CYCLIC AND DIHEDRAL GROUP RING CODES

by

TAN ZI SHYUAN

Thesis submitted in fulfillment of the requirements for the degree of Master of Science

August 2016

ACKNOWLEDGEMENT

First of all, I would like to dedicate my utmost appreciation to my main supervisor Associate Professor Dr. Ang Miin Huey for her guidance, patience and caring. The completion of this thesis would have been far more difficult without her passionate support along the way. Her guidance throughout this process was invaluable to me. Besides my main supervisor, I would also like to express my sincere gratitude to my co-supervisor Dr. Teh Wen Chean for his encouragement and insightful comments.

I am grateful to my family for their love and patience. They are constant source of concern, support and strength to me all the time. I would also like to express my appreciation to my friends for their care and motivation whenever I need mental support.

I acknowledge the financial assistance from MyBrainSc. I would also like to thank Universiti Sains Malaysia (USM) Research University (RU) Grant no. 1001/PMATHS/811286 that has partially funded our work.

Last but not least, I would like to thank others who have contributed in the completion of this thesis, in one way or another.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF SYMBOLS

$\subseteq$	Subset
$\subset$	Proper subset
$\lvert A \rvert$	Cardinality of the set A
Au	Set of all au for $a \in A$
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\langle\, , \rangle$	Inner product
$(x)f$	Image of the element x under function f
$(x)f^{-1}$	Preimage of the element x under function f
$[X]f$	Image of the set X under function f
$[X]f^{-1}$	Preimage of the set X under function f
$\mathbb{N}$	Set of integers
G	Finite group
R	Ring with unity
A^n	Set of n-tuples over the set A
RG	Group ring of G over R
C_n	Cyclic group of order n
D_{2n}	Dihedral group of order $2n$
F_q	Finite field of order q
U_γ	RG-matrix of $u \in RG$ with respect to ordering γ on G
$A_{\eta,\gamma}(u)$	RG-array of $u \in RG$ with respect to orderings η and γ on G

KOD GELANGGANG KUMPULAN KITARAN DAN DIHEDRAL

ABSTRAK

Dengan mengitlakkan idea melihat kod kitaran sebagai unggulan dalam gelanggang kumpulan kitaran, banyak kajian tentang kod gelanggang kumpulan yang merupakan unggulan telah dijalankan sejak setengah abad yang lalu. Pada tahun 2007, *T. Hurley* dan *P. Hurley* memperkenalkan satu keluarga kod gelanggang kumpulan yang baru dengan mengemukakan suatu pendekatan pengekodan baru. Berbeza dengan yang lalu, semua kod gelanggang kumpulan dari keluarga baru ini ialah submodul dan cuma merupakan unggulan dalam kes-kes tertentu. Sebagai notasi, kod gelanggang kumpulan baru ini ditulis sebagai kod-RG di mana R ialah satu domain integer dan G ialah satu kumpulan. Dalam tesis ini, kami mula dengan melihat $\text{kod}-F_2G$ sebagai suatu perwakilan kesetaraan bagi kod linear binari, di mana F_2 merupakan medan terhingga bersaiz dua. Satu syarat yang mencukupi untuk suatu kod linear binary setara dengan suatu $\text{kod}-F_2C_n$ telah ditentukan. Sehubungan ini, kami mengkaji kesetaraan antara kod-kod F_2G dengan mengemukakan tatasusunan gelanggang kumpulan. Didorong oleh satu contoh $\text{kod}-F_2D_{24}$ yang setara dengan suatu $\text{kod}-F_2C_{24}$, kami mengkaji sifat kesetaraan $\text{kod}-F_2C_n$ dan $\text{kod}-F_2D_{2n}$. Semua $\text{kod}-F_2D_{2n}$ bagi $n=2,3,4,5$ telah diperlihat sepenuhnya bersama-sama dengan penjana masing-masing dan didapati setiapnya adalah setara dengan suatu $\text{kod}-F_2C_n$. Akhir sekali, satu pencirian separa ke atas nilai *n* untuk $\text{kod}-F_2D_{2n}$ menjadi setara dengan suatu $\text{kod}-F_2C_{2n}$ telah ditemui.

CYCLIC AND DIHEDRAL GROUP RING CODES

ABSTRACT

By generalizing the idea of viewing cyclic codes as ideals in cyclic group rings, many studies on group ring codes which are ideals, have been done since half a century ago. In 2007, T. Hurley and P. Hurley introduced a new encoding approach of codes using group rings. Different from the previous studies, the resulting group ring codes introduced by Hurleys are submodules and are ideals only in certain restrictive cases. Group ring codes introduced by Hurley are denoted as RG-codes where R is an integral domain and G is a group. In this thesis, we first study the family of F_2G-codes where F_2 is the finite field of order two, by viewing the codes as equivalent forms of some binary linear codes. A sufficient condition for a binary linear code to be equivalent to an F_2C_n-code is determined. In addition to this, we start of the study of equivalence codes among F_2G-codes by inventing a tool named group ring array. Triggered by an example of an F_2D_{24}-code that is also an F_2C_{24}-code up to equivalence, properties of F_2C_n-codes as well as F_2D_{2n}-codes have been studied using group ring array. In particular, all F_2D_{2n}-codes for $n = 2,3,4,5$ are exhibited thoroughly together with their respective generator and each is found to be equivalent to some F_2C_{2n}-codes. Lastly, a partial characterisation on the value of n with respect to when an F_2D_{2n}-code is equivalent to some $F_2C_{2n}-$codes is established.

