1}^{n}\prod_{j=0}^{s-1}(1+x_{i,j})^4\left(\frac{1-x_{i,j}}{1+x_{i,j}}\right)^{w_L(p_{i,s-1-j})} \\
&= \frac{1}{|\mathcal{C}|}\prod_{i=1}^{n}\prod_{j=0}^{s-1}(1+x_{i,j})^4\sum_{P\in\mathcal{C}}\prod_{i=1}^{n}\prod_{j=0}^{s-1}\left(\frac{1-x_{i,j}}{1+x_{i,j}}\right)^{w_L(p_{i,s-1-j})}.
\end{aligned}$$

■

If we let $s = 1$ in Theorem 3.5.7, then we get the MacWilliams identity (Theorem 3.4.6) for linear codes of length n over R.

Corollary 3.5.8 (Theorem 3.4.6). *Let $\mathcal{C}$ be a linear code of length n over R. Then*

$$Lee_{\mathcal{C}^\perp}(X,\ Y) = \frac{1}{|\mathcal{C}|}Lee_{\mathcal{C}}(X+Y,\ X-Y)\ .$$

Proof. Putting $s = 1$ in Theorem 3.5.7, we get

$$\begin{aligned}\sum_{Q\in\mathcal{C}^{\perp}}\prod_{i=1}^{n} x_i^{w_L(q_i)} &= \frac{1}{|\mathcal{C}|}\sum_{P\in\mathcal{C}}\prod_{i=1}^{n}(1+x_i)^{4-wt_L(p_i)}(1+x_i)^{wt_L(p_i)} \\ &= \frac{1}{|\mathcal{C}|}\sum_{P\in\mathcal{C}}\prod_{i=1}^{n}\sum_{a_i\in R}\chi(a_ip_i)x_i^{w_L(a_i)}.\end{aligned}$$

Replacing each $x_i^{wt_L(a_i)}$ by $X^{4-wt_L(a_i)}Y^{wt_L(a_i)}$ and each $x_i^{wt_L(q_i)}$ by $X^{4-wt_L(q_i)}Y^{wt_L(q_i)}$, we get

$$\sum_{Q\in\mathcal{C}^{\perp}}\prod_{i=1}^{n}X^{4-wt_L(q_i)}Y^{wt_L(q_i)} = \frac{1}{|\mathcal{C}|}\sum_{P\in\mathcal{C}}\prod_{i=1}^{n}\sum_{a_i\in R}\chi(a_ip_i)X^{4-wt_L(a_i)}Y^{wt_L(a_i)} .$$

Then it follows from Lemma 3.5.5 that

$$\begin{aligned}\sum_{Q\in\mathcal{C}^{\perp}} X^{4n-wt_L(Q)}Y^{wt_L(Q)} &= \frac{1}{|\mathcal{C}|}\sum_{P\in\mathcal{C}}\prod_{i=1}^{n}(X+Y)^{4-wt_L(p_i)}(X-Y)^{wt_L(p_i)} \\ &= \frac{1}{|\mathcal{C}|}\sum_{P\in\mathcal{C}}(X+Y)^{4n-wt_L(P)}(X-Y)^{wt_L(P)}.\end{aligned}$$

Therefore, from the definition of Lee weight enumerator,

$$\mathrm{Lee}_{\mathcal{C}^{\perp}}(X,\ Y) = \frac{1}{|\mathcal{C}|}\mathrm{Lee}_{\mathcal{C}}(X+Y,\ X-Y) .$$

■

Examples

Example 3.5.9. *Let* $\mathcal{C} = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 2+2v \\ 0 & 2 & 2v \end{pmatrix}, \begin{pmatrix} 2v & 0 & 0 \\ 0 & 2v & 2v \end{pmatrix}, \begin{pmatrix} 2+2v & 0 & 2+2v \\ 0 & 2+2v & 0 \end{pmatrix} \right\}$ *be a linear code over* $\mathcal{M}_{2\times 3}(R)$. *Then the Lee complete* ρ*-weight enumerator of* $\mathcal{C}$ *is*

$$Lee_{\mathcal{C}}(X_{23}) = 1\ +\ x_{10}^{4}x_{12}^{2}\ x_{21}^{4}x_{22}^{2} +\ x_{10}^{2}\ x_{21}^{2}x_{22}^{2}\ +\ x_{10}^{2}x_{12}^{2}\ x_{21}^{2},$$

and the ρ-weight enumerator of $\mathcal{C}$ is $W_{\mathcal{C}}(z) = 1 + z^4 + z^5 + z^6$, which is obtained by the transformation

$$z^{3\left\lceil \frac{wt_L(a_{i2})}{4}\right\rceil + 2\left\lceil \frac{wt_L(a_{i1})}{4}\right\rceil\left(1-\left\lceil \frac{wt_L(a_{i2})}{4}\right\rceil\right)+\left\lceil \frac{wt_L(a_{i0})}{4}\right\rceil\left(1-\left\lceil \frac{wt_L(a_{i2})}{4}\right\rceil\right)\left(1-\left\lceil \frac{wt_L(a_{i1})}{4}\right\rceil\right)},$$

where a_{ij} is an element of i^{th} column and j^{th} row in a code word of $\mathcal{C}$, $i = 1, 2$ and $j = 0, 1, 2$. From Theorem 3.5.7, the Lee complete ρ-weight enumerator of code $\mathcal{C}^{\perp}$ is given by

$$\begin{aligned}
Lee_{\mathcal{C}^{\perp}}(X_{23}) &= \frac{1}{|\mathcal{C}|}\prod_{i=1}^{2}\ \prod_{j=0}^{2}(1+x_{i,j})^4 \sum_{P\in\mathcal{C}}\ \prod_{i=1}^{2}\ \prod_{j=0}^{2}\left(\frac{1-x_{i,j}}{1+x_{i,j}}\right)^{wt_L(a_{i,s-1-j})} \\
&= \frac{1}{4}(1+x_{10})^4(1+x_{11})^4(1+x_{12})^4(1+x_{20})^4(1+x_{21})^4(1+x_{22})^4\left(1+\left(\frac{1-x_{10}}{1+x_{10}}\right)^2\right. \\
&\left(\frac{1-x_{12}}{1+x_{12}}\right)^4\left(\frac{1-x_{20}}{1+x_{20}}\right)^2\left(\frac{1-x_{21}}{1+x_{21}}\right)^4+\left(\frac{1-x_{12}}{1+x_{12}}\right)^2\left(\frac{1-x_{21}}{1+x_{21}}\right)^2\left(\frac{1-x_{20}}{1+x_{20}}\right)^2 \\
&\left.+\left(\frac{1-x_{10}}{1+x_{10}}\right)^2\left(\frac{1-x_{12}}{1+x_{12}}\right)^2\left(\frac{1-x_{21}}{1+x_{21}}\right)^2\right) \\
&= \frac{1}{4}\left((1+x_{10})^4(1+x_{11})^4(1+x_{12})^4(1+x_{20})^4(1+x_{21})^4(1+x_{22})^4\right. \\
&+(1+x_{10})^2(1-x_{10})^2(1+x_{11})^4(1-x_{21})^4(1+x_{20})^2(1-x_{20})^2(1-x_{12})^4 \\
&(1+x_{22})^4+(1+x_{10})^4(1+x_{11})^4(1+x_{12})^2(1-x_{20})^2(1+x_{20})^2(1-x_{12})^2 \\
&(1-x_{21})^2(1+x_{21})^2(1-x_{22})^4+(1-x_{10})^2(1+x_{10})^2(1-x_{12})^2 \\
&\left.(1+x_{12})^2(1+x_{11})^4(1+x_{20})^4(1+x_{21})^2(1-x_{21})^2(1+x_{22})^4\right)\ .
\end{aligned}$$

Example 3.5.10. *Let* $\mathcal{C} = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2+2v & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2v \end{pmatrix}, \begin{pmatrix} 2+2v & 0 \\ 0 & 2+2v \end{pmatrix}\right\}$ *be a linear code over $\mathcal{M}_{2\times 2}(R)$. The Lee complete ρ-weight enumerator of $\mathcal{C}$ is*

$$Lee_{\mathcal{C}}(X_{22}) = 1\ +\ x_{10}^2\ x_{21}^4 +\ x_{21}^2\ +\ x_{10}^2\ x_{21}^2.$$

The ρ-weight enumerator of $\mathcal{C}$ is $1 + z^2 + 2z^3$, which is obtained by the transformation

$$z^{2\left\lceil \frac{wt_L(a_{i1})}{4}\right\rceil + \left\lceil \frac{wt_L(a_{i0})}{4}\right\rceil\left(1-\left\lceil \frac{wt_L(a_{i1})}{4}\right\rceil\right)},$$

where a_{ij} *is an element of* i^{th} *column and* j^{th} *row in a code word of* $\mathcal{C}$, $i = 1, 2$ *and* $j = 0, 1$. *From Theorem 3.5.7, the Lee complete* ρ*-weight enumerator of code* $\mathcal{C}^{\perp}$ *is given by*

$$\begin{aligned}
Lee_{\mathcal{C}^{\perp}}(X_{22}) &= \frac{1}{|\mathcal{C}|}\prod_{i=1}^{2}\prod_{j=0}^{1}(1+x_{i,j})^4 \sum_{P\in\mathcal{C}}\prod_{i=1}^{2}\prod_{j=0}^{1}\left(\frac{1-x_{i,j}}{1+x_{i,j}}\right)^{wt_L(a_{i,s-1-j})} \\
&= \frac{1}{4}(1+x_{10})^4(1+x_{11})^4(1+x_{20})^4(1+x_{21})^4 \\
&\left(1+\left(\frac{1-x_{11}}{1+x_{11}}\right)^2\left(\frac{1-x_{20}}{1+x_{20}}\right)^4+\left(\frac{1-x_{20}}{1+x_{20}}\right)^2+\left(\frac{1-x_{11}}{1+x_{11}}\right)^2\left(\frac{1-x_{20}}{1+x_{20}}\right)^2\right) \\
&= \frac{1}{4}(1+x_{10})^4(1+x_{11})^2(1+x_{21})^4\left((1+x_{11})^2(1+x_{20})^4+(1-x_{11})^2(1-x_{20})^4\right. \\
&\left.+(1+x_{11})^2(1+x_{20})^2(1-x_{20})^2+(1-x_{11})^2(1-x_{20})^2(1+x_{20})^2\right).
\end{aligned}$$

3.6 Self-dual codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$

A code $\mathcal{C}$ is said to be *self orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ and *self-dual* if $\mathcal{C} = \mathcal{C}^{\perp}$. A self-dual code is said to be *free* if it has a basis.

Theorem 3.6.1. *If* $\mathcal{C}$ *is a self-dual code over* R*, then so are* $\phi(\mathcal{C})$ *and* C_1 *and* C_2 *over* $\mathbb{Z}_4$.

Proof. This follows from Theorems 3.3.4 and 3.3.5. ■

Theorem 3.6.2. *A self-dual code of any length over* R *exists.*

Proof. Let $\mathcal{C}$ be a self-dual code of length n over R. We show that $\mathcal{C}$ can be of any length. Since $|\mathcal{C}||\mathcal{C}^{\perp}| = 16^n$ and $\mathcal{C}$ is a self-dual code, so $|\mathcal{C}|^2 = 16^n$. It implies that $|\mathcal{C}| = 16^{\frac{n}{2}} = 4^n$, which is a positive integer for all n. This shows that there may exist a self-dual code of any length n over R. Furthermore, the code of length 1 generated by $\langle 2 \rangle$ is a self-dual code over R. Therefore, by taking direct products of self-dual codes of length 1 we can obtain a self-dual code of any length n over R. ■

Lemma 3.6.3. *There is no free self-dual code of odd length over* R.

Proof. Let $\mathcal{C}$ be a free self-dual code of length n over R with basis A. Then $|\mathcal{C}| = 16^{k_0}$, where $k_0 = |A|$. Since $\mathcal{C}$ is self-dual, $|\mathcal{C}| = 16^{\frac{n}{2}}$. So, $k_0 = \frac{n}{2}$. Therefore n must be even. Hence there is no free self-dual code of odd length over R. ■

Theorem 3.6.4. *The length of any free self-dual code over R is at least* 8.

Proof. From Lemma 3.6.3, there is no free self-dual code of odd length over R. Suppose that there is a free self-dual code of length 2 over R. Then it must contain a codeword $(1,\ x)$, where $x \in R$. So $1 + x^2 = 0 \pmod 4$, which is impossible in R, since there is no element satisfying this relation. Therefore, there is no free self-dual code of length 2 over R.

Let $\mathcal{C}$ be a free self-dual code of length 4 generated by $G = (g_1,\ g_2)^T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{pmatrix}$, where $a_i,\ b_i \in R$. Since $\mathcal{C}$ is free, $g_1,\ g_2$ are linearly independent and hence both must contain at least one unit in its coordinates. So after some row transformations and column permutations, G can be written as $\begin{pmatrix} 1 & 0 & c_1 & d_1 \\ 0 & 1 & c_2 & d_2 \end{pmatrix}$ for some $c_i,\ d_i \in R,\ i = 1, 2$. Now since $\mathcal{C}$ is self-dual, $1 + c_i^2 + d_i^2 = 0$, which implies that either c_i^2 or d_i^2 is 2. But there is no element in R satisfying $x^2 = 2$. So $\mathcal{C}$ cannot be self-dual. Therefore there is no free self-dual code of length 4 over R.

Suppose that there is a free self-dual code of length 6 over R generated by a matrix G. After some row transformations and permutations of columns, G can be written as $\mathrm{G}' = \begin{pmatrix} 1 & 0 & 0 & a_{11} & a_{12} & a_{13} \\ 0 & 1 & 0 & a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 & a_{31} & a_{32} & a_{33} \end{pmatrix}$, where each $a_{ij} \in R,\ i, j = 1, 2, 3$. Since $\mathcal{C}$ is self-dual, $1 + \sum_{j=1}^{3} a_{ij}^2 = 0$ for $i = 1, 2, 3$, and $\sum_{j=1}^{3} a_{ij}a_{ik} = 0$ for $i \neq k,\ i, k = 1, 2, 3$. It implies from the first equation that a_{ij} is a unit in R. Thus we get a contradiction from second equation, as sum of three units never zero in R. Therefore there is no free self-dual code of length 6 over R.

Consider $G = (g_1, g_2, g_3, g_4)^T = \begin{pmatrix} 1 & 0 & 0 & 0 & a_{11} & a_{12} & a_{13} & a_{14} \\ 0 & 1 & 0 & 0 & a_{21} & a_{22} & a_{23} & a_{24} \\ 0 & 0 & 1 & 0 & a_{31} & a_{32} & a_{33} & a_{34} \\ 0 & 0 & 0 & 1 & a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$, where in each row one a_{ij} is zero and rest are units in R for $j = 1, 2, 3, 4$ such that $a_{i1}a_{k1} + a_{i2}a_{k2} + a_{i3}a_{k3} + a_{i4}a_{k4} = 0$, for $i \neq k$. Such a matrix exists over R (See Example 3.6.7). Clearly, the rows g_1, g_2, g_3, g_4 of G are linearly independent, self-orthogonal and orthogonal to other rows of

G. So the code $\mathcal{C}$ generated by G is a free self-orthogonal code of length 8 over R. We know that $|\mathcal{C}^{\perp}| = \frac{16^8}{|\mathcal{C}|} = 16^4 = |\mathcal{C}|$. Therefore $\mathcal{C}$ is self-dual. Hence the length of a free self-dual code over R is at least 8. ■

Theorem 3.6.5. *If $\mathcal{C}$ is a self-dual code of length n over R, then it must contain the codeword $(2, 2, \ldots, 2)$ and hence $(2v, 2v, \ldots, 2v)$ and $(2 + 2v, 2 + 2v, \ldots, 2 + 2v)$.*

Proof. The ring R can be partitioned into 4 sets as $A_0 = \{0, 2, 2v, 2 + 2v\}$, $A_1 = \{1, 3, 1 + 2v, 3 + 2v\}$, $A_v = \{v, 3v, 2 + v, 2 + 3v\}$, $A_{1+3v} = \{1 + v, 1 + 3v, 3 + v, 3 + 3v\}$, where A_i, $i = 0, 1, v, 1 + 3v$, contains the elements $a \in R$ such that $a^2 = i$. Let $c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$ and n_i denote the number of components of c which are from A_i for each $i = 0, 1, v, 1 + 3v$.

Since $\mathcal{C}$ is a self-dual code, we have $\langle c, c\rangle = 0$ for all $c \in \mathcal{C}$, which implies that $\sum_{i=1}^{n} c_i^2 = 0$. So, $\langle c, c\rangle = n_1 + v\ n_v + (1 + 3v)\ n_{1+3v} = 0$. It follows then that, $(c_1, c_2, \ldots, c_n) \cdot (2, 2, 2, \ldots, 2) = 2n_1 + (2v)n_v + (2 + 2v)n_{1+3v} = 2(n_1 + v\ n_v + (1 + 3v)\ n_{1+3v}) = 0$. Therefore, $(2, 2, \ldots, 2) \in \mathcal{C}^{\perp}$. Since $\mathcal{C}$ is self-dual, $(2, 2, \ldots, 2) \in \mathcal{C}$. The rest follows from the linearity of $\mathcal{C}$. ■

3.6.1 Construction of self-dual codes

Theorem 3.6.6. *Let $G = [I_n \mid A_n]$, where $A_n = (a_{ij})$, be a square matrix of order n such that $\sum_{j=1}^{n} a_{ij} = 1$ or 3, for $i = 1, 2, \ldots, n$. If G is a generator matrix of a free self-dual code $\mathcal{C}$ of length $2n$ (n is an even integer) over R, then*

$$G' = \begin{pmatrix} I_n & B_n & \cdots & B_n & A_n & B_n & \cdots & B_n \\ B_n & I_n & \cdots & B_n & B_n & A_n & \cdots & B_n \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ B_n & B_n & \cdots & I_n & B_n & B_n & \cdots & A_n \end{pmatrix}$$

generates a free self-dual code $\mathcal{C}'$ of length $2kn$ over R, where B_n is an all α matrix of order n, α a unit in R, and B_n is being repeated $2(k-1)$ times in each row of G'.

Proof. Let G be a generator matrix of a free self-dual code $\mathcal{C}$ of length $2n$, where n is an even integer. Since $\mathcal{C}$ is self-dual, $1 + \sum_{j=1}^{n} a_{ij}^2 = 0$ and $\sum_{k=1}^{n} a_{ik}a_{jk} = 0$ for $i \neq j$,

$i, j = 1, 2, \ldots, n$.

Now let $G' = [g'_1,\ g'_2,\ \ldots,\ g'_k]^T$, where g'_j represent the rows of $n \times n$ matrices in G', $j = 1, 2, \ldots, k$, as shown above and T represents the transpose. It is clear that the rows of each g'_j are independent and then so are the rows of G'. Therefore, it generates a free code, say $\mathcal{C}'$, of length $2kn$ and so $|\mathcal{C}'| = 16^{kn}$.

Now let each row of g'_j be g'_{jl}, $l = 1, 2, \ldots, n$. Then $g'_{jl} \cdot g'_{jl} = 1 + 2(k-1)n\alpha^2 + \sum_{k=1}^{n} a_{lk}^2 = 0$, as n is even and $1 + \sum_{k=1}^{n} a_{lk}^2 = 0$. Again $g'_{jl} \cdot g'_{js} = 2(k-1)n\alpha^2 + \sum_{k=1}^{n} a_{lk}a_{sk} = 0$, as n is even and $\sum_{k=1}^{n} a_{lk}a_{sk} = 0$ for $s \neq l$. Therefore, any row of g'_j is orthogonal to all the rows of g'_j. Similarly, we can see that the rows of g'_j are orthogonal to the rows of g'_k for $j \neq k$, as $2\alpha + 2(k-2)n\alpha^2 + 2\alpha\left(\sum_{k=1}^{n} a_{lk}\right) = 0$. Therefore the code $\mathcal{C}'$ generated by G' is self-orthogonal. Since $|(\mathcal{C}')^{\perp}| = \frac{16^{2kn}}{|\mathcal{C}'|} = 16^{kn} = |\mathcal{C}'|$, $\mathcal{C}'$ is self-dual. ■

Example 3.6.7. *Let $\mathcal{C}$ be the self-dual code of length 8 over R generated by*

$$G = \begin{pmatrix} 1000 & 0 & 1+2v & 3+2v & 3 \\ 0100 & 1 & 1 & 1 & 0 \\ 0010 & 3+2v & 0 & 1+2v & 3 \\ 0001 & 1+2v & 3+2v & 0 & 3 \end{pmatrix}.$$

Then the matrix

$$G' = \begin{pmatrix} I_4 & B_4 & A_4 & B_4 \\ B_4 & I_4 & B_4 & A_4 \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,0 & \alpha\alpha\alpha\alpha & 0\ a\ b\ 3 & \alpha\alpha\alpha\alpha \\ 0\,1\,0\,0 & \alpha\alpha\alpha\alpha & 1\,1\,1\,0 & \alpha\alpha\alpha\alpha \\ 0\,0\,1\,0 & \alpha\alpha\alpha\alpha & b\ 0\ a\ 3 & \alpha\alpha\alpha\alpha \\ 0\,0\,0\,1 & \alpha\alpha\alpha\alpha & a\ b\ 0\ 3 & \alpha\alpha\alpha\alpha \\ \alpha\alpha\alpha\alpha & 1\,0\,0\,0 & \alpha\alpha\alpha\alpha & 0\ a\ b\ 3 \\ \alpha\alpha\alpha\alpha & 0\,1\,0\,0 & \alpha\alpha\alpha\alpha & 1\,1\,1\,0 \\ \alpha\alpha\alpha\alpha & 0\,0\,1\,0 & \alpha\alpha\alpha\alpha & b\ 0\ a\ 3 \\ \alpha\alpha\alpha\alpha & 0\,0\,0\,1 & \alpha\alpha\alpha\alpha & a\ b\ 0\ 3 \end{pmatrix},$$

with $a = 1 + 2v$ and $b = 3 + 2v$, generates a free self-dual code of length 16 over R and its minimum Gray distance is 4.

The following theorem is a generalization of [71, Proposition 3.4].

Theorem 3.6.8. *Let $G = (g_1, g_2, \ldots, g_n)^T$, where $g_i = (g_{i1}, g_{i2}, \ldots, g_{in})$, be a generator matrix of a free self-dual code $\mathcal{C}$ of length $2n$ over R. Let $X \in R^n$ such that $1 + X^2 = 0$, and $Y_i := X \cdot g_i$. Then $G' = \begin{pmatrix} 1 & 0 & 0 & 0 & X \\ 3Y & Y & Y & Y & G \end{pmatrix}$ generates a free self-orthogonal code $\mathcal{C}'$ of length $(2n+4)$ over R, where $Y = (Y_1, Y_2, \ldots, Y_n)^T$.*

Proof. Let G be a generator matrix of a free self-dual code $\mathcal{C}$ of length $2n$. It can easily be seen that the rows of G' are linearly independent. So, G' generates a free code $\mathcal{C}'$ over R. Since $\mathcal{C}$ is self-dual, $1 + \sum_{j=1}^{n} g_{ij}^2 = 0$ and $\sum_{k=1}^{n} g_{ik}g_{jk} = 0$ for $i \neq j$, $i, j = 1, 2, \ldots, n$. The first row of G' is self-orthogonal and orthogonal to other rows, as $1 + X^2 = 0$ and $Y_i := X \cdot g_i$, $3Y_i + X \cdot g_{ij} = 0$, $i = 1, 2, \ldots, n$. The other rows of G' are also self-orthogonal and orthogonal to other rows, as $4Y_i^2 + \sum_{j=1}^{n} g_{ij}^2 = 0$ and $4Y_iY_j + \sum_{k=1}^{n} g_{ik}g_{jk} = 0$ for $i \neq j$, $i, j = 1, 2, \ldots, n$. Therefore, the code $\mathcal{C}'$ generated by G' is self-orthogonal. ∎

Example 3.6.9. *The matrix $G = \begin{pmatrix} 1000 & 0 & 1+2v & 3+2v & 3 \\ 0100 & 1 & 1 & 1 & 0 \\ 0010 & 3+2v & 0 & 1+2v & 3 \\ 0001 & 1+2v & 3+2v & 0 & 3 \end{pmatrix}$ generates a free self-dual code of length 8 over R.*

From the above code, we can construct a self-orthogonal code over R, as follows:

Let $X = (2+v,\ 0,\ 1,\ 3+v,\ 0,\ 3,\ 0,\ 2v)$. Then clearly $1 + X^2 = 0$. Since $Y_i = X \cdot g_i$, $Y = (1+v,\ 3,\ 1+2v,\ v)^T$, therefore

$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 2+v & 0 & 3+v & 1 & 0 & 3 & 0 & 2v \\ 3+3v & 1+v & 1+v & 1+v & 1 & 0 & 0 & 0 & 0 & 1+2v & 3+2v & 3 \\ 1 & 3 & 3 & 3 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 3+2v & 1+2v & 1+2v & 3+v & 0 & 0 & 1 & 0 & 3+2v & 0 & 1+2v & 3 \\ 3v & v & v & v & 0 & 0 & 0 & 1 & 1+2v & 3+2v & 0 & 3 \end{pmatrix}$$

generates a free self-orthogonal code of length 12.

3.7 Conclusion

In this chapter, we have studied linear codes over $R = \mathbb{Z}_4 + v\mathbb{Z}_4$, $v^2 = v$. We have obtained a MacWillaims type identity for linear codes over R with respect to Lee, Gray and RT metrics. We have given a transformation to obtain the ρ-weight enumerator from the Lee complete ρ-weight enumerator of a code. Some characterizations of self-dual codes over R are provided. We have proposed a new construction method for self-dual codes over R and also generalized a construction method for self-dual codes over Galois rings to self-orthogonal codes over R.

Chapter 4

Self-dual codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$

4.1 Introduction

Self-dual codes over finite fields have been studied extensively [59,69,70,72,74]. They are an interesting class of codes as they often produce optimal codes and have many links to other areas of mathematics such as lattices, t-designs, Hadamard matrices and quantum stabilizer codes [95]. The search for self-dual codes with good parameters is an interesting problem in coding theory. Several methods have been proposed by researchers to obtain good codes over finite fields, like quadratic residue codes, double circulant codes, etc. In recent years, the construction of self-codes over finite rings has got the attention of researchers [69–72,74]. In [59], Harada has introduced an easy way to generate many binary self-dual codes from a self-dual code of a smaller length. Kim [69] has introduced a building-up construction for self-dual codes over $\mathbb{F}_2$. This construction has been generalized to the codes over finite fields $\mathbb{F}_q$ [70], Galois rings [71] and finite chain rings [72]. Alfaro and Dhul-Qarnayn [6] have proposed a more general method for constructing self-dual codes over $\frac{\mathbb{F}_q[u]}{\langle u^t \rangle}$ and over finite chain rings, through which one can obtain the self-dual codes obtained by methods proposed in [69–71]. In this chapter, we introduce another new ring $\mathbb{Z}_4 + w\mathbb{Z}_4$, $w^2 = 2w$ and study linear and self-dual codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$.

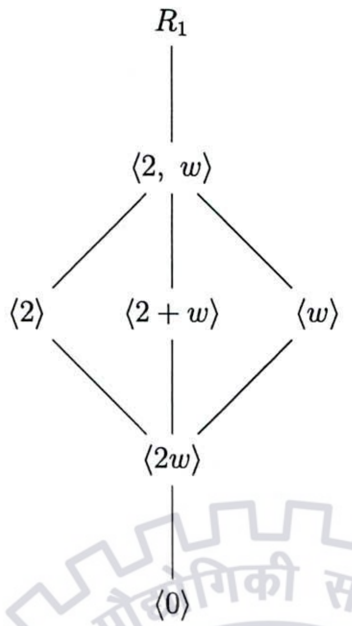

Figure 4.1: Lattice diagram of ideals of $\mathbb{Z}_4 + w\mathbb{Z}_4$

4.2 Linear codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$

Let R be the ring $\mathbb{Z}_4+w\mathbb{Z}_4 = \{0, 1, 2, 3,\ w, 2w, 3w,\ 1+w, 1+2w, 1+3w,\ 2+w, 2+2w, 2+3w,\ 3+w, 3+2w, 3+3w\}$, where $w^2 = 2w$. The units of R are $\{a+wb\ :\ a \text{ is a unit in } \mathbb{Z}_4\}$ and each unit is a self-inverse. R has 7 ideals in all. Figure 4.1 presents the lattice diagram of ideals of R. R is a local ring of characteristic 4 with $\langle 2, w\rangle$ as its unique maximal ideal. From the ideals of R, we can see that they do not form a chain; for instance, the ideals $\langle w\rangle$ and $\langle 2\rangle$ are not comparable. Therefore, R is a non-chain extension of $\mathbb{Z}_4$. Also R is not a principal ideal ring; for example, the ideal $\langle 2, w\rangle$ is not generated by any single element of R. We have $\frac{R}{\langle 2,\ w\rangle} \cong \mathbb{Z}_2$.

We can see that R is a group ring over $\mathbb{Z}_4$, as the multiplicative group $S = \{1,\ 1+w\}$ of two units 1 and $1+w$ of R generates R over $\mathbb{Z}_4$, i.e., $R = \mathbb{Z}_4[S]$. In other words, R is a free module over $\mathbb{Z}_4$ with S as a basis.

As in the previous chapter, we define the Gray map on R as a map $\psi :\ R \to \mathbb{Z}_4^2$ such that

$$\psi(a+wb) = (b,\ a+b)\ ,$$

for any $a+wb \in R$. ψ is an analogue of the Gray map on $\mathbb{Z}_4$ (Definition 2.3.21). This map is then extended component wise to $\phi:\ R^n \rightarrow \mathbb{Z}_4^{2n}$, so that for any $x = (x_1, x_2, \ldots, x_n) \in R^n$,

$$\phi(x) = (s,\ r + s),$$

where $r = (a_1, a_2, \ldots, a_n)$, $s = (b_1, b_2, \ldots, b_n) \in \mathbb{Z}_4^n$ and $x_j = a_j + wb_j, j = 1, 2, \ldots, n$. ϕ can easily be seen to be a $\mathbb{Z}_4$-module isomorphism. As noted earlier, the Lee weight and the Euclidean weight of any $x \in R^n$ are defined as the corresponding weights of its Gray image, i.e., $wt_L(x) = wt_L(b,\ a + b)$ and $wt_E(x) = wt_E(b,\ a + b)$.

A linear code $\mathcal{C}$ of length n over R is an R-submodule of the R-module R^n. The *dual* of $\mathcal{C}$ is the code $\mathcal{C}^\perp := \{x \in R^n :\ x \cdot y = 0, \forall y \in \mathcal{C}\}$, where $x \cdot y$ denotes the usual inner product of x and y over R. The ring R is a Frobenius ring [135] and hence $|\mathcal{C}||\mathcal{C}^\perp| = |R|^n$ [135]. Since the ring R is not a chain ring, it is difficult to write the standard form generator matrix for codes over R. However we can find a minimal set of generators for such codes.

Theorem 4.2.1. *The Gray map ϕ is a linear isometry with respect to the Lee and Euclidean distances in R^n and $\mathbb{Z}_4^{2n}$.*

Proof. Same as that of Lemma 3.3.1. ■

Theorem 4.2.2. *Let $\mathcal{C}$ be a $[n,\ M,\ d]$ linear code over R. Then $\phi(\mathcal{C})$ is a $[2n,\ M,\ d]$ linear code over $\mathbb{Z}_4$, where d is either Lee or Euclidean distance and $M = |\mathcal{C}|$.*

Proof. The result follows from Theorem 4.2.1. ■

Theorem 4.2.3. *Let $\mathcal{C}$ be a linear code of length n over R. Then $\phi(\mathcal{C}^\perp) = \phi(\mathcal{C})^\perp$.*

Proof. Let $\phi(c') \in \phi(\mathcal{C}^\perp)$, where $c' = a' + wb' \in \mathcal{C}^\perp$, and let $c = a + wb \in \mathcal{C}$. Now $c' \cdot c = 0$, implying that $a' \cdot a = 0$ and $a \cdot b' + a' \cdot b + 2(b' \cdot b) = 0$. Then $\phi(c) \cdot \phi(c') = (b,\ a + b) \cdot (b',\ a' + b') = (a \cdot a') + 2(b \cdot b') + (a \cdot b' + a' \cdot b) = 0$. This implies that $\phi(c') \in \phi(\mathcal{C})^\perp$, as $\phi(c) \in \phi(\mathcal{C})$. Therefore $\phi(\mathcal{C}^\perp) \subseteq \phi(\mathcal{C})^\perp$.

On the other hand, since ϕ is a module isomorphism and the Gray image $\phi(\mathcal{C})$ of $\mathcal{C}$ is a $\mathbb{Z}_4$-code of length $2n$, $|\phi(\mathcal{C})^\perp| = \frac{4^{2n}}{|\phi(\mathcal{C})|} = \frac{16^n}{|\mathcal{C}|} = |\mathcal{C}^\perp| = |\phi(\mathcal{C}^\perp)|$. Hence $\phi(\mathcal{C}^\perp) = \phi(\mathcal{C})^\perp$. ■

A map satisfying Theorem 4.2.3 is called *dual preserving map* [86]. Therefore ϕ is a dual preserving map. Since R is a Frobenius ring, for any linear code $\mathcal{C}$ of length n,

$|\mathcal{C}||\mathcal{C}^{\perp}| = 16^n$, and MacWilliams identities hold for a linear code $\mathcal{C}$ over R. First we define Lee weight enumerator as it was defined for a linear code over $\mathbb{Z}_4+v\mathbb{Z}_4$ in Chapter 3, Section 3.4.1. The Lee weight enumerator of a linear code $\mathcal{C}$ over R is a homogenous polynomial of degree $4n$ defined by $\mathrm{Lee}_{\mathcal{C}}(x,\ y) = \sum_{c\in\mathcal{C}} x^{4n-wt_L(c)}y^{wt_L(c)}$.

Theorem 4.2.4. *[86] Let $\mathcal{C}$ be a linear code of length n over R. Then*

$$Lee_{\mathcal{C}^{\perp}}(x,\ y) = \frac{1}{|\mathcal{C}|}\ Lee_{\mathcal{C}}(x+y,\ x-y)\ .$$

Proof. We know from Theorem 2.3.20 that the MacWillaims identities hold for linear codes over $\mathbb{Z}_4$. Now from Theorems 4.2.1 and 4.2.3, we get that

$$\begin{aligned}\mathrm{Lee}_{\mathcal{C}^{\perp}}(x,\ y) &= \mathrm{Lee}_{\phi(\mathcal{C}^{\perp})}(x,\ y)\\ &= \mathrm{Lee}_{\phi(\mathcal{C})^{\perp}}(x,\ y)\\ &= \frac{1}{|\phi(\mathcal{C})|}\mathrm{Lee}_{\phi(\mathcal{C})}(x+y,\ x-y)\\ &= \frac{1}{|\mathcal{C}|}\mathrm{Lee}_{\mathcal{C}}(x+y,\ x-y)\ .\end{aligned}$$

■

Remark 4.2.5. *One can also derive the MacWilliams identities for a linear code over R by defining a character on a non-trivial ideal I of R as $\chi : I \to \mathbb{C}^*$ such that $\chi(a+wb) = i^{a+b}$, where $a+wb \in I$, as was defined for linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ in Chapter 3, Section 3.4.*

The following examples are due to Martínez et al. [86].

Example 4.2.6. *Let $\mathcal{C}$ be the code generated by*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 2+2w & 3+3w & 3+3w & 3+3w\\ 0 & 1 & 0 & 0 & 3+3w & 2+2w & 3+3w & 1+w\\ 0 & 0 & 1 & 0 & 3+3w & 1+w & 2+2w & 3+3w\\ 0 & 0 & 0 & 1 & 3+3w & 3+3w & 1+w & 2+2w \end{pmatrix}.$$

Then the Lee and Euclidean weight enumerators of $\phi(\mathcal{C})$ are given by

$$\begin{aligned} W_L(\mathcal{C}) &= 1 + 380z^8 + 1920z^{10} + 7168z^{12} + 13440z^{14} + 19718z^{16} + 13440z^{18} \\ &+ 7168z^{20} + 1920z^{22} + 380z^{24} + z^{32} \end{aligned}$$

and

$$\begin{aligned} W_E(\mathcal{C}) &= 1 + 224z^8 + 2176z^{12} + 7836z^{16} + 14848z^{20} + 17088z^{24} + 13056z^{28} \\ &+ 6932z^{32} + 2560z^{36} + 608z^{40} + 128z^{44} + 28z^{48} + z^{64}, \end{aligned}$$

respectively.

Example 4.2.7. *Let $\mathcal{C}$ be the code of length 8 over R generated by*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 2w & 3+3w & 3+3w & 3+3w \\ 0 & 1 & 0 & 0 & 3+3w & 2w & 1+3w & 3+w \\ 0 & 0 & 1 & 0 & 3+3w & 3+w & 32w & 1+3w \\ 0 & 0 & 0 & 1 & 3+3w & 1+3w & 3+w & 2w \end{pmatrix}.$$

Then the Lee and Euclidean weight enumerators of $\phi(\mathcal{C})$ are given by

$$\begin{aligned} W_L(\mathcal{C}) &= 1 + 508z^8 + 896z^{10} + 10752z^{12} + 6272z^{14} + 28678z^{16} + 6272z^{18} \\ &+ 10752z^{20} + 896z^{22} + 508z^{24} + z^{32} \end{aligned}$$

and

$$W_E(\mathcal{C}) = 1 + 480z^8 + 15516z^{12} + 34496z^{24} + 13638z^{32} + 1376z^{40} + 28z^{48} + z^{64},$$

respectively.

4.3 Self-dual codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$

In this section, we study self-dual codes over R.

Theorem 4.3.1. *A self-dual code of any length over R exists.*

Proof. Let $\mathcal{C}$ be a self-dual code of length n over R. We show that $\mathcal{C}$ can be of any length. Since $|\mathcal{C}||\mathcal{C}^{\perp}| = 16^n$ and $\mathcal{C}$ is a self-dual code, so $|\mathcal{C}|^2 = 16^n$. It implies that $|\mathcal{C}| = 16^{\frac{n}{2}} = 4^n$, which is a positive integer for all n. This shows that there may exist a self-dual code of any length n. Furthermore, the code of length 1 generated by $\langle 2 \rangle$ is a self-dual code. Therefore, by taking direct products of self-dual codes of length 1 we can obtain a self-dual code of any length n over R. ■

We note here that no free self-dual code of odd length exists over R. This is because of the fact that for a free self-dual code of free rank k and length n over R we have $|\mathcal{C}| = 16^k = 16^{\frac{n}{2}}$, which implies that $k = \frac{n}{2}$.

In [48], Dougherty et al. have shown that a free self-dual code of even length and of length a multiple of 4 over a commutative Frobenious ring $\mathcal{R}$ with unique maximal ideal M exists if $|\frac{\mathcal{R}}{M}| = 1$ or 3 (mod 4). However they have not discussed about the case $|\frac{\mathcal{R}}{M}| = 2$ (mod 4). The following theorem shows the existence of free self-dual codes over R when $|\frac{R}{M}| = 2$ (mod 4) over R.

Theorem 4.3.2. *The length of any free self-dual code over R is at least* 8.

Proof. We know that no free self-dual code of odd length exists over R. If there exists a free self-dual code $\mathcal{C}$ of length 2 over R, then it must contain a codeword $(1,\ x)$ or $(x,\ 1)$, where $x \in R$. Since $\mathcal{C}$ is self-dual, $1 + x^2 = 0$ (mod 4), which is impossible in R, as there is no element in R satisfying this relation. Therefore, there is no free self-dual code of length 2 over R.

Let $\mathcal{C}$ be a free self-dual code of length 4 over R with a generator matrix G. After some row operations and column permutations on G, it can be written as $G' = (g_1,\ g_2)^T$, where $g_1 = (1, 0, a_{11}, a_{12})$ and $g_2 = (0, 1, a_{21}, a_{22})$, $a_{ij} \in R$, $i,\ j = 1, 2$. Since $\mathcal{C}$ is self-dual, $g_i^2 = 1 + a_{i1}^2 + a_{i2}^2 = 0$ (mod 4) for $i = 1, 2$. But no two elements a, b of R satisfy this relation. Therefore, there does not exist any free self-dual code of length 4 over R.

Now let $\mathcal{C}$ be a free self-dual code of length 6 over R generated by

$$G = \begin{pmatrix} 1 & 0 & 0 & a_{11} & a_{12} & a_{13} \\ 0 & 1 & 0 & a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 & a_{31} & a_{32} & a_{33} \end{pmatrix},$$

where $a_{ij} \in R,\ i,\ j = 1, 2, 3$ (if G is not in this form, we can reduce G to this form by elementary row operations and column permutations). Since $\mathcal{C}$ is self-dual, $1 + a_{i1}^2 + a_{i2}^2 + a_{i3}^2 = 0$ for $i = 1, 2, 3$. It implies that $a_{ij},\ i,\ j = 1, 2, 3$, are units. Since each row of G is orthogonal to other rows, we get $a_{i1}a_{j1} + a_{i2}a_{j2} + a_{i3}a_{j3} = 0$ for $i \neq j$, which is a contradiction, as the sum of three units is a unit in R. Hence there does not exist any free self-dual code of length 6 over R.

Now we show the existence of a free self-dual code of length 8 over R. Let $\mathcal{C}$ be a linear code generated by

$$G = (g_1, g_2, g_3, g_4)^T = \begin{pmatrix} 1 & 0 & 0 & 0 & a_1 & a_2 & a_3 & 0 \\ 0 & 1 & 0 & 0 & -a_2 & a_1 & 0 & a_3 \\ 0 & 0 & 1 & 0 & a_3 & 0 & -a_1 & a_2 \\ 0 & 0 & 0 & 1 & 0 & -a_3 & a_2 & a_1 \end{pmatrix},$$

where $a_j,\ j = 1, 2, 3, 4$, is a unit in R. Clearly the rows g_i of G are linearly independent. Since the units of R are self-inverse, $1 + a_1^2 + a_2^2 + a_3^2 = 0$. So, the rows g_i of G are self-orthogonal. Thus the code $\mathcal{C}$ generated by G is a free self-orthogonal code over R and $|\mathcal{C}| = 16^4$. Now $|\mathcal{C}^{\perp}| = \frac{16^8}{|\mathcal{C}|} = 16^4 = |\mathcal{C}|$. Therefore $\mathcal{C}$ is self-dual. Hence the length of a free self-dual code over R is at least 8. ■

Corollary 4.3.3. *There exists a free self-dual code of length a multiple of* 8 *over* R.

Proof. By Theorem 4.3.2, there exists a free self-dual code $\mathcal{C}$ of length 8 over R. Hence by taking the direct products of $\mathcal{C}$ we can obtain a free self-dual code of length a multiple of 8 over R. ■

Example 4.3.4. *The matrix* $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1+w & 0 \\ 0 & 1 & 0 & 0 & 3+3w & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 3+3w & 1 & 3 \\ 0 & 0 & 0 & 1 & 3+3w & 1+w & 0 & 3 \end{pmatrix}$ *generates a free self-dual code of length* 8 *over* R *and its minimum Hamming distance is* 4.

Theorem 4.3.5. *A self-dual code of length* n *over* R *contains the codeword* $(2w, 2w, \dots, 2w)$.

