Kingdom of Saudi Arabia
Ministry of Education
Umm Al-Qura University
College of Applied Sciences
Department of Mathematical Sciences

CODING MATRICES FOR THE SEMI-DIRECT PRODUCT GROUPS

A thesis submitted in partial fulfillment for the degree of master of mathematical sciences (Algebra)

by

AMNAH ABDU ALKINANI

Supervised by

Prof. **AHMED ALI KHAMMASH**

FEBRUARY 2020

Contents

Abstract

Coding theory is the study of methods for efficient and accurate transfer of information from one place to another. In [14], T. Hurley proved that the group ring RG of a group G of order n over a ring R is isomorphic to a certain ring of $n \times n$ matrices over R. This representation enabled them to describe the unit and zero-divisors of the group ring in terms of properties of these matrices, and where appropriate in terms of the determinate of the matrices. Now, the coding matrices were determined for several classes of finite groups such as cyclic [14], direct product [6], elementary-abelian [14], dihedral groups D_{2n} [14] and the general linear groups $GL(2, \mathbb{F})$ [7]. In this study, we generalize Hurley's theorem in [14] to semi-direct product groups and hence, determine the coding matrices of these groups.

Acknowledgements

I would like to express immense gratitude to my generous parents, my husband, my brothers and sisters who gave me courage, unconditional support and real prayers. And I would like thank my supervisor professor Dr. Ahmed Khammash for his motivation, taking time out of busy schedule and guiding me in this dissertation.
Moreover I would also be thanking my classmates in Masters at Umm Al-Qura University for our cooperation and sharing our experience.
Above all, I thank Allah for giving me the intellect to comprehend the subject, and for giving me the strength and endurance to complete this dissertation.

Notations

q	$q = p^n,\ n \geq 1$, n is a positive integer.
$\mathbb{F}_p$	The field with p elements, p is prime number.
$\mathbb{F}_q$	The field with q elements.
$\mathbb{F}_q^n$	The n-dimensional vector space over $\mathbb{F}_q$.
C	The symbol of a code.
(n, k, d)-code	The parameters of a code.
$wt(c)$	The weight of a codeword.
$d(u, v)$	The distance between two codewords.
$d(C)$	The minimum distance of the code C.
$C^{\perp}$	The dual of the code C.
G	Finite group of order n.
RG	The group ring with the group G over the ring R.
$M(G)$	The matrix of a group G.
$M(RG, a)$	The RG-matrix corresponds to a group ring element.
$M(RG)$	The ring of an RG-matrices.
$M_n(R)$ and $R_{n\times n}$	The ring of $(n \times n)$ of matrices over R.
S	The set of a basis for the submodule.
$\|S\|$	The order of the set S.
$G \setminus S$	The set of elements of G which is not in S.
$\overline{x}$	A vector in R^n corresponds to $x \in RG$.

Introduction

Claude Shannon [23] initiated the theory of Error-Correcting codes in connection with problems in information theory and coding theory regarding the search of a reliable and efficient transfer of digital information. Linear codes gained more attention from the work of W. Hamming in 1950 [8]. An (n, k, d) code over a field $\mathbb{F}$ with q elements should have a (reasonably) large size in order to encode a large number of source messages and on the other hand should have a relatively large weight (minimum distance) d for detecting and correcting large number of errors that may occur while transmission [21]. There are several types of known codes such as HAMING CODES, HADAMARD CODES, REED-MULLER CODES, REED SOLOMON CODES, BCH CODES and THE GOLAY CODES ,... etc. [19]. It turns out that, for error-correcting properties, the most important types of codes are cyclic codes.

The first connection between codes and group rings of finite groups appeared in the work of F. G. MacWilliams (1969) [17] in which cyclic codes were identified with ideals in the group algebras of cyclic groups, consequently; two sided ideals in $\mathbb{F}G$ are named codes. Since then the algebraic structure of the group ring has been deeply involved in the study and constructions of codes. In particular properties of (central) primitive idempotents in the group algebra of finite groups over finite fields are heavily used in codes construction [2] , [5].

In (2006) T. Hurley [14] (starting with a coding matrix of the finite group G based on an appropriate listing of its elements) proved that the group ring RG of a finite group of order n over a ring R is isomorphic to certain well-defined ring of matrices and hence gave a construction of codes from certain elements of the group ring such as units and zero divisors [11] (his construction was applied to obtain binary codes from the group algebra $\mathbb{F}_2 D_{2k}$). This allows matrix algebras to be used to produce codes by providing generating and check matrices for codes. The coding matrices are known for several classes of groups such as cyclic, elementary-abelian and dihedral groups D_{2k}. In 2018, M. Hamed determined the coding matrices for the general linear group $GL(2, q)$ using its BN-pair structure [6] , [7]. It turns out also that the coding matrix of the direct product group is the tensor (Kronecker) product of the coding matrices of the individual groups in the product deducing the corresponding known result for finite abelian groups.

The aim of this dissertation is to determine the coding matrix of the semi direct product group $G = C_n \times_\phi C_2$; $\phi : C_2 \to Aut(C_n)$ of two cyclic groups in order to generalize the known result for the dihedral group D_{2n} [14], which is known to be a semi direct product of the two cyclic groups C_n, C_2.

Chapter 1

Codes; the concept and the main problem

In this chapter, we define the linear code and the basic concept of codes, then we describe codes by generating matrices and parity-check matrices. Finally, we explain the main problem of coding theory. All facts and results in this chapter can be found in [21], [20], [9] and [10].

1.1 Linear Codes

Let $\mathbb{F}_q$ be the finite field of q elements, then $\mathbb{F}_q^n$ will be an n-dimensional vector space over $\mathbb{F}_q$. A code C is defined to be a subset of $\mathbb{F}_q^n$ and its elements called a codeword. If $q = |C| = 1$ the code is called a trivial, If $q = 2$ a binary code and for $q = 3$ a ternary code, etc.

Definition 1.1.1. *A code C is called linear if it is a subspace of $\mathbb{F}_q^n$.*

If C has dimension k, then we say that C is an (n,k)-code and n the length of the code C. The weight of any non zero codeword, denoted by $wt(c)$, is equal to the number of its non zero components, i.e.

$$wt(c) \;=\; |\{c_i \neq 0 : c = (c_1, c_2, \ldots, c_n) \in C,\ i = 1, 2, \cdots, n\}|$$

The minimum weight of the code is the minimum non zero weight of its codewords.
The minimum distance, or simply distance, of a code C, denoted by $d(c)$, is defined to be the minimum Hamming distance between two distinct codewords of C. That is,

$$d(c) = min_{c_i, c_j \in C}\ d(c_i, c_j)$$

The Hamming distance is a metric function, since it satisfies the three conditions:

1. $d(u, v) = 0\ if\ and\ only\ if\ u = v$

2. $d(u,v) = d(v,u)$

3. $d(u,v) \leq d(u,w) + d(w,v)$

For all u, v *and* $w \in \mathbb{F}_q^n$.

And if C has minimum distance d, we say that C is an (n,k,d)-code.The numbers n, k and d are called the parameters of the linear code.

Note that

1. An (n,k)-code contains q^k codewords, that is a linear code of dimension k contains precisely 2^k codewords (Theorem 2.3.13 [10]).

2. Clear by linear code definition, all linear codes contain the zero codewords, denoted by $0 = 000.....0$.

3. And clear by linear code definition, a binary code is linear if and only if the sum of any two codewords is a codeword.

Example 1.1.2. *(page 4 [9], page 29 [10])*
$C_1 = (00, 01, 10, 11)$ *is a linear* $(2,2)$*-code of* $\mathbb{F}_2^2$, $C_2 = (000, 011, 101, 110)$ *is a linear* $(3,2)$*-code of* $\mathbb{F}_2^3$ *and* $C_3 = (00000, 01101, 10110, 11011)$ *is a linear* $(5,2)$*-code of* $\mathbb{F}_2^5$.
But $C_4 = (000, 001, 101)$ *is not a linear* $(3,2)$*-code, since* 001 *and* 101 *are in* C_4 *but* 001+101 = 100 *is not in* C_4.
We have the minimum weight of C_1 *is* 1 *because*

$$wt(00) = 0, wt(01) = 1, wt(10) = 1, wt(11) = 2$$

so the minimum distance of C_1 *is* 1.

The following theorem relates the notion of the weight of a code with the minimum distance.

Lemma 1.1.3. *([21], Lemma 4.3.4 and [9], Lemma 5.1)*
If $u, v \in F_q^n$, *then* $d(u,v) = wt(u - v)$.

Theorem 1.1.4. *([21], Theorem 4.3.5 and [9], Theorem 5.2)*
Let C *be a linear code and let* $wt(C)$ *be the minimum weights of the non zero codewords of* C, *then*

$$d(C) = wt(C).$$

Proof: There exist codewords u, v in C with $u \neq v$, such that $d(u,v) = d(C)$, then by lemma above, $d(C) = d(u,v) = wt(u - v) \geq wt(C)$.
Conversely, for some $u \in C$, $wt(C) = wt(u) = wt(u - 0) = d(u,0) \geq d(C)$, since 0 belongs to the linear code C, hence $d(C) = wt(C)$.

1.2 Description of Codes

We can describe the linear code by a generator matrix. Since a linear code is a vector space. and there is another important way of describing it, by a parity-check matrix.

1.2.1 The Generator Matrix of Linear Code

Definition 1.2.1. *([21])*
Let C be an (n,k)-code and let G be a $(k \times n)$-matrix whose rows are the basis for C, then G is called a generator matrix for C.

A generator matrix of the form $G = (I_k, A)$, where I_k is the identity matrix of size $k \times k$, and A is a $k \times (n-k)$ matrix, is said to be in standard form. Every linear code has a generator matrix in standard form.
If G is a generator matrix for an (n,k)-linear code C and if i is a word of length k written as a row vector, then $c = iG$ is a word in C, since C is a linear combination of the rows of G, which form a basis for C.

Example 1.2.2. $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ *is a generator matrix for the binary linear* $(7,4)$*-code in standard form and this code is called Hamming code. Such that*

$$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

This code consists of 2^4 codewords $\mathbb{Z}_2^4 G$, one of these codewords is the following

$$c = \begin{pmatrix} 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

A linear code might have more than one generator matrix, because it is vector space, which is might have more than one basis.

Example 1.2.3. *we have binary linear* $(5,2,3)$*-code*

$$C_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

the possible generator matrix for C_3 *is* $G_1 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$ *or* $G_2 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$ *or* $G_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$.

The following theorem and procedures give us convertible the matrix G to be in standard form.

Theorem 1.2.4. *([9], Theorem 5.5)*
Let G *be a generator matrix of an* (n, k)*-code. Then by performing operations of the following types:*

(R1) Permutation of the rows.

(R2) Multiplication of a row by a non-zero scalar.

(R3) Addition of a scalar multiple of one row to another.

(C1) Permutation of the columns.

(C2) Multiplication of any column by a non-zero scalar.

G *can be transformed to the standard form*

$$(I_k, A),$$

where I_k *is the* $(k \times k)$ *identity matrix, and* A *is a* $(k \times (n-k))$ *matrix.*

We denote by g_{ij} the (i,j)th entry of G and by $r_1, r_2, ..., r_k$ and $c_1, c_2, ..., c_n$ the rows and columns respectively of this matrix. Suppose then G has already been transformed to

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & g_{1j} & \cdots & g_{1n} \\ 0 & 1 & \cdots & 0 & g_{2j} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & g_{i-1j} & \cdots & g_{i-1n} \\ 0 & 0 & \cdots & 0 & g_{ij} & \cdots & g_{in} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & g_{kj} & \cdots & g_{kn} \end{pmatrix}$$

step 1 If $g_{ij} \neq 0$, go to step 2. If $g_{ij} = 0$, and if for some $i > j, g_{ij} \neq 0$, then interchange r_j and r_i. If $g_{ij} = 0$ and $g_{ij} = 0$ for all $i > j$, then choose h ; $g_{ih} \neq 0$ and interchange c_i and c_h.

step 2 we now have $g_{ij} \neq 0$. Multiply r_i by g_{ij}^{-1}.

step 3 we now have $g_{ij} = 1$. For each of $i = 1, 2, ..., k$, with $i \neq j$, replace r_i by $r_i - g_{ij} r_j$.

The column c_j now has the desired form.
After this procedure has been applied for $j = 1, 2, ..., k$, the generator matrix will have standard form.
Consequently, the standard form of a generator matrix for C_3 in the (example 1.2.3) is:

$$G_1 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} \longrightarrow_{interchange} \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$G_2 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix} \longrightarrow_{interchange} \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \longrightarrow_{r_1 \to r_1 - r_2} \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$G_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix} \longrightarrow_{r_2 \to r_2 - r_1} \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

1.2.2 The Parity-Check Matrix

Definition 1.2.5. *Let $u = (u_1 u_2 .... u_n)$ and $v = (v_1 v_2 .... v_n)$ be two vectors in $\mathbb{F}_q^n$, then the inner product $u.v$ is defined by:*

$$u.v = u_1 v_1 + u_2 v_2 + ... + u_n v_n.$$

If $u.v = 0$, then u and v are called orthogonal.