CHAPTER 1 INTRODUCTION

Codes have been associated to group rings since half a century ago. Group ring codes were first discussed by Berman in 1967 by viewing every cyclic code as an ideal in a group algebra over a cyclic group and every Reed-Muller code as an ideal in a group algebra over an elementary abelian 2-group [1]. Two years later, MacWilliams examined the class of codes which are ideals in group rings over dihedral groups [11]. In 1983, Charpin discovered that the extended Reed-Solomon codes can be considered as ideals of modular group algebras [2]. Later in 1992, Landrock and Manz published a paper named “Classical codes as ideals in group algebras” [9].

In the year 2000, Hughes [4] defined a group ring code as an ideal in a group ring. Thereafter, various studies on group ring codes such as self-orthogonal group ring codes, checkable group ring codes, two sided and abelian group ring codes can also be found in the literature [3, 8, 14].

In 2006, Hurley discovered the isomorphism between a group ring and a ring of matrices [7]. This result leads to a group ring encoding method for codes which was introduced by Hurley and Hurley [5, 6]. Let G be a group and R be an integral domain. The group ring codes defined by Hurleys are called RG-codes in this thesis. These RG-codes are generally submodules of their corresponding group ring RG and are ideals only in certain restrictive cases.

Let F_q be the finite field of order q, C_n be the cyclic group of order n and D_{2n} be the dihedral group of order $2n$. Famous classical codes such as the extended binary $[8,4]$-Hamming code and the extended binary Golay code have been shown to be an $F_2(C_2 \times C_4)$-code and an F_2D_{24}-code respectively in [6, 12].

Throughout the past decade, knowledge on RG-codes is still limited. Hence, in this thesis, we study the properties of RG-codes. The objectives of this thesis are:

(i) To obtain the basic properties of F_qG-codes,

(ii) To determine the conditions for a linear code to be equivalent to an F_2C_n-code,

(iii) To determine the conditions for an F_2D_{2n}-code to be equivalent to an F_2C_{2n}-code.

In Chapter 2, some prerequisites on modules and group rings will be given. Besides, some relevant knowledge on coding theory that will be needed will also be refreshed.

Chapter 3 begins with some preliminary on RG-codes obtained by Hurley, followed by our own basic results on this family of codes. Since many linear codes are shown to be F_qG-codes in the literature, we viewed F_qG-codes as equivalent forms of some linear codes to obtain basic properties of F_qG-codes. In relation to this, a necessary condition for a linear code to be an F_qG-code will be discussed. Analogous to the concept of equivalent codes, the equivalence among F_qG-codes from the point of view of vector spaces, which has not been studied, will be discussed. For this, a tool called group ring arrays is introduced.

In Chapter 4, we study properties of F_2C_n -code and F_2D_{2n} -codes respectively up to equivalence. A few results for an F_2G-code to be equivalent to an F_2C_n-code are discussed. A partition on F_2D_{2n} to identify its distinct elements that generate equivalent F_2D_{2n}-codes, is obtained.

After laying down the basics that are needed, we investigate the possibility for an F_2D_{2n}-code to be equivalent to an F_2C_{2n}-code in Chapter 5. The F_2D_{2n}-arrays and F_2C_{2n}-arrays are fully utilised in this process. The F_2D_{2n}-codes for $n = 2,3,4,5$ are shown to be F_2C_{2n}-codes up to equivalence. A characterisation condition for elements in F_2D_{2n} to generate F_2C_{2n}-codes up to equivalence is presented.

Lastly, a conclusion is given in Chapter 6 and some future directions will be included in this chapter.

CHAPTER 2 PRELIMINARY

Before going into our main study on codes that are constructed using group ring encoding method that were introduced in [5], we need some fundamental concepts in algebra and coding theory. For the algebra part, we assume that the readers have adequate knowledge on groups, rings, fields as well as vector spaces. The focus of the first section is on a special family of rings called group rings. Since every group ring not only has a ring structure but also a module structure, some fundamental definitions and results on modules are given in the second section. After that, some relevant results in coding theory will be reviewed. All definitions and results discussed in Section 2.1 and 2.2 can be found in [13] whereas for Section 2.3 can be found in [10].

2.1 Group Rings

Group ring plays an important role in this thesis. Throughout this thesis, unless specified otherwise, G denotes a group and R denotes a ring. Furthermore, we assume G is finite and R is an integral domain, that is, a commutative ring with unity that has no zero-divisors.

Definition 2.1.1. The *group ring* of G over R, denoted by RG, is the set

$$\left\{ \sum_{g\in G} \alpha_g g \,\middle|\, \alpha_g \in R \right\}$$

together with addition and multiplication defined by

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} \left(\alpha_g + \beta_g\right) g\,;$$

$$\left(\sum_{g\in G} \alpha_g g \right)\left(\sum_{g\in G} \beta_g g \right) = \sum_{g,h\in G} \alpha_g \beta_h gh.$$

For an element $u = \sum_{g \in G} \alpha_g g \in RG$, the *support* of u is the set $\operatorname{supp}(u) = \{ g \in G \mid \alpha_g \neq 0 \}$ and the *weight* of u is $wt(u) = |\operatorname{supp}(u)|$.

It can be shown easily that RG is a ring with unity. Also, if R is a field or RG is finite, then every element in RG is either a zero-divisor or a unit [7].

In [7], Hurley discovered that there is an isomorphism, dependent on a total ordering on G, between RG and a subring of the $n \times n$ matrices over R, which will be presented in Theorem 2.1.4. The isomorphic images of the elements of RG are called RG-matrices. Note that for a given G, our concern is just on the elements ordering but not on the total ordering itself. By abuse of notation, we use the same symbol $<$ (not to be confused with "less than") for all the total orderings throughout this thesis, for example, $a < b < c$ and $a < c < b$ are different total orderings.

