CONSTRUCTION OF DESIGNS AND CODES INVARIANT UNDER THE GROUPS $PSp_4(q)$, WHERE q IS A PRIME POWER

by

CLARENCE KAREANA MOKALAPA

Thesis

Submitted in fulfillment of the requirements for the degree of

DOCTOR OF SCIENCE

in

MATHEMATICS

in the

FACULTY OF SCIENCE AND AGRICULTURE
School of Mathematical and Computer Sciences

at the

UNIVERSITY OF LIMPOPO

SUPERVISOR: Prof. TT Seretlo

CO-SUPERVISOR: Dr. A Saeidi

March 2025

Abstract

In this thesis, we aim to construct some designs and their codes from the projective symplectic group $PSp_4(q)$, where "q" is a prime power. We study the primitive permutation representations and conjugacy classes of projective symplectic groups and construct binary and ternary codes invariant under the group $PSp_4(q)$. To achieve this, we examine the structures of each maximal subgroup and study the conjugacy class table and character table within the group $PSp_4(q)$. We identify fixed points of the primitive actions of $PSp_4(q)$ and compute the designs parameters. We then construct codes that are invariant under the action of $PSp_4(q)$. Our investigation focuses on specific classes of maximal subgroups of $PSp_4(q)$, where we determine the design parameters using two methods known as Key-Moori Method 1 and 2. Finally, we construct codes based on these design parameters.

The goal is to find the suborbits corresponding to specific maximal subgroups. To do this, we first identify some maximal subgroups of the group, then examine how the group action partitions the set into suborbits under the action of each maximal subgroup. These suborbits can help us understand the structure of the group and its actions more effectively, as outlined in Method 1. We examine the character table of the group $PSp_4(q)$, which provides information about the irreducible representations and their degrees. Using this information, we then find the corresponding permutation characters, which describe how the group acts on sets, such as conjugacy classes or coset spaces, under Method 2. By employing the techniques of examining suborbits and character table of the group $PSp_4(q)$, we are able to derive block-primitive and point-transitive $1-(v,k,\lambda)$ designs from the conjugacy classes and maximal subgroups of the group $PSp_4(q)$. We analyze $1-(v,k,\lambda)$ design properties and construct codes that are defined by the action of groups matrices of the designs.

We also determine the corresponding linear codes associated with these designs in the

special case where $q = 3$. We examine various properties of these codes, such as their dual structure, weight distribution, and error-detection and error-correction capabilities. The codes, which are constructed using the permutation group, can be viewed as submodules of the permutation module corresponding to the action of $PSp_4(q)$. By analyzing these codes, we gain insights into their invariant properties and symmetries in relation to the group action. To demonstrate this, we focus on the finite simple group $G = PSp_4(3)$ and explore the linear and ternary codes derived from its 2- and 3-dimensional representations. Additionally, we establish connections between the combinatorial designs and the codes that remain invariant under the action of $PSp_4(3)$.

Preface

The work described in this thesis was carried out under the supervision and direction of Professor T.T. Seretlo and Doctor A. Saeidi, School of Mathematics and Computer Science, University of Limpopo, from January 2022 to November 2024.

The thesis represents original work by the author and has not otherwise been submitted in any form for any degree or diploma to any other University. Where the use of others work has been made it is duly acknowledged in the text.

Signed:

Mokalapa Clarence Kareana	04 SEP 2025 Date
Doctor A Saeidi (Co-supervisor)	04-Sep-25 Date
Professor T T Seretlo (Supervisor)	04/09/2025 Date

Dedication

TO MY DAUGHTERS AND EVERYONE AROUND THE WORLD ESPECIALLY THOSE WHO LOST THEIR LOVE-ONE'S DUE TO THE PANDEMIC CORONA VIRUS, MAY THEIR SOULS REST IN ETERNAL PEACE.

Acknowledgements

I heartily express my profound gratitude to my supervisor, Professor T.T. Seretlo, for his invaluable learned guidance, advice, encouragement, understanding and support he has provided me throughout the duration of my studies which led to the compilation of this thesis. I will be always indebted to both my supervisor and co-supervisor (Doctor A. Saeidi) for introducing me to this fascinating area of Mathematics and creating my interest in Designs and Coding Theory, Group Theory, Combinatorics and Abstract Algebra. I have learnt so much from them, not only in the academic orientations, but in various walks of life. I am uncertain as to what extent words like thankfulness and sense of obligation could express the relevance of their dedication and devoted attention to me. In the absent of words which could convey my sense of humble gratitude I would like to say it in my home language : "KEALEBOGA".

I am grateful for the facilities made available to me by the School of Mathematical Sciences in the University of Limpopo and the Centre for High Performance Computing (CHPC), South Africa, for providing computational resources (MAGMA) to this research project. Finally, I sincerely give thanks to my entire family for giving me strength to continue doing Mathematics as my destiny.

Notation and conventions

$\mathbb{N}$	the set of natural numbers
$\mathbb{Z}$	the set of integer numbers
$\mathbb{F}$	a field
$\mathbb{F}^*$	$\mathbb{F} - \{0\}$
$\mathbb{R}$	the field of real numbers
$\mathbb{C}$	the field of complex numbers
$char(\mathbb{F})$	characteristic of the field $\mathbb{F}$
V	a vector space
$dim(V)$	dimension of a vector space V
$V(n, 2)$	a vector space of dimension n over $\mathbb{F}_2$
$det(V)$	determinant of a matrix of vector space V
G	a group
1_G	the identity element of G
$K \leq G$	K is a subgroup of G
$K \not\leq G$	K is not a subgroup of G
$N \trianglelefteq G$	N is a normal subgroup of G
$Aut(G)$	the automorphism group of G
$N \cdot K$	a non-spit extension of N by K
$N{:}K$	a split extension of N by K
$N \circ K$	a central product of N by K
h^g	conjugation of h by g
$N_G(H)$	the normalizer of the subgroup H in G
$C_G(H)$	the centralizer of the subgroup H in G

C	a q-ary code
$\mathcal{D}$	an incident structure
$\mathbb{G}$	a generator matrix of a code
$\mathbb{H}$	the parity check matrix of a code
$Aut(C)$	the automorphism code of C
$Aut(\mathcal{D})$	the automorphism design of $\mathcal{D}$
Γ	a graph
$PG(V)$	the projective geometry
$AG(V)$	the affine geometry
$[n,k]_2$	a binary code of length n and dimension k
$[n,k,d]_2$	a binary code of length n, dimension k and minimum distance d
$F[x]$	a set of polynomials
$F_2[x]$	a set of polynomials over finite field $\mathbb{F}_2$
$F_2[x]/f(x)$	a set of ring polynomials over finite field $\mathbb{F}_2$
$\langle f(x) \rangle$	a code generated by $f(x)$
$\langle x_1, x_2, \cdots, x_n \rangle$	the subspace spanned over $\mathbb{F}$ by subset $\{x_1, x_2, \cdots, x_n\}$
Ω	a set
$\emptyset$	empty set
$\lvert\Omega\rvert$	the cardinality of the set Ω
$\mathbb{F}_q$	the Galois field of q elements
$GL_n(q)$	general linear group of dimension n over $\mathbb{F}_q$
$GL(V)$	general linear group over V
$Sc(V)$	the centre $GL(V)$
$v \cdot u$	the dot product of v and u
$GF(2)$	the Galois field of 2 elements
$GL_n(2)$	general linear group of dimension n over $\mathbb{F}_2$
S_n	the symmetric group on n symbols
A_n	the alternating group on n symbols
$Sp_{2m}(q)$	symplectic group of dimension $2m$ over $\mathbb{F}_q$
$PSp_{2m}(q)$	projective symplectic group of dimension $2m$ over $\mathbb{F}_q$

Contents

Introduction

In [34], Key and Moori used two methods to construct combinatorial designs and codes from finite simple groups. They considered the primitive permutation representation and the conjugacy classes of simple groups to construct 1-designs. These methods have been applied to some families of simple groups [34, 38, 42], including several sporadic simple groups [27, 28]. In 2020, Moori developed a third method to construct 1-designs from the fixed points of the action of a permutation group [37]. Using Method 1, Moori and Saeidi constructed some designs and codes that are invariant under the action of the Tits group [38]. In [12], Darafsheh applied Method 1 to construct designs from $PSL_2(q)$ and a pair of maximal subgroups that are isomorphic to dihedral groups. In [39] and [40], Saeidi and Moori applied Method 1 and 2 to construct designs and codes from all maximal subgroups of $PSL_2(q)$ for q even. They also constructed some designs that are invariant under Suzuki groups $Sz(q)$, where q is even. Thereafter, Mbaale, Rodrigues and Zandi applied Method 1 and 2 to construct designs and codes from maximal subgroups and conjugacy classes of $PSL_2(q)$ for q a power of an odd prime [32]. Moori used Method 3, which involves utilizing fixed points from a finite group, to construct designs and codes [37]. Saeidi then applied reduced designs developed using Key-Moori Method 2 and examined their relationship with those found by using Method 3 [49].

In this thesis, we construct designs using the maximal subgroups and conjugacy classes of the projective symplectic group $PSp_4(q)$. The projective symplectic group $PSp_4(q)$ is defined as the group of symmetries of a 4-dimensional vector space over the finite field $\mathbb{F}_q$ acting on a non-degenerate skew-symmetric bilinear form. It can be viewed as a quotient group of the symplectic group $Sp_4(q)$. We investigate specific classes of maximal subgroups of $PSp_4(q)$ and determine the design parameters employing Key-Moori Methods 1 and 2. The method involves constructing the suborbits corresponding

to specific maximal subgroups of $PSp_4(q)$ and examining the character table of the group. We analyze the character table and determine the corresponding permutation characters of $PSp_4(q)$ to construct the design parameters. We also construct linear codes and ternary codes which are invariant under the action of the group $PSp_4(3)$.
Our notations for designs follows as in [4]. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure; that is, a triple consisting of a point set $\mathcal{P}$, a block set $\mathcal{B}$ which is disjoint to $\mathcal{P}$, and an incidence set $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. If the ordered pair $(p, B) \in \mathcal{I}$, we say that p is incident with B. It is often convenient to assume that the blocks in $\mathcal{B}$ are subsets of $\mathcal{P}$, so (p, B) in $\mathcal{I}$ if and only if p in B. For a positive integer t, we say that $\mathcal{D}$ is a t-design if every block B in $\mathcal{B}$ is incident with exactly k points and every t distinct points are together incident with λ blocks. In this case, we write $\mathcal{D} = t-(v, k, \lambda)$, where $v = |\mathcal{P}|$. We say that $\mathcal{D}$ is symmetric if it has same number of points and blocks, otherwise, $\mathcal{D}$ is non-symmetric.
A finite field of q elements, is denoted by $\mathbb{F}_q$. A linear code of length n over $\mathbb{F}_q$ is defined as a vector subspace of $V = \mathbb{F}_q^n$. A codeword is a vector v in a linear code of a vector space V. The Hamming distance $d(u, v)$ between any two vectors u and v in the code C is the number of coordinates in which they differ. In a linear code, the minimum Hamming distance d is equal to the minimum weight of its non-zero codewords. This is denoted by $wt(C) = min\{wt(v)|v \text{ in } C, v \neq 0\}$, where $wt(v)$ denotes the weight of the vector v (the number of non-zero coordinates in v). The minimum weight among the non-zero codewords in the code C gives the minimum Hamming distance of the code. The dual code (or orthogonal code) of a linear code C, denoted by $C^{\perp}$, is the set of vectors in V that are orthogonal to every vector in C with respect to the standard dot product. A code is said to be self-dual if C is equal to its dual code $C^{\perp}$, and it is self-orthogonal if C is a subset of its dual code $C^{\perp}$. Consider, a binary (n, k)-code, where n denotes the length and k is the code dimension. If the minimum distance of a code is known and represented by d, then we write (n, k, d)-code.
In linear codes, the weight of a code is the minimum number of non-zero (or 1's) in any of the codewords. The weight of the code (often referred to as the minimum weight) is important in determining its error-detecting and error-correcting properties. The support of a codeword is the set of coordinate positions in which the codeword has non-zero entries. Two different codewords of weight w may have the same support. Let $\mathcal{P} = \{1, 2, 3, \cdots, n\}$ be the set of coordinate positions in the codewords. The set $\mathcal{B}$

can be defined as the set of supports of the codewords of weight w in a code C, where each support is a subset of $\mathcal{P}$ that contains exactly w positions. It is possible that $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a t-design for some t if the incidence relation $\mathcal{I}$ is the typical containment of sets. In this case, we say that the codewords of weight w in C hold or support a t-design, which is called a support design of C. A Steiner system is a type of block design, specifically a t-design with $\lambda = 1$ and $t \geq 2$. A Steiner system with parameters (t, k, n) written $S(t, k, n)$ for $n > 1$ is an n-element set S together with a set of k-element subsets of S called blocks, with the property that each t-element subset of S is contained in exactly one block.

The body of the thesis is structured as follows:

In Chapter 1, we give the preliminary definitions and results of group theory. The topics discussed include permutation groups, the transitive action of a group on some set; representation theory; vector spaces; modular representations; and permutation characters.

Chapter 2 is divided into six sections as follows: In Section 2.1, we explore design theory, discussing the definition of an incidence structure and the incidence matrix of a design. In Section 2.2.1, we construct designs using Key-Moori Method 1. We will discuss how to construct symmetric 1-designs from primitive permutation representations of a simple group. In Section 2.2.2, We use permutation characters to find the parameters of designs under Method 2. In Section 2.3, we discuss linear codes and their duals. A block code, denoted by (n, k, d), is defined by its word length n, the number of codewords k, and its minimum distance d. In Section 2.4, we provide a comprehensive overview of how G-invariant designs and codes are constructed using algebraic computational algorithms.

In Chapter 3, Sections 3.13.6, we provide a background on the projective symplectic group $PSp_4(q)$ in general. The behavior, cardinality, structure, simplicity, and polarity forms of the projective symplectic groups are discussed. We also discuss the conjugacy classes, class representatives, the order of centralizers, and the sizes of each conjugacy class of $Sp_4(q)$. Therefore, we use these results to construct the conjugacy classes and character table of $PSp_4(q)$ in order to construct 1-designs. In Section 3.7, we investigate some maximal subgroups of $PSp_4(q)$, along with their structures, properties, and indices.

In Chapter 4, we provide the designs constructed and obtained using the two methods:

Key-Moori Method 1 and Key-Moori Method 2. We also provide the corresponding codes and their duals that are invariant under $PSp_4(3)$.

Chapter 1

Groups and representation theory

In this chapter, we discuss groups and representation theory along with their applications. We refer the reader to the notes in [43], [47], [48] and [55] for more details.

1.1 Preliminary group concepts

Definition 1.1.1. *A group is a set G together with a binary operation $*$ satisfying the following conditions for $g, h, k \in G$:*

(i) there exist $1_G \in G$, such that $g * 1_G = 1_G * g = g$ for all $g \in G$;

(ii) for every $g \in G$, there exist $g^{-1} \in G$ such that $g^{-1} * g = g * g^{-1} = 1_G$;

(ii) $g * (h * k) = (g * h) * k$.

The element g^{-1} is called the inverse of $g \in G$, and the element 1_G is called the identity element of G.

