N° d'ordre: 136/2024-C/MT

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie Houari Boumediene
Faculté des Mathématiques

Thèse de Doctorat

Présentée pour l'obtention du grade de DOCTEUR

En : MATHEMATIQUES

Spécialité : Mathématiques Fondamentales et Cryptographie

Par : BELLIL Amina

Sujet

Bornes de codes correcteurs d'erreurs

Soutenue publiquement le 08/02/2024 devant le jury composé de:

M. Bouroubi Sadek	Professeur	à l'USTHB	Président
Mme. Guenda Kenza	Professeur	à l'USTHB	Directrice de thèse
M. Benoumhani Moussa	Professeur	à l'Université de M'sila	Examinateur
Mme. Mamache Fatiha	Maître de Conférence/A	à l'USTHB	Examinatrice
Mme. Selmane Schehrazad	Professeur	à l'USTHB	Examinatrice
M. Aydin Nuh	Professeur	à l'Université de Kenyon	Invité

Acknowledgement

I would like to express my sincere gratitude to my supervisor, Pr. Guenda Kenza for her consistent guidance, immense encouragement and endless support in every step throughout the process. In fact, without her effective guidance and dedicated involvement, this work would have never been carried out.

I would like to thank professor Nuh Aydin for his constructive and valuable advice, proper guidance, and opportunities.

I wish also to extend my gratitude and appreciation to Dr. Hebbache Zineb for her help, advice, support and encouragement.

I am extremely grateful to my doctoral committee members, Pr. Bouroubi Sadek, Pr. Benoumhani Moussa, Pr. Aydin Nuh, Dr. Selmane Schahrazad and Dr. Mamache Fatiha for their valuable time, effort and observation.

I am very grateful for the endless and priceless support that I received from my family. Specifically, my parents, my husband, my sisters and brothers.

To the memory of our beloved Pr. Laoudi Aini.

ملخص

من بين الخلفية الرياضية لنظرية الترميز، يمكننا أن نذكر الجبر الخطي، ونظرية المجموعات، والحلقات والحقول المحددة، ومناطق أخرى من الرياضيات المنفصلة، مثل نظرية الرسوم البيانية.

تشكل الرموز الدورية الثابتة على الحلقات مجموعة مهمة من الرموز. تُدرس هذه الرموز على نطاق واسع لهياكلها الجبرية المثيرة للاهتمام وتطبيقاتها المتنوعة.
دراستنا تتضمن دراسة الرموز الدورية الثابتة والرموز شبه ملتوية على $R = \mathbb{Z}_q + v\mathbb{Z}_q$ مع $v^2 = 1$. نقدم بعض الرموز الخطية الجديدة على $\mathbb{Z}_4$.

وأخيراً، يتم تقديم وصف للرموز الخطية المتكاملة الزوجية الدورية الثابتة على R.

الكلمات الرئيسية: الرموز الدورية الثابتة، الرموز شبه ملتوية، الرموز الخطية المتكاملة الزوجية .

Abstract

Among the mathematical background of coding theory, we can cite linear algebra, group theory, rings and finite fields and other areas of discrete mathematics, such as Graph Theory. Constacyclic codes over rings constitute an important class of codes. These codes are widely studied for their interesting algebraic structures and their various applications.

Our study consists, of studying constacyclic and quasi-twisted(QT) codes over $R = \mathbb{Z}_q + v\mathbb{Z}_q$ with $v^2 = 1$. We present some new linear codes over $\mathbb{Z}_4$. Finally, a characterization of linear complementary pair (LCP) constacyclic codes over R is provided.

Keywords: Constacyclic codes, Gray map, quasi-twisted codes, linear complementary pair codes.

Résumé

Parmi les bases mathématiques de la théorie des codes correcteurs d erreurs, on peut citer l'algèbre linéaire, la théorie des groupes, les anneaux et les corps finis, ainsi que d'autres domaines des mathématiques discrètes, tels que la théorie des graphes. Les codes constacycliques sur les anneaux constituent une classe importante de codes qui a été largement étudiée en raison de leurs structures algébriques intéressantes et de leurs nombreuses applications. Notre étude se concentre sur l'examen des codes constacycliques et quasi-twisted (QT) sur l'anneau R, où $R = \mathbb{Z}_q + v\mathbb{Z}_q$ tel que $v^2 = 1$. Nous présentons de nouveaux codes linéaires sur $\mathbb{Z}_4$. Enfin, nous fournissons une caractérisation des codes linéaires complémentaires par paires (LCP) constacycliques sur R.

Mots Clés : Codes constacycliques ; Gray map ; codes quasi-twisted ; LCP.

Notation

$\mathbb{Z}_p$: the ring of integers modulo p.

$\mathbb{Z}_p[X]$: polynomials over $\mathbb{Z}_p$ in the variable X.

$\mathbb{F}_q$: finite field of size q.

$[n, k, d]$-code: linear code of length n and dimension k with minimum distance d.

$C^{\perp}$: Euclidean dual code of a Linear code.

$C^{\perp H}$: Hermitian dual code of a Linear code.

$|C|$: size of C.

G: generator matrix of a Linear code.

G^t: the transpose of a matrix G.

H: Parity-check matrix of a Linear code.

$d(C) = d$: Minimum distance of a Linear code.

W_H: Hamming weight of a Linear code.

W_{Hom}: Homogeneous weight of a Linear code.

$\langle x.y \rangle$: the Euclidean scalar product of x and y.

$\langle x.y \rangle_H$: the Hermitian scalar product of x and y.

gcd : greatest common divisor.

QT: Quasi-twisted.

QC: Quasi-cyclic.

LCD: linear complementary dual.

LCP: Linear Complementary Pair.

Contents

Introduction

1 Review of Litterature

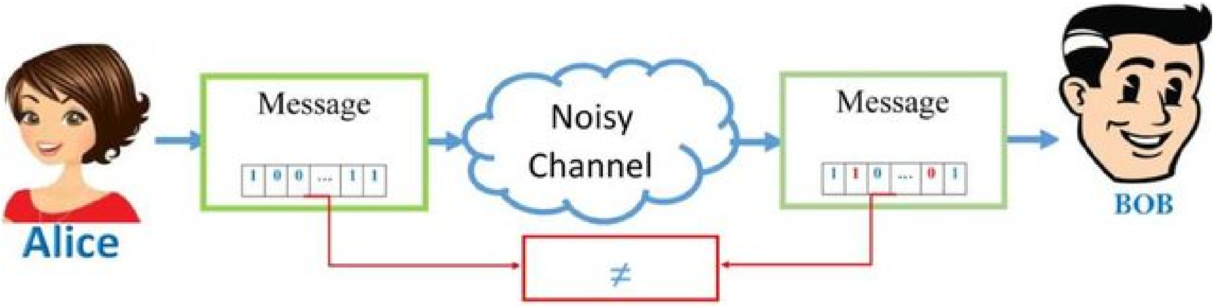
The birth of coding theory was inspired by a classic paper of Shannon in 1948 [53]. In 1949, the American Scientist, Physicist and Mathematician Warren Weaver (1894-1978) established, "The Mathematics of Communication" appeared in the Scientific American [51]. Moreover, other roots of the later so-called "Information Theory" could be found in the Cybernetics of the Norbert Wiener (1894-1964) in [51]. In the 20th century Coding theory arose as a problem in engineering concerning the efficient transmission of information. Hence, coding theory, in this perspective, using the binary field as the alphabet was largely done. Although, the alphabets were quickly generalized to finite fields, at least for mathematicians, because a lots of the techniques and proofs were identical to the binary case seen as the field with two elements [25]. In the very beginning of this study, coding theory was viewed by mathematicians not only as an application to electrical engineering and computer science, but also as a part of pure mathematics [25]. They were interested not only in the fundamental questions of coding theory, but also into its connections by other areas of discrete mathematics. The early results of the connected codes to lattices, combinatorics, and designs. While the alphabets were a finite field these connections were generally made by codes [25]. Some papers were written when the used alphabets were rings, such as Blake's early papers [15] and [16]. It was not until, coding theorists in 1990's started to study codes over finite rings in earnest [25]. The interested reader could consult Sloane's seminal text and MacWilliams "The Theory of Error-Correcting Codes", for the description of classical coding theory [39]. For more description, see Pless's and Huffman, "Fundamentals of Error Correcting Codes" [36]. For the description of the connection between codes and designs see Key's and Assmus "Designs and their Codes" [4]. Codes are generally defined over finite fields, in these all three classic text book. A great deal of research has been devoted to find efficient schemes by which digital information can be coded for reliable transmission through a noisy channel [35]. Error-correcting codes are now widely used in applications such as returning pictures from deep space, design of registration numbers, and storage of date on magnetic tape [36]. Coding theory is also of great mathematical interest, relying on ideas from pure mathematics and, in particular, illustrating the power and the beauty of algebra [35].

2 Toward Codes over Finite Rings

The theory of error-correcting codes has historically been most useful in the context of linear codes. Such codes may be viewed as vector spaces over finite fields carrying with them many familiar and well-studied properties. A generalization of finite fields is the concept of finite rings. Therefore, it is natural to consider codes over finite rings to study which properties such codes maintain in the move to a more general setting. Codes over rings started being of interest to many researchers since the appearance of [34], [39], where it was shown that the binary non-linear codes known as Kerdock and Preparata codes are actually dual codes when viewed as codes over $\mathbb{Z}_4$, via the Gray map. So the most natural class of rings that is suitable for coding theory is given by finite chain rings as it allows to formulate the dual code similar to finite fields. So it is worth to delve into codes over finite chain rings. The class of cyclic codes is one of the most studied class of linear codes. In particular, Dinh and Permouth [21] gave the algebraic structure of simple cyclic codes over finite chain rings. Cyclic codes and their various generalizations such as constacyclic codes and quasi-cyclic (QC) codes have played a key role in this quest. One particularly useful generalization of cyclic codes has been the class of quasi-twisted (QT) codes that produced hundreds of new codes with best known parameters.

3 Motivation

Coding theory was originated as the mathematical foundation for the transmission of messages over noisy communication channels and deals with the problem of detecting and correcting transmission errors caused by the noise of the channel.



The mathematical background of coding theory is, for example, linear algebra, theory of groups, rings and finite fields, and other areas of discrete mathematics, such as theory of designs. Thus, coding theory has now become an active part of mathematical research. Within the family of codes, linear codes are special codes with rich mathematical structure. One of the most studied class of linear codes is the class of cyclic codes. The algebraic structure of cyclic codes makes easier their implementation. For this reason many practically important codes are cyclic. The study of codes over rings has advanced from the middle of 90's. However, in 1963, Assmus and Mattson first considered rings as possible alphabets for codes in [5]. Later, Blake investigate linear codes over certain rings in [15] and [16]. But coding theory really gets a shock when it was discovered that the mentioned families of non-linear binary codes (Preparata, Kerdock, Goethals, ...) can be represented as linear codes over $\mathbb{Z}_4$, see [2] and [34], via the Gray map. The theory of codes over rings has not been developed in depth for general rings. It has been developed principally for codes over finite chain rings since they have similar properties to those of finite fields, as it will be shown later. In recent decades, codes over finite commutative chain rings have been studied considerably (see Refs. [3]; [45]). In the last few years, some specific non-chain rings have been used as an alphabet for codes (see Refs. [29]; [30]). Constacyclic codes form an important class of linear codes and have practical applications to other disciplines including classical and quantum communication systems as they can be encoded with shift registers because of their algebraic structures. Since the factorization of the polynomials over noncommutative structures is not unique, they are potentially more convenient for obtaining good code parameters than commutative structures. This fact made the study of polynomial rings more attractive. Over standard polynomial rings the algebraic structure of λ-constacyclic codes of length n is totally determined by the polynomial divisors of the binomial $x^n - \lambda$. The construction of constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = u$, together with a Gray map and their $\mathbb{Z}_4$-images was investigated in [22]. One of the extensions of $\mathbb{Z}_4$ of order 16 is the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$ with $u^2 = 1$. Codes

over this ring have been studied recently [46], [54], [61], [7]. This ring can be written as $\mathbb{Z}_4[u]/\langle u^2-1\rangle$ and it is isomorphic to $\mathbb{Z}_4[u]/\langle u^2+2u\rangle$ by the map $u \to u+1$. Codes over $\mathbb{Z}_4[u]/\langle u^2+2u\rangle$ were studied in [41]. The ring $\mathbb{Z}_4[u]/\langle u^2+2u\rangle$ is one of the four Frobenius local non-chain rings of characteristic 4 [40]. It was shown that there exists a duality-preserving map for codes over $\mathbb{Z}_4[u]/\langle u^2+2u\rangle$ to codes over $\mathbb{Z}_4$, whereas no such map exists for codes over $\mathbb{Z}_4[u]/\langle u^2\rangle$, which is another Frobenius local non-chain ring of characteristic 4. The other generalization of the constacyclic codes which is mentioned in our thesis is quasi-twisted (QT) codes which was first studied in [12], [19], [52], that contain the class of quasi-cyclic (QC) codes as a special case. They have been shown to be promising in addressing one of the most important problems in coding theory, namely the construction of codes with best possible parameters.
Linear Complementary Pair (LCP) of codes and Linear Complementary Dual (LCD) has drawn much attention recently due to their applications to cryptography, in the context of side channel and fault injection attacks. These codes offer valuable solutions for error detection, correction, and data compression. In the realm of cryptography, LCD and LCP codes can be employed to enhance the security of cryptographic systems. By incorporating these codes as part of the encryption process, additional layers of protection can be added to safeguard against potential vulnerabilities.

This thesis is organized as follows:

Chapter 1 aims to give a brief introduction about the research topics of the thesis

In **Chapter 2**, we give a brief introduction with elementary definitions and properties of rings and finite fields, also we will introduce modules and submodules, and we consider some basic theory about linear codes over finite fields and over rings, in particular, we give some structural properties of cylic and QC codes over the Galois ring $\mathbb{Z}_q$ and some basic definitions of computer algebra system.

In **Chapter 3**, we give some results on the linear codes over the ring $R=\mathbb{Z}_q+v\mathbb{Z}_q$ with $v^2=1$, $q=p^m$ for a prime p and a positive integer m. We give the algebraic structure of the ring R, define a suitable inner product to derive the dual codes and obtain the systematic form of their respective generator matrix, we investigate the algebraic structures and properties of constacyclic codes over the ring R and gave a direct sum decomposition of a λ-constacyclic code C over R. After that we give the standard generator of a free constacyclic code over R and finally, we show that the image of a constacyclic code over R under a natural Gray map is a QT code of index 2 over $\mathbb{Z}_q$.

In **Chapter 4**, we mainly focus on QT codes since QT codes include cyclic codes, quasi-cyclic codes and constacyclic codes as special cases. We decompose a QT code to a direct sum of component codes – linear codes over rings, it is shown that the dual of a QT code is a QT code of the same length and index. By decomposing R into a product of local rings, we show that the polynomial $x^s - \lambda$ factors into pairwise coprime monic irreducible polynomials over R, and finally, we use the Gray images of QT codes over this ring where $q = 4$, we obtain some new linear codes over $\mathbb{Z}_4$.

In **Chapter 5**, we consider linear complementary pair (LCP) codes (C, D), as a generalization of LCD (linear complementary dual) codes, we give a necessary and sufficient condition on the existence of LCD codes over R. We present a characterization of constacyclic LCP of codes over R. In particular, for any pair (C, D) of constacyclic LCP codes, we prove that C and $D^{\perp}$ are equivalent. Hence, finding best λ-constacyclic LCP codes (C, D) and finding best λ-constacyclic codes.

Chapter 1

Preliminaries

1 Introduction

In coding theory, a linear code is an error-correcting code for which any linear combination of codewords is also a codeword. In this section, we give some basics definitions and properties of linear codes over finite fields and rings.

Definition 1.1. Let A be an alphabet (often we consider finite fields) and let $\mathcal{A}$ be the set of vectors formed from A. A code C is a subset of vectors of $\mathcal{A}$. An element of C is called a codeword.

2 Coding Theory

2.1 Linear Codes over Finite Fields

In order to simplify the encoding and decoding methods, if we impose an additional structure to a code, then we may have many practical advantages. The most popular block codes are linear, this means that the component-wise sum of two codewords is again a codeword.
By choosing our alphabet to be $\mathbb{F}_q$, we see that all words of length n over $\mathbb{F}_q$ is the n-dimensional vector space over $\mathbb{F}_q$. We would like to take advantage of this vector space structure in order to perform vector space operations on our codewords. However, we need to ensure that the sum of any two codewords is a codeword and the scalar multiple of a codeword is also a codeword. This leads us to the following definition.

Definition 2.1. A code C of length n is said to be a linear code if it is a subspace of $\mathbb{F}_q$. If

C has dimension k over $\mathbb{F}_q$, we say that C is an $[n;k]$-code. Moreover, if C has minimum distance d, we say that C is an $[n;k;d]$-code. Notice that our code C must contain the codeword containing all zeros. We will call this codeword the zero codeword.

Example 2.1.

{0}

$\mathbb{F}_q^n$ are trivial linear codes.

In $\mathbb{F}_3^3$ the linear code generated by $(1,0,2)$ and $(1,1,2)$ on $\mathbb{F}_3$ is

$$C = \{000, 102, 112, 201, 221, 211, 020, 122, 010\}$$

The words of a linear code can be written in several ways depending on the choice of a code base. A base of a linear code is represented in matrix form.

2.2 Parameters of a Code

Let C be a linear code of dimension k and length n.

Definition 2.2. A generator matrix for C is a matrix, denoted as G, of size $k \times n$ with coefficients in $\mathbb{F}_q$, whose rows form a basis for C.

Proposition 1. *For any invertible matrix M of order k and with coefficients in $\mathbb{F}_q$, MG is a generating matrix of C, where G is the generator matrix of C.*

Example 2.2. Let $\mathcal{H}$ be the $[7,4]$-binary code defined by the following generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

This code is known as the Hamming code.

Definition 2.3. We can define over $\mathbb{F}_q^n$ a metric $d(.,.)$ called *Hamming distance*, given by:

$$d(x,y) = |\{i \mid 0 \leq i \leq n-1, x_i \neq y_i\}|.$$

Definition 2.4. The *Hamming weight* of a word x denoted by $w(x)$ is the number of non-zero coordinates of x, i.e.,

$$w(x) = d(x,0).$$

Definition 2.5. The *minimum distance* of a code $C \subset \mathbb{F}_q^n$ is given by:

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

Example 2.3. The triple binary repetition code $C = \{000, 111\}$ has minimum distance 3. The binary code of length n has minimum distance 2.

Definition 2.6. The *minimum weight* of a code C is :

$$w(C) = \min\{w(x) \mid x \in C, x \neq 0\}$$

Let C be an $[n,k]$ linear code over $\mathbb{F}_q$, then it is well known that there exists an $(n-k) \times n$ matrix $\mathbf{H}$, with entries in $\mathbb{F}_q$ and independent rows, such that C is the null space of $\mathbf{H}$, i.e., C is the set of all $\mathbf{c} \in \mathbb{F}_q^n$ such that $\mathbf{Hc}^t = 0$. The matrix $\mathbf{H}$ is called a *parity check matrix* of C.

Remark. For a linear code the minimum distance and the minimum weight are equals.

There is an important link between the capacity of correction of a linear codes and its minimum distance. It has been demonstrated (see [39]) that a linear code C of minimum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors and detect $d-1$ errors.