Definition 2.1.2. Let γ denote $g_1 < g_2 < \cdots < g_n$, a total ordering on *G*. The RG*-matrix* of $u = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$ with respect to γ is the $n \times n$ matrix denoted by

$$M(RG, \gamma, u) = \left[m_{ij} \right] = \left[\alpha_{g_i^{-1} g_j} \right].$$

For simplicity of notation, we write $\gamma : g_1 < g_2 < \cdots < g_n$ to mean γ denotes the total ordering $g_1 < g_2 < \cdots < g_n$ and denote the RG-matrix of u with respect to γ by U_γ. The following example shows that the RG-matrices of an element u with respect to different orderings on G may be different.

Example 2.1.3. Consider the group ring F_2C_4 where $C_4 = \langle g \,|\, g^4 = 1 \rangle$. Let $u = \sum_{i=0}^{3} \alpha_{g^i} g^i \in F_2C_4$, $\eta : 1 < g < g^2 < g^3$ and $\gamma : 1 < g^2 < g < g^3$. Note that the following are the F_2C_4-matrices of u with respect to η and γ:

$$U_\eta = \begin{bmatrix} \alpha_{g^0} & \alpha_{g^1} & \alpha_{g^2} & \alpha_{g^3} \\ \alpha_{g^3} & \alpha_{g^0} & \alpha_{g^1} & \alpha_{g^2} \\ \alpha_{g^2} & \alpha_{g^3} & \alpha_{g^0} & \alpha_{g^1} \\ \alpha_{g^1} & \alpha_{g^2} & \alpha_{g^3} & \alpha_{g^0} \end{bmatrix} \quad \text{and} \quad U_\gamma = \begin{bmatrix} \alpha_{g^0} & \alpha_{g^2} & \alpha_{g^1} & \alpha_{g^3} \\ \alpha_{g^2} & \alpha_{g^0} & \alpha_{g^3} & \alpha_{g^1} \\ \alpha_{g^3} & \alpha_{g^1} & \alpha_{g^0} & \alpha_{g^2} \\ \alpha_{g^1} & \alpha_{g^3} & \alpha_{g^2} & \alpha_{g^0} \end{bmatrix}.$$

It can be seen that U_η and U_γ are different except when $\alpha_{g^1} = \alpha_{g^2} = \alpha_{g^3}$. □

Although two RG-matrices of an element u with respect to different orderings may not be the same, they are always equivalent as one can be obtained from another by a permutation of rows and columns.

Theorem 2.1.4. Let γ be an ordering on G and $M(RG, \gamma) = \{U_\gamma \,|\, u \in RG\}$. The map $\phi : RG \to M(RG, \gamma)$ such that

$$\phi(u) = U_\gamma$$

is a ring isomorphism.

Since any two RG-matrices of an element u with respect to different orderings on G are equivalent, the ranks of the RG-matrices of u are the same, irrespective of the choice of the orderings. Using the isomorphism defined in Theorem 2.1.4, the rank of a group ring element is defined as follows.

Definition 2.1.5. The *rank* of $u \in RG$ is

$$rank(u) = rank(U_\gamma)$$

where γ is any ordering on G.

Example 2.1.6. Consider the group ring F_2D_6 where $D_6 = \langle a,b \mid a^3 = b^2 = 1, ab = ba^{-1} \rangle$.

Let $\gamma : 1 < a < a^2 < b < ab < a^2b$ and $u = 1 + a + b + a^2b \in F_2D_6$. Then

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

It is easy to check that $rank(u) = rank(U_\gamma) = 2$ by transforming U_γ to its reduced row echelon form. □

2.2 Modules

In this section, we are going to discuss group rings from the point of view of modules. All the proofs of the results here can be found in [13]. Roughly speaking, a module is a generalization of a vector space, which allows the scalars to lie in a ring instead of a field. Some notions for vector spaces such as linear transformations and basis can be extended to modules.

Definition 2.2.1. Let R be a ring. A set M with two operations $+$ and $\cdot$, is called an *R-module* (or a module over *R*) if M is an abelian group under the operation $+$ and the following conditions hold:

(i) $am \in M$,

(ii) $(a+b)m = am + bm$,

(iii) $a(m+m') = am + am'$,

(iv) $a(bm) = (ab)m$,

(v) $1m = m$,

for all $a, b \in R$ and $m, m' \in M$.

Note that when R is a field, an R-module is a vector space over R. Similar to the concept of subspace, the following is the definition of R-submodule.

Definition 2.2.2. A non-empty subset N of an R-module M is called an R-*submodule* of M if for all $a \in R$ and $n, n' \in N$:

(i) $an \in N$,

(ii) $n + n' \in N$.

It can be shown easily that every group ring RG is an R-module, with the scalar multiplication defined as

$$r\sum_{g\in G}\alpha_g g = \sum_{g\in G}\left(r\alpha_g\right)g \text{ for all } r \in R \text{ and } \sum_{g\in G}\alpha_g g \in RG.$$

As an R-module, the inner product on RG is defined as follows.

Definition 2.2.3. The *inner product* of elements $u = \sum_{g\in G}\alpha_g g \in RG$ and $v = \sum_{g\in G}\beta_g g \in RG$ is

$$\langle u, v\rangle = \left\langle \sum_{g\in G}\alpha_g g, \sum_{g\in G}\beta_g g\right\rangle = \sum_{g\in G}\alpha_g \beta_g.$$

The elements u and v are said to be *orthogonal* if $\langle u, v\rangle = 0$.