Proof. The ring R can be partitioned into 3 sets as $A_0 = \{0, 2, 2w, 2+2w\}$, $A_1 = \{1, 3, 1+w, 1+2w, 1+3w, 3+w, 3+2w, 3+3w\}$, $A_{2w} = \{w, 3w, 2+w, 2+3w\}$, where A_j, $j = 0, 1, 2w$, contain the elements $a \in R$ such that $a^2 = j$. Let $c = (c_1, c_2, \dots, c_n) \in \mathcal{C}$ and $n_j(c)$ denote the number of components of c which are from A_j, $j = 0, 1, 2w$.

Since $\mathcal{C}$ is a self-dual code, we have $c \cdot c = 0$ for all $c \in \mathcal{C}$, which implies that $\sum_{i=1}^{n} c_i^2 = 0$. Therefore, $c \cdot c = n_1(c) + (2w)n_{2w}(c) = 0$. It implies that $n_{2w}(c)$ is even and $n_1(c)$ is a multiple of 4.

Now for any codeword $(c_1, c_2, \dots, c_n) \in \mathcal{C}$, we have $(c_1, c_2, \dots, c_n) \cdot (2w, 2w, \dots, 2w) = (2w)n_1(c) = 0$, as $(2w) \cdot (unit) = 2w$; $(2w) \cdot (non-unit) = 0$ in R, and $n_1(c)$ is even. Therefore, $(2w, 2w, \dots, 2w) \in \mathcal{C}^{\perp}$. Since $\mathcal{C}$ is self-dual, $(2w, 2w, \dots, 2w) \in \mathcal{C}$. ■

Theorem 4.3.6. *If* $\mathcal{C}$ *is a self-dual code over* R, *then so is* $\phi(\mathcal{C})$ *over* $\mathbb{Z}_4$.

Proof. This follows from Theorem 4.2.3. ■

Define $\mu : R \to \mathbb{Z}_4$ such that $\mu(a + wb) = a$ and $\nu : R \to \mathbb{Z}_4$ such that $\nu(a + wb) = b$. These projection maps are linear and can be extended to R^n component wise. It is easy to see that if $\mathcal{C}$ is a linear code over R then so are $\mu(\mathcal{C})$, $\nu(\mathcal{C})$ over $\mathbb{Z}_4$.

Theorem 4.3.7. *Let* $\mathcal{C}$ *be a self-dual code over* R. *Then* $\mu(\mathcal{C})$ *and* $\nu(\mathcal{C})$ *are self-orthogonal codes over* $\mathbb{Z}_4$.

Proof. Let $\mathcal{C}$ be a self-dual code over R and $c_1, c_2 \in \mathcal{C}$, where $c_1 = a_1 + wb_1, c_2 = a_2 + wb_2$. Since $\mathcal{C}$ is self-dual, $c_1 \cdot c_2 = 0$, which implies that $a_1 \cdot a_2 + b_1 \cdot b_2 = 0$ and $a_1 \cdot b_2 + a_2 \cdot b_1 = 0$.

Now from Theorem 4.3.6, $\phi(\mathcal{C})$ is self-dual over $\mathbb{Z}_4$. Then $\phi(c_1) \cdot \phi(c_2) = 0$ for $c_1, c_2 \in \mathcal{C}$. This implies that $2(b_1 \cdot b_2) + a_1 \cdot a_2 + a_1 \cdot b_2 + a_2 \cdot b_1 = 0$, as $\phi(a + wb) = (b, a + b)$. This in turn implies that $b_1 \cdot b_2 = 0$ and $a_1 \cdot a_2 = 0$, as $a_1 \cdot b_2 + a_2 \cdot b_1 = 0$ and $a_1 \cdot a_2 + b_1 \cdot b_2 = 0$. Therefore $\mu(\mathcal{C})$ and $\nu(\mathcal{C})$ are self-orthogonal codes over $\mathbb{Z}_4$. ∎

Theorem 4.3.8. *The minimum Hamming distance of a free self-dual code $\mathcal{C}$ over R is at most $\frac{n}{2} + 1$.*

Proof. Let $\mathcal{C}$ be a free self-dual code $\mathcal{C}$ of free rank k over R, and let $d_H(\mathcal{C})$ be the minimum Hamming distance of $\mathcal{C}$. Since $\mathcal{C}$ is a self-dual code, $k = \frac{n}{2}$. Then from the Singleton bound, $d_H(\mathcal{C}) \leq n - \frac{n}{2} + 1 = \frac{n}{2} + 1$. ∎

4.3.1 A construction of self-dual codes

In this subsection we give a construction of self-dual codes over R.

Theorem 4.3.9. *Let $G = [I_n \mid A_n]$, where $A_n = (a_{jk})$, be a square matrix of order n such that $\sum_{k=1}^{n} a_{jk} = 1$, for $j = 1, 2, \ldots, n$. If G is a generator matrix of a free self-dual code $\mathcal{C}$ of length $2n$ (n an even integer) over R, then*

$$G' = \begin{pmatrix} I_n & B_n & \cdots & B_n & A_n & B_n & \cdots & B_n \\ B_n & I_n & \cdots & B_n & B_n & A_n & \cdots & B_n \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ B_n & B_n & \cdots & I_n & B_n & B_n & \cdots & A_n \end{pmatrix}$$

generates a free self-dual code $\mathcal{C}'$ of length $2kn$ over R, where B_n is an all α matrix of order n, α a unit in R, and B_n is being repeated $2(k-1)$ times in each row of G'.

Proof. Let G be a generator matrix of a free self-dual code $\mathcal{C}$ of length $2n$, where n is an even integer. Since $\mathcal{C}$ is self-dual, $1 + \sum_{k=1}^{n} a_{jk}^2 = 0$ and $\sum_{k=1}^{n} a_{jk} a_{lk} = 0$ for $j \neq l$, $j, l = 1, 2, \ldots, n$.

Now let $G' = [g_1' \ g_2' \ \cdots \ g_k']^T$, where g_j' represent the rows of $n \times n$ matrices in G', $j = 1, 2, \cdots, k$, as shown above and T represents the transpose. It is clear that the rows of each g_j' are independent and hence so are the rows of G'. Therefore, G' generates a free code, say $\mathcal{C}'$, of length $2kn$ and hence $|\mathcal{C}'| = 16^{kn}$.

Now let the rows of g'_j be g'_{jl}, $l = 1, 2, \ldots, n$. Then $g'_{jl} \cdot g'_{jl} = 1 + 2(k-1)n\alpha^2 + \sum_{k=1}^{n} a_{lk}^2 = 0$, as n is even and $1 + \sum_{k=1}^{n} a_{lk}^2 = 0$. Again $g'_{jl} \cdot g'_{js} = 2(k-1)n\alpha^2 + \sum_{k=1}^{n} a_{lk}a_{sk} = 0$, as n is even and $\sum_{k=1}^{n} a_{lk}a_{sk} = 0$ for $s \neq l$. Therefore, the rows of g'_j are orthogonal to all rows of g'_j. Similarly, we can see that the rows of g'_j are orthogonal to the rows of g'_k for $j \neq k$, as $2\alpha + 2(k-2)n\alpha^2 + 2\alpha\left(\sum_{k=1}^{n} a_{lk}\right) = 0$. Therefore the code $\mathcal{C}'$ generated by G' is self-orthogonal. Since $|(\mathcal{C}')^{\perp}| = \frac{16^{2kn}}{|\mathcal{C}'|} = 16^{kn} = |\mathcal{C}'|$, $\mathcal{C}'$ is self-dual. ■

Example 4.3.10. *Let $\mathcal{C}$ be the self-dual code of length* 8 *over R generated by*

$$G = \begin{pmatrix} 1000 & 0 & 1+2w & 3+2w & 3 \\ 0100 & 1 & 1 & 1 & 0 \\ 0010 & 3+2w & 0 & 1+2w & 3 \\ 0001 & 1+2w & 3+2w & 0 & 3 \end{pmatrix}.$$

Then the matrix $G' = \begin{pmatrix} I_4 & B_4 & A_4 & B_4 \\ B_4 & I_4 & B_4 & A_4 \end{pmatrix}$ *generates a free self-dual code of length* 16 *over R and its minimum Hamming distance is* 4.

4.3.2 Circulant self-dual codes

A matrix A_n is said to be a *α-circulant matrix* generated by $(a_1, a_2, \ldots, a_n)$ if

$$A_n = \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ \alpha a_n & a_1 & \cdots & a_{n-2} & a_{n-1} \\ \alpha a_{n-1} & \alpha a_n & \cdots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha a_2 & \alpha a_3 & \cdots & \alpha a_n & a_1 \end{pmatrix},$$

and it is denoted by $\alpha - \mathrm{cir}(a_1, a_2, \ldots, a_n)$. If $\alpha = 1$ then A_n is called a *circulant matrix* and a *nega circulant matrix* if $\alpha = -1$. A matrix B is said to be a *pure double circulant matrix* if $B = [I_n \mid A_n]$, where I_n is an identity matrix and A_n is any circulant matrix generated by $(a_1, a_2, \ldots, a_n)$.

Codes generated by circulant, pure double circulant and nega circulant matrices are called circulant (cycic), pure double circulant and nega circulant (negacyclic) codes, respectively.

Theorem 4.3.11. *No pure double circulant self-dual code exists over R.*

Proof. We know that a pure double circulant code is a free code, and there is no free self-dual code of odd length over R. Let $\mathcal{C}$ be a pure double circulant self-dual code of length $n = 2k$, $k \geq 1$, generated by $G = [I_k \mid A_k]$, where

$$A_k = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{k-1} & a_k \\ a_k & a_1 & a_2 & \cdots & a_{k-2} & a_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_k & a_1 \end{pmatrix},$$

$a_j \in R$, $j = 1, 2, \ldots, k$.

Since $\mathcal{C}$ is self-dual, $1 + \sum\limits_{j=1}^{k} a_j^2 = 0 \pmod 4$, which implies that $\sum\limits_{j=1}^{k} a_j^2 = 3 \pmod 4$. Also, since any two rows of G are orthogonal, from which follows that $2 \sum\limits_{j=1}^{k} \sum\limits_{l=1,\ j<l}^{k} a_j a_l = 0$. It implies that $\left(\sum\limits_{j=1}^{k} a_j\right)^2 = \sum\limits_{j=1}^{k} a_j^2 \pmod 4$, which in turn implies that $\left(\sum\limits_{j=1}^{k} a_j\right)^2 = 3 \pmod 4$. But no element in R satisfies $x^2 = 3 \pmod 4$. Hence there is no pure double circulant self-dual code of length n over R. ■

Now we define another class of codes called *formally self-dual codes.* A linear code $\mathcal{C}$ over R is called a formally self-dual code if $\mathcal{C}$ and $\mathcal{C}^{\perp}$ have the same weight enumerator. It is immediate that a self-dual code is necessarily formally self-dual but not the converse, i.e., a formally self-dual code may not be self-dual. It follows from Theorem 4.2.4 that, if a linear code $\mathcal{C}$ of length n over R is formally self-dual, then so is $\phi(\mathcal{C})$ over $\mathbb{Z}_4$. In [139], Yildiz and Karadeniz have extended the construction methods described in [61] to construct formally self-dual codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. They have also obtained some good formally self-dual codes over $\mathbb{Z}_4$ from the codes constructed by the previous methods over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$. It can be easily seen that these construction methods can be generalized to the ring R.

Theorem 4.3.12. *[139, Theorem 5.2] Let M_n be a circulant matrix over R of order n. Then the matrix $G = [I_n \mid M_n]$ generates a formally self-dual code over R.*

Theorem 4.3.13. *[139, Theorem 5.4] Let M_{n-1} be a circulant matrix over R of order $n-1$. Then the matrix*

$$G = \left(\begin{array}{cccccc} & \alpha & \beta & \beta & \cdots & \beta \\ & \gamma & & & & \\ I_n & \vdots & & & M_{n-1} & \\ & \gamma & & & & \end{array} \right),$$

where $\alpha, \beta, \gamma \in R$ such that $\gamma = \pm\beta$, generates a formally self-dual code of length $2n$ over R whose Gray image is a formally self-dual code of length $4n$ over $\mathbb{Z}_4$.

Example 4.3.14. *[86, Example 3.12] Let $M_6 = cir(0, w, 3, 2w, 3, 2)$ be a circulant matrix of order 6 over R. Then the code $\mathcal{C} = [I_6 \mid M_6]$ is a formally self-dual code of length 12 over R but not self-dual. The Gray image of $\mathcal{C}$ is a formally self-dual $\mathbb{Z}_4$-code of length 24 and minimum Lee distance 10.*

Example 4.3.15. *[86, Example 3.13] Let $M_5 = cir(0, w, 1, 1, 2 + w)$ be a circulant matrix of order 5 over R and take $\gamma = \beta = 3 + 2w$ and $\alpha = 2$. Then the matrix*

$$G = \left(\begin{array}{cccccc} & \alpha & \beta & \beta & \cdots & \beta \\ & \gamma & & & & \\ I_6 & \vdots & & & M_5 & \\ & \gamma & & & & \end{array} \right) = \left(\begin{array}{cccccc} & 2 & 3+2w & 3+2w & \cdots & 3+2w \\ & 3+2w & & & & \\ I_6 & \vdots & & & M_5 & \\ & 3+2w & & & & \end{array} \right)$$

generates a formally self-dual code of length 12 over R, which is not self-dual. The Gray image of $\mathcal{C}$ is a formally self-dual $\mathbb{Z}_4$-code of length 24 and minimum Lee distance 10 and has a different Lee weight enumerator than the previous example.

4.4 Type II codes

A self-dual code $\mathcal{C}$ over R is said to be a *Type II code* if the Euclidean weight of every codeword is divisible by 8, otherwise $\mathcal{C}$ is said to be a *Type I code.*

Theorem 4.4.1. *A Type II code of length n over R exists if and only if n is a multiple of 4.*

Proof. Let $\mathcal{C}$ be a Type II code of length n over R. From Theorem 4.3.6, $\phi(\mathcal{C})$ is a self-dual code of length $2n$ over $\mathbb{Z}_4$. Since ϕ is distance preserving, $\phi(\mathcal{C})$ is a Type II code over $\mathbb{Z}_4$.

Conversely, let $\mathcal{C}$ be a self-dual code of length n over R such that n is a multiple of 4. Then from Theorem 4.3.6, $\phi(\mathcal{C})$ is self-dual code of length $2n$ over $\mathbb{Z}_4$. From Theorem 2.3.23, $\phi(\mathcal{C})$ is Type II code of length $2n$ over $\mathbb{Z}_4$. Since ϕ is distance preserving, $\mathcal{C}$ is also a Type II code over R. ∎

The following theorem is analogous to [137, Theorem 2.13].

Theorem 4.4.2. *Let $d_E(II)$ and $d_E(I)$ be the minimum Euclidean weights of a Type II code and a Type I code of length n, respectively, over R. Then $d_E(II)$, $d_E(I) \leq 8\lfloor \frac{n}{12} \rfloor + 8$.*

Proof. Let $\mathcal{C}$ be a Type II or Type I code of length n over R. Since ϕ is distance preserving and $\phi(\mathcal{C})$ is a $\mathbb{Z}_4$-code of length $2n$, the result follows from Theorem 2.3.24. In Theorem 2.3.24, it is mentioned that the above result holds when the code length is not equal to 23 (mod 24). Since $\phi(\mathcal{C})$ is of length $2n$ and $2n \neq 23 \pmod{24}$ for $n \geq 1$, so the bound for $d_E(I)$ does not change. ∎

Codes satisfying the above bounds are said to be *Extremal Type II codes* and *Extremal Type I codes*, respectively.

Corollary 4.4.3. *If $\mathcal{C}$ is an Extremal Type II code over R, then so is $\phi(\mathcal{C})$ over $\mathbb{Z}_4$.*

Proof. This result follows from Theorems 4.4.1 and 4.4.2. ∎

The codes given in Examples 4.2.6 and 4.2.7 are extremal Type II codes over R.

4.5 Conclusion

In this chapter, we have studied linear codes over the rings $R = \mathbb{Z}_4 + w\mathbb{Z}_4$, $w^2 = 2w$. Some characterizations of self-dual codes over R are provided. We have proposed a new construction method for constructing self-dual codes over R. Circulant self-dual codes and Type II codes over R are briefly discussed.

Chapter 5

Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$

5.1 Introduction

Cyclic codes are amongst the most studied algebraic codes because of their rich algebraic structure and practical importance. They have been generalized to various finite rings. Their structure over finite chain rings is now well known [45, 83, 84, 90]. They have also been studied over finite polynomial rings such as $\mathbb{F}_2+u\mathbb{F}_2$, $u^2 = 0$ [26]; $\mathbb{F}_2+v\mathbb{F}_2$, $v^2 = v$ [140], $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, $u^2 = v^2 = 0, uv = vu$ [138], $\frac{\mathbb{Z}_p[u]}{\langle u^k\rangle}$ [114] and $\frac{\mathbb{Z}_p[u,v]}{\langle u^2,v^2,uv-vu\rangle}$ [68]. However, not much attention has been paid to cyclic codes over local non-chain rings.

Recently, Yildiz and Karadeniz [139] have studied linear codes over $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. Yildiz and Aydin [136] have studied cyclic codes over R and have obtained some good linear $\mathbb{Z}_4$-codes which are actually the Gray images of cyclic codes of odd lengths over R. In this chapter, we study cyclic codes and their structural properties extensively over R. We first study cyclic codes of odd lengths over R. For this we describe the Galois ring extension of R and then cyclic codes of odd length n through the factorization of $x^n - 1$ over R. We then consider cyclic codes of arbitrary lengths over R.

In [136, Theorem 6] Yildiz and Aydin have given the structure of cyclic codes over R. However the structure given therein does not cover all the cyclic codes over R. We present here a structure of generators of cyclic codes over R that is slightly different from that of [136, Thereom 6], and it covers all cyclic codes over R. Using the general form of the generators of a cyclic code over R we have obtained a minimal spanning set and a formula for the rank of such codes. We have also determined a necessary condition and a sufficient condition for cyclic codes over R to be R–free. For $n = 2^k$, we have shown that R_n is a local ring and determined the complete ideal structure of R_n.

5.2 The ring $\mathbb{Z}_4 + u\mathbb{Z}_4$

Throughout the chapter, R denotes the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 = \{a + ub \mid a, b \in \mathbb{Z}_4\}$ with $u^2 = 0$. R can be viewed as the quotient ring $\frac{\mathbb{Z}_4[u]}{\langle u^2 \rangle}$. The units of R are

$$1, 3, 1+u, 1+2u, 1+3u, 3+u, 3+2u, 3+3u \ ,$$

and the non-units are

$$0, 2, u, 2u, 2+u, 2+2u, 3u, 2+3u \ .$$

Thus an element $a + ub \in R$ is a unit if and only if $a \in \mathbb{Z}_4$ is a unit. R has five non-trivial ideals in all:

$$\begin{aligned}
\langle 2u \rangle &= \{0, 2u\}, \\
\langle u \rangle &= \{0, u, 2u, 3u\}, \\
\langle 2 \rangle &= \{0, 2, 2u, 2+2u\}, \\
\langle 2+u \rangle &= \{0, 2+u, 2u, 2+3u\} \\
\langle 2, u \rangle &= \{0, 2, u, 2u, 3u, 2+u, 2+2u, 2+3u\}.
\end{aligned}$$

From the ideals of R, we can see that they do not form a chain; for instance, the ideals $\langle u \rangle$ and $\langle 2 \rangle$ are not comparable. Therefore, R is a non-chain extension of $\mathbb{Z}_4$. Also R is not a principal ideal ring; for example, the ideal $\langle 2,\ u \rangle$ is not generated by any single element of R. Thus, the ring R is a local non-chain extension of $\mathbb{Z}_4$ with unique maximal ideal $\langle 2,\ u \rangle$. The residue ring of R is $\frac{R}{\langle 2,\ u \rangle} \cong \mathbb{Z}_2$. The ring R is not isomorphic to the ring $\mathbb{Z}_4 + w\mathbb{Z}_4$, $w^2 = 2w$ discussed in Chapter 4. Though both the rings look similar in the first glance, there are differences between them. For example, the ring $\mathbb{Z}_4 + w\mathbb{Z}_4$ is a group ring over $\mathbb{Z}_4$,

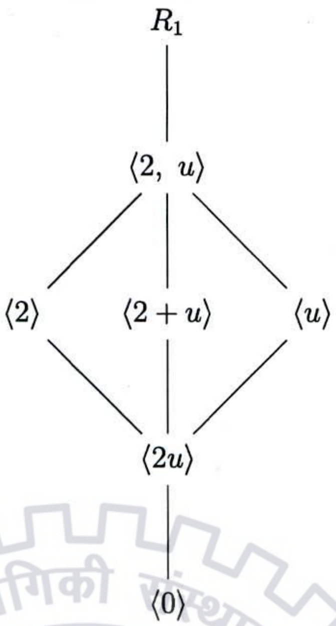

Figure 5.1: Lattice diagram of ideals of $\mathbb{Z}_4 + u\mathbb{Z}_4$

but R is not, as no multiplicative subgroup of units of R generates R over $\mathbb{Z}_4$. The lattice diagram of ideals of R is given in Figure 5.1.

The Gray map on R^n is defined in [139] as $\phi : R^n \to \mathbb{Z}_4^{2n}$ such that

$$\phi(\overline{a} + u\overline{b}) = (\overline{b},\ \overline{a} + \overline{b})\ .$$

This is same as the Gray map defined over $\mathbb{Z}_4^n$. However the Gray map on $\mathbb{Z}_4^n$ is non-linear whereas the Gray map defined on R^n is linear (Theorem 5.2.1).

The Lee weight and Euclidean weight on R are defined by

$$w_L(a + ub) = w_L(b,\ a + b)$$

and

$$w_E(a + ub) = w_E(b,\ a + b)\ .$$

where $w_L(b,\ a+b)$, $w_E(b,\ a+b)$ are the usual Lee and Euclidean weights of $(b,\ a+b)$ in $\mathbb{Z}_4^2$. These weights are then extended componentwise to R^n. The Lee/Euclidean weight of an element $x \in R^n$ is the sum of the Lee/Euclidean weights of its coordinates. The Hamming weight of $x \in R^n$ is the number of non-zero coordinate positions in x and is denoted by $w_H(x)$.

Theorem 5.2.1. *[139, Theorem 2.3] The Gray map ϕ is a linear isometry with respect to the Lee and Euclidean distances in R^n and $\mathbb{Z}_4^{2n}$.*

Theorem 5.2.2. *[86, Proposition 3.4] There is no injective $\mathbb{Z}_4$-linear map from R to $\mathbb{Z}_4^2$ of the form $av_1 + bv_2 \mapsto (a,\ b)$, where $\{v_1,\ v_2\}$ is a $\mathbb{Z}_4$ basis that preserves duality.*

It is to be noted from Theorem 5.2.2 that the map ϕ defined on R^n is not a dual preserving map. But the same map ϕ defined on $(\mathbb{Z}_4 + w\mathbb{Z}_4)^n$ in Chapter 4 is a dual preserving map. This is another difference between the rings $\mathbb{Z}_4 + w\mathbb{Z}_4$ and R.

A linear code $\mathcal{C}$ of length n over R is an R-submodule of R^n. $\mathcal{C}$ may not be an R-free module . We can express R^n as $R^n = \mathbb{Z}_4^n + u\mathbb{Z}_4^n$, and so a linear code $\mathcal{C}$ of length n over R can be expressed as $\mathcal{C} = C_1 + uC_2$, where C_1, C_2 are linear codes of length n over $\mathbb{Z}_4$.

We denote the residue field $\frac{R}{\langle 2,u\rangle}$ of R by $\overline{R}$. Since $\{0+\langle 2,u\rangle\} \cup \{1+\langle 2,u\rangle\} = R$, therefore $\overline{R} \cong \mathbb{F}_2$. The image of any element $a \in R$ under the projection map $\mu : R \to \overline{R}$ is denoted by $\overline{a}$. The map μ is extended to $R[x] \to \overline{R}[x]$ in the usual way. The image of an element $f(x) \in R[x]$ in $\overline{R}[x]$ under this projection is denoted by $\overline{f}(x)$. A polynomial $f(x) \in R[x]$ is called *basic irreducible (primitive)* if $\overline{f}(x)$ is an irreducible (primitive) polynomial in $\overline{R}[x]$.

5.3 Galois ring extensions of $\mathbb{Z}_4 + u\mathbb{Z}_4$

The factorization of $x^n - 1$ plays a vital role in the study of cyclic codes. So we first consider the factorization of $x^n - 1$ over R. Let n be an odd integer for the rest of this section. The following theorem gives the Hensel's lift of a polynomial to R and also guarantees the existence of a primitive element over R.

Theorem 5.3.1. *Let $g(x) \in \mathbb{F}_2[x]$ be a monic irreducible (primitive) divisor of $x^{2^r-1} - 1$. Then there exists a unique monic basic irreducible (primitive) polynomial $f(x)$ in $R[x]$ such that $\overline{f}(x) = g(x)$ and $f(x) \mid (x^{2^r-1} - 1)$ in $R[x]$.*

Proof. Let $x^{2^r-1}-1 = g(x)g'(x)$ in $\mathbb{F}_2[x]$. By Hensel's lemma, there exist $f(x), f'(x) \in \mathbb{Z}_4[x]$ such that

$$x^{2^r-1} - 1 = f(x)f'(x)$$

in $\mathbb{Z}_4[x]$ and $f(x) \pmod 2 = g(x)$, $f'(x) \pmod 2 = g'(x)$. Since $\mathbb{Z}_4$ is a subring of R, $f(x) \in R[x]$. Also $\overline{f}(x) = f(x) \pmod{\langle 2, u\rangle} = g(x)$ and $f(x) \mid (x^{2^r-1} - 1)$ in $R[x]$. ■

We call the polynomial $f(x)$ in Theorem 5.3.1 the *Hensel lift* of $g(x)$ to R.

Since n is odd, it follows from Theorem 2.3.15 that $x^n - 1$ factorizes uniquely into pairwise coprime basic irreducible polynomials over R. Let

$$x^n - 1 = f_1(x)f_2(x)\cdots f_m(x)$$

be such a factorization of $x^n - 1$. Then it follows from the Chinese Remainder Theorem that

$$\frac{R[x]}{\langle x^n - 1\rangle} = \oplus_{i=1}^m \frac{R[x]}{\langle f_i(x)\rangle}.$$

Therefore every ideal I of $\frac{R[x]}{\langle x^n-1\rangle}$ can be expressed as

$$I = \oplus_{i=1}^m I_i,$$

where I_i is an ideal of the ring $\frac{R[x]}{\langle f_i(x)\rangle}$, $i = 1, 2, \ldots, m$.

Let us recall the Galois ring extension of $\mathbb{Z}_4$. Let $h(x)$ be a monic basic irreducible polynomial of degree r in $\mathbb{Z}_4[x]$. Then the Galois ring $GR(4, r)$ over $\mathbb{Z}_4$ is defined as the residue class ring $\frac{\mathbb{Z}_4[x]}{\langle h(x)\rangle}$. The ring $GR(4, r)$ is a local ring with unique maximal ideal $\langle 2\rangle$ and the residue field $\mathbb{F}_{2^r}$.

Let $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^r-2}\}$ be the set of *Teichmüller* representatives of $GR(4, r)$, where ξ is a root of a basic primitive polynomial of degree r in $\mathbb{Z}_4[x]$. Then each element a of $GR(4, r)$ can be written as $a = a_0 + 2a_1$, where $a_0, a_1 \in \mathcal{T}$. This representation is called the 2-adic representation of the elements of $GR(4, r)$.

Now we define the Galois ring extension of R. Let $f(x)$ be a basic irreducible polynomial of degree r in $R[x]$. Then the Galois ring extension of R is defined as the quotient ring

$\frac{R[x]}{\langle f(x)\rangle}$ and is denoted by $GR(R,r)$. If α is a root of $f(x)$, then the elements of $GR(R,r)$ can uniquely be written as $m_0 + m_1\alpha + m_2\alpha^2 + \cdots + m_{r-1}\alpha^{r-1}$, $m_i \in R$, $i = 0, 1, \ldots, r-1$, i.e., $GR(R,r)$ is a free module of rank r over R with a basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ and $|GR(R,r)| = 16^r$. From Theorem 5.3.5 below, it follows that the ring $GR(R,r)$ is a local ring with unique maximal ideal $\langle\langle 2,\ u\rangle + \langle f\rangle\rangle$ and the residue field $\mathbb{F}_{2^r}$. Furthermore,

$$GR(R,r) \equiv \frac{GR(4,r)[u]}{\langle u^2\rangle} \equiv GR(4,r) + uGR(4,r)\ ,$$

where $GR(4,r)$ is the Galois ring of degree r over $\mathbb{Z}_4$.

Therefore, an element x of $GR(R,r)$ can be represented as $x = a + ub$, where $a, b \in GR(4,r)$. Using the 2-adic representation of $a = a_0 + 2a_1$, $b = a_2 + 2a_3$, $a_0, a_1, a_2, a_3 \in \mathcal{T}$, the element $x \in GR(R,r)$ can further be represented as $x = a_0 + 2a_1 + ua_2 + 2ua_3$.

Lemma 5.3.2. *A non-zero element $x = a_0 + 2a_1 + ua_2 + 2ua_3$ of $GR(R,r)$ is a unit if and only if a_0 is non-zero in $\mathcal{T}$.*

Proof. Since $x^4 = a_0^4$ for every non-zero element x in $GR(R,r)$, the result follows. ■

Thus the group of units of $GR(R,r)$, denoted by $GR(R,r)^*$, is given by

$$GR(R,r)^* = \{a_0 + 2a_1 + ua_2 + 2ua_3 \ \ : \ \ a_0, a_1, a_2, a_3 \in \mathcal{T}, a_0 \neq 0\}.$$

Theorem 5.3.3. *The group of units $GR(R,r)^*$ is a direct product of two groups G_C and G_A, i.e., $GR(R,r)^* = G_C \times G_A$, where G_C is a cyclic group of order $2^r - 1$ and G_A is an abelian group of order 8^r.*

Proof. Let ξ be a primitive element of $GR(R,r)$ and $G_C = \mathcal{T}^* = \{1, \xi, \ldots, \xi^{2^r-2}\}$. Then G_C is a multiplicative cyclic group of order $2^r - 1$. For $x = a_0 + 2a_1 + ua_2 + 2ua_3 \in GR(R,r)^*$, define a mapping $\Gamma : GR(R,r)^* \longrightarrow G_C$ such that $\Gamma(x) = a_0$. It can easily be seen that for any $\alpha, x, y \in GR(R,r)^*$, $\Gamma(\alpha x + y) = \Gamma(\alpha)\Gamma(x) + \Gamma(y)$. Γ is obviously a surjective map. Therefore $\frac{GR(R,r)^*}{\ker\,\Gamma} \equiv G_C$, where $\ker\,\Gamma = \{1 + 2a_1 + ua_2 + 2ua_3 \ : \ a_1, a_2, a_3 \in \mathcal{T}\}$. Denote $\ker\,\Gamma$ by G_A. Then it can easily be seen that $GR(R,r)^* \equiv G_C \times G_A$. Moreover $|GR(R,r)^*| = |G_c||G_A| = 8^r(2^r - 1)$. ■

The set of all zero divisors of $GR(R, r)$ is given by $\{2a_1 + ua_2 + 2ua_3 \ : \ a_1, a_2, a_3 \in \mathcal{T}\}$, which is a maximal ideal generated by $\langle 2, u\rangle$ in $GR(R, r)$.

Now we consider the ideal structure of $GR(R, r)$. We first prove the following Lemma.

Lemma 5.3.4. *Let $f(x),\ g(x) \in R[x]$. Then $f(x),\ g(x)$ are coprime if and only if their images $\overline{f}(x),\ \overline{g}(x)$ are coprime in $\overline{R}[x]$.*

Proof. If $f(x),\ g(x)$ are coprime, then it is immediate that $\overline{f}(x)$ and $\overline{g}(x)$ are coprime. Now suppose that $\overline{f}(x),\ \overline{g}(x)$ are coprime. Then there exist $a(x), b(x) \in R[x]$ such that

$$\overline{a}(x)\overline{f}(x) + \overline{b}(x)\overline{g}(x) = 1 \ .$$

Thus there exits $r(x), s(x) \in R[x]$ such that

$$a(x)f(x) + b(x)g(x) = 1 + 2r(x) + us(x) \ . \tag{5.3.1}$$

Multiplying (5.3.1) by $2r(x)$ and by $us(x)$, we respectively get equations:

$$\begin{aligned} 2r(x)a(x)f(x) + 2r(x)b(x)g(x) &= 2r(x) + 2ur(x)s(x) \ , && (5.3.2)\\ us(x)a(x)f(x) + us(x)b(x)g(x) &= us(x) + 2ur(x)s(x) \ . && (5.3.3)\end{aligned}$$

On adding (5.3.2) and (5.3.3), we get

$$a(x)(2r(x) + us(x))f(x) \ + \ b(x)(2r(x) + us(x))g(x) \ = \ 2r(x) + us(x) \ . \tag{5.3.4}$$

Putting the value of $2r(x) + us(x)$ in (5.3.1), we get

$$a(x)(1 - 2r(x) - us(x))f(x) + b(x)(1 - 2r(x) - us(x))g(x) = 1 \ .$$

Therefore $f(x)$ and $g(x)$ are coprime. ■

The following theorem presents the ideal structure of $\frac{R[x]}{\langle f(x)\rangle}$, where $f(x)$ is a basic irreducible polynomial over R.

Theorem 5.3.5. *Let $f(x) \in R[x]$ be a basic irreducible polynomial. Then the ideals of $\frac{R[x]}{\langle f(x)\rangle}$ are precisely, $\langle 0\rangle$, $\langle 1 + \langle f(x)\rangle\rangle$, $\langle 2 + \langle f(x)\rangle\rangle$, $\langle u + \langle f(x)\rangle\rangle$, $\langle 2u + \langle f(x)\rangle\rangle$, $\langle 2 + u + \langle f(x)\rangle\rangle$ and $\langle\langle 2, u\rangle + \langle f(x)\rangle\rangle$.*

Proof. Let I be a non-zero ideal of $\frac{R[x]}{\langle f(x)\rangle}$. Let $h(x) + \langle f(x)\rangle \in I$. Since $f(x)$ is basic irreducible, $\overline{f}(x)$ is irreducible in $\overline{R}[x]$. Therefore $\gcd(\overline{f}(x), \overline{h}(x)) = 1$ or $\overline{f}(x)$. Let $\gcd(\overline{f}(x), \overline{h}(x)) = 1$. Then $f(x)$ and $h(x)$ are coprime in $R[x]$, and hence there exist $\lambda_1, \lambda_2 \in R[x]$ such that

$$\lambda_1 f(x) + \lambda_2 h(x) = 1 \ .$$

From this follows that $\lambda_2 h(x) = 1 \pmod{f(x)}$. Thus $h(x)$ is an invertible element of $\frac{R[x]}{\langle f(x)\rangle}$ and so $I = \langle 1 + \langle f(x)\rangle\rangle = \frac{R[x]}{\langle f(x)\rangle}$.

Now suppose that $\gcd(\overline{f}(x), \overline{h}(x)) = \overline{f}(x)$. Then there exist polynomials $g(x), f_1(x), f_2(x) \in R[x]$ such that

$$h(x) = f(x)g(x) + 2f_1(x) + uf_2(x) \ ,$$

and $\gcd(\overline{f}(x), \overline{f}_1(x)) = 1$ or $\gcd(\overline{f}(x), \overline{f}_2(x)) = 1$. It follows that $h(x) + \langle f(x)\rangle \in \langle\langle 2, u\rangle + \langle f(x)\rangle\rangle$. Therefore if $I \neq \langle 1 + \langle f(x)\rangle\rangle$, then $I \subseteq \langle\langle 2, u\rangle + \langle f(x)\rangle\rangle$. The non-zero ideals contained in $\langle\langle 2, u\rangle + \langle f(x)\rangle\rangle$ are $\langle 2 + \langle f(x)\rangle\rangle$, $\langle u + \langle f(x)\rangle\rangle$, $\langle 2u + \langle f(x)\rangle\rangle$, $\langle 2 + u + \langle f(x)\rangle\rangle$ and $\langle\langle 2, u\rangle + \langle f(x)\rangle\rangle$ itself. Therefore I is in one of the ideals $\langle 2 + \langle f(x)\rangle\rangle$, $\langle u + \langle f(x)\rangle\rangle$, $\langle 2u + \langle f(x)\rangle\rangle$, $\langle 2 + u + \langle f(x)\rangle\rangle$ and $\langle\langle 2, u\rangle + \langle f(x)\rangle\rangle$.

On the other hand, suppose $h(x) + \langle f(x)\rangle = ug_1(x) + 2g_2(x) + \langle f(x)\rangle \in I$, where $g_1(x)$, $g_2(x) \in R[x]$ and $\gcd(\overline{g_1}(x), \overline{f}(x)) = 1$, $\gcd(\overline{g_2}(x), \overline{f}(x)) = 1$. Here we note that $\gcd(\overline{g_1}(x), \overline{f}(x)) = 1$, $\gcd(\overline{g_2}(x), \overline{f}(x)) = 1$. For if $\gcd(\overline{g_1}(x), \overline{f}(x)) \neq 1$, then $g_1(x) = f(x)g_1'(x) + ug_1''(x)$, which implies that $ug_1(x) = uf(x)g_1'(x)$, which in turn implies that $f(x)$ divides $g_1(x)$, a contradiction. Similarly we have $\gcd(\overline{g_2}(x), \overline{f}(x)) = 1$. From Lemma 5.3.4, there exist $a_1(x), a_2(x), b_1(x), b_2(x) \in R[x]$ such that $1 = g_1(x)a_1(x) + f(x)a_2(x)$ and $1 = g_1(x)b_1(x) + f(x)b_2(x)$. This implies that

$$ub_1(x) + \langle f(x)\rangle = (ug_1(x) + \langle f(x)\rangle)(a_1(x)b_1(x) + \langle f(x)\rangle)$$

and

$$2a_1(x) + \langle f(x)\rangle = (2g_2(x) + \langle f(x)\rangle)(a_1(x)b_1(x) + \langle f(x)\rangle) \,.$$

Adding these two equations, we get

$$2a_1(x) + ub_1(x) + \langle f(x)\rangle = (2g_2(x) + ug_1(x) + \langle f(x)\rangle)(a_1(x)b_1(x) + \langle f(x)\rangle) \,.$$

This implies that $2a_1(x) + ub_1(x) + \langle f(x)\rangle \in \langle 2g_2(x) + ug_1(x) + \langle f(x)\rangle\rangle \subseteq I$. Therefore $\langle\langle 2,\ u\rangle + \langle f(x)\rangle\rangle \subset I$. Hence the result. ■

The Galois group $\mathrm{Gal}(GR(R,r))$ of $GR(R,r)$ is a cyclic group of order $(2^r - 1)$, which is generated by the *Frobenius automorphism* σ of $GR(R,r)$ defined as

$$\sigma(x) = a_0^2 + 2a_1^2 + ua_2^2 + 2ua_3^2 \,,$$

where $x = a_0 + 2a_1 + ua_2 + 2ua_3 \in R$. The automorphism σ fixes the ring R.

Example 5.3.6. *Consider the basic irreducible polynomial $h(x) = x^4 + 3x^3 + 2x^2 + 1$, which is the Hensel lift to R of the irreducible polynomial $x^4 + x^3 + 1 \in \mathbb{F}_2[x]$. Let ξ be a root of $h(x)$. Then*

$$\begin{array}{rclrcl}
\xi^4 & = & \xi^3 + 2\xi^2 + 3, & \xi^5 & = & 3\xi^3 + 2\xi^2 + 3\xi + 3, \\
\xi^6 & = & \xi^3 + \xi^2 + 3\xi + 1, & \xi^7 & = & 2\xi^3 + \xi^2 + \xi + 3, \\
\xi^8 & = & 3\xi^3 + \xi^2 + \xi, & \xi^9 & = & 3\xi^2 + 3, \\
\xi^{10} & = & 3\xi^3 + 3\xi, & \xi^{11} & = & 3\xi^3 + \xi^2 + 1, \\
\xi^{12} & = & 2\xi^2 + \xi + 1, & \xi^{13} & = & 2\xi^3 + \xi^2 + \xi, \\
\xi^{14} & = & 3\xi^3 + \xi^2 + 2\xi, & \xi^{15} & = & 1.
\end{array}$$

Let $\mathcal{T} = \{0, 1, \xi, \xi^2, \xi^3, \xi^3 + 2\xi^2 + 3, 3\xi^3 + 2\xi^2 + 3\xi + 3, \xi^3 + \xi^2 + 3\xi + 1, 2\xi^3 + \xi^2 + \xi + 3, 3\xi^3 + \xi^2 + \xi, 3\xi^2 + 3, 3\xi^3 + 3\xi, 3\xi^3 + \xi^2 + 1, 2\xi^2 + \xi + 1, 2\xi^3 + \xi^2 + \xi, 3\xi^3 + \xi^2 + 2\xi\}$. Then

$$GR(R,4) = \{a_0 + 2a_1 + ua_2 + 2ua_3 \ :\ a_i \in \mathcal{T}, i = 0,1,2,3\}$$

and $|GR(R,4)| = 16^4$.

Let $x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 \ \in GR(R,4)$, $a_i \in R$. Define $\sigma : GR(R,4) \to GR(R,4)$ such that

$$\sigma(x) = a_0 + a_1\xi^2 + a_2(\xi^2)^2 + a_3(\xi^3)^2.$$

Clearly σ is an automorphism and $\sigma(a) = a$ for all $a \in R$. So σ leaves the elements of R fixed. Since $\xi^{15} = 1$, we have

$$\begin{aligned}
\sigma(x) &= \quad a_0 + a_1\xi^2 + a_2\xi^4 + a_3\xi^6, \qquad \sigma^2(x) = a_0 + a_1\xi^4 + a_2\xi^8 + a_3\xi^{12},\\
\sigma^3(x) &= a_0 + a_1\xi^8 + a_2\xi^{16} + a_3\xi^{24} \ = \quad a_0 + a_1\xi^8 + a_2\xi + a_3\xi^9 \quad \textit{and}\\
\sigma^4(x) &= a_0 + a_1\xi^{16} + a_2\xi^2 + a_3\xi^{18} = \quad a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 = x\ .
\end{aligned}$$

Thus the order of σ is 4 and σ generates the cyclic group $\{1, \sigma,\ \sigma^2, \sigma^3\} = Gal(GR(R,4))$.

5.4 Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$

Let τ be the standard cyclic shift operator on R^n. A linear code $\mathcal{C}$ of length n over R is *cyclic* if $\tau(c) \in \mathcal{C}$ whenever $c \in \mathcal{C}$, i.e., if for each $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, then $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. As usual, in the polynomial representation, a cyclic code of length n over R is an ideal of $\frac{R[x]}{\langle x^n-1\rangle}$.