2.3 The Duality of Linear Codes

Each linear code C can be associated with a linear code given by the following definition.

Definition 2.7. (The Euclidean Dual) *Let $C \subset \mathbb{F}_q^n$ be a linear code of dimension k and the size of C is q^k. The Euclidean dual code or simply, dual code of C is the orthogonal of C for the usual inner product defined over $\mathbb{F}_q^n \times \mathbb{F}_q^n$ by*

$$\langle x.y \rangle = \sum_{i=1}^{n} x_i y_i,$$

where $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$. This code is denoted $C^\perp$ and it is defined by

$$C^\perp = \{x \in \mathbb{F}_q^n \mid \langle x, y \rangle = 0, \forall y \in C\}.$$

Lemma 2.1. Let $\mathcal{C}$ be a code of length n over $\mathbb{F}$. Then

- $C^{\perp}$ is a linear code over $\mathbb{F}$.
- If C is an $[n,k]$-linear code, then $\left|C^{\perp}\right| \cdot |C| = |\mathbb{F}|^{n}$.

The dual code $C^{\perp}$ is a linear code of dimension $k^{\perp} = n - k$. Its generator matrix $\mathbf{H}$ is called the *parity check matrix* of C, because it satisfies:

$$C = \{x \in \mathbb{F}_q^n \mid \mathbf{H}\mathbf{x}^{\mathbf{t}} = 0\}.$$

The minimum distance of $C^{\perp}$ is called dual distance and noted $d^{\perp}$.

If we consider codes on $\mathbb{F}_{q^2}$, then we can consider the Hermitian inner product.

Definition 2.8. (The Hermitian dual) The *Hermitian dual* code is defined by:

$$C^{\perp h} = \{x \in \mathbb{F}_{q^2}^n \mid \sum_{i=1}^{n} x_i y_i^q = 0, \forall y \in C\}.$$

Definition 2.9. (Self-Dual Codes)

A linear code is said to be *self-orthogonal in the Euclidean sense* if it satisfies $C \subset C^{\perp}$. It is said to be *self-dual in the Euclidean sense* if it satisfies $C = C^{\perp}$. In this case, C must be an $[n, n/2]$ code with n even. This property comes from the fact that for a linear code C we have:

$$\dim C + \dim C^{\perp} = n.$$

From the above, we deduce that a linear $[n,k]$ code is self-dual if and only if it is self-orthogonal with $k = n/2$.

A linear code is said to be *self-orthogonal in the Hermitian sense* if it satisfies $C \subset C^{\perp h}$. It is said to be *self-dual in the Hermitian sense* if it verifies $C = C^{\perp h}$.

3 Cyclic Codes

Definition 3.1. A linear code C of length n is cyclic if:

$$c = (c_0, c_1, \ldots, c_{n-1}) \in C, then (c_{n-1}, c_0.c_1, \ldots, c_{n-2}) \in C.$$

In the following, each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is conventionally recognized via

its polynomial form $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$.
We remember that since $\mathbb{F}_q[x]$ is principle ideal domain also the ring $R_n = \mathbb{F}_q[X]/\langle X^n - 1\rangle$ is a principal ideal hence the cyclic codes are principal ideals of R_n when writing a code word of a cyclic code as $c(x)$ we mean the coset $c(x) + \langle X^n - 1\rangle$ in R_n.

Theorem 3.1. A linear code C in $\mathbb{F}_q$ is cyclic if and only if C is an ideal in $R_n = \mathbb{F}_q[X]/\langle X^n - 1\rangle$.

Proof. If C is an ideal in $\mathbb{F}_q[X]/\langle X^n - 1\rangle$ and $c(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$ is any codeword, then $Xc(X)$ is also a codeword, i.e. $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. Conversely, if C is cyclic, then $c(X) \in C$ we have $Xc(X) \in C$. Therefore $X^ic(X) \in C$, and since C is linear, then $a(X)c(X) \in C$ for each polynomial $a(X)$. Hence C is an ideal of $\mathbb{F}_q[X]/\langle X^n - 1\rangle$. □

4 Linear Codes over Rings

Galois rings are a generalization of finite fields. Like the latter, they can be defined by a quotient ring structure of a polynomial ring. Many properties result directly from the fact that Galois rings are finite, commutative, unitary and local which means that the number of elements is finite, their product is commutative and admits a neutral element, and that there exists a unique maximal ideal. However, we prefer a more concrete approach and use their quotient ring structure of a polynomial ring to obtain their properties.

4.1 Some Basic Properties of $\mathbb{Z}_q$

Let $q = p^r$,where p is a prime and r a positive integer. In the rest of this section, we shall recall some basic properties of $\mathbb{Z}_q$ and its extensions, called Galois rings. These rings are a special case of finite commutative local rings.

Definition 4.1. A Galois ring is a ring of the form $\mathbb{Z}_{p^r}[x]/(P)$, where small p is a prime number, r a strictly positive integer and $P \in \mathbb{Z}_{p^r}[x]$ a B-polynome.

A commutative ring R with identity is called a local ring if it has a unique maximal ideal M. Then the residue class ring R/M is a field, called the residue field of R. Let R be a finite commutative local ring with identity and let $\overline{R}$ be the residue field of R. We use the notation $-$ for the natural projection of $R[x]$ onto $\overline{R}[x]$. Thus the image of $f(x) \in R[x]$ under the map $-$ is denoted by $\overline{f}(x)$ in $\overline{R}[x]$.

Definition 4.2. Let R be a finite commutative local ring with identity. A polynomial $f(x) \in R[x]$ is said to be a regular polynomial if $f(x)$ is not a zero divisor in $R[x]$.

Equivalently, $f(x) = f_0 + f_1x + \cdots + f_nx^n \in R[x]$ is regular if and only if f_i is a unit in R for some $i = 0, 1, \ldots, n$, if and only if, $\overline{f}(x) \neq 0$ in $\overline{R}[x]$.
A simple example of a finite commutative local ring with identity is $\mathbb{Z}_q$, $q = p^r$, p a prime and r a positive integer. The maximal ideal of $\mathbb{Z}_q$ is $\langle p \rangle = p\mathbb{Z}_q$ and the residue field is $\mathbb{Z}_q/\langle p \rangle = \mathbb{F}_p$, the prime field of characteristic p. The image of an element $a \in \mathbb{Z}_q$ in the residue field $\mathbb{F}_p$ is the element $\overline{a} = a(modp)$ of $\mathbb{F}_p$. Two polynomials $f(x)$ and $g(x)$ over R are said to be coprime if there exist polynomials $a(x), b(x)$ in $R[x]$ such that

$$a(x)f(x) + b(x)g(x) = 1.$$

It is to be noted that in $R[x]$ two coprime polynomials may have a common divisor of degree ≥ 1.

Example 4.1. Let $R = \mathbb{Z}_4$. Let $f(x) = 2x^3 + x^2 + 2x + 1$ and $g(x) = 2x^2 + x + 2$. Then $f(x)$ and $g(x)$ are coprime over $\mathbb{Z}_4$ as we have $f(x) + (-x)g(x) = 1$. Also we have $f(x) = (x^2 + 1)(2x + 1)$ and $g(x) = (x + 2)(2x + 1)$. Therefore, $2x + 1$ is a common divisor of $f(x)$ and $g(x)$. We further note that the polynomial $2x + 1$ is a unit in $\mathbb{Z}_4$ since $(2x + 1)^2 = 1(\mathrm{mod} 4)$.

Definition 4.3. Let R be a finite commutative local ring with identity. A polynomial $f(x) \in R[x]$ is said to be basic irreducible if $\bar{f}(x)$ is irreducible in $\bar{R}[x]$, and basic primitive if $\bar{f}(x)$ is a primitive polynomial in $\bar{R}[x]$.

Definition 4.4. If $f(x) \in \mathbb{Z}_q[x]$ is a monic basic irreducible polynomial of degree m, then the Galois ring of degree m over $\mathbb{Z}_q$ is the residue class ring $GR(q, m) = \frac{\mathbb{Z}_q[x]}{\langle f(x) \rangle}$.

The Galois ring $GR(q, m)$ is a ring of characteristic $q = p^r$ and cardinality q^m. We have $GR(q, 1) = \mathbb{Z}_q$ and $GR(p, m) = \mathbb{F}_{p^m}$, the finite field of characteristic p with p^m elements. The Galois ring $GR(q, m)$ is a local ring with the maximal ideal $\langle p \rangle = pGR(q, m)$ and the residue field $GR(q, m)/pGR(q, m) = \mathbb{F}_{p^m}$.

To understand the structure of cyclic codes of length n over $\mathbb{Z}_q$, we often require divisors of $x^n - 1$ over $\mathbb{Z}_q$.

Theorem 4.1. [12] Let $q = p^r$, where p is a prime and r a positive integer, and $(n, q) = 1$. Let $g(x) \in Z_p[x]$ be a monic divisor of $x^n - 1$ over $\mathbb{Z}_p$. Then there exists a unique monic polynomial $f(x)$ in $\mathbb{Z}_q[x]$ such that $\overline{f}(x) = g(x)$ and $f(x)|(x^n - 1)$ in $\mathbb{Z}_q[x]$.

The monic polynomial $f(x)$ in Theorem 4.1 is called the Hensel lift to $\mathbb{Z}_q$ of the polynomial $g(x)$.

4.2 Linear Codes over $\mathbb{Z}_q$

Let C be a linear code on the Galois ring $\mathbb{Z}_q$ of length n, where q is a power of a prime number p.

Definition 4.5. A linear codes of length n over $\mathbb{Z}_q$ is a submodule of $\mathbb{Z}_q^n$. The generator matrix of a linear code on $\mathbb{Z}_q$ is any matrix of $\mathcal{M}(\mathbb{Z}_q)$ whose lines form a minimal generator family of code.

Theorem 4.2. [58] Let C_{p^r} be a linear code over $\mathbb{Z}_{p^r}$, with a permutation of coordinates, C_{p^r} admits a generator matrix of normal form:

$$G = \begin{pmatrix} \mathrm{I}_{\ell_0} & \mathrm{A}_{0,1} & \multicolumn{2}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} & \mathrm{A}_{0,k} \\ 0 & p \cdot \mathrm{I}_{\ell_1} & p \cdot \mathrm{A}_{1,2} & \dots\dots\dots & p \cdot \mathrm{A}_{1,k} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & p^{k-1} \cdot \mathrm{I}_{\ell_{k-1}} & p^{k-1} \cdot \mathrm{A}_{k-1,k} \end{pmatrix}$$

where $\mathrm{A}_{i,j}$ are matrices $\ell_i \times \ell_j$ with coefficients in $\{0, \dots, p-1\} \subset Z_{p^r}$ et I_{ℓ_i} is the identity matrix of size ℓ_i. In particular, the code $\mathbf{C}_{p^r}$ a $\prod_{=0}^{-1} p^{(r-i)\ell_i}$ elements.

Definition 4.6. (Dual code over $\mathbb{Z}_{p^r}$) Let C_{p^r} be a linear code over $\mathbb{Z}_{p^r}$, the dual code of C_{p^r} is $C_{p^r}^{\perp}$, defined by:

$$\mathbf{C}_{\mathbf{p}^r}^{\perp} = \left\{ \mathbf{a} \mid \forall \mathbf{b} \in \mathbf{C}_{\mathbf{p}^r}, \quad \mathbf{a} \cdot \mathbf{b} = 0 \right\}.$$

When the generating matrix of the $\mathbf{C}_{\mathrm{p}^r}$ is in normal form, the generating matrix of the dual code takes the form:

$$G^{\perp} = \begin{pmatrix} \mathrm{B}_{0,0} & \multicolumn{2}{c}{\dots\dots\dots\dots\dots\dots\dots\dots} & \mathrm{B}_{0,k-1} & \mathrm{I}_{\ell_k} \\ p \cdot \mathrm{B}_{1,0} & \dots\dots\dots & p \cdot \mathrm{B}_{1,k-2} & p \cdot \mathrm{I}_{\ell_{k-1}} & 0 \\ \vdots & \iddots & \iddots & \iddots & \vdots \\ p^{k-1} \cdot \mathrm{B}_{k-1,0} & p^{k-1} \cdot \mathrm{I}_{\ell_1} & 0 & \dots\dots & 0 \end{pmatrix}$$

where $B_{i,j}$ are matrices $\ell_{r-i} \times \ell_j$ with coefficients in $\{0, \ldots, p-1\} \subset Z_{p^r}$.

4.3 Weights and Distances on the Ring $\mathbb{Z}_{p^r}$

Associate with the vector $x = (x_1, x_2, \ldots x_n)$ different weights and distances other than the Hamming weight and distance. We have already defined the Hamming weight $w_{Ham}(x)$ as the number of non-zero components of x.

Euclidean weight:

$$w_E(x) = \sum_{i=1}^{n} \min \left\{ x_i^2, \left(q - x_i^2\right) \right\}.$$

Lee weight:

$$w_{\text{Lee}}\,(x) = \sum_{i=1}^{n} \min \left\{ |x_i|, |(q - x_i)| \right\}.$$

Similarly for the distance, we define these three distances.

Hamming distance

$$d_{Ham}(x, y) = w_{Ham}(x - y).$$

Lee Distance:

$$d_{Lee}(x, y) = w_{Lee}(x - y).$$

Euclidian Distance

$$d_E(x, y) = w_E(x - y).$$

Homogeneous distance

$$d_{Hom}(x, y) = w_{Hom}(x - y).$$

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

Binary codes are obtained from codes over $\mathbb{Z}_4$ by the Gray map

$$\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$$

$$\phi(0) = (0, 0),$$

$$\phi(1) = (0, 1),$$

$$\phi(2) = (1, 1),$$

and

$$\phi(3) = (1, 0).$$

This map is then extended componentwise from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ and ϕ is a distance preserving map from $\mathbb{Z}_4^n$ with Lee distance to $\mathbb{Z}_2^{2n}$ with Hamming distance.

Remark. The structure of the Gray map for the general case of q is not as well understood; it is not even uniquely defined and there are different interpretations on the right generalization. As we are studying codes over $\mathbb{Z}_q$, we prefer the usual Hamming distance.

5 Hensel Lifting

We present the Hensel lifting, which allows obtaining (lifting) a factorization of a polynomial in the ring $\mathbb{Z}_{p^r}$ under certain conditions, based on a factorization in $\mathbb{Z}_p$. This will serve us in two different contexts: firstly, it enables an effective construction of Galois rings, and secondly, Hensel's lifting will be a technique for constructing cyclic codes over $\mathbb{Z}_{p^r}$. We illustrate the lifting function by calculation algorithm in the case of $p = 2$.

Lemma 5.1. [43] (Hensel lemma) Let p be a prime number, r an integer greater than or equal to 2, and $P \in \mathbb{Z}_{p^r}[x]$ be a unitary polynomial such that:

$$P \equiv QR(modP),$$

for $Q, R \in \mathbb{Z}_p$ are coprime, then there is a unique pair $(Q^{(r)}, R^{(r)})$ unitary polynomial of $\mathbb{Z}_{p^r}$, such that

1. $P = Q^{(r)}R^{(r)}$,
2. $Q^{(r)} \equiv Q(modp)$ and $R^{(r)} \equiv R(modp)$,
3. $Q^{(r)}$ and $R^{(r)}$ are coprime,

and we have deg $(Q^{(r)})$= deg (Q) and deg $(R^{(r)})$= deg (R).

The ring $\mathbb{Z}_p[x]$ being factorial, so any polynomial with coefficient in $\mathbb{Z}_p$ uniquely decomposes into product of irreducibles factors. We have for any polynomial $P \in \mathbb{Z}_{p^r}[x]$

$$P \equiv f_1^{e_1} \dots f_l^{e_l} (modp),$$

where $f_1, \dots, f_l$ are irreductible poynomials of $\mathbb{Z}_p[x]$ and $e_1, \dots, e_l$ strictly positive integers. From its factorization in $\mathbb{Z}_p[X]$. It is thus possible to obtain a factorization of any polynomial in $\mathbb{Z}_{p^r}[x]$ based on its factorization in $\mathbb{Z}_p[x]$.

Theorem 5.2. [43] Let p be a prime number, r an integer greater than or equal to 2 and $P \in \mathbb{Z}_{p^r}[X]$ a monic polynomial. Let $P \bmod p = f_1^{e_1} \dots f_l^{e_l}$ the factorisation of P in $\mathbb{Z}_p[X]$ where $f_1, \dots, f_l$ are irreducible polynomials and $e_1, \dots, e_l$ strictly positive integers. There is a unique l-uplet $(g_1^{(r)}, \dots, g_l^{(r)})$ of unitary polynomials of $\mathbb{Z}_{p^r}[X]$ such that:

1. $P = g_1^{(r)} \dots g_l^{(r)}$
2. $g_i^{(r)} \equiv f_i^{e_i} (mod p)$.
3. The $g_i^{(r)}$ are pairwise coprime.

In other words, the unitary polynomials of $\mathbb{Z}_{p^r}[X]$ can be uniquely decomposed into products of polynomials of the type $g_i^{(r)}$. Reduced modulo p, they are powers of an irreducible polynomial. This property will allow us to define the Hensel lift by a factor of $Xn - 1$, where n is coprime with p. In this case, $X^n - 1$ includes only simple factors.

Definition 5.1. (Hensel lift) Let Q and R be two polynomials with coefficients in $\mathbb{Z}_p$ such that $X^n - 1 = Q(x)R(x)$, where n is coprime with p. We call Hensel lift of order r of the polynomial Q is the polynomial $Q^{(r)}$ for $(Q^{(r)}, R^{(r)})$.

5.1 Cyclic Codes over $\mathbb{Z}_q$

Definition 5.2. A linear code C of length n over $\mathbb{Z}_q$ is a $\mathbb{Z}_q$-submodule of $\mathbb{Z}_q^n$ and the elements of C are called codewords. We define the cyclic shift on Z_q^n as:

$$\rho(c_0, c_1, \dots, c_{n-1}) = (c_{n-1}, c_0.c_1, \dots, c_{n-2}).$$

A linear code C is called a cyclic code if $\rho(C) = C$. Each codeword $c = (c_0, c_1, \dots, c_{n-1})$ is conventionally recognized via its polynomial form $c(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$, and the code C is identified with the collection of all polynomial forms of its codewords. Then, ρ is the cyclic shift of $c(x)$ in the quotient ring $\frac{R[x]}{\langle x^n - 1 \rangle}$.

In this section, we briefly discuss cyclic codes over the Galois ring $\mathcal{R} = GR(q, l)$. As usual, a cyclic code of length n over $\mathcal{R}$ is an ideal of $\frac{\mathcal{R}[x]}{\langle x^n - 1 \rangle}$. We assume $(n, q) = 1$, then $x^n - 1$ factorizes uniquely into monic pairwise coprime basic irreducible polynomials over$\mathbb{Z}_q$ [58]. Also, in this case it is known that $\frac{\mathcal{R}[x]}{\langle x^n - 1 \rangle}$ is a principal ideal ring [58], and a cyclic code of length n over $\mathcal{R}[x]$ is a principal ideal of $\frac{\mathcal{R}[x]}{\langle x^n - 1 \rangle}$ generated by a polynomial:

$$g(x) = h_0 + ph_1 + \cdots + p^{r-1} h_{r-1},$$

where $h_0, h_1, \ldots, h_{r-1}$ are monic polynomials in $\mathcal{R}[x]$ satisfying:

$$h_{r-1}|h_{r-2}|\ldots|h_0|(x^n-1).$$

Let C be a cyclic code of length n over $\mathcal{R}$ generated by a polynomial $g(x)$. Unlike the finite field case, $g(x)$ does not necessarily divide x^n-1 over $\mathcal{R}$ [57]. It is related to whether C is a free $\mathcal{R}$-module or not. We first require the following lemma.