Now, we define the dual code as following.

Definition 1.2.6. *Let C be an (n, k)-linear code, then the dual code $C^\perp$ is defined by:*

$$C^\perp = \{u \in \mathbb{F}_q^n | u.v = 0 \ for \ all \ v \in C\}$$

Theorem 1.2.7. *([21], 5.1.3)*

1. *If G is a generator matrix of C, then*

$$C^\perp = \{u \in \mathbb{F}_q^n | uG^T = 0\}$$

   Where G^T is the transpose of the matrix G,

2. *The dual $C^\perp$ of a linear (n, k)-code is a linear $(n, n-k)$-code ,*

3. *For any linear code C, we have $C^{\perp\perp} = C$.*

Definition 1.2.8. *([9])*
A parity-check matrix H for an (n, k)-code C is a generator matrix of $C^\perp$.

Thus H is an $((n-k) \times n)$-matrix satisfying $GH^T = 0$, where H^T denotes the transpose of H and 0 is an all zero matrix, it follows from theorem $(1.2.7, (3))$ that if H is a parity-check matrix of C, then $C = \{x \in \mathbb{F}_q^n | xH^T = 0\}$.
A parity-check matrix of the form $H = (B|I_{n-k})$, where I_{n-k} is the identity matrix of size $n-k$, is said to be in standard form.

The following theorem gives an easy way of constructing a generator matrix for a linear code with given parity-check matrix (or vice versa).

Theorem 1.2.9. *([9], 7.6)*
Let $G = (I_k|A)$ be the standard form generator matrix of an (n,k)-code C, then a parity-check matrix for C is $H = (-A^T|I_{n-k})$.

Example 1.2.10. *The parity-check matrix H for the binary (Hamming) code defined in example (1.2.2) is the following:*

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

Such that

$$GH^T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0$$

For example, if we take $c = (0100011) \in C$, then

$$cH^T = (0100011) \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} = 0.$$

We have some examples for binary codes given by generating matrix as follows:

Code	Generating matrix
Hamming code	$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$ for a $(7, 4, 3)$-Hamming code.
Golay code	G $=[I_{12}, A]$, where I_{12} is (12×12)-identity matrix and $$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$ for a $(23, 12, 7)$-Golay code.
Reed-Muller code	$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$ for a $(8, 4, 4)$-RM code, which is $(1, 3)$-RM code such that $n = 2^m$, $k = \sum_{i=0}^{r} \binom{m}{i}$ and $d = 2^{m-r}$.

Hadamard code	$$G = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$ for a $(8, 3, 4)$-Hadamard code.
BCH code	$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$ for a $(15, 5, 7)$-BCH code.

1.3 The Main Problem of Coding Theory

A good (n, k, d)-code should have a relatively large size, i.e. a small n, large k and large d. So that it can be used to encode a large number of source messages and a large minimum distance in order to correct a large number of errors. The bad things, is that these two volumes are conflicting. Thus, the main problem is to determine what is the maximum size of a linear code C over $\mathbb{F}_q^n$ of length n and with a relatively large minimum distance.
We denoted by $A_q(n, d)$ the largest value of k such that there exist a q-ary (n, k, d)-code.

Definition 1.3.1. *A code C is called a q-ary code, if $q = 2$ or $q = 3$, the code is described as a binary code or a ternary code respectively.*

The problem is easily solved for $d = 1$ and $d = n$, for all q :

Theorem 1.3.2. *([9], Theorem 2.1)*
For any $n \geq 1$,

(i) $A_q(n, 1) = q^n$

(ii) $A_q(n, n) = q$

Proof. (i) For the minimum distance of a code to be at least 1, we require that the codewords are distinct. And so the largest q-ary (n, k, d)-code is the whole of $(\mathbb{F}_q)^n$, with $k = q^n$.

(ii) Suppose C is a q-ary (n, k, d)-code, then any two distinct codewords of C differ in all n position. Thus the symbols appearing in any fixed position. e.g. the first, in the k codewords must be distinct, giving $k \leq q$. Thus $A_q(n, n) \leq q$. On the other hand, the q-ary repetition code of length n (see example 1.3.7 and definition 1.3.8 bellow) is an (n, q, n)-code and so $A_q(n, n) = q$.

□

Theorem 1.3.3. *([21], Theorem 4.5.2)*
For any $n \geq 1$,

$$A_q(n, d) \leq q\ A_q(n-1, d)$$

Theorem 1.3.4. *([21], Theorem 4.5.3)*
For binary codes,

$$A_2(n, 2t+1) = A_2(n+1, 2t+2)$$

Put another way, if d is even, then $A_2(n, d) = A_2(n-1, d-1)$.

Thus for binary codes, it is enough to determine $A_2(n, d)$ for all odd values of d (or for all even values).

The following table of small values of $A_2(n,d)$ is taken from (Hill , 1986) [9], which in turn comes from (Sloane , 1982) :

n	$d=3$	$d=5$	$d=7$
5	4	2	-
6	8	2	-
7	16	2	2
8	20	4	2
9	40	6	2
10	72-79	12	2
11	144-158	24	4
12	256	32	4
13	512	64	8
14	1024	128	16
15	2048	256	32
16	2560-3276	256-340	36-37

Here, we present some bounds for sizes of a linear code C.

Sphere Packing or (Hamming) Bound

Let C be an (n,k,d)-linear code, then

$$q^k = \mid C \mid \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}$$

Where spheres of radius $t = \dfrac{d-1}{2}$, such that $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i$ is the number of vectors of length n and have distance at most t from a certain codeword.
For given values of q, n and d, the sphere-packing bound provides an upper bound on the (n,k,d)-code.

Example 1.3.5. *Suppose that $n=5$ and $d=3$, then $t = \dfrac{3-1}{2} = 1$, by using the Hamming bound we get:*

$$\mid C \mid \leq \frac{2^5}{(2-1)[\binom{5}{0}+\binom{5}{1}]} = \frac{32}{6} = 5,33$$

But, since C is binary, $\mid C \mid$ should be a power of 2, thus $k \leq 2$ and hence $\mid C \mid \leq 4$.

Definition 1.3.6. *A code C which achieves the sphere-packing bound (Hamming bound) is called a perfect code.*

Example 1.3.7.

- *The whole space $\mathbb{F}_q^n = C$ which is $(n,n,1)$-linear code.*

- *The repetition code of odd length n which is $(n, 1, n) = C_n$*

$$C_n = \{00...0, 11...1\}.$$

All of these examples are often called the trivial perfect codes.

Definition 1.3.8. *The repetition code is one of the most basic error-correcting codes, the idea of this code is to just repeat the message several times.*

Singleton Bound

Let C be an (n, k, d)-code, then we have $n - k \geq d - 1$.
An (n, k, d)-code having the largest possible minimum weight $d = n - k + 1$ is called a maximum distance separable code or an MDS code.
This code the next upper bound for the code C and is often not very good since the singleton bound in (example 1.3.5) gives $k \leq 3$ while Hamming bound gives $k \leq 2$.

The Gilbert-Varshamov Bound

Let C be an (n, k, d)-code, then we have the lower bound as in the following theorem:

Theorem 1.3.9. *([21], Theorem 4.5.4)*

$$q^k = \mid C \mid \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}.$$

Chapter 2

Group Rings as a Ring of Matrices

In this chapter, we revise the notion of the group ring RG of a finite group G over a ring R in order to introduce a theorem due to T. Hurley which proves an embedding of the group ring into a ring of matrices. This embedding is used to characterize the elements of the group ring in terms of the properties of matrices and construct certain types of linear codes.

2.1 The Group Ring

Let G be a group and R be a ring with identity, the group ring RG is defined by:

$$RG = \{\sum_{g\in G} \alpha_g g | \alpha_g \in R\}$$

Consider $a = \sum_{g\in G} \alpha_g g$ and $b = \sum_{g\in G} \beta_g g$, then addition is defined term-by-term;

$$a + b = \sum_{g\in G} (\alpha_g + \beta_g) g,$$

While multiplication is a convolution-like operation,

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

If R is a field in the group ring RG, then RG is called a group algebra.
The following definitions can be found in [11], [4], [18] and [16].

Definition 2.1.1.

- *Let R be a ring, a non zero element $u = \sum_{g\in G} \alpha_g g \in RG$ is called a zero-divisor if and only if there exists a non zero $v \in RG$ such that $uv = 0$ or $vu = 0$.*
- *Let R be a ring with identity $I_R \neq 0$, an element $u \in RG$ is called a unit if and only if there exists an element $v \in RG$, such that $uv = 1 = vu$. The group of units of RG is denoted by $U(RG)$.*

Definition 2.1.2.

- *The transpose of an element $u = \sum_{g\in G} \alpha_g g \in RG$ is $u^T = \sum_{g\in G} \alpha_g g^{-1}$ or equivalently $u^T = \sum_{g\in G} \alpha_{g^{-1}} g$.*

- *The support of a given element* $u = \sum_{g \in G} \alpha_g g \in RG$ *is the set*

$$Supp(u) = \{g \in G | \alpha_g \neq 0\}.$$

- *The element* $u \in RG$ *is symmetric if and only if* $u^T = u$.

2.2 Coding Matrices for Finite Groups

Let G be a finite group of order n, and $\{g_1, g_2, ..., g_n\}$ be a fixed listing of the element of G. Consider the matrix of G relative to its listing and denote it by $M(G)$, which has the following form:

$$M(G) = \begin{pmatrix} g_1^{-1}g_1 & g_1^{-1}g_2 & \cdots & g_1^{-1}g_n \\ g_2^{-1}g_1 & g_2^{-1}g_2 & \cdots & g_2^{-1}g_n \\ \vdots & \vdots & \vdots & \vdots \\ g_n^{-1}g_1 & g_n^{-1}g_2 & \cdots & g_n^{-1}g_n \end{pmatrix}_{n \times n}$$

Then for each $u = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$, define the matrix $M(RG, u) \in M_n(R)$ as follows:

$$M(RG, u) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}_{n \times n}$$

It is quite clear that the shape as well as the coefficients of the coding matrix $M(RG, u)$ depends on the listing of the group elements of the group G.

2.3 Hurley's Theorem

In [14], T. Hurley proved that the group ring RG of a group G of order n over a ring R is isomorphic to a certain ring of $(n \times n)$ matrices over R.

Theorem 2.3.1. *([14], Theorem 1)*
Let G be a group of order n with the given listing of the elements, then there is a bijective ring homomorphism is given by

$$\sigma : \alpha \longrightarrow M(RG, \alpha)$$

between RG and the ring of $(n \times n)$ G-matrices over R.

Proof. Let $\{g_1, g_2, \ldots, g_n\}$ be the listing of the elements of G and Let $M(RG)$ be the ring of $(n \times n)$ G-matrices over R, relative to this listing of G. Suppose that $a = \sum_{i=1}^{n} \alpha_{g_i} g_i$ in RG and define mapping:

$$\sigma : \ RG \ \longrightarrow M(RG)$$

such that,

$$\sigma(a) \;=\; M(RG,a) \;=\; \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & .... & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & .... & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & .... & \alpha_{g_n^{-1}g_n} \end{pmatrix}$$

this mapping is obviously surjective, injective and additive. It is thus sufficient to show that σ is multiplicative.
For that, let $a = \sum_{i=1}^{n} \alpha_{g_i} g_i$ and $b = \sum_{i=1}^{n} \beta_{g_i} g_i$ be two elements in RG, such that:

$$\sigma(b) \;=\; M(RG,b) \;=\; \begin{pmatrix} \beta_{g_1^{-1}g_1} & \beta_{g_1^{-1}g_2} & .... & \beta_{g_1^{-1}g_n} \\ \beta_{g_2^{-1}g_1} & \beta_{g_2^{-1}g_2} & .... & \beta_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{g_n^{-1}g_1} & \beta_{g_n^{-1}g_2} & .... & \beta_{g_n^{-1}g_n} \end{pmatrix}$$

We want to prove that $\sigma(a * b) \;=\; \sigma(a) \;* \sigma(b)$, where,

$$a * b \;=\; \Big(\sum_{i=1}^{n} \alpha_{g_i} g_i\Big)\Big(\sum_{i=1}^{n} \beta_{g_i} g_i\Big) \;=\; \sum_{i=1}^{n} \Big(\sum_{r,s=1}^{n} \alpha_{g_r}\beta_{g_s}\Big) g_i$$

where, $g_r.g_s \;=\; g_i \iff g_s \;=\; g_r^{-1} g_i$
Therefore,

$$a * b \;=\; \sum_{i=1}^{n} \Big(\sum_{r=1}^{n} \alpha_{g_r}\beta_{g_r^{-1}g_i}\Big)\, g_i \;=\; \sum_{i=1}^{n} \gamma_{g_i} g_i \;, \qquad where\ \gamma_{g_i} = \sum_{r=1}^{n} \alpha_{g_r}\beta_{g_r^{-1}g_i}.$$