Theorem 5.4.1. *A linear code $\mathcal{C} = C_1 + uC_2$ of length n over R is cyclic if and only if C_1, C_2 are cyclic codes of length n over $\mathbb{Z}_4$.*

Proof. Let $c_1 + uc_2 \in \mathcal{C}$, where $c_1 \in C_1$ and $c_2 \in C_2$. Then $\tau(c_1 + uc_2) = \tau(c_1) + u\tau(c_2) \in \mathcal{C}$, since $\mathcal{C}$ is cyclic and τ is a linear map. So, $\tau(c_1) \in C_1$ and $\tau(c_2) \in C_2$. Therefore C_1, C_2 are cyclic codes. Conversely, if C_1, C_2 are cyclic codes, then for any $c_1 + uc_2 \in \mathcal{C}$, where $c_1 \in C_1$ and $c_2 \in C_2$, we have $\tau(c_1) \in C_1$ and $\tau(c_2) \in C_2$, and so, $\tau(c_1 + uc_2) = \tau(c_1) + u\tau(c_2) \in \mathcal{C}$. Hence $\mathcal{C}$ is cyclic. ■

To find the ideal structure of $\frac{R[x]}{\langle x^n-1\rangle}$, we need to know the factorization of $x^n - 1$. Since R is a local ring, $x^n - 1$ factors into distinct irreducible polynomials if and only if n is an odd integer. In the following subsection we study cyclic codes odd length n over R through the factorization of $x^n - 1$. Later in this chapter, we consider cyclic codes of arbitrary length also.

5.4.1 Cyclic codes of odd lengths over $\mathbb{Z}_4 + u\mathbb{Z}_4$

We assume that n is odd throughout this subsection. For a finite chain ring $\mathcal{R}$, it is well known that the ring $\frac{\mathcal{R}[x]}{\langle x^n-1\rangle}$ is a principal ideal ring [90]. However, in the present case the ring R is not a chain ring and the situation is not as straightforward. In fact, the ring $\frac{R[x]}{\langle x^n-1\rangle}$ is not in general a principal ideal ring, as the next result shows. The result is a generalization of [136, Lemma 2.4].

Theorem 5.4.2. *The ring $R_n = \frac{R[x]}{\langle x^n-1\rangle}$ is not a principal ideal ring.*

Proof. Consider the augmentation mapping $\gamma : \frac{R[x]}{\langle x^n-1\rangle} \rightarrow R$ defined by

$$\gamma(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) = a_0 \ + \ a_1 \ + \ \cdots \ + \ a_{n-1} \ .$$

This is a surjective ring homomorphism. Consider now the ideal $I = \langle 2, u\rangle$ of R, which we know is not a principal ideal. Let $J = \gamma^{-1}(I)$. It is well known that the inverse image under a homomorphism of an ideal is an ideal. So J is an ideal of R_n. Now if we assume J to be a principal ideal, then its homomorphic image I must be principal, a contradiction. Hence J is not a principal ideal and R_n is therefore not a principal ideal ring. ■

Therefore, a cyclic code of length n over R is in general not principally generated.

In the following theorem we present the ideal structure of R_n.

Theorem 5.4.3. *Let $x^n - 1 = f_1(x)f_2(x)\cdots f_m(x)$, where $f_i(x)$, $i = 1, 2, \ldots, m$, are monic basic irreducible pairwise coprime polynomials in $R[x]$. Let $\hat{f}_i(x) = \frac{x^n-1}{f_i(x)}$. Then any ideal in R_n is the sum of the ideals:*

$$\begin{gathered}\left\langle \hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle, \quad \left\langle 2\hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle, \\ \left\langle u\hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle, \quad \left\langle 2u\hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle, \\ \left\langle (2+u)\hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle, \quad \left\langle \langle 2, u\rangle \, \hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle.\end{gathered}$$

Proof. Since $x^n - 1 = f_1(x)f_2(x)\cdots f_m(x)$, it follows the Chinese Remainder Theorem

$$\frac{R[x]}{\langle x^n - 1\rangle} = \oplus_{i=1}^{m} \frac{R[x]}{\langle f_i(x)\rangle} \, .$$

Thus, every ideal I of $\frac{R[x]}{\langle x^n-1\rangle}$ can be written as

$$I = \oplus_{i=1}^{m} I_i,$$

where I_i is an ideal of the ring $\frac{R[x]}{\langle f_i(x)\rangle}$, $i = 1, 2, \dots, m$. From Theorem 5.3.5, the ideals $\langle 1 + \langle f_i(x)\rangle\rangle$, $\langle 2 + \langle f_i(x)\rangle\rangle$, $\langle u + \langle f_i(x)\rangle\rangle$, $\langle 2u + \langle f_i(x)\rangle\rangle$, $\langle 2 + u + \langle f_i(x)\rangle\rangle$ and $\langle \langle 2, u\rangle + \langle f_i(x)\rangle\rangle$ of $\frac{R[x]}{\langle f_i(x)\rangle}$ correspond to the ideals

$$\begin{gathered} \left\langle \hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle, \quad \left\langle 2\hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle, \\ \left\langle u\hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle, \quad \left\langle 2u\hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle, \\ \left\langle (2+u)\hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle, \quad \left\langle \langle 2, u\rangle\, \hat{f}_i(x) + \langle x^n - 1\rangle \right\rangle \end{gathered}$$

in R_n, respectively. ∎

Corollary 5.4.4. *Let* $x^n - 1 = f_1(x)f_2(x)\cdots f_m(x)$, *where* $f_i(x)$, $i = 1, 2, \dots, m$, *are monic basic irreducible pairwise coprime polynomials in* $R[x]$. *The number of cyclic codes over* R *is* 7^m.

One generator cyclic codes as n^{th} roots of unity

From Theorem 5.3.1, there exists a primitive n^{th} root of unity in $GR(R, r)$. Let $\xi^{i_1}, \xi^{i_2}, \dots, \xi^{i_k}$ be n^{th} roots of unity in $GR(R, r)$. Define the minimal polynomial $M_i(x)$ of ξ^i as the monic polynomial of least degree having ξ^i as a root over R. Then a cyclic code $\mathcal{C}$ of length n over R can also be described in terms of n^{th} roots of unity, and a cyclic code $\mathcal{C}$ can be defined as $\mathcal{C} = \{c(x) \in R_n \ : \ c(\xi^{i_j}) = 0,\ 1 \le j \le k\}$. The generator polynomial $g(x)$ of $\mathcal{C}$ is the least common multiple of minimal polynomials of ξ^{i_j}, $1 \le j \le k$. Then $g(x) \mid (x^n - 1)$. Hence $\mathcal{C}$ is a free code over R.

The following is a straightforward generalization of [17, Proposition 2].

Proposition 5.4.5 (BCH bound). *Suppose that the generator polynomial $g(x)$ of a cyclic code $\mathcal{C}$ of length n over R divides $(x^n - 1)$ and has $\xi^b, \xi^{b+1}, \ldots, \xi^{b+\delta-1}$ as roots, where ξ is a primitive n^{th} root of unity in a Galois ring extension of R. Then $d_H(\mathcal{C}) \geq \delta$.*

Example 5.4.6. *Let ξ be a root of the basic primitive polynomial $f(x) = x^4 + 3x^3 + 2x^2 + 1$, which is a factor of $x^{15} - 1$ over R. Let the generator polynomial of a cyclic code of length 15 over R is defined as $g(x) = lcm\ (M_0(x), M_1(x), M_2(x), M_3(x), M_4(x), M_5(x), M_6(x))$, where $M_i(x)$ are the minimal polynomials of ξ^i, $i = 0, 1, 2, 3, 4, 5, 6$, respectively. We have*

$$\begin{aligned} M_0(x) &= x - 1, \\ M_1(x) = M_2(x) = M_4(x) &= x^4 + 3x^3 + 2x^2 + 1, \\ M_3(x) = M_6(x) &= x^4 + x^3 + x^2 + x + 1, \\ M_5(x) &= x^2 + x + 1. \end{aligned}$$

Therefore, $g(x) = x^{11} + 2x^9 + 3x^8 + 3x^7 + x^6 + 2x^4 + 3x^3 + x^2 + 3x + 3$. The cyclic code $\mathcal{C} = \langle g(x) \rangle$ is a free code of rank 4. Since $g(x)$ has 7 consecutive roots, $d_H(\mathcal{C}) \geq 8$, where $d_H(\mathcal{C})$ denotes the minimum Hamming distance of $\mathcal{C}$. Also, since $w_H(2g(x)) = 8$, we must have $d_H(\mathcal{C}) = 8$.

5.4.2 Cyclic codes of arbitrary length over $\mathbb{Z}_4 + u\mathbb{Z}_4$

Now we consider the general form of the generators of cyclic codes of arbitrary length n over R. The technique we have used here to find the generators of a cyclic code is same as in [136]. However the generators we have obtained differ slightly from that of [136, Theorem 6].

Define $\Psi : R \rightarrow \mathbb{Z}_4$ such that $\Psi(a + bu) = a \pmod{u}$. It can easily be seen that Ψ is a ring homomorphism with ker $\Psi = \langle u \rangle = u\mathbb{Z}_4$. Extend Ψ to the homomorphism $\Phi : \frac{R[x]}{\langle x^n - 1 \rangle} \rightarrow \frac{\mathbb{Z}_4[x]}{\langle x^n - 1 \rangle}$ such that $\Phi(a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}) = \Psi(a_0) + \Psi(a_1)x + \Psi(a_2)x^2 + \cdots + \Psi(a_{n-1})x^{n-1}$.

Let $\mathcal{C}$ be a cyclic code of length n over R. Restrict Φ to $\mathcal{C}$ and define

$$J = \left\{ h(x) \in \frac{\mathbb{Z}_4[x]}{\langle x^n - 1\rangle} \ : \ uh(x) \in \ker \Phi \right\}.$$

Clearly J is an ideal of $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$. So J is a cyclic code of length n over $\mathbb{Z}_4$. Similarly, the image of $\mathcal{C}$ under Φ is an ideal of $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$.

If n is odd, then $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$ is a principal ideal ring and hence $\Phi(\mathcal{C}) = \langle g(x)\rangle$ and ker Φ $= \langle ua(x)\rangle$ for some $g(x), a(x) \in \mathbb{Z}_4[x]$. In [136, Thereom 6] authors have defined a cyclic code $\mathcal{C}$ as $\mathcal{C} = \langle g(x), ua(x)\rangle$. However this does not cover all cases of cyclic codes. For example, if we consider the cyclic code $\mathcal{C} = \langle 2x^2 + u\rangle$ of length 3 over R, then $\Phi(\mathcal{C}) = \langle 2\rangle$ and ker $\Phi = \langle 2u\rangle$. But $\langle \Phi(\mathcal{C}),\ \ker \Phi\rangle = \langle 2, 2u\rangle = \langle 2\rangle \neq \mathcal{C}$. Similarly, for even n, the cyclic code structure $\mathcal{C} = \langle g_1(x), 2g_2(x), ua_1(x), 2ua_2(x)\rangle$ defined in [136] does not cover all cyclic codes. For example, if we consider the cyclic code $\mathcal{C} = \langle 2x + u\rangle$ of length 2 over R, then $\Phi(\mathcal{C}) = \langle 2\rangle$ and ker $\Phi = \langle 2u\rangle$. But $\langle \Phi(\mathcal{C}),\ \ker \Phi\rangle = \langle 2, 2u\rangle = \langle 2\rangle \neq \mathcal{C}$.

We discuss the structure of cyclic codes over R. From [5, Theorem 1], a cyclic code of length n over $\mathbb{Z}_4$ can be written as $\langle f_1(x) + 2f_{12}(x),\ 2f_2(x)\rangle$, where $f_2(x) \mid f_1(x) \mid x^n - 1$ for some $f_1(x), f_2(x), f_{12}(x) \in \mathbb{Z}_2[x]$. So $\Phi(\mathcal{C}) = \langle f_1(x) + 2f_{12}(x),\ 2f_2(x)\rangle$, where $f_2(x) \mid f_1(x) \mid x^n - 1$ for some $f_1(x), f_2(x), f_{12}(x) \in \mathbb{Z}_2[x]$ and $J = \langle f_3(x) + 2f_{34}(x),\ 2f_4(x)\rangle$. Moreover ker $\Phi = \langle uf_3(x) + 2uf_{34}(x),\ 2uf_4(x)\rangle$, where $f_4(x) \mid f_3(x) \mid x^n - 1$ for some $f_3(x), f_4(x), f_{34}(x) \in \mathbb{Z}_2[x]$. Hence

$$\begin{aligned} \mathcal{C} = \langle f_1(x) + 2f_{12}(x) + uf_{13}(x) + 2uf_{14}(x) &\ , \\ 2f_2(x) + uf_{23}(x) + 2uf_{24}(x) &\ , \\ uf_3(x) + 2uf_{34}(x) &\ , \\ 2uf_4(x)\rangle &\ . \end{aligned}$$

where $f_4(x) \mid f_3(x) \mid f_1(x) \mid x^n - 1$ and $f_4(x) \mid f_2(x) \mid f_1(x) \mid x^n - 1$.

Now we determine the conditions on polynomials $f_{ij}(x)$, $i, j = 1, 2, 3, 4$. The conditions we have obtained here (Theorem 5.4.8) are similar to the ones obtained in [68]. For an ideal

I of R_n, we define Tor $(\mathcal{C})$ and Res $(\mathcal{C})$ as follows:

$$\begin{aligned}\text{Tor } (\mathcal{C}) &= \left\{g(x) \in \frac{\mathbb{Z}_4[x]}{\langle x^n - 1\rangle} \ : \ ug(x) \in \mathcal{C}\right\}\\ \text{Res } (\mathcal{C}) &= \left\{g(x) \in \frac{\mathbb{Z}_4[x]}{\langle x^n - 1\rangle} \ : \ g(x) + up(x) \in \mathcal{C} \text{ for some } p(x) \in \frac{\mathbb{Z}_4[x]}{\langle x^n - 1\rangle}\right\}.\end{aligned}$$

It is easy to see that Res $(\mathcal{C}) = \Phi(\mathcal{C})$ and Tor $(\mathcal{C}) = J$. So we can associate four ideals to $\mathcal{C}$ as follows [68]:

$$\begin{aligned}\mathcal{C}_1 &= \text{Res}(\text{Res}(\mathcal{C})) = \mathcal{C} \bmod \langle 2,\ u\rangle,\\ \mathcal{C}_2 &= \text{Tor}(\text{Res}(\mathcal{C})) = \{f(x) \in \mathbb{Z}_2[x] \ : \ 2f(x) \in \mathcal{C} \bmod u\},\\ \mathcal{C}_3 &= \text{Res}(\text{Tor}(\mathcal{C})) = \{f(x) \in \mathbb{Z}_2[x] \ : \ uf(x) \in \mathcal{C} \bmod 2u\} \text{ and}\\ \mathcal{C}_4 &= \text{Tor}(\text{Tor}(\mathcal{C})) = \{f(x) \in \mathbb{Z}_2[x] \ : \ 2uf(x) \in \mathcal{C}\}.\end{aligned}$$

These all are ideals of $\frac{\mathbb{Z}_2[x]}{\langle x^n - 1\rangle}$.

Theorem 5.4.7. *Any ideal I of the ring $R_n = \frac{R[x]}{\langle x^n-1\rangle}$ is uniquely generated by the polynomials*

$$\begin{aligned}A_1(x) &= f_1(x) + 2f_{12}(x) + uf_{13}(x) + 2uf_{14}(x)\ ,\\ A_2(x) &= 2f_2(x) + uf_{23}(x) + 2uf_{24}(x)\ ,\\ A_3(x) &= uf_3(x) + 2uf_{34}(x)\ ,\\ A_4(x) &= 2uf_4(x)\ ,\end{aligned}$$

where $\mathcal{C}_j := \langle f_j(x)\rangle$ and $f_{ij}(x) = 0$ or deg $f_{ij}(x) <$ deg $f_j(x)$, $1 \leq i,\ j \leq 4$.

Proof. Same as [117, Theorem 1]. ■

Theorem 5.4.8. *Let $f_i(x)$, $f_{ij}(x)$ and $A_i(x)$, $i = 1, 2, 3, 4$ be defined as in Theorem 5.4.7* *and $I = \langle A_1(x),\ A_2(x),\ A_3(x),\ A_4(x)\rangle$. Then the following relations hold in $\frac{\mathbb{Z}_2[x]}{\langle x^n-1\rangle}$.*

$$f_4(x) \mid f_3(x) \mid f_1(x) \mid (x^n-1) \textit{ and } f_4(x) \mid f_2(x) \mid f_1(x) \mid (x^n-1)\ , \tag{5.4.1}$$

$$f_2(x) \mid f_{12}(x)\left(\tfrac{x^n-1}{f_1(x)}\right)\ , \tag{5.4.2}$$

$$f_3(x) \mid \tfrac{x^n-1}{f_1(x)}\left(f_{13}(x) - \tfrac{f_{12}(x)}{f_2(x)}f_{23}(x)\right)\ , \tag{5.4.3}$$

$$f_3(x) \mid \tfrac{f_1(x)}{f_2(x)}f_{23}(x)\ , \tag{5.4.4}$$

$$f_4(x) \mid f_{23}(x)\ , \tag{5.4.5}$$

$$f_4(x) \mid \left(\tfrac{x^n-1}{f_3(x)}\right)f_{34}(x)\ , \tag{5.4.6}$$

$$f_4(x) \mid \tfrac{x^n-1}{f_2(x)}\left(f_{24}(x) - \tfrac{f_{23}(x)}{f_3(x)}f_{34}(x)\right)\ , \tag{5.4.7}$$

$$f_4(x) \mid \left(f_{12}(x) - \tfrac{f_1(x)}{f_3(x)}f_{34}(x)\right)\ , \tag{5.4.8}$$

$$f_4(x) \mid \left(f_{13}(x) - \tfrac{f_1(x)}{f_2(x)}f_{24}(x) - \tfrac{f_1(x)}{f_2(x)f_3(x)}f_{23}(x)f_{34}(x)\right)\ , \tag{5.4.9}$$

$$f_4(x) \mid \tfrac{x^n-1}{f_1(x)}\left(f_{14}(x) - \tfrac{f_{12}(x)}{f_2(x)}f_{24}(x) - \tfrac{f_{13}(x)+\frac{f_{12}(x)}{f_2(x)}f_{23}(x)}{f_3(x)}f_{34}(x)\right)\ . \tag{5.4.10}$$

Proof. The result follows from [117, Proposition 1] with slight modifications in the present setting. ■

When n is odd

Let n be an odd integer. Then a cyclic code of length n over $\mathbb{Z}_4$ is principally generated. So $\Phi(\mathcal{C})$ and ker Φ are principal ideals of $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$, and so $\Phi(\mathcal{C}) = \langle f_1(x) + 2f_2(x)\rangle$ and ker $\Phi = \langle uf_3(x) + 2uf_4(x)\rangle$, where $f_2(x) \mid f_1(x) \mid x^n - 1$ and $f_4(x) \mid f_3(x) \mid x^n - 1$. Therefore $\mathcal{C} = \langle f_1(x) + 2f_2(x) + uf_{13}(x) + 2uf_{14}(x),\ uf_3(x) + 2uf_4(x)\rangle$. Using the technique used in [138, Theorem 3.2], we get the following result.

Theorem 5.4.9. *Let n be an odd integer and $\mathcal{C}$ a cyclic code of length n over R. Then*

$$\mathcal{C} = \langle f_1(x) + 2f_2(x) + 2uf_{14}(x),\ uf_3(x) + 2uf_4(x)\rangle\ ,$$

where $f_2(x) \mid f_1(x) \mid (x^n-1)$ and $f_4(x) \mid f_3(x) \mid f_1(x) \mid x^n - 1$ in R_n.

When $n = 2^k$

Theorem 5.4.10. *The ring $R_n = \frac{R[x]}{\langle x^n-1\rangle}$ is a local ring when $n = 2^k$ where $k \geq 1$.*

Proof. From the definition of Φ, we have Φ is a surjective ring homomorphism. From Theorem 2.3.33, the ring $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$ is a local ring with the unique maximal ideal $\langle 2, x-1\rangle$. The inverse image of the maximal ideal $\langle 2, x-1\rangle$ is $\Phi^{-1}(\langle 2, x-1\rangle) = \langle 2, u, x-1\rangle$, which is a maximal ideal in R_n as it contains all non-units of R_n. ∎

We know from Theorem 2.2.5 that $\frac{\mathbb{Z}_2[x]}{\langle x^n-1\rangle}$ is a finite chain ring, so each ideal of $\frac{\mathbb{Z}_2[x]}{\langle x^n-1\rangle}$ can be written as $\langle (x-1)^s\rangle$ for $0 \leq s \leq n$. Thus $\mathcal{C}_j = \langle (x-1)^{s_j}\rangle$, $0 \leq s_j \leq n$. Hence a cyclic code $\mathcal{C}$ of length 2^k over R can be written as

$$\begin{aligned}\mathcal{C} = \langle (x-1)^{s_1} + 2f_{12}(x) + uf_{13}(x) + 2uf_{14}(x)\ ,\\ 2(x-1)^{s_2} + uf_{23}(x) + 2uf_{24}(x),\\ u(x-1)^{s_3} + 2uf_{34}(x),\\ 2u(x-1)^{s_4}\rangle\ .\end{aligned}$$

For $n = 2^k$, the conditions on the polynomial $f_{ij}(x)$ in Theorem 5.4.8 can be put in much simpler form as shown in Theorem 5.4.13 using the following lemma.

Lemma 5.4.11. *In R_n,*

1. $(x-1)^n = 2(x-1)^{\frac{n}{2}}$.

2. $(x-1)$ *is nilpotent with nilpotency* $\frac{3n}{2}$.

3. *an element* $f(x) = \sum_{j=0}^{n-1} a_j(x-1)^j$ *is a unit if and only if* a_0 *is a unit in* R.

Proof.

1. We can show using induction on k that $x^n + 1 = (x+1)^n + 2x^{\frac{n}{2}}$ over R [4]. On replacing x by $x-1$, we get that $(x-1)^n + 1 = x^n + 2(x-1)^{\frac{n}{2}}$. This implies that $(x-1)^n = 2(x-1)^{\frac{n}{2}}$ in R_n.

2. It follows from (1) that $(x-1)^{n+\frac{n}{2}} = (x-1)^n(x-1)^{\frac{n}{2}} = 2(x-1)^{\frac{n}{2}}(x-1)^{\frac{n}{2}} = 2(x-1)^n = 0$. On the other hand, for any integer $0 \leq s < \frac{n}{2}$, we have $(x-1)^{n+s} =$

$2(x-1)^{\frac{n}{2}}(x-1)^s = 2(x-1)^{\frac{n}{2}+s} \neq 0$. Thus $(x-1)$ is nilpotent of nilpotency index $\frac{3n}{2}$.

3. Suppose that $f(x) = \sum_{j=0}^{n-1} a_j(x-1)^j$ is a unit in R_n and a_0 is a non-unit in R. Since $f(x)$ is a unit, it is regular. Then $2uf(x) = 2u\sum_{j=l}^{n-1} a_j(x-1)^j$, where $l > 0$ is the least positive integer such that a_l is a unit. This implies that $2uf(x) = 2u(x-1)^l \sum_{j=l}^{n-1} a_j(x-1)^{j-l}$, which in turn implies that $2u(x-1)^{n-l}f(x) = 2u(x-1)^n \sum_{j=l}^{n-1} a_j(x-1)^{j-l} = 0$, from (1). Therefore $f(x)$ is a non-unit, a contradiction. Hence a_0 must be a unit in R.

   Conversely, suppose that a_0 is a unit in R and $f(x) = \sum_{j=0}^{n-1} a_j(x-1)^j$ is a non-unit in R_n. Then $f(x) \in \langle 2,\ u,\ x-1\rangle$. This implies that $f(x) - \sum_{j=1}^{n-1} a_j(x-1)^j = a_0 \in \langle 2,\ u,\ x-1\rangle$, a contradiction. Therefore $f(x)$ is a unit in R_n.

■

In view of the above lemma, every polynomial $f(x)$ in $R[x]$ can be written as $f(x) = \sum_{j=0}^{n-1}(a_{1j} + 2a_{2j} + ua_{3j} + 2ua_{4j})(x-1)^j$. Thus the generators of an ideal I of R_n (cyclic codes over R) can be written as

$$\begin{aligned}
A_1(x) &= (x-1)^{s_1} + 2\sum_{j=0}^{n-1} a_j(x-1)^j + u\sum_{j=0}^{n-1} b_j(x-1)^j + 2u\sum_{j=0}^{n-1} c_j(x-1)^j \ , \\
A_2(x) &= 2(x-1)^{s_2} + u\sum_{j=0}^{n-1} b'_j(x-1)^j + 2u\sum_{j=0}^{n-1} c'_j(x-1)^j \ , \\
A_3(x) &= u(x-1)^{s_3} + 2u\sum_{j=0}^{n-1} c'_j(x-1)^j \ , \\
A_4(x) &= 2u(x-1)^{s_4} \ .
\end{aligned}$$

If t_1, t_2, t_3 are smallest non-negative integers such that $a_{t_1}, a_{t_2}, a_{t_3}$ are non-zero in $\mathbb{Z}_2$, then $A_1(x)$ can also be written as $A_1(x) = (x-1)^s + 2(x-1)^{t_1}h_1(x) + u(x-1)^{t_2}h_2(x) + 2u(x-1)^{t_3}h_3(x)$, where $h_1(x) = \sum_{j=t_1}^{n-1} a_j(x-1)^{j-t_1}$, $h_2(x) = \sum_{j=t_2}^{n-1} b_j(x-1)^{j-t_2}$ and

$h_3(x) = \sum_{j=t_3}^{n-1} c_j(x-1)^{j-t_3}$ are zero or units in $\frac{\mathbb{Z}_2[x]}{\langle x^n-1\rangle}$.

$$\begin{aligned} \text{Let } B_1(x) &= (x-1)^{s_1} + 2(x-1)^{i_1}g_1(x) + u(x-1)^{i_2}g_2(x) + 2u(x-1)^{i_3}g_3(x)\ , \\ B_2(x) &= 2(x-1)^{s_2} + u(x-1)^{j_2}h_2(x) + 2u(x-1)^{j_3}h_3(x)\ , \\ B_3(x) &= u(x-1)^{s_3} + 2u(x-1)^{k_3}l_3(x)\ , \\ B_4(x) &= 2u(x-1)^{s_4}\ , \end{aligned}$$

where $g_1(x)$, $g_2(x)$, $g_3(x)$, $h_2(x)$, $h_3(x)$ and $l_3(x)$ are either zero or units in $\frac{\mathbb{Z}_2[x]}{\langle x^n-1\rangle}$. The following theorem describes the complete ideal structure of R_n.

Lemma 5.4.12. *([4, Theorem 11] and [42, Theorem 4.4]) Let $\mathcal{R}$ be either $\mathbb{Z}_4$ or $\mathbb{F}_2+u\mathbb{F}_2$, $u^2=0$ and C be a cyclic code of length 2^k over $\mathcal{R}$. Then $C = \langle (x-1)^s + \delta(x-1)^t h(x),\ \delta(x-1)^m\rangle$, $1 \le s \le n-1$, $0 \le t \le s-1$, $0 \le m \le T-1$ and $h(x)$ is either zero or a unit in $\frac{\mathbb{F}_2[x]}{\langle x^n-1\rangle}$ with deg $h(x) \le T-t-1$, where $T = min\{s,\ \frac{n}{2},\ n-s+t\}$, $\delta = 2$ for $\mathbb{Z}_4$, and $T = min\{s,\ n-s+t\}$, $\delta = u$ for $\mathbb{F}_2+u\mathbb{F}_2$.*

Theorem 5.4.13. *Let I be a non-trivial ideal of R_n. Then I is one of the following:*

(I) Principal ideals:

1. $I = \langle 2u(x-1)^{s_4}\rangle$, $0 \le s_4 \le n-1$.
2. $I = \langle u(x-1)^{s_3}\rangle$, $0 \le s_3 \le n-1$.
3. $I = \langle B_2(x)\rangle$, $0 \le s_2, j_2 \le n-1$, $0 \le j_3 \le\ min\{s_2, j_2\}-1$.
4. $I = \langle B_1(x)\rangle$, $1 \le s_1, i_1, i_2 \le n-1$, $0 \le i_3 \le s_1-1$.

(II) Non-principal ideals:

1. $I = \langle B_1(x),\ B_2(x)\rangle$, $0 \le s_1 \le n-1$, $0 \le s_2 \le\ min\{\frac{n}{2}, s_1, n-s_1+i_1\}-1$, $0 \le i_1 \le n-1$, $0 \le i_3 < j_3 \le\ min\{s_2, j_2\}-1$, $0 \le i_2 < j_2 \le\ min\{s_1, n-s_1+i_2\}-1$.
2. $I = \langle B_1(x),\ B_3(x)\rangle$, $0 \le s_1 \le n-1$, $0 \le s_3 \le\ min\{\frac{n}{2}, s_1, n-s_1+i_2\}-1$, $0 \le i_2, i_3, k_3 \le s_3-1$ *and* $i_1 \le n-1$.
3. $I = \langle B_1(x),\ B_4(x)\rangle$, $0 \le s_1 \le n-1$, $0 \le s_4 \le s_1-1$, $i_3 \le s_4-1$ *and* $i_1, i_2 \le n-1$.

4. $I = \langle B_2(x), B_3(x)\rangle$, $0 \leq s_2, s_3 \leq n-1$, $0 \leq j_3 < k_3 < j_2 \leq s_3 - 1$.

5. $I = \langle B_2(x), B_4(x)\rangle$, $0 \leq s_2 \leq n-1$, $0 \leq s_4 \leq\ min\{s_2, j_2\} - 1$, $0 \leq j_3 \leq s_4 - 1$ *and* $0 \leq j_2 \leq n-1$.

6. $I = \langle B_3(x), B_4(x)\rangle$, $0 \leq s_3 \leq n-1$, $0 \leq s_4 \leq s_3 - 1$, $k_3 \leq s_4 - 1$.

7. $I = \langle B_1(x),\ B_2(x),\ B_3(x)\rangle$, $0 \leq s_1 \leq n-1$, $0 \leq s_2 \leq\ min\{\frac{n}{2}, s_1, n-s_1+i_1\}-1$, $0 \leq j_2 \leq\ min\{s_1, s_3, n-s_1+i_2\} - 1$, $0 \leq i_1 \leq s_2 - 1$, $0 \leq i_2 \leq s_3 - 1$, $0 \leq i_3 < k_3 <\ min\{s_2, j_2\}$ *and* $0 \leq s_3 \leq s_1 - 1$.

8. $I = \langle B_1(x),\ B_2(x),\ B_4(x)\rangle$, $0 \leq s_1 \leq n-1$, $0 \leq i_1 \leq s_2 - 1$, $0 \leq i_3, j_3 \leq s_4 - 1$, $0 \leq i_2 \leq n-1$, $0 \leq j_2 \leq\ min\{s_2, n-s_1+i_2\} - 1$.

9. $I = \langle B_1(x),\ B_3(x),\ B_4(x)\rangle$, $0 \leq s_1 \leq n-1$, $i_2 < s_3 \leq s_1 - 1$, $i_3, k_3 < s_4 \leq s_1 - 1$.

10. $I = \langle B_2(x),\ B_3(x),\ B_4(x)\rangle$, $0 \leq s_2,\ s_3 \leq n-1$, $0 \leq j_2 \leq s_3 - 1$, $0 \leq j_3, k_3 \leq s_4$.

11. $I = \langle B_1(x),\ B_2(x),\ B_3(x),\ B_4(x)\rangle$, $i_3, j_3, k_3 < j_2 < s_3 < s_1 \leq n-1$, $i_1 < s_2$, $i_2 < s_3$, $j_2 < s_4 < s_3 < s$.

Proof. We present here the proofs of I (1) and II (1). Other cases can be proved similarly. For I (1), if I is a principal ideal of R_n containing only multiples of $2u$, then Tor (Tor (I)) is an ideal of $\frac{\mathbb{Z}_2[x]}{\langle x^n-1\rangle}$. From Theorem 2.2.5, we get that Tor (Tor (I))$= \langle (x-1)^{s_4}\rangle$, for some $0 \leq s_4 \leq n-1$. Therefore $I = \langle 2u(x-1)^{s_4}\rangle$, $0 \leq s_4 \leq n-1$.

For II (1), consider the non-principal ideal $I = \langle B_1(x),\ B_2(x)\rangle$, where $B_1(x) = (x-1)^{s_1} + 2(x-1)^{i_1}g_1(x) + u(x-1)^{i_2}g_2(x) + 2u(x-1)^{i_3}g_3(x)$ and $B_2(x) = 2(x-1)^{s_2} + u(x-1)^{j_2}h_2(x) + 2u(x-1)^{j_3}h_3(x)$. We have $I \pmod u = \langle (x-1)^{s_1} + 2(x-1)^{i_1}g_1(x),\ 2(x-1)^{s_2}\rangle$ and $I \pmod 2 = \langle (x-1)^{s_1} + u(x-1)^{i_2}g_2(x),\ u(x-1)^{j_2}\rangle$. Then from Lemma 5.4.12, we get $0 \leq s_2 \leq \min\{\frac{n}{2}, s_1, n-s_1+i_1\} - 1$ and $0 \leq j_2 \leq \min\{s_1, n-s_1+i_2\} - 1$, respectively. Remaining conditions follow from Theorem 5.4.7. ■

5.5 Ranks and minimal spanning sets

It may be noted here that unlike in the case of finite fields, a generator polynomial of ker Φ or of $\Phi(\mathcal{C})$ (a generator polynomial of cyclic code over $\mathbb{Z}_4$) may not necessarily divide

$x^n - 1$. So a cyclic code $\mathcal{C}$ over R may not have a basis. However we can find a minimal set of generators for $\mathcal{C}$. Let $\mathcal{C} = \langle A_1(x),\ A_2(x),\ A_3(x),\ A_4(x)\rangle$, where we use the same notations as given in the preceding section, i.e.,

$$\begin{aligned} A_1(x) &= f_1(x) + 2f_{12}(x) + uf_{13}(x) + 2uf_{14}(x)\ , \\ A_2(x) &= 2f_2(x) + uf_{23}(x) + 2uf_{24}(x)\ , \\ A_3(x) &= uf_3(x) + 2uf_{34}(x)\ , \\ A_4(x) &= 2uf_4(x)\ . \end{aligned}$$

Theorem 5.5.1. *Let n be a positive integer and $\mathcal{C}$ a cyclic code of length n over R. If $\mathcal{C} = \langle A_1(x),\ A_2(x),\ A_3(x),\ A_4(x)\rangle$, with $s_1 = deg\ f_1(x)$, $s_2 = deg\ f_2(x)$, $s_3 = deg\ f_3(x)$, $s' = min\{deg\ f_2(x)\ ,\ deg\ f_3(x)\ \}$ and $s_4 = deg\ f_4(x)$, then $\mathcal{C}$ has rank $n+s_1+s'-s_2-s_3-s_4$ and a minimal spanning set $B = \{A_1(x), xA_1(x), \ldots, x^{n-s_1-1}A_1(x),\ A_2(x), xA_2(x), \ldots, x^{s_1-s_2-1}A_2(x),$ $A_3(x), xA_3(x), \ldots, x^{s_1-s_3-1}A_3(x),\ A_4(x), xA_4(x), \ldots, x^{s'-s_4-1}A_4(x)\}$. Furthermore, if $f_{23}(x) \neq 0$, we have $|\mathcal{C}| = 2^{4n+s_1+s'-3s_2-2s_3-s_4}$ and if $f_{23}(x) = 0$, we have $|\mathcal{C}| = 2^{4n+s'-2s_2-2s_3-s_4}$.*

Proof. Over finite fields, it is well known that if $g(x)$, with deg $g(x) = t$, is a generator polynomial of a cyclic code of length n, then the set $\{g(x), xg(x), \ldots, x^{n-t-1}g(x)\}$ spans the cyclic code. Since $A_i(x)$, $i = 1, 2, 3, 4$, are the generators of $\mathcal{C}$, the set $B' = \{A_1(x), xA_1(x), \ldots, x^{n-s_1-1}A_1(x), A_2(x), xA_2(x), \ldots, x^{n-s_2-1}A_2(x), A_3(x), xA_3(x), \ldots,$ $x^{n-s_3-1}A_3(x), A_4(x), xA_4(x), \ldots, x^{n-s_4-1}A_4(x)\}$ spans $\mathcal{C}$. But this is not a minimal set of generators. So it is sufficient to show that B spans B'.

Let $s' =$ deg $f_3(x)$. First we show that $2ux^{s_3-s_4}f_4(x) \in$ Span (B). Write $A_3(x) = uA_3'(x)$, where $A_3'(x)$ is a regular polynomial in $\mathbb{Z}_4[x]$. Dividing $x^{s_3-s_4}f_4(x)$ by $A_3'(x)$, we get $2ux^{s_3-s_4}f_4(x) = 2uA_3'(x) + 2um(x)$, where $2um(x)$ is either zero or deg $m(x) < s_3$. If $m(x) = 0$, then $2ux^{s_3-s_4}f_4(x) \in$ Span (B). Otherwise, $2um(x) \in \mathcal{C}$. This implies that $f_4(x) \mid m(x)$, as $m(x) \in \mathcal{C}_4 = \langle f_4(x)\rangle$. So $s_4 \leq$ deg $m(x) < s_3$. Thus $2um(x) = 2uq(x)f_4(x)$, where $q(x) \in R[x]$ with deg $q(x) < s_3 - s_4$. Therefore $2ux^{s_3-s_4}f_4(x) \in$ Span (B).

Next suppose $s' =$ deg $f_2(x)$. Since $A_2(x)$ is not regular, it is not appropriate to take $A_2(x)$ as divisor in the division algorithm. However, by direct computation, we find that

$2ux^{s_2-s_4}f_4(x) \in$ Span (B). Since $f_4(x) \mid f_2(x)$, there exists $q(x) \in \mathbb{Z}_2[x]$ such that $f_2(x) = q(x)f_4(x)$, where $q(x) = q_0+q_1x+\cdots+q_{s_2-s_4}x^{s_2-s_4}$. We have $uq^{-1}_{s_2-s_4}A_2(x) = 2uq^{-1}_{s_2-s_4}f_2(x)$. This implies that $uq^{-1}_{s_2-s_4}A_2(x) = 2uq^{-1}_{s_2-s_4}(q_0+q_1x+\cdots+q_{s_2-s_4}x^{s_2-s_4})f_4(x)$, which further implies that $2uf_4(x)x^{s_2-s_4} = uq^{-1}_{s_2-s_4}A_2(x) - 2uf_4(x)q^{-1}_{s_2-s_4}(q_0+q_1x+\cdots+q_{s_2-s_4-1}x^{s_2-s_4-1})$. Thus $2uf_4(x)x^{s_2-s_4} \in$ Span (B). Similarly, we can show that $x^{s_1-s_2}A_2(x)$, $x^{s_1-s_3}A_3(x) \in$ Span (B). So B spans B'.

Now we show that none of the elements of the set B can be written as a linear combination of other elements of B. Suppose, if possible $x^{n-s_1-1}A_1(x) = a(x)A_1(x) + b(x)A_2(x) + c(x)A_3(x) + d(x)A_4(x)$, where $a(x) = a_1(x) + 2a_2(x) + ua_3(x) + 2ua_4(x)$, $b(x)$, $c(x)$, $d(x) \in R[x]$ with degrees less than or equal to $n - s_1 - 2$, $s_1 - s_2 - 1$, $s_1 - s_3 - 1$ and $s' - s_4 - 1$, respectively. Then we have $x^{n-s_1-1}f_1(x) = a_1(x)f_1(x)$. This is a contradiction, as deg $x^{n-s_1-1}f_1(x) = n - 1$ and deg $a_1(x)f_1(x) \leq n - 2$. So $x^{n-s_1-1}A_1(x)$ cannot be written as a linear combination of other elements of B. The rest can be shown using similar arguments. ■

Theorem 5.5.2. *Let n be an odd integer and $\mathcal{C}$ be a cyclic code of length n over R. If $\mathcal{C} = \langle f_1(x) + 2f_2(x) + 2uf_{14}(x),\ uf_3(x) + 2uf_4(x)\rangle$, with deg $f_1(x) = k_1$ and deg $f_3(x) = k_2$, respectively, then $\mathcal{C}$ has rank $n - k_2$ and a minimal spanning set $B = \{(f_1(x) + 2f_2(x) + 2uf_{14}(x)), x(f_1(x) + 2f_2(x) + 2uf_{14}(x)), x^2(f_1(x) + 2f_2(x) + 2uf_{14}(x)), \ldots, x^{n-k_1-1}(f_1(x) + 2f_2(x)+2uf_{14}(x)),\ u(f_3(x)+2f_4(x)), xu(f_3(x)+2f_4(x)), x^2u(f_3(x)+2f_4(x)), \ldots, x^{k_1-k_2-1}u(f_3(x)+2f_4(x))\}$.*

Proof. The result can easily be proved using the argument used in Theorem 5.5.1. ■

Theorem 5.5.3. *Let $\mathcal{C} = \langle A_1(x),\ A_2(x),\ A_3(x),\ A_4(x)\rangle$ be a cyclic code of length n over R. Then $w_H(\mathcal{C}) = w_H(\mathcal{C}_4)$, i.e., $w_H(\mathcal{C}) = w_H(\langle 2uf_4(x)\rangle)$.*

Proof. Let $c(x) = c_1(x) + 2c_2(x) + uc_3(x) + 2uc_4(x) \in \mathcal{C}$. Then $2uc(x) = 2uc_0(x)$. This implies that $c_0(x) \in \mathcal{C}_4$. It is clear that $w_H(2uc(x)) = w_H(2uc_0(x)) = w_H(c_0(x)) \leq w_H(c(x))$. Therefore $w_H(\mathcal{C}_4) \leq w_H(\mathcal{C})$. Also, since $2u\mathcal{C}$ is a subcode of $\mathcal{C}$, $w_H(\mathcal{C}) \leq w_H(2u\mathcal{C})$. Hence the result. ■

5.6 One generator cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$

We now consider cyclic codes over R which are principal ideals in $\frac{R[x]}{\langle x^n-1\rangle}$. Below we generalize [17, Proposition 1] for the present case and provide a necessary condition (Theorem 5.6.4) and a sufficient condition (Theorem 5.6.5) for the cyclic codes over R to be free.

The following result gives a sufficient condition for a cyclic code $\mathcal{C}$ over R to be a free $\mathbb{Z}_4$-code.

Theorem 5.6.1. *Let $\mathcal{C} = C_1 + uC_2$ be a cyclic code of length n over R. If C_1, C_2 are free codes over $\mathbb{Z}_4$, then $\mathcal{C}$ is a free $\mathbb{Z}_4$-module.*

Proof. Suppose that C_1, C_2 are $\mathbb{Z}_4$-free codes of ranks k_1, k_2, respectively. Let $\{c_{11}, c_{12}, \ldots, c_{1k_1}\}$ and $\{c_{21}, c_{22}, \ldots, c_{2k_2}\}$ be $\mathbb{Z}_4$-bases of C_1 and C_2, respectively. Then the set $\{c_{11}, c_{12}, \ldots, c_{1k_1}, uc_{21}, uc_{22}, \ldots, uc_{2k_2}\}$ spans $\mathcal{C}$, as every element of $\mathcal{C}$ can be expressed as a linear combination of elements of this set. Now suppose there exist scalars $a_i, b_j \in \mathbb{Z}_4$ such that $\sum_{i=1}^{k_1} a_i c_{1i} + u\sum_{j=1}^{k_2} b_j c_{2j} = 0$. Then $\sum_{i=1}^{k_1} a_i c_{1i} = 0$ and $\sum_{j=1}^{k_2} b_j c_{2j} = 0$. Since the elements $c_{11}, c_{12}, \ldots, c_{1k_1}$ are independent and so are the elements $c_{21}, c_{22}, \ldots, c_{2k_2}$, therefore $a_i = 0$ and $b_j = 0$ for all i and j. Hence $\mathcal{C}$ is a $\mathbb{Z}_4$-free module. ■

The converse of above theorem is not true in general, i.e., if a cyclic code $\mathcal{C} = C_1 + uC_2$ is a free $\mathbb{Z}_4$-module of length n over R, then C_1 or C_2 may not be a free code of length n over $\mathbb{Z}_4$ (see example 5.6.3). However, if $\mathcal{C}$ is an R-free module (code) of length n over R then C_1 must be a free code of length n over $\mathbb{Z}_4$ (see Theorem 5.6.9).