Lemma 5.3. [58] Let C be a free cyclic code of length n over $\mathcal{R}$. Then there exists a monic polynomial over $\mathcal{R}$ generating C.

If the generating polynomial of $g(x)$ of a cyclic code C of length n over $\mathcal{R}$ divides x^n-1, then we have the following result, which is an immediate extension of a similar result for cyclic codes over $\mathbb{Z}_4$ given in [8].

Proposition 2. *[12] A non-zero cyclic code C of length n over $\mathcal{R}$ is a free module over $\mathcal{R}$ if and only if it is generated by a monic polynomial $g(x)$ dividing x^n-1 over $\mathcal{R}$. Further, if C is free, then C has rank $n-deg\ g(x)$ and the elements $g(x), xg(x), \ldots, x^{n-deg\ g(x)-1}g(x)$ form a basis for C.*

The monic polynomial $g(x)$ in the above Proposition which generates the free cyclic code C is called the generator polynomial of C.

5.2 Quasi Cyclic Codes over $\mathbb{Z}_q$

Definition 5.3. Let T be the standard cyclic shift operator. A linear code C of length n over R is said to be a quasi-cyclic (QC) code if it is invariant under T^l for some positive integer l, i.e., if $T^l(C)=C$. The smallest positive integer l such that $T^l(C)=C$ is called the index of C; in this case l is a divisor of n. For $l=1$, C is simply a cyclic code over R. A QC code of index l is also called an l-QC code.

A quasi-cyclic (QC) code C of length lm and index l over $\mathbb{Z}_q$ is a $\mathbb{Z}_q$-submodule of $\mathbb{Z}_q^{lm}$ invariant under T^l. It is well known that C can be regarded a $\frac{\mathbb{Z}_q}{\langle x^m-1\rangle}$-submodule of $\frac{(\mathbb{Z}_q}{\langle x^m-1\rangle)^l}$ [8]. This definition of QC codes is known as the conventional row circulant definition. We also use a different representation of QC codes over $\mathbb{Z}_q$, which goes as follows. Let $v=(v_{00}, v_{01}, \ldots, v_{0,l-1}, \ldots, v_{m-1,0}, v_{m-1,1}, \ldots, v_{m-1,l-1})$ be an element of $\mathbb{Z}_q^{lm}$. We define an isomorphism between $\mathbb{Z}_q^{lm}$ and $GR(q,l)^m$ by associating with each l-tuple $(v_{i0}, v_{i1}, \ldots, v_{i,l-1}) \in \mathbb{Z}_q^l, 0 \leq i \leq m-1$, the element:

$$v_i = v_{i0} + v_{i1}\xi +, \ldots, +v_{i,l-1}\xi^{l-1} \in GR(q,l),$$

where $\{1, \xi, \xi^2, \ldots, \xi^{l-1}\}$ is a fixed basis of $GR(q,l)$ over $\mathbb{Z}_q$ with ξ being a root of a monic basic irreducible polynomial of degree l over $\mathbb{Z}_q$. Then for every element $(v_{00}, v_{01}, v_{0,l-1}, \ldots, v_{m-1,0}, v_{m-1,1}, \ldots, v_{m-1,l-1})$ of $\mathbb{Z}_q^{lm}$, there is a corresponding element $(v_0, v_1, \ldots, v_{m-1})$ in $GR(q,l)^m$ and vice-versa. Under this isomorphism, $T^l(v)$ for some $v = (v_{00}, v_{01}, v_{0,l-1}, \ldots, v_{m-1,0}, v_{m-1,1}, \ldots, v_{m-1,l-1}) \in \mathbb{Z}_q^{lm}$ corresponds to the element $(v_{m-1}, v_0, \ldots, v_{m-2}) \in GR(q,l)^m$. We fix the notation $\mathcal{R}$ for the Galois ring $GR(q,l)$. Using the natural isomorphism between $\mathcal{R}^m$ and the residue class ring $\frac{\mathcal{R}}{\langle x^m-1\rangle}$, an element $(v_0, v_1, \ldots, v_{m-1}) \in \mathcal{R}^m$ can be represented by the element

$$v_0 + v_1 x + \cdots + v_{m-1}x^{m-1} + \langle x^m - 1\rangle,$$

in $\frac{\mathcal{R}}{x^m-1}$. For convenience, we simply write $v_0 + v_1 x + \cdots + v_{m-1}x^{m-1}$ for the residue class $v_0 + v_1 x + \cdots + v_{m-1}x^{m-1} + \langle x^m - 1\rangle$. In this setting, multiplication by x to any element of $\frac{\mathcal{R}}{\langle x^m-1\rangle}$ is equivalent to applying T^l on the corresponding element of $\mathbb{Z}_q^{lm}$. Now let C be a QC code of length lm and index l over $\mathbb{Z}_q$. Then by the equivalence shown above between $\mathbb{Z}_q^{lm}$ and $\frac{\mathcal{R}}{\langle x^m-1\rangle}$, C is a $\mathbb{Z}_q$-submodule of $\frac{\mathcal{R}}{\langle x^m-1\rangle}$. As C is a QC code of index l, for any $c(x) \in C$, $xc(x) mod(x^m - 1)$ is also in C. By linearity $a(x)c(x) \in C$ for all a(x) $\in \frac{\mathbb{Z}_q}{\langle x^n-1\rangle}$-submodule of $\frac{\mathcal{R}}{\langle x^m-1\rangle}$.

If a QC code C of length lm and index l over $\mathbb{Z}_q$ is generated by the elements $v_0(x)$, $v_1(x) \cdots v_t(x) \in \frac{\mathcal{R}[x]}{\langle x^m-1\rangle}$ as a $\frac{\mathbb{Z}_q}{\langle x^m-1\rangle}$-submodule of $\frac{\mathcal{R}}{\langle x^m-1\rangle}$, then

$$\mathcal{C} = \{a_1(x)v_1(x) + a_2(x)v_2(x) + \cdots + a_t(x)v_t(x) \mid \\ a_i(x) \in \frac{\mathbb{Z}_q[x]}{\langle x^m - 1\rangle}, i = 1, 2, \ldots, t\Big\}.$$

$\mathcal{C}$ is also a $\mathbb{Z}_q$-submodule of $\frac{\mathcal{R}[x]}{\langle x^m-1\rangle}$. As a $\mathbb{Z}_q$-submodule of $\frac{\mathcal{R}[x]}{\langle x^m-1\rangle}$, $\mathcal{C}$ is generated by the set:

$$\{v_1(x), xv_1(x), \ldots, x^{m-1}v_1(x), \ldots, \\ v_t(x), xv_t(x), \ldots, x^{m-1}v_t(x)\}.$$

If $\mathcal{C}$ is generated by a single element $v_0(x), v_1(x), \ldots, v_t(x) \in \frac{\mathcal{R}[x]}{\langle x^m-1\rangle}$, as a $\frac{\mathbb{Z}_q[x]}{\langle x^m-1\rangle}$-submodule of $\frac{\mathcal{R}[x]}{\langle x^m-1\rangle}$, then we say that $\mathcal{C}$ is a 1 -generator QC code.

6 Bounds on Codes

Several theorems on the existence and non-existence of bounds are known, but the exact bound is, in fact, still an open problem. We have introduced certain parameters

of a linear code in this section. In coding theory, one of the most fundamental problems is to find the optimal value of a parameter when other parameters have been given. In this section, we discuss some bounds on code parameters.
In the following bound, we provide the minimum and maximum distance of a code with a given length and dimension. This bound is called the Singleton bound.

Theorem 6.1. [47] Let C an $[n,k,d]_q$ code, then

$$d \leq n-k+1.$$

Theorem 6.2. [47](Griesmer Bound)
If C is an $[n,k,d]_d$ code with $k>0$, then

$$n \geq \sum_{i=0}^{i=k-1} \left\lceil \frac{d}{q^i} \right\rceil .$$

Since $\lceil d/q^0 \rceil = d$ and $\lceil d/q^i \rceil \geq 1$ for $i \in [k-1]$, then the Griesmer bound implies the Singleton bound.

Another important bound on the parameters that resolves one of the most significant problems in coding theory is whether there exists an $[n,k,d]$ code over $\mathbb{F}_q$ for given n,k and d.
The following theorem called the Hamming bound gives the answer.

Theorem 6.3. [47] For integers n,k,d there exists a $[n,k,d]$ code over $\mathbb{F}_q$ when :

$$q^k \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \left(\begin{array}{c} n \\ i \end{array} \right) (q-1)^i \leq q^n.$$

7 Computer Algebra System

The software packages *Maple* and *Magma* have been used in teaching and research in many universities throughout the world. They can be used for the construction of linear and non-linear codes. It is important to assess the relative merits of the two packages for the construction of codes.

Magma is a computer algebra system designed to deal with a wide variety of problems in algebra, number theory, geometry and combinatorics. It is produced and distributed by the *computational algebra group* within the school of Mathematics and statistics of the university of sydney. In June 1996 *Magma Version 2.0* was released and after that a new version of Magma has been released approximately once per year. *Magma* contains many of the most advanced and efficient known algorithms for the areas which it covers, such as, groups, rings, fields, algebras, vector spaces, algebraic geometries, lattices, graphs, combinatorics and codes. It has facilities provided for linear codes over fields $\mathbb{F}_q$, including codes constructed in terms of generator matrices, parity check matrices and generating polynomials. This facility will be used later to construct linear codes. In addition, a large number of constructions for particular families of codes, (e.g. quadratic residue codes) are available. There are also algorithms for the calculation of the minimum weight and weight enumerator, including the MacWilliams transform. For more details refer to [55].

Furthermore, the two software packages *Maple* and *Magma* have been applied to construct several classes of $[n, k, d]$ binary linear codes such as Hamming codes, cyclic codes. In fact *Magma* has many built-in facilities which aid the construction of linear codes. It is shown that *Magma* software is very much more convenient for the construction of linear codes, and makes the construction of $[n, k, d]$ binary linear codes much easier than *Maple*, saving both time and effort in developing the software. In terms of computation time, *Magma* appears generally to be faster than *Maple*.

Chapter 2

Constacyclic Codes over $\mathbb{Z}_q+v\mathbb{Z}_q$

In this chapter, we remind algebraic structure of the ring R and we present some basic results on linear codes and constacyclic codes over the ring $R = \mathbb{Z}_q + v\mathbb{Z}_q$, we recall the structure of the linear codes over the ring R. The results of this chapter can be found in [11].

Definition 0.1. Let R be a finite ring, a linear code C of length n on R is a submodule of the R-module of R^n, which can be free or not. The vectors of C are called the words of the code C.
We give R^n the following product :

$$v.w = \sum v_i w_i.$$

The dual code $C^{\perp}$ is defined by:

$$C^{\perp} = \{v \in R^n | v.w = 0, \forall w \in C\}.$$

If $C \subset C^{\perp}$, we say that the code C is self-orthogonal.

1 Algebraic Structure of the Ring R

The ring $R = \mathbb{Z}_q[v]/\langle v^2 - 1\rangle$ such that $v^2 = 1$ and $q = p^m$ for a prime p and a positive integer m. This ring is commutative, semi-local and non-chain principal ideal. It has two maximal ideals $\langle \alpha \rangle$ and $\langle \alpha^* \rangle$, where $\alpha = a + bv$ is an element of R and $\alpha^* = a - bv$, which is called as the conjugate of the element α. The ideal lattice of R is given in Figure 2.1.

$$\begin{tikzcd}
 & R = \mathbb{Z}_q[v]/\langle v^2-1\rangle \arrow[dl] \arrow[dr] & \\
\langle \alpha^* = a - bv\rangle \arrow[dr] & & \langle \alpha^* = a - bv\rangle \arrow[dl] \\
 & \langle 0\rangle &
\end{tikzcd}$$

Figure 2.1: The ideal lattice of the ring $R = \mathbb{Z}_q[v]/\langle v^2-1\rangle$

Each element x of R can be expressed uniquely as:

$$x = a + vb,$$

where $a, b \in \mathbb{Z}_q, i = 1, 2$.

Recall that $R = \mathbb{Z}_q + v\mathbb{Z}_q$ where $v^2 = 1$. Any $r \in R$ is of the form $r = a + vb = \epsilon_1\hat{a} + \epsilon_2\hat{b}$, where $a, b, \hat{a}, \hat{b} \in \mathbb{Z}_q$ and $\hat{a} = (a-b), \hat{b} = (a+b), \epsilon_1 = \frac{1-v}{2}$, and $\epsilon_2 = \frac{1+v}{2}$. It is easy to check that $\epsilon_i^2 = \epsilon_i, \epsilon_i\epsilon_j = 0$ and $\epsilon_1 + \epsilon_2 = 1$ for $i = 1, 2$ and $i \neq j$. Therefore, $R = \epsilon_1\mathbb{Z}_q \oplus \epsilon_2\mathbb{Z}_q$ and any $r \in R$ can be expressed as $r = \epsilon_1 r_1 + \epsilon_2 r_2$ where $r_1, r_2 \in \mathbb{Z}_q$.

Lemma 1.1. Let R^* denote the group of units of R then $R^* = \epsilon_1\mathbb{Z}_q^* \oplus \epsilon_2\mathbb{Z}_q^*$.

Definition 1.1. A subset C of R^n is a linear code over R if C is an R-submodule. For any codeword c $= (a_0, a_1, \ldots, a_{n-1}) \in R^n$ we can identified by polynomial such that:

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

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

$$R_n := R[X]/\left\langle X^n - \lambda\right\rangle.$$

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

$$c(X) \cdot r(X) \bmod \left(X^n - \lambda\right).$$

2 Gray Map over R

The Gray map is defined as follows:

$$\begin{aligned}\Phi : \mathbb{Z}_{p^m} + v\mathbb{Z}_{p^m} &\longrightarrow \mathbb{Z}_{p^m}^2\\ a + bv &\longmapsto (a, a+b)\end{aligned}$$

This map is naturally extended to $\left(\mathbb{Z}_{p^m} + v\mathbb{Z}_{p^m}\right)^n$, the Gray map Φ is a weight preserving map from $\left(R_{p^m}^n\right.$; Lee weight) to $\left(\mathbb{Z}_{p^m}^{2n}\right.$; Hamming weight) it is an isometry from $R_{p^m}^n$ to $\mathbb{Z}_{p^m}^{2n}$. The Hamming weight $w_H(c)$ of a codeword c is the number of nonzero components in c. For a linear C code of length n over R, define

$$\begin{aligned}C_1 = \{r_1 \in \mathbb{Z}_q^n : \epsilon_1 r_1 + \epsilon_2 r_2 \in C, \text{ for some } r_2 \in \mathbb{Z}_q^n\},\\ C_2 = \{r_2 \in \mathbb{Z}_q^n : \epsilon_1 r_1 + \epsilon_2 r_2 \in C, \text{ for some } r_1 \in \mathbb{Z}_q^n\}.\end{aligned}$$

It is clear that C_1 and C_2 are linear codes of length n over $\mathbb{Z}_q$. Let C_1 and C_2 be two linear codes. Then the operations $\oplus$ and $\otimes$ are defined as follows:

$$\begin{aligned}C_1 \oplus C_2 = \{(c_1 + c_2) : c_1 \in C_1, c_2 \in C_2\},\\ C_1 \otimes C_2 = \{(c_1, c_2) : c_1 \in C_1, c_2 \in C_2\}.\end{aligned}$$

Theorem 2.1. Let C be a linear code of length n over $\mathbb{Z}_q + v\mathbb{Z}_q$. Then $\Phi(C) = C_1 \otimes C_2$, and $|C| = |C_1||C_2|$.

Proof. For any,$(r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n) \in \Phi(C)$, let $c_i = (r_i + q_i) + (q_i - r_i)\, v, i = 1, 2, \ldots, n$. Since Φ is a bijection, $c = (c_1, c_2, \ldots, c_n) \in C$. By the definitions of C_1 and C_2, we obtain that $(r_1, r_2, \ldots, r_n) \in C_1, (q_1, q_2, \ldots, q_n) \in C_2$, therefore, $(r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n) \in C_1 \otimes C_2$. This implies that $\Phi(C) \subseteq C_1 \otimes C_2$. On the other hand, for any $(r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n) \in C_1 \otimes C_2$, where $(r_1, r_2, \ldots, r_n) \in C_1, (q_1, q_2, \ldots, q_n) \in C_2$, there are $c = (c_1, c_2, \ldots, c_n) \in C$. such that $c_i = (r_i + q_i) + (q_i - r_i)\, v$ where $1 \leqslant i \leqslant n$. Since C is linear, we have $c = r + q + (q - r)v = (1 + v)q + (1 - v)r \in C$. It follows that $\Phi(C) = (r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n)$, which gives $C_1 \otimes C_2 \subseteq \Phi(C)$. Therefore $\Phi(C) = C_1 \otimes C_2$. □

3 Generator matrix

A generator matrix for the code C is a matrix that comprises rows capable of generating the code C. Let G_1 and G_2 be the generator matrix of C_1 and C_2 respectively, then

$$\left[\begin{array}{c} (1-v)G_1 \\ (1+v)G_2 \end{array}\right],$$

is the generator matrix of the code C.

Proposition 3. *Let C be a linear code over $\mathbb{Z}_q+v\mathbb{Z}_q$. Then $d_L(C)=d_H(\Phi(C))=d_H(C_1\otimes C_2)=\min\{d_H(C_1),d_H(C_2)\}$.*

Proof. Because Φ is an weight-preserving map, then $d_L(C)=d_H(\Phi(C))=d_H\left(C_1\otimes C_2\right)=\min\left\{d\left(C_1\right),d\left(C_2\right)\right\}$, and $d_H=d_L$ is obvious. □

If we reduce the generator matrix of C then we obtain a matrix for the equivalent code of the form:

$$\left(\begin{array}{cccc} I_{k_1} & A & B & D_1+(1-v)D_2 \\ 0 & (1-v)I_{k_2} & 0 & (1-v)C_1 \\ 0 & 0 & (1+v)I_{k_3} & (1+v)E \end{array}\right),$$

where A,B,C,D_1,D_2,E are matrices with all entries in $\mathbb{Z}_{p^m}$. In this case we have $|C|=\left(p^{2m}\right)^{k_1}p^{mk_2}p^{mk_3}$.

4 Dual Codes of Linear Codes over R

The Euclidean inner product is given as $\langle x,y\rangle_E=\sum_{i=1}^n x_iy_i$. The dual code $C^\perp$ of C with respect to the Euclidean inner product is defined as follows:

$$C^\perp=\left\{x\in\left(\mathbb{Z}_q+v\mathbb{Z}_q\right)^n \mid \langle x,y\rangle_E=0 \text{ for all } y\in C\right\}.$$

The Hermitian inner product is given as $\langle x,y\rangle_H=\sum_{i=1}^n x_i\overline{y_i}$. The dual code $C^\perp$ of C with respect to the Hermitian inner product is defined as follows:

$$C^\perp=\left\{x\in\left(\mathbb{Z}_q+v\mathbb{Z}_q\right)^n \mid \langle x,y\rangle_H=0 \text{ for all } y\in C\right\}.$$

One of the important properties of the Gray map we defined is that it preserves the duality as illustrated in the following lemma:

Lemma 4.1. Let $C^{\perp}$ be the dual code of C then $\Phi\left(C^{\perp}\right)=\Phi(C)^{\perp}$. In particular, if C is self dual then so is $\Phi(C)$.

