

**CONSTRUCTING DESIGNS AND CODES FROM
THE FIXED POINTS OF ALTERNATING GROUPS**

by

KEKANA MADIMETJA JAN

Dissertation

Submitted in fulfillment of the requirements for the degree of

MASTER OF SCIENCE

in

MATHEMATICS

in the

FACULTY OF SCIENCE AND AGRICULTURE

School of Mathematics and Computer Sciences

at the

UNIVERSITY OF LIMPOPO

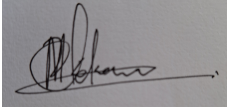
Supervisor: Dr A Saeidi

Co-Supervisor: Prof. T.T Seretlo

2024

Declaration

I declare that dissertation hereby submitted to the University of Limpopo, for the degree Master of Science in Mathematics has not previously been submitted by me for a degree at this or any other university; that it is my work in design and in execution, and that all material contained herein has been duly acknowledged.

Signed: 

Date: 09 October 2023

Dedication

I dedicate this work to honour the memory of my late father Hendrick Madimetja Kekana, may he continue to rest in perfect peace.

Abstract

The study of finite structures in discrete mathematics is a broad area which has many influential results not only in mathematics but also in practice. It is well known that 1–designs have many applications in coding theory. The construction of these designs and codes from fixed points of alternating groups plays a central role in obtaining properties of codes, structures and other general results that are useful in application of coding theory.

In this dissertation we construct some 1–designs from (Key-Moori method 2) and J Moori Method 3. In (Key-Moori method 2), we have a technique from which a large number of non-symmetric 1–designs could be constructed from maximal subgroups and conjugacy classes of elements of finite groups. In this dissertation, we consider the alternating group $G = A_n$ with its maximal subgroup $M = A_{n-1}$ where nX is a conjugacy class of elements of order n in G . Let $g \in nX$, then $|C_g| = |[g]| = [G : C_G(g)]$.

Using J Moori Method 3, we construct some 1–designs from the fixed points of elements of alternating groups. While J Moori has accomplished most of the work by constructing all designs and codes for alternating groups, and A Saeidi constructed designs and codes from involutions of alternating groups A_n and for maximamal subgroup isomorphic to S_{n-2} . In this dissertation we will be looking at other maximal subgroups (particularly the maximal subgroup A_{n-1} of A_n) which are not covered by J Moori and A Saeidi. Therefore, making this work an extention to J Moori and A Saeidi work.

Acknowledgement

I would like to express my words of gratitude and give thanks to my supervisor's Dr Amin Saeidi and Professor Thekiso Seretlo for their wonderful guidance and encouragement given to me during my studies which led to the completion of this dissertation. Am also grateful for the resource that were made available to me in pursuing my studies by the Department of Mathematics and Applied Mathematics at the University of Limpopo.

I also extend my sincere gratitude and acknowledge my family(my mother Maria Kekana and my siblings) and friends whom played a major role by giving words of advice and encouragement through this journey. My special thanks to my colleague friend Mr Nyikadzino Gift Tapiwanashe for the tremendous advices he gave all the time.

Lastly I would like express my sincere gratitude to the Almighty God(God of Mount Zion) for having safe guarded me up until I witness this day.

Notation and Convention

Throughout this dissertation all groups will be assumed to be finite. We will use notations and terminology from [21] and the ATLAS [10].

\mathbb{N}	Set of natural numbers
\mathbb{Z}	Set of Integers
\mathbb{R}	Set of real numbers
X	Finite set
\emptyset	empty set
$ X $	the cardinality of the set X
V	Vector Space
\mathbb{F}	A finite field
\mathbb{F}_q	A Galois field of q elements
G	a group
1_G	the identity element in G
$H \leq G$	H is a subgroup of G
$N \trianglelefteq G$	N is a normal subgroup of G
$[G : H]$	the index of H in G
G/H	the quotient group
C_g	the conjugacy class of g in G with representative g
$N_G(H)$	the normalizer of the subgroup H in G
$C_G(H)$	the centralizer of the subgroup H in G
$Fix_\Omega(g)$	the number of the elements in a set Ω fixed by $g \in G$ under the group action

χ	a character of finite group
χ_ϕ	a character afforded by the representation ϕ
$tr(A)$	the trace of a matrix A
M	A maximal subgroup of G
S_n	the symmetric group on n symbols
A_n	the alternating group on n symbols
$G : H$	a split extension of G by H
$G.H$	general extension
G, H, K	groups
$Aut(C)$	Automorphism group of a code C
$Aut(\mathcal{D})$	Automorphism group of a design \mathcal{D}
$[n, k, d]_q$	a q -ary code of length n , dimension k and minimum distance d

Contents

1	Introduction	1
2	Group Theory	4
2.1	Groups	4
2.1.1	Isomorphism Theorems	7
2.2	Group action and permutation groups	8
2.3	Alternating Groups	14
3	Representation Theory of Finite Groups	18
3.1	Permutation Representation	18
3.2	Character Theory	21
3.2.1	Permutation Character	24
4	Designs and Codes	26
4.1	Designs	26
4.2	Codes	30
4.2.1	Codes from designs	35
5	Key-Moori (Method 1 and 2) and Moori Method 3	36
5.1	Key-Moori Method 1	36
5.2	Key-Moori Method 2	38
5.3	J. Moori Method 3	41

6	Construction of Designs from Method 2 and 3	45
6.1	Designs from Method 2	47
6.1.1	Examples of Designs from A_n using Method 2.	48
6.2	Designs from Method 3	50
6.2.1	Examples of designs from A_n using Method 3	53

Chapter 1

Introduction

The concept of coding theory was formulated to ensure reliable transmission of information over a noisy channel, and this is one of the basic requirements of digital information and communication systems. Coding theory was initiated by the work of C. Shannon with his 1948 seminal paper [51]. Motivated by problems from information transmission, he proved that when a message is transmitted over a noisy channel, it is possible to encode it in such a way that it is received with an arbitrary low error rate. The study of finite structures in discrete mathematics is a broad area which has many influential results not only in mathematics but also in practice. Finite groups are used to construct designs and codes. The construction of 1-designs and codes from fixed points of alternating groups plays a central role in obtaining properties of codes, structures and other general results that are useful in application of coding theory. Codes associated with these designs over the finite field is the space spanned by the incidence vectors of the blocks over the field.

The first two methods were introduced by JD Key and J Moori in [22] where designs are constructed from the conjugacy classes of maximal subgroups and from the conjugacy classes of elements of finite primitive groups, of which the two methods were presented by Moori in (Information Security, Coding Theory and Related Combinatorics 2011) [33] and are commonly known as Key-Moori Method 1 and 2.

Methods 1 and 2 were both successfully applied to many finite simple groups in various papers like, on the automorphism of designs constructed from finite simple group by Tung Le and J Mouri [27], family of Suzuki group $Sz(q)$ where q is an odd power of 2 by J Mouri and A Saeidi [40], designs from maximal subgroups and conjugacy classes of finite simple group by Key and Mouri [24] and many other papers, see for example [38, 35, 12, 15, 37, 14, 13, 32, 42, 28, 41, 19, 20].

The third Method is the subject of the recent paper [30]. Method 3 is about designs from fixed points of transitive groups. In [29] the Method 3 was applied on fixed points of involutions of the alternating group A_n (*for* $n > 5$) on action of Ω , 2-subsets of the set Γ of size n . The study in [30] was completed by A Saeidi in [49] by constructing designs for all elements of the maximal subgroup isomorphic to S_{n-2} . Therefore, our main priority is to construct designs and associated codes using Method 3 from the fixed points of alternating groups. One of the main problems that arises in design theory is the classification of structures with the given parameters and a prescribed automorphism group. The construction of primitive designs from finite simple groups gives additional information on the group acting on a design, which is interesting from both the group theoretical and combinatorial point of view. While on the other hand designs have had tremendous impact in coding theory since the geometry of the design helps in the determination of the weight distribution of the code. Also, the properties of designs can be used in decoding algorithms, and geometrical configurations can be used to define good codes. We want to study the 1-designs and obtain codes from those designs using Method 2 and Method 3, where our main focus would be on Method three since our study is based on the fixed points of simple groups.

In Chapter 2, we give a brief background about the notion of groups which will be required in the sequel. The link between groups and combinatorial structures has proved and provided useful results in coding theory.

In Chapter 3, we present the general results from representation theory of finite groups.

The basic notion of permutation representation and permutation character plays an important role in determining the designs from Key-Moori Method 1 *and* 2. Where in Method 1 they consider the primitive permutation representation of simple groups to construct symmetric 1-designs, and in Method 2 we consider $\chi_M = \chi(G|M)$ the permutation character afforded by the action of group G on a finite set Ω , which is the set of all conjugates of M in G .

In Chapter 4, we introduces the theory of combinatorial structures needed in Chapter 5 and Chapter 6. We start by giving the notation, definitions and some properties of designs and codes.

In Chapter 5, we give full details of the two Key-Moori Methods and the third method by Moor, and these Methods will be applied to constructs designs from the fixed points of alternating groups. More specifically we will focus on Method two and three.

In Chapter 6, we consider the alternating group A_n with its maximal subgroup A_{n-1} and firstly show that for all n , the group $M = A_{n-1}$ is maximal in $G = A_n$. We then apply Method 2 and Method 3 to some of the alternating groups and construct designs. Since in this chapter we obtain main results for Method 2 we give the explicit formulae for the parameters of designs constructed from the alternating group A_n , acting on the set of all conjugacy classes of the maximal subgroup A_{n-1} and the fixed points of an arbitrary element g in A_n . Hence giving few examples of designs constructed from the method. With Method 3, we use the results of Method 2 to obtain the first two parameters of the design. Since in this study the group G is acting on M by conjugation, then the first parameter is just given by $|A_n : A_{n-1}| = n$. Hence our main work in Method 3 is to compute the third parameter.

Chapter 2

Group Theory

The main aim of this chapter is to give a brief overview about some important notions from the theory of groups (groups, permutation groups and alternating groups) which will be required in the subsequent chapters. Most of the results could be found in standard texts such as [8, 44, 45, 46, 50].

2.1 Groups

Definition 2.1.1 *Let X and Y be sets. Then the relation r from X to Y is a subset of $X \times Y$.*

Definition 2.1.2 *Let X be a set and r be a relation from X to X with the following properties:*

(i) *r is reflexive: $(x, x) \in r \forall x \in X$*

(ii) *r is symmetric: If $(x, y) \in r$, then $(y, x) \in r$.*

(iii) *r is transitive: If $(x, y) \in r$ and $(y, z) \in r$, then $(x, z) \in r$.*

Then r is called an equivalence relation on X .

Definition 2.1.3 *Let X be a set and r be an equivalence relation on X . Then for all $x \in X$ we define an equivalence relation, $[X]$, of class x by*

$$[x] = \{y \in X \mid (x, y) \in r\}.$$

Then $[x]$ is called the equivalence class of x .

Theorem 2.1.1 Let r be an equivalence relation on a set X and let $x, y \in X$. Then either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

Definition 2.1.4 A group $\langle G, * \rangle$ is a set G together with a binary operation $*$ closed on G such that the following axioms are satisfied:

(i) $*$ is associative i.e. $\forall f, g$ and $h \in G$, we have $f*(g*h) = (f*g)*h$.

(ii) $\exists e \in G$ (identity element in G) such that $e*x = x*e$ for all $x \in G$.

(iii) $\forall a \in G, \exists a' \in G$ (called the inverse) such that $a*a' = a'*a = e$.

Sometimes e is referred to as 1_G .

Definition 2.1.5 Let G be a group. A non-empty subset H of G is called a subgroup of G if H is a group under the same binary operation in G , and we write $H \leq G$.

Remark 2.1.1 Let G be a group. The subgroup $\{e\}$ is called the trivial subgroup of G . If $H \leq G$ and $H \neq G$, we say that H is a proper subgroup of G and we write $H < G$.

Lemma 2.1.1 Let G be a group and H a non-empty subset of G . Then H is a subgroup of G if and only if for every $a, b \in H$, we have $ab^{-1} \in H$.

Definition 2.1.6 Let $H \leq G$. Then for $a \in G$, we define the left and right cosets of H in G respectively as

$$aH = \{ah \mid h \in H\} \text{ and } Ha = \{ha \mid h \in H\}.$$

Theorem 2.1.2 Let G be a finite group and $H \leq G$, then we have $|H|$ divides $|G|$.

Definition 2.1.7 The elements x and y commute if $xy = yx$. We say x is a central element if x commutes with every element of G . The set of all central elements of G is called the center of G , denoted by $Z(G) = \{g \in G \mid gx = xg, \forall x \in G\}$.

Definition 2.1.8 Let G be group and $x \in G$. The centralizer of x in G is defined as follows:

$$C_G(x) = \{a \in G \mid ax = xa\}.$$

Lemma 2.1.2 For every $x \in G$, $C_G(x)$ is a subgroup of G , containing $Z(G)$. Moreover we have

$$Z(G) < C_G(x).$$

Definition 2.1.9 Let $N \leq G$. We say that N is normal in G if for every $a \in G$, we have $aN = Na$. We write $N \triangleleft G$.

Definition 2.1.10 A group G is said to be **simple** if the only normal subgroups of G are 1_G and G itself.

Definition 2.1.11 If $H \leq G$, we define

$$a^{-1}Ha = \{a^{-1}ha : h \in H\}.$$

We call $a^{-1}Ha$ a conjugate of H and denote it by H^a .

Theorem 2.1.3 Let $H \leq G$. Then $a^{-1}Ha = H$ is also a subgroup of G .

Lemma 2.1.3 Let $H \leq G$. Then H is normal in G if $a^{-1}Ha = H$ for all $a \in G$.

Definition 2.1.12 Let G be a group and $a, b \in G$. We say that a and b are **conjugate** in G if there exists an element $g \in G$ such that $ga = bg$. Equivalently, $b = gag^{-1}$.

Definition 2.1.13 The equivalence classes of the conjugacy relation are called the conjugacy classes of G . The conjugacy class of the element a in G is denoted by

$$a^G = \{gag^{-1} : g \in G\}.$$

Theorem 2.1.4 Let $H \leq G$. Then H is normal in G if and only if H is a union of conjugacy classes of G .

Definition 2.1.14 Let $H \leq G$, the **normalizer** $N_G(H)$ of H in G , is defined as

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

If $H = G$, then $N_G(H) = G$.

2.1.1 Isomorphism Theorems

Definition 2.1.15 Let G_1 and G_2 be groups. A function $\phi : G_1 \rightarrow G_2$ is called a *homomorphism* if $\phi(xy) = \phi(x)\phi(y)$.

Lemma 2.1.4 Let $\phi : G_1 \rightarrow G_2$ be a homomorphism. Then,

1. $\phi(e) = e$.
2. For any $a \in G_1$, we have $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof: See [45]. □

Definition 2.1.16 Let $\phi : G_1 \rightarrow G_2$ be a homomorphism. Then we define the **kernel** and **image** of the homomorphism respectively as follows:

1. $\ker(\phi) = \{x \in G_1 : \phi(x) = e\}$.
2. $\text{Im}(\phi) = \{\phi(x) : x \in G_1\}$.

