Some Error Correcting Codes Related to Finite Groups

Tokaua Tekabu

School of Computing, Information and Mathematical Sciences
Faculty of Science, Technology and Environment
The University of the South Pacific
November 2008

A thesis submitted in the partial fulfillment of the requirements of the degree of Master of Science

Declaration of Originality

I hereby declare that the work presented in this thesis is, to the best of my knowledge and belief, original, except as acknowledged in the text. The material in the thesis has not been submitted previously, either in whole or part, for a degree at this or any other institution.

.....

Tokaua. Tekabu

November, 2008

Dedication

This thesis is dedicated to the memory of my father Mr. Tekabu Beniaata. I can only wish that he is here to see this achievement.

Acknowledgement

I would like to take this opportunity to thank all those who contributed to the successful completion of this thesis.

My profound thanks go to my supervisor, Dr Valeriy Mnukhin, of the Department of Mathematics and Computing at the University of the South Pacific, for introducing me to this special topic, Coding Theory. I would like to express my deeply felt appreciation for his valuable suggestions, motivations and counselling in every phase of this arduous but meritorious task.

My sincere gratitude goes to AUSAID and Faculty of Science Research Committee for providing financial support towards my study.

Special thanks are also due to Mr and Mrs Ientaake Karakaua's family for providing care, support and motivation whenever is needed. I also wish to thank friends and colleagues for their words of advice. Lastly, my heartful thanks goes to my husband for his contributions and sacrifices which are beyond words. And to my beautiful girls, Maria, Marewe and Arame for being tirelessly waited for me late at nights, this thesis is a gift to you all.

Abstract

Error correcting codes related to finite groups are codes associated with the null space of an incidence matrix $V_k(\mathcal{L}(G))$ of lattices of subgroups of some finite groups G. We call such codes *Combinatorial codes*. The finite groups we are considering are of the following form:

- Cyclic groups $\mathbb{Z}_n$ where n is any square-free integer, that is any integer of the form $p_1 p_2 \dots p_n$, where $p_1, p_2, \dots, p_n$ are different primes.
- Cyclic groups $\mathbb{Z}_n$ where $n = s^t$, where s is any square free primes and $t > 1$ is integer.
- Some non-cyclic Abelian groups in the form $G = \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n}$, where p is prime.

We investigate properties of such codes, namely lengths, dimensions, ranks, weight distributions and minimum distances over finite fields $GF(p)$, where $p = 2, 3$ and 5. We obtain such properties by constructing the weight enumerator of the codes, using the assistance of GAP and GUAVA computer packages.

We extend Lefmann's theorem, as well as Mnukhin and Siemons findings on the minimum distance of codes related to Boolean lattices for small characteristics, $0 < p < n$. We also present tables of ranks over $GF(p)$ of the mysterious matrices in Hamanda's formula (incidence matrices of lattices of n-dimensional subspace over $GF(q)$) for some cases when $p = q$.

Contents

Chapter 1

Introduction

Coding theory has its origin in communication theory which study methods for efficient and accurate transfer of information from one place to another. Its applications are concerned with situations in which 'coded' messages are transmitted over a so-called 'noisy' channel that has the effect that symbols in 'words' of the message are sometimes changed to other symbols of the 'alphabet'. The system is designed in such a way that the most likely error-patterns (at the receiver end) can be recognized and corrected.

Coding theory was first developed in the 1940s when Claude Shannon published a paper with a central theme of: by using proper encoding of information, errors induced by noisy channels or storage media can be reduced without altering the rate of transmission [31]. Since then research on the development of efficient encoding and decoding methods for error control in a noisy environment has been done. These studies were initiated by Hamming, Golay and others in the late 1940s [18].

To construct a code C, one can use matrices [12, 18]. Namely, any matrix V whose rows form a basis for C is called a *generator matrix* for C. When V is known, one can find all codewords of C. To produce an interesting code with high error-correcting ability the matrix V must be quite special and often occurs to be an incidence matrix of a combinatorial structure [2, 5].

Recent developments have produced interesting results such as the well-known combinatorial structure, called the Fano plane $PG(2,2)$ can produce a famous perfect Hamming codes [2, 13]. The Fano Plane is the smallest example of projective

geometry.

In 1990 L. Tolhuizen and J. van Lint [27] extended a work of Da Rocha who introduced a new class of linear codes over a field F, called *combinatorial codes* $\mathcal{C}_k(n, F)$. These codes are related with incidence matrices of the Boolean algebra $\mathcal{B}(n)$. It is the partially ordered set of all subsets of an n-element set.

In general, incidence matrices of any ranked partially ordered set P produce codes that we continue to call combinatorial codes. The most interesting cases occur when P is a projective geometry or a product of chains. In all these cases P is the lattice of subgroups of an appropriate Abelian group.

The goal of the thesis is to investigate main characteristics of combinatorial codes, namely, their length, dimension, minimum distance and weight distribution. These characteristics strongly depend on the ground field F.

When the field F has characteristic $p = 0$, the minimum distance $d(B_k(n, p))$ of combinatorial codes associated with the Boolean algebra $\mathcal{B}(n)$ follows from a theorem of H. Lefmann [15]:

$$d(B_k(n, p)) = 2^{k+1} \text{ if } 2(k+1) \leq n$$

Similar result for fields of characteristic $p \geq n$ follows from results of Mnukhin and Siemons [23]. However, the case of small characteristics $0 < p < n$ seems to be open.

One of the major aim of this research was to study the minimum distance of van Lint-Tolhuizen codes when $0 < p < n$. My computer experiments show that the result of Lefmann is not always valid for such fields. Based on the results of such experiments, the following conjecture has been produced:

$$d(B_k(n, p)) = \begin{cases} 2^{k+1}, & \text{if } \quad 2(k+1) \leq n \text{ and } p \leq k+2 \ ; \\ \\ \binom{k+p}{p-1}, & \text{if } \quad 2(k+1) > n \text{ and } k+p \leq n. \end{cases}$$

I was able to prove (see Proposition 6.1.11 and Theorem 6.1.15) that $d(B_k(n, p))$ does not exceed the bound stated above, but does not manage to prove the equality. Nevertheless, this conjecture may be considered as the most important result of my thesis.

Furthermore, it is well known [7] that the dimension of a code C is related to the rank of the generator matrix V. Thus, the dimension of van Lint-Tolhuizen combinatorial codes follows from the well-known theorems of Frankl and Wilson [8, 30]. To extend such results there were several studies on the rank of other incidence matrices. One of these was the study of the subspace-inclusion matrices (incidence matrix of lattices of n-dimensional subspace over $GF(q)$) [9], [13], [32]. However these studies only consider ranks of such matrices over fields $GF(p)$ where $p = 0$ [13], p does not divide q [9].

The cases where $p = q$ is very interesting and mysterious. Xiang [32] studied this case but can only show results for special cases.

The second major goal of this research is to find ranks of Xiang's matrices when $p = q$. This mystery was another motivation to study codes related to lattices of n-dimensional subspace over $GF(q)$) when $p = q$.

The organization of my thesis is as follows: Chapters 2, 3 and 4 deal primarily with the introductory and background information. They do not contain any new results. It mainly discussed definitions, theorems on groups, lattices and codes.

In Chapter 5, the background information are related to the content of the thesis. We also discuss the main tools (GAP and GUAVA) used in collecting the data. In here I also elaborate what has been done in the thesis by presenting examples.

Finally Chapter 6 deals with the discussion of the new results of the thesis. We extend Lefmann's theorem, as well as generalize some of the properties of combinatorial codes. It also gives an account of the difficulties faced and suggestions on how we can improve to obtain better results.

Chapter 2

Groups

The term "Groups" was used for basic algebraic model for many types of mathematical objects such as groups of numbers, groups of permutation, matrices and linear transformation. However Group theory became evolved later from three different sources which are: a result of solving algebraic equations by radical; number theory; and geometry [12]. Today groups is recognized in various fields.

The purpose of this chapter is to provide the basic background information that will aid in understanding the discussion of Groups in this thesis.

2.1 Groups

A group is one of the main types of algebraic system, a set with operations defined on it. The main operation used is defined below.

Definition 2.1.1 Let S be a non empty set of elements. A *binary operation* $*$ on S is a rule that assigns to each pair of elements a and b in S a third element $c = a * b$ in S. When such a binary operation $*$ is defined on S, we say that S is closed under $*$.

Example 2.1.2 Let S be the set of all integers $\mathbb{Z}$. An addition, $+$, is a binary operation on S as for any two integers i and j in S, $i + j$ is an integer in S. Similarly, the subtraction, $(-)$ and multiplication, $(\times)$, are also binary operations

on S. A division, $(\div)$, operation on the other hand is not a binary operation on S because for some integers a and b, $\frac{a}{b}$ is not in S

Now let us now formally define a group.

Definition 2.1.3 A *group* $(G, *)$ is a non empty set G, together with a binary operation $*$ which satisfies the following properties:

G1: for all elements g and h of G, $g*h$ is an element of G (closure property).

G2: for all elements, g, h and k of G, $(g*h)*k = g*(h*k)$ (associativity property).

G3: there exists an element e of G, called the identity (or unit) of G, such that for all g in G we have $e*g = g*e = g$ (identity property).

G4: for every g in G there exist an element g^{-1} called the inverse of g, such that $g*g^{-1} = g^{-1}*g = e$ (inverse property).

Let us now consider some examples of groups.

Example 2.1.4 The set $\mathbb{Z}$ with an addition operation $+$ defined in Example 2.1.2 is a group. It satisfies the four axioms under the operation $+$. The integer 0 is the identity element since for any element x in $\mathbb{Z}$, $x + 0 = 0 + x = 0$. For every element x in $\mathbb{Z}$ there exist an inverse which is the negative $-x$ as $x + (-x) = (-x) + x = 0$. As we all know addition of integers are associative and the addition of two integer is also an integer so $(\mathbb{Z}, +)$ is a group.

Example 2.1.5 Let G be the set $\mathbb{N}$ of natural numbers and the operation $+$ be addition of numbers. Then $(\mathbb{N}, +)$ is not a group. Not all elements of $\mathbb{N}$ have additive inverses within the set $\mathbb{N}$, for example 2 inverse is -2, but -2 is not in $\mathbb{N}$.

Let us now consider this interesting and important example extracted from [16].

Example 2.1.6 Let m be the positive integer. Consider the set of integers $G = \{0, 1, 2, \cdots, m-1\}$. Let $+$ denote real addition. Let $+_m$, (addition modulo-m), be a binary operation on G defined as follows: For any integers i and j in G,

$$i +_m j = r,$$

where r is the remainder of $i+j$ when divided by m.

The set $G = \{0, 1, 2, \cdots, m-1\}$ is a group under addition modulo-m.

To prove this we need to show that the four axioms above, (G1), (G2), (G3) and (G4) are all satisfied. The remainder r is an integer between 0 and $m-1$ and is therefore in G so (G1) is satisfied. Obviously 0 is the identity element implies (G3) holds. Since

$$i + (m - i) = (m - i) + i = m$$

then by the definition of addition modulo-m

$$i +_m (m - i) = (m - i) +_m i = 0$$

therefore, i and $m-i$ are inverses of each other with respect to $+_m$. It is also clear that the inverse of 0 is itself. This implies that (G4) holds.

Now let show that (G2) also holds. Let i, j, k be in G. Since real addition is associative, we have

$$i + j + k = (i + j) + k = i + (j + k).$$

Dividing $i+j+k$ by m, we obtain

$$i + j + k = qm + r,$$

where q and r are the quotient and the remainder, respectively, and $0 \leq r < m$. Now dividing $i+j$ by m, we obtain

$$i + j = q_1 m + r_1 \tag{2.1}$$

with $0 \leq r_1 < m$. Therefore, $i +_m j = r_1$. Dividing $r_1 + k$ by m, we have

$$r_1 + k = q_2 m + r_2 \tag{2.2}$$

with $0 \leq r_2 < m$. Hence, $r_1 +_m k = r_2$, and

$$(i +_m j) +_m k = r_2.$$

Combining (2.1) and (2.2), we have

$$i + j + k = (q_1 + q_2)m + r_2.$$

This implies that r_2 is also the remainder when $i+j+k$ is divided by m. Because the remainder resulting from dividing an integer by another integer is unique, we must have $r_2 = r$. As a result, we have

$$(i +_m j) +_m k = r.$$

Similarly, we can show that

$$i +_m (j +_m k) = r.$$

Since $(i +_m j) +_m k = i +_m (j +_m k)$ then addition modulo-m is associative, thus (G2) holds. This concludes that $G = \{0, 1, 2, \cdots, m-1\}$ is a group.

Beside that $G = \{0, 1, 2, \cdots, m-1\}$ is an Abelian Group since real addition is commutative, hence from the definition of modulo-m addition, it is also commutative. In other words for any i and j in G, $i +_m j = j +_m i$

In fact a set of n positive integers together with the binary operation of *addition modulo* n as in the example above 2.1.6, forms the cyclic group of order n, denoted by $\mathbb{Z}_n$.

A group G could be defined in a table. Such tables enable us to see the effect of an operation $*$ on a set G. The table has the elements of the set G in some definite order as a heading row, and the elements, in the same order, as a leading column. We should note that each element of the group must appear only once in each row and column of the table. The entry at the intersection of the row i and column j is $i * j$.

It is possible to tell from the table whether or not G is Abelian. It is Abelian if the group table is symmetric about its main diagonal.

Example 2.1.7 For example, let G be a group $(\{a, b, c, d\}, \bullet)$. G could then be defined as:

•	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

From this table, we can say that the group G is Abelian since it is symmetric about its main diagonal.

Some groups when defined can be structurally alike to other groups even when their elements and operations are different. For instance consider the two group tables below:

$\bullet$	id	(12)(34)	(13)(24)	(14)(23)
id	id	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	(13)(24)	(14)(23)	id
(13)(24)	(13)(24)	(14)(23)	id	(12)(34)
(14)(23)	(14)(23)	id	(12)(34)	(13)(24)

$*$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The two tables are in fact could become the same if we replace $(\bullet)$ by $*$, id by 0, (12)(34) by 1, (13)(24) by 2, (14)(23) by 3, that is the first table will becoming the second table.

When two groups have this property then they are called *isomorphic* and could be considered the same.

Definition 2.1.8 Let G and H be groups. G and H are *isomorphic*, denoted as $G \backsimeq H$, if the following are satisfied:

1. a mapping from G to H, $\theta : G \longrightarrow H$, is bijection, that is a one to one and onto function,
2. for all $x, y \in G$ we have $\theta(xy) = \theta(x)\theta(y)$.

Finite Groups

Definition 2.1.9 A group G is said to be *finite* if the number of elements in the set G is finite, otherwise the group is *infinite*. Such number is called the *order* of the group G which is usually denoted by $|G|$.

There is only one group of order one. It is an identity group. It has only one element which is an identity element.

There exists groups with any finite order n such as follows:

There is only one group, of order two $G = \{e, a\}$ and of order three $G = \{e, a, b\}$ up to isomorphism. The first can be denoted as $\mathbb{Z}_2$ and represented in the table below.

$*$	e	a
e	e	a
a	a	e

The latter group has the table below and is denoted by $\mathbb{Z}_3$.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

For some finite order n, there are more than one non-isomorphic groups. For instance, for the order 4, there are exactly two non-isomorphic groups as shown below:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

and

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The first table corresponds to the *cyclic group*, $\mathbb{Z}_4$, while the second defines the *Klein 4-group* V which is constructed by $\mathbb{Z}_2 \times \mathbb{Z}_2$.

The next table (adapted from [28]) give names and numbers of the first finite groups up to isomorphism of different orders up to 15. (N_A stand for number of Abelian groups, N_{NA} stands for number of non-Abelian groups and N means total number of non-isomorphic groups).

Order	Names	N_A	N_{NA}	N
1	$< e >$	1	0	1
2	$\mathbb{Z}_2$	1	0	1
3	$\mathbb{Z}_3$	1	0	1
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$	2	0	2
5	$\mathbb{Z}_5$	1	0	1
6	$\mathbb{Z}_6$, D_3	1	1	2
7	$\mathbb{Z}_7$	1	0	1
8	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_8$, Q_8, D_4	3	2	5
9	$\mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_9$	2	0	2
10	$\mathbb{Z}_{10}$, D_5	1	1	2
11	$\mathbb{Z}_{11}$	1	0	1
12	$\mathbb{Z}_2 \times \mathbb{Z}_6$, $\mathbb{Z}_{12}$,A_4, D_6, T	2	3	5
13	$\mathbb{Z}_{13}$	1	0	1
14	$\mathbb{Z}_{14}$, D_7	1	1	2
15	$\mathbb{Z}_{15}$	1	0	1

Weisstein [28] shows that there is at least one Abelian group for every finite order while for some orders non-abelian groups do not exist.

Subgroups

In a group there could be other smaller groups which are called subgroups.

Definition 2.1.10 Let G be a group. H is a *subgroup* of G denoted $H \subset G$ if H is a non empty subset of G and H is itself a group under the same operation as that of G.

Every group G contains at least 2 subgroups: the *trivial* subgroup which contain just the identity element, $\{e\} \subset G$ and the *improper* subgroup, $G \subset G$, the subgroup consists of G itself. All other subgroups are called *proper* or *non-trivial*.

Every group whose order is a composite number contains a proper subgroup while a group with a prime order contains no proper subgroup [12]

In order to check whether or not H is a subgroup of a group G, one needs to check that H satisfies the four group axioms which gives a long process, however a theorem below which was proven in Humphreys and Prest [12] give a shorter method.

Theorem 2.1.11 *A nonempty subset H of a group G is a subgroup of G if and only if the following are satisfied:*

- *H is closed under the binary operation of G.*
- *the identity element e of G is in H, $e \in H$.*
- *for all $a \in H$ also $a^{-1} \in H$, in other words the inverse of any element of H lies in H and it just its inverse in G.*

Given below are examples of subgroups.

Example 2.1.12 We have seen in Example 2.1.4 that $\mathbb{Z}$ is a group under the addition operation $+$. Consider the subset of $\mathbb{Z}$ which is the set of even integers H. Every element a of H is in the form $\{a \in H : a = 2b, b \in \mathbb{Z}\}$. This subset H is in fact a subgroup of $\mathbb{Z}$ due to the facts that the addition of two even integers is an even integer, the identity element of integers, $\mathbb{Z}$ is 0 and is also an identity element of H. We should note that 0 is an even integer since $0 = 2 \times 0$. For any $\{a \in H : a = 2b, b \in \mathbb{Z}\}$ then the inverse of a is $-a = -2b, b \in Zn$ which is also an even integer.

Example 2.1.13 Let V be a group Klein 4-group V. As shown before in the V group table it has four elements which are {e, a, b, c}. Let H be the subset of V which is a set of {e, a}. The group table for H is given below.

$*$	e	a
e	e	a
a	a	e

From this table we should note that H is closed under the binary operation of V. The identity element e of V is in H and for all $a \in H$ also $a^{-1} \in H$, that is e^{-1} is e, a^{-1} is a which all lie in H and it just its inverse in G. Thus $H \subset V$. Similarly we can show that the sets {e, b}, and {e, c} are also subgroups of V.

One of the properties of a subgroup is given by the Lagrange theorem.

Theorem 2.1.14 (Lagrange Theorem) *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.*

Example 2.1.15 In Example 2.1.13, the V-Klein group has order 4 and the subgroup H has order 2. So $|H|$ divides $|V|$.

Subgroups of a group could be generated by its element as the following shows.

Definition 2.1.16 Let g be an element of a group G. The set $\langle g\rangle = \{g^n : n \in Z_n\}$ of all distinct powers of g is a subgroup known as the *cyclic subgroup generated by* g. It has n elements if g has order n and infinite if g has infinite order.

Example 2.1.17 Let G be the group $(Z_{12}, +_{12})$. Elements of G are {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}. $\langle 2\rangle = \{2, 2^2, 2^3, \ldots\}$. From this we noticed that $\langle 2\rangle = \{2, 2\cdot 2, 2\cdot 3, 2\cdot 4, 2\cdot 5, 2\cdot 6 = 0\}$. Thus $\langle 2\rangle$ is a cyclic subgroup generated by 2. It has 6 elements implies it is a finite subgroup.

Similarly we could find the other subgroups of G which are: $\langle 0\rangle = \{0\} = Z_1$, $\langle 6\rangle = \{0, 6\} = Z_2$, $\langle 4\rangle = \langle 8\rangle = \{0, 4, 8\} = Z_3$, $\langle 3\rangle = \langle 9\rangle = \{0, 3, 6, 9\} = Z_4$, $\langle 2\rangle = \langle 10\rangle = \{0, 2, 4, 6, 8, 10\} = Z_6$, $\langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle 11\rangle = \{0, 1, 2, \ldots, 11\} = Z_{12}$.

The theorem of Lagrange states that if H is a subgroup of a group G, then $|H|$ divides $|G|$. Would it be possible to converse this theorem? In other words If G is a group of order n, and m divides n, is there always a subgroup of order m?

In general, the answer is no for instance, the order of the alternating group A_4 is 12 but has no subgroup of order 6. However on the other hand the answer is yes for some classes of groups in particular the Abelian group.

2.2 Abelian Groups

Definition 2.2.1 An Abelian group, also known as a commutative group, is a group $(G, *)$ such that $a * b = b * a$, for all $a, b \in G$.

Abelian groups are named after the founder Niels Henrik Abel. Such groups have two main notational conventions, addition and multiplication. In this thesis we study Abelian groups with the additive notation, that is if G is an Abelian group, then the identity in this convention is an element 0 and the inverse is $-x$ for all $x \in G$.

Groups in Examples 2.1.4, 2.1.6 are Abelian groups since the binary operations they are using are commutative.

In here we will focus on properties and construction of such groups.

2.2.1 Cyclic Groups

There are many types of Abelian groups, one of these is a cyclic group as mentioned in Example 2.1.6. Let us now formally define a cyclic group.

Definition 2.2.2 A group G is called *cyclic* if there exists an element g in G such that $G = \langle g \rangle = \{g^n\}$ for all integers n.

For instance, in the example above, Example 2.1.17, we can say that $(Z_{12}, +_{12})$ is a cyclic group with generators 1, 5, 7, and 11. Thus a cyclic group could have more than one generator.

Definition 2.2.3 Two positive integers m and n are relatively prime if $gcd(m, n) = 1$, or equivalently, if m and n have no common prime factors.

Corollary 2.2.4 *If a is a generator of a finite cyclic group G of order n, then the other generators of G are the elements of the form a^r, where r is relatively prime to n.*

Cyclic groups for every order, finite or infinite do exist. Every finite cyclic group is isomorphic to the group $G = \{0, 1, 2, \cdots, n-1\}$ under addition modulo n denoted

$\mathbb{Z}_n$ (see Example 2.1.6) and any infinite cyclic group is isomorphic to $\mathbb{Z}$ (the set of all integers) under addition (see Example 2.1.4). Next is the well known [12] results in cyclic groups.

Theorem 2.2.5 *If G is a cyclic group of order n then every subgroup of G is cyclic.*

It is important to note that a cyclic group contains all cyclic subgroups generated by each of the elements in the group. However a group constructed from cyclic subgroups is itself not necessarily a cyclic group. For instance a Klein V group is not cyclic even though it is constructed from two copies of the cyclic group of order 2.

All groups with prime order are cyclic.

2.2.2 Structure of Finite Generated Abelian Groups

Definition 2.2.6 Let $(G, *)$ and $(H, \bullet)$ be groups. The *direct product* of the groups G and H denoted $G \times H$ is a group such that the operation $(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \bullet h_2)$ holds.

Any finite Abelian groups can be developed from other finite Abelian groups. In particular cyclic groups are used as building blocks together with a direct product to form more Abelian groups.

Example 2.2.7 Let consider the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$. As previously mentioned $\mathbb{Z}_2$ and $\mathbb{Z}_3$ have tables respectively

$*$	0	1
0	0	1
1	1	0

and

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

So $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

Since $\langle (1,1) \rangle = \{2(1,1), 3(1,1), 4(1,1), 5(1,1)\} = \{(1,1), (1+_2 1, 1+_3 1) = (0,2), (0+_2 1, 2+_3 1) = (1,0), (1+_2 1, 0+_3 1) = (0,1), (0+_2 1, 1+_3 1) = (1,2)\}$ then $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle \backsimeq \mathbb{Z}_6$.

Note that $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ are all Abelian Groups. Thus we have the following corollary which is also mentioned in [19]

Corollary 2.2.8 *The direct product of two Abelian groups is also Abelian.*

Example 2.2.9 $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$ We should note that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$. If $\mathbb{Z}_2 \times \mathbb{Z}_2 \backsimeq \mathbb{Z}_4$ then either $\langle(0,1)\rangle$ or $\langle(1,0)\rangle$ or $\langle(1,1)\rangle$ will be equal to $\mathbb{Z}_2 \times \mathbb{Z}_2$. But $\langle(1,0)\rangle = \{(1,0),(0,0)\} \backsimeq \mathbb{Z}_2$ and $\langle(0,1)\rangle = \{(0,1),(0,0)\} \backsimeq \mathbb{Z}_2$ and $\langle(1,1)\rangle = \{(1,1),(0,0)\} \backsimeq \mathbb{Z}_2$. So each elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2 hence cannot generate $\mathbb{Z}_2 \times \mathbb{Z}_2$ of order 4. Therefore $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic nor isomorphic to $\mathbb{Z}_4$.

Thus we have the following corollary which is also stated in [19]

Corollary 2.2.10 $\mathbb{Z}_n \times \mathbb{Z}_n$ *is not isomorphic to* $\mathbb{Z}_{n^2}$

Theorem 2.2.11 *The group* $\mathbb{Z}_m \times \mathbb{Z}_n$ *is isomorphic to* $\mathbb{Z}_{mn}$ *if and only if* m, n *are relatively prime or* $gcd(m,n) = 1$.

$$\mathbb{Z}_m \times \mathbb{Z}_n \backsimeq \mathbb{Z}_{mn} \Leftrightarrow gcd(m,n) = 1$$

Theorem 2.2.12 (The Fundamental Theorem of Finite Abelian Groups) *Let* G *be a finite Abelian group. Then* G *is isomorphic to the direct product of cyclic groups in the form*

$$G \backsimeq \mathbb{Z}_{p_1^{n1}} \times \mathbb{Z}_{p_2^{n2}} \times \cdots \times \mathbb{Z}_{p_r^{nr}},$$

where p_i *are primes, not necessarily distinct.*

The direct product is unique except for possible rearrangement of the factors.

Example 2.2.13 All Abelian groups of order 16 can be constructed as follows: Since

$$16 = 2^2 \times 2^2 = 2 \times 2^3 = 2 \times 2 \times 2^2 = 2 \times 2 \times 2 \times 2,$$

so there are 5 non-isomorphic Abelian groups of order 16 which are

$$\mathbb{Z}_{16}, \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}, \mathbb{Z}_2 \times \mathbb{Z}_{2^3}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^2}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Corollary 2.2.14 *The number of Abelian Groups of a primary order p^n is equal to the number of ways to write n as a sum of natural numbers, not necessarily distinct.*

Definition 2.2.15 An Abelian group $(G, *)$ is called *finitely generated* if there exists finitely many elements $g_1, \ldots, g_s$ in G such that every g in G can be written in the form

$$g = n_1 g_1 \times n_2 g_2 \times \cdots \times n_s g_s$$

with integers $n_1, \ldots, n_s$. In this case, we say that the set $\{g_1, \ldots, g_s\}$ is a *generating set* of G.

For example the integers under the addition, $(\mathbb{Z}, +)$ is a finitely generated abelian group. Similarly the integers modulo n, $\mathbb{Z}_n$ is a finitely generated Abelian group. Any direct product of finitely generated abelian groups is again finitely generated Abelian.

The following important known results [29] will be used in the thesis to find the subgroups of Abelian groups.

Theorem 2.2.16 (The Fundametal Theorem of Finitely Generated Groups.) *If G is a finitely generated Abelian group, then there are unique integers $n \geqslant 0$, $n_1, n_2, \ldots, n_k \geqslant 2$ where $n_{i+1} | n_i$ for $i = 1, 2, \ldots, k-1$ such that*

$$G \backsimeq \mathbb{Z}^n \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

where $\mathbb{Z}^n$ is a finite Abelian group.

Theorem 2.2.17 (The Inverse Lagrange Theorem for Abelian Groups) *If G is an Abelian group of order $|G| = n$, and m divides n, then there is a subgroup $H \leq G$ of order m.*

Theorem 2.2.18 *Every cyclic group G is Abelian.*

Proof. If x and y are in G then $xy = a^m a^n = a^{mn} = a^{nm} = a^n a^m = yx$

The theorem then implies that the converse of Lagrange theorem is also true for cyclic groups.

Corollary 2.2.19 (The Inverse Lagrange Theorem for Cyclic Groups) *Let G be a cyclic group of order n, $G = \mathbb{Z}_n$, and k be a positive divisor of n, then group G has exactly one subgroup of order k.*

Example 2.2.20 $\mathbb{Z}_{18}$ has 6 subgroups. Since 18 has 6 divisors which are 18,9,6,3,2,1 so there are 6 subgroups and these are $\mathbb{Z}_{18}, \mathbb{Z}_9, \mathbb{Z}_6, \mathbb{Z}_3, \mathbb{Z}_2$ and $\mathbb{Z}_1$.

The non-trivial proper subgroups are $\mathbb{Z}_9, \mathbb{Z}_6, \mathbb{Z}_3, \mathbb{Z}_2$. $\mathbb{Z}_{18}$ is an improper subgroup and $\mathbb{Z}_1$ is a trivial subgroup.

Chapter 3

Posets and Lattices

Lattices offer a natural way to formalize and study the ordering of objects using a general concept known as a POSET (partially ordered set). The study of lattices is called Lattice theory. It is an outgrowth of the study of Boolean Algebra and it provides a framework for unifying the study of classes or ordered sets in Mathematics.

In this chapter we will discuss the basic ideas on Posets and Lattices. We will cover posets, then lattices, and last but not the least are examples of lattices which are mainly studied in this thesis.

3.1 Posets

Let us begin by giving basic definitions. All sets discussed in this chapter will be assumed finite unless stated.

Definition 3.1.1 Let X and Y be non empty finite sets. A *binary relation* from X to Y is a set R of ordered pairs where the first element comes from the set X and the second element comes from the set Y. If xRy then it means that $x \in X$ is related to $y \in Y$ by R.

Definition 3.1.2 *A partial ordering* R on a finite set X is a binary relation that has the following properties:

1. reflexive: for all $x \in X$ xRx;

2. antisymmetric: for all $x, y \in X$, if xRy and yRx, then $x = y$;

3. transtive: for all $x, y, z \in X$, if xRy and yRz, then xRz.

Example 3.1.3 It is easy to check that the relation $(\backslash)$ of divisibility is a partial ordering.