Next, the familiar notion of basis for vector spaces is extended to modules.

Definition 2.2.4. Let M be a module over R. A set $S = \{s_1, s_2, \cdots, s_k\} \subseteq M$ is called a *spanning set* of M if $M = \left\{\sum_{i=1}^{k}\alpha_i s_i \,\middle|\, \alpha_i \in R\right\}$. The spanning set S is called a *basis* of M if it is *linearly independent*, that is, the condition $\sum_{i=1}^{k}\alpha_i s_i = 0$ implies that $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$.

Unlike vector spaces, not every module has a basis. The following is a counter example.

Example 2.2.5. Consider the set Z_5 that is a module over Z. Take an arbitrary subset $S = \{s_1, s_2, \cdots, s_k\} \subseteq Z_5$, $k \geq 1$. Note that $\sum_{i=1}^{k} \alpha_i s_i = 0$ has $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 5$ as a non-zero solution for every possible k. This implies that S is not linearly independent over Z. This indicates that there does not exist a linearly independent set that spans Z_5. Hence, Z_5 has no basis. □

Definition 2.2.6. An R-module M is called *free* if it has a basis.

If a free module M over R has a finite basis, then any basis of M has the same number of elements. The number of elements in any basis of M is called the *rank* of M and is denoted by $rank(M)$. From now on, when we say modules (or submodules), we mean free modules (or free submodules).

Remark 2.2.7. For each submodule N of M, $rank(N) \leq rank(M)$.

It is easy to see that every group ring RG is a R-module with G as a basis. Hence, RG is a module with $rank(RG) = |G|$.

Definition 2.2.8. Given two R-modules M and N. A mapping $T : M \to N$ is called an *R-linear map* if for all $a \in R$ and $m, m' \in M$:

(i) $(m + m')T = (m)T + (m')T$,

(ii) $(am)T = a(m)T$.

A bijective R-linear map T is called an *isomorphism*. The modules M and N are said to be *isomorphic* if there exists an isomorphism T between them.

Note that the kernel and the image of the R-linear map $T: M \to N$ defined by

$$\ker(T) = \{ m \in M | (m)T = 0 \},\ \mathrm{Im}(T) = \{ (m)T \in N | m \in M \}$$

are R-submodules of M and N, respectively. In addition, T is one-to-one if and only if $\ker(T) = \{0\}$.

Next is an isomorphism involving group rings that will be utilised in subsequent chapters.

Proposition 2.2.9. Let $\gamma : g_1 < g_2 < \cdots < g_n$ be an ordering on G. The R-linear map $\mathrm{T}_\gamma : RG \to R^n$ with respect to γ such that

$$\left(\alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \right) \mathrm{T}_\gamma = \alpha_{g_1} \alpha_{g_2} \cdots \alpha_{g_n}$$

is a module isomorphism and thus RG and R^n are isomorphic.

Recall that for $\gamma : g_1 < g_2 < \cdots < g_n$ and $u = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$, $U_\gamma = \left[\alpha_{g_i^{-1} g_j} \right]$ and $rank(u) = rank(U_\gamma)$. It can be seen that

$$\begin{aligned} (g_t u)\mathrm{T}_\gamma &= \left(\sum_{i=1}^{n} \alpha_{g_i} g_t g_i \right) \mathrm{T}_\gamma \\ &= \left(\sum_{i=1}^{n} \alpha_{g_t^{-1} g_i} g_i \right) \mathrm{T}_\gamma \\ &= \alpha_{g_t^{-1} g_1} \alpha_{g_t^{-1} g_2} \cdots \alpha_{g_t^{-1} g_n} \end{aligned}$$

is the t^{th} row in U_γ. Let u_t denote the t^{th} row in U_γ. This indicates that any non-empty set $\{ g_{i_1} u, g_{i_2} u, \ldots \cdots, g_{i_k} u \} \subseteq Gu$ is linearly independent if and only if $\{ u_{i_1}, u_{i_2}, \cdots, u_{i_k} \}$ is linearly independent. Thus $rank(u)$ is equal to the maximum number of linearly independent elements in Gu. On the other hand, the set containing all the linearly independent elements in Gu is a basis for the module $L_R(Gu)$. This observation is summarized in the following:

Proposition 2.2.10. Let $u \in RG$. Then $rank(u)$ is the maximum number of linearly independent elements in Gu and thus $rank(u) = rank(L_R(Gu))$.

2.3 Codes

Coding theory is a branch of mathematics that is used to improve the reliability of communication channels. In practice, all messages need to be digitalised. Let $A = \{a_1, a_2, \cdots, a_q\}$ be a given *alphabet*, whose elements are called *digits*. Each message will be digitalised into a string of digits of A called a *word over* A and the number of digits in a word is called the *length* of the word. In order to increase the error immunity of the transmitted words, a number of extra digits will be added to each of the word in a process called *encoding* process. The set of words of length n that is obtained after the encoding process is called a *code* of length n over A and every element in the code is called a *codeword*. The process where the receiver deduces the most possible transmitted message after receiving a word is called the *decoding* process.

The length of a code affects its performance in terms of the transmitting speed and the size of a code represents the maximum amount of distinct messages to be transmitted. A code of length n and size m is called an (n,m)-code.

Codes that have nice algebraic structures have better encoding and decoding algorithms. In real world applications, linear codes that have vector space structures are commonly used. From now on, let F_q be a finite field of order q.