Lemma 2.1.5 Let $\phi : G_1 \rightarrow G_2$ be a homomorphism. Then:

1. $\ker(\phi) \trianglelefteq G_1$.
2. $\text{Im}(\phi) \leq G_2$.

Proof: See [45]. □

Theorem 2.1.5 (First Isomorphism Theorem) If $\phi : G_1 \rightarrow G_2$ is a homomorphism, then ϕ induces an isomorphism:

$$G_1/\ker(\phi) \cong \text{Im}(\phi)$$

In particular, if ϕ is an epimorphism, then $G_1/\ker(\phi) \cong G_2$.

Proof: See [44, Theorem 1.4.3]. □

Theorem 2.1.6 (Second Isomorphism Theorem) *If H and K are subgroups of G and $K \trianglelefteq G$, Then we have:*

$$H/(H \cap K) \cong (HK)/K.$$

Proof: See [44, Theorem 1.4.4]. □

Theorem 2.1.7 (Third Isomorphism Theorem) *Let H and K be normal subgroups of G and $H \subset K$. Then, K/H is a normal subgroup of G/H . Then $(G/H)/(K/H) \cong G/K$.*

Proof: See [44, Theorem 1.4.5]. □

2.2 Group action and permutation groups

Group action is an important notion in group theory, since it gives an abstract group a more concrete aspect and a better tool to the understanding of the set X on which the group is acting, where a set can be the group itself or a subset of that group. Group action constitutes the main tool used in the construction methods that will be applied throughout this study. The notion of group action is in relation with the notion of permutation groups.

Definition 2.2.1 *Let X be a set. A **permutation** of X is a bijection of X onto X . The set of all permutations of X form a group called the **symmetric group** of X and is denoted by S_X .*

Definition 2.2.2 *Let G be a group and X be a set. We say that G **acts** on X if there exists a homomorphism $\phi : G \rightarrow S_X$. Then $\phi(g) \in S_X$ for all $g \in G$, and the action of $\phi(g)$ on X is denoted by x^g for any $x \in X$. We say that G is a **permutation group** on X .*

Definition 2.2.3 (Orbits). *Let G acts on a set X and let $x \in X$. Then the **orbit** of x under the action of G is defined by $x^G = \{x^g | g \in G\}$.*

Theorem 2.2.1 *Let G acts on a set X . The set of all orbits of G on X form a partition of X .*

Proof: We define the relation \sim on X by $x \sim y$ if and only if $x = y^g$ for some $g \in G$. It can be shown that \sim is an equivalence relation on X . Then $[x] = \{x^g | g \in G\} = x^G$. Hence the set of all orbits of G on X partitions X . \square

Example 2.2.1 (i) **(Action by left multiplication).** If G acts on itself by left regular representation, then for all $g \in G$ we have,

$$g^G = \{g^h | h \in G\} = \{hg | h \in G\} = Gg = G.$$

Hence under the action of G , we have only one orbit which is G itself.

(ii) If G acts on G/H , the set of all left cosets of H in G , then for all $aH \in G/H$ we have

$$(aH)^G = \{(aH)^g | g \in G\} = \{gaH | g \in G\} = G/H.$$

In this case we have only one orbit which is G/H .

(iii) **(Action by conjugation).** Assume that G acts on itself by conjugation, that is for $g \in G$ and for all $x \in G$ we have $x^g = gxg^{-1}$. Then,

$$x^G = \{x^g | g \in G\} = \{gxg^{-1} | g \in G\} = [x]$$

the conjugacy class of x in G . Moreover $|x^G| = |[x]| = [G : C_G(x)]$. In this case the number of orbits is equal to the number of conjugacy classes of G .

(iv) **(Action on the conjugates of a subgroup).** If for all $H \leq G$, G acts on the set of all its subgroups by conjugation, that is $H^g = gHg^{-1}$ for all $g \in G$, then for a fixed H in G we have

$$H^G = \{H^g | g \in G\} = \{gHg^{-1} | g \in G\}$$

the set of all conjugates of H in G . In this case the number of orbits of G is equal to the number of conjugacy classes of subgroups of G .

Definition 2.2.4 (Stabilizer). If G acts on a set X and $x \in X$ then the **stabilizer** of x in G , denoted by G_x is the set $G_x = \{g \mid x^g = x\}$. In other words, G_x is the set of elements of G that fixes x .

Theorem 2.2.2 Let G act on a set X . Then,

(i) $G_x \leq G$ for every $x \in X$.

(ii) $|x^G| = [G : G_x]$, this is, the number of elements in the orbit of x is equal to the index of G_x in G .

Proof:

(i) Since $x^{1_G} = x$, then $1_G \in G_x$. Hence $G_x \neq \emptyset$. Let $g, h \in G_x$. Then $x^g = x^h = x$. So that $(x^g)^{h^{-1}} = (x^h)^{h^{-1}} = x^{1_G} = x$, and therefore $x^{gh^{-1}} = x$ for all $x \in X$. Thus $gh^{-1} \in G_x$. Which implies that $G_x \leq G$.

(ii) Since

$$\begin{aligned} x^g = x^h &\Leftrightarrow x = x^{hg^{-1}} \\ &\Leftrightarrow hg^{-1} \in G_x \\ &\Leftrightarrow (G_x)g = (G_x)h, \end{aligned}$$

the map $\gamma : x^G \rightarrow G/G_x$ given by $\gamma(x^g) = (G_x)g$ is well-defined and one-to-one. Obviously γ is onto. Hence there is a one-to-one correspondence between x^G and G/G_x . Thus $|x^G| = |G/G_x| = |G : G_x|$. \square

Lemma 2.2.1 If G is a finite group acting on a finite set X then for all $x \in X$, $|x^G|$ divides $|G|$.

Proof: By Theorem 2.2.2 we have

$$|x^G| = [G : G_x] = |G|/|G_x|.$$

$$\Rightarrow |G| = |x^G| \times |G_x|.$$

Hence $|x^G|$ divides $|G|$. □

Theorem 2.2.3 (Application of Theorem 2.2.2).

(i) If G is a finite group, then for all $g \in G$ the number of conjugates of g in G is equal to $[G : C_G(g)]$.

(ii) If G is a finite group and H is a subgroup of G , then the number of conjugates of H in G is equal to $[G : N_G(H)]$.

Proof:

(i) Since G acts on itself by conjugation, applying Theorem 2.2.2 we have $|g^G| = [G : G_g]$.

But since

$$g^G = \{g^h | h \in G\} = \{hgh^{-1} | h \in G\} = [g]$$

and

$$G_g = \{h \in G | g^h = g\} = \{h \in G | hgh^{-1} = g\} = \{h \in G | hg = gh\} = C_G(g)$$

we have

$$|g^G| = |[g]| = [G : G_g] = [G : C_G(g)] = \frac{|G|}{|C_G(g)|}.$$

□

(ii) Let G acts on the set of all its subgroups by conjugation. Then by Theorem 2.2.2 (ii) we have $|H^G| = [G : G_H]$. Since

$$H^G = \{H^g | g \in G\} = \{ghg^{-1} | g \in G\} = [H]$$

and

$$G_H = \{g \in G | H^g = H\} = \{g \in G | gHg^{-1} = H\} = N_G(H)$$

we have

$$|[H]| = |H^G| = [G : G_H] = [G : N_G(H)] = \frac{|G|}{|N_G(H)|}.$$

□

Definition 2.2.5 (Transitive Groups). Let G be a group acting on a set X . If G has only one orbit on X , then we say that G is **transitive** on X , otherwise we say that G is **intransitive** on X . If G is transitive on X , then $x^G = X$ for all $x \in X$ which implies that for all $x, y \in X$, there is $g \in G$ such that $x^g = y$.

Remark 2.2.1 If G is a finite transitive group on a finite set X , then Theorem 2.2.2 implies that $|x^G| = |X| = |G|/|G_x|$. Hence $|G| = |X| \times |G_x|$.

Definition 2.2.6 Suppose G act on a set X and let $|X| = n$ and $1 \leq k \leq n$ be a positive integer. We say that G is **k -transitive** on X if two ordered k -tuples (x_1, x_2, \dots, x_k) and (y_1, y_2, \dots, y_k) with $x_i \neq x_j$ and $y_i \neq y_j$ for $i \neq j$ there exist $g \in G$ such that $x_i^g = y_i$ for $i = 1, 2, \dots, k$.

Lemma 2.2.2 Let G be a transitive group on a set Ω , $|\Omega| = n \geq 2$. If G_α is $(k-1)$ -transitive on $\Omega \setminus \{\alpha\}$ for every $\alpha \in \Omega$, then G is k -transitive on Ω .

Proof: See [8, Lemma 1.3.6].

□

Definition 2.2.7 A permutation group G is **primitive** on Ω if G is transitive on Ω and the only G -invariant partitions of Ω are the trivial partitions. Also G is **imprimitive** on Ω if G preserves some non-trivial partition on Ω .

Theorem 2.2.4 (i) For every n , the symmetric group S_n acts n -transitively on $\Omega = \{1, 2, \dots, n\}$.

(ii) For $n \geq 3$ the alternating group A_n acts $(n-2)$ -transitively, but not $(n-1)$ -transitively on Ω .

Proof:

- (i) Since S_n contains all permutations of the set Ω , it is clearly n -transitive on Ω .
- (ii) We use induction on n , beginning with the fact that A_3 is transitive, but not $(n-2)$ -transitive on $\{1, 2, 3\}$. For $n > 3$ we have that $(A_n)_n = A_{n-1}$, and A_{n-1} is $(n-3)$ -transitive on $\{1, 2, 3, \dots, n-1\}$ by the induction hypothesis. So A_n is $(n-2)$ -transitive by Lemma 2.2.2. Now suppose that A_n is $(n-1)$ -transitive, then there is $g \in A$ fixing each $1, 2, 3, \dots, n-2$ and taking $n-1$ to n . But the only $g \in A$ which does this is the transposition $(n-1 \ n) \notin A_n$. □

Theorem 2.2.5 *Every k -transitive group G (with $k \geq 2$) acting on a set Ω , is primitive.*

Proof: See [8, Lemma 1.6.3]. □

Theorem 2.2.6 *Let G be transitive permutation group on a set Ω . Then G is primitive if and only if G_α is a maximal subgroup of G for every $\alpha \in \Omega$*

Proof: See [46]. □

Theorem 2.2.7 *(Characterization of primitive permutation groups). Let G be a permutation group on the set Ω , then G is primitive if and only if for all $\alpha \in \Omega$ the stabilizer G_α is a maximal subgroup.*

Proof: See [8, Lemma 1.6.5]. □

Theorem 2.2.8 *(Classification of finite simple groups). Every finite simple group is isomorphic to one of the following, a group of prime order, an alternating group, one of the group of lie type or one of the 26 sporadic groups.*

Proof: See [46]. □

2.3 Alternating Groups

Definition 2.3.1 *The group of all bijective maps (permutations) $\phi : X \rightarrow X$, where X is a non-empty set is called the **symmetric group** on X and denoted by S_X . If $|X| = n$, then S_X is denoted by S_n and the order is $|S_n| = n!$.*

We use the cycle notation for the elements of S_n . Let $\sigma \in S_n$, $\sigma = (k_1 k_2 \cdots k_r)$, then σ is called an r -cycle, and this means that every k_i moves to k_{i+1} if $i < r$ and k_r moves to k_1 , while $n - r$ elements remains fixed. A non unique decomposition for any permutation σ into 2-cycles is possible (any permutation σ of r -cycle can be written as a products of 2-cycles) and the number of the 2-cycles determines whether a permutation σ is even or odd.

Definition 2.3.2 *(i) Any permutation of length 2 or a 2-cycle is called a **transposition**.
(ii) Any permutation that can be written as an even number of transpositions is called an **even permutation**, and any permutation that can be written as an odd number of transpositions is called an **odd permutation**.*

Definition 2.3.3 *The set of all even permutation in S_n form a normal subgroup of S_n known as the **alternating group** denoted by A_n . This group has order $n!/2$.*

If we consider the even permutation $\sigma = (1\ 2\ 3)$ then $C_\sigma^{A_5} = C_\sigma^{S_5}$ and contains 20 elements, whereas if we take σ to be the permutation $(1\ 2\ 3\ 4\ 5) \in A_5$, then $|C_\sigma^{A_5}| = 12$ and $|C_\sigma^{S_5}| = 24$. So an interesting question arises as to when does the conjugacy class of the even permutation σ in A_n coincide with that of σ considered in S_5 ? But before, we show that two distinct conjugacy classes have no elements in common.

Proposition 2.3.1 *If $x, y \in G$, then either $x^G = y^G$ or $x^G \cap y^G = \emptyset$*

Proof: Suppose that $x^G \cap y^G \neq \emptyset$, and pick $r \in x^G \cap y^G$. Then there exist $g, h \in G$ such that

$$r = g^{-1}xg = h^{-1}yh.$$

Hence $x = gh^{-1}yhg^{-1} = k^{-1}yk$, where $k = hg^{-1}$. So

$$\begin{aligned} a \in G &\Rightarrow a = b^{-1}xb \text{ for some } b \in G \\ &\Rightarrow a = b^{-1}k^{-1}ykb \\ &\Rightarrow a = c^{-1}yc \text{ where } c = kb \\ &\Rightarrow a \in y^G. \end{aligned}$$

Therefore $x^G \subseteq y^G$. Similarly $y^G \subseteq x^G$ (using $y = kxk^{-1}$) and so $x^G = y^G$. □

The following results are often useful when calculating conjugacy classes.

Lemma 2.3.1 *Let $x, y \in G$. If x is conjugate to y in G , then x^n is conjugate to y^n in G for every integer n , and x and y have the same order.*

Proof: Firstly we observe that for $a, b \in G$, we have

$$g^{-1}abg = (g^{-1}ag)(g^{-1}bg).$$

Hence $g^{-1}x^ng = (g^{-1}xg)^n$. Suppose that x is conjugate to y in G , so that $y = g^{-1}xg$ for some $g \in G$. Then $y^n = g^{-1}x^ng$ and therefore x^n is conjugate to y^n in G . Let x have order m . Then $y^m = g^{-1}x^mg = 1$, and for $0 < r < m$, $y^r = g^{-1}x^rg \neq 1$, so y also has order m . □

Theorem 2.3.1 *Let $x \in G$. Then the size of the conjugacy class x^G is given by*

$$|x^G| = |G : C_G(x)| = |G|/|C_G(x)|.$$

In particular, $|x^G|$ divides $|G|$.