Remark 1.1.2. *A group $(G, *)$ is said to be abelian if $g * h = h * g$ for all $g, h \in G$.*

In cases where the operation $*$ is trivial or well-known, we write G to denote the group $(G, *)$. We also simply write $a \cdot b$ or ab for $a * b$.

Definition 1.1.3. *Let G be a group. If $H \subseteq G$ then H is a subgroup of G if H is a group under the binary operation inherited from G.*

Theorem 1.1.4. [48] *Let H be a non-empty subset of a group G. Then H is a subgroup of G, denoted by $H \leq G$, if and only if the following conditions hold:*

1. *H is non-empty.*

2. *For all $a, b \in H$, the element $ab^{-1} \in H$.*

These conditions imply that H contains the identity element of G.

Note 1.1.5. *The order of a finite group G, denoted by $|G|$, is its cardinality, which is the total number of elements in G.*

Definition 1.1.6. *Let G be a finite group and p be a prime. Then G is called a p-group if the order of G, denoted by $|G|$, is a power of p; that is, $|G| = p^n$ for some non-negative integer n. Furthermore, in a p-group, the order of each element of G is also a power of p.*

Definition 1.1.7. *A group G is called cyclic if there exists an element $g \in G$ such that every element of G can be expressed as a power of g. That is, $G = \langle g \rangle = \{g^n | n \in \mathbb{Z}\}$.*

Definition 1.1.8. *Let $H \leq G$. We say that H is a normal subgroup of G if for all $g \in G$, we have $gHg^{-1} = H$. This is denoted by $H \trianglelefteq G$.*

Proposition 1.1.9. [48] *A subgroup H of a group G is said to be normal in G, denoted by $H \trianglelefteq G$, if for every element $g \in G$, the conjugate of H by g is contained within H. This means that for all $g \in G$ and $h \in H$, we have:*

$$gHg^{-1} = H.$$

That is, the set of all conjugates of elements of H by g is equal to H.

Remark 1.1.10. *The set gHg^{-1} is a subgroup of G.*

Definition 1.1.11. *Let g be an element of G. We define $\phi_g(x) = gxg^{-1}$ for any x in G. Then $\phi_g(x)$ is an automorphism of G, known as an Inner automorphism, denoted by $Inn(G)$, of G.*

Definition 1.1.12. *An Inner automorphism of a group G is an automorphism of the form $\phi_g(x) = gxg^{-1}$, where x is a fixed element of G. Moreover, there is isomorphism between quotient group $\frac{G}{Z(G)}$, where $Z(G)$ is the center of G and the inner automorphism $\frac{G}{Z(G)} \cong Inn(G)$.*

Theorem 1.1.13. [48] *A subgroup H of a group G is normal in G if and only if every left coset of H in G is a right coset of H in G, that is, $gH = Hg$ for all g in G.*

Theorem 1.1.14. [48] *A subgroup H of G is normal in G, if for $g \in G$ and $h \in H$, the conjugate of h of g is still in H. In other words, for all $g \in G$ and $h \in H$, the element $ghg^{-1} \in H$.*

Definition 1.1.15. *The centre of a group G is the subset,*

$$Z(G) = \{g \in G | gx = xg, \ for \ all \ x \in G\}.$$

Remark 1.1.16. *$Z(G)$ is a normal subgroup of G.*

Definition 1.1.17. *The set G/H is the collection of all distinct cosets of H in G, where each coset is of the form $gH = \{gh | h \in H\}$ for each $g \in G$.*

Definition 1.1.18. *If H is a normal subgroup of G, then the group G/H is called a quotient group (or factor group) of G by H.*

Definition 1.1.19. *Let G be a finite and H a finite subgroup of G. The index of H in G, denoted $[G : H]$, is defined as the number of distinct left cosets (or right cosets) of H in G. The index is given by:*

$$[G : H] = \frac{|G|}{|H|},$$

where $|G|$ is the order (number of elements) of the group G and $|H|$ is the order (number of elements) of the subgroup H.

Remark 1.1.20. *If G is a finite group, then we have $|G/H| = \frac{|G|}{|H|} = [G : H]$.*

Theorem 1.1.21. [48] *Let $H \leq G$ such that if $[G : H] = \frac{|G|}{|H|} = 2$. Then H is normal in G.*

Definition 1.1.22. *A map ϕ of a group G into $\overline{G}$ is a homomorphism if $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G.*

Definition 1.1.23. *A homomorphism if ϕ is called a*

1. *monomorphism if ϕ is one-to-one;*

2. *epimorphism if ϕ is onto;*

3. *isomorphism if ϕ is both one-to-one and onto.*

Remark 1.1.24. *If there exist an isomorphism from G to $\overline{G}$, then we say that G and $\overline{G}$ are isomorphism and we write $G \cong \overline{G}$. The isomorphism is an equivalency relation and two isomorphic groups have the same structure. An isomorphism from a group into itself is called an automorphism.*

Lemma 1.1.25. *Let $\phi : G \to \overline{G}$ be a homomorphism. Then:*

1. *$\phi(e) = e$;*

2. *for any element $a \in G$, we have $\phi(a^{-1}) = \phi(a)^{-1}$.*

Lemma 1.1.26. [43] *If ϕ is a homomorphism from G into $\overline{G}$, then the kernel of G, denoted by $Ker(\phi)$, and the image of G, denoted by $Im(\phi)$ are defined by*

(i) $Ker(\phi) = \{g | g \in G, \phi(g) = 1_{\overline{G}}\}$;

(ii) $Im(\phi) = \{\phi(g) | g \in G\} = \phi(G)$.

Theorem 1.1.27. [43] *If $\phi : G \to \overline{G}$ is a homomorphism, then*

(i) $Ker(\phi) \trianglelefteq G$;

(ii) $Im(\phi) \leq \overline{G}$.

Theorem 1.1.28. [43] *Let $\phi : G \to \overline{G}$ be a homomorphism. Then ϕ is a monomorphism if and only if $Ker(\phi) = \{1_G\}$.*

Theorem 1.1.29. [43] *(First isomorphism theorem) Let $\phi : G \to \overline{G}$ be a homomorphism with kernel K. Then $G/K \cong Im(\phi)$.*

Corollary 1.1.30. [43] *If $\phi : G \to \overline{G}$ is an epimorphism with kernel K. Then $G/K \cong \overline{G}$.*

Theorem 1.1.31. [43] *(Second isomorphism theorem) Let $H \trianglelefteq G$, $K \trianglelefteq G$ and $K \leq H$. Then $\frac{G/K}{H/K} \cong G/H$.*

Theorem 1.1.32. [43] *(Third isomorphism theorem) Let K and H be subgroups of G, assume that $H \trianglelefteq G$. Then $K/K \cap H \cong KH/H$.*

Definition 1.1.33. *Let G be a group. The commutator of two elements $a, b \in G$ is the element $[a, b] = a^{-1}b^{-1}ab$. The derived group $\overline{G}$ is the subgroup of G generated by all commutators, that is, $\overline{G} = \langle [a, b] : a, b \in G \rangle$.*

Remark 1.1.34. *G is abelian if and only if $G' = 1_G$.*

Definition 1.1.35. *A group G is said to be perfect if $G = G'$.*

1.2 Permutation groups

The groups of transformations on some set Ω are important groups in mathematics. For instance, a group of transformations that preserve the structure of a geometric figure, such as a polygon, is called a dihedral group D_n, where n refers to the number of sides of the polygon. The symmetric group S_Ω on a set Ω is the group of all permutation of Ω. A permutation is a bijection from the set Ω to itself.

Definition 1.2.1. [55] *A group action is a map $\tau : G \times \Omega \to \Omega$ such that two axioms are satisfied; for all g, h in G and ω in Ω,*

(i) $g \cdot (h\omega) = (gh) \cdot \omega$;

(ii) $1_G \cdot \omega = \omega$.

Definition 1.2.2. *If Ω is a non-empty set and $\phi : \Omega \to \Omega$ is a bijection, then we say that ϕ is a permutation on Ω. The set of all permutations on Ω forms a group under the composition of functions. This group is denoted by S_Ω and is called the symmetric group on Ω. If Ω is finite and $|\Omega| = n$, then we can represent Ω by $\{1, 2, 3, \cdots, n\}$ and we denote S_Ω by S_n, where $|S_n| = n!$.*

Note 1.2.3. *If $\phi \in S_n$, then we represent ϕ by* $\phi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \phi(1) & \phi(2) & \phi(3) & \cdots & \phi(n) \end{pmatrix}$ *where,*

$$\Omega = \{1, 2, 3, \cdots, n\} = \{\phi(1), \phi(2), \phi(3), \cdots, \phi(n)\}.$$

Definition 1.2.4. *Let G be a finite group acting on a set Ω, and let $\alpha \in \Omega$. Then the stabilizer of $\alpha \in G$ by Ω is given by*

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

In particular, G_α is the subgroup of G consisting of all elements that fix α under the group action.

Definition 1.2.5. [47] *The kernel of ϕ, denoted $ker(\phi)$ defined in 1.1.22, is the normal subgroup of G consisting of the elements acting trivially on Ω, defined as:*

$$ker(\phi) = \bigcap_{x \in \Omega} G_x.$$

Definition 1.2.6. [55] *The image of ϕ defined in 1.1.22, denoted by $\phi(G)$ is a subgroup of S_Ω. In particular $\phi(G)$ is a permutation group on Ω.*

Lemma 1.2.7. [42] *An action of a group G on a set Ω is said to be faithful if $Ker(\phi) = 1_G$. In this case, we have $G \cong \phi(G)$.*

Lemma 1.2.8. [42] *Let G act on Ω. For some $x, y \in \Omega$, define the relation $x \sim y$ if and only if there is $g \in G$ such that $g.x = y$. Then $\sim$ is an equivalent relation on Ω.*

Remark 1.2.9. *The action of G partitions the set Ω in to equivalence classes, which are called orbits of G on Ω (or G-orbits on Ω).*

Definition 1.2.10. *If G is a group and x, y are contained in G, then we say that x is conjugate to y in G if there is g in G such that $y = gxg^{-1}$. The relation x conjugate to y is an equivalence relation on G. The equivalence classes are called conjugacy classes of G and are denoted by $[x]$ for $x \in G$. Then we have:*

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

Definition 1.2.11. *If $x \in G$, then centralizer of x in G, denoted by $C_G(x)$, is the set of all $y \in G$ that commute with x, that is*

$$C_G(x) = \{y | xy = yx, y \in G\}.$$

Remark 1.2.12. *The centralizer $C_G(x)$ is a subgroup of G.*

Theorem 1.2.13. [43] *The number of conjugates of an element x in a group G is $[G : C_G(x)]$.*

Remark 1.2.14. *If G is a finite group then the number of conjugates of x in G is:*

$$|[x]| = [G : C_G(x)] = \frac{|G|}{|C_G(x)|}.$$

Definition 1.2.15. *The normalizer of a subgroup H in a group G is defined as:*

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

Remark 1.2.16. *The normalizer $N_G(H)$ is a subgroup of G containing H. Additionally, H is a normal subgroup of $N_G(H)$.*

Definition 1.2.17. *A group G is said to be simple if $G \neq \{1_G\}$ and it contains no normal subgroup except the trivial normal subgroups which are G and $\{1_G\}$.*

Classification of Finite Simple Groups (CFSG) was completed in 1981. It has a history of nearly 150 years and its proof occupies 15000 journal pages.

Theorem 1.2.18. *According to [55], the classification for finite simple groups states that every finite simple group is isomorphic to one of the following groups:*

(i) a cyclic group C_p of prime order p;

(ii) an alternating group A_n, for $n \geq 5$;

(iii) a classical group:
symplectic, $PSp_{2m}(q), m \geq 2$, except $PSp_4(2)$;

(iv) one of the finite groups of Lie type (classical or exceptional);

(v) one of the 26 sporadic simple groups.

Remark 1.2.19. $PSU_4(2) \cong PSp_4(3)$.

For further details, refer to The Atlas of Finite Groups or Wilson's book on Group Theory.

1.3 Transitive group action

A permutation group G is said to be transitive on Ω, if for all $\alpha, \beta \in \Omega$, there exist an element $g \in G$ such that the image α^g of α under g is equal to β.

Theorem 1.3.1. [47] *Let a group G acts on a set Ω. The set of all orbits of G on Ω form partition of Ω.*

Theorem 1.3.2. *A transitive group action of G on a subgroup H is equivalent to the action of G on the set of cosets G/H, which forms a quotient group if H is a normal subgroup of G.*

Theorem 1.3.3. [42] *If G is transitive on the set Ω, then G is k-transitive for $k > 1$, if for any two sets of k elements $(\alpha_1, \alpha_2, \cdots, \alpha_k)$ and $(\beta_1, \beta_2, \cdots, \beta_k)$ in Ω, there exists an element of $g \in G$ such that $(\alpha_1, \alpha_2, \cdots, \alpha_k)^g = (\beta_1, \beta_2, \cdots, \beta_k)$.*

Note 1.3.4. *If $k = 2$, then G is doubly transitive and $k = 3$ is triply transitive.*

Theorem 1.3.5. [40] *A k-transitive group is said to be sharply-transitive if for any k-distinct elements $x_1 x_2 \cdots x_k$ in the set Ω, the stabilizer of these k elements in the group G, denoted by $G_{[x_1 x_2 \cdots x_k]}$ is exactly the identity element $\{1_G\}$.*

Theorem 1.3.6. [42] *Let G be a sharply-transitive group on the set Ω, then $|G_{[x_1 x_2 \cdots x_k]}| = 1_G$ implies that $|G| = n(n-1)(n-2)\cdots(n-k+1)$.*

Proposition 1.3.7. [38] *Let G be a transitive permutation group of degree n acting on a set Ω if and only if G has a subgroup of index n.*

Theorem 1.3.8. [42] *If G is a group acting on a set Ω, then for each x in Ω there exists a bijection map $f : \frac{G}{G_x} \to G \cdot x$ given by $f(gG_x) = g \cdot x$. In particular, any transitive group action is equivalent to an action on cosets.*

Lemma 1.3.9. [38] *Assume that G is a transitive group on a set Ω, with $|\Omega| = n \geq 2$. If G_α is $(k-1)$-transitive on Ω for any α in Ω, then G is k-transitive on Ω.*

1.4 Primitive group action

In this section, we discuss blocks and the properties of primitive actions.

Definition 1.4.1. *Let G acts on a set Ω and $\mathcal{B}$ be a subset of a set Ω such that $\mathcal{B}^g = \mathcal{B}$ or $\mathcal{B}^g \cap \mathcal{B} = \emptyset$ for all g in G. Then, $\mathcal{B}$ is said to be a block for G.*

Remark 1.4.2. *For $\emptyset, \Omega$ and $\{\alpha\}$ a blocks of size 1 are blocks known as trivial blocks, otherwise, any other blocks are non-trivial.*

Definition 1.4.3. *If the action of a group G is transitive on a set Ω such that G has no non-trivial block on Ω, then we say G is primitive. Otherwise, G is said to be imprimitive.*

Corollary 1.4.4. [47] *Any transitive group G acting on a finite set Ω of size p, where p is a prime, is primitive.*

Lemma 1.4.5. [47] *Let G acts on a set Ω and let $\mathcal{B}_1$ and $\mathcal{B}_2$ be blocks of a permutation group G. Then $\mathcal{B}_1^g \cap \mathcal{B}_2^g = \mathcal{B}_1 \cap \mathcal{B}_2$.*

Theorem 1.4.6. [47] *If $\mathcal{B}_1$ and $\mathcal{B}_2$ are blocks of a permutation group G, then $\mathcal{B}_1^g \cap \mathcal{B}_2^g$ is also a block of G.*

Theorem 1.4.7. [55] *Let $\Omega = \{1, 2, 3, \cdots, n\}$ be a set. Then for every n,*

(i) the symmetric group S_n acts n-transitively on Ω;

(ii) the alternating group A_n acts $(n-2)$-transitively on Ω.