For a partial ordering R it is common to write $x \geq y$ instead of xRy. The word "partial" in this case means that there may be elements $a, b \in X$ such that neither $a \leq b$ nor $b \leq a$. Then we are saying that a and b are *incomparable*. We also write $a < b$ to denote that $a \leq b$ but $a \neq b$.

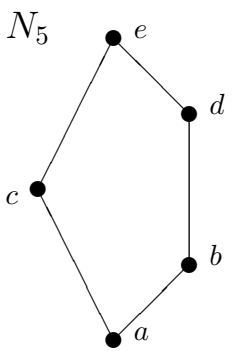
Now let formally defined poset.

Definition 3.1.4 A *partially ordered set* (or Poset) is an ordered pair $P = (X, \leq)$, consisting of a finite set X, together with a partial ordering $\leq$ on X.

Writing $x \in P$ means that $x \in X$. Let $a, b \in P$. If $a < b$ and there is no $c \in P$ such that $a < c < b$ then b *covers* a, denoted as $a \prec b$.

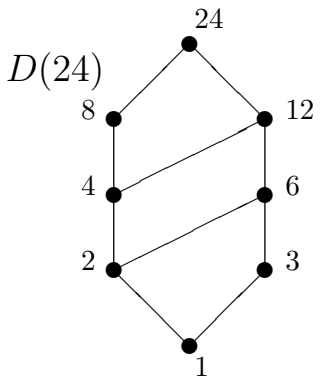
Any Poset P is often represented by the *Hasse diagram*. It is a graphical rendering of a Poset displayed via the relation $\leq$ of P. It is usually drawn in such a way that, each element in P is represented as a small black dot and if $y \in P$ covers $x \in P$, then the dot representing y is drawn higher than the dot representing x. The line segment is drawn between the points x and y if and only if $x \leq y$

Example 3.1.5 The Hasse diagram of poset $N_5 = (\{a, b, c, d, e\}, <)$ where $a < b$, $a < c$, $a < d$, $a < e$, $b < d$, $b < e$, $c < e$ and $d < e$ is given below.

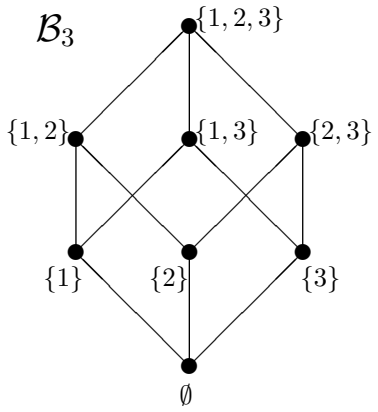


Given below are a few more examples of posets.

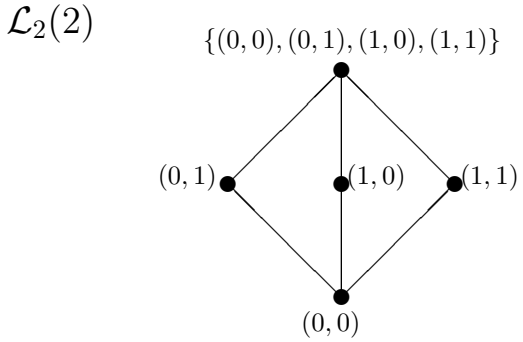
Example 3.1.6 Let $n > 1$ be an integer. The set $D(n)$ of divisors of n forms a poset $(\{1, 2, \ldots, n\}, \backslash)$. For instance, $D(24)$ is a poset with the given Hasse diagram.



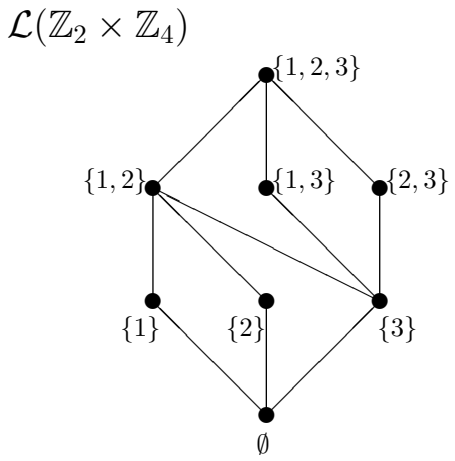
Example 3.1.7 Let S be a finite n-element set and let $P = 2^S$ be all subsets of S. Consider the partial order on P given by set inclusion: if $a, b \in S$ then $a \leq b \leftrightarrow a$ is a subset of b. The poset $\mathcal{B}_n = (2^S, \leq)$ is called the *Boolean poset*. For instance the Boolean poset $\mathcal{B}_3$ is shown below:



Example 3.1.8 Let $V_n(q)$ be the n-dimensional vector space over a finite field $GF(q)$, ($q = p^m$, p is prime). Let P consists of all subspaces of $V_n(q)$. The natural ordering on P is inclusion and the poset $(P, \subseteq)$ will be denoted by $\mathcal{L}_n(p)$. It is the *projective space of dimension* $n - 1$ over $GF(q)$ and is sometimes also called the *Gaussian poset*. The diagram of $\mathcal{L}_2(2)$ for instance is shown below:



Example 3.1.9 Let G be a finite group and $\mathcal{L}(G)$ be the set of all its subgroups ordered by inclusion. $\mathcal{L}(G)$ is indeed a poset. The diagram of the subgroup poset $\mathcal{L}(\mathbb{Z}_2 \times \mathbb{Z}_4)$ for the Abelian group $\mathbb{Z}_2 \times \mathbb{Z}_4$ (where $\mathbb{Z}_n$ is the cyclic group of order n) is shown below:



3.2 Ranked Posets and their incidence matrices

Let us now consider ranked posets. We begin with some basic properties of posets.

Definition 3.2.1 An element 0 of a poset P is said to be *minimal* if $0 \leq a$ for all $a \in P$. An element 1 is said to be *maximal* if $a \leq 1$ for all $a \in P$.

All posets in the previous examples have both maximal and minimal elements. In a general poset there may be no maximal element, or there may be more than one. But in a finite poset there is always at least one maximal element and minimal element.

Definition 3.2.2 An element x in a poset (P) is said to be a *lower bound* of a subset $F \subseteq P$, if $(\forall y \in F)\ \ x \leq y$; and an *upper bound* of F if $(\forall y \in F)\ \ y \leq x$.

Definition 3.2.3 A *least upper bound* denoted *lub* for a subset F of a poset P is an upper bound x such that if c is any other upper bound for F then $c \geq x$ or $x \leq c$; A *greatest lower bound* denoted *glb* for F is a lower bound x such that if c is any other lower bound for F then $c \leq x$.

Definition 3.2.4 Let $a_0, a_1, \ldots, a_k$ be the sequence of elements of a poset P. We shall say that it is a *chain* in P if $a_0 \prec a_1 \prec \cdots \prec a_k$. The number k is called the *length* of the chain denoted as $h(P)$.

Chains are just "upward" paths in the Hasse diagram of P.

Definition 3.2.5 An *anti-chain* in a poset P is a subset A of P such that any two elements of A are incomparable. The cardinality of the maximal anti-chain in P will be called the *width* of P denoted as $w(P)$.

We should note that there are no lines between the elements of an anti-chain in the Hasse diagram of P.

We will now describe a ranked poset.

Definition 3.2.6 Let P be a finite poset with minimal element 0. P is *ranked* (or *graded*) if for every $a \in P$, all chains between 0 and a have the same length. This length will be called the *rank* of the element a and denoted as $|a|$. (Note that $|0| = 0$.) The maximal rank of elements from P is named the *rank of poset P and denoted as $r(P)$*.

Let P be graded with $r(P) = n$ and $P_k = \{a \in P : |a| = k\}$. The set P_k is called the k-th level of P. Evidently then $P = P_0 \cup P_1 \cup \ldots P_n$ where $P_i \cap P_j = \emptyset, i \neq j$. Moreover:

1. all elements of P_k are non-comparable for all $k, 0 \leq k \leq n$, and
2. if $a \in P_k$ and $a \prec b$ then $b \in P_{k+1}$.

Thus points in the diagram of a graded poset P can be placed into $(n+1)$ levels such that there are lines between two neighboring levels only.

Example 3.2.7 The posets in Examples 3.1.7, 3.1.8, 3.1.9 are graded, however the poset in Example 3.1.5 is not graded.

Let P be a ranked poset ordered by $\leq$. Given two ranks (or levels) of P, k and l, where $k < l$, we can form an *incidence matrix* A_{kl}. It is a 0,1 matrix with columns indexed by the elements of level k and the rows indexed by the elements of level l. Let $P_l = \{l_1, l_2, \ldots, l_v\}$ and $P_k = \{k_1, k_2, \ldots, k_b\}$, then A_{kl} is a $b \times v$ matrix and $A_{kl} = (a_{ij})$ such that

$$a_{ij} = \begin{cases} 1 & \text{if } k_i \leq l_j \text{ for } i \leq v \text{ and } j \leq b\ ; \\ 0 & \text{otherwise.} \end{cases}$$

Example 3.2.8 An incidence matrix V_{23} which is constructed from the 2nd and 3rd levels of $\mathcal{B}_3$ in Example 3.1.7 is shown below:

$$V_2(3) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

3.3 Lattices

Definition 3.3.1 A lattice $\mathcal{L}$ is a poset $(P, \leq)$ with the following properties:

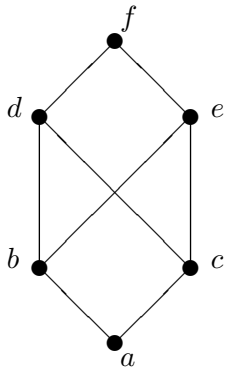
- for any two elements x and y of P, the set $\{x, y\}$ has both a least upper bound $\text{lub}\,(x, y)$ (or mostly known as supremum $\sup(x, y)$), and a greatest lower bound $\text{glb}\,(x, y)$ (or else mostly known as infimum $\inf(x, y)$);
- $\mathcal{L}$ has an upper bound 1 and a lower bound 0.

Example 3.3.2 Every chain is a lattice. In here we have $\inf\{x, y\} = \min\{x, y\}$ and $\sup\{x, y\} = \max\{x, y\}$.

Example 3.3.3 The Boolean posets, subgroup posets and Gaussian posets are a few examples of lattices.

Not all posets are lattices, a simple example of a poset which is not a lattice is given below.

Example 3.3.4



Note that element d and e have more than one minimal element, and b and c have more than one maximal element. Thus the poset is not a lattice.

In this thesis we will mainly concern ourselves with graded lattices. Thus we will deal with the following: Boolean lattices $\mathcal{B}_n$; lattices $\mathcal{F}(n)$ of divisors of an integer n where $n = s^t$, $s = p_1 p_2 \dots p_q$ and $t > 1$ is integer (product of chains) and lattices of subgroups $\mathcal{L}(G)$ of non-cyclic Abelian Groups G.

3.3.1 Boolean lattice

The Boolean poset $\mathcal{B}_n$ discussed in Example 3.1.7 is a Boolean lattice.

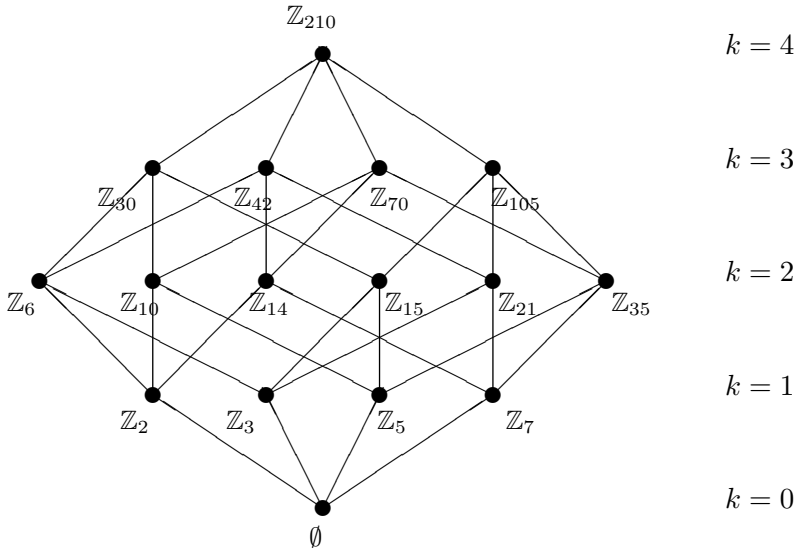
It is known [20] that if s is a square free integer, that is $s = p_1 p_2 \dots p_q$ where p_i is prime and $p_i \neq p_j$, then the lattices of subgroups of a cyclic group $\mathbb{Z}_s$, denoted as $\mathcal{L}(\mathbb{Z}_s)$ is also a Boolean lattice $\mathcal{B}_q$.

The two are isomorphic if $q = n$. So in this thesis when we are talking about *Boolean lattice* we are refereing to lattices of subgroups of cyclic groups of the form $\mathcal{L}(\mathbb{Z}_s) = \mathcal{L}(\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_m})$.

Every finite Boolean algebra have a special structure which is isomorphic to $\{0,1\}^n$ for some positive integer n. Thus the number of element of every finite Boolean

algebra is 2^n. For instance If $\mathcal{B}_4$ is a finite Boolean algebra with 4 atoms, then $\mathcal{B}_4$ has 2^4 elements.

Example 3.3.5 One example of such structure studied is $\mathcal{L}(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7)$. This is isomorphic to $\mathcal{B}_4$. The lattice is given below:



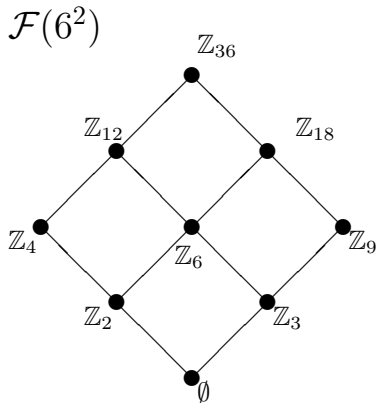
There are five levels in this lattice, $k = 0$, $k = 1$, $k = 2$, $k = 3$ and $k = 4$ as shown, and therefore we can construct incidence matrices V_{01}, V_{12}, V_{23} and V_{34}.

3.3.2 Lattices of divisors of an integer n

For every integer $n \geq 1$, the Boolean lattice $\mathcal{B}_n$ is the direct product of n chains of length 2. By this reason some authors are using the notation $\mathbf{2}^n$ to refer to $\mathcal{B}_n$. Similarly, the direct product of q copies of m-element chain is denoted by $\mathbf{m}^q$.

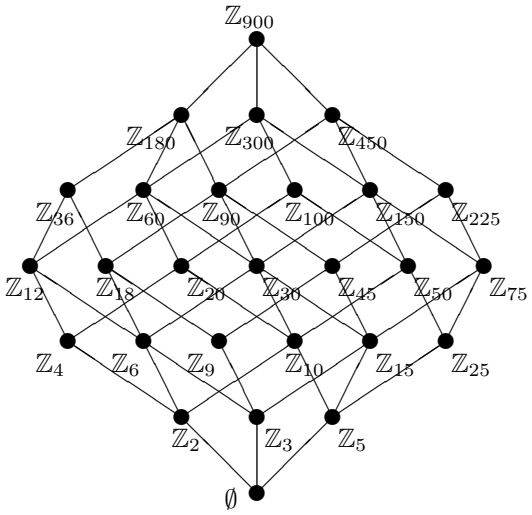
Note that $\mathbf{m}^q$ can also be considered as $\mathcal{F}(s^{m-1})$, the lattice of divisors of the integer n where $n = s^{m-1}$ where s is a square free integer of the form $p_1 p_2 \dots p_q$ and $p_i \neq p_j$. One more way to look at $\mathbf{m}^q$ is to consider it as the lattice of subgroups of the cyclic group $\mathbb{Z}_{s^{m-1}}$.

Example 3.3.6 The lattice $\mathbf{3}^2$, can also be considered as $\mathcal{L}(\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2})$ or $\mathcal{F}(6^2)$, is shown below:



In this thesis we will refer to both $\mathbf{m}^q$ and $\mathcal{F}(s^{m-1})$ as the same lattice.

Example 3.3.7 The lattice $\mathcal{L}(\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{5^2})$ which is a lattice of divisor of $n = 900$ or else known as $\mathbf{3}^3$ is given below:



Similarly we could construct matrices V_k for all levels of these lattices.

3.3.3 Lattices of subgroups of non-cyclic Abelian groups

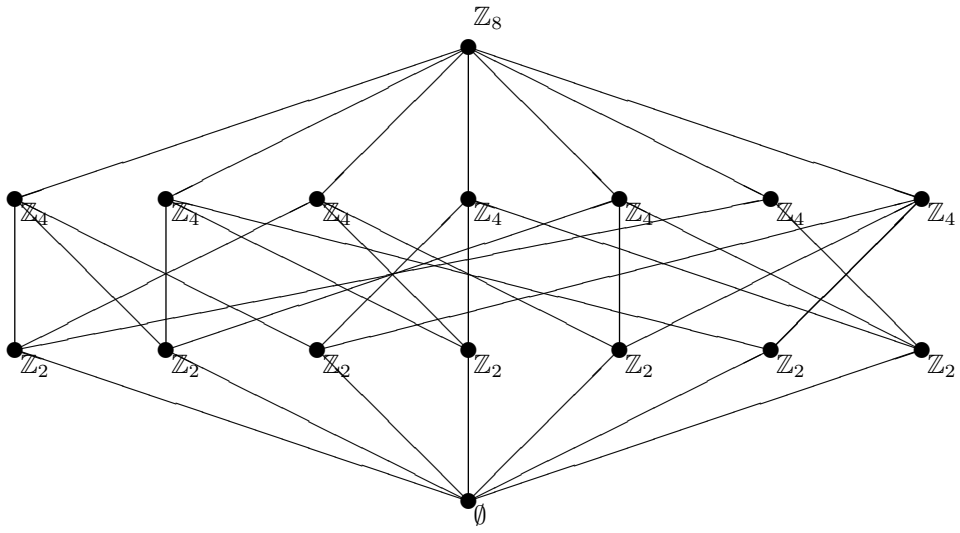
Just like previous lattices, this one is constructed from non-cyclic Abelian groups of the form $(\mathbb{Z}_q)^n$ (q is prime), under the subgroup relation.

We know that if G is an Abelian group, then $\mathcal{L}(G)$ is always ranked so matrices $V_k(\mathcal{L}(G))$ are defined. The previous lattices that were considered were also lattices of subgroups of Abelian groups but they have simpler structure. In here we will consider Abelian groups with more complicated structures. In particular we will

deal with lattices of subgroups of non-cyclic Abelian groups. We will study lattices $\mathcal{L}(G)$ where $G = (\underbrace{\mathbb{Z}_q \times \mathbb{Z}_q \times \ldots \mathbb{Z}_q}_{n}) = (\mathbb{Z}_q)^n$.

It is known [1] that such lattices $\mathcal{L}(\mathbb{Z}_q)^n$ are isomorphic to lattices $\mathcal{L}_n(q)$ of subspaces of n-dimensional vector space over a finite field $GF(q)$. For instance $\mathcal{L}_3(2)$ is isomorphic to $\mathcal{L}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$. We will denote such lattices as $\mathcal{L}(\mathbb{Z}_q^n)$.

Example 3.3.8 The diagram of $\mathcal{L}(\mathbb{Z}_2^3)$ (that is $\mathcal{L}_3(2)$ or $\mathcal{L}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$ is shown below.



All lattices above are graded poset therefore we can form incidence matrices from any two levels.

Chapter 4

Error Correcting Codes

Error Correcting Codes (sometimes refer to as codes) were invented to correct errors over unreliable transmission links. It works by encoding data (adding some redundancy) to the transmission so that the original message can be recovered even if a few errors have occurred. The study of codes is an active area with new and better codes being devised at a steady speed. In this chapter we will discuss the basic ideas in error correcting codes.

Codes are treated as vectors so we will start by introducing some basic definitions and theorems of vector space.

4.1 Vector Space over finite field

Definition 4.1.1 Let $\mathbb{F}$ be a finite field. A nonempty set V, together with two operations, vector addition $+$ and scalar multiplication by elements of $\mathbb{F}$, is a *vector space* over $\mathbb{F}$ if it satisfies all of the following conditions.

For all $u, v, w \in V$ and for all λ and $\mu \in \mathbb{F}$:

1. $u + v \in V$ (Closure under addition);
2. $(u + v) + w = u + (v + w)$ (Associative property of addition);
3. there is an element $0 \in V$ with the property $0 + v = v = v + 0$ (Additive identity);

4. for each $u \in V$ there is an element of V, called $-u$, such that $u + (-u) = 0 = (-u) + u$ (Additive inverse);

5. $u + v = v + u$ (Commutative property of addition);

6. $\lambda v \in V$ (Closure under scalar multiplication);

7. $\lambda(u + v) = \lambda u + \lambda v$ (Distributive property);

8. $(\lambda + \mu)u = \lambda u + \mu u$ (Distributive property);

9. $(\lambda\mu)u = \lambda(\mu u)$ (Associative property);

10. if 1 is the multiplicative identity of $\mathbb{F}$, $1u = u$ (Scalar identity).

Example 4.1.2 Let $\mathbb{F} = \mathbb{F}_q$ be the field of q elements, then it is easy to verify that $W_1 = \{(0,0,0),(0,1,2),(0,2,1)\}$ is a vector space over $\mathbb{F}_3$. Similarly for any q, $W_2 = \mathbb{F}_q^n$, the set of vectors of length n over the field $\mathbb{F}_q$ is also a vector space.

In particular, every vector space must contain at least one element (the zero vector).

Definition 4.1.3 Let C be a nonempty subset of a vector space V. Then C is a *subspace* of V if it is itself a vector space with the same vector addition and vector multiplication as in V.

Example 4.1.4 From the previous example we can say that W_1 is a subspace of $\mathbb{F}_2^3$ and $\{0\}$ is a subspace of W_2.

To verify whether a given subset of a vector space is a subspace or not it is suffice to use the following well known theorem (see [18]).

Theorem 4.1.5 *A nonempty subset C of a vector space V over $\mathbb{F}$ is a subspace if and only if the following conditions are satisfied:*

(i) *if $x, y \in C$, then $x + y \in C$*

(ii) *if $\lambda, \mu \in \mathbb{F}$ then $\lambda x + \mu y \in C$.*

Definition 4.1.6 Let V be a vector space over $\mathbb{F}_q$. A *linear combination* of $v_1, \ldots, v_r \in V$ is the vector of the form $\lambda_1 v_1 + \cdots + \lambda_r v_r$, where $\lambda_1, \ldots, \lambda_r \in \mathbb{F}_q$ are some scalars. A set of vectors $\{v_1, \ldots, v_r\} \in V$ is *linearly independent* if

$$\lambda_1 v_1 + \cdots + \lambda_r v_r = 0 \quad \text{where} \quad \lambda_1 = \cdots = \lambda_r = 0.$$

The set is *linearly dependent* if it is not linearly independent, that is, if there are $\lambda_1, \ldots, \lambda_r \in \mathbb{F}_q$, not all zero (but maybe some are), such that $\lambda_1 v_1 + \cdots + \lambda_r v_r = 0$.

Example 4.1.7 For any $\mathbb{F}_q$, the set $S_1 = \{(0,0,0,1), (0,0,1,0), (0,1,0,0)\}$ is linearly independent while the set $S_2 = \{(0,0,0,1), (1,0,0,0), (1,0,0,1)\}$ is linearly dependent.

Definition 4.1.8 Let V be a vector space over $\mathbb{F}_q$ and let $S = \{v_1, v_2, \ldots, v_k\}$ be a nonempty subset of V. The *span* of S is defined as

$$\langle S \rangle = \lambda_1 v_1 + \cdots + \lambda_k v_k \quad \text{where} \quad \lambda_i \in \mathbb{F}_q.$$

Example 4.1.9 If $q = 2$ and $S = \{0001, 0010, 0100\}$, then $\langle S \rangle = \{$0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111 $\}$. If $q = 3$ and $S = \{$0001, 1000, 1001 $\}$, then $\langle S \rangle = \{$0000, 0001, 0002, 1000, 2000, 1001, 1002, 2001, 2002 $\}$.

Definition 4.1.10 Let V be a vector space over $\mathbb{F}_q$. A nonempty subset $B = \{v_1, v_2, \ldots, v_k\}$ of V is called a *basis* for V if the following are true:

- if $V = \langle B \rangle$.
- B is linearly independent .

This means that if $B = \{v_1, v_2, \ldots, v_k\}$ is a basis of V, then any vector $v \in V$ can be expressed as a unique linear combination of vectors in B, that is there exist unique $\lambda_1, \ldots, \lambda_r \in \mathbb{F}_q$ such that

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k.$$

A vector space V over $\mathbb{F}_q$ can have many bases, but all bases contain the same number of elements. This number is called the *dimension* of V over $\mathbb{F}_q$, denoted by $\dim(V)$.

If a vector space V has a basis consisting of a finite number of vectors, then V is called a *finite dimensional* vector space. Otherwise, V is *infinite dimensional*. The following result is proven in [16].

Theorem 4.1.11 *Let V be a vector space over $\mathbb{F}_q$. If dim(V)=k, then V has q^k elements;*

Example 4.1.12 If $q = 2$ and $S = \{$ 0001, 0010, 0100$\}$ and $V = \langle S \rangle$, then $V = \{$0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111$\}$. Note that S is linearly independent, so $dim(V) = 3$.

Definition 4.1.13 Let $v = (v_1, v_2, \ldots, v_n)$, $w = (w_1, w_2, \ldots, w_n) \in \mathbb{F}_q^n$.

- The *scalar product* (also known as the *dot product*) of v and w is defined as $v.w = v_1w_1 + v_2w_2 + \cdots + v_nw_n \in \mathbb{F}_q$.
- The two vectors v and w are said to be *orthogonal* if $v.w = 0$.
- Let S be a nonempty subset of $\mathbb{F}_q^n$. The *orthogonal complement* $S^\perp$ of S is defined to be $S^\perp = \{v \in \mathbb{F}_q^n : v.s = 0 \text{ for all } s \in S\}$.

Example 4.1.14

(i) Let $q = 2$ and $n = 4$. If $u = (1111)$, $v = (1110)$ and $w = (1001)$, then

$$u.v = 1.1 + 1.1 + 1.1 + 1.0 = 1,$$

$$u.w = 1.1 + 1.0 + 1.0 + 1.1 = 0,$$

$$v.w = 1.1 + 1.0 + 1.0 + 0.1 = 1.$$

Hence, u and w are orthogonal.

(ii) Let $q = 2$ and $S = \{0100, 0101\}$. To find $S^\perp$, let $v = (v_1, v_2, v_3, v_4) \in S^\perp$. Then

$$v.(0, 1, 0, 0) = 0 \Rightarrow v_2 = 0,$$

$$v.(0, 1, 0, 1) = 0 \Rightarrow v_2 + v_4 = 0.$$

Hence, we can have $v_2 = v_4 = 0$. Since v_1 and v_3 can be either 0 or 1, we can conclude that

$$S^\perp = \{0000, 0010, 1000, 1010\}.$$

The next result is well known, the proof is given in [18]

Theorem 4.1.15 *Let S be the subset of $\mathbb{F}_q^n$, then we have*

$$dim(< S >) + dim(S^{\perp}) = n.$$

Example 4.1.16 Let $q = 2$, $n = 4$ and $S = \{0100, 0101\}$. Then $\langle S \rangle = \{0000, 0100, 0001, 0101\}$. Note that S is linearly independent, so $dim(\langle S \rangle) = 2$. We have computed (see Example 4.1.14) that $S^{\perp} = \{0000, 0100, 1000, 1010\}$. Note that $\{0010, 1000\}$ is a basis for $S^{\perp}$, so $dim(S^{\perp}) = 2$. Hence, we have verified that

$$dim(\langle S \rangle) + dim(S^{\perp}) = 2 + 2 = n.$$

4.2 Linear codes

Now let us look at some basic definitions for codes. We will begin with general codes and then we will consider linear codes.

General codes

Definition 4.2.1 Let $A = \{a_1, a_2, \ldots, a_q\}$ be the set of size q, which we refer to as a *code alphabet* and whose elements are called *code symbols.*

Definition 4.2.2 If A is an alphabet, an *A-block* or *A-word* of length n, is the set of all possible sequences, $w = w_1, w_2, \ldots, w_n$ with each $w_i \in A$ for all i, of n symbols from an alphabet A. The set of A-word of length n is denoted by A^n.

Example 4.2.3 Suppose $A = B = \{0,1\}$. Then $B^2 = \{00, 01, 10, 11\}$, $B^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

Definition 4.2.4 A *q-ary code* of length n over A is a nonempty set C of q-ary words having the same length n.

An element of a code C is called a *codeword* in C. The number of codewords in C, denoted by $|C|$, is called the *size* of C and a code of length n and size M is called an (n, M)-code.

As an example, let consider one of the type of codes called a block code. Let A be an alphabet of q elements. When sending a message in block coding across a noisy channel, the information sequence, from the information source is segmented into message blocks denoted by u of fixed length k. If the message symbols are elements of the alphabet A with length k then there are a total of q^k distinct messages. The encoder transforms each of these input message u into an n-tuple v with $n > k$ by adding the redundant information. This n-tuple v is referred to as a codeword of the message u. Therefore there are q^k codewords corresponding to the q^k possible messages. This set of q^k codewords is called a *block code*.

Example 4.2.5 Some examples of codes are: When $q = 2$, $C_1 = \{00, 01, 10, 11\}$ is a (2,4)-code; $C_2 = \{000, 011, 101, 110\}$ is a (3,4)-code.

There exist several types of error correcting codes however we will restrict our attention to an important class of codes, called linear codes.

Linear Codes

Definition 4.2.6 Let $\mathbb{F}_q$ be any finite field and let $V = \mathbb{F}_q^k$ be the k-dimensional vector space over $\mathbb{F}_q$. A code C of length n and q^k codewords is *linear* if C is a subspace of V. C is called an $[n, k]$ *-linear code over* $\mathbb{F}$ (or $[n, k]$ *code*).

Example 4.2.7 Let $C = \{0000, 1100, 2200, 0001, 0002, 1101, 1102, 2201, 2202\}$. Then C is a $[4, 2]$-linear code over $\mathbb{F}_3$.

Definition 4.2.8 A code is linear if the following holds:

- The sum or difference of two codewords is itself a codeword.
- The zero vector is always a codeword.
- The number of codewords in an $[n, k]$ code C of V is q^k.

The number of codewords in C is q^k because there are k vectors in a basis of C. Every codeword is a linear combination of the basis vectors, thus to count the number of codewords, we just have to count the number of linear combinations.

There are q choices for a scalar multiple of each basis vector and therefore q^k linear combinations in total.

Since the number of codewords of a linear code is determined by the dimension of the subspace, the (n, M) notation for general codes is replaced by $[n, k]$ for linear codes.