Which means that the coefficients of g_i in the multiplication is that $(\alpha_{g_1}, \alpha_{g_2}, \ldots, \alpha_{g_n})$ times the $i-th$ columns of $\sigma(b)$.Then,

$$\sigma(a) * \sigma(b) \;=\; \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & .... & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & .... & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & .... & \alpha_{g_n^{-1}g_n} \end{pmatrix} \begin{pmatrix} \beta_{g_1^{-1}g_1} & \beta_{g_1^{-1}g_2} & .... & \beta_{g_1^{-1}g_n} \\ \beta_{g_2^{-1}g_1} & \beta_{g_2^{-1}g_2} & .... & \beta_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{g_n^{-1}g_1} & \beta_{g_n^{-1}g_2} & .... & \beta_{g_n^{-1}g_n} \end{pmatrix}$$

$$= \begin{pmatrix} \sum_{r=1}^{n} \alpha_{g_1^{-1}g_r}\beta_{g_r^{-1}g_1} & \sum_{r=1}^{n} \alpha_{g_1^{-1}g_r}\beta_{g_r^{-1}g_2} & .... & \sum_{r=1}^{n} \alpha_{g_1^{-1}g_r}\beta_{g_r^{-1}g_n} \\ \sum_{r=1}^{n} \alpha_{g_2^{-1}g_r}\beta_{g_r^{-1}g_1} & \sum_{r=1}^{n} \alpha_{g_2^{-1}g_r}\beta_{g_r^{-1}g_2} & .... & \sum_{r=1}^{n} \alpha_{g_2^{-1}g_r}\beta_{g_r^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \sum_{r=1}^{n} \alpha_{g_n^{-1}g_r}\beta_{g_r^{-1}g_1} & \sum_{r=1}^{n} \alpha_{g_n^{-1}g_r}\beta_{g_r^{-1}g_2} & .... & \sum_{r=1}^{n} \alpha_{g_n^{-1}g_r}\beta_{g_r^{-1}g_n} \end{pmatrix}$$

$$= \begin{pmatrix} \gamma_{g_1^{-1}g_1} & \gamma_{g_1^{-1}g_2} & .... & \gamma_{g_1^{-1}g_n} \\ \gamma_{g_2^{-1}g_1} & \gamma_{g_2^{-1}g_2} & .... & \gamma_{g_2^{-2}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_{g_n^{-1}g_1} & \gamma_{g_n^{-1}g_2} & \cdots & \gamma_{g_n^{-1}g_n} \end{pmatrix} = \; \sigma(a \;* b).$$

Thus $\sigma(a * b) \;=\; \sigma(a) \;* \sigma(b)$, and hence σ is a ring isomorphism as required.

□

This isomorphism means that the group ring and the ring of matrices are interchangeable. Thus we can exploit results from group rings and ring of matrices as needed.

From now on σ denotes the mapping σ as in Theorem (2.3.1).
The map $\theta : RG \to R^n$, $\theta(\sum_{i=1}^{n} \alpha_{g_i} g_i) = (\alpha_1, \alpha_2, ..., \alpha_n)$ is a ring isomorphism from RG to R^n. Thus every element in RG can be considered as n-tuple in R^n.
In a finite group algebra, every element must be a unit or zero-divisor, and there is a method to determine which.

Corollary 2.3.2. *([14], Theorem 2 and Corollary 3)*
Let R be an integral domain, i.e. a nonzero commutative ring, has identity I_R and has no zero-divisor, then:

- *$a \in RG$ is a unit if and only if $\sigma(a)$ is a unit in $M(RG)$.*
- *$a \in RG$ is a zero-divisor if and only if $\sigma(a)$ is a zero-divisor in $M(RG)$.*

Theorem 2.3.3. *([14], Theorem 3 and [12], Theorem 5.2)*
Let R be a field, a non zero element $a \in RG$ is a zero-divisor if and only if $det(\sigma(a)) = 0$, and otherwise is a unit.

Proof. The proof of this theorem is a direct result of (Theorem 2.3.1) and (Corollary 2.3.2 , (1)). □

The following useful result of this isomorphism.

Corollary 2.3.4. *Let RG be a group ring, and $a \in RG$. If the inverse $\sigma(a)$ of $M(RG)$ exist, then this inverse is an $M(RG)$.*

Proof. Consider $\sigma(a)$ is invertible in $R_{n\times n}$, then there exist an $(n \times n)$-matrix U in $R_{n\times n}$ such that $\sigma(a).U = I_{n\times n}$. From (corollary 2.3.2) we get a is an invertible in RG, suppose that b its inverse such that $a * b = 1_{RG}$. Hence, the isomorphism between the group ring and the ring of matrices implies that $\sigma(a) * \sigma(b) = I_{n\times n}$, where $\sigma(b)$ is an RG-matrix corresponding to b. But, $\sigma(a).U = I_{n\times n}$. Hence, $\sigma(b) = U$, and thus U is an RG-matrix. □

Notation: For every element $u \in RG$, let the capital letter U denote its corresponding RG-matrix $\sigma(u)$.

2.4 Some Types of Coding Matrices

Cyclic Group

Let $G = \{1, g, g^2, ..., g^{n-1}\}$ be a cyclic group of order n such that $g^n = 1$. Then the RG-matrix U relative to this listing corresponds to a circulant matrix; if $u = \sum_{i=1}^{n} \alpha_i g^i \in RG$ then

$M(RG, u)$ has the following form:

$$U = \sigma(u) = \begin{pmatrix} \alpha_o & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} \\ \alpha_{n-1} & \alpha_o & \alpha_1 & \dots & \alpha_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_o \end{pmatrix}$$

where α_i is the coefficient of g^i in u.
Circulant matrices are special type of Toeplitz matrices.

Definition 2.4.1. *A Toplitz matrix is a matrix in which each descending diagonal from left to right is constant.*

For instance, the following matrix is a Toeplitz matrix:

$$\begin{pmatrix} a & b & c & d & e \\ f & a & b & c & d \\ g & f & a & b & c \\ h & g & f & a & b \\ i & h & g & f & a \end{pmatrix}.$$

A Toeplitz matrix is not necessarily square.

Dihedral Group

Let $G = D_{2n}$ be the dihedral group of order $2n$, such that $D_{2n} =< a, b : a^2 = b^n = 1, a * b = b^{-1} * a >$. There are a number of listings of the elements of D_{2n} but the following listing is the most convenient

$$D_{2n} = \{1, b, b^2, \dots, b^{n-1}, a, ab, ab^2, \dots, ab^{n-1}\}$$

Then the matrix of D_{2n} relative to this listing as:

$$\left(\begin{array}{ccccc|ccccc} 1 & b & b^2 & \dots & b^{n-1} & a & ab & ab^2 & \dots & ab^{n-1} \\ b^{n-1} & 1 & b & \dots & b^{n-2} & ab & ab^2 & ab^3 & \dots & a \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b & b^2 & b^3 & \dots & 1 & ab^{n-1} & a & ab & \dots & ab^{n-2} \\ \hline a & ab & ab^2 & \dots & ab^{n-1} & 1 & b & b^2 & \dots & b^{n-1} \\ ab & ab^2 & ab^3 & \dots & a & b^{n-1} & 1 & b & \dots & b^{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ ab^{n-1} & a & ab & \dots & ab^{n-2} & b & b^2 & b^3 & \dots & 1 \end{array}\right)$$

Thus the ring of matrices of the following form is isomorphic to the group ring of D_{2n} :

$$\left(\begin{array}{ccccc|ccccc} \alpha_o & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} & \beta_o & \beta_1 & \beta_2 & \dots & \beta_{n-1} \\ \alpha_{n-1} & \alpha_o & \alpha_1 & \dots & \alpha_{n-2} & \beta_1 & \beta_2 & \beta_3 & \dots & \beta_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_0 & \beta_{n-1} & \beta_0 & \beta_1 & \dots & \beta_{n-2} \\ \hline \beta_o & \beta_1 & \beta_2 & \dots & \beta_{n-1} & \alpha_o & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} \\ \beta_1 & \beta_2 & \beta_3 & \dots & \beta_0 & \alpha_{n-1} & \alpha_o & \alpha_1 & \dots & \alpha_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_{n-1} & \beta_0 & \beta_1 & \dots & \beta_{n-2} & \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_0 \end{array}\right)$$

Note that these matrices have the form $\begin{pmatrix} \text{A} & \text{B} \\ \text{B} & \text{A} \end{pmatrix}$, where A is a circulant matrix and B is a Hankel matrix of a special form (or reverse circulant matrix). In Chapter 3 we shall prove a generalization of this fact for a semi-direct product group.

Definition 2.4.2. *A Hankel matrix is a matrix which is constant on any diagonal from upper right to lower left.*

Finitely Generated Abelian Groups

In [4], from the fundamental theorem of finitely generated abelian group, a finite abelian group is isomorphic to the direct product of finite number of cyclic groups. Hence, in this case the group ring RG is isomorphic to the certain block-circulant matrices. Suppose that $G \cong C_{d_1} \times C_{d_2} \times \ldots \times C_{d_r}$, where d_1 , d_2 , $\ldots$, d_r are positive integers. Let S be a sequence $S = (d_1 , d_2 , \ldots, d_r)$. Define a S-block circulant matrix over R as follows:
If $S = (d_1)$, then an S-block circulant matrix is a $(d_1 \times d_1)$-circulant matrix. Now, suppose $r > 1$ and $S = (d_1 , d_2 , \ldots, d_r)$, then an S-block circulant matrix over R is a $(d_r \times d_r)$-circulant matrix, say U, where each entries in U is a $(d_1, d_2, \ldots, d_{r-1})$-block circulant matrices.

Example 2.4.3. *Let $G = C_2 \times C_4$ and R any ring. Then the group ring RG is isomorphic to the ring of matrices over R of the form:*

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_4 & A_1 & A_2 & A_3 \\ A_3 & A_4 & A_1 & A_2 \\ A_2 & A_3 & A_4 & A_1 \end{pmatrix}_{4\times 4},$$

where A_1, A_2, A_3 and A_4, are (2×2)-circulant matrices. If we re-list the elements of G using $C_2 \times C_4 = C_4 \times C_2$, then RG will be isomorphic to the ring of matrices of the form:

$$\begin{pmatrix} B_1 & B_2 \\ B_2 & B_1 \end{pmatrix}_{2\times 2},$$

where B_1 and B_2 are (4×4)-circulant matrices.

In this type of matrices over the commutative ring R are commute and normal.

Definition 2.4.4. *A matrix M is said to be normal if and only if $M^*M = MM^*$, where M^* is the conjugate transpose of M.*

The Direct Product of Finite Group

In this case, M. Hammed [6] proved that the coding matrix of the direct product group is the tensor (Kronecker) product of the coding matrices for the single groups appeared in the direct product. It follows that the coding matrix of the finite abelian group is the tensor product of circulant matrices.

Theorem 2.4.5. *Let G and H be two finite groups then,*

$$M(G \times H) = M(G) \otimes M(H).$$

Proof. Suppose that $|G| = n$, $|H| = m$ and let $G = \{g_1, g_2, \ldots, g_n\}$, $H = \{h_1, h_2, \ldots, h_m\}$ be the listing of the groups G and H respectively. Then we may take the following listing for the elements of the direct product as:
$G \times H = \{(g_1,h_1), (g_1,h_2), \ldots, (g_1,h_m), (g_2,h_1), (g_2,h_2), \ldots, (g_2,h_m), \ldots, \ldots, (g_n,h_1), (g_n,h_2), \ldots, (g_n,h_m)\}$. Hence we have,

$$M(G\times H) = \begin{pmatrix} (g_1^{-1}g_1, h_1^{-1}h_1) & (g_1^{-1}g_1, h_1^{-1}h_2) & \ldots & (g_1^{-1}g_1, h_1^{-1}h_m) & \ldots & \ldots & (g_1^{-1}g_n, h_1^{-1}h_m) \\ (g_1^{-1}g_1, h_2^{-1}h_1) & (g_1^{-1}g_1, h_2^{-1}h_2) & \ldots & (g_1^{-1}g_1, h_2^{-1}h_m) & \ldots & \ldots & (g_1^{-1}g_n, h_2^{-1}h_m) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (g_1^{-1}g_1, h_m^{-1}h_1) & (g_1^{-1}g_1, h_m^{-1}h_2) & \ldots & (g_1^{-1}g_1, h_m^{-1}h_m) & \ldots & \ldots & (g_1^{-1}g_n, h_m^{-1}h_m) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (g_n^{-1}g_1, h_m^{-1}h_1) & (g_n^{-1}g_1, h_m^{-1}h_2) & \ldots & (g_n^{-1}g_1, h_m^{-1}h_m) & \ldots & \ldots & (g_n^{-1}g_n, h_m^{-1}h_m) \end{pmatrix}_{nm\times nm}$$