Theorem 1.4.8. [47] *For $k \geq 2$, every k-transitive group G acting on a set Ω is primitive. In particular, we have:*

(i) for $n \geq 3$, all symmetric groups are primitive such that S_n is transitive on Ω;

(ii) for $n \geq 4$, all alternating groups are primitive such that for $n \geq 3$, then A_n is $(n-2)$-transitive on Ω.

Theorem 1.4.9. [46] *Let H be a subgroup of a primitive group G acting faithfully on a set Ω such that $\{1_G\} \neq H \trianglelefteq G$. Then H acts transitively on Ω.*

Theorem 1.4.10. [46] *(Characterization of primitive permutation groups) Let G be a transitive permutation group acting on the set Ω. Then G is primitive if and only if for each $\alpha \in \Omega$, the stabilizer G_α is a maximal subgroup of G.*

1.5 Representations and characters of groups

In this section, we discuss general background on representation theory. We refer the reader to [43] and [55] for notations additional details.

Definition 1.5.1. *A representation of a group G on a vector space V over a field $\mathbb{F}$ is a group homomorphism from G to $GL(V)$, the general linear group on V. That is, a representation is a map,*

$$\phi : G \to GL(V)$$

such that:

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \quad \text{for all } g_1, g_2 \in G.$$

In particular, if $GL(V)$ is a simple group, then a representation ϕ of $GL(V)$ is said to be irreducible if there are no non-trivial $\phi(GL(V))$-invariant subspaces of V.

Remark 1.5.2. *If V is of finite dimension n, then $GL(V)$ is identified as $GL(n, \mathbb{F})$, the group of $n \times n$ invertible matrices on the field $\mathbb{F}$.*

Definition 1.5.3. [43] *Let $f : G \to GL_n(\mathbb{F})$ be a representation of the group G over a field $\mathbb{F}$. Then the function $\chi : G \to \mathbb{F}$ defined by $\chi(g) = tr(f(g))$ is called the character of f.*

Definition 1.5.4. [43] *Let $\rho : G \to GL_n(\mathbb{F})$ be a function such that $\rho(g) = \rho(xgx^{-1})$ for all $x \in G$. Then ρ is said to be a class function.*

Definition 1.5.5. *Let χ be a character of G afforded by a representation ϕ of G. Then:*

1. *An irreducible character is a character afforded by an irreducible representation.*
2. *The degree of a character χ of G is the number $\chi(e)$.*
3. *A linear character is a character of degree one.*

Remark 1.5.6.

1. *If χ_1 and χ_2 are two characters of G, their sum is defined by $(\chi_1 + \chi_2)(y) = \chi_1(y) + \chi_2(y)$ and their product is defined by $(\chi_1\chi_2)(y) = \chi_1(y)\chi_2(y)$ for all $y \in G$.*
2. *If χ_1 is a character of G, its complex conjugate is defined by $\overline{\chi}(y) = \overline{\chi(y)}$ for all $y \in G$, where $\overline{\chi(y)}$ denotes the complex conjugate of the complex number $\chi(y)$.*

Definition 1.5.7. [55] *Let $V = \mathbb{F}^n$ be a vector space of dimension n over a field $\mathbb{F}$. Then any linear transformation $\rho : V \to V$ can be represented by an $n \times n$ matrix with entries from $\mathbb{F}$. Moreover, ρ is invertible if the corresponding matrix has non-zero determinant (non-singular).*

Definition 1.5.8. [55] *The general linear group of degree n over $\mathbb{F}_q$ (a finite field of q elements) is defined as,*

$$GL_n(q) = \{\mathcal{A} \,|\, \mathcal{A} \text{ is an } n \times n \text{ matrix over } \mathbb{F}_q \text{ with } det(\mathcal{A}) \neq 0\}.$$

Definition 1.5.9. *Let G be a group. The set of irreducible characters of G, denoted by $Irr(G)$, consists of characters that correspond to irreducible representations of G. These characters can have degrees greater than 1; specifically, the trivial character, which is of degree 1, is included in this set. All irreducible characters have positive integer degrees, starting from 1 for the trivial character.*

Remark 1.5.10. *The $GL_n(q)$ acts on V this implies that a matrix $\mathcal{A} \in GL_n(q)$ moves the vector $v \in V$ according to the linear transformation determined by $\mathcal{A}$.*

Example 1.5.11. *Define:*

$$\rho : GL_3(q) \times q^3 \to q^3 \qquad by \quad (\mathcal{A}, v) \mapsto \mathcal{A}v$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \to \begin{pmatrix} ax + by + cz \\ dx + ey + fz \\ gx + hy + iz \end{pmatrix},$$

ρ is an action of $GL_3(q)$ on q^3.

Observe that, the identity element in $GL_3(q)$ is the identity matrix $\begin{pmatrix} 1_G & 0_G & 0_G \\ 0_G & 1_G & 0_G \\ 0_G & 0_G & 1_G \end{pmatrix}$

such that

$$\begin{pmatrix} 1_G & 0_G & 0_G \\ 0_G & 1_G & 0_G \\ 0_G & 0_G & 1_G \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1_q x + 0_q y + 0_q z \\ 0_q x + 1_q y + 0_q z \\ 0_q x + 0_q y + 1_q z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Remark 1.5.12. *A group G acting on a set Ω is corresponds a homomorphism from G to S_Ω.*

Definition 1.5.13. *A character χ of G is faithful if its kernel consists of the identity element alone.*

Definition 1.5.14. *The principal character of G is the character 1_G satisfying $1_G(y) = 1$ for all $y \in G$.*

Remark 1.5.15. *If $\chi = \Sigma_{i=1}^{n} \alpha_i \psi_i$ are characters of G, then ψ_i are constituents of χ, which are irreducible characters of G.*

Lemma 1.5.16. [55] *Let G be a group and Ω a set. Then:*

(i) For $g \in G$, $(\cdot)$ is the action of G on Ω if

$$\Phi_g : \Omega \to \Omega, \qquad x \mapsto g \cdot x$$

Then $\Phi_g \in S_n$ and the map

$$\rho : G \to S_\Omega, \qquad g \mapsto \Phi_g$$

is a homomorphism. So ρ is called the homomorphism associated to the action of G on Ω.

(ii) Let $\rho : G \to S_\Omega$ be homomorphism of groups. Define a map,

$$\rho : G \times \Omega \to \Omega, \qquad (g, x) \to \rho(g)(x)$$

Then $(\cdot)$ is an action of G on Ω.

Theorem 1.5.17. [27] *(Cayley's 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.*

Note 1.5.18. *The homomorphism ρ, defined in Lemma 1.5.16 is called the left regular representation of G.*

Theorem 1.5.19. [27] *(Generalized Cayley's Theorem) Let $H \leq G$ and let Ω be the set of all left cosets of H in G. Then there is a homomorphism $\rho : G \to S_\Omega$ such that*

$$ker(\rho) = \bigcap_{g \in G} gHg^{-1}.$$

Remark 1.5.20. *The homomorphism ρ is called the permutation representation of G on the left cosets of H in G. In particular,*

$$ker(\rho) = \bigcap_{g \in G} gHg^{-1},$$

is known as the core of H in G.

Corollary 1.5.21. [34] *If G is a simple group containing a proper subgroup H of finite index n, then G is isomorphic to subgroup of S_n.*

Theorem 1.5.22. [42] *Let G be a group and $H \leq G$. If $\Omega = \{gHg^{-1} | g \in G\}$ then there exist a homomorphism $\phi : G \to S_\Omega$ such that*

$$ker(\rho) = \bigcap_{g \in G} gN_G(H)g^{-1}.$$

Then ϕ is called the permutation representation of G on the conjugates of H.

1.5.1 Modular representation theory

In this subsection, we discuss modular representation theory by first stating the Maschke's Theorem.

Definition 1.5.23. [54] *Let G be a finite group of order n, and let $\mathbb{F}$ be a field whose characteristic is a prime p. We define a linear G-representation as a homomorphism $\rho : G \to GL(V)$, where V is a vector space over $\mathbb{F}$. The representation ρ is called modular if $p \mid |G|$. The action of G on the vector space V is defined by $gv = \rho(g)(v)$ for $g \in G$ and $v \in V$, making V a G-module.*

Theorem 1.5.24. *(Maschke's Theorem) If ϕ is a representation of G over a field $\mathbb{F}$ whose characteristic does not divide the order of G, and W is a G-invariant subspace of V, then there exists a G-invariant vector space complement of W in V.*

Remark 1.5.25. *V is semi simple, Maschke's Theorem fails if the characteristic of the field divides $|G|$. Therefore, in modular representation theory, we may encounter indecomposable modules that are not irreducible. This issue arises because a finite-dimensional $\mathbb{F}G$-module can be indecomposable without being irreducible. In contrast, for infinite-dimensional modules, the situation is more nuanced; while a completely reducible module is made up of irreducible components, a module that is irreducible cannot be decomposed further into nontrivial submodules.*

Definition 1.5.26. *Let $V \neq \emptyset$ be a permutation module. Then V is said to be simple or irreducible if it has only trivial submodules and is reducible otherwise. It is decomposable if it can be expressed as the direct sum of two non-trivial submodules and indecomposable otherwise.*

Definition 1.5.27. *Let G be a group and p any prime. If any element $g \in G$ can be expressed as $g = st$, where the order of s is not divisible by p, (making s p-regular), and the order of t is a power of p, (making t p-singular), then we say s is p-regular and t is p-singular.*

Definition 1.5.28. *A composition series for an $\mathbb{F}G$-module V is a series of submodules of the form $V = V_0 \supseteq V_1 \supseteq V_2 \supseteq \cdots \supseteq V_t = 0$ such that each $i \geq 1$, the factor V_{i-1}/V_i is irreducible. The integer t is called the length of the module V. If t is infinite, we say V has no composition series.*

Theorem 1.5.29 (Krull-Schmidt Theorem)**.** *If the module M can be expressed as:*

$$M = W_1 \oplus W_2 \oplus W_3 \oplus \cdots \oplus W_\lambda,$$

and also as,

$$M = U_1 \oplus U_2 \oplus U_3 \oplus \cdots \oplus U_n,$$

where W_i and U_j are indecomposable module, then $\lambda = n$ and there exists a bijection between the indices such that $W_i \cong U_{\sigma(i)}$ for some permutation σ of the indices.

Proof. See ([10], Theorem 3.22). □

Theorem 1.5.30. *If G is a p-group and $\mathbb{F}$ is a field of characteristic p, then the group algebra $\mathbb{F}G$ is indecomposable as an $\mathbb{F}G$-module. This means that $\mathbb{F}G$ cannot be expressed as a direct sum of two nontrivial $\mathbb{F}G$-submodules.*

Proof. See ([45], Lemma 3.3). □

Theorem 1.5.31. *If G is a finite group and $\mathbb{F}$ is a field whose characteristic does not divide $|G|$, then every finitely generated $\mathbb{F}G$-module is completely reducible. Equivalently, every $\mathbb{F}$-representation of G of finite degree completely reducible.*

Proof. See ([15], Chapter 18.1, Corollary 2). □

Theorem 1.5.32. *(Jordan-Holder Theorem for $\mathbb{F}G$-modules) If V is a finite dimensional $\mathbb{F}G$-module, then V possess a composition series, and the composition factors are independent of the choice of factor series.*

Proof. See ([8], Corollary 8.7).

□

Remark 1.5.33. *The consequence of the Jordan-Holder Theorem is that any two composition series factors M_i/M_{i+1} of one of the series are simply a permutation of the composition factors of the other.*

Theorem 1.5.34. [43] *The set of all irreducible characters of G is a linear independent over $\mathbb{C}$. Then we have:*

(1) **Orthogonality Relation**

(i) $\sum_{g\in G}(\chi_1(g))^2 = |G|$, *where χ_1 is the principal (or trivial) character.*

(ii) $\sum_{g\in G}(\chi_i(g))^2 = 0$ *if $i \neq 1$.*

(2) **Inner Product of Character**

(iii) $\sum_{i=1} h_i\chi_i(g) = \delta_{1i}|G|$, *where h_i are the degrees of the irreducible characters, and δ_{1i} is the Kronecker delta.*

Definition 1.5.35. *Given a group G acting on a finite set Ω, the character χ of the permutation representation is defined by the condition that for each $g \in G$, the character $\chi(g)$ is equal to the number of fixed points of g acting on Ω.*

Proposition 1.5.36. *Let G be a group and χ be a character of G. For each $\chi \in Irr(G)$, we have:*

(i) $\chi(1_G) = deg(\chi)$ *(the value of the character at the identity element is equal to its degree).*

(ii) If $\chi \in Irr(G)$, then $\overline{\chi} \in Irr(G)$, where $\overline{\chi}(g) = \overline{\chi(g)}$ for all $g \in G$(the complex conjugate of an irreducible character is also irreducible).

(iii) $\chi(g^{-1}) = \overline{\chi(g)}$ *for all* $g \in G$.
In particular, if $g^{-1} \in [g]$, *then* $\chi(g) \in \mathbb{R}$ *for all* χ.

Definition 1.5.37. [51] *Let* ρ *and* ϕ *be two class functions on* G. *Then the inner product of* ρ *and* ϕ *is defined as:*

$$< \rho, \phi >= \frac{1}{|G|} \sum_{g \in G} \rho(g)\overline{\phi(g)} = \frac{1}{|G|} \sum_{g \in G} \rho(g)\phi(g^{-1}).$$

Proposition 1.5.38. *There are four properties of inner product:*

(i) $< \rho, \phi >= \overline{< \phi, \rho >}$.

(ii) $< \rho, \rho > \geq 0$ *equality holds if and only if* $\rho = 0$.

(iii) $< x_1\rho_1 + x_2\rho_2, \phi >= x_1 < \rho_1, \phi > + x_2 < \rho_2, \phi >$.

(iv) $< \rho, x_1\phi_1 + x_2\phi_2 >= \overline{x_1} < \rho, \phi_1 > + \overline{x_2} < \rho, \phi_2 >$.

Theorem 1.5.39. *Let* G *act transitively on the set* Ω. *Then the following holds:*

1. χ_Ω *is an ordinary character of* G *of degree* $|\Omega|$.
2. $\chi_\Omega = \sum_{i=1}^{k} r_i\psi_i$, *where* r_i *are positive integers and* ψ_i *are irreducible characters of* G.
3. *For some* j, ψ_j *is the trivial character of* G *and* $r_j = 1$.
4. $Rank(G) = \sum_{i=1}^{k} r_i^2$.