Proof. Let $c_1=r_1+vq_1, c_2=r_2+vq_2 \in \left(\mathbb{Z}_q+v\mathbb{Z}_q\right)^n$, where $r_1, q_1, r_2, q_2 \in \mathbb{Z}_q^n$ and $\langle c_1, c_2\rangle$ be the Euclidean inner product. If $\langle c_1, c_2\rangle=0$ in $\mathbb{Z}_q+v\mathbb{Z}_q$, then this means

$$\langle c_1, c_2\rangle=\left(r_1+vq_1\right)\left(r_2+vq_2\right)=r_1r_2+v\left(r_1q_2+q_1r_2+q_1q_2\right)=0,$$

which implies that $r_1r_2+q_1q_2=r_1q_2+q_1r_2=0$. Since, $\Phi\left(C_1\right)=\left(r_1, r_1+q_1\right), \Phi\left(C_2\right)=\left(r_2, r_2+q_2\right)$ we have $\left\langle\Phi\left(c_1\right), \Phi\left(c_2\right)\right\rangle=r_1r_2+r_1r_2+r_1q_2+q_1r_2+q_1q_2=0$. Thus $\Phi\left(C^{\perp}\right) \subseteq \Phi(C)^{\perp}$. Let $|C|=\left(p^{2t}\right)^{k_1} p^{tk_2} p^{tk_3}$ and C is of length n. Then $\Phi(C)$ has the parameters $[2n, 2k_1+k_2+k_3]$. Since $|\Phi(C)|=|C|$ then $\left|\Phi(C)^{\perp}\right|=p^{t(2n-(2k_1+k_2+k_3))}$.

Furthermore, $\left|\Phi\left(C^{\perp}\right)\right|=\left|C^{\perp}\right|=\left(p^{2t}\right)^n/|C|=\left(p^{2t}\right)^{n-(k_1+k_2+k_3)} p^{t(k_2+k_3)}=p^{t(2n-(2k_1+k_2+k_3))}$ therefore $\Phi\left(C^{\perp}\right)=\Phi(C)^{\perp}$. □

We can obtain the next commutative diagram over ring R.

$$\begin{tikzcd}
C \arrow[r] \arrow[d] & \Phi(C) \arrow[d] \\
C^{\perp} \arrow[r] & \Phi(C^{\perp})
\end{tikzcd}$$

Figure 2.2: Diagram Over Ring R

Theorem 4.2. Let C be a linear code of length n over $\mathbb{Z}_{p^m}+v\mathbb{Z}_{p^m}$ and let $\Phi(C)=C_1 \otimes C_2$. Then C can be uniquely expressed as $C=\epsilon_1C_1 \oplus \epsilon_2C_2$. Furthermore, $\Phi\left(C^{\perp}\right)=C_1^{\perp} \otimes C_2^{\perp}$, which then gives us $C^{\perp}=\epsilon_1C_1^{\perp} \oplus \epsilon_2C_2^{\perp}$.

Proof. By Lemma 4.1, $\Phi\left(C^{\perp}\right)=\left(C_1 \otimes C_2\right)^{\perp}$. Hence, we only need to prove that $\left(C_1 \otimes C_2\right)^{\perp}=C_1^{\perp} \otimes C_2^{\perp}$. Obviously, $C_1^{\perp} \otimes C_2^{\perp} \subseteq\left(C_1 \otimes C_2\right)^{\perp}$. On the other hand, suppose that C_1 and C_2 are $[n, k_1],[n, k_2]$ linear codes, respectively, then $C_1^{\perp}, C_2^{\perp}$ and $C_1 \otimes C_2$ are $[n, n-k_1],[n, n-k_2]$ and $[2n, k_1+k_2]$ linear codes, respectively, thus, $\left|C_1^{\perp} \otimes C_2^{\perp}\right|=\left|C_1^{\perp}\right|\left|C_2^{\perp}\right|=\left|\left(C_1 \otimes C_2\right)^{\perp}\right|=p^{t(2n-k_1-k_2)}$. Hence, $C_1^{\perp} \otimes C_2^{\perp}=\left(C_1 \otimes C_2\right)^{\perp}$.

□

5 Constacyclic Codes over R

5.1 Definition and Properties

We define the constacyclic shift on R^n as:

$$\rho_\lambda(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2}),$$

where λ is a unit in R. A linear code C is called constacyclic if $\rho_\lambda(C) = C$. As usual, we represent a vector $c = (c_0, c_1, \ldots, c_{n-1}) \in R^n$ as the corresponding polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ and the code C is identified with the codewords in polynomial form. Then, $\rho_\lambda(c)$ corresponds to $x \cdot c(x)$ in the quotient ring $\dfrac{R[x]}{\langle x^n - \lambda \rangle}$, and constacyclic codes are precisely the ideals of this ring.
Now we define a Gray map on R_q^n as follows:

$$\Psi : R^n \longrightarrow \mathbb{Z}_q^{2n}$$

$$\Psi(r_1 + vr_2) = (r_1, r_1 + r_2),$$

where $r_1, r_2 \in R^n$.
The Lee weight is defined as the Hamming weight of the Gray image

$$w_L(r) = w_H(r_1, r_1 + r_2).$$

The Lee distance between r and s is defined by:

$$d_L((r, s)) = w_L(r - s).$$

The minimum Lee distance between distinct pairs of code words of a code C is called the minimum distance of C and denoted by $d_L(C)$.

6 Generator Polynomials and Check Polynomials

We associate with the vector $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{Z}_q^n$ as the corresponding polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. Then a constacyclic code of length n over $\mathbb{Z}_q$ can be defined as an ideal in the ring of polynomials modulo $x^n - \lambda$ over $\mathbb{Z}_q$. Under this correspondence, a constacyclic code has the following properties.

Theorem 6.1. [39] Let C be a nonzero ideal in R, then

1. There is a unique monic polynomial $G(x)$ of minimal degree in C.
2. $C = \langle G(x) \rangle$, i.e., $G(x)$ is a generator polynomial generating of C.
3. $G(x)$ divides $x^n - \lambda$.
4. Any $c(x) \in C$ can be written uniquely as $c(x) = k(x)G(x)$ in $\mathbb{Z}_q[x]$, where $k(x) \in \mathbb{Z}_q[x]$ has degree $< n - \deg G(x)$. The dimension of C is $n - \deg G(x)$ Thus the message $k(x)$ becomes the codeword $k(x)G(x)$.
5. If $G(x) = G_0 + G_1 x + \cdots + G_b x^b$, then a generator matrix of C is

$$G = \begin{bmatrix} G_0 & G_1 & G_2 & \cdots & G_b & & 0 \\ & G_0 & G_1 & \cdots & G_{b-1} & G_b & \\ & & & \cdots & \cdots & & \\ & & & & & & \\ 0 & & G_0 & \cdots & \cdots & & G_b \end{bmatrix}_{(n-b)\times n},$$

$$= \begin{bmatrix} G(x) & & & \\ & xG(x) & & \\ & & \cdots & \\ & & & x^{n-b-1}G(x) \end{bmatrix}.$$

using an obvious notation. From the above theorem, for a constacyclic code C of length n, the generator polynomial $G(x)$ divides $x^n - \lambda$. Then

$$H(x) = (x^n - \lambda)/G(x) = \sum_{i=0}^{k} H_i x^i, H_k \neq 0.$$

is called the check polynomial of C. The reason for this name is that $H(x)$ can be used to compute a parity check matrix for C :

$$G=\begin{bmatrix} H_0 & H_1 & H_2 & \cdots & H_b & & 0 \\ & H_0 & H_1 & \cdots & H_{b-1} & H_b & \\ & & & \cdots & \cdots & & \\ & & & & & & \\ 0 & & H_0 & \cdots & \cdots & & H_b \end{bmatrix}.$$

Furthermore, the check polynomial $H(x)$ of C is related to the generator polynomial of $C^{\perp}$ as follows. To simplify the notation, we give the following definition regarding polynomials.

Definition 6.1. Let $f(x)=f_0+f_1x+\cdots+f_ix^i$ with $f_i\neq 0$ be a polynomial in $\mathbb{Z}_q[x]$. Then the reciprocal polynomial of $f(x)$, denoted by $f^*(x)$, is

$$\begin{aligned} f^*(x) &= f_0^{-1}\overleftarrow{f}(x) \\ &= f_0^{-1}x^if\left(x^{-1}\right) \\ &= f_0^{-1}\left(f_i+f_{i-1}x+\cdots+f_0x^i\right), \end{aligned}$$

where $\overleftarrow{f}(x)$ is the polynomial obtained by reversing the order of the coefficients of $f(x)$. In particular, if $f(x)=f^*(x)$, then $f(x)$ is called self-reciprocal. Note that $f^*(x)=f_0^{-1}x^if\left(x^{-1}\right)$ if $i=\deg(f(x))$.

Theorem 6.2. [39] Let C be a constacyclic code of length n with generator polynomial $G(x)$ and check polynomial $H(x)=\left(x^n-\lambda\right)/G(x)$. Then the dual code $C^{\perp}$ is constacyclic and has generator polynomial

$$G^{\perp}(x)=H^*(x).$$

Now we give some results about λ-constacyclic codes and free λ-constacyclic codes over R. First, let $\lambda\in R$ be such that $\lambda=\lambda_1+v\lambda_2$ where $\lambda_1,\lambda_2\in\mathbb{Z}_q$.

Since $v^2=1$, we have

$$\begin{aligned} \lambda\epsilon_1 &= (\lambda_1+v\lambda_2)\tfrac{1}{2}(1-v) \\ &= \tfrac{1}{2}\lambda_1-\tfrac{1}{2}v\lambda_1+\tfrac{1}{2}v\lambda_2-\tfrac{1}{2}\lambda_2 \\ &= \tfrac{\lambda_1}{2}(1-v)-\tfrac{\lambda_2}{2}(1-v) \\ &= \epsilon_1(\lambda_1-\lambda_2) \end{aligned}$$

$= \epsilon_1\alpha_1$, where $\alpha_1 = \lambda_1 - \lambda_2$.
Similarly, we can show that $\lambda\epsilon_2 = \epsilon_2\alpha_2$ where $\alpha_2 = \lambda_1 + \lambda_2$. Therefore

$$\lambda = \lambda(\epsilon_1 + \epsilon_2) = \epsilon_1\alpha_1 + \epsilon_2\alpha_2,$$

and $\lambda^{-1} = \lambda_1^* + v\lambda_2^*$, where $\alpha_1^{-1} = \lambda_1^* - \lambda_2^*$ and $\alpha_2^{-1} = \lambda_1^* + \lambda_2^*$.

Proposition 4. *An element $\lambda = \lambda_1 + v\lambda_2$ is a unit of R if and only if α_1, α_2 are units in $\mathbb{Z}_q^*$, where $\alpha_1 = \lambda_1 - \lambda_2$ and $\alpha_2 = \lambda_1 + \lambda_2$.*

Proof. Let $\lambda = \lambda_1 + v\lambda_2 = \epsilon_1\alpha_1 + \epsilon_2\alpha_2$ where $\alpha_1 = \lambda_1 - \lambda_2$ and $\alpha_2 = \lambda_1 + \lambda_2$. By the Chinese Remainder Theorem, λ is a unit of $R \iff \alpha_1, \alpha_2$ are both units of $\mathbb{Z}_q^*$. □

6.1 Decomposition of a λ-Constacyclic Code over R

The following theorem provide an explicit decomposition into a direct sum of a constacyclic code C over the ring R.

Theorem 6.3. Let C be a linear code over R of length n and let $C = \epsilon_1C_1 \oplus \epsilon_2C_2$ be its decomposition where C_1 and C_2 are codes over $\mathbb{Z}_q$ of length n. Then C is a λ-constacyclic code over R if and only if C_1 and C_2 are α_j-constacyclic codes over $\mathbb{Z}_q$ for $j = 1, 2$, where λ, α_1 and α_2 are as in Proposition 4.

Proof. For any $s = (s_0, s_1, \ldots, s_{n-1}) \in C$, we can write its components as $s_i = \epsilon_1a_i \oplus \epsilon_2b_i$ where $a_i, b_i \in \mathbb{Z}_q, 0 \leq i \leq n-1$. Let $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$. Now, assume that C_j is a α_j-constacyclic code of length n over $\mathbb{Z}_q$, $j = 1, 2$. This implies that

$$\rho_{\alpha_1}(a) = (\alpha_1a_{n-1}, a_0, \ldots, a_{n-2}) \in C_1, \rho_{\alpha_2}(b) = (\alpha_2b_{n-1}, b_0, \ldots, b_{n-2}) \in C_2. \qquad (2.1)$$

It is easily seen that $\epsilon_1\rho_{\alpha_1}(a) + \epsilon_2\rho_{\alpha_2}(b) = \rho_\lambda(s)$, so C is a λ-constacyclic code of length n over R.

Conversely, suppose that C is a λ-constacyclic code of length n over R. Let $s_i = \epsilon_1a_i + \epsilon_2b_i$ for any $a = (a_0, a_1, \ldots, a_{n-1}), b = (b_0, b_1, \ldots, b_{n-1})$. Then $a \in C_1, b \in C_2$ so $s = (s_0, s_1, \ldots, s_{n-1}) \in C$. By the hypothesis,

$$\rho_\lambda(s) = (\lambda(s_{n-1}), s_0, \ldots, s_{n-2}) \in C.$$

Using the fact that $\lambda\epsilon_j = \epsilon_j\alpha_j$ for $j = 1, 2$, we get

$$\lambda(s_{n-1}) = \lambda(\epsilon_1 a_{n-1} + \epsilon_2 b_{n-1})$$

$$= \epsilon_1\alpha_1(a_{n-1}) + \epsilon_2\alpha_2(b_{n-1}).$$

Therefore,

$$\rho_\lambda(s) = (\lambda(s_{n-1}), s_0, \ldots, s_{n-2})$$

$$= \epsilon_1(\alpha_1(a_{n-1}), a_0, \ldots, a_{n-2}) + \epsilon_2(\alpha_2(b_{n-1}), b_0, \ldots, b_{n-2}).$$

Thus, $\rho_{\alpha_1}(a) \in C_1, \rho_{\alpha_2}(b) \in C_2$. This implies that C_j is an α_j-constacyclic code of length n over $\mathbb{Z}_q$ for $j = 1, 2$. □

The previous Theorem gave a direct sum decomposition of a constacyclic code C over R. Now, we recall a fundamental fact about free constacyclic codes over R. Together with Theorem 7.4, this generalizes Theorem 4 in [59].

Definition 6.2. Let R be a commutative ring with identity. A linear code of length n over R is an R-submodule of R^n. If C is a free R-module, then it is called a free code.

7 The Standard Generator of a Free Constacyclic Code over R

The polynomial in the following Theorem is called the standard generator of a free constacyclic code over R and it characterizes all other generator polynomials. When we refer to "the generator" polynomial of a constacyclic code, we mean this standard generator, which is unique up to an associate.

Theorem 7.1. A λ-constacyclic code C over R is free if $C = \langle g(x)\rangle$ and $g(x)|x^n - \lambda$ in $R[x]$.

Proof. Let C be a λ-constacyclic code where $C = \langle g(x)\rangle$ and $x^n - \lambda = g(x)h(x)$. Since $x^n - 1$ is monic, the leading coefficients of $g(x)$ and $h(x)$ are units, and they are not zero divisors. Let $k = \deg(h(x))$. Then $\deg(g(x)) = n - k$. We claim that the set $B = \{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ is a basis for C. First we show that B is linearly independent. Suppose $a_0 g(x) + a_1 xg(x) + \cdots + a_{k-1}x^{k-1}g(x) = 0$ for some $a_0, a_1, \ldots a_{k-1}$ in R. This equation can be rewritten as $a(x)g(x) = 0$ where $a(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$. Hence, $a(x)g(x) \equiv 0 \mod x^n - \lambda$. Therefore, $x^n - \lambda | a(x)g(x)$. Since $g(x)$ is not a zero divisor, we conclude $h(x)|a(x)$, and $a(x) = h(x)s(x)$ for some $s(x) \in R[x]$. Since $h(x)$ is not a zero divisor, $\deg(a(x)) \geq \deg(h(x)) = k$. However, this yields a contradiction unless $a(x)$ is the zero polynomial. This shows that B is linearly independent.

Now we show that B spans C. Let $c(x) \in C$. For any polynomial $f(x)$ in $R[x]$, let $\overline{f(x)}$ denote $f(x) \mod x^n - \lambda$. Since $C = \langle g(x) \rangle$, $c(x) = b(x)g(x)$ for some $b(x) \in R[x]$. Then, $\overline{c(x)} = \overline{b(x)g(x)} = \overline{b(x)} \cdot \overline{g(x)} = \overline{b(x)} \cdot g(x)$. Since the leading coefficient of $g(x)$ is a unit and $\deg(\overline{c(x)}) < n$, we must have $\deg(\overline{b(x)}) < k$. Hence $c(x)$ is in the span of B. □

Lemma 7.2. Let $C = \langle g(x) \rangle$ be a free λ-constacyclic code of length n over R such that $\gcd(n, q) = 1$. Then $C_i = \langle g_i(x) \rangle$ is a free α_i-constacyclic code over $\mathbb{Z}_q$ where $g(x) = \epsilon_1 g_1(x) + \epsilon_2 g_2(x)$.

Proof. From Theorem 6.3, $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ and C is λ-constacyclic over R if and only if C_i is α_j-constacyclic $\mathbb{Z}_q[x]$. It is well known [31] that a constacyclic code C_i over $\mathbb{Z}_q[x]$ of length coprime with n is a principal ideal generated by a polynomial $g_i(x)$ in $\mathbb{Z}_q[x]$. Thus $C = \langle g(x) \rangle = \epsilon_1 \langle g_1 \rangle \oplus \epsilon_2 \langle g_2 \rangle$. Consider the projection map $Pr_i : C \longrightarrow C_i$ which is a module epimorphism. Since C is free, C_i as the image of Pr_i is also free [49] (Exercise 1 on page 137). Hence the result follows. □

Theorem 7.3. Let $C = \langle g(x) \rangle$ be a free λ-constacyclic code where $g(x)|x^n - \lambda$. Then $C = \langle g(x) \rangle = \langle g(x)f(x) \rangle$ if and only if $\gcd(f(x), h(x)) = 1$ over $R[x]$ where $g(x)h(x) = x^n - \lambda$.

Proof. $\Rightarrow$: Assume $\langle g(x) \rangle = \langle g(x)f(x) \rangle$. Since $g(x) \in \langle g(x) \rangle = \langle g(x)f(x) \rangle$, we have $g(x) = g(x)f(x)a(x)$ for some $a(x) \in R[x]$. Thus, $g(x)(1 - f(x)a(x)) = 0 = b(x)g(x)h(x)$ in $R[x]$ for some $b(x) \in R[x]$. Hence, $g(x)(1 - f(x)a(x) - b(x)h(x)) = 0$, and given that $g(x)$ cannot be a zero divisor in $R[x]$ (because its leading term is a unit), $1 = f(x)a(x) + b(x)h(x)$, which implies that $\gcd(f(x), h(x)) = 1$.

