N° d'ordre : 31/2021-C/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediène

Faculté de Mathématiques

THESE DE DOCTORAT

Présentée pour l'obtention du grade de Docteur

***En** : MATHEMATIQUES*

***Spécialité** : Mathématiques Fondamentales et Cryptographie*

Par : BENBELKACEM Nasreddine

Sujet

Les codes définis sur les anneaux non commutatifs

Soutenue publiquement, le 04 /04 /2021, devant le jury composé de :

M. Hernane Mohand Ouamar	Professeur	à l'USTHB	président
Mme. Batoul Aicha	Maître de conférences / A	à l'USTHB	Directrice de thèse
Mme. Belkredim Fatma Zohra	Professeur	à l'UHB,Chlef	Examinatrice
Mme. Guenda Kenza	Professeur	à l'USTHB	Examinatrice
M. Noui lamnouar	Professeur	à l'U,Batna	Examinateur
Mme. Mamache Fatiha	Maître de conférences / A	à l'USTHB	Examinatrice

Acknowledgments

First and for most, I am grateful to Allah for giving me the strength, health, and patience to conduct this thesis. I am so thankful to my supervisor Dr. Batoul Aicha for her commitments with work and administrative responsibilities, she has never taken a moment pause to provide me with all necessities, guidance, knowledge and kindness to get my thesis accomplished. Without her support and encouragement, my thesis would not have been possible. I am also thankful to the president of the jury Pr. Hernane Mohand Ouamar, for accepting my thesis to be read and evaluated. Pr. Belkredim Fatma Zohra, Pr. Guenda Kenza, Pr. Noui lamnouar and Dr. Mamache Fatiha for their time to read my thesis and hand me valuable and constructive pieces of advice. Not forgetting Pr. Abualrub Taher from Department of Mathemathics and Statistics, American University of Sharjah, United Arab Emirates and Dr. Ezerman Martinus Fredric from School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, in helping me with the findings and the articles, I thank them all. Taking into consideration my family, especially my parents who have always been supportive thoughout my studies, the ones who have given all to witness my success.

Notation

The following notation will be used throughout this thesis.

1. $\mathbb{N}$: the set of all natural numbers.
2. p : denotes a fixed prime.
3. $\mathbb{Z}$: the ring of integers.
4. $\mathbb{Z}_{\mid}$: the ring of integers modulo p.
5. $\mathbb{F}_q$: finite field of size q.
6. $\mathbb{F}_q[X]$: polynomials over $\mathbb{F}_q$ in the variable X.
7. $V_n(\mathbb{F}_q)$: set of n-tuples over $\mathbb{F}_q$.
8. $\mathbb{F}_q[X]/\langle f(X)\rangle$: equivalence classes in $\mathbb{F}_q[X]$ under congruence modulo the polynomial $f(X)$.
9. $f(X)$: generator matrix of a cyclic code.
10. $\mathbf{0}$: all zero vector.
11. I : identity matrix.
12. $a \,|\, b$: a divided b.
13. $a \mod b$: remainder of a when divided by b.
14. $a \equiv b(\mod c)$: a is congruent to b modulo c.
15. $|S|$: size of a set S.
16. $|\langle a\rangle|$: order of a field element.
17. (n, M)-code : code of length n and M codewords.
18. $[n, M]$-code : linear code of length n and M codewords.
19. $[n, k, d]$-code : linear code of length n and dimension k with minimum distance d.

20. $C^{\perp}$: orthogonal element of linear code C.

21. $gcld$: greatest common left divisor.

22. $gcrd$: greatest common right divisor.

23. $lclm$: least common left multiple.

24. $lcrm$: least common right multiple.

25. LCD : linear complementary dual.

26. ACD : Additive complementary dual.

Abstract

The overarching theme of this thesis is an algebraic coding and rings. At the beginning, we improve our knowledge in the field of skew polynomial ring $\mathbb{F}_4R[x,\theta]$ where θ is an automorphism of ring $\mathbb{F}_4R$. We denote by R the commutative ring, with 16 elements, $\mathbb{F}_4 + v\mathbb{F}_4 := \{a + vb : a, b \in \mathbb{F}_4\}$ where $v^2 = v$.

We merge the topic of skew cyclic codes with that of codes over a new alphabet set $\mathbb{F}_4R$. In the first aspect, if θ is identity, we then derive the systematic form of the respective generator matrices in the standard form of the codes and their dual codes. In three examples, we provide $\mathbb{F}_4R$-linear code under the Gray map is an optimal $\mathbb{F}_4$-linear code. We wrap the concept up by proving the MacWilliams identity for linear codes over $\mathbb{F}_4R$.

In the other aspect, we progress to classify all $\mathbb{F}_4R$-skew cyclic codes, by proposing a method to determine a generator polynomial and establish interesting results that relate these codes to cyclic and quasi-cyclic (QC) codes over $\mathbb{F}_4R$. We highlight several ways of obtaining $\mathbb{F}_4$-linear codes with good parameters from $\mathbb{F}_4R$-skew cyclic codes. Our setup provides a natural connection to DNA codes. We present a characterization of R-skew cyclic codes which are reversible complement.

Key-words : Linear codes, Codes over rings, Mixed alphabets, Skew cyclic

Résumé

Les codes algébriques ont un lien avec les anneaux finis dans différents concepts. Cette thèse a pour objetif d'améliorer les performances des codes correcteurs d'erreurs construits à partir des polynômes tordus "skew polynomial" $\mathbb{F}_4R[X,\theta]$ où θ est un automorphisme de l'anneau $\mathbb{F}_qR$. On note R l'anneau commutatif contenant 16 éléments,
$\mathbb{F}_4 + v\mathbb{F}_4 = \{a + vb : a, b \in \mathbb{F}_4\}$ avec $v^2 = v$.
Nous donnons le concept des codes θ-cycliques avec celui des codes sur un nouvel ensemble d'alphabets $\mathbb{F}_4R$. Dans le premier aspect, si θ est l'automorphisme identité, nous dérivons alors la forme systématique des matrices génératrices respectives des codes et de leurs codes duaux. Ensuite, nous avons construit trois $\mathbb{F}_4R$-codes linéaires en utilisant l'image de Gray, qui sont des $\mathbb{F}_4$-codes linéaires optimaux. De plus, nous avons présenté l'identité de MacWilliams pour les codes linéaires sur $\mathbb{F}_4R$.
Dans le second aspect, nous avons classifié tous les codes cycliques tordus sur l'anneau $\mathbb{F}_4R$, aboutissant à l'identification de leurs générateurs. Nous avons montré que, sous certaines conditions sur la longueur de ces codes, ils sont équivalents à des codes cycliques ou bien à des code 2-quasi-cycliques sur le même anneau. Nous avons procédé de différentes manières pour obtenir des codes $\mathbb{F}_4$-linéaires avec de bons paramètres comme images de codes. Cycliques tordus sur $\mathbb{F}_4R$ sous l'application Gray. A la fin de cette de nos travaux, nous avons appliqué les codes construits au DNA computing.

Mots-clés : Codes linéaires, Codes sur les anneaux, Alphabets mixtes, Codes θ-cyclique .

Introduction

Theory of non-commutative polynomial rings were introduced in 1933 by Oystein Ore **?**. He gave fundamental properties of them. Since then, many mathematicians have studied the structural theory of the skew polynomial rings, that was developed by N. Jacobson **?**, A. Leroy **?** and others. Since, algebraic codes and rings are closely connected in at least two fundamental ways. The code alphabets often has a ring structure, instead of just a set. The code itself can often be constructed and then studied as a module over some rings. A recent book **?** by Shi *et al.* highlights these facts. When the rings are finite fields, numerous studies have been done and are still being carried out actively on the constructions and properties of error-control codes since the pioneering works of Shannon, Hamming, and their contemporaries in the 1940s **?**. In terms of error-correcting capabilities, most codes over general rings do not surpass the performance of their finite fields cousins. Fortunately, useful applications remain abounds. Many codes over rings lead to good pseudo-random sequences, for example. Studies on codes over Galois rings are naturally built on results on the main structures of the underlying rings. The latter can be found, for example, in the collection of lectures by Z. X. Wan in **?**. Extensions beyond Galois, for instance, to chain rings have also been looked into.

Based on what Oystein Ore **?** brought, Boucher *et al.* **?** used this non-commutative ring to generalize the linear cyclic codes to be called later the skew cyclic codes. They identified skew cyclic codes of length n over a finite field $\mathbb{F}_q$, and θ be an automorphism of $\mathbb{F}_q$ with left ideal in the ring $\mathbb{F}_q[X,\theta]/\langle X^n-1\rangle$. The richness of code theory came from non-commutative rings that motivated many researchers to construct new codes with good parameters. Abualrub *et al.* **?**, and on the basis of Boucher *et al.* results **??**, they generalized the skew cyclic codes to skew quasi-cyclic codes under the property that, in

all cases, θ is an automorphism of $\mathbb{F}_q$ must divide the length n of codes. In 2011, Siap *et al.* **?** studied skew-cyclic codes without any restrictions about the length. A linear code of length n over $\mathbb{F}_q$ is skew cyclic codes if it is a left submodule of $\mathbb{F}_q[X,\theta]/\langle X^n-1\rangle$. After that, Abualrub *et al.* in 2012 **?**, they described skew-cyclic codes over the ring $\mathbb{F}_2+v\mathbb{F}_2=\{0,1,v,v+1\}$ where $v^2=v$. This is the only ring of order four and has a non-trivial ring automorphism. On the other hand, topics of error-correcting codes are additive codes over mixed alphabets. These codes were first introduced in 1997 **?**. Two rather recent works that provide some initial inspiration for our set up below are done over $\mathbb{Z}_2\mathbb{Z}_4$ by Borges *et al.* **?** and over $\mathbb{Z}_2\mathbb{Z}_2[u]$ by Aydogdu *et al.* **?**. This class generalizes binary and quaternary linear codes. Later, an exhaustive description of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes was done **?**, **?**, **?**, **?** and **?**. The structure and properties of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes have been intensively studied **??????**. For example **?**, we generalized the notion of LCD codes to *additive complementary dual* (ACD) codes in $\mathbb{Z}_2^{\alpha}\mathbb{Z}_4^{\beta}$. We constructed infinite families of codes that are ACD. We used the ACD codes to construct infinite families of binary LCD codes via the Gray map. We gave conditions for the case when the image of ACD code is a binary LCD code. see **?????**. In 2020, Melakhessou *et al.* **?** studied skew constacyclic codes over the ring $\mathbb{Z}_qR$ where $R=\mathbb{Z}_q+u\mathbb{Z}_q$, $q=p^s$ for a prime p and $u^2=0$. By using the Gray images of skew constacyclic codes over $\mathbb{Z}_qR$ they obtained some new linear codes over $\mathbb{Z}_4$.

The aim of this thesis is to construct error control codes. We focus on linear codes over finite rings. Our purpose is to merge the topic of skew cyclic codes with that of codes over mixed alphabets. In particular, we study the structure of linear skew cyclic codes over the ring $\mathbb{F}_4R$, where $\mathbb{F}_4$ is the field of four elements and $R=\{a+vb|a,b\in\mathbb{F}_4\}$ is the commutative ring with 16 elements where $v^2=v$. An $\mathbb{F}_4R$-linear code $\mathcal{C}$ is defined to be a submodule of $\mathbb{F}_4^{\alpha}R^{\beta}$. If $\beta=0$, then $\mathcal{C}$ is a quaternary linear code. If $\alpha=0$, then $\mathcal{C}$ is an R-submodule of a finite non-chain ring. We classify all $\mathbb{F}_4R$-skew cyclic codes. This thesis is divided into three chapters. Chapter 1 is divided into three sections. Firstly, we give basic definitions related to linear codes over finite field $\mathbb{F}_q$. We note that a codeword $\mathbf{x}=(x_1,x_2,\ldots,x_n)$ of length n can be viewed as an n-dimensional vector over $\mathbb{F}_q$. An (n,k) linear code over $\mathbb{F}_q$ is a k-dimensional subspace of the n-dimensional vector space

$$V_n(q)=\{(x_1,x_2,\ldots,x_n):x_i\in\mathbb{F}_q\};$$

where n is called the length of the code, k the dimension.

In this section, we present generator, parity check matrix and dual of an $[n, k]$-linear code. Also, we define the Hamming distance between any codewords. In the next section, we generalize the notion of cyclic codes from commutative to non-commutative ring. A linear code C over $\mathbb{F}_q$ is a left $\mathbb{F}_q$-*submodule* of $V_n(\mathbb{F}_q)$. Also, is said to be $\mathbb{F}_q$-skew cyclic codes if

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

Where θ is an *automorphism* over $\mathbb{F}_q$. Finally, we extend the above concepts from finite field $\mathbb{F}_q$ to finite ring $R = \mathbb{F}_q + v\mathbb{F}_q = \{a + vb | a, b \in \mathbb{F}_q\}$ with q elements where $v^2 = v$. A subset C of R^n is a *linear code over* R if C is an R-submodule. For any codeword $\mathbf{c} = (a_0, a_1, \ldots, a_{n-1}) \in R^n$ can be identified by polynomial such that

$$c(X) = a_0 + a_1X + \ldots + a_{n-1}X \in R[X]/\langle X^n - 1\rangle$$

This identification gives a one-to-one correspondence between R^n and

$$R_n := R[X]/\langle X^n - 1\rangle$$

The product of $c(X) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$ and $r(X) = b_0 + b_1X + \ldots + b_{n-1}X^{n-1}$ in R_n is given by

$$c(X).r(X) \mod (X^n - 1). \tag{2}$$

The interested reader may consult **?**, **?**, **?** and **?**.

In chapter 2, we consider codes whose alphabets come from a finite non-chain ring that we call $\mathbb{F}_4R$, with R soon to be formally defined. We obtain results on the structure of linear codes over the ring, define a suitable inner product to derive the dual codes, and obtain the systematic form of their respective generator matrices. The followings are our contributions.

1. We construct the respective generator matrices for any $\mathbb{F}_4R$-linear code $\mathcal{C}$.
2. We derive the parity-check matrices for an $\mathbb{F}_qR$-linear code C.
3. We provide the MacWilliams identity for linear codes over $\mathbb{F}_4R$.

In chapter 3, we consider a new alphabet set, which is a ring that we call $\mathbb{F}_4 R$, to construct linear error-control codes. Skew cyclic codes over this ring are then investigated in details. We define a nondegenerate inner product and provide a criteria to test for self-orthogonality.

Results on the algebraic structures lead us to characterize $\mathbb{F}_4R$-skew cyclic codes. Interesting connections between the image of such codes under the Gray map to linear cyclic and skew-cyclic codes over $\mathbb{F}_4$ are shown. These allow us to learn about the relative dimension and distance profile of the resulting codes. Our setup provides a natural connection to DNA codes where additional biomolecular constraints must be incorporated into the design. We present a characterization of R-skew cyclic codes which are reversible complement. The followings are our contributions **?**,**?** and **?**.

1. We show that the dual of a skew cyclic code over $\mathbb{F}_4R$ is also a skew cyclic code. In fact, skew cyclic codes over $\mathbb{F}_4R$ are left $R[X,\theta]$-submodules of $R_{\alpha,\beta} := \mathbb{F}_4[X]/\langle X^\alpha - 1\rangle \times R[X,\theta]/\left\langle X^\beta - 1\right\rangle$.

2. We determine their generator polynomials and establish interesting results that relate these codes to cyclic and quasi-cyclic (QC) codes over $\mathbb{F}_4R$. First, we show that a skew cyclic code over $\mathbb{F}_4R$ is equivalent to an $\mathbb{F}_4R$-cyclic code if α and β are both odd integers. Second, we establish that if α and β are both even integers, then an $\mathbb{F}_4R$-skew cyclic code C is equivalent to an $\mathbb{F}_4R$ quasi-cyclic code of index 2.

3. Conditions for skew cyclic codes over $\mathbb{F}_4R$ to be self-orthogonal are studied.

4. We use the Gray mapping to associate these codes to codes over $\mathbb{F}_4$ of length $\alpha+2\beta$ and exhibit a nice relationship between these codes and their images over $\mathbb{F}_4$. The Gray image of any skew cyclic code over $\mathbb{F}_4R$ is the product of a cyclic code over $\mathbb{F}_4$ of length α and two skew cyclic codes, each of length β, over $\mathbb{F}_4$. We supply examples of good skew cyclic codes over $\mathbb{F}_4R$ and their respective Gray images for different lengths.

5. We construct optimal linear codes over $\mathbb{F}_4$ as images of skew cyclic code over $\mathbb{F}_4R$ under the Gray mapping.

6. Applications of these codes to DNA computing are included in our treatment.

This thesis has been the subject of publications [chap 2 **?**, chap 4 **?**] and results submitted [chap 3 **?**].

Contents

Chapter 1

Fundamental background

In this chapter, we provide basic definitions and results to linear codes over $\mathbb{F}_q$, and then, we generalize them to linear codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$.

Let $\mathbb{F}_q$ be the finite fields with q elements. Let n be a nonnegative integers, and $V_n(\mathbb{F}_q)$ be the set of n-tuples over $\mathbb{F}_q$, *i.e.*,

$$V_n(\mathbb{F}_q) = \{(x_1, \ldots, x_n) | x_i \in \mathbb{F}_q \text{ for } i = 1, \ldots, n\}$$

This set is an n-dimensional vector space over $\mathbb{F}_q$. If q is a prime, $\mathbb{F}_q$ accords with $\mathbb{Z}_q$ which is the ring of integer residues modulo q.

Let I_n be the identity $n \times n$ matrix. Let $\mathbf{0}$ denote either the zero vector or the all-zero matrix whose dimension is clear from the context. A nonempty subset C of $\mathbb{F}_q^n$ is called a q-ary code or, easily and more accurately, a code over $\mathbb{F}_q$ or a $\mathbb{F}_q$-code, and n is called the length of the code. This code is also denoted by (n, M)-code, where M is the size of $V_n(\mathbb{F}_q)$, and the elements of the code are called codewords.

1.1 Linear codes over $\mathbb{F}_q$

Definition 1. *A linear $[n, k]$-code over $\mathbb{F}_q$ is a k-dimensional subspace of $V_n(\mathbb{F}_q)$. The parameter n is called the length of the code and k is the dimension of the code. Moreover, $|C| = M = q^k$.*

Definition 2. *Let C_1 and C_2 be two codes over $\mathbb{F}_q$. C_2 is equivalent to C_1 if there exists a fixed permutation of the positions to all codewords of C_1 to obtain C_2.*

An important parameter to take into account is the Hamming distance for (n, k)-code. The Hamming distance between two codewords $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^n$ is defined by

$$d(\mathbf{x}, \mathbf{y}) := |\{i \quad | \quad 1 \leq i \leq n, x_i \neq y_i\}$$

For any codewords $\mathbf{x}, \mathbf{y}$ and $\mathbf{z}$ in $\mathbb{F}_q$, it is easy to confirm that the Hamming distance satisfies the following properties of a metric.

- $d(\mathbf{x}, \mathbf{y}) = 0$ if and only if $\mathbf{x} = \mathbf{y}$
- $d(\mathbf{x}, \mathbf{y}) \geq 0$
- Symmetry: $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$
- Triangle inequality: $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.

We will now describe the Hamming distance of a code.

Definition 3. *Let C be an $[n, k]$-code. The minimum distance d of the code C is*

$$d := \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}. \tag{1.1}$$

The Hamming weight of vector $\mathbf{x} \in V_n(\mathbb{F}_q)$; denoted, $\mathrm{w_H}(\mathbf{x})$ is the Hamming distance between $\mathbf{x}$ and the zero vector, *i.e.*,

$$\mathrm{w_H}(\mathbf{x}) := d(\mathbf{x}, \mathbf{0})$$

Definition 4. ? *The Hamming weight of an $[n, k]$-code C is*

$$\mathrm{w_H}(C) = \min\{\mathrm{w_H}(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$$

From the Definition and , observe that for any two codewords $\mathbf{x}, \mathbf{y}$ in $V_n(\mathbb{F}_q)$, we have

$$d(\mathbf{x}, \mathbf{y}) = \mathrm{w_H}(\mathbf{x} - \mathbf{y})$$

A close relationship has been demonstrated in **?**.

Theorem 1. *Let d be the distance in a linear code $[n, k]$-code. Then*

$$d := \mathrm{w_H}(C) \tag{1.2}$$

Since C is a linear code, then the minimum distance and the minimum weight of any non-zero codewords of C are similar. From now, we reserve the notation $[n, k, d]$-code to refer a k-dimensional linear code of length n with minimum distance d. Next, we derive the generator matrix of a linear code.

Definition 5. ? *A generator matrix for an $[n, k]$-code C is any $k \times n$-matrix G whose rows form a basis for C.*

In general, we introduce a standard form of a generator matrix of a linear code by

$$G = [I_k \quad A], \tag{1.3}$$

where A is a $k \times (n - k)$-matrix. The difference $n - k$ is called the redundancy of C.

Definition 6. ? *Two $[n, k]$-codes C and C' over $\mathbb{F}_q$ are said to be equivalent codes if there exist generator matrices G and G' for C and C' respectively and an $n \times n$ permutation matrix P such that*

$$G' = GP$$

The matrix P permutes the columns of G, and thus permutes the coordinate positions in C to produce the the code C'. The above definition useful to the following result.

Theorem 2. ? *If C is an $[n, k]$-linear code over $\mathbb{F}_q$, then there exists a generator matrix G for C or for an equivalent code C' such that*

$$G = [I_k \quad A].$$

1.1.1 Dual code

Let C be a linear code $[n, k, d]$-code over $\mathbb{F}_q$. The standard Euclidean inner product of $\mathbf{x}$ and $\mathbf{y}$ in $V_n(\mathbb{F}_q)$, denoted by $\langle \mathbf{x}, \mathbf{y} \rangle_q$, is given as usual by

$$\langle \mathbf{x}, \mathbf{y} \rangle_q := \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_q.$$

From the definition of inner product we have the following properties.

