The Islamic University of Gaza
Deanery of Higher Studies
Fuculty of Science
Departemnt of Mathematics

On Codes Over The Rings

$$F_q + uF_q + vF_q + uvF_q$$

M.Sc. Thesis

Presented by
Ibrahim M. Yaghi

Supervised by
Dr. Mohammed M. AL-AShker

Submitted in Partial Fulfillment of
the Requirements for M.Sc. Degree

2013

Abstract

Codes over finite rings have been studied in the early 1970's [4]. A great deal of attention has been given to codes over finite rings from 1990 [20], because of their new role in algebraic coding theory and their successful applications.

In previous studies, some authors determined the structure of the ring $F_2 + uF_2 + vF_2 + uvF_2$, where $u^2 = v^2 = 0$ and $uv = vu$, also they obtained linear codes, self dual codes, cyclic codes, and consta-cyclic codes over this ring as in [24],[25],[26],[27].

In this thesis, we aim to generalize the previous studies from the ring $F_2+uF_2+vF_2+uvF_2$ to the ring $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p and $u^2 = v^2 = 0$ $uv = vu$, so we obtain the linear codes over $R = F_q + uF_q + vF_q + uvF_q$, then we investigate self dual codes over R and we find that it can be generalized only when q is a power of the prime 2, also we obtain cyclic and consta-cyclic codes over R, and we generalize the Gray map used for codes over $F_2 + uF_2 + vF_2 + uvF_2$, finally we obtain another gray map for codes over R.

Acknowledgements

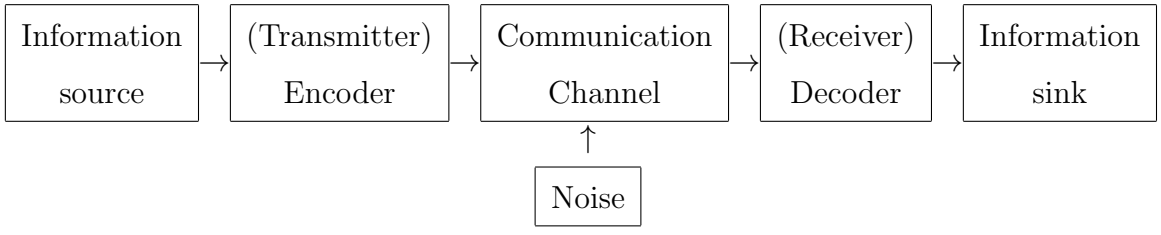
After Almighty Allah, I am grateful to ***my parents*** *for their subsidization, patience, and love. Without them this work would never have come into existence. I am heartily thankful to my supervisor, Dr.* ***Mohammed M. AL-Ashker****, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.*

Lastly, I offer my regards and blessings to all of those who supported me in any respect during the completion of this thesis.

Table of Contents

Introduction

Before 1948, communication was strictly an engineering discipline, with little scientific theory to back it up. In fact, one might even go as far as to liken communication engineering of the time to a black art rather than the hard science it is today.
Claude Shannons 1948 paper "A Mathematical Theory of Communication" [19] gave birth to the twin disciplines of information theory and coding theory. The basic goal is efficient and reliable communication in an uncooperative (and possibly hostile) environment. To be efficient, the transfer of information must not require a prohibitive amount of time and effort. To be reliable, the received data stream must resemble the transmitted stream to within narrow tolerances. These two desires will always be at odds, and our fundamental problem is to reconcile them as best as we can. At an early stage the mathematical study of such questions broke into the two broad areas. Information theory is the study of achievable bounds for communication and is largely probabilistic and analytic in nature. Coding theory then attempts to realize the promise of these bounds by models which are constructed through mainly algebraic means. Shannon was primarily interested in the information theory. Shannons colleague Richard Hamming had been laboring on error-correction for early computers even before Shannons 1948 paper, and he made some of the first breakthroughs of coding theory. The following diagram shows the communication system for transmitting information from a source to a destination through a channel.



the most important part of the diagram, as far as we are concerned is the noise, for without it there would be no need for the theory.

This thesis is organized as follows, we start by recalling background and notations about abstract algebra and coding theory in chapter 1.

In chapter 2, we investigate all the studies that have been made on codes over the ring $F_2+uF_2+vF_2+uvF_2$ where, $u^2 = v^2 = 0$ and $uv = vu$, first we study the main properties of the ring then the structure of linear codes, self dual codes, cyclic and consta-cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$, also the previous studies have found the images of these codes under the gray map and the lee weight through this map.

Chapter 3 is a generalization of chapter 2 from the ring $F_2+uF_2+vF_2+uvF_2$ to the ring $F_q+uF_q+vF_q+uvF_q$ where, q is a power of the prime p and $u^2 = v^2 = 0, uv = vu$, first we study the main properties of the ring then we get the generalized structure of linear codes, self dual codes, cyclic and consta-cyclic codes, also we obtain the generalized gray map and lee weight for these codes, finally we get another gray map for codes over this ring and find the lee weight through this map.

Chapter 1

preliminaries

1.1 Groups,Rings and Fields

Definition 1.1.1. [12] A nonempty set G, together with a binary operation $(*)$ is said to form a group,if for all $a,\ b,\ c \in\ G$, the following axioms are satisfied :

(i) $a * (b * c) = (a * b) * c$.

(ii) There exist an element e (called identity) in G such that,
$a * e = e * a = a$.

(iii) For each $a \in\ G$, *thereexist an element* $a^{-1} \in\ G$ (called inverse), such that,
$a * a^{-1} = a^{-1} * a = e$.

Definition 1.1.2. [12] A group G is called an Abelian group if $a * b = b * a$ for all $a, b \in\ G$.

Definition 1.1.3. [12] A non empty subset S of a group G is said to be a subgroup of G if S forms a group under the binary operation of G.

Theorem 1.1.4. [12] A non empty subset S of a group $(G, *)$ is a sub-group of G if and only if for all $a, b \in S$, $a * b^{-1} \in S$.

Definition 1.1.5. [12] The order of a group is its cardinality.

Definition 1.1.6. [12] A nonempty set R, together with two binary operations addition $(+)$ and multiplication $(.)$ is said to form a ring, if for all $a,\ b,\ c \in\ R$, the following axioms are satisfied :

(i) $a + (b + c) = (a + b) + c$.

(ii) $a + b = b + a$.

(iii) There exist an element 0 (called zero) in R such that,
$a + 0 = 0 + a = a$.

(iv) for each $a \in R$, there exist an element $(-a) \in R$, such that,
$a + (-a) = (-a) + a = 0$.

(v) $a.(b.c) = (a.b).c$.

(vi) $a.(b + c) = a.b + a.c$.
$(b + c).a = b.a + c.a$.

Definition 1.1.7. [12] A ring R is called a commutative ring if $ab = ba$ for all $a, b \in R$. If there exist a unique element $e \in R$ such that,

$$ae = ea = a \text{ for all } a \in R$$

then we say, R is a ring with unity. Unity is generally denoted by 1 (it is also called unit element or multiplicative identity).

Definition 1.1.8. [12] An element a in a ring R with unity, is called invertible (or a unit) with respect to multiplication if there exist $b \in R$ such that $ab = 1 = ba$.

Definition 1.1.9. [12] Let R be a ring. An element $a \neq 0 \in R$ is called a zero-divisor, if there exist an element $b \neq 0 \in R$ such that, $ab = 0$ or $ba = 0$.

Definition 1.1.10. [12] A commutative ring R with unity is called an integral domain if
$ab = 0$ in $R \implies$ either $a = 0$ or $b = 0$. In other words, a commutative ring R with unity is called an integral domain if R has no zero divisors.

Definition 1.1.11. [12] A field is a nonempty set F of elements with two operations $+$ (called addition) and . (called multiplication) satisfying the following axioms. For all $a,\ b,\ c \in F$:

(i) F is closed under $+$ and . i.e., $a + b$ and $a.b$ are in F.

(ii) Commutative laws: $a + b = b + a$, $a.b = b.a$.

(iii) Associative laws: $(a + b) + c = a + (b + c)$, $a.(b.c) = (a.b).c$.

(iv) Distributive law: $a.(b + c) = a.b + a.c$.

Furthermore, two distinct identity elements 0 and 1 (called the additive and multiplicative identities, respectively) must exist and satisfying the following:

(v) $a + 0 = a$ for all $a \in F$.

(vi) $a.1 = a$ and $a.0 = 0$ for all $a \in F$.

(vii) For any a in F, there exists an additive inverse element $(-a)$ in F such that $a + (-a) = 0$.

(viii) For any $a \neq 0$ in F, there exists a multiplicative inverse element a^{-1} in F such that $a.a^{-1} = 1$.

We usually write $a.b$ simply as ab, and denote by F^* the set $F \setminus \{0\}$.

Definition 1.1.12. [12] A ring R with unity is called a division ring or a skew field if all non zero elements of R have multiplicative inverse.

Lemma 1.1.13. [12] A finite integral domain is a field.

Example 1.1.14. [12] Z_p, the set of integers mod p is a field, for a prime integer p.

Subring and the characteristic of a ring

Definition 1.1.15. [12] A non empty subset S of a ring R is said to be a subring of R if S forms a ring under the binary operations of R.

Example 1.1.16. The ring $\big(\mathbf{Z}, +, .\big)$ of integers is a subring of the ring $\big(\mathbf{R}, +, .\big)$ of real numbers.

If R is a ring then $\{0\}$ and R are always subrings of R, called trivial subrings of R.

Theorem 1.1.17. [12] A non empty subset S of a ring R is a sub-ring of R if and only if for all $a, b \in S$, ab, $a - b \in S$.

Definition 1.1.18. [12] Let R be a ring. If there exists a positive integer n such that $na = 0$ for all $a \in R$, then R is said to have finite characteristic and also the smallest such positive integer n is called the characteristic of R.
If no such positive integer exists then R is said to have characteristic zero. Characteristic of R is denoted by char R or $ch(R)$.

Example 1.1.19.

(i) The characteristics of $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ are 0, where
$\mathbf{Q}$ is the set of all rational numbers, $\mathbf{R}$ is the set of all real numbers and
$\mathbf{C}$ is the set of all complex numbers.

(ii) The characteristic of the field Z_p is p for any prime p.

Ideals and Quotient Rings

Definition 1.1.20. [7] A nonempty subset I of a ring R is called a left ideal if

(i) For all $a, b \in I$, $a - b$ belongs *to* I.

(ii) For all $a \in I$ and all $r \in R$, $ra \in I$.

Symmetrically, we define a right ideal, as
A nonempty subset I of a ring R is called a right ideal if

(i) For all $a, b \in I$, $a - b$ belongs *to* I.

(ii) For all $a \in I$ and all $r \in R$, $ar \in I$.

A nonempty subset which is both a left and a right ideal is called an ideal, or sometimes, for the sake of emphasis, a two-sided ideal. In a commutative ring the distinction between a left and a right ideal disappears. From condition (i) above it is clear that every left (or right) ideal is a subring. However, the converse need not be true. For example, in the ring $\mathbf{Q}$ of rational numbers, the set $\mathbf{Z}$ of integers is a proper subring, but not an ideal because $\frac{1}{2} \in \mathbf{Q}$, $3 \in \mathbf{Z}$. But $3.\frac{1}{2} \notin \mathbf{Z}$. In any ring, the set $\{0\}$ consisting of the zero element alone is a two-sided ideal. It is called the zero ideal and denoted by $\{0\}$. Similarly, the whole ring R is a two-sided ideal. If R possesses an identity e, then R is called a unit ideal and is denoted by (e). The two sided ideals $\{0\}$ and R are said to be improper, any ideal other than $\{0\}$ and R is said to be proper.

Theorem 1.1.21. [7] If R is a ring with unity, and I is an ideal of R containing a unit, then $I = R$.

Definition 1.1.22. [7] Let R be a ring and let I be an ideal in R. We define the quotient ring R/I as:
$R/I = \{r + I : r \in R\} = set\ of\ all\ cosets\ of\ I\ in\ R.$

Definition 1.1.23. [7] An ideal $I \neq R$ in a commutative ring R is a prime ideal if $ab \in I$ implies that either $a \in I$ or $b \in I$ for every $a, b \in R$.

Definition 1.1.24. [12] Let R be a ring. An ideal $M \neq R$ of R is called a maximal ideal of R if whenever A is an ideal of R such that, $M \subseteq A \subseteq R$ then either $A = M$ or $A = R$.

Example 1.1.25. [12]

(i) A field F has only two ideals F and $\{0\}$. We can see that $\{0\}$ is the only maximal ideal of F.

(ii) $\{0\}$ in the ring $\mathbf{Z}$ of integers is a prime ideal as $ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a \in \{0\}\ or\ b \in \{0\}$.
It is an example of a prime ideal which is not maximal because $\{0\} \subsetneq 2\mathbf{Z} \subsetneq \mathbf{Z}$.

(iii) $4Z = \{4n : n \in \mathbf{Z}\}$it is a maximal ideal in the ring $2Z$ of even integers.
$4Z$, however, is not a prime ideal in $2Z$ as $2.2 = 4 \in 4Z$ but 2 does not belong to $4Z$, and also is not a maximal ideal in Z because $4\mathbf{Z} \subsetneq 2\mathbf{Z} \subsetneq \mathbf{Z}$.
In fact, $4Z$ is neither a maximal nor a prime ideal in $\mathbf{Z}$.

In the following two theorems we give alternative criterions for an ideal in an arbitrary commutative ring to be prime or maximal.

Theorem 1.1.26. [7] Let R be a commutative ring with unity, and let $I \neq R$ be an ideal in R. Then R/I is an integral domain if and only if I is a prime ideal in R.

Theorem 1.1.27. [12] Let R be a commutative ring with unity. An ideal M of R is a maximal ideal of R if and only if R/M is a field.

Corollary 1.1.28. [7] Every maximal ideal in a commutative ring R with unity is a prime ideal, but the converse is not true.

Definition 1.1.29. [7] An ideal I of a commutative ring R is called a principal ideal if there exists an element $g \in I$ such that $I =< g >$, where

$$< g >= \{rg : r \in R\}.$$

The element g is called a generator of I and I is said to be generated by g.

Definition 1.1.30. [7] A ring R is called a principal ideal ring if every ideal in R is a principal ideal.

Definition 1.1.31. [7] A principal ideal ring which is an integral domain is called a principal ideal domain.

Example 1.1.32. [7] **Z** is a principal ideal domain. Moreover, given any nonzero ideal I of **Z**, the smallest positive integer in I is a generator for the ideal I.

Definition 1.1.33. [12] An element x of a ring R is called nilpotent if there exists some positive integer n such that $x^n = 0$.

No nilpotent element can be a unit (except in the trivial ring $\{0\}$ which has only a single element $0 = 1$). All non-zero nilpotent elements are zero divisors.

Definition 1.1.34. [12] The nilradical of a commutative ring is the set of all nilpotent elements in the ring.

The nilradical is an ideal because the subtraction of any two nilpotent elements is nilpotent, and the product of any element with a nilpotent element is nilpotent.

Definition 1.1.35. [12] A finite ring R is called a chain ring if its ideals are linearly ordered by inclusion.

In particular, this means that any finite chain ring has a unique maximal ideal.

Definition 1.1.36. [3] A local ring is a ring that has a unique maximal ideal.

Definition 1.1.37. [3] A simple ring is a non-zero ring that has no two-sided ideal besides the zero ideal and the ring itself.

Definition 1.1.38. [3] 1. A nonzero left ideal I of a ring R is called simple if it doesn't contain any left ideals besides the zero ideal and the ideal itself.
2. A nonzero right ideal I of a ring R is called simple if it doesn't contain any right ideals besides the zero ideal and the ideal itself.

Homomorphisms and Isomorphisms

Definition 1.1.39. [7] Let R and S be rings (or fields).
A function ψ:$R \longrightarrow S$ is a **ring homomorphism** if for all $a, b \in R$,

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

and

$$\psi(ab) = \psi(a)\psi(b).$$

Definition 1.1.40. [7] An **isomorphism** ψ: $R \longrightarrow S$ is a homomorphism that is one-to-one and onto S.

Definition 1.1.41. [7] Let f:$R \longrightarrow S$ be a homomorphism, we define **kernel** of f by

$$\ker f = \{x \in R : f(x) = 0\}$$

where 0 is the zero of S.

Theorem 1.1.42. [7] If f:$R \longrightarrow S$ is a homomorphism, then

- $\ker f$ is an ideal of R.
- $\ker f =< 0 >$ if and only if f is one-to-one.

Polynomial Rings

Definition 1.1.43. [7] Let R be a ring. A polynomial $f(x)$ with coefficients in R is an infinite formal sum

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + \ldots,$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of i. The $a_i's$ are coefficients of $f(x)$. If for some $i \geq 0$ it is true that $a_i \neq 0$, the largest such value of i is the degree of $f(x)$. If all $a_i \neq 0$, then the degree of $f(x)$ is undefined.

Let us agree that if $f(x) = a_0 + a_1x + \ldots + a_nx^n + \ldots$ has $a_i = 0$ for $i > n$, then we may denote $f(x)$ by $a_0 + a_1x + \ldots + a_nx^n$.

Addition and multiplication of polynomials with coefficients in a ring R are defined in a way familiar to us. Let

$$f(x) = a_0 + a_1x + \ldots + a_mx^m,\ a_i \in R,$$

$$g(x) = b_0 + b_1x + \ldots + b_nx^n,\ b_i \in R,$$

be two polynomials over R, then we say $f(x) = g(x)$ if $m = n$ and $a_i = b_i$ for all i.

Addition of polynomials $f(x)$ and $g(x)$ is defined by

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots$$

Product is also defined in the usual way

$f(x)g(x) = (a_0 + a_1x + \ldots + a_mx^m)(b_0 + b_1x + \ldots + b_nx^n)$

$= a_0b_0 + (a_1b_0 + a_0b_1)x + \ldots = c_0 + c_1x + c_2x^2 + \ldots + c_{m+n}x^{m+n}$

where $c_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0 = \sum_{r=0}^{k} a_rb_{k-r}$

Let now $R[x]$ be the set of all polynomials over R. Zero of the ring will be the zero polynomial $O(x) = 0 + 0x + 0x^2 + \ldots$.

Additive inverse of $f(x) = a_0 + a_1x + \ldots + a_mx^m$ will be the polynomial $-f(x) = -a_0 - a_1x + \ldots + (-a_m)x^m$. In fact, if R has unity 1 then the polynomial $e(x) = 1 + 0x + 0x^2 + \ldots$ will be the unity of $R[x]$. $e(x)$ is also sometimes denoted by 1. Instead of a ring R if we start with a field F we get the corresponding ring $F[x]$ of polynomials.

Theorem 1.1.44. [12] Let $R[x]$ be the ring of polynomials over a ring R, then

(i) R is commutative if and only if $R[x]$ is commutative.

(ii) R has unity if and only if $R[x]$ has unity.

Theorem 1.1.45. [12] Let $R[x]$ be the ring of polynomial over a ring R and suppose

$$f(x) = a_0 + a_1x + \ldots + a_mx^m,$$

$$g(x) = b_0 + b_1x + \ldots + b_nx^n,$$

are two non zero polynomials of degree m and n respectively, then

(i) If R is an integral domain, $deg(f(x)g(x)) = m + n$.

(ii) R is an integral domain if and only if $R[x]$ is an integral domain.

(iii) If F is a field, $F[x]$ is not a field.

Definition 1.1.46. [7] Let $f(x)$ and $g(x)$ be polynomials over the field F. If $\gcd(f(x), g(x)) = 1$, we say that $f(x)$ and $g(x)$ are relatively prime (over F). In particular, $f(x)$ and $g(x)$ are relatively prime if and only if there exist polynomials $a(x)$ and $b(x)$ over F for which $a(x)f(x) + b(x)g(x) = 1$.

Definition 1.1.47. [7] A polynomial $f(x) \in R[x]$, is monic provided that it's leading coefficient is 1.

Definition 1.1.48. [3] Two polynomials f and g in $R[x]$ are called coprime, or relatively prime if

$$R[x] =< f > + < g > .$$

Definition 1.1.49. [12] A nonconstant polynomial $f(x) \in F[x]$ is irreducible if whenever $f(x) = p(x)q(x)$, then one of $p(x)$ or $q(x)$ must be constant.

Modules and Submodules

Definition 1.1.50. [13] Let R be any ring, and let M be an abelian group, then M is called a **left R-module** if there exists a scalar multiplication
$\psi : R \times M \to M$ denoted by $\psi(r, m) = rm$, for all $r \in R$ and all $m \in M$, such that for all $r, r_1, r_2 \in R$ and all $m, m_1, m_2 \in M$,

(i) $r(m_1 + m_2) = rm_1 + rm_2$

(ii) $(r_1 + r_2)m = r_1m + r_2m$

(iii) $r_1(r_2m) = (r_1r_2)m$

(iv) $1m = m$, if $1 \in R$.

To denote that M is a left R-module.

Example 1.1.51. [13] If R is a ring then R is an R-module (Left R-module and right R-module).
Vector spaces over F are F-modules where F is a field.

Definition 1.1.52. [13] Any subset of M that is a left R-module under operations induced from M is called a **submodule**.
The subset $\{0\}$ is called the trivial submodule.
The module M is a submodule of itself.

1.2 Finite Frobenius Rings

In this work we deal with a class of rings called Frobenius rings, in this section we define this kind of rings.

Definition 1.2.1. [8] Suppose G is a group. Two elements a and b of G are called conjugate if there exists an element g in G with $gag^{-1} = b$.

It can be readily shown that conjugacy is an equivalence relation and therefore partitions G into equivalence classes. (This means that every element of the group belongs to precisely one conjugacy class, and the classes $Cl(a)$ and $Cl(b)$ are equal if and only if a and b are conjugate, and disjoint otherwise) The equivalence class that contains the element a in G is
$Cl(a) = \{gag^{-1} : g \in G\}$
and is called the conjugacy class of a.
Let G be an abelian group. A function $f : G \to \mathbb{C}\backslash\{0\}$ mapping the group to the non-zero complex numbers is called a character of G if it is a group homomorphism that is, if $\forall g_1, g_2 \in G \;\; f(g_1g_2) = f(g_1)f(g_2)$.
If f is a character of a finite group G, then each function value $f(g)$ is a root of unity (since $\forall g \in G \;\; \exists k \in \mathbb{N}$ such that $g^k = e, f(g)^k = f(g^k) = f(e) = 1$).
Each character f is a constant on conjugacy classes of G, that is, $f(hgh^{-1}) = f(g)$ since G is abelian. For this reason, the character is sometimes called the class function.
A finite abelian group of order n has exactly n distinct characters. These are denoted by $f_1, ..., f_n$. The function f_1 is the trivial representation; that is, $\forall g \in G \;\; f_1(g) = 1$. It is called the principal character of G; the others are called the non-principal characters. The non-principal characters have the property that $f_i(g) \neq 1$ for some $g \in G$.

Definition 1.2.2. [8] If G is an abelian group of order n, then the set of characters f_k forms an abelian group under multiplication $(f_jf_k)(g) = f_j(g)f_k(g)$ for each element

$g \in G$. This group is the character group of G and is sometimes denoted as $\hat{G}$. It is of order n. The identity element of $\hat{G}$ is the principal character f_1. The inverse of f_k is the reciprocal $1/f_k$ which is defined since $f_k(g) \neq 0$ for all $g \in G$.

Definition 1.2.3. [8] Let R be a finite ring, then the Jacobson radical of R , $J(R)$ is the intersection of all maximal left ideals of R. Note that this is the same as the intersection of all maximal right ideals of R.

Definition 1.2.4. [8] Let R be a finite ring, then the left socle of R is the sum of all simple left ideals of R and will be denoted by $soc(R^R)$. Accordingly the right socle $soc(R_R)$ is defined as the sum of all simple right ideals of R.

Let R be a finite ring, and let $\hat{R}$ be the character group of the additive group of R. Then $\hat{R}$ has the structure of an R-bimodule (left and right module) by defining $\chi^r(x) = \chi(rx)$ and $\chi_r(x) = \chi(xr)$ for all $r, x \in R$, and for all $\chi \in \hat{R}$.

Theorem 1.2.5. [21] For a finite ring R the following are equivalent:
(1) $R/J(R)$ is isomorphic to $soc(R^R)$ as left R-modules.
(2) $R/J(R)$ is isomorphic to $soc(R_R)$ as right R-modules.
(3) $soc(R^R)$ is left principal.
(4) $soc(R_R)$ is right principal.
(5) $\hat{R}$ and R are isomorphic as left R-modules.
(6) $\hat{R}$ and R are isomorphic as right R-modules.

Definition 1.2.6. [8] A finite ring is called a Frobenius ring if it satisfies any (and hence all) of the equivalent statements in the last Theorem.

Note that for a finite Frobenius ring there exist characters χ and ψ such that
$\hat{R} = \{\chi_r | r \in R\} = \{\psi^r | r \in R\}$.
We call such χ a left generating character and ψ a right generating character.
It is worth mentioning that every left generating character is a right generating at the same time.

Example 1.2.7. [22] As examples of finite Frobenius Rings we have the finite fields F_q for any prime q, and also any finite chain ring.

Example 1.2.8. [22] The finite ring $F_2[X, Y]/(X^2, XY, Y^2)$ is not Frobenius.

1.3 Finite Fields

In this section we recall the fundamental properties of finite fields.

Vector spaces over finite fields

Definition 1.3.1. [13] Let F_q be the finite field of order q. A nonempty set V, together with some (vector) addition denoted + and scalar multiplication by elements of F_q, is a vector space (or linear space) over F_q if it satisfies all of the following conditions. For all $u, v, w \in V$ and for all $\lambda, \mu \in F_q$:

(i) $u + v \in V$;

(ii) $(u + v) + w = u + (v + w)$;

(iii) There is an element $0 \in V$ with the property $0 + v = v + 0 = v$ for all $v \in V$;

(iv) For each $u \in V$ there is an element $-u \in V$ such that $u + (-u) = 0 = (-u) + u$;

(v) $u + v = v + u$;

(vi) $\lambda v \in V$;

(vii) $\lambda(u + v) = \lambda u + \lambda v, (\lambda + \mu)u = \lambda u + \mu u$;

(viii) $(\lambda\mu)u = \lambda(\mu u)$;

(ix) if 1 is the multiplicative identity of F_q, then $1u = u$.

Definition 1.3.2. [13] A nonempty subset C of a vector space V is a subspace of V if it's itself a vector space with the same vector addition and scalar multiplication as V.

Extension Field

Definition 1.3.3. [7] **(Extension Field)** A field E is called an extension of a field F if $F \subseteq E$ and we write $F \leq E$.
Thus $\mathbf{R}$ is an extension field of $\mathbf{Q}$ and $\mathbf{C}$ is an extension field of both $\mathbf{R}$ and $\mathbf{Q}$.