4.3 Description of Linear Codes by Matrices

A linear code C can be described in two ways; either as a generator matrix or a check matrix. Since the two are matrices, they will satisfy basic properties of matrices. Let us now look at these basic properties.

Matrices

Definition 4.3.1 Let M be an (m, n) matrix. M is an ordered set of mn elements in a rectangular array of m rows and n columns.

$$M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

The elements of a matrix may in general be elements of any ring, however in this thesis only matrices with elements in a field will be applied. The m rows may be thought of as m n-tuples vectors. Similarly the n columns may be thought of as n m-tuples vectors.

Follows are the well known definitions and theorems.

Definition 4.3.2 The *transpose* of any (m, n) matrix M is an (n, m) matrix, denoted $M^\top$, whose rows are the columns of M, and thus whose columns are the rows of M

Definition 4.3.3 Let $\mathbb{F}_q$ be a field with q elements and M be any matrix of size (m, n) over the field $\mathbb{F}_q$. The *column space* of M is the set of all linear combinations of column vectors of M. It forms a *subspace* of the vector space $\mathbb{F}_q^n$.

A vector v is in a column space if the following properties holds.

Let

$$M = \begin{pmatrix} \vdots & \vdots & & \vdots \\ c_1 & c_2 & \dots & c_n \\ \vdots & \vdots & & \vdots \end{pmatrix}$$

and

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

be an n-tuple vector written as a column matrix, then

$$v = Mx = \begin{pmatrix} \vdots & \vdots & & \vdots \\ c_1 & c_2 & \dots & c_n \\ \vdots & \vdots & & \vdots \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

(or $v = x^\top M^\top$.)

Definition 4.3.4 The set of all linear combinations of row vectors of M forms a *row-space* of M. They also form a subspace of the vector space $\mathbb{F}_q^m$.

A vector r is in a row-space of M if the following holds.

Let

$$M = \begin{pmatrix} \vdots & \vdots & & \vdots \\ c_1 & c_2 & \dots & c_n \\ \vdots & \vdots & & \vdots \end{pmatrix}$$

then the transposed matrix of M, denoted $M^\top$ is

$$M^\top = \begin{pmatrix} \vdots & \vdots & & \vdots \\ r_1 & r_2 & \dots & r_m \\ \vdots & \vdots & & \vdots \end{pmatrix},$$

where column vectors becoming row vectors and vice versa. Let

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}$$

be a m-tuple vector written as a column matrix, then the vector r is in a row-space of M if

$$r = M^\top x = \begin{pmatrix} \vdots & \vdots & & \vdots \\ r_1 & r_2 & \dots & r_m \\ \vdots & \vdots & & \vdots \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}$$

(or $r = x^\top M$.)

Definition 4.3.5 Let x be the n-tuple column vector. The set of all solutions $x \in \mathbb{F}_q^n$ of the homogeneous system of linear equations $Mx = 0$ or $x^\top M^\top = 0$ is a subspace of $\mathbb{F}_q^n$ called the *null-space* (or the *kernel* of M).

Definition 4.3.6 The set of all solutions of the homogeneous linear equation $M^\top x = 0$ or $x^\top M = 0$ is a subspace of $\mathbb{F}_q^m$ called the *left null-space* of M.

The *dimension* of the row space is called the *row rank* and the dimension of the column space is called the *column rank*. It is well known that row rank equals column rank, and this value is referred to as the *rank of the matrix*.

There is a set of *elementary row operation* defined for matrices;

1. interchanging of any two rows.
2. multiplication of any row by a nonzero field element.
3. Addition of any multiple of one row to another.

Clearly the inverse of each elementary row operations is an elementary row operation of the same kind.

Theorem 4.3.7 *If one matrix is obtained from another by a succession of elementary row operations both matrices have the same row space.*

Elementary row operation can be used to simplify and put matrices in a standard form or *Reduced row echelon form* (RREF). This form is as follows:

1. every leading term of a nonzero row is 1.
2. every column containing such a leading term has all its other entries zero.
3. the leading term of any row is to the right of the leading term in every preceding row. All zero rows are below all nonzero rows.

Example 4.3.8 Consider the following matrix A, with real entries.

$$A = \begin{pmatrix} 0 & 0 & 2 & 2 & 0 & 2 \\ 2 & 2 & 6 & 8 & 4 & 8 \\ 1 & 1 & 5 & 6 & 2 & 5 \\ 1 & 1 & 3 & 4 & 2 & 7 \end{pmatrix}$$

Matrix A can be simplified and expressed as A', a matrix of Reduced row echelon form by a sequence of elementary row operations. The following matrix is a result.

$$A' = \begin{pmatrix} 1 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The nonzero rows of a matrix in echelon canonical form are linearly independent, thus the rank of matrix A' is 3. Therefore by Theorem 4.3.7, rank of A is also 3.

Now let us consider the two ways of describing codes.

Generator matrix

We can represent a linear code C by its generator matrix G.

Definition 4.3.9 If $g_0, g_1, \ldots, g_{k-1}$ is a basis for an $[n,k]$-linear code C, where $g_i = (g_{i0}, g_{i1}, \ldots, g_{i,n-1})$, then the matrix

$$G = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix},$$

is called a *generator matrix* for C.

Given the matrix G, the code C is obtained by multiplying G on the left by all possible $(1,k)$ row vectors.

Example 4.3.10 The $[7,4]$ code has the following matrix as a generator matrix:

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

The corresponding codeword can be constructed as follows: If the message to be encoded is $(u = u_0, u_1, \ldots, u_{k-1})$, then

$$\begin{aligned} & u \cdot G \\ &= (u_0, u_1, \ldots, u_{k-1}) \cdot \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} \\ &= u_0 g_0 + u_1 g_1 + \ldots, + u_{k-1} g_{k-1}. \end{aligned}$$

The rows of G generate the $[n,k]$ linear code C. It is for this reason that the matrix G is called a *generator* matrix for C.

Note that G has as its rows a set of basis vectors of the linear subspace C. If C is an $[n,k]$-code, then G will be a (k,n) matrix.

Parity Check Matrix and Dual Codes

Another useful matrix associated with every linear code is a parity check matrix H. For every (k, n) matrix G with k linearly independent rows, there exists an $((n-k), n)$ matrix H with $n-k$ linearly independent rows such that any vector in a row space of G is orthogonal to the row of H, and any vector that is orthogonal to the rows of H is in the row space of G. In other words we can describe the $[n, k]$-code C generated by G as follows:

Definition 4.3.11 An n-tuple v is a codeword in the code C generated by G if and only if $v \cdot H^T = 0$. This matrix H is called a *parity check matrix* of the code.

Example 4.3.12 The parity check matrix for the $[7, 4]$ code generated by G in Example 4.3.10 is:

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

The linear combinations of the rows of the matrix H form another linear code called *dual code* denoted $C^{\perp}$. This code is the null space of the $[n, k]$ linear code C.

Definition 4.3.13 Let C be a linear code with generator matrix G. The *dual code* denoted $C^{\perp}$ is the code consisting of all vectors v such that for any $v \in C$ and any $w \in C^{\perp}$, $v \cdot w = 0$. The code $C^{\perp}$ is an $[n, n-k]$ code.

Each subspace of a matrix M can be considered as a code. We will discuss such codes and their properties in the next chapter.

Chapter 5

Algorithms and GAP

In Chapter 3, we have defined $V_{k,l}(P)$, in this chapter we will discuss the construction of codes from such matrices with their properties. We will also discuss the algorithms in GAP which produce such codes.

5.1 Codes from matrix $V_{k,l}(P)$ with their properties

In this research we consider matrices that are formed from adjacent levels, k and $k+1$ of $\mathcal{L}(G)$, a lattice of subgroups of a group G, so we will denote such matrices as $V_{k,k+1}(\mathcal{L}(G))$. Note, for simplicity in this thesis $V_{k,k+1}\mathcal{L}(G)$ can also be represented as V_k. The two are interchangeable.

The constructions of the 4 subspaces of a matrix V_k in this thesis are quite differ to those which are commonly known defined in Chapter 4. We are using a GUAVA package in the research to construct codes and in GUAVA the *row-space* denoted $R(V)$ of matrix V_k is the set of all linear combinations of row vectors of V_k which is multiplied on the right.

Thus a vector $r \in R(V)$ is in a row-space of V_k if the following holds. Let

$$V_k = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

and

$$x = \begin{pmatrix} x_1 & x_2 & \dots & x_m \end{pmatrix}$$

be an m-tuple vector, then the vector $r \in R(V)$ is in a row-space of V_k if

$$r = xV_k = \begin{pmatrix} x_1 & x_2 & \dots & x_m \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

One should note that the row space is a subspace of the vector space $\mathbb{F}_q^n$.

Similarly, the *column space* denoted $C(V)$ is the set of all linear combinations of column vectors of V. It is the set of all vector c such that $c = xV^\top$ where $V^\top$ is the transposed matrix of V,

$$V^\top = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \dots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{nm} \end{pmatrix}$$

and

$$x = \begin{pmatrix} x_1 & x_2 & \dots & x_n \end{pmatrix}.$$

The column space is a subspace of the vector space $\mathbb{F}_q^m$.

Let x be the n-tuple column vector. The set of all solutions of the homogeneous linear equation $xV^\top = 0$ is a subspace of $\mathbb{F}_q^n$ called the *null-space* or the *kernel* of V and we will denote it as $K(V)$.

The set of all solutions $x \in \mathbb{F}_q^m$ of the homogeneous system of linear equations $xV = 0$ is a subspace of $\mathbb{F}_q^m$ called the *left null-space* of V. We will denote it as $L(V)$.

5.1.1 Codes associated with V_k

A generator matrix of a code must be of full rank m. However, every matrix can be used to generate a code. In this research we are using matrix V_k as a generator or check matrix. We should note that V_k is not a generator nor check matrix but we shall use computer assistance to transfer it to one by elementary row operations.

Theorem 5.1.1 *If G is any matrix with entries in a field $\mathbb{F}$, and G' is any matrix obtained from G by an elementary row operation then if G is a generator matrix for a linear code C then so is G'.*

According to Theorem 5.1.1 which is proven in [24] the matrix V_k can produce codes.

Since every subspace of a space $\mathbb{F}_q^n$ can be considered as a linear code, we will cover 4 codes, associated with the matrix V_k.

Note that we are considering the left multiplication of a matrix V_k, so the following holds:

Firstly, let C be the linear code, associated with the matrix V_k which is an (m, n) matrix. Then, if V_k is used as a generator matrix to produce C, then C is a row-space of V_k.

$$C = \{xV_k : x \in \mathbb{F}^m\} \subset \mathbb{F}^n.$$

We will denote such codes as $R_k(\mathcal{L}(G), \mathbb{F})$.

Secondly, Let C be a column-space of V_k if $V_k^\top$ is the generator matrix of C,

$$C = \{xV_k^\top : x \in \mathbb{F}^n\} \subset \mathbb{F}^m.$$

Such codes will be denoted by $C_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$.

The third code C is a null-space of V_k, denoted $K_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$, if V_k is the parity check matrix, that is,

$$C = \{u \in \mathbb{F}^m : uV_k = 0\}.$$

The fourth code C is a left null-space, denoted $L_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$ if $V_k^\top$ is a parity check matrix of C, that is

$$C = \{u \in \mathbb{F}^n : uV_k^\top = 0\}.$$

5.1.2 Properties of the codes

Codes are associated with properties, and we will study the following: lengths, dimensions, minimum distances and weight distributions. Let us define these properties.

Length and Dimension

The length of a code has previously mentioned in Definition 4.2.4. In our case the codes length is associated with the number of columns or rows of a matrix V_k. If V_k is an (m, n) matrix then

1. The length of the code $R_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$ is n the number of columns of the matrix V_k since it codewords are vectors $c \in \mathbb{F}^n$ such that $c = uV_k$ where $u \in \mathbb{F}^m$.

2. The length of $C_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$ is m, the number of rows of V_k since it is the set of vectors $c \in \mathbb{F}^m$ such that $c = uV_k^\top$ where $u \in \mathbb{F}^n$.

3. The length of $K_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$ is n since it is the code associated with null-space of V_k, that is it is a set of vectors $u \in \mathbb{F}^n$ such that $0 = V_k u$ or $0 = u^\top V_k^\top$.

4. The length of $L_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$ is m since it is the linear code associated with the left null space or the null-space of $V_k^\top$. The vectors in this code are vectors $u \in \mathbb{F}^m$ such that $0 = V_k^\top u$ or $0 = uV_k$.

Now let us define the dimension of codes. Since a linear code C is a vector space, then the dimension of C is the dimension of C as a vector space over $\mathbb{F}_q$.

Definition 5.1.2 The *dimension* of a vector space W denoted $dimW$ is the largest possible number of elements in a linearly independent subset of W.

To find the dimension of a code C, by the definition it means that one needs to examine all possible subsets of all vectors in C but it is impractical. In fact, finding the dimension is much easier, it has been proven by Pretzel [25] that one just needs to find the number of vectors in a single linearly independent subset S of C which cannot be extended.

Since codes in this thesis are associated with subspaces of a matrix V_k then the dimension of such codes are related to the rank of the matrix V_k.

Definition 5.1.3 Let A be an (m, n) matrix. The kernel of A is the set of vectors $u \in \mathbb{F}^n$ such that $Au = 0$ or $uA^\top = 0$. The image of A is the set of vectors $v \in \mathbb{F}^m$ such that $v = Au$ or $v = uA^\top$ for some $u \in \mathbb{F}^n$. The dimension of the kernel of A is called its *nullity*, and the dimension of the image of A is called the *rank* of A.

There is a relationship between the rank and nullity of a matrix A which is shown in the following theorem.

Theorem 5.1.4 *(Nullity theorem): Let A be an (m,n) matrix over a field $\mathbb{F}$ with rank r and nullity k, then $r + k = n$.*

The rank of an (m, n) matrix A is just the maximal size of a set of linearly independent rows or columns of A. It has been shown in [25] that the two, row rank and column rank are the same and that number is called a rank of a matrix.

So the dimension of the four codes associated with a matrix V_k in this thesis are given below.

Let V_k be an (m, n) matrix with rank r then,

1. The dimension of the code $R_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$ is r the rank of matrix V_k because it is a linear code corresponds to the row space of V_k.

2. The dimension of $C_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$ is also r since it is a code corresponds to the column space of V_k.

3. The dimension of $K_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$, a code associated with null-space or the kernel of V_k is $n - r$ according to the rank and nullity theorem.

4. Similarly the dimension of $L_k(\mathcal{L}(\mathcal{G}), \mathbb{F})$, a code associated with the left null space or the null-space of $V_k^\top$, is $m - r$

When the linear code has a length of n and a dimension of k then it is called $[n, k]$ code.

Since the number of codewords of a linear code is determined by the dimension of the subspace, then the number of codewords in an $[n, k]$ linear code or *size* of the code is k^q

Minimum Distances and their bounds

Apart from the length and size of a code, another important and useful characteristic of a code is its minimum distance.

When error occur in the transmission, the receiver reads a word v although the transmitter sent a word w.

Definition 5.1.5 If $v = v_1, \ldots, v_n$ and $w = w_1, \ldots, w_n$ are words in $\mathbb{F}_q^n$, we shall refer to v_j as an entry of v in place j and we shall say that v differ from w in place j if $v_j \neq w_j$.

We can call the word v that will be analyzed by the error processor the *received word*. If the received word v differs from the transmitted one in k places we say an error of weight k occurred.

Definition 5.1.6 Let v and w be words in $\mathbb{F}_q^n$. The *Hamming distance (or simply distance)* from v to w, denoted by $d(v, w)$, is defined to be the number of places at which v and w differ.

Example 5.1.7 Suppose $v = 01010$ and $w = 01101$ are words in $\mathbb{F}_2^5$ then

$$d(v, w) = 3$$

because v and w are differ in the 3rd, 4th and 5th positions.

Definition 5.1.8 For a code C containing at least two words, the *(minimum) distance* of C, denoted by $d(C)$, is the smallest Hamming distance between distinct codewords of C that is,

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

This parameter is very important. It determines the error detection and error correction capabilities of a code C, hence a linear code C can be described as an $[n, k, d]$-code.

Example 5.1.9 Let $C = \{00000, 00111, 11111\}$ be a binary code. Then $d(C) = 2$ since $d(00000, 00111) = 3$, $d(00000, 11111) = 5$ and $d(00111, 11111) = 2$. Thus C is a binary $[5, 3, 2]$-code.

Definition 5.1.10 Let v be a word in $\mathbb{F}_q^n$. The *Hamming weight* (or simply *weight*) of v, denoted by $w(v)$ is defined as the number of nonzero components of v that is,

$$w(v) = d(v, 0),$$

where 0 is a zero codeword.

Example 5.1.11 Let $v = 00111$, then the Hamming weight of v is 3.

Definition 5.1.12 Let C be a code. The *minimum Hamming weight* (or simply *minimum weight*), denoted $w_{min}(C)$, is the smallest of the weights of the nonzero codewords of C.

From Definition 5.1.8, we can determine the minimum distance of a non-linear code, the process involved checking all pairs of codewords; that is about $|C|^2/2$ checks. A useful fact about linear code is that you can read off the minimum distance by checking the weight of its codeword. Often the structure of a linear code enables the minimum weight to be found without checking all codewords as stated in the theorem below.

Theorem 5.1.13 *The minimum distance $d(C)$ of a linear code is equal to the minimum weight of its nonzero codeword.*

Proof: The sum of two codewords is also a codeword then the Hamming distance between two codewords in C is equal to the Hamming weight of a third codeword in C. Hence the minimum weight of the linear code C is equal to the minimum distance of C.

The number of codewords $M = q^k$ of any code C with a minimum distance $d(C)$ is bounded. There are several results that give the minimum distance bounds of a code such as BCH bound, residue bound, Singleton bound, Plotkin bound, Gilbert bound, and a lot more (see [3]).

Given below is a Singleton bound:

For any linear code of length n and dimension k, its Hamming distance is bounded by

$$d(C) \leq n + 1 - k.$$

Weight Distribution

Another important characteristics of a code is the weight distribution. As it was mentioned before the weight of word or vector is the number of non-zero components in the vector or it is the distance of the word from the zero vector.

Definition 5.1.14 Let C be an $[n, k]$ code over $\mathbb{F}_q$. Let A_i be the number of codewords with weight i in C. Then the numbers $A_0, A_1, \ldots, A_n$ are called the *weight distribution* of C and the polynomial $A(z) = A_0 + A_1 z + \cdots + A_n z^n$ is called the *weight enumerator* for C.

There is an interesting relationship between the weight distribution of a code C, and its dual code $C^{\perp}$. It is expressed in a *MacWilliam identity.*

For codes which have only a small number of codewords or short block length or low rates, the weight distribution can be easily determined. Unfortunately, the number of codewords in most high-rated codes are so large that we cannot determine the weight enumerator, even with the help of powerful computers. However, even though q^k may be very large, q^{n-k} may be relatively small. Thus it may be easier to determine the weight enumerator of the *dual* code, whose codewords are the parity checks of the original code. In fact, Berlekamp [3] claims that it is generally easier to obtain the weight enumerator of the dual code whenever the rate of the original code is $\geq \frac{1}{2}$.

Once the weight of the dual code has been determined, then the weight of the original code can be constructed by the MacWilliams theorem.

Theorem 5.1.15 (MacWilliams identity.) *If $A(z)$ and $B(z)$ are the weight enumerators of a linear k-dimensional code $C \in \mathbb{F}_q$ and of its dual $C^{\perp}$ respectively, then*

$$B(z) = \frac{1}{q^k}(1 + (q-1)z)^n A(\frac{1-z}{1+(q-1)z}).$$

The proof of this theorem is beyond the scope of this thesis but proven in Thomas Britz [4]. The MacWilliams theorem state that the weight distribution for larger codes could be computed if the weight distribution of their dual are known by using the relationship above.

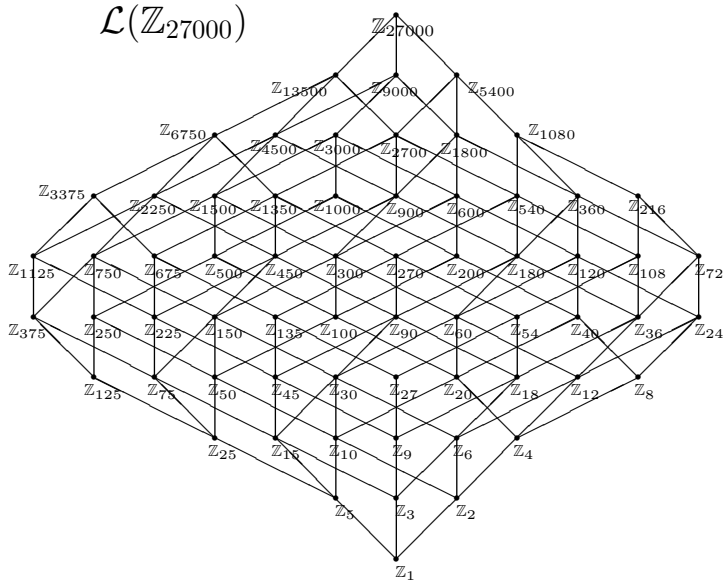
5.2 Examples of codes constructed from $V_{k,k+1}(\mathcal{L}(G))$

Given below is an example of a code generated from a matrix $V_k(\mathcal{L}(G))$. This example shows in steps what has been done in the research.

Let G be an Abelian group and $\mathcal{L}(G)$ be it lattice of subgroups. So for every subgroup of G one can define the *inclusion matrix* of k-level of $\mathcal{L}(G)$ versus its $k+1$-level, and associate $\mathcal{L}(G)$ with incidence matrices $V_k(G)$. Note as stated before cyclic groups are partial cases of Abelian groups so in this example we will use $\mathbb{Z}_{27000} = \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_{5^3}$ as the group G to generate these codes.

Construction of the matrix $V_2(\mathcal{L}(\mathbb{Z}_{27000}))$ from $\mathcal{L}(\mathbb{Z}_{27000})$

The lattice of subgroups of the Abelian group $\mathbb{Z}_{27000} = \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_{5^3}$ and the matrix $V_2(\mathcal{L}(\mathbb{Z}_{27000}))$ are shown below. The construction of these follow ideas in [7], [13], [20], [21].



$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

The matrix $V_2(\mathcal{L}(\mathbb{Z}_{27000}))$ shows how subgroups $\mathbb{Z}_{25}, \mathbb{Z}_{15}, \mathbb{Z}_{10}, \mathbb{Z}_9, \mathbb{Z}_6$ and $\mathbb{Z}_4$ are included into subgroups $\mathbb{Z}_{375}$, $\mathbb{Z}_{250}$, $\mathbb{Z}_{225}, \mathbb{Z}_{150}$, $\mathbb{Z}_{135}, \mathbb{Z}_{100}, \mathbb{Z}_{90}, \mathbb{Z}_{60}, \mathbb{Z}_{54}, \mathbb{Z}_{40}, \mathbb{Z}_{36}$ and $\mathbb{Z}_{24}$.

A linear code $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(2)$ generated by $V_2(\mathcal{L}(\mathbb{Z}_{27000}))$ matrix

The matrix $V_k(\mathcal{L}(G))$ can be used to construct linear codes over finite fields $GF(p)$. Let $\mathcal{C}_k(G, F)$ be the linear code over $GF(p)$ generated by this matrix.

Let $V_2(\mathbb{Z}_{27000})$ be a generator matrix for a code C. By following the procedure in O. Pretzel [25] and in S. Ling and C. Xing [18] we could transform the matrix $V_2(\mathcal{L}(\mathbb{Z}_{27000}))$ into its *standard form*.

In general any matrix G can be made into a generator matrix for a code C via elementary row operations. It has been proved by O. Pretzel [25] and in S. Ling and C. Xing [18] that a generator matrix G for a code C can be brought into reduced row echelon form and still generate C, and then, by permuting columns, it can be transformed into a so-called *standard form* $G' = [I_k|A]$ where it is now a generator matrix for an equivalent (in fact, isomorphic) code. Here A is a $k \times (n-k)$ matrix over the field $GF(p)$.

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

The matrix $V_2(\mathcal{L}(\mathbb{Z}_{27000}))$ can be brought into its reduced row echelon form by the following elementary row operations over $GF(2)$: (Note R_i means Row i).

$R_1 = R_2 + R_1$

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$R_1 = R_3 + R_1\,,\ R_2 = R_3 + R_2$

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$R_1 = R_4 + R_1$

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$R_2 = R_5 + R_2\,,\ R_4 = R_5 + R_4$

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

It can be brought into its *standard form* by first permuting column 5 with column 6 and then column 6 with column 10.

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

The matrix above is now in standard form and it will produce the code $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(2)$ which is isomorphic to the one generated by the matrix we started of with over the same field. This code has *length* of 10 because the matrix $V_2(\mathcal{L}(\mathbb{Z}_{27000}))$ has 10 columns and *dimension* of 6 because it has 6 linearly independent rows. There are 2^6 codewords in this code. So the code $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(2)$ is a $(10, 2^6)$-linear code.

The minimum distance of $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(2)$ can be determined using its parity check matrix H. We will use the theorems below which were stated and proven in [18].

Theorem 5.2.1 *If $G = (I_k/X)$ is a standard form generator matrix of an $[n, k]$-code, then a parity check matrix for C is $H = (-X^T/I_{n-k})$.*

From Theorem 5.2.1 the parity check matrix for the code $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(2)$ is given below and we will denote it as H_1:

$$H_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Theorem 5.2.2 *Let C be a linear code and let H be a parity-check matrix for C, then*

1. *C has distance $\geq d$ if and only if any $d-1$ columns of H are linearly independent; and*
2. *C has distance $\leq d$ if and only if H has d columns that are linearly dependent.*

Definition 5.2.3 Let 0 be a row vector with zero entries, then $0^\top$ is a column vector with zero entries.

Obviously there are no *zero column* in H_1 as well as none of any two columns in H_1 sum to $0^\top$. This implies that any two columns of H_1 are linearly independent. However there are three columns sum to $0^\top$ which are columns 1,2, and 4 hence three columns are linearly dependent.

From the result above and using theorem 5.2.2 the minimum distance of $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(2)$ is 3 so the code $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(2)$ is called a [10,6,3] linear code over $GF(3)$.

A linear code $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(3)$ generated by matrix $V_2(\mathcal{L}(\mathbb{Z}_{27000}))$

Note that when a different field is used another code could be constructed. Let $V_2(\mathcal{L}(\mathbb{Z}_{27000}))$ be a generator matrix for a code C over $GF(3)$.

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

This matrix can be developed into its reduced row echelon form by the following elementary row operations over $GF(3)$:

$R_1 = -R_2 + R_1$

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 2 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$R_1 = -2R_3 + R_1\,,\ R_2 = -R_3 + R_2$

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$R_1 = -R_4 + R_1$

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$R_1 = -R_5 + R_1\,,\ R_2 = -R_5 + R_2\,,\ R_4 = -R_5 + R_4$

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Just like before, it can be brought into *standard form* by permuting column 5 with

column 6 and then column 6 with column 10.

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & 2 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$V_2(\mathcal{L}(\mathbb{Z}_{27000})) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

This matrix is a generator matrix in standard form of the code $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(3)$. This linear code has *length* of 10, *dimension* of 6 and has 3^6 codewords.

In the same way, the minimum distance of $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(3)$ can be determined using its parity-check matrix, denoted as H_2.

The parity check matrix for the code $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(3)$ is:

$$H_2 = \begin{pmatrix} 0 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 2 & 2 & 0 & 0 & 1 & 0 \\ 2 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

There are no *zero column* in H_2 as well as none of any two columns in H_2 sum to $0^\top$. This implies that any two columns of H_2 are linearly independent. However there are three columns sum to $0^\top$ which are columns 1,2, and 4 hence three columns are linearly dependent. Therefore the minimum distance of $R_2(\mathcal{L}(\mathbb{Z}_{27000}))$ over $GF(3)$ is 3 so it is called a [10,6,3] linear code over $GF(3)$.

These examples showed that different codes could be generated by the same generator matrix when using different fields. We should also note that for each incident

matrix $V_k(\mathcal{L}(G))$ of the k and $k+1$ level of $\mathcal{L}(G)$, there are 4 sets of codes that could be generated. Each set corresponds to the 4 subspace of $V_k(\mathcal{L}(G))$. The example given corresponds to the row subspace of $V_k(\mathcal{L}(G))$. We should also noticed that for each lattice we could form several incident matrices $V_k(G)$ depending on the k-orbits of $L(G)$.

The 4 subspaces of a matrix V_k can be grouped into two categories, image space and kernel space. The first two, column and row spaces will be recognized in this thesis as *image subspace of* V_k and the latter two will be known as *kernel subspace* (as shall be shown later).

Initially we were studying the 4 codes associated with each subspace of V_k, however we found out that the image subspace does not have very interesting results so we concentrate only on codes associated with the kernel subspace of V_k.

In general we are studying these codes:

1. Codes associated with Boolean lattice, $\mathcal{B}_n$, we call them *Boolean codes* denoted by $B_k(n,p)$.

2. Codes related to the lattice $\mathbf{m}^n$, or $\mathcal{F}(s)^{m-1}$ lattices of divisor of an integer $(s)^{m-1}$. We call such codes *Divisor codes* denoted $F_k(m^n,p)$

3. Codes related to lattices of subgroups of non-cyclic Abelian groups, $\mathcal{L}(\mathbb{Z}_q^n)$. In particular $\mathcal{L}(Z_p \times Z_p \times \cdots \times Z_p)$ which is a lattice of subspaces of n-dimensional vector space over $GF(p)$. We call such codes *Projective codes*

We will study such codes which we will call *Combinatorial Codes* in more detail in the next chapter.

5.3 GAP

The goal of this section is to discuss the main tools used in collecting data for this research. The tools are programmes written in GAP. They also use the GAP coding-theory package GUAVA. We will also interprets the raw data produced by such programmes.

GAP stands for **Groups, Algorithms and Programming**. It is a computer algebra package software which is used for computation in discrete abstract algebra.

The GAP system consists of

- A kernel written in C language,
- a library of GAP functions and group theoretical data,
- documentation for users help.

Beside these there are available GAP shared packages such as GUAVA, SONATA, and others. However, these needs to be installed differently, because they are not part of the system. Most packages are written in GAP's own interpreted language.

GAP is extensible in the way that it allows the user to use their own programmes written in GAP's own interpreted language or in C or even in other languages, in just the same way as the programmes which form parts of the system library. GAP's open source kernel is written in the C programming language [10].

GUAVA is a GAP4 package for computing with error correcting codes. It is written in the GAP language and runs on any system supporting GAP4.3 and above. GUAVA main functions includes the construction and manipulation of codes as well as computations of information about codes [11].

5.3.1 GAP Programs and Interpretations

In the research we are using programs written in GAP language with the assistance of the GUAVA package to collect data.