Proof: We observe that for $g, h \in G$, we have

$$\begin{aligned} g^{-1}xg = h^{-1}xh &\Leftrightarrow hg^{-1}x = xhg^{-1} \\ &\Leftrightarrow hg^{-1} \in C_G(x) \\ &\Leftrightarrow C_G(x)g = C_G(x)h \end{aligned}$$

To this end, we may define an injective function f from x^G to the set of right cosets of $C_G(x)$ in G by

$$f : g^{-1}xg \rightarrow C_G(x)g \quad (g \in G).$$

Clearly f is surjective. Hence f is a bijection, proving that $|x^G| = |G : C_G(x)|$. □

Note 2.3.2

$$\begin{aligned} |x^G| = 1 &\Leftrightarrow g^{-1}xg = x \\ &\Leftrightarrow x \in Z(G) \end{aligned}$$

where $Z(G)$ is the center of G .

Theorem 2.3.3 *Let x_1, x_2, \dots, x_i be representatives of the conjugacy classes of G . Then*

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |x_i^G|,$$

where $|x_i^G| = |G : C_G(x_i)|$, and both $|Z(G)|$ and $|x_i^G|$ divide $|G|$.

Proof: See [18, Theorem 12.10]. □

Definition 2.3.4 *Let $\sigma \in A_n$. If $\sigma^{A^5} = \sigma^{S_5}$, then we say that the conjugacy class of σ does not split. Otherwise A_n will be a union of at least two conjugacy classes of S_5 . In this case, we say that the conjugacy class splits.*

Theorem 2.3.4 *Let $\sigma \in S_n$. If σ commutes with some odd permutation in S_n , then $C_\sigma^{A_n} = C_\sigma^{S_n}$. Otherwise $C_\sigma^{S_n}$ splits into two conjugacy classes in A_n of equal size.*

Proof:

- (i) Assume that σ commutes with an odd permutation g in S_n . Let $y \in C_\sigma^{S_n}$, so that $y = h^{-1}\sigma h$ for some $h \in S_n$, if y is even then $y \in C_\sigma^{A_n}$, and if y is odd then $gh \in A_n$ and

$$y = h^{-1}\sigma h = h^{-1}g^{-1}\sigma gh = (gh)^{-1}\sigma(gh),$$

so again $y \in C_\sigma^{A_n}$. Thus $C_\sigma^{S_n} \subseteq C_\sigma^{A_n}$, and so $C_\sigma^{A_n} = C_\sigma^{S_n}$.

- (ii) Assume that σ does not commute with any odd permutation. Then $C_{S_n}(\sigma) = C_{A_n}(\sigma)$. Hence by Theorem 2.3.1.

$$\begin{aligned}
|\sigma^{A_n}| &= |A_n : C_{A_n}(\sigma)| \\
&= \frac{1}{2} |S_n : C_{A_n}(\sigma)| \\
&= \frac{1}{2} |S_n : C_{S_n}(\sigma)| \\
&= \frac{1}{2} |\sigma^{S_n}|.
\end{aligned}$$

Next, we observe that

$$\{h^{-1}\sigma h : h \text{ is odd}\} = ((1\ 2)^{-1}\sigma(1\ 2))^{A_n}$$

since every odd permutation has the form $(1\ 2)a$ for some $a \in A_n$. Now

$$\begin{aligned}
\sigma^{S_n} &= \{h^{-1}\sigma h : h \text{ is even}\} \cup \{h^{-1}\sigma h : h \text{ is odd}\} \\
&= \sigma^{A_n} \cup ((1\ 2)^{-1}\sigma(1\ 2))^{A_n}.
\end{aligned}$$

Since $|\sigma^{A_n}| = \frac{1}{2}|\sigma^{S_n}|$, the conjugacy classes σ^{A_n} and $((1\ 2)^{-1}\sigma(1\ 2))^{A_n}$ must be disjoint and of equal size, as we wished to show. \square

Definition 2.3.5 Let X be a set of size n , we denote the set of all k subsets of X for $1 \leq k \leq n$ by $X^{\{k\}}$. If $k = 2$ we call $X^{\{2\}}$ the set of all **duads** of X .

Lemma 2.3.2 For $n \geq 3$ the alternating group A_n acts transitively on $X^{\{2\}}$ the set of duads of $X = \{1, 2, \dots, n\}$.

Proof: See [43, Lemma 2.4.11] \square

Chapter 3

Representation Theory of Finite Groups

Representation theory deals with representing elements of finite groups by $n \times n$ invertible matrices over the field $\mathbb{F} = \mathbb{C}$. The trace of such matrices defines the character of the finite groups as the map associating to each element of the group.

3.1 Permutation Representation

Definition 3.1.1 *A permutation representation of a group G is a homomorphism $\phi : G \rightarrow S_X$.*

Theorem 3.1.1 (Generalized Cayley Theorem). *Let H be a subgroup of G and let X be a set of distinct cosets of H in G . For any $x \in G$ the map $\phi_x : X \rightarrow X$ defined by $\phi_x(gH) = xgH$ is a permutation of X . The map ϕ_x is a homomorphism from G into S_X , and $\ker\phi = \bigcap_{g \in G} gHg^{-1}$*

Proof: We start by showing that ϕ_x is well-defined and injective. To establish this, we note that:

$$\begin{aligned}
gH = kH &\iff k^{-1}gH = H \\
&\iff k^{-1}g \in H \\
&\iff k^{-1}x^{-1}xg \in H \\
&\iff (xk)^{-1}xgH \in H \\
&\iff xgH = xkH \\
&\iff \phi_x(gH) = \phi_x(kH).
\end{aligned}$$

Therefore ϕ_x is well-defined and injective. For $x, y \in G$, consider ϕ_{xy} . For all $gH \in X$,

$$\begin{aligned}
\phi_{xy}(gH) &= (xy)gH = x\phi_y(gH) \\
&= \phi_x(\phi_y(gH)) \\
&= (\phi_x \circ \phi_y)(gH).
\end{aligned}$$

This shows that $\phi_{xy} = \phi_x \circ \phi_y$, so that $\phi(xy) = \phi_{xy} = \phi_x \circ \phi_y$ as required. We now show that $\ker\phi = \bigcap_{g \in G} gHg^{-1}$.

$$\begin{aligned}
\ker\phi &= \{x \in G \mid \phi_x = e_{s_X}\} \\
&= \{x \in G \mid \phi_x(gH) = gH, \forall g \in G\} \\
&= \{x \in G \mid xgH = gH, \forall g \in G\} \\
&= \{x \in G \mid g^{-1}xgH = H, \forall g \in G\} \\
&= \{x \in G \mid g^{-1}xg \in H, \forall g \in G\} \\
&= \{x \in G \mid x \in gHg^{-1}, \forall g \in G\} \\
&= \bigcap_{g \in G} gHg^{-1}.
\end{aligned}$$

□

The above Theorem has a number of corollaries. The first one is the special case which

we let $H = \{e\}$, with the result that $X = G$ and $\ker\phi = \{e\}$. Then we can reform the above Theorem to the following well known *Cayley Theorem*.

Theorem 3.1.2 (Cayley Theorem). *Every group G is isomorphic to a subgroup of S_G . In particular if, $|G| = n$, then G is isomorphic to a subgroup of S_n .*

Definition 3.1.2 (Permutation Matrix). *A permutation matrix is a matrix in which every row and column has a unique non-zero entry and all non-zero entries are equal to 1.*

Definition 3.1.3 *Let \mathbb{F} be a field. A general linear group $GL(n, \mathbb{F})$ is the group of invertible $n \times n$ matrices with entries in \mathbb{F} under the matrix multiplication.*

Remark 3.1.1 *Every permutation matrix is orthogonal and thus has an inverse that is again a permutation matrix, namely its transpose. In particular, all $n \times n$ permutation matrices lie in $GL(n, \mathbb{F})$.*

Corollary 3.1.1 *Any finite group G can be embedded into $GL(n, \mathbb{F})$, that is, G is isomorphic to subgroup of $GL(n, \mathbb{F})$.*

Proof: See [34, Corollary 1.1.2]. □

Theorem 3.1.3 *Let H be a proper subgroup of a finite group G with index n . Then there exists a proper normal subgroup N of G contained in H with finite index in G . Moreover $[G : N] | n!$.*

Proof: See [6, Corollary 2.1.4]. □

Lemma 3.1.1 *Let G be a simple group containing a proper subgroup H of finite index n . Then G is isomorphic to a subgroup of S_n .*

Proof: A homomorphism $\phi : G \rightarrow S_n$ which satisfies $\ker\phi = \bigcap_{g \in G} gHg^{-1}$ and $\ker\phi \leq H$ exist by **Generalized Cayley Theorem**. Since $\ker\phi \trianglelefteq G$ and G is simple, then $\ker\phi$ is either $\{e\}$ or G , But $\ker\phi \leq H \leq G$. Hence, $\ker\phi = \{e\}$, which is equivalent to saying that ϕ is a monomorphism. Therefore $G \cong \text{Im}\phi \leq S_n$. □

3.2 Character Theory

Definition 3.2.1 Character. Let $\rho : G \rightarrow G(n, \mathbb{C})$ be a representation of a group G . The character χ of ρ is a function $\chi : G \rightarrow \mathbb{C}$ given by $\chi(g) = \text{tr}(\rho(g)), \forall g \in G$. The degree of the character, $\text{deg}(\chi)$ is defined to be an integer n .

Definition 3.2.2 Class Function. If $\phi : G \rightarrow \mathbb{F}$ is a function that is constant on conjugacy classes of G , that is $\phi(g) = \phi(xgx^{-1})$ for all $x \in G$, then we say that ϕ is a **class function**.

Lemma 3.2.1 A character is a class function.

Proof: Let χ be a character of G . Then χ is afforded by a representation $\phi : G \rightarrow GL(n, \mathbb{F})$. Let $g \in G$, then for all $x \in G$ we have

$$\begin{aligned}\chi(xgx^{-1}) &= \text{tr}(\phi(xgx^{-1})) \\ &= \text{tr}(\phi(x) \cdot \phi(g) \cdot \phi(x^{-1})) \\ &= \text{tr}(\phi(x) \cdot \phi(g) \cdot [\phi(x)]^{-1}) \\ &= \text{tr}(\phi(g)) \\ &= \chi(g).\end{aligned}$$

□

Definition 3.2.3 (Equivalent Representation). Two representations $\rho, \phi : G \rightarrow GL(n, \mathbb{F})$ are said to be equivalent if there exists a $n \times n$ matrix P over \mathbb{F} such that $P^{-1}\rho(g)P = \phi(g)$, for all $g \in G$.

Theorem 3.2.1 Equivalent representations have the same character.

Proof: Let χ_1 and χ_2 be characters afforded by two representation ϕ_1 and ϕ_2 of degree n over a field \mathbb{F} . Assume that ϕ_1 is equivalent to ϕ_2 . Then there is a $n \times n$ matrix P such that $P^{-1}\phi_1P = \phi_2(g)$ for all $g \in G$. Now for all $g \in G$ we have

$$\chi_g(g) = \text{tr}(\phi_2(g)) = \text{tr}(P^{-1}\phi_1(g)P) = \text{tr}(\phi_1(g)) = \chi_1(g).$$

Hence $\chi_1 = \chi_2$. □

Definition 3.2.4 Permutation Character. *A permutation character χ_π is the character which is afforded by a permutation representation $\pi : G \rightarrow S_n$.*

Theorem 3.2.2 *If G is a subgroup of S_n , then the function $V : G \rightarrow \mathbb{C}$ defined by $V(g) = |\text{fix}(g)| - 1$ is a character of G .*

Proof: See [18]. □

Therefore by the above Theorem 3.2.2, it is clear that the permutation character of a group G is the number of fixed points of a group G minus 1.

Definition 3.2.5 *The matrix representation $A(x)$ is reducible over \mathbb{C} if there is a non-singular matrix T over \mathbb{C} such that $B(x) = T^{-1}A(x)T$ for all $x \in G$. If there is no such T , then we say B is irreducible.*

Definition 3.2.6 *Let $f : G \rightarrow G(n, \mathbb{C})$ be a representation of G over \mathbb{C} . Let $S = \text{Im}(f) = \{f(g) : g \in G\}$ then $S \subseteq G(n, \mathbb{C})$. We say f is reducible or fully reducible if S is reducible or fully reducible, otherwise f is irreducible.*

Theorem 3.2.3 Maschke's Theorem.

Let G be finite group and f be a representation of G over \mathbb{F} of characteristic 0 or a prime that does not divide $|G|$. If f is reducible then f is fully reducible.

Proof: See [6, Theorem 2.2.2]. □

Theorem 3.2.4 The General Form of Maschke's Theorem.

Let G be a finite group over a field \mathbb{F} whose characteristic is 0 or a prime that does not divide $|G|$, then every representation of G over \mathbb{F} is completely reducible.

Proof: See [34, Theorem 5.1.7]. □

Lemma 3.2.2 *Let ρ and ϕ be two irreducible representation of degree m and n respectively of G over \mathbb{F} . If there is a $m \times n$ matrix P such that $P\rho(g) = \phi(g)P$ for $g \in G$, then either P is a null matrix or P is a non-singular, in which case ρ and ϕ are equivalent representations of G .*

Proof: See [6, Theorem 2.2.4]

Definition 3.2.7 *If χ_π is a permutation character afforded by a representation π of G , then we say that χ_π is an irreducible character if π is an irreducible representation.*

Theorem 3.2.5 *The set of all irreducible permutation character of G is a linearly independent set over \mathbb{C} .*

Proof: See [6, Theorem 3.3.1]. □

Definition 3.2.8 Inner Product *Suppose θ and ψ are functions from $G \rightarrow \mathbb{C}$. Then we define the inner product of θ and ψ , denoted by \langle, \rangle to be $\langle \theta, \psi \rangle = \frac{1}{|G|} \sum \theta(g)\psi(g^{-1}), \forall g \in G$.*

Theorem 3.2.6 *Suppose that G has precisely k conjugacy classes. If χ and ρ are characters of G , then $\langle \chi, \rho \rangle = \langle \rho, \chi \rangle = \frac{1}{|G|} \sum \chi(g)\rho(g^{-1})$ for every $g \in G$.*

Proof: See [6, Proposition 3.2.1]

Definition 3.2.9 *An algebraic integer is a complex number which is a root of a polynomial of the form $x^n + a_{n-1}x^{n-1} + \dots + a_0, a_i \in \mathbb{Z}$ for $0 \leq i \leq n - 1$.*

The sum and product of algebraic integers are algebraic integers.

Theorem 3.2.7 *Let χ be a character of a group G . Then $\chi(g)$ is an algebraic integer for all $g \in G$.*

Proof: See [34, Theorem 5.2.12]. □

3.2.1 Permutation Character

Suppose that G is a finite group acting on a finite set Ω . For $\alpha \in \Omega$, the stabilizer is given by

$$G_\alpha = \{g \in G \mid \alpha^g = \alpha\}.$$

Then $G_\alpha \leq G$ and $[G : G_\alpha] = |\Delta|$ (Theorem 2.2.2) where Δ is the orbit containing α . Then the action of G on Ω gives a permutation representation π with corresponding permutation character χ_π denoted by $\chi(G|\Omega)$. Then from the representation theory we deduce the following.

Lemma 3.2.3 (i) *The action of G on Ω is isomorphic to the action of G on G/G_α , that is on the set of all left cosets of G_α in G . Hence $\chi(G|\Omega) = \chi(G|G_\alpha)$.*

(ii) $\chi(G|\Omega) = (1_{G_\alpha})$, the trivial character of G_α induced to G .