Example 5.6.2. *The polynomial $x^7 - 1$ factorizes into irreducible polynomials over $\mathbb{F}_2$ as $x^7-1 = (x-1)(x^3+x+1)(x^3+x^2+1)$. The Hensel lifts of x^3+x+1 and x^3+x^2+1 to $\mathbb{Z}_4$ are x^3+2x^2+x-1 and x^3-x^2-2x-1, respectively. Therefore x^3+2x^2+x-1 and x^3-x^2-2x-1 are divisors of x^7-1 over $\mathbb{Z}_4$. Define $\mathcal{C} = \langle x^3+2x^2+x-1\rangle + u\langle x^3-x^2-2x-1\rangle$. Then $\mathcal{C}$ is a cyclic code of length 7 over R, which is also a free $\mathbb{Z}_4$-module.*

Example 5.6.3. *Let $\mathcal{C} = C_1 + uC_2$ be a cyclic code of length 5 over R generated by $g(x) = 1 + u + 2x + ux^2$. We can see that $\mathcal{C}$ is $\mathbb{Z}_4$-free module over R. But the cyclic code C_1 of length 5 over $\mathbb{Z}_4$ generated by $g(x) \pmod{u} = 1 + 2x$ which is not a $\mathbb{Z}_4$-free, as $(1+2x) \nmid x^n - 1$.*

Theorem 5.6.4. *Let $\mathcal{C}$ be a principally generated cyclic code of length n over R generated by $g(x) \in R[x]$. If $g(x) \mid x^n - 1$, then $\mathcal{C}$ is R-free.*

Proof. Suppose that $g(x) \mid x^n - 1$ and $x^n - 1 = g(x)h(x)$. Since $x^n - 1$ is a regular polynomial, $g(x)$ and $h(x)$ must also be regular polynomials. By Theorem 2.3.8, there exist monic polynomials $g'(x), h'(x)$ such that $g(x) = v_1(x)g'(x)$ and $h(x) = v_2(x)h'(x)$ and $\overline{g}(x) = \overline{g'}(x)$ and $\overline{h}(x) = \overline{h'}(x)$, where $v_1(x), v_2(x) \in R[x]$ are units. Therefore, $x^n - 1 = g(x)h(x) = v_1(x)v_2(x)g'(x)h'(x)$. Since $x^n - 1, g'(x)$ and $h'(x)$ are all monic, we must have $v_1(x)v_2(x) = 1$ and $x^n - 1 = g'(x)h'(x)$. Let deg $g'(x) = n - k$. Then deg $h'(x) = k$. We have $\mathcal{C} = \langle g(x)\rangle = \langle v_1(x)g'(x)\rangle = \langle g'(x)\rangle$, as $v_1(x)$ is a unit. Obviously the set $S = \{g'(x), xg'(x), \ldots, x^{k-1}g'(x)\}$ spans $\mathcal{C}$.

Now suppose $a(x)g'(x) = 0 \pmod{x^n - 1}$ for some $a(x) \in R[x]$ with deg $a(x) < k$. Then $x^n - 1 \mid a(x)g'(x)$, which implies that $\frac{x^n-1}{g'(x)} \mid a(x)$, i.e., $h'(x) \mid a(x)$. Since $h'(x)$ is monic polynomial of degree k, it cannot divide a non-zero polynomial of degree less than k. It follows that $a(x) = 0$. So the set S is linearly independent and thus forms a basis for $\mathcal{C}$. Hence $\mathcal{C}$ is an R-free code. ■

We have following converse of Theorem 5.6.4.

Theorem 5.6.5. *Let $\mathcal{C}$ be a principally generated cyclic code of length n over R generated by $g(x) \in R[x]$. If $\mathcal{C}$ is R-free, then there exists a monic generator $g'(x)$ of $\mathcal{C}$ such that $g'(x) \mid x^n - 1$.*

Proof. Suppose that $\mathcal{C}$ is an R-free code. Since $g(x)$ generates an R-free code, $g(x)$ must be a regular polynomial. Therefore there exist a monic polynomial $g'(x) \in R[x]$ such that $g(x) = v(x)g'(x)$ and $\overline{g}(x) = \overline{g'}(x)$, where $v(x)$ is a unit in $R[x]$. Let the free rank of $\mathcal{C}$ be s and $S = \{c_1, c_2, \ldots, c_s\}$ an R-basis of $\mathcal{C}$. Then the set $\{\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_s\}$ forms a basis for the cyclic code $\overline{\mathcal{C}}$ over the finite field $\overline{R}$. Since $\mathcal{C} = \langle g(x)\rangle$, so $\overline{\mathcal{C}} = \langle \overline{g}(x)\rangle = \langle \overline{g'}(x)\rangle$. Since $\overline{g'}(x)$ is monic, therefore it is the generator polynomial of $\overline{\mathcal{C}}$. Let deg $\overline{g'}(x) = n - k$. Then the set $\{\overline{g'}(x), x\overline{g'}(x), \ldots, x^{k-1}\overline{g'}(x)\}$ forms a basis for $\overline{\mathcal{C}}$. So we must have $s = k$.

Now $\mathcal{C} = \langle g(x)\rangle = \langle g'(x)\rangle$. Clearly, the elements $g'(x), xg'(x), x^2g'(x), \ldots x^{k-1}g'(x)$ span $\mathcal{C}$. Also, the elements $\{g'(x), xg'(x), \ldots, x^{k-1}g'(x)\}$ are linearly independent over

R; for if they are not, then they give a dependence relation among the elements $\overline{g'}(x), x\overline{g'}(x), \ldots, x^{k-1}\overline{g'}(x)$, a contradiction. Now since $x^k g'(x)$ is a codeword, we can write $x^k g'(x)$ as a linear combination of the elements $x^i g'(x), i = 0, 1, \ldots, k-1$. Let $x^k g'(x) = \sum_{i=0}^{k-1} a_i x^i g'(x)$, which can be written as $\sum_{i=0}^{k} a_i x^i g'(x) = 0$ with $a_k = -1$, or $a(x)g'(x) = 0$. Then $x^n - 1 \mid a(x)g'(x)$ and since $a(x)g'(x)$ is a monic polynomial of degree n, we must have $x^n - 1 = a(x)g'(x)$. Therefore, $g'(x) \mid x^n - 1$. ■

The following result follows from Theorems 5.6.4 and 5.6.5.

Proposition 5.6.6. *Let $\mathcal{C}$ be a principally generated cyclic code of length over R. Then $\mathcal{C}$ is free if and only if there exists a monic generator $g(x)$ in $\mathcal{C}$ such that $g(x) \mid x^n - 1$. Furthermore, $\mathcal{C}$ has free rank $n - \deg\, g(x)$ and the elements $g(x)$, $xg(x)$, $\ldots$, $x^{n-\deg\, g(x)-1}g(x)$ form a basis for $\mathcal{C}$.*

Example 5.6.7. *Consider the cyclic code $\mathcal{C}$ of length 7 over R generated by the polynomial $g(x) = x^3 + 2x^2 + x - 1$. $g(x)$ is the Hensel lift of $x^3 + x + 1 \in \mathbb{F}_2[x]$ to R. The cyclic code $\mathcal{C} = \langle g(x) \rangle$ is an R-free cyclic code of length 7 and free rank 4.*

Theorem 5.6.8. *Let $\mathcal{C} = \langle A_1(x),\ A_2(x),\ A_3(x),\ A_4(x) \rangle$ be a cyclic code of length n over R. Then $\mathcal{C} = \langle A_1(x) \rangle$ if and only if $f_1(x) = f_4(x)$.*

Proof. Suppose $f_1(x) = f_4(x)$. Then from relation (5.4.1) of Theorem 5.4.8, we get that $f_1(x) = f_2(x) = f_3(x) = f_4(x)$. Since deg $f_{12}(x)$, deg $f_{34}(x) <$ deg $f_1(x)$, from relation (5.4.7) of Theorem 5.4.8, we get that $f_4(x) \mid (f_{12}(x) - f_{34}(x))$. So $f_{12}(x) = f_{34}(x)$. Therefore $A_3(x) = uf_3(x) + 2uf_{34}(x) = uf_1(x) + 2uf_{12}(x) = uA_1(x)$.

Again since deg $f_{13}(x)$, deg $f_{24}(x) <$ deg $f_1(x)$, so from relations (5.4.4) and (5.4.8) of Theorem 5.4.8 we get that $f_{23}(x) = 0$ and $f_{13}(x) = f_{24}(x)$, respectively. Therefore $A_2(x) = 2f_2(x) + uf_{23}(x) + 2uf_{24}(x) = 2f_1(x) + 2uf_{13}(x) = 2A_1(x)$. Hence $\mathcal{C} = \langle A_1(x) \rangle$. The converse is easy to prove. ■

In the above theorem the cyclic code $\mathcal{C} = \langle A_1(x) \rangle$ is principally generated, however $\mathcal{C}$ may not be a free code. For example, consider the cyclic code $\mathcal{C} = \langle x + 1 \rangle$ of length 3 over R. Since $x + 1 \nmid x^3 - 1$ in R_n, $\mathcal{C}$ is not free.

Theorem 5.6.9. *If $\mathcal{C} = C_1 + uC_2$ is a free cyclic code over R, then so is C_1 over $\mathbb{Z}_4$.*

Proof. From Proposition 5.6.6, if $\mathcal{C}$ is a free cyclic code over R with generator polynomial $g(x)$, then $x^n - 1 = g(x)h(x)$. If we can express $g(x) = g'(x) + ug''(x)$ and $h(x) = h'(x) + uh''(x)$, where $g'(x), g''(x), h'(x), h''(x) \in \mathbb{Z}_4[x]$. Then $x^n - 1 = g'(x)h'(x) \pmod{u}$. The result follows. ■

Example 5.6.10. *Consider again the cyclic code $\mathcal{C}$ of length 7 generated by $g(x) = x^3 + 2x^2 + x - 1$. Then $\mathcal{C}$ is free over R as $x^3 + 2x^2 + x - 1$ is a divisor of $x^7 - 1$ over R. Since $x^3 + 2x^2 + x - 1$ is a divisor of $x^7 - 1$ over $\mathbb{Z}_4$ as well, C_1 is a free cyclic code of length 7 over $\mathbb{Z}_4$.*

5.7 Examples

Example 5.7.1. *Consider cyclic codes of length 2 over R. We have $(x - 1)^2 = 2(x - 1)$. All cyclic codes of length 2 over R and their minimum Hamming distances are given in Table 5.1.*

Example 5.7.2. *Consider cyclic codes of length* 7 *over* R. *We have*

$$x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1) \text{ over } \mathbb{F}_2.$$

This factors are irreducible polynomials over $\mathbb{F}_2$. *The Hensel lifts of irreducible factors are* $g_1 = x-1$, $g_2 = x^3+2x^2+x-1$ *and* $g_3 = x^3-x^2-2x-1$, *respectively. The cyclic codes of length* 7 *over* R *are given in Table 5.2.*

5.8 Conclusion

In this chapter, we have studied some structural properties of cyclic codes of length n over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. First we have considered cyclic codes of odd lengths over R and obtained their structure through the factorization of $x^n - 1$, n odd integer, over R. Next, the general form of the generators of cyclic codes of arbitrary lengths over R is provided and a formula for their ranks is determined. We have obtained a necessary condition and a sufficient condition for such codes to be free R-modules. We have obtained the complete ideal structure of $\frac{R[x]}{\langle x^{2^k}-1\rangle}$. Some examples are presented.

Table 5.1: Complete ideal structure of R_2.

Ideals	$d_H(I)$
$\langle 0\rangle$	0
$\langle 1\rangle$	1
$\langle 2u\rangle$	1
$\langle 2u(x-1)\rangle$	2
$\langle u\rangle$	1
$\langle u(x-1)\rangle$	2
$\langle 2\rangle$	1
$\langle 2(x-1)\rangle$	2
$\langle (x-1)\rangle$	2
$\langle (x-1)+u\rangle$	2
$\langle (x-1)+2u\rangle$	2
$\langle (x-1)+2\rangle$	2
$\langle (x-1)+2+u\rangle$	2
$\langle (x-1)+2+2u\rangle$	2
$\langle (x-1)+u+2u\rangle$	2
$\langle (x-1)+2+u+2u\rangle$	2
$\langle u(x-1)+2\rangle$	2
$\langle u(x-1)+2u\rangle$	2
$\langle 2(x-1)+u\rangle$	2
$\langle 2(x-1)+2u\rangle$	2
$\langle 2(x-1)+u(x-1)\rangle$	2
$\langle (x-1),\quad u\rangle$	1
$\langle (x-1),\quad 2u\rangle$	1
$\langle (x-1)+2,\quad u\rangle$	1
$\langle (x-1)+u,\quad 2\rangle$	1
$\langle 2(x-1),\quad u\rangle$	1
$\langle 2(x-1),\quad 2u\rangle$	1
$\langle u(x-1),\quad 2\rangle$	1
$\langle u(x-1),\quad 2u\rangle$	1
$\langle 2,\quad u\rangle$	1
$\langle x-1,\quad 2,\quad u\rangle$	1
$\langle (x-1)+2+u,\quad 2u\rangle$	1

Table 5.2: Non-zero cyclic codes of length 7 over $\mathbb{Z}_4 + u\mathbb{Z}_4$.

Non-zero generator polynomials	**rank**
$\langle 2g_ig_j, \quad ug_1g_2 + 2ug_1\rangle, \qquad i \neq j = 1,2,3$	3
$\langle 2g_ig_j, \quad ug_1g_2 + 2ug_2\rangle, \qquad i \neq j = 1,2,3$	3
$\langle 2g_ig_j, \quad ug_1g_2 + 2u\rangle, \qquad i \neq j = 1,2,3$	3
$\langle 2g_ig_j, \quad ug_1g_3 + 2ug_1\rangle, \qquad i \neq j = 1,2,3$	3
$\langle 2g_ig_j, \quad ug_1g_3 + 2ug_3\rangle, \qquad i \neq j = 1,2,3$	3
$\langle 2g_ig_j, \quad ug_1g_3 + 2u\rangle, \qquad i \neq j = 1,2,3$	3
$\langle 2g_ig_j, \quad ug_2g_3 + 2ug_2\rangle, \qquad i \neq j = 1,2,3$	1
$\langle 2g_ig_j, \quad ug_2g_3 + 2ug_3\rangle, \qquad i \neq j = 1,2,3$	1
$\langle 2g_ig_j, \quad ug_2g_3 + 2u\rangle, \qquad i \neq j = 1,2,3$	1
$\langle 2g_ig_j, \quad ug_1 + 2u\rangle, \qquad i \neq j = 1,2,3$	6
$\langle 2g_ig_j, \quad ug_2 + 2u\rangle, \qquad i \neq j = 1,2,3$	4
$\langle 2g_ig_j, \quad ug_3 + 2u\rangle, \qquad i \neq j = 1,2,3$	4
$\langle 2g_ig_j, \quad 3u\rangle, \qquad i \neq j = 1,2,3$	7
$\langle 2g_i, \quad ug_1g_2 + 2ug_1\rangle, \qquad i = 1,2,3$	3
$\langle 2g_i, \quad ug_1g_2 + 2ug_2\rangle, \qquad i = 1,2,3$	3
$\langle 2g_i, \quad ug_1g_2 + 2u\rangle, \qquad i = 1,2,3$	3
$\langle 2g_i, \quad ug_1g_3 + 2ug_1\rangle, \qquad i = 1,2,3$	3
$\langle 2g_i, \quad ug_1g_3 + 2ug_3\rangle, \qquad i = 1,2,3$	3
$\langle 2g_i, \quad ug_1g_3 + 2u\rangle, \qquad i = 1,2,3$	3
$\langle 2g_i, \quad ug_2g_3 + 2ug_2\rangle, \qquad i = 1,2,3$	1
$\langle 2g_i, \quad ug_2g_3 + 2ug_3\rangle, \qquad i = 1,2,3$	1
$\langle 2g_i, \quad ug_2g_3 + 2u\rangle, \qquad i = 1,2,3$	1
$\langle 2g_i, \quad ug_1 + 2u\rangle, \qquad i = 1,2,3$	6
$\langle 2g_i, \quad ug_2 + 2u\rangle, \qquad i = 1,2,3$	4
$\langle 2g_i, \quad ug_3 + 2u\rangle, \qquad i = 1,2,3$	4
$\langle 2g_i, \quad 3u\rangle, \qquad i = 1,2,3$	7
$\langle 2, \quad ug_1g_2 + 2ug_1\rangle$	3
$\langle 2, \quad ug_1g_2 + 2ug_2\rangle$	3
$\langle 2, \quad ug_1g_2 + 2u\rangle$	3
$\langle 2, \quad ug_1g_3 + 2ug_1\rangle$	3
$\langle 2, \quad ug_1g_3 + 2ug_3\rangle$	3
$\langle 2, \quad ug_1g_3 + 2u\rangle$	3
$\langle 2, \quad ug_2g_3 + 2ug_2\rangle$	1
$\langle 2, \quad ug_2g_3 + 2ug_3\rangle$	1
$\langle 2, \quad ug_2g_3 + 2u\rangle$	1

Non-zero generator polynomials	rank
$\langle 2, \quad ug_1 + 2u \rangle$	6
$\langle 2, \quad ug_2 + 2u \rangle$	4
$\langle 2, \quad ug_3 + 2u \rangle$	4
$\langle 2, \quad 3u \rangle$	7
$\langle g_1g_2 + 2g_1, \quad ug_1 + 2u \rangle$	6
$\langle g_1g_2 + 2g_1, \quad ug_2 + 2u \rangle$	4
$\langle g_1g_2 + 2g_1, \quad 3u \rangle$	7
$\langle g_1g_2 + 2g_2, \quad ug_1 + 2u \rangle$	6
$\langle g_1g_2 + 2g_2, \quad ug_2 + 2u \rangle$	4
$\langle g_1g_2 + 2g_2, \quad 3u \rangle$	7
$\langle g_1g_2 + 2, \quad ug_1 + 2u \rangle$	6
$\langle g_1g_2 + 2, \quad ug_2 + 2u \rangle$	4
$\langle g_1g_2 + 2, \quad 3u \rangle$	7
$\langle g_1g_3 + 2g_1, \quad ug_1 + 2u \rangle$	6
$\langle g_1g_3 + 2g_1, \quad ug_3 + 2u \rangle$	4
$\langle g_1g_3 + 2g_1, \quad 3u \rangle$	7
$\langle g_1g_3 + 2g_3, \quad ug_1 + 2u \rangle$	6
$\langle g_1g_3 + 2g_3, \quad ug_3 + 2u \rangle$	4
$\langle g_1g_3 + 2g_3, \quad 3u \rangle$	7
$\langle g_1g_3 + 2, \quad ug_1 + 2u \rangle$	6
$\langle g_1g_3 + 2, \quad ug_3 + 2u \rangle$	4
$\langle g_1g_3 + 2, \quad 3u \rangle$	7
$\langle g_2g_3 + 2g_2, \quad ug_2 + 2u \rangle$	4
$\langle g_2g_3 + 2g_2, \quad ug_3 + 2u \rangle$	4
$\langle g_2g_3 + 2g_2, \quad 3u \rangle$	7
$\langle g_2g_3 + 2g_3, \quad ug_2 + 2u \rangle$	4
$\langle g_2g_3 + 2g_3, \quad ug_3 + 2u \rangle$	4
$\langle g_2g_3 + 2g_3, \quad 3u \rangle$	7
$\langle g_2g_3 + 2, \quad ug_2 + 2u \rangle$	4
$\langle g_2g_3 + 2, \quad ug_3 + 2u \rangle$	4
$\langle g_2g_3 + 2, \quad 3u \rangle$	7
$\langle g_1 + 2, \quad 3u \rangle$	7
$\langle g_2 + 2, \quad 3u \rangle$	7
$\langle g_3 + 2, \quad 3u \rangle$	7

Chapter 6

Negacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$

6.1 Introduction

Negacyclic codes are a generalization of cyclic codes and were first studied by Berlekamp [15]. There is a lot of literature available on negacyclic codes. In this chapter, we consider negacyclic codes over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. In Chapter 5, we have studied cyclic codes over R. When the code length n is odd, there exists an isomorphism between cyclic codes and negacyclic codes of length n (See Theorem 6.2.3). However, the same is not the case when n is even. So we mainly focus on negacyclic codes of even lengths, in particular of length 2^k, in this chapter. We have seen in Chapter 5, Theorem 5.4.10 that for $n = 2^k$, the ring $\frac{R[x]}{\langle x^n - 1\rangle}$ is a local ring with the unique maximal ideal M with three generators 2, u and $x-1$, i.e., $M = \langle 2,\ u,\ x-1\rangle$. The presence of three generators makes the characterization of cyclic codes of length n over R complicated (Theorem 5.4.13). However, the ring $\frac{R[x]}{\langle x^n+1\rangle}$, which is also a local ring, has the unique maximal ideal with two generators only (See Theorem 6.3.1). This motivated us to study negacyclic codes of length 2^k over R. We also study negacyclic codes of arbitrary even length in this chapter.

Throughout this chapter R denotes the ring $\mathbb{Z}_4 + uZ_4$, $u^2 = 0$. Recall that an element $a + ub \in R$ is a unit if and only if a is unit in $\mathbb{Z}_4$.

6.2 Negacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$

Let λ be a unit in R and n a positive integer. A linear code $\mathcal{C}$ of length n over R is said to be a *λ-constacyclic code* if $\mathcal{C}$ is invariant under λ-constacyclic shits, i.e., if $(c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$, then $(\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}$. If $\lambda = -1$, then $\mathcal{C}$ is called a *negacyclic code.* For $\lambda = 1$ constacyclic codes coincide with cyclic codes.

In the polynomial representation of elements of R_n, a λ-constacyclic code of length n over R is an ideal of $\frac{R[x]}{\langle x^n - \lambda \rangle}$. In particular, a negacyclic code is an ideal of $\frac{R[x]}{\langle x^n + 1 \rangle}$.

Theorem 6.2.1. *If $\mathcal{C} = C_1 + uC_2$ is a λ-constacyclic code of length n over R, then C_1 is either a cyclic code or a negacyclic code of length n over $\mathbb{Z}_4$.*

Proof. Let T_λ be the λ-constacylic shift operator on R^n and $\mathcal{C}$ a λ-constacyclic code of length n over R. Let $(a_0, a_1, \dots, a_{n-1}) \in C_1$, $(b_0, b_1, \dots, b_{n-1}) \in C_2$. Then the corresponding element of $\mathcal{C}$ is $c = (c_0, c_1, \dots, c_{n-1}) = (a_0, a_1, \dots, a_{n-1}) + u(b_0, b_1, \dots, b_{n-1}) = (a_0 + ub_0, a_1 + ub_1, \dots, a_{n-1} + ub_{n-1})$. Since $\mathcal{C}$ is a λ-constacyclic code, so $T_\lambda(c) = (\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}$. Let $\lambda = \alpha + u\beta$, where $\alpha, \beta \in \mathbb{Z}_4$. Then $T_\lambda(c) = (\alpha a_{n-1}, a_0, \dots, a_{n-2}) + u((\alpha b_{n-1} + \beta a_{n-1}), b_0, \dots, b_{n-2}) \in \mathcal{C}$. This implies that $(\alpha a_{n-1}, a_0, \dots, a_{n-2}) \in C_1$. Therefore C_1 is a α-constacyclic code over $\mathbb{Z}_4$. Since the units of $\mathbb{Z}_4$ are 1 and -1, so $\alpha = \pm 1$. Hence the result. ■

Corollary 6.2.2. *If $\mathcal{C}$ is a negacyclic code of length n over R, then both C_1 and C_2 are negacylic codes over $\mathbb{Z}_4$.*

Proof. Since $\lambda = -1$, so $\alpha = -1$, $\beta = 0$. Then we get $T_\lambda(c) = (-a_{n-1}, a_0, \dots, a_{n-2}) + u(-b_{n-1}, b_0, \dots, b_{n-2})$ for some $c \in \mathcal{C}$, from which follows that C_1 and C_2 are negacyclic. ■

6.2.1 Negacyclic codes of odd lengths over $\mathbb{Z}_4 + u\mathbb{Z}_4$

For the rest of this section, we assume that n is odd. Define $\Theta : \frac{R[x]}{\langle x^n - 1 \rangle} \to \frac{R[x]}{\langle x^n + 1 \rangle}$ such that $\Theta(f(x)) = f(-x)$. It was shown in [45, Theorem 5.1] that the map Θ is a ring isomorphism when R is a finite chain ring. The result can be immediately generalized to finite local rings. Therefore I is an ideal of $\frac{R[x]}{\langle x^n - 1 \rangle}$ if and only if $J = \Theta(I)$ is an ideal of $\frac{R[x]}{\langle x^n + 1 \rangle}$.

Theorem 6.2.3. *$\mathcal{C}$ is a cyclic code of length n over R if and only if $\Theta(\mathcal{C})$ is a negacyclic code over R.*

Proof. Let τ and τ' be cyclic and negacyclic shifts, respectively. Then the result follows from the fact that $\Theta \circ \tau = \tau' \circ \Theta$. ■

The following results (Theorem 6.2.4 through Theorem 6.2.13) are discussed for cyclic codes over R in Chapter 5, and are straightforward generalizations thereof via the isomorphism Θ defined above. So we present them here without proofs.

Theorem 6.2.4. *The ring $R_n = \frac{R[x]}{\langle x^n+1\rangle}$ is not a principal ideal ring.*

Since n is odd, $x^n + 1$ factors uniquely into pairwise coprime irreducible polynomials over R. Let $x^n + 1 = f_1(x)f_2(x)\cdots f_m(x)$. Then it follows from the Chinese Remainder Theorem that

$$\frac{R[x]}{\langle x^n+1\rangle} = \oplus_{i=1}^{m} \frac{R[x]}{\langle f_i(x)\rangle}\ .$$

Any ideal I of $\frac{R[x]}{\langle x^n+1\rangle}$ can be expressed as

$$I = \oplus_{i=1}^{m} I_i,$$

where I_i is an ideal of the ring $\frac{R[x]}{\langle f_i(x)\rangle}$, $i = 1, 2, \ldots, m$. Therefore a negacyclic code of length n over R is a sum of the ideals listed in Chapter 5, Theorem 5.3.5.

Theorem 6.2.5. *The number of negacyclic codes of length n over R is 7^m, where m is the number of distinct basic irreducible factors of $x^n + 1$.*

The following result gives a sufficient condition for a negacyclic code $\mathcal{C}$ over R to be a free $\mathbb{Z}_4$-code

Theorem 6.2.6. *Let $\mathcal{C} = C_1 + uC_2$ be a negacyclic code of length n over R. If C_1, C_2 are free codes over $\mathbb{Z}_4$, then $\mathcal{C}$ is a free $\mathbb{Z}_4$-module.*

The converse of the above theorem is in general not true, i.e., if a negacyclic code $\mathcal{C} = C_1 + uC_2$ is a free $\mathbb{Z}_4$-module of length n over R, then C_1 or C_2 may not be a free code over $\mathbb{Z}_4$, it is demonstrated by Example 6.2.8.

Example 6.2.7. *The polynomial $x^{15} - 1$ factorizes into irreducible polynomials over $\mathbb{F}_2$ as $x^{15} - 1 = (x-1)(x^4 + x^3 + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$. The Hensel lifts of $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$ and $x^2 + x + 1$ to $\mathbb{Z}_4$ are $x^4 - x^3 + 2x^2 + 1$, $x^4 + 2x^2 - x + 1$, $x^4 + x^3 + x^2 + x + 1$ and $x^2 + x + 1$, respectively. Therefore $x^{15} - 1 = (x-1)(x^4 - x^3 + 2x^2 + 1)(x^4 + 2x^2 - x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$. Replacing x by $-x$, we get $x^{15} + 1 = (x+1)(x^4 + x^3 + 2x^2 + 1)(x^4 + 2x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)(x^2 - x + 1)$. Define $\mathcal{C} = \langle x^4 - x^3 + x^2 - x + 1\rangle + u\,\langle x^4 + 2x^2 + x + 1\rangle$. Then $\mathcal{C}$ is a negacyclic code of length 15 over R, which is also a free $\mathbb{Z}_4$-module.*

Example 6.2.8. *Let $\mathcal{C} = C_1 + uC_2$ be a free $\mathbb{Z}_4$-negacyclic code of length 7 over R generated by $g(x) = 2x^2 + u(x^3 + x + 1)$. Then C_1 is a negacyclic code of length 7 over $\mathbb{Z}_4$ generated by $g(x)$ $(mod\ u) = g_1(x) = 2x^2$. Since $g_1(x) \nmid x^7 + 1$, so C_1 is not $\mathbb{Z}_4$-free.*

From Theorem 5.4.9, the general form of a negacyclic code $\mathcal{C}$ of length n over R is $\mathcal{C} = \langle g(x) + up(x),\ ua(x)\rangle$, where $g(x)$, $p(x)$, $a(x) \in \mathbb{Z}_4[x]$.

Theorem 6.2.9 through Theorem 6.2.13 below are the generalizations of corresponding theorems in Chapter 5 to negacyclic codes of odd lengths over R.

Theorem 6.2.9. *Let $\mathcal{C} = \langle g(x) + up(x),\ ua(x)\rangle$ be a negacyclic code of length n over R with deg $g(x) = k_1$ and deg $a(x) = k_2$, respectively. Then $\mathcal{C}$ has rank $n - k_2$ and a minimal spanning set $B = \{(g(x) + up(x)),\ x(g(x) + up(x)),\ x^2(g(x) + up(x)), \cdots,\ x^{n-k_1-1}(g(x) + up(x)),\ \ ua(x),\ xua(x), x^2ua(x), \cdots, x^{k_1-k_2-1}ua(x)\}$.*

Example 6.2.10. *Consider the negacyclic code $\mathcal{C}$ of length 7 over R generated by the polynomials $g(x) = x^3 + (2+u)x^2 + (1+u)x + (1+u)$ and $a(x) = x + 1$. Then the rank of $\mathcal{C}$ is 6 and a minimal spanning set of $\mathcal{C}$ is $\{g(x), xg(x), x^2g(x), x^3g(x),\ ua(x), uxa(x)\}$.*

Theorem 6.2.11. *Let $\mathcal{C}$ be a principally generated negacyclic code of length n over R. Then $\mathcal{C}$ is free if and only if there exists a monic generator $g(x)$ in $\mathcal{C}$ such that $g(x) \mid x^n + 1$. Furthermore, $\mathcal{C}$ has free rank $n -$ deg $g(x)$ and the elements $g(x)$, $xg(x)$, $\cdots$, $x^{n-deg\ g(x)-1}g(x)$ form a basis for $\mathcal{C}$.*

Example 6.2.12. *Consider the negacyclic code $\mathcal{C}$ of length 15 over R generated by the polynomial $g(x) = x^4 + 2x^2 + x + 1$, where $g(x)$ is the Hensel lift of $x^4 + x + 1 \in \mathbb{F}_2[x]$ to*

R and $g(x) \mid x^{15} + 1$. The negacyclic code $\mathcal{C} = \langle g(x) \rangle$ is an R-free negacyclic code of length 15 and the free rank 11.

Theorem 6.2.13. *If $\mathcal{C} = C_1 + uC_2$ is a free negacyclic code of length n over R, then so is C_1 over $\mathbb{Z}_4$.*

Example 6.2.14. *Consider again the negacyclic code $\mathcal{C}$ of length 15 generated by $g(x) = x^4 + 2x^2 + x + 1$. Then $\mathcal{C}$ is free over R, as $x^4 + 2x^2 + x + 1$ is a divisor of $x^{15} + 1$ over R. Since $x^4 + 2x^2 + x + 1$ is a divisor of $x^{15} + 1$ over $\mathbb{Z}_4$ as well, C_1 is a free negacyclic code of length 15 over $\mathbb{Z}_4$.*

6.3 Negacyclic codes of length 2^k over $\mathbb{Z}_4 + u\mathbb{Z}_4$

So far we considered negacyclic codes with the assumption that the code length n is coprime to the characteristic of the ring R, i.e, $(n, 4) = 1$. Now we extend our study to negacyclic codes of length $n = 2^k$, $k \geq 1$. Then $(n, 4) \neq 1$. Negacyclic codes whose lengths are not relatively prime to characteristic of R are known as repeated root negacyclic codes.

Now we study negacyclic codes of length 2^k, $k \geq 1$. For the rest of this section $n = 2^k$, $k \geq 1$. Let $R'_n = \frac{\mathbb{Z}_4[x]}{\langle x^n+1 \rangle}$ and $R''_n = \frac{\mathbb{Z}_2[x]}{\langle x^n+1 \rangle}$.

Theorem 6.3.1. *The ring $R_n = \frac{R[x]}{\langle x^n+1 \rangle}$ is a local ring.*

Proof. Define the map $\Phi : R_n \rightarrow \frac{\mathbb{Z}_4[x]}{\langle x^n+1 \rangle}$ such that $\Phi(f(x)) = f_1(x) \pmod{u}$, where $f(x) = f_1(x) + uf_2(x)$. It is easy to verify that Φ is a surjective ring homomorphism. We have from Theorem 2.3.34 that the ring $\frac{\mathbb{Z}_4[x]}{\langle x^n+1 \rangle}$ is a local ring with the unique maximal ideal $\langle x+1 \rangle$. The inverse image of $\langle x+1 \rangle$ is $\Phi^{-1}(\langle x+1 \rangle) = \langle u, x+1 \rangle$. Suppose that y be a non-unit in R_n such that $y \notin \langle u, x+1 \rangle$. Since y is a non-unit in R_n, $\Phi(y)$ is a non-unit in R'_n. It follows that $\Phi(y) \in \langle x+1 \rangle$, as $\langle x+1 \rangle$ is the maximal ideal of R'_n. This in turn implies that $y \in \langle u, x+1 \rangle$, a contradiction. Therefore $\langle u, x+1 \rangle$ contains all non-units of R_n. Thus it is the unique maximal ideal of R_n and hence R_n is local. ∎

Now onward, we prefer to express a polynomial in terms of $x + 1$, rather than in x, to make the computations easier in R_n. Each polynomial in R_n can uniquely be written as

$\sum_{j=0}^{n-1} f_j(x+1)^j$, $f_j \in R$, and such a polynomial will be denoted in the rest of this chapter by $f(x)$.

Lemma 6.3.2. *In R_n, $(x+1)^n = 2x^{\frac{n}{2}}$ and $(x+1)$ is nilpotent with nilpotency $2n$.*

Proof. It can easily be seen by induction on n that $(x+1)^n = x^n + 1 + 2x^{\frac{n}{2}}$. Since $x^n = -1$ in R_n, $(x+1)^n = 2x^{\frac{n}{2}}$. It follows that $(x+1)^{2n} = 0$. There is no l, $0 \leq l \leq n-1$ such that $(x+1)^l = 0$ in R_n. Now suppose $(x+1)^l = 0$ for some $n \leq l \leq 2n-1$. Then $(x+1)^l = (x+1)^n(x+1)^{l-n} = 2x^{\frac{n}{2}}(x+1)^{l-n} = 0$. Since $x^{\frac{n}{2}}$ is a unit in R_n, $2(x+1)^{l-n} = 0$. But $2(x+1)^{l'} \neq 0$ for any $0 \leq l' \leq n-1$ in R_n. So no such l exists. Hence $2n$ is the nilpotency of $x+1$. ■

Lemma 6.3.3. *An element $f(x) = \sum_{j=0}^{n-1} a_j(x+1)^j$ is a unit in R_n if and only if a_0 is a unit in R.*

Proof. Suppose that $f(x) = \sum_{j=0}^{n-1} a_j(x+1)^j$ is a unit in R_n and a_0 is a non-unit in R. Then $a_0 \in \langle 2, u\rangle$. It follows then that $f(x) = \sum_{j=0}^{n-1} a_j(x+1)^j \in \langle u,\ x+1\rangle$. This implies that $f(x)$ is a non-unit, a contradiction. Therefore a_0 must be a unit in R.

On the other hand, suppose that a_0 is a unit in R and $f(x) = \sum_{j=0}^{n-1} a_j(x+1)^j$ is a non-unit in R_n. Then $f(x) \in \langle u,\ x+1\rangle$, as $\langle u,\ x+1\rangle$ is the maximal ideal of R_n. Also $\sum_{j=1}^{n-1} a_j(x+1)^j \in \langle u,\ x+1\rangle$, which implies that $f(x) - \sum_{j=1}^{n-1} a_j(x+1)^j = a_0 \in \langle u,\ x+1\rangle$, a contradiction. Therefore $f(x)$ is a unit in R_n. ■

Lemma 6.3.4. *In R_n, $(x+1)^n = 2\left((x+1)^{\frac{n}{2}} + 1\right)$ and $\langle (x+1)^n \rangle = \langle 2 \rangle$.*

Proof. From Lemma 6.3.2, we have

$$\begin{aligned}
(x+1)^n &= 2x^{\frac{n}{2}} \\
&= 2\left((x+1)-1\right)^{\frac{n}{2}} \\
&= 2\left((x+1)^{\frac{n}{2}} - \binom{\frac{n}{2}}{1}(x+1)^{\frac{n}{2}-1} + \binom{\frac{n}{2}}{2}(x+1)^{\frac{n}{2}-2} + \cdots + (-1)^{\frac{n}{2}}\right).
\end{aligned}$$

It is well known that $\binom{\frac{n}{2}}{i} = 0$ or $2 \pmod 4$ for $0 < i < \frac{n}{2}$. Therefore $(x+1)^n = 2\left((x+1)^{\frac{n}{2}} + 1\right)$. Since $(x+1)^{\frac{n}{2}} + 1$ is a unit in R_n, $\langle (x+1)^n \rangle = \langle 2 \rangle$. ■

An element $f(x)$ in R_n can be written as $f(x) = f_1(x) + uf_2(x)$, where $f_i(x) \in R'_n$, $i = 1, 2$. Define $\Psi : R \to \mathbb{Z}_4$ such that $\Psi(a + bu) = a \pmod u$. It can easily be seen that Ψ is a ring homomorphism with ker $\Psi = \langle u \rangle = u\mathbb{Z}_4$. Extend Ψ to the homomorphism $\Phi : R_n \to R'_n$ such that $\Phi(a(x) + ub(x)) = a(x) \pmod u$, where $a(x), b(x) \in \mathbb{Z}_4[x]$. Let I be a non-trivial ideal of R_n. Restrict Φ to I and define $J = \{h(x) \in R'_n \,:\, uh(x) \in \ker \Phi\}$. Clearly J is an ideal of R'_n. We know from Theorem 2.3.34 that R'_n is a finite chain ring with the maximal ideal $\langle x + 1 \rangle$, so $J = \langle (x + 1)^m \rangle$ for some $0 \leq m \leq 2n - 1$. Therefore ker $\Phi = \langle u(x + 1)^m \rangle$. Similarly, the image of I under Φ, i.e., $\Phi(I)$ is an ideal of R'_n and $\Phi(I) = \langle (x + 1)^s \rangle$ for some $1 \leq s \leq 2n$. Hence $I = \langle (x + 1)^s + up(x),\ u(x + 1)^m \rangle$ for some $p(x) = \sum_{j=0}^{n-1} p_j(x + 1)^j \in \mathbb{Z}_4[x]$. Since $u(x + 1)^s = u((x + 1)^s + up(x)) \in I$ and $\Phi(u(x + 1)^s) = 0$, so $(x + 1)^m \mid (x + 1)^s$. This implies that $m \leq s$. When $m = s$, we get $u(x + 1)^m \in \langle (x + 1)^s + up(x) \rangle = I$. Therefore a non-principal ideal I of R_n has the form $I = \left\langle (x+1)^s + u\sum_{j=0}^{n-1} p_j(x + 1)^j,\ u(x + 1)^m \right\rangle$, $1 \leq s \leq 2n - 1$ and $0 \leq m \leq s - 1$. When $m < n$, $I = \left\langle (x+1)^s + u\sum_{j=0}^{n-1} p_j(x + 1)^j,\ u(x + 1)^m \right\rangle = \left\langle (x+1)^s + u\sum_{j=0}^{m-1} p_j(x + 1)^j,\ u(x + 1)^m \right\rangle$.

If t is the smallest non-negative integer such that p_t is non-zero, then a polynomial $f(x) = (x + 1)^s + u\sum_{j=0}^{n-1} p_j(x + 1)^j \in R[x]$ can be represented as $f(x) = (x + 1)^s + u(x + 1)^t h(x)$, where $h(x) \in \mathbb{Z}_4[x]$ and deg $h(x) \leq n - t - 1$. Hence I can be written as $I = \langle (x + 1)^s + u(x + 1)^t h(x),\ u(x + 1)^m \rangle$, where $1 \leq s \leq 2n - 1$, $0 \leq t < \min\{m, n\}$, $0 \leq m \leq s - 1$ and $h(x) \in \mathbb{Z}_4[x]$.

Summarizing this discussion, we present the complete ideal structure of R_n in the following theorem.

Theorem 6.3.5. *Let I be an ideal of R_n. Then I is one of the following:*

1. *Trivial ideals:*

   $\langle 0 \rangle$ *or* $\langle 1 \rangle$.

2. *Principal ideals:*

   (a) $\langle u(x + 1)^m \rangle$, $0 \leq m \leq 2n - 1$

(b) $\langle (x+1)^s + u(x+1)^t h(x)\rangle$, $1 \le s \le 2n-1$, $0 \le t \le n-1$, $h(x) \in \mathbb{Z}_4[x]$ *and deg* $h(x) \le n-t-1$.

3. *Non-principal ideals:* $\langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m\rangle$, $1 \le s \le 2n-1$, $0 \le t \le n-1$, $0 \le m \le s-1$, $h(x) \in \mathbb{Z}_4[x]$ *and deg* $h(x) \le\ min\{m,n\} - t - 1$.

The ideals described in Theorem 6.3.5 are not distinct. For instance, in R_2, the ideals $\langle (x+1)^3 + u\rangle$ and $\langle (x+1)^3 + u(1+(x+1))\rangle$ are same, as $(x+1)^3 + u(1+(x+1)) = ((x+1)^3+u)(1+(x+1))$ and $(1+(x+1))$ is a unit in R_n. Similarly, the ideals $\langle (x+1)^2+u\rangle$ and $\langle (x+1)^2+3u)\rangle$ are same. But the ideals $\langle (x+1)^2+u\rangle$ and $\langle (x+1)^2 + u(1+(x+1))\rangle$ are distinct, as $u(x+1)$ is neither in $\langle (x+1)^2+u\rangle$ nor in $\langle (x+1)^2+u(1+(x+1))\rangle$. Similarly, the ideals $\langle (x+1)^3+2u\rangle = \langle (x+1)^3 + 2u(1+(x+1))\rangle$, as $(x+1)^3 + 2u(1+(x+1)) = ((x+1)^3+2u)(1+(x+1))$ and $1+(x+1)$ is a unit. So it is required to know the smallest values of T and T_1 such that $u(x+1)^T \in \langle (x+1)^s + u(x+1)^t h(x)\rangle$ and $2u(x+1)^{T_1} \in \langle (x+1)^s + u(x+1)^t h(x)\rangle$, respectively, through which the repetition of ideals can be avoided and ideals (negacyclic codes) can be determined distinctly. For computing T, we follow a similar line of argument as in [39]. However, due the presence of zero divisors 2 and u, the results are not a straightforward generalization.