$\Leftarrow$: Assume $\gcd(f(x), h(x)) = 1$. The inclusion $\langle g(x) \rangle \supseteq \langle g(x)f(x) \rangle$ is obvious. For the other direction, take an arbitrary $c(x) \in \langle g(x) \rangle = C$, so $c(x) = g(x)a(x)$ for some $a(x) \in R[x]$. Given that $\gcd(f(x), h(x)) = 1$, there exist $A(x), B(x) \in R[x]$ such that

$A(x)f(x) + B(x)g(x) = 1$. Hence, we have

$$\begin{aligned} c(x) = g(x)a(x) &= g(x)a(x)A(x)f(x) + g(x)a(x)B(x)h(x) \\ &= g(x)f(x)(a(x)A(x)) + (x^n - \lambda)B(x)a(x) \\ &= g(x)f(x)(a(x)A(x)) \in \langle g(x)f(x)\rangle \text{ in } \frac{R[x]}{\langle x^n - \lambda\rangle}, \end{aligned}$$

so that $\langle g(x)\rangle \subseteq \langle g(x)f(x)\rangle$, which implies $\langle g(x)\rangle = \langle g(x)f(x)\rangle$. □

Theorem 7.4. Let $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ be a free λ-constacyclic code of length n over R where C_j is a constacyclic code over $\mathbb{Z}_q$ with shift constant α_j for $j = 1, 2$. Then

(i)
$$C = \langle \epsilon_1 g_1(x), \epsilon_2 g_2(x)\rangle, \text{ and } \quad |C| = q^{2n-(\deg(g_1)+\deg(g_2))}.$$

(ii) There exists a polynomial $g(x) \in R[x]$ such that $C = \langle g(x)\rangle$ and $g(x) \mid x^n - \lambda$ where $g(x) = \epsilon_1 g_1(x) + \epsilon_2 g_2(x)$.

Pro(i)f) Let $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ be a free λ-constacyclic code of length n over R. Since C is a free module and R a principal ideal ring, C_j's as submodules are also free, so C_j is a free α_j-constacyclic code of length n over $\mathbb{Z}_q$ for $j = 1, 2$, and from Lemma 1, $g_j(x)$ is the generator polynomial of C_j, so $C_j = \langle g_j(x)\rangle \subseteq \mathbb{Z}_q[x]/\langle x^n - \alpha_j\rangle$ for $j = 1, 2$. Therefore, by the construction, C has the form

$$C = \langle \epsilon_1 g_1(x), \epsilon_2 g_2(x)\rangle.$$

For the statement on the size, since $|C| = |\phi(C)| = |C_1||C_2|$, we have

$$|C| = q^{2n-(\deg(g_1)+\deg(g_2))}.$$

(ii) From the first part

$$C = \langle \epsilon_1 g_1(x), \epsilon_2 g_2(x)\rangle.$$

Let $g(x) = \epsilon_1 g_1(x) + \epsilon_2 g_2(x)$. Then it is easily seen that $\langle g(x)\rangle \subseteq C$. On the other hand, $C \subseteq (\epsilon_1 g_1(x), \epsilon_2 g_2(x)) \subseteq R[x]/x^n - \lambda$, which means $C \subseteq \langle g(x)\rangle$ and hence $C = \langle g(x)\rangle$.

Now suppose $g_j(x)$ is the generator polynomial of C_j for $j = 1, 2$, respectively. Since C_j is free, $g_j(x)$ divides $x^n - \alpha_j$ so that $x^n - \alpha_j = h_j(x)g_j(x)$. This implies that $\epsilon_j(x^n - \alpha_j) =$

$\epsilon_j h_j(x) g_j(x)$ for $j = 1, 2$. Then
$x^n - \lambda = (\epsilon_1 + \epsilon_2)x^n - (\epsilon_1\alpha_1 + \epsilon_2\alpha_2)$ (because $\epsilon_1 + \epsilon_2 = 1$)
$= \epsilon_1(x^n - \alpha_1) + \epsilon_2(x^n - \alpha_2))$
$= \epsilon_1 h_1(x) g_1(x) + \epsilon_2 h_2(x) g_2(x)$
$= (\epsilon_1 h_1(x) + \epsilon_2 h_2(x))(\epsilon_1 g_1(x) + \epsilon_2 g_2(x))$ (because $\epsilon_i^2 = \epsilon_i, \epsilon_i\epsilon_j = 0$ where $i = 1, 2$ and $i \neq j$).
$= (\epsilon_1 h_1(x) + \epsilon_2 h_2(x)) g(x)$.
Therefore, $g(x)$ is a divisor of $x^n - \lambda$.

□

8 Dual of a Free λ-Constacyclic Code over R

Theorem 8.1. Let C_1, C_2 be free codes over $\mathbb{Z}_q$ and let $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ be a free λ-constacyclic code of length n over R. Then $C^\perp = \epsilon_1 C_1^\perp \oplus \epsilon_2 C_2^\perp$ is a free λ^{-1}-constacyclic code of length n over R where $C_j^\perp$ is a free α_j^{-1}-constacyclic code of length n over $\mathbb{Z}_q$ for $j = 1, 2$.

Proof. Let $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ be a linear code of length n over R. Then by the direct sum decomposition, the dual code $C^\perp = \epsilon_1 C_1^\perp \oplus \epsilon_2 C_2^\perp$ of C is also a linear code of length n over R. Theorems 6.3 and 7.4 give the direct sum decomposition of a λ-constacyclic code over R and its generators, respectively. According to [23], [24], the dual of a free λ-constacyclic code of length n over R is a free λ^{-1}-constacyclic code of length n over R. Therefore, $C^\perp = \epsilon_1 C_1^\perp \oplus \epsilon_2 C_2^\perp$ is also a free λ^{-1}-constacyclic code of length n over R where $C_j^\perp$ is a free α_j^{-1}-constacyclic code of length n over $\mathbb{Z}_q$ for $j = 1, 2$. □

corollary 1. *Let $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ be a free λ-constacyclic code of length n over R, and let $g_j(x)$ be the generator polynomial of the constacyclic code C_j for $j = 1, 2$ which divides $x^n - \lambda$. Then*

$C^\perp = \langle \epsilon_1 h_1^*, \epsilon_2 h_2^* \rangle$ *and* $|C^\perp| = q^{(deg\,(g_1(x)) + deg\,(g_2(x)))}$,

$C^\perp = \langle h^*(x) \rangle$, *where* $h^*(x) = \langle \epsilon_1 h_1^* + \epsilon_2 h_2^* \rangle$,

where $x^n - \lambda = h_j(x) g_j(x)$ for some $h_j(x) \in \mathbb{Z}_q[x]$ and $h_j^*(x) = x^{deg\,(h_j(x))} h_j(x^{-1})$ generates the dual constacyclic code $C_j^\perp$ for $j = 1, 2$.

9 Gray Image of a Free λ-Constacyclic Code over R

In this section, we recall the definition of a Gray map on R, and other results which we will needed in the sequel.

Definition 9.1. Let C_β be a linear code over R of length $\beta = N\ell$ and let λ be unit in R. If for any codeword

$$(c_{0,0}, c_{0,1}, \ldots, c_{0,\ell-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,\ell-1}, \ldots, c_{N-1,0}, c_{N-1,1}, \ldots, c_{N-1,\ell-1}) \in C_\beta$$

then

$$(\lambda(c_{N-1,0}), \lambda(c_{N-1,1}), \ldots, \lambda(c_{N-1,\ell-1}), c_{0,0}, c_{0,1}, \ldots, c_{0,\ell-1}, \ldots, c_{N-2,0}, c_{N-2,1}, \ldots, c_{N-2,\ell-1}) \in C_\beta$$

Then we say that C_β is a λ-quasi-twisted code of length β. If ℓ is the least positive integer such that $\beta = N\ell$, then C_β is called an ℓ-quasi-twisted code or a quasi-twisted code with index ℓ over R.

According to the subsection 1.8.2, we define a Gray map Φ over R by

$$\Phi : R^\beta \longrightarrow \mathbb{Z}_q^{2\beta}$$

$$\Phi(a + vb) = (a, a + b),$$

where $a, b \in R^\beta$.
Let $a \in \mathbb{Z}_q^{2\beta}$ with $a^{(0)}, a^{(1)} = (a^{(0)} \mid a^{(1)})$, $a^{(i)} \in R^\beta$, for $i = 0, 1$. Let σ a quasi twisted shift from $\mathbb{Z}_q^{2\beta}$ to $\mathbb{Z}_q^{2\beta}$ given by

$$\sigma(a^{(0)} \mid a^{(1)}) = (\rho_\lambda(a^{(0)}) \mid \rho_\lambda(a^{(1)})),$$

where $\mid$ is vector concatenation, and and ρ_λ is the constacyclic shift operator from $\mathbb{Z}_q^\beta$ to $\mathbb{Z}_q^\beta$ defined by

$$\rho_\lambda(a^{(i)}) = (\lambda a^{(i,\beta-1)}, a^{(i,0)} \ldots, a^{(i,\beta-2)}),$$

For every $a^{(i)} = (a^{(i,0)}, a^{(i,1)}, \ldots, a^{(i,\beta-1)})$ where $a^{(i,j)} \in \mathbb{Z}_q$, for $j = 0, 1, \ldots, \beta - 1$.

Proposition 5. *With the notation above, we have $\Phi \circ \rho_\lambda = \sigma \circ \Phi$.*

Proof. Let $r = (r_0, r_1, \ldots, r_{\beta-1}) \in R^\beta$ where $r_i = a_i + ub_i, 0 \leq i \leq \beta - 1$. Then we have $\Phi(r) = (a_0, a_1, \ldots, a_{\beta-1}, a_0 + b_0, a_1 + b_1, \ldots, a_{\beta-1} + b_{\beta-1})$, so that

$$\Phi(\rho_\lambda(r)) = (\lambda a_{\beta-1}, a_0, \ldots, a_{\beta-2}, \lambda(a_{\beta-1} + b_{\beta-1}), a_0 + b_0, \ldots, a_{\beta-2} + b_{\beta-2}).$$

On the other hand,

$$\begin{aligned} \sigma(\Phi(r)) &= \sigma(a_0, a_1, \ldots, a_{\beta-1}, a_0 + b_0, a_1 + b_1, \ldots, a_{\beta-1} + b_{\beta-1}) \\ &= \left(\lambda a_{\beta-1}, a_0, \ldots, a_{\beta-2}, \lambda(a_{\beta-1} + b_{\beta-1}), a_0 + b_0, \ldots, a_{\beta-2} + b_{\beta-2}\right). \end{aligned}$$

Hence the result follows. □

Proposition 6. *Let C be a linear code of length β over R. Then C is a constacyclic code of length β over R if and only if $\Psi(C)$ is a QT code of length 2β over $\mathbb{Z}_q$ of index 2.*

Proof. Let C be a constacyclic code. Then $\rho_\lambda(C) = C$. We have $\Phi\left(\rho_\lambda(C)\right) = \Phi\left(C\right)$, and from Proposition 1

$$\sigma\left(\Phi(C)\right) = \Phi\left(\rho_\lambda(C)\right) = \Phi(C).$$

Hence, $\Phi(C)$ is a QT code of index 2.

Conversely, let $\Phi(C)$ be a QT code of index 2. Then we have

$$\sigma(\Phi(C)) = \Phi(C).$$

By Proposition 1

$$\Phi(C) = \sigma\left(\Phi(C)\right) = \Phi\left(\rho_\lambda(C)\right).$$

Since Φ is injective, it follows that $\rho_\lambda(C) = C$. □

Remark. Based on computational findings, it seems that the Gray image of a free constacyclic code over R, particularly when $q = 4$, shows characteristics of a free code over $\mathbb{Z}_4$. Subsequently, it has been established that this holds true in a general case.

We prove this one in the following theorem.

Theorem 9.1. Let C be a free constacyclic code of length n over R. Then the Gray image $\Phi(C)$ is also a free code over $\mathbb{Z}_q$.

Proof. Let C be a free constacyclic code of length β over R. Then from Theorem 2, there exists a minimum degree polynomial $g(x)$ whose leading coefficient is a unit such that $C = \langle g(x)\rangle$, $g(x)|x^\beta - \lambda$, and the set

$$\{g(x), xg(x), \ldots, x^{\beta-deg(g(x)-1}g(x)\},$$

where $k = \beta - \deg(g(x))$, forms a basis for C. We claim that the set $B := \{\Phi(g(x)), \Phi(xg(x)), \dots, \Phi(x^{k-1}g(x)), \Phi(ug(x)), \Psi(uxg(x)), \dots, \Psi(ux^{k-1}g(x))\}$ is a basis for $\Phi(C)$.

Note that the map Φ is a vector space isomorphism. First we show that B is linearly independent. Suppose

$$a_0\Phi(g(x)) + a_1\Phi(xg(x)) + \cdots + a_{k-1}\Phi(x^{k-1}g(x))$$

$$+b_0\Phi(ug(x)) + b_1\Phi(uxg(x)) + \cdots + b_{k-1}\Phi(ux^{k-1}g(x)) = 0.$$

Since Φ is a vector space homomorphism, we have

$$\Phi(a_0g(x) + a_1xg(x) + \cdots + a_{k-1}x^{k-1}g(x) + b_0ug(x) + \cdots + b_{k-1}ux^{k-1}g(x)) = 0.$$

Since Φ is injective, we conclude that

$$a_0g(x) + a_1xg(x) + \cdots a_{k-1}x^{k-1}g(x) + b_0ug(x) + b_1uxg(x) + \cdots + b_{k-1}ux^{k-1}g(x) = 0.$$

We can rewrite this equation as $A(x)g(x) = 0$ in $\dfrac{R[x]}{\langle x^\beta - \lambda\rangle}$ where $A(x) = a_0 + a_1x + \cdots + b_{k-1}ux^{k-1}$. Since $g(x)|x^\beta - \lambda$, the leading coefficient of $g(x)$ is a unit and $\deg(A(x)) < k = \beta - \deg(g(x))$. This is only possible if $A(x)$ is the zero polynomial. Hence, $a_i = 0 = b_j$ for all i and j, and B is linearly independent.

Now we show that B spans $\Phi(C)$. Let $z \in \Phi(C)$. Then $z = \Phi(c)$ for some $c \in C$ and $c(c) = a(x)g(x)$ for some $a(x) \in R[x]$ with $\deg(a(x)) < k$. Let $a(x) = A(x) + uB(x)$ where $A(x), B(x) \in \mathbb{Z}_q[x]$. Then we have

$$z = \Phi(A(x)g(x) + uB(x)g(x)) = \Phi(A(x)g(x)) + \Phi(uB(x)g(x)).$$

Now let $A(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ and $B(x) = b_0 + b_1x + \cdots + b_{k-1}x^{k-1}$ where $a_i, b_j \in \mathbb{Z}_q$. Using the fact that Φ is a vector space homomorphism we have

$$c = a_0\Phi(g(x)) + a_1\Phi(xg(x)) + \cdots + b_{k-1}\Phi(ux^{k-1}g(x)).$$

Hence, c is in the span of B. □

Chapter 3

Quasi Twisted Codes over R

1 Introduction

We have seen that the class of QC codes contain many codes with good or the best possible parameters. Therefore a larger class of linear codes, called quasi-twisted (QT) codes, deserves a careful study. The class of QT codes is not as well studied as that of QC codes.

Quasi-twisted (QT) codes over rings form an important class of block codes that includes cyclic codes, quasi-cyclic codes and constacyclic codes as special cases.
In this chapter, we investigate issues related to the decomposition and construction of a QT code. From [1], we give the definition of λ-quasi-twisted codes. Some results of this chapter can be found in [11]

Definition 1.1. Let λ be a unit in R, ℓ be a positive integer, and $\tau_{\ell,\lambda}$ be the permutation of R^n, given by

$$\tau_{\ell,\lambda}(c) = (\lambda c_{n-\ell}, \dots, \lambda c_{n-1,} c_0, \dots, c_{n-\ell-1})$$

for any $c = (c_0, \dots, c_{n-1}) \in R$. For a linear code C of length n over R, if $\tau_{\ell,\lambda}(C) = C$, then C is called an ℓ-quasi twisted (QT) code (or a QT code of index ℓ), over R. For $\ell = 1$, we obtain the important special case $\tau_{1,\lambda} = \rho_\lambda$ of a λ-constacyclic code of length n over R. The unit λ is called the shift constant.

In this section, we consider that $\gcd(n, p) = 1$ where $q = p^m$ for a prime p and a positive integer m. Let $R_t = R[x]/\langle x^t - \lambda\rangle$ and suppose C is a QT code of length $n = t\ell$ and index ℓ over R.

2 Factorisation of $x^n - \lambda$ over R

Definition 2.1. A polynomial $f(x) \in \mathbb{Z}_q[x]$ is irreducible in $\mathbb{Z}_q$ if whenever $f(x) = g(x)h(x)$ for two polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}_q[x]$, one of $g(x)$ or $h(x)$ is a unit.

We now consider the factorization of $x^n - \lambda$ over R. We denote by $^-$ the natural ring homomorphism

$$^- : R \longrightarrow \mathbb{Z}_q$$

$$a + bu \rightarrow a$$

Now extend $^-$ to a ring homomorphism from $R[x]$ into $\mathbb{Z}_q[x]$ by

$$\overline{f(x)} = \sum \overline{u}_k x^k, \text{ for all } f(x) = \sum u_k x^k \in R[x] \text{ where } u_k \in R.$$

A monic polynomial $f(x) \in R[x]$ is said to be monic basic irreducible over R if $\overline{f(x)}$ is an irreducible polynomial over $\mathbb{Z}_q[x]$.

Lemma 2.1. Let $g(x)$ be an irreducible polynomial over $\mathbb{Z}_q[x]$, where $g(x) \mid (x^n - \lambda)$. Then there exists a unique basic irreducible polynomial $f(x) \in R[x]$ such that $\overline{f(x)} = g(x)$ and $f(x) \mid (x^n - \lambda)$ over R.

Proof. Let $x^n - \lambda = g(x)k(x) \in \mathbb{Z}_q[x]$. Since $\gcd(n, p) = 1$, $g(x)$ has no multiple roots. Further, it is clear that $x \nmid g(x)$. Then according to ([56] Theorem 13.10), we have that $g(x)$ has a unique Hensel lift $f(x)$ over $\mathbb{Z}_q[x]$ such that $f(x) \mid (x^n - \lambda)$. Since $\mathbb{Z}_q[x]$ is a subring of R, the factorization of $x^n - \lambda$ is still valid over R. This means that $f(x) \mid (x^n - \lambda)$ over R. Therefore, $g(x)$ is irreducible over $\mathbb{Z}_q[x]$ and $f(x)$ is basic irreducible over R. □

Since $\gcd(n, p) = 1$ and $\mathbb{Z}_q[x]$ is a subring of R, the factorization of $x^n - \lambda$ is still valid over R. It follows that $x^t - \lambda$ can be factored uniquely into pairwise coprime basic irreducible polynomials over R, i.e., for $i = 1, \ldots, s$

$$x^t - \lambda = f_1(x) f_2(x) \ldots f_s(x), \tag{3.1}$$

where $f_i(x)$ is a basic irreducible polynomial over $\mathbb{Z}_q[x]$.