Definition 1.3.4. [12] The order of a field is the number of elements in the field. If the order is infinite, we call the field an infinite field, and if the order is finite, we call the field a finite field or a Galois field.

Definition 1.3.5. [12] A finite field with p^m elements is called a Galois field of order p^m and is denoted by $GF(p^m)$.

Theorem 1.3.6. [12] For any prime p and any positive integer m, there exists a finite field, unique up to isomorphism, with $q = p^m$ elements.

Lemma 1.3.7. [10] For every element β of a finite field F with q elements, we have $\beta^q = \beta$.

Definition 1.3.8. [7] The order of a nonzero element $\alpha \in F_q$, denoted by $ord(\alpha)$, is the smallest positive integer k such that $\alpha^k = 1$.

Definition 1.3.9. [7] **(Primitive Root of Unity)** An element α of a field F_q is an nth root of unity if $\alpha^n = 1$,
It is a primitive nth root of unity if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$.
An element α in a finite field F_q is called a primitive element (or a generator) of F_q if $F_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$.

Theorem 1.3.10. [10] The elements of F_q are precisely the roots of the polynomial $x^q - x$.

Theorem 1.3.11. [7] **Division Algorithm**
Let $f(x)$ and $g(x)$ be in $F_q[x]$, where $F_q[x]$ is the ring of all polynomials over the field F_q with $g(x)$ nonzero, then

1. There exist unique polynomials $h(x),\ r(x) \in F_q[x]$, such that
   $f(x) = g(x)h(x) + r(x), \qquad$ where $deg\ \ r(x) < deg\ \ g(x)$ or $r(x) = 0$.

2. If $f(x) = g(x)h(x) + r(x), \Rightarrow \gcd(f(x), g(x)) = \gcd(g(x), r(x))$.

Corollary 1.3.12. [12] Let $f(x) \in F[x]$, then α is root of $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$ over F.

Theorem 1.3.13. [7] Let F be a field and let $f(x) \in F[x]$ be a nonconstant polynomial. Then there exists an extension E of F and $\alpha \in E$ such that $f(\alpha) = 0$.

Example 1.3.14. [7] Let $F = \mathbf{R}$ and let $f(x) = x^2 + 1$, which is well known to have no zeros in $\mathbf{R}$ and thus is irreducible over $\mathbf{R}$.
Then $< x^2 + 1 >$ is a maximal ideal in $\mathbf{R}[x]$, so $\mathbf{R}[x]/ < x^2 + 1 >$ is a field.

Identifying $r \in \mathbf{R}$ with $r+ < x^2+1 >$ in $\mathbf{R}[x]/ < x^2+1 >$, we can view $\mathbf{R}$ as a subfield of $E = \mathbf{R}[x]/ < x^2+1 >$.

Let $\alpha = x+ < x^2+1 >$, computing in $\mathbf{R}[x]/< x^2+1 >$,
we find $\alpha^2+1 = (x+ < x^2+1 >)^2 + (1+ < x^2+1 >)$
$=< x^2+1 > + < x^2+1 >= 0$. Thus α is a zero of x^2+1.

Minimal Polynomials

Let E be a finite extension of F_q. Then E is a vector space over F_q and so $E= F_{q^t}$ for some positive integer t. Each element α of E is a root of the polynomial $x^{q^t} - x$. Thus there is a monic polynomial M_α in $F_q[x]$ of smallest degree which has α as a root, this polynomial is called the minimal polynomial of α over F_q. In the following theorem we collect some elementary facts about minimal polynomials.

Definition 1.3.15. [10] A minimal polynomial of an element $\alpha \in F_{q^m}$ with respect to F_q is a nonzero monic polynomial $f(x)$ of the least degree such that $f(\alpha) = 0$.

Theorem 1.3.16. [12] Let $F < E$ be fields, and let $\alpha \in E$ have minimal polynomial $m(x)$ over F.

1) The polynomial $m(x)$ is the unique monic irreducible polynomial over F for which $m(\alpha) = 0$.

2) The polynomial $m(x)$ is the unique monic polynomial of smallest degree over F for which $m(\alpha) = 0$.

3) The polynomial $m(x)$ is the unique monic polynomial over F with property that, for all $f(x) \in F[x]$, we have $f(\alpha) = 0$ if and only if $m(x)|f(x)$. $\square$

Definition 1.3.17. [10] Let n be coprime to q. The cyclotomic coset of q (or q-cyclotomic coset) modulo n containing $i \in Z_n$ is defined by

$$C_i = \{i \,.\, q^j (mod\ n) \in Z_n : j = 0, 1, \dots\}.$$

A subset $\{i_1, \dots, i_t\}$ of Z_n is called a complete set of representatives of cyclotomic cosets of q modulo n if $C_{i_1}, \dots, C_{i_t}$ are distinct and $\bigcup_j^t C_{i_j} = Z_n$.

Example 1.3.18. [10] The polynomial $f(x) = 1 + x + x^3$ is irreducible over F_2;
if it were reducible, it would have a factor of degree 1 and hence a root in F_2, which it does not. So $F_8 = F_2/ < f(x) >$, The elements of F_8 for the given polynomial $f(x)$, are given by:

Cosets	*Vectors*	*Polynomials* in α	*Power* of α
$0+ < f(x) >$	000	0	0
$1+ < f(x) >$	001	1	$1 = \alpha^0$
$x+ < f(x) >$	010	α	α
$x+1+ < f(x) >$	011	$\alpha + 1$	α^3
$x^2+ < f(x) >$	100	α^2	α^2
$1 + x^2+ < f(x) >$	101	$\alpha^2 + 1$	α^6
$x^2 + x+ < f(x) >$	110	$\alpha^2 + \alpha$	α^4
$x^2 + x + 1+ < f(x) >$	111	$\alpha^2 + \alpha + 1$	α^5

The column "power of α" is obtained by using $f(\alpha) = \alpha^3 + \alpha + 1 = 0$, which implies that $\alpha^3 = \alpha + 1$. So $\alpha^4 = \alpha\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha$, $\alpha^5 = \alpha\alpha^4 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$, etc.

Example 1.3.19. [10] Consider the cyclotomic cosets of 2 modulo 15:
$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 9, 12\}$, $C_5 = \{5, 10\}$,
$C_7 = \{7, 11, 13, 14\}$. Thus, $C_1 = C_2 = C_4 = C_8$, and so on.
The set $\{0, 1, 3, 5, 7\}$ is a complete set of representatives of cyclotomic cosets of 2 modulo 15.

Example 1.3.20. [10] The field F_8 was constructed in the Example above. In the table below we give the minimal polynomial over F_2 of each element of F_8 and the associated 2-cyclotomic coset modulo 7.

Roots	*Minimal polynomial*	$2 - cyclotomic\ coset$
0	x	
1	$1 + x$	$\{0\}$
$\alpha, \alpha^2, \alpha^4$	$x^3 + x + 1$	$\{1, 2, 4\}$
$\alpha^3, \alpha^5, \alpha^6$	$x^3 + x^2 + 1$	$\{3, 5, 6\}$

1.4 Basic Concepts of Coding Theory

Coding theory deals with the problem of detecting and / or correcting transmission errors caused by noise on the channel.
In many cases, the information to be sent is transmitted by a sequence of zeros and ones. We call a 0 or a 1 a digit. A word is a sequence of digits. The length of a word is the number of digits in the word. Thus 0110101 is a word of length seven.
A word is transmitted by sending its digits, one after the other, across a binary channel. The term binary refers to the fact that only two digits 0 and 1 are used. Each digit is transmitted mechanically, electrically, magnetically, or otherwise by one of two types of easily differentiated poulses.

Codes, generator and parity check matrices

Definition 1.4.1. [10] Let F_q^n denote the vector space of all $n-$tuples over finite field F_q, n is the length of the vectors in F_q^n. An (n, M) code C over F_q is a subset of F_q^n of size M, that is $|C| = M$ =the number of all codewords of C.
We usually write the vectors $(c_1, c_2, \ldots, c_n)$ in F_q^n in the form $c_1c_2\ldots\ c_n$ and call the vectors in C codewords .

A code whose alphabet is $Z_2 = F_2 = \{0, 1\}$ is called a binary code or a Z_2-code, a code whose alphabet is $Z_3 = F_3 = \{0, 1, 2\}$ is called a ternary code or a Z_3-code, and a code whose alphabet consists of four elements such as $Z_4 = \{0, 1, 2, 3\}$ is called quaternary code or a Z_4-code.

Definition 1.4.2. [10] If C is a $k-$dimensional subspace of F_q^n, then C will be called an $[n, k]$ linear code over F_q .

Definition 1.4.3. [7] The **rank** of a matrix over $k \in N$ is the number of nonzero rows in any row echelon form of the matrix.

Definition 1.4.4. [10] A generator matrix for an $[n, k]$ code C is any $k \times n$ matrix G whose rows form a basis for C.
Note that a generator matrix for C must have k rows and n columns, and it must have rank k.

Definition 1.4.5. [10] A generator matrix of the form $[I_k|A]$ where I_k is the $k \times k$ identity matrix is said to be in the standard or (systematic) form.

Definition 1.4.6. [10] If $G = [I_k|A]$ is a generator matrix for the $[n, k]$ code C is in systematic form, then $H = [-A^T|I_{n-k}]$ is called the parity check matrix for C.

Example 1.4.7. The matrix $G = [I_4|X]$, where

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

is a generator matrix in standard form for [7,4] binary code. A parity-check matrix is $H = [X^T|I_3]$, where

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

This code is called a $[7, 4]$ Hamming code.

Dual codes and weight distribution

Definition 1.4.8. [10] Let C be a linear $[n, k]$-code. The set

$$C^{\perp} = \{x \in F_q^n | \ \ x.c = 0, \forall c \in C\}.$$

is called the **dual code** for C, where **x.c** is the usual scalar product $x_1c_1 + x_2c_2 + ... + x_nc_n$ of the vectors **x** and **c**. **Note** that $C^{\perp}$ is an $[n, n-k]$ code. Also the generator matrices G for the linear code C=the parity check matrices H for the code $C^{\perp}$.

Remark: If C is a linear code of length n then $dim(C) + dim(C^{\perp}) = n$.

Definition 1.4.9. [10] The inner product of vectors $x = x_1 \dots x_n$, $y = y_1 \dots y_n$ in F_q^n is

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

Definition 1.4.10. [10]

- The (**Hamming distance**) $d_H(x, y)$ between two vectors $x, \ y \in F_q^n$ is defined to be the number of coordinates in which x and y differ.

. The (**Hamming weight**) $w_H(x)$ of a vector $x \in F_q^n$ is the number of nonzero coordinates in x.

Definition 1.4.11. [10] For a code C containing at least two words, the minimum distance of a code C, denoted by $d(C)$, is

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

Theorem 1.4.12. [10] If $x,\ y \in F_q^n$, then $d(x, y) = wt(x - y)$. If C is a linear code, the minimum distance d is the same as the minimum weight of the nonzero codewords of C .

Theorem 1.4.13. [10] The distance function $d(x, y)$ satisfies the following four properties:

(i) (non-negativity) $d(x, y) \geq 0$ for all $x,\ y \in F_q^n$.

(ii) $d(x, y) = 0\ if\ and\ only\ if\ x = y$.

(iii) (symmetry) $d(x, y) = d(y, x)$ for all $x,\ y \in F_q^n$.

(iv) (triangle inequality) $d(x, z) \leq d(x, y) + d(y, z)$ for all $x,\ y,\ z \in F_q^n$. □

Example 1.4.14. Let $C = \{00000, 00111, 11111\}$ be binary code. Then $d(C) = 2$ since $d(00000, 00111) = 3$, $d(00000, 11111) = 5$, $d(00111, 11111) = 2$. Hence, C is a binary $[5, 3, 2]$-code.

Definition 1.4.15. [10] Let A_i, also denoted $A_i(C)$, be the number of codewords of weight i in C. The list A_i for $0 \leq i \leq n$ is called the weight distribution or weight spectrum of C.

Example 1.4.16. Let C be binary code with generator matrix

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

The weight distribution of C is $A_0 = A_6 = 1$ and $A_2 = A_4 = 3$. Notice that only the nonzero A_i are usually listed.

Definition 1.4.17. [10] A code $\mathcal{C}$ is called self-orthogonal provided $\mathcal{C} \subseteq \mathcal{C}^{\perp}$.

Definition 1.4.18. [10] A code $\mathcal{C}$ is called self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$.

Remark: [10] The length n of a self-dual code C is even and the dimension of C is $n/2$.

Proof. $dim(C) + dim(C^{\perp}) = n \Rightarrow dim(C) + dim(C) = n$
$2dim(C) = n \Rightarrow dim(C) = \frac{n}{2}$. □

1.5 Cyclic Codes over Finite Fields

One of the most important classes of linear codes are the class of cyclic code. These codes have great practical importance and they are also of considerable interest from an algebraic point of view since they are easy to encode. They also include the important family Bose-Chadhuri-Hocquengham (BCH) codes which are of great practical importance for error correction, particularly the number of errors is expected to be small compared with the length of the code. Moreover cyclic codes are considered important since they are the building blocks for many other codes. We assume throughout our discussion of cyclic codes that n and q are relatively prime. In particular, if $q = 2$ then n must be odd. When examining cyclic codes over F_q, we will most often represent the codewords in polynomial form. There is bijective correspondence between the vectors $\mathbf{c} = c_0c_1 \dots c_{n-1}$ in F_q^n and the polynomials $c(x) = c_0 + c_1x + \dots c_{n-1}x^{n-1}$ in $F_q[x]$ of degree at most $n-1$. Notice that if $c(x) = c_0 + c_1x + \dots c_{n-1}x^{n-1}$, then $xc(x) = c_{n-1}x^n + c_0x + c_1x^2 + \dots + c_{n-2}x^{n-1}$, which would represent the codeword $\mathbf{c}$ cyclically shifted one to the right if x^n were set equal to 1. More formally, the fact that a cyclic code C is invariant under a cyclic shift implies that if $c(x)$ is in C, then so is $xc(x)$ provided we multiply modulo $x^n - 1$. Also the cyclic code C will correct $t = \lfloor (d-1)/2 \rfloor$ errors, where d is the minimum distance of C.

Polynomials and Words

The polynomial $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$ of degree at most $n-1$ over field $\mathbb{K}$ may regarded as the word $v = a_0a_1a_2 \dots a_{n-1}$ of length n in $\mathbb{K}^n$.
For example if $n = 7$,

polynomial	word
$1+x+x^2+x^4$	1110100
$1+x^4+x^5+x^6$	1000111
$1+x+x^3$	1101000

Thus a code of length n can be represented as a set of polynomials over $\mathbb{K}$ of degree at most $n-1$. The word $a_0a_1a_2a_3$ of length 4 is represented by the polynomial $a_0+a_1x+a_2x^2+a_3x^3$ of degree 3, for instance.

Definition 1.5.1. [9] Let υ be a word of length n, the cyclic shift $T(\upsilon)$ is the word of length n

$$T(\upsilon_0,\upsilon_1,\ldots,\upsilon_{n-1})=(\upsilon_{n-1},\upsilon_0,\ldots,\upsilon_{n-2}).$$

Definition 1.5.2. [10] A code C is said to be cyclic if $T(\upsilon)\in C$, whenever $\upsilon\in C$.

Example 1.5.3. $C_1=\{102,210,021,201,120,012,222,111,000\}$ is a linear cyclic code over Z_3, but $C_2=\{000,221,212,200,121,112,100,021,012\}$ is not cyclic since $T(112)=211$ *which is not* in C_2

Theorem 1.5.4. [10] If C_1 and C_2 are cyclic codes of length n over F_q, then

(i) $C_1+C_2=\{c_1+c_2 : c_1\in C_1,\ c_2\in C_2\}$ is cyclic.

(ii) $C_1\bigcap C_2$ is cyclic.

We remember that since $F_q[x]$ is a principle ideal domain also the ring $R_n=F_q[x]/<x^n-1>$ is a principle ideal hence the cyclic codes are principle ideals of R_n when writing a code word of a cyclic code as c(x) we mean the coset $c(x)+<x^n-1>$ in R_n.

Corollary 1.5.5. [10] The number of cyclic codes in R_n equal 2^m, where m is the number of q-cyclotomic cosets modulo n. Moreover, the dimensions of cyclic codes in R_n are all possible sums of the sizes of the q-cyclotomic cosets modulo n.

Generating polynomial of a cyclic code

Theorem 1.5.6. [10] A linear code C in F_q is cyclic $\iff$ C is an ideal in $R_n=F_q[x]/(x^n-1)$.

Proof. ($\Leftarrow$) If C is an ideal in $F_q[x]/(x^n-1)$ and $c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ is any codeword, then $xc(x)$ is also a codeword, i.e $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$.

($\Rightarrow$) 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. □

Theorem 1.5.7. [10] Let C be an ideal in R_n, then

(i) There is a unique monic polynomial $g(x)$ of minimum degree in $C =< g(x) >$, and it is called the generating polynomial for C.

(ii) The generating polynomial $g(x)$ divides $x^n - 1$.

(iii) If $\deg(g(x)) = r$, then C has dimension $n - r$ and $C =< g(x) >= \{s(x)g(x) : \deg s(x) < n - r\}$.

(iv) If $g(x) = g_0+g_1x+\ldots+g_rx^r$, then $g_0 \neq 0$ and C has the following generator matrix:

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \ldots & g_r & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & g_2 & \ldots & g_r & 0 & \ldots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \ldots & g_r & \ldots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \vdots & 0 & g_0 & g_1 & g_2 & \vdots & g_r \end{bmatrix}$$

Proof. (i) Suppose that C contains two distinct monic polynomials g_1 and g_2 of minimum degree r. Then their difference $g_1 - g_2$ would be a nonzero polynomial in C of degree less than r, which is not possible. Hence, there is a unique monic polynomial $g(x)$ of degree r in C. Since $g(x) \in C$ and C is an ideal, we have $< g(x) > \subseteq C$.
On the other hand, Suppose that $p(x) \in C$, then by Division Algorithm $\exists\ q(x),\ r(x)$ such that

$$p(x) = q(x)g(x) + r(x) \text{ where } r(x) = 0 \text{ or } \deg(r(x)) < r.$$

Then $r(x) = p(x) - q(x)g(x) \in C$ has degree less than r, which possible only if $r(x) = 0$. Hence $p(x) = q(x)g(x) \in < g(x) >$, and so $C \subseteq < g(x) >$. Thus $C =< g(x) >$.

(ii) Dividing $x^n - 1$ by $g(x)$, using Division Algorithm we have

$$x^n - 1 = q(x)g(x) + r(x), \text{ where } \deg(r(x)) < r.$$

Since C is an ideal in $\mathbb{R}_n$, we see that $r(x) \in C$, a contradiction unless $r(x) = 0$, which shows that $g(x)|(x^n - 1)$.

(iii) The ideal generated by $g(x)$ is

$$< g(x) >= \{f(x)g(x) : f(x) \in \mathbb{R}_n\}$$

with the usual reduction $\mod (x^n-1)$. Now $g(x)$ divides x^n-1, and so $x^n-1 = h(x)g(x)$ for some $h(x)$ of degree $n - r$.
Divide $f(x)$ by $h(x)$, we get $f(x) = q(x)h(x)+s(x)$, where $\deg(s(x)) < n-r$ or $s(x) = 0$, then

$$f(x)g(x) = q(x)g(x)h(x) + s(x)g(x) = q(x)(x^n - 1) + s(x)g(x).$$

So $f(x)g(x) = s(x)g(x) \in C$. Now let $c(x)$ *be* in C, then

$$c(x) = s(x)g(x) = (a_0 + a_1x + a_2x^2 + \ldots + a_{n-r-1}x^{n-r-1})g(x) =$$
$$a_0g(x) + a_1xg(x) + \ldots + a_{n-r-1}x^{n-r-1}g(x).$$

So $c(x) \in < \{g(x), xg(x), \ldots, x^{n-r-1}g(x)\} >$, which shows that the set

$$\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\} \text{ spans C.}$$

Also $\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$ is linearly independent, since if

$$a_0g(x) + a_1xg(x) + \ldots + a_{n-r-1}x^{n-r-1}g(x) = 0,$$

then $(a_0 + a_1x + a_2x^2 + \ldots + a_{n-r-1}x^{n-r-1})g(x) = 0$ which implies that

$$(a_0 + a_1x + a_2x^2 + \ldots + a_{n-r-1}x^{n-r-1}) = 0,$$

and since $1, x, x^2, \ldots, x^{n-r-1}$ are linearly independent, then $a_0 = a_1 = \ldots = a_{n-r-1} = 0$ and hence $\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$ forms a basis for C.
Hence $\dim(c) = n - r$.

(iv) If $g_0 = 0$ then $g(x) = xg_1(x)$, where $\deg(g_1(x)) < r$ and $g_1(x) = 1.g_1(x) = x^{n-1}g(x)$, *so* $g_1(x) \in C$ which contradict, the fact that no nonzero polynomial in C has degree less than r. Thus $g_0 \neq 0$.
Finally, G is a generator matrix of C since $\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$ is a basis for C. □

Corollary 1.5.8. [10] Let C be a nonzero cyclic code in R_n. The following are equivalent:
(i) $g(x)$ is the monic polynomial of minimum degree in C.
(ii) $C =< g(x) >,\ g(x)$ is monic, and $g(x)|(x^n - 1)$.

The Parity Check Matrix

Theorem 1.5.9. [10] Let C be a cyclic code in R_n with generator polynomial $g(x)$, such that $deg\ g(x) = r$. Let $h(x) = (x^n - 1)/g(x) = \sum_{i=0}^{n-r} h_i x^i$. Then the generator polynomial of $C^\perp$ is $g^\perp(x) = x^{n-r}h(x^{-1})/h(0)$. Furthermore, a generator matrix for $C^\perp$, and hence a parity check matrix for C, is given by

$$H = \begin{bmatrix} h_{n-r} & \dots & \dots & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_{n-r} & \dots & \dots & \dots & h_0 & 0 & \dots & 0 \\ \dots & 0 & h_{n-r} & \dots & \dots & \dots & h_0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots & h_{n-r} & \dots & \dots & h_0 \end{bmatrix}$$

Example 1.5.10. [10] Let C be a cyclic code of length $n = 9$. Since $x^9 - 1$ factors over F_2

$$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1) = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1).$$

Hence, there are $2^3 = 8$ cyclic codes in $R_9 = F_2/ < x^9 - 1 >$. Take $C =< x^6 + x^3 + 1 >$ with generating polynomial $g(x) = x^6 + x^3 + 1$.
Then C has dimension $9 - 6 = 3$ and generating matrix

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

Also C has check polynomial $h(x) = \frac{x^9-1}{g(x)} = (x - 1)(x^2 + x + 1) = x^3 - 1$. Then C has the parity check matrix

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

Encoding With Cyclic Code

There are two rather straight forward ways to encode message strings using a cyclic code one systematic method and one nonsystematic.

The First Procedure:[10]

Let G be the generator matrix of the cyclic code $C =< g(x) >$, then

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

We encode the message $m \in \mathbb{F}_q^k$ as the codeword $c = mG$. But if we transform $m, c \in \mathbb{F}_q^k$ to the polynomials $m(x), c(x) \in \mathbb{F}_q[x]$, then

We encode $m(x)$ as a codeword $c(x)$ by forming the product $c(x) = m(x)g(x)$.

However, this encoding is not systematic.

Example 1.5.11. [10] Let C be a binary cyclic code of length 15 with generator polynomial $g(x) = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)$.

Encode the message $m(x) = 1 + x^2 + x^5$ using the first procedure, we have

$g(x) = 1 + x^4 + x^6 + x^7 + x^8$.

$c(x) = m(x)g(x) = (1 + x^2 + x^5)(1 + x^4 + x^6 + x^7 + x^8) =$

$1 + x^2 + x^4 + x^5 + x^7 + x^{10} + x^{11} + x^{12} + x^{13} \longleftrightarrow (101011010011110)$.

The Second Procedure:[10]

This way is systematic. The message $m(x)$ associated to the message m is of degree at most $k - 1$ (or is the zero polynomial). The polynomial $x^{n-k}m(x)$ has degree at most $n - 1$ and has its first n-k coefficients equal to 0, thus the message is contained in the coefficients of $x^{n-k},\ x^{n-k+1},\ \dots,\ x^{n-1}$. By the Division Algorithm,

$x^{n-k}m(x) = g(x)a(x) + r(x)$, where $\deg r(x) < n - k$ or $r(x) = 0$.

Let $c(x) = x^{n-k}m(x) - r(x)$, as $c(x)$ is a multiple of $g(x)$, $c(x) \in C$. Also $c(x)$ differs from $x^{n-k}m(x)$ possibly in the coefficients of $1,\ x,\ \dots,\ x^{n-k-1}$ as $\deg r(x) < n - k$. So $c(x)$ contains the message m in the coefficients of the terms of degree at least $n - k$.

Example 1.5.12. [10] Let C be a binary cyclic code of length 15 with generator polynomial $g(x) = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)$.

Encode the message $m(x) = 1 + x^2 + x^5$ using the second procedure, we have

$g(x) = 1 + x^4 + x^6 + x^7 + x^8$.

$x^{n-k} = x^{15-7} = x^8$.

$x^8 m(x) = x^8.(1 + x^2 + x^5) = x^8 + x^{10} + x^{13}$.

Now divide $x^8 m(x)$ by $g(x)$.

$$
\begin{array}{r|l}
 & x^5 + x^4 + x + 1 \\
\hline
x^8 + x^7 + x^6 + x^4 + 1 & x^{13} + \quad + x^{10} + \quad + x^8 \\
 & \underline{x^{13} + x^{12} + x^{11} + \quad + x^9 + \quad + x^5} \\
 & x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^5 \\
 & \underline{x^{12} + x^{11} + x^{10} + \quad + x^8 + \quad + x^4} \\
 & x^9 + \quad + x^5 + x^4 \\
 & \underline{x^9 + x^8 + x^7 + \quad + x^5 + \quad + x} \\
 & x^8 + x^7 + \quad + x^4 + x \\
 & \underline{x^8 + x^7 + x^6 + \quad + x^4 + 1} \\
 & x^6 + x + 1
\end{array}
$$

$x^8 m(x) = g(x).(x^5 + x^4 + x + 1) + (x^6 + x + 1)$

$c(x) = x^8 m(x) + (x^6 + x + 1) = (x^{13} + x^{10} + x^8) + x^6 + x + 1$

as a vector $C = (1100001010100 10) \in \mathbb{F}_q^n$.

Decoding With Cyclic Code

Following[10], let C be an $[n, k, d]$ cyclic code over $\mathbb{F}_q$ with generator polynomial $g(x)$ of degree $n-k$, C will correct $t = \lfloor (d-1)/2 \rfloor$ errors. Suppose that $c(x) \in C$ is transmitted and y(x) =c(x)+e(x) is received, where $e(x) = e_0 + e_1 x + \ldots + e_{n-1} x^{n-1}$ is the error vector with $wt(e(x)) \leq t$.