Proof. See ([22], Chapter 5). □

Corollary 1.5.40. [22] *Let* ρ *and* ϕ *be (not necessarily irreducible) characters of* G. *Then* $< \rho, \phi >=< \phi, \rho >$ *is a non-negative integer. Moveover,* ϕ *is irreducible if and only if* $< \rho, \rho >= 1$.

Definition 1.5.41. [22] *Let* $H \leq G$ *and let* ρ *be a class function of* H. *Then* ρ^G *the induced class function on* G, *is given by:*

$$\rho(g) = \frac{1}{|H|} \sum_{x \in G} \rho^\circ(xgx^{-1}),$$

where ρ° is defined by:

$$\rho^\circ(h) = \begin{cases} \rho(h), & if \quad h \in H; \\ 0, & if \quad h \notin H. \end{cases}$$

Remark 1.5.42. *If ρ^G is a class function on G, then $\rho^G(1) = [G : H]\rho(1)$. Thus ρ^G is obtained on the set of left cosets given by T as:*

$$\rho^G(g) = \sum_{t \in T} \rho^\circ(tgt^{-1}).$$

Lemma 1.5.43. [22] *(Frobenius Reciprocity) If $H \leq G$ and φ is a class function on H that can be extended to a class function on G, then the relationship between the inner products is given by:*

$$< \varphi^G, \varphi >=< \varphi, \varphi_H >,$$

where φ^G is the induced class function on G and φ_H is the restriction of φ to H.

Corollary 1.5.44. [22] *Suppose $H \leq G$ and φ is a character of H. Then the induced character φ^G, which is defined from φ to G, is a character of G.*

1.5.2 Induced characters

In this subsection, we discuss the induced characters.

Definition 1.5.45. [38] *Let G be a finite group acting on a finite set Ω, and let $\alpha \in \Omega$. The stabilizer of α in G is denoted by G_α. The orbit of α under the action of G is denoted by Δ. Then we have the following relationship:*

$$[G : G_\alpha] = |\Delta|,$$

where Δ is the size of the orbit containing α.

Remark 1.5.46. *The action of G on Ω gives a permutation representation π with corresponding permutation character, denoted by χ_π or $\chi(G|\Omega)$.*

Lemma 1.5.47. [41]

(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) *If* $\chi(G|\Omega) = (I_{G_\alpha})^G$, *then the trivial character of* G_α *induced to* G.

(iii) *For all* $g \in G$, *we have* $\chi(G|\Omega)(g) = \chi(G|G_\alpha)(g)$, *which is equals the number of points in* Ω *fixed by* g.

Lemma 1.5.48. [41] *Let* H *be a subgroup of* G *and let* Ω *be the set of all conjugates of* H *in* G. *Then:*

(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*

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

where x_i*'s and* h_i*'s are representatives of conjugacy classes of* $N_G(H)$ *and* H *that fuse to* $[g] = C_g$ *in* G.

Remark 1.5.49.

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

Corollary 1.5.50. [41] *If* G *is a finite simple group and* M *is a maximal subgroup of* G, *then number* λ *of conjugates of* M *in* G *containing* g *is given by*

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

where $x_1, x_2, x_3, \cdots x_k$ *are representatives of conjugacy classes of* M *that fuse to* $[g] = C_g$ *in* G.

1.6 Binary linear codes

In this section, we construct linear codes invariant under the simple group $PSp_4(q)$ for some q prime power.

Definition 1.6.1. *Let C be a code of length n over field $\mathbb{F}_2$, then C is a linear code over $\mathbb{F}_2$ if for all c, $c' \in C$ and all for $\alpha \in \mathbb{F}_2$,*

1. *$c + c' \in C$;*
2. *$\alpha\, c \in C$.*

Theorem 1.6.2. *All linear codes must contain the all-zero codeword.*

Proof. Suppose $\alpha = 0$, so since $\alpha\, c \in C$,
Hence $0 \in C$.
Therefore, if presented with a code for which $0 \notin C$, then C cannot be linear. □

Definition 1.6.3. [46] *A **linear code** C of length n over $\mathbb{F}_2$ is a subspace of $V = \mathbb{F}_q^n$. We write $C = [n, k]_2$ where $dim(C) = k$.*
The repetition code $C = \{\underbrace{(x, \cdots, x)}_{n} | x \in \mathbb{F}_2\}$ is a linear code.

Definition 1.6.4. *A* **linearcode** *with length n over $\mathbb{F}_q$ is a vector subspace of $V = \mathbb{F}_q^n$.*

Definition 1.6.5. *A* **binarylinearcode** *C is a subspace of $\mathbb{F}_2^n$. We call it $[n, k]$-code where n is the length of a code and k is its dimension. Codewords are vectors of C.*

Theorem 1.6.6. [31] *[Theorem 2.21] Let C be a binary linear $[n, k]$-code over $\mathbb{F}_2$. Then:*

1. *For every $v \in V$, there exists a coset of C that contains v.*
2. *For every $v \in V$, we have $|C + v| = |C| = 2^k$.*
3. *For every $v, u \in V$, $v \in C + u$ implies that $C + v = C + u$.*
4. *For every $v, u \in V$, either $C + v = C + u$ or $(C + v) \cap (C + u) = \emptyset$.*
5. *There are 2^{n-k} different cosets for C.*
6. *For every $v, u \in V$, it hold that $v - u \in C$ if and only if v and u are in the same coset.*

Theorem 1.6.7. *If C is an $[n, k]$-code over $\mathbb{F}_2$. Then:*

1. *Every vector of V is in some coset of C.*

2. *Every coset contains exactly* 2^k *vectors.*

3. *Two cosets either disjoint or coincide (partial overlap is impossible).*

Proof. See ([20], pp. 57). □

Definition 1.6.8. *If* $\mathbb{F}_q$ *is a field,* C *is a vector subspace of* $\mathbb{F}_q^n$ *known as linear code, and* G *is a subgroup of linear automorphisms of* $\mathbb{F}_q^n$*, then* C *is said to be* G*-invariant if* $g(C) = C$ *for all* $g \in G$*.*

Theorem 1.6.9. *Suppose* G *is a finite group and* Ω *is a finite* G*-set. Then the* $\mathbb{F}_2G$*-submodules of* $\mathbb{F}\Omega$ *are precisely the* G*-invariant codes such that* G*-invariant subspaces of* $\mathbb{F}\Omega$*.*

Proof. Suppose G is a finite permutation group acting on a set Ω. Let $V = \mathbb{F}\Omega$ be the $\mathbb{F}$ vector space with basis the elements of Ω. Let $\rho : G \to GL(V)$ be a representation of G given by:

$$\rho(g)(x) = g(x) \quad \text{for all} \quad g \text{ in } G \quad \text{and} \quad x \text{ in } \Omega.$$

We can consider V as the $\mathbb{F}_2G$-module obtained from ρ. Let S be an $\mathbb{F}_2G$-submodule of the permutation module V. Then by Definition 1.6.8 we have:

$$\left(\sum_{g\in G} \alpha_g g\right) \cdot S \in \mathcal{S}, \quad \text{for all} \quad \sum_{g\in G} \alpha_g g \quad \text{in} \quad \mathbb{F}_2G \quad \text{and} \quad S \in \mathcal{S}.$$

In particular, $g \cdot S$ in $\mathcal{S}$ for all g in G and S in $\mathcal{S}$.

Thus, for all g in G and S in $\mathcal{S}$, we obtain $\rho(g)(S)$ in $\mathcal{S}$ or $g(s)$ in $\mathcal{S}$ and so $\mathcal{S}$ is G-Invariant. Conversely. If $\mathcal{S}$ is G-invariant, then for all g in G and S in $\mathcal{S}$, we have $\rho(g)(S)$ in $\mathcal{S}$. Therefore for scalars α_g in $\mathbb{F}_2$. we have:

$$\sum_{g\in G} \alpha_g \rho(g)(S) \text{ in } \mathcal{S}.$$

by linearity. This implies that:

$$\left(\sum_{g\in G} \alpha_g g\right) \cdot S \text{ in } \mathcal{S}.$$

□

Example 1.6.10. *Suppose x in V and $X = \{i_1, i_2, i_3, \cdots, i_k\} \subseteq \{1, 2, 3, \cdots, n\}$ are the non-zero coordinates of x. Then $x = (1010001) = e_1 + e_3 + e_7$ is represented as $X = \{1, 3, 7\}$.*

Definition 1.6.11. *The Hamming distance $d(u, v)$ between vectors u, v in C is the number of coordinates in which they differ.*

Lemma 1.6.12. *The Hamming distance between any vectors is a metric on $\mathbb{F}^n$, such that:*

1. *$d(v, w) = 0$ if $v = w$,*
2. *$d(v, w) = d(w, v)$, for all $v, w \in \mathbb{F}^n$,*
3. *$d(u, w) \leq d(u, v) + d(v, w)$, for all u, v, w in $\mathbb{F}^n$.*

Proof. See ([4], Proposition 2.1.1]). □

Definition 1.6.13. *Let $V = \mathbb{F}^n$ for any vector $v = (v_1, v_2, v_3, \ldots, v_n)$, let $S = \{i | v_i \neq 0\}$. Then the set S is called the support of v and the weight of v, denoted by $wt(v)$ is $|S|$. The minimum weight of a code C, denoted by $wt(C)$, is*

$$wt(C) = min\left\{wt(v) | v \in C, v \neq 0\right\},$$

such that the minimum of the weights of the non-zero codewords.

Lemma 1.6.14. *We have $d(u, v) = wt(u - v)$ for all u, v in $\mathbb{F}_2^n$.*

Proof. Let $u, v \in \mathbb{F}_2^n$. By definition, $d(u, v)$ is the number of places where u and v differ. Then the vector $u - v$ will have 1 precisely in the places where u and v differ and 0 in the places where they are the same. In other words, $d(u, v)$ is equal to the number of places where there is 1 in the vector $u - v$. But, the number of places with 1, by definition, is the weight of that vector. Hence, $d(u, v) = wt(u - v)$. □

Theorem 1.6.15. *In a linear code C that is a vector space over $\mathbb{F}_2$. If the dimension $dim(C) = k$, then the number of codewords in C is 2^k.*

Proof. Suppose $dim(C) = k$ and let $\{x_1, x_2, x_3, \ldots, x_k\}$ be a basis for C. Then $C = \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 + \cdots + \lambda_k x_k \in \mathbb{F}_2$. Since $|\mathbb{F}_2| = 2$, there are exactly 2 choices for each $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_k$. Each choice gives a different word and so C has exactly 2^k codewords. □

Definition 1.6.16. *For any code C, the minimum distance of the code, denoted $d(C)$, is defined by,*

$$d(C) = min\left\{d(u,v)|u,v \in C, u \neq v\right\}.$$

An $[n,k]$-code of minimum distance d is called an $[n,k,d]-$code. The values $[n,k,d]$ are called the parameters of the code.

Remark 1.6.17. *If the minimum distance of a code of length n is 0 or n, we consider the code trivial. If the minimum distance is 1, we call it a repetition code 1.6.3.*

Theorem 1.6.18. *Let C be an $[n,k,d]$ linear code. Then the minimum distance $d = d(C)$ is the minimum weight of C.*

Proof. In a linear code C over a field $\mathbb{F}$, the distance $d(v,w)$ between two codewords v and w can be expressed in terms of the weight of their difference. We have:

$$d(v,w) = wt(v-w),$$

where $wt(v)$ denotes the weight of the vector v, defined as the number of non-zero entries in v. Since C is a linear subspace, the difference $v-w$ is also in C for any $v,w \in C$. Therefore, the minimum distance $d(C)$ of the code C can be determined by finding the minimum weight of all non-zero codewords in C. □

Definition 1.6.19. *Suppose C is a linear code, and A_k is the number of codewords of weight k. Then the weight numerator of C is the polynomial $\sum_{k=0}^{n} A_k x^{n-k} y^k$, where x is the zero point and y is a non-zero coordinates of the code.*

Clearly the coefficient of A_k is the number of vectors with weight k. Therefore, the weight distribution classifies codewords according to the number of non-zero coordinates. A list of non-zero A_k is usually called the weight distribution of a code.

Definition 1.6.20. *Suppose C is a code in V, then $C^{\perp}$ is the dual code or orthogonal code of C, defined as:*

$$C^{\perp} = \left\{y \in \mathbb{F}_p^n | x \cdot y = 0 \ \ for\ all\ x \in C\right\}.$$

Lemma 1.6.21. *The $C^{\perp}$ is a linear code.*

Proof. See ([6]). □

Remark 1.6.22. *If $C = [n, k, d]$ then $C^{\perp} = [n, n-k, d']$ and d' is not necessarily related to d, which can be proven using Lemma 1.6.21 and the Rank-Nullity Theorem from Linear Algebra [23]. The minimum distance d' of $C^{\perp}$ is called the dual distance of C.*

Definition 1.6.23. *A code is called projective if any two of its coordinates are linearly independent such that it has a dual distance $d^{\perp} \geq 3$.*

Definition 1.6.24. *A binary code is even if the weight each of its codewords is divisible by 2.*

Definition 1.6.25. *A binary code is doubly even if the weight of each of its codewords are divisible by 4.*

Remark 1.6.26. *It can be seen that doubly even implies even.*

Definition 1.6.27. *A linear code is self-dual if $C = C^{\perp}$ and it is self-orthogonal if $C \subseteq C^{\perp}$.*

Lemma 1.6.28. *A binary self-orthogonal code C is even.*

Proof. Suppose, we have the $w = (a_1, a_2, a_3, \ldots, a_n)$ where $a_i \in \{0, 1\}$. If it is in the self-orthogonal code, then $w \cdot w = 0$ over the field of two elements. But $w \cdot w = a_1^2 + a_2^2 + a_3^2 + \cdots + a_n^2$ which equals the number of ones in w, that is the weight of w. So $w \cdot w = 0$ in $\mathbb{F}_2$ if and only if w has even weight. □

Definition 1.6.29. *Let $\mathbb{F}$ be a field and let C be a linear code over $\mathbb{F}$ then hull of C is the intersection of C and its dual code, denoted by $Hull(C) = C \cap C^{\perp}$.*

It is clear that $Hull(C)$ is also a linear code. It is easy to see that a linear code C is self-orthogonal if and only if the dimension of $Hull(C)$ is equal to the dimension of C such that $Hull(C) = C$, and it is self-dual if and only if $Hull(C) = C^{\perp}$.

Definition 1.6.30. *A linear code C is said to be linear complementary dual (LCD) if $Hull(C) = \{0\}$.*

Corollary 1.6.31. *A code is even if and only if it is contained in the dual of the repetition code.*

Proof. See ([13]). □

Definition 1.6.32. *Let C be a binary (n,k)-code. An automorphism of C is an element of S_n that sends codewords to codewords. The automorphism group of C is,*

$$Aut(C) = \{\pi \in S_n | c\pi \in C, \quad for\ all\ c \in C\}.$$

An automorphism group of a code C is the group of all permutations S_n of the coordinates that map codewords to codewords. The existence of an automorphism for C can provide a richer structure for the code and allows us to make some deeper results from algebra. This is particularly the case when C has a regular automorphism group $G \subseteq Aut(C)$, this means that G is transitive on X and thus $|G| = |X| = n$ the block length of C.