3 Decomposition of QT Code over R

Let C be a (λ, ℓ)-QT code of length n over $\mathbb{Z}_q$. Recall that C is a module over the ring $R[x]/(x^t - \lambda)$, where $t = n/\ell$. Denote $R[x]/(x^t - \lambda)$ by R_t.
In order to know more about the algebraic structure of QT codes, we next focus on the ring R_t.
Therefore, since R_t is a principal ideal ring, it can be decomposed into a direct sum of semi local rings. Hence, the Chinese Remainder Theorem gives the following decomposition

$$R_t = R[x]/\langle x^t - \lambda \rangle = R[x]/\langle f_1(x) \rangle \oplus R[x]/\langle f_2(x) \rangle \oplus \cdots \oplus R[x]/\langle f_s(x) \rangle. \tag{3.2}$$

The direct sum on the right hand side is endowed with coordinate-wise addition and multiplication. For convenience, we denote the ring $R[x]/\langle f_i(x) \rangle$ by R_i for $1 \leq i \leq t$ It follows that

$$R_t^\ell \cong \bigoplus_{i=1}^{s} R_i^\ell.$$

Then the following theorem is an immediate consequence.

Theorem 3.1. Let C be a QT code of length $n = t\ell$ over R. Then C is a linear code over R_t of length ℓ which can be decomposed as the direct sum

$$C \cong \bigoplus_{i=1}^{m} C_i, \tag{3.3}$$

where C_i is a linear code over R_i of length ℓ for $1 \leq i \leq s$.

Theorem 3.2. Let $T = \mathbb{Z}_{q^n} + v\mathbb{Z}_{q^n}$ where $v^2 = 1$. Further, let $f, g \in T[x]$ and $\tilde{f}, \tilde{g} \in \mathbb{Z}_q[x]$ where $\tilde{f} = f \mod q^{n-1}v$ and $\tilde{g} = g \mod q^{n-1}v$. Then $\gcd(f, g) = 1$ if and only if $\gcd(\tilde{f}, \tilde{g}) = 1$.

Proof. Let $f, g \in T[x]$ and suppose $\gcd(f, g) = 1$. Then there exist $a, b \in T[x]$ such that $af + bg = 1$. Therefore, we have the following

$$\begin{aligned} 1 &= af + bg \\ &= \tilde{af} + \tilde{bg} \\ &= \tilde{a}\tilde{f} + \tilde{b}\tilde{g}, \end{aligned}$$

where $\tilde{a}, \tilde{b}, \tilde{f}, \tilde{g} \in \mathbb{Z}_q[x]$. Hence, $\gcd(\tilde{f}, \tilde{g}) = 1$.

Now suppose $\gcd(\tilde{f}, \tilde{g}) = 1$. Then there exist $\tilde{a}, \tilde{b} \in \mathbb{Z}_q$ such that $\tilde{a}\tilde{f} + \tilde{b}\tilde{g} = 1$. Thus, for some $k \in T[x]$ we have $af + bg = 1 + kq^{n-1}v$. Multiplying both sides by kq^{n-1}, we have

$$kq^{n-1}v(af + bg) = kq^{n-1}v + kq^{n-1}ukq^{n-1}v, \tag{3.4}$$

$$kq^{n-1}v(af + bg) = kq^{n-1}v + q^n k^2 q^{n-2} = kq^{n-1}v. \tag{3.5}$$

Substituting (3.4) in $af + bg = 1 + kq^{n-1}v$ gives $af + bg = 1 + kq^{n-1}v(af + bg)$. Then $(1 - kq^{n-1}v)af + (1 - kq^{n-1}v)bg = 1$, which implies that $\gcd(f, g) = 1$. □

4 Dual Codes of QT Codes over R

In this section, we examine more closely the structure of the dual code of a QT code when $\lambda^2 = 1$. In particular, we show that the dual of a QT code over R of length $t\ell$ and index ℓ is also a QT code of the same length and index. We first recall some basic definitions.

Definition 4.1. Let $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$ be two n-tuples whose elements are from R^ℓ where $a_i = (a_{i0}, a_{i1}, \ldots, a_{i(\ell-1)})$ and $b_i = (b_{i0}, b_{i1}, \ldots, b_{i(\ell-1)}) \in R^\ell$ for $0 \leq i \leq n-1$. The usual Euclidean inner product of a and b is defined by

$$a.b = \sum_{i=0}^{n-1} a_i b_i = \sum_{i=0}^{n-1} \sum_{j=0}^{\ell-1} a_{ij} b_{ij},$$

and the dual of C with respect to Euclidean inner product is then

$$C^\perp = \{b \in R^{t\ell} \mid a \cdot b = 0 \forall a \in C\}.$$

If $C \cap C^\perp = \{0\}$, then C is an LCD code over R.

For any $a_i = (a_{i0}, a_{i1}, \ldots, a_{i(\ell-1)})$ and $b_i = (b_{i0}, b_{i1}, \ldots, b_{i(\ell-1)}) \in R^\ell$ for $0 \leq i \leq n-1$, the usual Hermitian inner product of $a(x)$ and $b(x)$ is defined as

$$a(x) * b(x) = \sum_{j=0}^{\ell-1} a_{ij}(x) b_{ij}(x^{-1}).$$

Further, for the element $a = (a_0, a_1, \ldots, a_{s-1}) \in R^{t\ell}$, the action of the map τ_ℓ on $R^{t\ell}$ can be expressed as

$$\tau_\ell(u_0, u_1, \ldots, u_{s-1}) = (u_{s-1}, u_0, \ldots, u_{s-2}),$$

where $u_i = (u_{i,0}, u_{i,1}, \ldots, u_{i,\ell-1})$. Thus, τ_ℓ is a QT shift operator on the t-tuples of elements from R^ℓ.

In the next proposition, we show that the dual of a QT code over R of length $t\ell$ and index ℓ is a QT code of the same index.

Proposition 7. *Let C be a QT code of length $t\ell$ over R and $C^\perp$ be the dual code of C. Then $C^\perp$ is a QT code of length $t\ell$ and index ℓ over R.*

Proof. Let C be a QT code of length $t\ell$ and index ℓ, and let $a \in C$ and $b \in C^\perp$ be two arbitrary elements. Then we have

$$a \cdot \tau_\ell(b) = \sum_{i=0}^{t-1} a_i \cdot b_{i+t-1} = \sum_{i=0}^{t-1} a_i b_{i+t-1} = \tau_\ell^{t-1}(a) \cdot b = 0,$$

where the subscript $i + t - 1$ is taken modulo t. Hence, $\tau_\ell(a) \in C^\perp$ and so $C^\perp$ is also a QT code of length $t\ell$ and index ℓ. □

By the above proposition, we know that $C^\perp$ is a submodule of $R_t^{'} = \frac{R[x]}{\langle x^t - \lambda^{-1} \rangle}$ over R_t and hence a linear code over R_t.
First, note that $\lambda^2 = 1$, and notice that a QT code is an R_t-module while its dual code is an $R_t^{'}$-module. However, two rings R_t and $R_t^{'}$ are isomorphic:

$$R_t \simeq R_t^{'}$$

$$x \longleftrightarrow x^{-1}$$

where $x^{-1} = \lambda^{-1} x^{t-1}$ in the ring R_t and $x^{-1} = \lambda x^{t-1}$ in the ring R_t'.
By the above isomorphism, we now define a map which induces a one-to-one correspondence between QT codes over R of length $t\ell$ with index ℓ and linear codes over R_t of length ℓ.

Definition 4.2. For all $r_1(x), r_2(x), \ldots, r_\ell(x) \in \acute{R}_t^\ell$, we define the map $\Phi : \acute{R}_t^\ell \longrightarrow R_t^\ell$ by

$$\Phi(r_1(x), r_2(x), \ldots, r_\ell(x)) = (r_1(x^{-1}), r_2(x^{-1}), \ldots, r_\ell(x^{-1})). \tag{3.6}$$

It follows that the map Φ is bijective since it is derived from the isomorphism between R_t' and R_t.

Hence we have proved the following proposition.

Proposition 8. *The map Φ gives a one-to-one correspondence between the set of linear codes of length ℓ over R_t and the set of linear codes of length ℓ over R'_t.*

Next, we consider the case when $\lambda \in \{-1, 1\}$. It is well know that a finite commutative ring always decomposes into a product of local rings. We will make use of this decomposition in our context to facilitate the study of QT codes over R. According to (3.1), we have that the polynomial $x^t - \lambda$ factors into pairwise coprime monic irreducible polynomials over R and hence we may write

$$x^t - \lambda = f_1(x) f_2(x) \dots f_s(x), \text{ with } \lambda \in \{-1, 1\}.$$

In this section, we focus on the case when $\lambda = \pm 1$, that is, $x^t - \lambda = x^t - \lambda^{-1}$ and hence $R_t = R_t^{'}$. Denote the factors f_i in the factorization of $x^t - \lambda$ which are self-reciprocal by $g_1 \dots g_l$ and the remaining f_i's grouped in pairs by $h_1, h_1^*, \dots, h_t, h_t^*$. Then we have

$$x^t - \lambda = g_1(x) \dots g_l(x) \left(h_1(x) h_1^*(x) \dots h_l(x) h_t^*(x) \right).$$

Consequently, we have the following expression

$$R_t \cong \left(\bigoplus_{i=1}^{m} \frac{R[x]}{g_i} \right) \oplus \left(\bigoplus_{j=1}^{t} \left(\frac{R[x]}{h_j} \oplus \frac{R[x]}{h_j^*} \right) \right). \tag{3.7}$$

Throughout this section, we denote $\frac{R[x]}{g_i}$ by $\mathbb{G}_i$, $\frac{R[x]}{h_j}$ by $\mathbb{H}_j$ and $\frac{R[x]}{h_j^*}$ by $\mathbb{H}_j^*$. It follows from (3.7) that

$$R_s^\ell = \left(\bigoplus_{i=1}^{m} \mathbb{G}_i^\ell \right) \oplus \left(\bigoplus_{j=1}^{t} (\mathbb{H}_j^\ell \oplus (\mathbb{H}_j^*)^\ell) \right). \tag{3.8}$$

In particular, every linear code C of length ℓ over R_t can be decomposed as follows

$$C \cong \bigoplus_{i=1}^{m} \acute{C}_i \oplus \left(\bigoplus_{j=1}^{t} (\acute{C}_j \oplus \acute{\acute{C}}_j) \right), \tag{3.9}$$

where for each $1 \leq i \leq m, C_i$ is a linear code of length ℓ over $\mathbb{G}_i$ and for each $1 \leq j \leq t, \acute{C}_j$ is a linear code of length ℓ over $\mathbb{H}_j$ and $\acute{\acute{C}}_j$ is a linear code of length ℓ over $\mathbb{H}_j^*$. Therefore, in this case the map Φ is an automorphism of R_t^ℓ. We also define isomorphisms between component rings as follows.

Definition 4.3. For $1 \leq i \leq m$, define

$$\Phi_i : \mathbb{G}_i^\ell \longrightarrow \mathbb{G}_i^\ell$$

by

$$\Phi_i((r_1(x) + (g_i(x)), \dots, r_\ell(x) + (g_i(x)))$$
$$= (r_1(x^{-1}) + (g_i(x)), \dots, r_\ell(x^{-1}) + (g_i(x))).$$

For $1 \leq j \leq t$, define

$$\acute{\Phi}_j : (\mathbb{H}_j)^\ell \longrightarrow (\mathbb{H}_j^*)^\ell$$

by

$$\acute{\Phi}_j(r_1(x) + (h_j(x)), \dots, r_\ell(x) + (h_j(x)))$$
$$= (r_1(x^{-1}) + (h_j^*)(x)), \dots, r_\ell(x^{-1}) + (h_j^*(x))).$$

Actually, when $\lambda = \pm 1$, the maps Φ,Φ_i and Φ_j are exactly the conjugate maps defined in [37].

Lemma 4.1. Let the decomposition of the ring R be as in (3.7). Assume that $\lambda = \pm 1$ and $r(x) \in R_t$ and its decomposition in R_t is

$$(r_1(x), \dots, r_m(x), \acute{r}_1(x), \acute{\acute{r}}_1(x), \dots, \acute{r}_s(x), \acute{\acute{r}}_s(x)),$$

where for $1 \leq i \leq m$, $r_i(x) = r(x) + (g_i(x)) \in \mathbb{G}_i$ and for $1 \leq j \leq t$, $\acute{r}_j(x) = r(x) + (h_j(x)) \in \mathbb{H}_j$ and $\acute{\acute{r}}_j(x) = r(x) + ((h_j^*)(x)) \in \mathbb{H}_j^*$. Then the decomposition $\Phi^{-1}(r(x)) \in R_t$ is

$$(r_1(x^{-1}), \dots, r_m(x^{-1}), \acute{\acute{r}}_1(x^{-1}), \acute{r}_1(x^{-1}), \dots, \acute{\acute{r}}_s(x^{-1}), \acute{r}_s(x^{-1})).$$

Proof. for $1 \leq i \leq m$, since $r_i(x) = r(x) + (g_i(x))$, then

$$r_i(x^{-1}) = r(x^{-1} + g_i(x^{-1})$$

Since $g(x)$ is an associate of its reciprocal polynomial, then

$$(g_i(x) = g_i(x^{-1}).$$

Therefore, we have

$$r_i(x^{-1}) = r(x^{-1}) + g_i(x),$$

i.e., the component of $\Phi^{-1}(r(x)) = r(x^{-1})$ in $\mathbb{G}_i$ is $r_i(x^{-1})$
For $1 \leq j \leq t$, we have

$$\acute{r}_j(x^{-1}) = r(x^{-1}) + ((h_j)(x^{-1})).$$

Then

$$\acute{r}_j(x^{-1}) = r(x^{-1}) + ((h_j^*)(x^{-1})),$$

i.e., the component of $\Phi^{-1}(r(x)) = r(x^{-1})$ in $\mathbb{H}_j^*$ is $\acute{r}_j(x^{-1})$. Similarly, the component of $\Phi^{-1}(r(x)) = r(x^{-1})$ in $\mathbb{H}_j^*$ is $\acute{\acute{r}}_j(x^{-1})$. □

An immediate consequence of this lemma is the following theorem which gives the algebraic structure of the dual of a QT code when $\lambda \in \{-1, 1\}$.

Theorem 4.2. Let C be a QT code of length $n = t\ell$ over R and $\lambda \in \{-1, 1\}$. Assume that the decomposition of R_t is as in (3.8) and the corresponding decomposition of C is as in (3.9). Then the decomposition of its dual code is

$$C^{\perp} \cong \bigoplus_{i=1}^{r} \Psi_i(C_i^{\perp \mathbb{G}_i}) \oplus \left(\bigoplus_{j=1}^{t} (\acute{\Psi}_j)^{-1}((\acute{\acute{C}}_j)^{\perp \mathbb{H}_j^*}) \oplus \acute{\Psi}_j((\acute{C}_j)^{\perp \mathbb{H}_j}) \right),$$

where the duality on the left is the duality with respect to the inner product over R, while the dualities on the right are the dualities with respect to the inner products over the respective component rings. For simplicity, we denote $\acute{\acute{C}}_j^{\perp} = (\acute{\Psi}_j)^{-1}((\acute{\acute{C}}_j)^{\perp \mathbb{H}_j^*})$ and $\acute{C}_j^{\perp} = \acute{\Psi}_j((\acute{C}_j)^{\perp \mathbb{H}_j})$. Then we can write C as

$$C^{\perp} \cong \bigoplus_{i=1}^{r} C_i^{\perp \mathbb{G}_i} \oplus \left(\bigoplus_{j=1}^{t} \acute{\acute{C}}_j^{\perp} \oplus \acute{C}_j^{\perp} \right). \tag{3.10}$$

5 New Linear Codes over $\mathbb{Z}_4$

Codes over $\mathbb{Z}_4$, sometimes called quaternary codes as well, have a special place in coding theory. Due to their importance, a database of quaternary codes was introduced in [6] and it is availabe online [10]. Hence we consider the case $q = 4$ to possibly obtain quaternary codes with good parameters.
We now present a theorem which is the basis of the ASR search algorithm (first introduced in [9] and subsequently generalized), which has been very effective in finding new linear codes from the class of QT codes. Our goal is to generalize this theorem to codes over R and adapt the search method for codes over this ring.

Theorem 5.1. Let $C_g = \langle g(x) \rangle$ be a free λ-constacyclic code of length n and minimum distance d where $x^n - \lambda = g(x)h(x)$ and $g(x), h(x) \in R[x]$. In addition, let $C = \langle gf_1, gf_2, \ldots, gf_\ell \rangle$ where $\gcd(f_i, h) = 1$ for $i = 1, 2, \ldots, \ell$. Then C is a QT code of length $n\ell$, dimension $n - \deg(g(x))$, and minimum distance $D \geq d\ell$.

Proof. Since $gh = x^n - \lambda$, it follows that if $h|gf_i$, then $pgf_i = 0$ for all $p \in R[x]$. Further, note that if $pgf_i = 0$ for all $p \in R[x]$, then $pgf_i = (x^n - \lambda)A = ghA$ where $A \in R[x]$. Given that g and $x^n - \lambda$ are monic polynomials, g cannot be a zero divisor. Moreover, $\gcd(f_i, h) = 1$ for $i = 1, 2, \ldots, l$, so $h|gf_i$. Therefore, $pgf_i = 0$ for some i if and only if $h|gf_i$ for all $i = 1, 2, \ldots, \ell$. This implies that $p(gf_1, gf_2, \ldots, gf_\ell) = 0$ if and only if $pgf_i = 0$ for $i = 1, 2, \ldots, \ell$. Since every nonzero codeword in each component has weight greater than or equal to d, any nonzero codeword in P has weight greater than $d\ell$. Since each component of C is the λ-constacyclic code C_g of length n and dimension $n - \deg(g)$, we conclude that C is a QT code of length $n\ell$, dimension $n - \deg(g)$, and minimum distance $D \geq d\ell$. □

We conducted a search over QT codes with generators of the form given in Theorem 5.1. Taking the Gray images of these codes we found 116 new linear codes over $\mathbb{Z}_4$ and some examples are shown in Table 1. All 116 codes have been added to the database [10]. Note that since the QT codes obtained have index 2, $n = 4 \times m$. A $\mathbb{Z}_4$-linear code of length n is often denoted by $(n, 4^{k_1}2^{k_2}, d)$ where d is the minimum Lee distance. We will denoted such a code by $[n, k_1, k_2, d]$. Table 1 below shows the parameters and generators of a sample of these 116 new codes. The parameters of the codes not given in Table 1 are given below and the corresponding generators are available in the database[10].