On the other hand, we have:

$$M(G) = \begin{pmatrix} g_1^{-1}g_1 & g_1^{-1}g_2 & \ldots & \ldots & g_1^{-1}g_n \\ g_2^{-1}g_1 & g_2^{-1}g_2 & \ldots & \ldots & g_2^{-1}g_n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_n^{-1}g_1 & g_n^{-1}g_2 & \ldots & \ldots & g_n^{-1}g_n \end{pmatrix}_{n\times n},$$

and

$$M(H) = \begin{pmatrix} h_1^{-1}h_1 & h_1^{-1}h_2 & \ldots & \ldots & h_1^{-1}h_m \\ h_2^{-1}h_1 & h_2^{-1}h_2 & \ldots & \ldots & h_2^{-1}h_m \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ h_m^{-1}h_1 & h_m^{-1}h_2 & \ldots & \ldots & h_m^{-1}h_m \end{pmatrix}_{m\times m}.$$

Then the Kronecker product of $M(G)$ and $M(H)$ will be:

$$M(G) \otimes M(H) = \begin{pmatrix} g_1^{-1}g_1.M(H) & g_1^{-1}g_2.M(H) & \ldots & \ldots & g_1^{-1}g_n.M(H) \\ g_2^{-1}g_1.M(H) & g_2^{-1}g_2.M(H) & \ldots & \ldots & g_2^{-1}g_n.M(H) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_n^{-1}g_1.M(H) & g_n^{-1}g_2.M(H) & \ldots & \ldots & g_n^{-1}g_n.M(H) \end{pmatrix}_{nm\times nm}$$

$$= \begin{pmatrix} (g_1^{-1}g_1, h_1^{-1}h_1) & (g_1^{-1}g_1, h_1^{-1}h_2) & \dots & (g_1^{-1}g_1, h_1^{-1}h_m) & \dots & \dots & (g_1^{-1}g_n, h_1^{-1}h_m) \\ (g_1^{-1}g_1, h_2^{-1}h_1) & (g_1^{-1}g_1, h_2^{-1}h_2) & \dots & (g_1^{-1}g_1, h_2^{-1}h_m) & \dots & \dots & (g_1^{-1}g_n, h_2^{-1}h_m) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (g_1^{-1}g_1, h_m^{-1}h_1) & (g_1^{-1}g_1, h_m^{-1}h_2) & \dots & (g_1^{-1}g_1, h_m^{-1}h_m) & \dots & \dots & (g_1^{-1}g_n, h_m^{-1}h_m) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (g_n^{-1}g_1, h_m^{-1}h_1) & (g_n^{-1}g_1, h_m^{-1}h_2) & \dots & (g_n^{-1}g_1, h_m^{-1}h_m) & \dots & \dots & (g_n^{-1}g_n, h_m^{-1}h_m) \end{pmatrix}_{nm \times nm}$$

Which is equal to $M(G \times H)$, and hence we get:

$$M(G \times H) \;=\; M(G) \;\otimes M(H)$$

□

As a consequence we have:

Corollary 2.4.6. *$M(C_n \times C_m) = M(C_n) \otimes M(C_m)$, where C_n and C_m are the cyclic groups of order n and m, respectively.*

Corollary 2.4.7. *The Kronecker product of two circulant matrices is block circulant.*

Elementary Abelian Group

The matrix $M(G)$ of a group G is symmetric if and only if G has exponent 2 which happens if and only if G is elementary abelian of exponent 2. Then $G \cong \mathbb{Z}_2^n$ which has order 2^n and rank n. To see the isomorphism in (Theorem 2.3.1) we need a listing of the elements of the elementary abelian 2-group G of rank n.
Suppose that G is generated by $\{g_1, g_2, \dots, g_n\}$, then list the elements of G as:
1 , g_1 , g_2 , $g_1 * g_2$, g_3 , $g_1 * g_3$, $g_2 * g_3$, $g_1 * g_2 * g_3$, g_4 , $\dots$, $\dots$, $\dots$, $g_1 * g_2 * \dots * g_{n-1}$, g_n , $\dots$, $\dots$, $\dots$, $g_1 * g_2 * \dots * g_n$.
Then the group ring RG with this listing is isomorphic to Walsh-Toeplitz $(2^n \times 2^n)$-matrices over R.

Definition 2.4.8. *Walsh-Toeplitz matrices of size $(2^n \times 2^n)$ are defined to be matrices of the form:*

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

where A and B are $(2^{n-1} \times 2^{n-1})$ Walsh-Toeplitz matrices. The diagonal of this matrices is the initial element.

So for example an (8×8) Walsh-Toeplitz matrix is

$$\left(\begin{array}{cccc|cccc} \alpha_o & \alpha_1 & \alpha_2 & \alpha_3 & \beta_o & \beta_1 & \beta_2 & \beta_3 \\ \alpha_1 & \alpha_o & \alpha_3 & \alpha_2 & \beta_1 & \beta_o & \beta_3 & \beta_2 \\ \alpha_2 & \alpha_3 & \alpha_o & \alpha_1 & \beta_2 & \beta_3 & \beta_o & \beta_1 \\ \alpha_3 & \alpha_2 & \alpha_1 & \alpha_o & \beta_3 & \beta_2 & \beta_1 & \beta_o \\ \hline \beta_o & \beta_1 & \beta_2 & \beta_3 & \alpha_o & \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_o & \beta_3 & \beta_2 & \alpha_1 & \alpha_o & \alpha_3 & \alpha_2 \\ \beta_2 & \beta_3 & \beta_o & \beta_1 & \alpha_2 & \alpha_3 & \alpha_o & \alpha_1 \\ \beta_3 & \beta_2 & \beta_1 & \beta_o & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_o \end{array}\right)$$

In general, when G is elementary abelian p-group we will get an isomorphism between RG and a ring of $(p^n \times p^n)$-matrices over R. Thus define an elementary $(p^n \times p^n)$-matrix as follows:

Definition 2.4.9. *An elementary $(p \times p)$-matrix is a $(p \times p)$-circulant matrix, and an elementary $(p^n \times p^n)$-matrix, for $n \geq 2$, is defined to be of the form:*

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

where A ,B are elementary $(p^{n-1} \times p^{n-1})$-matrices.

General Linear Group $GL(2, q)$

And in this case, M. Hammed and A. Khammash determined the ring of matrices for the general linear group $GL(2, q)$ using its BN-pair structure with respect to the element listing for $GL(2, q)$ (see [7] , Theorem 7.2), which has the form of block circulant matrix.

2.5 Codes from Group Rings

In this section, we describe the structure of codes from unit and zero-divisor in group ring RG and illustrate that with examples. Here all facts and results were done by P. Hurley and T. Hurley in [14], [11], [17], [12] and [13] .

Definition 2.5.1. *Let RG be the group ring of the group G over the ring R, where the listing of the elements of G is given by $\{g_1, g_2, \ldots, g_n\}$. Suppose W is a submodule of RG, $x \in W$ and $u \in RG$ is given. Then the group ring encoding is a mapping $f : W \longrightarrow RG$ such that $f(x) = xu$ or $f(x) = ux$. In the first case, f is a right group ring encoding and in the letter case is a left group ring encoding.*

Thus, a code C derived from a group ring encoding is the image of a group ring encoding, for a given $u \in RG$, either $C = \{ux : x \in W\}$ or $C = \{xu : x \in W\}$.
In the group ring the multiplication is not necessary be commute, and this allows the construction of non-commutative.

Definition 2.5.2. *If $xu = ux$ for all x, then the code $C = \{xu : x \in W\}$ is said to be commutative, and otherwise non-commutative codes.*

When u is a zero-divisor, it generates a zero-divisor code and when it is a unit, it generates a unit-derived code.
when RG is finite and has an identity, only zero-divisors and units are contained in RG, this is also true where R is a field by (Theorem 2.3.3).

2.5.1 Unit-Derived Codes

Let G be a group of order n with the given listing $G = \{g_1, g_2, \ldots, g_n\}$, and let u be a unit in RG. Suppose that W a submodule of RG generated (as an R-module) by r group elements $S = \{g_{k_1}, g_{k_2}, \ldots, g_{k_r}\}$ such that $r \prec n$ and $\{k_1, k_2, \ldots, k_r\}$ is a subset of $\{1, 2, \ldots, n\}$.

The unit-derived code is $C = \{ux : x \in W\}$ or $C = \{xu : x \in W\}$. Thus the code is constructed from a unit u, a submodule W and, when RG is not commutative, the chosen of left or right encoding. In follows we assume that the encoding is on the right $(x \to xu)$, and in the left case $(x \to ux)$ is similar and has the same procedure.
Now $c \in C$ is a codeword if and only if $cu^{-1} \in W$ i.e. $c \in C$ if and only if the coefficients of $G \setminus S$ in cu^{-1} are zero.
A unit-derived code can also be considered a mapping from R^r to R^n. First, map a vector $\overline{x} = (\alpha_1, \alpha_2, \ldots, \alpha_r) \in R^r$ by $\lambda w(\overline{x}) = \sum_{i=1}^{r} \alpha_i g_{ki}$ to an element $x \in W$. Then a codeword $xu \in C$ is obtained which may be written $xu = \sum_{i=1}^{n} \beta_i g_i$. This gives an encoding $\overline{x} \mapsto (\beta_1, \beta_2, \ldots, \beta_n)$ which is a map from R^r to R^n.
There is another equivalent code, which called the matrix-generated code $\mathcal{D}$. This is a code from R^r to R^n and has an $(r \times n)$ generated matrix A, which is a constructed by using the RG-matrix U, and a check matrix constructed by using the RG-matrix V. Hence, the matrix-generated code is given by $\mathcal{D} = \{\overline{x}A : \overline{x} \in R^r\}$. Therefore, C and $\mathcal{D}$ are equivalent and they exhibit the same properties.

Generator and Check Matrices

Since u is a unit in RG, then there exist $u^{-1} \in RG$ such that $uu^{-1} = 1$. Suppose that U, U^{-1} respectively are the corresponding $(n \times n)$ RG-matrices. Consider W to be the submodule generated by $S = \{g_1, g_2, \ldots, g_r\}$ with $r \prec n$. (i.e. In this case we choose S to be the first r elements of the given listing by G). Later we will describe the general case. An element $x \in W$ is thus of the form $x = \sum_{i=1}^{r} \alpha_i g_i$. To construct the generator and check matrices for the code C, we will follow the following procedure:
Divide the RG-matrix U as $U = \begin{pmatrix} A \\ B \end{pmatrix}$ into block matrices where A is an $(r \times n)$-matrix and B is an $((n-r) \times n)$-matrix. Similarly, Let $U^{-1} = \begin{pmatrix} C & D \end{pmatrix}$ where C is an $(n \times r)$-matrix and D is an $(n \times (n-r))$-matrix.

Since $UU^{-1} = I_n$, then $AD = 0$, where A is the generator matrix for the matrix generated code. The following theorem shows that D^T is a check matrix.

Theorem 2.5.3. *([11], Theorem 5.1)*
Let $\overline{y} \in R^n$ and $\mathcal{D} = \{\overline{x}A : \overline{x} \in R^r\}$, then $\overline{y} \in \mathcal{D}$ if and only if $\overline{y}D = 0$.

Proof. Let $\overline{y} \in \mathcal{D}$, then there exist $\overline{x} \in R^r$ such that $\overline{y} = \overline{x}A$. since $AD = 0$, then clearly $\overline{y}D = 0$.
Conversely, let $\overline{y}D = 0$,

$$\overline{y} = \overline{y}I_n = \overline{y}.UU^{-1} = \overline{y}\begin{pmatrix} C & D \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} \overline{y}C & \overline{y}D \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} \overline{y}C & 0 \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix} = \overline{y}CA.$$

Now $\overline{y}$ is a vector in R^n and C is an $(n \times r)$-matrix, then $\overline{y}C \in R^r$ and $\overline{y} = \overline{y}UU^{-1} = \overline{x}A$ for some $\overline{x} \in R^r$ as required. □

So, D^T is a check matrix for the matrix-generated code $\mathcal{D}$. Therefore, $\overline{y}$ is a codeword in the matrix-generated code if and only if $D^T y^T = 0$ if and only if $\overline{y}D = 0$. The generator matrix A and the check matrix D^T produced from the RG-matrices U, U^{-1} and the submodule W have full allowable rank r and $n - r$ respectively. The RG-matrices of a units group ring elements are non-singular matrices, and this property allows the construction of codes from units. Hence, any non-singular matrix could produce a code by the above arguments.
When W is generated by a general basis $S = \{g_{k_1}, g_{k_2}, \ldots, g_{k_r}\}$, the generator and check matrices are obtained by extracting and adding to certain rows and columns from U and U^{-1}. A generator matrix results from the $(r \times n)$-matrix from the rows $k_1, k_2, \ldots, k_r$ of U. Additionally, consider D the $((n - r) \times n)$-matrix obtained by deleting the columns $k_1, k_2, \ldots, k_r$ columns of V. Then D^T is a check matrix.

Dual and orthogonal codes

As previously, the dual of a code from a group ring encoding is given by $C^{\perp} = \{y \in RG : < xu, y > = 0, \ \forall x \in W\}$, and the concept of the transpose (definition 2.1.2), we will show that the dual of a unit-derived code can be generated from $(u^{-1})^T$ as the following theorem.