Proposition 1. ? *Let* $\mathbf{x}, \mathbf{y}$ *and* $\mathbf{z}$ *in* $V_n(\mathbb{F}_q)$*, then*

- $\langle \mathbf{x}+\mathbf{y}, \mathbf{z}\rangle_q := \langle \mathbf{x}, \mathbf{z}\rangle_q + \langle \mathbf{y}, \mathbf{z}\rangle_q$
- *For any* $\lambda \in \mathbb{F}_q$*,* $\langle \lambda\mathbf{x}, \mathbf{y}\rangle_q = \lambda\langle \mathbf{x}, \mathbf{y}\rangle_q$

If $\langle \mathbf{y}, \mathbf{z}\rangle_q = 0$, we say that the vectors $\mathbf{x}$ and $\mathbf{y}$ are orthogonal to each other.

Definition 7. *If* C *is a linear code over* $\mathbb{F}_q$*, then the dual of* C*, denoted by* $C^\perp$*, is*

$$C^\perp := \{\mathbf{y} \in V_n(\mathbb{F}_q) | \langle \mathbf{x}, \mathbf{y}\rangle = 0 \text{ for all } \mathbf{x} \in C\}$$

If $C = C^\perp$ *then* C *is called a self-dual codes.*

Theorem 3. ? *If* C *is an* $[n, k]$*-linear code over* $\mathbb{F}_q$*, then* $C^\perp$ *is an* $[n, k]$*-linear code over* $\mathbb{F}_q$*.*

Corollary 1. ? *If* $G = [I_k \quad A]$ *is a generator matrix for* C*, then* $H = [-A^T \quad I_{n-k}]$ *is a generator matrix for* $\mathcal{C}^\perp$*.*

The following results construct the *parity-check matrix* for any $\mathbb{F}_q$-linear code.

Definition 8. *Let* C *be an* $[n, k]$*-linear code over* $\mathbb{F}_q$*. If* H *is a generator matrix for* $C^\perp$*, then* H *is called a parity-check matrix for* C*.*

The next theorem gives a description of the minimum distance of a linear via any parity-check matrix of the code.

Theorem 4. ? *Let* H *be a parity-check matrix of a linear code* $C \neq 0$*. The minimum distance of* C *is the largest integer* d *such that every set of* $d-1$ *columns in* H *is linearly independent.*

1.1.2 Cyclic codes

Cyclic codes are the important classes of linear codes. Next, we introduce some definitions and notations for the cyclic codes.

Definition 9. *A subset* C *of* $V_n(\mathbb{F}_q)$ *is said to be an* $\mathbb{F}_q$*-cyclic code of length* n *if two conditions are satisfied.*

1. C *is an* $\mathbb{F}_q$*-subspace of* $V_n(\mathbb{F}_q)$*.*

2. *If* $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ *then the cyclic shift of* $\mathbf{c}$ *over* $\mathbb{F}_q$*, denoted by* $T(\mathbf{c}) := (c_{n-1}, c_0, \ldots, c_{n-2})$*, is also in* C

It is often convenient to associate a vector $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ with a polynomial

$$\mathbf{a}(X) := a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}$$

in an indeterminate X. This allows for conditions of codes using results from the algebra of polynomial rings. More formally, a code C is said to be a cyclic code of length n if it is invariant under the cyclic shift implies that if $\mathbf{c}(X) \in C$, then $X\mathbf{c}(X) \mod (X^n - 1)$ is also in C. From now, we represent any vector $(a_0, a_1, \ldots, a_{n-1})$ in $V_n(\mathbb{F}_q)$ by

$$a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} \mod (X^n - 1)$$

Theorem 5. ? $\mathbb{F}_q[X]/\langle X^n - 1\rangle$ *is a principal ideal ring.*

Proof. Let I be an ideal in $\mathbb{F}_q[X]/\langle X^n - 1\rangle$. If $I = \langle 0\rangle$, then I is generated by 0. Else, let $f(X)$ be a monic polynomial of least degree in I. Let $g(X) \in I$, by the division algorithm, we have

$$g(X) = q(X)f(X) + r(X),$$

where $\deg(r(X)) < \deg(f(X))$ or $r(X) = 0$. Since $q(X)f(X) \in I$, it follows that

$$r(X) = g(X) - q(Xf(X)) \in I$$

since $g(X)$ is a polynomial of least degree in I, we must have $r(X) = 0$. Hence, $f(X)$ divides $g(X)$, so I is generated by $g(X)$. □

The following result establishes a fundamental theorem of cyclic codes.

Theorem 6. ? *A linear code* C *in* $V_n(\mathbb{F}_q)$ *is cyclic if and only if* C *is an ideal in* $\mathbb{F}_q[X]/\langle X^n - 1\rangle$.

Proof. Suppose that C is cyclic, then for any codeword $c(X) \in C$ the word $X.c(X)$ is also in C. Therefore, X^i is in C for every $i \geq 0$. By linearity, $a(X)c(X)$ is in C for every polynomial $a(X)$. Hence, C is an ideal in the ring $\mathbb{F}_q[X]/\langle X^n - 1\rangle$.
Conversely, if C is an ideal in $\mathbb{F}_q[X]/\langle X^n - 1\rangle$. let $c(X)$ be any codeword, then $Xc(X)$ is also codeword. Hence, by a linear code C is cyclic. □

1.2 Skew polynomial rings

Ore ring or skew polynomial ring is introduced by Oystein Ore **?**. In this section, we study a brief account of a particular kind of non-commutative ring. Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements where p is prime number and r is a non-negative integer. Let θ be an *automorphism* of $\mathbb{F}_q$. *i.e.*, $\theta \in Aut(\mathbb{F}_q) := \{Id, x \mapsto x^p, x \mapsto x^{p^2}, \ldots, x \mapsto x^{p^{r-1}}\}$. Hence, $|\langle\theta\rangle| = r$, denoted, the order of *automorphism* θ. The skew polynomial ring $\mathbb{F}_q[X, \theta]$ is defined by

$$\mathbb{F}_q[X, \theta] := \{a_0 + a_1X + \ldots + a_nX^n : a_i \in \mathbb{F}_q \text{ for all } i = 0, 1, \ldots, n\},$$

where addition of these polynomials is defined in the usual way while multiplication is defined using the distributive (associativity) laws and the rule

$$(aX^i).(bX^j) = a\theta^i(b)X^{i+j}$$

The ring $\mathbb{F}_q[X, \theta]$ is not commutative. If θ is the identity automorphism we back to the concept of commutative ring. In the next step, we derive some fundamental properties of a non-commutative ring over $\mathbb{F}_q[X, \theta]$. Let $P = \sum_{i=1}^{n} a_iX^i$ and $Q = \sum_{j=0}^{m} b_jX^j$ in $\mathbb{F}_q[X, \theta]$, then the multiplication of P and Q defined by

$$PQ = \sum_{i=1}^{n}\sum_{j=0}^{m} a_i\theta^i(b_j)X^{i+j}$$

θ^i is the composition of θ i-times. We essential to state left or right divisibility, when we talk about divisibility, and when discuss ideals we need to talk fixed a left, right or two-sided *i.e.*, a left and a right ideal.

Definition 10. *The degree of skew polynomial is defined in the usual way as the largest exponent of X appearing in the polynomial, and $\deg(0) := -\infty$. This does not depend on the side where we place the coefficients because θ is an automorphism*

The next proposition follows immediately from the definition.

Proposition 2. **?** *Let f and g two polynomials in $\mathbb{F}_q[X, \theta]$, then*

1. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(fg) = \deg(f) + \deg(g)$

The above Proposition implies that $\mathbb{F}_q[X,\theta]$ is a domain which has non-zero divisors different to zero. Next, we derive the right division algorithm in $\mathbb{F}_q[X,\theta]$.

Theorem 7. ? *Let $f(X)$ and $g(X)$ in $\mathbb{F}_q[X,\theta]$ with $g(X) \neq 0$. There exist unique $q(X)$ and $r(X)$ in $\mathbb{F}_q[X,\theta]$ such that*

$$f(X) = q(X)g(X) + r(X)$$

with $\deg(r(X)) < \deg(g(X))$

Proof. $f(X) = a_0 + a_1X + \ldots + a_nX^n$ and $g(X) = b_0 + b_1X + \ldots + b_mX^m$ two polynomials in $\mathbb{F}_q[X,\theta]$ with $b_m \neq 0$. If $n < m$ then we have to take $q(X) = 0$ and $r(X) = f(X)$. Otherwise, we have

$$f(X) - a_n\theta^{n-m}(b_m^{-1})X^{n-m}g$$

By induction on n and the degree we get the existence, and the uniqueness of $q(X)$ and $r(X)$. □

If $f = gh$ (resp. $f = hg$) for some $h \in \mathbb{F}_q[X,\theta]$, then we say that g is a left multiplicative (resp. multiplication) of f, denoted, $g|_l f$ (resp. $g|_r f$). For any two non-zero polynomials f and g in $\mathbb{F}_q[X,\theta]$, not boths zero, we have the following results.
The polynomial $d = gcld(f,g) \in \mathbb{F}_q[X,\theta]$ is called the greatest common left divisor of f and g, if $d|_l f$, $d|_l g$ and for any polynomial $h \in \mathbb{F}_q[X,\theta]$ satisfies $h|_l f$ and $h|_l g$ then $h|_l d$.
The polynomial $l = lclm(f,g) \in \mathbb{F}_q[X,\theta]$ is called the least common left multiple of f and g, if $f|_r l$, $g|_r l$ and for any polynomial $h \in \mathbb{F}_q[X,\theta]$ satisfies $f|_r h$ and $g|_r h$ then $l|_r h$.
For all non-zero $f, g \in \mathbb{F}_q[X,\theta]$

$$\deg(gcrd(f,g)) + \deg(lclm(f,g)) = \deg(f) + \deg(g). \tag{1.4}$$

Theorem 8. ? $\mathbb{F}_q[X,\theta]$ *is a left and a right Euclidean ring.*

In particular, we can also define a left (resp. a right) Bezout identity.

Theorem 9. ? $\mathbb{F}_q[X,\theta]$ *is a left (resp. right) principal ideal ring. Moreover, any two-sided ideal must be generated by*

$$f(X) = (a_0 + a_1X^r + a_2X^{2r} + \ldots + a_nX^{nr}).X^t$$

where $|\langle\theta\rangle| = r$ and t are positive integer.

1.2.1 Skew cyclic codes over $\mathbb{F}_q$

Lemma 1. ? *$X^n - 1$ is two-sided if and only if $r \mid n$.*

Proof. If $X^n - 1$ is two-sided, then by definition $X^n - 1$ commutes with aX^r, for any a in $\mathbb{F}_q$, this implies that $(X^n - 1).aX^r = aX^r.(X^n - 1)$. Then

$$(X^n - 1).aX^r = \theta(a)^n X^{n+r} - aX^r,$$

and

$$aX^r.(X^n - 1) = aX^{n+r} - aX^r,$$

Thus, $\theta(a)^n = a$ for all a in $\mathbb{F}_q$, hence $r \mid n$.
Conversely, let $f(X) = a_0 + a_1X + \ldots + a_rX^r \in \mathbb{F}_q[X, \theta]$. Then

$$\begin{aligned}(X^n - 1).f(X) &= X^n.f(X) - f(X)\\ &= X^n.(a_0 + a_1X + \ldots + a_rX^r) - f(X)\\ &= \theta(a_0)^n X^n + \theta(a_1)^n X^{n+1} + \ldots + \theta(a_r)^n X^{n+r} - f(X)\end{aligned}$$

If $r \mid n$ then $\theta(a)^n = a$ for all $a \in \mathbb{F}_q$, we have

$$\begin{aligned}(X^n - 1).f(X) &= (a_0 + a_1X + \ldots + a_rX^r).X^n - f(X)\\ &= f(X).(X^n - 1)\end{aligned}$$

This concludes the proof. □

The previous lemma shows that the quotient $\mathbb{F}_q[X, \theta]/\langle X^n - 1\rangle$ is a ring.

Lemma 2. ? *If $r \mid n$. Then the ring $\mathbb{F}_q[X, \theta]/\langle X^n - 1\rangle$ is a principal left ideal ring.*

Now, if $r \nmid n$ then we need to verify that $S_n := \mathbb{F}_q[X, \theta]/\langle X^n - 1\rangle$ is a left $\mathbb{F}_q[X, \theta]$-module under the multiplication

$$d(X).(f(X) + \langle X^n - 1\rangle) = d(X).f(X) + \langle X^n - 1\rangle \tag{1.5}$$

Where $f(X) \in S_n$ and for all $d(X) \in \mathbb{F}_q[X, \theta]$.

Theorem 10. ? *S_n is a left $\mathbb{F}_q[X, \theta]$-module with respect to the multiplication in Equation (??).*

Proof. It is clear that the properties of a left module are satisfied over S_n. □

The following results establish a fundamental theorem of θ-cyclic codes. For the proof of the next results see **?**, **?**.

Theorem 11. *Let $C = \langle f(X)\rangle$ be a linear code over $\mathbb{F}_q$ of length n, where $f(X)$ is the generator polynomial of C.*

1. *If $r \mid n$, then C is a θ-cyclic code if and only if $C = \langle f(X)\rangle$ is a left ideal of $\mathbb{F}_q[X,\theta]/\langle X^n - 1\rangle$, where $f(X)$ is right divisor of $X^n - 1$ in $\mathbb{F}_q[X,\theta]$.*

2. *$r \nmid n$, then C is a left $\mathbb{F}_q[X,\theta]$-submodule of S_n with respect to the multiplication in Equation (**??**).*

In general, we consider an arbitrary length without any restriction. In this case, a linear code C over $\mathbb{F}_q$ is a left $\mathbb{F}_q$-*submodule* of $V_n(\mathbb{F}_q)$. Also, is said to be $\mathbb{F}_q$-skew cyclic codes if

$$(c_0, c_1, \ldots, c_{n-1}) \in C \implies (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C. \tag{1.6}$$

Let $f(X) = f_0 + f_1X + \ldots + f_tX^t$, let $C = \langle f(X)\rangle$ be a left $\mathbb{F}_q[X,\theta]$-*submodule* of S_n generated $f(X)$. From **?**, the generator matrix of C is given by

$$\begin{pmatrix} f_0 & \ldots & f_{t-1} & f_t & 0 & \ldots & 0 \\ 0 & \theta(f_0) & \ldots & \theta(f_{t-1}) & \theta(f_t) & \ldots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & & & & \\ 0 & \ldots & 0 & \theta^{n-t-1}(f_0) & \ldots & \theta^{n-t-1}(f_1) & \theta^{n-t-1}(f_t) \end{pmatrix}$$

1.3 Codes over finite ring $\mathbb{F}_q + v\mathbb{F}_q$

In this section, we generalize the concept of linear codes over finite fields $\mathbb{F}_q$ to the linear codes over non-chain ring $\mathbb{F}_q + v\mathbb{F}_q$. We give some definitions and characterization related to main results.

1.3.1 Introduction

Let $R := \mathbb{F}_q + v\mathbb{F}_q := \{a + vb : a, b \in \mathbb{F}_q\}$ is the commutative ring with q^2 elements where $v^2 = v$, this ring are isomorphic to the quotient ring $\mathbb{F}_q[v]/\langle v - v^2\rangle$. It is well known that R is a finite non-chain ring with two maximal ideals

$$\langle v\rangle := \{av : a \in \mathbb{F}_q\} \text{ and } \langle v - 1\rangle := \{b(1 - v) : b \in \mathbb{F}_q\},$$

making each $R/\langle v\rangle$ and $R/\langle 1 - v\rangle$ isomorphic to $\mathbb{F}_q$. The Chinese Remainder Theorem then implies that

$$R = \langle v\rangle \times \langle 1 - v\rangle.$$

Let R^n denote the R-module of n-tuples over R. Any element in R can be uniquely expressed as

$$a + vb = (b + a)v + a(1 - v) \text{ for } a, b \in \mathbb{F}_q$$

Lemma 3. ? *Let R^* denote the group of units of R then $R^* = v\mathbb{F}_q^* \oplus (1 - v)\mathbb{F}_q^*$.*

Definition 11. *A subset C of R^n is a linear code over R if C is an R-submodule.*

For any codeword $\mathbf{c} = (a_0, a_1, \ldots, a_{n-1}) \in R^n$ we can identified by polynomial such that

$$c(X) = a_0 + a_1 + \ldots + a_{n-1} \in R[X]/\langle X^n - 1\rangle$$

This identification gives a one-to-one correspondence between R^n and

$$R_n := R[X]/\langle X^n - 1\rangle$$

The product of $c(X) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$ and $r(X) = b_0 + b_1X + \ldots + b_{n-1}X^{n-1}$ in R_n is given by

$$c(X).r(X) \mod (X^n - 1). \tag{1.7}$$

For $a + vb \in R$, the classical Gray map $\phi : R \mapsto \mathbb{F}_q^n$ sends $a + vb$ to $(a + b, a)$. The *Lee weight* of any element in R is the *Hamming weight* of its image under ϕ.

Lemma 4. ? *The mapping $\phi : R \mapsto \mathbb{F}_q^2$ is a bijection.*

Proof. It is easy to verify that ϕ is one-to-one. Let $(v_1, v_2) \in \mathbb{F}_q^2$ such that v_1 and v_2 are in $\mathbb{F}_q$. Let $b = v_1 + v_2$, and $a = v_2$. Then, $\phi(a + vb) = (v_1, v_2)$ and, hence, the mapping ϕ is onto. □

This map extends naturally to R^n. For any $\mathbf{c} = (\mathbf{a} + v\mathbf{b}) = (a_1 + vb_1, a_2 + vb_2, \ldots, a_n + vy_n) \in R^n$ with $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ in $\mathbb{F}_q^n$. Then the *Gray map* over R^n is defined by

$$\phi : R^n \mapsto \mathbb{F}_q^{2n} \text{ with } \phi(\mathbf{c}) = \phi(\mathbf{a} + v\mathbf{b}) = (\mathbf{a} + \mathbf{b}, \mathbf{a}). \tag{1.8}$$

The map ϕ is an isometry which transforms the Lee distance in R^n to the Hamming distance in $\mathbb{F}_q^{2n}$. For any R-linear code C, the code $\phi(C)$ is $\mathbb{F}_q$-linear. Furthermore, since the inner product in Equation (**??**) is nondegenerate, we have $|\mathcal{C}|\cdot|\mathcal{C}^\perp| = |\phi(\mathcal{C})|\cdot|\phi(\mathcal{C})^\perp| = q^{2n}$.

1.3.2 Linear codes over $R = \mathbb{F}_q + v\mathbb{F}_q$

Let $A \oplus B = \{a + b \mid a \in A, b \in B\}$ and $A \otimes B = \{(a, b) \mid a \in A, b \in B\}$ as defined in **?**. Given a linear code C over R, let

$$C_1 := \{\mathbf{x} + \mathbf{y} \in \mathbb{F}_q^n \mid (\mathbf{x} + \mathbf{y})v + \mathbf{x}(v + 1) \in C \text{ for some } \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n\} \text{ and}$$
$$C_2 := \{\mathbf{x} \in \mathbb{F}_q^n \mid (\mathbf{x} + \mathbf{y})v + \mathbf{x}(v + 1) \in C \text{ for some } \mathbf{y} \in \mathbb{F}_q^n\}.$$

One can quickly verify that C_1 and C_2 are linear codes over $\mathbb{F}_q$. Let $r = a + vb \in R$ and $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in C$, *i.e.*, $c_j = a_j + vb_j$ with $a_j, b_j \in \mathbb{F}_q$ for $1 \le j \le n$.
The j-th entry of $r\mathbf{c}$ is

$$\begin{aligned}(a + vb)(a_j + vb_j) &= ((b + a)v + a(1 - v))(a_j + vb_j) \\ &= \underbrace{aa_j}_{x} + v(\underbrace{ab_j + ba_j + bb_j}_{y}) = (x + y)v + x(1 - v).\end{aligned}$$

Hence, $r\mathbf{c}$ can be written in terms of C_1 and C_2 with

$$\mathbf{x} = a(a_1, a_2, \ldots, a_n) \text{ and } \mathbf{y} = (a + b)(b_1, b_2, \ldots, b_n) + b(a_1, a_2, \ldots, a_n).$$

The *Gray map* can be restricted from R^n to a linear code C over R. The next results can be concluded by a slight modification from **?**, with 2 extends to q.

Theorem 12. ? *Let C be a R-submodule of R^n. Then $\Phi(C) = C_1 \otimes C_2$ and* $\mid C \mid = \mid C_1 \mid\mid C_2 \mid$.

Proof. For any codeword $c_j = a_j + vb_j$ in C can be expressed as $c_j = (b_j + a_j) + a_j(1 - v)$ with $a_j, b_j \in \mathbb{F}_q^n$ for $1 \leq j \leq n$. It suffices to show that, $\Phi(c_j) \in C_1 \otimes C_2$. Since Φ is bijection, $\Phi(c_j) = (b_j + a_j, a_j)$. By definition of C_1 and C_2 we obtain $b_j + a_j \in C_1$ and $a_j \in C_2$, therefore, $\Phi(c_j) \subseteq C_1 \otimes C_2$.
Conversely, let $(v_1, v_2, \ldots, v_n, w_1, w_2, \ldots, w_n) \in C_1 \otimes C_2$, where $(v_1, v_2, \ldots, v_n)\mathcal{C}_1$ and $(w_1, w_2, \ldots, w_n) \in C_2$ such that $v_j = b_j + a_j$ and $w_j = a_j$ for $1 \leq j \leq n$. There are $c = (c_0, c_1, \ldots, c_n) \in C$ with $c_j = a_j + vb_j$ for $1 \leq j \leq n$, then we obtain $\Phi(c) = (b_1 + a_2, b_2 + a_2, \ldots, b_n + a_n, a_1, a_2, \ldots, a_n) \in C_1 \otimes C_2$, therefore, $C_1 \otimes C_2 \subseteq \Phi(C)$.
Moreover, it is easy to see that $|C_1|.|C_2| = q^{2n} = |C|$. □

Let C_1 and C_2 be two codes over $\mathbb{F}_q$, by the definition **??**, then they are equivalent to a codes that has a generator matrices G_1 and G_2, respectively.

$$\begin{pmatrix} G_1 & \mathbf{0} \\ \mathbf{0} & G_2 \end{pmatrix} \tag{1.9}$$

Let C be a linear code of length n over R. If G_1 and G_2 are the generator matrices of a $\mathbb{F}_q$-linear codes C_1 and C_2, respectively, then the generator matrix of C is

$$\begin{pmatrix} vG_1 \\ (1 - v)G_2 \end{pmatrix} \tag{1.10}$$

It is clear that, if $G_1 = G_2$ then $G = G_1$.