Definition 1.5.13. [10] For any vector $\nu(x) \in \mathbb{F}_q[x]$, let $R_{g(x)}$ be the unique remainder when $\nu(x)$ is divided by $g(x)$ according to Division Algorithm, that is, $R_{g(x)}(\nu(x)) = r(x)$, where

$$\nu(x) = g(x)f(x) + r(x), \quad with \quad r(x) = 0 \quad or \quad deg \quad r(x) < n - k.$$

The function $R_{g(x)}$ satisfies the following properties.

Theorem 1.5.14. [10] With the preceding notation the following hold:

(i) $R_{g(x)}(a\nu(x) + b\nu^{'}(x)) = aR_{g(x)}(\nu(x)) + bR_{g(x)}(\nu^{'}(x))$ for all $\nu(x),\ \nu^{'}(x) \in \mathbb{F}_q[x]$ and all $a, b \in \mathbb{F}_q$.

(ii) $R_{g(x)}(\nu(x) + a(x)(x^n - 1)) = R_{g(x)}(\nu(x))$.

(iii) $R_{g(x)}(\nu(x)) = 0$ *if and only if* $\nu(x) \mod (x^n - 1) \in C$.

(iv) If $c(x) \in C$, then $R_{g(x)}(c(x) + e(x)) = R_{g(x)}(e(x))$.

(v) If $R_{g(x)}(e(x)) = R_{g(x)}(e^{'}(x))$, where $e(x)$ and $e^{'}(x)$ each have weight at most t, then $e(x) = e^{'}(x)$.

(vi) $R_{g(x)}(\nu(x)) = \nu(x)$ if $\deg \nu(x) < n - k$.

Theorem 1.5.15. [10] Let $g(x)$ be a monic divisor of $x^n - 1$ of degree $n - k$. If $R_{g(x)}(\nu(x)) = s(x)$, then
$R_{g(x)}(x\nu(x) \mod (x^n - 1)) = R_{g(x)}(xs(x)) = xs(x) - g(x)s_{n-k-1}$, where s_{n-k-1} is the coefficient of x^{n-k-1} in $s(x)$.

We now describe the first version of the Meggitt Decoding Algorithm and use example to illustrate each step. Define the syndrome polynomial $S(\nu(x))$ of any $\nu(x)$ to be $S(\nu(x)) = R_{g(x)}(x^{n-k}\nu(x))$.

step I:
We find the syndrome polynomials $S(e(x))$ of error patterns $e(x) = \sum_{i=0}^{n-1} e_i x^i$ such that $wt(e(x)) \leq t$ and $e_{n-1} \neq 0$.

Example 1.5.16. [10] Let C be the $[15, 7, 5]$ binary cyclic code with a generating polynomial
$g(x) = 1+x^4+x^6+x^7+x^8 = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^6)(x-\alpha^8)(x-\alpha^9)(x-\alpha^{12})$
where α is a 15th root of unity in $\mathbb{F}_{16}$. Then the syndrome polynomial of $e(x)$ is $S(e(x)) = R_{g(x)}(x^8 e(x))$. Step I produces the following syndrome polynomial:

$e(x)$	$S(e(x))$	$e(x)$	$S(e(x))$
x^{14}	x^7	x^6+x^{14}	$x^3+x^5+x^6$
$x^{13}+x^{14}$	x^6+x^7	x^5+x^{14}	$x^2+x^4+x^5+x^6+x^7$
$x^{12}+x^{14}$	x^5+x^7	x^4+x^{14}	$x+x^3+x^4+x^5+x^7$
$x^{11}+x^{14}$	x^4+x^7	x^3+x^{14}	$1+x^2+x^3+x^4+x^7$
$x^{10}+x^{14}$	x^3+x^7	x^2+x^{14}	$x+x^2+x^5+x^6$
x^9+x^{14}	x^2+x^7	$x+x^{14}$	$1+x+x^4+x^5+x^6+x^7$
x^8+x^{14}	$x+x^7$	$1+x^{14}$	$1+x^4+x^6$
x^7+x^{14}	$1+x^7$		

The computations of these syndrome polynomials were aided by Theorem 1.5.14 and Theorem 1.5.15. For example, in computing the syndrome polynomial of $x^{12}+x^{14}$, we have $S(x^{12}+x^{14}) = R_{g(x)}(x^8(x^{12}+x^{14})) = R_{g(x)}(x^5+x^7) = x^5+x^7$ using Theorem 1.5.14.(vi). In computing the syndrome polynomial for $1+x^{14}$, first observe that $R_{g(x)}(x^8) = 1+x^4+x^6+x^7$, then
$S(1+x^{14}) = R_{g(x)}(x^8(1+x^{14})) = R_{g(x)}(x^8)+R_{g(x)}(x^7) = 1+x^4+x^6$.
We see by Theorem 1.5.14 that $R_{g(x)}(x^9) = R_{g(x)}(xx^8) =$
$R_{g(x)}(x+x^5+x^7)+R_{g(x)}(x^8) = x+x^5+x^7+1+x^4+x^6+x^7 = 1+x+x^4+x^5+x^6$.
Therefore in computing the syndrome polynomial for $x+x^{14}$, we have
$S(x+x^{14}) = R_{g(x)}(x^8(x+x^{14})) = R_{g(x)}(x^9)+R_{g(x)}(x^7) = 1+x+x^4+x^5+x^6+x^7$.
The others follow similarly.

Step II:
Suppose that $y(x)$ is the received vector. Compute the syndrome polynomial $S(y(x)) = R_{g(x)}(x^{n-k}y(x))$. By Theorem 1.5.14.$(iv)$, $S(y(x)) = S(e(x))$, where $y(x) = c(x)+e(x)$ with $c(x) \in C$.

Example 1.5.17. [10] Continuing with Example 1.5.16, suppose that $y(x) = 1+x^4+x^7+x^9+x^{10}+x^{12}$ is received.

Then $S(y(x)) = x+x^2+x^6+x^7$.

Step III:
If $S(y(x))$ is in the list computed in the Step I, then we know the error polynomial $e(x)$ and this can be subtracted from $y(x)$ to the corrected codeword $c(x) = y(x)-e(x)$. If $S(y(x))$ is not in the list, go on to Step IV.
Step IV:
Compute the syndrome polynomial of $xy(x),\ x^2y(x),\ \ldots$ in succession until the syndrome polynomial is in the list from Step I. If $S(x^iy(x))$ is in this list and is

associated with the error polynomial $e^{'}(x)$, then the received vector is decoded as $y(x) - x^{n-i}e^{'}(x)$.

The computation in Step IV is most easily carried out using Theorem 1.5.15 As $R_{g(x)}(x^{n-k}y(x)) = S(y(x)) = \sum_{i=0}^{n-k-1} s_i x^i$, $S(xy(x)) = R_{g(x)}(x^{n-k}xy(x)) = R_{g(x)}(x(x^{n-k}y(x))) = R_{g(x)}(xS(y(x))) = xS(y(x)) - s_{n-k-1}g(x)$.

Example 1.5.18. [10] Continuing with Example 1.5.17, we have $S(y(x)) = x + x^2 + x^6 + x^7$, that $S(xy(x)) = x(x + x^2 + x^6 + x^7) - 1.g(x) = 1 + x^2 + x^3 + x^4 + x^6$, which is not in the list in Example 1.5.16

$S(x^2y(x)) = x(1 + x^2 + x^3 + x^4 + x^6) - 0.g(x) = x + x^3 + x^4 + x^5 + x^7$, which corresponds to the error $x^4 + x^{14}$ implying that $y(x)$ is decoded as $y(x) - (x^2 + x^{12}) = 1 + x^2 + x^4 + x^7 + x^9 + x^{10}$.

Chapter 2

Codes Over The Ring

$F_2 + uF_2 + vF_2 + uvF_2$

2.1 Linear Codes Over The Ring $F_2 + uF_2 + vF_2 + uvF_2$

Linear codes over rings have been studied extensively in the past decade, with the emergence of the ground-breaking work done in linear codes over Z_4 see [10]. Since then, many different types of rings have been studied in connection with coding theory. The two main classes of rings that have been studied are Galois rings and rings of the form $F_{2^m} + uF_{2^m}$ for some positive integer m and some variations of these. An important aspect of these rings is that they are all finite chain rings and also they are all principal ideal rings. From [24] the finite chain property allows the codes to have unique forms of generating matrices as well as unique types. In this work, we aim to study a ring which is fundamentally different from the ones we mentioned above, even though it looks like a variation of those rings. The ring that we study, i.e, $F_2 + uF_2 + vF_2 + uvF_2$ differs from the rings previously studied in two main points, one is that the ring $F_2+uF_2+vF_2+uvF_2$ is not a chain ring and the other is that it is not a Principal Ideal Ring.

First lets talk about the properties of our ring as was established in [24], The ring $F_2 + uF_2 + vF_2 + uvF_2$ is defined as a characteristic 2 ring subject to the restrictions $u^2 = v^2 = 0$ and $uv = vu$.

Remark: [24] $F_2+uF_2+vF_2+uvF_2$ is isomorphic to $F_2[X,Y]/ < X^2, Y^2, XY - YX >$.

Proof. First we define a map

$f : F_2 + uF_2 + vF_2 + uvF_2 \to F_2[X,Y]/ < X^2, Y^2, XY - YX >$

s.t. $f(a+bu+cv+duv) = a+bx+cy+dxy+ < X^2, Y^2, XY-YX >, \forall (a+bu+cv+duv) \in F_2 + uF_2 + vF_2 + uvF_2$, now we show that f is an isomorphism as follows :

Let $h_1, h_2 \in F_2+uF_2+vF_2+uvF_2$ s.t. $h_1 = a_1+b_1u+c_1v+d_1uv, h_2 = a_2+b_2u+c_2v+d_2uv$ then :

(1) $f(h_1 + h_2) = f(a_1 + b_1u + c_1v + d_1uv + a_2 + b_2u + c_2v + d_2uv) = f((a_1 + a_2) + u(b_1 + b_2) + v(c_1 + c_2) + uv(d_1 + d_2)) = (a_1 + a_2) + (b_1 + b_2)x + (c_1 + c_2)y + (d_1 + d_2)xy+ < X^2, Y^2, XY - YX >= a_1 + b_1x + c_1y + d_1xy+ < X^2, Y^2, XY - YX > +a_2 + b_2x + c_2y + d_2xy+ < X^2, Y^2, XY - YX >= f(h_1) + f(h_2)$.

(2) $f(h_1h_2) = f((a_1+b_1u+c_1v+d_1uv)(a_2+b_2u+c_2v+d_2uv))$, and after some cancelation because $u^2 = v^2 = 0$ we have

$= f(a_1a_2 + u(a_1b_2 + b_1a_2) + v(a_1c_2 + c_1a_2) + uv(a_1d_2 + b_1c_2 + c_1b_2 + d_1a_2))$

$= a_1a_2 + (a_1b_2 + b_1a_2)x + (a_1c_2 + c_1a_2)y + (a_1d_2 + b_1c_2 + c_1b_2 + d_1a_2)xy+ < X^2, Y^2, XY - YX >$

$f(h_1)f(h_2) = (a_1 + b_1x + c_1y + d_1xy+ < X^2, Y^2, XY - YX >)(a_2 + b_2x + c_2y + d_2xy+ < X^2, Y^2, XY - YX >) = a_1a_2 + a_1b_2x + a_1c_2y + a_1d_2xy + b_1a_2x + b_1b_2x^2 + b_1c_2xy + b_1d_2x^2y + c_1a_2y + c_1b_2xy + c_1c_2y^2 + c_1d_2xy^2 + d_1a_2xy + d_1b_2x^2y + c_2d_1xy^2 + d_1d_2x^2y^2+ < X^2, Y^2, XY - YX >$

$= a_1a_2 + (a_1b_2 + b_1a_2)x + (a_1c_2 + c_1a_2)y + (a_1d_2 + b_1c_2 + c_1b_2 + d_1a_2)xy+ < X^2, Y^2, XY - YX >$

$= f(h_1h_2)$.

(3) Let $f(h_1) = f(h_2)$ that is $a_1 + b_1x + c_1y + d_1xy+ < X^2, Y^2, XY - YX >= a_2 + b_2x + c_2y + d_2xy+ < X^2, Y^2, XY - YX >$

then $(a_1 - a_2) + (b_1 - b_2)x + (c_1 - c_2)y + (d_1 - d_2)xy+ < X^2, Y^2, XY - YX >= 0+ < X^2, Y^2, XY - YX >$

so $(a_1 - a_2) + (b_1 - b_2)x + (c_1 - c_2)y + (d_1 - d_2)xy \in < X^2, Y^2, XY - YX >$

and this happens if and only if $a_1 - a_2 = b_1 - b_2 = c_1 - c_2 = d_1 - d_2 = 0$

which implies $a_1 = a_2, b_1 = b_2, c_1 = c_2, d_1 = d_2$, then $h_1 = h_2$, so f is one to one function.

(4) Since f is one to one function and $| F_2 + uF_2 + vF_2 + uvF_2 |=| F_2[X,Y]/ < X^2, Y^2, XY - YX >|= 2^4 = 16$, then f is onto.

From 1,2,3 and 4 f is an isomorphism. □

We next note that the units of $F_2 + uF_2 + vF_2 + uvF_2$ can easily be found to be the following:

$\{1, 1+u, 1+v, 1+u+v, 1+u+uv, 1+v+uv, 1+uv, 1+u+v+uv\}$.

As for the ideal structure we can easily fined all the ideals of $F_2 + uF_2 + vF_2 + uvF_2$ to be listed as $I_0 = \{0\} \subseteq I_{uv} = uv(F_2 + uF_2 + vF_2 + uvF_2)$ $=\{0, uv\} \subseteq I_u, I_v, I_{u+v} \subseteq I_{u,v}$ $\subseteq I_1 = F_2 + uF_2 + vF_2 + uvF_2$

where

$I_u = u(F_2 + uF_2 + vF_2 + uvF_2) = \{0, u, uv, u+uv\}$,

$I_v = v(F_2 + uF_2 + vF_2 + uvF_2) = \{0, v, uv, v+uv\}$,

$I_{u+v} = (u+v)(F_2 + uF_2 + vF_2 + uvF_2) = \{0, u+v, uv, u+v+uv\}$,

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

As we see from the ideals, one of the differences between the ring $F_2 + uF_2 + vF_2 + uvF_2$ and the Galois rings is that, unlike Galois rings, $F_2 + uF_2 + vF_2 + uvF_2$ is not a chain ring since $I_u \nsubseteq I_v$ and $I_v \nsubseteq I_u$ but it is a commutative Frobenius ring as was shown in [6], and $I_{u,v}$ is the nil-radical of $F_2 + uF_2 + vF_2 + uvF_2$ which contains all the zero devisors in the ring with everything outside $I_{u,v}$ being a unit moreover the ring $F_2 + uF_2 + vF_2 + uvF_2$ is a local ring since $I_{u,v}$ is the unique maximal ideal, moreover the ideal $I_{u,v}$ is not a principal ideal so the ring $F_2 + uF_2 + vF_2 + uvF_2$ is not a principal ideal ring.

Linear Codes over $F_2 + uF_2 + vF_2 + uvF_2$ are defined just as all codes over rings are defined:

Definition 2.1.1. [24] A linear code C of length n over the ring $F_2 + uF_2 + vF_2 + uvF_2$ is an $F_2 + uF_2 + vF_2 + uvF_2$-submodule of $(F_2 + uF_2 + vF_2 + uvF_2)^n$.

One of the disadvantages of working with a ring that is not a finite chain ring is that we cannot get a generating matrix of the form that we had for Galois rings However, we can at least classify the generators and we can define $F_2 + uF_2 + vF_2 + uvF_2$-linear independence of them to introduce a possible type for linear codes over $F_2 + uF_2 + vF_2 + uvF_2$.

There are six types of generators for linear codes over $F_2 + uF_2 + vF_2 + uvF_2$ as was established in [24], and we can classify them as $\bar{a}, \bar{b}, \bar{c}, \bar{d}, \bar{e}, \bar{f}$, where

$\bar{a} \in (F_2 + uF_2 + vF_2 + uvF_2)^n \backslash (I_{u,v})^n$

$\bar{b} \in (I_{u,v})^n$,$\bar{b} \notin (\mathrm{I}_u)^n$,$(I_v)^n$,$(I_{u+v})^n$,

$\bar{c} \in (I_u)^n \backslash (I_{uv})^n$

$\bar{d} \in (I_v)^n \backslash (I_{uv})^n$

$\bar{e} \in (I_{u+v})^n \backslash (I_{uv})^n$

$\bar{f} \in (I_{uv})^n = \{0, uv\}^n$.

Remark: [24] The generators of the form $\bar{a}$ contain some units.

Proof. Let $(x_1, x_2, ..., x_n) \in \bar{a}$ s.t. $x_i \notin I_{u,v} \forall i$ then x_i is a unit in $F_2 + uF_2 + vF_2 + uvF_2$, so $\exists$ a unit $x_i^{-1} \notin I_{u,v} \forall i$, so $\exists (x_1^{-1}, x_2^{-1}, ..., x_n^{-1}) \in \bar{a}$ s.t. $(x_1, x_2, ..., x_n).(x_1^{-1}, x_2^{-1}, ..., x_n^{-1}) = (x_1.x_1^{-1}, x_2.x_2^{-1}, ..., x_n.x_n^{-1}) = (1, 1, ..., 1)$ which is the unity of $(F_2 + uF_2 + vF_2 + uvF_2)^n$, so $(x_1, x_2, ..., x_n)$ is a unit in $(F_2 + uF_2 + vF_2 + uvF_2)^n$. □

The generators of the form $\bar{a}$ that contain some units are called free generators.
We next define independence over $F_2 + uF_2 + vF_2 + uvF_2$ for these generators:

Definition 2.1.2. [24] A subset
$S = \{\{\bar{a}_i\}_1^{k_1}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$
of $(F_2 + uF_2 + vF_2 + uvF_2)^n$ is said to be $F_2 + uF_2 + vF_2 + uvF_2$-linearly independent if the only solution to the equation
$\sum_{i=1}^{k_1} \alpha_i \bar{a}_i + \sum_{j=1}^{k_2} \beta_j \bar{b}_j + \sum_{m=1}^{k_3} \gamma_m \bar{c}_m + \sum_{t=1}^{k_4} \mu_t \bar{d}_t + \sum_{r=1}^{k_5} \eta_r \bar{e}_r + \sum_{s=1}^{k_6} \zeta_s \bar{f}_s = \bar{0}$,
where
$\alpha_i \in F_2 + uF_2 + vF_2 + uvF_2$, $\beta_j \in F_2 + uF_2 + vF_2$, $\gamma_m \in F_2 + vF_2$, $\mu_t \in F_2 + uF_2$, $\eta_r \in F_2 + uF_2$, $\zeta_s \in F_2$
is
$\alpha_i, \beta_j, \gamma_m, \mu_t, \eta_r, \zeta_s = 0$ for all indices i, j, m, t, r, s.

Throughout this work, this will be the definition of independence for us. Now we can take independent vectors as our generators to generate a linear code over $F_2 + uF_2 + vF_2 + uvF_2$:

Definition 2.1.3. [24] Suppose
$S = \{\{\bar{a}_i\}_1^{k_1}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$
is a set of linearly independent generators as was defined above. The linear code C of length n generated by S is the submodule
$\{\sum_{i=1}^{k_1} \alpha_i \bar{a}_i + \sum_{j=1}^{k_2} \beta_j \bar{b}_j + \sum_{m=1}^{k_3} \gamma_m \bar{c}_m + \sum_{t=1}^{k_4} \mu_t \bar{d}_t + \sum_{r=1}^{k_5} \eta_r \bar{e}_r + \sum_{s=1}^{k_6} \zeta_s \bar{f}_s$: $\alpha_i \in F_2 + uF_2 + vF_2 + uvF_2$, $\beta_j \in F_2 + uF_2 + vF_2$, $\gamma_m \in F_2 + vF_2$, $\mu_t \in F_2 + uF_2$, $\eta_r \in F_2 + uF_2$,

$\zeta_s \in F_2\}$

In this case we say C is of type $(16)^{k_1}(8)^{k_2}(u)^{k_3}(v)^{k_4}(u+v)^{k_5}(2)^{k_6}$.

Is the type of a code unique? Before answering this question, we should note that the definition of the type depends on the existence of generators of the form that was described in the Definition As an $F_2 + uF_2 + vF_2 + uvF_2$-module, it might not always be possible for a linear code C to have these kind of generators. To characterize the cases when it is possible to have such generators we will first establish the uniqueness of the type, if there exists a set of linearly independent generators. then we will try to extract more information about such codes after which we can classify the codes that cannot have such generators. The following theorem will be quite useful in establishing the uniqueness of the type for codes over $F_2 + uF_2 + vF_2 + uvF_2$:

Lemma 2.1.4. [24]
If $S = \{\{\bar{a}_i\}_1^{k_1}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$ is a set of linearly independent generators which generate the linear code C, then the number of codewords in C that belong to I_{uv}^n is exactly $2^{k_1+2k_2+k_3+k_4+k_5+k_6}$.

Proof. Because of the linear independence the only codewords in C that belong toI_{uv}^n can arise from the binary linear combinations of
$\{\{\bar{a}_i uv\}_1^{k_1}, \{\bar{b}_{j_1} u\}_1^{k_2}, \{\bar{b}_{j_2} v\}_1^{k_2}\{\bar{c}_m v\}_1^{k_3}, \{\bar{d}_t u\}_1^{k_4}, \{\bar{e}_r u\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$
Again, because of linear independence, these generators will all be linearly independent over F_2. That is why we will have exactly $2^{k_1+2k_2+k_3+k_4+k_5+k_6}$ such codewords. □

After this auxiliary result, we are now ready to settle the main question about the uniqueness of the type, given the existence of independent generators:

Theorem 2.1.5. [24]
If $S = \{\{\bar{a}_i\}_1^{k_1}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$ is a set of linearly independent generators which generate the linear code C, then C cannot be generated by another type, i.e. $k_1, k_2, ..., k_6$ are uniquely determined by the code.

Proof. Suppose S generates a linear code C. Then the first equation we get is about the size of the code.
$2^{4k_1+3k_2+2k_3+2k_4+2k_5+k_6} = \mid C \mid$.
If we multiply every element of the code by u, then this will nullify some of the generators,

because uI_u=0,$uI_{uv} = 0$. Since $uI_{u,v}$=uI_v=uI_{u+v}=I_{uv} and $u(F_2 + uF_2 + vF_2 + uvF_2)$= I_u, the linear independence of the generators tells us that

$2^{2k_1+k_2+k_4+k_5}$=| uC |.

Similarly we obtain

$2^{2k_1+k_2+k_3+k_5}$=| vC |,

$2^{2k_1+k_2+k_3+k_4}$=| $(u+v)C$ |.

If C_{uv} denotes the set of all codewords in C that belong to I^n_{uv}, then by Lemma 2.1.4 we see that

$2^{k_1+2k_2+k_3+k_4+k_5+k_6}$=| C_{uv} |.

Finally multiplying the elements of $F_2 + uF_2 + vF_2 + uvF_2$ by uv nullifies every element except the units, which are turned into uv, hence we get

2^{k_1}=| uvC |

Since all the sizes on the right hand side of the equations are powers of 2, we will take logarithms base 2 from the first to the last equation, and calling $\log_2$ | C |=A_1, $\log_2$ | uC |=A_2, and so on. We obtain the following system of linear equations for k_i's:

$4k_1 + 3k_2 + 2k_3 + 2k_4 + 2k_5 + k_6 = A_1$

$2k_1 + k_2 + k_4 + k_5 = A_2$

$2k_1 + k_2 + k_3 + k_5 = A_3$

$2k_1 + k_2 + k_3 + k_4 = A_4$

$k_1 + 2k_2 + k_3 + k_4 + k_5 + k_6 = A_5$

$k_1 = A_6$

The coefficient matrix for the system of equations is

$$\begin{pmatrix} 4 & 3 & 2 & 2 & 2 & 1 \\ 2 & 1 & 0 & 1 & 1 & 0 \\ 2 & 1 & 1 & 0 & 1 & 0 \\ 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

which has determinant 1. This proves the uniqueness of $k_1, k_2, ..., k_6$ which means we can talk about a unique type for the code C, provided that independent generators are given for C. □

Remark: [24] Note that the theorem uses the fact that we already have an independent

set of vectors. If C is generated by such a linearly independent set
$S = \{\{\bar{a}_i\}_1^{k_2}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$
where $\bar{a}_i$'s are free(they contain units), $\bar{b}_j$'s are from $I_{u,v}\backslash I_u, I_v, I_{u+v}$, $\bar{c}_m$'s are from $I_u\backslash I_{uv}$, $\bar{d}_n$'s are from $I_v\backslash I_{uv}$, $\bar{e}_r$'s are from $I_{u+v}\backslash I_{uv}$ and $\bar{f}_s$'s are from I_{uv} then we will say C is of type $(16)^{k_1}(8)^{k_2}(u)^{k_3}(v)^{k_4}(u+v)^{k_5}(2)^{k_6}$.