Theorem 2.5.4. *([11], Theorem 5.2)*
Let W be a submodule with basis of group elements $S \subset G$ and $W^{\perp}$ be the submodule of RG with basis $G \setminus S$. Let $u \in RG$ be a unit such that $uu^{-1} = 1$. Then the dual code of $C = \{xu : x \in W\}$ is $C^{\perp} = \{x(u^{-1})^T : x \in W^{\perp}\}$.

Proof. Let $z \neq 0$ be an element in RG. We want to show that $\prec xu, z \succ = 0, \forall x \in W$ i.e. $z \in C^{\perp}$ if and only if $zu^T \in W^{\perp}$. Note that $\prec xu, y(u^{-1})^T \succ = \prec x, y \succ$. Thus, if $zu^T \in W^{\perp}$, then for all $x \in W$, $\prec xu, z \succ = \prec x, zu^T \succ = 0$
Conversely, by contra-position, if $zu^T \in W$ and choose an element $g \in S$ which has a non-zero coefficient γ in zu^T. Then $\prec gu, z \succ = \prec g, zu^T \succ = \gamma \neq 0$. □

Unit-derived code is said to be a self-dual code if C and $C^{\perp}$ are equivalent, or equivalently, that resultant matrix-generated code $\mathcal{D}$ and $\mathcal{D}^{\perp}$ are equal.

Definition 2.5.5. *([11], 5.3)*
An unit $u \in RG$ is orthogonal if and only if its inverse is u^T (i.e. $uu^T = 1$).

It is easy to see that the RG-matrix from an orthogonal unit u is an orthogonal matrix.

Example 2.5.6. *Let $R = \mathbb{Z}_2 = \{0, 1\}$ be the finite field of two elements and $G = S_3 =< a, b \mid a^3 = b^2 = 1, ba = a^2b >= \{1, a, a^2, b, ab, a^2b\}$ be the symmetric group of order 6. Then the coding matrices of S_3 is:*

$\times$	1	a	a^2	a^2b	ab	b
1	1	a	a^2	a^2b	ab	b
a^2	a^2	1	a	ab	b	a^2b
a	a	a^2	1	b	a^2b	ab
a^2b	a^2b	ab	b	1	a	a^2
ab	ab	b	a^2b	a^2	1	a
b	b	a^2b	ab	a	a^2	1

Thus,

$$M(S_3) = \begin{pmatrix} 1 & a & a^2 & a^2b & ab & b \\ a^2 & 1 & a & ab & b & a^2b \\ a & a^2 & 1 & b & a^2b & ab \\ a^2b & ab & b & 1 & a & a^2 \\ ab & b & a^2b & a^2 & 1 & a \\ b & a^2b & ab & a & a^2 & 1 \end{pmatrix}_{6\times 6}$$

And the group ring $RG = \mathbb{Z}_2S_3 = \sum_{g\in S_3} \alpha_g g \mid \alpha_g \in \mathbb{Z}_2 = \{c_0+c_1a+c_2a^2+c_3a^2b+c_4ab+c_5b \ ; \ c_i \in \mathbb{Z}_2\}$,Such that $(\mathbb{Z}_2S_3, +, .)$ is $\mathbb{F}$-algebra.
From T. Hurley's theorem (2.3.1) : $\mathbb{Z}_2S_3 \hookrightarrow M_{|S_3|\times|S_3|}(\mathbb{Z}_2)$.
So, if $u \in \mathbb{Z}_2S_3$; $u = c_0 + c_1a + c_2a^2 + c_3a^2b + c_4ab + c_5b$, then :

$$M(\mathbb{Z}_2S_3, u) = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 \\ c_2 & c_0 & c_1 & c_4 & c_5 & c_3 \\ c_1 & c_2 & c_0 & c_5 & c_3 & c_4 \\ c_3 & c_4 & c_5 & c_0 & c_1 & c_2 \\ c_4 & c_5 & c_3 & c_2 & c_0 & c_1 \\ c_5 & c_3 & c_4 & c_1 & c_2 & c_0 \end{pmatrix}_{6\times 6}$$

For the unit element $u = 1+a+a^2+ab+a^2b \in U(\mathbb{Z}_2S_3)$ there exists $u^{-1} = 1+a+a^2+ab+a^2b$ such that $uu^{-1} = 1$. Then we have $M(\mathbb{Z}_2S_3, u)$ as follows :

$$M(\mathbb{Z}_2S_3, u) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}_{6\times 6}$$

Also , from Hurley's theorems : If R has an identity 1_R , then $u \in RG$ is a unit if and only if $\sigma(u)$ is a unit in $R_{n\times n}$. Hence we have the invertible matrix as follows :

$U = \begin{pmatrix} A \\ B \end{pmatrix}$ *and* $V = \begin{pmatrix} C & D \end{pmatrix}$ *such that* $UV = 1_6$ *in* $R_{6\times 6}$.

Taking any r rows of U as a generator matrix define an $(n, r)-$code. Then we have

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}_{3\times 6},$$

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}_{3\times 6},$$

$$C = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}_{6\times 3}$$

And

$$D = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}_{6\times 3}$$

Such that

$$AC = BD = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_{3\times 3}$$

And

$$AD = BC = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}_{3\times 3}$$

Then, $UV = \begin{pmatrix} A \\ B \end{pmatrix} . \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = \begin{pmatrix} I_3 & O_3 \\ O_3 & I_3 \end{pmatrix} = I_{6\times 6}$.

The linear code C of dimension $k = 3$, generated by the matrix

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}_{3\times 6},$$

is the unit derived code $C = \{ux \mid x \in W\}$, *where* $S = \{a\} \subset G$ *and* $W =< a >= \{1, a, a^2\}$. *The dual code* $C^{\perp}$ *is the linear code generated by the matrix*

$$D^T = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}_{3\times 6},$$

with dimension $n - k = 3$. *The dual code can be considered as the submodule* $C^{\perp} = \{(u^{-1})^T y \mid y \in W^{\perp}\}$, *where* $W^{\perp} =< G - S >= \{a^2b, ab, b\}$.
So, $C = \{ux \mid x \in W\} = \{1 + a + a^2 + a^2b + ab, 1 + a + a^2 + b + a^2b, 1 + a^2 + a + ab + b\}$, $\theta(C) = \{111110, 111101, 111011\}$, *and* $C^{\perp} = \{(u^{-1})^T y \mid y \in W^{\perp}\} = \{1 + a^2b + ab + b + a, 1 + ab + b + a^2b + a^2, b + a^2b + ab + b + a\}$, $\theta(C^{\perp}) = \{110111, 101111, 011111\}$.
Clearly, the matrix A is the generator matrix for an $(6, 3)-$*code, and* D^T *is the parity-check matrix for this code, since it is a generator matrix of* $C^{\perp}$ *as defined in (definition 1.2.8).*

Definition 2.5.7. *([16])*
A linear code with a complementary dual (or an LCD code) is defined to be a linear code C *whose dual code* $C^{\perp}$ *satisfies* $C \cap C^{\perp} = \{0\}$.

From the last example (2.5.6) :

$$\theta(C) \cap \theta(C^{\perp}) = \{000000\}$$

So, this is satisfy $C \cap C^{\perp} = 0$, i.e. C is LCD code.

2.5.2 Zero-Divisors Codes

Let G be a group of order n with listing $\{g_1, g_2, \ldots, g_n\}$. Then the resultant code will be of length n and its dimension depending on the choice of the submodule W.
Suppose that a zero-divisor is $u \in RG$, such that $uv = 0$ for some non-zero element $v \in RG$. And W is a submodule of RG with basis of group elements $S \subseteq G$.
The zero-divisor code is $C = \{ux : x \in W\} = uW$ or $C = \{xu : x \in W\} = Wu$. This code constructed from a zero-divisor u, a submodule W, and when RG is non-commutative, the chosen of right or left encoding. We will describe the right-encoding case, where the left one is similar.
Consider u is a generator element of the code $C = Wu$ relative to the submodule W. Also, C may have another generator element and in fact may also be defined in terms of a different submodule.
The particular traditional case in which the code is a left ideal, when $C = Wu = RGu$, which means that $rank(u) = rank(U)$ has the same rank or dimension as (Wu), when u is a zero-divisor then $rank(U) = r < n$, and there is $v \neq 0$ and thus $y \in C$ satisfies $yv = 0$.

Definition 2.5.8. *([12], Definition 5.8)*
An element $v \in RG$ *is said to be a (left) check element for a zero-divisor code* C *when* $y \in C$ *if and only if* $vy = 0$. *Then we can write* $C = \{y \in RG : vy = 0\}$.

The code C may have more than one check element. Consider there is a set of check elements $v_1, v_2, \ldots, v_r$, then $y \in C$ if and only if $yv_i = 0$ for $1 \leq i \leq t$.
We note that in addition to using a zero-divisor as a generator, codes can also be constructed by using a zero-divisor instead directly as a check element, regardless of whether the code has one generator element or more.

Definition 2.5.9. *([12], Definition 5.9)*
Suppose T is a submodule of RG. Define $T_v = \{x \in T \mid xv = 0\}$ and say T_v is the check zero-divisor code relative to T.

Note that T_v is a submodule of RG and in the case where $T = RG$ we have that the code T_v is actually a left ideal.

Module

For the particular choice of module, now we restrict to the case when R is a field. Although some of results hold over integral domains also for rings in general.

Definition 2.5.10. *([11], Definition 5.10)*
Let T be a set of group ring elements $T \subset RG$, then T is linearly independent if $\sum_{x \in T} \alpha_x x = 0$, for $a_x \in R$, only when $\alpha_x = 0, \forall x \in T$. Otherwise, T is linearly dependent.

We define $rank(T)$ to be the maximum number of linearly independent elements of T. Thus $rank(T) = |T|$ if and only if T is linearly independent.
A zero-divisors code $C = Wu$, where W is the submodule of RG generated by $S \subseteq G$, and all element of C of the form $\sum_{g \in S} \alpha_g gu$. Thus the dimension of C is $rank(Su)$.
If we require R to be a field, and Su is linearly dependent, then there exists $S'u$ of Su which is linearly independent and generates the same module as Su. So let W' to be the submodule of W generated by S', then the code $C = Wu = W'u$, $S'u$ is linearly independent. Note that when we require Su is linearly independent this is equivalent to say that W has no zero-divisor of u. The maximum dimension a code for a given zero-divisor u is $r = rank(Gu)$.

Example 2.5.11. *Let $R = \mathbb{Z}_2 = \{0, 1\}$ be the finite field of two elements, and $G = C_3 =< g \mid g^3 = 1 >= \{1, g, g^2\}$ be a cyclic group of order 3. Such that the coding matrices of C_3 is:*

$$M(C_3) = \begin{pmatrix} 1 & g & g^2 \\ g^2 & 1 & g \\ g & g^2 & 1 \end{pmatrix}_{3\times 3}$$

And the group ring $RG = \mathbb{Z}_2 C_3 = \sum_{g \in C_3} \alpha_g g \mid \alpha_g \in \mathbb{Z}_2 = \{0, 1, g, g^2, 1+g, 1+g^2, g+g^2, 1+g+g^2\}$.
From T. Hurley's theorem (2.3.1) : $\mathbb{Z}_2 C_3 \hookrightarrow M_{|C_3|\times|C_3|}(\mathbb{Z}_2)$.
Suppose that $u, v \in \mathbb{Z}_2 C_3$; $u = 1 + g$ and $v = 1 + g + g^2$ such that $u.v = (1+g)(1+g+g^2) = 1 + g + g^2 + g + g^2 + 1 = 0$, this mean that u is zero-divisor in $\mathbb{Z}_2 C_3$, then we have $M(\mathbb{Z}_2 C_3, u)$ as follows:

$$U = M(\mathbb{Z}_2 C_3, u) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}_{3\times 3}$$

And,

$$V = M(\mathbb{Z}_2C_3, v) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}_{3\times 3}$$

Let W be the submodule of $\mathbb{Z}_2C_3$ generated by $S = \{1, g\}$ i.e. $W =< S >= \{0, 1, g, 1 + g\}$. Then $(Su) = \{1, g\}(1 + g) = \{1 + g, g + g^2\}$ and so $rank(Su) = 2$. Then a zero-divisor code is $C = \{ux \mid x \in W\} = \{0, 1 + g, g + g^2, 1 + g^2\}$. Thus $\theta(C) = \{000, 110, 011, 101\}$ is a $(3, 2, 2)$ binary cyclic linear code.
The generator matrix of this code is

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}_{2\times 3}$$

and the parity-check matrix is

$$H^T = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}_{3\times 2},$$

such that $G.H^T = 0$ as follows:

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

Chapter 3

Coding Matrices for the Semi-Direct Product Groups

In this chapter, we explain the definition of the semi-direct product group. And generalize some known results for semi-direct product groups of cyclic groups.