The following Proposition shown that any linear code C over R can be uniquely expressed as a direct sum of two $\mathbb{F}_q$-linear codes.

Proposition 3. ? *Let C be a R-submodule of R^n. Then C can be written as*

$$C = vC_1 \oplus (1 - v)C_2. \tag{1.11}$$

Proof. Let $\mathbf{c} = (c_0, c_1, \ldots, c_n)$ be codeword in C, where $c_j = a_j + vb_j$ for $1 \leq j \leq n$. Then $(c_0, c_1, \ldots, c_n)$ expressed as

$$((b_0 + a_0)v + a_0(1 - v), (b_1 + a_1)v + a_1(1 - v), \ldots, (b_n + a_n)v + a_n(1 - v)),$$

this implies that

$$\mathbf{c} = v(b_0 + a_1, b_1 + a_1, \ldots, b_n + a_n) \oplus (1 - v)(a_0, a_1, \ldots, a_n) \in vC_1 \oplus (1 - v)C_2.$$

Completing the proof. □

Since Φ is preserving distance between the *lee distance* in R^n to the *Hamming distance* in $\mathbb{F}_q^n$. Then

$$d_L(C) = d_H(\Phi(C)) = d_H(C_1 \otimes C_2). \tag{1.12}$$

One gets $d_L = d_H = \min\{d_H(C_1), d_H(C_2)\}$. This result it follows from the next proposition.

Proposition 4. ? *Let C be a R-submodule of R^n. Let d_L and d_H be the minimum Lee distance and minimum Hamming distance of C, respectively. Then $d_L = d_H = \min\{d(C_1); d(C_2)\}$, where $d(C_1)$ and $d(C_2)$ denotes the minimum Hamming distance of C_1 and C_2 over $\mathbb{F}_q$ defined in (**??**), respectively.*

By Equation (**??**) and above Proposition it is easy to verify the following Corollary.

Corollary 2. ? *Let $C = vC_1 \oplus (1 - v)C_2$ be a R-submodule of R^n. Let C_1 (respectively C_2) be $[n, k_1, d(C_1)]$ (respectively $[n, k_2, d(C_2)]$) linear code over $\mathbb{F}_q$. Then $\Phi(C)$ is $[2n, k_1 + k_2, \min\{d(C_1), d(C_2)\}]$ linear code over $\mathbb{F}_q$.*

Now, we are ready to introduce the generator matrix over the ring R. It follows from the next Theorem.

Theorem 13. ? *Let C be a R-linear code of length n. Then C is permutation equivalent to an R-linear code with a generator matrix in the standard form*

$$\begin{pmatrix} I_{k_1} & A & B & D_1 + vD_2 \\ 0 & vI_{k_2} & 0 & vC \\ 0 & 0 & (1-v)I_{k_3} & (1-v)E \end{pmatrix} \tag{1.13}$$

where A, B, C, D_1, D_2, and E are $\mathbb{F}_q$-matrices.

Proof. Similar to (**?**, Proposition 1.1). It analogue to obtain the generator matrix over quaternary codes. □

A inner product between $\mathbf{x} = (a_0, a_1, \ldots, a_{n-1})$ and $\mathbf{y} = (b_0, b_1, \ldots, b_{n-1})$ in R^n is given by

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=0}^{n-1} a_i b_i \in R. \tag{1.14}$$

The dual code of an R-linear code C, denoted by $C^\perp$, is also R-linear code and is defined by

$$C^\perp := \{\mathbf{y} \in R^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}. \tag{1.15}$$

As for $\mathbb{F}_q$-codes, we say that a R-linear code C is *self-orthogonal* if $C = C^\perp$ and *self-dual* if $C = C^\perp$.

Lemma 5. ? *Let C be a R-linear code. Then $\phi(C)^\perp = \phi(C^\perp)$ and we have the commutative diagram*

$$\begin{array}{ccc} C & \to & \phi(C) \\ \downarrow & & \downarrow \\ C^\perp & \to & \phi(C^\perp) \end{array} .$$

Proof. Let $\mathbf{u} = (\mathbf{b} + \mathbf{a}, \mathbf{a}) \in \phi(C^\perp)$ where $(\mathbf{a} + v\mathbf{b}) \in \mathcal{C}^\perp$ with $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ in $\mathbb{F}_q^n$. Suppose that

$$\mathbf{v} = \phi(\mathbf{r} + v\mathbf{p}) = (\mathbf{p} + \mathbf{r}, \mathbf{r}) \in \phi(C),$$

where $(\mathbf{r} + v\mathbf{p}) \in C$ with $\mathbf{r} = (r_1, r_2, \ldots, r_n)$ and $\mathbf{p} = (p_1, p_2, \ldots, p_n)$ in $\mathbb{F}_q^n$. Then, by Equation (**??**), we have

$$\begin{aligned} \langle (\mathbf{a} + v\mathbf{b}), (\mathbf{r} + v\mathbf{p}) \rangle &= \langle \mathbf{a}, \mathbf{r} \rangle_q + v\left[\langle \mathbf{a}, \mathbf{p} \rangle_q + \langle \mathbf{b}, \mathbf{r} \rangle_q + \langle \mathbf{b}, \mathbf{p} \rangle_q\right] \\ &= \mathbf{0} + v\,\mathbf{0}. \end{aligned}$$

This implies that $\langle \mathbf{a}, \mathbf{r} \rangle_q = \mathbf{0}$ and $\langle \mathbf{a}, \mathbf{p} \rangle_q + \langle \mathbf{b}, \mathbf{r} \rangle_q + \langle \mathbf{b}, \mathbf{p} \rangle_q = \mathbf{0}$.
Hence, $\mathbf{u} = (\mathbf{b} + \mathbf{a}, \mathbf{a}) \in \phi(C)^\perp$ and $\phi(C^\perp) \subseteq \phi(C)^\perp$. Since ϕ is bijective, we have

$$|C^\perp| = |\phi(C^\perp)| = \frac{q^{2n}}{|C|} = \frac{q^{2n}}{|\phi(C)|} = |\phi(C)^\perp|.$$

Thus, $\phi(C^\perp) = \phi(C)^\perp$. □

For the proof of the following Theorem is immediately from the previous Lemma, and by Equation (**??**)

Theorem 14. **?** *Let C be a R-linear code of length n. Then $\Phi(C^{\perp}) = C_1^{\perp} \otimes C_2^{\perp}$. Moreover, $C^{\perp}$ is also uniquely expressed as*

$$v\, C_1^{\perp} \oplus (1-v)\, C_2^{\perp} \tag{1.16}$$

Next, we derive the generator matrix of the dual $C^{\perp}$ of a R-linear code C.

Proposition 5. **?** *Let C be a $\mathbb{F}_q + v\mathbb{F}_q$-linear code of length n. Then, he dual code $C^{\perp}$, under the inner product in Equation (**??**), has as generator the matrix H given by*

$$\begin{pmatrix} -(D_1 + vD_2)^{\top} + C^{\top}A^{\top} + E^{\top}B^{\top} & C^{\top} & E^{\top} & I_{n-k_1-k_2-k_3} \\ -vB^{\top} & 0 & vI_{k_3} & 0 \\ -(1-v)A^{\top} & (1-v)I_{k_2} & 0 & 0 \end{pmatrix} \tag{1.17}$$

where A, B, C, D_1, D_2, and E are $\mathbb{F}_q$-matrices.

1.3.3 Cyclic codes over $R = \mathbb{F}_q + v\mathbb{F}_q$

Now, we present a description of R-cyclic codes. Also, we give some definitions and results to define the most important class of linear codes. A subset C of R^n is said to be an R-cyclic code of length n if two conditions are satisfied:

1. C is an R-submodule of R^n.
2. $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$, for any codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$.

For the proof of the following theorems are introduced and generalized in **??**.

Theorem 15. **?** *Let $C = vC_1 \oplus (1-v)$ be a linear code of length n over R then C is cyclic code of length n over R if and only if C_1 and C_2 are cyclic codes of length n over $\mathbb{F}_q$.*

Proof. Similar to (**?**, Theorem 4.1). Here, we extends proof from $\mathbb{F}_2 + v\mathbb{F}_2$ to R. □

The following results classify all cyclic codes over R.

Theorem 16. **?** *Let $C = vC_1 \oplus (1-v)C_2$ be a cyclic code of length n over R. There exist a unique polynomial $f(X)$ such that $C = \langle f(X) \rangle$, where $f(X) = vf_1(X) + (1-v)f_2(X)$*

Corollary 3. **?** *Let $C = vC_1 \oplus (1-v)C_2$ be a cyclic code of length n over R and $f_1(X), f_2(X)$ are the generator polynomials of C_1 and C_2 respectively. Then*

$$|C| = q^{2n - \deg(f_1(X)) - \deg(f_2(X))}.$$

Next, we derive the generator polynomial of the dual code $C^{\perp}$ of an R-cyclic code C.

Theorem 17. ? *Let $C = vC_1 \oplus (1-v)C_2$ be a cyclic code of length n over R, then its dual code $C^{\perp}$ is also cyclic code. Moreover, we have $C^{\perp} = vC_1^{\perp} \oplus (1-v)C_2^{\perp}$.*

Corollary 4. ? *Let $C = \langle vf_1(X), (1-v)f_2(X)$ be a cyclic code of length n over R, with $f_1(X)$ and $f_2(X)$ as the generator polynomials of C_1 and C_2 respectively such that $X^n - 1 = f_1(X)h_1(X)$ and $X^n - 1 = f_2(X)h_2(X)$. Then*

1. *$C^{\perp} = \langle vh_1^*(X), (1-v)h_2^*(X)\rangle$ and $|C^{\perp}| = q^{\deg(f_1(X))+\deg(f_2(X))}$*
2. *$C^{\perp} = \langle h(X)\rangle$ where $h(X) = vh_1^*(X) + (1-v)h_2(X)$.*

The interested reader may consult **?**, for more details and proofs.

Lemma 6. ? *A linear cyclic code over $\mathbb{F}_q$ with generator polynomial $f(X)$ is self-orthogonal if and only if $h(X)h^*(X)|(X^n-1)$, where $h^*(X) = X^{\deg(h(X))h(X^{-1})}$ is the reciprocal polynomial of $h(X)$ with $h(X) = (X^n-1)/f(X)$.*

Theorem 18. ? *Suppose $C = \langle f(X)\rangle$ is cyclic code over R, where $f(X) = vf_1(X) + (1-v)f_2(X)$, then $C \subset C^{\perp}$ if and only if $C_1 \subset C_1^{\perp}$ and $C_2 \subset C_2^{\perp}$ where $C_1 = \langle f_1(X)\rangle$ and $C_2 = \langle f_2(X)\rangle$.*

Corollary 5. ? *Suppose $C = vC_1 \oplus (1-v)C_2$ is a cyclic code of arbitrary length n over R then $C \subset C^{\perp}$, if and only if $C_1 \subset C_1^{\perp}$ and $C_2 \subset C_2^{\perp}$.*

Lemma 7. ? *Let C_1 and C_2 be two linear codes if length n over $\mathbb{F}_q$ and*

$$C = vC_1 \oplus (1-v)C_2 = \{(vc_1 + (1-v)c_2), c_1 \in C_1, c_2 \in C_2\},$$

we have

$$C^{\perp} = vC_1^{\perp} \oplus (1-v)C_2^{\perp} = \{(vc_1 + (1-v)c_2), c_1 \in C_1^{\perp}, c_2 \in C_2^{\perp}\},$$

C is self-dual if and only if C_1 and C_2 are self-dual.

Proposition 6. ? *Let C_1, C_2, C_1' and C_2' be four linear codes of length n over $\mathbb{F}_q$. Then*

$$C = vC_1 \oplus (1-v)C_2 = \{(vc_1 + (1-v)c_2), c_1 \in C_1, c_2 \in C_2\},$$

is equivalent to

$$C' = vC_1' \oplus (1-v)C_2' = \{(vc_1' + (1-v)c_2'), c_1' \in C_1', c_2' \in C_2'\},$$

over R if and only if C_1 and C_2 are equivalent respectively to C_1' and C_2'.

Chapter 2

Linear codes over $\mathbb{F}_4 R$ and their MacWilliams identity

In this chapter, we construct error control codes over a new alphabet set, we focus on linear codes over mixed alphabets. In particular, we study the structure of linear codes over the ring $\mathbb{F}_q R$, where $\mathbb{F}_4$ be the field of four elements. We denote by R the commutative ring, with 16 elements, $\mathbb{F}_4 + v\mathbb{F}_4 := \{a + vb \mid a, b \in \mathbb{F}_4\}$ with $v^2 = v$. First, we define linear codes over the ring of mixed alphabets $\mathbb{F}_4 R$ as well as their dual codes under a nondegenerate inner product. Next, we derive the systematic form of the respective generator matrices of the codes and their dual codes. Finally, we establish the MacWilliams identity for linear codes over $\mathbb{F}_4 R$. We refer to see **???**

2.1 Introduction

We recall some definitions and notations to describe our results.
Let I_n be the identity $n \times n$ matrix. Let $\mathbf{0}$ denote either the zero vector or the all-zero matrix whose dimension is clear from the context. Vectors are denoted by bold lower case letters. For example, $(\mathbf{x}_n, \mathbf{y}_m)$ denotes $(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$ for $\mathbf{x}_n := (x_1, x_2, \ldots, x_n)$ and $\mathbf{y}_m := (y_1, y_2, \ldots, y_m)$.

We write the finite field with four elements as $\mathbb{F}_4 = \{0, 1, w, w^2 = 1 + w\}$ and denote by R the commutative ring $R := \mathbb{F}_4 + v\mathbb{F}_4 := \{a + vb : a, b \in \mathbb{F}_4\}$ with 16 elements where $v^2 = v$. It is well-known that R is a finite non-chain ring with two maximal ideals $\langle v \rangle$ and $\langle v + 1 \rangle$, making each of $R/\langle v \rangle$ and $R/\langle v + 1 \rangle$ isomorphic to $\mathbb{F}_4$.

Definition 12. *Let R be any commutative ring and let θ be an automorphism of S. The skew polynomial ring $R[X, \theta]$ is defined by*

$$R[X,\theta] = \left\{ \begin{array}{c} f(X) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n | \\ a_i \in R \textit{ for all } i = 0, 1, \ldots, n \end{array} \right\},$$

where addition of these polynomials is defined in the usual way while multiplication is defined using the distributive law and the rule

$$(aX^i) \cdot (bX^j) = a\theta^i(b)X^{i+j}$$

The ring $R[X, \theta]$ is not commutative even when R is. Therefore, when we talk about divisibility, we need to specify left or right divisibility, and when we discuss ideals we need to talk about left, right, or two-sided ideals. For example, we say that $f(X)$ is a left divisor of $g(X)$ in $R[X, \theta]$ if there exists $h(X) \in R[X, \theta]$ such that $g(X) = f(X) \cdot h(X)$ with skew multiplication of polynomials. Please note that, given a ring S, the notation $R[X, \theta]/\left\langle X^\beta - 1 \right\rangle$ does not automatically imply that a quotient ring structure is defined. It denotes the quotient space, that is, the set of cosets of the additive group $\left\langle X^\beta - 1 \right\rangle$.

Definition 13. *Let an automorphism θ over R be defined by*

$$\theta : R \mapsto R \textit{ sending } a + vb \mapsto a^2 + (v+1)\, b^2. \tag{2.1}$$

Restricted to $\mathbb{F}_4$, it interchanges w and w^2 while keeping $\{0, 1\}$ fixed. Note that our θ here is equal to the composition of automorphisms $\varphi \circ \theta_1$ in **?**. If θ be an identity, then the skew polynomial ring $R[X, \theta]$ is equal to the commutative ring $R[X]$. We use the identity *automorphism* θ throughout the chapter.

Let α and β be nonnegative integers. A linear code C_1 of length α over $\mathbb{F}_4$ is a subspace of $\mathbb{F}_4^\alpha$. The number of codewords in a k_0-dimensional code C_1 of $\mathbb{F}_4^\alpha$ is 4^{k_0}. Analogously, a linear code C_2 over R has been defined to be a submodule of R^β. The discussion in (**?**, Section 2), using the results established in (**?**, Sections 2 and 3), showed that if C_2 is a linear code over R, then it has $4^{2k_1+k_2+k_3}$ codewords for some nonnegative integers k_1, k_2, and k_3. For any element in R, we introduce a new ring homomorphism

$$\eta : R \mapsto \mathbb{F}_4 \text{ sending } a + vb \text{ to } a. \tag{2.2}$$

Let $\mathbb{F}_4R := \{(a,b) : a \in \mathbb{F}_4 \text{ and } b \in R\}$. It is straightforward to verify that $\mathbb{F}_4R$ is an R-module under the multiplication

$$d * (a,b) = (\eta(d)a, db) \text{ with } d \in R \text{ and } (a,b) \in \mathbb{F}_4R. \tag{2.3}$$

Let $\mathbf{x} := (a_1, a_2, \ldots, a_\alpha, b_1, b_2, ..., b_\beta) \in \mathbb{F}_4^\alpha R^\beta$ and $d \in R$. The multiplication extends naturally to

$$d * \mathbf{x} = (\eta(d)a_1, \eta(d)a_2, \ldots, \eta(d)a_\alpha, db_1, db_2, \ldots, db_\beta). \tag{2.4}$$

Definition 14. *A nonempty subset $\mathcal{C}$ of $\mathbb{F}_4^\alpha R^\beta$ is an $\mathbb{F}_4R$-linear code if it is an R-submodule of $\mathbb{F}_4^\alpha R^\beta$ with respect to the scalar multiplication $*$ in Equation (**??**). An $\mathbb{F}_4^\alpha R^\beta$-linear code is a generalization of a linear code over $\mathbb{F}_4$ when $\beta = 0$ and a linear code over a finite non-chain ring over R when $\alpha = 0$.*

Two $\mathbb{F}_4R$-linear codes of the same length and cardinality are *equivalent* if one can be obtained from the other by a composition of operations of the following types: (a) any permutation of the first α positions, (b) any permutation of the last β positions, and (c) multiplication of the symbols appearing in a fixed position by a nonzero scalar. An $\mathbb{F}_4R$-linear code $\mathcal{C}$, seen as a group, is isomorphic to $\mathbb{F}_4^{k_0} \times \mathbb{F}_4^{2k_1} \times \mathbb{F}_4^{k_2} \times \mathbb{F}_4^{k_3}$ and we say that $\mathcal{C}$ has *type* $(\alpha, \beta; k_0, k_1, k_2, k_3)$.

2.2 Generator Matrices

Obtaining a standard form of the generator matrix of a linear code is useful. It helps in constructing or searching for codes with some desired properties. When the search space is large, a standard form often leads to algorithmic tools with least time and or memory complexities.

Theorem 19. *Let $\mathcal{C}$ be a $\mathbb{F}_4R$-linear code of type $(\alpha, \beta; k_0, k_1, k_2, k_3)$ Then $\mathcal{C}$ is permutation equivalent to an $\mathbb{F}_4R$-linear code with a generator matrix in the standard form*

$$G = \left(\begin{array}{cc|cccc} I_{k_0} & M & 0 & 0 & 0 & vT \\ 0 & S & I_{k_1} & A & B & D_1 + vD_2 \\ 0 & 0 & 0 & vI_{k_2} & 0 & vC \\ 0 & 0 & 0 & 0 & (1+v)I_{k_3} & (1+v)E \end{array}\right) \tag{2.5}$$

where M, A, B, C, D_1, D_2, E, S, and T are $\mathbb{F}_4$-matrices.