Now that we have established the uniqueness of the type for linear codes over $F_2 + uF_2 + vF_2 + uvF_2$, we can extract some further information about these codes given the type. This will help us characterize the codes that have independent generators. To this extent, we will take a code C of type$(16)^{k_1}(8)^{k_2}(u)^{k_3}(v)^{k_4}(u+v)^{k_5}(2)^{k_6}$ which has generators of the form
$S = \{\{\bar{a}_i\}_1^{k_2}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$
that are linearly independent. The independence tells us that to obtain codewords that fall in the ideal I_{uv}, we need to take the binary combinations of
$\{\{\bar{a}_i uv\}_1^{k_2}, \{\bar{b}_{j_1} u\}_1^{k_2}, \{\bar{b}_{j_2} v\}_1^{k_2}\{\bar{c}_m v\}_1^{k_3}, \{\bar{d}_t u\}_1^{k_4}, \{\bar{e}_r u\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$.
A similar argument can easily be employed to see that the codewords that fall entirely in the ideal I_u will arise from the combinations of the form
$\sum_{i=1}^{k_1} \alpha_i\bar{a}_i + \sum_{j=1}^{k_2} \beta_j\bar{b}_j + \sum_{m=1}^{k_3} \gamma_m\bar{c}_m + \sum_{t=1}^{k_4} \mu_t\bar{d}_t + \sum_{r=1}^{k_5} \eta_r\bar{e}_r + \sum_{s=1}^{k_6} \zeta_s\bar{f}_s$
where $\alpha_i \in uF_2 + uvF_2$, $\beta_j \in uF_2 + vF_2$, $\gamma_m \in F_2 + vF_2$, $\mu_t \in uF_2$, $\eta_r \in uF_2$, $\zeta_s \in F_2$. This tells us that the total number of codewords in C that fall entirely in the ideal I_u is
$2^{2k_1+2k_2+2k_3+k_4+k_5+k_6}$- - - - - - - - - - -(1)

For the ideal I_v, the codewords that fall entirely in the ideal I_v will arise from the combinations of the form
$\sum_{i=1}^{k_1} \alpha_i\bar{a}_i + \sum_{j=1}^{k_2} \beta_j\bar{b}_j + \sum_{m=1}^{k_3} \gamma_m\bar{c}_m + \sum_{t=1}^{k_4} \mu_t\bar{d}_t + \sum_{r=1}^{k_5} \eta_r\bar{e}_r + \sum_{s=1}^{k_6} \zeta_s\bar{f}_s$
where $\alpha_i \in vF_2 + uvF_2$, $\beta_j \in uF_2 + vF_2$, $\gamma_m \in vF_2$, $\mu_t \in F_2 + uF_2$, $\eta_r \in uF_2$, $\zeta_s \in F_2$. This tells us that the total number of codewords in C that fall entirely in the ideal I_v is
$2^{2k_1+2k_2+k_3+2k_4+k_5+k_6}$- - - - - - - - - - -(2)

For the ideal I_{u+v}, the codewords that fall entirely in the ideal I_{u+v} will arise from the combinations of the form
$\sum_{i=1}^{k_1} \alpha_i\bar{a}_i + \sum_{j=1}^{k_2} \beta_j\bar{b}_j + \sum_{m=1}^{k_3} \gamma_m\bar{c}_m + \sum_{t=1}^{k_4} \mu_t\bar{d}_t + \sum_{r=1}^{k_5} \eta_r\bar{e}_r + \sum_{s=1}^{k_6} \zeta_s\bar{f}_s$
where $\alpha_i \in uF_2 + vF_2$, $\beta_j \in uF_2 + vF_2$, $\gamma_m \in vF_2$, $\mu_t \in uF_2$, $\eta_r \in F_2 + uF_2$, $\zeta_s \in F_2$. This tells us that the total number of codewords in C that fall entirely in the ideal I_{u+v} is
$2^{2k_1+2k_2+k_3+2k_4+2k_5+k_6}$- - - - - - - - - - -(3)

For the ideal $I_{u,v}$, for a codeword to be entirely in $I_{u,v}$ it must be of the form
$\sum_{i=1}^{k_1} \alpha_i \bar{a}_i + \sum_{j=1}^{k_2} \beta_j \bar{b}_j + \sum_{m=1}^{k_3} \gamma_m \bar{c}_m + \sum_{t=1}^{k_4} \mu_t \bar{d}_t + \sum_{r=1}^{k_5} \eta_r \bar{e}_r + \sum_{s=1}^{k_6} \zeta_s \bar{f}_s$
where $\alpha_i \in uF_2 + vF_2 + uvF_2$, $\beta_j \in F_2 + uF_2 + vF_2$, $\gamma_m \in F_2 + vF_2$, $\mu_t \in F_2 + uF_2$, $\eta_r \in F_2 + uF_2$, $\zeta_s \in F_2$, which means the total number of codewords in C that fall entirely in the ideal $I_{u,v}$ is
$2^{3k_1+3k_2+2k_3+2k_4+2k_5+k_6}$ - - - - - - - - - - -(4)

So, combining Lemma 2.1.4. with the equations (1),(2),(3) and (4) we obtain the following result

Lemma 2.1.6. [24] Let C be a linear code over the ring $F_2 + uF_2 + vF_2 + uvF_2$ of type $(16)^{k_1}(8)^{k_2}(u)^{k_3}(v)^{k_4}(u+v)^{k_5}(2)^{k_6}$, If $N_{uv}, N_u, N_v, N_{u+v}, N_{u,v}$ denote the number of codewords in C that fall entirely in the ideals $I_{uv}, I_u, I_v, I_{u+v}, I_{u,v}$, respectively, then
$\{N_{uv}, N_u, N_v, N_{u+v}, N_{u,v}\} = 2^{k_1+2k_2+k_3+k_4+k_5+k_6}\{1, 2^{k_1+k_3}, 2^{k_1+k_4}, 2^{k_1+k_5}, 2^{2k_1+k_2+k_3+k_4+k_5}\}$

To understand the codes that can have a certain type, let
$N = |C| = 2^{B_1}, N_{u,v} = 2^{B_2}, N_u = 2^{B_3}, N_v = 2^{B_4}, N_{u+v} = 2^{B_5}, N_{uv} = 2^{B_6}$
be given for a code C. Now for the code C to be of type
$(16)^{k_1}(8)^{k_2}(u)^{k_3}(v)^{k_4}(u+v)^{k_5}(uv)^{k_6}$
by Lemma 2.1.6., the solution to the following system of equations must be nonnegative:

$$\begin{pmatrix} 4 & 3 & 2 & 2 & 2 & 1 \\ 3 & 3 & 2 & 2 & 2 & 1 \\ 2 & 2 & 2 & 1 & 1 & 1 \\ 2 & 2 & 1 & 2 & 1 & 1 \\ 2 & 2 & 1 & 1 & 2 & 1 \\ 1 & 2 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \\ k_5 \\ k_6 \end{pmatrix} = \begin{pmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \end{pmatrix}$$

An easy calculation shows us that the coefficient matrix has determinant $1 \neq 0$ and hence when multiplied by the inverse of the matrix we get

$$\begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \\ k_5 \\ k_6 \end{pmatrix} = \begin{pmatrix} B_1 - B_2 \\ B_1 - B_3 - B_4 - B_5 + 2B_6 \\ -B_1 + B_2 + B_3 - B_6 \\ -B_1 + B_2 + B_4 - B_6 \\ -B_1 + B_2 + B_5 - B_6 \\ -2B_2 + B_3 + B_4 + B_5 \end{pmatrix} - - - - - - - - - - - -(*)$$

So for the code C to have independent generators, the vector on the right hand side of

$(*)$ must have all nonnegative coordinates. This gives us a system of five inequalities, since $2^{B_1} = |C| \geq N_{u,v} = 2^{B_2}$ automatically takes care of the first coordinate. Writing back what B_i's means, we see that we get the following from Lemma 2.1.6.:

Theorem 2.1.7. [24] For a linear code C over$F_2+uF_2+vF_2+uvF_2$ to have independent generators as described before, we must have
$N.N_{uv}^2 \geq N_u.N_v.N_{u+v}$,
$N_{u,v}.N_u \geq N.N_{uv}$,
$N_{u,v}.N_v \geq N.N_{uv}$,
$N_{u,v}.N_{u+v} \geq N.N_{uv}$,
$N_u.N_v.N_{u+v} \geq N_{u,v}^2$

For this classification to make sense, we will give an example to a linear code for which the above inequalities don't hold simultaneously:

Example 2.1.8. [24] Let C be the linear code that is generated as all the linear combinations of the vectors
$\{1, 1+v, u\}, \{u+uv, u, u+uv\}, \{v+uv, v+uv, v\}$.
Note that these three vectors are not independent in our sense of the definition, because
$v.\{u+uv, u, u+uv\} + u.\{v+uv, v+uv, v\} = \{0, 0, 0\}$.
Just looking at the code we see that, for the code C we have
$(N, N_{u,v}, N_u, N_v, N_{u+v}, N_{uv}) = (128, 64, 16, 16, 16, 4)$.
We see that, the first inequality in Corollary fails here since
$N.N_{uv}^2 = 2^{11} < 2^{12} = N_u.N_v.N_{u+v}$.

Similarly all the other inequalities except the last one fail for C which means the code C cannot have a type in our sense. In other words we cannot find independent generators for the code C. This is an important point where codes over $F_2+uF_2+vF_2+uvF_2$ differ from codes over finite chain rings such as Galois rings.

Definition 2.1.9. [24] Let $\phi_L : (F_2 + uF_2 + vF_2 + uvF_2)^n \to F_2^{4n}$ be the map given by $\phi_L(\bar{a} + u\bar{b} + v\bar{c} + uv\bar{d}) = (\bar{a} + \bar{b} + \bar{c} + \bar{d}, \bar{c} + \bar{d}, \bar{b} + \bar{d}, \bar{d})$.

We note from the definition that ϕ_L is a linear map that takes a linear code over $F_2 + uF_2 + vF_2 + uvF_2$ of length n to a binary linear code of length $4n$, By using this map, we can define the Lee weight w_L as follows:

Definition 2.1.10. [24] For any element $a+ub+vc+uvd \in \mathrm{F}_2+uF_2+vF_2+uvF_2$ we define the lee weight of $a+ub+vc+uvd$ as $w_L(a+ub+vc+uvd) = w_H(a+b+c+d, c+d, b+d, d)$, where w_H denotes the ordinary Hamming weight for binary codes, also for any two codewords $c_1, c_2 \in \mathrm{F}_2+uF_2+vF_2+uvF_2$ we define the lee distance $d_L(c_1, c_2) = w_L(c_1-c_2)$.

From the definition of ϕ_L we can see that ϕ_L is a distance preserving isometry from $((F_2 + uF_2 + vF_2 + uvF_2)^n, d_L)$ to (F_2^{4n}, d_H), where d_L denotes the lee distance in $(F_2 + uF_2 + vF_2 + uvF_2)^n$ and d_H denotes the hamming distance in F_2^{4n}.

As a result we get one element whose weight is 0, four elements whose weights are 1 $(1, 1+u, 1+v, 1+u+v+uv)$, six elements whose weights are 2 $(u, v, u+v, u+uv, v+uv, u+v+uv)$, four elements whose weights are 3 $(1+uv, 1+u+uv, 1+v+uv, 1+u+v)$, and one element whose weight is 4 (uv).

Remark: [24] An interesting thing to notice here is that the map ϕ_L, when restricted to $F_2+uF_2+vF_2+uvF_2$ is surjective onto F_2^4, So, our weight definition is barely covered by the vectors in F_2^4.

In order to define the dual of a code over $F_2 + uF_2 + vF_2 + uvF_2$, we first need to define an inner product on $F_2+uF_2+vF_2+uvF_2$. From [24] the definition of the inner product is just like the natural Euclidean product, i.e. we define
$< (x_1, x_2, ..., x_n), (y_1, y_2, ..., y_n) >= x_1y_1 + x_2y_2 + ... + x_ny_n$
where the operations are performed in the ring $F_2 + uF_2 + vF_2 + uvF_2$. Note that we can actually define the same inner product in terms of the ordinary dot product in F_2 as follows:
$< \bar{a}_1 + u\bar{b}_1 + v\bar{c}_1 + uv\bar{d}_1, \bar{a}_2 + u\bar{b}_2 + v\bar{c}_2 + uv\bar{d}_2 >$
$= \bar{a}_1.\bar{a}_2 + u(\bar{a}_1.\bar{b}_2 + \bar{a}_2.\bar{b}_1) + v(\bar{a}_1.\bar{c}_2 + \bar{c}_1.\bar{a}_2) + uv(\bar{a}_1.\bar{d}_2 + \bar{b}_1.\bar{c}_2 + \bar{c}_1.\bar{b}_2 + \bar{d}_1.\bar{a}_2)$
where $\bar{a}.\bar{x}$ denotes the ordinary dot product in F_2 of the binary vectors $\bar{a}$ and $\bar{x}$.
We are now ready to define the dual of a linear code C over $F_2 + uF_2 + vF_2 + uvF_2$:

Definition 2.1.11. [24] Let C be a linear code over $F_2 + uF_2 + vF_2 + uvF_2$ of length n, then we define the dual of C as
$C^\perp = \{\bar{y} \in (F_2 + uF_2 + vF_2 + uvF_2)^n \mid < \bar{y}, \bar{x} >= 0, \forall \bar{x} \in C\}$.

Note that from the definition of the inner product, it is obvious that $C^\perp$ is also a linear code over $F_2 + uF_2 + vF_2 + uvF_2$ of length n. An important connection that we

want to investigate is the relation between the dual and the Gray image of a code. The following theorem helps us partially resolve this issue:

Theorem 2.1.12. [24] Let C be a linear code over $F_2 + uF_2 + vF_2 + uvF_2$ of length n. Then $\phi_L(C^{\perp}) \subseteq (\phi_L(C))^{\perp}$ with $(\phi_L(C))^{\perp}$ denoting the ordinary dual of $(\phi_L(C))$ as a binary code.

Proof. To prove the theorem, it is enough to show that,
$< \bar{x}_1, \bar{x}_2 >= 0 \Rightarrow \phi_L(\bar{x}_1).\phi_L(\bar{x}_2) = 0$ for all $\bar{x}_1, \bar{x}_2 \in (F_2 + uF_2 + vF_2 + uvF_2)^n$.
To this extent, let's assume that $\bar{x}_1 = \bar{a}_1 + u\bar{b}_1 + v\bar{c}_1 + uv\bar{d}_1$and that $\bar{x}_2 = \bar{a}_2 + u\bar{b}_2 + v\bar{c}_2 + uv\bar{d}_2$.Then
$< \bar{x}_1, \bar{x}_2 >= 0$ if and only if $\bar{a}_1.\bar{a}_2 = 0$, $\bar{a}_1.\bar{b}_2 + \bar{a}_2.\bar{b}_1 = 0$, $\bar{a}_1.\bar{c}_2 + \bar{c}_1.\bar{a}_2 = 0$, $\bar{a}_1.\bar{d}_2 + \bar{b}_1.\bar{c}_2 + \bar{c}_1.\bar{b}_2 + \bar{d}_1.\bar{a}_2 = 0$
Now, since $\phi_L(\bar{x}_1) = (\bar{a}_1 + \bar{b}_1 + \bar{c}_1 + \bar{d}_1, \bar{c}_1 + \bar{d}_1, \bar{b}_1 + \bar{d}_1, \bar{d}_1)$ and $\phi_L(\bar{x}_2) = (\bar{a}_2 + \bar{b}_2 + \bar{c}_2 + \bar{d}_2, \bar{c}_2 + \bar{d}_2, \bar{b}_2 + \bar{d}_2, \bar{d}_2)$, we get, after some cancelations because of the characteristic being 2,
$\phi_L(\bar{x}_1).\phi_L(\bar{x}_2) = (\bar{a}_1 + \bar{b}_1 + \bar{c}_1 + \bar{d}_1).(\bar{a}_2 + \bar{b}_2 + \bar{c}_2 + \bar{d}_2) + (\bar{c}_1 + \bar{d}_1).(\bar{c}_2 + \bar{d}_2) + (\bar{b}_1 + \bar{d}_1).(\bar{b}_2 + \bar{d}_2) + \bar{d}_1.\bar{d}_2$
$= (\bar{a}_1.\bar{a}_2) + (\bar{a}_1.\bar{c}_2 + \bar{a}_2.\bar{c}_1) + (\bar{a}_1.\bar{b}_2 + \bar{b}_1.\bar{a}_2) + (\bar{a}_1.\bar{d}_2 + \bar{b}_1.\bar{c}_2 + \bar{c}_1.\bar{b}_2 + \bar{d}_1.\bar{a}_2) = 0$ □

Let $F_2 + uF_2 + vF_2 + uvF_2 = \{g_1, g_2, ..., g_{16}\}$ in some order. For example, we might assume $g_1 = 0$,$g_2 = 1$,... and so on.

Definition 2.1.13. [24] The complete weight enumerator of a linear code C over $F_2 + uF_2 + vF_2 + uvF_2$ is defined as
$cwe_C(X_1, X_2, ..., X_{16}) = \sum_{\bar{c} \in C}(X_1^{n_{g_1}(\bar{c})} X_2^{n_{g_2}(\bar{c})} ... X_{16}^{n_{g_{16}}(\bar{c})})$
where $n_{g_i}(\bar{c})$ is the number of appearances of g_i in the vector $\bar{c}$.

Remark: [24] Note that $cwe_C(X_1, X_2, ..., X_{16})$ is a homogeneous polynomial in 16 variables with the total degree of each term being n, the length of the code. Since $\bar{0} \in C$, we see that the term X_1^n always appears in $cwe_C(X_1, X_2, ..., X_{16})$.
We also observe that $cwe_C(1, 1, ..., 1) = \mid C \mid$.

Recall from lemma 2.1.6 that $N_u(C)$ was the number of codewords in C that lie entirely in the ideal I_u, we can see that
$N_u(C) = cwe_C(x_1, x_2, ..., x_{16})$

with $x_i = 0$ when $g_i \notin I_u$ and $x_i = 1$ when $g_i \in I_u$ Similar descriptions can be given for N_{uv}, N_v, and so on.

From [24] we can talk about the size of $C^{\perp}$ through the following theorem :

Theorem 2.1.14. [24] If C is a linear code over $F_2 + uF_2 + vF_2 + uvF_2$ of length n, then $\mid C^{\perp} \mid = (16)^n / \mid C \mid$.

Corollary 2.1.15. [24] If C is a linear code over $F_2 + uF_2 + vF_2 + uvF_2$ of length n and ϕ_L is the Gray map defined before, then
$\phi_L(C^{\perp}) = (\phi_L(C))^{\perp}$.

Proof. We know from Theorem 2.1.12. that
$\phi_L(C^{\perp}) \subseteq (\phi_L(C))^{\perp}$.
But, by the definition of ϕ_L, $\phi_L(C)$ is a binary linear code of length $4n$ of size $\mid C \mid$. So, by the usual properties of the dual of binary codes, we know that $\mid (\phi_L(C))^{\perp} \mid = (2)^{4n} / \mid C \mid = (16)^n / \mid C \mid = \mid C^{\perp} \mid = \mid \phi_L(C^{\perp}) \mid$, by the last Theorem, this implies
$\mid \phi_L(C^{\perp}) \mid = \mid (\phi_L(C))^{\perp} \mid$ and combining this result with $\phi_L(C^{\perp}) \subseteq (\phi_L(C))^{\perp}$ we have that $\phi_L(C^{\perp}) = (\phi_L(C))^{\perp}$. □

2.2 Self-dual Codes Over The Ring $F_2 + uF_2 + vF_2 + uvF_2$

Self-dual codes form an important class of codes and have been studied by researchers for along time. After the distinction of the types of self-dual codes was made, studies focused on distinguishing the different types, finding bounds for their parameters and simply constructing self-dual codes of the two types with good parameters. In the early periods the focus was on binary codes, and there was a lot of work towards classifying binary self-dual codes up to certain lengths. Later, when rings became more popular in coding theory, the scope of self-dual codes extended to rings as well. In [6] worked out the theoretical back ground of self-dual codes over commutative Frobenius rings. In our work, we aim to focus on self-dual codes over the ring $R = F_2 + uF_2 + vF_2 + uvF_2$, which is not a chain ring, but is a commutative Frobenius ring. We will study some of the properties of self-dual codes over R and after wards we will construct some good self-dual codes of Type I and Type II up to certain lengths.

First we recall the definition 2.1.9 and definition 2.1.10 of the gray map ϕ_L and the lee weight w_L.

Definition 2.2.1. [25] if C is a linear code over R then the lee weight enumerator of C is $W_C(z) = \sum_{c \in C} z^{w_L(c)}$.

and also recall that ϕ is linear and distance-preserving map thus we obtain the following lemma, which will later be useful

Lemma 2.2.2. [25] If C is a linear code over R of length n, size 2^k and minimum lee distance d, then $\phi(C)$ is a binary $[4n, k, d]$-linear code.

Theorem 2.2.3. [25] Suppose C is a self-dual linear code over R of length n. Then $\phi_L(C)$ is a self-dual binary linear code of length 4n.

Proof. since C is self dual then $C = C^{\perp}$ and $\mid C \mid = \mid C^{\perp} \mid$ but by Theorem 2.1.14 $\mid C \mid . \mid C^{\perp} \mid = (16)^n$ then $\mid C \mid = \mid C^{\perp} \mid = (16)^{\frac{n}{2}} = 4^n$, now $\phi_L(C^{\perp}) = \phi_L(C) \subseteq (\phi_L(C))^{\perp}$ by Theorem 2.1.12. that is $\phi_L(C)$ is self orthogonal code, also by Lemma 2.2.2. $\mid C \mid = \mid \phi_L(C) \mid = 4^n$, and since $\mid \phi_L(C) \mid . \mid (\phi_L(C))^{\perp} \mid = (16)^n$ then $\mid (\phi_L(C))^{\perp} \mid = 4^n = \mid \phi_L(C) \mid$, combining this result with $\phi_L(C) \subseteq (\phi_L(C))^{\perp}$ we have $\phi_L(C) = (\phi_L(C))^{\perp}$, that is $\phi_L(C)$ is self dual code of length 4n by Lemma 2.2.2. □

We first need an example of a self dual code over R of length $n = 1$:

Example 2.2.4. For the element $u \in R = F_2 + uF_2 + vF_2 + uvF_2 =$ $\{0, 1, u, v, uv, 1+u, 1+v, 1+uv, u+v, u+uv, v+uv, 1+u+uv, 1+v+uv, u+v+uv, 1+u+v, 1+u+v+uv\}$, let C be generated by u of length $n = 1$, i.e. $C = < u > = \{0, uv, u, u+uv\}$, note that any element of $< u >$ is orthogonal to itself and to any other element in $< u >$, that is C is self orthogonal, i.e. $C \subseteq C^{\perp}$, note that $\mid C \mid = 4$ but we know by Theorem 2.1.14 that $\mid C \mid . \mid C^{\perp} \mid = (16)^1$ and since $\mid C \mid = 4$ then $\mid C^{\perp} \mid = 4$, combining this result with $C \subseteq C^{\perp}$ we have $C = C^{\perp}$, that is C is a self dual code of length $n = 1$.

Lemma 2.2.5. [6] Let R be a finite Frobenius ring. Let C be a self-dual code of length n over R and D be a self-dual code of length m over R. Then the direct product $C \times D$ is a self-dual code of length n + m over R.

Proof. Let $(v_1, w_1), (v_2, w_2) \in C \times D$. Then
$< (v_1, w_1), (v_2, w_2) >=< v_1, v_2 > + < w_1, w_2 >= 0 + 0 = 0$, so any vector in $C \times D$ is orthogonal to itself and orthogonal to any other vector in $C \times D$, This implies that $C \times D \subseteq (C \times D)^{\perp}$, i.e. $C \times D$ is self-orthogonal. We have that $\mid C \times D \mid = \mid C \mid . \mid D \mid$. Since C and D are both self-dual codes, this implies that $\mid C \mid = \mid C^{\perp} \mid$, $\mid D \mid = \mid D^{\perp} \mid$, but by Theorem 2.1.14 $\mid C \mid . \mid C^{\perp} \mid = \mid R \mid^n$, $\mid D \mid . \mid D^{\perp} \mid = \mid R \mid^m$, so
$\mid C \mid = \mid R \mid^{\frac{n}{2}}$, $\mid D \mid = \mid R \mid^{\frac{m}{2}}$.
Hence we have that
$\mid C \times D \mid = \mid R \mid^{\frac{n}{2}} . \mid R \mid^{\frac{m}{2}} = \mid R \mid^{\frac{n+m}{2}}$.
By Theorem 2.1.14 we have that
$\mid C \times D \mid . \mid (C \times D)^{\perp} \mid = \mid R \mid^{m+n}$.
This implies that $\mid (C \times D)^{\perp} \mid = \mid R \mid^{\frac{n+m}{2}} = \mid C \times D \mid$.
combinig this result with $C \times D \subseteq (C \times D)^{\perp}$, we have $(C \times D)^{\perp} = C \times D$. This gives that $C \times D$ is self-dual. □

by the previous Lemma The existence of a self-dual code of length 1 implies that

Theorem 2.2.6. [25] Self-dual codes over R of all lengths n exist.

Theorem 2.2.7. [25] If C is a self-dual code over R, then C contains the all-uv vector.

Proof. Since $(unit)^2 = 1$ and $(non - unit)^2 = 0$ in R, a self-orthogonal vector c must have an even number of units. Since $uv.(any\ unit) = uv$, and $uv.(any\ non - unit) = 0$ in R, this means c is orthogonal to the all uv-vector, and since $C = C^{\perp}$, this means that C contains the all uv-vector. □

We next consider Type I and Type II codes. The definitions are just as in the case of binary codes:

Definition 2.2.8. [25] Let C be a self-dual code over R. If the Lee weight of every code word is divisible by 4, C is said to be of Type II, other wise it is called Type I.

Note that, because ϕ_L is an isometry, the Lee weight of every code word in a self-dual code must necessarily be even. We also observe that Theorem 2.2.6 implies that Type I codes over R of all lengths exist. For Type II, we have the following theorem:

Theorem 2.2.9. [25] A Type II code of length n over R exists if and only if n is even.

Proof. For the necessary part, note that by Theorem 2.2.3, if C is a Type II code of length n over R, then $\phi_L(C)$ is a Type II binary code of length 4n. So, the result follows from [17], which says binary Type II codes exist only when the length is divisible by 8. For the sufficient part, we first note that $C =< 1, 1+uv >$ is a self-dual code over R of length 2 with Lee weight enumerator $W_C(z) = 1 + 14z^4 + z^8$, so it is a Type II code. In fact the binary image of C has parameters [8,4,4], the extended Hamming code of degree 3.

We now can extend this code to any even length by taking the matrices of the form

$$\begin{pmatrix} 1 & 1+uv & 0 & 0 \\ 0 & 0 & 1 & 1+uv \end{pmatrix}, \begin{pmatrix} 1 & 1+uv & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1+uv & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1+uv \end{pmatrix}, \ldots.$$

It is clear that rows of these matrices would generate Type II codes of all even lengths. □

We next give upper bounds for the minimum Lee weights of Type I and Type II codes over R:

Theorem 2.2.10. [25] Let $d_L(II, n)$ and $d_L(I, n)$ be the highest minimum Lee weights of a Type II code and a Type I code, respectively, over R of length n. Then
$d_L(II, n) \leq 4\lfloor \frac{n}{6} \rfloor + 4$, $d_L(I, n) \leq 4\lfloor \frac{n}{6} \rfloor + 4$.

Proof. By Theorem 2.2.3, if C is a Type II code or Type I code of length n, then $\phi_L(C)$ is a binary Type II code or Type I code, respectively, of length 4n. Since ϕ_L is distance preserving, the results follow from [18]. We note that since $4n \ncong 22 \bmod 24$, the bound for $d_L(I, n)$ does not change. □

We now give a list of the constructions of Type I and Type II codes and the parameters of their binary Gray images from [25].

Type I codes over R of length n

$n = 1$: We take $C_1 =< (u) >$.
C_1 is self-dual of size 4, with Lee weight enumerator $W_{C1}(z) = 1 + 2z^2 + z^4$ and $\phi_L(C_1)$ is a binary Type I code with parameters [4,2,2] which is the best possible binary Type I code.
$n = 2$: Take $C_2 =< (1, 1) >$.
C_2 is self-dual, with Lee weight enumerator $W_{C2}(z) = 1 + 4z^2 + 6z^4 + 4z^6 + z^8$, and

thus $\phi_L(C_2)$ is a binary Type I code of parameters [8,4,2] which has the highest possible minimum distance for a binary Type I code of length 8.