3.1 The Semi-Direct Product Groups

In group theory, a semi-direct-product is a generalization of the direct product which expresses a group as a product of subgroups. Such that G is a direct product of two groups if contains normal subgroups N_1, N_2 ; $N_1 \cap N_2 = \{e\}$ and $G = N_1 N_2$. While G is a semi-direct product of two groups if it contains subgroups H and K ; $H \lhd G$, $H \cap K = \{e\}$ and that $G = HK$ (i.e. every element of HK can be written uniquely as a product hk , $\forall\ h \in H$, $k \in K$ - by proposition 8 in [4]).
Since H is a normal in G, the group K acts on H by conjugation: $k.h = khk^{-1}\ for\ h \in H$, $k \in K$.

Definition 3.1.1. *([22], Definition 9.1)*
Let H and K be groups and K acts on H if to each $h \in H$ and $k \in K$ there corresponds a unique element $h^k = hk \in H$ such that $\forall\ h_1, h_2 \in H$ and $k_1, k_2 \in K$, $(h^{k1})^{k_2} = h^{k_1 k_2}, h^1 = h$ and $(h_1 h_2)^k = h_1^k h_2^k$.

This definition means that there is a homomorphism ϕ ; $\phi : K \longrightarrow Aut(H)$, defined by $\phi : K \longmapsto \phi_k$ and we call ϕ the automorphism representation of K corresponding to the action (or simply, call ϕ the action).

Theorem 3.1.2. *([4], Theorem 10 in ch 5)*
Let H and K be groups and let ϕ be a homomorphism , $\phi : K \longrightarrow Aut(H)$ and let denote the action of K on H determined by ϕ. Suppose that G is the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define the following multiplication on G:

$$(h_1, k_1)(h_2, k_2) = (h_1 \phi_{k_1} h_2\ ,\ k_1 k_2).$$

such that:

1 • *This multiplication makes G into a group of order $|G| = |H|\ |K|$.*

2 • *The sets $\{(h,1) \mid h \in H\}$ and $\{(1,k) \mid k \in K\}$ are subgroups of G and the maps $h \longmapsto (h,1)$, $k \longmapsto (1,k)$ are*

$$H : h \longmapsto (h,1) \cong \{(h,1) \mid h \in H\} \leq G,$$

$$K : k \longmapsto (1,k) \cong \{(1,k) \mid k \in K\} \leq G$$

for all $h \in H$ and $k \in K$.
by (2 •), then we have:

3 • *$H \trianglelefteq G$*

4 • *$H \bigcap K = 1$*

5 • *for all $h \in H$ and $k \in k$, $khk^{-1} = kh = \phi_k(h)$ where $\phi_k : h \longmapsto h$.*

The proof of this theorem is clearly in [4] .
So the group described in above theorem is called the semi-direct product as following:

Definition 3.1.3. *([22] and [4])*
Let H and K be groups and let ϕ be a homomorphism,

$$\phi : K \longrightarrow Aut(H)$$

Then the semi-direct product of H and K with respect the action ϕ is the group G containing of ordered pairs (h,k) with $h \in H$ and $k \in K$ defined by:

$$(h_1,k_1)(h_2,k_2) = (h_1\phi_{k_1}h_2\ ,\ k_1k_2)$$

Where $\phi_k(h) = kh = khk^{-1}$, $\forall\ h \in H$, $k \in K$.

Denote of semi-direct product by $H \rtimes_\phi K$ (or simply, write $H \rtimes K$).

Example 3.1.4. *Let $G = S_3$, let N be the normal subgroup of order 3 generated by a 3-cycle, and let H be a subgroup of order 2 generated by a 2-cycle. Then $G = N \rtimes H$. This example generalizes a long two different lines:*

1 • *Let $G = S_n$, $N = A_n$ and H a subgroup of order 2 generated by a 2-cycle. Then $G = N \rtimes H$.*

2 • *Let $G = D_{2n}$, the dihedral group of order $2n$. Then let $N = C_n$ and $H = C_2$. Then $D_{2n} \cong C_n \rtimes C_2$.*

In the next section, we shall generalize (theorem 8 of [14]) to semi-direct product group of cyclic groups in the light of (example 3.1.4, (2)) above.

3.2 Coding Matrices of Semi-Direct Product Groups

According to ([14] ,Theorem 8), the coding matrices of the dihedral group $D_{2n} \cong C_n \rtimes C_2$ is known to be of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$ (where A is a circulant matrix and B is an $(n \times n)$ Hankel-type-matrix). This can to be generalized to the semi-direct product groups $G = C_n \rtimes C_2$.

A circulant matrix is special type of Toeplitz matrix, which is one that is constant a long any diagonal running from upper left to lower right as defined in (definition 2.4.1).

While a (general) Hankel matrix is one which is constant on any diagonal from upper right to lower left as defined in(definition 2.4.2).

Consider $G = C_n \rtimes C_m$; $C_n \lhd G$ of two groups $C_n =< x >= \{x \mid x^n = 1\}$ and $C_m =< y >= \{y \mid y^m = 1\}$. We may list the elements of the semi-direct product $C_n \rtimes C_m$ as follows: $x^i y^j \ ; \ 0 \leqslant i \leqslant n-1, \ 0 \leqslant j \leqslant m-1 \ :$

$$1, x, x^2, \ldots, x^{n-1} \ , \ y, xy, x^2y, \ldots, x^{n-1}y \ , \ y^2, xy^2, x^2y^2, \ldots, x^{n-1}y^2 \ , \ \ldots\ldots\ldots \ ,$$
$$y^{m-1}, xy^{m-1}, x^2y^{m-1}, \ldots \ , \ x^{n-1}y^{m-1} \ .$$

(m blocks each with n elements).
This product defined by the action of C_m on C_n (or group homomorphism) given by $\phi : C_m \longrightarrow Aut(C_n)$; $C_n \rtimes C_m = \{x^i y^j \ : \ x^i \in C_n \ , \ y^j \in C_m \mid x^i y^j . x^s y^t = x^i \phi_{y^j} x^s . y^j y^t\}$. The inverse of the element $x^i y^j$ in $C_n \rtimes C_m$ is $\phi_{(m-j)} x^{n-i} . y^{m-j}$.

In fact, the automorphism group $Aut(C_n)$ is one to one correspondence with the set $\{x^r \mid hcf(n, r) = 1\}$ of generators of C_n, so $|Aut(C_n)| = \varphi(n)$, where φ is the Euler function.

Definition 3.2.1. *The Euler φ-function is defined as: for $n \in Z^+$, let $\varphi(n)$ be the number of positive integers $a \leqslant n$ with $(a, n) = 1$.*

Here, the non-identity element of C_2 acts on C_n by inverting elements; this is an automorphisms since C_n is an abelian, and the presentation for this group is:

$$< xy | x^n = y^m = 1, yxy^{-1} = x^{-1} >$$

More generally, a semi-direct product of any two cyclic groups C_n with generator x and C_m with generator y is given by one extra relation, $yxy^{-1} = x^k$, with $(k, n) = 1$, where $Aut(C_n) : x \longrightarrow x^k$ for some k; that is, the presentation:

$$< xy | x^n = y^m = 1, yxy^{-1} = x^k >$$

If y^r is a generator of C_m and $(r, m) = 1$, hence we have the presentation:

$$< xy | x^n = y^m = 1, y^r x y^{r^{-1}} = x^{k^r} > .$$

Now, taking the trivial homomorphism $\phi : C_m \longrightarrow Aut(C_n)$; $C_m \mapsto I_{C_n}$ gives the direct product $G = C_n \rtimes C_m = C_n \times C_m$.
Now, consider $G = C_n \rtimes C_m$, we need to know when there is a non-trivial homomorphism $\phi : C_m \longrightarrow Aut(C_n)$ but since $Aut(C_n) \cong C_{\varphi(n)}$ and since $Hom(C_m, C_{\varphi(n)}) \cong C_{hcf(m,\varphi(n)\ )}$ we have the following:

Lemma 3.2.2. *There is a non-trivial homomorphism $\phi : C_m \longrightarrow Aut(C_n)$ iff $hcf(m, \varphi(n)) \neq 1$.*

Proof. We have $Hom(C_m, C_{\varphi(n)}) \cong C_{hcf(m,\varphi(n)\ )}$.
If $hcf(\ m, \varphi(n)\ ) = 1$ then $Hom(C_m, C_{\varphi(n)}) \cong C_1$ the trivial subgroup and so the only element $\phi \in Hom(C_m, C_{\varphi(n)})$ is the trivial one given by $\phi(y) = I_{C_n}$. Conversely, suppose that $hcf(m, \varphi(n)) \neq 1$, to define $\phi \in Hom(C_m, C_{\varphi(n)})$ by $\phi(y) : x \longmapsto x^t$ (where $1 \leq t < \varphi(n)$ with $hcf(t, \varphi(n)) \neq 1$ in order for x^t to be a generator for $C_{\varphi(n)}$), we must have $order(\phi(y)) \mid m$ (as $y^m = 1$) and $order(\phi(y)) \mid \varphi(n)$ (as $\phi(y) \in C_{\varphi(n)}$). But this is possible since $hcf(m, \varphi(n)) \neq 1$. □

So for example there will be no non-trivial semi-direct product $C_n \rtimes C_m$ (i.e. different from the direct product $C_n \times C_m$) if $hcf(m, \varphi(n)) = 1$, for instance $C_4 \rtimes C_3$ the only homomorphism $\phi : C_3 \longrightarrow Aut(C_4)$ is the one, which takes $y \in C_m =< y >$ to the identity $I_{C_4} \in Aut(C_4) =< \theta_3 >= \{I_{C_4}, \theta_3\}; \theta_3 : x \longmapsto x^3 = x^{-1}$, therefore the only semi-direct product $C_4 \rtimes C_3$ is the direct product $C_4 \times C_3$. We consider another following example:

Example 3.2.3. *Consider the semi-direct product $G = C_7 \rtimes C_3$, where $\phi : C_3 \longrightarrow Aut(C_7) \cong C_6$. In fact $Aut(C_7) = \{\theta_i | i = 1, 2, 3, 4, 5, 6\} =< \theta_3 >=< \theta_5 > \cong C_6$; i.e. $order(\theta_3) = order(\theta_5) = 6$, while $order(\theta_2) = order(\theta_4) = 3$ and $order(\theta_6) = 2$. Therefore we may take $\phi_i : C_3 \longrightarrow Aut(C_7)$ to be the group homomorphism (or the action of C_3 on C_7) defined as $(\phi_i(y) = \theta_i; i = 1, 2, 4)$, since $order(y) = 3 \mid order(\theta_i); i = 1, 2, 4$.*
Clearly $\phi_1(y) = \theta_1 = I_{C_7}$ will induce the direct product $C_7 \times C_3$. (In fact it is easy to prove from the relations that $C_7 \rtimes_{\phi_4} C_3 \cong C_7 \rtimes_{\phi_2} C_3$). So we take $\phi_2(y) = \theta_2 : x \longmapsto x^2$ and consider the semi-direct product group $G = C_7 \rtimes_{\phi_2} C_3 =< xy | x^7 = y^3 = 1, yxy^{-1} = x^2 >$, generally $G = C_7 \rtimes_{\phi_i} C_3 =< xy | x^7 = y^3 = 1, yxy^{-1} = x^i; i = 1, 2, 4 >$.

In the following examples, we will clarify the coding matrices of $C_n \rtimes C_2$.

Example 3.2.4. *The semi-direct product of two cyclic groups* $C_3 \rtimes C_2$ *;* $C_3 =\prec x \mid x^3 = 1 \succ = \{1, x, x^2\}$ *and* $C_2 =\prec y \mid y^2 = 1 \succ = \{1, y\}$*. The listing of elements of* $C_3 \rtimes C_2$ *are :* $1, x, x^2, y, xy, x^2y$*. And we have non-trivial homomorphism since* $(2, \varphi(3)\ ) = (2, 2) = 2 \neq 1$*, the action of* C_2 *on* C_3 *given by* $\phi : C_2 \to Aut(C_3)$*, such that* $Aut(C_3)$ *is* $\phi : C_3 \longrightarrow C_3$ *;* $\mid Aut(C_3) \mid = \varphi(3) = 2$*, hence we have* $Aut(C_3) = \{\phi_1 : x \longrightarrow x\ ,\ \phi_2 : x \longrightarrow x^2\}$*.*

At ϕ_1 *give us the semi-direct product as a direct product, but at* ϕ_2 *give us the semi-direct product with the presentation* $< xy | x^3 = y^2 = 1, yxy^{-1} = x^{-1} >$ *;* $C_3 \rtimes C_2 = \{\ xy\ :\ x \in C_3\ ,\ y \in C_2\ :\ x_1y_1.x_2y_2 = x_1\phi_{y_1}(x_2).y_1y_2\ \}$ *and the inverse of the element* yx *is* $(\phi_{y^{-1}}(x^{-1}).y^{-1})$ *as following:*

at ϕ_1

$\times$	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x^2	x^2	1	x	x^2y	y	xy
x	x	x^2	1	xy	x^2y	y
y	y	xy	x^2y	1	x	x^2
x^2y	x^2y	y	xy	x^2	1	x
xy	xy	x^2y	y	x	x^2	1

and at ϕ_2

$\rtimes$	1	x	x^2	x^2y	xy	y
1	1	x	x^2	x^2y	xy	y
x^2	x^2	1	x	xy	y	x^2y
x	x	x^2	1	y	x^2y	xy
x^2y	x^2y	xy	y	1	x	x^2
xy	xy	y	x^2y	x^2	1	x
y	y	x^2y	xy	x	x^2	1

Note that the coding matrices of the semi-direct product group $C_3 \rtimes C_2$ is known to be of the form

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}_{6\times 6}$$

Where A is an (3×3) circulant matrix and B is an (3×3) Hankel-type-matrix.