The main aim of the thesis is to investigate the properties of the combinatorial codes related to finite groups. Thus these programs were aimed to do the following:

1. generate the finite group G,
2. generate the lattice of subgroups of G,
3. Construct the matrix V_k,
4. identify the properties of this matrix V_k.

Secondly, having generated the matrix V_k, we then need to construct combinatorial codes. To identify the codes we need to calculate their parameters. So we must

1. Generate the combinatorial codes associated with V_k.
2. calculate the length and dimension of the codes,
3. calculate the weight distribution if possible otherwise calculate the minimum distance.

The programs are written in a straight forward usage of the commands in GAP. There are 2 different programs used, one to produce Boolean and Divisor codes with their properties and the other is to produce Non-cyclic Abelian codes with their properties.

Programme(1) Construction of Boolean and Divisor codes

The program (see Appendix A.4.1) has two parts, the first develop the matrix V_k and the second produces the codes with its weight distribution.

In constructing the matrix V_k for Boolean codes and divisor code, we are not constructing a lattice of subgroups of G using the command in GUAVA. It takes so long to compute so we are using another idea. It involved developing sets $S = [0, 1, 2, \ldots, m-1]$ and $T = S \times S \times \cdots \times S$ and then find the sum of all the entries in s. If $s = [a_1, a_2, \ldots]$, then $sum(s) = a_1 + a_2 + \ldots$. Level l is the array of all tuples in $S \times S \times \cdots \times S$ such that $sum(s) = l$. All such s form a level L in the lattice $\mathbf{m}^n$. The values of the "Included" function are true or false (the Boolean function). It compares elements in $s = (s_1, s_2, \ldots, s_n)$ and $t = (t_1, t_2, \ldots, t_n)$. If $s_i \leq t_i$ for all $i = 1, 2, \ldots, n$ then s is included in t, otherwise s is not included in t.

The matrix V_k are then constructed using the included function. If s_i is included in t_j then the entry of the V_k corresponds to the i-th row and j-th column is 1 otherwise 0.

The properties of such matrices are then calculated such as number of rows and columns, maximum and minimum column and row weight. The rank of V_k over $GF(p)$ is also determined.

The second part of the programme involves the construction of the combinatorial codes. We are interested in the null space codes so we construct only codes developed from the null space of the matrix V_k, and from the null space of the transposed matrix of V_k.

The weight distribution of such codes are calculated . If this cannot be obtained then the minimum distance is calculated. When the code contains a very large number of codewords it takes so long for both to compute so instead we find the probabilistic minimum distance using the command developed in [6].

Programme(2) Construction of non-cyclic Abelian codes

The program (see Appendix A.4.2) is used to construct non-cyclic Abelian codes. It is quite similar to programme(1). The only difference is that in here the lattice of subgroups of the group G is constructed using a direct command 'LatticeSubgroups(g)' in GAP. Based on such lattices the matrix V_k is constructed.

Just like in Programme(1), the matrix is constructed first then the codes are generated with their properties.

The results from these programs are presented nicely in tables in the Appendix section. In both programs we construct two codes, one as a null-space of V_k and the other as null space of $V_k^\top$ (or left null space). However in our tables A.4 we have only produced a code related to the null space due to the following.

Definition 5.3.1 Let the first level of the lattice be level 0, $k = 0$ and the last level be level n, $k = n$. The lattice is *symmetric* if V_i is the transposed matrix of $V_{(n-i+1)}$, for $0 \leq i \leq \frac{n}{2}$.

For instance V_0 is the transposed matrix of $V_{(n-1)}$, V_1 is a transposed matrix of $V_{(n-2)}$ and so on.

The finite groups we studied are all Abelian groups. Lattices of such groups have the beautiful property of being symmetric. We were supposed to present results on the two codes, the null space and the left null space of V_k, related to the kernel of our matrix V_k, but because of this beautiful property we put them together under one.

The code corresponds to the null space at the lower half of the lattice is the same to the code associated with the left-null space of the upper half of the lattice.

For instance lets consider the Boolean code when n=5, $\mathcal{B}_5$ over $GF(2)$. Recall it is the same as the lattice of subgroups of a group $\mathbb{Z}_n$ where $n = p_1 \times p_2 \times \cdots \times p_5$ and p_i is any prime number. By using GAP we get these results:

There are 5 levels in the subgroup lattice and the matrices are given below.

$$V_{0,1} = V_{4,5}^{\top} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$V_{1,2} = V_{3,4}^{\top} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$V_{2,3} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Similarly the weight distribution of each codes from different levels are given below. Note L_i is the code associated with the left null space of V_i, and K_j is the code associated with the null space of V_j.

Level k	*matrix*		*Code name*		Weight distribution
	size	rank	Space	[l,dim,d]	
0	(1,5)	1	L_0	[1,0,1]	[1, 0]
			K_0	[5,4,2]	[1, 0, 10, 0, 5, 0]
1	(5,10)	4	L_1	[5,1,5]	[1, 0, 0, 0, 0, 1]
			K_1	[10,6,3]	[1, 0, 0, 10, 15, 12, 15, 10, 0, 0, 1]
2	(10,10)	6	L_2	[10,4,4]	[1, 0, 0, 0, 5, 0, 10, 0, 0, 0, 0]
			K_2	[10,4,4]	[1, 0, 0, 0, 5, 0, 10, 0, 0, 0, 0]
3	(10,5)	4	L_3	[10,6,3]	[1, 0, 0, 10, 15, 12, 15, 10, 0, 0, 1]
			K_3	[5,1,5]	[1, 0, 0, 0, 0, 1]
4	(5,1)	1	L_4	[5,4,2]	[1, 0, 10, 0, 5, 0]
			K_4	[1,0,1]	[1, 0]

We should notice that code $L_4 = K_0$, and $K_4 = L_0$. Similarly $L_3 = K_1$, and $K_3 = L_1$ so the results in this thesis will be presented as:

Level k	*matrix*		*Code name*		Weight distribution
	size	rank	Space	[l,dim,d]	
0	(1,5)	1	$K_0 = L_4$	[5,4,2]	[1, 0, 10, 0, 5, 0]
1	(5,10)	4	$K_1 = L_3$	[10,6,3]	[1, 0, 0, 10, 15, 12, 15, 10, 0, 0, 1]
2	(10,10)	6	$K_2 = L_2$	[10,4,4]	[1, 0, 0, 0, 5, 0, 10, 0, 0, 0, 0]
3	(10,5)	4	$K_3 = L_1$	[5,1,5]	[1, 0, 0, 0, 0, 1]
4	(5,1)	1	$K_4 = L_0$	[1,0,1]	[1, 0]

The matrix V_0 or V_{n-1} are just row vectors and column vectors and they do not give interesting results, so we will not include them in our results.

5.3.2 Interpretation of Raw Data

In here we will interpret what is given in the raw data.

The raw data (see Appendix A.4.3) is produced from the Boolean and Divisor code program (see Appendix A.4.1) when $m = 2$, $n = 4$, $k = 1$ and $p = 2$.

The data shows that the matrix V_1 is a (4,6) matrix with rank 3 over $GF(2)$ and the weight enumerator polynomial is $1 + 4x^3 + 3x^4$. '$n = 4$' here means that a

lattice $\mathcal{L}(\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_3} \times \mathbb{Z}_{p_4})$, $p_i \neq p_j$ is considered. The Hasse diagram of this lattice is shown in Example 3.3.5. We should note that these diagrams are drawn using information in the matrix V_k.

There were four levels in the given lattice, $k = 0$, $k = 1$, $k = 2$ and $k = 3$ as shown in the diagram. In the data, when $k = 1$, it means that the incidence matrix $V_{1,2}(\mathcal{B}_4)$ is used to generate a code. This matrix is constructed in the manner that the rows are the 1-element subsets and the columns are the 2-elements subsets hence it has a size of $\binom{4}{1}$ by $\binom{4}{2}$. This is so because there are 4 subsets in level 1, $\{\{1\}, \{2\}, \{3\}, \{4\}\}$ and there are 6 subsets in level 2, $\{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$. The matrix $V_{1,2}(\mathcal{B}_4)$ is shown below.

$$V_{1,2}(\mathcal{B}_4) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

The code $K_1(\mathcal{B}_4, GF(2))$ is the set of column vectors x such that

$$V_{1,2}(\mathcal{B}_4)x = 0$$

(or null-space of $V_{1,2}(\mathcal{B}_4)$). The code has length 6 and dimension 3. Note that later in the thesis this code is defined as $B_1(4,2)$.

The weight enumerator polynomial of this code is given as $1+4x^3+3x^4$. This means that the code has 8 codewords (sum of the coefficients). There were a zero vector, four vectors with weight 3 and three vectors with weight 4. So from this polynomial the minimum distance of the code is 3 which is given by the lowest positive number n in x^n. Thus the code $K_{1,2}(\mathcal{B}_4, GF(2))$ is a [6,3,3] linear code.

The next data (see Appendix A.4.4) is produced from program 2 (see A.4.2). In here we are using the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $k = 1$ and $p = 3$. The data produce the same structure as in the first program and interpreted in the same manner.

Chapter 6

Combinatorial Codes

In this chapter we are discussing the main findings on combinatorial codes, defined as follows:

Definition 6.0.2 Let $\mathbb{F}$ be a field and $\mathcal{P}$ be any ranked poset. Let $V_{kl}(\mathcal{P})$ be an incidence matrix between levels k and l in $\mathcal{P}$. *Combinatorial code* denoted $C_{kl}(\mathcal{P}, \mathbb{F})$ is the linear code over the field $\mathbb{F}$ with $V_{kl}(\mathcal{P})$ as the check matrix.

One of the goals of the thesis is to study minimal distances of combinatorial codes over finite fields of small characteristics. All the codes we will investigate are associated with the lattices of subgroups of finite Abelian groups. Depending on the group G, the lattices we study includes

- Boolean lattices $\mathcal{B}_n$ which correspond to the cyclic groups $\mathbb{Z}_n$ where n is any square-free integer, that is any integer of the form $p_1 p_2 \dots p_n$, where $p_1, p_2, \dots, p_n$ are different primes;
- Lattices $\mathcal{F}(n)$ of divisors of an integer $n = s^t$, where s is any square free integer and $t > 1$;
- Lattices $\mathcal{L}(\mathbb{Z}_q^n)$ of subgroups of the groups $\mathbb{Z}_q^n$, where q is prime. These are the lattices of subspaces of projective vector spaces.

It is well known [1] that these lattices are ranked and so can be used to construct combinatorial codes.

6.1 Codes related with the Boolean lattices $\mathcal{B}_n$.

Let $\mathcal{B}_n$ be a Boolean lattice. Combinatorial codes related to the matrix $V_{k,k+1}(\mathcal{B}_n)$ are of special interest. These matrices are constructed as follows:

Let n, k be integers such that $n > k > 0$. Let S be a set with n elements and let $P_k(S)$ denote the set of all k-subsets of S. Then $V_{k,k+1}(\mathcal{B}_n)$ is the $\binom{n}{k}$ by $\binom{n}{k+1}$ matrix whose rows are indexed by the k-subsets of S and columns are indexed by $(k+1)$-subsets of S (for some fixed ordering for k-subsets and some fixed ordering for $(k+1)$-subsets of S). The entry $V_{k,k+1}$ in the intersection of row A and column B is 1 if A is the subset of B and 0 otherwise. We will denote matrix $V_{k,k+1}(\mathcal{B}_n)$ as $V_k(\mathcal{B}_n)$.

For simplicity we call codes with check matrix $V_k(\mathcal{B}_n)$ the *Boolean codes* and denote it as $B_k(n,p)$.

Example 6.1.1 The code $B_2(7,3)$ may be considered as the kernel of matrix $V_2(\mathcal{B}_7)$ over $GF(3)$. It is a $[35,20,8]$ linear code. This means that the code has length $n = 35$, dimension 20 and minimum distance 8. The weight enumerator is given below:

$$1 + 210x^8 + 42x^{10} + 2940x^{12} + 2100x^{13} + 9900x^{14} + 46368x^{15}$$
$$+52290x^{16} + 95760x^{17} + 572460x^{18} + 402990x^{19} + 692496x^{20}$$
$$+2328900x^{21} + 1189650x^{22} + 1294020x^{23} + 3339000x^{24} + 1173564x^{25}$$
$$+928620x^{26} + 1512560x^{27} + 346380x^{28} + 162540x^{29} + 167496x^{30}$$
$$+21630x^{31} + 5040x^{32} + 1890x^{33} + 60x^{35}.$$

Recently such codes have been intensively studied. They were introduced by V.C. Da Rocha in 1985 [27] and later in 1990 studied by L Tolhuizen and J.H. van Lint [27]. They were also considered by H. Lefmann [15], Mnukhin and Siemons [22, 23], and lately studied by G.B. Khosrovshahi, R. Naserasr and B. Tayfeh-Rezaie [14]. The results of these studies will later be discussed in the text.

We will discuss the main characteristics of such codes.

6.1.1 Lengths and Dimensions

The length of $B_k(n,p)$ code is $\binom{n}{k+1}$ and does not depend on characteristics p. It follows from the fact that $V_k(\mathcal{B}_n)$ is an $\binom{n}{k}$ by $\binom{n}{k+1}$ matrix and $B_k(n,p)$ codewords are the set of vectors u such that $V_{k,k+1} \cdot u = 0$.

To find the dimension of any combinatorial code $C_{kl}(\mathcal{P}, \mathbb{F})$, note that it is related to the rank of the matrix $V_{kl}(\mathcal{P})$ over finite field $\mathbb{F}$ (refer to rank and nullity Definition 5.1.3 and to the Nullity Theorem 5.1.4).

The rank of matrix $V_k(\mathcal{B}_n)$ over $GF(q)$ has been studied in [8], [30], [17], [26]. The next result is well known.

Theorem 6.1.2 (Frankl [8], Wilson [30]) *If $\mathbb{F} = GF(q)$ and $k+l \leq n$, then*

$$rank_q V_{kl}(\mathcal{B}_n) = \sum_{i \in S} \binom{n}{i} - \binom{n}{i-1},$$

where

$$S = \{i = 0, 1, \ldots, l : q \nmid \binom{l-i}{k-i}\}.$$

Example 6.1.3 Let the lattice be $\mathcal{B}_6$, the rank of the matrix $V_2(\mathcal{B}_6)$ over $GF(3)$ can be determined as follows. First, let us find the set S. We can see that $k = 2$ and $l = 3$ so $i = 0, 1, 2, 3$. The values of $\binom{l-i}{k-i}$ for a particular i are given in the table below:

i	$\binom{l-i}{k-i}$
0	3
1	2
2	1
3	0

We can see that $3 \nmid \binom{l-i}{k-i}$ at $i = 1, 2$, so $S = \{1, 2\}$. We then have

$$rank_3 V_2(\mathcal{B}_6) = \binom{6}{2} - \binom{6}{1} + \binom{6}{1} - \binom{6}{0} = 15 - 6 + 6 - 1 = 14.$$

According to the Nullity theorem, the dimension of kernel of $V_2(\mathcal{B}_6)$ is $6 = 20 - 14$.

So in general the dimension of $B_k(n,p)$ is $\binom{n}{k+1} - rank_p V_{k,k+1}(\mathcal{B}_n)$ where the rank is given by the theorem of Frankl and Wilson.

6.1.2 Weight distributions

The weight distribution of these codes as far as I know have not been intensively studied. However, recently some special cases were considered by G.B Khosrovshahi, R. Naserasr and B. Tayfeh-Rezaie [14]. They were studying *ternary codes*, that is codes $B_k(n,3)$ and proved the following theorems:

Theorem 6.1.4 (Khosrovshahi, Naserasr and Tayfeh-Rezaie [14]) *For every n, the code $B_2(n,3)$ has length $\binom{n}{3}$, dimension $\binom{n}{3}-\binom{n}{2}+1$ and minimum distance of 8.*

Other results of [14] are related with the structure of the weight enumerator polynomial. For example, the weight enumerator polynomial of $B_2(6,3)$ is given below:

$$1+30x^8+12x^{10}+240x^{12}+120x^{13}+120x^{14}$$
$$+144x^{15}+30x^{16}+20x^{18}+12x^{20}\,.$$

Note that the polynomial does not contain x^s, where $s=9$ and 11.

Theorem 6.1.5 (Khosrovshahi, Naserasr and Tayfeh-Rezaie [14]) *Let $n\equiv 0 \pmod 3$ and $n\geq 9$. Then $B_2(n,3)$ has a codeword of weight d if and only if $d=8,10,12,13,\ldots,\binom{n}{3}$.*

In [14] the authors also claim that for $n\geq 9$, there exists a codeword of any weight at least 12 and that the same result is also valid for all sufficiently large n.

In this thesis we consider cases of characteristics different from 3 also. We were only able to study similar properties for $n=6$ but not for $n\geq 7$ due to the fact that the number of codewords in these codes were very large and therefore it takes so long to compute the weight distribution.

However we were able to observe properties similar to that in Theorem 6.1.5 but over the field $GF(5)$. We were able to see that over $GF(5)$, there cannot be a codeword of weight 9,10,11 and 13 in the codes $B_2(n,5)$.

So we can formulate the following conjecture:

Conjecture 6.1.6 *For every $n\geq 6$, the code $B_2(n,5)$ has a codeword of weight d if and only if $d=8,12,14,15,\ldots,\binom{n}{3}$.*

Another observation in our study was that for $n \leq 8$ and $p = 3, 5$ we could see that codes $B_1(n, p)$ have minimum distance 4 and have no codewords of weight 5.

So we formulate the following conjecture:

Conjecture 6.1.7 *For every n the codes $B_1(n, p)$ over the field $GF(p)$, where $p \geq 3$ is prime, have minimum distance 4 and have no codewords of weight 5.*

Furthermore, the following result gives a relationship between the rank of the matrix $V_k(\mathcal{B}_n)$ when $k = n - 3$ and the weight enumerator of the code $B_k(n, 3)$ as shown below:

In our research we have been able to show the following:

Proposition 6.1.8 *If $k = n - 3$, then $rank_3 V_k(\mathcal{B}_n)$ is $\binom{n}{k+1} - 1$.*

Proof: Note that when $k = n - 3$, then

$$rank_3 V_{n-3,n-2}(\mathcal{B}_n) = \binom{n}{(n-3)+1} - 1 = \binom{n}{n-2} - 1 = \binom{n}{2} - 1.$$

The matrix $V_{n-3,n-2}(\mathcal{B}_n)$ is the transposed matrix of $V_{2,3}(\mathcal{B}_n)$, thus

$$rank_3 V_{n-3,n-2}(\mathcal{B}_n) = rank_3 V_{2,3}(\mathcal{B}_n).$$

We need to show that $rank_3 V_{2,3}(\mathcal{B}_n)$ is $\binom{n}{2} - 1$. Using Frankl and Wilson rank theorem

$$rank_3 V_{2,3}(\mathcal{B}_n) = \sum_{i \in S} \binom{n}{i} - \binom{n}{i-1},$$

where $S = \{i = 0, 1, 2, 3 : 3 \nmid \binom{3-i}{2-i}\}$.

Let us find the set S. The values of $\binom{3-i}{2-i}$ for a particular i are given in the table below:

i	$\binom{3-i}{2-i}$
0	3
1	2
2	1
3	0

We can see that $3 \nmid \binom{l-i}{k-i}$ at $i = 1, 2$ thus the set $S = \{1, 2\}$. We then have

$$rank_3 V_2(\mathcal{B}_n) = \binom{n}{1} - \binom{n}{0} + \binom{n}{2} - \binom{n}{1} = \binom{n}{2} - 1.$$

Therefore

$$rank_3 V_{n-3}(\mathcal{B}_n) = \binom{n}{k+1} - 1.$$

□

Proposition 6.1.9 *The weight enumerator of* $B_k(n, 3)$ *when* $k = n - 3$ *is* $1 + 2x^{\binom{n}{k}}$.

Proof: It follows from Proposition 6.1.8 that the rank of $V_k(\mathcal{B}_n)$ over $GF(3)$ when $k = n - 3$ is $\binom{n}{k+1} - 1$, then by the Nullity theorem the dimension of the kernel of the matrix $V_k(\mathcal{B}_n, GF(3))$ is $\binom{n}{k+1}$-$\binom{n}{k+1}-1 = 1$ and therefore the weight enumerator is $1 + 2x^{\binom{n}{k}}$. □

6.1.3 Minimum distances

There is an evident relationship between the minimum distance of any code C and its weight enumerator. By the weight enumerator Definition 5.1.14 the weight distribution of a code C with A_i be the number of codewords with weight i is the numbers $A_0, A_1, \ldots, A_n$ and the polynomial $A(x) = A_0 + A_1 x + \cdots + A_n x^n$ is called the *weight enumerator* for C. The minimum distance of this code is the minimum positive value of n, such that $A_n \neq 0$. It follows from the fact that the number of codeword with the minimum weight will be the first coefficient to appear after the first term.

Example 6.1.10 Let us consider the weight enumerator of the code $B_2(6, 3)$ in which is

$$1 + 30x^8 + 12x^{10} + 240x^{12} + 120x^{13} + 120x^{14}$$
$$+144x^{15} + 30x^{16} + 20x^{18} + 12x^{20}.$$

The minimum distance of this code is 8, which is the minimum positive power of x.

Investigation of Boolean codes over finite fields of small characteristics $< n$ is one of the main task of the thesis.

Our results are shown in the following tables.

Minimum Distance of $B_k(n, p)$

(n=5) $p \diagdown k$	0	1	2	3	4
2	2	3	4	5	0
3	2	4	10	0	0
5	2	4	0	0	0
7	2	4	0	0	0
11	2	4	0	0	0

(n=6) $p \diagdown k$	0	1	2	3	4	5
2	2	3	4	5	6	0
3	2	4	8	15	0	0
5	2	4	8	0	0	0
7	2	4	8	0	0	0
11	2	4	8	0	0	0

(n=7) $p \diagdown k$	0	1	2	3	4	5	6
2	2	3	4	5	6	7	0
3	2	4	8	15	21	0	0
5	2	4	8	0	0	0	0
7	2	4	≤ 8	0	0	0	0
11	2	4	≤ 8	0	0	0	0

(n=8) $p \diagdown k$	0	1	2	3	4	5	6	7
2	2	3	4	5	6	7	8	0
3	2	4	8	15	21	28	0	0
5	2	4	≤ 8	15	0	0	0	0
7	2	4	8	≤ 16	0	0	0	0
11	2	4	8	0	0	0	0	0

The entries in the tables gives the exact minimum distance constructed from the weight enumerator and the probabilistic minimum distances shown by the inequality sign.

The next table show more results in the case when $p = 3$ for $n > 8$. The entries ?? corresponds to the fact that we could not compute, it takes a very long time. The empty entries implies that there is no such level for that particular n.

Minimum Distance of $B_k(n, 3)$ for $n \geq 9$

$n \diagdown k$	0	1	2	3	4	5	6	7	8	9	10	11
9	2	4	8	15	21	28	36	0	0	0		
10	2	4	$\leq$8	15	21	28	36	45	0	0	0	
11	2	4	$\leq$8	$\leq$15	??	??	36	45	55	0	0	0

In [27] Tolhuizen and van Lint found that the minimum distance of the codes generated by the matrix $V_k(\mathcal{B}_n)$ over $GF(2)$ is $k + 1$.

The next general result is one of the observed pattern in the thesis.

Let $d_k(B_k(n, p))$ be the minimum distance of the code $B_k(n, p)$.

Proposition 6.1.11 *For every field of characteristics p,*

$$d_k(B_k(n, p)) \leq 2^{k+1} \quad \textit{if} \quad 2(k + 1) \leq n.$$

Proof Let $S = \{s_1, s_2, \ldots, s_n\}$ be a set with n elements. Let $A = \{s_{\alpha_1}, s_{\alpha_2}, \ldots, s_{\alpha_k}\}$ be a k-subset of S. We associate with such set A the monomial

$$p(A) = x_{\alpha_1} x_{\alpha_2} \ldots x_{\alpha_k} \quad \in \mathbb{F}[x_1, x_2, \ldots, x_n]$$

where $x_1, x_2, \ldots x_n$ are indeterminates.

Let X be the vector space over $\mathbb{F}$ spanned by all the monomials $p(A)$

$$X = \langle p(A) : A \subseteq S, |A| = k \rangle.$$

Thus, elements of X are all linear combinations of the monomials $p(A)$:
if $f \in X$ then

$$f = \sum_{A \subseteq S, |A| = k} c_A p(A), \quad c_A \in \mathbb{F}.$$

Similarly, let Y be another vector space, spanned by the monomials $p(B)$, where B runs through all $(k + 1)$-subsets of S

$$Y = \langle p(B) : B \subseteq S, |B| = k + 1 \rangle.$$

It follows from basic properties of partial derivatives that the differential operator

$$\partial = \frac{\partial}{\partial x_1} + \frac{\partial}{\partial x_2} + \cdots + \frac{\partial}{\partial x_n}$$

acts from Y to X and is linear. Evidently, $V_{k,k+1}$ is exactly the matrix of ∂ with respect to the bases $\{p(A)\}$ and $\{p(B)\}$.

Now, for $2(k+1) \leq n$, consider the polynomial

$$e = (x_{\alpha_1} - x_{\beta_1})(x_{\alpha_2} - x_{\beta_2}) \ldots (x_{\alpha_k} - x_{\beta_k})(x_{\alpha_{k+1}} - x_{\beta_{k+1}}),$$

where α_1, α_2, ..., α_{k+1}, β_1, β_2, ..., β_{k+1} are all distinct: $1 \leq \alpha_i,\ \beta_i \leq n$, then

- $e \in Y$,
- e is a linear combination of 2^{k+1} monomials,
- it follows from the Product Rule for derivative that $\partial(e) = 0$.

Thus e, is a vector of weight 2^{k+1} in the null-space of $V_{k,k+1}$. Since the null-space of $V_{k,k+1}$ contains vectors of weight 2^{k+1}, we have the following inequality for the minimal distance of the code,

$$d_k(C) \leq 2^{k+1}.$$

□

Example 6.1.12 Let $S = \{1,2,3,4,5,6\}$ and A be a 2-elements subset of S, then $A \in \{\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{1,6\},\{2,3\},\{2,4\},\{2,5\},\{2,6\},\{3,4\},$ $\{3,5\},\{3,6\},\{4,5\},\{4,6\},\{5,6\}\}$.

Thus the monomials $p(A)$ are x_1x_2, x_1x_3, x_1x_4, x_1x_5, x_1x_6, x_2x_3, x_2x_4, x_2x_5, x_2x_6, x_3x_4, x_3x_5, x_3x_6, x_4x_5, x_4x_6, x_5x_6.

Let X be the vector space spanned by all monomials $p(A)$, then
$X = \{c_1x_1x_2 + c_2x_1x_3 + \cdots + c_{15}x_5x_6 :\ c_i \in \mathbb{F}\}$.

Similarly let B be a 3-element subset of S. Then
$B \in \{\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,2,6\},\{1,3,4\},\{1,3,5\},\{1,3,6\},\{1,4,5\},$
$\{1,4,6\},\{1,5,6\},\{2,3,4\},\{2,3,5\},\{2,3,6\},\{2,4,5\},\{2,4,6\},\{2,5,6\},$

$\{3,4,5\},\{3,4,6\},\{3,5,6\},\{4,5,6\}\}$.

Thus

$$Y = \sum_{B\subseteq S,|B|=k+1} c_B p(B), \quad c_B \in \mathbb{F}.$$

Let $e = (x_1 - x_2)(x_3 - x_4)(x_5 - x_6)$, then

$$\begin{aligned} e = {} & x_1x_3x_5 - x_1x_3x_6 - x_2x_3x_5 + x_2x_3x_6 - x_1x_4x_5 + x_1x_4x_6 \\ & + x_2x_4x_5 - x_2x_4x_6, \end{aligned}$$

and

$$\begin{aligned} \partial(e) = {} & x_3x_5 - x_3x_6 - x_4x_5 + x_4x_6 + \\ & - x_3x_5 + x_3x_6 + x_4x_5 - x_4x_6 + \\ & + x_1x_5 - x_1x_6 - x_2x_5 + x_2x_6 + \\ & - x_1x_5 + x_1x_6 + x_2x_5 - x_2x_6 + \\ & + x_1x_3 - x_2x_3 - x_1x_4 + x_2x_4 + \\ & - x_1x_3 + x_2x_3 + x_1x_4 - x_2x_4 + \\ & = 0 \end{aligned}$$

hence $e \in Y$. Thus the minimal distance of $B_2(6,p)$ is less or equal to 8.

Note that the condition $2(k+1) \leq n$ is important. Indeed, the polynomial e does not exist if $2(k+1) > n$ as there is not enough indeterminates to construct it. So other methods should be used in this case. It is also possible that $d(B_k(n,p))$ is less than 2^{k+1} for **some** fields.

This result was improved by H. Lefmann [15], who was able to show that the equality holds over fields of characteristics 0:

Theorem 6.1.13 (Lefmann's Theorem) The minimum distance of the code $B_k(n,p)$ over fields of characteristic 0 is 2^{k+1} if $2(k+1) < n$.

The theorem of Lefmann does not include the case of codes over finite fields. It follows from results of Mnukhin and Siemone [22, 23] that the theorem of Lefmann is also valid for finite fields of characteristics $p \geq n$. For fields of characteristics $p < n$, simple examples show that Lefmann's theorem is not valid.

Example 6.1.14 For the case where $n = 8$ and $k = 3$ over $GF(3)$, the minimum distance of the code $B_3(8,3)$ is 15, but not 16 as it should be according to Lefmann's theorem.

We could observe from the tables above that the minimum distance of $B_k(n,p)$ when $2 \leq p < n$ does not follow Lefmann's theorem in particular when $p = 3$.

To explain the observation we will show that there exists a vector v of weight 15 in the code $B_3(8,3)$. Let us construct a vector of weight 15 in the code $B_3(8,3)$ over a field of characteristics 3.