The parameters of the new $\mathbb{Z}_4$-linear codes found are as follows. [8,0,2,8], [12,0,2,12], [16, 2, 1, 8], [16, 2, 2, 8], [16, 2, 3, 8], [16, 2, 4, 4], [16, 3, 1, 8], [16, 3, 2, 4], [16, 3, 3, 4], [16, 4, 1, 8], [16, 4, 2, 6], [20,0,2,20], [24, 2, 1, 12], [24, 2, 2, 12], [24, 2, 3, 8], [24, 2, 4, 8], [24, 2, 5, 8], [24, 2, 6, 8], [24, 3, 1, 12], [24, 3, 2, 4], [24, 3, 4, 8], [24, 4, 2, 12], [24, 4, 4, 10], [24, 4, 5, 8], [24, 4, 6, 8], [24, 5, 1, 8], [24, 5, 4, 8], [24, 5, 5, 4], [24, 6, 2, 8], [24, 6, 4, 8], [24, 7, 1, 4], [24, 8, 1, 8], [24, 8, 2, 8], [28, 2, 3, 12], [28, 2, 6, 12], [28, 5, 3, 8], [28, 6, 1, 12], [28,0,2,28], [28, 6, 2, 12], [28, 6, 6, 8], [28, 7, 1, 10], [28, 9, 3, 8], [32, 2, 1, 16], [32, 2, 2, 16], [32, 2, 3, 16], [32, 2, 4, 16], [32, 2, 5, 16], [32, 2, 6, 16], [32, 2, 7, 8], [32, 2, 8, 8], [32, 2, 10, 8], [32, 3, 1, 16], [32, 3, 2, 16], [32, 3, 3, 16], [32, 3, 4, 16], [32, 3, 5, 8], [32, 3, 6, 8], [32, 3, 7, 8], [32, 3, 8, 8], [32, 4, 1, 16], [32, 4, 2, 16], [32, 4, 3, 16], [32, 4, 4, 16], [32, 4, 5, 8], [32, 4, 6, 8], [32, 4, 7, 8], [32, 4, 8, 8], [32, 5, 1, 16], [32, 5, 2, 16], [32, 5, 3, 12], [32, 5, 4, 8], [32, 5, 5, 8], [32, 5, 6, 8], [32, 5, 7, 8], [32, 6, 1, 12], [32, 6, 2, 12], [32, 6, 3, 12], [32, 6, 4, 8], [32, 6, 5, 8], [32, 6,

Tableau 3.1: Examples of new $\mathbb{Z}_4$ codes $[n, k_1, k_2, d]$ obtained by Gray maps from 2-QT codes of the form $\langle gf_1, gf_2 \rangle$ over $\mathbb{Z}_4 + u\mathbb{Z}_4$

$[n,k,d]_2$	$x^m - \lambda$	g	f_1	f_2
$[16,2,1,8]$	x^4+3	x^2+2u+1	$x+2u+1$	$x+2u+1$
$[24,2,2,12]$	x^6+1	x^4+3x^2+1	$x+u+2$	$x+u$
$[24,4,6,8]$	x^6+3	$x+u+2$	$x^4+(u+3)x^2+(u+2)x+u+3$	$x^4+3ux^3+(2u+1)x+u+2$
$[24,8,2,8]$	x^6+2	$x+u+2$	$x^4+ux^3+(u+2)x^2+(3u+3)x+2u+1$	$x^4+(3u+1)x^3+(u+2)x^2+(u+3)x+3u+3$
$[28,6,2,12]$	x^7+3u	x^3+2ux^2+x+3u	$x^3+(2u+2)x^2+(u+2)x+u+3$	$x^3+(3u+1)x^2+(2u+2)x+1$
$[32,2,6,16]$	x^8+3	$x^4+2ux^2+(2u+2)x+2u+3$	$x^3+3ux^2+(2u+3)x+u+2$	$x^3+ux^2+3x+3u+2$
$[36,12,4,10]$	x^9+u	$x+u$	$x^7+(3u+2)x^6+(u+2)x^5+x^4+2ux^3+2x^2+(2u+1)x+u+1$	$x^7+2x^6+(2u+1)x^5+(u+3)x^4+(u+1)x^3+(3u+3)x^2+2ux+u+2$

6, 8], [32, 6, 7, 8], [32, 6, 8, 4], [32, 7, 1, 8], [32, 7, 2, 8], [32, 7, 3, 8], [32, 7, 4, 8], [32, 7, 5, 8], [32, 7, 6, 4], [32, 7, 7, 4], [32, 8, 1, 12], [32, 8, 2, 8], [32, 8, 3, 8], [32, 8, 4, 8], [32, 8, 5, 8], [32, 8, 6, 8], [32, 9, 1, 8], [32, 9, 2, 8], [32, 9, 3, 8], [32, 9, 4, 8], [32, 10, 1, 8], [32, 10, 2, 8], [32, 10, 3, 8], [32, 11, 1, 8], [32, 12, 1, 8], [36, 2, 4, 12], [36, 4, 1, 12], [36, 4, 2, 12], [36, 5, 1, 12], [36, 10, 6, 4], [36, 12, 1, 10], [36, 12, 2, 10], [36, 12, 4, 10], [36, 13, 1, 10], and [36, 14, 2, 8].

Chapter 4

LCD Codes and LCP of Codes

1 Introduction

Linear Complementary Dual (LCD) codes and Linear Complementary Pair (LCP) of codes have been intensively studied in literature due to their cryptographic applications [13], [44]. They are used in protection against side channel (SCA) and fault injection (FIA) attacks. A pair of linear codes (C,D) over $\mathbb{F}_q$ of length n is called LCP if $C \oplus D = \mathbb{F}_q^n$. When $D = C^{\perp}$, C is called an LCD code. In this context the security parameter for LCP of codes (C, D) is defined to be the minimum of the minimum distances of C and $D^{\perp}$, i.e. it is $mind(C), d(D^{\perp})$. For the LCD case, this parameter is simply $d(C)$ since $D^{\perp} = C$.

From now on we focus on giving cryptographic motivation on LCD and LCP of codes. We also provide some important results on these codes accordingly for the rest of this section.

1.1 Construction of LCD Codes over R

A linear codes with complementary dual (LCD) code is defined as a linear code C whose dual code $C^{\perp}$ satisfies $C \cap C^{\perp} = 0$, that is, $Hull(C) = C \cap C^{\perp} = 0$.

LCD codes have been shown to provide an optimum linear coding solution. For LCD codes over R, we have the following result due to Massey [43].

Proposition 9. *If G is a generator matrix for an $[n, k, d]$ linear code C over $\mathbb{Z}_q$, then C is an LCD code if and only if the $k \times k$ matrix GG^t be non-singular.*

Theorem 1.1. If G is a generator matrix for a linear code C over R , then C is an LCD code if and only if GG^t is non-singular.

Proof. The generator matrix of C can be expressed in canonical formas

$$\begin{pmatrix} \epsilon_1 G_1 \\ \epsilon_2 G_2 \end{pmatrix}$$

Since the ϵ_1 and ϵ_2 are idempotents, a simple calculation gives

$$GG^t = \begin{pmatrix} \epsilon_1 G_1 G_1^t & 0 \\ 0 & \epsilon_2 G_2 G_2^t \end{pmatrix}$$

From the above proposition, a necessary and sufficient condition for a code over $\mathbb{Z}_q$ with generator matrix G_i to be LCD is that GG^t be non-singular. Hence the proof follows from the generator matrix given in the above matrix. □

Theorem 1.2. Let $\lambda \in \{\pm 1\}$ and C be a λ-constacyclic code of length n over $\mathbb{Z}_q$ with $C = \langle g(x) \rangle$. Let $h(x) \in \mathbb{Z}_q[x]$ with $h(x)g(x) = x^n - \lambda$. Then,

- C is an Euclidean LCD code $\Leftrightarrow$ gcd $(g, h^*) = 1$. (Here, gcd (g, h^*) represents the greatest common divisor of g and h^*.)
- Let q be an even power of a prime number. Then, C is a Hermitian LCD code $\Leftrightarrow$ gcd $(g, h^*) = 1$. (For $a(x) = \sum a_i x^i, a(x) = \sum a_i^q x^i$.)

Definition 1.1. A linear code C over R is called an Euclidean (resp. Hermitian) LCD code if $C \cap C^{\perp} = 0$ (resp, $C \cap C^{\perp h} = 0$).

Lemma 1.3. Let $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ is a LCD code over $\mathbb{Z}_{p^m} + v\mathbb{Z}_{p^m}$ if and only if C_1 and C_2 are LCD codes of length n over $\mathbb{Z}_{p^m}$.

Proof. The dual of $C = \epsilon_1 C_1 \oplus \epsilon_2 C_2$ is $C^{\perp} = \epsilon_1 C_1^{\perp} \oplus \epsilon_2 C_2^{\perp}$

$$\text{Hull}(C) = \epsilon_1 \left(C_1 \cap C_1^{\perp} \right) \oplus \epsilon_2 \left(C_2 \cap C_2^{\perp} \right)$$

Then we have,

$$\text{Hull}(C) = 0 \text{ if and only if } C_1 \cap C_1^{\perp} = 0 \text{ and } C_2 \cap C_2^{\perp} = 0.$$

□

In the next, the construction of LCD codes over $\mathbb{Z}_q + v\mathbb{Z}_q$ are given.

Theorem 1.4. A λ-constacyclic code $C = \langle \epsilon_1 g_1(x) + \epsilon_2 g_2(x) \rangle$, is an Euclidean LCD code (resp. Hermitian LCD code) over $\mathbb{Z}_q + v\mathbb{Z}_q$ if and only if GCD $\left(g_i(x), h_i^*(x)\right) = 1$ (resp. GCD $\left(g_i(x), \left(h_i^*\right)(x)\right) = 1\right)$ for $i = 1, 2$. Where $g_i(x)$ and $h_i^*(x)$ in $\mathbb{Z}_q[x]$ and $g_i(x)$ is a generated polynomial such a condition above for $\lambda \in \{-1, 1\}$

2 Cryptographic Motivation on LCD and LCP of Codes

Definition 2.1. pair of linear codes (C, D) in R^n is called a linear complementary pair (LCP) of codes if

$$C \oplus D = R^n.$$

In the case $D = C^\perp$, C is referred to as a linear complementary dual (LCD) code over R.

Recent studies have shown that LCD and LCP of codes help to improve the security of the information (processed by sensitive devices), especially against side-channel attacks (SCA) and fault injection attacks (FIA). The aim is to produce an LCP of codes (C,D) which has a security parameter as high as possible. Let us explain how LCD codes are used in the FIA.
Let $x \in \mathbb{F}_q^k$ be our sensitive data. For a $k \times n$ matrix G of rank k, we code our information to $xG \in \mathbb{F}_2^n$. Then we add an $(n-k)$ bit "mask" y via encoding it with a $(n-k) \times n$ matrix H of rank $(n-k)$: yH - encoded mask. So, we work with $z = xG + yH$ and try not to reveal x at any point. Let C and D be length n codes with generating matrices G and H, respectively.
Assume that $D = C^\perp$ and the two codes satisfy $C \oplus C^\perp = \mathbb{F}_2^n$ (i.e. $C \cap C^\perp = 0$). i.e a code C is an LCD code. Here we need the following characterization by Massey in [20].

Theorem 2.1. Let C be a linear code with a generator matrix G and a parity-check matrix H. Then C is an LCD code iff GG^T is non-singular iff HH^T is non-singular.

Note that one can recover both the sensitive info x and the mask y from z as follows:

$$zG^t(GG^t)^{-1} = (xG + yH)G^t(GG^t)^{-1}$$

$$= xGG^t(GG^t)^{-1} + yHG^t(GG^t)^{-1} = x$$

$$zH^t(HH^t)^{-1} = y$$

Suppose one inserts an error ϵ into z to observe the system statistically, with the hope of reaching x. This is called FIA. Since $C \oplus C^{\perp} = \mathbb{F}_2^n$, we have $\epsilon = eG + fH$ for some e and f. So, the corrupted word is $z + \epsilon$. We want to detect if there is such an attack but we do not want to reveal x. Check y during the process:

$$(z+\epsilon)H^t(HH^t)^{-1} = y + f = y \Longleftrightarrow f = 0$$

So the attack may be undetected if $f = 0$ in ϵ. In this case $\epsilon = eG \in C$. Therefore, set $d(C)$ (security parameter) as high as possible so that FIA is only successful when a high weight codeword is inserted.
The definition of the security parameter for LCP of codes is as follows:

Definition 2.2. The security parameter of an LCP (C, D) is defined to be $min\{d(C), d(D^{\perp})\}$. For the LCD case, this parameter is simply $d(C)$, since $D^{\perp} = C$.

In the following we give the construction of LCP constacyclic codes.

2.1 Construction of LCP Constacyclic Codes

Definition 2.3. An R-module C of rank k is projective if there is an R-module M such that R^n and $C \oplus M$ are isomorphic (as R-modules).

Remark. Note that, with the notation in the above definition, if C and D are two R-modules and $C \oplus D$ is a free R-module, then both C and D are projective modules.

Lemma 2.2. If (C, D) are LCP codes in R^n, then both C and D are free modules (codes).

Proof. Note that by definition (being direct summands of the free module R^n), both C and D are projective modules over R. By [62], any projective module over a commutative semi local ring is free. □

Theorem 2.3. Let C and D be free λ-constacyclic codes of length n over R^n with the generator polynomials $g(x)$ and $h(x)$, respectively. Then (C, D) is LCP if and only if $h(x) = (x^n - \lambda)/g(x)$ and $\gcd(g(x), h(x)) = 1$.

Proof. The intersection of C and D has generator polynomial $\operatorname{lcm}(g(x), h(x))$. For a trivial intersection, the least common multiple must be $x^n - \lambda$. If $C + D = R^n = R[x]/\langle x^n - \lambda \rangle$, then $1 \equiv a(x)g(x) + b(x)h(x) \mod x^n - \lambda$ for some $a(x), b(x) \in R[x]$. A non-trivial common divisor for g and h would contradict this congruence, hence $\gcd(g, h) = 1$. These two observations together imply in particular that $h(x) = (x^n -$

$\lambda)/g(x)$. For the converse, g and h being relatively prime implies that $C + D = R[x]/\langle x^n - \lambda\rangle$. This, combined with the assumption $h(x) = (x^n - \lambda)/g(x)$ implies that $\mathrm{lcm}(h, g) = x^n - \lambda$, which yields $C \cap D = \{0\}$. □

Corresponding scheme of constacyclic codes in terms of generator polynomials when (C, D) is LCP of codes would be as follows :

$$C^{\perp} \longleftrightarrow C \longleftrightarrow D \longleftrightarrow D^{\perp}$$

$$h^*(x) \longleftrightarrow g(x) \longleftrightarrow h(x) \longleftrightarrow g^*(x)$$

where $h(x) = (x^n - \lambda)/g(x)$.

Remark. In the case $\gcd(p, n) = 1$, the polynomial $x^n - \lambda$ is separable hence $\gcd(x^n - \lambda)/g(x), g(x)) = 1$. Therefore, the above condition for (C, D) to be LCP simply reduces to $h(x) = (x^n - \lambda)/g(x)$.

Remark. Theorem 2.3 generalizes the result of Yang and Massey on the characterization of LCD cyclic codes ([60]). Note that $\lambda = 1$ in this case. A cyclic code C being LCD means $(C, C^{\perp})$ is LCP. If C has a generator polynomial $g(x)$, then a generator polynomial of $C^{\perp}$ is $h^*(x)$ for $h(x) = (x^n - \lambda)/g(x)$. Theorem 2.3 yields $\left(\dfrac{x^n - \lambda}{g(x)}\right)^* = \dfrac{x^n - \lambda}{g(x)}$, which is equivalent to $g(x)$ being self-reciprocal as stated in [60].

Now, we give some examples of LCP codes.

Example 2.1. Let $g = x^4 + x^3 + (3u + 1)x^2 + (2u + 1)x + u + 2 | x^6 - 3 - 2u$ and $h = \frac{x^6 - 3 - 2u}{g} = x^2 + 3x + u$. Then (C, D) is an LCP of codes where $C = \langle g\rangle$ whose Gray image has the parameters $[12, 4, 0, 6]$ and $D = \langle h\rangle$ whose Gray image has the parameters $[12, 4, 0, 3]$.

Example 2.2. let $g = x^3 + (u + 2)x^2 + 2x + u + 2 | x^7 - 2 - 3u$ and $h = \frac{x^7 - 2 - 3u}{g}$. Then (C, D) is an LCP code where $C = \langle g\rangle$ whose Gray image parameters are $[14, 8, 0, 4]$ and $D = \langle h\rangle$ whose Gray image parameters are $[14, 6, 0, 6]$.

The previous results lead to the following important conclusion.

Theorem 2.4. If (C, D) are free λ-constacyclic LCP of codes, then C and $D^{\perp}$ are equivalent.

Proof. By Theorem 11, if $g(x) = g_0 + g_1 x + \ldots + x^k$ is the (standard) generator polynomial of C, then the dual $D^{\perp}$ of the complementary free λ-constacyclic code is generated by

$$g^*(x) = g_0^{-1}x^k g(x^{-1}).$$

The generator matrices of C and $D^\perp$ are

$$G_C = \begin{pmatrix} g_0 & g_1 & \dots & 1 & 0 & \dots & \\ 0 & g_0 & g_1 & \dots & 1 & 0 & \dots \\ \vdots & & \vdots & & & \vdots & \\ 0 & \dots & 0 & g_0 & g_1 & \dots & 1 \end{pmatrix},$$

and

$$G_{D^\perp} = g_0^{-1} \begin{pmatrix} 1 & g_{k-1} & \dots & g_1 & g_0 & 0 & \dots & & \\ 0 & 1 & g_{k-1} & \dots & g_1 & g_0 & 0 & \dots & \\ \vdots & & \vdots & & & & \vdots & & \\ 0 & \dots & 0 & & 1 & g_{k-1} & \dots & g_1 & g_0 \end{pmatrix}.$$

The codes generated by these matrices are equivalent (up to a multiplication by a nonzero scalar in each coordinate), under the coordinate permutation that sends the ith coordinate to the $(n-1-i)$th coordinate for $0 \le i \le n-1$. □

Hence, finding the best λ-constacyclic LCP of codes (C, D) and finding the best λ-constacyclic codes are equivalent problems.

Appendix

1 Mathematics for codes

1.1 Ring Theory

Starting from number theory to the modern algebraic geometry, ring has an importance part in the pure algebra and applied algebra. They are important in the number theory, cryptology, and many types of another a mathematical sections. A multiplication ring has a multiplication identity, and it is also commutative. Family of the rings were always chosen for a particular application, with understanding that all the finite commutative rings was being direct products of the local ring by Chinese Remainder Theorem. Thus, in this study we are studying codes over rings, and using the assumption that all the rings work like the alphabets to the codes in a finite Frobenius ring. There is now a rapidly expanding literature on codes over various ring families [27] and [25] .The binary field was largely used as the alphabet in coding theory. The alphabet, on the other hand, was applied to finite fields quickly and effectively. Rings and codes could be communicate through two an important ways. In the first way, a ring structure can have the alphabet to the any codes, including finite field. In second way, some rings could become an ideal or even a module over through the code.

1.2 Finite Commutative Rings

Finite commutative ring theory is a fast-developing subject and has recently been seen to have important applications in theoretical areas like combinatorics, Finite Geometries and the Analysis of Algorithms. Moreover, in the last twenty years, there has been a growing interest in application of commutative rings to Algebraic Cryptography and Coding Theory. In fact, several codes over finite fields, which are widely used in Information and Communication Theory, have been investigated as images of codes over Galois rings (especially over the ring of integers modulo 4). On the one side, applied mathematical research has motivated a more systematic analysis of Finite Commutative Algebra; on the other side, pure Mathematics has offered innovative tools in Coding Theory. This work is not intended as an exhaustive survey of all topics of either Finite Commutative Algebra or Coding Theory over finite rings. Mc Donald's classical reference (see [43]) offers a more theoretical approach to the algebraic point of view of the subject. MacWilliams' and Sloane's book or van Lint's book just to mention a few-are standard references for codes over finite fields, whereas [48] collects some of the latest articles concerning codes over Galois rings.