Proof. It is well-known that any linear code over $\mathbb{F}_4$ is equivalent to one that has a generator matrix of the form $G_1 := \begin{pmatrix} I_{k_0} & M' \end{pmatrix}$. where M' is an $\mathbb{F}_4$ matrix. We know from (**?**, Section 3) that any linear code over $\mathbb{F}_4 + v\mathbb{F}_4$ is equivalent to a code that has a generator matrix of the form

$$G_2 := \begin{pmatrix} I_{k_1} & A' & B' & D_1' + vD_2' \\ 0 & vI_{k_2} & 0 & vC' \\ 0 & 0 & (1+v)I_{k_3} & (1+v)E' \end{pmatrix} \tag{2.6}$$

where A', B', C', D_1', D_2', and E' are $\mathbb{F}_4$-matrices. We can now combine the two matrices by putting the matrix G_1 on the first α coordinates and the matrix G_2 on the last β coordinates before filling up the other entries to arrive at the matrix

$$\left(\begin{array}{cc|cccc} I_{k_0} & M' & M_1 & M_2 & M_3 & M_4 \\ P_1 & Q_1 & I_{k_1} & A' & B' & D_1' + D_2' \\ P_2 & Q_2 & 0 & vI_{k_2} & 0 & vC' \\ P_3 & Q_3 & 0 & 0 & (1+v)I_{k_3} & (1+v)E' \end{array}\right)$$

where P_ℓ, Q_ℓ, and M_k are suitable $\mathbb{F}_4$-matrices for $1 \le \ell \le 3$ and $1 \le k \le 4$. By applying the necessary row and column operations to the matrix we obtain, as promised,

$$G = \left(\begin{array}{cc|cccc} I_{k_0} & M & 0 & 0 & 0 & vT \\ 0 & S & I_{k_1} & A & B & D_1 + vD_2 \\ 0 & 0 & 0 & vI_{k_2} & 0 & vC \\ 0 & 0 & 0 & 0 & (1+v)I_{k_3} & (1+v)E \end{array}\right).$$

□

We can now repeat the analysis for the dual codes. The standard Euclidean inner product of $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$ in $\mathbb{F}_4^n$, denoted by $\langle \mathbf{a}, \mathbf{b} \rangle_4$, is given, as usual, by

$$\langle \mathbf{a}, \mathbf{b} \rangle_4 := \sum_{j=1}^{n} a_j b_j \in \mathbb{F}_4.$$

Given two elements $\mathbf{x}, \mathbf{y} \in \mathbb{F}_4^\alpha \times (\mathbb{F}_4 + v\mathbb{F}_4)^\beta$ with

$$\mathbf{x} := (x_1, x_2, \ldots, x_\alpha, x_{\alpha+1}, x_{\alpha+2}, \ldots, x_{\alpha+\beta}) \text{ and}$$

$$\mathbf{y} := (y_1, y_2, \ldots, y_\alpha, y_{\alpha+1}, y_{\alpha+2}, \ldots, y_{\alpha+\beta}),$$

we define their *inner product* to be

$$\langle \mathbf{x}, \mathbf{y} \rangle = \left[\sum_{j=\alpha+1}^{\alpha+\beta} x_j y_j + v \left(\sum_{i=1}^{\alpha} x_i y_i \right) \right] \in \mathbb{F}_4 + v\mathbb{F}_4. \tag{2.7}$$

It is immediate to verify that the inner product is nondegenerate. If $\mathcal{C}$ is a linear code over $\mathbb{F}_4 R$, then the dual of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is

$$\mathcal{C}^\perp \triangleq \{\mathbf{y} \in \mathbb{F}_4^\alpha R^\beta \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in \mathcal{C}\} \tag{2.8}$$

For $a + vb \in R$, the classical Gray map $\phi^* : R \mapsto \mathbb{F}_4^2$ sends $a + vb$ to $(a + b, a)$. The *Lee weight* of any element in R is the *Hamming weight* of its image under ϕ^*. This map extends naturally to R^n. For any $\mathbf{x} = (x_1, x_2, \ldots, x_\alpha) \in \mathbb{F}_4^\alpha$ and $\mathbf{b} = (\mathbf{z} + v\mathbf{y}) = (z_1 + vy_1, z_2 + vy_2, \ldots, z_\beta + vy_\beta) \in R^\beta$ the *Gray map* over $\mathbb{F}_4 R$ is defined by

$$\phi : \mathbb{F}_4^\alpha R^\beta \mapsto \mathbb{F}_4^{\alpha+2\beta} \text{ with } \phi(\mathbf{x}, \mathbf{b}) = \phi(\mathbf{x}, \mathbf{z} + v\mathbf{y}) = (\mathbf{x}, \mathbf{z} + \mathbf{y}, \mathbf{z}). \tag{2.9}$$

The map ϕ is an isometry which transforms the Lee distance in $\mathbb{F}_4^\alpha R^\beta$ to the Hamming distance in $\mathbb{F}_4^{\alpha+2\beta}$. For any $\mathbb{F}_4 R$-linear code $\mathcal{C}$, the code $\phi(\mathcal{C})$ is $\mathbb{F}_4$-linear. Furthermore, since the inner product in Equation (**??**) is nondegenerate, we have $|\mathcal{C}| \cdot |\mathcal{C}^\perp| = |\phi(\mathcal{C})| \cdot |\phi(\mathcal{C})^\perp| = 4^{\alpha+2\beta}$.

Lemma 8. *The mapping $\phi : \mathbb{F}_4^\alpha R^\beta \mapsto \mathbb{F}_4^{\alpha+2\beta}$ is a bijection.*

Proof. It is clear that ϕ is one-to-one. Let $(\mathbf{x}, \mathbf{v}_1, \mathbf{v}_2) \in \mathbb{F}_4^{\alpha+2\beta}$ be such that $\mathbf{x} \in \mathbb{F}_4^\alpha$ and both $\mathbf{v}_1$ and $\mathbf{v}_2$ are in $\mathbb{F}_4^\beta$. Let $\mathbf{y} = \mathbf{v}_1 + \mathbf{v}_2$, and $\mathbf{z} = \mathbf{v}_2$. Then, $\phi(\mathbf{x}, \mathbf{z} + v\mathbf{y}) = (\mathbf{x}, \mathbf{v}_1, \mathbf{v}_2)$ and, hence, the mapping ϕ is onto. □

There are numerous occasions where the Gray image of an $\mathbb{F}_4 R$-linear code, seen now as an $\mathbb{F}_4$-linear code, has good parameters. In the next three examples, we provide $\mathbb{F}_4 R$-linear codes whose Gray images yield $\mathbb{F}_4$-linear codes with good parameters, based on the corresponding entries in the Grassl Table **?**.

Example 1. *Let $\mathcal{C}$ be an $\mathbb{F}_4 R$-linear code generated by*

$$G_1 = \left(\begin{array}{ccc|cccc} 1 & 0 & 1 & w + vw^2 & 0 & w^2 + v & 1 + vw \\ 0 & 1 & 1 & 0 & w + vw^2 & 1 + vw & w^2 + v \end{array} \right).$$

The Gray image $\phi(\mathcal{C})$ is an optimal $\mathbb{F}_4$-linear code of length 11, dimension 2, and minimum distance 8. Its generator matrix, as a code over $\mathbb{F}_4$ is

$$\phi(G_1) = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & w & w^2 & w & 0 & w^2 & 1 \\ 0 & 1 & 1 & 0 & 1 & w^2 & w & 0 & w & 1 & w^2 \end{pmatrix}.$$

Example 2. *Let $\mathcal{C}$ be an an $\mathbb{F}_4R$-linear code generated by a single codeword*

$$\mathbf{v} = \left(\underbrace{1, 1, \ldots, 1}_{\alpha} \mid \underbrace{1 + vw^2, 1 + vw^2, \ldots, 1 + vw^2}_{\beta} \right).$$

The image under the Gray map is, therefore, an $\mathbb{F}_4$-linear code generated by

$$\phi(\mathbf{v}) = \left(\underbrace{1, 1, \ldots, 1,}_{\alpha} \underbrace{w, w, \ldots, w,}_{\beta} \underbrace{1, 1, \ldots, 1}_{\beta} \right).$$

The latter is a maximal distance separable (MDS) code of length $n = \alpha + 2\beta$, dimension 1, and minimum distance n. Its dual, under the usual Euclidean or Hermitian inner product, is an MDS code of dimension $n - 1$ and minimum distance 2.

Example 3. *Let $\mathcal{C}$ be an $\mathbb{F}_4R$-linear code generated by*

$$G_2 = \left(\begin{array}{ccccc|cccccc} 1 & 0 & 0 & 1 & w^2 & w + vw^2 & 0 & 0 & w + vw^2 & 1 + vw & 1 + vw \\ 0 & 1 & 0 & w^2 & w^2 & 0 & w + vw^2 & 0 & 1 + vw & 1 + vw & w + vw^2 \\ 0 & 0 & 1 & w^2 & 1 & 0 & 0 & w + vw^2 & 1 + vw & w + vw^2 & 1 + vw \end{array} \right).$$

The Gray image $\phi(\mathcal{C})$ is an $\mathbb{F}_4$-linear code of length 17, dimension 3, and minimum distance 11. As a code over $\mathbb{F}_4$, it is generated by

$$\phi(G_2) = \begin{pmatrix} 1 & 0 & 0 & 1 & w^2 & 1 & 0 & 0 & 1 & w^2 & w^2 & 1 & 0 & 0 & 1 & w^2 & w^2 \\ 0 & 1 & 0 & w^2 & w^2 & 0 & 1 & 0 & w^2 & w^2 & 1 & 0 & 1 & 0 & w^2 & w^2 & 1 \\ 0 & 0 & 1 & w^2 & 1 & 0 & 0 & 1 & w^2 & 1 & w^2 & 0 & 0 & 1 & w^2 & 1 & w^2 \end{pmatrix}.$$

The optimal minimum distance of an $\mathbb{F}_4$-linear code of length 17 and dimension 3 is 12. Our code $\phi(\mathcal{C})$ here has distance one less than optimal. It corrects the same number of errors, which is 5, as the optimal one.

2.3 Parity-check Matrices

Lemma 9. *Let $\mathcal{C}$ be an $\mathbb{F}_4R$-linear code. Then $\phi(\mathcal{C})^\perp = \phi(\mathcal{C}^\perp)$ and we have the commutative diagram*

$$\begin{array}{ccc} \mathcal{C} & \to & \phi(\mathcal{C}) \\ \downarrow & & \downarrow \\ \mathcal{C}^\perp & \to & \phi(\mathcal{C}^\perp) \end{array}.$$

Proof. Let $\mathbf{u} = (\mathbf{x}, \mathbf{y}+\mathbf{z}, \mathbf{z}) \in \phi(\mathcal{C}^\perp)$ where $(\mathbf{x}, \mathbf{z}+v\mathbf{y}) \in \mathcal{C}^\perp$. Suppose that $\phi(\mathbf{e}, \mathbf{r}+v\mathbf{p}) = \mathbf{v} = (\mathbf{e}, \mathbf{p}+\mathbf{r}, \mathbf{r}) \in \phi(\mathcal{C})$ where $(\mathbf{e}, \mathbf{r}+v\mathbf{p}) \in \mathcal{C}$. Then, by Equation (**??**), we have

$$\begin{aligned} \langle (\mathbf{x}, \mathbf{z}+v\mathbf{y}), (\mathbf{e}, \mathbf{r}+v\mathbf{p}) \rangle &= v\langle \mathbf{x}, \mathbf{e} \rangle_4 + \langle \mathbf{z}, \mathbf{r} \rangle_4 + v\langle \mathbf{z}, \mathbf{p} \rangle_4 + v\langle \mathbf{y}, \mathbf{r} \rangle_4 + v\langle \mathbf{y}, \mathbf{p} \rangle_4 \\ &= v\left[\langle \mathbf{x}, \mathbf{e} \rangle_4 + \langle \mathbf{z}, \mathbf{p} \rangle_4 + \langle \mathbf{y}, \mathbf{r} \rangle_4 + \langle \mathbf{y}, \mathbf{p} \rangle_4\right] + \langle \mathbf{z}, \mathbf{r} \rangle_4 = 0 + v\,0. \end{aligned}$$

This implies that $\langle \mathbf{x}, \mathbf{e} \rangle_4 + \langle \mathbf{z}, \mathbf{p} \rangle_4 + \langle \mathbf{y}, \mathbf{r} \rangle_4 + \langle \mathbf{y}, \mathbf{p} \rangle_4 = 0$ and $\langle \mathbf{z}, \mathbf{r} \rangle_4 = 0$. It is now clear that

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} \rangle_4 = \langle \mathbf{x}, \mathbf{e} \rangle_4 + \langle \mathbf{y}+\mathbf{z}, \mathbf{p}+\mathbf{r} \rangle_4 + \langle \mathbf{z}, \mathbf{r} \rangle_4 = \\ \langle \mathbf{x}, \mathbf{e} \rangle_4 + \langle \mathbf{y}, \mathbf{p} \rangle_4 + \langle \mathbf{y}, \mathbf{r} \rangle_4 + \langle \mathbf{z}, \mathbf{p} \rangle_4 + \langle \mathbf{z}, \mathbf{r} \rangle_4 + \langle \mathbf{z}, \mathbf{r} \rangle_4 = 0. \end{aligned}$$

Hence, $\mathbf{u} = (\mathbf{x}, \mathbf{y}+\mathbf{z}, \mathbf{z}) \in \phi(\mathcal{C})^\perp$ and $\phi(\mathcal{C}^\perp) \subseteq \phi(\mathcal{C})^\perp$. Since ϕ is bijective, we have

$$|\mathcal{C}^\perp| = |\phi(\mathcal{C}^\perp)| = \frac{4^{\alpha+2\beta}}{|\mathcal{C}|} = \frac{4^{\alpha+2\beta}}{|\phi(\mathcal{C})|} = |\phi(\mathcal{C})^\perp|.$$

Thus, $\phi(\mathcal{C}^\perp) = \phi(\mathcal{C})^\perp$. □

Example 4. *Let $\mathcal{C}$ be the code in Example* **??**. *We have that $\phi(\mathcal{C}^\perp)$ is an $\mathbb{F}_4$-linear code of length 5 and dimension 4 with generator matrix*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & w & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

There are 4^4 codewords in $\phi(\mathcal{C}^\perp) = \phi(\mathcal{C})^\perp$.

We now derive the generator matrix of the dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ of a given type.

Theorem 20. *Let $\mathcal{C}$ be an $\mathbb{F}_4R$-linear code of type $(\alpha, \beta; k_0, k_1, k_2, k_3)$. Then, the dual code $\mathcal{C}^\perp$, under the inner product in Equation (**??**), has as generator the matrix H given by*

$$\left(\begin{array}{cc|cccc} M^\top & I_{\alpha-k_0} & -vS^\top & 0 & 0 & 0 \\ T^\top & 0 & -(D_1+vD_2)^\top + C^\top A^\top + E^\top B^\top & C^\top & E^\top & I_{\beta-k_1-k_2-k_3} \\ 0 & 0 & -vB^\top & 0 & vI_{k_3} & 0 \\ 0 & 0 & -(1+v)A^\top & (1+v)I_{k_2} & 0 & 0 \end{array}\right). \tag{2.10}$$

Proof. Let $\mathcal{C}'$ be an $\mathbb{F}_4R$-linear code generated by H given in Equation (**??**). It is clear that $\mathcal{C}' \subseteq \mathcal{C}^\perp$ since $HG^\top = \mathbf{0}$.

Let $\mathbf{c} = (a_1, a_2, \ldots, a_\alpha, b_1, b_2, \ldots, b_\beta) \in \mathcal{C}^\perp$. After adding some linear combination of the first $\beta - k_1 - k_2 - k_3$ rows of the matrix H in Equation (**??**) to $\mathbf{c}$ we obtain a codeword of $\mathcal{C}^\perp$ of the form

$$\mathbf{c}' = (0, \ldots, 0, c_1, \ldots, c_{k_1}, c_{k_1+1}, \ldots, c_{k_1+k_2}, c_{k_1+k_2+1}, \ldots, c_{k_1+k_2+k_3}, 0, \ldots, 0).$$

Since $\mathbf{c}'$ is orthogonal to the last k_3 rows of the matrix G in Equation (**??**), the entries $c_{k_1+k_2+j}$ must be either 0 or v for <u>all</u> $1 \leq j \leq k_3$.

Next, we add some linear combination of the middle k_3 rows of H to $\mathbf{c}'$ to obtain a codeword $\mathbf{c}'' \in \mathcal{C}^\perp$ of the form $\mathbf{c}'' = (0, \ldots, 0, c_1, \ldots, c_{k_1}, c_{k_1+1}, \ldots, c_{k_1+k_2}, 0, \ldots, 0)$. Since $\mathbf{c}''$ is orthogonal to the middle k_2 rows of G, the entries $c_{k_1+k_2+j}$ must be either 0 or $1+v$ for <u>all</u> $1 \leq j \leq k_3$. After adding some linear combination of the last k_2 rows of H to $\mathbf{c}''$, we get to a codeword $\mathbf{c}''' \in \mathcal{C}^\perp$ that has the form $\mathbf{c}''' = (0, \ldots, 0, c_1, \ldots, c_{k_1}, 0, \ldots, 0)$. Since $\mathbf{c}'''$ is orthogonal to the middle k_1 rows of G, we infer $c_1 = \ldots = c_{k_1} = 0$, which means $\mathbf{0} \in \mathcal{C}'$. Thus, $\mathbf{c} = (a_1, c_2, \ldots, a_\alpha, b_1, c_2, \ldots, b_\beta) \in \mathcal{C}'$. □

To illustrate the process explained above, we present two examples. Example **??** exhibits the steps taken to express the respective generator and parity check matrices of a given code in the standard form. Example **??** present the Gray image $\phi(\mathcal{C})$ of an $\mathbb{F}_4R$-linear code $\mathcal{C}$.

Example 5. *Let $\mathcal{C}$ be the type $(3,5;1,2,1,0)$ linear code over $\mathbb{F}_4^3 \times R^5$ generated by*

$$G_{\mathcal{C}} := \left(\begin{array}{ccc|ccccc} 1 & w^2 & w^2 & 0 & 1 & 0 & wv & 0 \\ 1 & 1 & w^2 & 1 & 0 & w & vw^2 & vw \\ 1 & 0 & 1 & 1 & 1 & w & 0 & vw^2 \\ 1 & 0 & 1 & 1 & 1 & v+w & 0 & vw \end{array}\right).$$

Now, applying elementary row operations to the above generator matrix, we obtain the standard form

$$G = \left(\begin{array}{ccc|ccccc} 1 & w & 1 & 0 & 0 & 0 & v & v \\ 0 & w^2 & w & 1 & 0 & w & vw & vw^2 \\ 0 & 1 & w & 0 & 1 & 0 & vw^2 & v \\ 0 & 0 & 0 & 0 & 0 & v & 0 & v \end{array}\right).$$

The code $\mathcal{C}$ has $|\mathcal{C}| = 4^1 \times 4^{2\times 2} \times 4^1 = 4096$ codewords.

The parity-check matrix H of $\mathcal{C}$, in the standard form, is

$$H = \left(\begin{array}{ccc|ccccc} w & 1 & 0 & vw^2 & v & 0 & 0 & 0 \\ 1 & 0 & 1 & vw & vw & 0 & 0 & 0 \\ 1 & 0 & 0 & vw & vw^2 & 0 & 1 & 0 \\ 1 & 0 & 0 & w+vw^2 & v & v & 0 & 1 \\ 0 & 0 & 0 & (1+v)w & 0 & 1+v & 0 & 0 \end{array}\right).$$

Example 6. *Let $\mathcal{C}$ be the linear code over $\mathbb{F}_4^5 \times R^6$ of type $(5,6;2,3,1,1)$ with*

$$G_{\mathcal{C}} := \left(\begin{array}{ccccc|cccccc} w^2 & 1 & w & 1 & 0 & w+vw & 0 & 0 & v & w+vw & w+vw \\ 0 & w^2 & 0 & w & 1 & v & 0 & 1 & 0 & v & v \\ w & 0 & w & 0 & 0 & w^2+v & 1 & 0 & 1 & v & 1+v \\ 0 & 1 & 0 & w^2 & w & vw^2 & 1 & w & 1 & vw^2 & vw^2 \\ 1 & 1 & 1 & w & w^2 & w+vw^2 & w & w & 1 & vw^2 & w+vw^2 \\ w^2 & 1 & w & 1 & 0 & w+vw^2 & 1+v & 0 & 0 & w^2+vw & v \\ w & 0 & w^2 & w^2 & w^2 & vw & w^2+v & w & 1+v & w^2+vw^2 & w \end{array}\right).$$

Now, applying elementary row and column operations to the above generator matrix, we obtain the standard form

$$G = \left(\begin{array}{ccccc|cccccc} 1 & 0 & w & 1 & 0 & 0 & 0 & 0 & 0 & 0 & v \\ 0 & 1 & 0 & w & 1 & 0 & 0 & 0 & 0 & 0 & v \\ 0 & 0 & w & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1+v \\ 0 & 0 & 0 & w^2 & w & 0 & 1 & 0 & 1 & 0 & vw^2 \\ 0 & 0 & 1 & w & w^2 & 0 & 0 & 1 & 1 & w & w+vw^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v & 0 & vw \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1+v & (1+v)w \end{array}\right).$$

The code $\mathcal{C}$ has $|\mathcal{C}| = 4^2 \times 4^{2\times 3} \times 4^1 \times 4^1 = 4^9$ codewords.

The parity-check matrix H of $\mathcal{C}$, in the standard form, is

$$H = \left(\begin{array}{ccccc|cccccc} w & 0 & 1 & 0 & 0 & vw & 0 & v & 0 & 0 & 0 \\ 1 & w & 0 & 1 & 0 & 0 & vw^2 & vw & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & vw & vw^2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1+v & w+vw^2 & w^2+vw^2 & w & w & 1 \\ 0 & 0 & 0 & 0 & 0 & v & 0 & vw & 0 & v & 0 \\ 0 & 0 & 0 & 0 & 0 & 1+v & 1+v & 1+v & 1+v & 0 & 0 \end{array}\right).$$

2.4 MacWilliams identity over $\mathbb{F}_4 R$

Let $\mathbf{x} = (x_1, x_2, \ldots, x_\alpha, x_{\alpha+1}, x_{\alpha+2}, \ldots, x_{\alpha+\beta}) = (\mathbf{x}_\alpha, \mathbf{x}_\beta) \in \mathbb{F}_4^\alpha R^\beta$ and recall that the Lee weight of $a + vb \in \mathbb{F}_4 R$, denoted by $\mathrm{w_L}(a + vb)$, is given by $\mathrm{w_H}(a + b, a)$. Hence, the weight of $\mathbf{x}$ is defined to be $\mathrm{wt}(\mathbf{x}) := \mathrm{w_H}(\mathbf{x}_\alpha) + \mathrm{w_L}(\mathbf{x}_\beta)$. We consider $\mathbb{F}_4$ as an extension of degree 2 over $\mathbb{F}_2$ with basis $\{1, w\}$, where w is a primitive element of $\mathbb{F}_4$ such that $w^3 = 1$. We write any $b \in \mathbb{F}_4$ as $b := b_0 + b_1 w$, with $b_0, b_1 \in \mathbb{F}_2$, and define the map $\tau : \mathbb{F}_4 \mapsto \mathbb{F}_2$ to send $b \to \tau(b) = b_1$.

Definition 15. *The map $\chi : R \mapsto \mathbb{C}^*$ that sends $\chi(a + vb) \to (-1)^{\tau(b)}$ for all $a + vb \in R$ is a nontrivial character of R.*

The next lemma follows immediately from how the map χ is defined.