$n = 3$: Take $C_3 =< (1, 1 + uv, u), (0, uv, v) >$.

C_3 is self-dual, with Lee weight enumerator $W_{C3}(z) = 1 + 15z^4 + 32z^6 + 15z^8 + z^{12}$, and thus $\phi_L(C_3)$ is a binary Type I code of parameters [12,6,4] which is an extremal binary Type I code of length 12 by Theorem 2.2.10 .

$n = 4$: Take $C_4 =< (1, 1 + uv, 1 + u, 1 + v + uv), (0, 1 + uv, 1 + u + uv, uv) >$.

C_4 is self-dual, with Lee weight enumerator $W_{C4}(z) = 1 + 12z^4 + 64z^6 + 102z^8 + 64z^{10} + 12z^{12} + z^{16}$, and thus $\phi_L(C_4)$ is a binary Type I code of parameters [16,8,4] which is an extremal binary Type I code of length 16 by Theorem 2.2.10.

$n = 5$: Take $C_5 =< (1, 1+u+v, 0, 0, 0), (u+v, u+v, v, u, uv), (0, 0, u, v, u+v), (0, 0, 0, u, u) >$.

C_5 is self-dual, with Lee weight enumerator $W_{C5}(z) = 1 + 29z^4 + 32z^6 + 226z^8 + 448z^{10} + 226z^{12} + ...$, where the rest is completed via symmetry, and thus $\phi_L(C_5)$ is a binary Type I code of parameters [20,10,4] which is an extremal binary Type I code of length 20 by Theorem 2.2.10.

$n = 7$: Take $C_7 =< (1, 0, 0, 1 + u + v, 1 + v, 1 + u, uv), (0, 1, 0, 1 + u, 1 + uv, uv, 1 + u), (0, 0, 1, u, 1 + uv, 1 + v, 1 + uv), (0, 0, 0, u, 0, u + uv, u) >$.

C_7 is self-dual, with Lee weight enumerator $W_{C7}(z) = 1 + 42z^6 + 378z^8 + 1624z^{10} + 3717z^{12} + 4860z^{14} + ...$, where the rest is completed via symmetry, and thus $\phi_L(C_7)$ is a binary Type I code of parameters [28,14,6].

$n = 8$: Take $C_8 =< (1, 0, 0, 0, 1 + u + uv, v, u + v, u + v + uv), (0, 1, 0, 0, v + uv, 1 + v + uv, u, u+uv), (0, 0, 1, 0, u+v, u, 1+u+v, u+v), (0, 0, 0, 1, u+v, u, u+v+uv, 1+u+uv) >$.

C_8 is self-dual, with Lee weight enumerator $W_{C8}(z) = 1 + 364z^8 + 2048z^{10} + 6720z^{12} + 14336z^{14} + 18598z^{16} + ...$, where the rest is completed via symmetry, and thus $\phi_L(C_8)$ is a binary Type I code of parameters [32,16,8] which is extremal of length 32 by Theorem 2.2.10.

Type II codes over R of length n

$n = 2$: Take $D_2 =< (1, 1 + uv) >$.

D_2 is self-dual, with Lee weight enumerator $W_{D2}(z) = 1 + 14z^4 + z^8$, and thus $\phi_L(D_2)$ is a binary Type II code of parameters [8,4,4], which is extremal and unique, as it is the extended Hamming code of order 3.

$n = 4$: Take $D_4 =< (1, 1+uv, 1+u, 1+u+uv), (0, 0, 1+u, 1+u+uv)) >$.
D_4 is self-dual, with Lee weight enumerator $W_{D4}(z) = 1 + 28z^4 + 198z^8 + 28z^{12} + z^{16}$, and thus $\phi_L(D_4)$ is a binary Type II code of parameters [16,8,4], which is extremal by Theorem 2.2.10.
$n = 8$: Take $D_8 =< (1,0,0,0,1+u+uv,1+v,1+u,u+uv), (0,1,0,0,u+uv,1+u,1+v,1+u+uv), (0,0,1,0,1,1+uv,v+uv,1+u+v+uv), (0,0,0,1,1,1,v,1+u+v,1+u+v+uv) >$.
D_8 is self-dual, with Lee weight enumerator $W_{D8}(z) = 1+620z^8+13888z^{12}+36518z^{16}+13888z^{20}+620z^{24}+z^{32}$, and thus $\phi_L(D_8)$ is a binary Type II code of parameters [32,16,8] which is extremal of length 32 by Theorem 2.2.10.

2.3 Cyclic Codes Over The Ring $F_2+uF_2+vF_2+uvF_2$

Among the first codes used practically were the cyclic codes which were generated using shift registers. It was quickly noticed by Prange [15] that the class of cyclic codes has a rich algebraic structure, the first indication that algebra would be a valuable tool in code design.

Another nice observation about the ring $F_2 + uF_2 + vF_2 + uvF_2$ is that if $a \in F_2 + uF_2 + vF_2 + uvF_2$ is any element, then $a^2 = 1$ if a is a unit, 0 otherwise.
The notions of the cyclic shift and cyclic codes are standard for codes over all rings. Briefly, for any ring R, a cyclic shift on R^n is a permutation T such that
$T(c_0, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$.
A linear code C over the ring R that is invariant under the cyclic shift is called a cyclic code i.e. $T(C) = C$. We will use the usual ideas of identifying
$\bar{c} = (c_0, c_1, ..., c_{n-1}) \in R^n \Leftrightarrow c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1} \in R[x]$.
With this convention we see that $T(\bar{c})$ is identified with $x.c(x)$ in $R[x]/(x^n - 1)$. So cyclic codes over R are identified with ideals in the ring $R[x]/(x^n - 1)$. Hence, in order to understand cyclic codes over the ring $R = F_2+uF_2+vF_2+uvF_2$, it is essential for us to understand the structure of the polynomial ring $R_n = (F_2+uF_2+vF_2+uvF_2)[x]/(x^n-1)$. We know that if R is a finite chain ring and n is relatively prime to the characteristic of R, then $R[x]/(x^n - 1)$ is a principal ideal ring [5]. However in our case the base ring is not a chain ring, hence things dont work out in the same way. We first start with showing that the above is not the case for us:

Lemma 2.3.1. [26] The ring R_n is not a principal ideal ring.

Proof. We will import an idea from [1] which identifies the ring we want to study with a group ring. We know that for any finite ring R, $R[x]/(x^n - 1)$ is isomorphic to the group ring RG where $G =< g|g^n = 1 >$ is the cyclic group of order n. Now for any group ring RG we can define a surjective ring homomorphism $\gamma : RG \longrightarrow R$ called the augmentation homomorphism as
$\gamma(r_0 + r_1 g + ... + r_{n-1}g^{n-1}) = r_0 + r_1 + ... + r_{n-1}$.
So, in our case, with the identification that was used in [1], we can define $\gamma : R_n \longrightarrow F_2 + uF_2 + vF_2 + uvF_2$ as $\gamma(c_0 + c_1 x + ... + c_{n-1}x^{n-1}) = c_0 + c_1 + ... + c_{n-1}$.
We start with the ideal $I =< u, v >$ of $F_2 + uF_2 + vF_2 + uvF_2$. Obviously I is not a principal ideal. Now let $J = \gamma^{-1}(I)$. and Since γ is onto then J is an ideal in R_n, also $\gamma(J) = \gamma(\gamma^{-1}(I)) = I$.
So, if J were a principal ideal, then its homomorphic image under γ would have to be principal as well. But $\gamma(J) = I$ is not a principal ideal. This proves the lemma. □

What about the locality of R_n? It can be done in two different cases:

Theorem 2.3.2. [26] The ring R_n is not a local ring when $n = 2^k.m$ with $m > 1$ an odd number.

Proof. We will use a characterization of local rings from [11] in which it is stated that a ring is a local ring if and only if the non-units in the ring form an ideal(the maximal ideal). Now, suppose that $n = 2^k.m$ where m is an odd number> 1. Note that
$0 = x^{2^k.m} + 1 = (x^{2^k} + 1)(x^{2^k(m-1)} + x^{2^k(m-2)} + ... + x^{2^k} + 1)$ in R_n. So,
$f_1(x) = x^{2^k(m-1)} + x^{2^k(m-2)} + ... + x^{2^k} + 1$
is a zero-divisor and hence a non-unit. Now, when m is an odd number> 1, we have
$\gamma(x^{2^k(m-2)} + ... + x^{2^k} + 1) = 1 + 1 + ... + 1 = m - 1 = 0$ in R, where γ is defined in Lemma 2.3.1
Since γ is a ring homomorphism, this means that if we take
$f_2(x) = x^{2^k(m-2)} + ... + x^{2^k} + 1$
then $f_2(x)$ is also a non-unit. But $f_1(x) + f_2(x) = x^{2^k(m-1)}$ which is a unit in R_n because $x^{2^k}.x^{2^k(m-1)} = x^n = 1$ in R_n. This implies that non-units cannot form an ideal and hence R_n cannot be a local ring when n is not a power of 2. □

Despite the fact that R_n is not a local ring, we still have a nice classification for the elements of R_n.

Lemma 2.3.3. [26] Every non-zero, non-unit element of R_n must be a zero divisor.

Proof. Suppose $0 \neq a \in R_n$ is not a unit. This means $< a > \neq R_n$. Now $< a >= \{b.a | b \in R_n\}$. Since $| < a > | < |R_n|$, this means, $\exists b_1, b_2 \in R_n$ with $b_1 \neq b_2$ such that $b_1.a = b_2.a$. But this implies $(b_1 - b_2).a = 0$ with $b_1 - b_2 \neq 0$ and so a must be a zero-divisor. □

Theorem 2.3.4. [26] R_n is a local ring when $n = 2^k$ for all $k \in N$.

Proof. We will prove that non-units in R_n form an ideal. This will prove that R_{2^k} is a local ring by [11]. We know that (non-unit).(any element) cannot be a unit. Hence the only thing we need to prove is that the non-units form an additive subgroup of R_{2^k} . To this extent, let

$\alpha = c_0 + c_1 x + ... + c_{2^k-1} x^{2^k-1} \neq 0$

be an element in R_{2^k} . Now, since the characteristic of our ring is 2 and $x^{2^k} = 1$ in R_{2^k}, we have

$\alpha^{2^k} = c_0^{2^k} + c_1^{2^k} + ... + c_{2^k-1}^{2^k}$

But we know that each $c_i^{2^k} = 0$ or 1. Hence in R_{2^k} we get $\alpha^{2^k} = 0$ or 1. Now if $\alpha^{2^k} = 0$, this means $\alpha.\alpha^{2^k-1} = 0$ and hence α is a zero-divisor. Similarly, if $\alpha^{2^k} = 1$, this means $\alpha.\alpha^{2^k-1} = 1$ and hence α is a unit. This gives us a nice characterization of units and non-units in R_{2^k}, An element

$\alpha = c_0 + c_1 x + ... + c_{2^k-1} x^{2^k-1} \in R_{2^k}$

is a non-unit if and only if an even number of c_i's are units and hence an even number of c_i's are non-units in $F_2 + uF_2 + vF_2 + uvF_2$. But, in $F_2 + uF_2 + vF_2 + uvF_2$, non-unit+ non-unit = non-unit; non-unit +unit = unit and unit+unit = non-unit. This implies that the number of $\alpha \in R_{2^k}$ with an even number of non-unit coefficients forms an additive subgroup of R_{2^k} which completes the proof. □

Now we talk about the Characterization of cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$ From [26] we will introduce a homomorphism from $F_2 + uF_2 + vF_2 + uvF_2$ to $F_2 + uF_2$ and use this homomorphism to characterize cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$ by using the results obtained for cyclic codes over $F_2 + uF_2$. The two main cases to be considered are the cases when n is general and when n is odd.

First if n is any positive integer

Lets start with the homomorphism

$\psi : F_2 + uF_2 + vF_2 + uvF_2 \longrightarrow F_2 + uF_2$

with $\psi(a + ub + vc + uvd) = a + ub$. This homomorphism then can be extended to a homomorphism of rings of polynomials

$\Psi : (F_2 + uF_2 + vF_2 + uvF_2)[x]/(x^n - 1) \longrightarrow (F_2 + uF_2)[x]/(x^n - 1)$

by letting

$\Psi(c_0 + c_1x + ... + c_{n-1}x^{n-1}) = \psi(c_0) + \psi(c_1)x + ... + \psi(c_{n-1})x^{n-1}$.

Note that $ker(\psi) = vF_2 + uvF_2 = v(F_2 + uF_2)$.

Now, let us assume that C is a cyclic code over $F_2 + uF_2 + vF_2 + uvF_2$. Restrict Ψ onto C. Since C is invariant under the cyclic shift, so is $\Psi(C)$. This means $Im(\Psi)$ is a cyclic code over $F_2 + uF_2$. But cyclic codes over $F_2 + uF_2$ are characterized. So we can make use of these results. On the other hand $ker(\Psi)$ is also a cyclic code over $v(F_2+uF_2)$. We can consider it to be v times a cyclic code over $F_2 + uF_2$. By using the characterization in [2], we have

$ker(\Psi) = v < g_1(x) + up_1(x), ua_1(x) >$

where g_1, p_1, a_1 are polynomials in $F_2[x]/(x^n - 1)$ satisfying the conditions

$a_1(x)|g_1(x)|x^n - 1$, $a_1(x)|p_1(x)\frac{x^n-1}{g_1(x)}$.

Similarly, $Im(\Psi)$ is also a cyclic code over $F_2 + uF_2$ and hence can be written as

$Im(\Psi) =< g_2(x) + up_2(x), ua_2(x) >$

where g_2, p_2, a_2 are polynomials in $F_2[x]/(x^n - 1)$ satisfying the conditions

$a_2(x)|g_2(x)|x^n - 1$, $a_2(x)|p_2(x)\frac{x^n-1}{g_2(x)}$.

Thus we have proved the following theorem for the characterization of cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$:

Theorem 2.3.5. [26] Let C be a cyclic code over $F_2 + uF_2 + vF_2 + uvF_2$ of length n. Then C is an ideal in R_n that can be generated by $C =< g_2(x) + up_2(x) + vg_3(x) + uvp_3(x), ua_2(x) + vg_4(x) + uvp_4(x), vg_1(x) + uvp_1(x), uva_1(x) >$ where g_i, p_i, a_i are polynomials in $F_2[x]/(x^n - 1)$ with

$a_2|g_2|x^n - 1$, $a_2|p_2\frac{x^n-1}{g_2}$, $a_1|g_1|x^n - 1$, $a_1|p_1\frac{x^n-1}{g_1}$.

Of course, the lack of conditions on g_3, g_4, p_3, p_4 takes away from the practical value of this characterization. However, things become more promising when n is odd.

Second if n is odd

When n is odd, by [5], $(F_2 + uF_2)[x]/(x^n - 1)$ is a principal ideal ring and so, cyclic codes over $F_2 + uF_2$ are characterized as principal ideals. We will make use of that characterization to simplify the result in the last Theorem when n is odd.

With the same notations as before, suppose C is a cyclic code of length n over the ring $F_2 + uF_2 + vF_2 + uvF_2$. Then $\Psi(C)$ is a cyclic code over $F_2 + uF_2$ and $ker(\Psi)$ is v times a cyclic code of length over $F_2 + uF_2$ of odd length n. Thus we have

$Im(\Psi) =< g_1(x) + ua_1(x) >$

where g_1 and a_1 are binary polynomials with $a_1|g_1|x^n - 1$ and similarly

$ker(\Psi) = v < g_2(x) + ua_2(x) >$

where g_2 and a_2 are binary polynomials with $a_2|g_2|x^n - 1$. Now combining these two we see that we can write

$C =< g_1(x) + up_1(x) + vb(x), vg_2(x) + uvp_2(x) >$

with the same conditions on g_i and p_i. Now $b(x)$ is a polynomial in $(F_2+uF_2)[x]/(x^n-1)$. Hence we can write

$b(x) = b_1(x) + ub_2(x)$, $b_1, b_2 \in F_2[x]/(x^n - 1)$.

Now, in order to get conditions on b_1, b_2, we will use a different homomorphism. Define

$\Psi_v : F_2 + uF_2 + vF_2 + uvF_2 \longrightarrow F_2 + vF_2$ as

$\Psi_v(a + bu + vc + uvd) = a + vc$.

Note that $F_2 + vF_2$ and $F_2 + uF_2$ are exactly the same sub-rings because $v^2 = 0$ in $F_2 + uF_2 + vF_2 + uvF_2$ and so everything works in the exact same way as the case of $F_2 + uF_2$. Now if $C =< g_1(x) + up_1(x) + vb(x), vg_2(x) + uvp_2(x) >$, we get

$\Psi_v(C) =< g_1(x) + vb_1(x), vg_2(x) >$.

Now, we know $\Psi_v(C)$ is a cyclic code over $F_2 + vF_2$ of odd length. By [2], the form of $\Psi_v(c)$ is unique for any cyclic code over $F_2 + vF_2$. So, we see that we must have $g_2|g_1|x^n - 1$ and $g_2|b_1\frac{x^n-1}{g_1}$. We can take $deg(b_1) < deg(g_2)$. Since n is odd, $x^n - 1$ can be written uniquely as the product of distinct irreducible factors and hence

$GCD(g_2, \frac{x^n-1}{g_1}) = 1$.

But we know $g_2|b_1\frac{x^n-1}{g_1}$, which means $g_2|b_1$. But $deg(b_1) < deg(g_2)$ implies that $b_1 = 0$. Thus we have proved the following theorem:

Theorem 2.3.6. [26] Let C be a cyclic code over $F_2 + uF_2 + vF_2 + uvF_2$ of length n for odd n. Then C is an ideal in R_n that can be generated by

$C =< g_1(x) + up_1(x) + uvb_2(x), vg_2(x) + uvp_2(x) >$

where g_i, p_i, b_2 are polynomials in $F_2[x]/(x^n - 1)$ satisfying the conditions

$p_1|g_1|x^n - 1$, $p_2|g_2|x^n - 1$, $g_2|g_1|x^n - 1$.

Cyclic codes of length 2^k for some k:

We saw in the proof of Theorem 2.3.4, that it is very easy to distinguish units from non-units in R_{2^k}. To obtain zero-divisors, all we need is to take $g(x) = c_0+c_1x+...+c_{2^k-1}x^{2^k-1}$ such that an even number of c_i's are units.

First we recall the definition 2.1.9 and definition 2.1.10 of the gray map ϕ_L and the lee weight w_L.

The case $k = 2$ By taking suitable $g(x) \in R_4$, we get the following Table of cyclic codes of length 4 and their binary images under the gray map ϕ_L :

$g(x) = 1 + uv + (1 + u)x + (u + v)x^2 + uvx^3$ and $\phi_L(< g(x) >) = [16, 12, 2]$

$g(x) = u + uv + ux + (u + v)x^2 + ux^3$ and $\phi_L(< g(x) >) = [16, 8, 4]$

$g(x) = uv + vx + (u + v)x^2 + ux^3$ and $\phi_L(< g(x) >) = [16, 6, 6]$

$g(x) = 1 + (1 + u)x + (1 + uv)x^2 + (1 + u + uv)x^3$ and $\phi_L(< g(x) >) = [16, 5, 8]$

$g(x) = uv + uvx$ and $\phi_L(< g(x) >) = [16, 3, 8]$

The case $k = 3$ By taking suitable generators, one can get some good binary codes as images. We will only give a few non-trivial examples. If we take

$g(x) = ux + vx^2 + (u + v)x^3 + uvx^4 + (u + uv)x^5 + (v + uv)x^6 + (u + v + uv)x^7$,

then $\phi_L(< g(x) >)$ turns out to be a linear code with parameters $[32, 6, 16]$. If we take

$g(x) = 1 + u + uv + (1 + u)x + x^2 + (1 + v)x^3 + (1 + uv)x^4 + (1 + u + v + uv)x^5 + (1 + v + uv)x^6 + (1 + u + uv)x^7$,

then $\phi_L(< g(x) >)$ is a linear code with parameters $[32, 14, 8]$.

The last case we want to look at is the case when $k = 1$. In this case we will obtain cyclic codes of length 2 in our ring. If we take $g(x) = u + vx$, then $\phi_L(< g(x) >)$ is a self-dual optimal code with parameters $[8, 4, 4]$.

Binary images of cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$

Definition 2.3.7. [26] Let T be the cyclic shift as defined before . We say that a linear code C is an ι-quasi-cyclic code if it is invariant under T^ι.

Lemma 2.3.8. [26] Let T be the cyclic shift. Then

$\phi_L \circ T = T^4 \circ \phi_L$.

Proof. Note that if $\bar{c} = (c_0, c_1, ..., c_{n-1}) \in (F_2 + uF_2 + vF_2 + uvF_2)^n$, then
$(\phi_L \circ T)(\bar{c}) = (\phi_L(c_{n-1}), \phi_L(c_0), ..., \phi_L(c_{n-2}))$.
Now, on the other hand we know
$\phi_L(c_0, c_1, ..., c_{n-1}) = (\phi_L(c_0), \phi_L(c_1), ..., \phi_L(c_{n-1}))$
where each $\phi_L(c_i)$ is of length 4, hence if we apply the cyclic shift four times, the whole of $\phi_L(c_{n-1})$ will shift from the end to the beginning, which means we will get
$(T^4 \circ \phi_L)(\bar{c}) = (\phi_L(c_{n-1}), \phi_L(c_0), ..., \phi_L(c_{n-2}))$.
then the desired equality is obtained □

Theorem 2.3.9. [26] Let C be a cyclic code of length n over the ring $F_2 + uF_2 + vF_2 + uvF_2$. Then $\phi_L(C)$ is a 4-quasi-cyclic binary linear code of length $4n$.

Proof. We know that C is cyclic over R if and only if $T(C) = C$. Now suppose $T(C) = C$, applying ϕ_L to both sides we get
$\phi_L(T(C)) = \phi_L(C)$.
But, by the last Lemma, we know $\phi_L \circ T = T^4 \circ \phi_L$, then we obtain
$\phi_L(C) = \phi_L(T(C)) = (\phi_L \circ T)(C) = T^4(\phi_L(C))$,
which implies that $\phi_L(C)$ is invariant under T^4. But this proves that $\phi_L(C)$ is a 4-quasi-cyclic code. □

2.4 Consta-cyclic Codes Over The Ring $F_2 + uF_2 + vF_2 + uvF_2$

Consta-cyclic codes constitute a remarkable generalization of cyclic codes, hence form an important class of linear codes in the coding theory. and, Consta-cyclic codes also have practical applications as they can be encoded with shift registers.
In this section we denote $F_2 + uF_2 + vF_2 + uvF_2$ as R_2, and $F_2 + uF_2$ as R_1.

First we recall the definition 2.1.9 and definition 2.1.10 of the gray map ϕ_L and the lee weight w_L. ϕ_L is a distance preserving isometry from (R_2^n, d_L) to (F_2^{4n}, d_H), where d_L and d_H denote the Lee and Hamming distance in R_2^n and F_2^{4n} respectively. This means if C is a linear code over R_2 with parameters $[n, k, d]$, then $\phi_L(C)$ is a binary linear code of parameters $[4n, k, d]$ by Lemma 2.2.2.
Expressing elements of R_2 as $a + bu + cv + duv = r + vq$, where $r = a + bu$ and $q = c + du$

are both in R_1, we see that

$w_{L_2}(a + bu + cv + duv) = w_{L_2}(r + vq) = w_{L_1}(q, r + q)$,

where w_{L_i} denotes the Lee weight defined in R_i. This leads to the following Gray map

$\Phi : R_2 \to R_1^2$

$\Phi(a + ub + vc + duv) = \Phi(r + vq) = (q, q + r) = (c + du, a + c + (b + d)u)$.

It is easy to verify Φ is a linear map and distance preserving. We will extend Φ to R_2^n naturally as follows:

$\Phi(c_1, c_2, ..., c_n) = (q_1, q_2, ..., q_n, q_1 + r_1, q_2 + r_2, ..., q_n + r_n)$,- - - - -(*)

where $c_i = r_i + vq_i$. Now we can say that Φ is a linear isometry from (R_2^n,Lee distance) to (R_1^{2n},Lee distance).

$(1 + v)$-Consta cyclic codes over R_2 of odd length

A cyclic shift on R_2^n is a permutation T such that

$T(c_0, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, c_1, ..., c_{n-2})$,

A linear code C over R_2 of length n is said to be a cyclic code if it is invariant under the cyclic shift, i.e., $T(C) = C$.

Definition 2.4.1. [16] Let $c = (c_0, c_1, ..., c_{n-1})$ be a word of length n then a $(1 + v)$-consta cyclic shift $\gamma(c)$ is a word of length n

$\gamma(c_0, c_1, ..., c_{n-1}) = ((1 + v)c_{n-1}, c_0, ..., c_{n-2})$

Definition 2.4.2. [16] A code C is said to be $(1+v)$-consta cyclic if $\gamma(c) \in C$, whenever $c \in C$.

Using the polynomial representation of code words in R_2^n in $R_2[x]$, we see that for a codeword $\bar{c} \in R_2^n$, $T(\bar{c})$ corresponds to $xc(x)$ in $R_2[x]/(x^n - 1)$, while $\gamma(\bar{c})$ corresponds to $xc(x)$ in $R_2[x]/(x^n - (1+v))$. The following is an extension of the characterization of cyclic and consta cyclic codes over R_1:

Proposition 2.4.3. [27] (1) A subset C of R_2^n is a linear cyclic code of length n over R_2 if and only if its polynomial representation is an ideal of the ring $R_n = R_2[x]/(x^n - 1)$. (2) A subset C of R_2^n is a linear $(1+v)$-consta cyclic code of length n over R_2 if and only if its polynomial representation is an ideal of the ring $S_n = R_2[x]/(x^n - (1 + v))$.

Proposition 2.4.4. [27] Let $\mu : R_2[x]/(x^n-1) \to R_2[x]/(x^n-(1+v))$ be defined as $\mu(c(x)) = c((1+v)x)$.
If n is odd, then μ is a ring isomorphism from R_n to S_n.