The following theorem discusses the value of T when $1 \le s \le n-1$.

Theorem 6.3.6. *Let T be the smallest non-negative integer such that $u(x+1)^T \in I = \langle (x+1)^s + u(x+1)^t h(x)\rangle$, where $1 \le s \le n-1$, $0 \le t \le n-1$ and $h(x) \in \mathbb{Z}_4[x]$. Then $T = s$.*

Proof. Let $f(x) = (x+1)^s + u(x+1)^t h(x)$, so that $I = \langle f(x)\rangle$. Then $uf(x) = u(x+1)^s \in I$. Since T is the smallest non-negative integer such that $u(x+1)^T \in I$, we get $T \le s$.

On the other hand, since $u(x+1)^T \in I$, there exists $g(x) = g_1(x) + ug_2(x) \in R_n$, where $g_1(x), g_2(x) \in R'_n$, such that $u(x+1)^T = f(x)g(x)$. This implies that

$$\begin{aligned} u(x+1)^T &= \left((x+1)^s + u(x+1)^t h(x)\right)\left(g_1(x) + ug_2(x)\right) \\ &= (x+1)^s g_1(x) + u(x+1)^s g_2(x) + u(x+1)^t h(x) g_1(x). \qquad (6.3.1) \end{aligned}$$

From equation (6.3.1), we get $(x+1)^s g_1(x) = 0$, and so $g_1(x) = (x+1)^{2n-s} l(x)$

for some $l(x) \in R'_n$. Therefore equation (6.3.1) can be rewritten as $u(x+1)^T = u(x+1)^s\,(g_2(x) + (x+1)^{2n-2s+t}h(x)l(x))$, as $s < n$ and $2n - s + t > n$. This implies that $u(x+1)^T \in \langle u(x+1)^s \rangle$. Thus $s \leq T$, and hence $T = s$. ■

In Theorem 6.3.6, the value of T does not depend on whether or not the polynomial $h(x)$ is unit in R'_n. However, the same is not the case when $n \leq s \leq 2n-1$. This is another difference between the results obtained in here and that of [39].

Theorem 6.3.7. *Let T be the smallest non-negative integer such that $u(x+1)^T \in I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $n \leq s \leq 2n-1$ and $h(x)$ is a unit in R'_n. Then $T = min\{s, 2n-s+t\}$.*

Proof. Let $f(x) = (x+1)^s + u(x+1)^t h(x)$. Then $uf(x) = u(x+1)^s \in I$ and $(x+1)^{2n-s} f(x)h(x)^{-1} = u(x+1)^{2n-s+t} \in I$. Since T is the smallest non-negative integer such that $u(x+1)^T \in I$, we have $T \leq \min\{s, 2n-s+t\}$.

On the other hand, we can write $u(x+1)^T = f(x)g(x)$ for some $g(x) = g_1(x) + ug_2(x) \in R_n$, $g_1(x), g_2(x) \in R'_n$. This implies that $u(x+1)^T = (x+1)^s g_1(x) + u(x+1)^s g_2(x) + u(x+1)^t h(x) g_1(x)$. This in turn implies that $g_1(x) = (x+1)^{2n-s} l(x)$ for some $l(x) \in R'_n$, and so $u(x+1)^T = u(x+1)^s g_2(x) + u(x+1)^{2n-s+t} h(x) l(x)$. It follows from this that $u(x+1)^T \in \left\langle u(x+1)^{\min\{s,\ 2n-s+t\}} \right\rangle$. Therefore $T \geq \min\{s,\ 2n-s+t\}$. Hence $T = \min\{s,\ 2n-s+t\}$. ■

Theorem 6.3.7 gives the value of T such that $u(x+1)^T \in I$ only when $h(x)$ is a unit in R'_n. If $h(x)$ is not a unit in R'_n, then we can have either $h(x) = 2h'(x)$ or $h(x) = 2h_1(x) + (x+1)^l h_2(x)$, where $h'(x)$, $h_1(x)$ are units in R''_n and $h_2(x)$ is a unit in R'_n. For example,

$$\begin{aligned} h(x) &= 2 + 2(x+1) + (x+1)^3 + 3(x+1)^4 + 2(x+1)^5 + (x+1)^6 + 3(x+1)^7 \\ &= 2(1 + (x+1) + (x+1)^5) + (x+1)^3(1 + 3(x+1) + (x+1)^3 + 3(x+1)^4) \\ &= 2h_1(x) + (x+1)^3 h_2(x), \end{aligned}$$

where $h_1(x)$, $h_2(x)$ are units in R''_n and R'_n, respectively.

Now we find the smallest value of T in these two cases of $h(x)$ also.

Lemma 6.3.8. *Let $I = \langle (x+1)^s + u(x+1)^t h(x)\rangle$, where $n \leq s \leq 2n-1$, $h(x)$ is a non-zero non-unit in R'_n and deg $h(x) \leq n-t-1$. Then $t < s-n$.*

Proof. Since $h(x)$ is not a unit in R'_n, either $h(x) = 2h'(x)$ or $h(x) = 2h_1(x) + (x+1)^l h_2(x)$, where $h'(x)$, $h_1(x)$ are units in R''_n and $h_2(x)$ is a unit in R'_n. We prove the two cases separately.

Case (i): Let $h(x) = 2h'(x)$. Then $I = \langle f(x)\rangle \neq \langle (x+1)^s\rangle$, where $f(x) = (x+1)^s + 2u(x+1)^t h'(x)$.

Suppose $s-n \leq t$. From Lemma 6.3.4, we have $(x+1)^n = 2x^{\frac{n}{2}} = 2(1+(1+x)^{\frac{n}{2}})$. So

$$\begin{aligned} f(x) &= 2x^{\frac{n}{2}}(x+1)^{s-n} + 2u(x+1)^t h'(x) \\ &= 2((x+1)^{\frac{n}{2}}+1)(x+1)^{s-n} + 2u(x+1)^t h'(x) \\ &= 2(x+1)^{s-n}(1+(1+x)^{\frac{n}{2}} + (x+1)^{t-s+n}h(x)'). \end{aligned}$$

From Lemma 6.3.3, $1+(1+x)^{\frac{n}{2}} + u(x+1)^{t-s+n}h(x)'$ is a unit in R_n. This implies that $I = \langle f(x)\rangle = \langle 2(x+1)^{s-n}\rangle = \langle (x+1)^s\rangle$, which is a contradiction. Therefore $t < s-n$.

Case (ii): Let $h(x) = 2h_1(x)+(x+1)^l h_2(x)$. Then $I = \langle f(x)\rangle \neq \big\langle (x+1)^s + u(x+1)^{l+t}h_2(x)\big\rangle$, where $f(x) = (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x))$.

Suppose $s-n \leq t$. Then $f(x) = 2x^{\frac{n}{2}}(x+1)^{s-n} + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x))$. This implies that $ux^{\frac{n}{2}}f(x) = 2u(x+1)^{s-n} \in I$. Now $f(x) - ux^{\frac{n}{2}}f(x)(x+1)^{t-s+n}h_1(x) = (x+1)^s + u(x+1)^{l+t}h_2(x)$. Since $1 - ux^{\frac{n}{2}}(x+1)^{t-s+n}h_1(x)$ is a unit in R_n, $I = \langle f(x)\rangle = \big\langle (x+1)^s + u(x+1)^{l+t}h_2(x)\big\rangle$, which is a contradiction. Therefore $t < s-n$. ■

Theorem 6.3.9. *Let T be the smallest non-negative integer such that $u(x+1)^T \in I = \langle (x+1)^s + 2u(x+1)^t h(x)\rangle$, where $n \leq s \leq 2n-1$ and $h(x)$ is a unit in R''_n. Then $T = min\{s,\ 3n-s+t\}$.*

Proof. Let $I = \langle f(x)\rangle$, where $f(x) = (x+1)^s + 2u(x+1)^t h(x)$. Then from Lemma 6.3.8, $t < s-n$. This implies that $2n-s+t < n$. Now $uf(x) = u(x+1)^s \in I$. Also, $(x+1)^{2n-s}f(x) = 2u(x+1)^{2n-s+t}h(x) \in I$, which implies that $x^{\frac{n}{2}}(x+1)^{2n-s}f(x)h(x)^{-1} = 2x^{\frac{n}{2}}u(x+1)^{2n-s+t} = u(x+1)^{3n-s+t} \in I$, as $(x+1)^n = 2x^{\frac{n}{2}}$. Since T is the smallest non-negative integer such that $u(x+1)^T \in I$, we have $T \leq \min\{s, 3n-s+t\}$.

For the other half, we obtain $T \geq \min\{s, 3n - s + t\}$ using the same arguments as in Theorems 6.3.6 and 6.3.7. Hence $T = \min\{s, 3n - s + t\}$. ■

Theorem 6.3.10. *Let T be the smallest non-negative integer such that $u(x+1)^T \in I = \left\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)) \right\rangle$, where $n \leq s \leq 2n-1$, $h_1(x)$, $h_2(x)$ are units in R''_n and R'_n, respectively. Then $T = min\{s, 2n - s + t + l\}$.*

Proof. The proof is similar to that of Theorem 6.3.9. ■

We summarize the value of T for different cases of $h(x)$, s, and t in the following theorem.

Theorem 6.3.11. *Let $0 \leq T \leq 2n-1$ be the smallest non-negative integer such that $u(x+1)^T \in I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $0 \leq s \leq 2n-1$, $h(x) \in \mathbb{Z}_4[x]$ and deg $h(x) \leq n - t - 1$. Then*

$$T = \begin{cases} s & \text{if } 1 \leq s \leq n-1, \\ 2n - s + t & \text{if } n \leq s \leq 2n-1,\ 0 \leq t < 2s - 2n \ \text{ and } \ h(x) \text{ is a unit in } R'_n, \\ s & \text{if } n \leq s \leq 2n-1 \ \text{ and } t \geq 2s - 2n, \ \text{ and } \ h(x) \text{ is a unit in } R'_n, \\ 3n - s + t & \text{if } n < s \leq 2n-1,\ 0 \leq t < 2s - 3n \ \text{ and } h(x) = 2h'(x), \\ s & \text{if } n < s \leq 2n-1,\ 2s - 3n \leq t < s - n \ \text{ and } h(x) = 2h'(x), \\ 2n - s + l + t & \text{if } n < s \leq 2n-1,\ 0 \leq t < s - n,\ 0 \leq l + t < 2s - 2n \\ & \quad \text{and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \\ s & \text{if } n < s \leq 2n-1,\ 0 \leq t < s - n,\ l + t \geq 2s - 2n \\ & \quad \text{and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \end{cases}$$

where $h'(x)$, $h_1(x)$ are units in R''_n and $h_2(x)$ is a unit in R'_n.

In the following theorem we present the value of T_1 for different cases of $h(x)$, s, and t.

Theorem 6.3.12. *Let $0 \leq T_1 \leq n-1$ be the smallest non-negative integer such that $2u(x+1)^{T_1} \in I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $0 \leq s \leq 2n-1$, $h(x) \in \mathbb{Z}_4[x]$ and deg*

$h(x) \leq n - t - 1$. Then

$$T_1 = \begin{cases} 0 & \text{if } 1 \leq s \leq n-1, \\ 0 & \text{if } n \leq s \leq 2n-1,\ 0 \leq t < s-n \text{ and } h(x) \text{ is a unit in } R'_n, \\ n-s+t & \text{if } n \leq s \leq 2n-1,\ s-n \leq t < 2s-2n \text{ and } h(x) \text{ is a unit in } R'_n, \\ s-n & \text{if } n \leq s \leq 2n-1,\ 2s-2n \leq t < n \text{ and } h(x) \text{ is a unit in } R'_n, \\ 2n-s+t & \text{if } n < s \leq 2n-1,\ 0 \leq t < 2s-3n \text{ and } h(x) = 2h'(x), \\ s-n & \text{if } n \leq s \leq 2n-1,\ 2s-3n \leq t < s-n \text{ and } h(x) = 2h'(x), \\ 0 & \text{if } n \leq s \leq 2n-1,\ 0 \leq t < s-n,\ 0 \leq l+t \leq s-n \\ & \quad \text{and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \\ l+t-s+n & \text{if } n < s \leq 2n-1,\ 0 \leq t < s-n,\ s-n < l+t < 2s-2n \\ & \quad \text{and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \\ s-n & \text{if } n < s \leq 2n-1,\ 0 \leq t < s-n,\ l+t \geq 2s-2n \\ & \quad \text{and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \end{cases}$$

where $h'(x)$, $h_1(x)$ are units in R''_n and $h_2(x)$ is a unit in R'_n.

Proof. We present the proof of case (i) and the remaining cases can be proved using similar arguments as in Theorems 6.3.6 and 6.3.9.

Let $f(x) = (x+1)^s + u(x+1)^t h(x)$ such that $I = \langle f(x) \rangle$, where $1 \leq s \leq n-1$. Then $u(x+1)^{n-s} f(x) = u(x+1)^n$. Since $(x+1)^n = 2x^{\frac{n}{2}}$ and $x^{\frac{n}{2}}$ is a unit R_n, we get that $u(x+1)^{n-1} x^{\frac{n}{2}} f(x) = 2u \in I$. Therefore $T_1 = 0$, as T_1 is the non-negative integer such that $2u(x+1)^{T_1} \in I$. ■

Making use of Theorems 6.3.11 and 6.3.12, we can now distinguish the ideals of R_n. The following theorem gives the distinct principal ideals.

Theorem 6.3.13. *The distinct non-trivial principal ideals of R_n are*

1. *$I = \langle u(x+1)^m \rangle$, $0 \leq m \leq 2n-1$.*

2. *$I = \langle (x+1)^s + u(x+1)^t h(x)\rangle$, where $1 \le s \le n-1$, $0 \le t \le s-1$, $h(x)$ is either zero or a unit in R_n'' and deg $h(x) \le s-t-1$.*

3. *$I = \langle (x+1)^s + u(x+1)^t h(x)\rangle$, where $n \le s \le 2n-1$, $0 \le t \le n-1$, $h(x)$ is either zero or a unit in R_n'' and deg $h(x) \le T-t-1$.*

4. *$I = \langle (x+1)^s + 2u(x+1)^t h(x)\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $h(x)$ is a unit in R_n'' and deg $h(x) \le T_1-t-1$.*

5. *$I = \big\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x))\big\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t < s-n < l+t < n$, $h_1(x)$, $h_2(x)$ are units in R_n'', deg $h_1(x) \le T_1-t-1$ and deg $h_2(x) \le n-t-l-1$.*

Proof. 1. Suppose that I contains only the multiples of u, i.e., $I = \langle uf(x)\rangle$, where $f(x) \in \mathbb{Z}_4[x]$. This implies that $\langle f(x)\rangle$ is an ideal of R_n'. So from Theorem 2.3.34 we get $I = \langle u(x+1)^m\rangle$ for some $0 \le m \le 2n-1$.

2. Let $I = \langle f(x)\rangle$, where $f(x) = (x+1)^s + u(x+1)^t g(x)$, $1 \le s \le n-1$, $0 \le t \le n-1$ and $g(x) \in \mathbb{Z}_4[x]$. If $g(x) = 0$, then $I = \langle f(x)\rangle = \langle (x+1)^s\rangle$, $1 \le s \le n-1$.

Let $g(x) = g_1(x) + 2g_2(x) \neq 0$, $g_1(x)$, $g_2(x) \in \mathbb{Z}_2[x]$. Since $1 \le s \le n-1$, we have $T_1 = 0$ from Theorem 6.3.12, i.e., $2u \in I$. This implies that $2u(x+1)^t g_2(x) \in I$. On multiplying $f(x)$ by $u(x+1)^{n-s+t} x^{\frac{n}{2}} g_2(x)$, we get

$$u(x+1)^{n-s+t} x^{\frac{n}{2}} g_2(x) f(x) = 2u(x+1)^t g_2(x), \tag{6.3.2}$$

as $(x+1)^n = 2x^{\frac{n}{2}}$. Now

$$\begin{aligned} f(x) - u(x+1)^{n-s+t} x^{\frac{n}{2}} g_2(x) f(x) &= \big((x+1)^s + u(x+1)^t g_1(x) + 2u(x+1)^t g_2(x)\big) \\ &- 2u(x+1)^t g_2(x) \quad \text{(from 6.3.2)}, \end{aligned}$$

which implies that

$$f(x)\left(1 - u(x+1)^{n-s+t} x^{\frac{n}{2}} g_2(x)\right) = (x+1)^s + u(x+1)^t g_1(x).$$

Since $1 - u(x+1)^{n-s+t}x^{\frac{n}{2}}g_2(x)$ is a unit in R_n, $\langle f(x)\rangle = \langle (x+1)^s + u(x+1)^t h(x)\rangle$, where $g_1(x) = h(x)$. When $1 \le s \le n-1$, from Theorem 6.3.11, $T = s$. Therefore $\deg h(x) \le s - t - 1$.

3. Let $I = \langle f(x)\rangle$, where $f(x) = (x+1)^s + u(x+1)^t g(x)$, $n \le s \le 2n-1$, $0 \le t \le n-1$ and $g(x)$ is either zero or a unit in R'_n. If $g(x) = 0$, then $I = \langle f(x)\rangle = \langle (x+1)^s\rangle$, $n \le s \le 2n-1$.

   Let $g(x) = g_1(x) + 2g_2(x)$, $g_1(x), g_2(x) \in \mathbb{Z}_2[x]$, be a unit in R'_n. Then $g_1(x)$ is also a unit in R''_n. We first consider the case $n \le s \le 2n-1$ and $0 \le t < s-n$. Then from Theorem 6.3.12, we have $2u \in I$. This implies that $2u(x+1)^t g_2(x) \in I$. Since $(x+1)^n = 2x^{\frac{n}{2}}$, $f(x) = 2(x+1)^{s-n}x^{\frac{n}{2}} + u(x+1)^t g_1(x) + 2u(x+1)^t g_2(x)$, which implies that $2f(x) = 2u(x+1)^t g_1(x)$. It follows from this that $2f(x)g_1(x)^{-1}g_2(x) = 2u(x+1)^t g_2(x)$. Now $f(x) - 2u(x+1)^t g_2(x) = (x+1)^s + u(x+1)^t g_1(x) + 2ug_2(x)(x+1)^t - 2u(x+1)^t g_2(x)$. So $f(x)(1 - 2g_2(x)g_1(x)^{-1}) = (x+1)^s + u(x+1)^t h(x)$, where $h(x) = g_1(x)$. Since $1 + 2g_2(x)g_1(x)^{-1}$ is a unit in R_n, we get $I = \langle f(x)\rangle = \langle (x+1)^s + u(x+1)^t h(x)\rangle$. Similarly, when $s - n \le t \le n-1$, we can see that $I = \langle (x+1)^s + u(x+1)^t h(x)\rangle$, where $h(x) \in R''_n$ is a unit.

   Now we determine the degree of $h(x)$. From Theorem 6.3.11, we have $T = 2n - s + t$ when $t < s - n$, and there is no $T < n$ such that $u(x+1)^T \in I$ when $t \ge s - n$. Therefore $\deg h(x) \le \begin{cases} 2n - s - 1 & \text{if } t < s - n, \\ n - t - 1 & \text{if } t \ge s - n \end{cases}.$

4. Let $I = \langle f(x)\rangle$, where $f(x) = (x+1)^s + 2u(x+1)^t g(x)$, $n \le s \le 2n-1$, and $g(x)$ is a unit in R''_n. Then from Lemma 6.3.8, we have $t < s - n$. From Theorem 6.3.12, the smallest value of T_1 such that $2u(x+1)^{T_1} \in I$ is $T_1 = \begin{cases} 2n - s + t & \text{if } t < 2s - 3n, \\ s - n & \text{if } 2s - 3n \le t < s - n \end{cases}$. Therefore $I = \langle (x+1)^s + 2u(x+1)^t h(x)\rangle$, where $h(x)$ is a unit in R''_n and $\deg h(x) \le T_1 - t - 1$.

5. Let $I = \langle f(x)\rangle$, where $f(x) = (x+1)^s + u(x+1)^t g(x)$, $n \le s \le 2n-1$, $g(x) = 2h'_1(x) + (x+1)^l h'_2(x)$ and $h'_1(x)$, $h'_2(x)$ are units in R''_n, R'_n, respectively. Then from

Lemma 6.3.8, we have $t < s - n$. Now let $h_2'(x) = h_{21}'(x) + 2h_{22}'(x)$, where $h_{21}'(x)$, $h_{22}'(x) \in \mathbb{Z}_2[x]$. Since $2f(x) = 2u(x+1)^{l+t}h_2'(x) \in I$, we get $2f(x)(h_2'(x))^{-1}h_{22}'(x) = 2u(x+1)^{l+t}h_{22}'(x) \in I$. Then $f(x)+2f(x)h_2'(x)^{-1}h_{22}'(x) = (x+1)^s+u(x+1)^t(2h_1'(x)+(x+1)^l h_2'(x)) + 2u(x+1)^{l+t}h_{22}'(x)$. This implies that

$$\begin{aligned} f(x)\left(1+2h_2'(x)^{-1}h_{22}'(x)\right) &= (x+1)^s + 2u(x+1)^t h_1'(x) + u(x+1)^{l+t}h_{21}'(x) \\ &+ 2u(x+1)^{l+t}h_{22}'(x) + 2u(x+1)^{l+t}h_{22}'(x) \\ &= (x+1)^s + 2u(x+1)^t h_1'(x) + u(x+1)^{l+t}h_{21}'(x) \\ &= (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)), \end{aligned}$$

where $h_1(x) = h_1'(x)$, $h_2(x) = h_{21}'(x)$ are units in R_n''. Since $1+2h_2'(x)^{-1}h_{22}'(x)$ is a unit in R_n, $I = \left\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)) \right\rangle$. However, when $l+t \leq s-n$, from Theorem 6.3.12, we have $T_1 = 0$, i.e., $2u \in I$. Then I will be one of the ideals discussed in Case (3). Therefore $I = \left\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)) \right\rangle$, where $0 \leq t < s-n < l+t < n$, $h_1(x)$, $h_2(x) \in R_n''$ and deg $h_1(x) \leq T_1 - t - 1$ and deg $h_2(x) \leq n - t - l - 1$.

■

Using the principal ideals of R_n, as discussed in Theorem 6.3.13, the non-principal ideals of R_n can be described as follows:

Theorem 6.3.14. *The distinct non-principal ideals of R_n are*

1. $I = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, *where* $1 \leq s \leq n-1$, $0 \leq t \leq s-1$, $1+t \leq m \leq T-1$, $h(x)$ *is either zero or a unit in* R_n'' *and deg* $h(x) \leq m-t-1$.

2. $I = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, *where* $n \leq s \leq 2n-1$, $0 \leq t \leq n-1$, $1+t \leq m \leq T-1$, $h(x)$ *is either zero or a unit in* R_n'' *and deg* $h(x) \leq$ *min*$\{m,n\}-t-1$.

3. $I = \langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^m \rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $1+t \leq m \leq T-1$, $h(x)$ *is a unit in* R_n'' *and deg* $h(x) \leq$ *min*$\{m,T_1\}-t-1$.

4. $I = \langle (x+1)^s + 2u(x+1)^t h(x),\ 2u(x+1)^{m_1} \rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $1+t \leq m_1 \leq T_1-1$, $h(x)$ *is a unit in* R_n'' *and deg* $h(x) \leq m_1-t-1$.

5. *$I = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^m \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $t+l < m < n$, $h_1(x)$, $h_2(x)$ are units in R''_n, deg $h_1(x) \leq T_1 - t - 1$, deg $h_2(x) < n - t - l$.*

6. *$I = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ 2u(x+1)^{m_1} \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, deg $h_1(x) < m_1 <$ min$\{s-n, n-s+l+t\}$, $h_1(x)$, $h_2(x)$ are units in R''_n.*

Proof. We present the proof of (1). The proofs of the rest follow similar lines of arguments. When $h(x) = 0$, $I = \langle (x+1)^s,\ u(x+1)^m \rangle$, where $1 \leq s \leq n-1$, $0 \leq m \leq s-1$. When $h(x) \neq 0$, from Theorem 6.3.11, the smallest value of T such that $u(x+1)^s \in \langle (x+1)^s + u(x+1)^t h(x) \rangle$ is $T = s$. Since I is non-principal, we must have $m < s$. Hence $I = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $1 \leq s \leq n-1$, $0 \leq t \leq s-1$, $1 + t \leq m \leq T - 1$, and deg $h(x) \leq m - t - 1$. ■

Summarizing Theorems 6.3.13 and 6.3.14 we present the complete structure of negacyclic codes of length n over R.

Theorem 6.3.15. *Let C be a negacyclic code of length n over R. Then C is one of the following:*

- ***Type 0:*** *$\langle 0 \rangle$ or $\langle 1 \rangle$.*

- ***Type 1:*** *$\langle u(x+1)^m \rangle$, $0 \leq m \leq 2n-1$.*

- ***Type 2.0:*** *$\langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $1 \leq s \leq n-1$, $0 \leq t \leq s-1$, $h(x)$ is either zero or a unit in R''_n and deg $h(x) \leq s - t - 1$.*

- ***Type 2.1:*** *$\langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $n \leq s \leq 2n-1$, $0 \leq t \leq n-1$, $h(x)$ is either zero or a unit in R''_n and deg $h(x) \leq T - t - 1$.*

- ***Type 2.2:*** *$\langle (x+1)^s + 2u(x+1)^t h(x) \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $h(x)$ is a unit in R''_n and deg $h(x) \leq T_1 - t - 1$.*

- ***Type 2.3:*** *$\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)) \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l+t < n$, $h_1(x)$, $h_2(x)$ are units in R''_n, deg $h_1(x) \leq T_1 - t - 1$ and deg $h_2(x) \leq n - t - l - 1$.*

- ***Type 3.0:*** *$\langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $1 \le s \le n-1$, $0 \le t \le s-1$, $1+t \le m \le T-1$, $h(x)$ is either zero or a unit in R''_n and deg $h(x) \le m-t-1$.*

- ***Type 3.1:*** *$\langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $n \le s \le 2n-1$, $0 \le t \le n-1$, $1+t \le m \le n-1$, $h(x)$ is either zero or a unit in R''_n and deg $h(x) \le m-t-1$.*

- ***Type 3.2:*** *$\langle (x+1)^s + u(x+1)^t h(x),\ 2u(x+1)^{m_1} \rangle$, where $n+1 \le s \le 2n-1$, $s-n+1 \le t \le n-1$, $0 \le m_1 \le T_1 - 1$, $h(x)$ is either zero or a unit in R''_n and deg $h(x) \le n-t-1$.*

- ***Type 3.3:*** *$\langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $1+t \le m \le n-1$, $h(x)$ is a unit in R''_n and deg $h(x) \le$ min$\{m,\ T_1\} - t - 1$.*

- ***Type 3.4:*** *$\langle (x+1)^s + 2u(x+1)^t h(x),\ 2u(x+1)^{m_1} \rangle$, where $n \le s \le 2n-1$, $0 \le t \le s-n-1$, $1+t \le m_1 \le T_1 - 1$, $h(x)$ is a unit in R''_n and deg $h(x) \le m_1 - t - 1$.*

- ***Type 3.5:*** *$\big\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^m \big\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$ $s-n < t+l < m < n$, $h_1(x)$, $h_2(x)$ are units in R''_n and deg $h_1(x) \le T_1 - t - 1$, deg $h_2(x) \le m-t-l-1$.*

- ***Type 3.6:*** *$\big\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)),\ 2u(x+1)^{m_1} \big\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $1+t \le m_1 \le T_1 - 1$, $h_1(x)$, $h_2(x)$ are units in R''_n and deg $h_1(x) \le m_1 - t - 1$, deg $h_2(x) \le n-t-l-1$.*

6.4 A Mass formula for the number of negacylic codes of length 2^k over $\mathbb{Z}_4 + u\mathbb{Z}_4$

In this section, we obtain a mass formula for the number of negacylic codes of length $n = 2^k$ over R. The following lemmas (Lemmas 6.4.1 and 6.4.2) are used in Theorem 6.4.3 to find out the number of negacyclic codes of length n over R.

Lemma 6.4.1. *For $0 \le a_1,\ a_2 \le 2n-1$, $\sum\limits_{s=a_2}^{a_1} (2n-s)2^{2n-s-1} = (2n-a_1-1)2^{2n-a_1} - (2n-a_2-2)2^{2n-a_2-1}$.*

Proof. Let $G(x) = \sum\limits_{s=a_2}^{a_1} x^{2n-s}$. Then $G(x) = \frac{x^{2n-a_1+1} - x^{2n-a_2}}{x-1}$, which implies that the derivative of $G(x)$ is $G'(x) = \frac{(x-1)\left((2n-a_1+1)x^{2n-a_1} - (2n-a_2)x^{2n-a_2-1}\right) - \left(x^{2n-a_1+1} - x^{2n-a_2}\right)}{(x-1)^2}$. Therefore $G'(2) = (2n - a_1 - 1)2^{2n-a_1} - (2n - a_2 - 2)2^{2n-a_2-1}$. Also $G(x) = \sum\limits_{s=a_2}^{a_1} x^{2n-s}$ implies that $G'(x) = \sum\limits_{s=a_2}^{a_1} (2n-s)x^{2n-s-1}$. Hence $G'(2) = \sum\limits_{s=a_2}^{a_1} (2n-s)2^{2n-s-1} = (2n - a_1 - 1)2^{2n-a_1} - (2n - a_2 - 2)2^{2n-a_2-1}$. ■

Lemma 6.4.2. *For* $0 \leq b_1,\ b_2 \leq 2n-1,\ \sum\limits_{t=b_2}^{b_1} (2n-s-t-1)2^{2n-s-t-2} = (2n-s-b_1-2)2^{2n-s-b_1-1} - (2n-s-b_2-3)2^{2n-s-b_2-2}$.

Proof. Similar to the proof of Lemma 6.4.1. ■

Theorem 6.4.3. *The number of negacyclic codes of length n over R is*

$$11 \cdot 2^n + 2^{\frac{n}{2}-1}(5n-12) - (n^2 + 5n + 4).$$

Proof. Let $\mathcal{N}_i$ denote the number of negacyclic codes of length n of each Type i and $\mathcal{N}$ denote the total number of negacyclic codes of length n over R. First we find the number of negacyclic codes in each case.

Type 0: There are two trivial negacyclic codes, $\langle 0 \rangle$ and $\langle 1 \rangle$. Therefore $\mathcal{N}_0 = 2$.

Type 1: Let $\mathcal{C} = \langle u(x+1)^m \rangle$, $0 \leq m \leq 2n-1$. Therefore the number of negacyclic codes of this type is $\mathcal{N}_1 = 2n$.

Type 2.0: Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $1 \leq s \leq n-1$, $0 \leq t \leq s-1$, and $h(x)$ is either zero or unit in R''_n.

If $h(x) = 0$, then the number of negacyclic codes of this type is $\mathcal{N}'_{2.0} = n-1$.

If $h(x) \neq 0$, then $\mathcal{N}''_{2.0} = \sum\limits_{s=1}^{n-1}\sum\limits_{t=0}^{s-1} 2^{s-t-1} = \sum\limits_{s=1}^{n-1}(2^s - 1) = 2^n - 2 - (n-1) = 2^n - n - 1$.

Therefore the total number of negacyclic codes of this type is

$$\mathcal{N}_{2.0} = \mathcal{N}'_{2.0} + \mathcal{N}''_{2.0} = n - 1 + 2^n - n - 1 = 2^n - 2.$$

Type 2.1: Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $n \leq s \leq 2n-1$, $0 \leq t \leq n-1$, and $h(x)$ is either zero or unit in R''_n.

If $h(x) = 0$, then $\mathcal{N}'_{2.1} = n$.

If $h(x) \neq 0$, then from Theorem 6.3.11, we have $T = \begin{cases} 2n - s + t & \text{if } 0 \leq t < 2s - 2n, \\ s & \text{if } 2s - 2n \leq t < n \end{cases}$.

This implies that deg $h(x) \leq \min\,\{T,\ n\} - t - 1 = \begin{cases} 2n - s - 1 & \text{if } 0 \leq t < s - n, \\ n - t - 1 & \text{if } 2s - 2n \leq t < n \end{cases}$.

Therefore

$$\begin{aligned}
\mathcal{N}''_{2.1} &= \underbrace{\sum_{t=0}^{n-1} 2^{n-t-1}}_{\text{for } s = n} + \sum_{s=n+1}^{2n-1} \left[\sum_{t=0}^{s-n-1} 2^{2n-s+t-t-1} + \sum_{t=s-n}^{n-1} 2^{n-t-1} \right] \\
&= (2^n - 1) + \sum_{s=n+1}^{2n-1} \left[(s-n)2^{2n-s-1} + 2^{2n-s} - 1 \right] \\
&= (2^n - 1) + \sum_{s=n+1}^{2n-1} \left[(n - (2n - s))2^{2n-s-1} + 2^{2n-s} - 1 \right] \\
&= (2^n - 1) + (n+2) \sum_{s=n+1}^{2n-1} 2^{2n-s-1} - \sum_{s=n+1}^{2n-1} (2n - s)2^{2n-s-1} - \sum_{s=n+1}^{2n-1} 1 \\
&= (2^n - 1) + (n+2)(2^{n-1} - 1) - ((n-2)2^{n-1} - 1) - (n-1) \quad \text{(from Lemma 6.4.1)} \\
&= 3 \cdot 2^n - 2n - 3.
\end{aligned}$$

Thus the total number of negacyclic codes of this type is

$$\mathcal{N}_{2.1} = \mathcal{N}'_{2.1} + \mathcal{N}''_{2.1} = n + 3 \cdot 2^n - 2n - 3 = 3 \cdot 2^n - n - 3.$$

Type 2.2: Let $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$, where $n + 1 \leq s \leq 2n - 1$, $0 \leq t \leq s - n - 1$, and $h(x)$ is a unit in R''_n. Then from Theorem 6.3.12, we have $T_1 = \begin{cases} 2n - s + t & \text{if } 0 \leq t < 2s - 3n, \\ s - n & \text{if } 2s - 3n \leq t < s - n \end{cases}$. This implies that deg $h(x) \leq \begin{cases} 2n - s - 1 & \text{if } 0 \leq t < 2s - 3n, \\ s - n - t - 1 & \text{if } 2s - 3n \leq t < s - n \end{cases}$. Therefore the number of negacyclic codes of this type is

$$\begin{aligned}
\mathcal{N}_{2.2} &= \sum_{s=n+1}^{\frac{3n}{2}-1}\sum_{t=0}^{s-n-1} 2^{s-n-t-1} + \sum_{s=\frac{3n}{2}}^{2n-1}\left[\sum_{t=0}^{2s-3n-1} 2^{2n-s-1} + \sum_{t=2s-3n}^{s-n-1} 2^{s-n-t-1}\right] \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1} (2^{s-n}-1) + \sum_{s=\frac{3n}{2}}^{2n-1} \left[(2s-3n)2^{2n-s-1} + 2^{2n-s} - 1\right] \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1} (2^{s-n}-1) + \sum_{s=\frac{3n}{2}}^{2n-1} \left[\left((n+2) - 2(2n-s)\right) 2^{2n-s-1} - 1\right] \\
&= \left(2^{\frac{n}{2}} - 2 - \frac{n}{2} + 1\right) + \left[(n+2)\left(2^{\frac{n}{2}} - 1\right) - 2\left(\left(\frac{n}{2} - 1\right) 2^{\frac{n}{2}} + 1\right) - \frac{n}{2}\right] \\
&= 5 \cdot 2^{\frac{n}{2}} - 2n - 5.
\end{aligned}$$

Type 2.3: Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)) \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l+t < n$, $h_1(x)$, $h_2(x)$ are units in R''_n, deg $h_1(x) \leq T_1 - t - 1$ and deg $h_2(x) \leq n-t-l-1$. Then from Theorem 6.3.12, we have $T_1 = \begin{cases} n-s+l+t & \text{if } \ s-n \leq l+t < 2s-2n, \\ s-n & \text{if } \ 2s-2n \leq l+t < n \end{cases}$. Since $0 \leq$ deg $h_1(x) \leq T_1 - t - 1$ and $s-n+1 \leq l+t \leq n-1$, we have $l \geq s-n+1$ and $s \leq 2n-2$, respectively. Therefore the number of negacyclic codes of this type is

$$\begin{aligned}
\mathcal{N}_{2.3} &= \sum_{s=n+1}^{\frac{3n}{2}-1}\sum_{t=0}^{s-n-1}\left[\sum_{l=s-n+1}^{2s-2n-t} 2^{l-s+n-1}\cdot 2^{n-l-t-1} + \sum_{l=2s-2n-t+1}^{n-t-1} 2^{s-n-t-1}\cdot 2^{n-l-t-1}\right] \\
&+ \sum_{s=\frac{3n}{2}}^{2n-2}\sum_{t=0}^{2n-s-2}\sum_{l=s-n+1}^{n-t-1} 2^{l-s+n-1}\cdot 2^{n-l-t-1} \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1}\sum_{t=0}^{s-n-1}\left[\sum_{l=s-n+1}^{2s-2n-t} 2^{2n-s-t-2} + \sum_{l=2s-2n-t+1}^{n-t-1} 2^{s-l-2t-2}\right] + \sum_{s=\frac{3n}{2}}^{2n-2}\sum_{t=0}^{2n-s-2}\sum_{l=s-n+1}^{n-t-1} 2^{2n-s-t-2} \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1}\sum_{t=0}^{s-n-1}\left[(s-n-t+1)2^{2n-s+t-2} - 2^{s-n-t-1}\right] \\
&+ \sum_{s=\frac{3n}{2}}^{2n-1}\sum_{t=0}^{2n-s-2} (2n-s-t-1)2^{2n-s-t-2}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{s=n+1}^{\frac{3n}{2}-1}\sum_{t=0}^{s-n-1}\left[((2n-s-t-1)-(3n-2s-2))2^{2n-s+t-2}-2^{s-n-t-1}\right]\\
&+ \sum_{s=\frac{3n}{2}}^{2n-2}\left[(2n-s-2)2^{2n-s-1}+1\right]\\
&= \sum_{s=n+1}^{\frac{3n}{2}-1}\left[\left((2n-s-2)2^{2n-s-1}-(3n-2s-2)2^{3n-2s-1}\right)-(3n-2s-2)\right.\\
&\quad \left.\left(2^{2n-s-1}-2^{3n-2s-1}\right)-\left(2^{s-n}-1\right)\right]+\sum_{s=\frac{3n}{2}}^{2n-2}\left[(2n-s)2^{2n-s-1}-2^{2n-s}+1\right]\\
&= \sum_{s=n+1}^{\frac{3n}{2}-1}\left[(s-n)2^{2n-s-1}-\left(2^{s-n}-1\right)\right]+\left[\left(\frac{n}{2}-1\right)2^{\frac{n}{2}}-\left(2^{\frac{n}{2}+1}-4\right)+\left(\frac{n}{2}-1\right)\right]\\
&= \sum_{s=n+1}^{\frac{3n}{2}-1}\left[\left(n-(2n-s)\right)2^{2n-s-1}-2^{s-n}-1\right]+\left[\left(\frac{n}{2}-3\right)2^{\frac{n}{2}}+3+\frac{n}{2}\right]\\
&= \left[n(2^{n-1}-2^{\frac{n}{2}})-\left((n-2)2^{n-1}-\left(\frac{n}{2}-1\right)2^{\frac{n}{2}}\right)-(2^{\frac{n}{2}}-2)+\left(\frac{n}{2}-1\right)\right]\\
&+ \left[\left(\frac{n}{2}-3\right)2^{\frac{n}{2}}+3+\frac{n}{2}\right]\\
&= 2^n-5\cdot 2^{\frac{n}{2}}+n+4.
\end{aligned}$$

Type 3.0: Let $\mathcal{C}=\langle (x+1)^s+u(x+1)^t h(x),\ u(x+1)^m\rangle$, where $1\leq s\leq n-1$, $0\leq t<s$, $1+t\leq m\leq T-1$, $h(x)$ is either zero or a unit in R_n'' and $\deg h(x)\leq m-t-1$.

If $h(x)=0$, then $\mathcal{C}=\langle (x+1)^s,\ u(x+1)^m\rangle$, where $1\leq s\leq n-1$, $0\leq m\leq s-1$. So $\mathcal{N}_{3.0}'=\sum\limits_{s=1}^{n-1}s=\frac{(n-1)n}{2}$.

If $h(x)\neq 0$, then $0\leq \deg h(x)\leq m-t-1$. Since $1+t\leq m\leq s-1$, so $t\leq s-2$ and then $s\geq 2$. Thus

$$\begin{aligned}
\mathcal{N}_{3.0}'' &= \sum_{s=2}^{n-1}\sum_{t=0}^{s-2}\sum_{m=1+t}^{s-1}2^{m-t-1}\\
&= \sum_{s=2}^{n-1}\sum_{t=0}^{s-2}\left(2^{s-t-1}-1\right)\\
&= 2^n-\left(\frac{n^2+n+2}{2}\right).
\end{aligned}$$

Therefore the total number of negacyclic codes of this type is

$$\mathcal{N}_{3.0} = \frac{(n-1)n}{2} + 2^n - \left(\frac{n^2+n+2}{2}\right) = 2^n - (n+1).$$

Type 3.1: Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $n \leq s \leq 2n-1$, $0 \leq t \leq n-1$, $1+t \leq m \leq \min\{T, n\} - 1$, $h(x)$ is either zero or a unit in R''_n and deg $h(x) \leq m-t-1$.

If $h(x) = 0$, then $\mathcal{C} = \langle (x+1)^s,\ u(x+1)^m \rangle$, where $n \leq s \leq 2n-1$, $0 \leq m \leq n-1$. So the number of negacyclic codes of this type is $\mathcal{N}'_{3.1} = \sum\limits_{s=n}^{2n-1} n = n^2$.

If $h(x) \neq 0$, then from Theorem 6.3.11, we have $T = \begin{cases} 2n-s+t & \text{if } 0 \leq t \leq s-n, \\ s & \text{if } s-n+1 \leq t < n \end{cases}$.

Since $1+t \leq m \leq n-1$ and $1+t \leq m \leq 2n-s+t-1$, we have $t \leq n-2$ and $s \leq 2n-2$, respectively. So the number of negacyclic codes with $h(x) \neq 0$ is

$$\begin{aligned} \mathcal{N}''_{3.1} &= \sum_{s=n}^{2n-2}\left[\sum_{t=0}^{s-n}\sum_{m=1+t}^{2n-s+t-1} 2^{m-t-1} + \sum_{t=s-n+1}^{n-2}\sum_{m=1+t}^{n-1} 2^{m-t-1}\right] \\ &= \sum_{s=n}^{2n-2}\left[\sum_{t=0}^{s-n}\left(2^{2n-s-1}-1\right) + \sum_{t=s-n+1}^{n-2}\left(2^{n-t-1}-1\right)\right] \\ &= \sum_{s=n}^{2n-2}\left[\left(2^{2n-s-1}-1\right)(s-n+1) + \left(2^{2n-s-1}-2\right) - (2n-s-2)\right] \\ &= \sum_{s=n}^{2n-2}\left[2^{2n-s-1}(s-n+2) - (n+1)\right] + (n-1) \\ &= \sum_{s=n}^{2n-2}\left[\left((n+2)-(2n-s)\right)2^{2n-s-1} - (n+1)\right] \\ &= (n+2)\left(2^n-2\right) - (n-1)2^n - (n+1)(n-1) \\ &= 3 \cdot 2^n - (n^2+2n+3). \end{aligned}$$

Therefore the total number of negacyclic codes of this type is

$$\mathcal{N}_{3.1} = n^2 + 3 \cdot 2^n - (n^2+2n+3) = 3 \cdot 2^n - (2n+3).$$

Type 3.2: Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ 2u(x+1)^{m_1} \rangle$, where $n+1 \leq s \leq 2n-1$,

$s-n+1 \leq t \leq n-1$, $0 \leq m_1 \leq T_1 - 1$, $h(x)$ is either zero or a unit in R_n'' and deg $h(x) \leq n-t-1$.