(iii) For all $g \in G$, we have $\chi(G|\Omega)(g) = \text{number of points in } \Omega \text{ fixed by } g$.

Proof: See [17]. □

Note 3.2.8 For any subgroup H in G we have

$$\chi(G|H)(g) = \sum_{i=1}^k \frac{|C_G(g)|}{|C_H(h_i)|},$$

where h_1, h_2, \dots, h_k are representation of the conjugacy classes of H that fuse to $[g] = C_g$ in G .

Lemma 3.2.4 Let H be a subgroup of G and let Ω be the set of all conjugates of H in G . Then we have,

(i) $G_H = N_G(H)$ and $\chi(G|\Omega) = \chi(G|N_G(H))$.

(ii) For any g in G , the number of conjugates of H in G containing g is given by

$$\chi(G|\Omega)(g) = \sum_{i=1}^k \frac{|C_G(g)|}{|C_{N_G(H)}(x_i)|} = [N_G(H) : H]^{-1} \sum_{i=1}^k \frac{|C_G(g)|}{|C_H(h_i)|},$$

where the x'_i 's and h'_i 's are representatives of the conjugacy classes of $N_G(H)$ and H that fuse to $[g] = C_g$ in G respectively.

Proof:

$$(i) \ G_H = \{x \in G | H^x = H\} = \{x \in G | x \in N_G(H)\} = N_G(H).$$

And the second part follows from Lemma 3.2.3.

(ii) The proof follows from the second part of Lemma 3.2.4 (i) and [16]. □

Remark 3.2.1 *Note that*

$$\begin{aligned} \chi(G|\Omega)(g) &= |\{H^x | (H^x)^g = H^x\}| \\ &= |H^x | H^{x^{-1}gx} = H| \\ &= |\{H^x | x^{-1}gx \in N_G(H)\}| \\ &= |\{H^x | g \in xN_G(H)x^{-1}\}| \\ &= |\{H^x | g \in N_G(H)^x\}|. \end{aligned}$$

Proposition 3.2.1 *If G is a finite simple group and M is a maximal subgroup of G , then the number λ of conjugates of M in G containing g is given by*

$$\chi(G|M)(g) = \sum_{i=1}^k \frac{|C_G(g)|}{|C_M(x_i)|},$$

where x_1, x_2, \dots, x_k are representatives of the conjugacy classes of M that fuse to the class $[g] = C_g$ in G .

Proof: See [22, Corollary 3]. □

Chapter 4

Designs and Codes

In this chapter we present terminology, notation and an overview of known results related to designs and codes which are needed later in the dissertation for reference purposes. For more detailed and additional information the reader may consult [3, 4, 9, 7].

4.1 Designs

The important notion of finite geometry is that of an incidence structure, since it contains the idea that two objects from distinct classes of objects may be incident with each other. This section is mainly concerned to a summary of basic results and concepts from the theory of designs. These can be found in [3, 4]. We discuss basic concepts from design theory needed in our development of constructing designs and as an aid in classifying designs. In this dissertation we restrict our attention to finite structures. We will consider an incidence structures with a particular degree of regularity. If the degree of regularity is emphasized, we call these t -designs.

Definition 4.1.1 *An incidence structure is a triple $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ where \mathcal{P} and \mathcal{B} are two disjoint finite sets and \mathcal{I} is a binary relation between \mathcal{P} and \mathcal{B} , i.e $\mathcal{I} \subset \mathcal{P} \times \mathcal{B}$. The elements of \mathcal{P} will be called points, those of \mathcal{B} blocks and those of \mathcal{I} flags.*

We will denote the points with lower case letters and the blocks with upper case letters.

Definition 4.1.2 An incidence structure is called simple if $(B) \neq (C)$ whenever B and C are distinct blocks. Here the trace (B) of a block B is the set $\{x \in P : (x, B) \in I\}$.

Definition 4.1.3 Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a finite incidence structure and label points as P_1, \dots, P_p and blocks as B_1, \dots, B_b . Then the matrix $M = (M_{ij})(i = 1, \dots, p ; j = 1, \dots, b)$ defined by

$$M_{ij} = \begin{cases} 1, & \text{if } (P_i, B_j) \in \mathcal{I} \\ 0, & \text{if } (P_i, B_j) \notin \mathcal{I} \end{cases}$$

is called an incidence matrix for \mathcal{D} . The column of M belonging to a block B is called the incidence vector of B .

Definition 4.1.4 A finite incidence structure $\mathcal{D} = (\mathcal{D}, \mathcal{B}, \mathcal{I})$ is called a block design with parameters v, k, λ ($v, k, \lambda \in \mathbb{N}$) if it satisfies the following conditions:

1. $|\mathcal{P}| = v$.
2. $|(p, q)| = \lambda$, i.e any two distinct points are joined by exactly λ blocks.
3. $|(B)| = k$ for any block $B \in \mathcal{B}$.

The above block design is also referred as a $t - (v, k, \lambda)$ design. We shall assume that all parameters are positive integers, and that $v > k \geq t$. Also the members of the blocks must be distinct.

Theorem 4.1.1 A t -design \mathcal{D} is also an s -design for $1 \leq s \leq t$. If the given design has parameters $t - (v, k, \lambda)$ then its parameters as an s -design are $s - (v, k, \lambda_s)$ where

$$\lambda_s = \lambda \cdot \frac{(v-s)(v-s-1)\cdots(v-t+1)}{(k-s)(k-s-1)\cdots(k-t+1)}.$$

Proof: Let S be a set of points and let m be the number of blocks that contain S . Let

$$\mathcal{T} = \{(T, B) : S \subset T \subset B, |T| = t, B \in \mathcal{B}\}$$

Now count the number of elements of \mathcal{T} in two different way, we have

$$\lambda \binom{v-s}{t-s} = m \binom{k-s}{t-s}$$

We can see that m is independent of S and hence

$$\lambda_s = m = \lambda \binom{v-s}{t-s} / \binom{k-s}{t-s}$$

which gives the formula. □

Remark 4.1.1 (i) $\lambda_t = \lambda$ and $\lambda_s = \frac{v-s}{k-s} \times \lambda_{s+1}$.

(ii) If the number of blocks in a t -design \mathcal{D} is denoted by b , then we have

$$b = \lambda_0 = \frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)}.$$

If we denote λ_1 (replication number) by r , then we have

$$r = \lambda_1 = \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}.$$

Hence we get

$$b = \frac{v}{k} \times r$$

and we deduce that

$$bk = vr.$$

(iii) For a 2-design, $2 - (v, k, \lambda)$ we have $\lambda_2 = \lambda$ and by part (i) we get

$$\lambda_1 = \frac{v-1}{k-1} \times \lambda_2$$

and hence

$$\lambda_1(k-1) = \lambda(v-1)$$

so that

$$r(k-1) = \lambda(v-1).$$

Definition 4.1.5 (i) A design is **trivial** if every k -set of points is incident with a block of the design.

(ii) A design is said to be **simple** if distinct blocks are not incident with the same set of k points.

Definition 4.1.6 The dual structure of \mathcal{D} is $D^t = (\mathcal{B}^t, \mathcal{P}^t, \mathcal{I}^t)$ where $\mathcal{P}^t = \mathcal{B}$, $\mathcal{B}^t = \mathcal{P}$ and $\mathcal{I}^t = \{(\mathcal{B}, p) | (p, \mathcal{B}) \in \mathcal{I}\}$.

Definition 4.1.7 (i) A design is said to be **symmetric** if it has the same number of points and blocks.

(ii) A design is said to be **self – dual** if it is isomorphic to its dual.

Definition 4.1.8 Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. Then the complement of \mathcal{D} is the structure $\overline{\mathcal{D}} = (\overline{\mathcal{P}}, \overline{\mathcal{B}}, \overline{\mathcal{I}})$ where $\overline{\mathcal{P}} = p$, $\overline{\mathcal{B}} = b$ and $\overline{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$.

Theorem 4.1.2 If \mathcal{D} is a $t - (v, k, \lambda)$ design with $v - k \geq t$ then $\overline{\mathcal{D}}$ is a $t - (v, v - k, \overline{\lambda})$ design, where

$$\overline{\lambda} = \lambda \cdot \frac{(v-k)(v-k-1)\cdots(v-k-t+1)}{k(k-1)\cdots(k-t+1)}.$$

Proof: See [3, Theorem 1.3.1]. □

Definition 4.1.9 An automorphism of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a permutation π of \mathcal{P} such that $B \in \mathcal{B}$ implies $\pi(B) \in \mathcal{B}$.

Definition 4.1.10 An isomorphism between two designs \mathcal{D}_1 and \mathcal{D}_2 is a bijection ϕ between sets of points \mathcal{P}_1 and \mathcal{P}_2 and between sets of blocks \mathcal{B}_1 and \mathcal{B}_2 such that for any $p \in \mathcal{P}_1$ and $B \in \mathcal{B}_1$, $p \mathcal{I}_1 B$ implies that $\phi(p) \mathcal{I}_2 \phi(B)$. If $\mathcal{D}_1 = \mathcal{D}_2$, then ϕ is called an automorphism. The group of automorphisms of a design \mathcal{D} is denoted by $\text{Aut}(\mathcal{D})$.

Definition 4.1.11 If $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is any incident structure and p is any prime, the p -rank of \mathcal{D} is the dimensions of the code $C_F(\mathcal{D})$, where $\mathbb{F} = \mathbb{F}_p$ and is written $\text{rank}_F(\mathcal{D}) = \text{rank}_p(\mathcal{D}) = \dim(C_F(\mathcal{D}))$.

4.2 Codes

We will denote a finite field \mathbb{F}_q of order q where q is a prime power. Denote the vector space spanned by n -tuples of elements of \mathbb{F}_q by $V = \mathbb{F}_q^n$. We define the standard dot product of x and y in V to be $x \cdot y = xy^T$ where y^T is the transpose of y . And the subspace spanned over \mathbb{F}_q by the subset $\{x_1, x_2, \dots, x_n\}$ of V will be denoted by $\langle x_1, x_2, \dots, x_n \rangle$.

Definition 4.2.1 Let F_q be a finite set of q elements. A q -ary code C is a set of finite sequences of symbols of F called codewords and written (x_1, x_2, \dots, x_n) where $x_i \in F$ for $i = 1, 2, \dots, n$. If all the sequences have the same length n , then C is a block code of block length n . Hence A code over F of block length n is any subset of \mathbb{F}^n .

In order to have efficiency in the transmission of message, the difference between the transmitted codewords and the error in that codeword must not differ too much. Hence we look at the concepts of the distance between codewords.

Definition 4.2.2 Let $V = (v_1, v_2, \dots, v_n)$ and $W = (w_1, w_2, \dots, w_m)$ be two vectors in \mathbb{F}^n . The Hamming distance, $d(x, y)$ between v and w is the number of coordinates places in which

they differ. That is, $d(v, w) = |\{i : v_i \neq w_i\}|$ and this Hamming distance is usually referred as simply the distance between two vectors.

Definition 4.2.3 The minimum distance $d(c)$ of a code C is the smallest distance between distinct codewords, i.e $d(c) = \min\{d(v, w) | v, w \in C, v \neq w\}$.

Theorem 4.2.1 Let C be a code of minimum distance d . If $d \geq s + 1 > 1$, then C can be used to detect up to s errors in any codewords or, if $d \geq 2t + 1$, C can be used to correct up to t errors.

Proof:

- (i) Suppose that v is transmitted and w received with less than or equal to s errors. Then $d(v, w) \leq s \leq d - 1 < d$ and therefore $w \notin C$ or $w = v$. Meaning if we had errors it would be detected.
- (ii) Suppose v is transmitted and w received with less than or equal t errors. Then we have $d(v, w) \leq t$. Now suppose that $u \in C$ such that $u \neq v$, then we have

$$d(u, w) + d(w, v) \geq d(u, v) \geq d \geq 2t + 1,$$

and hence

$$d(u, w) \geq 2t + 1 - d(v, w) \geq 2t + 1 - t = t + 1$$

Therefore v is the closest codeword to w in C and it could be picked. □

Lemma 4.2.1 If $d(c) = d$ then C can detect up to $d - 1$ errors or correct up to $\lfloor (\frac{d-1}{2}) \rfloor$ errors.

Proof: See [33, Corollary 6]. □

If C is a block code of length n having k codewords and minimum distance d , then we

say that C is an (n, k, d) q -ary code, where $|\mathbb{F}| = q$. From the above corollary we observe that in order to have a good code (n, k, d) which detects or corrects many errors, we require d to be large. However we also require n to be small for fast transmission of message and k to be large for a large number of messages to be transmitted.

There are many bounds connecting the three parameters, the code rate $R = \frac{k}{n}$ and the Hamming distance d are important parameters of a linear block code (n, k, d) . It is therefore useful to know whether a linear block code theoretically exist for a given combination of R and d . In particular, for a given minimum Hamming distance d we will consider a block code C to be better than another block code with the same Hamming distance d if it has a higher code rate R .

The simplest bound is the Singleton bound for a linear block code (n, k, d) is given by $k \leq n - d + 1$. A block code that fulfills the singleton bound with equality according to $k = n - d + 1$ is called the maximum distance separable. The sphere packing/Hamming bound can be derived for a linear error-correcting q -ary block code (n, k, d) by considering the correction balls within the code space \mathbb{F}_q^n . Each correction ball encompasses a total of

$$\sum_{i=0}^{e_{cor}} \binom{n}{i} (q-1)^i \leq q^{n-k}$$

with $e_{cor} = \lfloor (d-1)/2 \rfloor$.

Theorem 4.2.2 *If C is an (n, k, d) q -ary code, then $k \leq n - d + 1$.*

Proof: See [3, Theorem 2.1.2]. □

Definition 4.2.4 *Let C and C' be two q -ary code of same length n and having same number of codewords. Then they are equivalent if each can be obtained from the other by a combination of operations of the following types:*

- (i) Any permutation on the n coordinates positions.

(ii) Any permutation on the letters of the alphabet in any fixed coordinates position.

Definition 4.2.5 A code C over a field F_q of length n is linear if C is a subspace of $V = F^n$. If dimension of C is k and $d(c) = d$, then we write $[n, k, d]$.

Since every vector space V contains the zero vector, then every linear code of length n over F_q contains the zero vector $0 \in F_q$ where entries are all the zero elements of the field. Consider the Hamming distance $d(x, y)$ of x, y in C , then $x - y$ is in C and $d(x, y) = d(0, x - y)$. Which implies that for a linear code, the minimum distance d of the code is the smallest number of non-zero entries of the codewords of the code.

Definition 4.2.6 If C is a linear code of length n over field F_q then the weight of a word x in C is defined to be $wt(x) = d(0, x)$.

Hence it follows that the minimum distance of a linear code C is the minimum weight of the code. When the minimum weight d is known we write $C = [n, k, d]$ with the singleton bound $d \leq n - k + 1$.