Definition 1.1. *A ring A is a nonempty set, endowed with two laws of internal composition, often denoted by $(+)$ and $(.)$ (by analogy to integers) such as:*

- *the set $(A, +)$ is a commutative group.*
- *$(.)$ is distributive with respect to $(+)$.*
- *$(.)$ is associative.*

It is about an abelian group, noted additively, on which is defined a second internal law noted multiplicative. This second law is associative and distributive with respect to the first. If, moreover, the second law is commutative then the ring is said to be commutative. And if, the ring A has a neutral element for the second law (often noted 1_A), then A is said to be unitary.

In the following we consider $(A, +, .)$ a unitary ring, x and y two elements of A.

A is said to be integral, if it has no divisors of zero, in other words, if $x.y = 0$ implies that x is zero or y is zero.

In the case where A is not integral, x is called a left divisor and y is a right divisor. If A is abelian the two notions coincide and we will simply speak of divisors of zero.

The nilpotent elements are a type of divisors of zero, we define them as follows: we always consider the ring A, and x element of A, we say that x is nilpotent if there exists an integer n such that $x^n = 0$.

In mathematics and computer science, the concept of idempotents essentially means that an operation has the same effect, whether it is applied once or several times. An element of x is said to be idempotent if $x^2 = x$. Note that 0_A and 1_A are trivial idempotents.

Let B be a finite ring, a ring homomorphism is a map g, from A to B, satisfying the following three conditions, for all x, y in A:

- $g(x+y) = g(x) + g(x)$.
- $g(x.y) = g(x).g(y)$.
- $g(1_A) = 1_B$.

We speak of endomorphism if $A = B$, of isomorphism if the map g is a one to one and of automorphism if there is bijectivity and the equality of the two sets.

Let B be a subset of A, $(B, +, .)$ is a subring of A if $(B, +, .)$ is a ring such as 1_A is the neutral element of the "." law on B.

A part I of A is said to be an ideal to the left of A, if I is a subgroup of A, and for all x of I and a of A, the product $a.x$ is an element of I. In the same way we can define an ideal on the right, but instead of requiring that $a.x$ be in A, it is necessary to require that $x.a$ be in A. In the commutative case the two notions are confused and we then speak of ideal simply. If $1 \in I$ then $I = A$.

A ring A is said to be semi-simple if it is isomorphic to a fields product. Let I be a proper ideal of A (different from A), I is said to be maximal if for any ideal J of A we have: $I \subset J$ then $J = A$ or $I = J$.

Remark. If an ideal is a sub-ring, then $1_A \in I$ and therefore $1_A.x \in I$ (according to the definition of an ideal), thus $A = I$.

Theorem 1.1. (Krull) *Any ideal $I \neq A$ of a commutative ring A is included in a maximal ideal.*

Definition 1.2. *Let A be an abelian ring, and I an ideal of A, I is a principal ideal if $I = aA$ with a in A.*

This definition brings us directly to that of a principal ring. A ring is said to be principal if it is integral and if all of its ideals are principals.

property 1. *A finite commutative ring with unity is called*

1. *A local ring if it has a unique maximal ideal.*
2. *A Galois ring if all its zero-divisors including 0 (or equivalently, all its non-units) form an*

ideal generated by some prime number p.

3. *A finite chain ring, $\mathcal{R}$, is a finite commutative local ring such that its ideals are linearly ordered by inclusion, i.e., if γ is a fixed generator of the maximal ideal of $\mathcal{R}$ and e is the nilpotency of γ, then the ideals of $\mathcal{R}$ form a chain*

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

2 Quotient rings

The study of quotient rings requires an introduction to equivalence relations.

Definition 2.1. *A binary relation R on a set E is defined by a part E_R of $E \times E$ such that aRb (a is in relation to b) if and only if $(a, b) \in E_R$.*

A binary relation R on a set E is an equivalence relation if and only if R is reflexive, symmetric and transitive.

For any element x of E, we call the equivalence class of x modulo R, denoted by $\bar{x}$, the set $\bar{x} = \{y \in E \mid yRx\}$.

The set of equivalence classes of x modulo R is called the quotient set of E by R, and denoted E/R.

Solving some simple arithmetic equations on $\mathbb{Z}$ can be a little more complex on $\mathbb{Z}/b\mathbb{Z}$, and the primality of b plays a very decisive role. If b is a prime number then $\mathbb{Z}/b\mathbb{Z}$ is a field which makes it possible to benefit from the richness of this structure.

Definition 2.2. *Let E and F be two sets, and f be a map of E in F. If A is a part of E and B is a part of F, such that $\forall a \in A$ we have $f(a) \in B$, then f is the map induced by f on A.*

Let I be an ideal of A, we define the quotient ring A/I as the set classes of equivalences of the relation induced by I on A. Hence the proposition:

Proposition 10. *We consider the commutative ring A, and I an ideal of A. The quotient ring A/I is a ring for addition and induced multiplication, such that: $\overline{a} + \overline{b} = \overline{a+b}$, and $\overline{a}.\overline{b} = \overline{a.b}$.*

We immediately deduce the following theorem.

Theorem 2.1. *We consider the ring morphism $f : A \to B$, there is a unique morphism of rings:*

$$g : A/\ker(f) \to B$$

$$g \mapsto g \circ p$$

Where p is the canonical surjection from A into ker (f)*. Moreover* $A/ker\ (f)$ *is isomorphic to Im* (f).

An ideal I is said to be prime, if A/I is integral.

Proposition 11. *Let I be an ideal, I is maximal if and only if* A/I *is a field.*

In ring theory, the Chinese remainder theorem is fundamental. It allows, among other things, to perform the rapid multiplication of polynomials.

Theorem 2.2. (Chinese RemainderTheorem) Let R be a ring, and let $I1, I2$ be ideals of R such that $I1 + I2 = R$. Then

$$R/(I_1) \cap (I_2) \cap (I_3) \cap \cdots \cap (I_r) = R/(I_1) \oplus R/(I_2) \oplus R/(I_3) \oplus \cdots \oplus R/(I_r)$$

2.1 Modules

Definition 2.3. Let R be a ring. A right R-module is a set M which has addition and scalar multiplication on the right by elements of R; thus if $m, n \in M$ and $r \in R$, there are element $sm + n \in M$ and $mr \in M$. Under addition, M must be an Abelian group. The scalar multiplication must

- $m(rs) = (mr)s$ for all $m \in M$ and $r, s \in R$,
- $(m + n)r = mr + nr$ and $m(r + s) = mr + ms$ for all $m, n \in M$ and $r, s \in R$,
- $m1 = m$ for all $m \in M$ and $r, s \in R$, where 1-is the identity element in R.

A left R-module-is defined similarly, except that we have a left scalar multiplication: if m is in M and r in R, then $rm \in M$. The axioms are

- $(rs)m = r(sm)$ for all $m \in M$ and $r, s \in R$,
- $r(m + n) = rm + rn$ and $(r + s)m = rm + sm$ for all $m, n \in M$ and $r, s \in R$,
- $1m = m$ for all $m \in M$ and $r, s \in R$, where 1-is the identity element in R.

Example 2.1. A ring R can be viewed as a right R-module, using its addition and multiplication as a ring to define its addition and scalar multiplication as a right module. More generally, any right ideal of R is a right R-module, the zero ideal being thought of as the zero module $0 = 0$. Likewise, left ideals of R can be considered to be left R-modules.

Definition 2.4. Let M be an R- module. A subset $N \subseteq M$ is said to be a submodule of M if:

- N is a subgroup of $(M, +)$.
- For all $r \in R$, and for all $m \in N$ one has $rm \in N$.

2.1.1 Free module

Definition 2.5. Let M be an R- module and let subset $N \subseteq M$. Then

- N is linearly independent, that is

$$r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0 \implies r_1 = r_2 = \cdots = r_n = 0$$

for $r_i \in R$ and distinct $x_1, x_2, \ldots, x_n \in N$.

- N spans M if every $m \in M$ can be written as

$$m = r_1x_1 + r_2x_2 + \cdots + r_nx_n$$

where $r_1, r_2, \ldots r_n \in R$ and $x_1, x_2, \ldots x_n \in N$.

- N is a basis of M if M is linearly independent and N spans M.

Definition 2.6. Let N be a subset of an R-module M. If M has a nonempty basis N, then M is a free R-module on the set N.

Example 2.2.

R-module R has the base 1. Then R is a free R-module.

The vector space $\mathbb{F}$ over a field F is a free F-module.

Proposition 12. *If M is a finitely generated free R-module, then the cardinality of any basis of M is finite. Furthermore, any two bases have the same cardinality.*

Definition 2.7. Let M be a finitely generated free R-module. Then the cardinality of any basis of M is called the rank of the free module M.

Conclusion and future works

In this thesis, We have studied some structural properties of some linear codes over Zq to find the structure of some codes over R, at the beginnig, we investigate some properties of constacyclic codes and QT codes over the ring $R = \mathbb{Z}_q + v\mathbb{Z}_q$, $v^2 = 1$ and $q = p^m$ for a prime p and a positive integer m. It is shown that the Gray image of a free constacyclic code over R is also free over $\mathbb{Z}_q$. The decomposition of a QT code and its dual code are obtained. Considering the case $q = 4$, we obtained dozens of new linear codes over $\mathbb{Z}_4$ from Gray images of QT codes over R. Based on our survey and study, now we present a few open directions for future investigation .

- It would be an interesting problem to determine 1-generator QT codes over this ring.
- Another interesting problem would be to study the characterizations for LCP of QT codes over this ring.
- the notion of ℓ-intersection codes introduced in [32] can be extended to this ring.

Bibliography

[1] R. Ackerman and N. Aydin. New quinary linear codes from quasi-twisted codes and their duals. *Appl. Math. Lett.*, 24:512–515, 2011.

[2] A-N. Aleksandr. Kerdock's code in cyclic form. *Diskret. Mat.*, 1(4):123–139, 1989.

[3] M-C-V. Amarra and F-R. Nemenzo. On $(1-u)$-cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. *Applied Mathematics Letters*, 21:1129–1133, 2008.

[4] E. F. Assmus and J. D. Key. *Designs and Codes: An Update*. Springer, Boston, MA, 1996.

[5] E-F. Assmus and H-F. Mattson. Error-correcting codes and an axiomatic approach. *Information and Control*, 6:315–330, 1963.

[6] N. Aydin and T. Asamov. *A Database of $\mathbb{Z}_4$ Codes*, volume 34 (1-4), pp. 1–12. 2009.

[7] N. Aydin, A. Dertli, and Y. Cengellenmis. On some constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2-1\rangle$, their $\mathbb{Z}_4$ images, and new codes. *Des. Codes Cryptogr.*, 86:1249–1255, 2018.

[8] N. Aydin and D.K. Ray-Chaudhuri. Quasi-cyclic codes over z4 and some new binary codes. *IEEE Trans. Inf. Theory*, 48:2065–2069, 2002.

[9] N. Aydin, I. Siap, and D. K. Ray-Chaudhuri. The structure of 1-generator quasi-twisted codes and new linear codes. *Des. Codes Cryptogr.*, 24:313–326, 2001.

[10] N. Aydin and B. Yoshino. Database of $\mathbb{Z}_4$ codes, 2023.

[11] A. Bellil, K. Guenda, N. Aydin, P. Liu, and & T. Aaron Gulliver. Constacyclic and quasi-twisted codes over $\mathbb{Z}_q[u]/\langle u^2-1\rangle$ and new $\mathbb{Z}_4$-linear codes. *Advances in Mathematics of Communications*, 2023.

[12] M. Bhaintwal and S. K. Wasan. On quasi-cyclic codes over $\mathbb{Z}_q$. *Appl. Algebra Eng. Commun. Comput.*, 20:459–480, 2009.

[13] S. Bhasin, J-L. Danger, S. Guilley, Z. Najm, and X. T. Ngo. Linear complementary dual code improvement to strengthen encoded circuit against hardware trojan horses. In *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages May 5–7, 2015.

[14] R-E. Blahut. *Algebraic codes on lines, planes, and curves*. Cambridge University Press, Cambridge, An engineering approach, 2008.

[15] I-F. Blake. Codes over certain rings. *Information and Control*, 20:396–404, 1972.

[16] I-F. Blake. Codes over integer residue rings. *Information and Control*, 29(4):295–300, 1975.

[17] C. Carlet and S. Guilley. Complementary dual codes for counter-measures to side-channel attacks. *Advances in Mathematics of Communications*, 10:131–150, 2016.

[18] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya, and P. Solé. On linear complementary pairs of codes. *IEEE Trans. Inf. Theory*, 64:6583–6589, 2018.

[19] R. Dasklov and P. Histrov. Some new quasi-twisted ternary linear codes. *J. Algebra Comb. Discret. Struct. Appl.*, 2:211–216, 2016.

[20] M. Demazure. *Cours D'Algèbre : Primalité, Divisibilité, Codes*. Cassini, Paris, 1997.

[21] H. Q. Dinh and S. R. López-Permouth. Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inform. Theory*, 50:1728–1744, 2004.

[22] H. Q. Dinh, A. K. Singh, N. Kumar, and S. Sriboonchitta. On constacyclic codes over $\mathbb{Z}_4[v]/\langle v^2 - v\rangle$ and their gray images. *IEEE Commun. Lett.*, 22:1758–1761, 2018.

[23] H.Q. Dinh. Constacyclic codes of length 2^s over galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inf. Theory*, 55:1730–1740, 2009.

[24] H.Q. Dinh. Constacyclic codes of length p^s over ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *J. Algebra*, 324:940–950, 2010.

[25] S.T. Dougherty. *Algebraic Coding Theory over Finite Commutative Rings*. Springer International Publishing, Scraton, PA, USA, 2017.

[26] S.T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, and P. Solé. Type iv self-dual codes over rings. *IEEE Transactions on Information Theory*, 45(7):2345–2360, 1999.

[27] S.T. Dougherty and H. Liu. Independence of vectors in codes over rings. *Designs, Codes and Cryptography*, 51:55–68, 2009.

[28] J. Gao, F. Fu F, and Y. Gao. Some classes of linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ and their applications to construct good and new $\mathbb{Z}_4$-linear codes. *Appl. Algebra Eng. Commun. Comput.*, 28:131–153, 2017.

[29] J. Gao, F-W. Fu, L. Xiao, and R-K. Bandi. Some results on cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$. *Discrete Math. Algorithms Appl.*, 7:1550058, 2015.

[30] J. Gao, F. Ma, and F. Fu. Skew constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$. *Appl. Comput. Math.*, 6(3):286–295, 2017.

[31] K. Guenda and T. A. Gulliver. Mds and self-dual codes over rings. *Finite Fields Appl.*, 18:1061–1075, 2012.

[32] K. Guenda, T. A. Gulliver, S. Jitman, and S. Thipworawimon. Linear ℓ-intersection pairs of codes and their applications. *Des. Codes Cryptogr.*, 88:133–152, 2020.

[33] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes. *IEEE Trans. Inf. Theory*, 40:301–319, 1994.

[34] 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 Transactions on Information Theory*, 40(2):301–319, 1994.

[35] R. Hill. *A First Course in Coding Theory*. Oxford University Press, US, 1986.

[36] W.C. Huffman and V. Pless. *Fundamentals of Error Correcting Codes*. Cambridge University Press, New York, US, 2010.

[37] Y. Jia. On quasi-twisted codes over finite fields. *Finite Fields Appl.*, 18:237–257, 2012.

[38] G. D. Forney Jr, N. J. Sloane, and M. D. Trott. The nordstrom-robinson code is the binary image of the octacode. In *Coding and Quantization: DIMACS/IEEE workshop*, pages 19–26. Amer. Math. Soc., 1992.

[39] F. J. Macwilliams and N.J.A Sloane. *The theory of error correcting-codes*. Benjamin, Inc. Amsterdam, North-Holland, 1977.

[40] E. Martinez-Moro and S. Szabo. On codes over local frobenius non-chain rings of order 16. *Noncommutative Rings Applic.*, 634:227–241, 2015.

[41] E. Martinez-Moro, S. Szabo, and B. Yildiz. Linear codes over $\mathbb{Z}_4[x]/\langle x^2+2x\rangle$. *Int J. Info. Coding Theory*, 3:78–96, 2015.

[42] J-L. Massey. Linear codes with complementary duals. *Discrete Math*, 106/107:337–342, 1992.

[43] B-R. McDonald. *Finite Rings with Identity*. Marcel Dekker: New York, NY, 1974.

[44] X. T. Ngo, S. Bhasin, J. L. Danger, S. Guilley, and Z. Najm. Linear complementary dual code improvement to strengthen encoded circuit against hardware trojan horses. In *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust*, pages 82–87, May 2015.

[45] G.H. Norton and A. Sâlâgean. Strong gröbner bases and cyclic codes over a finite-chain ring. *Electron. Notes Discret. Math.*, 6:240–250, 2001.

[46] M. Ozen, F. Z. Uzekmek, N. Aydin, and N. T. Ozzaim. Cyclic and some constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2-1\rangle$. *Finite Fields Appl.*, 38:27–39, 2016.

[47] R. Pellikaan, Xin-Wen Wu, S. Bulygin, and R. Jurrius. *Error-correcting codes and cryptology*, volume 10. 2012.

[48] A. Pott, P-V. Kumar, T. Helleseth, and D. Jungnickel. *Proceedings of the NATO Advanced Study Institute on Difference Sets and Sequences and their Correlation Properties*. Kluwer Academic Publishers, 1999.

[49] S. Roman. *Coding and Information Theory*. Graduate Texts in Mathematics, 134. Springer-Verlag, New-York, 1992.

[50] S. Roman. *Advanced Linear Algebra*. Springer-Verlag, New York, 3rd edition, 2008.

[51] S. Rudolf. A mathematical theory of communication. *Towards a Fuzzy Information Theory*, pages 1332–1337, 2009.

[52] A. Saleh and M. Esmaeili. Some classes of quasi-twisted codes over finite chain rings. *J. Applied Math. Comput.*, 57:629–646, 2018.

[53] C. E. Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27:379–423, 1948.

[54] M. Shi, L. Qian, L. Sok, N. Aydin, and P. Solé. On constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2-1\rangle$. *Finite Fields Appl.*, 45:86–95, 2017.

[55] The University of Sydney, Computer Algebra Group. Magma computational al-

gebra system, 2008. Accessed 4 November 2008.

[56] Z. X. Wan. *Lectures on Finite Fields and Galois Rings*, volume 10. 2003.

[57] Z.X. Wan. *Quaternary Codes*. World Scientific, Singapore, 1997.

[58] Z.X. Wan. Cyclic codes over galois rings. *Algebra Colloq.*, 6:291–304, 1999.

[59] S. S. Woo. Free cyclic codes over finite local rings. *Bull. Korean Math. Soc.*, 43:723–735, 2006.

[60] X. Yang and J. L. Massey. The condition for a cyclic code to have a complementary dual. *Discrete Math.*, 126:391–393, 1994.

[61] B. Yildiz and S. Karadeniz. Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$: Macwilliams identities, projections, and formally self dual codes. *Finite Fields Appl.*, 27:24–40, 2014.

[62] H. Yukitoshi. Projective modules over semilocal rings. *Tohoku Math. J.*, 14:205–211, 1962.

[63] S. Zhu, Y. Wang, and M. Shi. Some results on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. *IEEE Trans. Inf. Theory*, 56:1680–1684, 2010.