Proof. Note that since $(1+v)$ is a unit in R_2, this means, $(1+v)^2 = 1$. But, this implies that if n is odd, then
$(1+v)^n = (1+v)$.
Now, suppose $a(x) \equiv b(x) \pmod{x^n-1}$, i.e. $a(x) - b(x) = (x^n-1)q(x)$ for some $q(x) \in R_2[x]$. then if we replace x by $(1+v)x$ we have
$a((1+v)x) - b((1+v)x) = ((1+v)^n x^n - 1)q((1+v)x) = ((1+v)x^n - (1+v)^2)q((1+v)x) = (1+v)(x^n-(1+v))q((1+v)x)$,
which means if $a(x) \equiv b(x) \pmod{x^n-1}$, then $a((1+v)x) \equiv b((1+v)x) \pmod{x^n-(1+v)}$.
And the converse can easily be shown as
Let $a((1+v)x) \equiv b((1+v)x)(mod\ x^n-(1+v))$, then
$a((1+v)x) - b((1+v)x) = (x^n-(1+v)).r(x)$ for some $r(x) \in R_2[x]$, now if we replace x by $(1+v)x$ we have
$a((1+v)^2x) - b((1+v)^2x) = (x^n(1+v)^n - (1+v)).r((1+v)x)$
$a(x) - b(x) = ((1+v)x^n - (1+v)).r((1+v)x) = (1+v)(x^n-1)r((1+v)x)$
so $a(x) \equiv b(x)(mod\ x^n-1)$, Then we have

$$a(x) \equiv b(x) \pmod{x^n-1} \Longleftrightarrow a((1+v)x) \equiv b((1+v)x) \pmod{x^n-(1+v)}.$$

Note that one side of the implication tells us that μ is well defined and the other side tells us that it is injective, but since the rings are finite this proves that μ is an isomorphism. □

The following is a natural corollary of the proposition:

Corollary 2.4.5. [27] I is an ideal of R_n if and only if $\mu(I)$ is an ideal of S_n when n is odd.

Now by using Theorem 2.3.6 and the isomorphism μ defined above, we can classify the consta cyclic codes over R_2 of odd length

Corollary 2.4.6. [27] Let C be a $(1+v)$-consta cyclic code over R_2 of odd length n. Then C is an ideal in $S_n = R_2[x]/(x^n-(1+v))$ that can be generated by
$C =< g_1(\tilde{x}) + up_1(\tilde{x}) + uvb_2(\tilde{x}), vg_2(\tilde{x}) + uvp_2(\tilde{x}) >$,

where $\tilde{x} = (1+v)x$ and g_i, p_i, b_2 are polynomials in $F_2[x]/(x^n-1)$ satisfying the conditions $p_1 \mid g_1 \mid x^n - 1, p_2 \mid g_2 \mid x^n - 1, g_2 \mid g_1 \mid x^n - 1$.

Note that if we define $\bar{\mu} : R_2^n \to R_2^n$ by
$\bar{\mu}(c_0, c_1, ..., c_{n-1}) = (c_0, (1+v)c_1, (1+v)^2 c_2, ..., (1+v)^{n-1} c_{n-1})$
we see that $\bar{\mu}$ acts as the vector equivalent of μ on R_2^n. So, we can restate Corollary 2.4.5 in terms of vectors as well:

Corollary 2.4.7. [27] C is a linear cyclic code over R_2 of odd length n if and only if $\bar{\mu}(C)$ is a linear $(1+v)$-consta cyclic code of length n over R_2.

Now, note that if $r = a+ub+vc+uvd \in R_2$, then $(1+v)r = a+ub+v(a+c)+uv(b+d)$ which means that
$w_{L_2}(r) = w_H((a+b+c+d, c+d, b+d, d)) = w_H(c+d, a+b+c+d, d, b+d) = w_{L_2}((1+v)r)$
Going back to the last Corollary, we have the following result:

Corollary 2.4.8. [27] C is a cyclic code over R_2 of parameters $[n, k, d]$ if and only if $\bar{\mu}(C)$ is a $(1+v)$-consta cyclic code over R_2 of parameters $[n, k, d]$, where n is odd.

Proposition 2.4.9. [27] Let γ be the $(1+v)$-consta cyclic shift on R_2^n and let T be the cyclic shift on R_1^n. With Φ being the Gray map from R_2^n to R_1^{2n} defined as $(*)$ in page 54, then we have
$\Phi\gamma = T\Phi$.

Proof. Let $\bar{c} = (c_0, c_1, ..., c_{n-1}) \in R_2^n$ with $c_i = r_i + vq_i$, where $r_i, q_i \in R_1$. Then we have that
$\Phi(c_0, c_1, ..., c_{n-1}) = (q_0, q_1, ..., q_{n-1}, q_0 + r_0, q_1 + r_1, ..., q_{n-1} + r_{n-1})$
and so we get
$T\Phi(\bar{c}) = (q_{n-1} + r_{n-1}, q_0, q_1, ..., q_{n-1}, q_0 + r_0, ..., q_{n-2} + r_{n-2})$.
On the other hand, we know
$\gamma(\bar{c}) = ((1+v)c_{n-1}, c_0, c_1, ..., c_{n-2})$,
which, combined with $c_{n-1} = r_{n-1} + vq_{n-1}$ and $(1+v)c_{n-1} = r_{n-1} + v(r_{n-1} + q_{n-1})$ gives us
$\Phi\gamma(\bar{c}) = (q_{n-1} + r_{n-1}, q_0, q_1, ..., q_{n-1}, q_0 + r_0, ..., q_{n-2} + r_{n-2})$.
which proofs the proposition. □

Now we obtain the following main result:

Theorem 2.4.10. [27] The Gray image of a linear $(1+v)$-consta cyclic code over R_2 of length n is a linear cyclic code over R_1 of length 2n.

Proof. Let C be a linear $(1+v)$-consta cyclic code over R_2 of length n. Then this means $\gamma(C) = C$ and so
$\Phi\gamma(C) = \Phi(C)$.
But, then by the last Proposition we see that
$T\Phi(C) = \Phi\gamma(C) = \Phi(C)$,
which means $\Phi(C)$ is cyclic over R_1. □

Now let us take a one-generator $(1 + v)$-consta cyclic code over R_2 of length n, i.e. we take an ideal in $R_2[x]/(x^n - (1 + v))$ that is generated by some polynomial $r(x) + vq(x) \in R_2[x]/(x^n - (1 + v))$. Note that in this case, $r(x), q(x)$ are in $R_1[x]$ of degree $< n$. We have the following result about the Gray image of such a code in R_1:

Theorem 2.4.11. [27] Suppose $C =< r(x) + vq(x) >$ is a $(1 + v)$-consta cyclic code over R_2 of length n. Then $\Phi(C)$ is a cyclic code over R_1 of length $2n$ that is generated by the polynomials $q(x) + x^n(r(x) + q(x))$ and $r(x) + x^n r(x)$.

Proof. Here, we will actually just apply Φ to polynomials. Note that $\Phi(r(x) + vq(x)) = (q(x), r(x)+q(x))$ which gives us the same vector as $q(x)+x^n(r(x)+q(x))$ in $R_1[x]/(x^{2n}-1)$. On the other hand, C being an ideal, we know that $va(x)(r(x) + vq(x)) \in C$ for all $a(x) \in R_1[x]$, so as a result we get $va(x)r(x) \in C$ whose image under Φ is $a(x)(r(x), r(x))$ which gives us the same vector as $a(x)(r(x) + x^n r(x))$ in $R_1[x]/(x^{2n} - 1)$. Note that
$(a(x) + vb(x))(r(x) + vq(x)) = a(x)(r(x) + vq(x)) + vb(x)r(x)$
and so
$\Phi[(a(x) + vb(x))(r(x) + vq(x))] = a(x)[q(x) + x^n(r(x) + q(x))] + b(x)(r(x) + x^n r(x))$.
Since, $a(x)$ and $b(x)$ are arbitrary polynomials in $R_1[x]$ of degrees $< n$, this proves the theorem. □

We finish this section with a few examples of even length $(1+v)$-consta cyclic codes:

Example 2.4.12. [27] Let $n = 2$ and take the one-generator $(1 + v)$-consta cyclic code $< (1 + u) + (1 + v)x >$. Then by the last Theorem, $\Phi(C)$ is a cyclic code over R_1 of length 4, generated by the polynomials $x + (1 + u)x^2$ and $(1 + u) + x + (1 + u)x^2 + x^3$. The binary image of C turns out to be a linear code with parameters $[8, 6, 2]$.

Example 2.4.13. [27] Let $n = 4$. Take C_1, C_2, C_3 to be $(1+v)$-consta cyclic codes over R_2 of length 4, generated by the polynomials $1 + ux + (1 + u + v)x^2 + vx^3, 1 + (1 + u + v)x + (1 + u)x^2 + (1 + u + uv)x^3$ and $u + vx + (u + v)x^2 + uvx^3$ respectively. Then $\Phi(C_1), \Phi(C_2), \Phi(C_3)$ are cyclic codes over R_1 of length 8 that are generated by pairs
$\{x^2 + x^3 + x^4 + ux^5 + ux^6 + x^7, (1 + ux + (1 + u)x^2)(1 + x^4)\}$,
$\{x + ux^3 + x^4 + ux^5 + (1 + u)x^6 + x^7, (1 + (1 + u)x + (1 + u)x^2 + (1 + u)x^3)(1 + x^4)\}$,
and $\{x + x^2 + ux^3 + ux^4 + x^5 + (1 + u)x^6 + ux^7, u + ux^2 + ux^4 + ux^6\}$
respectively. The binary images of C_1, C_2 and C_3 turn out to be binary linear codes of parameters $[16, 12, 2], [16, 10, 4]$ and $[16, 6, 6]$, respectively.

Remark: 1. For odd length $(1+v)$-consta cyclic codes, a full characterization is given in section 2.4, However for even length a partial characterization is given for one generator $(1 + v)$-consta cyclic codes in terms of cyclic codes over R_1 in Theorem 2.4.11.
2. For any unit $x \in R_2$ we have $x^2 = 1$, so for any odd $n \in N$ we have $x^n = x$. for this reason the characterization of $(1 + v)$-consta cyclic codes over R_2 of odd length in section 2.4 holds for any x-consta cyclic codes over R_2 of odd length.

Chapter 3

Codes Over The Ring

$F_q + uF_q + vF_q + uvF_q$

3.1 linear Codes Over The Ring $F_q + uF_q + vF_q + uvF_q$

In this section we want to make a generalization for the work in section 2.1. from the ring $F_2 + uF_2 + vF_2 + uvF_2$ to the ring $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p, and $u^2 = v^2 = 0$,$uv = vu$.

First lets talk a bout some properties of the ring $R = F_q + uF_q + vF_q + uvF_q$ which were established in [23]:

R is a Frobenius, local ring with characteristic p which is not principal ideal nor a chain ring. The ideals can be listed as:

$I_0 = \{0\} \subseteq I_{uv} = uv(F_q + uF_q + vF_q + uvF_q) = uvF_q \subseteq I_u, I_v, I_{u+v} \subseteq I_{u,v} \subseteq I_1 = R$, where

$I_u = u(F_q + uF_q + vF_q + uvF_q) = uF_q + u^2F_q + uvF_q + u^2vF_q = uF_q + uvF_q$,

$I_v = v(F_q + uF_q + vF_q + uvF_q) = vF_q + uvF_q + v^2F_q + uv^2F_q = vF_q + uvF_q$,

$I_{u,v} = uF_q + vF_q + uvF_q$,

$I_{u+v} = (u+v)(F_q+uF_q+vF_q+uvF_q) = (u+v)F_q+u(u+v)F_q+v(u+v)F_q+uv(u+v)F_q =$
$(u+v)F_q + (u^2+uv)F_q + (uv+v^2)F_q + (u^2v+uv^2)F_q = (u+v)F_q + uvF_q + uvF_q =$
$(u+v)F_q + 2uvF_q = (u+v)F_q + uvF_q$, since 2 is a unit in R.

Let $R^* = R - I_{u,v}$, we can see that R^* consists of all units in R. The unique maximal ideal $I_{u,v}$ is not a principal ideal. $I_{u,v}$ contains all the zero divisors in R.

Remark: [23] Another nice conclusion about the ring R is that if $x = a + bu + cv + duv$

is any element in R, then $x^q = a$, where $a, b, c, d \in F_q$.

Proof. Let $x = a + bu + cv + duv \in R$, where $a, b, c, d \in F_q$. Then
If x is a nonunit then $x \in I_{u,v} = uF_q + vF_q + uvF_q$, so $a = 0$ and $x^q = 0 = a$ since $u^2 = v^2 = 0$ and $uv = vu$.
If x is a unit then $x \in R - I_{u,v}$, so $a \neq 0$ and $x^q = a^q$ since $u^2 = v^2 = 0$ and $uv = vu$, but $a \in F_q$ and $F_q - \{0\}$ is a cyclic group under multiplication of order $q-1$ so $a^{q-1} = 1$ then $a^q = a$ so $x^q = a$. □

Remark: $F_q + uF_q + vF_q + uvF_q$ is isomorphic to $F_q[X, Y]/ < X^2, Y^2, XY - YX >$.

Proof. we define a map
$f : F_q + uF_q + vF_q + uvF_q \to F_q[X, Y]/ < X^2, Y^2, XY - YX >$
s.t. $f(a+bu+cv+duv) = a+bx+cy+dxy+ < X^2, Y^2, XY-YX >, \forall a+bu+cv+duv \in F_q + uF_q + vF_q + uvF_q$, now we show that f is an isomorphism similarly as the proof of the remark in section 2.1 page (31). □

Definition 3.1.1. A linear code C of length n over the ring $F_q + uF_q + vF_q + uvF_q$ is an $F_q + uF_q + vF_q + uvF_q$-submodule of $(F_q + uF_q + vF_q + uvF_q)^n$.

Now we classify the generators of the linear codes over R and we define R-linear independence of them to introduce a possible type for linear codes over R.
There are six types of generators for linear codes over R, and we can classify them as $\bar{a}, \bar{b}, \bar{c}, \bar{d}, \bar{e}, \bar{f}$, where
$\bar{a} \in (F_q + uF_q + vF_q + uvF_q)^n \backslash (I_{u,v})^n$
$\bar{b} \in (I_{u,v})^n$,$\bar{b} \notin$(I$_u$)^n,$(I_v)^n$,$(I_{u+v})^n$,
$\bar{c} \in (I_u)^n \backslash (I_{uv})^n$
$\bar{d} \in (I_v)^n \backslash (I_{uv})^n$
$\bar{e} \in (I_{u+v})^n \backslash (I_{uv})^n$
$\bar{f} \in (I_{uv})^n$.

Remark: [23] The generators of the form $\bar{a}$ contain some units.

Proof. Let $(x_1, x_2, ..., x_n) \in \bar{a}$ s.t. $x_i \notin I_{u,v} \forall i$ then x_i is a unit in $F_q + uF_q + vF_q + uvF_q$, so $\exists$ a unit $x_i^{-1} \notin I_{u,v} \forall i$, so $\exists (x_1^{-1}, x_2^{-1}, ..., x_n^{-1}) \in \bar{a}$ s.t. $(x_1, x_2, ..., x_n).(x_1^{-1}, x_2^{-1}, ..., x_n^{-1}) = (x_1.x_1^{-1}, x_2.x_2^{-1}, ..., x_n.x_n^{-1}) = (1, 1, ..., 1)$ which is the unity of $(F_q + uF_q + vF_q + uvF_q)^n$, so $(x_1, x_2, ..., x_n)$ is a unit in $(F_q + uF_q + vF_q + uvF_q)^n$. □

The generators of the form $\bar{a}$ that contain some units are called free generators. We next define independence over R for these generators.

Definition 3.1.2. A subset
$S = \{\{\bar{a}_i\}_1^{k_1}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$
of R^n is said to be R-linearly independent if the only solution to the equation
$\sum_{i=1}^{k_1} \alpha_i \bar{a}_i + \sum_{j=1}^{k_2} \beta_j \bar{b}_j + \sum_{m=1}^{k_3} \gamma_m \bar{c}_m + \sum_{t=1}^{k_4} \mu_t \bar{d}_t + \sum_{r=1}^{k_5} \eta_r \bar{e}_r + \sum_{s=1}^{k_6} \zeta_s \bar{f}_s = \bar{0}$,
where
$\alpha_i \in F_q + uF_q + vF_q + uvF_q, \beta_j \in F_q + uF_q + vF_q, \gamma_m \in F_q + vF_q, \mu_t \in F_q + uF_q, \eta_r \in F_q + uF_q, \zeta_s \in F_q$
is
$\alpha_i, \beta_j, \gamma_m, \mu_t, \eta_r, \zeta_s = 0$ for all indices i, j, m, t, r, s.
Now we can take independent vectors as our generators to generate a linear code over R:

Definition 3.1.3. Suppose
$S = \{\{\bar{a}_i\}_1^{k_1}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$
is a set of linearly independent generators as was defined above. The linear code C of length n generated by S is the submodule
$\{\sum_{i=1}^{k_1} \alpha_i \bar{a}_i + \sum_{j=1}^{k_2} \beta_j \bar{b}_j + \sum_{m=1}^{k_3} \gamma_m \bar{c}_m + \sum_{t=1}^{k_4} \mu_t \bar{d}_t + \sum_{r=1}^{k_5} \eta_r \bar{e}_r + \sum_{s=1}^{k_6} \zeta_s \bar{f}_s$: $\alpha_i \in F_q + uF_q + vF_q + uvF_q, \beta_j \in F_q + uF_q + vF_q, \gamma_m \in F_q + vF_q, \mu_t \in F_q + uF_q, \eta_r \in F_q + uF_q, \zeta_s \in F_q\}$
In this case we say C is of type $(q^4)^{k_1}(q^3)^{k_2}(u)^{k_3}(v)^{k_4}(u+v)^{k_5}(q)^{k_6}$.

The following theorem will be quite useful in establishing the uniqueness of the type for codes over R.

Lemma 3.1.4. If $S = \{\{\bar{a}_i\}_1^{k_1}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$ is a set of linearly independent generators which generate the linear code C, then the number of codewords in C that belong to I_{uv}^n is exactly $q^{k_1+2k_2+k_3+k_4+k_5+k_6}$.

Proof. Because of the linear independence the only codewords in C that belong toI_{uv}^n can arise from the binary linear combinations of
$\{\{uv\bar{a}_i\}_1^{k_1}, \{u\bar{b}_{j_1}\}_1^{k_2}, \{v\bar{b}_{j_2}\}_1^{k_2}\{v\bar{c}_m\}_1^{k_3}, \{u\bar{d}_t\}_1^{k_4}, \{u\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$
Again, because of linear independence, these generators will all be linearly independent over F_q. That is why we will have exactly $q^{k_1+2k_2+k_3+k_4+k_5+k_6}$ such codewords. □

After this auxiliary result, we are now ready to settle the main question about the uniqueness of the type, given the existence of independent generators.

Theorem 3.1.5. If $S = \{\{\bar{a}_i\}_1^{k_1}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$ is a set of linearly independent generators which generate the linear code C, then C cannot be generated by another type, i.e. $k_1, k_2, ..., k_6$ are uniquely determined by the code.

Proof. Suppose S generates a linear code C. Then the first equation we get is about the size of the code.

$q^{4k_1+3k_2+2k_3+2k_4+2k_5+k_6}=\mid C \mid$.

If we multiply every element of the code by u, then this will nullify some of the generators, because uI_u=0,$uI_{uv} = 0$. Since $uI_{u,v}$=uI_v=uI_{u+v}=I_{uv} and $u(F_2 + uF_2 + vF_2 + uvF_2)$= I_u, the linear independence of the generators tells us that

$q^{2k_1+k_2+k_4+k_5}=\mid uC \mid$.

Similarly we obtain

$q^{2k_1+k_2+k_3+k_5}=\mid vC \mid$,

$q^{2k_1+k_2+k_3+k_4}=\mid (u+v)C \mid$.

If C_{uv} denotes the set of all codewords in C that belong to I_{uv}^n, then by the last Lemma we see that

$q^{k_1+2k_2+k_3+k_4+k_5+k_6}=\mid C_{uv} \mid$.

Finally multiplying the elements of R by uv nullifies every element except the units, hence we get

$q^{k_1}=\mid uvC \mid$

Since all the sizes on the right hand side of the equations are powers of q, we will take logarithms base q from the first to the last equation, and calling $\log_q \mid C \mid$=A_1, $\log_q \mid uC \mid$=A_2, and so on. We obtain the following system of linear equations for $k_i's$:

$4k_1 + 3k_2 + 2k_3 + 2k_4 + 2k_5 + k_6 = A_1$

$2k_1 + k_2 + k_4 + k_5 = A_2$

$2k_1 + k_2 + k_3 + k_5 = A_3$

$2k_1 + k_2 + k_3 + k_4 = A_4$

$k_1 + 2k_2 + k_3 + k_4 + k_5 + k_6 = A_5$

$k_1 = A_6$

The coefficient matrix for the system of equations is

$$\begin{pmatrix} 4 & 3 & 2 & 2 & 2 & 1 \\ 2 & 1 & 0 & 1 & 1 & 0 \\ 2 & 1 & 1 & 0 & 1 & 0 \\ 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

which has determinant 1. This proves the uniqueness of $k_1, k_2, ..., k_6$ which means we can talk about a unique type for the code C, provided that independent generators are given for C. □

Now that we have established the uniqueness of the type for linear codes over R, we can extract some further information about these codes given the type. This will help us characterize the codes that have independent generators. To this extent, we will take a code C of type$(q^4)^{k_1}(q^3)^{k_2}(u)^{k_3}(v)^{k_4}(u+v)^{k_5}(q)^{k_6}$ which has generators of the form
$S = \{\{\bar{a}_i\}_1^{k_2}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$
that are linearly independent. The independence tells us that to obtain codewords that fall in the ideal I_{uv}, we need to take the binary combinations of
$\{\{uv\bar{a}_i\}_1^{k_2}, \{u\bar{b}_{j_1}\}_1^{k_2}, \{v\bar{b}_{j_2}\}_1^{k_2}\{v\bar{c}_m\}_1^{k_3}, \{u\bar{d}_t\}_1^{k_4}, \{u\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}$.
A similar argument can easily be employed to see that the codewords that fall entirely in the ideal I_u will arise from the combinations of the form
$\sum_{i=1}^{k_1} \alpha_i\bar{a}_i + \sum_{j=1}^{k_2} \beta_j\bar{b}_j + \sum_{m=1}^{k_3} \gamma_m\bar{c}_m + \sum_{t=1}^{k_4} \mu_t\bar{d}_t + \sum_{r=1}^{k_5} \eta_r\bar{e}_r + \sum_{s=1}^{k_6} \zeta_s\bar{f}_s$
where $\alpha_i \in uF_q + uvF_q$,$\beta_j \in uF_q + vF_q$,$\gamma_m \in F_q + vF_q$,$\mu_t \in uF_q$,$\eta_r \in uF_q$,$\zeta_s \in F_q$. This tells us that the total number of codewords in C that fall entirely in the ideal I_u is
$q^{2k_1+2k_2+2k_3+k_4+k_5+k_6}$- - - - - - - - - - -(1)

For the ideal I_v, the codewords that fall entirely in the ideal I_v will arise from the combinations of the form
$\sum_{i=1}^{k_1} \alpha_i\bar{a}_i + \sum_{j=1}^{k_2} \beta_j\bar{b}_j + \sum_{m=1}^{k_3} \gamma_m\bar{c}_m + \sum_{t=1}^{k_4} \mu_t\bar{d}_t + \sum_{r=1}^{k_5} \eta_r\bar{e}_r + \sum_{s=1}^{k_6} \zeta_s\bar{f}_s$
where $\alpha_i \in vF_q + uvF_q$, $\beta_j \in uF_q + vF_q$, $\gamma_m \in vF_q$, $\mu_t \in F_q + uF_q$, $\eta_r \in uF_q$, $\zeta_s \in F_q$. This tells us that the total number of codewords in C that fall entirely in the ideal I_v is
$q^{2k_1+2k_2+k_3+2k_4+k_5+k_6}$- - - - - - - - - - -(2)

For the ideal I_{u+v}, the codewords that fall entirely in the ideal I_{u+v} will arise from the combinations of the form

$\sum_{i=1}^{k_1} \alpha_i \bar{a}_i + \sum_{j=1}^{k_2} \beta_j \bar{b}_j + \sum_{m=1}^{k_3} \gamma_m \bar{c}_m + \sum_{t=1}^{k_4} \mu_t \bar{d}_t + \sum_{r=1}^{k_5} \eta_r \bar{e}_r + \sum_{s=1}^{k_6} \zeta_s \bar{f}_s$
where $\alpha_i \in uF_q + vF_q$, $\beta_j \in uF_q + vF_q$, $\gamma_m \in vF_q$, $\mu_t \in uF_q$, $\eta_r \in F_q + uF_q$, $\zeta_s \in F_q$. This tells us that the total number of codewords in C that fall entirely in the ideal I_{u+v} is
$q^{2k_1+2k_2+k_3+2k_4+2k_5+k_6}$- - - - - - - - - - -(3)

For the ideal $I_{u,v}$, for a codeword to be entirely in $I_{u,v}$ it must be of the form
$\sum_{i=1}^{k_1} \alpha_i \bar{a}_i + \sum_{j=1}^{k_2} \beta_j \bar{b}_j + \sum_{m=1}^{k_3} \gamma_m \bar{c}_m + \sum_{t=1}^{k_4} \mu_t \bar{d}_t + \sum_{r=1}^{k_5} \eta_r \bar{e}_r + \sum_{s=1}^{k_6} \zeta_s \bar{f}_s$
where $\alpha_i \in uF_q + vF_q + uvF_q$,$\beta_j \in F_q + uF_q + vF_q$,$\gamma_m \in F_q + vF_q$,$\mu_t \in F_q + uF_q$,$\eta_r \in F_q + uF_q$,$\zeta_s \in F_q$. which means the total number of codewords in C that fall entirely in the ideal $I_{u,v}$ is
$q^{3k_1+3k_2+2k_3+2k_4+2k_5+k_6}$- - - - - - - - - - -(4)

So, combining the last Lemma with the equations (1),(2),(3) and (4) we obtain the following result:

Lemma 3.1.6. Let C be a linear code over the ring R of type $(q^4)^{k_1}(q^3)^{k_2}(u)^{k_3}(v)^{k_4}(u+v)^{k_5}(q)^{k_6}$, If $N_{uv}, N_u, N_v, N_{u+v}, N_{u,v}$ denote the number of codewords in C that fall entirely in the ideals $I_{uv}, I_u, I_v, I_{u+v}, I_{u,v}$, respectively, then
$\{N_{uv}, N_u, N_v, N_{u+v}, N_{u,v}\}$=$q^{k_1+2k_2+k_3+k_4+k_5+k_6}\{1, q^{k_1+k_3}, q^{k_1+k_4}, q^{k_1+k_5}, q^{2k_1+k_2+k_3+k_4+k_5}\}$.

Now lets define the Gray map over R and the Lee weight on R similarly as the definition in section 2.1.:

Definition 3.1.7. Let $\phi : (F_q + uF_q + vF_q + uvF_q)^n \to F_q^{4n}$ be the map given by $\phi(\bar{a} + u\bar{b} + v\bar{c} + uv\bar{d}) = (\bar{a} + \bar{b} + \bar{c} + \bar{d}, \bar{c} + \bar{d}, \bar{b} + \bar{d}, \bar{d})$, where $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in F_q^n$.