Example 3.2.5. *If we take another example* $C_4 \rtimes C_2$ *;* $C_4 =\prec x \mid x^4 = 1 \succ = \{1, x, x^2, x^3\}$ *and* $C_2 =\prec y \mid y^2 = 1 \succ = \{1, y\}$*. The listing of elements of* $C_4 \rtimes C_2$ *are :* $1, x, x^2, x^3, y, xy, x^2y, x^3y$*. And we have non-trivial homomorphism since* $(2, \varphi(4)\ ) = (2, 2) = 2 \neq 1$*, so the action of* C_2 *on* C_4 *given by* $\phi : C_2 \to Aut(C_4)$*, such that* $Aut(C_4)$ *is* $\phi : C_4 \longrightarrow C_4$ *;* $\mid Aut(C_4) \mid = \varphi(4) = 2$*,*

hence we have $Aut(C_4) = \{\phi_1 : x \longrightarrow x \ , \ \phi_3 : x \longrightarrow x^3\}$

At ϕ_1 *give us the semi-direct product as a direct product, but at* ϕ_3 *give us the semi-direct product with the presentation* $< xy | x^4 = y^2 = 1, yxy^{-1} = x^{-1} >$ *;* $C_4 \rtimes C_2 = \{ \ xy \ : \ x \in C_4 \ , \ y \in C_2 \ : \ x_1y_1.x_2y_2 = x_1\phi_{y_1}(x_2).y_1y_2 \ \}$ *and the inverse of the element* yx *is* $(\phi_{y^{-1}}(x^{-1}).y^{-1})$ *as following:*

at ϕ_1

$\times$	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x^3	x^3	1	x	x^2	x^3y	y	xy	x^2y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x	x	x^2	x^3	1	xy	x^2y	x^3y	y
y	y	xy	x^2y	x^3y	1	x	x^2	x^3
x^3y	x^3y	y	xy	x^2y	x^3	1	x	x^2
x^2y	x^2y	x^3y	y	xy	x^2	x^3	1	x
xy	xy	x^2y	x^3y	y	x	x^2	x^3	1

and at ϕ_3

$\rtimes$	1	x	x^2	x^3	x^3y	x^2y	xy	y
1	1	x	x^2	x^3	x^3y	x^2y	xy	y
x^3	x^3	1	x	x^2	x^2y	xy	y	x^3y
x^2	x^2	x^3	1	x	xy	y	x^3y	x^2y
x	x	x^2	x^3	1	y	x^3y	x^2y	xy
x^3y	x^3y	x^2y	xy	y	1	x	x^2	x^3
x^2y	x^2y	xy	y	x^3y	x^3	1	x	x^2
xy	xy	y	x^3y	x^2y	x^2	x^3	1	x
y	y	x^3y	x^2y	xy	x	x^2	x^3	1

Note that the coding matrices of the semi-direct product group $C_4 \rtimes C_2$ is known to be of the form

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}_{8\times 8}$$

Where A is an (4×4) circulant matrix and B is an (4×4) Hankel-type-matrix.

Example 3.2.6. *Also, if we take an example* $C_7 \rtimes C_2$ *;* $C_7 =< x \mid x^7 = 1 >= \{1, x, x^2, x^3, x^4, x^5, x^6\}$ *and* $C_2 =< y \mid y^2 = 1 >= \{1, y\}$*. The listing of elements of* $C_7 \rtimes C_2$ *are :* $1, x, x^2, x^3, x^4, x^5, x^6, y, xy, x^2y, x^3y, x^4y, x^5y, x^6y$*. And we have the non-trivial homomorphism since* $(2, \varphi(7)) = (2, 6) = 2 \neq 1$*, so the action of* C_2 *on* C_7 *given by* $\phi : C_2 \to Aut(C_7) \cong C_6$*, such that* $Aut(C_7)$ *is*

$\{\theta_i \mid i = 1,2,3,4,5,6\}$, *here this action defines as* $\phi_i(y) = \theta_i \mid i = 1,6$, *since* $order(y) = 2 \mid order(\theta_i); i = 1,6$.

At ϕ_1 *give us the semi-direct product as a direct product, but at* $\phi_6 : x \longmapsto x^6$ *give us the semi-direct product with the presentation* $< xy|x^7 = y^2 = 1, yxy^{-1} = x^{-1} >$ *;* $C_7 \rtimes C_2 = \{\ xy\ :\ x \in C_7\ ,\ y \in C_2\ :\ x_1y_1.x_2y_2 = x_1\phi_{y_1}(x_2).y_1y_2\ \}$ *and the inverse of the element* yx *is* $(\phi_{y^{-1}}(x^{-1}).y^{-1})$ *as following:*

at ϕ_6

$\rtimes$	1	x	x^2	x^3	x^4	x^5	x^6	x^6y	x^5y	x^4y	x^3y	x^2y	xy	y
1	1	x	x^2	x^3	x^4	x^5	x^6	x^6y	x^5y	x^4y	x^3y	x^2y	xy	y
x^6	x^6	1	x	x^2	x^3	x^4	x^5	x^5y	x^4y	x^3y	x^2y	xy	y	x^6y
x^5	x^5	x^6	1	x	x^2	x^3	x^4	x^4y	x^3y	x^2y	xy	y	x^6y	x^5y
x^4	x^4	x^5	x^6	1	x	x^2	x^3	x^3y	x^2y	xy	y	x^6y	x^5y	x^4y
x^3	x^3	x^4	x^5	x^6	1	x	x^2	x^2y	xy	y	x^6y	x^5y	x^4y	x^3y
x^2	x^2	x^3	x^4	x^5	x^6	1	x	xy	y	x^6y	x^5y	x^4y	x^3y	x^2y
x	x	x^2	x^3	x^4	x^5	x^6	1	y	x^6y	x^5y	x^4y	x^3y	x^2y	xy
x^6y	x^6y	x^5y	x^4y	x^3y	x^2y	xy	y	1	x	x^2	x^3	x^4	x^5	x^6
x^5y	x^5y	x^4y	x^3y	x^2y	xy	y	x^6y	x^6	1	x	x^2	x^3	x^4	x^5
x^4y	x^4y	x^3y	x^2y	xy	y	x^6y	x^5y	x^5	x^6	1	x	x^2	x^3	x^4
x^3y	x^3y	x^2y	xy	y	x^6y	x^5y	x^4y	x^4	x^5	x^6	1	x	x^2	x^3
x^2y	x^2y	xy	y	x^6y	x^5y	x^4y	x^3y	x^3	x^4	x^5	x^6	1	x	x^2
xy	xy	y	x^6y	x^5y	x^4y	x^3y	x^2y	x^2	x^3	x^4	x^5	x^6	1	x
y	y	x^6y	x^5y	x^4y	x^3y	x^2y	xy	x	x^2	x^3	x^4	x^5	x^6	1

Note that the coding matrices of this product group is known to be of the form

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}_{14\times 14}$$

Where A is an (7×7) circulant matrix and B is an (7×7) Hankel-type-matrix.

In general, the following example describes the coding matrix for the dihedral group as semi-direct product group.

Example 3.2.7. $C_n \rtimes C_2 \cong D_{2n}$ *such that* $C_n =< x \mid x^n = 1 >= \{1, x, x^2, \ldots, x^{n-1}\}$, $C_2 =< y \mid y^2 = 1 >= \{1, y\}$, *the listing of elements of* $C_n \rtimes C_2$ *are :* $1, x, x^2, ..., x^{n-1}, y, xy, x^2y, ..., x^{n-1}y$. *And there is a non-trivial homomorphism since* $(2, \varphi(n)\ ) \neq 1$, *so the action of* C_2 *on* C_n *given by* $\phi : C_2 \longrightarrow Aut(C_n)$; $Aut(C_n) : \phi : C_n \longrightarrow C_n$,
$\mid Aut(C_n) \mid = \varphi(n)$, *hence we have* $Aut(C_n) = \{\phi_1 : x \longrightarrow x\ ,\ \phi_{n-1} : x \longrightarrow x^{n-1}\}$.

$C_n \rtimes C_2 = \{\ xy\ :\ x \in C_n\ ,\ y \in C_2\ :\ x_1y_1.x_2y_2 = x_1\phi_{y_1}(x_2).y_1y_2\ \}$, and the inverse of the element yx is $(\phi_{y^{-1}}(x^{-1}).y^{-1})$.
At ϕ_1 give us the semi-direct product as a direct product, but at ϕ_{n-1} give us the semi-direct product groups as following:

at ϕ_1

$\times$	1	x	x^2	..	x^{n-1}	y	xy	x^2y	..	$x^{n-1}y$
1	1	x	x^2	..	x^{n-1}	y	xy	x^2y	..	$x^{n-1}y$
x^{n-1}	x^{n-1}	1	x	..	x^{n-2}	$x^{n-1}x$	y	xy	..	$x^{n-2}y$
x^{n-2}	x^{n-2}	x^{n-1}	1	..	x^{n-3}	$x^{n-2}y$	$x^{n-1}y$	y	..	$x^{n-3}y$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
x	x	x^2	x^3	..	1	xy	x^2y	x^3y	..	y
y	y	xy	x^2y	..	$x^{n-1}y$	1	x	x^2	..	x^{n-1}
$x^{n-1}y$	$x^{n-1}y$	y	xy	..	$x^{n-2}y$	x^{n-1}	1	x	..	x^{n-2}
$x^{n-2}y$	$x^{n-2}y$	$x^{n-1}y$	y	..	$x^{n-3}y$	x^{n-2}	x^{n-1}	1	..	x^{n-3}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
xy	xy	x^2y	x^3y	..	y	x	x^2	x^3	..	1

and at ϕ_{n-1}

$\rtimes$	1	x	x^2	..	x^{n-1}	$x^{n-1}y$	..	x^2y	xy	y
1	1	x	x^2	..	x^{n-1}	$x^{n-1}y$	..	x^2y	xy	y
x^{n-1}	x^{n-1}	1	x	..	x^{n-2}	$x^{n-2}y$	..	xy	y	$x^{n-1}y$
x^{n-2}	x^{n-2}	x^{n-1}	1	..	x^{n-3}	$x^{n-3}y$	..	y	$x^{n-1}y$	$x^{n-2}y$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
x	x	x^2	x^3	..	1	y	..	x^3y	x^2y	xy
$x^{n-1}y$	$x^{n-1}y$	$x^{n-2}y$	$x^{n-3}y$	..	y	1	..	x^{n-3}	x^{n-2}	x^{n-1}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
x^2	x^2	xy	y	..	x^3y	x^3	..	1	x	x^2
xy	xy	y	$x^{n-1}y$	..	x^2y	x^2	..	x^{n-1}	1	x
y	y	$x^{n-1}y$	x^2y	..	xy	x	..	x^{n-2}	x^{n-1}	1

Note that the coding matrices of the semi-direct product group $C_n \rtimes C_2$ is known to be of the form

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

Where A is an $(n \times n)$ circulant matrix and B is an $(n \times n)$ Hankel-type-matrix.

Summarizing, we have the following theorem which describes the coding matrices for the semi-direct product of $C_n \rtimes C_2$.

Theorem 3.2.8. *Let $G = C_n \rtimes C_2$ be a semi direct product of two cyclic groups, such that $C_n \lhd G$, $C_n =\prec x \succ$ and $C_m =\prec y \succ$ depends of the action on the normal subgroup (or the automorphism). Then we may choose a listing for the group G according to which its coding matrix will have the form*

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

Where A is an $(n \times n)$ circulant matrix and B is an $(n \times n)$ Hankel-type-matrix.