Definition 2.3.1. A *linear code* of length n over F_q is a subspace of $F_q^{\,n}$. A linear code over F_q with length n and dimension k is called a q-ary $[n,k]$-code.

Clearly, a q-ary $[n,k]$-code is an (n,q^k)-code.

For a codeword $x \in C$, the *weight* of x denoted by $wt(x)$ is the number of non-zero positions in x.

Definition 2.3.2. An *even code* is a linear code over F_2 where every codeword in it has even weight.

A basis for a linear code is normally represented in the form of a matrix as defined in the following definition.

Definition 2.3.3. A $k \times n$ matrix G whose rows form a basis for an $[n,k]$-code is called a *generator matrix* of the code.

Let G be a generator matrix of an $[n,k]$-code over F_q. Note that G is a matrix of rank k as all the rows are linearly independent. Denote the i^{th} row of G as r_i. The encoding of linear code C is a linear transformation represented by the map $T : F_q^{\,k} \to C$ defined by

$$(a_1 a_2 \dots a_k)T = \sum_{i=1}^{k} a_i r_i = (a_1 a_2 \dots a_k)G$$

such that $C = \operatorname{Im}(T)$.

Linear codes are inner product spaces with the inner product defined as follows.

Definition 2.3.4. Let C be an $[n,k]$-code over F_q. The *inner product* of any two codewords $x = a_1a_2\cdots a_n$ and $y = b_1b_2\cdots b_n$ in C is

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

The elements x and y are *orthogonal* if $\langle x,y\rangle = 0$.

Definition 2.3.5. Let C be an $[n,k]$-code over F_q. The orthogonal complement $C^\perp$ of C, that is, $C^\perp = \{x \in F_q^{\,n} \mid \langle x,y\rangle = 0 \text{ for all } y \in C\}$, is called the *dual code* of C. A matrix H is a *parity check matrix* of C if H^T is a generator matrix of $C^\perp$.

Two distinct linear codes are usually regarded as the same code if they are equivalent, to be defined next.

Definition 2.3.6. Two linear codes of length n over F_q are *equivalent* if one can be obtained from another by a combination of operations of the following types:

(i) Permutation of the n digits of the codewords.

(ii) Multiplication of the symbols appearing in a fixed position by a non-zero scalar in F_q.

We extend analogously the concept of equivalence between codes in Definition 2.3.6 to subsets of $F_q^{\,n}$. For the binary case, two linear codes C_1 and C_2 over F_2 are equivalent if and only if C_2 can be obtained from C_1 by a permutation of the digits of the codewords. This permutation induces naturally a bijection $\Phi : C_1 \to C_2$. Under the map Φ, if B_1 is a basis of C_1, then $[B_1]\Phi$ is a basis of C_2. The bases B_1 and $B_2 = [B_1]\Phi$ are equivalent as B_2 is obtained from B_1 by a permutation of digits.

Next, we turn our focus to a family of linear codes called cyclic codes. These codes, especially for those over F_2, are very important in practice and widely applicable as encoding and decoding algorithm can be implemented on them easily using shift register that requires very little memory in real applications. For the remainder of this section, all the proofs of the results can be found in [10].

Definition 2.3.7. The *cyclic shift map* on $F_q^{\,n}$ is the map $\pi : F_q^n \to F_q^n$ defined by $(\alpha_0\alpha_1\cdots\alpha_{n-1})\pi = \alpha_{n-1}\alpha_0\alpha_1\cdots\alpha_{n-2}$. For every $v \in F_q^n$, the image $(v)\pi$ is called a *cyclic shift* of v. The set $\{v,(v)\pi,\cdots,(v)\pi^{n-1}\}$ is called a *complete cyclic shift cycle of v*.

Let s be the smallest positive integer such that $v=(v)\pi^s$. Then the size of the complete cyclic shift cycle of v is equal to s. Note that s may be smaller than $n-1$.

Definition 2.3.8. An $[n,k]$-code C is a *cyclic code* if for all $v \in C,\ (v)\pi \in C.$

Besides having the structure of a vector space, every cyclic code also has a ring structure. In fact, each cyclic code over F_q is a principal ideal of a quotient polynomial ring over F_q.

Consider the ring $F_q[x]/\langle x^n-1\rangle = \left\{ \sum_{i=1}^{n-1}\alpha_i x^i \,\middle|\, \alpha_i \in F_q \right\}$ which is also a vector space. Define the map $\psi : F_q^{\,n} \to F_q[x]/\langle x^n-1\rangle$ such that

$$(\alpha_0\alpha_1\cdots\alpha_{n-1})\psi = \alpha_0+\alpha_1 x+\cdots+\alpha_{n-1}x^{n-1} = \sum_{i=0}^{n-1}\alpha_i x^i .$$

It is easy to verify that ψ is a linear transformation of vector spaces over F_q. Let C be a q-ary $[n,k]$-code and $C(x) = \mathrm{Im}(\psi|_C) = [C]\psi$. Clearly $C(x)$ is isomorphic to C as a vector space.

Next is a result showing how cyclic codes are related to polynomial rings from the point of view of rings.

Theorem 2.3.9. A q-ary $[n,k]$-code C is a cyclic code if and only if $C(x)$ is an ideal of the ring $F_q[x]/\langle x^n - 1\rangle$.

Note that $F_q[x]/\langle x^n - 1\rangle$ is a principle ideal domain and thus for every cyclic code C, the isomorphic image $C(x) = \langle g(x)\rangle$ for some $g(x) \in F_q[x]/\langle x^n - 1\rangle$. This $g(x)$ is unique if it is chosen to be the monic polynomial of the least degree in $C(x)$. Moreover, any element in $C(x)$ has the form $g(x)f(x)$ where $\deg f(x) < (n - \deg g(x))$.