Definition 1.6.33. *Let C be an $[n,k,d]_q$ code, we have two matrices that determine the code.*

1. *A generator matrix of C, denoted by $\mathcal{G}$, is a $k \times n$ matrix over $\mathbb{F}_q$ whose rows forms a basis of C.*

2. *A parity check matrix of $C^{\perp}$, denoted by $\mathcal{H}$, is a $(n-k) \times n$ matrix over $\mathbb{F}_q$ whose rows forms a basis of $C^{\perp}$.*

Theorem 1.6.34. *Let $\mathcal{H}$ be a parity check matrix of linear code C. A linear code has minimum weight d if and only if any $d-1$ columns of $\mathcal{H}$, are linearly independent and there exists some d columns that are linearly dependent.*

Proof. Let C be a linear code. Then $wt(C) = d(C) = d$. So, there must exist some codewords in C with weight d. Suppose that the vector u is a codeword in C such that $wt(u) = d$. Since, $u \in C$ implies that $\mathcal{H}u^T = 0$ and u has d non-zero components, then there are some d columns of $\mathcal{H}$ that are linearly dependent. For the other side, suppose that there are $d-1$ linearly dependent columns in $\mathcal{H}$. Then there must exist a non-zero vector $v \in C$ such that $wt(v) = d-1$. This however contradicts the fact that the minimum weight of C is d. So, any $d-1$ columns of $\mathcal{H}$ are linearly independent. □

Definition 1.6.35. *Let $\mathcal{H}$ be a parity matrix of C. Then the permutation automorphism group of C is the stabilizer of C in the symmetric group S_n with respect to the action on the set of the columns of $\mathcal{H}$. We denote the permutation automorphism group of C by $PAut(C)$.*

Remark 1.6.36. *The permutation automorphism group of a code must be distinguished from the full automorphism group of a code, stabilizer of the action of* $\mathbb{F}_q^{n*} \rtimes S_n$ *sending every column of* $\mathcal{H}$ *to a scalar multiple of another column. Clearly* $Aut(C) = PAut(C)$ *in the binary case.*

Definition 1.6.37. *Two linear codes with the same length over a field* $\mathbb{F}_q$ *are equivalent and isomorphic if the following conditions are satisfied:*

1. *Two linear codes of the same length over the field* $\mathbb{F}_q$ *are said to be equivalent if one can be transformed into the other by a combination of:*
   (a) *Permuting the coordinates of the code.*
   (b) *Multiplying each coordinate by a non-zero scalar from the field* $\mathbb{F}_q$.
2. *Two linear codes are said to be isomorphic if there exists a bijective linear transformation between them that maps codewords of one code to codewords of the other, specifically through a permutation of coordinates. Isomorphism focuses on the structural similarity of the codes, without the additional flexibility of scalar multiplication.*
3. *In the case of binary linear codes, where* $q = 2$*, the notions of equivalence and isomorphism coincide. This is because the only non-zero scalar in* $\mathbb{F}_2$ *is* 1*, so multiplying by a non-zero scalar does not introduce any new transformations beyond those achieved by permuting coordinates.*

Theorem 1.6.38. [20] *(Singleton Bound) For any code* C *with minimum distance* d*, we have* $|C| \leq q^{n-d+1}$*. For a linear code,* $[n, k, d]$*-code, this means that* $q^k \leq q^{n-d+1}$*. This turn implies that,* $k \leq n - d + 1$ *or* $d \leq n - k + 1$*.*

Proof. If we consider a code with size $|C|$ and distance d, we know that every word differs in at least d positions. If we were to truncate the codewords by ignoring the last $d - 1$ positions, all the new codewords must be different. So, we still have $|C|$ codewords remaining, but now we are in dimension $n - (d - 1)$. We know that there is a total of $q^{(n-1)+d}$ codewords of this dimension, therefore we see that $|C| \leq q^{n-d+1}$. This proves the result along with the knowledge that when C is linear, $|C|$ is just the size of the k-dimensional subspace over $\mathbb{F}_q$, which is q^k. □

Theorem 1.6.39. [20] *[Theorem 2.16] (The sphere-packing or Hamming bound) A* $q-$*ary* $(n, k, 2t+1)$*-code satisfies,*

$$k\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t \leq q^n$$

$$M \leq q^n \left[\sum_{t=0}^{t} \binom{n}{t}(q-1)^t\right]^{-1}.$$

Proof. See ([20], pp 20). □

Chapter 2

Designs and codes

In this chapter, we explore designs and their corresponding codes that are invariant under finite simple groups, along with their fundamental properties. Additionally, we explain two methods, referred to as the Key-Moori Methods, for constructing these combinatorial structures. A reader is referred to [4] and [20], for notation.

2.1 Designs

Definition 2.1.1. [4] *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ and $\mathcal{F} = (\mathcal{Q}, \mathcal{C}, \mathcal{J})$ be two incident structures. Suppose ϕ is a bijection from $\mathcal{P} \cup \mathcal{B}$ to $\mathcal{Q} \cup \mathcal{C}$. Then if $\phi(\mathcal{P}) = \mathcal{Q}$ with $p \in \mathcal{P}$ incident with $B \in \mathcal{B}$ if and only if $\phi(p) \in \mathcal{Q}$ is incident with $\phi(B) \in \mathcal{C}$, then ϕ is an isomorphism from $\mathcal{D}$ to $\mathcal{F}$. If $\mathcal{D} = \mathcal{F}$, then ϕ is an automorphism.*

Definition 2.1.2. [4] *An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a $t-(v, k, \lambda)$ design if it satisfies the following conditions:*

1. *The number of points $|\mathcal{P}| = v$.*
2. *Each block $B \in \mathcal{B}$ is incident with k points.*
3. *Any t distinct points are incident with exactly λ blocks.*

Theorem 2.1.3. [42] *A t-design $\mathcal{D}$ is a s-design with $1 \leq s \leq t$ by replacing $t-(v, k, \lambda)$ by $s-(v, k, \lambda_s)$ where:*

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

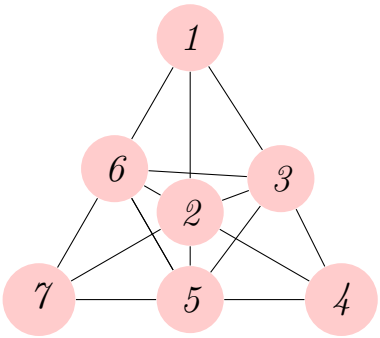
Definition 2.1.4. [4] *A Steiner system is a* $t-(v,k,1)$ *design for some integers* $1<k<v$, *for some* $t\geq 2$.

Definition 2.1.5. [40] *Two designs* $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$ *and* $\mathcal{D}'=(\mathcal{P}',\mathcal{B}',\mathcal{I}')$ *are isomorphic if there is a bijection* Φ *from* $\mathcal{P}$ *to* $\mathcal{P}'$ *so that* $(p,B)\in\mathcal{I}$, *if and only if* $(\Phi(p),\Phi(B))\in\mathcal{I}'$. *A bijection from a design* $\mathcal{D}$ *to itself is called an automorphism. The group of all automorphism of* $\mathcal{D}$ *is denoted by* $Aut(\mathcal{D})$.

Remark 2.1.6. *Two designs with the same parameters need not to be isomorphic.*

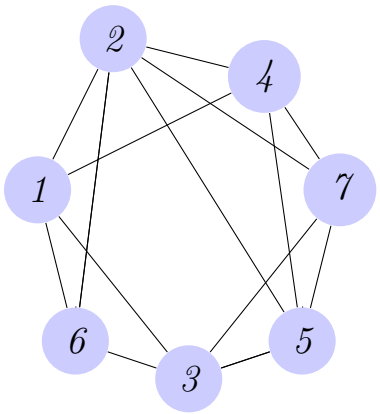
Example 2.1.7. *Fano plane as a* $1-(7,3,3)$ *design or a* $2-(7,3,1)$ *design.*

$$\mathcal{B}=\{\{4,5,7\},\{1,6,7\},\{1,2,5\},\{2,3,7\},\{1,3,4\},\{2,4,6\},\{3,5,6\}\}.$$



A $1-(7,3,3)$ *design not isomorphic to Fano plane.*

$$\mathcal{B}=\{\{1,2,6\},\{1,2,4\},\{2,4,7\},\{4,5,7\},\{3,5,7\},\{3,5,6\},\{1,3,6\}\}.$$



Definition 2.1.8. [40] *Let* $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$, *with* $|\mathcal{P}|=v$ *and* $|\mathcal{B}|=b$, *in which* $\mathcal{P}=\{p_1,p_2,\cdots,p_v\}$ *and* $\mathcal{B}=\{B_1,B_2,\cdots,B_b\}$. *Then an incidence matrix of* $\mathcal{D}$ *is a* $b\times v$ *matrix* $A=a_{ij}$ *of 0's and 1's such that:*

$$a_{ij} = \begin{cases} 1, & if \quad (p_j, B_i) \in \mathcal{I}; \\ 0, & if \quad (p_j, B_i) \notin \mathcal{I}. \end{cases}$$

Example 2.1.9. *Incidence matrix of a* $1-(7,3,3)$ *design.*

	$\{1,2,6\}$	$\{1,2,4\}$	$\{2,4,7\}$	$\{4,5,7\}$	$\{3,5,7\}$	$\{3,5,6\}$	$\{1,3,6\}$
1	1	1	0	0	0	0	1
2	1	1	1	0	0	0	0
3	0	0	0	0	1	1	1
4	0	1	1	1	0	0	0
5	0	0	0	1	1	1	0
6	1	0	0	0	0	1	1
7	0	0	1	1	1	0	0

Definition 2.1.10. [39] *The dual structure of* $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *is* $\mathcal{D}^t = (\mathcal{P}^t, \mathcal{B}^t, \mathcal{I}^t)$*, where* $\mathcal{P} = \mathcal{B}^t$*,* $\mathcal{B} = \mathcal{P}^t$ *and* $\mathcal{I}^t = \{(B,p) | (p,B) \in \mathcal{I}\}$*.*

Definition 2.1.11. [39] *Any design* $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *is said to be symmetric if it has same number of points and blocks. That is,* $|\mathcal{P}| = |\mathcal{B}|$*.*

Definition 2.1.12. [40] *The design* $\mathcal{D}$ *is self-dual if it is isomorphic to its dual. That is* $\mathcal{D} \cong \mathcal{D}^t$*.*

Definition 2.1.13. [4] *The complement structure of* $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *is* $\overline{\mathcal{D}} = (\overline{\mathcal{P}}, \overline{\mathcal{B}}, \overline{\mathcal{I}})$*, where* $\overline{\mathcal{P}} = \mathcal{P}$*,* $\overline{\mathcal{B}} = \mathcal{B}$ *and* $\overline{\mathcal{I}} = (\mathcal{P} \times \mathcal{B}) - \mathcal{I}$*.*

Theorem 2.1.14. [4] *If* $\mathcal{D}$ *is a* $t-(v,k,\lambda)$ *design with* $v-k \geq t$*, then the complement of* $\mathcal{D}$ *is a* t*-*$(v, v-k, \overline{\lambda})$ *design, where:*

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

Definition 2.1.15. [27] *An automorphism of a design* $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *is a permutation* Φ *of the point set* $\mathcal{P}$ *such that:*

1. *If* $B \in \mathcal{B}$ *then* $\Phi(B)$ *is also in* $\mathcal{B}$*.*
2. *For all points* $p \in \mathcal{P}$ *and blocks* $B \in \mathcal{B}$*, if* p *is incident with* B*, that is* $(p,B) \in \mathcal{I}$*, then* $(\Phi(p), \Phi(B)) \in \mathcal{I}$*.*

Lemma 2.1.16. [47] *If* $\mathcal{D}$ *is any* t*-design with* $t \geq 2$*. Then the group of automorphisms of the design acts faithfully on* $\mathcal{B}$*.*

Theorem 2.1.17. [34] *Let G be a t-transitive permutation group on a finite set Ω, with $t \geq 2$. If Δ is a subset of Ω, with $|\Delta| = k$, $|\Omega| = v$ and $1 < k < v - 1$. Then the set $\mathcal{B} = \{\Delta^g | g \in G\}$ is the set of blocks of a t-design $\mathcal{D}$, and G is a group of automorphisms acting transitively on $\mathcal{B}$.*

2.2 Key-Moori methods

In this section, we discuss how to construct designs using primitive permutation representation, conjugacy classes, maximal subgroups and fixed points of a group G. We first discuss Key-Moori Method 1 and 2. We will refer to Key-Moori Method 1 and 2, as Method 1 and Method 2.

2.2.1 Method 1

In Method 1, we use primitive permutation representation of $PSp_4(q)$ group to construct symmetric 1-designs. Let G be a finite group with maximal subgroup M, we define $\mathcal{A}_M = \{|M \cap M^g| : g \in G\}$. It is clear that $\mathcal{A}_M \neq \emptyset$, since $|M| \in \mathcal{A}_M$. These notations are used throughout this chapter. Our method to construct designs is based on the following results.

Lemma 2.2.1. [38] *Let G be a finite simple group with a maximal subgroup M with $\mathcal{M}$ is the set of all conjugates of M in G. Then G acts on $\mathcal{M}$ by conjugation. The point stabilizer of G is M, which implies that the action of G on $\mathcal{M}$ is primitive.*

Definition 2.2.2. [38] *Let G acts primitively on M, with the action of G on $\mathcal{M}$. Then the number of orbits of this action is called the rank of G, denoted by $rank(G)$.*

Lemma 2.2.3. *(Method 1)* [39] *Let G be a finite primitive permutation group acting on the set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α. If*

$$\mathcal{B} = \{\Delta^g : g \in G\}$$

, then $\mathcal{B}$ forms a $1-(n, |\Delta|, |\Delta|)$ design with n points, with G acting as an automorphism group on this structure, primitive on points and transitive on blocks (not necessary primitive) of the designs.

Lemma 2.2.4. *Let M be a maximal subgroup of G. If the action of G on the set of maximal subgroups of G is doubly transitive, then the designs constructed by Method* 1 *are trivial.*

Proof. Since G is doubly transitive the action of M on $\mathcal{M} \setminus \{M\}$ would be transitive. Therefore, $rank(G) = 2$ and the possible sizes of Δ are 1 and $n-1$. □

Theorem 2.2.5. *Let G be a finite simple group acting primitively on a set Ω and if $M = G_\alpha$, then $\{|M : M \cap M^g | g \in G\}$ is equal to orbit sizes of G_α acting on a set Ω.*

Lemma 2.2.6. [39] *Let G be a finite simple group acting on the set of the conjugates of maximal subgroup M by conjugation. Then the size of orbits of point stabilizer of G are as elements of the set,*

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

Every design constructed from Method 1 *is given as* $1 - \left(|G : M|, \frac{|M|}{n}, \frac{|M|}{n}\right)$ *for some* $n \in \mathcal{A}_M$.

Theorem 2.2.7. [39] *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 point-stabilizer.*

2.2.2 Method 2

In Method 2, we discuss how to obtain the parameters of some possible designs from the some conjugacy classes and maximal subgroups of projective symplectic group $PSp_4(q)$. Let χ_M be the permutation character afforded by the actions of G on the set of conjugates of M inside G. From [36], χ_M will vanish on the set of all elements of G not conjugate with any element of M. We can see that our designs are not necessarily symmetric 1-design for this method.