Lemma 10. *Let χ be the nontrivial character defined on R in Definition* **??**. *Then the following properties hold.*

1. *For all $x, y \in R$, we have $\chi(x+y) = \chi(x) \cdot \chi(y)$.*
2. *For any fixed $y \in R$, we have $\sum_{x \in R} \chi(xy)$*

Lemma 11. *Let $\mathcal{C}$ be an $\mathbb{F}_4 R$-linear code. Let $\mathbf{x} := (\mathbf{x}_\alpha, \mathbf{x}_\beta)$ and $\mathbf{y} := (\mathbf{y}_\alpha, \mathbf{y}_\beta)$ be elements in $\mathbb{F}_4^\alpha R^\beta$. Then*

$$\sum_{\mathbf{x} \in \mathcal{C}} \chi(\langle \mathbf{x}, \mathbf{y} \rangle) = \begin{cases} 0 & \text{if } \mathbf{y} \notin \mathcal{C}^\perp, \\ |\mathcal{C}| & \text{if } \mathbf{y} \in \mathcal{C}^\perp. \end{cases} \tag{2.11}$$

Proof. If $\mathbf{y} \in \mathcal{C}^\perp$, then $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ for any $\mathbf{x} \in \mathcal{C}$. This implies $\chi(\langle \mathbf{x}, \mathbf{y} \rangle) = \chi(0) = 1$. Hence,

$$\sum_{\mathbf{x} \in \mathcal{C}} \chi(\langle \mathbf{x}, \mathbf{y} \rangle) = \sum_{\mathbf{x} \in \mathcal{C}} 1 = |\mathcal{C}|.$$

Now, let $\mathbf{y} \notin \mathcal{C}^\perp$. Then $\langle \mathbf{x}, \mathbf{y} \rangle \neq 0$ for all $\mathbf{x} \in \mathcal{C}$. Since $\sum_{i=1}^{\alpha} x_i y_i \in \mathbb{F}_4$, we write

$$\begin{aligned} \chi(\langle \mathbf{x}, \mathbf{y} \rangle) &= \chi\left(\sum_{j=\alpha+1}^{\alpha+\beta} x_j y_j \right) \chi\left(v\left(\sum_{i=1}^{\alpha} x_i y_i \right) \right) \\ &= \left[\prod_{j=\alpha+1}^{\alpha+\beta} \chi(x_j y_j) \right] (-1)^{\tau\left(\sum_{i=1}^{\alpha} x_i y_i \right)}. \end{aligned} \tag{2.12}$$

Summing up over all elements $\mathbf{x} \in \mathcal{C}$, one arrives at

$$\begin{aligned} \sum_{\mathbf{x} \in \mathcal{C}} \chi(\langle \mathbf{x}, \mathbf{y} \rangle) &= \sum_{\mathbf{x} \in \mathcal{C}} \left((-1)^{\tau\left(\sum_{i=1}^{\alpha} x_i y_i \right)} \cdot \prod_{j=\alpha+1}^{\alpha+\beta} \chi(x_j y_j) \right) \\ &= \sum_{\mathbf{x}_\alpha \in \mathbb{F}_4^\alpha} (-1)^{\tau\left(\sum_{i=1}^{\alpha} x_i y_i \right)} \cdot \sum_{\mathbf{x}_\beta \in R^\beta} \prod_{j=\alpha+1}^{\alpha+\beta} \chi(x_j y_j) \\ &= \sum_{\mathbf{x}_\alpha \in \mathbb{F}_4^\alpha} (-1)^{\tau\left(\sum_{i=1}^{\alpha} x_i y_i \right)} \underbrace{\prod_{j=\alpha+1}^{\alpha+\beta} \sum_{x_j \in R} \chi(x_j y_j)}_{=0} \\ &= \sum_{\mathbf{x} \in \mathcal{C}} (-1)^{\tau\left(\sum_{i=1}^{\alpha} x_i y_i \right)} \cdot 0 = 0. \end{aligned}$$

□

Lemma 12. *For any fixed $b \in R$, we have*

$$\sum_{a\in R} \chi(ab)\ X^{2-\mathrm{wt}(a)}\ Y^{\mathrm{wt}(a)} = (X+3Y)^{2-\mathrm{wt}(b)}\ (X-Y)^{\mathrm{wt}(b)}.$$

Proof. We partition the set $R \setminus \{0\}$ into

$$A := \{v,\ wv,\ w^2v,\ v+1,\ wv+w,\ w^2v+w^2\} \text{ and}$$
$$B := \{1,\ w,\ w^2,\ wv+1,\ w^2v+1,\ v+w,\ w^2v+w,\ v+w^2,\ wv+w^2\}.$$

By the definition of the Lee weight over R, we have $\mathrm{w_L}(a) \in \{0,1,2\}$ for any a in R. If $b=0$, then $\mathrm{w_L}(0)=0$ and $\chi(0)=1$. Hence,

$$\sum_{a\in R} \chi(ab)\ X^{2-\mathrm{w_L}(a)}\ Y^{\mathrm{w_L}(a)} = X^2+9Y^2+6XY = (X+3Y)^2.$$

Next, for any $b \in A$, we have $\mathrm{w_L}(b)=1$ and $\chi(ab)=\pm 1$. Hence,

$$\sum_{a\in R} \chi(ab)\ X^{2-\mathrm{w_L}(a)}\ Y^{\mathrm{w_L}(a)} = X^2+2XY-3Y^2 = (X+3Y)(X-Y).$$

Finally, for any $b \in B$, we have $\mathrm{w_L}(b)=2$ and $\chi(ab)=\pm 1$. Hence,

$$\sum_{a\in R} \chi(ab)\ X^{2-\mathrm{w_L}(a)}\ Y^{\mathrm{w_L}(a)} = X^2-2XY+Y^2 = (X-Y)^2.$$

Thus,

$$\begin{aligned}\sum_{a\in R} \chi(ab)\ X^{2-\mathrm{w_L}(a)}\ Y^{\mathrm{w_L}(a)} &= \begin{cases} (X+3Y)^2 & \text{if } b=0 \\ (X+3Y)(X-Y) & \text{if } b\in A \\ (X-Y)^2 & \text{if } b\in B \end{cases} \\ &= (X+3Y)^{2-\mathrm{wt}(b)}(X-Y)^{\mathrm{wt}(b)}.\end{aligned} \tag{2.13}$$

□

Theorem 21. *Let $\mathbf{z} \in \mathbb{F}_4^\alpha R^\beta$ and $N := \alpha+2\beta$. Let χ be the character of R given in Definition* **??**. *Then*

$$\sum_{\mathbf{l}\in\mathbb{F}_4^\alpha R^\beta} \chi(\langle \mathbf{l},\mathbf{z}\rangle) X^{N-\mathrm{wt}(\mathbf{l})} Y^{\mathrm{wt}(\mathbf{l})} = (X+3Y)^{N-\mathrm{wt}(\mathbf{z})}(X-Y)^{\mathrm{wt}(\mathbf{z})}.$$

Proof. We can rewrite

$$\sum_{\mathbf{l}\in\mathbb{F}_4^\alpha R^\beta} \chi(\langle \mathbf{l}, \mathbf{z}\rangle) X^{N-\mathrm{wt}(\mathbf{l})} Y^{\mathrm{wt}(\mathbf{l})}$$

as

$$\begin{aligned}
&\sum_{\mathbf{l}_\alpha\in\mathbb{F}_4^\alpha} \sum_{\mathbf{l}_\beta\in R^\beta} \chi(\langle \mathbf{l}_\alpha, \mathbf{z}_\alpha\rangle) X^{\alpha-\mathrm{w_H}(\mathbf{l}_\alpha)} Y^{\mathrm{w_H}(\mathbf{l}_\alpha)} \chi(\langle \mathbf{l}_\beta, \mathbf{z}_\beta\rangle) X^{2\beta-\mathrm{w_L}(\mathbf{l}_\beta)} Y^{\mathrm{w_L}(\mathbf{l}_\beta)} \\
&= \left(\prod_{i=1}^{\alpha} \sum_{\mathbf{l}_i\in\mathbb{F}_4} \chi(\mathbf{l}_i\mathbf{z}_i) X^{1-wH(\mathbf{l}_i)} Y^{\mathrm{w_H}(\mathbf{l}_i)}\right) \left(\prod_{i=1}^{\beta} \sum_{\mathbf{l}_i\in R} \chi(\mathbf{l}_i\mathbf{z}_i) X^{2-\mathrm{w_L}(\mathbf{l}_i)} Y^{\mathrm{w_L}(\mathbf{l}_i)}\right) \\
&= \left(\prod_{i=1}^{\alpha} (X+3Y)^{1-\mathrm{w_H}(\mathbf{z}_i)} (X-Y)^{\mathrm{w_H}(\mathbf{z}_i)}\right) \left(\prod_{i=1}^{\beta} (X+3Y)^{2-\mathrm{w_L}(\mathbf{z}_i)} (X-Y)^{\mathrm{w_L}(\mathbf{z}_i)}\right) \\
&= (X+3Y)^{N-\mathrm{wt}(\mathbf{z})} (X-Y)^{\mathrm{wt}(\mathbf{z})}.
\end{aligned}$$

□

The following Lemma gives the Discrete Fourier Transform (DFT) formula for our setup, which will be useful in the proof of the MacWilliams identity.

Lemma 13. *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_4R$ and $\mathcal{C}^\perp$ be its dual code. Let the weight enumerator of the codeword $\mathbf{u} \in \mathbb{F}_4^\alpha R^\beta$ be $f(\mathbf{u}) := X^{N-\mathrm{wt}(\mathbf{u})} Y^{\mathrm{wt}(\mathbf{u})}$. Let*

$$\widehat{f}(\mathbf{z}) := \sum_{\mathbf{u}\in\mathbb{F}_4^\alpha R^\beta} \chi(\langle \mathbf{u}, \mathbf{z}\rangle) f(\mathbf{u}).$$

Then

$$\sum_{\mathbf{u}\in\mathcal{C}^\perp} f(\mathbf{u}) = \frac{1}{|\mathcal{C}|} \sum_{\mathbf{z}\in\mathcal{C}} \widehat{f}(\mathbf{z}).$$

Proof. Notice that

$$\begin{aligned}
\sum_{\mathbf{z}\in\mathcal{C}} \widehat{f}(\mathbf{z}) &= \sum_{\mathbf{z}\in\mathcal{C}} \sum_{\mathbf{u}\in\mathbb{F}_4^\alpha R^\beta} \chi(\langle \mathbf{u}, \mathbf{z}\rangle) f(\mathbf{u}) \\
&= \sum_{\mathbf{z}\in\mathcal{C}} \sum_{\mathbf{u}\in\mathcal{C}^\perp} \chi(\langle \mathbf{u}, \mathbf{z}\rangle) f(\mathbf{u}) + \sum_{\mathbf{z}\in\mathcal{C}} \sum_{\mathbf{u}\notin\mathcal{C}^\perp} \chi(\langle \mathbf{u}, \mathbf{z}\rangle) f(\mathbf{u}) \\
&= \sum_{\mathbf{u}\in\mathcal{C}^\perp} f(\mathbf{u}) \sum_{\mathbf{z}\in\mathcal{C}} \chi(\langle \mathbf{u}, \mathbf{z}\rangle) + \sum_{\mathbf{u}\notin\mathcal{C}^\perp} f(\mathbf{u}) \sum_{\mathbf{z}\in\mathcal{C}} \chi(\langle \mathbf{u}, \mathbf{z}\rangle).
\end{aligned}$$

By Lemma **??**, we obtain $\sum_{\mathbf{u}\in\mathcal{C}^\perp} f(\mathbf{u}) = \frac{1}{|\mathcal{C}|} \sum_{\mathbf{z}\in\mathcal{C}} \widehat{f}(\mathbf{z})$. □

We are now finally ready to establish the MacWilliams identity.

Theorem 22. *Let $\mathcal{C}$ be an $\mathbb{F}_4 R$ code. The relation between the weight enumerators of $\mathcal{C}$ and that of its dual is given by the identity*

$$W_{\mathcal{C}^\perp}(X,Y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(X+3Y, X-Y).$$

Proof. We apply Lemma (**??**) with

$$f(\mathbf{u}) = X^{N-\mathrm{wt}(\mathbf{u})} Y^{\mathrm{wt}(\mathbf{u})} \text{ and } \widehat{f}(\mathbf{z}) = \sum_{\mathbf{u} \in \mathbb{F}_4^\alpha R^\beta} \chi(\langle \mathbf{u}, \mathbf{z} \rangle) X^{N-\mathrm{wt}(\mathbf{u})} Y^{\mathrm{wt}(\mathbf{u})}.$$

Let us rewrite $\displaystyle\sum_{\mathbf{u} \in \mathcal{C}^\perp} f(\mathbf{u}) = \frac{1}{|\mathcal{C}|} \sum_{\mathbf{z} \in \mathcal{C}} \widehat{f}(\mathbf{z})$ as

$$\sum_{\mathbf{u} \in \mathcal{C}^\perp} X^{N-\mathrm{wt}(\mathbf{u})} Y^{\mathrm{wt}(\mathbf{u})} = \frac{1}{|\mathcal{C}|} \sum_{\mathbf{z} \in \mathcal{C}} \left(\sum_{\mathbf{u} \in \mathbb{F}_4^\alpha R^\beta} \chi(\langle \mathbf{u}, \mathbf{z} \rangle) X^{N-\mathrm{wt}(\mathbf{u})} Y^{\mathrm{wt}(\mathbf{u})} \right).$$

Applying Theorem **??**, one obtains

$$\sum_{\mathbf{u} \in \mathcal{C}^\perp} X^{N-\mathrm{wt}(\mathbf{u})} Y^{\mathrm{wt}(\mathbf{u})} = \frac{1}{|\mathcal{C}|} \sum_{\mathbf{z} \in \mathcal{C}} (X+3Y)^{N-\mathrm{wt}(\mathbf{z})} (X-Y)^{\mathrm{wt}(\mathbf{z})}.$$

Thus,

$$W_{\mathcal{C}^\perp}(X,Y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(X+3Y, X-Y).$$

□

Example 7. *Let $\mathcal{C}$ be the linear code over $\mathbb{F}_4 R$ of type $(1,1;1,0,1,0)$ with generator matrix $G_{\mathcal{C}} := \left(\begin{array}{c|c} 1 & v \end{array} \right)$. The code $\mathcal{C}$ has $|\mathcal{C}| = 16$ codewords. Its dual code has $|\mathcal{C}^\perp| = 4$ codewords. The codewords of $\mathcal{C}$ and their respective weights are as follow.*

$\mathbf{z} \in \mathcal{C}$	$\mathrm{wt}(\mathbf{z})$	$\mathbf{z} \in \mathcal{C}$	$\mathrm{wt}(\mathbf{z})$	$\mathbf{z} \in \mathcal{C}$	$\mathrm{wt}(\mathbf{z})$	$\mathbf{z} \in \mathcal{C}$	$\mathrm{wt}(\mathbf{z})$
$(0 \mid 0)$	0	$(0 \mid v)$	1	$(0 \mid vw)$	1	$(0 \mid vw^2)$	1
$(1 \mid 0)$	1	$(1 \mid v)$	2	$(1 \mid vw)$	2	$(1 \mid vw^2)$	2
$(w \mid 0)$	1	$(w \mid v)$	2	$(w \mid vw)$	2	$(w \mid vw^2)$	2
$(w^2 \mid 0)$	1	$(w^2 \mid v)$	2	$(w^2 \mid vw)$	2	$(w^2 \mid vw^2)$	2

*The weight distribution of $\mathcal{C}$ is $W_C(X,Y) = X^3 + 6X^2Y + 9XY^2$. By Theorem **??**, the weight distribution of $\mathcal{C}^\perp$ is $W_{\mathcal{C}^\perp}(X,Y) = X^3 + 3X^2Y$.*

The presented results are publish in International Journal. See **?**.

Chapter 3

Skew cyclic codes $\mathbb{F}_4 R$

Recent topics in the studies of error correcting codes are additive codes over mixed alphabets on one hand and codes using skew polynomial rings on the other. In this chapter, we generalize different ways of building linear codes. We present our study on skew cyclic codes over the ring $\mathbb{F}_4 R$, resulting in the identification of their generators. We have shown that, under some simple conditions on their length, they are equivalent to cyclic or 2-quasi-cyclic codes over the same ring. We supplied several ways of obtaining $\mathbb{F}_4$-linear codes with good parameters as images of $\mathbb{F}_4 R$-skew cyclic codes under the Gray mapping. Finally, Applications of these codes to DNA computing are included in our treatment. We refer to see **?**, **?**, **?** and **?**.

3.1 Introduction

Let $A \oplus B = \{a + b \mid a \in A, b \in B\}$ and $A \otimes B = \{(a, b) \mid a \in A, b \in B\}$ as defined in **?**. An $\mathbb{F}_4$-linear code of length n is a subspace of $\mathbb{F}_4^n$. A subset C of R^n is a *linear code over* R if C is an R-submodule. Given a linear code C over R, let

$$C_1 := \{\mathbf{x} + \mathbf{y} \in \mathbb{F}_4^n \mid (\mathbf{x} + \mathbf{y})v + \mathbf{x}(v + 1) \in C \text{ for some } \mathbf{x}, \mathbf{y} \in \mathbb{F}_4^n\} \text{ and}$$
$$C_2 := \{\mathbf{x} \in \mathbb{F}_4^n \mid (\mathbf{x} + \mathbf{y})v + \mathbf{x}(v + 1) \in C \text{ for some } \mathbf{y} \in \mathbb{F}_4^n\}.$$

One can quickly verify that C_1 and C_2 are linear codes over $\mathbb{F}_4$. In fact, any linear code C over R can be expressed as $C = vC_1 \oplus (v + 1)C_2$. Let $r = a + vb \in R$ and $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in C$, *i.e.*, $c_j = a_j + vb_j$ with $a_j, b_j \in \mathbb{F}_4$ for $1 \leq j \leq n$.

The j-th entry of $r\mathbf{c}$ is

$$\begin{aligned}(a+vb)(a_j+vb_j) &= ((a+b)v+a(v+1))(a_j+vb_j)\\ &= \underbrace{aa_j}_{x} + v(\underbrace{ab_j+ba_j+bb_j}_{y}) = (x+y)v+x(v+1).\end{aligned}$$

Hence, $r\mathbf{c}$ can be written in terms of C_1 and C_2 with

$$\mathbf{x} = a(a_1, a_2, \ldots, a_n) \text{ and } \mathbf{y} = (a+b)(b_1, b_2, \ldots, b_n) + b(a_1, a_2, \ldots, a_n).$$

We recall the definition of *automorphim* θ.

Definition 16. *Let an automorphism θ over R be defined by*

$$\theta : R \mapsto R \text{ sending } a+vb \mapsto a^2 + (v+1)\, b^2. \tag{3.1}$$

it is clear that $|\langle\theta\rangle| = 2$ i.e. *for all c in R, $\theta(c) = c$. A subset C of R^n is said to be an R-skew cyclic code of length n if two conditions are satisfied.*

1. *C is an R-submodule of R^n.*
2. *If $\mathbf{c} = (c_0, c_1, ..., c_{n-1}) \in C$ then the skew cyclic shift of $\mathbf{c}$ over R, denoted by $T_\theta(\mathbf{c}) := (\theta(c_{n-1}), \theta(c_0), ..., \theta(c_{n-2}))$, is also in C.*

It is often convenient to associate a vector $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ with a polynomial $a(X) := a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$ in an indeterminate X. This allows for constructions of codes using results from the algebra of polynomial rings.

The next two theorems can be inferred by a slight modification on the corresponding theorems in **?**, with q restricted to 4. The respective proof is therefore omitted for brevity.

Theorem 23. *(From (**?**, Theorem 3)) Let $C = vC_1 \oplus (v+1)C_2$ be an R-linear code. Then C is an R-skew cyclic code if and only if C_1 and C_2 are skew cyclic codes over $\mathbb{F}_4$.*

Theorem 24. *(From (**?**, Theorem 5)) Let $C = vC_1 \oplus (v+1)C_2$ be an R-skew cyclic code of length n. Let $g_1(X)$ and $g_2(X)$ be the respective generator polynomials of C_1 and C_2 as $\mathbb{F}_4$-skew cyclic codes. Then $C = \langle vg_1(X) + (v+1)g_2(X)\rangle$.*

For any element in R, we introduce a new ring homomorphism

$$\eta : R \mapsto \mathbb{F}_4 \text{ sending } a+vb \text{ to } a. \tag{3.2}$$

Let $\mathbb{F}_4 R := \{(a, b) \mid a \in \mathbb{F}_4 \text{ and } b \in R\}$. It is straightforward to verify that $\mathbb{F}_4 R$ is an R-module under the multiplication

$$d * (a, b) = (\eta(d)a, db) \text{ with } d \in R \text{ and } (a, b) \in \mathbb{F}_4 R. \tag{3.3}$$

This extends naturally to $\mathbb{F}_4^\alpha R^\beta$. Let $\mathbf{x} = (a_0, a_1, ..., a_{\alpha-1}, b_0, b_1, ..., b_{\beta-1}) \in \mathbb{F}_4^\alpha R^\beta$, for α and $\beta \in \mathbb{N}$, and $d \in R$. Then

$$d * \mathbf{x} = (\eta(d)a_0, \eta(d)a_1, ..., \eta(d)a_{\alpha-1}, db_0, db_1, ..., db_{\beta-1}). \tag{3.4}$$

Definition 17. *A nonempty subset C of $\mathbb{F}_4^\alpha R^\beta$ is called an $\mathbb{F}_4 R$-linear code if it is an R-submodule of $\mathbb{F}_4^\alpha R^\beta$ with respect to the scalar multiplication in Equation (**??**).*

A nondegenerate *inner product* between $\mathbf{x} = (a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1})$ and $\mathbf{y} = (d_0, d_1, \ldots, d_{\alpha-1}, e_0, e_1, ..., e_{\beta-1})$ in $\mathbb{F}_4^\alpha R^\beta$ is given by

$$\langle \mathbf{x}, \mathbf{y} \rangle = v \sum_{i=0}^{\alpha-1} a_i d_i + \sum_{j=0}^{\beta-1} b_j e_j \in R. \tag{3.5}$$

Note that if $\alpha = 0$, then the inner product is well-defined for elements $\mathbf{x}, \mathbf{y} \in R^\beta$. The dual code of an $\mathbb{F}_4 R$-linear code C, denoted by $C^\perp$, is also $\mathbb{F}_4 R$-linear and is defined in the usual way as

$$C^\perp := \{\mathbf{y} \in \mathbb{F}_4^\alpha R^\beta \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}.$$

Let

$$a(X) = a_0 + a_1 X + \ldots + a_{\alpha-1} X^{\alpha-1} \in \mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle \text{ and}$$
$$b(X) = b_0 + b_1 X + \ldots + b_{\beta-1} X^{\beta-1} \in R[X, \theta]/\langle X^\beta - 1 \rangle.$$

Then any codeword $\mathbf{c} = (a_0, a_1, ..., a_{\alpha-1}, b_0, b_1, ..., b_{\beta-1}) \in \mathbb{F}_4^\alpha R^\beta$ can be identified with a module element consisting of two polynomials such that

$$c(X) = (a(X), b(X)). \tag{3.6}$$

This identification gives a one-to-one correspondence between $\mathbb{F}_4^\alpha R^\beta$ and

$$R_{\alpha,\beta} := \mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle \times R[X, \theta]/\langle X^\beta - 1 \rangle. \tag{3.7}$$

The product of $r(X) = r_0 + r_1 X + \ldots + r_t X^t \in R[X, \theta]$ and $(a(X), b(X)) \in R_{\alpha,\beta}$ is

$$r(X) * (a(X), b(X)) = (\eta(r(X))a(X), r(X)b(X)), \tag{3.8}$$

where $\eta(r(X)) = \eta(r_0) + \eta(r_1)X + \ldots + \eta(r_t)X^t \in \mathbb{F}_4[X]$. Here, $\eta(r(X))a(X)$ is the usual polynomial multiplication in $\mathbb{F}_4[X]/\langle X^\alpha - 1\rangle$ while $r(X)b(X)$ is the polynomial multiplication in $R[X,\theta]/\langle X^\beta - 1\rangle$ where $X(a + vb) = (a^2 + (v+1)b^2)\, X$.