Definition 2.3.10. For a cyclic code C, the unique monic polynomial of the least degree $g(x) \in C(x)$ is called the *generator polynomial* of $C(x)$, which is also called the *generator polynomial* of C.

The following result gives a way to identify all cyclic codes of length n with their corresponding generator polynomials.

Theorem 2.3.11. A non-zero monic polynomial $g(x) \in F_q[x]/\langle x^n - 1\rangle$ is the generator polynomial of some cyclic code in F_q^n if and only if $g(x)$ is a monic factor of $x^n - 1$.

When the generator polynomial $g(x)$ of a cyclic code C of length n is of degree $n-k$, then $S=\{g(x),xg(x),\cdots,x^{k-1}g(x)\}$ is a basis of $C(x)$, or equivalently, $[S]\psi^{-1}$ is a basis of C and thus $\dim(C)=k$.

CHAPTER 3 GROUP RING CODES

From this chapter onwards, all discussions are concentrated on the new family of group ring codes that were introduced by Hurley in 2007. The group ring codes that are discussed here are not necessarily ideals of group rings. In this chapter, we first review some preliminaries on this family of group ring codes that can be found in [5, 6]. From Section 3.2 onwards, the focus turns to *our* basic results on these group ring codes that will be needed in subsequent studies.

3.1 Preliminaries on Group Ring Codes

Let RG be a group ring where R is an integral domain and G is a group. Recall from Chapter 2 that RG is a module over R. Let W be a submodule of RG and $u \in RG - \{0\}$. Consider the function

$$f_u : W \longrightarrow RG$$

defined by $(x) f_u = xu$. Let $x, y \in RG$ and $\alpha \in R$, we have

(i) $(x+y) f_u = (x+y)u = xu + yu = (x) f_u + (y) f_u$,

(ii) $(\alpha x) f_u = (\alpha x)u = \alpha(xu) = \alpha(x) f_u$.

Hence f_u is an R-linear map. However, f_u might not be one-to-one as shown below.

Example 3.1.1. Consider $f_{1+g^3} : W \to F_2C_6$ with $W = L_{F_2}\{1, g, g^3\}$ and $C_6 = \langle g \mid g^6 = 1 \rangle$. Note that $(1) f_{1+g^3} = 1 + g^3$ and $(g^3) f_{1+g^3} = g^3(1+g^3) = 1 + g^3$ which implies that f_{1+g^3} is not one-to-one. □

Suppose $N = \{x_1, x_2, \cdots, x_k\}$ is a basis of W. By looking at the kernel of f_u, it can be seen that f_u is one-to-one if and only if the set $Nu = \{x_1u, x_2u, \ldots, x_ku\}$ is linearly independent over R.

Note that

$$
\begin{aligned}
ker(f_u) &= \{x \in W \mid (x) f_u = 0\} \\
&= \{a_1 x_1 + a_2 x_2 + \cdots + a_k x_k \mid (a_1 x_1 + a_2 x_2 + \cdots + a_k x_k) u = 0 \text{ and } a_1, \cdots, a_k \in R\} \\
&= \{a_1 x_1 + a_2 x_2 + \cdots + a_k x_k \mid a_1 (x_1 u) + a_2 (x_2 u) + \cdots + a_k (x_k u) = 0 \text{ and } a_1, \cdots, a_k \in R\}.
\end{aligned}
$$

If Nu is linearly dependent, then f_u can be restricted to $f_u|_{W'} : W' \to RG$ where W' is also a submodule of RG with basis $N' \subset N$ such that $N'u$ is linearly independent and $\mathrm{Im}(f_u|_{W'}) = \mathrm{Im}(f_u)$.

From now on, given $u \in RG - \{0\}$, the domain W is restricted to be a submodule with basis N such that Nu is linearly independent, so that f_u is one-to-one. In the year 2007, Hurley introduced a new family of group ring codes by using the f_u as encoding functions.

Definition 3.1.2. Let RG be a group ring. Suppose W is a R-submodule of RG and $u \in RG - \{0\}$. A one-to-one function $f_u : W \to RG$ defined by $(x) f_u = xu$ is called a *group ring encoding function*. The RG*-code with generator u relative to the submodule W*, denoted $C_G(W, u)$, is the image of f_u, that is

$$C_G(W, u) = [W] f_u = Wu.$$

Note that $C_G(W, u)$ is an R-submodule of RG. Clearly, W is isomorphic to $C_G(W, u)$ under f_u and thus $rank(W) = rank(C_G(W, u))$. Suppose N is a basis of W. It can be verified easily that $C_G(W, u) = Wu = L_R(Nu)$. Since f_u is one-to-one, the linear independency of N over R guarantees the linear independency of Nu over R. Hence, Nu is a basis of $C_G(W, u)$ and $rank(C_G(W, u)) = |Nu| = |N|$.

This result is summarized as follows for the references of our later discussion.

Proposition 3.1.3. Let $C_G(W,u)$ be an RG-code with generator u relative to a submodule W. If N is any basis of W, then Nu is a basis of $C_G(W,u)$.

By Remark 2.2.7 and Proposition 2.2.10, it can be seen that $|Nu| = rank(C_G(W,u)) \leq rank(L_R(Gu)) = rank(u)$. This brings us to the following result.

Proposition 3.1.4. Let $C_G(W,u)$ be an RG-code with generator u relative to a submodule W. Then $rank(C_G(W,u)) \leq rank(u)$.