Proposition 4.2.1 Let C be a $[n, k, d]$ code. Then we have

(i) $d = d(C)$ is the minimum weight of C .

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

Proof:

(i) From $V = F^n$ we have $d(v, w) = wt(v - w)$. Now since C is a subspace of V , for any $v, w \in C$ we have $v - w \in C$ and hence the result follows.

(ii) Since C is a subspace of V with $dim(C) = k$, we have $|C| = q^k$ and from Theorem 4.2.2 we have $q^k \leq q^{n-d+1}$. Hence $k \leq n - d + 1$, so that $d \leq n - k + 1$. \square

Definition 4.2.7 Two linear codes in F^n are equivalent if each can be obtained from the other by permuting the coordinate positions in F^n and multiplying each coordinate by a non-zero field element.

And these codes are said to be isomorphic if a permutation of the coordinate positions suffices to take one to the other.

Definition 4.2.8 *If C is a linear code of length n over a field F then any isomorphism of C onto itself is called an automorphism of C .*

The set of all automorphism of C is the automorphism group of C denoted by $Aut(C)$.

Definition 4.2.9 *If C is a q -ary $[n, k]$ code, a generator matrix for C is a $k \times n$ array obtained for any k linearly independent vectors of C .*

Definition 4.2.10 *Let C be a q -ary $[n, k]$ code. The orthogonal code is denoted by C^\perp and is given by $C^\perp = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$. Hence we call C self-orthogonal if $C \subseteq C^\perp$ and self dual if $C = C^\perp$.*

Proposition 4.2.2 *For any linear code C of length n , $dim(C) + dim(C^\perp) = n$.*

Proof: Let G be a generating matrix for C . Then $(v)G^t \in F^k$ for all $v \in F^n$ and G^t can be regarded as a linear transformation from F^n onto F^k . Clearly $ker(G^t) = C^\perp$ and hence $F^n/C^\perp \cong F^k$, that is $dim(F^n) - dim(C^\perp) = dim(F^k)$. Hence $n = dim(C) + dim(C^\perp)$ as required. \square

Taking G to be a generator matrix for C , a generator matrix H for C^\perp satisfies $GH^t = 0$. i.e $c \in C$ if and only if $cH^t = 0$.

Definition 4.2.11 *Any generator matrix H for C^\perp is called a parity check matrix for C .*

In general it is not easy to say anything about the minimum weight of C^\perp knowing only the minimum weight of C . But either a generator matrix or a check matrix gives a complete information about C and C^\perp .

Theorem 4.2.3 *Let H be a parity check matrix for a $[n, k, d]$ code C . Then every choice of $d - 1$ or fewer columns of H forms a linearly independent set.*

Proof: See [33, Proposition 10]. \square

4.2.1 Codes from designs

Codes constructed from designs have enriched the theory of designs in that new designs have been constructed and existing designs have been extended in some cases. Certain designs have been shown not to exist at all. In [3, 4] it has been shown that not all codes yield designs.

The code $C_{\mathbb{F}}$ of the design \mathcal{D} over the finite field \mathbb{F} is the space spanned by the incidence vectors of the blocks over \mathbb{F} . If we take \mathbb{F} to be prime field $\mathbb{F}_p = \text{GF}(p)$, we write C_p for $C_{\mathbb{F}}$, and refer to the dimension of C_p as the p – **rank** of \mathcal{D} . The point-set of \mathcal{D} is denoted by \mathcal{P} and the blocks set by \mathcal{B} . If \mathcal{Q} is any subset of \mathcal{P} , then we will denote the incidence vector of \mathcal{Q} by $v^{\mathcal{Q}}$. Thus $C_{\mathbb{F}} = \langle v^B | B \in \mathcal{B} \rangle$ is a subspace of $\mathbb{F}^{\mathcal{P}}$, the full vector space of functions from \mathcal{P} to \mathbb{F} . The length of the code is the cardinality of \mathcal{P} and its dimension is the rank of the incidence matrix of the design \mathcal{D} .

We can now observe immediately a way in which a linear code can be associated with a design or with any incidence structure from the definition below.

Definition 4.2.12 *The code of $D = (\mathcal{P}, \mathcal{B}, I)$ over a field F is the subspace $C_F(D)$ of $F^{\mathcal{P}}$ spanned by the vectors corresponding to the characteristic function of the blocks of s . Thus $C_F(D) = \langle v^B | B \in \mathcal{B} \rangle$.*

Chapter 5

Key-Moori (Method 1 and 2) and Moori Method 3

In this chapter we look into details the two methods provided by Key-Moori [24] for constructing designs under finite simple groups . Also the third method by Moori [29]. Method 1 and 2 constructs 1-designs from finite non-abelian simple groups.

5.1 Key-Moori Method 1

Method 1 provides a construction of symmetric 1-designs obtained from the primitive permutation representation of simple groups.

Let G be a finite primitive permutation group acting on the set Ω of size n . Consider the action of G on $\Omega \times \Omega$ given by $(\alpha, \beta)^g = (\alpha^g, \beta^g)$ for all $\alpha, \beta \in \Omega$ and all $g \in G$.

Definition 5.1.1 *An orbit of G on $\Omega \times \Omega$ is called an **orbital**. If $\overline{\Delta}$ is an orbital, then $\overline{\Delta}^* = \{(\alpha, \beta) : (\beta, \alpha) \in \overline{\Delta}\}$ is also an orbital of G on $\Omega \times \Omega$, which is called the **paired orbital** of $\overline{\Delta}$. Also $\overline{\Delta}$ is self-paired if $\overline{\Delta} = \overline{\Delta}^*$.*

The construction of symmetric 1-designs is based on the following result.

Theorem 5.1.1 *Let G be a finite primitive permutation group acting on the set Ω of size n . Let $\alpha \in \Omega$, and $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α . If $\mathcal{B} = \{\Delta^g : g \in G\}$ and*

given $\delta \in \Delta$, $\epsilon = \{(\alpha, \delta)^g : g \in G\}$, then $\Delta = (\Omega, \mathcal{B})$ forms a $1 - (n, |\Delta|, |\Delta|)$ design with n blocks. With G acting as an automorphism group on this structure, primitive on the points and blocks of the design.

Proof: We have $|G| = |\Delta^G||G_\Delta|$, and clearly $G_\alpha \subseteq G_\Delta$. Since G is primitive on Ω , G_α is maximal in G , and thus $G_\alpha = G_\Delta$, and $|\Delta^G| = |\mathcal{B}| = n$. This proves that we have a $1 - (n, |\Delta|, |\Delta|)$ design. \square

Note 5.1.2 *If we form any union of orbits of the stabilizer of a point, including the orbit consisting of the single point, and orbit this under the full group, we still get a self dual symmetric 1-design with group operations. Hence the orbits of the stabilizer can be regarded as building blocks.*

Lemma 5.1.1 *If the group G acts primitively on the points and the blocks of a symmetric 1-design \mathcal{D} , then the design can be obtained by orbiting a union of orbits of a points stabilizer as described in the above theorem.*

Proof: Suppose that G acts primitively on the points and the blocks of a symmetric 1-design \mathcal{D} . Let \mathcal{B} be the block set of \mathcal{D} , then if B is any block of \mathcal{D} , $\mathcal{B} = B^G$. Thus $|G| = |\mathcal{B}||G_B|$, and hence G is primitive, G_B is maximal and thus $G_B = G_\alpha$ for some point. Thus G_α fixes B , so this must be a union of orbits of G_α . \square

We note that if \mathcal{D} is any design obtained from the construction in the manner described above, then the automorphism group of \mathcal{D} will contain G . Further if C is the code of \mathcal{D} over a field F , then the automorphism group of \mathcal{D} is contained in the automorphism group of C .

Remark 5.1.1 *Let G be a finite simple group with a maximal subgroup M . Then the action of G by conjugation on the set \mathcal{M} of all conjugates of M in G is primitive.*

Lemma 5.1.2 *If G is a primitive simple group acting on Ω , then for any $\alpha \in \Omega$, the point stabilizer G_α has only one orbit of length 1.*

Proof: Suppose that G_α fixes β . Then $G_\alpha = G_\beta$. Since G is transitive, there exist $g \in G$ such that $\alpha^g = \beta$. Then

$$(G_\alpha)^g = G_{\alpha^g} = G_\beta = G_\alpha,$$

and therefore $g \in N_G(G_\alpha) = N$, the normalizer of G_α in G . Since G_α is maximal in G , we have $N = G$ or $N = G_\alpha$. But G is simple, so we must have $N = G_\alpha$, so that $g \in G_\alpha$ and hence $\beta = \alpha$. \square

Theorem 5.1.3 *Let G be a finite simple group acting on the set of the conjugates of a maximal subgroup M by conjugation. Then the size of orbits of a point stabilizer of G are given as elements of the set*

$$\left\{ \frac{|M|}{n} : n \in \mathcal{M} \right\}.$$

Proof: Let \mathcal{M} be the set of conjugates of M in G on which G acts on by conjugation. Assume that $\alpha = M$ is a letter in \mathcal{M} . It is clear that $G_\alpha = M$. Let β^M be an orbit of the action of M on \mathcal{M} , where $\beta = M^g$. Hence $|\beta^M| = |M : M_\beta|$. Our goal is to show that $M_\beta = M \cap M^g$. We write

$$M_\beta = \{x \in M \mid \beta^x = \beta\} = \{x \in M \mid M^{gx} = M^g\} = \{x \in M \mid gxg^{-1} \in N_G(M)\}.$$

Since M is maximal subgroup of G and G is simple, we have $M = N_G(M)$. Hence $M_\beta = M \cap M^g$. Therefore, $|\beta^M| = |M : M \cap M^g|$ and the result follows. \square

5.2 Key-Moori Method 2

Method 2 introduces a technique from which a large number of non-symmetric 1-designs could be constructed.

Definition 5.2.1 *Let G be a finite group, M be a maximal subgroup of G and nX be the conjugacy class of elements of order n in G and $g \in nX$ then $C_g = [g] = nX$ and $|nX| = [G : C_g]$.*

We construct $1 - (v, k, \lambda)$ designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, where $\mathcal{P} = nX$ and $\mathcal{B} = \{(M \cap nX)^y | y \in G\}$.

Definition 5.2.2 *Let $\chi_m = \chi(G|M)$ be the permutation character afforded by the action of G on the set M , then the set of all conjugates of M in G , such that if g is not conjugate to any element in M , then $\chi_M(g) = 0$.*

The construction of 1-designs on Method 2 is based on the following theorem.

Theorem 5.2.1 *Let G be a finite simple group, M a maximal subgroup of G and nX a conjugacy class of element in G , such that $M \cap nX \neq \emptyset$. Let $\mathcal{B} = \{(M \cap nX)^y | y \in G\}$ and $\mathcal{P} = nX$. Then we have a $1 - (|nX|, |M \cap nX|, \chi_M(g))$ design \mathcal{D} , where $g \in nX$. The group G acts as an automorphism group on \mathcal{D} , primitive on blocks and transitive (not necessarily primitive) on points of \mathcal{D} .*

Proof: We first note that

$$\mathcal{B} = \{M^y \cap nX | y \in G\}$$

We claim that $M^y \cap nX = M \cap nX$ if and only if $y \in M$ or $nX = \{1_G\}$. Clearly if $y \in M$ or $nX = \{1_G\}$, then $M^y \cap nX = M \cap nX$. Conversely suppose there exist $y \notin M$ such that $M^y \cap nX = M \cap nX$. Then maximality of M in G implies that $G = \langle M, y \rangle$ and hence $M^z \cap nX = M \cap nX$ for $z \in G$. We can deduce that $nX \subseteq M$ and hence $\langle nX \rangle \leq M$. Since $\langle nX \rangle$ is a normal subgroup of G and G is simple, we must have $\langle nX \rangle = \{1_G\}$. Note that maximality of M and the fact that $\langle nX \rangle \leq M$, excludes the case $\langle nX \rangle = G$.

From the above we deduce that

$$b = |\mathcal{B}| = |\Omega| = [G : M].$$

If $B \in \mathcal{B}$, then

$$k = |B| = |M \cap nX| = \sum_{i=1}^k |[x_i]M| = |M| \sum_{i=1}^k \frac{1}{|C_M(x_i)|},$$

where x_1, x_2, \dots, x_k are the representatives of conjugacy classes of M that fuse to g . Let $v = |\mathcal{P}| = |nX| = [G : C_G(g)]$. From the design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with points set \mathcal{P} , blocks set

\mathcal{B} and incidence \mathcal{I} given by $x\mathcal{I}B$ if and only if $x \in B$. Since the number of blocks containing an element x in \mathcal{P} is $\lambda = \chi_M(x) = \chi_M(g)$, we have produced a $1 - (v, k, \lambda)$ design \mathcal{D} , where $v = |nX|$, $k = |M \cap nX|$ and $\lambda = \chi_m(g)$.

The action of G on blocks arises from the action of G on Ω and hence the maximality of M in G implies the primitivity. The action of G on nX , that is on points, is equivalent to the action of G on the cosets of $C_G(g)$. So the action on points is primitive if and only if $C_G(g)$ is a maximal subgroup of G . \square

Remark 5.2.1 *Since in a $1 - (v, k, \lambda)$ design \mathcal{D} we have $kb = \lambda v$, we deduce that*

$$\begin{aligned} k &= |M \cap nX| \\ &= \frac{\chi_M(g) \times |nX|}{[G : M]} \\ &= (\chi_M(g) \times |nX|) \div \frac{|G|}{|M|} \\ &= (\chi_M(g) \times |nX|) \times \frac{|M|}{|G|} \\ &= \frac{|M| \chi_M(g) \times |nX|}{|G|}. \end{aligned}$$

Also note that $\tilde{\mathcal{D}}$, the complement of \mathcal{D} , is a $1 - (v, v - k, \bar{\lambda})$ design, where $\bar{\lambda} = \lambda \times \frac{v-k}{k}$.

Remark 5.2.2 *If $\lambda = 1$, then \mathcal{D} is a $1 - (|nX|, k, 1)$ design. Since nX is the disjoint union of b blocks of size k each, we have $\text{Aut}(\mathcal{D}) = (S_k)^b : S_b$. Therefore for all p , we have $C = C_p(\mathcal{D})$ is $[|nX|, b, k]_p$ with $\text{Aut}(C) = \text{Aut}(\mathcal{D})$.*

Note 5.2.2 *The designs \mathcal{D} constructed by using Theorem 5.2.1 are are not symmetric in*

general. In fact \mathcal{D} is symmetric if and only if

$$\begin{aligned}
b &= |\mathcal{B}| \\
&= v \\
&= |\mathcal{P}| \\
&\Leftrightarrow [G : M] = |nX| \\
&\Leftrightarrow [G : M] = [G : C_G(g)] \\
&\Leftrightarrow |M| = |C_G(g)|.
\end{aligned}$$

5.3 J. Moori Method 3

Method 3 is the new method introduced by J Moori in [30]. This method introduces a technique from which a large number of 1-designs could be constructed on a finite simple group.