If $h(x) = 0$, then $\mathcal{C} = \langle (x+1)^s,\ 2u(x+1)^{m_1} \rangle = \langle 2(x+1)^{s-n},\ 2u(x+1)^{m_1} \rangle$, where $0 \leq m_1 \leq s-n-1$. So the number of negacyclic codes of this type is $\mathcal{N}_{3.2}' = \sum\limits_{s=n+1}^{2n-1} (s-n) = \frac{n(n-1)}{2}$.

If $h(x) \neq 0$, then from Theorem 6.3.12, $T_1 = \begin{cases} 0 & \text{if } 0 \leq t \leq s-n, \\ n-s+t & \text{if } \ s-n+1 \leq t \leq 2s-2n, \\ s-n & \text{if } \ 2s-2n+1 \leq t < n \end{cases}$ $\cdot$

Also, $s \leq 2n-2$, as $s-n+1 \leq t \leq n-1$. So the number of negacyclic codes with $h(x) \neq 0$ is

$$\begin{aligned}
\mathcal{N}_{3.2}'' &= \sum_{s=n+1}^{\frac{3n}{2}-1} \left[\sum_{t=s-n+1}^{2s-2n} \sum_{m_1=0}^{n-s+t-1} 2^{n-t-1} + \sum_{t=2s-2n+1}^{n-1} \sum_{m_1=0}^{s-n-1} 2^{n-t-1} \right] \\
&+ \sum_{s=\frac{3n}{2}}^{2n-2} \sum_{t=s-n+1}^{n-1} \sum_{m_1=0}^{n-s+t-1} 2^{n-t-1} \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1} \left[\sum_{t=s-n+1}^{2s-2n} 2^{n-t-1}(n-s+t) + \sum_{t=2s-2n+1}^{n-1} 2^{n-t-1}(s-n) \right] \\
&+ \sum_{s=\frac{3n}{2}}^{2n-2} \sum_{t=s-n+1}^{n-1} (n-s+t) 2^{n-t-1} \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1} \left[\sum_{t=s-n+1}^{2s-2n} 2^{n-t-1} \left((2n-s) - (n-t) \right) + \left(2^{3n-2s-1} - 1 \right)(s-n) \right] \\
&+ \sum_{s=\frac{3n}{2}}^{2n-2} \sum_{t=s-n+1}^{n-1} 2^{n-t-1} \left((2n-s) - (n-t) \right) \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1} \left[(2n-s) \left(2^{2n-s-1} - 2^{3n-2s-1} \right) - \left((2n-s-2) 2^{2n-s-1} - (3n-2s-2) 2^{3n-2s-1} \right) \right. \\
&+ \left. \left(2^{3n-2s-1} - 1 \right)(s-n) \right] + \sum_{s=\frac{3n}{2}}^{2n-2} \left[(2n-s) \left(2^{2n-s-1} - 1 \right) - \left((2n-s-2) 2^{2n-s-1} + 1 \right) \right] \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1} \left[2^{2n-s} - 2^{3n-2s} - (s-n) \right] + \sum_{s=\frac{3n}{2}}^{2n-2} \left[2^{2n-s} - (2n-s+1) \right]
\end{aligned}$$

$$\begin{aligned} &= (2^n - 4) - \left(\frac{2^n - 4}{3}\right) - \left(\frac{\frac{n}{2}\left(\frac{n}{2} - 1\right)}{2}\right) - \left(\frac{\left(\frac{n}{2} + 1\right)\left(\frac{n}{2} + 2\right)}{2} - 3\right) \\ &= \frac{2^{n+3} - (3n^2 + 6n + 8)}{12}. \end{aligned}$$

Therefore the number of negacyclic codes of this type is

$$\mathcal{N}_{3.2} = \frac{n(n-1)}{2} + \frac{2^{n+3} - (3n^2 + 6n + 8)}{12}.$$

Type 3.3: Let $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $1+t \leq m \leq n-1$, $h(x)$ is a unit in R''_n and $\deg h(x) \leq \ \min\{m, T_1\} - t - 1$. Then from Theorem 6.3.12, we have $T_1 = \begin{cases} 2n - s + t & \text{if } \ 0 \leq t \leq 2s - 3n, \\ s - n & \text{if } \ 2s - 3n + 1 \leq t < s - n \end{cases}$.

Therefore, $\deg h(x) \leq \begin{cases} 2n - s - 1 & \text{if } \ 0 \leq t \leq 2s - 3n, \\ s - n - t - 1 & \text{if } \ 2s - 3n + 1 \leq t < s - n \end{cases}$. So the number of negacyclic codes of this type is

$$\begin{aligned} \mathcal{N}_{3.3} &= \sum_{s=n+1}^{\frac{3n}{2}-1} \sum_{t=0}^{s-n-1} \left(\sum_{m=1+t}^{s-n} 2^{m-t-1} + \sum_{m=s-n+1}^{n-1} 2^{s-n-t-1} \right) + \sum_{s=\frac{3n}{2}}^{2n-2} \left[\sum_{t=0}^{2s-3n} \left(\sum_{m=1+t}^{2n-s+t} 2^{m-t-1} \right.\right. \\ &+ \left.\left. \sum_{m=2n-s+t+1}^{n-1} 2^{2n-s-1} \right) + \sum_{t=2s-3n+1}^{s-n-1} \left(\sum_{m=1+t}^{s-n} 2^{m-t-1} + \sum_{m=s-n+1}^{n-1} 2^{s-n-t-1} \right) \right] + \underbrace{\sum_{t=0}^{n-2} \sum_{m=1+t}^{n-1} 2^{2n-s-1}}_{\text{for } s = 2n-1} \\ &= \sum_{s=n+1}^{\frac{3n}{2}-1} \sum_{t=0}^{s-n-1} \left[\left(2^{s-n-t} - 1\right) + (2n - s - 1)\, 2^{s-n-t-1} \right] + \sum_{s=\frac{3n}{2}}^{2n-2} \left[\sum_{t=0}^{2s-3n} \left(\left(2^{2n-s} - 1\right) \right.\right. \\ &+ \left. (s - n - t - 1)\, 2^{2n-s-1} \right) + \left. \sum_{t=2s-3n+1}^{s-n-1} \left(\left(2^{s-n-t} - 1\right) + 2^{s-n-t-1}(2n - s - 1) \right) \right] + \frac{n(n-1)}{2} \\ &= \sum_{s=n+1}^{\frac{3n}{2}-1} \sum_{t=0}^{s-n-1} \left[(2n - s + 1) 2^{s-n-t-1} - 1 \right] + \sum_{s=\frac{3n}{2}}^{2n-2} \left[\sum_{t=0}^{2s-3n} \left((s - n - t + 1) 2^{2n-s-1} - 1 \right) \right. \\ &+ \left. \sum_{t=2s-3n+1}^{s-n-1} \left((2n - s + 1) 2^{s-n-t-1} - 1 \right) \right] + \frac{n(n-1)}{2} \end{aligned}$$

$$\begin{aligned}
&= \sum_{s=n+1}^{\frac{3n}{2}-1} \left[(2n-s+1)2^{s-n} - (n+1)\right] + \sum_{s=\frac{3n}{2}}^{2n-2} \Bigg[\Bigg(2^{2n-s-1}\frac{(2s-3n+1)(n+2)}{2} \\
&- (2s-3n+1)\Big) + \left((2n-s+1)\left(2^{2n-s-1}-1\right) - (2n-s-1)\right)\Big] + \frac{n(n-1)}{2} \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1} \left[(2n-s+1)2^{s-n} - (n+1)\right] + \sum_{s=\frac{3n}{2}}^{2n-2} \Bigg(2^{2n-s-1}\Bigg(\frac{(2s-3n+2)(n+1)}{2} \\
&+ 1\Big) - (n+1)\Big) + \frac{n(n-1)}{2} \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1} \left(\left((n+1)-(n-s)\right)2^{s-n} - (n+1)\right) \\
&+ \sum_{s=\frac{3n}{2}}^{2n-2} \left(2^{2n-s-1}\left(\frac{((n+2)-2(2n-s))\,(n+1)}{2}+1\right) - (n+1)\right) + \frac{n(n-1)}{2} \\
&= (n+1)\left(2^{\frac{n}{2}}-2\right) - \left(\left(\frac{n}{2}-2\right)2^{\frac{n}{2}}+2\right) - (n+1)\left(\frac{n}{2}-1\right) + \left(\frac{(n+1)(n+2)}{2}+1\right)\left(2^{\frac{n}{2}}-2\right) \\
&- (n+1)\left(\frac{n}{2}-1\right)2^{\frac{n}{2}} - (n+1)\left(\frac{n}{2}-1\right) + \frac{n(n-1)}{2} \\
&= \frac{2^{\frac{n}{2}}(5n+12)}{2} - \frac{3(n^2+3n+4)}{2}
\end{aligned}$$

Type 3.4: Let $C = \langle (x+1)^s + 2u(x+1)^t h(x),\ 2u(x+1)^{m_1}\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $1+t \le m_1 \le T_1 - 1$, $h(x)$ is a unit in R''_n and $\deg h(x) \le m_1 - t - 1$. Then from Theorem 6.3.12, we have $T_1 = \begin{cases} 2n-s+t & \text{if } 0 \le t \le 2s-3n, \\ s-n & \text{if } 2s-3n+1 \le t < s-n \end{cases}$. Therefore, $\deg\ h(x)\ \le \begin{cases} 2n-s-1 & \text{if } 0 \le t < 2s-3n, \\ s-n & \text{if } 2s-3n \le t < s-n \end{cases}$. Since $1+t \le s-n-1$, we have $t \le s-n-2$. So the number of negacyclic codes of this type is

$$\begin{aligned}
\mathcal{N}_{3.4} &= \sum_{s=n+2}^{\frac{3n}{2}} \sum_{t=0}^{s-n-2} \sum_{m_1=1+t}^{s-n-1} 2^{m_1-t-1} + \sum_{s=\frac{3n}{2}+1}^{2n-2} \left[\sum_{t=0}^{2s-3n-1} \sum_{m_1=1+t}^{2n-s+t-1} 2^{m_1-t-1} + \sum_{t=2s-3n}^{s-n-2} \sum_{m=1+t}^{s-n-1} 2^{m_1-t-1}\right] \\
&= \sum_{s=n+2}^{\frac{3n}{2}} \sum_{t=0}^{s-n-2} \left(2^{s-n-t-1}-1\right) + \sum_{s=\frac{3n}{2}+1}^{2n-2} \left[\sum_{t=0}^{2s-3n-1} \left(2^{2n-s-1}-1\right) + \sum_{t=2s-3n}^{s-n-2} \left(2^{s-n-t-1}-1\right)\right]
\end{aligned}$$

$$\begin{aligned}
&= \sum_{s=n+2}^{\frac{3n}{2}} \left(\left(2^{s-n}-2\right)-(s-n-1)\right) + \sum_{s=\frac{3n}{2}+1}^{2n-2} \left[\left((2s-3n)\left(2^{2n-s-1}-1\right)\right)+\left(2^{2n-s}-2\right)\right.\\
&- \left.(2n-s-1)\right]\\
&= \sum_{s=n+2}^{\frac{3n}{2}} \left(2^{s-n}-s+n-1\right) + \sum_{s=\frac{3n}{2}+1}^{2n-2} \left[2^{2n-s-1}(2s-3n+2)-(s-n+1)\right]\\
&= \left(2^{\frac{n}{2}+1}-4\right) - \sum_{s=n+2}^{2n-2}(s-n+1) + \sum_{s=\frac{3n}{2}+1}^{2n-2}\left((n+2)-2(2n-s)\right)2^{2n-s-1}\\
&= \left(2^{\frac{n}{2}+1}-4\right) - \sum_{s=n+2}^{2n-2}(s-n+1) + (n+2)\left(2^{\frac{n}{2}-1}-2\right) - 2\left(\frac{n}{2}2^{\frac{n}{2}-1}-2^{\frac{n}{2}}\right)\\
&= \left(2^{\frac{n}{2}+1}-4\right) - \left(\frac{n(n-1)}{2}-3\right) + (n+2)\left(2^{\frac{n}{2}-1}-2\right) - 2\left(\frac{n}{2}2^{\frac{n}{2}-1}-2^{\frac{n}{2}}\right)\\
&= 5\cdot 2^{\frac{n}{2}} - \frac{(n^2+3n+10)}{2}
\end{aligned}$$

Type 3.5: Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t(2h_1(x)+(x+1)^l h_2(x)),\ u(x+1)^m \rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $s-n < l+t < m < n$, $h_1(x)$, $h_2(x)$ are units in R''_n, deg $h_1(x) \le T_1 - t - 1$ and deg $h_2(x) \le m-t-l-1$. Then from Theorem 6.3.12, we have $T_1 = \begin{cases} n-s+l+t & \text{if} \quad s-n+1 \le l+t < 2s-2n, \\ s-n & \text{if} \quad 2s-2n \le l+t < n \end{cases}$. As $s-n+1 \le l+t \le n-1$, we have $s \le 2n-2$. So the number of negacyclic codes of this type is $\mathcal{N}_{3.5}$

$$\begin{aligned}
&= \sum_{s=n+1}^{\frac{3n}{2}-2}\sum_{t=0}^{s-n-1}\left[\sum_{l=s-n+1}^{2s-2n-t}\sum_{m=l+t+1}^{n-1} 2^{l+n-s-1}.2^{m-l-t-1} + \sum_{l=2s-2n-t+1}^{n-t-2}\sum_{m=l+t+1}^{n-1} 2^{s-n-t-1}.2^{m-l-t-1}\right]\\
&+ \sum_{s=\frac{3n}{2}-1}^{2n-3}\sum_{t=0}^{2n-s-3}\sum_{l=s-n+1}^{n-t-2}\sum_{m=l+t+1}^{n-1} 2^{l+n-s-1}.2^{m-l-t-1}\\
&= \sum_{s=n+1}^{\frac{3n}{2}-2}\sum_{t=0}^{s-n-1}\left[\sum_{l=s-n+1}^{2s-2n-t}\sum_{m=l+t+1}^{n-1} 2^{m+n-s-t-2} + \sum_{l=2s-2n-t+1}^{n-t-2}\sum_{m=l+t+1}^{n-1} 2^{m+s-n-l-2t-2}\right]\\
&+ \sum_{s=\frac{3n}{2}-1}^{2n-3}\sum_{t=0}^{2n-s-3}\sum_{l=s-n+1}^{n-t-2}\sum_{m=l+t+1}^{n-1} 2^{m+n-s-t-2}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{s=n+1}^{\frac{3n}{2}-2} \sum_{t=0}^{s-n-2} \left[\sum_{l=s-n+1}^{2s-2n-t} \left(2^{2n-s-t-2} - 2^{l+n-s-1}\right) + \sum_{l=2s-2n-t+1}^{n-t-2} \left(2^{s-l-2t-2} - 2^{s-n-t-1}\right) \right] \\
&+ \sum_{s=\frac{3n}{2}-1}^{2n-3} \sum_{t=0}^{2n-s-3} \sum_{l=s-n+1}^{n-t-2} \left(2^{2n-s-t-2} - 2^{l+n-s-1}\right) \\
&= \sum_{s=n+1}^{\frac{3n}{2}-2} \sum_{t=0}^{s-n-2} \left[\left(2^{2n-s-t-2}(s-n-t) - \left(2^{s-n-t} - 1\right)\right) + \left(2^{2s-s-t-2} - (3n-2s)2^{s-n-t-1}\right) \right] \\
&+ \sum_{s=\frac{3n}{2}-1}^{2n-3} \sum_{t=0}^{2n-s-3} \left(2^{2n-s-t-2}(2n-s-t-3) + 1\right) \\
&= \sum_{s=n+1}^{\frac{3n}{2}-2} \sum_{t=0}^{s-n-2} \left(2^{2n-s-t-2}(s-n-t+1) - (3n-2s+2)2^{s-n-t-1} + 1\right) \\
&+ \sum_{s=\frac{3n}{2}-1}^{2n-3} \sum_{t=0}^{2n-s-3} \left(2^{2n-s-t-2}(2n-s-t-3) + 1\right) \\
&= \sum_{s=n+1}^{\frac{3n}{2}-2} \left(2^{2n-s-1}(s-n) - (3n-2s+2)2^{s-n} + (2n-s+2)\right) \\
&+ \sum_{s=\frac{3n}{2}-1}^{2n-3} \left(2^{2n-s-t-1}(2n-s-4) + (2n-s+2)\right) \\
&= \sum_{s=n+1}^{\frac{3n}{2}-2} \left(2^{2n-s-1}(s-n) - (3n-2s+2)2^{s-n}\right) + \sum_{s=\frac{3n}{2}-1}^{2n-3} \left(2^{2n-s-t-1}(2n-s-4)\right) \\
&+ \sum_{s=n+1}^{2n-3} (2n-s+2) \\
&= \left(2^n - (n+4)2^{\frac{n}{2}} + 2(n+4)\right) + \left((n-8)2^{\frac{n}{2}} + 12\right) + \left(\frac{(n+1)(n+2)}{2} - 10\right) \\
&= 2^n - 12 \cdot 2^{\frac{n}{2}} + \frac{n^2+7n+22}{2}
\end{aligned}$$

Type 3.6: Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ 2u(x+1)^{m_1} \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l < n-t$, $t+1 \leq m_1 \leq T_1 - 1$, $h_1(x)$, $h_2(x)$ are units in R''_n, deg $h_1(x) \leq m_1 - t - 1$ and deg $h_2(x) \leq n-t-l-1$. Then from Theorem 6.3.12, we have $T_1 = \begin{cases} n-s+l+t & \text{if } \ 0 \leq l+t < 2s-2n, \\ s-n & \text{if } \ 2s-2n \leq l+t < n \end{cases}$. So the number of negacyclic codes in this case is

$$\begin{aligned}
\mathcal{N}_{3.6} &= \sum_{s=n+2}^{\frac{3n}{2}-1} \sum_{t=0}^{s-n-2} \left[\sum_{l=s-n+2}^{2s-2n-t} \sum_{m_1=t+1}^{l-s+n+t-1} 2^{m+n-l-2t-2} + \sum_{l=2s-2n-t+1}^{n-t-1} \sum_{m_1=t+1}^{s-n-1} 2^{m+n-l-2t-2} \right] \\
&+ \sum_{s=\frac{3n}{2}}^{2n-3} \sum_{t=0}^{2n-s-3} \sum_{l=s-n+2}^{n-t-1} \sum_{m_1=t+1}^{l-s+n+t-1} 2^{m+n-l-2t-2} \\
&= \sum_{s=n+2}^{\frac{3n}{2}-1} \sum_{t=0}^{s-n-2} \left[\sum_{l=s-n+2}^{2s-2n-t} \left(2^{2n-s-t-2} - 2^{n-l-s-1}\right) + \sum_{l=2s-2n-t+1}^{n-t-1} \left(2^{s-l-2t-2} - 2^{n-l-t-1}\right) \right] \\
&+ \sum_{s=\frac{3n}{2}}^{2n-3} \sum_{t=0}^{2n-s-3} \sum_{l=s-n+2}^{n-t-1} \left(2^{2n-s-t-2} - 2^{n-l-t-1}\right) \\
&= \sum_{s=n+2}^{\frac{3n}{2}-1} \sum_{t=0}^{s-n-2} \Big[\Big(2^{2n-s-t-2}\,(s-n-t-2) + 2^{3n-2s-1}\Big) + \Big(2^{2s-s-t-2} - 2^{3n-2s-1} \\
&- \quad 2^{s-n-t-1} + 1\Big)\Big] + \sum_{s=\frac{3n}{2}}^{2n-3} \sum_{t=0}^{2n-s-3} \left(2^{2n-s-t-2}(2n-s-t-3) + 1\right) \\
&= \sum_{s=n+2}^{\frac{3n}{2}-1} \left(2^{2n-s-1}\,(s-n-2) + 2^{3n-2s} - 2^{s-n} + (s-n+1)\right) \\
&+ \sum_{s=\frac{3n}{2}}^{2n-3} \left(2^{2n-s-1}(2n-s-2) - (2^{2n-s}-4) + (2n-s-2)\right) \\
&= \left(\frac{2^n}{3} - \frac{n2^{\frac{n}{2}}}{2} - \frac{1}{3} + \frac{n(n+2)}{8}\right) + \Bigg(\left(\frac{n-2}{2}\right)2^{\frac{n}{2}} - 4 - (2^{\frac{n}{2}+2} - 16) \\
&+ \frac{(2n+2)(n-4) - (2n-3)(2n-2)}{2} + \frac{3n(3n-2)}{8}\Bigg) \\
&= \frac{2^n}{3} - 5 \cdot 2^{\frac{n}{2}} + \frac{3n^2 + 18n + 56}{12}
\end{aligned}$$

The total number of negacyclic codes of length n over R is obtained by summing all types (Type 0 through Type 3.6) of negacyclic codes over R. Hence the total number of negacyclic codes of length n over R is

$$\mathcal{N} = 11 \cdot 2^n + 2^{\frac{n}{2}-1}(5n-12) - (n^2 + 5n + 4).$$

■

6.5 Negacyclic codes of even length over $\mathbb{Z}_4 + u\mathbb{Z}_4$

In this section, we discuss negacyclic codes of any even length over R. In [21], Blackford has discussed cyclic codes of length $2n$ over $\mathbb{Z}_4$ using discrete Fourier transform approach. Dougherty and Ling [49] have generalized this study to cyclic codes of any even length over $\mathbb{Z}_4$ using the same approach. We use the same technique to study negacyclic codes of even length over R.

Any even integer N can be written as $N = ne$, where $n = 2^k$ and e an odd integer. As usual a negacyclic code of length N over R is an ideal of $R_N = \frac{R[x]}{\langle x^N+1\rangle}$. Let $R_n = \frac{R[y]}{\langle y^n+1\rangle}$. We define a mapping $\eta : R_n^e \to R^N$ such that $\eta(\sum\limits_{i=0}^{n-1} a_{0,i}y^i, \ \sum\limits_{i=0}^{n-1} a_{1,i}y^i, \ldots, \sum\limits_{i=0}^{n-1} a_{e-1,i}y^i) = (a_{0,0}, a_{1,0}, \ldots, a_{e-1,0}, \ a_{0,1}, a_{1,1}, \ldots, a_{e-1,1}, \ldots, a_{0,n-1}, a_{1,n-1}, \ldots, a_{e-1,n-1})$. We can see that $\eta(y\sum\limits_{i=0}^{n-1} a_{e-1,i}y^i, \ \sum\limits_{i=0}^{n-1} a_{0,i}y^i, \ldots, \sum\limits_{i=0}^{n-1} a_{e-2,i}y^i) = (-a_{e-1,n-1}, a_{0,0}, a_{1,0}, \ldots, a_{e-1,0}, \ a_{0,1}, a_{1,1}, \ldots, a_{e-1,1}, \ldots, a_{0,n-1}, a_{1,n-1}, \ldots, a_{e-2,n-1})$. This shows that a negacyclic shift in R^N corresponds to a y-constacylic shift in R_n^e. Thus we have the following theorem.

Theorem 6.5.1. *[21, Theorem 1] Negacyclic codes of length N over R correspond to y-constacyclic codes of length e over R_n i.e., $\frac{R[x]}{\langle x^N+1\rangle} \cong \frac{R_n[x]}{\langle x^e-y\rangle}$.*

From Theorem 6.3.1, the ring R_n is a local ring. So by Hensel's Lemma, there exist pairwise coprime monic basic irreducible polynomials $f_1(x), f_2(x), \ldots, f_r(x)$ in $R_n[x]$ such that $x^e - y = f_1(x)f_2(x)\cdots f_r(x)$. Therefore by the Chinese Remainder Theorem $\frac{R_n[x]}{\langle x^e-y\rangle} = \bigoplus\limits_{i=1}^{r} \frac{R_n[x]}{\langle f_i(x)\rangle}$. Further the ring $\frac{R_n[x]}{\langle f_i(x)\rangle}$ is isomorphic to $\frac{GR(R,r_i)[x]}{\langle x^n+1\rangle}$, where deg $f_i(x) = r_i$ and $GR(R, r_i) = \frac{R[x]}{\langle f_i(x)\rangle}$ is the Galois ring extension of R of degree r_i.

Let $S_r = \frac{GR(R,r)[x]}{\langle x^n+1\rangle}$, $S_r' = \frac{GR(4,r)[x]}{\langle x^n+1\rangle}$ and $S_r'' = \frac{\mathbb{F}_{2^r}[x]}{\langle x^n+1\rangle}$. We now discuss the ideal structure of S_r. Since the ring $R_n = S_1 = \frac{GR(R,1)[x]}{\langle x^n+1\rangle} = \frac{R[x]}{\langle x^n+1\rangle}$, the results obtained in Section 6.3 and Section 6.4 can be straightaway generalized to S_r.

Lemma 6.5.2. *In S_r,*

1. *$(x+1)^n = 2x^{\frac{n}{2}}$ and $(x+1)$ is nilpotent with nilpotency $2n$.*

2. *an element $f(x) = \sum\limits_{j=0}^{n-1} a_j(x+1)^j$ is a unit if and only if a_0 is a unit in $GR(R,r)$.*

3. *$(x+1)^n = 2\left((x+1)^{\frac{n}{2}}+1\right)$ and $\langle(x+1)^n\rangle = \langle 2\rangle$.*

Theorem 6.5.3. *Let $0 \leq T \leq 2n-1$ be the smallest non-negative integer such that*

$$u(x+1)^T \in \left\langle (x+1)^s + u(x+1)^t h(x) \right\rangle,$$

where $0 \leq s \leq 2n-1$, $h(x) \in GR(R,r)[x]$ and deg $h(x) \leq n-t-1$. Then

$$T = \begin{cases} s & \text{if } 1 \leq s \leq n-1, \\ 2n-s+t & \text{if } n \leq s \leq 2n-1,\ 0 \leq t < 2s-2n \ \text{ and } \ h(x) \text{ is a unit in } S'_r, \\ s & \text{if } n \leq s \leq 2n-1 \ \text{ and } t \geq 2s-2n, \ \text{ and } \ h(x) \text{ is a unit in } S'_r, \\ 3n-s+t & \text{if } n < s \leq 2n-1,\ 0 \leq t < 2s-3n \ \text{ and } h(x) = 2h'(x), \\ s & \text{if } n < s \leq 2n-1,\ 2s-3n \leq t < s-n \ \text{ and } h(x) = 2h'(x), \\ 2n-s+l+t & \text{if } n < s \leq 2n-1,\ 0 \leq t < s-n,\ 0 \leq l+t < 2s-2n \\ & \ \text{and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \\ s & \text{if } n < s \leq 2n-1,\ 0 \leq t < s-n,\ l+t \geq 2s-2n \\ & \ \text{and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \end{cases}$$

where $h'(x)$, $h_1(x)$ are units in S''_r and $h_2(x)$ is a unit in S'_r.

Theorem 6.5.4. *Let $0 \leq T_1 \leq n-1$ be the smallest non-negative integer such that*

$$2u(x+1)^{T_1} \in \left\langle (x+1)^s + u(x+1)^t h(x) \right\rangle,$$

where $0 \leq s \leq 2n-1$, $h(x) \in GR(R,r)[x]$ and deg $h(x) \leq n-t-1$. Then

$$T_1 = \begin{cases} 0 & \text{if } 1 \leq s \leq n-1, \\ 0 & \text{if } n \leq s \leq 2n-1,\ 0 \leq t < s-n \text{ and } h(x) \text{ is a unit in } S'_r, \\ n-s+t & \text{if } n \leq s \leq 2n-1,\ s-n \leq t < 2s-2n \text{ and } h(x) \text{ is a unit in } S'_r, \\ s-n & \text{if } n \leq s \leq 2n-1,\ 2s-2n \leq t < n \text{ and } h(x) \text{ is a unit in } S'_r, \\ 2n-s+t & \text{if } n < s \leq 2n-1,\ 0 \leq t < 2s-3n \text{ and } h(x) = 2h'(x), \\ s-n & \text{if } n \leq s \leq 2n-1,\ 2s-3n \leq t < s-n \text{ and } h(x) = 2h'(x), \\ 0 & \text{if } n \leq s \leq 2n-1,\ 0 \leq t < s-n,\ 0 \leq l+t \leq s-n \\ & \quad \text{and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \\ l+t-s+n & \text{if } n < s \leq 2n-1,\ 0 \leq t < s-n,\ s-n < l+t < 2s-2n \\ & \quad \text{and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \\ s-n & \text{if } n < s \leq 2n-1,\ 0 \leq t < s-n,\ l+t \geq 2s-2n \\ & \quad \text{and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \end{cases}$$

where $h'(x)$, $h_1(x)$ are units in S''_r and $h_2(x)$ is a unit in S'_r.

Theorem 6.5.5. *Let I be an ideal of S_r. Then I is one of the following:*

- ***Type 0:*** $\langle 0 \rangle$ *or* $\langle 1 \rangle$.
- ***Type 1:*** $\langle u(x+1)^m \rangle$, $0 \leq m \leq 2n-1$.
- ***Type 2.0:*** $\langle (x+1)^s + u(x+1)^t h(x) \rangle$, *where* $1 \leq s \leq n-1$, $0 \leq t \leq s-1$, $h(x)$ *is either zero or a unit in* S''_r *and deg* $h(x) \leq s-t-1$.
- ***Type 2.1:*** $\langle (x+1)^s + u(x+1)^t h(x) \rangle$, *where* $n \leq s \leq 2n-1$, $0 \leq t \leq n-1$, $h(x)$ *is either zero or a unit in* S''_r *and deg* $h(x) \leq T-t-1$.
- ***Type 2.2:*** $\langle (x+1)^s + 2u(x+1)^t h(x) \rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $h(x)$ *is a unit in* S''_r *and deg* $h(x) \leq T_1-t-1$.

- ***Type 2.3:*** *$\big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x))\big\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $s-n < l+t < n$, $h_1(x)$, $h_2(x)$ are units in S_r'', deg $h_1(x) \le T_1 - t - 1$ and deg $h_2(x) \le n-t-l-1$.*

- ***Type 3.0:*** *$\langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m\rangle$, where $1 \le s \le n-1$, $0 \le t \le s-1$, $1+t \le m \le T-1$, $h(x)$ is either zero or a unit in S_r'' and deg $h(x) \le m-t-1$.*

- ***Type 3.1:*** *$\langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m\rangle$, where $n \le s \le 2n-1$, $0 \le t \le n-1$, $1+t \le m \le n-1$, $h(x)$ is either zero or a unit in S_r'' and deg $h(x) \le m-t-1$.*

- ***Type 3.2:*** *$\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ 2u(x+1)^{m_1}\rangle$, where $n+1 \le s \le 2n-1$, $s-n+1 \le t \le n-1$, $0 \le m_1 \le T_1 - 1$, $h(x)$ is either zero or a unit in S_r'' and deg $h(x) \le n-t-1$.*

- ***Type 3.3:*** *$\langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^m\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $1+t \le m \le n-1$, $h(x)$ is a unit in S_r'' and deg $h(x) \le$ min$\{m, T_1\} - t - 1$.*

- ***Type 3.4:*** *$\langle (x+1)^s + 2u(x+1)^t h(x),\ 2u(x+1)^{m_1}\rangle$, where $n \le s \le 2n-1$, $0 \le t \le s-n-1$, $1+t \le m_1 \le T_1 - 1$, $h(x)$ is a unit in S_r'' and deg $h(x) \le m_1 - t - 1$.*

- ***Type 3.5:*** *$\big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^m\big\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $s-n < t+l < m < n$, $h_1(x)$, $h_2(x)$ are units in S_r'' and deg $h_1(x) \le T_1 - t - 1$, deg $h_2(x) \le m-t-l-1$.*

- ***Type 3.6:*** *$\big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ 2u(x+1)^{m_1}\big\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $1+t \le m_1 \le T_1 - 1$, $h_1(x)$, $h_2(x)$ are units in S_r'' and deg $h_1(x) \le m_1 - t - 1$, deg $h_2(x) \le n-t-l-1$.*

6.5.1 Discrete Fourier transform

We now define the discrete Fourier transform to study negacyclic codes of length N over R. Let M be the order of 2 modulo e and ξ be a primitive e^{th} root of unity in $GR(R, M)$, where $GR(R, M)$ is Galois ring extension of R of degree M.

Let $a = (a_{0,0}, a_{0,1}, \ldots, a_{0,n-1}, a_{1,0}, a_{1,1}, \ldots, a_{1,n-1}, \ldots, a_{e-1,0}, a_{e-1,1}, \ldots, a_{e-1,n-1}) \in R^N$. The discrete Fourier transform of a is the vector $(A_0, A_1, \ldots, A_{e-1}) \in S_r^e$, where $A_h = a(y^{e'}\xi^h) = \sum_{i=0}^{e-1}\sum_{j=0}^{n-1} a_{i,j} y^{e'i+j}\xi^{ih}$, $0 \le h \le e-1$, and $ee' = 1 \pmod{n}$.

Define the Mattson-Solomon polynomial of a to be $A(Z) = \sum_{h=0}^{e-1} A_{e-h}Z^h$. Note that $A_e = A_0$. The following is the generalization of [21, Theorem 2] to the present setting.

Lemma 6.5.6. *[Inversion formula] Let $a \in R^N$ and $A(Z)$ be its Mattson-Solomon polynomial. Then*

$$a = \Omega[(1, y^{-e'}, y^{-2e'}, \ldots, y^{-(e-1)e'}) * \frac{1}{e}(A(1), A(\xi), A(\xi^2), \ldots, A(\xi^{e-1}))],$$

where $*$ is componentwise multiplication.

Proof. Let $0 \le t \le e-1$. Then

$$\begin{aligned} A(\xi^t) &= \sum_{h=0}^{e-1} A_h \xi^{-ht} \\ &= \sum_{h=0}^{e-1}\left(\sum_{i=0}^{e-1}\sum_{j=0}^{n-1} a_{i,j}y^{e'i+j}\xi^{ih}\right)\xi^{-ht} \\ &= \sum_{i=0}^{e-1}\sum_{j=0}^{n-1} a_{i,j}y^{e'i+j}\sum_{h=0}^{e-1}\xi^{h(i-t)} \\ &= ey^{e't}\sum_{j=0}^{n-1} a_{t,j}y^j \end{aligned}$$

The rest can easily be derived from the definition of the map Ω. ∎

Extend the automorphism on $GR(R,r)$ defined by $\sigma(a) = a_0^2 + 2a_1^2 + ua_2^2 + 2ua_3^2$, where $a = a_0 + 2a_1 + ua_2 + 2ua_3 \in GR(R,r)$, $a_0, a_1, a_2, a_3 \in \mathcal{T}$ to S_r by $\sigma(a) = a$, $a \in S_r$. For each $A_h \in S_r$, we have $A_{2h} = \sigma(A_h)$, where subscripts are calculated modulo e. Let $\mathcal{A} = \{(A_0, A_1, \ldots, A_{e-1}) \in S_r^e \ : \ A_h \in S_r \text{ with } A_{2h} = \sigma(A_h)\}$. Then it is easy to verify that the ring $\mathcal{A}$ isomorphic to $\oplus_{h\in L} S_{r_h}$, where L denotes a complete set of representatives of the 2-cyclotomic cosets modulo e. For each $\xi \in L$, let r_ξ denote the size of the 2-cyclotomic coset containing ξ.

The following theorem is a generalization of [21, Theorem 2].

Theorem 6.5.7. *The map $\Lambda : R_N \longmapsto \bigoplus_{\xi \in L} S_{r_\xi}$ such that $\Lambda(a(X)) = [A_\xi]_{\xi \in L}$ for $a(X) \in R_N$ is a ring isomorphism. In particular, if $\mathcal{C}$ is a negacyclic code of length N over R, then $\mathcal{C} \cong \bigoplus_{\xi \in L} \mathcal{C}_\xi$, where, for each $\xi \in L$, $\mathcal{C}_\xi$ is an ideal in S_{r_ξ}.*

Proof. Define a map $\gamma : \ R_N \longmapsto \mathcal{A}$ such that $\gamma(a(x)) = (A_0, A_1, \dots, A_{e-1})$, $a(x) \in R_N$. Let $a(x), b(x) \in R_N$. Then it is easy to see that $\gamma(a(x) + b(x)) = \gamma(a(x)) + \gamma(b(x))$. It follows from $a(x)b(x) = q(x)(x^N + 1) + r(x)$, where $q(x), r(x) \in R[x]$ with deg $r(x) < N$, that $\gamma(a(x)b(x)) = \gamma(a(x)) * \gamma(b(x))$, as $y^{e'}\xi^h$ is a root of $x^N + 1 = 0$ for each $h \in L$. So γ is a ring homomorphism. From Inversion Formula, if $\gamma(a(x)) = 0$, then we get $a(x) = 0$. Therefore γ is one-to-one. To show γ is surjective, let $A = (A_0, A_1, \dots, A_{e-1}) \in \mathcal{A}$ and $A(z) = \sum_{i=0}^{e-1} A_i z^i$. We show that there exists an $a(x) \in R_N$ such that $\gamma(a(x)) = A$. We have $A(\xi^h) = \sum_{h' \in L} \sum_{i \in cl_2(h',e)} A_i \xi^{hi}$. Since $\sigma(\sum_{i \in cl_2(h',e)} A_i \xi^{hi}) = \sum_{i \in cl_2(h',e)} A_i \xi^{hi}$, we have $\sum_{i \in cl_2(h',e)} A_i \xi^{hi} \in S_1$. So from Lemma 6.5.6, we get that γ is surjective. Hence γ is an isomorphism. Thus, if $\mathcal{C}$ is a negacyclic code of length N over R, then $\mathcal{C} \cong \bigoplus_{\xi \in L} \mathcal{C}_\xi$, where, for each $\xi \in L$, $\mathcal{C}_\xi$ is an ideal in S_{r_ξ}. ■

Theorem 6.5.8. *The number of distinct negacyclic codes of length N over R is $\prod_{\xi \in L} N_\xi$, where N_ξ is the number of distinct ideals of S_{r_ξ} for each $\xi \in L$.*

6.6 Conclusion

In this chapter, we have studied negacyclic codes of both odd and even lengths over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. We have classified negacyclic codes of length 2^k over R. A mass formula for the number of negacyclic codes of length 2^k over R has been derived. Further, we have also studied negacyclic codes of any even length over R.

Chapter 7

Duals of negacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$

7.1 Introduction

Throughout this chapter, we assume that $n = 2^k$ and $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. In this chapter, we study the duals of negacyclic codes of length n over R. We use the same notations as in Chapter 6. Let $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_rx^r$ be a polynomial in R_n. Then the reciprocal of $g(x)$ is the polynomial $g^*(x) = x^r g(\frac{1}{x}) = g_r + g_{r-1}x + g_{r-2}x^2 + \cdots + g_0x^r$ in R_n. Let I be an ideal of R_n. Then the annihilator of I is denoted by $A(I)$ and is defined as

$$A(I) = \{g(x) \in R_n \ : \ f(x)g(x) = 0 \ \ \forall \ f(x) \in I\} \ .$$

We define $A(I)^*$ as

$$A(I)^* = \{g^*(x) \ : \ g(x) \in A(I)\} \ .$$

It is well known that if $\mathcal{C}$ is a negacyclic code, then the dual of $\mathcal{C}$ is $\mathcal{C}^{\perp} = A(\mathcal{C})^*$. A negacyclic code $\mathcal{C}$ is said to be self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ and self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$. There are two codes associated with a negacyclic code $\mathcal{C}$ over R, namely, Tor ($\mathcal{C}$)= $\{a \in \mathbb{Z}_4^n \ : \ au \in \mathcal{C}\}$ and Res ($\mathcal{C}$)= $\{a \in \mathbb{Z}_4^n \ : \ a + bu \in \mathcal{C}$ for some $b \in \mathbb{Z}_4^n\}$. Since $\mathcal{C}$ is a negacyclic code over R, Tor ($\mathcal{C}$) and Res ($\mathcal{C}$) are negacylic codes over $\mathbb{Z}_4$. It is easy to see that Res ($\mathcal{C}$) = $\Phi(\mathcal{C})$

and Tor $(\mathcal{C}) = J$, where Φ is the projection map defined in Chapter 6, Section 6.3 and $J = \{h(x) \in R'_n \ : \ uh(x) \in \ker \Phi\}$. It follows from first isomorphism theorem that $|\mathcal{C}| = |\Phi(\mathcal{C})||\ker \Phi| = |\mathrm{Res}(\mathcal{C})||\mathrm{Tor}(\mathcal{C})|$. The Hamming, Lee and Euclidean distances are as defined on R in Chapter 5.

7.2 Duals of negacyclic codes of length 2^k over $\mathbb{Z}_4+u\mathbb{Z}_4$

In this section, we consider the duals of negacyclic codes of length n over R. First we recall the ideal structure of R_n (Theorem 6.3.15).

Theorem 7.2.1. *Let I be an ideal of R_n. Then I is one of the followings:*

- ***Type 0:*** $\langle 0\rangle$ *or* $\langle 1\rangle$.
- ***Type 1:*** $\langle u(x+1)^m\rangle$, $0 \le m \le 2n-1$.
- ***Type 2.0:*** $\langle (x+1)^s + u(x+1)^t h(x)\rangle$, *where* $1 \le s \le n-1$, $0 \le t \le s-1$, $h(x)$ *is either zero or a unit in* R''_n *and deg* $h(x) \le s-t-1$.
- ***Type 2.1:*** $\langle (x+1)^s + u(x+1)^t h(x)\rangle$, *where* $n \le s \le 2n-1$, $0 \le t \le n-1$, $h(x)$ *is either zero or a unit in* R''_n *and deg* $h(x) \le T-t-1$.
- ***Type 2.2:*** $\langle (x+1)^s + 2u(x+1)^t h(x)\rangle$, *where* $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $h(x)$ *is a unit in* R''_n *and deg* $h(x) \le T_1-t-1$.
- ***Type 2.3:*** $\big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x))\big\rangle$, *where* $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $s-n < l+t < n$, $h_1(x)$, $h_2(x)$ *are units in* R''_n, *deg* $h_1(x) \le T_1-t-1$ *and deg* $h_2(x) \le n-t-l-1$.
- ***Type 3.0:*** $\langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m\rangle$, *where* $1 \le s \le n-1$, $0 \le t \le s-1$, $1+t \le m \le T-1$, $h(x)$ *is either zero or a unit in* R''_n *and deg* $h(x) \le m-t-1$.
- ***Type 3.1:*** $\langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m\rangle$, *where* $n \le s \le 2n-1$, $0 \le t \le n-1$, $1+t \le m \le n-1$, $h(x)$ *is either zero or a unit in* R''_n *and deg* $h(x) \le m-t-1$.