3.2 Some Fundamental Properties of Group Ring Codes

Following Hurley's approach, attention is now restricted to the RG-codes $C_G(W,u)$ where the submodule $W = L_R(N)$ for some $N \subseteq G$. By abuse of notation, we denote the RG-code $C_G(W,u) = C_G(L_R(N),u)$ as $C_G(N,u)$ in the remainder of our discussions. In this section, we discuss some basic properties of RG-codes in terms of their generators and submodules.

Definition 3.2.1. Let $u \in RG - \{0\}$ and $N \subseteq G$ such that Nu is linearly independent. The RG-code $C_G(N,u)$ is called a *zero-divisor code* if u is a zero-divisor. Otherwise, $C_G(N,u)$ is called a *unit-derived code* when $u \in RG$ is a unit [6].

Note that the set of zero-divisor codes and the set of unit-derived codes are mutually disjoint, as shown in the following.

Proposition 3.2.2. A zero-divisor code cannot be a unit-derived code and vice versa.

Proof. Consider the RG-code $C_G(N,u)$ where $N=\{x_1,x_2,\cdots,x_k\}\subseteq G$. Suppose u is a zero-divisor in RG, that is, there exists $v\in RG-\{0\}$ such that $uv=0$. Then, for any $y=\sum_{i=1}^{k}\alpha_i x_i u\in C_G(N,u)$, we have

$$\begin{aligned} yv &= \left(\sum_{i=1}^{k}\alpha_i x_i u\right)v \\ &= \left(\sum_{i=1}^{k}\alpha_i x_i\right)uv \\ &= \left(\sum_{i=1}^{k}\alpha_i x_i\right)0 \\ &= 0 \end{aligned}$$

which implies that y is a zero-divisor in RG. Hence, no unit exists in $C_G(N,u)$.

On the other hand, suppose u is a unit in RG. Note that every element in $x_i\in N\subseteq G$ for $i\in\{1,2,\cdots,k\}$ is a unit in RG. Then each $x_iu\in Nu\subseteq C_G(N,u)$ is a unit. This indicates that there exist at least k units in $C_G(N,u)$.

Therefore, a zero-divisor code cannot be a unit-derived code and vice versa. □

Next is a property of zero-divisor codes.

Proposition 3.2.3. Let $u=\sum_{g\in G}\alpha_g g\in RG$. If $\sum_{g\in G}\alpha_g=0_R$, then u is a zero-divisor.

Proof. Suppose $G=\{g_1,g_2,\cdots,g_n\}$ and $u=\sum_{i=1}^{n}\alpha_i g_i$ where $\sum_{i=1}^{n}\alpha_i=0$. Let $v=g_1+g_2+\cdots+g_n\in RG$. Note that for all $g_i\in G$,

$$\begin{aligned} g_i v &= g_i\left(g_1+g_2+\cdots+g_n\right) \\ &= g_ig_1+g_ig_2+\cdots+g_ig_n \\ &= g_1+g_2+\cdots+g_n \\ &= v. \end{aligned}$$

Then

$$\begin{aligned} uv &= \left(\sum_{i=1}^{n}\alpha_i g_i\right)v \\ &= \sum_{i=1}^{n}\alpha_i\left(g_i v\right) \\ &= \sum_{i=1}^{n}\alpha_i\left(v\right) \\ &= \left(\sum_{i=1}^{n}\alpha_i\right)v \\ &= 0 \end{aligned}$$

implies that u is a zero-divisor in RG. □

Based on Proposition 3.2.3, by fixing $R=F_2$, a result related to zero-divisor codes whose codewords are of even weight is obtained. Before moving on to the proof of this result in Proposition 3.2.5, the following lemma is needed.

Lemma 3.2.4. Let G be a group and $x,y\in F_2G$. If $wt(x)$ and $wt(y)$ are even, then $wt(x+y)$ is even.

Proof. Let $x=\sum_{g\in G}\alpha_g g,\ y=\sum_{g\in G}\beta_g g\in F_2G$ with even weight. For the element $x+y=\sum_{g\in G}\left(\alpha_g+\beta_g\right)g$,

$$\begin{aligned} wt(x+y) &= \left|\operatorname{supp}(x+y)\right| \\ &= \left|\left\{g\,\middle|\,\alpha_g+\beta_g\neq 0\right\}\right|. \end{aligned}$$

Note that over F_2, $\alpha_g+\beta_g=0$ if and only if $\alpha_g=\beta_g$. This indicates that

$$\operatorname{supp}(x+y)=\left(\operatorname{supp}(x)\cup\operatorname{supp}(y)\right)-\left(\operatorname{supp}(x)\cap\operatorname{supp}(y)\right)$$

Hence in terms of weight, we have

$$wt(x+y) = wt(x) + wt(y) - 2\left|\operatorname{supp}(x) \cap \operatorname{supp}(y)\right|$$

which is also even. □

Proposition 3.2.5. Let $u \in F_2G$ with even weight. Then u is a zero-divisor and every codeword in any F_2G-code with generator u has even weight.

Proof. Let $u \in F_2G$ with even weight. The result that u is a zero-divisor follows immediately from Proposition 3.2.3.