Suppose that G is a finite group acting on a finite set Ω , nX a conjugacy class of elements of order $n \neq 1$ in G and $g \in nX$. Thus $C_g = [g] = nX = |G : C_G(g)|$. Let χ_Ω be the permutation character afforded by the action of G on Ω . If M is a maximal subgroup of G then Ω can be regarded as the set of all conjugates of M in G and $\chi_g = \chi = \chi(G|M)$.

We construct 1-designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, with $\mathcal{P} = \Omega$ and $\mathcal{B} = \{B^y | y \in G\}$ where $B = \text{Fix}_\Omega(g)$ is the fixed points of g . The construction of our designs is based on the following Theorem.

Theorem 5.3.1 *Let G be a finite group acting transitively on a finite set Ω , $|\Omega| = v > 1$. Let $g \in nX$ and $B = \text{Fix}_\Omega(g)$ be the set of fixed points of the action of g on Ω . Let $\mathcal{B} = \{B^y | y \in G\}$, $\mathcal{P} = \Omega$ and $S = \{h \in nX : \text{Fix}_\Omega(h) = B\}$ with $|S| = s$. Then*

(i) $|\mathcal{B}| = |nX|/s$ and we have a $1 - (v, \chi_\Omega(g), \lambda)$ design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ where $\lambda = (\chi_\Omega(g) \times |nX|)/(s \times |\Omega|)$.

(ii) *The group G acts as an automorphism group on \mathcal{D} transitive both on point and blocks. In particular, if M is a maximal subgroup of G and Ω is the set of all conjugacy*

of M in G , then G is primitive on points and transitive (not necessarily primitive) on blocks of \mathcal{D} .

Proof: We firstly note that $\alpha \in \text{Fix}_\Omega(g) = B$ if and only if $\alpha^y \in \text{Fix}_\Omega(y^{-1}gy) = B^y$ for all $y \in G$. This implies that the number of blocks containing α is the same as the number of blocks containing α^y for all $y \in G$. Since G is transitive on Ω , we have that any point γ in Ω is contained in the same λ of blocks. Furthermore, if k is the size of each block, then,

$$k = |B^y| = |B| = \text{Fix}_\Omega(g) = \chi_\Omega(g).$$

- (i) Clearly each block B^y is produced by s distinct elements of nX , that is there are s distinct elements $h \in nX$ such that $\text{Fix}_\Omega(h) = B^y$. Hence,

$$b = |\mathcal{B}| = |\{B^y : y \in G\}| = |nX|/s.$$

Since in a $1 - (v, k, \lambda)$ design \mathcal{D} we have $kb = \lambda v$, we deduce that

$$\lambda = kb/v = \frac{\chi_\Omega(g) \times |nX|}{s \times |\Omega|}.$$

- (ii) The action of G on points arises from the action of G on Ω . Since $\mathcal{B} = B^G$, G is transitive on \mathcal{B} with $G_B = \{y \in G : B^y = B\}$ as the stabilizer of the action on blocks. Clearly G acts as an automorphism group on \mathcal{D} . The maximality of M in G implies the primitivity of the action on points. The action of G on \mathcal{B} , that is on blocks, is equivalent to the action of G on the cosets of G_B . so the action on blocks is primitive if and only if G_B is a maximal subgroup of G . \square

The following results give more information on the parameters of \mathcal{D} constructed above. It could be used for calculating the values of s, b and λ .

Proposition 5.3.1 *With $nX = [g]$, $B = \text{Fix}_\Omega(g)$ and S given in the theorem above, we have*

- (i) $S = nX \cap G_{|B|}$ where $G_{|B|}$ is the pointwise stabilizer of B in G .

(ii) $b = [G : G_B]$ and $|G_B| = |G| \times s/|nX|$.

(iii) $s = |S| = [G_B : C_G(g)]$.

Proof:

(i) If $y \in S$, then, $y \in nX$ and $Fix_\Omega(y) = B$. Hence, y fixes B pointwise and $y \in G_{|B|}$. Thus $y \in nX \cap G_{|B|}$. Conversely if $y \in nX \cap G_{|B|}$, implies $y \in nX$ and $y \in G_{|B|}$, then, $Fix_\Omega(y) \supseteq B$. Since $y \in nX$, Y is conjugate to g and hence $\chi_\Omega(y) = \chi_\Omega(g)$. Therefore $|Fix_\Omega(y)| = |Fix_\Omega(g)| = |B|$, so that $Fix_\Omega(y) = B$. Hence, $y \in S$.

(ii) Since we have proved in Theorem 5.3.1, G acts transitively on \mathcal{B} and hence $|G| = |\mathcal{B}| \times |G_B|$, that is $b = |\mathcal{B}| = |G|/|G_B| = [G : G_B]$. Since by Theorem 5.3.1 we have $b = |nX|/s$, we deduce that $|G_B| = |G| \times s/|nX|$.

(iii) It is clear that $C_G(g) \leq G_B$, since for any $y \in C_G(g)$ we have $B^y = Fix_\Omega(g^y) = Fix_\Omega(g) = B$. Now, by part (ii) we have $|G_B| = |G| \times s/|nX|$ and hence

$$\begin{aligned} s &= |G_B| \times |nX|/|G| \\ &= |G_B|/|C_G(g)| \\ &= [G_B : C_G(g)] \end{aligned}$$

□

Remark 5.3.1 (i) We note that

$$G > G_B \geq N_G(\langle g \rangle) \geq C_G(g).$$

Firstly, if $G = G_B$, then we have $\mathcal{B} = \{B\}$ which implies that we have $b = 1$ and $k = |B| = v$. And that is to say g fixes all elements of Ω and $g = 1_G$, hence this gives a contradiction since in our construction we assumed that g is a non-identity element. Secondly, for $y \in N_G(\langle g \rangle)$ we have

$$B^y = \text{Fix}_\Omega(g^y) = \text{Fix}_\Omega(g^m) \supseteq \text{Fix}_\Omega(g) = B,$$

for some integer m . Which implies $B^y = B$ and $y \in G_B$

(ii) By part (iii) of Proposition 5.3.1, we can see that $s = 1$ if and only if $G_B = C_G(g)$.

(iii) If $C_G(g)$ is maximal in G , then, clearly $G_B = C_G(g)$, and hence, $s = 1$. But the converse is not true, that is there are cases where $s = 1$ and G_B is not maximal in G .

Note 5.3.2 (i) If $\lambda = 1$, then, \mathcal{D} is a $1 - (v, k, 1)$ design. Since Ω is the disjoint union of b blocks each of size k , we have $\text{Aut}(\mathcal{D}) = s_k \wr s_b = (s_k)^b : s_b$. Clearly, in this case for all p , we have $C = C_p(\mathcal{D}) = [v, b, k]_p$, with $\text{Aut}(C) = \text{Aut}(\mathcal{D})$.

(ii) In this method, when Ω is the set of all conjugates of maximal subgroup M in G , we have $\lambda = 1$ if and only if $G_B = M$ and $k = 1$. In this regard, we will have \mathcal{D} as a $1 - (v, 1, 1)$ design with corresponding $C = C_p(\mathcal{D}) = [v, v, 1]_p$. which is the full space \mathbb{F}_p^v , with $\text{Aut}(C) = \text{Aut}(\mathcal{D}) = s_v$ for all p .

(iii) The designs \mathcal{D} constructed by using Theorem 5.3.1 are not symmetric in general. In fact, \mathcal{D} is symmetric if and only if

$$b = |\mathcal{B}| = v = |\mathcal{P}| \iff [G : G_B] = |\Omega|.$$

In particular, if Ω is the set of all conjugates of a maximal subgroup M of G , then, it means \mathcal{D} is symmetric if and only if

$$[G : M] = [G : G_B] \iff |M| = |G_B|.$$

Chapter 6

Construction of Designs from Method 2 and 3

In this chapter we give explicit formulae to compute the parameters of designs from Method 2 and 3 based on the cycle structure of an arbitrary element g in A_n and thereafter we construct designs from the fixed points of alternating groups, where we consider the group A_n with its maximal subgroup A_{n-1} for $n \geq 5$.

We start by showing that $M = A_{n-1}$ is a maximal subgroup of $G = A_n$ for all n .

Lemma 6.0.1 *For $n \geq 5$, the group A_n has a maximal subgroup A_{n-1} .*

Proof: To prove that M is a maximal subgroup of G , we need to show that M is a proper subgroup of G and there is no other subgroup of G that properly contains M , that is to say if $M \leq H \leq G$ then either $M = H$ or $H = G$.

Firstly we show that M is a proper subgroup of G . We know that G is a group of all even permutation of n elements and M is a group of all even permutation of $n - 1$ elements. Since $n > n - 1$, then there exist some permutation in G that are not M . Therefore M is a proper subgroup of G .

To show that there are no other subgroup of G that properly contains M . Suppose that G acts on a set X of cardinality m , then there exist a homomorphism $\phi : G \rightarrow S_X$ such that:

- (i) $\text{Ker}(\phi)$ is a normal subgroup of G .

(ii) $Im(\phi)$ is a subgroup of S_X .

By the definition of kernel we have

$$Ker(\phi) = \{x \in G : \phi(x) = 1_G\}$$

which implies that $Ker(\phi) = \{1_G\}$. And by the **First Isomorphism Theorem** we have,

$$G/Ker(\phi) \cong Im(\phi) \leq S_X$$

$$G/1_G \cong Im(\phi) \leq S_X$$

$$G \cong Im(\phi) \leq S_X$$

$$|G|/|S_X| = m!.$$

Suppose that $H \leq G$ and define the set $X = \{aH : a \in G\}$ to be set of all left cosets of H in G . Then $|G : H| = |X| \Rightarrow \frac{|G|}{|H|} = |X| = m \Rightarrow n \leq m \leq |G : H|$. But

$$\begin{aligned} |G/H| &= |G : H| \times |H : M| \\ &\Rightarrow \frac{n!/2}{(n-1)!/2} = m \times x \\ &\Rightarrow n!/(n-1)! = mx \\ &\Rightarrow n = mx \\ &\Rightarrow x = 1 \\ &\Rightarrow |H : M| = 1 \\ &\Rightarrow H = M. \end{aligned}$$

$\Rightarrow M$ is a maximal subgroup of G . □

The result of the above proof gives the results of the following lemma.

Lemma 6.0.2 *If H is a proper subgroup of A_n ($n > 5$), then $|G : H| \geq n$.*

For every $g \in S_n$, we can write g as a product of disjoint cycles. Let $\mu(g)$ be the cycle structure of g , that is a multiset whose underlying set is all the lengths of the cycle of g .

Definition 6.0.1 (Multiset). *A multiset is a 2-tuple $\mathcal{M}(U, r)$, where U is the underlying set and r is the multiplicity function $r : U \rightarrow \mathbb{Z}^+$.*

Definition 6.0.2 *Let $\mathcal{M}(U, r) = \{u_1^{r_1}, u_2^{r_2}, \dots, u_k^{r_k}\}$ be a multiset and $u_1 r_1 + u_2 r_2 + \dots + u_k r_k = m$. We define $\mathcal{S}(U, r)$ as follows:*

$$\mathcal{S}(U, r) = \frac{\binom{m}{\mathcal{M}(U, r)} \times \prod_{i=1}^k (u_i - 1)!^{r_i}}{\prod_{j=1}^k r_j!}$$

Lemma 6.0.3 *Let $g \in S_n$ and $\mu(g) = \{u_1^{r_1}, u_2^{r_2}, \dots, u_k^{r_k}\}$. Then we have,*

$$|g^G| = \frac{n!}{\prod_{i=1}^k (u_i)^{r_i} \times r_i!}$$

Note 6.0.1 *If $g \in A_n$, then either $|g^{A_n}| = |g^{S_n}|$ or $|g^{A_n}| = \frac{|g^{S_n}|}{2}$ (see Theorem 2.3.4). The latter happens only if $r_i = 1$ for all $1 \leq i \leq k$ and u_i are odd.*

6.1 Designs from Method 2

In this section, we use method 2 to obtain the designs from the maximal subgroup M of G . We have already given some background information about Method 2 in chapter 5 section 5.2. The results of method 2 is given by Theorem 5.2.1.

Remark 6.1.1 *Let G be a finite simple group with a maximal subgroup M . Then the action of G on the set of all conjugates in M is normal, that is, G acts on M by conjugation.*

The following results shows that if we have two parameters, then the third one can always be computed.

Lemma 6.1.1 *Let $\mathcal{D} = 1 - (v, k, \lambda)$ be a design obtained by method 2. Then $|G : M| = \lambda v/k$.*

Proof: See [39, Lemma 3.2]. □

Theorem 6.1.1 *Let G be an alternating group with a maximal subgroup M , and G acting on M by conjugation. Then the designs constructed by Method 2 are $1 - (|g^G|, \frac{\lambda v}{n}, \lambda)$.*

Proof: Suppose that \mathcal{D} is a $1 - (v, k, \lambda)$ design and $g \in G$. So the first parameter is the length of g , that is, $v = |g^G|$. Since G acts on M by conjugation then in this case λ is the number of fixed points of g in G . To complete the proof, we only need to find the parameter k . By the results of Lemma 6.1.1 we have

$$|G : M| = \frac{\lambda v}{k}$$

$$n = \frac{\lambda v}{k}$$

$$k = \frac{\lambda v}{n}.$$

This completes the proof. □

6.1.1 Examples of Designs from A_n using Method 2.

Conjugacy Classes of A_8	$ Fix(g) $	$ g^G $	$\frac{\lambda v}{n}$	1-design
(1 2)(3 4)	$\lambda = 4$	$v = 210$	$k = 105$	$\mathcal{D} = 1 - (210, 105, 4)$
(1 2 3 4)(5 6)	$\lambda = 2$	$v = 2520$	$k = 630$	$\mathcal{D} = 1 - (2520, 630, 2)$
(1 2 3 4 5 6 7)	$\lambda = 1$	$v = 2880$	$k = 360$	$\mathcal{D} = 1 - (2880, 360, 1)$

Table 6.1: Some 1-designs from A_8

- (i) The complement of the design $\mathcal{D} = 1 - (210, 105, 4)$ is $\tilde{\mathcal{D}} = 1 - (210, 105, 4)$ design. Construction using MAGMA shows that the binary code of this design is a $\mathcal{C}(\mathcal{D}) = [210, 7, 96]$ and the dual code of \mathcal{C} is $[210, 203]$.
- (ii) The complement of the design $\mathcal{D} = 1 - (2520, 630, 2)$ is $\tilde{\mathcal{D}} = 1 - (2520, 1890, 6)$ design. Construction using MAGMA shows that the binary code of this design is a $\mathcal{C}(\mathcal{D}) = [2520, 7, 630]$ linear code over $GF(2)$ with the binary code of the complement design being $\mathcal{C}(\tilde{\mathcal{D}}) = [2520, 7, 1080]$
- (iii) The complement of the design $\mathcal{D} = 1 - (2880, 360, 1)$ is $\tilde{\mathcal{D}} = 1 - (2880, 2520, 7)$ design. Construction using MAGMA shows that the binary code of this design is a $\mathcal{C}(\mathcal{D}) = [2880, 8, 360]$ linear code over $GF(2)$ with the binary code of the complement design being $\mathcal{C}(\tilde{\mathcal{D}}) = [2880, 8, 360]$

Conjugacy Classes	$ Fix(g) $	$ g^G $	$\frac{\lambda v}{n}$	1-design
(1 2 3 4 5)	$\lambda = 4$	$v = 3024$	$k = 1344$	$\mathcal{D} = 1 - (3024, 1344, 4)$
(1 2 3 4 5 6 7)	$\lambda = 2$	$v = 7560$	$k = 1680$	$\mathcal{D} = 1 - (7560, 1680, 2)$

Table 6.2: Some 1-designs from A_9

- (i) The complement of the design $\mathcal{D} = 1 - (3024, 1344, 4)$ is $\tilde{\mathcal{D}} = 1 - (3024, 1680, 5)$ design. Construction using MAGMA shows that the binary code of this design is a $\mathcal{C}(\mathcal{D}) = [3024, 8, 1344]$ linear code over $GF(2)$ with the binary code of the complement design being $\mathcal{C}(\tilde{\mathcal{D}}) = [3024, 9, 1344]$.
- (ii) The complement of the design $\mathcal{D} = 1 - (7560, 1680, 2)$ is $\tilde{\mathcal{D}} = 1 - (7560, 5880, 7)$ design. Construction using MAGMA shows that the binary code of this design is a $\mathcal{C}(\mathcal{D}) = [7560, 8, 1680]$ linear code over $GF(2)$.