Definition 2.2.8. [41] *Let G be a finite simple group, M a maximal subgroup of G, nX a conjugacy class of elements of order n in G containing g. Then $[g] = nX$ and $|nX| = [G : C_G(g)] = |g^G|$, which is the size of the orbit of g under conjugation by G.*

Definition 2.2.9. [41] *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, is such that if $g \in G$ is not conjugate to any element in M, then $\chi_M(g) = 0$.*

Theorem 2.2.10. *(Method 2)[41] Let G be a finite simple group, M a maximal subgroup of G, and x^G a conjugacy class of elements of order n in G such that $M \cap x^G \neq \emptyset$. Let $\mathcal{B} = \{(M \cap x^G)^y | y \in G\}$ and $|\mathcal{P}| = |x^G|$. Then we have a $1-\big(|x^G|, |M \cap x^G|, \chi_M(g)\big)$ design $\mathcal{D}$, where $g \in x^G$.*

Note 2.2.11. *The group G acts as an automorphism group on $\mathcal{D}$, primitive on blocks and transitive (not necessarily primitive) on points of $\mathcal{D}$.*

Lemma 2.2.12. *Let $\mathcal{D}$ be $1-(v,k,\lambda)$ design constructed by Method 2, then:*

$$k = \frac{|M|\left(\chi_M(g) \times |x^G|\right)}{|G|}.$$

Proof. According to [30], $kb = \lambda v$. Then we have:

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

□

$\widetilde{\mathcal{D}}$, the complement of $\mathcal{D}$, is a $1-\left(v,k,\widetilde{\lambda}\right)$ design, where $\widetilde{\lambda} = \lambda \times \frac{vk}{k}$.

Remark 2.2.13. *[34] If $\lambda = 1$, then $\mathcal{D}$ is a $1-\big(|x^G|,k,1\big)$ design. Since, x^G is the disjoint union of b blocks each of size k, we have $Aut(\mathcal{D}) = S_k \wr S_b = S_k{:}S_b$. For all p, we have $C = C_p(\mathcal{D}) = \big[|x^G|,b,k\big]_p$, with $Aut(C) = Aut(\mathcal{D})$.*

Remark 2.2.14. *The design $\mathcal{D}$ constructed by Method 2 is symmetric 1-design if and only if $b = |C_G(g)|$.*

2.2.3 Method 3

In Method 3, we obtain all possible parameters of designs from the fixed points of each conjugacy class of a group G to construct a 1-design. From [49], we observe

a relationship between Method 2 and Method 3. Therefore, we use this connection between the two methods to find 1-designs under Method 3, which are not necessarily symmetric.

Definition 2.2.15. *Let G be finite group acting on a finite set Ω and nX is a conjugacy class of elements of order $n \neq 1$ in G and with $g \in nX$. Thus $C_g = [g] = nX = x^G$ and $|x^G| = [x^G{:}C_G(g)]$. 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 $\chi_\Omega = \chi_M = \chi(G|M)$.*

Theorem 2.2.16. [41] *Let G be a finite group acting transitively on a finite set Ω, where $v = |\Omega| > 1$. Let x^G and $B = Fix_{\Omega(g)}$ 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 $S = \{h \in x^G{:}Fix_{\Omega(h)} = B\}$ with $|S| = s$, then*

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

(ii) the group G acts as an automorphism group on $\mathcal{D}$, transitive on both points and blocks. In particular, if M is a maximal subgroup of G and Ω is the set of all conjugates of $M \in G$, then G is primitive on points and transitive (not necessarily primitive) on blocks of $\mathcal{D}$.

Proposition 2.2.17. [41] *If $nX = x^G = [g]$, $B = Fix_{\Omega(g)}$ and $S = \{h \in x^G{:}Fix_{\Omega(h)} = B\}$ with $|S| = s$. Then*

(i) $S = x^G \cap G_B$, where G_B is the point-wise stabilizer of $B \in G$;

(ii) $b = [G{:}G_B]$ and $|G_B| = |G| \times s/|x^G|$;

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

For remark 2.2.18 and remark 2.2.19 the reader may refer to [41].

Remark 2.2.18. *(i) $G > G_B \geq N_G(< g >) \geq C_G(g)$. If $G = G_B$, then $\mathcal{B} = \{B\}$ implies that $b = 1$ and $k = |B| = v$. That is g fixes all elements of Ω and $g = 1_G$, a contradiction, since in our construction we assume g is a non-identity element. Also if $y \in N_G(< g >)$, then $B^y = Fix_{\Omega(g^y)} = Fix_{\Omega(g^m)} \supseteq Fix_{\Omega(g)} = B$, for some integer m, this implies that $B^y = B$ and $y \in C_B$.*

(ii) $s = 1$ *if and only if* $C_B = C_G(g)$.

(iii) If $C_G(g)$ *is maximal in* G, *then* $G_B = C_G(g)$ *and hence,* $s = 1$. *But the converse is not true, that is there are cases where* $s = 1$, *that is,* $G_B = C_G(g)$ *and* G_B *is not maximal in* G. *For example when* $G = A_9$ *acts on* 2*-sets and* $nX = 2A$, *for* $g \in 2A$ *of cycle-type* $1^5 2^2$, *we have* $C_G(g) = G_B = S_5 \times 2^2$ *but* G_B *is not a maximal subgroup of* A_9. *In fact* G_B *sits inside the maximal subgroup* $(A_5 \times A_4)$:2 *with index* 3 *in* A_9.

Remark 2.2.19. *(i) From our construction*

$$G \leq Aut(\mathcal{D}) \leq Aut(C) \leq S_\Omega$$

but in general G *may not sit inside* $Aut(\mathcal{D})$.

(ii) If $\lambda = 1$, *then* $Aut(\mathcal{D})$ *is a* $1-(v,k,1)$ *design. Since* Ω *is the disjoint union of* b *blocks each of size* k *and we have* $Aut(\mathcal{D}) = S_k \wr S_b = (S_k)^b{:}S_b$. *In this case for all* p, *we have* $C = C_p(\mathcal{D}) = [v,b,k]_p$, *with* $Aut(C) = Aut(\mathcal{D})$.

(iii) In the method 3, *when* Ω *is the set of all conjugates of a maximal subgroup* M *of* G, *we have* $\lambda = 1$ *if and only if* $G_B = M$ *and* $k = 1$. *In this case, we have* $\mathcal{D}$ *as a* $1-(v,1,1)$ *design with corresponding* $Aut(C) = Aut(\mathcal{D}) = [v,v,1]_p$, *the full space* $\mathbb{F}_p^v$, *with* $Aut(C) = Aut(\mathcal{D}) = S_v$, $\forall p$.

(iv) The design $\mathcal{D}$ *constructed by Method* 3 *are not symmetric in general. In fact,* $\mathcal{D}$ *is symmetric if and only if*

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

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* $[G : M] = [G : G_B] \Leftrightarrow |M| = |G_B|$.

2.3 Constructions of combinatorial structures

In this section, we discuss the methods used in this thesis to construct designs and codes. For these methods we use MAGMA [7] to develop algorithms used in our constructions.

Given a representation of group elements of a group G by permutations one can work modulo q and obtain a representation of G on a vector space V over $\mathbb{F}_q$. The invariant subspaces are then all the binary codes C for which G is a subgroup of $Aut(C)$.

2.3.1 Codes from maximal submodules

In this subsection, we provide a comprehensive overview of the focus and methods of the chapter regarding G-invariant designs and codes, as follows:

1. Focus on G-Invariant Designs and Codes: We are investigating codes that remain invariant under the action of a group G, particularly using primitive representations and permutation modules.

2. Permutation Modules and Submodules: By considering the permutation modules from the groups action on cosets of its maximal subgroups, you can identify corresponding $\mathbb{F}\Omega$-submodules. This approach leads to the construction of explicit bases for the invariant codes.

3. Connection to Linear Codes:

   The G-invariant submodules are viewed as linear codes, allowing us to analyze their properties, including weight distributions.

4. Use of MAGMA: We utilize MAGMA for computational purposes to construct the associated permutation module over $\mathbb{F}_2$, facilitating the exploration of maximal submodules and their properties.

5. Action of a Group on Cosets:

   The discussion about the action of G on cosets, particularly the structure of G/H, is crucial for establishing the transitive and primitive action necessary for our results.

6. Focusing on Binary and Ternary Codes:

   We restriction to the fields $\mathbb{F}_2$ and $\mathbb{F}_3$ is relevant and aligns well with the typical applications in coding theory.

2.3.2 Construction of G-invariant codes

In this subsection, the construction presented is based on Theorem 1.6.9, Theorem 2.3.1, and Theorem 2.3.2.

Theorem 2.3.1. *Assume (G, X) is a primitive permutation group and $\mathbb{F}$ a field such that $Ext(G/G', \mathbb{F}^*) = 0$. Let E be a stem cover of G and E_0 the inverse in E of the stabilizer of G induced up to E all $1-$dimensional $\mathbb{F}E_0-$module. Then the submodules of the resulting $\mathbb{F}E-$modules provide for a complete list of codes over $\mathbb{F}$ admitting (G, X) as a permutation group.*

Proof. See ([13], Theorem 1). □

Theorem 2.3.2. *Let G be a finite simple group with a maximal subgroup M. Let P be the permutation $\mathbb{F}_n$-module corresponding to the primitive action of G on M, where $\mathbb{F}_n$ is a finite field. Also assume that the Schur multiplier of G is trivial and $(|M/M'|, |\mathbb{F}_n^*|) = 1$, for M' a derived group of M. Then the set of linear codes of length m over $GV(q)$ equals the set of all submodules of P.*

Proposition 2.3.3. *Let X be G-set and P be a primitive permutation module over a finite field $\mathbb{F}$ with respect to the action of G on X. Then P contains submodules S_1 and S_2 of degree 1 and $|X| - 1$, respectively.*

Proof. See ([13]). □

Definition 2.3.4. *Given a permutation module acting on a set Ω, and $\rho : G \to GF(V)$ where $\rho(g)v = g.v$ for g in G and v in V. We can find all codes with a group G acting as an automorphism group as follows:*

1. *Let $\mathbb{F}\Omega$ be a permutation module.*
2. *Use MAGMA to find all $\mathbb{F}\Omega$-submodules.*
3. *By Theorem 1.6.9 and Theorem 2.3.2 these submodules are G-invariant codes.*

As a result, we can locate every submodule of the permutation module thanks to the construction. To achieve this, we break down the permutation module into smaller components, which serve as the building blocks for assembling a lattice of submodules. After describing these codes, we address the issue of the code's classification. Theorem

of Maschke (see Theorem 1.5.24) provides a framework for the decomposition over a field whose characteristic is 0 or is relatively prime to the order of the group. In this case, the permutation module is fully reducible and can be expressed as a direct sum of irreducible modules.
In situations where a prime p divides the order of the group ($p \mid |G|$), we rely on the Krull-Schmidt theorem (see Theorem 1.5.29), which states that any module can be expressed as a direct sum of indecomposable modules.

Lemma 2.3.5. *Let C be a code of length n over a finite field $\mathbb{F}_q$, and $C^\perp$ the dual of code C. The all one codeword 1 lies in C if and only if q divides the sum of all coordinates of each $w \in C^\perp$. In particular if $q = 2$, then $1 \in C$ if and only if the length is even.*

Proof. If 1 in C, then for all w in $C^\perp$ we have $\langle w, 1\rangle = 0$. Since $\langle w, 1\rangle$ is the sum of all coordinates of w, we get $q|\langle w, 1\rangle$. This completes the proof. □

Chapter 3

Structure of symplectic groups

In this chapter, we study structures such as conjugacy classes, maximal subgroups, and the character table of the projective symplectic groups. We follow the notation from ATLAS [11] and Wilson [55].

3.1 Polarity forms

There are a number of useful inner products on real and complex vector spaces. These inner products give rise to various bilinear, sesquilinear and quadratic forms.

Definition 3.1.1. *An element T in $GL_n(q)$ is called a transvection if T satisfies, rank$(T_n - I_n) = 1$ and $(T_n - I_n)^2 = 0$.*

Definition 3.1.2. *The collineation of projective space induced by a transvection is called an elation. In particular, the axes of the transvection is the hyperplane $ker(T - I_n)$, this subspace is fixed element-wise by T. Dually, the center of T is the image of $(T - I_n)$.*

Definition 3.1.3. [55] *There are three types of polarity forms namely:*

(i) skew-symmetric bilinear;

(ii) conjugate-symmetric sesquilinear;

(iii) symmetric bilinear.

Remark 3.1.4. *These polarity forms have similar behaviour with vector space over a finite field, the only difference is the forms classification.*

In characteristic "0", the three types of polarity forms are generalised as an inner products.

Definition 3.1.5. [55] *There are two corresponding generalised norms derived from three types of polarity forms:*

1. *Hermitian forms (derived from* 3.1.3, *(ii)).*
2. *Quadratic forms (derived from* 3.1.3, *(iii)).*

Definition 3.1.6. [55] *A bilinear form on a vector space V over a field $\mathbb{F}_q$ of dimension n is a map $f : V \times V \to \mathbb{F}_q$ such that satisfies some axioms, for all $v, u, w \in V$ and $\lambda \in \mathbb{F}_q$:*

(i) $f(\lambda v + u, w) = \lambda f(v, w) + f(u, w)$;

(ii) $f(v, \lambda u + w) = f(v, w) + \lambda f(v, u)$.

Definition 3.1.7. [55] *A bilinear form f on a vector space V over a field $\mathbb{F}_q$ is said to be:*

(i) Symmetric if $f(v, u) = f(u, v)$ for all $v, u \in V$.

(ii) Skew-symmetric or anti-symmetric if $f(v, u) = -f(u, v)$ for all $v, u \in V$.

(iii) Alternating if $f(v, v) = 0$ for all $v \in V$.

Proposition 3.1.8. [55] *If characteristic of $\mathbb{F}_q \neq 2$, then an alternating bilinear form is a skew-symmetric form.*

Definition 3.1.9. [55] *A quadratic form is a map $Q : V \to \mathbb{F}_q$ satisfying, for all $v, u \in V$ and $\lambda \in \mathbb{F}_q$:*

$$Q(\lambda v + u) = \lambda^2 Q(v) + \lambda f(v, u) + Q(u),$$

where f is a symmetric bilinear form.

Definition 3.1.10. [55] *A conjugate-symmetric sesquilinear over a vector space V, defined over $\mathbb{F}_{q^2}$ is a map $f : V \times V \to \mathbb{F}_{q^2}$ satisfying, for all $v, u, w \in V$ and $\lambda \in \mathbb{F}_q$:*

(i) $f(\lambda v + u, w) = \lambda f(v, w) + f(u, w)$;

(ii) $f(v, w) = \overline{f(w, v)}$.

Remark 3.1.11. *We have* $f(v, \lambda u + w) = \overline{\lambda} f(v, u) + f(v, w)$.

Definition 3.1.12. [55] *The form* H *defined by* $H(v) = f(v, v)$ *is called Hermitian form, satisfying:*

$$H(\lambda v + u) = \lambda\overline{\lambda} H(v) + \lambda f(v, u) + \overline{\lambda} f(u, v) + H(u).$$

Definition 3.1.13. [55] *A non-zero vector* v *in* V *is called isotropic if it satisfies* $f(v, v) = 0$, *indicating that it is perpendicular to itself.*

Lemma 3.1.14. [55] *If* $f : V \times V \to \mathbb{F}_q$ *is a bilinear form and with* $W \subseteq V$, *then the restriction of* f *to* W *is defined as* $f|_W : W \times W \to \mathbb{F}_q$. *The radical of this restricted bilinear form is given by* $W \cap W^{\perp}$, *where* $W^{\perp}$ *is the orthogonal complement of* W *in* V.