We note from the definition that ϕ is a linear map that takes a linear code over $F_q + uF_q + vF_q + uvF_q$ of length n to a linear code of length $4n$. By using this map, we can define the Lee weight w_L as follows:

Definition 3.1.8. For any element $a+ub+vc+uvd$∈$\mathrm{F}_q+uF_q+vF_q+uvF_q$ we define the lee weight of $a+ub+vc+uvd$ as $w_L(a+ub+vc+uvd) = w_H(a+b+c+d, c+d, b+d, d)$, where w_H denotes the ordinary Hamming weight for codes over F_q, also for any two codewords c_1,c_2 ∈$\mathrm{F}_q + uF_q + vF_q + uvF_q$ we define the lee distance $d_L(c_1, c_2) = w_L(c_1 - c_2)$.

From the definition of ϕ we can see that ϕ is a distance preserving isometry from $((F_q + uF_q + vF_q + uvF_q)^n, d_L)$ to (F_q^{4n}, d_H), where d_L denotes the lee distance in $(F_q + uF_q + vF_q + uvF_q)^n$ and d_H denotes the hamming distance in F_q^{4n}.

Let $F_q + uF_q + vF_q + uvF_q = \{g_1, g_2, ..., g_{q^4}\}$ in some order. For example, we might assume $g_1 = 0$,$g_2 = 1$,... and so on.

Definition 3.1.9. The complete weight enumerator of a linear code C over $F_q + uF_q + vF_q + uvF_q$ is defined as
$cwe_C(X_1, X_2, ..., X_{q^4}) = \sum_{\bar{c} \in C}(X_1^{n_{g_1}(\bar{c})} X_2^{n_{g_2}(\bar{c})} ... X_{q^4}^{n_{g_{q^4}}(\bar{c})})$
where $n_{g_i}(\bar{c})$ is the number of appearances of g_i in the vector $\bar{c}$.

Remark: Note that $cwe_C(X_1, X_2, ..., X_{q^4})$ is a homogeneous polynomial in q^4 variables with the total degree of each term being n, the length of the code. Since $\bar{0} \in C$, we see that the term X_1^n always appears in $cwe_C(X_1, X_2, ..., X_{q^4})$.
We also observe that $cwe_C(1, 1, ..., 1) = \mid C \mid$.

Recall that $N_u(C)$ was the number of codewords in C that lie entirely in the ideal I_u, we can see that
$N_u(C) = cwe_C(x_1, x_2, ..., x_{q^4})$
with $x_i = 0$ when $g_i \notin I_u$ and $x_i = 1$ when $g_i \in I_u$ Similar descriptions can be given for N_{uv}, N_v, and so on.

3.2 Self-dual Codes Over The Ring F_q+uF_q+vF_q+uvF_q

In this section we are trying to make an extension for the work in section 2.2. from the ring $F_2 + uF_2 + vF_2 + uvF_2$ to the ring $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p, and $u^2 = v^2 = 0, uv = vu$, The problem we face in this section is that some of the theorems in section 2.2. holds only when the characteristic of the ring is 2 so it holds only for the ring $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime 2, and other theorems in section 2.2. hold for any commutative finite Frobenius ring so it holds for the ring $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p.

Let $R = F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p, and lets recall definition 3.1.7 and definition 3.1.8 of the gray map ϕ and the lee weight w_L.

And similarly as in section 2.2. we can see from the definitions that ϕ is linear and distance-preserving map thus we obtain the following lemma, which will later be useful:

Lemma 3.2.1. If C is a linear code over R of length n, size q^k and minimum lee distance d, then $\phi(C)$ is an $[4n, k, d]$-linear code over F_q.

Also the inner product and duality are defined as before in section 1.4, and note that if C is a linear code of length n, then $C^{\perp}$ is also a linear code over R of length n.

Theorem 3.2.2. Let C be a linear code over R of length n, where q is a power of the prime 2. Then $\phi(C^{\perp}) \subseteq (\phi(C))^{\perp}$ with $(\phi(C))^{\perp}$ denoting the ordinary dual of $(\phi(C))$ as a code over F_q.

Proof. same proof of Theorem 2.1.12. □

We first start with the following lemma which is called the double-annihilator relation from [6], and holds for all Frobenius rings and in particular for our ring R, since R is a Frobenius ring:

Lemma 3.2.3. If C is a linear code over R of length n, then $\mid C \mid . \mid C^{\perp} \mid = \mid R \mid^n = (q^4)^n$.

Theorem 3.2.4. Suppose C is a self-dual linear code over R of length n, where q is a power of the prime 2. Then $\phi(C)$ is a self-dual linear code of length 4n.

Proof. since C is self dual then $C = C^{\perp}$ and $\mid C \mid = \mid C^{\perp} \mid$ but by Lemma 3.2.3 $\mid C \mid . \mid C^{\perp} \mid = (q^4)^n$ then $\mid C \mid = \mid C^{\perp} \mid = (q^4)^{\frac{n}{2}} = q^{2n}$, now $\phi(C^{\perp}) = \phi(C) \subseteq (\phi(C))^{\perp}$ by Theorem 3.2.2 that is $\phi(C)$ is self orthogonal code, also by Lemma 3.2.1 $\mid C \mid = \mid \phi(C) \mid = q^{2n}$, and since $\mid \phi(C) \mid . \mid (\phi(C))^{\perp} \mid = (q^4)^n$ then $\mid (\phi(C))^{\perp} \mid = q^{2n} = \mid \phi(C) \mid$, combining this result with $\phi(C) \subseteq (\phi(C))^{\perp}$ we have $\phi(C) = (\phi(C))^{\perp}$, that is $\phi(C)$ is self dual code of length 4n by Lemma 3.2.1. □

We first need an example of a self dual code over R of length $n = 1$.

Example 3.2.5. Let $R = F_q + uF_q + vF_q + uvF_q$ where q is a power of the prime p and $u^2 = v^2 = 0, uv = vu$ and let C be the linear code of length $n = 1$ over R generated by the element $u \in R$ which is not a unit since $u \in I_{u,v}$ i.e. $C =< u >$, any element in $< u >$ has the form $u(a+bu+cv+duv) = au+bu^2+cuv+du^2v = au+b.0+cuv+d.0 = au+cuv$, for some $a, b, c, d \in F_q$, so $< u >= \{au + cuv : a, c \in F_q\}$ that is $\mid < u > \mid = q^2$, more over if $au + buv, cu + duv \in < u >$ then:

1) $(au + buv)^2 = a^2u^2 + 2abu^2v + b^2u^2v^2 = a^2.0 + 2ab.0.v + b^2.0.0 = 0$

2) $(au+buv)(cu+duv) = acu^2+adu^2v+bcu^2v+bdu^2v^2 = ac.0+ad.0.v+bc.0.v+bd.0.0 = 0$

Hence every element of $< u >$ is orthogonal to itself and orthogonal to any other element in $< u >$ so $C \subseteq C^{\perp}$ that is C is self orthogonal, but $\mid C \mid . \mid C^{\perp} \mid = |R|^n = |R|^1 = q^4$,

and since $|C| = q^2$ then $|C^{\perp}| = q^2 =\mid C \mid$, combining this result with $C \subseteq C^{\perp}$ we have $C = C^{\perp}$, i.e. $C =< u >$ is a self dual linear code over R of length 1.

Now we need to recall lemma 2.2.5 which holds for the ring $R = F_q + uF_q + vF_q + uvF_q$ since R is a finite Frobenius ring.

The existence of a self-dual code over R of length $n = 1$ implies by lemma 2.2.5 that:

Theorem 3.2.6. Self-dual codes over R of all lengths $n \in N$ exist.

3.3 Cyclic Codes Over The Ring $F_q + uF_q + vF_q + uvF_q$

In this section we recall the cyclic codes over the ring $R = F_q + uF_q + vF_q + uvF_q$ where the ring R is not a chain ring, see [23]. we study the polynomial ring $R_n = (F_q + uF_q + vF_q + uvF_q)[x]/(x^n - 1)$ and use the correspondence relationship between the cyclic codes over R and the ideals of R_n, also we recall the characterization of cyclic codes over R. Finally, we study the characterization of the Gray map and the image of cyclic codes over R.

The notions of the cyclic shift and cyclic codes are standard for codes over all rings. Briefly, a cyclic shift on R^n is a permutation T such that
$T(c_0, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$.
A linear code C over the ring R that is invariant under the cyclic shift is called a cyclic code i.e. $T(C) = C$.
For any ring $\tilde{R}$, we can define a mapping $P : \tilde{R}^n \to \tilde{R}[x]/(x^n - 1)$ by $P(c_0, c_1, ..., c_{n-1}) = c_0 + c_1 x + ... + c_{n-1}x^{n-1}$.
Then a linear code C of length n over $\tilde{R}$ is a cyclic code if and only if $P(C)$ is an ideal of $\tilde{R}[x]/(x^n - 1)$.
Hence, in order to discuss cyclic codes over the ring R, we are necessary to discuss the ideals of the polynomial ring R_n.

Lemma 3.3.1. [23] The ring R_n is not a principal ideal ring.

Proof. Similar to the proof of Lemma 2.3.1. □

Theorem 3.3.2. [23] if $n = p^k.m$, with $m \equiv 1(modp)$, then the ring R_n is not a local ring.

Proof. We will use the definition of local rings from [11] in which it is described that a ring R is a local ring if and only if the set of all non-units in R forms a maximal ideal. Define $\gamma : R_n \to R$, where $\gamma(c_0 + c_1x + ... + c_{n-1}x^{n-1}) = c_0 + c_1 + ... + c_{n-1}$. then γ is a surjective ring homomorphism.

Now, suppose that $n = p^k m$, $m \equiv 1(modp)$. Note that $0 = x^{p^k m} - 1 = x^{p^k m} + p - 1 = (x^{p^k} + p - 1)(x^{p^k(m-1)} + x^{p^k(m-2)} + ... + x^{p^k} + 1)$ in R_n. so $f_1(x) = x^{p^k(m-1)} + x^{p^k(m-2)} + ... + x^{p^k} + 1$ is a zero divisor. Hence $f_1(x)$ is a non-unit.

when $m \equiv 1(modp)$, we have $\gamma(x^{p^k(m-2)}+x^{p^k(m-3)}+...+x^{p^k}+1) = 1+1+...+1 = m-1 = 0$ in R. because γ is a ring homomorphism, let $f_2(x) = -x^{p^k(m-2)} - x^{p^k(m-3)} - ... - x^{p^k} - 1$. then $f_2(x)$ is also a non-unit. because $x^{p^k(m-1)}x^{p^k} = x^{p^k m} = 1$ and $f_1(x) + f_2(x) = x^{p^k(m-1)}$, so $f_1(x) + f_2(x)$ is a unit in R_n. this means that non-units can not form an ideal and hence R_n can not be a local ring. □

Lemma 3.3.3. [23] Every non-unit, non-zero element of R_n must be a zero divisor.

Proof. Similar to the proof of Lemma 2.3.3. □

Theorem 3.3.4. [23] If $n = q^k$, where q is the power of the prime p, then R_n is a local ring for all natural numbers k.

Proof. Because (any element).(non-unit) cannot be a unit. so, in order to prove the theorem, we need to prove that the set of all non-units in R_{q^k} forms an additive subgroup. Let $\alpha = c_0 + c_1x + ... + c_{q^k-1}x^{q^k-1} \in R_{q^k}$. Because the characteristic of R_{q^k} is p and $x^{q^k} = 1$ in R_{q^k}, we have $\alpha^{q^k} = c_0^{q^k} + c_1^{q^k} + ... + c_{q^k-1}^{q^k}$. also we know that each $c_i \in R$. Hence in R_{q^k}, we get $\alpha^{q^k} \in F_q$. Now if $\alpha^{q^k} = 0$, this means $\alpha^{q^k} = \alpha.\alpha^{q^k-1} = 0$, so α is a zero devisor. If $\alpha^{q^k} \neq 0$, then α is a unit. So if α is not a unit, then $\alpha^{q^k} = 0$.

Let $c_i = \acute{a}_i + \acute{b}_i u + \acute{c}_i v + \acute{d}_i uv$, where $(i = 0, 1, ..., q^k - 1)$ with $\acute{a}_i, \acute{b}_i, \acute{c}_i, \acute{d}_i \in F_q$. but we know that each $c_i^{q^k} = \acute{a}_i$ by the Remark in page (59), so

$\alpha^{q^k} = \acute{a}_0 + \acute{a}_1 + ... + \acute{a}_{q^k-1}$.

Let $\forall \beta, \mu \in R_{q^k}$ are two non-units. When $\beta = 0$, $\mu \neq 0$, we have $\beta - \mu$ is also a non-unit, when $\beta \neq 0$, $\mu \neq 0$, let $\beta = b_0 + b_1x + ... + b_{q^k-1}x^{q^k-1}$, $\mu = d_0 + d_1x + ... + d_{q^k-1}x^{q^k-1}$ where $b_i = f_i + g_iu + h_iv + k_iuv$, $d_i = \acute{f}_i + \acute{g}_iu + \acute{h}_iv + \acute{k}_iuv$ $(i = 0, 1, ..., q^k - 1)$ with $f_i, g_i, h_i, k_i, \acute{f}_i, \acute{g}_i, \acute{h}_i, \acute{k}_i \in F_q$ namely, also we have $\beta^{q^k} = f_0 + f_1 + ... + f_{q^k-1} = 0$, $\mu^{q^k} = \acute{f}_0 + \acute{f}_1 + ... + \acute{f}_{q^k-1} = 0$. Then

$(\beta - \mu)^{q^k} = (b_0 - d_0)^{q^k} + (b_1 - d_1)^{q^k} + ... + (b_{q^k-1} - d_{q^k-1})^{q^k} = (b_0^{q^k} - d_0^{q^k}) + (b_1^{q^k} - d_1^{q^k}) +$

$... + (b_{q^k-1}^{q^k} - d_{q^k-1}^{q^k}) = (f_0 + f_1 + ... + f_{q^k-1}) - (\acute{f}_0 + \acute{f}_1 + ... + \acute{f}_{q^k-1}) = 0.$
So, $\beta - \mu$ is a non-unit. This implies that the set of all non-units in R_{q^k} forms an additive subgroup. This proves the theorem. □

Now lets talk about the characterization of cyclic codes over R

Lemma 3.3.5. [14] let C be a cyclic code in $S = F_q + uF_q$ of length n where q is the power of the prime p. Then C is an ideal of $S[x]/(x^n - 1)$ that can be generated by $C =< g(x) + up(x), ua(x) >$ with $a(x) \mid g(x) \mid (x^n - 1)$, $a(x) \mid p(x)\frac{x^n-1}{g(x)}$, deg $a <$ deg p.

Lemma 3.3.6. [14] with the same notations as the last lemma, if $gcd(n, p) = 1$, then $C =< g(x) + up(x), ua(x) >=< g(x) + ua(x) >$.

Theorem 3.3.7. [23] Let C be a cyclic code in R of length n where q is the power of the prime p. Then C is an ideal of R_n that can be generated by $C =< g_2(x) + up_2(x) + vg_3(x) + uvp_3(x), ua_2(x) + vg_4(x) + uvp_4(x), vg_1(x) + uvp_1(x), uva_1(x) >$ where g_i, p_i, a_i are polynomials in $F_q[x]/(x^n - 1)$ with
$a_1 \mid g_1 \mid (x^n - 1)$, $a_1 \mid p_1\frac{x^n-1}{g_1}$, $a_2 \mid g_2 \mid (x^n - 1)$, $a_2 \mid p_2\frac{x^n-1}{g_2}$.

Proof. Define $\psi : R \to S$ by $\psi(a+bu+cv+duv) = a+bu$, then ψ is a ring homomorphism with $ker(\psi) = vF_q + uvF_q = v(F_q + uF_q)$. The homomorphism ψ can be extended to a homomorphism $\Psi : R_n \to (F_q + uF_q)[x]/(x^n - 1)$ by
$\Psi(c_0 + c_1x + ... + c_{n-1}x^{n-1}) = \psi(c_0) + \psi(c_1)x + ... + \psi(c_{n-1})x^{n-1}$.
Let C be a cyclic code in R of length n, then C is an ideal of the ring R_n. Restrict Ψ onto C, it is clear that $\Psi(C)$ is an ideal in $(F_q + uF_q)[x]/(x^n - 1)$ and hence a cyclic code over the ring $F_q + uF_q$. By the property of homomorphism, we know that $ker(\Psi)$ is an ideal in $v(F_q+uF_q)[x]/(x^n-1)$ and hence a cyclic code over $v(F_q+uF_q)$. We can think of $ker(\Psi)$ to be v times a cyclic code in F_q+uF_q. By using the characterization of the cyclic code over $F_q + uF_q$ in lemma 3.3.5, we can have $ker(\Psi) = v < g_1(x) + up_1(x), ua_1(x) >$, $\Psi(C) =< g_2(x) + up_2(x), ua_2(x) >$ where g_i, p_i, a_i are polynomials in $F_q[x]/(x^n - 1)$ satisfying the conditions $a_1 \mid g_1 \mid (x^n - 1), a_1 \mid p_1\frac{x^n-1}{g_1}$,$a_2 \mid g_2 \mid (x^n - 1), a_2 \mid p_2\frac{x^n-1}{g_2}$. So, $C =< g_2(x) + up_2(x) + vg_3(x) + uvp_3(x), ua_2(x) + vg_4(x) + uvp_4(x), vg_1(x) + uvp_1(x), uva_1(x) >$. □

Theorem 3.3.8. [23] Let C be a cyclic code in R of length n where q is the power of the prime p. When $gcd(n, p) = 1$, then C is an ideal of R_n that can be generated by $C =< g_1(x) + up_1(x) + uvb_2(x), vg_2(x) + uvp_2(x) >$ where g_i, p_i, b_2 are polynomials in $F_q[x]/(x^n - 1)$ with $p_1 \mid g_1 \mid (x^n - 1)$, $p_2 \mid g_2 \mid (x^n - 1)$, $g_2 \mid g_1 \mid (x^n - 1)$.

Proof. By following the same process, let C be a cyclic code in R of length n. Then $\Psi(C)$ is a cyclic code in $F_q + uF_q$ and $ker(\Psi)$ is v times a cyclic code in $F_q + uF_q$. When $gcd(n,p) = 1$, by the last lemma, we have $ker(\Psi) = v < g_1(x) + up_1(x) >$, $\Psi(C) =< g_2(x) + up_2(x) >$ where g_i, p_i are polynomials in $F_q[x]/(x^n - 1)$ with $p_1 \mid g_1 \mid (x^n - 1)$, $p_2 \mid g_2 \mid (x^n - 1)$. Then we can write

$C =< g_1(x) + up_1(x) + vb(x), vg_2(x) + uvp_2(x) >$

with the same conditions on g_i, p_i. Now $b(x)$ is a polynomial in $(F_q + uF_q)[x]/(x^n - 1)$. Let $b(x) = b_1(x) + ub_2(x)$. $b_1, b_2 \in F_q[x]/(x^n - 1)$.

Now, we will use a different ring homomorphism to get conditions on b_1, b_2.

Define $\varphi : F_q + uF_q + vF_q + uvF_q \to F_q + vF_q$, by letting $\varphi(a + bu + cv + duv) = a + cv$. Note that $F_q + uF_q \cong F_q + vF_q$. By following the same process we have

$\varphi(C) =< g_1(x) + vb_1(x), vg_2(x) >$

So, $\varphi(c)$ is a cyclic code in $F_q + vF_q$ satisfying the conditions $g_2 \mid g_1 \mid (x^n - 1), g_2 \mid b_1 . \frac{(x^n-1)}{g_1}$. We may assume $deg(b_1) < deg(g_2)$. Since $gcd(n,p) = 1$, then $x^n - 1$ factors uniquely into a product of distinct irreducible polynomials and hence $gcd(g_2, \frac{(x^n-1)}{g_1}) = 1$. We know $g_2 \mid b_1$. But $deg(b_1) < deg(g_2)$ implies that $b_1 = 0$. Therefore we have proved the theorem. □

We can also study the images of cyclic codes over R, see [23]

Let T be the cyclic shift, which is given by $T(c_0, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$. If the linear code C is invariant under T^ι, then C an ι-quasi-cyclic code.

Now consider the following definition of the gray map ϕ as in section 3.1 but in a different way.

Definition 3.3.9. [23] $\phi : R \to F_q^4$, as $a + bu + cv + duv \mapsto (a + b + c + d, c + d, b + d, d)$. Then ϕ can naturally be extended to

$\Phi : R^n \to F_q^{4n}$ by $(c_0, c_1, ..., c_{n-1}) \mapsto (\phi(c_0), \phi(c_1), ..., \phi(c_{n-1}))$.

Lemma 3.3.10. Let T be the cyclic shift defined before. Then

$\Phi \circ T = T^4 \circ \Phi$.

Proof. Let $\bar{c} = (c_0, c_1, ..., c_{n-1}) \in R^n$, then $(\Phi \circ T)\bar{c} = (\phi(c_{n-1}), \phi(c_0), ..., \phi(c_{n-2}))$.

On the other hand we have $\Phi(c_0, c_1, ..., c_{n-1}) = (\phi(c_0), \phi(c_1), ..., \phi(c_{n-1}))$ where each $\phi(c_i)$ is of length 4, therefore if we use the cyclic shift T four times, the whole of $\phi(c_{n-1})$ will move from the last to the beginning, which implies we will get $(T^4 \circ \Phi)\bar{c} =$

$(\phi(c_{n-1}), \phi(c_0), ..., \phi(c_{n-2}))$.

Thus we have

$\Phi \circ T = T^4 \circ \Phi$. □

Lemma 3.3.11. [23] Let C be a cyclic code in R of length n, then $\Phi(C)$ is a 4-quasi-cyclic linear code in F_q of length 4n.

Proof. We know that C is a cyclic code over R if and only if $T(C) = C$. Now applying Φ to both sides we get

$\Phi(T(C)) = \Phi(C)$ and so we have

$\Phi(C) = \Phi(T(C)) = (\Phi \circ T)(C) = (T^4 \circ \Phi)(C) = T^4(\Phi(C))$,

which means that $\Phi(C)$ is invariant under T^4. This proves the Lemma. □

3.4 Consta-cyclic Codes Over The Ring $F_q + uF_q + vF_q + uvF_q$

In this section we are trying to make an extension for the work in section 2.4 from the ring $F_2 + uF_2 + vF_2 + uvF_2$ to the ring $F_q + uF_q + vF_q + uvF_q$ where q is a power of a prime p, $u^2 = v^2 = 0$ and $uv = vu$.

In this section we denote the ring $F_q + uF_q + vF_q + uvF_q$ as R.

Note that the element $1 + v \in \mathrm{R}^* = R - I_{u,v}$ as in section 3.1. which means that $1 + v$ is a unit.

A $(1 + v)$-consta cyclic shift γ acts on R^n as

$\gamma(c_0, c_1, ..., c_{n-1}) = ((1 + v)c_{n-1}, c_0, c_1, ..., c_{n-2})$.

Using the polynomial representation of code words in R^n in $R[x]$, we see that for a codeword $\bar{c} \in R^n$, $T(\bar{c})$ corresponds to $xc(x)$ in $R[x]/(x^n - 1)$, while $\gamma(\bar{c})$ corresponds to $xc(x)$ in $R[x]/(x^n - (1 + v))$.

Proposition 3.4.1. (1) A subset C of R^n is a linear cyclic code of length n over R if and only if its polynomial representation is an ideal of the ring $R_n = R[x]/(x^n - 1)$.

(2) A subset C of R^n is a linear $(1 + v)$-consta cyclic code of length n over R if and only if its polynomial representation is an ideal of the ring $S_n = R[x]/(x^n - (1 + v))$.

$(1 + v)$-Consta cyclic codes over R where $n = q - 1$

Proposition 3.4.2. Let $\mu : R[x]/(x^n - 1) \to R[x]/(x^n - (1 + v))$ be defined as $\mu(c(x)) = c((1 + v)x)$.

If $n = q - 1$, then μ is a ring isomorphism from R_n to S_n.

Proof. Note that since $(1 + v) \in R$, then $(1 + v)^q = 1$ by the Remark in page (59).

Now, suppose $a(x) \equiv b(x)(mod(x^n - 1))$, for some $a(x), b(x) \in R_n$, i.e. $a(x) - b(x) = (x^n - 1)r(x)$ for some $r(x) \in R[x]$. Then

$a((1+v)x)-b((1+v)x) = ((1+v)^n x^n-1)r((1+v)x) = ((1+v)^{q-1}x^n-(1+v)^q)r((1+v)x) = (1 + v)^{q-1}(x^n - (1 + v))r((1 + v)x)$,

which means if $a(x) \equiv b(x)(mod(x^n - 1))$, then $a((1 + v)x) \equiv b((1 + v)x)(mod(x^n - (1 + v)))$, that is $\mu(a(x)) \equiv \mu(b(x))(mod(x^n - (1 + v)))$, this proves that μ is well defined.

to prove the converse let

$\mu(a(x)) \equiv \mu(b(x))mod(x^n - (1 + v))$, i.e. $a((1 + v)x) \equiv b((1 + v)x)mod(x^n - (1 + v))$, that is $a((1 + v)x) - b((1 + v)x) = (x^n - (1 + v))h(x)$, fore some $h(x) \in R[x]$, now if we replace x by $(1 + v)^{q-1}x$ we get:

$a((1+v)(1+v)^{q-1}x) - b((1+v)(1+v)^{q-1}x) = [x^n(1+v)^{n(q-1)} - (1+v)]h((1+v)^{q-1}x) \Rightarrow$

$a((1 + v)^q x) - b((1 + v)^q x) = [x^n(1 + v)^{n(q-1)} - (1 + v)]h((1 + v)^{q-1}x) \Rightarrow$

$a(x) - b(x) = [x^n(1 + v)^{(q-1)(q-1)} - (1 + v)]h((1 + v)^{q-1}x) =$

$[x^n(1 + v)^{(q-1)^2} - (1 + v)]h((1 + v)^{q-1}x) =$

$[x^n(1 + v)^{q^2-2q+1} - (1 + v)]h((1 + v)^{q-1}x) =$

$[x^n(1 + v)^{q^2}(1 + v)^{-2q}(1 + v)^1 - (1 + v)]h((1 + v)^{q-1}x) =$

$[x^n((1 + v)^q)^2((1 + v)^q)^{-2}(1 + v) - (1 + v)]h((1 + v)^{q-1}x) =$

$[x^n(1)^2(1)^{-2}(1 + v) - (1 + v)]h((1 + v)^{q-1}x) =$

$[x^n(1)(1)(1 + v) - (1 + v)]h((1 + v)^{q-1}x) =$

$[x^n(1 + v) - (1 + v)]h((1 + v)^{q-1}x) =$

$(1 + v)[x^n - 1]h((1 + v)^{q-1}x)$,

which means that $a(x) \equiv b(x)(mod(x^n - 1))$, this proves that μ is injective (one to one), so

$a(x) \equiv b(x)(mod(x^n - 1)) \iff a((1 + v)x) \equiv b((1 + v)x)(mod(x^n - (1 + v)))$.