Suppose $N = \{x_1, x_2, \cdots, x_k\} \subseteq G$ such that Nu is linearly independent. Take any element $y = \sum_{i=1}^{k} \alpha_i x_i u \in C_G(N,u)$, where $\alpha_i \in F_2$ for all $i \in \{1, 2, \cdots, k\}$. Note that for each $x_i \in N$, we have $wt(x_i u) = wt(u)$ is even. Using Lemma 3.2.4, it can be proved by mathematical induction that $wt(y) = wt\left(\sum_{i=1}^{k} \alpha_i x_i u\right)$ is even, which means every codeword in $C_G(N,u)$ has even weight. □

From the next section onwards, we concentrate on RG-codes where $R = F_q$, a finite field of order q, as a study of linear codes versus RG-codes will be done.

3.3 Equivalence of F_qG-codes

The importance of the study of equivalence of F_qG-codes is discussed in this section. From the discussion in Section 3.1, we know that $C_G(N,u)$ over F_q is the image of an injective linear transformation. Let $\gamma : g_1 < g_2 < \cdots < g_n$ be an ordering on G. By Proposition 2.2.9, the isomorphism $\mathrm{T}_\gamma : F_qG \to F_q^{\,n}$ with respect to γ is defined by $(\alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_n g_n)\mathrm{T}_\gamma = \alpha_1 \alpha_2 \cdots \alpha_n$. From now on, each codeword in each $F_q G$-code $C_G(N,u)$ will be associated to its isomorphic image under T_γ and $C_G(N,u)$ will be associated to $[C_G(N,u)]\mathrm{T}_\gamma = \mathrm{Im}\left(\mathrm{T}_\gamma\big|_{C_G(N,u)}\right)$, which is a linear code of length n.

By Proposition 3.1.3, Nu is a basis of $C_G(N,u)$. Hence, $[Nu]\mathrm{T}_\gamma$ is a basis for the linear code $[C_G(N,u)]\mathrm{T}_\gamma$. Note that for $y \in C_G(N,u)$ and an ordering $\gamma' \neq \gamma$, $(y)\mathrm{T}_{\gamma'}$ is different from $(y)\mathrm{T}_\gamma$ simply by a permutation of digits. Therefore, $[C_G(N,u)]\mathrm{T}_{\gamma'}$ and $[C_G(N,u)]\mathrm{T}_\gamma$ are equivalent codes. Let $\overline{C_G(N,u)} = \{[C_G(N,u)]\mathrm{T}_\eta \mid \eta \text{ denotes an ordering on } G\}$. From now on, when we say "a linear code C is an $F_q G$-code $C_G(N,u)$" or "$C_G(N,u)$ can be associated to a linear code C", we mean $C \in \overline{C_G(N,u)}$. In other words, there exists an ordering γ on G such that $C = [C_G(N,u)]\mathrm{T}_\gamma$.

Note that two distinct group ring codes can be associated to the same linear code (up to equivalence) in some cases.

Example 3.3.1. Consider the group ring $F_2 C_4$ where $C_4 = \langle g \mid g^4 = 1 \rangle$ and let $\gamma : 1 < g < g^2 < g^3$. Let $u = 1 + g$, $N = \{1, g\}$ and $N' = \{1, g^3\}$. Then

$$\begin{aligned} C_{C_4}(N,u) &= L_{F_2}\left(\{1+g, g+g^2\}\right) \\ &= \{0, 1+g, g+g^2, 1+g^2\} \end{aligned}$$

and

$$
\begin{aligned}
C_{C_4}(N',u) &= L_{F_2}\left(\left\{1+g, 1+g^3\right\}\right) \\
&= \left\{0, 1+g, 1+g^3, g+g^3\right\}.
\end{aligned}
$$

Clearly, $C_{C_4}(N,u) \neq C_{C_4}(N',u)$. However,

$$\left[C_{C_4}(N,u)\right]\mathrm{T}_\gamma = \{0000, 1100, 0110, 1010\}$$

and $$\left[C_{C_4}(N',u)\right]\mathrm{T}_\gamma = \{0000, 1100, 1001, 0101\}$$

are equivalent, as the permutation $(1\ 2)(3\ 4)$ on digits of codewords sends $\left[C_{C_4}(N,u)\right]\mathrm{T}_\gamma$ to $\left[C_{C_4}(N',u)\right]\mathrm{T}_\gamma$. □

Example 3.3.1 indicates the possibility that $\overline{C_G(N,u)} = \overline{C_G(N',u)}$ for distinct N and N'. In fact, $\overline{C_{G_1}(N_1,u_1)}$ and $\overline{C_{G_2}(N_2,u_2)}$ could be the same under certain circumstances.

Example 3.3.2. Consider F_2C_4 where $C_4 = \left\langle g \middle| g^4 = 1 \right\rangle$ and let $\gamma : 1 < g < g^2 < g^3$. Consider the u, N and N' in Example 3.3.1 and let $u' = g + g^2$. Then

$$
\begin{aligned}
\left[C_{C_4}(N,u')\right]\mathrm{T}_\gamma &= L_{F_2}\left(\left\{\left(g+g^2\right)\mathrm{T}_\gamma, \left(g\left(g+g^2\right)\right)\mathrm{T}_\gamma\right\}\right) \\
&= L_{F_2}\left(\{0110, 0011\}\right) \\
&= \{0000, 0110, 0011, 0101\}
\end{aligned}
$$

and

$$
\begin{aligned}
\left[C_{C_4}(N',u')\right]\mathrm{T}_\gamma &= L_{F_2}\left(\left\{\left(g+g^2\right)\mathrm{T}_\gamma, \left(g^3\left(g+g^2\right)\right)\mathrm{T}_\gamma\right\}\right) \\
&= L_{F_2}\left(\{0110, 1100\}\right) \\
&= \{0000, 0110, 1100, 1010\}.
\end{aligned}
$$