Remark 3.1.15. *If* $f|_W = 0$, *then* W *is said to be totally isotropic.*

3.2 Projective symplectic groups

In this section, we discuss the projective symplectic groups, which are the groups that preserve reflexive sesquilinear forms or quadratic forms. They are associated with non-degeneration alternating bilinear forms.

3.2.1 The Pfaffin

The determinant of a skew-symmetric matrix is a square. This is visible in some small cases, observe:

$$det(A) = \begin{pmatrix} 0 & a_{12} \\ -a_{12} & 0 \end{pmatrix} = a_{12}^2$$

$$det(B) = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & a_{23} & a_{24} \\ -a_{13} & -a_{23} & 0 & a_{34} \\ -a_{14} & -a_{24} & -a_{34} & 0 \end{pmatrix} = (a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23})^2.$$

Theorem 3.2.1. [24] *Let A be a skew-symmetric matrix. Then:*

(1) the determinate of a skew-symmetric matrix of odd size is zero;

(2) there is a unique polynomial $Pf(A)$ in the indeterminate a_{ij} for some $1 \leq i, j \leq 2m$, having the properties:

(2.1) if A is a skew-symmetric $2m \times 2m$ matrix with (i, j) entry a_{ij} for $1 \leq i < j \leq 2m$;

(2.2) $Pf(A)$ contains the term $a_{1,2}a_{3,4} \cdots a_{2m-1,2m}a_{2m+1,2m+2}$.

Theorem 3.2.2. [24] *If A is a skew-symmetric matrix and B any invertible matric, then:*

$$Pf(BAB^T) = det(B)Pf(A).$$

Lemma 3.2.3. [24] *For $m \geq 1$, the group $PSp_{2m}(\mathbb{F})$ acts primitively on the points of $PG_{2m-1}(\mathbb{F})$.*

Remark 3.2.4. *The number of points in the projective space $PG_{2m-1}(q)$ is given by $\frac{q^{2m}-1}{q-1}$.*

3.3 Properties of projective symplectic groups

A split extension (a semidirect product) $A : B$ is a group G with normal subgroup A and a subgroup B such that $G = AB$ and $A \cap B = 1$. A non-split extension $A \cdot B$ is a group G with a normal subgroup A and $G \cong B$, but with no subgroup B satisfying $G = AB$ and $A \cap B = 1$. A group $G = A \circ B$ is a central product of its subgroups A and B. If $G = AB$ and $[A, B]$, then the commutator of $A = B = \{1\}$ in this case A and B are normal subgroups of G and $A \cap B = Z(G)$. If $A \cap B = \{1\}$, then $G = A \circ B = AB$, see ([55]).

The symplectic group $Sp_{2m}(q)$ is the isometry group of a non-singular alternating bilinear form f on $V \cong \mathbb{F}_q^{2m}$, that is, the subgroup of General linear group $GL_{2m}(q)$. Consisting of those elements $g \in G$ such that $f(u^g, v^g) = f(u, v)$ for all u, v in V [55]. The order of $Sp_{2m}(q)$ is given by:

$$|Sp_{2m}(q)| = \prod_{i=1}^{m}(q^{2i} - 1)q^{2i-1} = q^{m^2}\prod_{i=1}^{m}(q^{2i} - 1).$$

Observe that $f(\alpha u, \alpha v) = \alpha^2 f(u,v)$, which equals $f(u,v)$ if and only if $\alpha = \pm 1$. The determinate of elements in the symplectic group $Sp_{2m}(q)$ is 1. The projective symplectic group $PSp_{2m}(q)$ is the quotient group of $Sp_{2m}(q)$ by its center. It is the inner automorphism group given by the order:

$$|PSp_{2m}(q)| = \frac{\prod_{i=1}^{m}(q^{2i}-1)q^{2i-1}}{gcd(2,q-1)} = \frac{q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)}{gcd(2,q-1)}.$$

Rank-3 symplectic groups

Consider group G acting on the set Ω where $|G| = |\Omega| = n$.

Definition 3.3.1. *A block design (n,k,λ) is an incidence structure consisting of a set together with a family of subsets known as blocks, chosen such that frequency of the elements satisfies certain conditions making the collection of blocks exhibit symmetry.*

Lemma 3.3.2. [19] *A block design B is a symmetric balanced incomplete block design (BIBD) if it satisfies the following conditions related to its parameters:*

1. *n: the number of points,*
2. *k: the number of points in each block,*
3. *λ: the number of blocks in which each pair of points appears.*

For a symmetric BIBD, the number of blocks b is given by

$$b = \frac{n(n-1)}{k(k-1)}$$

and each point appears in r blocks, where

$$r = \frac{\lambda(n-1)}{k-1}.$$

Additionally, in a symmetric BIBD, $n = b$ and each block contains the same number of points k. This means that the incidence structure exhibits a high degree of symmetry.

Remark 3.3.3. *If B is symmetric with the parameters $(n, k+1, \mu)$. That is, B has n points and n blocks, $k+1$ points (or blocks) are incident with each block (or point), and any two distinct points (or blocks) are incident with exactly μ blocks (or points). The condition $n \neq k+2$ is equivalent to the condition $0 < \mu < k+1 < n-1$.*

Note 3.3.4. *The projective symplectic groups associated with symmetric design B are $PSp_{2m}(q)$, where m is an integer and q is an odd prime power. Moreover, for $m = 2$, this corresponds to $PSp_4(q)$.*

Lemma 3.3.5. [19]

1. *If B is symmetric, then G is primitive and has even order.*
2. *If $k + 1 - \mu = e^2$, then e^2 is a square*
3. *If n is even, e but not $2e$ divides $n - (k + 1)$.*
4. *If n is odd, $2e$ divides $n - (k + 1)$.*

Lemma 3.3.6. [19] *If B is a projective space of dimension 3, then the conditions are:*

1. *$\mu = \lambda + 2$,*
2. *$n \neq k + 2$*
3. *A hyperbolic line contains μ points, where the coordinating field is $\mathbb{F}_q$, $q = \mu - 1$.*

Corollary 3.3.7. *The projective symplectic group $PSp_4(q)$ has three orbits on the ordered pairs of points including diagonal orbit, which is give by*

$$\nabla = \{(t, t) : t \in PG(3, q)\}.$$

Note 3.3.8. *The group projective symplectic group $PSp_4(q)$ is a rank-3 permutation group on the projective plane $PG(3, q)$.*

3.4 Conjugacy classes and character table

In this section, we are following the notations in [50] and [51]. Firstly, we give conjugacy classes of $Sp_4(q)$, and use them to obtain conjugacy classes of $PSp_4(q)$ which are split into two parts; $q = 4k + 1$ and $q = 4k + 3$ for some integer k. Thereafter, character table for $PSp_4(q)$ is then constructed.
If $q = p^n$ is odd (odd prime power) and $PSp_4(q) \times C_{Sp_4(q)}(PSp_4(q)) \lneq Sp_4(q)$. Then $Sp_4(q)$ induces on $PSp_4(q)$ some outer automorphism α. With $|Out(PSp_4(q))| = 2n$, every element of $Out(PSp_4(q))$ can be written as the composition of a diagonal

matrix and field automorphism. If the automorphisms are represented by matrices each with a basis, then the diagonal matrices automorphisms are induced by conjugation of diagonal matrices. If $q = p^n$, $GF(\mathbb{F}_q/\mathbb{F}_p) =< \phi >$, where $\phi : \mathbb{F}_q \to \mathbb{F}_p$ is given by $\phi(x) = x^p$ for all $x \in \mathbb{F}_q$. The field automorphisms are induced by $\phi \in GF(\mathbb{F}_q/\mathbb{F}_p)$ for $1 \leq k \leq n-1$ by mapping $A = (a_{ij})$ to $A^{\phi^k} = (a_{ij})^{\phi^k} = (a_{ij}^{p^k})$. Since $\mathbb{F}_{q^4}^{\times} =< k >$ and $\xi = k^{q^2-1}$, $\theta = k^{q^2+1}$, $\eta = k^{q-1}$ and $\gamma = k^{q+1}$. Then by [51], $|\gamma| = q-1$ and $|\eta| = q+1$. The symplectic group $Sp_4(q)$ is the set of all 4×4 matrices X which satisfies $XJX^T = J$, where:

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

The center of the symplectic group is $Z(Sp_4(q)) = \{I, -I\}$, where I is the identity matrix. Additionally, the quotient group $Sp_4(q)/Z(Sp_4(q))$ is the projective symplectic group $PSp_4(q)$.

3.4.1 Conjugacy classes of $Sp_4(q)$

Let k be a generator of the multiplicative group of $GF(q^4)$ and let $\xi = k^{q^2-1}$, $\theta = k^{q^2+1}$, $\eta = k^{q-1}$ and $\gamma = k^{q+1}$. Choose, a fixed monomorphism from the multiplicative group of the $GF(q^4)$ into the multiplicative group of the complex numbers. Let $\tilde{\xi}$, $\tilde{\theta}$, $\tilde{\eta}$ and $\tilde{\gamma}$ be the image of ξ, θ, η and γ under this monomorphism.

Let $R_1 = \frac{q^2-1}{4}$ be the set with distinct positive integers i, such that all of the scalars ξ^i, ξ^{-i}, ξ^{qi} and ξ^{-qi} are distinct. Let $R_2 = \frac{(q-1)^2}{4}$ be the set of distinct positive integers i, such that all of the scalars θ^i, θ^{-i}, θ^{qi} and θ^{-qi} are distinct. Assume $T_1 = \{1, 2, \cdots, \frac{q-3}{2}\}$, $T_2 = \{1, 2, \cdots, \frac{q-1}{2}\}$, $\alpha_j = \tilde{\gamma}^j + \tilde{\gamma}^{-j}$, $\beta_j = \tilde{\eta}^j + \tilde{\eta}^{-j}$, $\tilde{\varepsilon} = -s(s+\sqrt{sq})$ and $\tilde{\varepsilon}' = -s(s-\sqrt{sq})$ where $s = (-1)^{\frac{q-1}{2}}$.

The following conjugacy class table for $Sp_4(q)$, first constructed by Srinivasa, will be used to construct the conjugacy class table for $PSp_4(q)$.

Table 3.1: Conjugacy classes of $Sp_4(q)$

Conjugacy class Class representative	No. of classes	Order of centralizer	$[G : C_G(g)]$ $= \lvert nX \rvert$
$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $A_1' = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	$q^4(q^4-1)(q^2-1)$	1
$A_{21} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $A_{21}' = \begin{bmatrix} -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	$q^4(q^2-1)$	q^4-1
$A_{22} = \begin{bmatrix} 1 & \gamma & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $A_{22}' = \begin{bmatrix} -1 & -\gamma & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	$q^3(q-1)$	$q(q^4-1)(q+1)$
$A_{31} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $A_{31}' = \begin{bmatrix} -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	$q^3(q+1)$	$q(q^4-1)(q-1)$
$A_{32} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -\gamma \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $A_{32}' = \begin{bmatrix} -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & \gamma \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	q^2	$q^2(q^4-1)(q^2-1)$
$A_{41} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $A_{41}' = \begin{bmatrix} -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	q^2	$q^2(q^4-1)(q^2-1)$
$A_{42} = \begin{bmatrix} 1 & \gamma & 0 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $A_{42}' = \begin{bmatrix} -1 & -\gamma & 0 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 0 & -1 & \gamma \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	q^2	$q^2(q^4-1)(q^2-1)$

Table 3.1 continued:

Conjugacy class Class representative	No. of classes	Order of centralizer	$[G : C_G(g)]$ $= \lvert nX \rvert$
$B_1(i) = \begin{bmatrix} \zeta^i & 0 & 0 & 0 \\ 0 & \zeta^{-i} & 0 & 0 \\ 0 & 0 & \zeta^{qi} & 0 \\ 0 & 0 & 0 & \zeta^{-qi} \end{bmatrix}$	$\frac{q^2-1}{4}$ $i \in R_1$	q^2+1	$q^4(q^2-1)^2$
$B_2(i) = \begin{bmatrix} \theta^i & 0 & 0 & 0 \\ 0 & \theta^{-i} & 0 & 0 \\ 0 & 0 & \theta^{qi} & 0 \\ 0 & 0 & 0 & \theta^{-qi} \end{bmatrix}$	$\frac{(q-1)^2}{2}$ $i \in R_2$	q^2-1	$q^4(q^4-1)$
$B_3(i,j) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & \gamma^j & 0 \\ 0 & 0 & 0 & \gamma^{-j} \end{bmatrix}$	$\frac{(q-3)(q-5)}{8}$ $i,j \in T_1,\ i \neq j$	$(q-1)^2$	$q^4(q^2+1)(q+1)^2$
$B_4(i,j) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & \eta^j & 0 \\ 0 & 0 & 0 & \eta^{-j} \end{bmatrix}$	$\frac{(q-1)(q-3)}{8}$ $i,j \in T_2,\ i \neq j$	$(q+1)^2$	$q^4(q^2+1)(q-1)^2$
$B_5(i,j) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & \gamma^j & 0 \\ 0 & 0 & 0 & \gamma^{-j} \end{bmatrix}$	$\frac{(q-1)(q-3)}{4}$ $i \in T_2,\ J \in T_1$	q^2-1	$q^4(q^4-1)$
$B_6(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & \eta^i & 0 \\ 0 & 0 & 0 & \eta^{-i} \end{bmatrix}$	$\frac{(q-1)}{2}$ $i \in T_2$	$q(q+1)(q^2-1)$	$q^3(q^2+1)(q-1)$
$B_7(i) = \begin{bmatrix} \eta^i & 0 & 1 & 0 \\ 0 & \eta^{-i} & 0 & 1 \\ 0 & 0 & \eta^i & 0 \\ 0 & 0 & 0 & \eta^{-i} \end{bmatrix}$	$\frac{(q-1)}{2}$ $i \in T_2$	$q+1$	$q^4(q^4-1)(q-1)$

Table 3.1 continued:

Conjugacy class Class representative	No. of classes	Order of centralizer	$[G : C_G(g)]$ $= \lvert nX \rvert$
$B_8(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & \gamma^i & 0 \\ 0 & 0 & 0 & \gamma^{-i} \end{bmatrix}$	$\frac{(q-3)}{2}$ $i \in T_1$	$q(q+1)(q-1)^2$	$q^3(q^2-1)(q+1)$
$B_9(i) = \begin{bmatrix} \gamma^i & 0 & 1 & 0 \\ 0 & \gamma^{-i} & 0 & 1 \\ 0 & 0 & \gamma^i & 0 \\ 0 & 0 & 0 & \gamma^{-i} \end{bmatrix}$	$\frac{(q-3)}{2}$ $i \in T_1$	$q-1$	$q^4(q^4-1)(q+1)$
$C_1(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $C_1'(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	$\frac{(q-1)}{2}$ $i \in T_2$	$q(q+1)(q^2-1)$	$q^3(q^2+1)(q-1)$
$C_{21}(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $C_{21}'(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	$\frac{(q-1)}{2}$ $i \in T_2$	$q(q+1)$	$q^3(q^4-1)(q-1)$
$C_{22}(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & 1 & \gamma \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $C_{22}'(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & -1 & -\gamma \\ 0 & 0 & 0 & -1 \end{bmatrix}$	$\frac{(q-1)}{2}$ $i \in T_2$	$q(q-1)(q^2-1)$	$q^3(q^2+1)(q+1)$
$C_3(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $C_3'(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	$\frac{(q-3)}{2}$ $i \in T_1$	$q(q-1)$	$q^3(q^4-1)(q+1)$