Conjugacy Classes	$ Fix(g) $	$ g^G $	$\frac{\lambda v}{n}$	1-design
(1 2 3 4)(5 6)	$\lambda = 6$	$v = 83160$	$k = 41580$	$\mathcal{D} = 1 - (83160, 41580, 6)$
(1 2 3 4 5 6 7)	$\lambda = 5$	$v = 570240$	$k = 237600$	$\mathcal{D} = 1 - (570240, 237600, 5)$
(1 2 3 4)(5 6 7)(8 9)	$\lambda = 3$	$v = 3326400$	$k = 831600$	$\mathcal{D} = 1 - (3326400, 831600, 3)$
(1 2 3 4 6 7 8 9 10 11)	$\lambda = 1$	$v = 21772800$	$k = 1814400$	$\mathcal{D} = 1 - (21772800, 1814400, 1)$
$\alpha_1 = (1 2 3 4 5 6)(7 8)$	$\lambda_1 = 4$	$v = 1663200$	$k_1 = 554400$	$\mathcal{D}_{\alpha_1} = 1 - (1663200, 554400, 4)$
$\alpha_2 = (1 2 3)(4 5 6)(7 8)(9 10)$	$\lambda_2 = 2$	$v = 1663200$	$k_2 = 277200$	$\mathcal{D}_{\alpha_2} = 1 - (1663200, 277200, 2)$
$\alpha_3 = (1 2 3 4 5 6)(7 8)(9 10)(11 12)$	$\lambda_3 = 0$	$v = 1663200$	$k_3 = 0$	\mathcal{D}_{α_3} has no design.

Table 6.3: Some 1-designs from A_{12}

In the following examples, let \mathcal{D} be a 1-design and let $\tilde{\mathcal{D}}$ be the complement of \mathcal{D} .

- (i) If $\mathcal{D} = 1 - (83160, 41580, 6)$ then $\tilde{\mathcal{D}} = 1 - (83160, 41580, 20790)$.
- (ii) If $\mathcal{D} = 1 - (570240, 237600, 5)$ then $\tilde{\mathcal{D}} = 1 - (570240, 332640, 7)$.
- (iii) If $\mathcal{D} = 1 - (3326400, 831600, 3)$ then $\tilde{\mathcal{D}} = 1 - (3326400, 2494800, 9)$.
- (iv) If $\mathcal{D} = 1 - (21772800, 1814400, 1)$ then $\tilde{\mathcal{D}} = 1 - (21772800, 1995800, 11)$.
- (v) If $\mathcal{D} = 1 - (1663200, 554400, 4)$ then $\tilde{\mathcal{D}} = 1 - (1663200, 1108800, 8)$.
- (vi) If $\mathcal{D} = 1 - (1663200, 277200, 2)$ then $\tilde{\mathcal{D}} = 1 - (1663200, 1386000, 10)$.

6.2 Designs from Method 3

In this section, we obtain explicit formulae for the parameters of designs constructed from the fixed points of the alternating group A_n and the maximal subgroup A_{n-1} , with A_n acting on the set of conjugacy classes of elements and the fixed points of elements g in A_{n-1} . Our construction and results are based on the following Theorem.

Theorem 6.2.1 *Let G be a finite group acting transitively on a finite set Ω , $|\Omega| \leq 1$ for some $g \in G$, let $B = Fix_{\Omega}(g)$ and $\mathcal{B} = \{B^y : y \in G\}$. If $S = \{h \in g^G : Fix_{\Omega}(h) = Fix_{\Omega}(g)\}$,*

then $|\mathcal{B}| = \frac{|g^G|}{|S|}$ and we have a 1-design $1 - (v, k, \lambda)$ with point set Ω and blocks \mathcal{B} . Moreover $v = |\Omega|$, $k = \text{Fix}_\Omega(g)$ and $\lambda = \frac{k \times |g^G|}{v \times |S|}$.

To this end, we can find the parameters of designs constructed by method 3 using the results of method 2.

Proposition 6.2.1 *Let G be an alternating group acting normally on a set Ω . Suppose that for some $g \in G$ the design constructed by using Method 2 is $1 - (v, k, \lambda)$. Then the design \mathcal{D}' constructed by applying Method 3 to a maximal subgroup M containing g is*

$$\mathcal{D}' = 1 - (n, \lambda, \frac{\lambda \times |g^G|}{n \times |S|}).$$

Proof: Suppose \mathcal{D}' is a $1 - (v', k', \lambda')$ design. So since G acts on M by conjugation, we have $v' = |A_n : A_{n-1}| = |G : M| = n$ and $k' = |\text{Fix}_n(g)| = \lambda$.

□

We consider every possible structure of the conjugacy classes of A_n . From Definition 6.0.2 we deduce that for every multiset of the cycle $g \in A_n$, the general formular for all cycles is given by

$$\mu(g) = (1^{n-u_2r_2-u_3r_3\dots u_n r_n} u_2^{r_2} u_3^{r_3} \dots u_n^{r_n})$$

where u_i is the cycle length and $r_i := r(u_i)$ is the number of occurrence of u_i . With the fixed points of g being given by

$$|\text{Fix}(g)| = n - u_2r_2 - u_3r_3 \dots u_n r_n.$$

In view of the above cycle we can now deduce the general results and draw our attention to the main formula for determining the value of S given any type of cycle in A_n . Throughout we observed that for any cycle the value of S is computed by taking a factorial of the total of all the elements in the cycle and divide by the product of the occurrence for each cycle set. For every cycle g the value of S is computed as follows, which bring us to the main Theorem of this work.

Theorem 6.2.2 Let \mathcal{D} be a $1 - (n, |Fix(g)|, \frac{|Fix(g)| \times |g^G|}{n \times |S|})$ design constructed by applying Method 3 to the conjugacy classes of maximal subgroup of G . Assume that $g \in A_n$ and $\mu(g) = \{u_1^{r_1}, u_2^{r_2}, \dots, u_n^{r_n}\}$ be the cycle structure of g . Then we have

$$|S| = \frac{(n - Fix(g))!}{\prod_{i=2}^n (u_i^{r_i} \times r_i!),}$$

and with the case were the cycle splits in A_n we have the following results

$$|S| = \frac{(n - Fix(g))!}{2 \prod_{i=2}^n (u_i^{r_i} \times r_i!).}$$

Proof: Let $g \in A_n$ and

$$\mu(g) = (1^{n-u_2r_2-u_3r_3-\dots-u_nr_n} u_2^{r_2} u_3^{r_3} \dots u_n^{r_n})$$

be the cycle structure of g with

$$|Fix(g)| = n - u_2r_2 - u_3r_3 \dots u_nr_n.$$

Let $m = |Fix(g)|$ and g' be a fixed point free element of $H = A_{n-m}$, whose cyclic structure is the same as g . We claim that for a permutation h in A_n , we have $h \in S$ if and only if h' is an element of g'^H . Suppose that $h \in S$, then since $h \in A_n$ there is $h' \in A_{n-m}$ whose cyclic structure is same as that of h . Which would mean $|Fix(h)| = |Fix(h')|$, and thus h is a fixed point free element. To find all the possibilities for h , consider $\mu(h)$, the cycle structure of h with $u_1r_1 + u_2r_2 + \dots + u_nr_n = n - m$. Then for every $h \in S$, we should put aside $u_i = 1$, so that we can choose the u_i from $n - m$. Hence we can totally choose

$$\binom{n - m}{\mathcal{M}(U - \{1\}, r)} = \frac{(n - m)!}{\prod_{i=2}^n (u_i)^{r_i}}$$

elements for h . Since every cycle of length u_i have $(u_i - 1)!$ permutations, now to avoid repetition we divide this by the number of the permutations of cycles with equal length $(r_i)!$. So if the conjugacy classes of h does not split, then the number of possible $h \in S$ is equal to

$$S(U - \{1\}, r) = \frac{(n - m)!}{\prod_{i=2}^n (u_i)^{r_i} (r_i)!}.$$

If the conjugacy classes of h splits then,

$$S(U - \{i\}, r)/2 = \frac{(n - m)!}{2 \prod_{i=2}^n (u_i)^{r_i} (r_i)!}.$$

But for every $h' \in H = A_{n-m}$ we have

$$|g^{A_{n-m}}| = \frac{(n - m)!}{\prod_{i=2}^n (u_i)^{r_i} (r_i)!}$$

by results of Lemma 6.0.3.

Therefore, $|S| = |g^{A_{n-m}}|$ and the result follows by Lemma 6.0.3. \square

6.2.1 Examples of designs from A_n using Method 3

In this section we apply Theorem 6.2.2 and obtain some designs under the family of alternating groups.

1. Consider $g = (1\ 2\ 3\ 4)(5\ 6) \in A_n$. Now by the above results of Theorem 6.2.2, we compute the value of S corresponding to g as

$$\begin{aligned} |S| &= \frac{(n - \text{Fix}(g))!}{\prod_{i=1}^n u_i^{r_i}} \\ &= \frac{6!}{4 \times 2} \\ &= 90. \end{aligned}$$

Since the value of S hold for the cycle g in any alternating group, we can find the 1-designs from various groups for the same cycle structure g . Then we have the following designs,

A_n	$\mathbf{Fix}(\mathbf{g})$	$ g^G $	$\lambda' = \frac{k' \times g^G }{v' \times S }$	1-design
If $g \in A_7$	$k' = 1$	$ g^G = 630$	$\lambda' = 1$	$\mathcal{D} = 1 - (7, 1, 1)$
If $g \in A_8$	$k' = 2$	$ g^G = 2520$	$\lambda' = 7$	$\mathcal{D} = 1 - (8, 2, 7)$
If $g \in A_9$	$k' = 3$	$ g^G = 7560$	$\lambda' = 28$	$\mathcal{D} = 1 - (9, 3, 28)$
If $g \in A_{10}$	$k' = 4$	$ g^G = 18900$	$\lambda' = 84$	$\mathcal{D} = 1 - (10, 4, 84)$
If $g \in A_{11}$	$k' = 5$	$ g^G = 41580$	$\lambda' = 210$	$\mathcal{D} = 1 - (11, 5, 210)$

Table 6.4: Some 1-designs from $A_7, A_8, A_9, A_{10}, A_{11}$

- (i) The design $\mathcal{D} = 1 - (7, 1, 1)$ has $\lambda = k = 1$ and by Note 5.3.2 part (ii) we have the corresponding code $\mathcal{C}_p(\mathcal{D}) = [7, 7, 1]_p$ which is the full space \mathbb{F}_p^7 , with $Aut(C) = Aut(\mathcal{D}) = s_7$ for all p .

2. Consider $g = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9)(10\ 11) \in A_n$.

Now by the above results of Theorem 6.2.2 , we compute the value of S corresponding to g as

$$\begin{aligned}
|S| &= \frac{(n - Fix(g))!}{\prod_{i=1}^n u_i^{r_i}} \\
&= \frac{11!}{5 \times 4 \times 2} \\
&= 997920.
\end{aligned}$$

Since the value of S hold for the cycle g in any alternating group, we can find the 1-designs from various groups for the same cycle structure g . Hence the designs follows in the table 6.8 below.

A_n	Number of $\text{Fix}(g)$	$ g^G $	$\lambda' = \frac{k' \times g^G }{v' \times S }$	1-design
If $g \in A_{17}$	$k' = 6$	$ g^G = 12350257920$	$\lambda' = 4368$	$\mathcal{D} = 1 - (17, 6, 4368)$
If $g \in A_{12}$	$k' = 1$	$ g^G = 11975040$	$\lambda' = 1$	$\mathcal{D} = 1 - (12, 1, 1)$
If $g \in A_{13}$	$k' = 2$	$ g^G = 77837760$	$\lambda' = 12$	$\mathcal{D} = 1 - (13, 2, 12)$

Table 6.5: Some 1-designs from A_{17}, A_{12}, A_{13}

(i) The design $\mathcal{D} = 1 - (12, 1, 1)$ has $\lambda = k = 1$ and by Note 5.3.2 part (ii) we have the corresponding code $\mathcal{C}_p(\mathcal{D}) = [12, 12, 1]_p$ which is the full space \mathbb{F}_p^{12} , with $\text{Aut}(C) = \text{Aut}(\mathcal{D}) = s_{12}$ for all p .

3. Let $g_1 = (1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9\ 10\ 11\ 12)$ and $g_2 = (1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9)(10\ 11)$ be two conjugacy classes in A_{13} , then g_1 is conjugate to g_2 by Theorem 2.3.4 and

$$|g_1^{A_{13}}| = |g_2^{A_{13}}| = 86486400$$

Now we can apply part two of Theorem 6.2.2 to compute the value of S for the above cycles,

$$\begin{aligned} |S_{g_1}| &= \frac{(n - \text{Fix}(g))!}{2 \times \prod_{i=1}^n u_i^{r_i}} \\ &= \frac{12!}{2 \times 6^2} \\ &= 6652800 \end{aligned}$$

and

$$\begin{aligned} |S_{g_2}| &= \frac{(n - \text{Fix}(g))!}{2 \times \prod_{i=1}^n u_i^{r_i}} \\ &= \frac{11!}{2 \times 6 \times 3 \times 2} \\ &= 554400 \end{aligned}$$

A_n	$ Fix(g) $	$ g^G $	$\lambda' = \frac{k' \times g^G }{v' \times S }$	1-design
If $g_1 \in A_{13}$	$k' = 1$	$ g_1^G = 86486400$	$\lambda' = 1$	$\mathcal{D} = 1 - (13, 1, 1)$
If $g_2 \in A_{13}$	$k' = 2$	$ g_2^G = 86486400$	$\lambda' = 2$	$\mathcal{D} = 1 - (13, 2, 24)$

Table 6.6: Some 1-designs from $g_1, g_2 \in A_{13}$

- (i) The design $\mathcal{D} = 1 - (13, 1, 1)$ has $\lambda = k = 1$ and by Note 5.3.2 part (ii) we have the corresponding code $\mathcal{C}_p(\mathcal{D}) = [13, 13, 1]_p$ which is the full space \mathbb{F}_p^{13} , with $Aut(C) = Aut(\mathcal{D}) = s_{13}$ for all p .