Theorem 25. *$R_{\alpha,\beta}$ is a left $R[X,\theta]$-module with respect to $*$ in Equation (??).*

Proof. Verifying that the required properties are satisfied over $\mathbb{F}_4[X]/\langle X^\alpha - 1\rangle$ is easy since we do not have to deal with skewness. Verifying over $R[X,\theta]/\langle X^\beta - 1\rangle$ is routine, albeit tedious. It suffices to use the fact that θ is a homomorphism with $\theta^{-1} = \theta$. □

We define skew cyclic codes to be left $R[X,\theta]$-submodule of

$$R_{\alpha,\beta} := \mathbb{F}_4[X]/\langle X^\alpha - 1\rangle \times R[X,\theta]/\langle X^\beta - 1\rangle.$$

This definition implies that the results are applied for any β.

3.2 Generator Polynomials of $\mathbb{F}_4R$-Skew Cyclic Codes

This section begins with a formal definition of an $\mathbb{F}_4R$-skew cyclic code and, then, proposes a method to determine a generator polynomial of any $\mathbb{F}_4R$-skew cyclic code C in $R_{\alpha,\beta}$. We use a general notion of equivalence to say that two codes are *equivalent* if one can be obtained from the other by a combination of the following operations: (a) some composition of a permutation of the first α positions, a permutation of the last β positions, (b) multiplication of the scalars appearing in a chosen position by a nonzero scalar, and (c) applying a ring (or field) automorphism to elements in a chosen position.

Definition 18. *An $\mathbb{F}_4R$-linear code C of length $n = \alpha + \beta$ is said to be $\mathbb{F}_4R$-skew cyclic if, for any codeword $\mathbf{c} = (a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1}) \in C$, its skew cyclic shift*
$T_\theta(\mathbf{c}) := (a_{\alpha-1}, a_0, \ldots, a_{\alpha-2}, \theta(b_{\beta-1}), \theta(b_0), \ldots, \theta(b_{\beta-2}))$ is also in C.

Theorem 26. *Let C be an $\mathbb{F}_4R$-skew cyclic code of length $n = \alpha + \beta$ such that β is an even integer. Then $C^\perp$ is also an $\mathbb{F}_4R$-skew cyclic code of the same length.*

Proof. It suffices to show that, for any $\mathbf{x} = (a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1}) \in C^\perp$, we have $T_\theta(\mathbf{x}) \in C^\perp$. Let $\mathbf{y} = (d_0, d_1, \ldots, d_{\alpha-1}, e_0, e_1, \ldots, e_{\beta-1})$ be any codeword in C. Then we write $\langle T_\theta(\mathbf{x}), \mathbf{y}\rangle$ as

$$\begin{aligned}&\langle (a_{\alpha-1}, a_0, \ldots, a_{\alpha-2}, \theta(b_{\beta-1}), \theta(b_0), \ldots, \theta(b_{\beta-2})), (d_0, d_1, \ldots, d_{\alpha-1}, e_0, e_1, \ldots, e_{\beta-1})\rangle \\ &= v(a_{\alpha-1}d_0 + a_0d_1 + \ldots + a_{\alpha-2}d_{\alpha-1}) + (\theta(b_{\beta-1})e_0 + \theta(b_0)e_1 + \ldots + \theta(b_{\beta-2})e_{\beta-1}).\end{aligned}$$

Hence, one only needs to show that

$$a_{\alpha-1}d_0 + a_0d_1 + \ldots + a_{\alpha-2}d_{\alpha-1} = 0 \text{ and } \theta(b_{\beta-1})e_0 + \theta(b_0)e_1 + \ldots + \theta(b_{\beta-2})e_{\beta-1} = 0.$$

Now, let $\gamma := \mathrm{lcm}(\alpha, \beta)$. Then γ is an even integer since β is an even integer. Since C is $\mathbb{F}_4R$-skew cyclic, for any $\mathbf{y} \in C$ we have $T_\theta^\gamma(\mathbf{y}) = \mathbf{y}$ and $T_\theta^{\gamma-1}(\mathbf{y}) \in C$. Hence, $\langle \mathbf{x}, T_\theta^{\gamma-1}(\mathbf{y}) \rangle = 0$. Since $T_\theta^{\gamma-1}(\mathbf{y}) = (d_1, \ldots, d_{\alpha-1}, d_0, \theta(e_1), \ldots, \theta(e_{\beta-1}), \theta(e_0))$, we then obtain

$$v \sum_{j=0}^{\alpha-1} a_j \, d_{(j+1) \pmod{\alpha}} + \sum_{j=0}^{\beta-1} b_j \, \theta\left(e_{(j+1) \pmod{\beta}}\right) = 0.$$

This implies

$$\begin{aligned} 0 &= a_{\alpha-1}d_0 + a_0d_1 + a_1d_2 + \ldots + a_{\alpha-2}d_{\alpha-1} \text{ and} \\ 0 &= b_{\beta-1}\theta(e_0) + b_0\theta(e_1) + b_1\theta(e_2) + \ldots + b_{\beta-2}\theta(e_{\beta-1}). \end{aligned}$$

Applying θ to both sides of the last equation yields

$$\theta(0) = \theta(b_{\beta-1})e_0 + \theta(b_0)e_1 + \theta(b_1)e_2 + \ldots + \theta(b_{\beta-2})e_{\beta-1} = 0,$$

completing the proof. □

Theorem 27. *A code C is $\mathbb{F}_4R$-skew cyclic if and only if C is a left $R[X, \theta]$-submodule of $R_{\alpha,\beta}$ under the multiplication $*$.*

Proof. Let $c(X) = (a(X), b(X))$ be any codeword of an $\mathbb{F}_4R$-skew cyclic code C. Hence, $(a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1})$ and all of it's T_θ-skew cyclic shifts are in C. We associate, for each $j \in \mathbb{N}$, the polynomial

$$\begin{aligned} X^j * c(X) = (a_{\alpha-j} + a_{\alpha-j+1}X + \ldots + a_{\alpha-j-1}X^{\alpha-1}, \\ \theta^j(b_{\beta-j}) + \theta^j(b_{\beta-j+1})X + \ldots + \theta^j(b_{\beta-j-1})X^{\beta-1}) \end{aligned}$$

with the vector

$$(a_{\alpha-j}, a_{\alpha-j+1}, \ldots, a_{\alpha-j-1}, \theta^j(b_{\beta-j}), \theta^j(b_{\beta-j+1}), \ldots, \theta^j(b_{\beta-j-1})).$$

The indices of the first block (of length α) are taken modulo α and those of the second block (of length β) are taken modulo β. By the $\mathbb{F}_4R$-linearity of C, we have $r(X) * c(X) \in C$ for any $r(X) \in R[X, \theta]$. Thus, C is a left $R[X, \theta]$-submodule of $R_{\alpha,\beta}$.

Conversely, let C be a left $R[X,\theta]$-submodule of the left $R[X,\theta]$-module $R_{\alpha,\beta}$. Then, for any $c(X) \in C$, we have $X^j * c(X) \in C$ for any $j \in \mathbb{N}$. Thus, C is indeed an $\mathbb{F}_4R$-skew cyclic code. □

Let C be an $\mathbb{F}_4R$-skew cyclic code. Let $c(X) = (a(X), b(X))$ be an element in C. Let $\ell(X)$ be an element in $\mathbb{F}_4[X]/\langle X^\alpha - 1\rangle$. We use $\mathbf{0}$ to denote either the zero vector $(0, 0, \ldots, 0)$ or the zero polynomial. Let

$$I := \{b(X) \in R[X,\theta]/\langle X^\beta - 1\rangle \mid (\ell(X), b(X)) \in C,\ \exists \ell(X) \in \mathbb{F}_4[X]/\langle X^\alpha - 1\rangle\} \text{ and}$$
$$J := \{a(X) \in \mathbb{F}_4[X]/\langle X^\alpha - 1\rangle \mid (a(X), \mathbf{0}) \in C\}.$$

The following results establish useful properties of the sets I and J

Lemma 14. *J is an ideal in $\mathbb{F}_4[X]/\langle X^\alpha - 1\rangle$ generated by a divisor of $X^\alpha - 1$.*

Proof. If $a_1(X)$ and $a_2(X)$ are in J, then $(a_1(X), \mathbf{0})$ and $(a_2(X), \mathbf{0})$ are in C by definition. Hence, $(a_1(X), \mathbf{0}) + (a_2(X), \mathbf{0}) = (a_1(X) + a_2(X), \mathbf{0}) \in C$, ensuring that $a_1(X) + a_2(X) \in J$. Let $s(X) \in \mathbb{F}_4[X]/\langle X^\alpha - 1\rangle$ and $a(X) \in J$. Then $(a(X), \mathbf{0})$ is in C. Because C is a left $R[X,\theta]$-module, we have

$$s(X) * (a(X), \mathbf{0}) = (s(X)a(X), \mathbf{0}) \in C \implies s(X)a(X) \text{ modulo } (X^\alpha - 1) \in J.$$

Thus, J is an ideal in $\mathbb{F}_4[X]/\langle X^\alpha - 1\rangle$ generated by a divisor $f(X)$ of $X^\alpha - 1$. □

Lemma 15. *I is a principally generated left $R[X,\theta]$-submodule of $R[X,\theta]/\langle X^\beta - 1\rangle$.*

Proof. Let $b_1(X)$ and $b_2(X)$ be elements in I. Then there exist polynomials $\ell_1(X)$ and $\ell_2(X)$ in $\mathbb{F}_4[X]/\langle X^\alpha - 1\rangle$ such that $(\ell_1(X), b_1(X)), (\ell_2(X), b_2(X)) \in C$. Hence,

$$(\ell_1(X), b_1(X)) + (\ell_2(X), b_2(X)) = (\ell_1(X) + \ell_2(X), b_1(X) + b_2(X)) \in C,$$

implying $b_1(X) + b_2(X) \in I$. Let $r(X) \in R[X,\theta]/\langle X^\beta - 1\rangle$ and $(\ell(X), b(X)) \in C$. Since C is a left $R[X,\theta]$-submodule of $R_{\alpha,\beta}$, we have

$$r(X) * (\ell(X), b(X)) = (\eta(r(X))\ell(X) \text{ modulo } (X^\alpha - 1), r(X)b(X) \text{ modulo } (X^\beta - 1))$$

in C, making $r(X)b(X)$ modulo $(X^\beta - 1) \in I$. Thus, I is a left submodule in $R[X,\theta]/\langle X^\beta - 1\rangle$ and, by Theorem **??**, $I = \langle g(X)\rangle$ where

$$g(X) := vg_1(X) + (v+1)g_2(X). \tag{3.9}$$

Our proof is now complete. □

The following result classifies all $\mathbb{F}_4R$-skew cyclic codes.

Theorem 28. *Let $g(X)$ be as defined in Equation (??). Let C be an $\mathbb{F}_4R$-skew cyclic code. Then C is generated as a left submodule of $R_{\alpha,\beta}$ by $(f(X), \mathbf{0})$ and $(\ell(X), g(X))$, where $\ell(X)$ is an element in $\mathbb{F}_4[X]/\langle X^\alpha - 1\rangle$ and $f(X)$ divides $X^\alpha - 1$.*

Proof. Let $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in C$ with $\mathbf{c}_1 \in \mathbb{F}_4^\alpha$ and $\mathbf{c}_2 \in R^\beta$. Then $c_2(X) \in I$ and we write $c_2(X) = q(X)\, g(X)$ for some $q(X) \in R[X,\theta]/\langle X^\beta - 1\rangle$. There exists $\ell(X) \in \mathbb{F}_4[X]/\langle X^\alpha - 1\rangle$ such that $(\ell(X), g(X)) \in C$, since $g(X) \in I$. We have

$$\begin{aligned}\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) &= (c_1(X), \mathbf{0}) + (\mathbf{0}, q(X)g(X)) \\ &= (c_1(X), \mathbf{0}) + (\eta(q(X))\ell(X), q(X)g(X)) + (\eta(q(X))\ell(X), \mathbf{0}) \\ &= (c_1(X), \mathbf{0}) + q(X) * ((\ell(X), g(X)) + (\ell(X), \mathbf{0}))\,.\end{aligned}$$

Hence, $(\eta(q(X))\ell(X) + c_1(X), \mathbf{0}) \in C$, making $\eta(q(X))\ell(X) + c_1(X) \in J$. By Lemma **??**, there exists $p(X) \in J$ satisfying $\eta(q(X))\ell(X) + c_1(X) = p(X)f(X)$. Thus, $c(X) = q(X) * (\ell(X), g(X)) + (p(X)f(X), \mathbf{0})$. □

Lemma 16. *Let C be an $\mathbb{F}_4R$-skew cyclic code. Then, without loss of generality, we can assume $\deg(\ell(X)) < \deg(f(X))$, where $f(X)$ is the divisor of $X^\alpha - 1$ as in Theorem* **??**.

Proof. Suppose that $\deg(\ell(X)) - \deg(f(X)) = k \geq 0$. Consider the code D generated by $\{(f(X), \mathbf{0}), (\ell(X), g(X)) + sX^k * (f(X), \mathbf{0})\} = \{(f(X), \mathbf{0}), (\ell_1(X), g(X))\}$, where $\ell_1(X) = \ell(X) + sX^k f(X)$ for some $s \in \mathbb{F}_4$. Hence, $D \subseteq C$. On the other hand, $(\ell(X), g(X)) = (\ell(X), g(X)) + sX^k * (f(X), \mathbf{0}) - sX^k * (f(X), \mathbf{0})$. Hence, $C \subseteq D$, making $C = D$. Notice here that $\deg(\ell_1(X)) < \deg(\ell(X))$. We repeat the same process on $\ell_1(X)$ until we obtain $\deg(\ell(X)) < \deg(f(X))$. □

Theorem 29. *An $\mathbb{F}_4R$-skew cyclic code is equivalent to an $\mathbb{F}_4R$-cyclic code if both α and β are odd integers.*

Proof. Let C be an $\mathbb{F}_4R$-skew cyclic code and $\gamma := \mathrm{lcm}(\alpha, \beta)$. Then $\gcd(\gamma, 2) = 1$ since γ is odd. Then there exist integers k and j such that $\gamma k + 2j = 1$. Hence, $2j = 1 - \gamma k = 1 + \gamma t$, for some $t > 0$ where $t \equiv -k \pmod{\gamma}$. As in Equation (**??**), let $c(X) = (a(X), b(X)) \in$

C. Then

$$\begin{aligned} X^{2j} * c(X) &= X^{2j} * \left(\sum_{i=0}^{\alpha-1} a_i X^i, \sum_{i=0}^{\beta-1} b_i X^i \right) = \left(\sum_{i=0}^{\alpha-1} a_i X^{i+2j}, \sum_{i=0}^{\beta-1} \theta^{2j}(b_i) X^{i+2j} \right) \\ &= \left(\sum_{i=0}^{\alpha-1} a_i X^{i+1+\gamma t}, \sum_{i=0}^{\beta-1} \theta^{2j}(b_i) X^{i+1+\gamma t} \right) \\ &= \left(\sum_{i=0}^{\alpha-2} a_i X^{i+1+\gamma t} + a_{\alpha-1} X^{\alpha+\gamma t}, \sum_{i=0}^{\beta-2} b_i X^{i+1+\gamma t} + b_{\beta-1} X^{\beta+\gamma t} \right) \\ &= \left(\sum_{i=0}^{\alpha-2} a_i X^{i+1} + a_{\alpha-1}, \sum_{i=0}^{\beta-2} b_i X^{i+1} + b_{\beta-1} \right) \in C. \end{aligned}$$

The second to the last equation is due to $\theta^2(r) = r$ for all $r \in R$, while the last equation follows because $X^\alpha = X^\beta = X^\gamma = 1$. This shows that $X^{2j} * c(X)$ is the cyclic shift of $c(X)$ over $\mathbb{F}_4 R$. Thus, C is cyclic. □

Theorem 30. *An $\mathbb{F}_4 R$-skew cyclic code is equivalent to an $\mathbb{F}_4 R$-quasi-cyclic code of index 2 if both α and β are even integers.*

Proof. Let C be an $\mathbb{F}_4 R$-skew cyclic code, $\alpha = 2N$, and $\beta = 2M$ for some $N, M \in \mathbb{N}$. Then $\gamma = \mathrm{lcm}(\alpha, \beta)$ is an even integer with $\gcd(\gamma, 2) = 2$. For any

$$\mathbf{c} = (a_{0,0}, a_{0,1}, \ldots, a_{N-1,0}, a_{N-1,1}\ ,\ b_{0,0}, b_{0,1}, \ldots, b_{M-1,0}, b_{M-1,1}) \in C$$

there exist integers $k \geq 0$ and j such that $2j = 2 + k\gamma$. Consider

$$\begin{aligned} &T_{\theta^{2+k\gamma}} (a_{0,0}, a_{0,1}, \ldots, a_{N-1,0}, a_{N-1,1}, b_{0,0}, b_{0,1}, \ldots, b_{M-1,0}, b_{M-1,1}) = \\ &T_{\theta^{k\gamma}} (a_{N-1,0}, a_{N-1,1}, \ldots, a_{N-2,0}, a_{N-2,1}, b_{M-1,0}, b_{M-1,1}, \ldots, b_{M-2,0}, b_{M-2,1}) = \\ &(a_{N-1,0}, a_{N-1,1}, \ldots, a_{N-2,0}, a_{N-2,1}, b_{M-1,0}, b_{M-1,1}, \ldots, b_{M-2,0}, b_{M-2,1}) \in C, \end{aligned}$$

since $T_{\theta^{k\gamma}}(\mathbf{c}) = \mathbf{c}$ for any $\mathbf{c} \in \mathbb{F}_4^\alpha R^\beta$. Thus, C is equivalent to an $\mathbb{F}_4 R$-quasi cyclic code of length $n = \alpha + \beta$ and index 2. □

3.3 The Gray Mapping

The classical Gray mapping $\phi^* : R \mapsto \mathbb{F}_4^2$ is defined by $\phi^*(a + vb) = (a + b, a)$ for any $a + vb \in R$. The *Lee weight* of any element in R is the Hamming weight of its image under

ϕ^*. This map extends naturally to vectors in R^n. For any $\mathbf{x} = (x_0, x_1, \ldots, x_{\alpha-1}) \in \mathbb{F}_4^\alpha$ and $\mathbf{y} = (y_0, y_1, \ldots, y_{\beta-1}) \in R^\beta$, the *Gray map* over $\mathbb{F}_4 R$ is defined by

$$\phi : \mathbb{F}_4^\alpha R^\beta \mapsto \mathbb{F}_4^{\alpha+2\beta} \text{ sending } (\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x}, \phi^*(\mathbf{y})).$$

The map ϕ is an isometry which transforms the Lee distance in $\mathbb{F}_4^\alpha R^\beta$ to the Hamming distance in $\mathbb{F}_4^{\alpha+2\beta}$. For any $\mathbb{F}_4 R$-linear code C, the code $\phi(C)$ is $\mathbb{F}_4$-linear. Furthermore, we have

$$wt(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x}) + wt_L(\mathbf{y}) \tag{3.10}$$

where $wt_H(\mathbf{x})$ is the Hamming weight of $\mathbf{x}$ and $wt_L(\mathbf{y})$ is the Lee weight of $\mathbf{y}$.