- ***Type 3.2:*** *$C = \langle (x+1)^s + u(x+1)^t h(x),\ 2u(x+1)^{m_1} \rangle$, where $n+1 \le s \le 2n-1$, $s-n+1 \le t \le n-1$, $0 \le m_1 \le T_1 - 1$, $h(x)$ is either zero or a unit in R''_n and deg $h(x) \le n-t-1$.*

- ***Type 3.3:*** *$\langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $1+t \le m \le n-1$, $h(x)$ is a unit in R''_n and deg $h(x) \le$ min$\{m,\ T_1\} - t - 1$.*

- ***Type 3.4:*** *$\langle (x+1)^s + 2u(x+1)^t h(x),\ 2u(x+1)^{m_1} \rangle$, where $n \le s \le 2n-1$, $0 \le t \le s-n-1$, $1+t \le m_1 \le T_1 - 1$, $h(x)$ is a unit in R''_n and deg $h(x) \le m_1 - t - 1$.*

- ***Type 3.5:*** *$\big\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^m \big\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$ $s-n < t+l < m < n$, $h_1(x)$, $h_2(x)$ are units in R''_n and deg $h_1(x) \le T_1 - t - 1$, deg $h_2(x) \le m - t - l - 1$.*

- ***Type 3.6:*** *$\big\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)),\ 2u(x+1)^{m_1} \big\rangle$, where $n+1 \le s \le 2n-1$, $0 \le t \le s-n-1$, $1+t \le m_1 \le T_1 - 1$, $h_1(x)$, $h_2(x)$ are units in R''_n and deg $h_1(x) \le m_1 - t - 1$, deg $h_2(x) \le n - t - l - 1$.*

The following theorem gives the annihilators of principal ideals of R_n.

Theorem 7.2.2. *Let I be a non-trivial principal ideal and $A(I)$ be its annihilator in R_n.*

1. *If $I = \langle u(x+1)^m \rangle$, where $0 \le m \le 2n-1$, then $A(I) = \langle (x+1)^{2n-m},\ u \rangle$.*

2. *If $I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $1 \le s \le n-1$, $0 \le t < s$, $h(x)$ is either zero or a unit in R''_n and deg $h(x) \le s-t-1$, then*

$$A(I) = \begin{cases} \langle (x+1)^{2n-s} + u(x+1)^{2n-2s+t} h(x) \rangle, & \textit{when } t < 2s-n, \\ \big\langle (x+1)^{2n-s} + 2u(x+1)^{n-2s+t}(1 + (1+x)^{\frac{n}{2}}) h(x) \big\rangle, & \textit{when } t \ge 2s-n. \end{cases}$$

3. *If $I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $n \le s \le 2n-1$, $0 \le t \le n-1$ and $h(x)$ is either zero or a unit in R''_n, then*

$$A(I) = \begin{cases} \langle (x+1)^{s-t} + uh(x),\ u(x+1)^{2n-s} \rangle, & \textit{when } t < 2s-2n, \\ \langle (x+1)^{2n-s} + u(x+1)^{2n-2s+t} h(x) \rangle, & \textit{when } t \ge 2s-2n. \end{cases}$$

4. *If $I = \langle (x+1)^s + 2u(x+1)^t h(x)\rangle$, where $n < s \leq 2n-1$, $0 \leq t < s-n$ and $h(x)$ is a unit in R''_n, then*

$$A(I) = \begin{cases} \left\langle (x+1)^{2n-s} + u(x+1)^{3n-2s+t}(1+(x+1)^{\frac{n}{2}})h(x)\right\rangle, & \text{when } 2s-3n \leq t < s-n, \\ \left\langle (x+1)^{n-t},\ u(x+1)^{2n-s}\right\rangle, & \text{when } 0 \leq t < 2s-3n. \end{cases}$$

5. *If $I = \left\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x))\right\rangle$, where $n < s \leq 2n-1$, $0 \leq t < s-n$, $l > s-n-t$ and $h_1(x)$, $h_2(x)$ are units in R''_n, then*

$$A(I) = \left\langle (x+1)^{s-t} + u(2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^{2n-s}\right\rangle.$$

Proof. 1. Let $I = \langle u(x+1)^m\rangle$, $1 \leq m \leq 2n-1$.

Suppose $A(I) = \langle g(x),\ u(x+1)^r\rangle$, where $g(x) = (x+1)^i + uq(x)$, $q(x) \in \mathbb{Z}_4[x]$, $0 \leq r < i$. Since $g(x) \in A(I)$, $g(x)u(x+1)^m = 0$. This implies that $u(x+1)^{m+i} = 0$, which in turn implies that $m+i \geq 2n$. Thus $2n-m \leq i$. No integer $l < 2n-m$ satisfies $(x+1)^{l+m} = 0$, as the nilpotency of $x+1$ is $2n$. Therefore $i = 2n-m$ and $g(x) = (x+1)^{2n-m} + uq(x)$. It can easily be seen that $u \in A(I)$. So $r = 0$. Therefore $A(I) = \langle (x+1)^{2n-m} + uq(x),\ u\rangle = \langle (x+1)^{2n-m},\ u\rangle$.

2. Let $I = \langle f(x)\rangle$, where $f(x) = (x+1)^s + u(x+1)^t h(x)$, $1 \leq s \leq n-1$.

Suppose $A(I) = \langle g(x),\ u(x+1)^r\rangle$, where $g(x) = (x+1)^i + uq(x)$, $q(x) \in \mathbb{Z}_4[x]$, $0 \leq r < i$. Since $\Phi(I) = \langle (x+1)^s\rangle$, we have $A(\Phi(I)) = \langle (x+1)^{2n-s}\rangle$, where Φ is the projection map defined in Chapter 6, Section 6.3. Thus $g(x)$ must be of the form $g(x) = (x+1)^{2n-s} + uq(x)$, where $q(x) \in \mathbb{Z}_4[x]$. As $g(x) \in A(I)$, so $f(x)g(x) = 0$. This implies that $(x+1)^s q(x) + (x+1)^{2n-s+t}h(x) = 0$. Thus $(x+1)^s\,(q(x) + (x+1)^{2n-2s+t}h(x)) = 0$, as $s < n$. Therefore $q(x) + (x+1)^{2n-2s+t}h(x) = (x+1)^{2n-s}q'(x)$, where $q'(x) \in \mathbb{Z}_4[x]$. Since the degrees of both $q(x)$ and $(x+1)^{2n-2s+t}h(x)$ are less than $2n-s$, we must have $q'(x) = 0$. Therefore $q(x) = 3(x+1)^{2n-2s+t}h(x)$ and hence $g(x) = (x+1)^{2n-s} + 3u(x+1)^{2n-2s+t}h(x)$. Also we have $f(x)u(x+1)^r = 0$. This implies that $r \geq 2n-s$. Since there is no $l < 2n-s$ such that $f(x)u(x+1)^l = 0$, we get $r = 2n - s$. Further we can see that $ug(x) = u(x+1)^{2n-s} \in \langle g(x) \rangle$. So

$$\begin{aligned} A(I) = \langle g(x) \rangle &= \left\langle (x+1)^{2n-s} + 3u(x+1)^{2n-2s+t}h(x) \right\rangle \\ &= \left\langle (x+1)^{2n-s} + u(x+1)^{2n-2s+t}h(x) \right\rangle. \end{aligned}$$

However, when $t \geq 2s - n$, we have $2n - 2s + t \geq n$. Then

$$\begin{aligned} g(x) &= (x+1)^{2n-s} + u(x+1)^{2n-2s+t}h(x) \\ &= (x+1)^{2n-s} + 2u(x+1)^{n-2s+t}h(x)x^{\frac{n}{2}} \\ &= (x+1)^{2n-s} + 2u(x+1)^{n-2s+t}(1 + (1+x)^{\frac{n}{2}})h(x) \quad \text{(from Lemma 6.3.4).} \end{aligned}$$

Therefore $A(I) = \left\langle (x+1)^{2n-s} + 2u(x+1)^{n-2s+t}(1 + (1+x)^{\frac{n}{2}})h(x) \right\rangle$.

3. Let $I = \langle f(x) \rangle$, where $f(x) = (x+1)^s + u(x+1)^t h(x)$, $n \leq s \leq 2n - 1$. Then $(f(x))^2 = 0$.

   Suppose $A(I) = \langle g(x),\ u(x+1)^r \rangle$, where $g(x) = (x+1)^i + uq(x)$, $q(x) \in \mathbb{Z}_4[x]$, $0 \leq r < i$. Since $f(x)g(x) = 0$, we get $((x+1)^i + uq(x))((x+1)^s + u(x+1)^t h(x)) = 0$. This implies that $i \geq 2n - s$, and

$$(x+1)^s q(x) + (x+1)^{i+t}h(x) = 0. \tag{7.2.1}$$

   Now suppose that $i = 2n - s$. Then from equation (7.2.1), we get

$$(x+1)^s q(x) + (x+1)^{2n-s+t}h(x) = 0. \tag{7.2.2}$$

   If $t \geq 2s - 2n$, then $2n - s + t \geq s$. So from equation (7.2.2), we get $q(x) = 3(x+1)^{2n-2s+t}h(x)$, as was shown in part (2). If $t < 2s - 2n$, then $2n - s + t < s$. Again from equation (7.2.2), we get $(x+1)^{2n-s+t}(h(x) + q(x)(x+1)^{2s-2n-t}) = 0$. Since $h(x)$ is a unit, $h(x) + q(x)(x+1)^{2s-2n-t}$ is also a unit. Therefore $(x+1)^{2n-s+t} = 0$, a contradiction, as $2n$ is the nilpotency of $(x+1)$. Hence in this case, $i > 2n - s$. So, to determine $A(I)$, we consider the cases $t \geq 2s - 2n$ and $t < 2s - 2n$ separately.

Case (i) When $t \geq 2s-2n$, we have $q(x) = 3(x+1)^{2n-2s+t}h(x)$. Therefore $g(x) = (x+1)^{2n-s} + 3u(x+1)^{2n-2s+t}h(x)$. Again as was seen in part (2), $r = 2n-s$. Since $ug(x) = u(x+1)^{2n-s} \in \langle g(x) \rangle$,

$$A(I) = \langle g(x) \rangle = \left\langle (x+1)^{2n-s} + 3u(x+1)^{2n-2s+t}h(x) \right\rangle .$$

From Theorem 6.3.12, we have $2u \in A(I)$, as $2s-n < n$. Therefore

$$A(I) = \left\langle (x+1)^{2n-s} + u(x+1)^{2n-2s+t}h(x) \right\rangle .$$

Case (ii) When $t < 2s-2n$, we have $i > 2n-s$. From equation (7.2.1), we get that $i \geq s-t$, otherwise we get a contradiction. So we can choose $i = s-t$ and hence $q(x) = h(x)$. Therefore

$$A(I) = \left\langle (x+1)^{s-t} + uh(x),\ u(x+1)^{2n-s} \right\rangle .$$

4. Let $I = \langle f(x) \rangle$, where $f(x) = (x+1)^s + 2u(x+1)^t h(x)$, $n+1 \leq s \leq 2n-1$ and $t < s-n$. Then $(f(x))^2 = 0$.

Suppose $A(I) = \langle g(x),\ u(x+1)^r \rangle$, where $g(x) = (x+1)^i + uq(x)$, where $q(x) \in \mathbb{Z}_4[x]$, $0 \leq r < i$. Since $f(x)g(x) = 0$, we have $i \geq 2n-s$ and $(x+1)^s q(x) + 2(x+1)^{i+t}h(x) = 0$, which implies that

$$2(x+1)^{s-n}x^{\frac{n}{2}}q(x) + 2(x+1)^{i+t}h(x) = 0. \tag{7.2.3}$$

Now suppose that $i = 2n-s$. Then from equation (7.2.3), we get $2(x+1)^{s-n}x^{\frac{n}{2}}q(x) + 2(x+1)^{2n-s+t}h(x) = 0$. It follows that $q(x) = 3(x+1)^{2n-2s+t}(1+(x+1)^{\frac{n}{2}})h(x)$ for $t < 2s-3n$. If $t \geq 2s-3n$, then we get a contradiction, and hence $i > 2n-s$. So we consider the following cases.

Case (i) When $t < 2s-3n$, we have $q(x) = 3(x+1)^{3n-2s+t}(1+(x+1)^{\frac{n}{2}})h(x)$. This implies that $g(x) = (x+1)^{2n-s} + 3u(x+1)^{3n-2s+t}(1+(x+1)^{\frac{n}{2}})h(x)$. Also we have

$r = 2n - s$ and $u(x+1)^{2n-s} \in \langle g(x)\rangle$, as was shown in part (1). Therefore

$$A(I) = \left\langle (x+1)^{2n-s} + u(x+1)^{3n-2s+t}(1+(x+1)^{\frac{n}{2}})h(x)\right\rangle .$$

Case (ii) When $3n - 2s \leq t < s - n$, we have $i > 2n - s$. So, as was shown in part (3), $g(x) = (x+1)^{n-t} + u(x+1)^{2n-s}h(x)$. Since $2n - s < n - t$, $u(x+1)^{2n-s} \notin \langle g(x)\rangle$. Therefore

$$A(I) = \left\langle (x+1)^{n-t} + u(x+1)^{2n-s}h(x),\ u(x+1)^{2n-s}\right\rangle = \left\langle (x+1)^{n-t},\ u(x+1)^{2n-s}\right\rangle .$$

5. Can be proved similarly.

■

In the following theorem we present the annihilators of non-principal ideals of R_n.

Theorem 7.2.3. *Let I be a non-principal ideal and $A(I)$ be its annihilator in R_n.*

1. *If $I = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m\rangle$, where $1 \leq s < n$, $0 \leq t < m < s$ and $h(x)$ is either zero or a unit in R''_n, then*

$$A(I) = \left\langle (x+1)^{2n-m} + u(x+1)^{2n-m-s+t}h(x),\ u(x+1)^{2n-s}\right\rangle .$$

2. *If $I = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m\rangle$, where $n \leq s < 2n$, $0 \leq t < n$, $1 + t \leq m < T$ and $h(x)$ is either zero or a unit in R''_n, then $A(I) =$*

$$\begin{cases} \langle (x+1)^{2n-m} + u(x+1)^{2n-m-s+t}h(x),\ u(x+1)^{2n-s}\rangle, & \text{when } t \geq s + m - 2n, \\ \langle (x+1)^{s-t} + uh(x),\ u(x+1)^{2n-s}\rangle, & \text{when } 0 \leq t < s + m - 2n \end{cases} .$$

3. *If $I = \langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^m\rangle$, where $n < s \leq 2n - 1$, $0 \leq t < s - n$, $1 + t \leq m < n$ and $h(x)$ is a unit in R''_n, then*

$$A(I) = \left\langle (x+1)^{2n-m},\ u(x+1)^{2n-s}\right\rangle .$$

4. *If $I = \langle (x+1)^s + 2u(x+1)^t h(x),\ 2u(x+1)^{m_1} \rangle$, where $n < s \leq 2n-1$, $0 \leq t < s-n$, $1+t \leq m_1 < T_1$ and $h(x)$ is a unit in R''_n, then*

$$A(I) = \begin{cases} \left\langle (x+1)^{n-m_1} + u(x+1)^{2n-m-s+t}\hat{h}(x),\ u(x+1)^{2n-s} \right\rangle, & \textit{when } t \geq s+m_1-2n, \\ \langle (x+1)^{n-t},\ u(x+1)^{2n-s} \rangle, & \textit{when } t < s+m_1-2n, \end{cases}$$

where $\hat{h}(x) = (1+(x+1)^{\frac{n}{2}})h(x)$.

5. *If $I = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^m \rangle$, where $n < s \leq 2n-1$, $0 \leq t < s-n$, $t+l+1 \leq m < n$ and $h_1(x)$, $h_2(x)$ are units in R''_n then*

$$A(I) = \begin{cases} \langle (x+1)^{2n-m} + u(x+1)^{2n-m-s+t+l}h_2(x),\ u(x+1)^{2n-s} \rangle, & \textit{when } t+l \geq s+m-2n, \\ \langle (x+1)^{2n-l},\ u(x+1)^{2n-s} \rangle, & \textit{when } t+l < s+m-2n \end{cases}$$

6. *If $I = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ 2u(x+1)^{m_1} \rangle$, where $n < s \leq 2n-1$, $0 \leq t < s-n$, $t < m_1 < T_1$ and $h_1(x)$, $h_2(x)$ are units in R''_n, then*

$$A(I) = \begin{cases} \left\langle (x+1)^{n-m_1} + u(x+1)^{n-m_1-s+t+l}\hat{h}(x),\ u(x+1)^{2n-s} \right\rangle, & \textit{when } t+l \geq s+m_1-n, \\ \langle (x+1)^{2n-l},\ u(x+1)^{2n-s} \rangle, & \textit{when } t+l < s+m_1-n, \end{cases}$$

where $\hat{h}(x) = h_1(x)(x+1)^{n-l} + h_2(x)(1+(x+1)^{\frac{n}{2}})$.

Proof. 1. Let $I = \langle f(x),\ u(x+1)^m \rangle$, where $f(x) = (x+1)^s + u(x+1)^t h(x)$ and $0 \leq m < s \leq n-1$, $0 \leq t \leq m-1$.

Suppose $A(I) = \langle g(x), u(x+1)^r \rangle$, where $g(x) = (x+1)^i + uq(x)$, $q(x) \in \mathbb{Z}_4[x]$. Then we get $g(x)u(x+1)^m = 0$, which implies that $(x+1)^{i+m} = 0$. Thus $i \geq 2n-m$. We can see that no $i < 2n-m$ satisfies $u(x+1)^m g(x) = 0$. Therefore $i = 2n-m$. We have $g(x) \in A(I)$, so $g(x)f(x) = 0$. It follows that $(x+1)^s q(x) + (x+1)^{2n-m+t}h(x) = 0$. Since $2n-m > s$, we get $(x+1)^s\,(q(x) + (x+1)^{2n-m-s+t}h(x)) = 0$. This implies that $q(x) + 3(x+1)^{2n-m-s+t}h(x) = (x+1)^{2n-s}q'(x)$, where $q'(x) \in \mathbb{Z}_4[x]$. But the degrees of both $q(x)$ and $h(x)(x+1)^{2n-m-s+t}$ are at most $2n-s-1$, so $q'(x) = 0$.

Thus $q(x) = 3(x+1)^{2n-m-s+t}h(x)$. Hence $g(x) = (x+1)^i + 3u(x+1)^{i-s+t}h(x)$.

It is easy to see that $2n-s$ is the least positive integer such that $u(x+1)^{2n-s} \in A(I)$ and $u(x+1)^{2n-s} \notin \langle g(x) \rangle$, as $2n-m > 2n-s$. Therefore $A(I) = \langle g(x),\ u(x+1)^{2n-s} \rangle$. Therefore $A(I) = \langle (x+1)^{2n-m} + u(x+1)^{2n-m-s+t}h(x),\ u(x+1)^{2n-s} \rangle$.

2. Let $I = \langle f(x),\ u(x+1)^m \rangle$, where $f(x) = (x+1)^s + u(x+1)^t h(x)$, $n \leq s < 2n$ and $0 \leq t < n$, $1 + t \leq m < \min\{s, 2n-s+t\}$.

   Suppose $A(I) = \langle g(x), u(x+1)^r \rangle$, where $g(x) = (x+1)^i + uq(x)$, $q(x) \in \mathbb{Z}_4[x]$. As was seen in part (1), $i \geq 2n-m$ and

$$(x+1)^s q(x) + (x+1)^{i+t} h(x) = 0. \tag{7.2.4}$$

   Suppose $i = 2n-m$. Then from equation (7.2.4), $(x+1)^s q(x) + (x+1)^{2n-m+t} = 0$. If $s+m-2n < t$, then $q(x) = 3(x+1)^{2n-m-s+t}h(x)$, which implies that $g(x) = (x+1)^{2n-m} + 3u(x+1)^{2n-m-s+t}h(x)$. If $t \leq s+m-2n$, then again from equation (7.2.4), $(x+1)^{2n-m-s+t}\left(h(x) + (x+1)^{s+m-t-2n}q(x)\right) = 0$. Since $h(x) + (x+1)^{s+m-t-2n}q(x)$ is a unit in R_n and $2n$ is the nilpotency of $(x+1)$, so $(x+1)^{2n-m-s+t} = 0$, a contradiction. Hence, in this case $i > 2n-m$. So we consider the following cases.

   Case (i) When $s+m-2n < 0 \leq t$, we have $g(x) = (x+1)^{2n-m} + 3u(x+1)^{2n-m-s+t}h(x)$. As was seen in part (1), $u(x+1)^{2n-s} \in A(I)$. Since there is no $l < 2n-s$ such that $f(x)u(x+1)^l = 0$ and $u(x+1)^{2n-s} \notin \langle g(x) \rangle$, we have

$$A(I) = \left\langle (x+1)^{2n-m} + 3u(x+1)^{2n-m-s+t}h(x),\ u(x+1)^{2n-s} \right\rangle.$$

   Case (ii) When $t \leq s+m-2n$, we have $s \geq 2n-m+t$. Rest of the proof is similar to that of Theorem 7.2.2 (3).

Other parts of the theorem can be proved using similar lines of arguments. ■

Theorems 7.2.2 and 7.2.3 provide the duals of negacyclic codes of length n over R. We now find the structure of negacylic codes $\mathcal{C}$ of length n over R satisfying $\mathcal{C} \subset A(\mathcal{C})$ and $\mathcal{C} = A(\mathcal{C})$. For this we need to know the size of a negacyclic code $\mathcal{C}$ over R. Since

$|\mathcal{C}| = |\text{Res } (\mathcal{C})||\text{Tor } (\mathcal{C})|$, we have to find the Res $(\mathcal{C})$ and Tor $(\mathcal{C})$ of a negacyclic code $\mathcal{C}$ over R. The following theorem presents Res $(\mathcal{C})$ and Tor $(\mathcal{C})$ of $\mathcal{C}$ in each case of $\mathcal{C}$ as described in Theorem 7.2.1.

Theorem 7.2.4. *Let $\mathcal{C}$ be a non-trivial negacyclic code of length n over R.*

1. *If $\mathcal{C} = \langle u(x+1)^m \rangle$, where $0 \leq m \leq 2n$, then Res $(\mathcal{C}) = \langle 0 \rangle$ and Tor $(\mathcal{C}) = \langle (x+1)^m \rangle$.*

2. *If $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $0 \leq s \leq n-1$, $0 \leq t \leq s-1$ and $h(x)$ is either zero or a unit in R''_n, then Res $(\mathcal{C}) =$ Tor $(\mathcal{C}) = \langle (x+1)^s \rangle$.*

3. *If $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, where $n \leq s \leq 2n-1$, $0 \leq t \leq n-1$ and $h(x)$ is either zero or a unit in R''_n, then Res $(\mathcal{C}) = \langle (x+1)^s \rangle$ and Tor $(\mathcal{C}) = \big\langle (x+1)^T \big\rangle$.*

4. *If $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$ and $h(x)$ is a unit in R''_n, then Res $(\mathcal{C}) = \langle (x+1)^s \rangle$ and Tor $(\mathcal{C}) = \big\langle (x+1)^T \big\rangle$.*

5. *If $\mathcal{C} = \big\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)) \big\rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l+t < n$ and $h_1(x)$, $h_2(x)$ are units in R''_n, then Res $(\mathcal{C}) = \langle (x+1)^s \rangle$ and Tor $(\mathcal{C}) = \big\langle (x+1)^T \big\rangle$.*

6. *If $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $1 \leq s \leq n-1$, $0 \leq t \leq s-1$, $1+t \leq m \leq T-1$, $h(x)$ is either zero or a unit in R''_n, then Res $(\mathcal{C}) = \langle (x+1)^s \rangle$ and Tor $(\mathcal{C}) = \langle (x+1)^m \rangle$.*

7. *If $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $n \leq s \leq 2n-1$, $0 \leq t \leq n-1$, $1+t \leq m \leq T-1$ and $h(x)$ is either zero or a unit in R''_n, then Res $(\mathcal{C}) = \langle (x+1)^s \rangle$ and Tor $(\mathcal{C}) = \langle (x+1)^m \rangle$.*

8. *If $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $1+t \leq m \leq n-1$ and $h(x)$ is a unit in R''_n, then Res $(\mathcal{C}) = \langle (x+1)^s \rangle$ and Tor $(\mathcal{C}) = \langle (x+1)^m \rangle$.*

9. *If $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x),\ 2u(x+1)^{m_1} \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $1+t \leq m_1 \leq T_1 - 1$ and $h(x)$ is a unit in R''_n, then Res $(\mathcal{C}) = \langle (x+1)^s \rangle$ and Tor $(\mathcal{C}) = \langle (x+1)^{n+m_1} \rangle$.*

10. *If $\mathcal{C} = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^m \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l+t < m < n$ and $h_1(x), h_2(x)$ are units in R''_n, then Res $(\mathcal{C}) = \langle (x+1)^s \rangle$ and Tor $(\mathcal{C}) = \langle (x+1)^m \rangle$.*

11. *If $\mathcal{C} = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ 2u(x+1)^{m_1} \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l+t < n\ t < m_1 < T_1$ and $h_1(x)$, $h_2(x)$ are units in R''_n, then Res $(\mathcal{C}) = \langle (x+1)^s \rangle$ and Tor $(\mathcal{C}) = \langle (x+1)^{n+m_1} \rangle$.*

Proof. Since Tor $(\mathcal{C})$ and Res $(\mathcal{C})$ are negacyclic codes over $\mathbb{Z}_4$, using Theorem 2.3.34, we may assume that their generators are of the form $(x+1)^i$, $1 \leq i \leq 2n$.

1. Suppose $\mathcal{C} = \langle u(x+1)^m \rangle$, $0 \leq m \leq 2n-1$. Let Tor $(\mathcal{C}) = \langle (x+1)^i \rangle$, $1 \leq i \leq 2n$. Then $u(x+1)^i \in \mathcal{C}$, which implies that $m \leq i$. On the other hand, since $u(x+1)^m \in \mathcal{C}$, $(x+1)^m \in$ Tor $(\mathcal{C})$. From this follows that $i \leq m$. Therefore $i = m$. So Tor $(\mathcal{C}) = \langle (x+1)^m \rangle$.

   Since $\mathcal{C}$ contains only multiples of u, Res $(\mathcal{C}) = \langle 0 \rangle$.

2. Suppose $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, $1 \leq s \leq n-1$. Then $\Phi(\mathcal{C}) = \langle (x+1)^s \rangle$, where Φ is the projection map defined in Chapter 6, Section 6.3.

   Let Tor $(\mathcal{C}) = \langle (x+1)^i \rangle$, $1 \leq i \leq 2n-1$. Then $u(x+1)^i \in \mathcal{C}$. From Theorem 6.3.11, s is the smallest integer such that $u(x+1)^s \in \mathcal{C}$. Then $s \leq i$. On the other hand, $u(x+1)^s \in \mathcal{C}$, which implies that $(x+1)^s \in$ Tor $(\mathcal{C})$. So $i \leq s$. Thus $i = s$ and so Tor $(\mathcal{C}) = \langle (x+1)^s \rangle$.

   Now assume that Res $(\mathcal{C}) = \langle (x+1)^i \rangle$. Then there exists some $q(x) \in R_n$ such that $d = (x+1)^i + uq(x) \in \mathcal{C}$. So $s \leq i$, as $\Phi(d) = (x+1)^i \in \Phi(\mathcal{C})$. Since $(x+1)^s + u(x+1)^t h(x) \in \mathcal{C}$, we have $(x+1)^s \in$ Res $(\mathcal{C})$. This implies that $i \leq s$. Therefore $i = s$, and hence Res $(\mathcal{C}) = \langle (x+1)^s \rangle$.

Rest of the results can be proved using similar lines of arguments. ■

The following theorem presents the size of negacyclic codes of length n over R.

Theorem 7.2.5. *Let $\mathcal{C}$ be a negacyclic code of length n over R.*

1. *If* $\mathcal{C} = \langle u(x+1)^m \rangle$, *where* $0 \leq m \leq 2n$, *then* $|\mathcal{C}| = 2^{2n-m}$.

2. *If* $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, *where* $0 \leq s \leq n-1$ *and* $0 \leq t \leq s-1$, *then* $|\mathcal{C}| = 4^{2n-s}$.

3. *If* $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, *where* $n \leq s \leq 2n-1$ *and* $0 \leq t \leq n-1$, *then*
$$|\mathcal{C}| = \begin{cases} 2^{2n-t} & \text{if } 0 \leq t < 2s-2n, \\ 4^{2n-s} & \text{if } t \geq 2s-2n. \end{cases}$$

4. *If* $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$, *where* $n+1 \leq s \leq 2n-1$ *and* $0 \leq t \leq s-n-1$, *then*
$$|\mathcal{C}| = \begin{cases} 2^{n-t} & \text{if } 0 \leq t < 2s-3n, \\ 4^{2n-s} & \text{if } 2s-3n \leq t < s-n. \end{cases}$$

5. *If* $\mathcal{C} = \big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)) \big\rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$ *and* $s-n < l+t < n$, *then*
$$|\mathcal{C}| = \begin{cases} 2^{2n-l-t} & \text{if } s-n < l+t < 2s-2n, \\ 4^{2n-s} & \text{if } l+t \geq 2s-2n. \end{cases}$$

6. *If* $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, *where* $1 \leq s \leq n-1$, $0 \leq t \leq s-1$, $1+t \leq m \leq T-1$ *and* $h(x)$ *is either zero or a unit in* R_n'', *then* $|\mathcal{C}| = 2^{4n-(m+s)}$.

7. *If* $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, *where* $n \leq s \leq 2n-1$, $0 \leq t \leq n-1$, $1+t \leq m \leq T-1$ *and* $h(x)$ *is either zero or a unit in* R_n'', *then* $|\mathcal{C}| = 2^{4n-(m+s)}$.

8. *If* $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^m \rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $1+t \leq m \leq n-1$ *and* $h(x)$ *is a unit in* R_n'', *then* $|\mathcal{C}| = 2^{4n-(m+s)}$.

9. *If* $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x),\ 2u(x+1)^{m_1} \rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $1+t \leq m_1 \leq T_1-1$ *and* $h(x)$ *is a unit in* R_n'', *then* $|\mathcal{C}| = 2^{3n-(m_1+s)}$.

10. *If* $\mathcal{C} = \big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^m \big\rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l+t < m < n$ *and* $h_1(x), h_2(x)$ *are units in* R''_n, *then* $|\mathcal{C}| = 2^{4n-(m+s)}$.

11. *If* $\mathcal{C} = \big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ 2u(x+1)^{m_1} \big\rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l+t < n$, $t < m_1 < T_1$ *and* $h_1(x)$, $h_2(x)$ *are units in* R''_n, *then* $|\mathcal{C}| = 2^{3n-(m_1+s)}$.

Proof. From Theorem 2.3.34, if C is a negacyclic code of length n over $\mathbb{Z}_4$, then $C = \langle (x+1)^i \rangle$, $0 \leq i \leq 2n$ and $|C| = 2^{2n-i}$. The cardinalities of Tor $(\mathcal{C})$ and Res $(\mathcal{C})$ can be computed using Theorem 7.2.4. By multiplying the cardinalities of Tor $(\mathcal{C})$ and Res $(\mathcal{C})$, we get $|\mathcal{C}|$ in each case. ∎

The following theorem provides negacyclic codes $\mathcal{C}$ such that $\mathcal{C} \subset A(\mathcal{C})$ over R. It can easily be seen that all the negacyclic codes $\mathcal{C}$ presented in Theorem 7.2.1 satisfy $\mathcal{C} \subset A(\mathcal{C})$ except the negacyclic codes of Type 2.0 and Type 3.0.

Theorem 7.2.6. *The negcyclic codes* $\mathcal{C}$ *of length* n *over* R *satisfying* $\mathcal{C} \subset A(\mathcal{C})$ *are:*

1. $\mathcal{C} = \langle u(x+1)^m \rangle$, *where* $0 \leq m \leq 2n$.

2. $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x) \rangle$, *where* $n \leq s \leq 2n-1$, $0 \leq t \leq n-1$ *and* $h(x)$ *is either zero or a unit in* R''_n.

3. $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$ *and* $h(x)$ *is a unit in* R''_n.

4. $\mathcal{C} = \big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)) \big\rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l < n$ *and* $h_1(x)$, $h_2(x)$ *are units in* R''_n.

5. $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, *where* $n \leq s \leq 2n-1$, $0 \leq t < m < T$, $h(x)$ *is either zero or a unit in* R''_n, *and* $s+m \geq 2n$.

6. $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^m \rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t < s-n$, $1+t \leq m \leq n-1$, $h(x)$ *is a unit in* R''_n, *and* $s+m \geq 2n$.

7. $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x),\ 2u(x+1)^{m_1} \rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $1+t \leq m_1 \leq T_1 - 1$, $h(x)$ *is a unit in* R''_n, *and* $s + m_1 \geq n$.

8. $\mathcal{C} = \big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^m \big\rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l+t < m < n$, $h_1(x)$, $h_2(x)$ *are units in* R''_n, *and* $s+m \geq 2n$.

9. $\mathcal{C} = \big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ 2u(x+1)^{m_1} \big\rangle$, *where* $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < l+t < n$, $t < m_1 < T_1$, $h_1(x)$, $h_2(x)$ *are units in* R''_n, *and* $s + m_1 \geq n$.

Proof. Each generator of the negacyclic code is self-orthogonal in all the above cases. In a non-principal negacyclic code, the two generators are orthogonal to each other only when $s+m \geq 2n$ or $s+m_1 \geq n$. ■

Now we consider the structure of negacyclic codes $\mathcal{C}$ such that $\mathcal{C} = A(\mathcal{C})$. Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ be a such negacyclic code of length n over R. Then from Theorem 7.2.6, $n \leq s < 2n$. Hence from Theorem 7.2.5, we have

$$|\mathcal{C}| = \begin{cases} 2^{2n-t} & \text{if } \ 0 \leq t < 2s-2n, \\ 2^{4n-2s} & \text{if } \ t \geq 2s-2n. \end{cases}$$

We know that $|\mathcal{C}^{\perp}| = |A(\mathcal{C})|$ and $|\mathcal{C}||\mathcal{C}^{\perp}| = 16^n$. So

$$|A(\mathcal{C})| = \begin{cases} 2^{2n+t} & \text{if } \ 0 \leq t < 2s-2n, \\ 2^{2s} & \text{if } \ t \geq 2s-2n. \end{cases}$$

Since $\mathcal{C} = A(\mathcal{C})$, $|\mathcal{C}| = |A(\mathcal{C})|$, which implies that $t = 0$ or $s = n$. Thus negacyclic codes of the form $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ satisfy $\mathcal{C} = A(\mathcal{C})$ when $t = 0$ or $s = n$. Further, we can show that there are no negacyclic codes of the forms $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$ and $\mathcal{C} = \big\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)) \big\rangle$ over R satisfying $\mathcal{C} = A(\mathcal{C})$. For if there is such a negacyclic code of the form $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$, where $n+1 \leq$

$s \leq 2n - 1$ and $0 \leq t \leq s - n - 1$, then from Theorem 7.2.5, we have

$$|\mathcal{C}| = \begin{cases} 2^{n-t} & \text{if } \ 0 \leq t < 2s - 3n, \\ 2^{4n-2s} & \text{if } \ t \geq 2s - 3n. \end{cases}$$

This implies that

$$|A(\mathcal{C})| = \begin{cases} 2^{3n+t} & \text{if } \ 0 \leq t < 2s - 3n, \\ 2^{2s} & \text{if } \ t \geq 2s - 3n. \end{cases}$$

Since $\mathcal{C} = A(\mathcal{C})$, $|\mathcal{C}| = |A(\mathcal{C})|$, which implies that $t = -n$ or $s = n$, which is a contradiction, as both cases are not possible.

Now we see non-principal negacyclic codes $\mathcal{C}$ over R such that $\mathcal{C} = A(\mathcal{C})$. Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $n \leq s \leq 2n-1$, $0 \leq m \leq T - t - 1$, and $h(x)$ is either zero or a unit in R_n'', be a non-principal such negacyclic code over R. Then from Theorem 7.2.5, we have $|\mathcal{C}| = 2^{4n-(m+s)}$, which implies that $|A(\mathcal{C})| = 2^{(m+s)}$. This in turn implies that $m = 2n - s$.

In the following theorem we list all negacylic codes of length n over R such that $\mathcal{C} = A(\mathcal{C})$.

Theorem 7.2.7. *The only negacyclic codes $\mathcal{C}$ of length n over R satisfying $\mathcal{C} = A(\mathcal{C})$ are:*

1. *$\mathcal{C} = \langle u \rangle$*

2. *$\mathcal{C} = \langle (x+1)^n + u(x+1)^t h(x) \rangle$, where $t \geq 0$ and $h(x)$ is either zero or a unit in R_n''.*

3. *$\mathcal{C} = \langle (x+1)^s + uh(x) \rangle$, where $n+1 \leq s \leq 2n-1$ and $h(x)$ is unit in R_n''.*

4. *$\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^{2n-s} \rangle$, where $n \leq s \leq 2n-1$, $0 \leq t \leq 2n-s-1$ and $h(x)$ is either zero or a unit in R_n''.*

5. *$\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^{2n-s} \rangle$, where $n < s \leq 2n-1$, $0 \leq t \leq$ min$\{2n-s, s-n\} - 1$ and $h(x)$ is a unit in R_n''.*

6. *$\mathcal{C} = \big\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^{2n-s} \big\rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $t + l < 2n - s$ and $h_1(x)$, $h_2(x)$ are units in R_n''.*

Proof. 1. Let $\mathcal{C} = \langle u \rangle$. Then $\mathcal{C} \subset A(\mathcal{C})$, as u is self-orthogonal. From Theorem 7.2.5, $|A(\mathcal{C})| = 4^n$. We know that $|\mathcal{C}||\mathcal{C}^\perp| = 16^n = |\mathcal{C}||A(\mathcal{C})|$, which implies that $|A(\mathcal{C})| = \frac{16^n}{4^n} = 4^n = |\mathcal{C}|$. Hence $\mathcal{C} = A(\mathcal{C})$.

2. Let $f(x) = (x+1)^n + u(x+1)^t h(x)$ and $\mathcal{C} = \langle f(x) \rangle$. Then $(f(x))^2 = \left((x+1)^n + u(x+1)^t h(x)\right)^2 = 0$, which implies that $\mathcal{C} \subset A(\mathcal{C})$. From Theorem 7.2.5, $|\mathcal{C}| = 4^n$. This implies that $|A(\mathcal{C})| = \frac{16^n}{4^n} = 4^n = |\mathcal{C}|$. Hence $\mathcal{C} = A(\mathcal{C})$.

3. Same as above.

4. Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^m \rangle$, where $n \le s \le 2n-1$, $0 \le m \le T-1$ and $h(x)$ is either zero or a unit in R''_n. Then from Theorem 7.2.5, we have $|\mathcal{C}| = 2^{4n-(m+s)}$, which implies that $|A(\mathcal{C})| = 2^{(m+s)}$. This in turn implies that $m = 2n - s$.

Rest of the results can be proved similarly. ∎

7.3 A Mass formula for the number of negacylic codes $\mathcal{C}$ of length 2^k over $\mathbb{Z}_4 + u\mathbb{Z}_4$ satisfying $\mathcal{C} = A(\mathcal{C})$

In this section, we determine a mass formula for number of negacyclic codes $\mathcal{C}$ of length n over R satisfying $\mathcal{C} = A(\mathcal{C})$. In view of this, recall Lemmas 6.4.1 and 6.4.2.

Lemma 7.3.1. *For* $0 \le a_1,\ a_2 \le 2n-1$, $\sum\limits_{s=a_2}^{a_1} (2n-s)2^{2n-s-1} = (2n-a_1-1)2^{2n-a_1} - (2n-a_2-2)2^{2n-a_2-1}$.

Lemma 7.3.2. *For* $0 \le b_1,\ b_2 \le 2n-1$, $\sum\limits_{t=b_2}^{b_1} (2n-s-t-1)2^{2n-s-t-2} = (2n-s-b_1-2)2^{2n-s-b_1-1} - (2n-s-b_2-3)2^{2n-s-b_2-2}$.

Theorem 7.3.3. *The number of negacyclic codes* $\mathcal{C}$ *of length* 2^k *over* R *satisfying* $\mathcal{C} = A(\mathcal{C})$ *is*

$$\left(5 \cdot 2^{n+2} - 9 \cdot 2^{e-n+1} + 9 \cdot 2^{\frac{n}{2}-1} + 2^{3n-2e-1}(12n - 9e - 18) + 25\right)/9\ ,$$

where $e = \lfloor (4n-2)/3 \rfloor$.

Proof. Let $\mathcal{M}_i$ and $\mathcal{M}$, respectively, denote the number of negacyclic codes $\mathcal{C}$ of length n satisfying $\mathcal{C} = A(\mathcal{C})$ of each type i and the total number of such negacyclic codes of length n over R. First we find the number of such negacyclic codes in each case.

1. Let $\mathcal{C} = \langle u \rangle$. Then the number of negacyclic codes $\mathcal{C}$ satisfying $\mathcal{C} = A(\mathcal{C})$ of this type is $\mathcal{M}_1 = 1$.

2. Let $\mathcal{C} = \langle f(x) \rangle$, where $f(x) = (x+1)^n + u(x+1)^t h(x)$, $0 \leq t \leq n-1$, $h(x)$ is either zero or unit in R''_n, be a principal such negacyclic code of length n over R.

   If $h(x) = 0$, then the number of such negacyclic codes of this type is $\mathcal{M}'_2 = 1$.

   If $h(x) \neq 0$, then from Theorem 6.3.11, we have $T = n$. Therefore deg $h(x) \leq n-t-1$. So the number of negacyclic codes is $\mathcal{M}''_2 = \sum\limits_{t=0}^{n-1} 2^{n-t-1} = 2^n - 1$. Therefore the total number of negacyclic codes of this type is $\mathcal{M}_2 = \mathcal{M}'_2 + \mathcal{M}''_2 = 1 + 2^n - 1 = 2^n$.

3. Let $\mathcal{C} = \langle (x+1)^s + uh(x) \rangle$, where $n+1 \leq s \leq 2n-1$, $h(x)$ is a unit in R''_n, be a such negacyclic code of length n over R. Since $h(x) \neq 0$, we have from Theorem 6.3.11 that $T = 2n - s$. Therefore deg $h(x) \leq 2n-s-1$. So the number of negacyclic codes is $\mathcal{M}_3 = \sum\limits_{s=n+1}^{2n-1} 2^{2n-s-1} = 2^{n-1} - 1$.

4. Let $\mathcal{C} = \langle (x+1)^s + u(x+1)^t h(x),\ u(x+1)^{2n-s} \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq 2n-s-1$ and $h(x)$ is either zero or a unit in R''_n, be a such negacyclic code of length n over R. Since $\mathcal{C}$ is a non-principal, we have $2n - s < T$. From Theorem 6.3.11, $T = \begin{cases} 2n-s+t & \text{if } 0 < t < 2s-2n, \\ s & \text{if } t \geq 2s-2n \end{cases}$. This implies that $t > 0$, which further implies that $s \leq 2n-2$.

   If $h(x) = 0$, then the number of such negacyclic codes of this type is $\mathcal{M}'_4 = n - 1$.