In the Boolean lattice when $n = 8$, there are 56 subsets in L_3 which are listed below:

{ { 1, 2, 3 }, { 1, 2, 4 }, { 1, 2, 5 }, { 1, 2, 6 }, { 1, 2, 7 }, { 1, 2, 8 },
{ 1, 3, 4 }, { 1, 3, 5 }, { 1, 3, 6 }, { 1, 3, 7 }, { 1, 3, 8 }, { 1, 4, 5 },
{ 1, 4, 6 }, { 1, 4, 7 }, { 1, 4, 8 }, { 1, 5, 6 }, { 1, 5, 7 }, { 1, 5, 8 },
{ 1, 6, 7 }, { 1, 6, 8 }, { 1, 7, 8 }, { 2, 3, 4 }, { 2, 3, 5 }, { 2, 3, 6 },
{ 2, 3, 7 }, { 2, 3, 8 }, { 2, 4, 5 }, { 2, 4, 6 }, { 2, 4, 7 }, { 2, 4, 8 },
{ 2, 5, 6 }, { 2, 5, 7 }, { 2, 5, 8 }, { 2, 6, 7 }, { 2, 6, 8 }, { 2, 7, 8 },
{ 3, 4, 5 }, { 3, 4, 6 }, { 3, 4, 7 }, { 3, 4, 8 }, { 3, 5, 6 }, { 3, 5, 7 },
{ 3, 5, 8 }, { 3, 6, 7 }, { 3, 6, 8 }, { 3, 7, 8 }, { 4, 5, 6 }, { 4, 5, 7 },
{ 4, 5, 8 }, { 4, 6, 7 }, { 4, 6, 8 }, { 4, 7, 8 }, { 5, 6, 7 }, { 5, 6, 8 },
{ 5, 7, 8 }, { 6, 7, 8 }}

and there are 70 subset in the fourth level L_4 as shown

{ { 1, 2, 3, 4 }, { 1, 2, 3, 5 }, { 1, 2, 3, 6 }, { 1, 2, 3, 7 }, { 1, 2, 3, 8 },
{ 1, 2, 4, 5 }, { 1, 2, 4, 6 }, { 1, 2, 4, 7 }, { 1, 2, 4, 8 }, { 1, 2, 5, 6 },
{ 1, 2, 5, 7 }, { 1, 2, 5, 8 }, { 1, 2, 6, 7 }, { 1, 2, 6, 8 }, { 1, 2, 7, 8 },
{ 1, 3, 4, 5 }, { 1, 3, 4, 6 }, { 1, 3, 4, 7 }, { 1, 3, 4, 8 }, { 1, 3, 5, 6 },
{ 1, 3, 5, 7 }, { 1, 3, 5, 8 }, { 1, 3, 6, 7 }, { 1, 3, 6, 8 }, { 1, 3, 7, 8 },
{ 1, 4, 5, 6 }, { 1, 4, 5, 7 }, { 1, 4, 5, 8 }, { 1, 4, 6, 7 }, { 1, 4, 6, 8 },
{ 1, 4, 7, 8 }, { 1, 5, 6, 7 }, { 1, 5, 6, 8 }, { 1, 5, 7, 8 }, { 1, 6, 7, 8 },
{ 2, 3, 4, 5 }, { 2, 3, 4, 6 }, { 2, 3, 4, 7 }, { 2, 3, 4, 8 }, { 2, 3, 5, 6 },
{ 2, 3, 5, 7 }, { 2, 3, 5, 8 }, { 2, 3, 6, 7 }, { 2, 3, 6, 8 }, { 2, 3, 7, 8 },
{ 2, 4, 5, 6 }, { 2, 4, 5, 7 }, { 2, 4, 5, 8 }, { 2, 4, 6, 7 }, { 2, 4, 6, 8 },

{ 2, 4, 7, 8 }, { 2, 5, 6, 7 }, { 2, 5, 6, 8 }, { 2, 5, 7, 8 }, { 2, 6, 7, 8 },
{ 3, 4, 5, 6 }, { 3, 4, 5, 7 }, { 3, 4, 5, 8 }, { 3, 4, 6, 7 }, { 3, 4, 6, 8 },
{ 3, 4, 7, 8 }, { 3, 5, 6, 7 }, { 3, 5, 6, 8 }, { 3, 5, 7, 8 }, { 3, 6, 7, 8 },
{ 4, 5, 6, 7 }, { 4, 5, 6, 8 }, { 4, 5, 7, 8 }, { 4, 6, 7, 8 }, { 5, 6, 7, 8 } }

so $V_3(\mathcal{B}_8)$ is a 56×70 matrix.

Let

$v = [00000000000000000000000000011111111110000000000000000000000000000011111]$.

The 1 entries in v corresponds to the following subsets in L_4, the 26th to the 35th and 66th to the 70th subsets which are $[1456]$, $[1457]$, $[1458]$, $[1467]$, $[1468]$, $[1478]$, $[1567]$, $[1568]$, $[1578]$, $[1678]$, $[4567]$, $[4568]$, $[4578]$, $[4678]$, $[5678]$.

It is easy to note that $V_3 v = 0$. Since weight of v is $15 < 16 = 2^4$, this example shows that the result of the previous theorem can be improved.

Now we will generalize this example using the same polynomial technique as above.

Theorem 6.1.15 *If $k + p \leq n$, then*

$$d(B_k(n,p)) \leq \begin{pmatrix} k+p \\ p-1 \end{pmatrix}.$$

Proof We keep notations of the previous proof. Let $B \subseteq S$ be any $(k+p)$-subset of S, where $k + p \leq n$. Let $l = \partial^{p-1}(p(B))$. Then

$$l = (p-1)! \sum_{A \subseteq B,\, |A|=k+1} p(A)$$

and the weight of l is $\begin{pmatrix} k+p \\ p-1 \end{pmatrix}$.

Indeed, the number of $k+1$-subsets A in $(k+p)$-subsets B is

$$\begin{pmatrix} k+p \\ k+1 \end{pmatrix} = \begin{pmatrix} k+p \\ k+p-k-1 \end{pmatrix} = \begin{pmatrix} k+p \\ p-1 \end{pmatrix}.$$

Now,

$$\partial l = \partial(\partial^{p-1}(B)) = \partial^p(B) = p! \sum_{X \subset B,\, |X|=k} p(X).$$

Since we are working over a field $\mathbb{F}$ of characteristics p, we have $p! = 0$ in $\mathbb{F}$ and so

$$\partial l = 0.$$

Thus, l corresponds to a vector of weight $\binom{k+p}{p-1}$ if $k+p \leq n$ is the null space of the matrix $V_k(\mathcal{B}_n)$. So

$$d(B_k(n,p)) \leq \begin{pmatrix} k+p \\ p-1 \end{pmatrix} \quad \text{if} \quad k+p \leq n.$$

□

Example 6.1.16 Let $\mathbb{F}$ be a field of characteristic $p = 3$. Let $n = 8$ and $k = 3$. Then $S = \{1, 2, \ldots, 8\}$. Take any 6-element subset of S, say $B = \{1, 2, \ldots, 6\}$. Then $p(B) = x_1x_2x_3 \ldots x_6$, and

$$\begin{aligned}
l = \quad & \partial^2(x_1x_2x_3x_4x_5x_6) \\
= \quad & \partial(x_2x_3x_4x_5x_6 + x_1x_3x_4x_5x_6 + x_1x_2x_4x_5x_6 + x_1x_2x_3x_5x_6 + x_1x_2x_3x_4x_6 \\
& + x_1x_2x_3x_4x_5) \\
= \quad & x_3x_4x_5x_6 + x_2x_4x_5x_6 + x_2x_3x_5x_6 + x_2x_3x_4x_6 + x_2x_3x_4x_5 \\
& + x_3x_4x_5x_6 + x_1x_4x_5x_6 + x_1x_3x_5x_6 + x_1x_3x_4x_6 + x_1x_3x_4x_5 \\
& + x_2x_4x_5x_6 + x_1x_4x_5x_6 + x_1x_2x_5x_6 + x_1x_2x_4x_6 + x_1x_2x_4x_5 \\
& + x_2x_3x_5x_6 + x_1x_3x_5x_6 + x_1x_2x_5x_6 + x_1x_2x_3x_6 + x_1x_2x_3x_5 \\
& + x_2x_3x_4x_6 + x_1x_3x_4x_6 + x_1x_2x_4x_6 + x_1x_2x_3x_6 + x_1x_2x_3x_4 \\
& + x_2x_3x_4x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_5 + x_1x_2x_3x_5 + x_1x_2x_3x_4 \\
= \quad & 2(x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_3x_6 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_2x_3x_4x_5 \\
& + x_1x_2x_4x_6 + x_1x_3x_4x_6 + x_2x_3x_4x_6 + x_1x_2x_5x_6 + x_1x_3x_5x_6 + x_2x_3x_5x_6 \\
& + x_1x_4x_5x_6 + x_2x_4x_5x_6 + x_3x_4x_5x_6) \\
= \quad & 2! \sum p(A), \quad \text{where } A \text{ is a 4-element subsets of } B.
\end{aligned}$$

The theorem of Lefmann also holds for finite fields of large characteristic. The next result follows from the results of [23]:

$$d(B_k(n,p)) = 2^{k+1} \text{ if } 2(k+1) \leq n \text{ and } p = 0 \text{ or } p \geq n.$$

Here we state an improved version as a conjecture:

Conjecture 6.1.17

$$d(B_k(n,p)) = \begin{cases} 2^{k+1}, & \text{if } 2(k+1) \leq n \text{ and } p \leq k+2 \text{ ;} \\ \binom{k+p}{p-1}, & \text{if } 2(k+1) > n \text{ and } k+p \leq n \end{cases} \tag{6.1}$$

6.2 Codes related to the lattice $\mathbf{m}^q$, $m \geq 3$

We have studied properties of Boolean codes. We now investigate properties of codes related to lattices $\mathbf{m}^q$ where q is any integer greater than 1.

The lattices $\mathbf{m}^q$ has been defined in Section 3.3.2 and we know that $\mathbf{m}^q$ can also be considered as $\mathcal{F}(s^{m-1})$, the lattice of divisors of the integer s^{m-1}, where s is any integer of the form $p_1 p_2 \dots p_q$, where $p_1, p_2, \dots, p_q$ are different prime numbers. Another way to look at $\mathbf{m}^q$ is to consider it as the lattice of subgroups of the cyclic group $\mathbb{Z}_{s^{m-1}}$.

We will call codes associated with such lattices *Divisor codes* and denote it as $F_k(n,p)$ where $n = s^{m-1}$ and $s = p_1 p_2 \dots p_q$.

6.2.1 Lengths

The length of the Boolean codes $B_k(n,p)$ and Divisor codes $F_k(n,p)$ are well known. We should note that the length of such codes are related to the column size of the matrix $V_k(\mathcal{L})$. Therefore it depends on the number of elements in L_{k+1}, the $(k+1)$-level of the lattice $\mathcal{L}$.

In the Boolean case, the number of elements in the k-level is given by the coefficients of the polynomial $(1+x)^n$.

$$\begin{aligned} (1+x)^n &= \binom{n}{0} x^n + \binom{n}{1} x^{n-1} + \binom{n}{2} x^{n-2} + \cdots + 1 \\ &= \sum_{k=0}^{n} \binom{n}{k} x^{n-k}. \end{aligned}$$

Example 6.2.1 The number of elements in the k-level of $\mathcal{B}_3$ is given by the coefficient of the polynomial $(1+x)^3$.

$$\begin{aligned}(1+x)^3 = &\quad \binom{3}{0}x^3 + \binom{3}{1}x^2 + \binom{3}{2}x^1 + 1\\ = &\quad x^3 + 3x^2 + 3x + 1.\end{aligned}$$

So $\mathcal{B}_3$ has 3 levels and 8 total number of elements. The elements are arranged in such a way that there is one element in level 0, three in levels 1 and 2 and only one in level 3 (refer to Example 3.1.7). Thus the length of $B_1(3,p)$ is 3 corresponds to the coefficient $\binom{3}{k+1} = \binom{3}{2}$.

Similarly for Divisor codes $F_k(n,p)$, the number of elements in the k-level of a lattice $\mathbf{m}^q$ which is isomorphic to $\mathcal{F}(s^{m-1})$ can be determined by the coefficient of the polynomial

$$(1 + x + \cdots + x^{m-1})^q = \sum_{i=0}^{q(m-1)} l_i x^i,$$

where l_i is the number of elements in the level i of the lattice $\mathbf{m}^n$.

Example 6.2.2 Let consider the lattice $\mathbf{3}^2$ which is isomorphic to $\mathcal{F}(6^2)$. The number of elements in the k-level of $\mathbf{3}^2$ is given by the coefficient of the polynomial

$$\begin{aligned}(1+x+x^2)^2 = &\quad 1 + x + x^2 + x + x^2 + x^3 + x^2 + x^3 + x^4\\ = &\quad 1 + 2x + 3x^2 + 2x^3 + x^4.\end{aligned}$$

Thus the lattice $\mathbf{3}^2$ has 4 levels and 9 elements. There is one element in level 0, two in levels 1 and 3, three in level 2 and only one in level 4 (refer to Example 3.3.6). Thus the length of $F_3(6^2,p)$ is 3.

The following table shows the number of elements in the k-levels for the given lattices.

The number of elements in the k-th level of lattice $(\mathbf{3}^n)$ for $k \leq n$ and $n < 8$

Lattice$\diagdown$ **k**	0	1	2	3	4	5	6	7	8	9	10	11	12
$\mathbf{3}^2$	1	2	3	2	1								
$\mathbf{3}^3$	1	3	6	7	6	3	1						
$\mathbf{3}^4$	1	4	10	16	19	16	10	4	1				
$\mathbf{3}^5$	1	5	15	30	45	51	45	30	15	5	1		
$\mathbf{3}^6$	1	6	21	50	90	126	141	126	90	50	21	6	1

Let us consider columns $k = 2$ and $k = 3$ of the table. These shows the size of the matrix $V_2(\mathbf{3}^n)$. For instance when $n = 6$, $V_2(\mathbf{3}^6)$ is the matrix of size 21×50. The code $F_2(30030^2, p)$ has length 50 which corresponds to the column size of matrix $V_2(\mathbf{3}^6)$.

The following tables show the number of elements in the k level of $(\mathbf{m}^n)$ for $m = 4$ and 5.

The number of elements in the k-th level of lattice $(\mathbf{4}^n)$ for $n \leq 6$

$Lattice \diagdown \mathbf{k}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathbf{4}^2$	1	2	3	4	3	2	1												
$\mathbf{4}^3$	1	3	6	10	12	12	10	6	3	1									
$\mathbf{4}^4$	1	4	10	20	31	40	44	40	31	20	10	4	1						
$\mathbf{4}^5$	1	5	15	35	65	101	135	155	155	135	101	65	35	15	5	1			
$\mathbf{4}^6$	1	6	21	56	120	216	336	458	546	580	546	458	336	216	120	56	21	6	1

The number of elements in the k-th level of lattice $(\mathbf{5}^n)$ for $n \leq 6$

Lattice$\diagdown$ **k**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
$\mathbf{5}^2$	1	2	3	4	5	4	3	2	1																
$\mathbf{5}^3$	1	3	6	10	15	18	19	18	15	10	6	3	1												
$\mathbf{5}^4$	1	4	10	20	35	52	68	80	85	80	68	52	35	20	10	4	1								
$\mathbf{5}^5$	1	5	15	35	70	121	185	255	320	365	381	365	320	255	185	121	70	35	15	5	1				
$\mathbf{5}^6$	1	6	21	56	126	246	426	666	951	1246	1506	1686	1751	1686	1506	1246	951	666	426	246	126	56	21	6	1

6.2.2 Dimensions and Ranks

The dimensions of Boolean codes are well known as shown by Frankl and Wilson rank theorem and in the nullity theorem. However as far as I know there has been no findings on the dimensions of Divisor codes. Similarly, we could not find general pattern concerning the above but we will produce tables of dimensions and ranks of such codes.

The dimensions of the divisor codes followed by the ranks of their check matrices V_k are presented in the following tables. For instance, the dimension of $F_3(210^2, 3)$ can be read from the second table, third row fifth column which is 6. This is because $n = 210^2 = (2 \times 3 \times 5 \times 7)^2$ and since $n = s^{m-1}$ so we are considering $m = 3$ and $q = 4$. Therefore we should look at the lattice $\mathbf{3^4}$. Similarly, the rank of the check matrix for the code $F_2(60^4, 2)$ is 15, which can be obtained in the fourth table, row 12, column 6.

Dimensions of $F_k(n,p)$

Dimensions of $F_k(n,2)$

$\mathbf{m}^q \diagdown \mathbf{k}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
$\mathbf{3}^2$	1	1	0	0																				
$\mathbf{3}^3$	2	3	1	0	0	0																		
$\mathbf{3}^4$	3	6	6	4	1	0	0	0																
$\mathbf{3}^5$	4	10	15	16	10	4	1	0	0	0														
$\mathbf{3}^6$	5	15	29	41	41	30	15	5	1	0	0	0												
$\mathbf{4}^2$	1	1	1	0	0	0																		
$\mathbf{4}^3$	2	3	4	3	2	1	0	0	0															
$\mathbf{4}^4$	3	6	10	12	12	10	6	3	1	0	0	0												
$\mathbf{4}^5$	4	10	20	31	40	44	40	31	20	10	4	1	0	0	0									
$\mathbf{4}^6$	5	15	35	65	101	135	155	155	135	101	65	35	15	5	1	0	0	0						
$\mathbf{5}^2$	1	1	1	1	0	0	0	0																
$\mathbf{5}^3$	2	3	4	5	3	1	0	0	0	0	0	0												
$\mathbf{5}^4$	3	6	10	15	17	16	12	7	2	0	0	0	0	0	0	0								
$\mathbf{5}^5$	4	10	20	35	51	64	70	66	50	30	50	5	1	0	0	0	0	0	0	0				
$\mathbf{5}^6$	5	15	35	70	120	180	240	286	300	276	220	150	85	40	16	5	1	0	0	0	0	0	0	0

Dimensions of $F_k(n,3)$

$\mathbf{m}^q \diagdown \mathbf{k}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\mathbf{3}^2$	1	1	0	0																
$\mathbf{3}^3$	2	3	2	1	0	0														
$\mathbf{3}^4$	3	6	17	6	3	1	0	0												
$\mathbf{3}^5$	4	10	16	19	16	10	4	1	0	0										
$\mathbf{3}^6$	5	15	30	45	51	45	30	15	5	1	0	0								
$\mathbf{4}^2$	1	1	1	0	0	0														
$\mathbf{4}^3$	2	3	4	10	0	0	0	0	0											
$\mathbf{4}^4$	3	6	10	11	9	4	0	0	0	0	0	0								
$\mathbf{4}^5$	4	10	20	30	36	34	20	1	0	0	0	0	0	0	0					
$\mathbf{4}^6$	5	15	35	64	96	120	120	90	36	2	0	0	0	0	0	0	0	0		
$\mathbf{5}^2$	1	1	1	1	0	0	0	0												
$\mathbf{5}^3$	2	3	4	5	3	1	0	0	0	0	0	0								
$\mathbf{5}^4$	3	6	10	15	17	16	12	5	0	0	0	0	0	0	0	0				
$\mathbf{5}^5$	4	10	20	35	51	64	70	65	46	20	4	1	0	0	0	0	0	0	0	0

Dimensions of $F_k(n,5)$

$\mathbf{m}^q \diagdown \mathbf{k}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\mathbf{3}^2$	1	1	0	0																
$\mathbf{3}^3$	2	3	1	0	0	0														
$\mathbf{3}^4$	3	6	6	3	0	0	0	0												
$\mathbf{3}^5$	4	10	15	15	7	1	0	0	0	0										
$\mathbf{3}^6$	5	15	29	40	37	20	5	1	0	0	0	0								
$\mathbf{4}^2$	1	1	1	0	0	0														
$\mathbf{4}^3$	2	3	4	3	1	0	0	0	0											
$\mathbf{4}^4$	3	6	10	11	10	7	3	1	0	0	0	0								
$\mathbf{4}^5$	4	10	20	25	36	38	30	20	10	4	0	0	0	0	0					
$\mathbf{5}^2$	1	1	1	1	0	0	0	0												
$\mathbf{5}^3$	2	3	4	5	4	3	2	1	0	0	0	0								
$\mathbf{5}^4$	3	6	10	15	18	19	18	15	10	6	3	1	0	0	0	0				
$\mathbf{5}^5$	4	10	20	35	52	68	80	85	80	68	52	35	20	10	4	1	0	0	0	0

Ranks of check matrices for $F_k(n,p)$

Ranks of check matrices for $F_k(n,2)$

$\mathbf{m}^q \diagdown \mathbf{k}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
$\mathbf{3}^2$	1	2	2	1																				
$\mathbf{3}^3$	1	3	6	6	3	1																		
$\mathbf{3}^4$	1	4	10	15	15	10	4	1																
$\mathbf{3}^5$	1	5	15	29	41	41	29	15	5	1														
$\mathbf{3}^6$	1	6	21	49	85	111	111	85	49	21	6	1												
$\mathbf{4}^2$	1	2	3	3	2	1																		
$\mathbf{4}^3$	1	3	6	9	10	9	6	3	1															
$\mathbf{4}^4$	1	4	10	19	28	34	34	28	19	10	4	1												
$\mathbf{4}^5$	1	5	15	34	61	91	115	124	115	91	61	34	15	5	1									
$\mathbf{4}^6$	1	6	21	55	115	201	301	391	445	445	391	301	201	115	55	21	6	1						
$\mathbf{5}^2$	1	2	3	4	4	3	2	1																
$\mathbf{5}^3$	1	3	6	10	15	18	18	15	10	6	3	1												
$\mathbf{5}^4$	1	4	10	20	35	52	68	78	78	68	52	35	20	10	4	1								
$\mathbf{5}^5$	1	5	15	35	70	121	185	254	315	351	351	315	254	185	121	70	35	15	5	1				
$\mathbf{5}^6$	1	6	21	56	126	246	426	665	946	1230	1466	1601	1601	1466	1230	946	665	426	246	126	56	21	6	1

Ranks of check matrices for $F_k(n,3)$

$\mathbf{m}^q \diagdown \mathbf{k}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\mathbf{3}^2$	1	2	2	1																
$\mathbf{3}^3$	1	3	5	5	3	1														
$\mathbf{3}^4$	1	4	9	13	13	9	4	1												
$\mathbf{3}^5$	1	5	14	26	35	35	26	14	5	1										
$\mathbf{3}^6$	1	6	20	45	75	96	96	75	45	20	6	1								
$\mathbf{4}^2$	1	2	3	3	2	1														
$\mathbf{4}^3$	1	3	6	10	12	10	6	3	1											
$\mathbf{4}^4$	1	4	10	20	31	40	40	31	20	10	4	1								
$\mathbf{4}^5$	1	5	15	35	65	101	135	154	135	101	65	35	15	5	1					
$\mathbf{4}^6$	1	6	21	56	120	216	336	456	544	544	456	336	216	120	56	21	6	1		
$\mathbf{5}^2$	1	2	3	4	4	3	2	1												
$\mathbf{5}^3$	1	3	6	10	15	18	18	15	10	6	3	1								
$\mathbf{5}^4$	1	4	10	20	35	52	68	80	80	68	52	35	20	10	4	1				
$\mathbf{5}^5$	1	5	15	35	70	121	185	255	319	361	361	319	255	185	121	70	35	15	5	1

Ranks of check matrices for $F_k(n,5)$

$\mathbf{m}^q \diagdown \mathbf{k}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\mathbf{3}^2$	1	2	2	1																
$\mathbf{3}^3$	1	3	6	6	3	1														
$\mathbf{3}^4$	1	4	10	16	16	10	4	1												
$\mathbf{3}^5$	1	5	15	30	44	44	30	15	5	1										
$\mathbf{3}^6$	1	6	21	50	89	121	121	89	50	21	6	1								
$\mathbf{4}^2$	1	2	3	3	2	1														
$\mathbf{4}^3$	1	3	6	9	11	9	6	3	1											
$\mathbf{4}^4$	1	4	10	20	30	37	37	30	20	10	4	1								
$\mathbf{4}^5$	1	5	15	35	65	97	125	135	125	97	65	35	15	5	1					
$\mathbf{5}^2$	1	2	3	4	4	3	2	1												
$\mathbf{5}^3$	1	3	6	10	14	16	16	14	10	6	3	1								
$\mathbf{5}^4$	1	4	10	20	34	49	62	70	70	62	49	34	20	10	4	1				
$\mathbf{5}^5$	1	5	15	35	69	117	175	235	285	313	313	285	235	175	117	69	35	15	5	1

6.2.3 Weight distributions

We could observe some general patterns in the weight enumerator of the code $F_k(n,p)$. The results will be presented according to the fields.

For the field $GF(2)$, we observe that the codes $F_4(n,2)$ have even weights. For instance, codes $F_4(s^2,2)$ have codewords of even weight greater than and equal to 12. Similarly $F_4(s^3,2)$ and $F_4(s^4,2)$ have codewords of even weight greater than and equal to 8.

Thus we formulate the following conjecture.

Conjecture 6.2.3 *For all n and m, the code $F_4(s^{m-1},2)$ has codewords of even weight (not necessarily all, some even weight codewords can be missed).*

Over the field of $GF(3)$ there are several observations.

First we could observe that in codes $F_2(m^q,3)$ for $n \geq 4$, there exists codewords of all weight larger than 3.

Secondly there exists no codeword of weight 7 in codes $F_3(m^q,3)$ when $m = 3,4$. Similarly in codes $F_4(m^q,3)$ there exists no codeword of weight 10 and 11 for $n \geq 4$.

In the field $GF(5)$, there is no codeword of weight 5 in the code $F_2(m^q,5)$ for $n \leq 6$ and when $m = 3,4,5$. Unfortunately we are not able to state whether the same occur for larger values of m and n, but we could generalize the result as follows:

Conjecture 6.2.4 *For all n and m, the code $F_2(m^q,5)$ over the field $GF(5)$ has no codeword of weight 5.*

6.2.4 Minimum distances

We will now examine the minimum distance of the divisor code $F_k(s^{m-1},p)$. Unfortunately, we have not been able to find previous studies on such codes, hence we base our discussion only on the results we obtained in this thesis.

The minimum distance for the Divisor codes are quite similar to those of the Boolean codes. However, we were only able to generalize results for the case when $m = 3$ over the field $GF(3)$. The following tables show the results.

Minimum Distance of $F_k(s^2, p)$ over GF(p)

$q = 3$ $p \diagdown k$	1	2	3	4
2	3	6	0	0
3	3	5	6	0
5	3	6	1	0
7	3	6	1	0

(q=4) $p \diagdown k$	1	2	3	4	5	6
2	3	4	9	12	0	0
3	3	5	6	9	10	0
5	3	6	9	0	0	0
7	3	6	9	0	0	0

(q=5) $p \diagdown k$	1	2	3	4	5	6	7	8
2	3	4	5	12	16	20	0	0
3	3	5	6	9	10	14	15	0
5	3	6	≤ 9	18	45	0	0	0
7	3	6	??	??	??	??	??	??

(q=6) $p \diagdown k$	1	2	3	4	5	6	7	8	9	10
2	3	4	≤ 8	≤ 12	≤ 15	≤ 20	≤ 25	≤ 30	0	0
3	3	5	≤ 6	≤ 9	≤ 10	≤ 14	≤ 15	20	21	0

The tables are presented in such a way that each table represents a particular class of divisor code and all tables are organized in the same way. For instance, the first table represents a class of divisor code where $m = 3$ and $q = 3$. The first row gives the minimum distance for the code $F_k(30^2, 2)$ for different values of k. Thus the minimum distance of $F_2(30^2, 2)$ is 6. The question marks means that we cannot obtain neither the weight distribution nor the probabilistic minimum distance.

From the tables, we could observe that the minimum distance of codes $F_k(s^2, 3)$ has the following properties: For $3 \leq q \leq 6$ (recall that $s = p_1 p_2 \ldots p_q$, is the product of the first q primes), the minimum distance when $k = 1$ is 3. The next minimum distance, that is when $k = 2$ is obtained by adding 1 to the minimum distance of the previous level. The next minimum distance when $k = 3$ is obtained by adding 2 to the previous minimum distance. The number added to the previous minimum distance is alternated, either 1 or a number which is added previously but increased by 1. In other words the difference between the minimum distances has a pattern

of alternating 1 with the number which increases by 1 that is $1, 2, 1, 3, 1, 4, 1, 5, \ldots$

The following table shows the observation more clearly.

Minimum Distance of $F_k(s^2, 3)$

(m=3) $q \diagdown k$	1	2	3	4	5	6	7	8	9	10
3	3	5	6	0						
4	3	5	6	9	10	0				
5	3	5	6	9	10	14	15	0		
6	3	5	≤ 6	≤ 9	≤ 10	≤ 14	≤ 15	20	21	0

We could generalize this pattern as the following conjecture.

Conjecture 6.2.5 *For every q,*

$$d(F_k(s^2,3)) = \begin{cases} \binom{l+3}{2} & \text{if } k = 2l+1 \\ \binom{l+3}{2} - 1 & \text{if } k = 2l \end{cases}$$

Example 6.2.6 Let consider $F_2(210^2, 3)$, so $k = 2$, thus $l = 1$, then

$$d(F_2(210^2,3)) = \binom{l+3}{2} - 1 = \binom{4}{2} - 1 = 5.$$

Similarly, for the code $F_5(210^2, 3)$ where $k = 5$, thus $l = 2$, then

$$d(F_5(210^2,3)) = \binom{l+3}{2} = \binom{5}{2} = 10.$$

Unfortunately, we could not generalize the results for the cases when $m = 4$ and 5 however, we were able to produce tables of their minimum distances as follows:

Minimum Distance of $F_k(s^3, p)$

(q=2) $p \diagdown k$	1	2	3	4
2	3	4	0	0
3	3	4	0	0
5	3	4	0	0

(q=3) $p \diagdown k$	1	2	3	4	5	6	7
2	3	4	6	8	9	0	0
3	3	4	6	0	0	0	0
5	3	4	10	12	0	0	

(q=4) $p \diagdown k$	1	2	3	4	5	6	7	8	9	10
2	3	4	6	8	9	12	15	16	0	0
3	3	4	6	9	10	0	0	0	0	0
5	3	4	8	12	16	28	31	0	0	0

(q=5) $p \diagdown k$	1	2	3	4	5	6	7	8	9	10	11	12	13
2	3	4	??	≤ 8	≤ 9	12	≤ 15	??	20	24	25	0	0
3	3	4	≤ 6	≤ 9	≤ 10	≤ 14	15	0	0	0	0	0	0
5	3	≤ 4	≤ 8	??	16	??	??	51	61	??	??	0	0

Minimum Distance of $F_k(s^4, p)$

(q=3) $p \diagdown k$	1	2	3	4	5	6	7	8	9	10
2	3	4	5	8	9	0	0	0	0	0
3	3	4	5	10	16	0	0	0	0	0
5	3	4	5	9	12	14	15	0	0	0

(q=4) $p \diagdown k$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	3	4	5	≤ 8	≤ 9	≤ 12	≤ 15	≤ 16	0	0	0	0	0	0
3	3	4	5	≤ 9	≤ 10	≤ 18	25	0	0	0	0	0	0	0
5	3	4	≤ 5	≤ 9	≤ 12	≤ 14	≤ 15	25	31	34	35	0	0	0

6.3 Codes related to subgroup lattices of non-cyclic Abelian Groups

Now we are at the last part of our discussion on Combinatorial codes. We have discussed Boolean codes and Divisor codes. In here we will investigate the properties of codes related to some lattices of subgroups of non-cyclic Abelian groups.

Non-cyclic Abelian groups we study are of the form $(\mathbb{Z}_q)^n$ where q is prime. In

fact we are concentrating mainly on cases where $q = 2, 3$ and $n \leq 6$.