Theorem 31. *Let C be a self-orthogonal $\mathbb{F}_4 R$-linear code under the inner product defined in Equation (**??**). Then $\phi(C)$ is a Euclidean self-orthogonal code over $\mathbb{F}_4$.*

Proof. It suffices to show that the Gray images of codewords are Euclidean orthogonal whenever the codewords are orthogonal. Let C be a self-orthogonal $\mathbb{F}_4 R$-linear code of length $\alpha + \beta$. Let $\mathbf{v} = (\mathbf{a}, \mathbf{b} + v\,\mathbf{c}), \mathbf{w} = (\mathbf{d}, \mathbf{u} + v\,\mathbf{s}) \in \mathbb{F}_4^\alpha \times R^\beta$ be codewords in C with $\mathbf{a}, \mathbf{d} \in \mathbb{F}_4^\alpha$ and $\mathbf{b}, \mathbf{c}, \mathbf{u}, \mathbf{s} \in \mathbb{F}_4^\beta$. Then, by Equation (**??**),

$$\langle \mathbf{v}, \mathbf{w} \rangle = v(\mathbf{a} \cdot \mathbf{d}) + \mathbf{b} \cdot \mathbf{u} + v(\mathbf{b} \cdot \mathbf{s} + \mathbf{c} \cdot \mathbf{u} + \mathbf{c} \cdot \mathbf{s}) = 0 + v0 \in R.$$

Hence, $\mathbf{b} \cdot \mathbf{u} = 0$ and $\mathbf{a} \cdot \mathbf{d} + \mathbf{b} \cdot \mathbf{s} + \mathbf{c} \cdot \mathbf{u} + \mathbf{c} \cdot \mathbf{s} = 0$. Since $\phi(\mathbf{v}) = (\mathbf{a}, \mathbf{b} + \mathbf{c}, \mathbf{b})$ and $\phi(\mathbf{w}) = (\mathbf{d}, \mathbf{u} + \mathbf{s}, \mathbf{u})$, one gets

$$\phi(\mathbf{v}) \cdot \phi(\mathbf{w}) = \mathbf{a} \cdot \mathbf{d} + \mathbf{b} \cdot \mathbf{u} + \mathbf{b} \cdot \mathbf{s} + \mathbf{c} \cdot \mathbf{u} + \mathbf{c} \cdot \mathbf{s} + \mathbf{b} \cdot \mathbf{u} = 0.$$

Therefore, the code $\phi(C)$ is Euclidean self-orthogonal. □

Theorem 32. *Let C be an $\mathbb{F}_4 R$-skew cyclic code of length $n = \alpha + \beta$. Then, $\phi(C) = C_0 \otimes C_1 \otimes C_2$, where C_0 is a cyclic code of length α in $\mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$ and both C_1 and C_2 are skew cyclic codes of length β in $R[X, \theta]/\langle X^\beta - 1 \rangle$. Moreover, $|\phi(C)| = \prod_{i=0}^{2} |C_i|$.*

Proof. From $\{\mathbf{x} = (a_0, a_1, \ldots, a_{\alpha-1}, b_0 + vc_0, b_1 + vc_1, \ldots, b_{\beta-1} + vc_{\beta-1}) : \mathbf{x} \in C\}$, we construct the codes

$$C_0 := \{(a_0, a_1, \ldots, a_{\alpha-1})\}, C_1 := \{(b_0 + c_0, b_1 + c_1, \ldots, b_{\beta-1} + c_{\beta-1})\},$$
$$\text{and } C_2 := \{(b_0, b_1, \ldots, b_{\beta-1})\}.$$

A codeword $\mathbf{u} := (a_0, a_1, \ldots, a_{\alpha-1}) \in C_0$ corresponds to a codeword

$$\mathbf{x} = (a_0, a_1, \ldots, a_{\alpha-1}, b_0 + vc_0, b_1 + vc_1, \ldots, b_{\beta-1} + vc_{\beta-1}) \in C.$$

Since C is an $\mathbb{F}_4R$-skew cyclic code, we know that $T_\theta(\mathbf{x})$ is given by

$$(a_{\alpha-1}, a_0, a_1, \ldots, a_{\alpha-2}, \theta(b_{\beta-1} + vc_{\beta-1}), \theta(b_0 + vc_0), \ldots, \theta(b_{\beta-2} + vc_{\beta-2})) \in C.$$

Hence, $(a_{\alpha-1}, a_0, a_1, \ldots, a_{\alpha-2}) \in C_0$. This implies that C_0 is a cyclic code of length α in $\mathbb{F}_4[X]/\langle X^\alpha - 1\rangle$.

The proof that both C_1 and C_2 are skew cyclic codes of length β in $R[X]/\langle X^\beta - 1\rangle$ follows the same line of argument. Thus, $\phi(C) = C_0 \otimes C_1 \otimes C_2$ and $|\phi(C)| = \prod_{i=0}^{2} |C_i|$. □

Lemma 17. *Let $C = \langle (f(X), \mathbf{0}), (\mathbf{0}, g(X))\rangle$ be an $\mathbb{F}_4R$-skew cyclic code with $\ell(X) := \mathbf{0}$. Then $C = C_1 \otimes C_2$ where C_1 is a skew cyclic code over $\mathbb{F}_4$ and C_2 is a skew cyclic code over R.*

Proof. Note that $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in C$ if and only if $\mathbf{c}_1 = q_1 f(X)$ and $\mathbf{c}_2 = q_2 g(X)$ if and only if $\mathbf{c}_1 \in C_1 = (f(X))$ and $\mathbf{c}_2 \in C_2 = (g(X))$ if and only if $C = C_1 \otimes C_2$ where $C_1 = (f(X))$ and $\mathbf{c}_2 \in C_2 = (g(X))$. □

Lemma 18. *Let $C = C_1 \otimes C_2$ where C_1 is an $\mathbb{F}_4$-skew cyclic Euclidean self-orthogonal code and C_2 is an R-skew cyclic self-orthogonal code over R. Then C is a self-orthogonal $\mathbb{F}_4R$-skew cyclic code.*

Proof. Suppose $C_1 \subseteq C_1^\perp$ and $C_2 \subseteq C_2^\perp$. Let $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in C$ and $\mathbf{u} = (\mathbf{c}_3, \mathbf{c}_4) \in C$. Then $\mathbf{c}_1, \mathbf{c}_3 \in C_1 = (f(X))$ and $\mathbf{c}_2, \mathbf{c}_4 \in C_2 = (g(X))$. This implies that $\mathbf{c}_1 \cdot \mathbf{c}_3 = 0 \in \mathbb{F}_4$ and $\langle \mathbf{c}_2, \mathbf{c}_4\rangle = 0 \in R$. Hence,

$$\langle \mathbf{c}, \mathbf{u}\rangle = v(\mathbf{c}_1 \cdot \mathbf{c}_3) + \langle \mathbf{c}_2, \mathbf{c}_4\rangle = v \cdot 0 + 0 = 0.$$

Therefore, $C \subseteq C^\perp$, *i.e.*, the $\mathbb{F}_4R$-skew cyclic code C is self-orthogonal. □

Note that the converse does not hold. In fact, $C^\perp \neq C_1^\perp \otimes C_2^\perp$ in general. For an example, consider the following $C := C_1 \otimes C_2 \in \mathbb{F}_4^6 R^3$. Let C_1 be the $\mathbb{F}_4$-skew cyclic codes with parameters $[6, 3, 4]_4$ generated by $w + w^2X + w^2X^2 + X^3$. This codes is not self-dual although the dual, under the usual Euclidean inner product over $\mathbb{F}_4$, has

the same parameters $[6,3,4]_4$. The standard generator and parity check matrices are, respectively,

$$G_{C_1} = \begin{pmatrix} 1 & 0 & 0 & w^2 & w & w \\ 0 & 1 & 0 & w & w^2 & w \\ 0 & 0 & 1 & w & w & w^2 \end{pmatrix} \text{ and } H_{C_1} = \begin{pmatrix} 1 & 0 & 0 & w & w^2 & w^2 \\ 0 & 1 & 0 & w^2 & w & w^2 \\ 0 & 0 & 1 & w^2 & w^2 & w \end{pmatrix}.$$

For C_2 we use the R-skew cyclic code generated by $X + (w + v)$. As an R-code, its standard generator and parity check matrices are, respectively,

$$G_{C_2} = \begin{pmatrix} 1 & 0 & w^2 + v \\ 0 & 1 & w + v \end{pmatrix} \text{ and } H_{C_2} = \begin{pmatrix} w^2 + v & w + v & 1 \end{pmatrix}.$$

Notice that $x = (1, 0, 0, w^2, w, w, w^2v, v, wv)$ is a codeword in $C_1^{\perp} \otimes C_2^{\perp}$ and $y = (w, w^2, w^2, 1, 0, 0, w+ v, v, wv)$ is a codeword in C, but $\mathbf{x} \notin C^{\perp}$, since

$$\langle \mathbf{x}, \mathbf{y} \rangle = v \sum_{i=0}^{5} x_i y_i + \sum_{j=0}^{2} x_j y_j = v \neq 0.$$

3.4 $\mathbb{F}_4$-Codes with Good Parameters from $\mathbb{F}_4 R$-Skew Cyclic Codes

This section highlights several ways of obtaining $\mathbb{F}_4$-linear codes with good parameters from $\mathbb{F}_4 R$-skew cyclic codes.

First, we consider the case of $\alpha = 0$. This yields skew cyclic codes over R. We start by finding a divisor $g_\beta(X)$ of $X^\beta - 1$ in the skew polynomial ring $R[X, \theta]$. Then the skew cyclic code C_β over R has a generator matrix

$$G = \begin{pmatrix} g(X) \\ Xg(X) \\ \vdots \\ X^{k-1}g(X) \end{pmatrix} = \begin{pmatrix} \mathbf{g} \\ T_\theta(\mathbf{g}) \\ \vdots \\ T_\theta^{k-1}(\mathbf{g}) \end{pmatrix}$$

where $k = \beta - \deg(g(X))$ is the dimension of C_β. Its Gray image is an $\mathbb{F}_4$-linear code of length 2β and dimension $2k$ with a generator matrix

$$\phi(G) = \left(\begin{array}{c} \phi(\mathbf{g}) \\ \phi(T_\theta(\mathbf{g})) \\ \vdots \\ \phi(T_\theta^{k-1}(\mathbf{g})) \\ \hline \phi(v\mathbf{g}) \\ \phi(T_\theta(v\mathbf{g})) \\ \vdots \\ \phi(T_\theta^{k-1}(v\mathbf{g})) \end{array}\right) = \left(\begin{array}{c} G_{up} \\ \hline G_{lo} \end{array}\right). \tag{3.11}$$

Note that G_{up} and G_{lo}, individually, generate linear codes over $\mathbb{F}_4$ of length 2β. There are some optimal codes that can be obtained in this way.

Example 8. *For $\beta = 6$, the polynomial $g(X) = X^3 + w^2X^2 + w^2X + w$ divides $X^\beta - 1$ in $R[X, \theta]$. The matrix G_{up}, obtained from $g(X)$, generates a $[12, 3, 8]_4$ quasi-cyclic code, which is optimal according to the Grassl table* **?**. *Moreover, checking the online database* **?**, *we see that it is a new code among the class of quasi-cyclic codes. Table* **??** *includes a few more examples of optimal $\mathbb{F}_4$ codes of length 2β.*

TABLE 3.1

Examples of Optimal $\mathbb{F}_4$-Linear Codes from G_{up}

No.	Parameters	$g(X) \in R[X, \theta]$	Remark
1	$[6, 2, 4]_4$	$X + (v + w)$	
2	$[8, 2, 6]_4$	$X^2 + wX + w$	New as a QC code
3	$[10, 2, 8]_4$	$X^3 + (v + w)X^2 + (v + w)X + 1$	
4	$[10, 3, 6]_4$	$X^2 + (v + w^2)X + 1$	
5	$[12, 3, 8]_4$	$X^3 + w^2X^2 + w^2X + w$	New as a QC code

A number of high-rate optimal linear codes over $\mathbb{F}_4$ from skew cyclic codes over R (that is, $\alpha = 0$) can be constructed from the full matrix $\phi(G)$ in Equation (**??**). Table **??** provides a representative subset of such codes, each of length 2β.

TABLE 3.2

Examples of Optimal $\mathbb{F}_4$-Linear Codes from $\phi(G)$

No.	Parameter	$g(X) \in R[X,\theta]$	No.	Parameter	$g(X) \in R[X,\theta]$
1	$[8,6,2]_4$	$X+w^2$	5	$[16,14,2]_4$	$X+w^2$
2	$[10,8,2]_4$	$X+1$	6	$[18,16,2]_4$	$X+v+w^2$
3	$[12,10,2]_4$	$X+w$	7	$[20,18,2]_4$	$X+w^2$
4	$[14,12,2]_4$	$X+1$	8	$[30,28,2]_4$	$X+v+w^2$

Finally, for $\alpha \neq 0$ and $\beta \neq 0$, to maximize the minimum distance of the image of an $\mathbb{F}_4 R$ skew cyclic code, one can consider codes with generators of the form $(g_\alpha(X), g_\beta(X))$ where $g_\alpha(X)$ divides $X^\alpha - 1$ over $\mathbb{F}_4$ and $g_\beta(X)$ divides $X^\beta - 1$ in $R[X,\theta]$ such that $\alpha - \deg g_\alpha(X) = 2(\beta - \deg g_\beta(X))$. This ensures that the dimension of the cyclic code over $\mathbb{F}_4$ generated by $g_\alpha(X)$ is equal to the dimension of the Gray ($\mathbb{F}_4$)-image of the skew cyclic code over R generated by $g_\beta(X)$. A generator matrix of the Gray image is of the form

$$\Big(G_{g_\alpha} | \phi(G)\Big)$$

where G_{g_α} is the circulant matrix obtained from $g_\alpha(X)$, *i.e.*, the standard generator of the cyclic code generated by $g_\alpha(X)$, and $\phi(G)$ is as in Equation (**??**). Moreover, the ranks of these two matrices are the same.

The main advantage of this construction is to enable us to find codes with minimum distances much higher than what we would have gotten from the direct sum construction in Theorem **??**. The codes in Table **??** have minimum distances that are within 2 to 4 units of the minimum distances of the comparable best-known linear codes in **?**. We present the polynomials in a compact form by listing the coefficients in the decreasing order of exponents. In Entry 1, for example, $[1ww^2w^2w^2]$ stands for $X^4 + wX^3 + w^2X^2 + w^2X + w^2$. For brevity, since a cyclic code can also be defined by its check polynomial $h(X) := (X^n - 1)/g(X)$, we give the check polynomial $h_\alpha(X)$, instead of $g_\alpha(X)$, whenever $\deg(h_\alpha(X)) < \deg(g_\alpha(X))$.

We have thus shown that there are several possible ways to construct good quaternary codes via skew cyclic codes over $\mathbb{F}_4 R$.

TABLE 3.3

Examples of $\mathbb{F}_4$-Linear Codes with Good Parameters

No.	α	β	h_α	g_β	Parameters
1	10	5	$[1ww1]$	$[1(v+w)(v+w)1]$	$[20,4,9]_4$
2	15	3	$[1ww^2w^2w^2]$	$[1(v+w^2)]$	$[21,4,12]_4$
3	17	3	$[11w11]$	$[1(v+w)]$	$[23,4,14]_4$
4	15	5	$[1ww^2w^2w^2]$	$[1(v+w)(v+w)1]$	$[25,4,14]_4$
5	30	3	$[1ww^2w^2w^2]$	$[1(v+w)]$	$[36,4,22]_4$
6	34	3	$[11w11]$	$[11]$	$[40,4,26]_4$
7	45	3	$[1ww^2w^2w^2]$	$[1(v+w)]$	$[51,4,32]_4$
8	51	3	$[11w11]$	$[1(v+w^2)]$	$[57,4,38]_4$
9	63	3	$[10w^21w^2]$	$[1(v+w)]$	$[69,4,49]_4$

3.5 DNA Skew Cyclic Code over $\mathbb{F}_4R$

The encoding and decoding systems to store or transfer information or data by mimicking DNA sequences are known collectively as *DNA codes*. The strands, *i.e.*, DNA strings, are preferred to be short to make the synthesis easy and cheap. They must, however, satisfy numerous constraints to be useful for applications. The two most common applications are as basic tools for biomolecular computation and as biomolecular barcoding-tagging system to identify and manipulate individual molecules in complex libraries.

Numerous approaches to DNA codes have been extensively investigated. A recent addition to several surveys that have appeared in the literature is the work of Limbachiya *et al*in **?**. Tools from algebraic coding theory, both from finite fields as well as rings, have been fruitfully used since the inception. A relatively early work by Marathe *et al*in **?** discussed important design criteria and bounds derived from error-correcting codes. We continue on this line of studies by constructing $\mathbb{F}_4R$-DNA skew cyclic codes.

The *Watson-Crick complement* of a strand is the strand obtained by replacing each A by T and vice versa, and each G by C and vice versa. One writes $\overline{\mathtt{A}} = \mathtt{T}$, $\overline{\mathtt{T}} = \mathtt{A}$, $\overline{\mathtt{C}} = \mathtt{G}$, and $\overline{\mathtt{G}} = \mathtt{C}$. Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ be distinct codewords in

a DNA code $\mathcal{D}$. The *reverse* of $\mathbf{x}$ is $\mathbf{x}_{\text{rev}} = (x_n, x_{n-1}, \ldots, x_1)$. The *complement* of $\mathbf{x}$ is $\mathbf{x}^c = (\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})$. Hence, $\mathbf{x}^c_{\text{rev}} = (\overline{x_n}, \overline{x_{n-1}}, \ldots, \overline{x_1})$ is the *reverse complement* of $\mathbf{x}$.

The process in which a strand and its complement bound to form a double-helix is known as *hybridization*. Constraints on the codewords in a DNA code are imposed to avoid it. Let $\mathcal{D}$ be a DNA code of fixed length n, cardinality M, and minimum distance d. Then the constraints on the Hamming distances

$$\mathrm{wt_H}(\mathbf{x}, \mathbf{y}) \geq \mathrm{d} \text{ and } \mathrm{wt_H}(\mathbf{x}^{\mathrm{c}}, \mathbf{y}_{\mathrm{rev}}) \geq \mathrm{d} \text{ for all } \mathbf{x}, \mathbf{y} \in \mathcal{D} \tag{3.12}$$

are imposed to prevent hybridization between any two strands as well as between a strand and the reverse of any other strand. A *reverse-complement DNA code* $\mathcal{D}$ has parameters $(n, M, d)_4$ that satisfies Equation (**??**).

Abualrub *et al*studied $\mathbb{F}_4$-DNA codes of odd lengths in **?**, using the bijection between the set of DNA alphabets $\{\mathtt{A}, \mathtt{T}, \mathtt{C}, \mathtt{G}\}$ and $\mathbb{F}_4 := \{0, 1, w, w^2\}$, in that respective ordering. They also established that any $\mathbb{F}_4$-cyclic code with generator polynomial $f(X)$ is reverse-complement if and only if $f(X) \in \mathbb{F}_4[X]$ is a self-reciprocal polynomial, *i.e.*, $f(X) = X^{\deg(f(X))} \cdot f(X^{-1})$, which is not divisible by $X - 1$ in (**?**, Theorem 11).

We now extend their bijection to a bijection between the elements of R and the 16 DNA codons in $\{\mathtt{A}, \mathtt{C}, \mathtt{G}, \mathtt{T}\}^2$. Let $a := a_1 + vb_1 \in R$, with $a_1, b_1 \in \mathbb{F}_4$. The complement $\overline{a}$ of a is given by

$$\overline{a} := a + v = a_1 + v(b_1 + 1). \tag{3.13}$$

The next lemma follows immediately from the definition.

Lemma 19. *For all $a, b \in R$, we have*

$$\overline{a + b} = \overline{a} + \overline{b} + v,\ \overline{(v+1)a} = (v+1)\overline{a} + v, \text{ and } \overline{va} = v\overline{a}.$$

The bijection that we use here can be explicitly given as a list.

$a \in R$	Base pairs	$\overline{a} \in R$	Base pairs	$a \in R$	Base pairs	$\overline{a} \in R$	Base pairs
0	AA	v	TT	$1 + vw^2$	CG	$1 + vw$	GC
1	TA	$1 + v$	AT	$w^2 + vw^2$	AG	$w^2 + vw$	TC
w	CA	$w + v$	GT	vw^2	GG	vw	CC
w^2	GA	$w^2 + v$	CT	$w + vw^2$	TG	$w + vw$	AC

Definition 19. *An R-linear code C of length β is called DNA-skew cyclic if*

1. *The code C is R-skew cyclic of length β.*

2. *For any codeword $\mathbf{x} \in C$, $\mathbf{x} \neq \mathbf{x}^c_{rev}$ with $\mathbf{x}^c_{rev} \in C$.*

We adopt the following definition of reciprocal polynomials.

Definition 20. *Let $f(X) = \sum_{i=0}^{\alpha} a_i X^i$ be a polynomial in $R[X, \theta]$. The reciprocal polynomial of $f(X)$ is the polynomial $f^\star(X)$ given by*

$$f^\star(X) := (f(X))^\star = X^\alpha \cdot f(X^{-1}) = \sum_{i=0}^{\alpha} \theta^\alpha(a_i) X^{\alpha-i} = \sum_{i=0}^{\alpha} \theta^\alpha(a_{\alpha-i}) X^i. \tag{3.14}$$

If $f(X) = f^\star(X)$, then $f(X)$ is skew self-reciprocal.

Lemma 20. *Let $f(X), g(X) \in R[X, \theta]$, with $\alpha = \deg(f(X)) \geq \deg(g(X)) = \beta$. Then the following assertions hold.*

1. *The reciprocal of $f(X) \cdot g(X)$ is given by*

$$(f(X) \cdot g(X))^\star = \begin{cases} f^\star(X) \cdot g^\star(X) & \text{if } \beta \text{ is even}, \\ \Theta(f^\star(X)) \cdot g^\star(X) & \text{if } \beta \text{ is odd}. \end{cases} \tag{3.15}$$

2. $(f(X) + g(X))^\star = f^\star(X) + X^{\alpha-\beta} \cdot g^\star(X)$.