   If $h(x) \neq 0$, then we have deg $h(x) \leq 2n-s-t-1$. So the number of such negacyclic codes is

   $$\mathcal{M}''_4 = \sum_{s=n+1}^{2n-2} \sum_{t=1}^{2n-s-1} 2^{2n-s-t-1} = \sum_{s=n+1}^{2n-2} \left(2^{2n-s-1} - 1\right) = (2^{n-1} - 2) - (n-2) = 2^{n-1} - n.$$

   Therefore the total number of such negacyclic codes of this type is $\mathcal{M}_4 = 2^{n-1} - 1$.

5. Let $\mathcal{C} = \langle (x+1)^s + 2u(x+1)^t h(x),\ u(x+1)^{2n-s} \rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq \min\{2n-s, s-n\}-1$ and $h(x)$ is a unit in R''_n. As in case (4), we can see here that $t > 0$ and $s > \frac{3n}{2}$, as $2n - s < T_1 = \begin{cases} 2n-s+t & \text{if } \ 0 < t < 2s-3n, \\ s-n & \text{if } \ 2s-3n \leq t < s-n \end{cases}$. This implies that $s \leq 2n-2$. We also have that deg $h(x) \leq 2n-s-t-1$. So the number of such negacyclic codes is $\mathcal{M}_5 = \sum\limits_{s=\frac{3n}{2}+1}^{2n-2} \sum\limits_{t=1}^{2n-s-1} 2^{2n-s-t-1} = \sum\limits_{s=n+1}^{2n-2} (2^{2n-s-1}-1) = 2^{\frac{n}{2}-1} - \frac{n}{2} + 1$.

6. Let $\mathcal{C} = \left\langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)),\ u(x+1)^{2n-s} \right\rangle$, where $n+1 \leq s \leq 2n-1$, $0 \leq t \leq s-n-1$, $s-n < t+l < 2n-s$ and $h_1(x)$, $h_2(x)$ are units in R''_n. Since $s-n < l+t < 2n-s$, $s \leq \frac{3n}{2}-1$. From Theorem 6.3.12, deg $\ h_1(x) \leq T_1 - t - 1 = \begin{cases} l+n-s-1 & \text{if } \ s-n < l+t \leq 2s-2n, \\ s-n-t-1 & \text{if } \ 2s-2n < l+t < s-n, \end{cases}$ and deg $h_2(x) \leq 2n-s-t-l-1$. So the number of such negacyclic codes is

$$\begin{aligned}
\mathcal{M}_6 \ &= \ \sum_{s=n+1}^{e} \sum_{t=0}^{s-n-1} \left(\sum_{l=s-n+1}^{2s-2n-t} 2^{l-s+n-1} 2^{2n-s-t-l-1} + \sum_{l=2s-2n-t+1}^{2n-s-t-1} 2^{s-n-t-1} 2^{2n-s-t-l-1} \right) \\
&+ \ \sum_{s=e+1}^{\frac{3n}{2}-1} \sum_{t=0}^{3n-2s-2} \sum_{l=s-n+1}^{2n-s-t-1} 2^{l-s+n-1} 2^{2n-s-t-l-1}, \text{ where } e = \left\lfloor \frac{4n-2}{3} \right\rfloor \\
&= \ \sum_{s=n+1}^{e} \sum_{t=0}^{s-n-1} \left(\sum_{l=s-n+1}^{2s-2n-t} 2^{3n-2s-t-2} + \sum_{l=2s-2n-t+1}^{2n-s-t-1} 2^{n-2t-l-2} \right) \\
&+ \ \sum_{s=e+1}^{\frac{3n}{2}-1} \sum_{t=0}^{3n-2s-2} \sum_{l=s-n+1}^{2n-s-t-1} 2^{3n-2s-t-2} \\
&= \ \sum_{s=n+1}^{e} \sum_{t=0}^{s-n-1} (s-n-t) 2^{3n-2s-t-2} + \left(2^{3n-2s-t-2} - 2^{s-n-t-1} \right) \\
&+ \ \sum_{s=e+1}^{\frac{3n}{2}-1} \sum_{t=0}^{3n-2s-2} 2^{3n-2s-t-2} (2n-2s-t-1) \\
&= \ \sum_{s=n+1}^{e} \sum_{t=0}^{s-n-1} \left((3n-2s-t-1) - (4n-3s-2) \right) 2^{3n-2s-t-2} - 2^{s-n-t-1} \\
&+ \ \sum_{s=e+1}^{\frac{3n}{2}-1} \left(\sum_{t=0}^{3n-2s-2} 2^{3n-2s-t-2} (3n-2s-t-1) \right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{s=n+1}^{e} \Big(\big(2^{3n-2s-1}(3n-2s-1) - 2^{4n-3s-1}(4n-3s-2)\big) \\
&- (4n-3s-2)\left(2^{3n-2s-1} - 2^{4n-3s-1}\right) - \left(2^{s-n}-1\right)\Big) + \sum_{s=e+1}^{\frac{3n}{2}-1} \left(2^{3n-2s-1}(3n-2s-2)+1\right) \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1} \left((3n-2s-2)2^{3n-2s-1}+1\right) - \sum_{s=n+1}^{e} (4n-3s-2)2^{3n-2s-1} - 2^{s-n} \\
&= \sum_{s=n+1}^{\frac{3n}{2}-1} \left((3n-2s)2^{3n-2s-1} - 2^{3n-2s}+1\right) - \sum_{s=n+1}^{e} (n+1) - 3(3n-2s-1)2^{3n-2s-2} - 2^{s-n} \\
&= \frac{2^{n-1}(3n-8)+4}{9} - \frac{2^{n}-4}{3} + (n+1)\frac{2^{n-2}-2^{3n-2e-2}}{3} \\
&- \frac{2^{n-2}(3n-11) - 2^{3n-2e-2}(9n-6e-11)}{3} - (2^{e-n+1}-2) + (\frac{n}{2}-1) \\
&= \frac{2^{n+1} + 2^{3n-2e-1}(12n-9e-18)+25}{9} - 2^{e-n+1} + \frac{n}{2}
\end{aligned}
$$

Hence the total number of negacyclic codes $\mathcal{C}$ of length 2^k over R satisfying $\mathcal{C} = A(\mathcal{C})$ is

$$\mathcal{M} = \left(5 \cdot 2^{n+2} - 9 \cdot 2^{e-n+1} + 9 \cdot 2^{\frac{n}{2}-1} + 2^{3n-2e-1}(12n-9e-18)+25\right)/9 \, ,$$

where $e = \lfloor (4n-2)/3 \rfloor$. ∎

Now we consider the minimum distance of negacyclic codes of length n over R.

Theorem 7.3.4. *Let $d_H(\mathcal{C})$, $d_L(\mathcal{C})$ and $d_E(\mathcal{C})$ be the minimum Hamming, Lee and Euclidean distances of a negacyclic code $\mathcal{C}$ of length n over R, respectively. Then $d_H(\mathcal{C}) = d_H(Tor\ (\mathcal{C}))$, $d_L(\mathcal{C}) = d_L(Tor\ (\mathcal{C}))$ and $d_E(\mathcal{C}) = d_E(Tor\ (\mathcal{C}))$.*

Proof. Let $c = a + ub \in \mathcal{C}$ with $a \neq 0$. Then $uc = ua \in \mathcal{C}$. This implies that $a \in \text{Tor }(\mathcal{C})$. Since $d_H(\text{Tor }(\mathcal{C})) \leq wt_H(a) \leq wt_H(uc) \leq wt_H(c) \leq d_H(\mathcal{C})$, we have $d_H(\text{Tor }(\mathcal{C})) \leq wt_H(c)$ for all non-zero $c \in \mathcal{C}$. Thus $d_H(\text{Tor }(\mathcal{C})) \leq d_H(\mathcal{C})$.

On the other hand, $d_H(\mathcal{C}) \leq d_H(\text{Tor }(\mathcal{C}))$, as $u\text{Tor }(\mathcal{C}) \subseteq \mathcal{C}$ and $wt_H(u\text{Tor }(\mathcal{C})) = wt_H(\text{Tor }(\mathcal{C}))$. Hence $d_H(\mathcal{C}) = d_H(\text{Tor }(\mathcal{C}))$. The remaining parts of the theorem follow by similar arguments. ∎

Example 7.3.5. *For $n = 2$, $R_2 = \frac{R[x]}{\langle x^2+1 \rangle}$ has 24 ideals (negacyclic codes of length 2 over R), out of which 8 are self-dual ($\mathcal{C}^*$) and 15 are self-orthogonal ($\mathcal{C}^\dagger$). They are listed in the* *following in Table 7.1 along with their duals, size, minimum Hamming, Lee and Euclidean distances.*

Table 7.1: Negacyclic codes of length 2 over $\mathbb{Z}_4 + u\mathbb{Z}_4$

Negacyclic code $\mathcal{C}$	Annihilator $A(\mathcal{C})$	Size of $\mathcal{C}$	$d_H(\mathcal{C})$	$d_L(\mathcal{C})$	$d_E(\mathcal{C})$
$\mathcal{C}_1 = \langle 0 \rangle$	$\mathcal{C}_2$	1	0	0	0
$\mathcal{C}_2 = \langle 1 \rangle$	$\mathcal{C}_1$	256	1	1	1
$\mathcal{C}_3 = \langle u \rangle$	$\mathcal{C}_3^*$	16	1	1	1
$\mathcal{C}_4 = \langle u(x+1) \rangle$	$\mathcal{C}_{22}^\dagger$	8	1	2	2
$\mathcal{C}_5 = \langle u(x+1)^2 \rangle$	$\mathcal{C}_{19}^\dagger$	4	1	2	4
$\mathcal{C}_6 = \langle u(x+1)^3 \rangle$	$\mathcal{C}_{17}^\dagger$	2	2	4	8
$\mathcal{C}_7 = \langle (x+1) \rangle$	$\mathcal{C}_9$	64	1	2	2
$\mathcal{C}_8 = \langle (x+1)^2 \rangle$	$\mathcal{C}_8^*$	16	1	2	4
$\mathcal{C}_9 = \langle (x+1)^3 \rangle$	$\mathcal{C}_7^\dagger$	4	2	4	8
$\mathcal{C}_{10} = \langle (x+1) + u \rangle$	$\mathcal{C}_{16}$	64	1	2	2
$\mathcal{C}_{11} = \langle (x+1)^2 + u \rangle$	$\mathcal{C}_{11}^*$	16	1	2	4
$\mathcal{C}_{12} = \langle (x+1)^2 + u(x+1) \rangle$	$\mathcal{C}_{12}^*$	16	1	2	4
$\mathcal{C}_{13} = \langle (x+1)^2 + u(1+(x+1)) \rangle$	$\mathcal{C}_{13}^*$	16	1	2	4
$\mathcal{C}_{14} = \langle (x+1)^3 + u \rangle$	$\mathcal{C}_{14}^*$	16	1	2	2
$\mathcal{C}_{15} = \langle (x+1)^3 + u(x+1) \rangle$	$\mathcal{C}_{20}^\dagger$	8	1	2	4
$\mathcal{C}_{16} = \langle (x+1)^3 + 2u \rangle$	$\mathcal{C}_{10}^\dagger$	4	2	4	8
$\mathcal{C}_{17} = \langle (x+1),\ u \rangle$	$\mathcal{C}_6$	128	1	1	1
$\mathcal{C}_{18} = \langle (x+1)^2,\ u \rangle$	$\mathcal{C}_5$	64	1	1	1
$\mathcal{C}_{19} = \langle (x+1)^2,\ u(x+1) \rangle$	$\mathcal{C}_{23}$	32	1	2	2
$\mathcal{C}_{20} = \langle (x+1)^2 + u,\ u(x+1) \rangle$	$\mathcal{C}_{15}$	32	1	2	2
$\mathcal{C}_{21} = \langle (x+1)^3,\ u \rangle$	$\mathcal{C}_4$	32	1	1	1
$\mathcal{C}_{22} = \langle (x+1)^3,\ u(x+1) \rangle$	$\mathcal{C}_{22}^*$	16	1	2	2
$\mathcal{C}_{23} = \langle (x+1)^3,\ 2u \rangle$	$\mathcal{C}_{19}^\dagger$	8	1	2	4
$\mathcal{C}_{24} = \langle (x+1)^3 + 2u,\ u(x+1) \rangle$	$\mathcal{C}_{24}^*$	16	1	2	2

7.4 Computational Results

We conducted a computer search to exhaustively search for all negacyclic codes of length 2^k over R for small values of k of certain types. We also looked at their $\mathbb{Z}_4$-images under the Gray map $\phi : R^n \to \mathbb{Z}_4^{2n}$ such that $\phi(\overline{a} + u\overline{b}) = (\overline{b}, \overline{a} + \overline{b})$, $\overline{a}, \overline{b} \in \mathbb{Z}_4^n$, defined in Chapter 5. Clearly, the length of the image of a code of length n over R under this map becomes $2n$. Comparing the codes we have obtained with the database of $\mathbb{Z}_4$-codes [1, 8], we found that we obtained some new linear codes over $\mathbb{Z}_4$. They are added to the database of $\mathbb{Z}_4$ codes. We considered both the Lee weight and the Euclidean weight of the codes over $\mathbb{Z}_4$. In Table 7.2, we present a subset of the new codes we have obtained so far. The minimum Lee and Euclidean weights are denoted by d_L and d_E, respectively. In many cases $\mathbb{Z}_4$ images are cyclic. Once we obtain the $\mathbb{Z}_4$ image of a negacyclic code over R, we can also apply the well-known Gray map to obtain its binary image. We found that in many cases the binary images are linear. Some of them are Type II codes, which are marked with $*$ in Table 7.2.

7.5 Conclusion

In this chapter, we have obtained the duals of negacyclic codes of length 2^k over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. We have classified negacyclic codes $\mathcal{C}$ of length 2^k over R satisfying $\mathcal{C} \subset A(\mathcal{C})$ and the codes satisfying $\mathcal{C} = A(\mathcal{C})$. A mass formula for the number of negacyclic codes $\mathcal{C}$ of length 2^k over R satisfying $\mathcal{C} = A(\mathcal{C})$ has been derived. A number of negacyclic codes over R that lead to new $\mathbb{Z}_4$-linear codes are obtained by a computational search that made use of their structural properties determined in this work.

Table 7.2: Some negacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and their $\mathbb{Z}_4$ images

Length n	**Type/Parameters**	**Generator**	**$\mathbb{Z}_4$-Parameters**	**Comments**
8	$T1 : m = 1$	$u(x+1)$	$[16, 4^7 2^1, d_L = 4]$	Cyclic
8	$T1 : m = 5$	$u(x+1)^5$	$[16, 4^3 2^5, d_E = 8]$	Cyclic
8	$T1 : m = 1$	$u(x+1)$	$[16, 4^7 2^1, d_E = 4]$	Cyclic
8	$T2.0 : s = 5, h = 0$	$(x+1)^5$	$[16, 4^3 2^5, d_E = 4]$	Linear
8	$T2.0 : s = 5, t = 1, h = 1$	$(x+1)^5 + u(x+1)$	$[16, 4^{10} 2^6, d_E = 4]$	Linear
8	$T2.1 : s = 9, t = 7, h = 1$	$(x+1)^9 + u(x+1)^7$	$[16, 4^1 2^{14}, d_L = 4]$	Cyclic, Linear
8	$T2.1 : s = 9, t = 5, h = 1$	$(x+1)^9 + u(x+1)^5$	$[16, 4^3 2^{12}, d_E = 8]^*$	Cyclic, Linear
8	$T2.1 : s = 10, t = 4, h = 1$	$(x+1)^{10} + u(x+1)^4$	$[16, 4^4 2^{10}, d_E = 4]$	Cyclic, Linear
16	$T1 : m = 1$	$u(x+1)^1$	$[32, 4^{15} 2^1, d_L = 4]$	Cyclic, Linear
16	$T1 : m = 10$	$u(x+1)^{10}$	$[32, 4^6 2^{10}, d_E = 8]$	Cyclic, Linear
16	$T2.0 : s = 9, h = 0$	$(x+1)^9$	$[32, 4^7 2^9, d_E = 4]$	Linear
16	$T2.1 : s = 17, t = 12, h = 1$	$(x+1)^{17} + u(x+1)^{12}$	$[32, 4^4 2^{27}, d_L = 4]$	Cyclic, Linear
16	$T2.1 : s = 17, t = 9, h = 1$	$(x+1)^{17} + u(x+1)^9$	$[32, 4^4 2^{24}, d_E = 8]^*$	Cyclic, Linear
16	$T2.1 : s = 16, t = 9, h = 1$	$(x+1)^{16} + u(x+1)^9$	$[32, 4^7 2^{25}, d_E = 4]$	Cyclic, Linear
16	$T2.1 : s = 12, t = 2, h = 1$	$(x+1)^{12} + u(x+1)^2$	$[32, 4^{14} 2^{12}, d_E = 4]$	Cyclic, Linear
32	$T1 : m = 24$	$u(x+1)^{24}$	$[64, 4^8 2^4, d_L = 4]$	Cyclic, Linear
32	$T1 : m = 24$	$u(x+1)^{24}$	$[64, 4^6 2^4, d_E = 8]$	Cyclic, Linear

Cyclic: The $\mathbb{Z}_4$ image is cyclic; Linear: The binary Gray image of the code is linear

The two negacyclic codes of length 8 and 16 of type 2.1 generated by $(x+1)^9 + u(x+1)^5$ and $(x+1)^{17} + u(x+1)^9$, respectively, are Type II codes over R. They are denoted by $*$ in above table.

Chapter 8

Conclusion and future scope

The study of codes over finite fields is very old. The ring linear coding on other hand is rather young. Unlike the codes over finite fields, codes over rings have not been well established both in theoretical and practical aspects. However, some studies proved that the codes over rings are promising and can produce many good codes with better parameters than the codes over fields.

The main purpose of this thesis is a systematic study of algebraic codes over some non-chain extensions of $\mathbb{Z}_4$ and searching for good codes over them. In the first part (Chapters 3 and 4) of the thesis, we introduced two rings structures $\mathbb{Z}_4 + v\mathbb{Z}_4$, $v^2 = v$ and $\mathbb{Z}_4 + w\mathbb{Z}_4$, $w^2 = 2w$ in coding theory, and explored linear and self-dual codes over these rings. We have proposed few construction methods for constructing self-orthogonal and self-dual codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ and $\mathbb{Z}_4 + w\mathbb{Z}_4$. In the later part of the thesis, an extensive study of cyclic and negacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2 = 0$ has been done. We obtained all cyclic and negacyclic codes of both odd and even lengths over $\mathbb{Z}_4 + u\mathbb{Z}_4$, and classified them. Using the general form of generators of cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, we have given a minimal spanning set for a cyclic code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and determined a formula for its rank. It has been shown that the cyclic codes and negacyclic codes of same odd lengths over a finite local ring are isomorphic through a mapping. So we mainly focused on negacyclic codes of even length over $\mathbb{Z}_4 + u\mathbb{Z}_4$, in particular, of length 2^k. A complete classification of negacyclic codes of length 2^k is provided. The dual of each of such negacyclic codes is obtained. This allowed us to list all negacyclic codes $\mathcal{C}$ of length 2^k over $\mathbb{Z}_4 + u\mathbb{Z}_4$ satisfying $\mathcal{C} \subset A(\mathcal{C})$ and $\mathcal{C} = A(\mathcal{C})$.

We have also enumerated the total number of negacyclic codes of length 2^k over $\mathbb{Z}_4 + u\mathbb{Z}_4$. This was accomplished by computing the total number of negacyclic codes of length 2^k of each type. The classification of negacylic codes led to some new good $\mathbb{Z}_4$-codes as Gray images of negacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ via the Gray map on $\mathbb{Z}_4 + u\mathbb{Z}_4$.

8.1 Scope for future research

The following are some possible research directions for the future work that we can suggest on the basis of the results obtained in this thesis.

1. The study of codes over these non-chain extensions of $\mathbb{Z}_4$ can be generalized to non-chain extensions of $\mathbb{Z}_q$, q a prime power. This study may lead to some new codes with better parameters.

2. As an application of the study of codes over the rings described in this thesis, DNA codes and quantum codes can be considered over these rings.

3. Skew codes over these non-chain extensions of $\mathbb{Z}_4$ could be another interesting and challenging area.

4. One can also consider the rings of the form $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$, where $u^2 = 0$, $v^2 = 0$, $uv = vu$; $u^2 = 0$, $v^2 = v$, $uv = vu$ and $u^2 = u$, $v^2 = v$, $uv = vu$ for studying of codes over them.

5. Most of the work carried out here is about the structural properties and enumeration of codes. Developing encoding and decoding algorithms for the same will be an interesting problem.

Bibliography

[1] Database of $\mathbb{Z}_4$ codes. [online] Z4Codes.info, Accessed on 28 January 2015.

[2] Abualrub, T., Ghrayeb, A., and Oehmke, R. H. A mass formula and rank of $\mathbb{Z}_4$ cyclic codes of length 2^e. *IEEE Trans. Inform. Theory 50*, 12 (2004), 3306–3312.

[3] Abualrub, T., and Oehmke, R. Cyclic codes of length 2^e over $\mathbb{Z}_4$. *Discrete Appl. Math. 128*, 1 (2003), 3–9.

[4] Abualrub, T., and Oehmke, R. On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e. *IEEE Trans. Inform. Theory 49*, 9 (2003), 2126–2133.

[5] Abualrub, T., and Siap, I. Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$. *Des. Codes Cryptogr. 42*, 3 (2007), 273–287.

[6] Alfaro, R., and Dhul-Qarnayn, K. Constructing self-dual codes over $\mathbb{F}_p[u]/\langle u^t \rangle$. *Des. Codes Cryptogr. 74*, 2 (2015), 453–465.

[7] Atiyah, M. F., and Macdonald, I. G. *Introduction to Commutative Algebra.* Addison Wesely Publishing Co., Massachusets, Reading, 1969.

[8] Aydin, N., and Asamov, T. S. V. E. T. A. N. A Database of $\mathbb{Z}_4$–codes. *J. Combin. Inform. Sys. Sci. 34*, 1–4 (2009), 1–12.

[9] Bachoc, C. Applications of coding theory to the construction of modular lattices. *J. Combin. Theory Ser. A 78*, 1 (1997), 92–119.

[10] Bakshi, G. K., and Raka, M. Minimal cyclic codes of length p^nq. *Finite Fields Appl. 9*, 4 (2003), 432–448.

[11] Bakshi, G. K., and Raka, M. A class of constacyclic codes over a finite field. *Finite Fields Appl. 18*, 2 (2012), 362–377.

[12] Bakshi, G. K., and Raka, M. Self-dual and self-orthogonal negacyclic codes of length $2p^n$ over a finite field. *Finite Fields Appl. 19*, 1 (2013), 39–54.

[13] Bannai, E., Dougherty, S. T., Harada, M., and Oura, M. Type II codes, even unimodular lattices, and invariant rings. *IEEE Trans. Inform. Theory 45*, 4 (1999), 1194–1205.

[14] Berlekamp, E. R. *Algebraic Coding Theory.* McGraw Hill Co., New York, 1968.

[15] Berlekamp, E. R. Negacyclic codes for the Lee metric. In *Combinatorial Mathematics and Its Applications (Proc. Conference, University of North Carolina, Chapel Hill, NC, 1967)* (1968), pp. 298–316.

[16] Berman, S. Semisimple cyclic and abelian codes. II. *Cybernet. Systems Anal. 3*, 3 (1967), 17–23.

[17] Bhaintwal, M., and Wasan, S. K. On quasi-cyclic codes over $\mathbb{Z}_q$. *Appl. Algebra Engrg. Comm. Comput. 45*, 20 (2009), 459–480.

[18] Bhaintwal, M., and Wasan, S. K. Generalized Reed–Muller codes over $\mathbb{Z}_q$. *Des. Codes Cryptogr. 54*, 2 (2010), 149–166.

[19] Bhandari, M. C., Gupta, M. K., and Lal, A. K. On $\mathbb{Z}_4$–simplex codes and their Gray images. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes.* Springer, 1999, pp. 170–179.

[20] Bhat, H. *Linear Sequential Systems over Residue Class Polynomial Rings: Theory and Applications.* PhD thesis, 1985.

[21] Blackford, T. Cyclic codes over $\mathbb{Z}_4$ of oddly even length. *Discrete Appl. Math. 128*, 1 (2003), 27–46.

[22] Blackford, T. Negacyclic codes over $\mathbb{Z}_4$ of even length. *IEEE Trans. Inform. Theory 49*, 6 (2003), 1417–1424.

[23] Blake, I. F. Codes over certain rings. *Inform. and Control 20* (1972), 396–404.

[24] Blake, I. F. Codes over integer residue rings. *Inform. and Control 29* (1975), 295–300.

[25] Bonnecaze, A., Solé, P., and Calderbank, A. R. Quaternary quadratic residue codes and unimodular lattices. *IEEE Trans. Inform. Theory 41* (1995), 366–377.

[26] Bonnecaze, A., and Udaya, P. Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inform. Theory 45*, 4 (1999), 1250–1255.

[27] Bose, R. C., and Ray-Chaudhuri, D. K. On a class of error correcting binary group codes. *Information and control 3*, 1 (1960), 68–79.

[28] Boztaş, S., Hammons, R., and Kumar, P. V. 4-phase sequences with near-optimum correlation properties. *IEEE Trans. Inform. Theory 38* (1992), 1101–1113.

[29] Brualdi, R. A., Graves, J. S., and Lawrence, K. M. Codes with a poset metric. *Discrete Mathematics 147*, 1 (1995), 57–72.

[30] Calderbank, A. R., Cameron, P. J., Kantor, W. M., and Seidel, J. J. $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *In: Proc. London Math. Soc. 3* (1997), 436–480.

[31] Calderbank, A. R., and Sloane, N. J. A. Modular and p-adic cyclic codes. *Des. Codes Cryptogr. 6* (1995), 21–35.

[32] Carlet, C. $\mathbb{Z}_{2^k}$-linear codes. *IEEE Trans. Inform. Theory 44* (1998), 1543–1547.

[33] Castagnoli, G., Massey, J. L., Schoeller, P., Von Seemann, N., et al. On repeated-root cyclic codes. *IEEE Trans. Inform. Theory 37*, 2 (1991), 337–342.

[34] Claasen, H. L. *Studies of the Multiplications in $GF(q)[x]/(a(x))$*. PhD thesis, 1976.

[35] Conway, J. H., and Sloane, N. J. A. Self-dual codes over the intgers modulo 4. *J. Combinatorial Theory 62* (1993), 30–45.

[36] Dass, B. K., and Muttoo, S. K. A note on Reed–Muller codes. *Discrete Appl. Math. 2*, 4 (1980), 345–348.

[37] Dass, B. K., and Tyagi, V. On duals of GRM codes of order $r + (r + 1)m, s$. *Bull. Calcutta Math. Soc 80* (1988), 270–277.

[38] Dass, B. K., and Wasan, S. K. A note on quasi-cyclic codes. *Int. J. of Electron. 54*, 1 (1983), 91–94.

[39] Dinh, H. Q. Negacyclic codes of length 2^s over Galois rings. *IEEE Trans. Inform. Theory 51*, 12 (2005), 4252–4262.

[40] Dinh, H. Q. Complete distances of all negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$. *IEEE Trans. Inform. Theory 53*, 1 (2007), 147–161.

[41] Dinh, H. Q. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. *Finite Fields Appl. 14*, 1 (2008), 22–40.

[42] Dinh, H. Q. Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inform. Theory 55*, 4 (2009), 1730–1740.

[43] Dinh, H. Q. Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *J. Algebra 324*, 5 (2010), 940–950.

[44] Dinh, H. Q. Repeated-root constacyclic codes of length $2p^s$. *Finite Fields Appl. 18*, 1 (2012), 133–143.

[45] Dinh, H. Q., and Lopez-Permouth, S. Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inform. Theory 50* (2004), 1728–1744.

[46] Dougherty, S., Saltürk, E., and Szabo, S. Codes over rings of order 16. *ACM Commun. Comput. Algebra 49*, 1 (2015), 15–15.

[47] Dougherty, S. T., Gupta, M. K., and Shiromoto, K. On generalized weights for codes over $\mathbb{Z}_k$. *Australas. J. Combin. 31* (2005), 231–248.

[48] Dougherty, S. T., Kim, J.-L., Kulosman, H., and Liu, H. Self-dual codes over commutative Frobenius rings. *Finite Fields Appl. 16*, 1 (2010), 14–26.

[49] Dougherty, S. T., and Ling, S. Cyclic codes over $\mathbb{Z}_4$ of even length. *Des. Codes Cryptogr. 39*, 2 (2006), 127–153.

[50] Dougherty, S. T., and Skriganov, M. M. MacWilliams duality and the Rosenbloom–Tsfasman metric. *Mosc. Math. J. 2*, 1 (2002), 81–97.

[51] Falkner, G., Kowol, B., Heise, W., and Zehendner, E. On the existence of cyclic optimal codes. *Atti Sem. Mat. Fis. Univ. Modena 28* (1979), 326–341.

[52] Fujiwara, E. *Code design for dependable systems: theory and practical applications.* John Wiley & Sons, 2006.

[53] Gabidulin, E. M. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii 21*, 1 (1985), 3–16.

[54] Gao, J., Gao, Y., and Fu, F.-W. On linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$. *arXiv preprint arXiv:1402.6771* (2014).

[55] Golay, M. J. Notes on digital coding. vol. 37, pp. 657–657.

[56] Gupta, M. K., Bhandari, M. C., and Lal, A. K. On linear codes over $\mathbb{Z}_{2^s}$. *Des. Codes Cryptogr. 36*, 3 (2005), 227–244.

[57] Hamming, R. W. Error detecting and error corrceting codes. *Bell Syst. Tech. J. 29* (1950), 147–160.

[58] Hammons, A. R. Jr., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., and Solé, P. The $\mathbb{Z}_4$ linearity of Kerdock, Preparata Goethals and related codes. *IEEE Trans. Inform. Theory 40* (1994), 301–319.

[59] Harada, M. The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes. *Finite Fields Appl. 3*, 2 (1997), 131–139.

[60] Hocquenghem, A. Codes correcteurs derreurs. *Chiffres (paris) 2*, 147-156 (1959), 116.

[61] Huffman, W. C., and Pless, V. *Fundamentals of error-correcting codes.* Cambridge university press, 2003.

[62] Hughes, G. Constacyclic codes, cocycles and a $(u + v|u - v)$ construction. *IEEE Trans. Inform. Theory 46* (2000), 674–680.

[63] Interlando, J. C., Palazzo Jr, R., and Elia, M. On the decoding of Reed–Solomon and BCH codes over integer residue rings. *IEEE Trans. Inform. Theory 43*, 3 (1997), 1013–1021.

[64] Janwa, H., and Lal, A. K. On the generalized Hamming weights of cyclic codes. *IEEE Trans. Inform. Theory 43*, 1 (1997), 299–308.

[65] Jensen, J. M. Cyclic concatenated codes with constacyclic outer codes. *IEEE Trans. Inform. Theory 40* (1992), 951–954.

[66] Jensen, J. M. A class of constacyclic codes. *IEEE Trans. Inform. Theory 38* (1994), 950–959.

[67] Kanwar, P., and Lopez-permouth, S. R. Cyclic codes over integers modulo p^m. *Finite Fields Appl. 3* (1997), 334–352.

[68] Kewat, P. K., Ghosh, B., and Pattanayak, S. Cyclic codes over the ring $\mathbb{Z}_p[u, v]/\langle u^2, v^2, uv - vu\rangle$. *Finite Fields Appl. 34* (2015), 161–175.

[69] Kim, J.-L. New extremal self-dual codes of lengths 36, 38, and 58. *IEEE Trans. Inform. Theory 47*, 1 (2001), 386–393.

[70] Kim, J.-L., and Lee, Y. Euclidean and Hermitian self-dual MDS codes over large finite fields. *J. Combin. Theory Ser. A 105*, 1 (2004), 79–95.

[71] Kim, J.-L., and Lee, Y. Construction of MDS self-dual codes over Galois rings. *Des. Codes Cryptogr. 45*, 2 (2007), 247–258.

[72] Kim, J.-L., and Lee, Y. An efficient construction of self-dual codes. *Bull. Korean Math. Soc. 52*, 3 (2015), 915–923.

[73] Lee, C. Some properties of nonbinary error-correcting codes. *IRE Trans. Inform. Theory 4*, 2 (1958), 77–82.

[74] Lee, H., and Lee, Y. Construction of self-dual codes over finite rings $\mathbb{Z}_{p^m}$. *J. Combin. Theory Ser. A 115*, 3 (2008), 407–422.

[75] Ling, S., Niederreiter, H., and Solé, P. On the algebraic structure of quasi-cyclic codes IV: repeated roots. *Des. Codes Cryptogr. 38*, 3 (2006), 337–361.

[76] Ling, S., and Solé, P. On the algebraic structure of quasi-cyclic codes. I. finite fields. *IEEE Trans. Inform. Theory 47*, 7 (2001), 2751–2760.

[77] Ling, S., and Solé, P. On the algebraic structure of quasi-cyclic codes II: chain rings. *Des. Codes Cryptogr. 30*, 1 (2003), 113–130.

[78] Ling, S., and Solé, P. On the algebraic structure of quasi-cyclic codes III: generator theory. *IEEE Trans. Inform. Theory 51*, 7 (2005), 2692–2700.

[79] Liu, Y., Shi, M., and Solé, P. Quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$. In *Arithmetic of Finite Fields*. Springer, 2014, pp. 204–211.

[80] Luo, R., and Parampalli, U. Self-dual cyclic codes over??? 4+ u??? 4. In *2015 Seventh International Workshop on Signal Design and its Applications in Communications (IWSDA)* (2015), IEEE, pp. 57–61.

[81] MacWilliams, F. J., and Sloane, N. J. A. *The Theory of Error Correcting Codes*. North Holland, 1977.

[82] Martin, W. J., and Stinson, D. R. Association schemes for ordered orthogonal arrays and (t, m, s)-nets. *Canad. J. Math. 51*, 2 (1999), 326–346.

[83] Martínez-Moro, E., and Rúa, I. F. Multivariable codes over finite chain rings: serial codes. *SIAM J. Discrete Math. 20*, 4 (2006), 947–959.

[84] Martínez-Moro, E., and Rúa, I. F. On repeated-root multivariable codes over a finite chain ring. *Des. Codes Cryptogr. 45*, 2 (2007), 219–227.

[85] Martínez-Moro, E., and Szabo, S. On codes over local Frobenius non-chain rings of order 16. *Noncommutative Rings and Their Applications 634* (2015), 227.

[86] Martínez-Moro, E., Szabo, S., and Yildiz, B. Linear codes over $\mathbb{Z}_4[x]/\langle x^2 + 2x\rangle$. *Int. J. Inf. Coding Theory 3*, 1 (2015), 78–96.

[87] Massey, J. L., Costello Jr, D. J., and Justesen, J. Polynomial weights and code constructions. *IEEE Trans. Inform. Theory 19*, 1 (1973), 101–110.

[88] McDonald, B. R. *Finite Rings with Identity.* Marcel Dekker, New York, 1974.

[89] Nechaev, A. A. Kerdock codes in a cyclic form. *Diskret Mat. 1* (1989), 123–139.

[90] Norton, G. H., and Salăgean, A. On the structures of linear and cyclic codes over finite chain rings. *Appl. Algebra Engrg. Comm. Comput. 10* (2000), 489–506.

[91] Özen, M., and Siap, I. On the structure and decoding of linear codes with respect to the Rosenbloom–Tsfasman metric. *Selcuk J. Appl. Math. 5*, 2 (2004), 25–31.

[92] Özen, M., and Siap, I. Linear codes over $\mathbb{F}_q[u]/\langle u^s\rangle$ with respect to the Rosenbloom–Tsfasman metric. *Des. Codes Cryptogr. 38*, 1 (2006), 17–29.

[93] Özen, M., and Siap, I. Codes over Galois rings with respect to the Rosenbloom–Tsfasman metric. *J. Franklin Inst. 344*, 5 (2007), 790–799.

[94] Özen, M., Uzekmek, F. Z., Aydin, N., and Özzaim, N. T. Cyclic and some constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$. *Finite Fields Appl. 38* (2016), 27–39.

[95] Pless, V., and Huffman, W. C. *Handbook of coding theory.* Elsevier Science Inc., 1998.

[96] Pless, V., and Qian, Z. Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory 42* (1996), 1594–1600.

[97] Pless, V., Solé, P., and Qian, Z. Cyclic self–dual $\mathbb{Z}_4$–codes. *Finite Fields Appl. 3*, 1 (1997), 48–69.

[98] Prange, E. *Cyclic Error-Correcting codes in two symbols.* Air Force Cambridge Research Center, 1957.

[99] Prange, E. Some cyclic error-correcting codes with simple decoding algorithms. *Air Force Cambridge Research Center-TN-58-156* (1958).

[100] Raghavendran, R. Finite associative rings. *Compos. Math. 21* (1969), 195–229.

[101] Rajan, B. S., and Siddiqi, M. U. Transform domain characterization of cyclic codes over $\mathbb{Z}_m$. *Applicable Algebra in Engineering, Communication and Computing 5*, 5 (1994), 261–275.

[102] Reed, I. S. A class of multiple-eror-correcting codes and decoding scheme. *IEEE Trans. Inform. Theory 4* (1954), 38–49.

[103] Reed, I. S., and Solomon, G. Polynomial codes over certain finite fields. *J. Society for Ind. Appl. Math. 8*, 2 (1960), 300–304.

[104] Rosenbloom, M. Y., and Tsfasman, M. A. Codes for the m-metric. *Problemy Peredachi Informatsii 33*, 1 (1997), 55–63.

[105] Roth, R. M., and Seroussi, G. On cyclic MDS codes of length q over GF(q). *IEEE Trans. Inform. Theory 32*, 2 (1986), 284–285.

[106] Satyanarayana, C. Lee metric codes over integer residue rings. *IEEE Trans. Inform. Theory 25* (1979), 250–254.

[107] Shankar, P. On BCH codes over arbitrary integer rings. *IEEE Trans. Inform. Theory 25*, 4 (1979), 480–483.

[108] Shannon, C. E. A mathematical theory of communication. *Bell Syst. Tech. J. 27* (1948), 379–423, 623–656.

[109] Sharma, A. Repeated-root constacyclic codes of length $l^t p^s$ and their dual codes. *Cryptography and Communications 7*, 2 (2015), 229–255.

[110] Shi, M. J., Solé, P., and Wu, B. Cyclic codes and the weight enumerator of linear codes over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$. *Applied and Computational Mathematics 12*, 2 (2013), 247–255.

[111] Siap, I. The complete weight enumerator for codes over $\mathrm{M}_{n\times s}(\mathbb{F}_q)$. In *Cryptography and coding*, vol. 2260 of *LNCS*. Springer, Berlin, 2001, pp. 20–26.

[112] Siap, I. A MacWilliams type identity. *Turkish J. Math. 26*, 4 (2002), 465–473.

[113] Siap, I., and Özen, M. The complete weight enumerator for codes over $\mathrm{M}_{n\times s}(\mathrm{R})$. *Appl. Math. Lett. 17*, 1 (2004), 65–69.

[114] Singh, A. K., and Kewat, P. K. On cyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^k\rangle$. *Des. Codes Cryptogr. 74*, 1 (2015), 1–13.

[115] Skriganov, M. M. Uniform distributions, error-correcting codes, and interpolations over finite fields. Preprint, 1998.

[116] Skriganov, M. M. Coding theory and uniform distributions. *Algebra i Analiz 13*, 2 (2001), 191–239.

[117] Sobhani, R., and Molakarimi, M. Some results on cyclic codes over the ring $\mathrm{R}_{2,m}$. *Turkish J. Math. 37*, 6 (2013), 1061–1074.

[118] Solé, P. A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties. In *International Colloquium on Coding Theory and Applications* (1988), Springer, pp. 193–201.

[119] Spiegel, E. Codes over $\mathbb{Z}_m$. *Inform. and Control 35* (1977), 48–51.

[120] Spiegel, E. Codes over $\mathbb{Z}_m$, Revisited. *Inform. and Control 37* (1978), 100–104.

[121] SUNDAR RAJAN, B. *Transform Domain Study of Cyclic and Abelian Codes over Residue Class Rings.* PhD thesis, PhD thesis, Indian Institute of Technology, Kanpur, India, 1989.

[122] TANG, L.-Z., SOH, C. B., AND GUNAWAN, E. A note on the q-ary image of a q^m-ary repeated-root cyclic code. *IEEE Trans. Inform. Theory 43*, 2 (1997), 732–737.

[123] UDAYA, P. *Polyphase and frequency hopping sequences obtained from finite rings.* PhD thesis, 1992.

[124] UDAYA, P., AND BONNECAZE, A. Decoding of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inform. Theory 45*, 6 (1999), 2148–2157.

[125] UDAYA, P., AND SIDDIQI, M. Large linear complexity sequences over z 4 for quadriphase modulated communication systems having good correlation properties. In *Information Theory, 1991 (papers in summary form only received), Proceedings. 1991 IEEE International Symposium on (Cat. No. 91CH3003-1)* (1991), IEEE, pp. 386–386.

[126] UDAYA, P., AND SIDDIQI, M. Optimal and suboptimal quadriphase sequences derived from maximal length sequences over z _ {{\ bf 4}}. *Applicable Algebra in Engineering, Communication and Computing 9*, 2 (1998), 161–191.

[127] UDAYA, P., AND SIDDIQI, M. U. Optimal biphase sequences with large linear complexity derived from sequences over z 4. *IEEE Transactions on Information Theory 42*, 1 (1996), 206–216.

[128] VAN LINT, J. H. Repeated-root cyclic codes. *IEEE Trans. Inform. Theory 37*, 2 (1991), 343–345.

[129] WAN, Z. X. *Quaternary Codes.* World Scientific, Singapore, 1997.

[130] WAN, Z. X. Cyclic codes over Galois rings. *Algebra Colloq. 06* (1999), 291–304.

[131] WAN, Z. X. *Finite Fields and Galois Rings.* World Scientific, Singapore, 2012.

[132] Wasan, S. K. On codes over $\mathbb{Z}_m$. *IEEE Trans. Inform. Theory 28* (1982), 117–120.

[133] Wei, V. K. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory 37*, 5 (1991), 1412–1418.

[134] Wolfmann, J. Binary images of cyclic codes over $\mathbb{Z}_4$. *Electron. Notes Discrete Math. 6* (2001), 281–286.

[135] Wood, J. A. Duality for modules over finite rings and applications to coding theory. *Amer. J. Math. 121* (1999), 555–575.

[136] Yildiz, B., and Aydin, N. On cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and their $\mathbb{Z}_4$–images. *Int. J. Inf. Coding Theory 2*, 4 (2014), 226–237.

[137] 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. 347*, 10 (2010), 1888–1894.

[138] 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 Cryptogr. 58*, 3 (2011), 221–234.

[139] Yildiz, B., and Karadeniz, S. Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$: MacWilliams identities, projections, and formally self-dual codes. *Finite Fields Appl. 27* (2014), 24–40.

[140] Zhu, S., Wang, Y., and Shi, M. Some results on cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inform. Theory 56*, 4 (2010), 1680–1684.

[141] Zhu, S., and Xu, H. MacWilliams identities over $\mathrm{M}_{n\times s}(\mathbb{Z}_4)$ with respect to the RT metric. *J. Appl. Math. Inform. 26*, 1-2 (2008), 107–120.

[142] Zimmermann, K.-H. On generalizations of repeated-root cyclic codes. *IEEE Trans. Inform. Theory 42*, 2 (1996), 641–649.

Index