4. Let $g = (1\ 2\ 3\ 4)(5\ 6)(7\ 8)(9\ 10)$ with $r_2 > 1$ then,

$$\begin{aligned}
|S| &= \frac{(n - Fix(g))!}{\prod_{i=1}^n u_i^{r_i}(r_i)!} \\
&= \frac{10!}{4 \times 2^3 \times 3!} \\
&= 18900.
\end{aligned}$$

A_n	Number of Fix(g)	$ g^G $	$\lambda' = \frac{k' \times g^G }{v' \times S }$	1-design
If $g \in A_{17}$	$k' = 7$	$ g^G = 367567200$	$\lambda' = 8008$	$\mathcal{D} = 1 - (17, 7, 8008)$
If $g \in A_{12}$	$k' = 2$	$ g^G = 1247400$	$\lambda' = 11$	$\mathcal{D} = 1 - (12, 2, 11)$
If $g \in A_{13}$	$k' = 3$	$ g^G = 5405400$	$\lambda' = 66$	$\mathcal{D} = 1 - (13, 3, 66)$

Table 6.7: Some 1-designs from A_{17}, A_{12}, A_{13}

5. Let $g = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)$ with $r_3 = 3$ then,

$$\begin{aligned} |S| &= \frac{(n - \text{Fix}(g))!}{\prod_{i=1}^n u_i^{r_i}(r_i)!} \\ &= \frac{9!}{3^3 \times 3!} \\ &= 2240. \end{aligned}$$

A_n	Number of $\text{Fix}(\mathbf{g})$	$ g^G $	$\lambda' = \frac{k' \times g^G }{v' \times S }$	1-design
If $g \in A_{17}$	$k' = 8$	$ g^G = 54454400$	$\lambda' = 11440$	$\mathcal{D} = 1 - (17, 8, 11440)$
If $g \in A_{12}$	$k' = 3$	$ g^G = 492800$	$\lambda' = 55$	$\mathcal{D} = 1 - (12, 3, 55)$
If $g \in A_{13}$	$k' = 4$	$ g^G = 1601600$	$\lambda' = 220$	$\mathcal{D} = 1 - (13, 4, 220)$

Table 6.8: Some 1-designs from A_{17}, A_{12}, A_{13}

6. Let $g = (1\ 2\ 3)(4\ 5\ 6)(7\ 8)(9\ 10)$ with $r_2 = 2$ and $r_3 = 2$ then,

$$\begin{aligned} |S| &= \frac{(n - \text{Fix}(g))!}{\prod_{i=1}^n u_i^{r_i}(r_i)!} \\ &= \frac{10!}{3^2 \times 2! \times 2^2 \times 2!} \\ &= 8400. \end{aligned}$$

A_n	Number of $\text{Fix}(\mathbf{g})$	$ g^G $	$\lambda' = \frac{k' \times g^G }{v' \times S }$	1-design
If $g \in A_{17}$	$k' = 7$	$ g^G = 490089600$	$\lambda' = 24024$	$\mathcal{D} = 1 - (17, 7, 2404)$
If $g \in A_{13}$	$k' = 3$	$ g^G = 7207200$	$\lambda' = 198$	$\mathcal{D} = 1 - (13, 3, 198)$

Table 6.9: Some 1-designs from A_{17}, A_{12}, A_{13}

7. Let $g = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(9\ 10)(11\ 12)$ with $r_4 = 2$ and $r_2 = 2$ then,

$$\begin{aligned} |S| &= \frac{(n - \text{Fix}(g))!}{\prod_{i=1}^n u_i^{r_i}} \\ &= \frac{12!}{4^2 \times 2! \times 4^2 \times 2!} \\ &= 1871100. \end{aligned}$$

A_n	Number of $\text{Fix}(\mathbf{g})$	$ g^G $	$\lambda' = \frac{k' \times g^G }{v' \times S }$	1-design
If $g \in A_{17}$	$k' = 5$	$ g^G = 11578366800$	$\lambda' = 1820$	$\mathcal{D} = 1 - (17, 5, 1820)$
If $g \in A_{13}$	$k' = 1$	$ g^G = 24324300$	$\lambda' = 1$	$\mathcal{D} = 1 - (13, 1, 1)$

Table 6.10: Some 1-designs from A_{17}, A_{13}

- (i) The design $\mathcal{D} = 1 - (13, 1, 1)$ has $\lambda = k = 1$ and by Note 5.3.2 part (ii) we have the corresponding code $\mathcal{C}_p(\mathcal{D}) = [13, 13, 1]_p$ which is the full space \mathbb{F}_p^7 , with $\text{Aut}(C) = \text{Aut}(\mathcal{D}) = s_7$ for all p .

Appendix

Programme

We have included main programme written in Magma that was used to obtain the corresponding codes from the designs obtained by applying Method 2 from the conjugacy classes of maximal subgroup A_{n-1} . All of this work was carried out on CHCP Lengau Cluster with University of Limpopo with Magma version 2.26.

```
G:=AlternatingGroup(n);
max:=MaximalSubgroups(G);
i:=1;
m:=max[i]'subgroup;
a1,g,a3:=CosetAction(G,m);
M:=Set(m);
C:=ConjugacyClasses(G);
c:={};d:={};
for i:=1 to #C do
if (M meet C[i][3]G) ne {} then
c:=c join {C[i][3]G};
d:=d join {i};
end if;
end for;
```

```

c:=Setseq(c);
dd:=[];
for i:=1 to #c do
dd[i]:= Setseq(c[i]);
end for;
//lambda:=#(M meet c[i])*#G /(#m * #c[i]);
[[i, Order(dd[i][1]), #c[i], #(M meet c[i]), #(M meet c[i]) * #G /(#m * #c[i])] : i in [1..#c]];
j:=2;
P:=c[j];//(P= 2X)
u:=M meet P;
B:={};
for g in G do
B:=B join {ug};
end for;
B:=Setseq(B);
D:=Design< 1, P|B >;
C:=LinearCode(D,GF(2));
D1:=Complement(D);
C1:=LinearCode(D1,GF(2));
Cc:=Dual(C);
Dimension(C);Dimension(C1);Dimension(Cc);
hull:=Dimension(C meet Cc);hull;

```

Bibliography

- [1] Amery, G., Gomani, S. and Rodrigues, B.G., 2021. Designs and binary codes from maximal subgroups and conjugacy classes of M_{11} . *Mathematical Communications*, pp.159-175.
- [2] Assmus, E.F. and Key, J.D., 1996. Designs and codes: an update. *Codes, Designs and Geometry*, pp.3-23.
- [3] Assmus, E.F. and Key, J.D., 1994. *Designs and their Codes* (No. 103). Cambridge University Press.
- [4] Assmus, E.F.Jr., Key, J.D.: *Designs and their codes*. In: *Cambridge Tracts in Mathematics*, vol. 103. Cambridge University Press, Cambridge (1992) (second printing with corrections, 1993).
- [5] Assmus, E.F., Assmus Jr, E.F., Key, J.D. and Key, J.D., 1992. *Designs and their Codes* (No. 103). Cambridge University Press.
- [6] Basheer, A.M., 2006. *Representation Theory of Finite Groups*. AIMS, south Africa.
- [7] Beth, T., Jungnickel, D. and Lenz, H., 1999. *Design Theory: Volume 1*. Cambridge University Press.
- [8] Biggs, N.L. and White, A.T., 1979. *Permutation groups and combinatorial structures* (Vol. 33). Cambridge University Press.

- [9] Cameron, P.J., Van Lint, J.H. and Cameron, P.J., 1991. Designs, graphs, codes and their links (Vol. 3). Cambridge: Cambridge University Press.
- [10] Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A. and Wilson, R.A., 1985. ATLAS of finite groups.
- [11] Conway, J.H., 1985. Atlas of finite groups: maximal subgroups and ordinary characters for simple groups. Oxford University Press.
- [12] Crnkovi, D., Mikuli Crnkovi, V. and Rodrigues, B.G., 2011. Designs, strongly regular graphs and codes constructed from some primitive groups. In Information Security, Coding Theory and Related Combinatorics (pp. 231-252).
- [13] Darafsheh, M.R., 2006. Designs from the group $PSL_2(q)$, q even. Designs, Codes and Cryptography, 39(3), pp.311-316.
- [14] Darafsheh, M.R., Iranmanesh, A. and Kahkeshani, R., 2009. Some designs and codes invariant under the groups S_9 and A_8 . Designs, Codes and Cryptography, 51, pp.211-223.
- [15] Fish, W., Key, J.D. and Mwambene, E., 2009. Codes, designs and groups from the Hamming graphs. J. Combin. Inform. System Sci, 34(1-4), pp.169-182.
- [16] Ganief, M.S., 1997. 2-generations of the sporadic simple groups (Doctoral dissertation).
- [17] Isaacs, I.M., 1976. Character theory of finite groups, vol. 69. Pure and Applied Mathematics, Academic Press, New York-London.
- [18] James, G. and Liebeck, M., 1993. Representations and Characters of Groups, Cambridge Univ.
- [19] Kahkeshani, R., 2020. On some designs constructed from the groups $PSL_2(q)$, $q = 53, 61, 64$. Algebraic Structures and Their Applications, 7(1), pp.59-67.

- [20] Kahkeshani, R., 2018. 1-Designs from the group $PSL_2(59)$ and their automorphism groups. *Mathematics Interdisciplinary Research*, 3(2), pp.147-158.
- [21] Key, J.D. and Mattson Jr, H.F., 1999. Edward F. Assmus, Jr.(1931-1998). *Designs, Codes and Cryptography*, 17(1-3), pp.7-11.
- [22] Key, J.D. and Moori, J., 2016. Designs from maximal subgroups and conjugacy classes of finite simple groups. *J. Combin. Math. Combin. Comput*, 99, pp.41-60.
- [23] Key, J.D. and Moori, J., 2008. Erratum: Codes, designs and graphs from the Janko groups J_1 and J_2 . *Journal of Combinatorial Mathematics and Combinatorial Computing*, 64, Comput. 64 (2008), 153. pp.143-159.
- [24] Key, J.D. and Moori, J., 2002. Codes, Designs and Graphs from the Janko Groups J_1 and J_2 . *Journal of combinatorial mathematics and combinatorial computing*, 40, pp.143-160
- [25] Key, J.D., Moori, J. and Rodrigues, B.G., 2003. On some designs and codes from primitive representations of some finite simple groups. *Journal of combinatorial mathematics and combinatorial computing*, 45, pp.3-20.
- [26] Kumwenda, K., 2011. Codes, graphs and designs related to iterated line graphs of complete graphs (Doctoral dissertation, University of the Western Cape).
- [27] Le, T. and Moori, J., 2015. On the automorphisms of designs constructed from finite simple groups. *Designs, Codes and Cryptography*, 76(3), pp.505-517.
- [28] Mbaale, X. and Rodrigues, B.G., 2021. Symmetric 1-designs from $PSL_2(q)$, for q a power of an odd prime. *Transactions on Combinatorics*, 10(1), pp.43-61.
- [29] Moori, J., 2021. Designs and Codes from Involutions of An . *Quaestiones Mathematicae*, pp.1-15.
- [30] Moori, J., 2021. Designs and codes from fixed points of finite groups. *Communications in Algebra*, 49(2), pp.706-720.

- [31] Moori, J., 2021. Designs and codes from fixed points of elements of Janko simple group J 1. *Communications in Algebra*, 49(10), pp.4159-4171.
- [32] Moori, J., 2014. Designs and Codes from $PSL_2(q)$. *Group theory, Combinatorics and Computing*, (RF Morse, D. Nikolova-Popova, S. Witherspoon, Eds.), Providence, RI: American Mathematical Society, *Contemp. Math*, 611, pp.137-149.
- [33] Moori, J., 2011. Finite groups, designs and codes. In *Information Security, Coding Theory and Related Combinatorics* (pp. 202-230).
- [34] Moori, J., 2006. *Finite Groups and Representation Theory*. University of Kawzulu-Natal.
- [35] Moori, J. and Rodrigues, B.G., 2011. On some designs and codes invariant under the Higman-Sims group. *Utilitas Mathematica*, 86.
- [36] Moori, J. and Rodrigues, B.G., 2009. A self-orthogonal doubly-even code invariant under McL. *Ars Combinatoria*, 91, pp.321-332.
- [37] Moori, J. and Rodrigues, B.G., 2007. Some designs and codes invariant under the simple group Co_2 . *J. Algebra*, 316(2), pp.649-661.
- [38] Moori, J., Rodrigues, B.G., Saeidi, A. and Zandi, S., 2020. Designs from maximal subgroups and conjugacy classes of Ree groups. *Advances in Mathematics of Communications*, 14(4), pp.135-202.
- [39] Moori, J. and Saeidi, A., 2018. Constructing some designs invariant under $PSL_2(q)$, q even. *Communications in Algebra*, 46(1), pp.160-166.
- [40] Moori, J. and Saeidi, A., 2018. Some designs invariant under the Suzuki groups. *Util. Math*, 109, pp.105-114.
- [41] Rahimipour, A.R., 2019. On a design from primitive representations of the finite simple groups. *Facta Universitatis, Series: Mathematics and Informatics*, pp.771-780.

- [42] Randriafanomezantsoa-Rodehery, G.F., 2013. Designs and codes from certain finite simple groups (Doctoral dissertation, North-West University (South Africa)).
- [43] Rodrigues, B.G., 2002. Codes of designs and graphs from finite simple groups (Doctoral dissertation).
- [44] Robinson, D.J., 2012. A Course in the Theory of Groups (Vol. 80). Springer Science and Business Media.
- [45] Rose, H.E., 2009. A course on finite groups. Springer Science and Business Media.
- [46] Rotman, J.J., 2012. An introduction to the theory of groups (Vol. 148). Springer Science and Business Media.
- [47] Roy, A. and Scott, A.J., 2009. Unitary designs and codes. *Designs, codes and cryptography*, 53, pp.13-31.
- [48] Saeidi, A., 2022. Designs and codes from fixed points of alternating groups. *Communications in Algebra*, 50(5), pp.2215-2222.
- [49] Saeidi, A., 2021. Designs and Codes from fixed points of alternating groups, *Communications in Algebra*, DOI: 10.1080/00927872.2021.2002886.
- [50] Scott, W.R., 2012. Group theory. Courier Corporation.
- [51] Shannon, C.E., 1948. A mathematical theory of communication. *The Bell system technical journal*, 27(3), pp.379-423.