The lattice of subgroups of such groups are well known. Some authors (see [1]) call them lattices of subspaces of n-dimensional vector space over $GF(q)$ (or projective lattices) denoted by $\mathcal{L}_n(q)$. In this thesis we will denote such lattice as $\mathcal{L}(\mathbb{Z}_q^n)$.

Example 6.3.1 Let consider the lattice when $q = 2$ and $n = 3$, we are talking about the lattice $\mathcal{L}(\mathbb{Z}_2^3)$ or $\mathcal{L}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$ which is shown in Example 3.3.8.

We will call codes associated with such lattices *projective codes* denoted $C_k(\mathbb{Z}_q^n, p)$ where q and p are primes.

6.3.1 Lengths

The length of projective codes $C_k(\mathbb{Z}_q^n, p)$ is well known. Just like Boolean and Divisor codes, it depends on $|\mathcal{L}_{k+1}|$, the number of elements in the $k+1$-level of the lattice $\mathbb{Z}_q^n$.

It is well known [1] that $|\mathcal{L}_k|$ can be calculated by the following formula:

$$|\mathcal{L}_k| = \binom{n}{k}_q := \frac{[n]_q \times [n-1]_q \times \cdots \times [n-k+1]_q}{[k]_q \times [k-1]_q \times \cdots \times [1]_q}$$

where $[i]_q := 1 + q + q^2 + \cdots + q^{i-1}$ and $\binom{n}{k}_q = 0$ if $k < 0$ or $k > n$

Example 6.3.2 Let consider the code $C_1(\mathbb{Z}_2^3, p)$. The lattice $\mathcal{L}(\mathbb{Z}_2^3)$ is given in the example above. The length of $C_1(\mathbb{Z}_2^3)$ is the number of elements in level 2, $|L_2|$, of the lattice $\mathcal{L}(\mathbb{Z}_2^3)$. $|L_2|$ can be determined as follows:

In this case $k = 2$, $n = 3$ and $q = 2$ so

$$|L_2| = \binom{3}{2}_2 = \frac{[3]_2}{[1]_2} = \frac{1 + 2 + 2^2}{2^0} = 7.$$

This means that the length of $C_1(\mathbb{Z}_2^3, p)$ is 7.

The tables below shows the number of elements in the k-level of the subgroup lattice of the given group G.

The number of elements in the k-th level of lattice $\mathcal{L}(G)$ where $G = \mathbb{Z}_q^n$.

Group $\setminus$ **k**	0	1	2	3	4	5	6
$\mathbb{Z}_2^3$	1	7	7	1			
$\mathbb{Z}_2^4$	1	15	35	15	1		
$\mathbb{Z}_2^5$	1	31	155	155	31	1	
$\mathbb{Z}_2^6$	1	63	651	1395	651	63	1
$\mathbb{Z}_3^3$	1	13	13	1			
$\mathbb{Z}_3^4$	1	40	130	40	1		
$\mathbb{Z}_3^5$	1	121	1210	1210	121	1	

The table is interpreted in the same way as in the previous codes. For instance, the length of $C_1(\mathbb{Z}_3^3, p)$ is 13. This code is generated from level 1 and 2 of the lattice $\mathcal{L}_3(3)$ thus $V_{3,4}(\mathcal{L}(\mathbb{Z}_3^3))$ is a 13×13 matrix as shown in columns 3 and 4, row 5 of the table. We refer to the column size of the matrix as the length of the code because we are dealing with the null-space codes. Note that such lengths do not depend on the field p.

6.3.2 Dimensions and Ranks

In general it is known that dimensions of codes are depending on the rank of the generator matrix $V_{k,l}(\mathcal{L}(G))$. Ranks for such matrices over $GF(p)$ are well known for cases when $p \neq q$

The rank of such matrices over rational fields $\mathbb{Q}$ was studied by Kantor [13] who showed that they have full ranks. Cases where $p = r$ where r does not divide q has also been considered by Frumkin and Yakir [9].

The most interesting and mysterious case is when $p = q$. Xiang [32] claims that ranks of such matrices are q-analog of the Frankl- Wilson rank formula. However, there are some special cases that has been considered. Hamada produce the rank of $V_{1,l}\mathcal{L}(\mathbb{Z}_q^n)$ over $GF(q)$ where $1 < l \leq n$ in the Hamada's formula. It is then

extended by Chandler, Sin and Xiang who showed that

$$rank_2 V_{1,2}(\mathcal{L}(\mathbb{Z}_q^n)) = 1 + \left(\frac{9+\sqrt{17}}{2}\right)^t + \left(\frac{9-\sqrt{17}}{2}\right)^t.$$

Xiang [32] extends it further and states that

$$rank_p(V_{1,2}(\mathcal{L}^4_{p^t})) = 1 + \alpha_1^t + \alpha_2^t,$$

where

$$\alpha_1, \alpha_2 = \frac{p(p+1)^2}{4} \pm \frac{p(p+1)(p-1)}{12}\sqrt{17}.$$

As far as I know it is still an unsolved problem.

In this research we study the dimensions of a few of such codes $C_{k,l}(\mathbb{Z}_q^n, p)$ where $p = q$. Unfortunately we are not able to produce the general pattern but we managed to produce tables of dimensions of such codes and ranks of matrices $V_{k,k+1}\mathcal{L}(\mathbb{Z}_q^n)$ as shown below.

Dimensions

Dimensions of $C_k(\mathbb{Z}_q^n, 2)$

Group $(\mathbb{Z}_q^n) \setminus$ **k**	0	1	2	3	4	5
$\mathbb{Z}_2^3$	6	3	0			
$\mathbb{Z}_2^4$	14	24	4	0		
$\mathbb{Z}_2^5$	30	129	79	5	0	
$\mathbb{Z}_2^6$	62	594	974	230	6	0
$\mathbb{Z}_3^3$	12	1	0			
$\mathbb{Z}_3^4$	39	91	1	0		
$\mathbb{Z}_3^5$	120	1090	120	1	0	

Dimensions of $C_k(\mathbb{Z}_q^n, 3)$

Group $(\mathbb{Z}_q^n) \setminus \mathbf{k}$	0	1	2	3	4	5
$\mathbb{Z}_2^3$	6	1	0			
$\mathbb{Z}_2^4$	14	21	1	0		
$\mathbb{Z}_2^5$	30	125	30	1	0	
$\mathbb{Z}_2^6$	62	589	806	12	1	0
$\mathbb{Z}_3^3$	12	6	0			
$\mathbb{Z}_3^4$	39	100	10	0		
$\mathbb{Z}_3^5$	120	1104	659	15	0	

We were not able to produce the dimension table for $GF(5)$ since we could not run it by the computer. It takes so long to run or else the computer virtual memory is not enough to store the data. For the same reason the rank table for $GF(5)$ is not produced.

Ranks

$V_k(\mathcal{L}(\mathbb{Z}_q^n))$ over $GF(2)$

Group $(\mathbb{Z}_q^n) \setminus \mathbf{k}$	0	1	2	3	4	5
$\mathbb{Z}_2^3$	1	4	1			
$\mathbb{Z}_2^4$	1	11	11	1		
$\mathbb{Z}_2^5$	1	26	76	26	1	
$\mathbb{Z}_2^6$	1	57	421	421	57	1
$\mathbb{Z}_3^3$	1	12	1			
$\mathbb{Z}_3^4$	1	39	39	1		
$\mathbb{Z}_3^5$	1	120	1090	1		

Ranks of $V_k(\mathcal{L}(\mathbb{Z}_q^n))$ over $GF(3)$

Group $(\mathbb{Z}_q^n) \setminus \mathbf{k}$	0	1	2	3	4	5
$\mathbb{Z}_2^3$	1	6	1			
$\mathbb{Z}_2^4$	1	14	14	1		
$\mathbb{Z}_2^5$	1	30	125	30	1	
$\mathbb{Z}_2^6$	1	62	589	589	62	1
$\mathbb{Z}_3^3$	1	7	1			
$\mathbb{Z}_3^4$	1	30	30	1		
$\mathbb{Z}_3^5$	1	106	551	106	1	

6.3.3 Weight distributions

The weight distribution of projective codes was quite hard to construct. These codes contain large number of codewords thus, the construction of weight distribution takes a very long time. However from the collected data we were able to observe a few interesting pattern.

First we could observe that for every level k and $n \leq 6$ the codes $C_k(\mathbb{Z}_2^n, 2)$ has no odd weight codewords. It is not the case over $GF(3)$ and $GF(5)$.

From the observations above we could formulate a conjecture.

Conjecture 6.3.3 For every k, m and n the codes $C_k(\mathbb{Z}_2^n, 2)$, has codewords of only even weight.

Example 6.3.4 For the case when $k = 1$, $n = 4$ and $m = 1$, we are considering the code $C_1(\mathbb{Z}_2^4, 2)$. It is constructed from level 1 and 2 of the lattice $\mathcal{L}(\mathbb{Z}_2^4)$. It has weight enumerator of

$$1 + 105x^4 + 1960x^6 + 21525x^8 + 179648x^{10} + 813645x^{12} + 2283560x^{14} + 3924515x^{16} + 4468800x^{18} + 3155131x^{20} + 1448440x^{22} + 401415x^{24} + 71680x^{26} + 6735x^{28} + 56x^{30}.$$

We were also able to observe that the codes $C_k(\mathbb{Z}_3^n, 3)$ has codewords of weights multiples of 3 for all k and n.

6.3.4 Minimum distances

The minimum distance of the projective codes $C_k(\mathbb{Z}_q^n, p)$ as far as I know is not known. In this study we are considering such codes.

Due to the fact that these codes contain very large number of codewords which shows by the large matrix $V_{k,k+1}(\mathcal{L}(G))$ we were not able to produce much data and that limit our ability to generalize patterns on such codes. However we were able to see that the minimum distance of $C_k(\mathbb{Z}_2^n, 2)$ follows Lefmann's theorem. However this is not observed in the case when $p = 3$.

The minimum distance of a few of such codes are shown in the following tables.

Minimum Distance of $L_k(n(q), 2)$

Group $\mathbb{Z}_q^n \diagdown$ **k**	1	2	3	4
$\mathbb{Z}_2^3$	4			
$\mathbb{Z}_2^4$	4	8		
$\mathbb{Z}_2^5$	4	≤ 8	16	
$\mathbb{Z}_2^6$	≤ 4	≤ 8	≤ 16	≤ 32
$\mathbb{Z}_3^3$	13			
$\mathbb{Z}_3^4$	≤ 8	40		
$\mathbb{Z}_3^5$	≤ 8	≤ 40	121	

Minimum Distance of $C_k(\mathbb{Z}_q^n), 3)$

Lattice $\mathbb{Z}_q^n \diagdown$ **k**	1	2	3	4
$\mathbb{Z}_2^3$	7			
$\mathbb{Z}_2^4$	6	15		
$\mathbb{Z}_2^5$	≤ 6	≤ 15	31	
$\mathbb{Z}_2^6$	≤ 6	≤ 15	≤ 31	≤ 63
$\mathbb{Z}_3^3$	6			
$\mathbb{Z}_3^4$	≤ 6	18		
$\mathbb{Z}_3^5$	≤ 6	≤ 18	??	

Bibliography

[1] Aigner, M., *Combinatorial Theory*, Springer-Verlag Berlin Heidelberg, Germany, 1997.

[2] Assmus, E.F *and* Key, J.D., *Designs and their Codes*, Cambridge University Press, 1992.

[3] Berlekamp, E.R., *Algebraic coding theory*, MacGraw-Hill Inc, 1968.

[4] Britz, T., MacWilliams identities and matroid polynomials, *Electronics Journal of Combinatorics*, **9**(2002), R19.

[5] Brouwer, A.E., *Block Designs*, Chapter 14 in *Handbook in Combinatorics*, vol. 1, Elsiver, 1995, 693–745.

[6] A, Foster A polynomial-time probabilistic algorithm for the minimum distance of an arbitrary linear error -correcting code, Mathematics Honors Report, Spring 2003-2004.

[7] Fraleigh, J.B., *A first course in Abstract Algebra* (7th ed), Pearson Education Inc, 2003.

[8] Frankl, P., Intersection theorems and mod p rank of inclusion matrices, *J. Comb.Theory(A)*, **54**(1990), 85-94.

[9] Frumkin, A *and* Yakir, A., Rank of inclusion matrices and modular representation theory, *Israel J. Math.*, **71**(1990), 309–320.

[10] GAP 4.4, Groups Algorithms Programming, version 4.4 http://www.gap-system.org

[11] GUAVA, http://cadigweb.ew.usna.edu/ wdj/gap/GUAVA/

[12] Humphreys, J.F *and* Prest, M.Y., *Numbers, Groups and Codes* (2nd ed), Cambridge University Press, 2004.

[13] Kantor, W.M., On incidence matrices of finite projective and affine spaces, *Math. Z.*, **124**(1972), 315–318.

[14] Khosrovshahi, G.B., Naserasr, R *and* Tayfeh-Rezaie, B., Ternary trades and their codes, *J. Statist. Plann. Inference* **95**(2001), 237–243.

[15] Lefmann, H., An extremal problem for Graham-Rothschild parameter words. *Combinatorica*, **9**(1989), 153–160.

[16] Lin,S *and* Costello,D.J., *Error Control Coding*(2nd ed), Pearson Prentices Hall, USA, 2004.

[17] Linial, N., *and* Rothschild, B.L., Incidence matrix of subsets-a rank formula, *SIAM J. Algebraic Discr. Meth.*, **2**(1981), 330-340.

[18] Ling, S *and* Xing, C., *Coding Theory: A first course*, Cambridge University Press, 2004.

[19] Ikenaga, Bruce. (2007) *Direct product*[online] Available from: http://Marauder.millersville.edu/ bikenaga/abstractalgebra/product/product.html.

[20] Mnukhin, V.B., The k-orbit reconstruction and the orbit algebra, *Acta Applicandae Mathematicae*, **29**(1992), 83–117.

[21] Mnukhin, V.B., Combinatorial Properties of Partially Ordered Sets and Group Actions, *TEMPUS Lecture Notes in Discrete Mathematics*, **8**, University of East Anglia, Norwich, 1993, 53 pp.

[22] Mnukhin, V.B *and* Siemons, I.J., On modular homology of simplicial complexes: Shellability, *J. Comb. Theory*, **A93** (2001), 350–370.

[23] Mnukhin, V.B *and* Siemons, I.J., On modular homology of simplicial complexes: Saturation, *J. Comb. Theory*, **A98** (2002), 377–394.

[24] Peterson, W.W *and* Weldon, E.J., *Error Correcting Codes*(2nd ed), MIT Press, Massachusetts, 1972.

[25] Pretzel, O., *Error-Correcting Codes and Finite Fields: student edition*, Oxford University Press Inc., New York, 1996.

[26] Smith, K.J.C., On the p-rank of the incidence matrix of points and hyperplanes in finite projective geometry, *J. Comb. Theory*, **7**(1969), 122-129.

[27] Tolhuizen, L *and* van Lint, J.H., On the minimum distance of combinatorial codes, *IEEE Trans. Inf. Theory*, **36**(1990), 922–923.

[28] Weisstein, E.W., *CRC Concise Encyclopedia of Mathematics*, CRC Press LLC, USA, 1991.

[29] Wikipedia, the free encyclopedia [online] Available from:http://en.wikipedia.org/wiki/ Date Accessed:19/05/2008

[30] Wilson, R.M., A diagonal form for the incidence matrices of t-subsets vs k-subsets, *Europ.J.Combin.* **11** (1990), 609-615.

[31] van Lint, J.H., *Codes*, Chapter 16 in *Handbook in Combinatorics*, vol. 1, Elsiver, 1995, 773–807.

[32] Xiang, Q., Modular ranks of Geometric Inclusion Matrices, *ICCM*, **1**, (2007), 348–358.

Appendix A

Results

In here we are presenting raw data collected in the research. There are three set of data, the first is the data on Boolean codes, next is Divisor codes and last is on the Projective codes. They are presented in tables.

The tables have 5 columns, the first column shows the lattice that has been used to generate the code. For the Boolean codes it is the number n which stands for the number of elements used in the Boolean algebra. For instance if $n = 4$ then the lattice used is $\mathcal{B}_4$. For the other sets, Divisor codes and Abelian Codes, the lattice is given.

The second column consists of the number k which stands for the level of the lattice used to form a matrix $V_k(\mathcal{B}_n)$. Say $k = 1$ this means that the matrix is V_1 which is made from levels 1 and 2 of the lattice $\mathcal{B}_n$.

The third column has the size of matrix V_k. The fourth column consists of the rank of the matrix V_k and the last column contains the weight enumerator.

In the tables there are rows which has ?? as the weight enumerator. This means that it is not possible to evaluate the weight distribution and the minimum distance, either it takes so long or not enough virtual memory to store the data.It is for this same reason that the tables were constructed only up to $n \leq 8$ and for only $p = 2, 3$ and 5.

Sometimes the lowest degree of the polynomial is shown. It was in this case where the time taken for the computer to produce the weight distribution was so long or sometimes impossible therefore the minimum distance was then determined. If the

minimum distance has the equality sign then it is calculated using the minimum distance command, where every codeword are compared. If the sign is an inequality then it is calculated using the probabilistic minimum distance where the codeword are randomly chosen and compared. Not all codewords are compared.

The weight enumerator of 1 means that there is only one codeword in the code which is a zero vector.

A.1 Boolean Codes $B_k(n, p)$

The following sets of tables shows the weight enumerator of the Boolean codes $B_k(n, p)$ for $n \leq 8$ and $p = 2, 3, 5$.

A.1.1 Weight enumerator over $GF(2)$

Weight Enumerator Polynomial of $B_k(n, 2)$ for $n \leq 7$

n	**k**	V_k		**Weight Enumerator**
		size	rank	
3	1	(3,3)	2	$1 + x^3$
4	1	(4,6)	3	$1 + 4x^3 + 3x^4$
	2	(6,4)	3	$1 + x^4$
5	1	(5,10)	4	$1 + 10x^3 + 15x^4 + 12x^5 + 15x^6 + 10x^7 + 1x^10$
	2	(10,10)	6	$1 + 5x^4 + 10x^6$
	3	(10,5)	4	$1 + 1x^5$
6	1	(6,15)	5	$1 + 20x^3 + 45x^4 + 72x^5 + 160x^6 + 240x^7 + 195x^8 + 120x^9$ $+96x^{10} + 60x^{11} + 15x^{12}$
	2	(15,20)	10	$1 + 15x^4 + 60x^6 + 240x^8 + 392x^{10} + 240x^{12} + 60x^{14}$ $+15x^{16} + x^{20}$
	3	(20,15)	10	$1 + 6x^5 + 15x^8 + 10x^9$
	4	(15,6)	5	$1 + 1x^6$
7	1	(7,21)	6	$1 + 35x^3 + 105x^4 + 252x^5 + 805x^6 + 1935x^7 + 3255x^8 + 4515x^9 + 5481x^{10}$ $+5481x^{11} + 4515x^{12} + 3255x^{13} + 1935x^{14} + 805x^{15} + 252x^{16} + 105x^{17}$ $+35x^{18} + 1x^{20}$
	2	(21,35)	15	$1 + 35x^4 + 210x^6 + 1750x^8 + 10556x^{10} + 49700x^{12} + 140540x^{14} + 253925x^{16}$ $+277200x^{18} + 190939x^{20} + 91490x^{22} + 28420x^{24} + 3780x^{26} + 30x^{28}+$
	3	(35,35)	20	$1 + 21x^5 + 105x^8 + 70x^9 + 105x^{10} + 420x^{11} + 735x^{12} + 1295x^{13} + 2040x^{14}$ $+2877x^{15} + 3990x^{16} + 4725x^{17} + 4725x^{18} + 3990x^{19} + 2877x^{20} + 2040x^{21}$ $+1295x^{22} + 735x^{23} + 420x^{24} + 105x^{25} + 70x^{26} + 105x^{27} + 21x^{28} + 1x^{33}$
	4	(35,21)	15	$1 + 7x^6 + 21x^{10} + 35x^{12}$
	5	(21,7)	6	$1 + x^7$

Weight Enumerator Polynomial of $B_k(n,2)$ for $n=8$

n	**k**	V_k size	V_k rank	**Weight Enumerator**
8	1	(8,28)	7	$1+56x^3+210x^4+672x^5+2800x^6+9320x^7+24087x^8+53760x^9$ $+103936x^{10}+169008x^{11}+235228x^{12}+289856x^{13}+315360x^{14}+295120x^{15}$ $+236831x^{16}+166656x^{17}+103040x^{18}+54040x^{19}+23730x^{20}+9248x^{21}+3248x^{22}$ $+840x^{23}+105x^{24}$
	2	(28,56)	21	$1+70x^4+560x^6+7315x^8+76272x^{10}+735980x^{12}+6061360x^{14}$ $+39938241x^{16}+198847600x^{18}+744783578x^{20}+2048051040x^{22}+4172993195x^{24}$ $+6328509152x^{26}+7279729640x^{28}+6328509152x^{30}+4172993195x^{32}$ $+2048051040x^{34}+744783578x^{36}+198847600x^{38}+39938241x^{40}+6061360x^{42}$ $+735980x^{44}+76272x^{46}+7315x^{48}+560x^{50}+70x^{52}+1x^{56}$
	3	(56,70)	35	$1+56x^5+420x^8+280x^9+1120x^{10}+3360x^{11}+5880x^{12}+18760x^{13}$ $+38720x^{14}+83328x^{15}+227815x^{16}+521640x^{17}+1170400x^{18}+2675680x^{19}$ $+5888624x^{20}+12792240x^{21}+26602240x^{22}+52147200x^{23}+99585990x^{24}$ $+184521456x^{25}+319354560x^{26}+,514964800x^{27}+796914000x^{28}+1181771920x^{29}$ $+1626527616x^{30}+2077152000x^{31}+2538466735x^{32}+2968317520x^{33}+3220835520x^{34}$ $+3245622720x^{35}+3137068480x^{36}+2913120280x^{37}+2522428160x^{38}+2038364160x^{39}$ $+1587159448x^{40}+1190131320x^{41}+831446240x^{42}+539892640x^{43}+334742520x^{44}$ $+196892584x^{45}+105689920x^{46}+51166080x^{47}+22629705x^{48}+8941960x^{49}$ $+2948960x^{50}+753760x^{51}+136080x^{52}+13440x^{53}+30x^{56}$
	4	(70,56)	35	$1+28x^6+168x^{10}+490x^{12}+840x^{14}+5306x^{16}+12460x^{18}$ $+46872x^{20}+98840x^{22}+272965x^{24}+346416x^{26}+528380x^{28}$ $+346416x^{30}+272965x^{32}+98840x^{34}+46872x^{36}+12460x^{38}$ $+5306x^{40}+840x^{42}+490x^{44}+168x^{46}+28x^{50}+1x^{56}$
	5	(56,28)	21	$1+8x^7+28x^{12}+56x^{15}+35x^{16}$
	6	(28,8)	7	$1+1x^8$

Weight Enumerator Polynomial of $B_k(n,2)$ for $n=9$

n	**k**	V_k size	V_k rank	**Weight Enumerator**
9	1	(9,36)	8	$1+84x^3+378x^4+1512x^5+7770x^6+33120x^7$ $+115983x^8+361396x^9+993636x^{10}+2361996x^{11}+4900077x^{12}$ $+9018576x^{13}+14816070x^{14}+21736296x^{15}+28533897x^{16}$ $+33595884x^{17}+35482104x^{18}+33595884x^{19}+28533897x^{20}$ $+21736296x^{21}+14816070x^{22}+9018576x^{23}+4900077x^{24}+2361996x^{25}$ $+993636x^{26}+361396x^{27}+115983x^{28}+33120x^{29}+7770x^{30}$ $+1512x^{31}+378x^{32}+84x^{33}+1x^{36}$
	2	(36,84)	28	$1+126x^4+1260x^6+22995x^8+340620x^{10}+5014800x^{12}$ $+68761080x^{14}861561729x^{16}+9606055704x^{18}+91683519690x^{20}$ $+733113295236x^{22}+4830446860155x^{24}+25982067176100x^{26}$ $+113525040900900x^{28}+402784301447360x^{30}+1163909373880995x^{32}$ $+2751839686874880x^{34}+5348325012105810x^{36}+8577775446823380x^{38}$ $+11381602525960905x^{40}+12508981304986260x^{42}+11388218135764680x^{44}$ $+8581892924897880x^{46}+5346164438692035x^{48}+2748291755522040x^{50}$ $+1163036254691430x^{52}+403715654278300x^{54}+114286041282465x^{56}$ $+26124400548540x^{58}+4739818974660x^{60}+662053780080x^{62}$ $+67356719640x^{64}+4498366320x^{66}+157227840x^{68}+1591200x^{70}$ $+840x^{72}$
	3	(84,126)	56	$1+ax^d+\cdots+bx^m$: where $d\leq 5$
	4	(126,126)	70	$1+ax^d+\cdots+bx^m$: where $d\leq 6$
	5	(126,84)	56	$1+36x^7+252x^{12}+378x^{14}+504x^{15}+315x^{16}+1512x^{17}$ $+3864x^{19}+7938x^{20}+6300x^{21}+14112x^{22}+18900x^{23}$ $+39060x^{24}+74592x^{25}+110880x^{26}+186256x^{27}+294525x^{28}$ $+491400x^{29}+799470x^{30}+1302840x^{31}+2144772x^{32}$ $+3175200x^{33}+4632516x^{34}+6741360x^{35}+9225090x^{36}$ $+12354804x^{37}+15922200x^{38}+19123776x^{39}+21838383x^{40}$ $+23627520x^{41}+24157944x^{42}+23627520x^{43}+21838383x^{44}$ $+19123776x^{45}+15922200x^{46}+12354804x^{47}+9225090x^{48}$ $+6741360x^{49}+4632516x^{50}+3175200x^{51}+2144772x^{52}$ $+1302840x^{53}+799470x^{54}+491400x^{55}+294525x^{56}+186256x^{57}$ $+110880x^{58}+74592x^{59}+39060x^{60}+18900x^{61}+14112x^{62}$ $+6300x^{63}+7938x^{64}+3864x^{65}+1512x^{67}+315x^{68}+504x^{69}$ $+378x^{70}+252x^{72}+36x^{77}+x^{84}$
	6	(84,36)	28	$1+9x^8+36x^{14}+84x^{18}+126x^{20}$
	7	(36,9)	8	$1+x^9$

Weight Enumerator Polynomial of $B_k(n,2)$ for $n = 10$

n	**k**	V_k size	V_k rank	**Weight Enumerator**
10	1	(10,45)	9	$1 + 120x^3 + 630x^4 + 3024x^5 + 18480x^6 + 96120x^7 + 425565x^8 + 1711360x^9$ $+6183936x^{10} + 19766880x^{11} + 56133000x^{12} + 142712640x^{13} + 326312640x^{14}$ $+673842144x^{15} + 1262570130x^{16} + 2153756160x^{17} + 3350995200x^{18} + 4762250640x^{19}$ $+6191313156x^{20} + 7371750240x^{21} + 8041963680x^{22} + 8039892240x^{23} + 7368316530x^{24}$ $+6190168320x^{25} + 4763082240x^{26} + 3352192480x^{27} + 2154869640x^{28} + 1263113280x^{29}$ $+673406400x^{30} + 325553760x^{31} + 142407405x^{32} + 56232960x^{33} + 19918080x^{34}$ $+6262200x^{35} + 1735030x^{36} + 421200x^{37} + 85680x^{38} + 12600x^{39} + 945x^{40}$
	2	(45,120)	36	$1 + ax^d + \cdots + bx^m$: where $d \leq 4$
	3	(120,210)	84	$1 + ax^d + \cdots + bx^m$: where $d \leq 5$
	4	(210,252)	126	$1 + ax^d + \cdots + bx^m$: where $d \leq 6$
	5	(252,210)	126	$1 + ax^d + \cdots + bx^m$: where $d \leq 7$
	6	(210,120)	84	$1 + ax^d + \cdots + bx^m$: where $d \leq 8$
	7	(20,45)	36	$1 + 10x^9 + 45x^{16} + 120x^{21} + 210x^{24} + 126x^{25}$
	8	(45,10)	9	$1 + x^{10}$

Weight Enumerator Polynomial of $B_k(n,2)$ for $n = 11$

n	**k**	V_k size	V_k rank	**Weight Enumerator**
11	1	(11,55)	10	$1 + 165x^3 + 990x^4 + 5544x^5 + 39270x^6 + 241230x^7 + 1292445x^8$ $+6384070x^9 + 28757916x^{10} + 116657865x^{11} + 426896085x^{12}$ $+1414038780x^{13} + 4249310670x^{14} + 11623307289x^{15} + 29060903520x^{16}$ $+66663330030x^{17} + 140716227960x^{18} + 273992550040x^{19} + 493156386261x^{20}$ $+821944221120x^{21} + 1270350223020x^{22} + 1822754616705x^{23} + 2430364889370x^{24}$ $+3013600549740x^{25} + 3477122031240x^{26} + 3734593183090x^{27} + 3734593183090x^{28}$ $+3477122031240x^{29} + 3013600549740x^{30} + 2430364889370x^{31} + 1822754616705x^{32}$ $+1270350223020x^{33} + 821944221120x^{34} + 493156386261x^{35} + 273992550040x^{36}$ $+140716227960x^{37} + 66663330030x^{38} + 29060903520x^{39} + 11623307289x^{40}$ $+4249310670x^{41} + 1414038780x^{42} + 426896085x^{43} + 116657865x^{44} + 28757916x^{45}$ $+6384070x^{46} + 1292445x^{47} + 241230x^{48} + 39270x^{49} + 5544x^{50} + 990x^{51}$ $+165x^{52} + x^{53}$
	2	(55,165)	45	$1 + ax^d + \cdots + bx^m$: where $d \leq 4$
	3	(165,330)	120	$1 + ax^d + \cdots + bx^m$: where $d \leq 5$
	4	(330,462)	210	$1 + ax^d + \cdots + bx^m$: where $d \leq 6$
	5	(462,462)	252	$1 + ax^d + \cdots + bx^m$: where $d \leq 7$
	6	(462,330)	210	$1 + ax^d + \cdots + bx^m$: where $d \leq 8$
	7	(330,165)	120	$1 + ax^d + \cdots + bx^m$: where $d \leq 9$
	8	(165,55)	45	$1 + 11x^{10} + 55x^{18} + 165x^{24} + 330x^{28} + 462x^{30}$
	9	(55,11)	10	$1 + x^{11}$