But since the rings are finite $\mid R_n \mid = \mid S_n \mid$ this proves that μ is an isomorphism. □

The following is a natural corollary of the proposition:

Corollary 3.4.3. I is an ideal of R_n if and only if $\mu(I)$ is an ideal of S_n when $n = q - 1$.

By using Theorem 3.3.7 and the isomorphism μ defined above, we can classify the $(1+v)$-consta cyclic codes over R of length $n = q-1$:

Corollary 3.4.4. Let C be a $(1+v)$-consta cyclic code over R of length $n = q-1$ where q is a power of the prime p. then C is an ideal of $S_n = R[x]/(x^n - (1+v))$ that can be generated by $C =< g_2(\tilde{x}) + up_2(\tilde{x}) + vg_3(\tilde{x}) + uvp_3(\tilde{x}), ua_2(\tilde{x}) + vg_4(\tilde{x}) + uvp_4(\tilde{x}), vg_1(\tilde{x}) + uvp_1(\tilde{x}), uva_1(\tilde{x}) >$ where $\tilde{x} = (1+v)x$ and g_i, p_i, a_i are polynomials in $F_q[x]/(x^n-1)$ with
$a_1 \mid g_1 \mid (x^n-1), a_1 \mid p_1\frac{x^n-1}{g_1}, a_2 \mid g_2 \mid (x^n-1), a_2 \mid p_2\frac{x^n-1}{g_2}$.

Note that if we define $\bar{\mu} : R^n \to R^n$ by
$\bar{\mu}(c_0, c_1, ..., c_{n-1}) = (c_0, (1+v)c_1, (1+v)^2c_2, ..., (1+v)^{n-1}c_{n-1})$
we see that $\bar{\mu}$ acts as the vector equivalent of μ on R^n. So, we can restate Corollary 3.4.3 in terms of vectors as well.

Corollary 3.4.5. C is a linear cyclic code over R of length $n = q-1$ if and only if $\bar{\mu}(C)$ is a linear $(1+v)$-consta cyclic code of length n over R.

Now lets take another especial case:

$(1+v)$-Consta cyclic codes over R When q is a power of 2

If $p = 2$ then the characteristic of R is 2, and so
$(1+v)^2 = 1^2+2v+v^2 = 1+0+0 = 1$ and also if n is any odd number then $(1+v)^n = (1+v)$, note that n is odd which means that $gcd(n, p) = 1$ since $p = 2$, in this case we see that things going to work may be the same as in section 2.4.

Proposition 3.4.6. Let $\mu : R[x]/(x^n-1) \to R[x]/(x^n-(1+v))$ be defined as
$\mu(c(x)) = c((1+v)x)$.
If n is odd, then μ is a ring isomorphism from R_n to S_n.

Proof. the same proof of Proposition 2.4.4. □

Corollary 3.4.7. I is an ideal of R_n if and only if $\mu(I)$ is an ideal of S_n when n is odd.

By using Theorem 3.3.8 and the isomorphism μ defined above, we can classify the $(1+v)$-consta cyclic codes over R of odd length.

Corollary 3.4.8. Let C be a $(1+v)$-consta cyclic code over R of odd length n, where q is the power of the prime 2, then C is an ideal of S_n that can be generated by $C =< g_1(\tilde{x}) + up_1(\tilde{x}) + uvb_2(\tilde{x}), vg_2(\tilde{x}) + uvp_2(\tilde{x}) >$ where $\tilde{x} = (1+v)x$ and g_i, p_i, b_2 are polynomials in $F_q[x]/(x^n-1)$ with $p_1 \mid g_1 \mid (x^n-1)$, $p_2 \mid g_2 \mid (x^n-1)$, $g_2 \mid g_1 \mid (x^n-1)$.

Corollary 3.4.9. C is a linear cyclic code over R of odd length n if and only if $\bar{\mu}(C)$ is a linear $(1+v)$-consta cyclic code of length n over R.

Note that if $r = a+ub+vc+uvd \in R$, then $(1+v)r = a+ub+v(a+c)+uv(b+d)$ which means that
$w_L(r) = w_H((a+b+c+d, c+d, b+d, d)) = w_H(c+d, a+b+c+d, d, b+d) = w_L((1+v)r)$
Going back to the last Corollary, we have the following result:

Corollary 3.4.10. C is a cyclic code over R of parameters $[n,k,d]$ if and only if $\bar{\mu}(C)$ is a $(1+v)$-consta cyclic code over R of parameters $[n,k,d]$, where n is odd.

Now let $R = F_q + uF_q + vF_q + uvF_q$ and $R_1 = F_q + uF_q$ where q is a power of the prime p.

Expressing elements of R as $a+bu+cv+duv = r+vq$, where $r = a+bu$ and $q = c+du$ are both in R_1, we see that
$w_L(a+bu+cv+duv) = w_L(r+vq) = w_{L_1}(q, r+q)$,
where w_L and w_{L_1} denotes the Lee weight defined in R and R_1 respectively. This leads to the following Gray map $\Phi : R \to R_1^2$
$\Phi(a+ub+vc+duv) = \Phi(r+vq) = (q, q+r) = (c+du, a+c+(b+d)u)$.
It is easy to verify Φ is a linear map and distance preserving. We will extend Φ to R^n naturally as follows:
$\Phi(c_1, c_2, ..., c_n) = (q_1, q_2, ..., q_n, q_1+r_1, q_2+r_2, ..., q_n+r_n)$,
where $c_i = r_i + vq_i$. Now we can say that Φ is a linear isometry from (R^n,Lee distance) to (R_1^{2n},Lee distance).

Proposition 3.4.11. Let γ be the $(1+v)$-consta cyclic shift on R^n and let T be the cyclic shift on R_1^n, with Φ being the previous Gray map from R^n to R_1^{2n}, then we have $\Phi\gamma = T\Phi$.

Proof. the same proof of Proposition 2.4.9. □

Theorem 3.4.12. The Gray image of a linear $(1+v)$-consta cyclic code over R of length n is a linear cyclic code over R_1 of length $2n$.

Proof. the same proof of Theorem 2.4.10. □

We finish this section with some examples

Example 3.4.13. Let $q = 2^2 = 4$, and let $n = 1$, then $x^1-1 = (x-1).1$ in F_4, let C be the ideal in $S_1 = F_4+uF_4+vF_4+uvF_4[x]/(x-(1+v))$ generated by $C =< 1+u+uv, v+uv >$ of length $n = 1$, Then by corollary 3.4.8 C is a $(1 + v)$-consta cyclic code over the ring $F_4 + uF_4 + vF_4 + uvF_4$ of length $n = 1$, also by Theorem 3.4.12 $\Phi(C)$ is a cyclic code over $F_4 + uF_4$ of length 2.

Example 3.4.14. Let $q = 3$, and let $n = 2 = q - 1$, then $x^2 - 1 = (x - 1)(x + 1)$ in F_3, let C be the ideal in $S_2 = F_3 + uF_3 + vF_3 + uvF_3[x]/(x^2 - (1 + v))$ generated by $C =< (\tilde{x}+1)+u(\tilde{x}+1), u, v(\tilde{x}-1)+uv(\tilde{x}-1), uv >$ of length $n = 2$ where $\tilde{x} = (1+v)x$, Then by corollary 3.4.4 C is a $(1+v)$-consta cyclic code over the ring $F_3+uF_3+vF_3+uvF_3$ of length $n = 2$, also by Theorem 3.4.12 $\Phi(C)$ is a cyclic code over $F_3 + uF_3$ of length 4.

3.5 Another Gray Map On The Ring $F_q + uF_q + vF_q + uvF_q$

During this work we have dealt with a gray map ϕ over the ring $F_2 + uF_2 + vF_2 + uvF_2$ as was introduced in section 2.1., then we have used the same gray map ϕ over the ring $F_q + uF_q + vF_q + uvF_q$ as in section 3.1., also through the gray map ϕ we have defined the lee weight over the ring $F_q + uF_q + vF_q + uvF_q$ where q is a power of the prime p and $u^2 = v^2 = 0, uv = vu$.
In this section we are about to introduce a gray map on the ring $F_q + uF_q + vF_q + uvF_q$ which can be extended to $(F_q + uF_q + vF_q + uvF_q)^n$, and by this map we define the lee weight over the ring $F_q + uF_q + vF_q + uvF_q$.

Definition 3.5.1. Let ϕ be a gray map defined as $\phi : F_q + uF_q + vF_q + uvF_q \to F_q^9$ s.t. for any $a + ub + vc + uvd \in F_q + uF_q + vF_q + uvF_q$
$\phi(a+ub+vc+uvd) = (a+b+c+d, c+d, b+d, a+d, b+c+d, a+c+d, a+b+d, a+b+c, d)$.

Definition 3.5.2. For any $a+ub+vc+uvd \in F_q+uF_q+vF_q+uvF_q$ we define the lee weight W_L as $W_L(a+ub+vc+uvd) = W_H(\phi(a+ub+vc+uvd))$, where W_H denotes the ordinary hamming weight over F_q, also for any x_1,x_2 $\in$F$_q+uF_q+vF_q+uvF_q$ we define the lee distance $d_L(x_1,x_2) = W_L(x_1-x_2)$.

Claim: ϕ is a linear map.

Proof. 1$\cdot$ for any $a_1+ub_1+vc_1+uvd_1, a_2+ub_2+vc_2+uvd_2 \in F_q+uF_q+vF_q+uvF_q$
$\phi((a_1+ub_1+vc_1+uvd_1)+(a_2+ub_2+vc_2+uvd_2)) = \phi(a_1+a_2+u(b_1+b_2)+v(c_1+c_2)+uv(d_1+d_2)) = ((a_1+b_1+c_1+d_1)+(a_2+b_2+c_2+d_2),(c_1+d_1)+(c_2+d_2),(b_1+d_1)+(b_2+d_2),(a_1+d_1)+(a_2+d_2),(b_1+c_1+d_1)+(b_2+c_2+d_2),(a_1+c_1+d_1)+(a_2+c_2+d_2),(a_1+b_1+d_1)+(a_2+b_2+d_2),(a_1+b_1+c_1)+(a_2+b_2+c_2),d_1+d_2) = (a_1+b_1+c_1+d_1,c_1+d_1,b_1+d_1,a_1+d_1,b_1+c_1+d_1,a_1+c_1+d_1,a_1+b_1+d_1,a_1+b_1+c_1,d_1)+(a_2+b_2+c_2+d_2,c_2+d_2,b_2+d_2,a_2+d_2,b_2+c_2+d_2,a_2+c_2+d_2,a_2+b_2+d_2,a_2+b_2+c_2,d_2) = \phi(a_1+ub_1+vc_1+uvd_1)+\phi(a_2+ub_2+vc_2+uvd_2)$.
2$\cdot$ let $r \in F_q$ then for any $a+ub+vc+uvd \in F_q+uF_q+vF_q+uvF_q$
$\phi(r(a+ub+vc+uvd)) = \phi(ra+urb+vrc+uvrd) = (ra+rb+rc+rd,rc+rd,rb+rd,ra+rd,rb+rc+rd,ra+rc+rd,ra+rb+rd,ra+rb+rc,rd) = r(a+b+c+d,c+d,b+d,a+d,b+c+d,a+c+d,a+b+d,a+b+c,d) = r\phi(a+ub+vc+uvd)$.
from 1 and 2 we have that ϕ is a linear map. □

Claim: ϕ is an injective function (one to one).

Proof. let $a_1+ub_1+vc_1+uvd_1, a_2+ub_2+vc_2+uvd_2 \in F_q+uF_q+vF_q+uvF_q$ s.t.
$\phi(a_1+ub_1+vc_1+uvd_1) = \phi(a_2+ub_2+vc_2+uvd_2) \Rightarrow$(a$_1+b_1+c_1+d_1,c_1+d_1,b_1+d_1,a_1+d_1,b_1+c_1+d_1,a_1+c_1+d_1,a_1+b_1+d_1,a_1+b_1+c_1,d_1) = (a_2+b_2+c_2+d_2,c_2+d_2,b_2+d_2,a_2+d_2,b_2+c_2+d_2,a_2+c_2+d_2,a_2+b_2+d_2,a_2+b_2+c_2,d_2)$
then $d_1 = d_2$, and since $a_1+d_1 = a_2+d_2$ then $a_1 = a_2$, also $b_1+d_1 = b_2+d_2$ then $b_1 = b_2$, finally $c_1+d_1 = c_2+d_2$ then $c_1 = c_2$, which means $a_1+ub_1+vc_1+uvd_1 = a_2+ub_2+vc_2+uvd_2$ □

Claim: ϕ is a distance preserving isometry $(F_q+uF_q+vF_q+uvF_q, d_L) \to (F_q^9, d_H)$.

Proof. for any $x,y \in F_q+uF_q+vF_q+uvF_q$
$d_L(x,y) = W_L(x-y) = W_H(\phi(x-y)) = W_H(\phi(x)-\phi(y)) = d_H(\phi(x),\phi(y))$, because ϕ is a linear map. □

Now we are ready to make an extension of the gray map ϕ:

Definition 3.5.3. Let Φ be a gray map defined as $\Phi : (F_q + uF_q + vF_q + uvF_q)^n \to F_q^{9n}$ s.t. for any $(x_1, x_2, ..., x_n) \in (F_q + uF_q + vF_q + uvF_q)^n$
$\Phi(x_1, x_2, ..., x_n) = (\phi(x_1), \phi(x_2), ..., \phi(x_n))$, where $x_i \in F_q + uF_q + vF_q + uvF_q \ \forall i$

Definition 3.5.4. For any $x = (x_1, x_2, ...x_n) \in (F_q + uF_q + vF_q + uvF_q)^n$ we define the lee weight W_L as $W_L(x) = \sum_{i=1}^n W_L(x_i) = \sum_{i=1}^n W_H(\phi(x_i)) = W_H(\Phi(x))$, where W_H denotes the ordinary hamming weight over F_q, also for any x,$y \in$($F_q + uF_q + vF_q + uvF_q)^n$ we define the lee distance $d_L(x, y) = W_L(x - y)$.

Claim: Φ is a linear map.

Proof. 1· for any $(x_1, x_2, ..., x_n), (y_1, y_2, ..., y_n) \in (F_q + uF_q + vF_q + uvF_q)^n$
$\Phi((x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n)) = \Phi(x_1 + y_1, x_2 + y_2, ..., x_n + y_n) = (\phi(x_1 + y_1), \phi(x_2 + y_2), ..., \phi(x_n + y_n))$, and since ϕ is a linear map then:
$= (\phi(x_1)+\phi(y_1), \phi(x_2)+\phi(y_2), ..., \phi(x_n)+\phi(y_n)) = (\phi(x_1), \phi(x_2), ..., \phi(x_n))+(\phi(y_1), \phi(y_2), ..., \phi(y_n)) = \Phi(x_1, x_2, ..., x_n) + \Phi(y_1, y_2, ..., y_n)$.
2· let $r \in F_q$ then for any $(x_1, x_2, ..., x_n) \in (F_q + uF_q + vF_q + uvF_q)^n$
$\Phi(r(x_1, x_2, ..., x_n)) = \Phi(rx_1, rx_2, ..., rx_n) = (\phi(rx_1), \phi(rx_2), ..., \phi(rx_n))$, and since ϕ is a linear map then :
$= (r\phi(x_1), r\phi(x_2), ..., r\phi(x_n)) = r(\phi(x_1), \phi(x_2), ..., \phi(x_n)) = r\Phi(x_1, x_2, ..., x_n)$.
from 1 and 2 we have that Φ is a linear map. □

Claim: Φ is an injective function (one to one).

Proof. let $(x_1, x_2, ..., x_n), (y_1, y_2, ..., y_n) \in (F_q + uF_q + vF_q + uvF_q)^n$ s.t.
$\Phi(x_1, x_2, ..., x_n) = \Phi(y_1, y_2, ..., y_n) \Rightarrow (\phi(x_1), \phi(x_2), ..., \phi(x_n)) = (\phi(y_1), \phi(y_2), ..., \phi(y_n)) \Rightarrow \phi(x_1) = \phi(y_1), \phi(x_2) = \phi(y_2), ..., \phi(x_n) = \phi(y_n)$, and since ϕ is one to one function then :
$x_1 = y_1, x_2 = y_2, ..., x_n = y_n$, so $(x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_n)$. □

Claim: Φ is a distance preserving isometry $((F_q + uF_q + vF_q + uvF_q)^n, d_L) \to (F_q^{9n}, d_H)$.

Proof. for any $x, y \in (F_q + uF_q + vF_q + uvF_q)^n$
$d_L(x, y) = W_L(x - y) = W_H(\Phi(x - y)) = W_H(\Phi(x) - \Phi(y)) = d_H(\Phi(x), \Phi(y))$, because Φ is a linear map. □

As a result, the following observation is obvious to see:

Lemma 3.5.5. If C is a linear code over $F_q + uF_q + vF_q + uvF_q$ with parameters $[n, k, d]$ then $\Phi(C)$ is a linear code over F_q with parameters $[9n, k, d]$.

As an example, we obtain all the elements of the ring $F_3 + uF_3 + vF_3 + uvF_3$ then we find their images under the gray map $\phi : F_3 + uF_3 + vF_3 + uvF_3 \to F_3^9$, s.t. for any $a + ub + vc + uvd \in F_3 + uF_3 + vF_3 + uvF_3$
$\phi(a + ub + vc + uvd) = (a + b + c + d, c + d, b + d, a + d, b + c + d, a + c + d, a + b + d, a + b + c, d)$, at last we find the lee weight for each element in $F_3 + uF_3 + vF_3 + uvF_3$ as $W_L(a + ub + vc + uvd) = W_H(\phi(a + ub + vc + uvd))$.
First note that the ring $F_3 + uF_3 + vF_3 + uvF_3$ has $3^4 = 81$ elements and characteristic 3:

x	$\phi(x)$	$W_L(x) = W_H(\phi(x))$
0	(000000000)	0
uv	(111100001)	5
2uv	(222200002)	5
v	(110011000)	4
v+uv	(221111001)	7
v+2uv	(002211002)	5
2v	(220022000)	4
2v+uv	(001122001)	5
2v+2uv	(112222002)	7
u	(101010100)	4
u+uv	(212110101)	7
u+2uv	(020210102)	5
u+v	(211021100)	6
u+v+uv	(022121101)	7
u+v+2uv	(100221102)	6
u+2v	(021002100)	4
u+2v+uv	(102102101)	6
u+2v+2uv	(210202102)	6
2u	(202020200)	4
2u+uv	(010120201)	5
2u+2uv	(121220222)	8
2u+v	(012001200)	4
2u+v+uv	(120101201)	6
2u+v+2uv	(201201202)	6
2u+2v	(122012200)	6

x	$\phi(x)$	$W_L(x) = W_H(\phi(x))$
2u+2v+uv	(200112201)	6
2u+2v+2uv	(011212202)	7
1	(100101110)	5
1+uv	(211212211)	9
1+2uv	(022220012)	6
1+v	(210112120)	7
1+v+uv	(021220221)	7
1+v+2uv	(102001022)	5
1+2v	(020120100)	4
1+2v+uv	(101201201)	6
1+2v+2uv	(212012002)	6
1+u	(201111121)	8
1+u+uv	(012222021)	7
1+u+2uv	(120000122)	5
1+u+v	(011122200)	6
1+u+v+uv	(122200001)	5
1+u+v+2uv	(200011102)	5
1+u+2v	(121100210)	6
1+u+2v+uv	(202211011)	7
1+u+2v+2uv	(010022112)	6
1+2u	(002121000)	4
1+2u+uv	(110102102)	6
1+2u+2uv	(221010202)	6
1+2u+v	(112102010)	6
1+2u+v+uv	(220210111)	7
1+2u+v+2uv	(001021212)	6
1+2u+2v	(222110020)	6
1+2u+2v+uv	(000221121)	6

x	$\phi(x)$	$W_L(x) = W_H(\phi(x))$
1+2u+2v+2uv	(111002222)	7
2	(200202220)	5
2+uv	(011002221)	6
2+2uv	(122102222)	8
2+v	(010210220)	5
2+v+uv	(121010221)	7
2+v+2uv	(202110222)	7
2+2v	(120221220)	7
2+2v+uv	(201021221)	7
2+2v+2uv	(012121222)	8
2+u	(001212020)	5
2+u+uv	(112012021)	7
2+u+2uv	(220112022)	7
2+u+v	(111220020)	6
2+u+v+uv	(222020021)	6
2+u+v+2uv	(000120022)	4
2+u+2v	(221201020)	6
2+u+2v+uv	(002001021)	4
2+u+2v+2uv	(110101022)	6
2+2u	(102222120)	7
2+2u+uv	(210022121)	7
2+2u+2uv	(021122122)	8
2+2u+v	(212200120)	6
2+2u+v+uv	(020000121)	4
2+2u+v+2uv	(101100122)	6
2+2u+2v	(022211120)	7
2+2u+2v+uv	(100011121)	6
2+2u+2v+2uv	(211111122)	9

Example 3.5.6. Consider the gray map

$\Phi : (F_3 + uF_3 + vF_3 + uvF_3)^4 \to F_3^{9\times 4=36}$

and consider the element $(2u+2v, 1+2u+2v+uv, 2+2u+2v+2uv, 2+2u+2v+uv) \in$

$(F_3 + uF_3 + vF_3 + uvF_3)^4$

then $\Phi(2u + 2v, 1 + 2u + 2v + uv, 2 + 2u + 2v + 2uv, 2 + 2u + 2v + uv) =$

$(122012200000221121211111122100011121)$

and $W_L(2u + 2v, 1 + 2u + 2v + uv, 2 + 2u + 2v + 2uv, 2 + 2u + 2v + uv) =$

$W_H(\Phi(2u + 2v, 1 + 2u + 2v + uv, 2 + 2u + 2v + 2uv, 2 + 2u + 2v + uv)) =$

$W_H(122012200000221121211111122100011121) = 27.$

Conclusion

[1] **In this thesis, we have studied a new Gray map**
$\Phi : (F_q + uF_q + vF_q + uvF_q)^n \to F_q^{9n}$
where q is a power of prime, also we have defined the lee weight of codes over $F_q + uF_q + vF_q + uvF_q$ **through this map, and we have proved that** Φ **is linear, injective, and distance preserving.**
It would be interesting to investigate the images of linear, self dual, cyclic, and consta-cyclic codes over $F_q + uF_q + vF_q + uvF_q$ **under this map, and to see if we can apply the theorems of the old gray map to this gray map.**
[2] **Also, we have studied (1+v)-consta-cyclic codes over the ring** $F_q + uF_q + vF_q + uvF_q$ **when** $n = q - 1$**.**
It would be interesting to investigate (1+v)-consta-cyclic codes over the ring $F_q + uF_q + vF_q + uvF_q$ **when n is odd, or when n is even.**

Refrences

[1] T. Abualrub, Cyclic Codes over the ring of integers modulo m. Thesis, University of Iowa, P(46),P(66), 1998.

[2] T. Abualrub, I. Saip, Cyclic codes over the Rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$ Designs, Codes and Creptography vol.42, no.03, pp.273-287, 2007.

[3] G. Bini, F. Flamini, Finite commutative rings and their applications, University of Michigan, Universita degli Studi Roma Tre, U.S.A and Italy, 2002.

[4] I.F. Blake, Codes over certain rings, Inform. Contr. 20:396-404, 1972.

[5] H.Q. Dinh, S.R. Lopez, Cyclic and negacyclic codes over finite chain rings. IEEE Trans. Inform., pp.17281744, 2004.

[6] S.T. Dougherty, J.L. Kim, H. Kulosman, H. Liu, Self-dual codes over commutative Frobenius rings, Finite Fields Appl., inpress, doi:10.1016/j.ffa.2009.11.004.

[7] J.B. Fraleigh, First course in abstract algebra, 5^{th} Edition, 1993.

[8] M. Greferath, G.M. Guire , M.E. O'sullivan, Optimal Codes over Finite Frobenius Rings, National University of Ireland and San Diego State University, Maynooth, 2005.

[9] D. Hofman, Coding theory, 1990.

[10] W.C. Huffman, V. Pless, Fundementals of Error-Correcting Codes, Cam-

bridge, U.K. Cambridge Univ. Press, 2003.

[11] T.W. Hungerford, Algebra. Springer, New York, P(66), 1974.

[12] V.K. Khanna, A course in abstract algebra, University of Delhi Second Edition, 1998.

[13] C. Musiti, Introduction to Rings and Modules, University of Hyderabad, Second Rivisted Edition, 1994.

[14] L. ping, Z. shixin, Cyclic Codes Of Arbitrary Lengths Over The Ring $F_q + uF_q$, Journal Of University Of Science And Technology Of China, 2008.

[15] E. Prange, Cyclic Error-Correcting Codes In Two Symbols, Air Force Cambridge Research Center, Cambridge, 1957.

[16] J.F. Qian, L.N. Zhang, S.X. Zhu, $(1 + v)-$consta cyclic and cyclic codes over $F_2 + vF_2$, Appl. Math. Lett, vol.19, pp.820-823, 2006.

[17] E. Rains, N.J.A. Sloane, Self dual codes, in: V.S. Pless, W.C. Huffman(Eds.), Hand book of Coding Theory, Elsevier, Amsterdam, 1998.

[18] E.M. Rains, Shadow bounds for self dual codes, IEEETrans. Inform., pp.134139, 1998.

[19] C. Shannons, A Mathematical Theory Of Communication, Bell System Tech.J.27, 1948.

[20] J.L. Walker, Algebraic Geometric Codes Over Rings, 1991.

[21] R. Wisbauer, Foundations Of Modules And Ring Theory, Gordon and Breach Science Publishers, 1991.

[22] J.A. Wood, Finite Frobenius Rings As A Setting For Algebraic Coding Theory, Hefei University Of Technology, Hefei, Anhui June 30, 2011.

[23] X. Xiaofang, L. Xiusheng, On the Structure of Cyclic Codes over $F_q + uF_q + vF_q + uvF_q$, J.natural sciences of wuhan university,5, 2011.

[24] B. Yildiz, S. Karadeniz, Linear codes over $F_2 + uF_2 + vF_2 + uvF_2$, Des.Codes Crypt.54, 2010.

[25] B. Yildiz, S. Karadeniz, Self-dual codes over $F_2 + uF_2 + vF_2 + uvF_2$, J.Frank.Inst.347, 2010.

[26] B. Yildiz, S. Karadeniz, Cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$, Des.Codes Crypt.58, 2011.

[27] B. Yildiz, S. Karadeniz, $(1 + v)$-Consta cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$, J.Frank.Inst.348, 2011.