All automorphisms will give rise to the same form, and note that there is a transfer map from one matrix to another matrix coming from two automorphisms as following:

Theorem 3.2.9. *If $G = C_n \rtimes_\phi C_2$ and $G = C_n \rtimes_\psi C_2$; $\phi, \psi \in Aut(C_n)$, ϕ is trivial automorphism and ψ is any automorphism. Then there is a transfer map from the coding matrices of $C_n \rtimes_\phi C_2$ to the coding matrices of $C_n \rtimes_\psi C_2$, $T_{\phi\to\psi} : M(C_n \rtimes_\phi C_2) \to M(C_n \rtimes_\psi C_2)$ defined by $T_{\phi\to\psi}(x^i y^j) = \psi(x^i).y^j$ such that $x^i y^j \in C_n \rtimes_\phi C_2$ and y^j is the non-identity element of C_2, $1 \le i \le n$ and $1 \le j \le m$. These automorphisms ϕ, ψ will give rise to the same form of coding matrices in terms of the number of blocks, but the type of shown blocks depends on these automorphisms.*

Proof. Suppose that $G = C_n \rtimes C_2$ defined as (theorem 3.2.8) above. Then, by (theorem 3.2.8) the coding matrix of $C_n \rtimes_\phi C_2 = C_n \times C_2$, since ϕ is trivial automorphism in C_n has the form :

$$M(C_n \rtimes_\phi C_2) = M(C_n \times C_2) = \begin{pmatrix} A & A' \\ A' & A \end{pmatrix}_{(2n\times 2n)}$$

and, the coding matrix of $C_n \rtimes_\psi C_2$, $\psi \in Aut(C_n)$ has the form :

$$M(C_n \rtimes_\psi C_2) = \begin{pmatrix} A & B \\ B & A \end{pmatrix}_{(nm\times nm)}$$

Where A,A' are $(n \times n)$ circulant matrices and B is an $(n \times n)$ Hankel matrix of a special form, i.e. it has the same number $(n \times n)$ of blocks each with (2×2) of elements.
Consider $M(C_n \rtimes_\phi C_2)$ with respect the action $\phi : x \longrightarrow x$ and $M(C_n \rtimes_\psi C_2)$ with respect the action $\psi : x \longrightarrow x^{-1} = x^{n-1}$.
Comparing the opposite elements in both matrices, we have an element $x^i y^j \in C_n \rtimes_\phi C_2$; y^j is the non-identity element of C_2, and an element $x^{n-i} y^j \in C_n \rtimes_\psi C_2$.

Then, there is a transfer map between the elements of these matrices which is defined as following:

$$T_{\phi\to\psi}(x^i y^j) = x^{n-i} y^j = \psi(x^i).y^j$$

where $1 \le i \le n$ and $1 \le j \le m$. □

3.3 Semi-Direct Product Groups Zero-Divisor Codes

In ([12], section 5.4.1, p.188), P. Hurley and T. Hurley showed how to construct zero-divisor elements, and hence codes in dihedral group from zero-divisors in its cyclic subgroup. In this section we provide a generalization of this construction for the semi-direct product groups.

Consider $R(C_n \rtimes C_2)$, the group ring of the semi-direct product of the cyclic group of order n with the cyclic group of order 2 over the ring R. Let $u \in C_n$ be a zero-divisor such that $uv = 0$ and let C_2 be generated by y and let C_n be generated by x. From it a zero-divisor of the form $u + uya \in C_n \rtimes C_2$ can be constructed for any $a \in C_n$ with $(u + uya)(v + v^T yb) = 0$ for any $b \in C_n$. For simplicity, consider the case $a = b = 1$ as the following theorem.

Theorem 3.3.1. *Let u be a zero-divisor in $\mathbb{Z}_2 C_n$, then there is a zero-divisor in $\mathbb{Z}_2(C_n \rtimes C_2)$ has the form $u + uy$.*

Proof. Consider the group ring $\mathbb{Z}_2(C_n \rtimes C_2)$ has $\mid \mathbb{Z}_2 \mid^{|C_n \rtimes C_2|} = 2^{2n}$ elements of the form $\sum_{g \in C_n \rtimes C_2} \alpha_g g \ ; \ \alpha_g \in \mathbb{Z}_2$.
Let $u = \sum_{g \in C_n} u_g g \ ; \ u_g \in \mathbb{Z}_2$ be a zero-divisor in $\mathbb{Z}_2 C_n$ such that $uv = 0$ where $v = \sum_{h \in C_n} v_h h \ ; \ v_h \in \mathbb{Z}_2 \ , \ v \in \mathbb{Z}_2 C_n$. From it there is an element of the form $u + uy \ \in \mathbb{Z}_2(C_n \rtimes C_2)$ such that

$$(u + uy)(v + v^T y) = uv + uv^T y + uvy + uv^T = uv^T y + uv^T$$

Since $uv = 0 \ , \ \mathbb{Z}_2 C_n \subseteq \mathbb{Z}_2(C_n \rtimes C_2)$.
So, $uv^T y + uv^T = (y + 1)uv^T = (y + 1) \sum_{g \in C_n} u_g g \ \sum_{h \in C_n} v_h h^{-1} = (y + 1) \sum_{g \in C_n} \sum_{h \in C_n} u_g v_h g h^{-1} \ ;$
$u_g v_h \in \mathbb{Z}_2$, hence $\sum_{g \in C_n} \sum_{h \in C_n} u_g v_h \ = \ 2k \ ; \ k \in \mathbb{Z}$.
Therefore, $uv^T y + uv^T$ must be equal to (even number) mod 2.
Since we have three cases of multiplication (uv^T) and two cases of addition $uv^T y + uv^T$ as following:

u	v^T	uv^T	$uv^T + uv^T$
even	even	even	even+even=even
even	odd	even	even+even=even
odd	odd	odd	odd+odd=even

Thus, $uv^T y + uv^T = (even\ number)\ mod\ 2 = 0$. So, $(u + uy)(v + v^T y) = 0 \ ; \ (u + uy) \neq 0\ and\ (v + v^T y) \neq 0$. Then $u + uy$ is a zero-divisor in $\mathbb{Z}_2(C_n \rtimes C_2)$. □

Example 3.3.2. *Consider $\mathbb{Z}_2(C_3 \rtimes C_2)$, the group ring of the semi-direct product of the cyclic group of order 2 with cyclic group of order 3 over the field of two elements. Let $C_2 =< y >= \{1, y\}$ be generated by y and let $C_3 =< x >= \{1, x, x^2\}$ be generated by x. The listing of elements of $C_3 \rtimes C_2$ are: $1, x, x^2, y, xy, x^2 y$ and has the coding matrices of the form*

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

(As already mentioned in an example 3.2.4).
The group ring $\mathbb{Z}_2(C_3 \rtimes C_2)$ *has* $|R|^{|G|} = 2^6 = 64$ *elements of the form* $\sum_{g \in C_3 \rtimes C_2} \alpha_g g \mid \alpha_g \in \mathbb{Z}_2$.
Consider $u \in \mathbb{Z}_2 C_3$; *u is zero-divisor such that*

$$u.v \;=\; (1+x^2)\;(1+x+x^2) \;=\; 1+x+x^2+x^2+1+x \;=\; 0.$$

At the non-trivial homomorphism $\phi_2 : x \longmapsto x^2$ *in (example 3.2.4), we have* $(u+uy)(v+v^T y)$ *as*

$$(1+x^2+(1+x^2)y)\;(1+x+x^2+(1+x^2+x)y) \;=\; (1+x^2+y+x^2y)(1+x+x^2+y+x^2y+xy) \;=$$
$$1+x+x^2+y+x^2y+xy+x^2+1+x+x^2y+xy+y+y+x^2y+xy+1+x+x^2+x^2y+xy+y+x^2+1+x=0$$

So, $u+uy = 1+x^2+y+x^2y$ *is zero-divisor in* $\mathbb{Z}_2(C_3 \rtimes C_2)$. *Then we have*

$$U = M(\mathbb{Z}_2(C_3 \rtimes C_2), u) = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}_{6\times 6}$$

And,

$$V = M(\mathbb{Z}_2(C_3 \rtimes C_2), v) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}_{6\times 6}$$

Let W *be the submodule of* $\mathbb{Z}_2(C_3 \rtimes C_2)$ *generated by* $S = \{1, x\}$ *i.e.* $W =< 1, x >= \{0, 1, x, 1+x\}$. *Then a zero-divisor code is* $C = \{ux \mid x \in W\} = \{0, 1+x^2+y+x^2y, x+1+xy+y, x+x^2+x^2y+xy\}$. *Thus* $\theta(C) = \{000000, 101101, 110011, 011110\}$ *is a* $(6,3)$ *binary linear code.*
The generator matrix of this code is

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}_{3\times 6} .$$

Example 3.3.3. *Similarly, at the group ring* $\mathbb{Z}_2(C_7 \rtimes C_2)$, *suppose that* $C_7 =< x >= \{1, x, x^2, ..., x^6\}$, $C_2 =< y >= \{1, y\}$. *And* $C_7 \rtimes C_2$ *has the coding matrices of the form*

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

(As already mentioned in an example 3.2.6).
Consider $u = 1 + x + x^3 \in \mathbb{Z}_2 C_7$ *is a zero-divisor such that*

$$u.v = (1 + x + x^3)\ (1 + x + x^2 + x^4)\ =\ 1 + x + x^2 + x^4 + x + x^2 + x^3 + x^5 + x^3 + x^4 + x^5 + 1\ =\ 0.$$

So, at $\phi_6 : x \longmapsto x^6$ *in this semi-direct product group we have* $(u + uy)(v + v^T y)\ =\ (1 + x + x^3 + (1 + x + x^3)y)\ (1 + x + x^2 + x^4 + (1 + x^6 + x^5 + x^3)y)\ =\ (1 + x + x^3 + y + xy + x^3y)\ (1 + x + x^2 + x^4 + y + x^6y + x^5y + x^3y)\ =\ 1 + x + x^2 + x^4 + y + x^6y + x^5y + x^3y + x + x^2 + x^3 + x^5 + xy + y + x^6y + x^4y + x^3 + x^4 + x^6 + 1 + x^3y + x^2y + xy + x^6y + y + x^6y + x^5y + x^3y + 1 + x + x^2 + x^4 + xy + y + x^6y + x^4y + x + x^2 + x^3 + x^5 + x^3y + x^2y + xy + x^6y + x^3 + x^4 + x^5 + 1\ =\ 0$. *Hence,* $u + uy\ =\ 1 + x + x^3 + y + xy + x^3y$ *is a zero-divisor in* $\mathbb{Z}_2(C_7 \rtimes C_2)$.

Bibliography

[1] A. Alkinani and A. Khammash, Coding matrices for the semi-direct product group, submitted for publication.

[2] G. Chalom, R. Ferraz, M. Guerreiro and C. Milies, Minimal binary abelian codes of length $p^x q^n$, Preprint in arXiv:1205.5699, (2012).

[3] C. Curtis and I. Reiner, *Methods of Representation Theory*, Vol. 2, Willy, New York, 1985.

[4] D. Dummit and R. Foote, *Abstract Algebra*, 3rd Edition, John Wiley & Sons, Hoboken, 2004.

[5] R. Ferraz, M. Guerreiro and C. Milies, G-Equivalence in group algebras and minimal abelian codes, Preprint in arXiv:1203.5742v1, (2012).

[6] M. Hamed, *Constructing Codes from Group Rings*, Msc dissertation, Umm Al-Qura University, Makkah, 2018.

[7] M. Hamed and A. Khammash, Coding matrices for GL (2, q), Fundemental Journal of Mathematics and Applications, 1 (2) (2018) 118-130.

[8] R. Hamming, Error detecting and error correcting codes, The Bell System Technical Journal, 29 (1950) 147-160.

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

[10] D. Hoffman, D. Leonard, C. Linder, K. Phelps, C. Rodger and J. Wall, *Coding Theory : The Essentials*, Marcel Dekker, Inc. , New York, 1992.

[11] P. Hurley and T. Hurley, Codes from zero-divisors and units in group rings, Preprint in arXiv:0710.5893, (2007).

[12] P. Hurley and T. Hurley, Block codes from matrix and group rings, Chapter 5, 159-194, in *Selected Topics in Information and Coding Theory*, Vol. 7, Isaac, Woungang, Misra Sudip, and Misra Subhas Chandra, eds. World Scientific, 2010.

[13] P. Hurley and T. Hurley, Module codes in group rings, IEEE International Symposium on Information Theory, (2007) 1981-1985.

[14] T. Hurley, Group rings and rings of matrices, Int. J. Pure Appl. Math, 31(3) (2006) 319-335.

[15] M. Köroğlu, A Class of constacyclic codes from group algebras, JSTOR, 31 (10) (2017) 2917-2923.

[16] M. Köroğlu, LCD codes and LCP of codes from units of group rings, Sakarya University Journal of Science, 23 (3) (2019) 486-492.

[17] F. MacWilliams, Codes and ideals in group algebra, Combinatorial Mathematics and its Applications, (1969) 317-328.

[18] C. Milies and S. Sehgal, *An Introduction to Group Rings*, Vol. 1, Springer Science & Business Media, London, 2002.

[19] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, 2nd Eddition, John Wiley & Sons, New York, 1989.

[20] V. Pless, *Introduction to The Theory of Error-Correcting Codes*, 3rd Edition, John Wiley & Sons, New York, 1998.

[21] S. Roman, *Coding and Information Theory*, Vol.134, Springer Science & Business Media, New York, 1992.

[22] J. Rose, *A Course on Group Theory*, Cambridge University Press, Cambridge, 1978.

[23] C. Shannon, The mathematical theory of communication, Bell Syst. Tech. J., 27 (1948) 379-423 and 623-656.