A.1.2 Weight Enumerator over $GF(3)$

Weight Enumerator Polynomial of $B_k(n,3)$ for $n \leq 7$

n	**k**	V_k size	V_k rank	**Weight Enumerator**
3	1	(3,3)	3	1
4	1	(4,6)	4	$1 + 6x^4 + 2x^6$
	2	(6,4)	4	1
5	1	(5,10)	5	$1 + 30x^4 + 60x^6 + 120x^7 + 20x^9 + 12x^{10}$
	2	(10,10)	9	$1 + 2x^{10}$
	3	(10,5)	5	1
6	1	(6,15)	6	$1 + 90x^4 + 450x^6 + 1260x^7 + 2250x^8 + 3500x^9 + 4122x^{10} + 3870x^{11}$ $+2580x^{12} + 1170x^{13} + 360x^{14} + 30x^{15}$
	2	(15,20)	14	$1 + 30x^8 + 12x^{10} + 240x^{12} + 120x^{13} + 120x^{14} + 144x^{15} + 30x^{16}$ $+20x^{18} + 12x^{20}$
	3	(20,15)	14	$1 + 2x^{15}$
	4	(15,6)	6	1
7	1	(7,21)	7	$1 + 210x^4 + 1960x^6 + 6300x^7 + 24570x^8 + 66290x^9 + 165732x^{10}$ $+335160x^{11} + 550270x^{12} + 760200x^{13} + 863190x^{14} + 819560x^{15}$ $+609714x^{16} + 362880x^{17} + 155190x^{18} + 49980x^{19} + 10710x^{20} + 1052x^{21}$
	2	(21,35)	20	$1 + 210x^8 + 42x^{10} + 2940x^{12} + 2100x^{13} + 9900x^{14} + 46368x^{15}$ $+52290x^{16} + 95760x^{17} + 572460x^{18} + 402990x^{19} + 692496x^{20}$ $+2328900x^{21} + 1189650x^{22} + 1294020x^{23} + 3339000x^{24} + 1173564x^{25}$ $+928620x^{26} + 1512560x^{27} + 346380x^{28} + 162540x^{29} + 167496x^{30}$ $+21630x^{31} + 5040x^{32} + 1890x^{33} + 60x^{35}$
	3	(35,35)	29	$1 + 14x^{15} + 42x^{20} + 210x^{22} + 210x^{23} + 140x^{24} + 42x^{25} + 70x^{30}$
	4	(35,21)	20	$1 + 2x^{21}$
	5	(21,7)	7	1

Weight Enumerator Polynomial of $B_k(n,3)$ for $n=8$

n	**k**	V_k size	V_k rank	**Weight Enumerator**
8	1	(8,28)	8	$1+420x^4+6300x^6+21840x^7+139860x^8+510720x^9+2036832x^{10}$ $+6645240x^{11}+19021716x^{12}+46804632x^{13}+100430280x^{14}+187074720x^{15}$ $+303074142x^{16}+429460920x^{17}+524203428x^{18}+551702760x^{19}+497514150x^{20}$ $+378481896x^{21}+240169524x^{22}+125783280x^{23}+52414110x^{24}+16820160x^{25}$ $+3882060x^{26}+548576x^{27}+36834x^{28}$
	2	(28,56)	27	$1+ax^d+\cdots+bx^m$: where $d\leq 8$
	3	(56,70)	49	$1+56x^{15}+210x^{16}+336x^{20}+1680x^{22}+1680x^{23}+7840x^{24}+10416x^{25}+23520x^{26}$ $+26880x^{27}+67440x^{28}+158340x^{29}+347424x^{30}+564480x^{31}+1862280x^{32}$ $+3924760x^{33}+7483560x^{34}+15824088x^{35}+31464300x^{36}+53355120x^{37}$ $+103527900x^{38}+159891480x^{39}+251780592x^{40}+379246140x^{41}+509283880x^{42}$ $+681045120x^{43}+838313280x^{44}+913567704x^{45}+1059026220x^{46}+1043730240x^{47}$ $+983631600x^{48}+921012960x^{49}+776064198x^{50}+581894600x^{51}+437847900x^{52}$ $+305809980x^{53}+185958920x^{54}+105431424x^{55}+60028800x^{56}+28401240x^{57}$ $+11711700x^{58}+5047560x^{59}+2260664x^{60}+477120x^{61}+192780x^{62}+27720x^{63}$ $+13440x^{64}+0x+1890x^{66}+1680x^{67}+0x+0x+60x^{70}$
	4	(70,56)	49	$1+16x^{21}+56x^{30}+1372x^{36}+560x^{39}+112x^{45}+70x^{48}$
	5	(56,28)	27	$1+2x^{28}$
	6	(28,8)	8	1

A.1.3 Weight enumerator over $GF(5)$

Weight Enumerator Polynomial of $B_k(n,5)$ for $n \leq 7$

n	**k**	V_k size	V_k rank	**Weight Enumerator**
3	1	(3,3)	3	1
4	1	(4,6)	4	$1+12x^4+12x^6$
	2	(6,4)	4	1
5	1	(5,10)	5	$1+60x^4+240x^6+720x^7+1080x^8+600x^9+424x^{10}$
	2	(10,10)	10	1
6	1	(6,15)	6	$1+180x^4+1500x^6+6840x^7+23820x^8+88200x^9+204252x^{10}$ $+359100x^{11}+493560x^{12}+446580x^{13}+261720x^{14}+67372x^{15}$
	2	(15,20)	15	$1+60x^8+240x^{12}+720x^{14}+1080x^{16}+600x^{18}+424x^{20}$
	3	(20,15)	15	1
7	1	(7,21)	7	$1+420x^4+5880x^6+32760x^7+176820x^8+994140x^9+4689384x^{10}$ $+18699240x^{11}+63216580x^{12}+175008960x^{13}+400576860x^{14}+744926728x^{15}$ $+1117182780x^{16}+1316657160x^{17}+1171705220x^{18}+738139080x^{19}+294852012x^{20}$ $+56651600x^{21}$
	2	(21,35)	21	$1+420x^8+5040x^{12}+38280x^{14}+30240x^{15}+37800x^{16}+446880x^{17}$ $+1061760x^{18}+1942080x^{19}+7158592x^{20}+20260800x^{21}$ $+50621760x^{22}+122380440x^{23}+254953440x^{24}+436711968x^{25}$ $+672249200x^{26}+877671480x^{27}+1010111040x^{28}+980421960x^{29}$ $+788511696x^{30}+512173200x^{31}+252651840x^{32}+90164340x^{33}$ $+21443240x^{34}+2468128x^{35}$
	3	(35,35)	35	1

Weight Enumerator Polynomial of $B_k(n,5)$ for $n=8$

n	**k**	V_k size	V_k rank	**Weight Enumerator**
8	1	(8,28)	8	$1+840x^4+17640x^6+110880x^7+823200x^8+5859840x^9+39709040x^{10}$ $+239069040x^{11}+1313753280x^{12}+6407914800x^{13}+27453007440x^{14}$ $+102825829120x^{15}+334585658540x^{16}+944951768880x^{17}+2309130321400x^{18}$ $+4859788852240x^{19}+8746914835260x^{20}+13330607140240x^{21}+16969240573880x^{22}$ $+17705909340000x^{23}+14752109617140x^{24}+9440888104704x^{25}+4359018452040x^{26}$ $+1291892318080x^{27}+184108563100x^{28}$
	2	(28,56)	28	$1+ax^d+\cdots+bx^m$: where $d\leq 8$
	3	(56,70)	56	$1+420x^{16}+5040x^{24}+38280x^{28}+30240x^{30}+37800x^{32}0,446880x^{34}$ $+1061760x^{36}+1942080x^{38}+7158592x^{40}+20260800x^{42}+50621760x^{44}$ $+122380440x^{46}+254953440x^{48}+436711968x^{50}+672249200x^{52}$ $+877671480x^{54}+1010111040x^{56}+980421960x^{58}+788511696x^{60}$ $+512173200x^{62}+252651840x^{64}+90164340x^{66}+21443240x^{68}+2468128x^{70}$
	4	(70,56)	56	1

A.2 Divisor Codes $F_k(n,p)$

In here we are presenting results on the Divisor Codes $F_k(n,p)$. Recall that $n = s^{m-1}$ and $s = p_1 p_2 \ldots p_q$

A.2.1 Codes associated with $\mathbf{3}^q$

The following sets of tables shows the weight enumerator of the codes associated with the null-space of $V_{k,k+1}(\mathbf{3}^n)$ for $n = 2,3,4,5,6$ over $GF(p)$ where $p = 2,3,5$.

Weight Enumerator Polynomial of $F_k(s^2, GF(2))$ for $q = 2,3,4$

Lattice	**k**	V_k		**Weight Enumerator**
		size	rank	
$\mathbf{3}^2$	1	(2,3)	2	$1 + x^3$
	2	(3,2)	2	1
$\mathbf{3}^3$	1	(3,6)	3	$1 + 4x^3 + 3x^4$
	2	(6,7)	6	$1 + x^6$
	3	(7,6)	6	1
$\mathbf{3}^4$	1	(4,10)	4	$1 + 10x^3 + 15x^4 + 12x^5 + 15x^6 + 10x^7 + x^{10}$
	2	(10,16)	10	$1 + x^4 + 16x^6 + 27x^8 + 16x^{10} + 3x^{12}$
	3	(16,19)	15	$1 + 7x^9 + 4x^{10} + 3x^{12} + x^{13}$
	4	(19,16)	15	$1 + x^{12}$
	5	(16,10)	10	1

Weight Enumerator Polynomial of $F_k(s^2, GF(2))$ for $q = 5, 6$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{3}^5$	1	(5,15)	5	$1 + 20x^3 + 45x^4 + 72x^5 + 160x^6 + 240x^7 + 195x^8 + 120x^9 + 96x^{10}$ $+60x^{11} + 15x^{12}$
	2	(15,30)	15	$1 + 5x^4 + 80x^6 + 345x^8 + 1742x^{10} + 5050x^{12} + 9260x^{14} + 9035x^{16}$ $+5000x^{18} + 1785x^{20} + 420x^{22} + 35x^{24} + 10x^{26}$
	3	(30,45)	29	$1 + x^5 + 10x^8 + 45x^9 + 20x^{10} + 115x^{12} + 360x^{13} + 440x^{14}$ $+1105x^{16} + 3930x^{17} + 2840x^{18} + 5758x^{20} + 13665x^{21}$ $+7840x^{22} + 7280x^{24} + 12537x^{25} + 4660x^{26} + 2015x^{28}$ $+2150x^{29} + 584x^{30} + 100x^{32} + 80x^{33}$
	4	(45,51)	41	$1 + 15x^{12} + 70x^{18} + 56x^{20} + 120x^{22} + 270x^{24} + 210x^{26}$ $+105x^{28} + 102x^{30} + 65x^{32} + 10x^{38}$
	5	(51,45)	41	$1 + 5x^{16} + 10x^{24}$
	6	(45,30)	29	$1 + x^{20}$
	7	(30,15)	15	1
$\mathbf{3}^6$	1	(6,21)	6	$1 + 35x^3 + 105x^4 + 252x^5 + 805x^6 + 1935x^7 + 3255x^8 + 4515x^9$ $+5481x^{10} + 5481x^{11} + 4515x^{12} + 3255x^{13} + 1935x^{14} + 805x^{15}$ $+252x^{16} + 105x^{17} + 35x^{18} + x^{21}$
	2	(21,50)	21	$1 + 15x^4 + 260x^6 + 1905x^8 + 18104x^{10} + 142675x^{12} + 932400x^{14}$ $+4551250x^{16} + 17088000x^{18} + 44660542x^{20} + 85854680x^{22} + 115218810x^{24}$ $+116317680x^{26} + 83593950x^{28} + 45476784x^{30} + 17326285x^{32} + 4742720x^{34}$ $+834675x^{36} + 101700x^{38} + 8181x^{40} + 280x^{42} + 15x^{44}$
	3	(50,90)	49	$1 + ax^d + \cdots + bx^m$: where $d \leq 8$
	4	(90,126)	85	$1 + ax^d + \cdots + bx^m$: where $d \leq 12$
	5	(126,141)	111	$1 + ax^d + \cdots + bx^m$: where $d \leq 15$
	6	(141,126)	111	$1 + ax^d + \cdots + bx^m$: where $d \leq 20$
	7	(126,90)	85	$1 + 6x^{25} + 15x^{40} + 10x^{45}$
	8	(90,50)	49	$1 + x^{30}$
	9	(50,21)	21	1

Weight Enumerator Polynomial of $F_k(s^2, GF(3))$ for $q = 2, 3, 4$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{3}^2$	1	(2,3)	2	$1 + 2x^3$
	2	(3,2)	2	1
$\mathbf{3}^3$	1	(3,6)	3	$1 + 6x^3 + 12x^4 + 6x^5 + 2x^6$
	2	(6,7)	5	$1 + 6x^5 + 2x^6$
	3	(7,6)	5	$1 + 2x^6$
	4	(6,3)	3	1
$\mathbf{3}^4$	1	(4,10)	4	$1 + 12x^3 + 54x^4 + 72x^5 + 162x^6 + 252x^7 + 90x^8 + 68x^9 + 18x^{10}$
	2	(10,16)	9	$1 + 24x^5 + 20x^6 + 56x^7 + 198x^8 + 232x^9 + 460x^{10} + 384x^{11}$ $+476x^{12} + 232x^{13} + 96x^{14} + 8x^{16}$
	3	(16,19)	13	$1 + 8x^6 + 12x^8 + 30x^9 + 60x^{10} + 60x^{11} + 102x^{12} + 240x^{13}$ $+78x^{14} + 100x^{15} + 24x^{16} + 12x^{17} + 2x^{18}$
	4	(19,16)	13	$1 + 8x^9 + 18x^{12}$
	5	(16,10)	9	$1 + 2x^{10}$
	6	(10,4)	4	1

Weight Enumerator Polynomial of $F_k(s^2, GF(3))$ for $q = 5$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{3}^5$	1	(5,15)	5	$1 + 20x^3 + 150x^4 + 300x^5 + 1200x^6 + 3510x^7 + 6840x^8$ $+10760x^9 + 12456x^{10} + 11340x^{11} + 7600x^{12} + 3810x^{13} + 960x^{14}$ $+102x^{15}$
	2	(15,30)	14	$1 + 60x^5 + 80x^6 + 280x^7 + 1110x^8 + 2140x^9 + 9476x^{10}$ $+29280x^{11} + 80310x^{12} + 215760x^{13} + 461760x^{14} + 1032056x^{15}$ $+2023840x^{16} + 3147060x^{17} + 4785820x^{18} + 6285560x^{19}$ $+6408516x^{20} + 6248160x^{21} + 5273340x^{22} + 3380280x^{23}$ $+2083880x^{24} + 1044592x^{25} + 385320x^{26} + 116400x^{27} + 27500x^{28}$ $+4080x^{29} + 60x^{30}$
	3	(30,45)	26	$1 + 20x^6 + 0x + 60x^8 + 150x^9 + 360x^{10} + 310x^{11} + 1190x^{12}$ $+2520x^{13} + 8570x^{14} + 15260x^{15} + 48480x^{16} + 122860x^{17}$ $+265440x^{18} + 635460x^{19} + 1483240x^{20} + 3257160x^{21}$ $+6761610x^{22} + 13203720x^{23} + 24198970x^{24} + 40791900x^{25}$ $+63381370x^{26} + 89934890x^{27} + 117337650x^{28} + 138489760x^{29}$ $+148259886x^{30} + 142244910x^{31} + 123353940x^{32} + 95710550x^{33}$ $+67148220x^{34} + 41828326x^{35} + 23681790x^{36} + 11742360x^{37}$ $+5326020x^{38} + 2051050x^{39} + 722052x^{40} + 202450x^{41}$ $+44120x^{42} + 4650x^{43} + 180x^{44} + 12x^{45}$
	4	(45,51)	35	$1 + 40x^9 + 130x^{12} + 120x^{14} + 200x^{15} + 660x^{16} + 840x^{17}$ $+1820x^{18} + 3960x^{19} + 8790x^{20} + 14470x^{21} + 27990x^{22}$ $+43710x^{23} + 95950x^{24} + 182040x^{25} + 350370x^{26} + 607900x^{27}$ $+988980x^{28} + 1651020x^{29} + 2382998x^{30} + 3215160x^{31}$ $+4127850x^{32} + 4727870x^{33} + 5068950x^{34} + 5051916x^{35}$ $+4539466x^{36} + 3593220x^{37} + 2747220x^{38} + 1745530x^{39}$ $+995040x^{40} + 516966x^{41} + 222120x^{42} + 91380x^{43}$ $+26520x^{44} + 9960x^{45} + 4380x^{46} + 720x^{47} + 400x^{48}$ $+12x^{50} + 52x^{51}$
	5	(51,45)	35	$1 + 10x^{10} + 20x^{13} + 40x^{16} + 170x^{18} + 200x^{19} + 60x^{21}$ $+760x^{22} + 1140x^{24} + 3344x^{25} + 4270x^{27} + 11700x^{28}$ $+7662x^{30} + 15560x^{31} + 5430x^{33} + 6750x^{34} + 860x^{36}$ $+960x^{37} + 90x^{39} + 22x^{40}$
	6	(45,30)	26	$1 + 10x^{14} + 20x^{20} + 20x^{21} + 30x^{22}$
	7	(30,15)	14	$1 + 2x^{15}$
	8	(15,5)	5	1

Weight Enumerator Polynomial of $F_k(s^2, GF(3))$ for $q = 6$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{3}^6$	1	(6,21)	6	$1 + 30x^3 + 330x^4 + 840x^5 + 4930x^6 + 20160x^7 + 69840x^8$ $+203600x^9 + 499026x^{10} + 1001526x^{11} + 1646620x^{12}$ $+2280270x^{13} + 2603130x^{14} + 2449532x^{15} + 1832436x^{16}$ $+1078830x^{17} + 474810x^{18} + 148560x^{19} + 30990x^{20}$ $+3446x^{21}$
	2	(21,50)	20	$1 + 120x^5 + 220x^6 + 840x^7 + 3720x^8 + 9360x^9 + 51756x^{10}$ $+197520x^{11} + 713500x^{12} + 2844180x^{13} + 10609260x^{14}$ $+40044408x^{15} + 145356270x^{16} + 500129880x^{17} + 1647434640x^{18}$ $+5133603840x^{19} + 15063058596x^{20} + 41564561760x^{21}$ $+107398020660x^{22} + 258965687520x^{23} + 581012762520x^{24}$ $+1209441631356x^{25} + 2331237134610x^{26} + 4154371498520x^{27}$ $+6836862180600x^{28} + 10381610578860x^{29} + 14533884557454x^{30}$ $+18742340210400x^{31} + 22238955304080x^{32} + 24244170398240x^{33}$ $+24236608402500x^{34} + 22162054224696x^{35} + 18478972590810x^{36}$ $+13994794719120x^{37} + 9582512782080x^{38} + 5898607138280x^{39}$ $+3242849022900x^{40} + 1579388865600x^{41} + 675039431700x^{42}$ $+250177437840x^{43} + 79254757740x^{44} + 21053095992x^{45}$ $+4572625980x^{46} + 780648360x^{47} + 99220920x^{48} + 8209920x^{49}$ $+335520x^{50}$
	3	(50,90)	45	$1 + ax^d + \cdots + bx^m$: where $d \leq 6$
	4	(90,126)	75	$1 + ax^d + \cdots + bx^m$: where $d \leq 9$
	5	(126,141)	96	$1 + ax^d + \cdots + bx^m$: where $d \leq 10$
	6	(141,126)	96	$1 + ax^d + \cdots + bx^m$: where $d \leq 14$
	7	(126,90)	75	$1 + ax^d + \cdots + bx^m$: where $d \leq 15$
	8	(90,50)	45	$1 + 12x^{20} + 30x^{10} + 30x^{12} + 120x^{15} + 50x^{16}$
	9	(50,21)	20	$1 + 2x^{21}$
	10	(21,6)	6	1

Weight Enumerator Polynomial of $F_k(s^2, GF(5))$ for $q = 2, 3, 4$

Lattice	**k**	V_k		**Weight Enumerator**
		size	rank	
$\mathbf{3}^2$	1	(2,3)	2	$1 + 4x^3$
	2	(2,3)	2	1
$\mathbf{3}^3$	1	(3,6)	3	$1 + 12x^3 + 24x^4 + 60x^5 + 28x^6$
	2	(6,7)	6	$1 + 4x^6$
	3	(7,6)	6	1
$\mathbf{3}^4$	1	(4,10)	4	$1 + 24x^3 + 108x^4 + 336x^5 + 1300x^6 + 3320x^7 + 4836x^8 + 3912x^9 + 1788x^{10}$
	2	(10,16)	10	$1 + 40x^6 + 180x^8 + 96x^9 + 1064x^{10} + 1392x^{11} + 3600x^{12} + 3600x^{13} + 3744x^{14} + 1440x^{15} + 468x^{16}$
	3	(16,19)	16	$1 + 12x^9 + 12x^{12} + 48x^{15} + 24x^{17} + 12x^{18} + 16x^{19}$
	4	(19,16)	16	1

A.2.2 Codes associated with 4^n

Weight Enumerator Polynomial of $F_k(s^3, GF(2))$ for $q = 2, 3, 4$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{4}^2$	1	(2,3)	2	$1 + x^3$
	2	(3,4)	3	$1 + x^4$
	3	(4,3)	3	1
$\mathbf{4}^3$	1	(3,6)	3	$1 + 4x^3 + 3x^4$
	2	(6,10)	6	$1 + 3x^4 + 6x^5 + 4x^6 + 2x^7$
	3	(10,12)	9	$1 + 3x^6 + 3x^7 + x^9$
	4	(12,12)	10	$1 + 3x^8$
	5	(12,10)	9	$1 + 1x^9$
	6	(10,6)	6	1
$\mathbf{4}^4$	1	(4,10)	4	$1 + 10x^3 + 15x^4 + 12x^5 + 15x^6 + 10x^7 + x^{10}$
	2	(10,20)	10	$1 + 7x^4 + 24x^5 + 28x^6 + 56x^7 + 120x^8 + 176x^9 + 200x^{10}$ $+176x^{11} + 120x^{12} + 56x^{13} + 28x^{14} + 24x^{15} + 7x^{16} + x^{20}$
	3	(20,31)	19	$1 + 12x^6 + 24x^7 + 6x^8 + 23x^9 + 112x^{10} + 156x^{11} + 228x^{12}$ $+376x^{13} + 408x^{14} + 524x^{15} + 737x^{16} + 654x^{17} + 336x^{18}$ $+180x^{19} + 180x^{20} + 96x^{21} + 28x^{22} + 12x^{23} + 0x + 3x^{25}$
	4	(31,40)	28	$1 + 18x^8 + 12x^{10} + 61x^{12} + 168x^{14} + 469x^{16} + 624x^{18}$ $+1002x^{20} + 1080x^{22} + 600x^{24} + 36x^{26} + 25x^{28}$
	5	(40,44)	34	$1 + 4x^9 + 12x^{11} + 4x^{13} + 24x^{14} + 27x^{16} + 12x^{17}$ $+60x^{18} + 144x^{19} + 54x^{20} + 52x^{21} + 128x^{22} + 144x^{23}$ $+124x^{24} + 48x^{25} + 44x^{26} + 84x^{27} + 50x^{28} + 8x^{29}$
	6	(44,40)	34	$1 + 4x^{12} + 6x^{14} + x^{16} + 12x^{18} + 30x^{22} + 8x^{28}$
	7	(40,31)	28	$1 + 4x^{15} + 3x^{20}$
	8	(31,20)	19	$1 + x^{16}$
	9	(20,10)	10	1

Weight Enumerator Polynomial of $F_k(s^3, GF(2))$ for $q = 5$

Lattice	**k**	V_k		**Weight Enumerator**
		size	rank	
$\mathbf{4}^5$	1	(5,15)	5	$1 + 20x^3 + 45x^4 + 72x^5 + 160x^6 + 240x^7 + 195x^8 + 120x^9 + 96x^{10}$ $+60x^{11} + 15x^{12}$
	2	(15,35)	15	$1 + 15x^4 + 60x^5 + 110x^6 + 260x^7 + 830x^8 + 2320x^9 + 5412x^{10}$ $+11800x^{11} + 24780x^{12} + 44840x^{13} + 70020x^{14} + 100344x^{15}$ $+127365x^{16} + 139920x^{17} + 138480x^{18} + 122400x^{19} + 95335x^{20}$ $+68860x^{21} + 45790x^{22} + 26980x^{23} + 14300x^{24} + 6144x^{25}$ $+1820x^{26} + 360x^{27} + 30x^{28}$
	3	(35,65)	34	$1 + ax^d + \cdots + bx^m$: where $d \leq 7$
	4	(65,101)	61	$1 + ax^d + \cdots + bx^m$: where $d \leq 8$
	5	(101,135)	91	$1 + ax^d + \cdots + bx^m$: where $d \leq 9$
	6	(135,155)	115	$1 + ax^d + \cdots + bx^m$: where $d \leq 12$
	7	(155,155)	124	$1 + ax^d + \cdots + bx^m$: where $d \leq 15$
	8	(155,135)	115	$1 + ax^d + \cdots + bx^m$: where $d \leq 19$
	9	(135,101)	91	$1 + 5x^{20} + 10x^{23} + 10x^{30} + 20x^{33} + 30x^{34} + 30x^{39} + 10x^{41}$ $+60x^{43} + 75x^{44} + 90x^{45} + 75x^{46} + 15x^{48} + 60x^{50} + 60x^{51}$ $+60x^{52} + 70x^{53} + 12x^{55} + 90x^{56} + 30x^{57} + 75x^{58} + 40x^{59}$ $+20x^{61} + 60x^{63} + x^{70} + 5x^{74} + 10x^{76}+$
	10	(101,65)	61	$1 + 5x^{24} + 10x^{36}$
	11	(65,35)	34	$1 + x^{25}$
	12	(35,15)	15	1

Weight Enumerator Polynomial of $F_k(s^3, GF(3))$ for $q = 2, 3, 4$

Lattice	**k**	V_k		**Weight Enumerator**
		size	rank	
$\mathbf{4}^2$	1	(2,3)	2	$1 + 2x^3$
	2	(3,4)	3	$1 + 2x^4$
	3	(4,3)	3	1
$\mathbf{4}^3$	1	(3,6)	3	$1 + 6x^3 + 12x^4 + 6x^5 + 2x^6$
	2	(6,10)	6	$1 + 6x^4 + 6x^5 + 20x^6 + 22x^7 + 24x^8 + 2x^{10}$
	3	(10,12)	10	$1 + 2x^6 + 6x^{10}$
	4	(12,12)	12	1
$\mathbf{4}^4$	1	(4,10)	4	$1 + 12x^3 + 54x^4 + 72x^5 + 162x^6 + 252x^7 + 90x^8 + 68x^9 + 18x^{10}$
	2	(10,20)	10	$1 + 12x^4 + 24x^5 + 92x^6 + 144x^7 + 534x^8 + 1368x^9 + 3092x^{10}$ $+5592x^{11} + 8892x^{12} + 10944x^{13} + 11460x^{14} + 8248x^{15} + 5244x^{16}$ $+2112x^{17} + 920x^{18} + 328x^{19} + 42x^{20}$
	3	(20,31)	20	$1 + 8x^6 + 24x^8 + 30x^9 + 132x^{10} + 132x^{11} + 416x^{12} + 624x^{13}$ $+1302x^{14} + 2716x^{15} + 5544x^{16} + 8556x^{17} + 14496x^{18} + 20742x^{19}$ $+26202x^{20} + 27840x^{21} + 25128x^{22} + 19848x^{23} + 12798x^{24} + 6426x^{25}$ $+2652x^{26} + 1220x^{27} + 204x^{28} + 90x^{29} + 10x^{30} + 6x^{31}$
	4	(31,40)	31	$1 + 8x^9 + 42x^{12} + 96x^{15} + 524x^{18} + 1176x^{21} + 4500x^{24} + 7264x^{27}$ $+5316x^{30} + 696x^{33} + 60x^{36}$
	5	(40,44)	40	$1 + 2x^{10} + 6x^{16} + 12x^{20} + 8x^{24} + 6x^{26} + 18x^{28} + 12x^{32} + 4x^{34}$ $+12x^{36}$
	6	(44,40)	40	1

Weight Enumerator Polynomial of $F_k(s^3, GF(3))$ for $q = 5$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{4}^5$	1	(5,15)	5	$1 + 20x^3 + 150x^4 + 300x^5 + 1200x^6 + 3510x^7 + 6840x^8 + 10760x^9 + 12456x^{10} + 11340x^{11} + 7600x^{12} + 3810x^{13} + 960x^{14} + 102x^{15}$
	2	(15,35)	15	$1 + 20x^4 + 60x^5 + 260x^6 + 500x^7 + 2550x^8 + 7940x^9 + 27516x^{10} + 93400x^{11} + 306860x^{12} + 957690x^{13} + 2732620x^{14} + 7450586x^{15} + 18228180x^{16} + 40372660x^{17} + 81768440x^{18} + 148397430x^{19} + 238670986x^{20} + 341800820x^{21} + 433579260x^{22} + 487287460x^{23} + 485298320x^{24} + 426665292x^{25} + 329163100x^{26} + 220838350x^{27} + 127452630x^{28} + 61713430x^{29} + 24530180x^{30} + 7462210x^{31} + 1692520x^{32} + 259710x^{33} + 22180x^{34} + 1240x^{35}$
	3	(35,65)	35	$1 + ax^d + \cdots + bx^m$: where $d \leq 6$
	4	(65,101)	65	$1 + ax^d + \cdots + bx^m$: where $d \leq 9$
	5	(101,135)	101	$1 + ax^d + \cdots + bx^m$: where $d \leq 10$
	6	(135,155)	135	$1 + ax^d + \cdots + bx^m$: where $d \leq 14$
	7	(155,155)	154	$1 + 2x^{15}$
	8	(155,135)	135	1