Proof. Let $f(X) = \sum_{i=0}^{\alpha} a_i X^i$ and $g(X) = \sum_{j=0}^{\beta} b_j X^j$ be polynomials in $R[X, \theta]$ with $\alpha \geq \beta$. Then,

$$f(X) \cdot g(X) = \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} a_i \theta^i(b_j) X^{i+j}.$$

To prove the first assertion, we use Equation (**??**) to obtain

$$\begin{aligned} (f(X) \cdot g(X))^\star &= \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \theta^{\alpha+\beta}(a_i)\, \theta^{\alpha+\beta-i}(b_j) X^{\alpha+\beta-i-j} \\ &= \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \theta^{\alpha+\beta}(a_{\alpha-i})\, \theta^{\beta+i}(b_{\beta-j}) X^{i+j}. \end{aligned} \tag{3.16}$$

On the other hand, applying Equation (**??**) on $f(X)$ and $g(X)$, we get

$$\begin{aligned} f^\star(X) \cdot g^\star(X) &= \left(\sum_{i=0}^{\alpha} \theta^\alpha(a_{\alpha-i}) X^i \right) \left(\sum_{j=0}^{\beta} \theta^\beta(b_{\beta-j}) X^j \right) \\ &= \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \theta^\alpha(a_{\alpha-i})\, \theta^{\beta+i}(b_{\beta-j}) X^{i+j}. \end{aligned} \tag{3.17}$$

Since θ has order 2, the expression in Equations (**??**) and (**??**) are equal when β is even. When β is odd, we can write the expression in Equation (**??**) as

$$\sum_{i=0}^{\alpha}\sum_{j=0}^{\beta}\theta^{\alpha+1}(a_{\alpha-i})\,\theta^{\beta+i}(b_{\beta-j})X^{i+j} = \Theta(f^{\star}(X))\cdot g^{\star}(X).$$

To prove the second assertion, we use Equation (**??**) to write

$$(f(X)+g(X))^{\star} = \sum_{j=0}^{\beta}\theta^{\alpha}(a_j+b_j)X^{\alpha-j} + \sum_{i=\beta}^{\alpha}\theta^{\alpha}(a_i)X^{\alpha-i} = \sum_{i=0}^{\alpha}\theta^{\alpha}(a_{\alpha-i})X^{i} + \sum_{j=0}^{\beta}\theta^{\alpha}(b_{\beta-j})X^{j} = f^{\star}(X) + X^{\alpha-\beta}\cdot g^{\star}(X).$$

□

Example 9. *Given $f(X) = X + 1$ and $g(X) = X + v$ in $R[X, \theta]$, we have*

$$(f(X)\cdot g(X))^{\star} = vX^2 + vX + 1 = \Theta(f^{\star}(X))\cdot g^{\star}(X).$$

A code is *reversible complement* if $\mathbf{c}^{c}_{\text{rev}} \in C$ for any $\mathbf{c} \in C$. The next theorem characterizes reversible complement R-skew cyclic codes.

Theorem 33. *Let $g_1(X)$ and $g_2(X)$ divide $X^{\beta} - 1$ in $\mathbb{F}_4[X]$. Let $C = \langle g(X)\rangle$ be R-skew cyclic of odd length β with $g(X) = vg_1(X)+(v+1)g_2(X)$. Then C is reversible complement if and only if $g(X)$ is skew self-reciprocal and $v(X^{\beta} - 1)/(X - 1) \in C$.*

Proof. Let $g(X) = vg_1(X) + (v + 1)g_2(X)$ and $C = \langle g(X)\rangle$ be an R-skew cyclic code of odd length β. Suppose that C is reversible complement. Since $\mathbf{0} \in C$, we have $\left(\overline{0}, \overline{0}, \ldots, \overline{0}\right) = (v, v, \ldots, v) = v(X^{\beta} - 1)/(X - 1) \in C$. Let

$$g_1(X) = g_0 + g_1X + \ldots + g_{t-1}X^{t-1} + X^t \text{ and}$$
$$g_2(X) = h_0 + h_1X + \ldots + h_{k-1}X^{k-1} + X^k,$$

where $t \leq k$. Then

$$\begin{aligned} g(X) &= vg_1(X) + (v + 1)g_2(X)\\ &= (vg_0 + (v + 1)h_0) + (vg_1 + (v + 1)h_1)X + \ldots\\ &+ (vg_{t-1} + (v + 1)h_{t-1})X^{t-1} + (v + (v + 1)h_t)X^t\\ &+ (v + 1)h_{t+1}X^{t+1} + \ldots + (v + 1)h_{k-1}X^{k-1} + (v + 1)X^k. \end{aligned}$$

Since C is reversible complement, it contains

$$\begin{aligned} g^c_{\mathsf{rev}}(X) = v(1 + X + \ldots + X^{\beta-k-2}) + \overline{(v+1)}X^{\beta-k-1} + \overline{(v+1)h_{k-1}}X^{\beta-k} \\ + \ldots + \overline{(v+1)h_{t+1}}X^{\beta-t-2} + \overline{(v+(v+1)h_t)}X^{\beta-t-1} \\ + \overline{(vg_{t-1}+(v+1)h_{t-1})}X^{\beta-t} + \ldots + \overline{(vg_1+(v+1)h_1)}X^{\beta-2} \\ + \overline{(vg_0+(v+1)h_0)}X^{\beta-1}. \end{aligned}$$

Using Lemma **??** we can write

$$\begin{aligned} g^c_{\mathsf{rev}}(X) = v(1 + X + \ldots + X^{\beta-k-2}) + \overline{(v+1)}X^{\beta-k-1} + \overline{(v+1)h_{k-1}}X^{\beta-k} \\ + \ldots + \overline{(v+1)h_{t+1}}X^{\beta-t-2} + \overline{v}X^{\beta-t-1} + \overline{(v+1)h_t}X^{\beta-t-1} + vX^{\beta-t-1} \\ + \overline{vg_{t-1}}X^{\beta-t} + \overline{(v+1)h_{t-1}}X^{\beta-t} + vX^{\beta-t} + \ldots + \overline{vg_1}X^{\beta-2} \\ + \overline{(v+1)h_1}X^{\beta-2} + vx^{\beta-2} + \overline{vg_0}X^{\beta-1} + \overline{(v+1)h_0}X^{\beta-1} + vX^{\beta-1}. \end{aligned}$$

Because C is R-linear, $g^c_{\mathsf{rev}}(X) + v(X^\beta - 1)/(X-1) \in C$. This implies

$$\begin{aligned} & g^c_{\mathsf{rev}}(X) + v(X^\beta - 1)/(X-1) = \\ & (\overline{(v+1)} + v)X^{\beta-k-1} + (\overline{(v+1)h_{k-1}} + v)X^{\beta-k} + \ldots + \\ & (\overline{(v+1)h_{t+1}} + v)X^{\beta-t-2} + (\overline{v} + v)X^{\beta-t-1+} (\overline{(v+1)h_t} + v)X^{\beta-t-1} + \\ & (\overline{vg_{t-1}} + v)X^{\beta-t} + (\overline{(v+1)h_{t-1}} + v)X^{\beta-t} + \ldots + (\overline{vg_1} + v)X^{\beta-2} + \\ & (\overline{(v+1)h_1} + v)X^{\beta-2} + (\overline{vg_0} + v)X^{\beta-1} + (\overline{(v+1)h_0} + v)X^{\beta-1}. \end{aligned}$$

By Equation (**??**) we can write

$$\begin{aligned} & (v+1)X^{\beta-k-1} + (v+1)h_{k-1}X^{\beta-k} + \ldots + (v+1)h_{t+1}X^{\beta-t-2} + \\ & vX^{\beta-t-1} + (v+1)h_tX^{\beta-t-1} + X^{\beta-t} + (v+1)h_{t-1}X^{\beta-t} + \ldots + \\ & vg_1X^{\beta-2} + (v+1)h_1X^{\beta-2} + vg_0X^{\beta-1} + (v+1)h_0X^{\beta-1} \end{aligned}$$

as

$$\begin{aligned} & (v+1)X^{\beta-k-1} + (v+1)h_{k-1}X^{\beta-k} + \ldots + (v+1)h_{t+1}X^{\beta-t-2} + \\ & (v+(v+1)h_t)X^{\beta-t-1} + (vg_{t-1} + (v+1)h_{t-1})X^{\beta-t} + \ldots + \\ & (vg_1 + (v+1)h_1)X^{\beta-2} + (vg_0 + (v+1)h_0)X^{\beta-1}. \end{aligned}$$

Multiplying on the left by $X^{k+1-\beta}$, we obtain

$$\theta^k(v+1)+\theta^k((v+1)h_{k-1})X+\ldots+\theta^k((v+1)h_{t+1})X^{k-t-1}$$
$$+\theta^k(v+(v+1)h_t)X^{k-t}+\theta^k(vg_{t-1}+\theta^k(v+1)h_{t-1})X^{k-t+1}+\ldots$$
$$+\theta^k(vg_1+(v+1)h_1)X^{k-1}+\theta^k(vg_0+(v+1)h_0)X^k.$$

Hence, $g^\star(X)\in C$. Since $C=\langle g(X)\rangle$, there exists $q(X)\in R[X,\theta]$ such that $g^\star(X)=q(X)\cdot g(X)$, which implies $\deg(g^\star(X))=\deg(g(X))$ and $q(X)=1$. Thus, $g^\star(X)=g(X)$, as required.

Conversely, let $C=\langle g(X)\rangle$ be an R-skew cyclic code of length β generated by $g(X)=vg_1(X)+(v+1)g_2(X)$, where $g_1(X)$ and $g_2(X)$ are two divisors of $X^\beta-1$ in $\mathbb{F}_4[X]$. Let $c(X)=c_0+c_1X+\ldots+c_kX^k\in C$, then there exists $q(X)\in R[X,\theta]$ such that $c(X)=q(X)\cdot g(X)$. By Lemma **??**, $c^\star(X)=q^\star(X)\cdot g^\star(X)$. Since C is skew self-reciprocal, $c^\star(X)=q^\star(X)\cdot g(X)\in C$ for any $c(X)\in C$. We have

$$c^\star(X)=\theta^k(c_k)+\theta^k(c_{k-1})X+\ldots+\theta^k(c_0)X^k\in C.$$

Hence,

$$v(X^\beta-1)/(X-1)=v(1+\ldots+X^{\beta-1})\in C.$$

Since C is R-linear,

$$X^{\beta-k-1}\cdot c^\star(X)+v(X^\beta-1)/(X-1)=$$
$$v+\ldots+vX^{\beta-k-2}+(c_0+v)X^{\beta-k-1}+\ldots+(c_k+v)X^{\beta-1}.$$

By Equation (**??**),

$$v+\ldots+vX^{\beta-k-2}+\overline{c_0}X^{\beta-k-1}+\ldots+\overline{c_K}X^{\beta-1}=(c^\star(X))^c_{\text{rev}}\in C.$$

This concludes the proof. □

The theorem that we have just proved leads us from R-skew cyclic codes to the definition and subsequent characterization of $\mathbb{F}_4R$-skew cyclic codes in the context of DNA coding.

Definition 21. *An $\mathbb{F}_4R$-linear code C is DNA-skew cyclic if the following conditions hold.*

1. *C is an $\mathbb{F}_4R$-skew cyclic code,* i.e.*, C is an R-left submodule of*

$$F[X]/\langle X^{\alpha}-1\rangle \times R[X,\theta]/\left\langle X^{\beta}-1\right\rangle.$$

2. *Any codeword $\mathbf{c}=(\mathbf{c}_1,\mathbf{c}_2)\in C$ and its reverse complement*

$$\mathbf{c}^{c}_{rev}=((\mathbf{c}_1)^{c}_{rev},(\mathbf{c}_2)^{c}_{rev})\in C$$

are distinct.

The characterization of reverse complement codes over $\mathbb{F}_4R$ can now be established.

Theorem 34. *Let $C=\langle(f(X),\mathbf{0}),(\mathbf{0},g(X)\rangle$ be an $\mathbb{F}_4R$-skew cyclic code. Note that $\ell(X):=\mathbf{0}$ and $C=C_1\otimes C_2$, with C_1 an $\mathbb{F}_4$-cyclic code and C_2 an R-skew cyclic code. Then C is reversible complement if and only if C_1 and C_2 are reversible complement over $\mathbb{F}_4$ and R, respectively.*

Proof. Let C be an $\mathbb{F}_4R$-skew cyclic code generated by $(f(X),\mathbf{0})$ and $(\mathbf{0},g(X))$. Lemma **??** shows how to find $C=C_1\otimes C_2$. Let $\mathbf{c}=(\mathbf{c}_1,\mathbf{c}_2)\in C=C_1\otimes C_2$ with $\mathbf{c}_1\in C_1$ and $\mathbf{c}_2\in C_2$. Suppose that C_1 and C_2 are reversible complement over $\mathbb{F}_4$ and R, respectively. Then we have $(\mathbf{c}_1)^{c}_{\text{rev}}\in C_1$ and $(\mathbf{c}_2)^{c}_{\text{rev}}\in C_2$. Thus,

$$((\mathbf{c}_1)^{c}_{\text{rev}},(\mathbf{c}_2)^{c}_{\text{rev}})=\mathbf{c}^{c}_{\text{rev}}\in C_1\otimes C_2=C.$$

Conversely, let $\mathbf{c}_1\in C_1$ and $\mathbf{c}_2\in C_2$. Then $\mathbf{c}=(\mathbf{c}_1,\mathbf{c}_2)\in C$. If C is reversible complement, then

$$\mathbf{c}^{c}_{\text{rev}}=((\mathbf{c}_1)^{c}_{\text{rev}},(\mathbf{c}_2)^{c}_{\text{rev}})\in C=C_1\otimes C_2.$$

This implies $\mathbf{c}^{c}_{1,\text{rev}}\in C_1$ and $\mathbf{c}^{c}_{2,\text{rev}}\in C_2$, as required. □

The presented results are publish in International Journal. See **?**.

3.6 Conclusion

In this thesis, in chapter 2 we have presented the generator matrices of linear codes over $\mathbb{F}_4R$ and those of their dual codes. This is a salient step in determining the parameters of such codes. As computational tools, the matrices can be used to search for, or otherwise rule out the existence of, codes with specified parameter sets. Future classification effort is likely to benefit as well. Towards the end, we established the MacWilliams identity for linear codes over $\mathbb{F}_4R$.

Also, in chapter 3, we have presented our study on skew cyclic codes over the ring $\mathbb{F}_4R$. Their algebraic structure as left submodules of a skew-polynomial ring is investigated, resulting in the identification of their generators. We have shown that, under some simple conditions on their length, they are equivalent to cyclic or 2-quasi-cyclic codes over the same ring. We supplied several ways of obtaining $\mathbb{F}_4$-linear codes with good parameters as images of $\mathbb{F}_4R$-skew cyclic codes under the Gray mapping.
Finally, In terms of practical applications, we are currently looking into DNA computing, we have demonstrated how this setup leads naturally to DNA codes and proved a condition on the associated generator polynomial of an $\mathbb{F}_4R$-skew cyclic code that guarantees the code to be reversible complement. One of the interesting questions to explore in this topic is to find out whether the class of codes that we propose here contains codes with better relative minimum distances or sizes than known DNA codes. Usage as DNA codes, which are encoding and decoding systems to store or transfer information by mimicking DNA sequences. They are commonly used in biomolecular computation and as biomolecular barcoding system.

Bibliography

T. Abualrub and N. Aydin, Additive cyclic codes over mixed alphabets and the football pool problem, *Discrete Math., Algorithms and Appl.*, **9** (2017), https://doi.org/10.1142/S1793830917500100.

T. Abualrub, N. Aydin, P. Seneviratne, On θ-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, *Australasian Journal of Combinatorics*. Volume **54** (2012), Pages 115–126.

T. Abualrub, A. Ghrayeb, N. Aydin and I. Siap, On the construction of skew quasi-cyclic codes, *IEEE Trans. Inform. Theory*, **56** (2010), 2081–2090.

T. Abualrub, A. Ghrayeb and X. N. Zeng, Construction of cyclic codes over $GF(4)$ for DNA computing, *J. Franklin Inst.*, **343** (2006), 448–457.

T. Abualrub, I. Siap and N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, *IEEE Trans. Inform. Theory*, **60** (2014), 1508–1514.

I. Aydogdu, T. Abualrub, and I. Siap : On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. Int. J. of Comput. Math. **92** (9), 1806–1814 (2015)

A. Batoul, K. Guenda, A. Kaya, B. Yildiz, Cyclic Isodual and Formally Self-dual Codes over $\mathbb{F}_q + v\mathbb{F}_q$. *European Journal of Pure and Applied Mathematics*, **8** (2015), 64–80.

A. Bayram, E. Oztas and I. Siap, Codes over $\mathbb{F}_4 + v\mathbb{F}_4$ and some DNA applications, *Des. Codes Cryptogr.*, **80** (2016), 379–393.

N.Benbelkacem, J. Borges, S.T. Dougherty, C. C. Fernández-Córdoba. On $\mathbb{Z}_2\mathbb{Z}_4$-additive complementary dual codes and related LCD-codes, *Finite Fields Appl.* 62 (2020), 101622.

N. Benbelkacem, M.F. Ezerman, A. Abualrub, Linear codes over F4R and their MacWilliams Identity, *Discrete Mathematics, Algorithms and Applications*, Doi: 10.1142/S1793830920500858.

N.Benbelkacem, M.F. Ezerman, T. Abualrub, A.Batoul, Skew Cyclic Codes over F4R, Journal of Algebra and its Applications.

N. Bennenni, K. Guenda and S. Mesnager, DNA cyclic codes over rings, *Adv. Math. Commun.*, **11** (2017), 83–98.

M. Bilal, J. Borges, S.T. Dougherty, C. Fernández-Córdoba. Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$. *Designs, Codes Cryptogr.*, vol. 61, no. 1, pp. 31–40, 2011.

J. Borges, S.T. Dougherty, C. Fernández-Córdoba. Characterization and constructions of self-dual codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$. *Adv. Math. Commun.*, vol. 6, no. 3, pp. 287–303, 2012.

J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: Generator matrices and duality, *Des. Codes Cryptogr.*, **54** (2010), 167–179.

D. Boucher, W. Geiselmann and F. Ulmer, Skew-cyclic codes, *Appl. Algebra Engrg. Comm. Comput.*, **18** (2007), 379–389.

D. Boucher, P. Sole and F. Ulmer, Skew constacyclic codes over Galois rings, *Adv. Math. Commun.*, **2** (2008), 273–292.

C. Carlet, S. Guilley, “Complementary dual codes for counter-measures to side-channel attacks," in Coding Theory and Applications (CIM Series in Mathematical Sciences), vol. 3, E. R. Pinto Eds. Berlín, Germany: Springer Verlag, 2014, pp. 97-105.

Z. Chen, Online database of quasi-twisted codes http://www.tec.hkr.se/~chen/research/codes/searchqc2.htm. Accessed on April 26, 2019.

S.T. Dougherty, J. L. Kim, B. Ozkaya, L. Sok, P. Solé, “The combinatorics LCD codes: Linear programming bound and orthogonal,” *I*nternational Journal of Information and Coding Theory, vol. 4, no. 2-3, pp 116-128, 2017.

M. Esmaeili, S. Yari, “On complementary-dual quasi-cyclic codes," *Finite, Fields Appl.*, vol. 15, no. 3, pp. 375-386, 2009.

C. Fernández-Córdoba, J. Pujol, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel," *Designs, Codes and Cryptography*, vol. 56, pp. 43-59, 2010.

M. Grassl Bounds on the minimum distance of linear codes and quantum codes. Online at http://www.codetables.de. Accessed on May 12, 2019.

F. Gursoy, I. Siap and B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, *Adv. Math. Commun.*, **8** (2014), 313–322.

C. Güneri, B. Özkaya, P. Solé, "Quasi-cyclic complementary dual codes," *Finite, Fields Appl.*, vol. 42, pp. 67-80, 2016.

Hall, J. (2010). Notes on Coding Theory. lecture notes.

A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, "The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes," *IEEE Trans. on Information Theory*, vol. 40, 301-319, 1994.

M. Harada, K. Saito, "Binary linear complementary dual codes," *Cryptography and Communications*, vol. 11, pp. 677-696, 2019.

Huffman, W. and Pless, V. (2003). Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge, first edition.

Jacobson, N. The Theory of rings, New York: American Mathematical Society. 1943.

A. Leroy, Pseudo-linear transformations and evaluation in Ore extensions, *Bull. Belg. Math. Soc.* **2** (1995), 321–347.

C. Li, C. Ding, S. Li, "LCD cyclic codes over finite fields," *IEEE Trans. on Information Theory*, vol. 63, n. 7, pp. 4344-4356, 2017.

Lidl, R., Niederreiter, H., and Cohn, P. (1997). Finite Fields. Cambridge University Press, second edition.

D. Limbachiya, B. Rao and M. K. Gupta, The art of DNA strings: Sixteen years of DNA coding theory. Online at http://arxiv.org/abs/1607.00266

X. Liu, H. Liu, “LCD codes over finite chain rings,” *Finite Fields and Their Applications*, vol. 34, pp. 1-19, 2015.

J.L. Massey, “Reversible codes," *Inf. Control*, vol. 7, no 3, pp. 369-380, 1964.

J.L. Massey, Linear Codes with Complementary Duals, Disc. Math, **106-107**, 337 - 342, 1992.

A. Marathe, A. E. Condon and R. M. Corn, On combinatorial DNA word design, *J. Comput. Biology* **8** (2001), 201–219.

McDonald, B. R. Finite Rings with identity. New York: Marcel Dekker Inc. 1974

A. Melakhessou, N. Aydin, Z. Hebbache, K. Guenda, $\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q)$-linear skew constacyclic codes, *J. Algebra Comb. Discrete Appl.* **7(1)** (2020), 85–101.

Pless, V. (1998). Introduction to the Theory of Error-Correcting Codes. In Discrete Mathematics And Optimization. John Wiley and Sons, third edition.

H. Rifá-Pous, J. Rifá, and L. Ronquillo, $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes in steganography, *Adv. Math. Commun.*, **5** (2011), 425–433.

J. Rifà and J. Pujol. Translation-invariant propelinear codes, *IEEE Trans. Inf. Theory*, vol. 43, no. 2, pp. 590–598, 1997.

R. M. Roth, Introduction to coding Theory. Cambride University Press.

O.Ore, Theory of non-commutative polynomials. *Ann. Math.* **34**. 480–508, 1933

M. Shi, A. Alahmadi, and P. Solé : Codes and Rings: Theory and Practice. Academic Press, Orlando, FL, USA (2017)

C. Shannon, A mathematical theory of communication, *Bell System Tech.J.* **27** (1948), 379–423 and 623–656.

I. Siap, T. Abualrub, N. Aydin, and P. Seneviratne Skew cyclic codes of arbitrary length, *Int. J. Information and Coding Theory*, **2** (2011), 425–433.

J. H. VanLint, Introduction to Coding Theory. Springer. Third Edition.

S. A. Vanstone, P. C. Van Oorschol. An Introduction to Error Correcting Codes With Applications. University of Waterloo.

Z. X. Wan : Lectures on Finite Fields and Galois Rings. World Scientific, Singapore (2003)

S. Zhu, Y. Wang, and M. Shi, Some result on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, *IEEE Trans. Inform. Theory*, **56** (2010), 1680–1684.