Weight Enumerator Polynomial of $F_k(s^3, GF(5))$ for $q = 2, 3, 4$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{4}^2$	1	(2,3)	2	$1 + 4x^3$
	2	(3,4)	3	$1 + 4x^4$
$\mathbf{4}^3$	1	(3,6)	3	$1 + 12x^3 + 24x^4 + 60x^5 + 28x^6$
	2	(6,10)	6	$1 + 12x^4 + 64x^6 + 104x^7 + 204x^8 + 192x^9 + 48x^{10}$
	3	(10,12)	9	$1 + 24x^{10}$
	4	(12,12)	11	$1 + 4x^{12}$
$\mathbf{4}^4$	1	(4,10)	4	$1 + 24x^3 + 108x^4 + 336x^5 + 1300x^6 + 3320x^7 + 4836x^8 + 3912x^9$ $+1788x^{10}$
	2	(10,20)	10	$1 + 24x^4 + 280x^6 + 416x^7 + 1708x^8 + 6192x^9 + 21808x^{10} + 71360x^{11}$ $+212528x^{12} + 500864x^{13} + 1059704x^{14} + 1755360x^{15} + 2162460x^{16}$ $+1989056x^{17} + 1294128x^{18} + 557280x^{19} + 132456x^{20}$
	3	(20,31)	20	$1 + 24x^8 + 12x^9 + 96x^{10} + 688x^{12} + 480x^{13} + 3456x^{14} + 9168x^{15}$ $+26552x^{16} + 64080x^{17} + 172056x^{18} + 412924x^{19} + 981924x^{20}$ $+1955872x^{21} + 3600696x^{22} + 5692032x^{23} + 7822996x^{24} + 8854868x^{25}$ $+8190180x^{26} + 5968536x^{27} + 3303608x^{28} + 1368012x^{29} + 352668x^{30}$ $+47196x^{31}$
	4	(31,40)	30	$1 + 40x^{12} + 352x^{18} + 384x^{19} + 1056x^{20} + 1952x^{21} + 5112x^{22}$ $+12192x^{23} + 29824x^{24} + 55888x^{25} + 121344x^{26} + 209792x^{27}$ $+399444x^{28} + 683280x^{29} + 1014152x^{30} + 1354736x^{31} + 1561500x^{32}$ $+1535728x^{33} + 1246192x^{34} + 833040x^{35} + 457968x^{36} + 178256x^{37}$ $+52584x^{38} + 9120x^{39} + 1688x^{40}$
	5	(40,44)	37	$1 + 12x^{16} + 16x^{22} + 16x^{24} + 24x^{25} + 48x^{26} + 336x^{27} + 900x^{28}$ $+432x^{29} + 1680x^{30} + 3088x^{31} + 5120x^{32} + 7320x^{33} + 10052x^{34}$ $+11200x^{35} + 12396x^{36} + 10992x^{37} + 7084x^{38} + 4512x^{39}$ $+2120x^{40} + 496x^{41} + 216x^{42} + 16x^{43} + 48x^{44}]$

Weight Enumerator Polynomial of $F_k(s^3, GF(5))$ for $q = 5$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{4}^5$	1	(5,15)	5	$1 + 40x^3 + 300x^4 + 1080x^5 + 7120x^6 + 33460x^7 + 126160x^9$ $+427680x^{10} + 1015112x^{11} + 1835480x^{12} + 2424440x^{13}$ $+2252700x^{14} + 1305120x^{15} + 336932x^{16}$
	2	(15,35)	15	$1 + ax^d + \cdots + bx^m$: where $d \leq 4$
	3	(35,65)	35	$1 + ax^d + \cdots + bx^m$: where $d \leq 8$
	4	(65,101)	65	$1 + ax^d + \cdots + bx^m$: where $d \leq 9$
	5	(101,135)	97	$1 + ax^d + \cdots + bx^m$: where $d \leq 16$
	6	(135,155)	125	$1 + ax^d + \cdots + bx^m$: where $d \leq$
	7	(155,155)	135	$1 + ax^d + \cdots + bx^m$: where $d \leq$
	8	(155,135)	125	$1 + 20x^{51} + 40x^{57} + 80x^{66} + 200x^{70} + 360x^{72} + 1400x^{73}$ $+240x^{74} + 280x^{75} + 240x^{76} + 140x^{78} + 120x^{80}$ $+40x^{82} + 140x^{84} + 1360x^{86} + 720x^{87} + 800x^{88}$ $+920x^{89} + 1320x^{90} + 3620x^{91} + 5280x^{92} + 9120x^{93}$ $+11380x^{94} + 30120x^{95} + 41080x^{96} + 64500x^{97} + 88960x^{98}$ $+120480x^{99} + 171480x^{100} + 225060x^{101} + 334760x^{102}$ $+440400x^{103} + 540100x^{104} + 627168x^{05} + 719100x^{106}$ $+847820x^{107} + 882260x^{108} + 877640x^{109} + 808412x^{110}$ $+733460x^{111} + 617960x^{112} + 497240x^{113} + 362800x^{114}$ $+263060x^{115} + 172960x^{116} + 116740x^{117} + 66060x^{118}$ $+37900x^{119} + 18200x^{120} + 9880x^{121} + 7080x^{122} + 2300x^{123}$ $+1600x^{124} + 200x^{125} + 840x^{126} + 120x^{128} + 60x^{130} + 4x^{135}$
	9	(135,101)	97	$1 + 20x^{61} + 40x^{76} + 104x^{80} + 240x^{81} + 120x^{83} + 60x^{84} + 40x^{87}$
	10	(101,65)	65	1

A.2.3 Codes associated with $\mathbf{5}^n$

Weight Enumerator Polynomial of $F_k(s^4, GF(2))$ for $q = 3, 4$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{5}^3$	1	(3,6)	3	$1 + 4x^3 + 3x^4$
	2	(6,10)	6	$1 + 3x^4 + 6x^5 + 4x^6 + 2x^7$
	3	(10,15)	10	$1 + 3x^5 + 3x^6 + 6x^7 + 9x^8 + 7x^9 + 3x^{10}$
	4	(15,18)	15	$1 + 3x^8 + 4x^{12}$
	5	(18,19)	18	$1 + x^9$
	6	(19,18)	18	1
$\mathbf{5}^4$	1	(4,10)	4	$1 + 10x^3 + 15x^4 + 12x^5 + 15x^6 + 10x^7 + x^{10}$
	2	(10,20)	10	$1 + 7x^4 + 24x^5 + 28x^6 + 56x^7 + 120x^8 + 176x^9 + 200x^{10}$ $+176x^{11} + 120x^{12} + 56x^{13} + 28x^{14} + 24x^{15} + 7x^{16} + x^{20}$
	3	(20,35)	20	$1 + 6x^5 + 12x^6 + 36x^7 + 42x^8 + 47x^9 + 199x^{10} + 420x^{11}$ $+696x^{12} + 1268x^{13} + 2034x^{14} + 2972x^{15} + 4025x^{16}$ $+4626x^{17} + 4626x^{18} + 4025x^{19} + 2972x^{20} + 2034x^{21}$ $+1268x^{22} + 696x^{23} + 420x^{24} + 199x^{25} + 47x^{26} + 42x^{27}$ $+36x^{28} + 12x^{29} + 6x^{30} + x^{35}]$
	4	(35,52)	35	$1 + ax^d + \cdots + bx^m$: where $d \leq 8$
	5	(52,68)	52	$1 + ax^d + \cdots + bx^m$: where $d \leq 9$
	6	(68,80)	68	$1 + ax^d + \cdots + bx^m$: where $d \leq 12$
	7	(80,85)	78	$1 + 4x^{15} + 3x^{20} + 3x^{25} + 4x^{27} + 12x^{32} + 6x^{33} + 12x^{34} + 12x^{35}$ $+15x^{36} + 3x^{37} + 12x^{39} + 7x^{40} + 4x^{42} + 16x^{43} + 6x^{48}$ $+x^{49} + 4x^{52} + 3x^{53}$
	8	(85,80)	78	$1 + x^{16} + x^{36} + x^{52}$
	9	(80,68)	68	1

Weight Enumerator Polynomial of $F_k(s^4, GF(3))$ for $q = 3, 4$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{5}^3$	1	(3,6)	3	$1 + 6x^3 + 12x^4 + 6x^5 + 2x^6$
	2	(6,10)	6	$1 + 6x^4 + 6x^5 + 20x^6 + 22x^7 + 24x^8 + 2x^{10}$
	3	(10,15)	10	$1 + 6x^5 + 2x^6 + 12x^7 + 24x^8 + 24x^9 + 72x^{10} + 60x^{11} + 34x^{12} + 6x^{13} + 2x^{15}$
	4	(15,18)	15	$1 + 6x^{10} + 8x^{12} + 12x^{14}$
	5	(18,19)	18	$1 + 2x^{16}$
$\mathbf{5}^4$	1	(4,10)	4	$1 + 12x^3 + 54x^4 + 72x^5 + 162x^6 + 252x^7 + 90x^8 + 68x^9 + 18x^{10}$
	2	(10,20)	10	$1 + 12x^4 + 24x^5 + 92x^6 + 144x^7 + 534x^8 + 1368x^9 + 3092x^{10}$ $+5592x^{11} + 8892x^{12} + 10944x^{13} + 11460x^{14} + 8248x^{15} + 5244x^{16}$ $+2112x^{17} + 920x^{18} + 328x^{19} + 42x^{20}$
	3	(20,35)	20	$1 + 12x^5 + 8x^6 + 48x^7 + 120x^8 + 126x^9 + 504x^{10} + 936x^{11}$ $+2312x^{12} + 6360x^{13} + 15318x^{14} + 35184x^{15} + 76806x^{16}$ $+158790x^{17} + 328640x^{18} + 583302x^{19} + 952752x^{20} + 1389946x^{21}$ $+1801572x^{22} + 2071068x^{23} + 2052260x^{24} + 1782240x^{25}$ $+1326180x^{26} + 862392x^{27} + 491748x^{28} + 241674x^{29} + 107610x^{30}$ $+41820x^{31} + 13842x^{32} + 4490x^{33} + 756x^{34} + 90x^{35}$
	4	(35,52)	35	$1 + ax^d + \cdots + bx^m$: where $d \leq 9$
	5	(52,68)	52	$1 + ax^d + \cdots + bx^m$: where $d \leq 10$
	6	(68,80)	68	$1 + ax^d + \cdots + bx^m$: where $d \leq 18$
	7	(80,85)	80	$1 + 6x^{25} + 6x^{32} + 12x^{33} + 2x^{36} + 6x^{40} + 12x^{41} + 36x^{45}$ $+38x^{48} + 24x^{49} + 12x^{52} + 36x^{53} + 12x^{56} + 6x^{57}$ $+2x^{60} + 24x^{61} + 6x^{65} + 2x^{72}$
	8	(85,80)	80	1

Weight Enumerator Polynomial of $F_k(s^4, GF(5))$ for $q = 3$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{5}^3$	1	(3,6)	3	$1 + 12x^3 + 24x^4 + 60x^5 + 28x^6$
	2	(6,10)	6	$1 + 12x^4 + 64x^6 + 104x^7 + 204x^8 + 192x^9 + 48x^{10}$
	3	(10,15)	10	$1 + 12x^5 + 72x^8 + 120x^9 + 252x^{10} + 540x^{11} + 880x^{12} + 768x^{13} + 420x^{14} + 60x^{15}$
	4	(15,18)	14	$1 + 12x^9 + 48x^{11} + 56x^{12} + 36x^{13} + 132x^{14} + 128x^{15} + 156x^{16} + 48x^{17} + 8x^{18}$
	5	(18,19)	16	$1 + 12x^{12} + 12x^{13} + 36x^{14} + 0x + 12x^{16} + 36x^{17} + 12x^{18} + 4x^{19}$
	6	(19,18)	16	$1 + 12x^{14} + 12x^{16}$
	7	(18,15)	14	$1 + 4x^{15}$
	8	(15,10)	10	1

Weight Enumerator Polynomial of $F_k(s^4, GF(5))$ for $q = 4$

Lattice	**k**	V_k size	V_k rank	**Weight Enumerator**
$\mathbf{5}^4$	1	(4,10)	4	$1 + 24x^3 + 108x^4 + 336x^5 + 1300x^6 + 3320x^7 + 4836x^8 + 3912x^9$ $+1788x^{10}$
	2	(10,20)	10	$1 + 24x^4 + 280x^6 + 416x^7 + 1708x^8 + 6192x^9 + 21808x^{10} + 71360x^{11}$ $+212528x^{12} + 500864x^{13} + 1059704x^{14} + 1755360x^{15} + 2162460x^{16}$ $+1989056x^{17} + 1294128x^{18} + 557280x^{19} + 132456x^{20}$
	3	(20,35)	20	$1 + ax^d + \cdots + bx^m$: where $d \leq 5$
	4	(35,52)	34	$1 + ax^d + \cdots + bx^m$: where $d \leq 9$
	5	(52,68)	49	$1 + ax^d + \cdots + bx^m$: where $d \leq 12$
	6	(68,80)	62	$1 + ax^d + \cdots + bx^m$: where $d \leq 14$
	7	(80,85)	70	$1 + ax^d + \cdots + bx^m$: where $d \leq 15$
	8	(85,80)	70	$1 + 16x^{25} + 48x^{30} + 16x^{32} + 48x^{33} + 48x^{34} + 312x^{36}$ $+192x^{37} + 360x^{38} + 48x^{39} + 156x^{40} + 48x^{41} + 96x^{42}$ $+528x^{43} + 1104x^{44} + 912x^{45} + 3792x^{46} + 5616x^{47}$ $+8380x^{48} + 9408x^{49} + 12664x^{50} + 11136x^{51} + 19792x^{52}$ $+23008x^{53} + 38544x^{54} + 66624x^{55} + 116264x^{56}$ $+174912x^{57} + 261304x^{58} + 367664x^{59} + 534096x^{60}$ $+661728x^{61} + 823808x^{62} + 936464x^{63} + 1037324x^{64}$ $+1047056x^{65} + 1011216x^{66} + 867312x^{67} + 689896x^{68}$ $+473760x^{69} + 297448x^{70} + 148944x^{71} + 73656x^{72}$ $+28112x^{73} + 8800x^{74} + 2304x^{75} + 660x^{76}$
	9	(80,68)	62	$1 + 16x^{31} + 24x^{33} + 48x^{39} + 144x^{40} + 192x^{41} + 48x^{42}$ $+60x^{46} + 96x^{47} + 204x^{48} + 96x^{49} + 336x^{50} + 1224x^{51}$ $+1512x^{52} + 2112x^{53} + 1740x^{54} + 1728x^{55} + 1372x^{56}$ $+1704x^{57} + 1008x^{58} + 448x^{59} + 816x^{60} + 456x^{61}$ $+160x^{62} + 48x^{63} + 28x^{64} + 4x^{68}$
	10	(68,52)	49	$1 + 16x^{34} + 24x^{42} + 48x^{43} + 36x^{44}$
	11	(52,35)	34	$1 + 4x^{35}$
	12	(35,20)	20	1

A.3 Codes associated with non-cyclic Abelian Groups

In this part we are presenting the weight enumerator of Projective codes $C_k(\mathbb{Z}_q^n, p)$. The *weight enumerator* and the *minimum distance* of such codes are presented in the following tables.

A.3.1 Rank and Weight enumerator polynomial of $C_k(\mathbb{Z}_q^n, p)$

Weight Enumerator Polynomial of $C_k(\mathbb{Z}_2^n, 2)$ for $n = 3, 4, 5, 6$

Lattice	**k**	V_k		**Weight Enumerator**
		size	rank	
$\mathcal{L}(\mathbb{Z}_2^3)$	1	(7,7)	4	$1 + 7x^4$
$\mathcal{L}(\mathbb{Z}_2^4)$	1	(15,35)	11	$1 + 105x^4 + 1960x^6 + 21525x^8 + 179648x^{10} + 813645x^{12}$ $+2283560x^{14} + 3924515x^{16} + 4468800x^{18} + 3155131x^{20}$ $+1448440x^{22} + 401415x^{24} + 71680x^{26} + 6735x^{28} + 56x^{30}$
	2	(35,15)	11	$1 + 15x^8$
$\mathcal{L}(\mathbb{Z}_2^5)$	1	(31,155)	26	$1 + ax^d + \cdots + bx^m$: where $d = 4$
	2	(155,155)	76	$1 + ax^d + \cdots + bx^m$: where $d \leq 8$
	3	(155,31)	26	$1 + 31x^{16}$
$\mathcal{L}(\mathbb{Z}_2^6)$	1	(63,651)	57	$1 + ax^d + \cdots + bx^m$: where $d \leq 4$
	2	(651,1395)	421	$1 + ax^d + \cdots + bx^m$: where $d \leq 8$
	3	(1395,651)	421	$1 + ax^d + \cdots + bx^m$: where $d \leq 16$
	4	(651,63)	57	$1 + ax^d + \cdots + bx^m$: where $d \leq 32$

Weight Enumerator Polynomial of $C_k(\mathbb{Z}_2^n, 3)$ for $n = 3, 4, 5, 6$

Lattice	**k**	V_k		**Weight Enumerator**
		size	rank	
$\mathcal{L}(\mathbb{Z}_2^3)$	1	(7,7)	6	$1 + 2x^7$
$\mathcal{L}(\mathbb{Z}_2^4)$	1	(15,35)	14	$1 + 560x^6 + 30x^7 + 1470x^8 + 2940x^9 + 54936x^{10} + 201600x^{11}$ $+695520x^{12} + 2543310x^{13} + 7829100x^{14} + 21778680x^{15} + 56177100x^{16}$ $+126572040x^{17} + 242385780x^{18} + 450953370x^{19} + 719890920x^{20}$ $+992083680x^{21} + 1310098230x^{22} + 1482056100x^{23} + 1427824860x^{24}$ $+1304110206x^{25} + 1003057020x^{26} + 643524560x^{27} + 381940290x^{28}$ $+184193100x^{29} + 71425368x^{30} + 23834160x^{31} + 6022800x^{32} + 969010x^{33}$ $+119490x^{34} + 6972x^{35}$
	2	(35,15)	14	$1 + 2x^{15}$
$\mathcal{L}(\mathbb{Z}_2^5)$	1	(31,155)	30	$1 + ax^d + \cdots + bx^m$: where $d \leq 6$
	2	(155,155)	125	$1 + ax^d + \cdots + bx^m$: where $d \leq 15$
	3	(155,31)	30	$1 + 2x^{31}$
$\mathcal{L}(\mathbb{Z}_2^6)$	1	(63,651)	62	$1 + ax^d + \cdots + bx^m$: where $d \leq 6$
	2	(651,1395)	589	$1 + ax^d + \cdots + bx^m$: where $d \leq 15$
	3	(1395,651)	589	$1 + ax^d + \cdots + bx^m$: where $d \leq 31$
	4	(651,63)	62	$1 + ax^d + \cdots + bx^m$: where $d \leq 63$

Weight Enumerator Polynomial of $C_k(\mathbb{Z}_2^n, 5)$ for $n = 3, 4, 5, 6$

Lattice	**k**	V_k		**Weight Enumerator**
		size	rank	
$\mathcal{L}(\mathbb{Z}_2^3)$	1	(7,7)	7	1
$\mathcal{L}(\mathbb{Z}_2^4)$	1	(15,35)	15	$1 + ax^d + \cdots + bx^m$: where $d \leq 6$
	2	(35,15)	15	1
$\mathcal{L}(\mathbb{Z}_2^5)$	1	(31,155)	31	$1 + ax^d + \cdots + bx^m$: where $d \leq 6$
	2	(155,155)	155	1
$\mathcal{L}(\mathbb{Z}_2^6)$	1	(63,651)	63	$1 + ax^d + \cdots + bx^m$: where $d \leq 26$
	2	(651,1395)	589	??
	3	(1395,651)	589	1

Weight Enumerator Polynomial of $C_k(\mathbb{Z}_3^n, 2)$ for $n = 3, 4, 5$

Lattice	**k**	V_k		**Weight Enumerator**
		size	rank	
$\mathcal{L}(\mathbb{Z}_3^3)$	1	(13,13)	12	$1 + x^{13}$
$\mathcal{L}(\mathbb{Z}_3^4)$	1	(40,130)	39	$1 + ax^d + \cdots + bx^m$: where $d \leq 8$
	2	(130,40)	39	$1 + x^{40}$
$\mathcal{L}(\mathbb{Z}_3^5$	1	(121,1210)	120	$1 + ax^d + \cdots + bx^m$: where $d \leq 8$
	2	(1210,1210)	1090	$1 + ax^d + \cdots + bx^m$: where $d \leq 40$
	3	(1210,121)	120	$1 + x^{121}$

Weight Enumerator Polynomial of $C_k(\mathbb{Z}_3^n, 3)$ for $n = 3, 4, 5$

Lattice	**k**	V_k		**Weight Enumerator**
		size	rank	
$\mathcal{L}(\mathbb{Z}_3^3)$	1	(13,13)	7	$1 + 156x^6 + 494x^9 + 78x^{12}$
$\mathcal{L}(\mathbb{Z}_3^4)$	1	(40,130)	30	$1 + ax^d + \cdots + bx^m$: where $d \leq 6$
	2	(130,40)	30	$1 + 1560x^{18} + 21060x^{24} + 18800x^{27} + 16848x^{30} + 780x^{36}$
$\mathcal{L}(\mathbb{Z}_3^5)$	1	(121,1210)	106	$1 + ax^d + \cdots + bx^m$: where $d \leq 6$
	2	(1210,1210)	551	$1 + ax^d + \cdots + bx^m$: where $d \leq 18$
	3	(1210,121)	106	??

A.4 GAP Programs

A.4.1 Boolean and Divisor codes Program (1)

```
LogTo("newlog.txt");
LoadPackage("guava");
r0:=Runtime();

m:=2; n:=4; k:=1; l:=k+1;
p:=2;

rwl:=[ ]; cwl:=[ ];nu:=[ ]; rwlmT:=[ ]; cwlmT:=[ ]; InclusionMatrix:=function(m,n,k,l)

local S,T,i,j,sum,Level,Included,K,L,m1,Nrow,Ncol;

S:=[ ];
for i in [1..m]
     do
      Add(S,i-1);     od;
T:=Tuples(S,n);

sum:=function(s)
local i,x;
x:=0;
for i in [1..Length(s)]
    do
     x:=x+s[i];
    od;
return x;
end;

Level:=function(l)
local i,L; L:=[];
for i in [1..Length(T)]
    do
     if sum(T[i])=l
     then
     Add(L,T[i]);
     fi;
    od;
return L;
end;

Included:=function(s,t)
local i,result; result:=true;
for i in [1..Length(s)]
    do
     if s[i]>t[i]
     then result:=false;
     break;
     fi;
    od;
return result;
end;
```

```
K:=Level(k); L:=Level(l); Nrow:=Length(K); Ncol:=Length(L);

m1:=NullMat(Nrow,Ncol);
for i in [1..Nrow]
   do
   for j in [1..Ncol]
    do
     if Included(K[i],L[j])
     then m1[i][j]:=1;
     fi;
    od;
   od;
return m1;
end; m1:=InclusionMatrix(m,n,k,l);

Print(" length n:=",n," layer m:=",m, "\n"); Print("\n");

rwl:=[]; cwl:=[];nu:=[]; rwlmT:=[]; cwlmT:=[];

Print("A matrix (M) constructed from level ",k," versus level ",l," over GF(",p,"):","\n");
r1:=Runtime();
row:=DimensionsMat(m1)[1];
col:=DimensionsMat(m1)[2];
Print("number of rows:  ",row,"\n");
Print("number of columns:  ",col,"\n");
Print("\n");


for i in[1..row]
   do wr:=Sum(m1[i]);
     Add (rwl,wr);
   od;
Print("Max row weight is:  ",Maximum(rwl),"\n");
Print("Min row weight is:  ",Minimum(rwl),"\n");


m1T:= TransposedMat(m1);
for i in[1..col]
   do
    wc:=Sum(m1T[i]);
    Add (cwl,wc);
   od;
Print("Max col weight is:  ",Maximum(cwl),"\n");
Print("Min col weight is:  ",Minimum(cwl),"\n");
Print(" ","\n");

mat:=m1*Z(p);;

rank:=RankMat(mat);

Print("Rank of matrix over GF(",p,") is:  ", rank,"\n");

r1:=Runtime(); Print("runtime:  ",r1-r0,"\n");
```

Part2:

```
Print(".......Null-Space Of M,(M as a check matrix)......  "," \ n");
CcheM:=CheckMatCode(m1,GF(p));
Print("Code is ",CcheM," \ n");
wCcheM:=WeightDistribution(CcheM);
Print("weight distribution:  ",wCcheM," \ n");
     if Sum(wCcheM)=p^col-rank)
     then Print("Ok...Ok"," \  n");
    else Print("Bad.....Bad"," \ n");
    fi;


r4:=Runtime();

Print("-------------Null-Space Of MT,(MT as a check matrix)-------"," \ n");

CcheMT:=CheckMatCode(m1T,GF(p));
Print("Code is ",CcheMT," \ n");

wCcheMT:=WeightDistribution(CcheMT);
Print("weight distribution:  ",wCcheMT," \ n");
if Sum(wCcheMT)=p^row-rank)
then
     Print("Ok...Ok"," \ n");
     else
     Print("Bad.....Bad"," \ n");
fi; Print(" "," \ n");

r5:=Runtime(); Print("total running time:  ",r5-r0," \ n");
```

A.4.2 Non-cyclic Abelian codes Program (2)

```
LogTo("newlog.txt");
LoadPackage("guava");
r0:=Runtime();


pm := [2,2,2] ; g:=AbelianGroup(pm);


Print("-------Group [G(",pm,")]--------------","\n");


cl:=ConjugacyClassesSubgroups(g);
l:=LatticeSubgroups(g);
maxsub:=MaximalSubgroupsLattice(l);


p:=3; k1:=1; k2:=k1+1; Level1:=[]; Level2:=[]; rwl:=[]; cwl:=[];nu:=[]; rwlmT:=[]; cwlmT:=[];


for i in [1..Size(cl)]
    do
    ri:=Representative(cl[i]);
    if i>1
     then pi:=Size(FactorsInt(Size(ri)));
     else pi:=0;
    fi;
    if pi=k1
     then Add(Level1,i);
     else
     if pi=k2
      then Add(Level2,i);
     fi;
    fi;
    od;


Print("This group has an order of ",Size(ri),",","\n");
Print(i," Conjugacy Classes of Subgroups and ","\n");
Print(pi," levels of the Hasse diagram.","\n"); Print(" ","\n");


m1:=NullMat(Size(Level1),Size(Level2));


for r in [1..Size(Level1)]
do
   rs:=Level1[r];
   for c in [1..Size(Level2)]
   do
    cs:=Level2[c];
    for j in [1..Size(maxsub[cs])]
    do
     k:=maxsub[cs][j][1];
     if k=rs then
```

```
        m1[r][c]:=1;
       fi;
      od;
    od;
od;


Print("--------Matrix (M) and its properties-----------------------------)","\n");

Print(" ","\n");
Print("A matrix (M) constructed from level ",k1," versus level ",k2," over GF(",p,"):","\n");
#PrintArray(m1);
r1:=Runtime();
row:=DimensionsMat(m1)[1];
col:=DimensionsMat(m1)[2];
Print("number of rows:  ",row,"\n");
Print("number of columns:  ",col,"\n");
Print("\n");


for i in[1..DimensionsMat(m1)[1]]
do wr:=Sum(m1[i]);
   Add (rwl,wr);
od;
Print("Max row weight is:  ",Maximum(rwl),"\n");
Print("Min row weight is:  ",Minimum(rwl),"\n");


m1T:= TransposedMat(m1);
for i in[1..DimensionsMat(m1)[2]]
do
   wc:=Sum(m1T[i]);
   Add (cwl,wc);
od;
Print("Max col weight is:  ",Maximum(cwl),"\n");
Print("Min col weight is:  ",Minimum(cwl),"\n");
Print(" ","\n");

mat:=m1*Z(p);;
rank:=RankMat(mat);
Print("Rank of matrix over GF(",p,") is:  ", rank,"\n");
r1:=Runtime(); Print("runtime:  ",r1-r0,"\n");


Print("-------------Null-Space Of M,(M as a check matrix)-------","\n");


CcheM:=CheckMatCode(m1,GF(p));
Print("Code is ",CcheM,"\n");


wCcheM:=WeightDistribution(CcheM);
Print("weight distribution:  ",wCcheM,"\n");


if Sum(wCcheM)= p^(col - rank)
```

```
   then
     Print("Ok...Ok","\n");
    else
    Print("Bad.....Bad","\n");
fi;
Print(" ","\n");
r4:=Runtime(); Print("runtime:  ",r4-r1,"\n");

Print("-------------Null-Space Of MT,(MT as a check matrix)-------","\n");
CcheMT:=CheckMatCode(m1T,GF(p));
Print("Code is ",CcheMT,"\n");
wCcheMT:=WeightDistribution(CcheMT);
Print("weight distribution:  ",wCcheMT,"\n");


if Sum(wCcheMT)= p^(row - rank)
   then
    Print("Ok...Ok","\n");
    else
    Print("Bad.....Bad","\n");
fi;
Print(" ","\n");
r5:=Runtime(); Print("runtime:  ",r5-r4,"\n");
Print("total running time:  ",r5-r0,"\n");
```

A.4.3 Sample of raw Data from program(1)

Samples of Raw Data from program(1)

```
length n:=4 layer m:=2
A matrix (M) constructed from level 1
versus level 2 over GF(2):  [[ 1, 1, 0, 1,
0, 0 ], [ 1, 0, 1, 0, 1, 0 ], [ 0, 1, 1, 0,
0, 1 ], [ 0, 0, 0, 1, 1, 1 ] ]

runtime:  31

number of rows:  4 number of columns:  6

Max row weight is:  3 Min row weight is:  3
Max col weight is:  2 Min col weight is:  2

Rank of matrix over GF(2) is:  3
runtime:  0

-------------Null-Space 0f M,(M as a check
matrix)-------
Code is a linear [6,3,1..3]2 code defined
by check matrix over GF(2)
weight distribution:  [ 1, 0, 0, 4, 3, 0, 0
] Ok...Ok
runtime:  281

------Null-Space of M Transposed,(MT as a
check matrix)------
code is:  a linear [4,1,4]2 code defined by
check matrix over GF(2)
weight distribution:  [ 1, 0, 0, 0, 1 ]
Ok...Ok
runtime:  78
total running time:  390
```

A.4.4 Sample of Raw Data from program 2

Samples of Raw Data from program(2)

```
-------Group [G([ 2, 2, 2 ])]--------------
This group has an order of 8, 16 Conjugacy
Classes of Subgroups
and 3 levels of the Hasse diagram.
There are 7 subgroups in level 1
There are 7 subgroups in level 2
--------Matrix (M) and its
properties-----------------------------
A matrix (M) constructed from level 1
versus level 2 over GF(3):  [ [ 1, 0, 1, 0,
0, 1, 0 ], [ 1, 1, 0, 0, 1, 0, 0 ], [ 1, 0,
0, 1, 0, 0, 1 ], [ 0, 1, 1, 1, 0, 0, 0 ], [
0, 0, 1, 0, 1, 0, 1 ], [ 0, 1, 0, 0, 0, 1,
1 ], [ 0, 0, 0, 1, 1, 1, 0 ] ]
number of rows:  7 number of columns:  7
Max row weight is:  3 Min row weight is:  3
Max col weight is:  3 Min col weight is:  3
Rank of matrix over GF(3) is:  6
runtime:  531
-------------Null-Space Of M,(M as a check
matrix)-------
Code is a linear [7,1,7]4 code defined by
check matrix over GF(3)
weight distribution:  [ 1, 0, 0, 0, 0, 0,
0, 2 ] Ok...Ok
runtime:  375
------Null-Space of M Transposed,(MT as
a check matrix)------- Code is a linear
[7,1,7]4 code defined by check matrix over
GF(3)
weight distribution of CcheMT: [ 1, 0, 0,
0, 0, 0, 0, 2 ] Ok...Ok
runtime:  79 total running time:  985
```