Table 3.1 continued:

Conjugacy class Class representative	No. of classes	Order of centralizer	$[G : C_G(g)]$ $= \lvert nX \rvert$
$C_{41}(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $C'_{41}(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$ $i \in T_1$	$\frac{(q-3)}{2}$	$q(q-1)$	$q^3(q^4-1)(q+1)$
$C_{42}(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & 1 & \gamma \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $C'_{42}(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & -1 & -\gamma \\ 0 & 0 & 0 & -1 \end{bmatrix}$ $i \in T_1$	$\frac{q-3}{2}$	$q(q-1)$	$q^3(q^4-1)(q+1)$
$D_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1	$q^2(q^2-1)^2$	$q^2(q^2+1)$
$D_{21} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$, $D_{22} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -\gamma \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	$q^2(q^2-1)$	$q^2(q^4-1)$
$D_{23} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$, $D_{24} = \begin{bmatrix} 1 & \gamma & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	$2q^2$	$\frac{q^2(q^4-1)(q^2-1)}{2}$
$D_{31} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$, $D_{32} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -\gamma \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	$4q^2$	$\frac{q^2(q^4-1)(q^2-1)}{4}$
$D_{33} = \begin{bmatrix} 1 & \gamma & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$, $D_{34} = \begin{bmatrix} 1 & \gamma & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -\gamma \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1,1	$4q^2$	$\frac{q^2(q^4-1)(q^2-1)}{4}$

3.5 Conjugacy classes of $PSp_4(q)$

In this section, we determine the conjugacy classes of $PSp_4(q)$ from the conjugacy classes and character table of $Sp_4(q)$ [50, 51]. We choose a representative X of a conjugacy class A and then multiply it by $-I$. Hence, we search if $-I$ lies in which

conjugacy classes of $Sp_4(q)$. If both X and $-X$ lies in A, then the canonical image of A in $PSp_4(q)$ will form an independent conjugacy class, where its size is half of the size of the conjugacy class A. If X and $-X$ lie in the distinct classes A and A', then any element of A' will be the additive inverse of some element in A, and so the canonical image of A and A' coincide in $PSp_4(q)$. Therefore, they form only one class, $\bar{A}$ in $PSp_4(q)$, where its size is the same as A. But this method does not work for any class of $Sp_4(q)$. Some classes it need lots of work to check that $-X$ lies in which classes of $Sp_4(q)$. Therefore, the use of character table of the group $Sp_4(q)$ is necessary. Consider the irreducible characters of $Sp_4(q)$, which their values in I and $-I$ are equal. Then these irreducible characters will also be the irreducible characters in $PSp_4(q)$ [51]. Therefore, if the values of these irreducible characters are the same in some conjugacy classes of $Sp_4(q)$, then the canonical image of these classes form an independent class in $PSp_4(q)$. The size of this new conjugacy class is half of the sum of the sizes of these merged classes. This method can not work for any classes in $Sp_4(q)$. For instead, the existence of a large numbers of the irreducible characters of $Sp_4(q)$ and the n^{th} roots of unity in their values is an obstacle, so more work in some classes is needed.

Note 3.5.1. *We use a single notation to refer to both a conjugacy class and its representative.*

By [50, 51], we have type A, B, C, and D families of conjugacy classes of $PSp_4(q)$.

(1) The classes A and A' :
Any conjugacy class A' is the additive inverse of A with the same index. Hence, from the two classes A and A' with the same index, we obtain a class $\bar{A}$ with the same index in $PSp_4(q)$, where its size is equal to the size of class A.

(2) Families of the classes B :
From the table of the conjugacy classes in [50, 51], the conjugacy classes of type B have been classified with respect to their indices. Each type B considered separately:

(2.1) Families of the classes B_1 :

$$B_1(i) = Diag(\xi^i, \xi^{-i}, \xi^{qi}, \xi^{-qi}), \quad i \in R_1 \text{ and } \xi^{q^2+1} = 1.$$

Note that the conjugacy classes $B_1(i)$ cannot be distinct with this definition of R_1. However, [50], has provided a definition of R_1, allowing the classes $B_1(i)$ with $i \in R_1$ to be distinguished by the corresponding irreducible characters $\chi_1(i)$ with $i \in R_1$. Each conjugacy class $B_1(i)$ with $i \in R_1$ is determined with the set:

$$\{\pm i, \pm qi\} \ mod \ (q^2+1). \tag{3.1}$$

Since $\xi^{\pm\frac{(q+1)}{2}} = -1$, if we multiplying $B_1(i)$ by $-I$, transforms modulo (q^2+1), the set (3.1) into:

$$\{\pm i \pm \frac{q^2+1}{2}, \pm qi \pm \frac{q^2+1}{2}\}. \tag{3.2}$$

Since $\frac{q^2+1}{2}$ is odd, if i is odd (even), then $\frac{q^2+1}{2} - i$ is even (odd). It follows that the elements of the classes $B_1(i)$ with $i \in R_1$, where i is odd, are additive inverses of the elements of the classes $B_1(i)$ with $i \in R_1$ and i is even. Hence, their canonical images has size $\frac{(q^2+1)}{8}$ for $i \in R_1$ and i even, where their sizes are the same as $B_1(i)$.

(2.2) Families of the classes B_2 :

$$B_2(i) = Diag(\theta^i, \theta^{-i}, \theta^{qi}, \theta^{-qi}), \quad i \in R_2 \text{ and } \theta^{q^2-1} = 1.$$

Each conjugacy class $B_2(i)$ with $i \in R_2$ is determined BY the set:

$$\{\pm i, \pm qi\} \ mod \ (q^2-1). \tag{3.3}$$

Since $\theta^{\pm\frac{(q-1)}{2}} = -1$, if multiplying $B_2(i)$ by $-I$ transforms modulo (q^2-1), the set (3.3) into:

$$\{\pm i \pm \frac{q^2-1}{2}, \pm qi \pm \frac{q^2-1}{2}\}. \tag{3.4}$$

There are two cases to consider:

(2.2.1) Case 1 : If $i \in R_2$ satisfying equation 3.5 :

$$i - \frac{q^2-1}{2} \equiv \pm qi \mod (q^2-1). \tag{3.5}$$

Then the conjugacy class $B_2(i)$ contains the additive inverse of each of its elements. Hence, the size of its canonical image $\overline{B_2}(i)$ is half of the

size of $B_2(i)$. The congruent equation (3.5), has $\frac{q-1}{2}$ distinct solutions in R_2. Denote this set of solutions by R_2'. In $PSp_4(q)$, we have $\frac{q-1}{2}$ conjugacy classes $\overline{B_2}(i)$ with $i \in R_2'$ such that their sizes are $\frac{q^4(q^4-1)}{2}$.

(2.2.2) Case 2 : If $i \in R_2$ does not satisfying equation (3.5), then $-B_2(i)$ is another class from the remaining classes in this family. In other word, there exists a $j \in R_2 - R_2'$ with $j \neq i$, such that $-B_2(i) = B_2(j)$. Thus, these two classes are merge in $PSp_4(q)$ under the canonical homomorphism. Therefore, we have $\frac{(q-1)(q-3)}{8}$ classes $\overline{B_2}(i)$ with $i \in R_2''$ of size $q^4(q^4-1)$, where R'' is the set of $\frac{(q-1)(q-3)}{8}$ positive integers $i \in R_2 - R_2'$ such that all of the scalars $\theta^i, \theta^{-i}, \theta^{qi}$, and θ^{-qi} are distinct.

(2.3) Families of the classes B_3 :

$$B_3(i,j) = Diag(\gamma^i, \gamma^{-i}, \gamma^{qi}, \gamma^{-qi}), \quad i,j \in T_1 \text{ with } i < j \text{ and } \gamma^{q-1} = 1.$$

Each conjugacy class $B_3(i,j)$ is determined by the set:

$$\{\pm i, \pm j\} \ mod\ (q-1). \tag{3.6}$$

If we multiply $B_3(i,j)$ by $-I$, then the set (3.6) transforms into:

$$\{\pm i + \frac{q-1}{2}, \pm j + \frac{q-1}{2}\}. \tag{3.7}$$

Since $\gamma^{\frac{q-1}{2}} = -1$. Now if the modulo $(q-1)$, the set (3.7) is given by:

$$\{\pm i \pm \frac{q-1}{2}, \pm j \pm \frac{q-1}{2}\}. \tag{3.8}$$

Therefore, the classes $B_3(i,j)$ and $-B_3(i,j)$ are equal if and only if $-i + \frac{q-1}{2} = j$ or equivalently if $\frac{q-1}{2} = i + j$.

Note that the classes $B_3(i,j)$ and $B_3(j,i)$ are equal. Observe that $EB_3(i,j) = B_3(j,i)$, where:

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

Therefore, there is two cases to consider:

(2.3.1) Case 1 : $q = 4k + 1$.

The classes $B_3(i,j)$ and $-B_3(i,j)$ are equal if and only if $i = 1, 2, \cdots, \frac{q-5}{4}$ and $j = \frac{q-1}{2} - i$. Each of the $\frac{q-5}{4}$ classes $B_3(i,j)$ with $i = 1, 2, \cdots, \frac{q-5}{4}$ and $j = \frac{q-1}{2} - i$, constrains the additive inverse of each element within itself. Hence, the canonical image of these classes in $PSp_4(q)$ forms an independent class $\overline{B_3}(i,j)$, with its size equals to half of $B_3(i,j)$. For the remaining classes of the families B_3, we observe that for any class $B_3(i,j)$ with $i + j < \frac{q-1}{2}$, multiplying by $-I$ yields the class $B_3(i',j')$ where $i' = \frac{q-1}{2} - j$ and $j' = \frac{q-1}{2} - i$. Therefore, the canonical images of these two classes coincide in $PSp_4(q)$ and form a class with the same size as $B_3(i,j)$. Consequently, from the remaining classes, we obtain $\frac{(q-1)^2}{16}$ distinct classes:

$$\overline{B_3}(i,j), \quad 1 \leq i \leq \frac{q-5}{4} \quad \text{and} \quad i < j \leq \frac{q-3}{4} - i,$$

in $PSp_4(q)$ with the same size as $B_3(i,j)$.

(2.3.2) Case 2 : $q = 4k + 3$.

The classes $B_3(i,j)$ and $-B_3(i,j)$ are equal if and only if $i = 1, 2, \cdots, k$ and $j = \frac{q-1}{2} - i$. Using a similar argument as in case 1, in $PSp_4(q)$. We obtain $k = \frac{q-3}{4}$ classes $B_3(i,j)$ whose sizes equal half the size of $B_3(i,j)$, where $i = 1, 2, \cdots, \frac{q-3}{4}$ and $j = \frac{q-1}{2} - i$. Additionally, we have $\frac{(q-3)(q-7)}{16}$ classes $\overline{B_3}(i,j)$ with sizes to $B_3(i,j)$, such that $1 \leq i \leq \frac{q-7}{4}$ and $i < j \leq \frac{q-3}{4} - i$.

(2.4) Families of the classes B_4 :

$$B_4(i,j) = Diag(\eta^i, \eta^{-i}, \eta^j, \eta^{-j}), \quad i,j \text{ in } T_2 \text{ with } i < j \text{ and } \eta^{q+1} = 1.$$

As referenced (3.5), if $q = 4k + 1$ (or $q = 4k + 3$), where $k = \frac{q-1}{4}$ the classes $B_4(i,j)$ $i = 1, 2, 3, \cdots, k$ and $j = \frac{q+1}{4} - i$ contains the additive inverse of their elements. The canonical images of these classes are distinct, and their sizes are divided by 2. From the remaining classes of this family, we obtain the classes in $PSp_4(q)$.

If $q = 4k + 1$, then we have $\frac{(q-1)(q-5)}{16}$ classes,

$$\overline{B_4}(i,j), \quad 1 \leq i \leq \frac{q-5}{4} \quad \text{and } i < j \leq \frac{q-1}{2} - i.$$

If $q = 4k+3$, then we have $\frac{(q-3)^2}{16}$ classes,

$$\overline{B_4}(i,j),\ 1 \leq i \leq \frac{q-3}{4} \text{ and } i < j < \frac{q-1}{2} - i.$$

Remark 3.5.2. *In both cases for q, the size of $\overline{B_4}(i,j)$ is the same as that of $B_4(i,j)$.*

(2.5) Families of the classes B_5 :

$$B_5(i,j) = Diag(\eta^i, \eta^{-i}, \eta^j, \eta^{-j}),\quad i \in T_2 \text{ and } j \in T_1 \text{ with } \eta^{q+1} = 1 = \gamma^{q-1}.$$

By multiplying $B_5(i,j)$ by $-I$, we obtain two distinct classes:
$B_5(\frac{q+1}{2} - i, \frac{q-1}{2} - j)$.

Note 3.5.3. *If equality occurs, then $i = \frac{q-1}{4}$ and $j = \frac{q-3}{3}$, for such i and j, there is no integral solution for q.*

Consequently, this family of classes contains $B_5(i,j)$ and $-B_5(i,j)$ for each $i \in T_2$ and $j \in T_1$. Hence, the canonical images of these classes coincide in $PSp_4(q)$. Thus, in $PSp_4(q)$, there are a total of $\frac{(q-1)(q-3)}{8}$ distinct classes $\overline{B_5}(i,j)$ with size $q^4(q^4-1)$. If $q = 4k+1$, then $1 \leq i \leq \frac{q-1}{4}$ and $1 \leq j \leq \frac{q-3}{2}$. If $q = 4k+3$, then $1 \leq i \leq \frac{q-1}{2}$ and $1 \leq j \leq \frac{q-3}{4}$.

(2.6) Families of the classes B_6 :

$$B_6(i) = Diag(\eta^i, \eta^{-i}, \eta^i, \eta^{-i}),\ i \in T_2 \text{ with } \eta^{q+1} = 1.$$

Each class $B_6(i)$ is determined by the set:

$$\{\pm i\}\ mod\ (q+1). \tag{3.9}$$

Each class $-B_6(i)$ is determined by the set:

$$\{\pm\frac{q-1}{2} \pm i\}\ mod\ (q+1). \tag{3.10}$$

Observe that modulo $(q+1)$, the two sets, (3.9) and (3.10), are distinct unless $i = \frac{q+1}{4}$ and $q = 4k+1$.
Therefore, there are two cases:

(2.6.1) Case 1 : If $q = 4k+1$, then under the canonical homomorphism, the classes $B_6(i)$, for $i \in T_2$. This will yield $\frac{q-1}{4}$ classes $\overline{B_6}(i)$, where $i = 1, 2, \cdots, \frac{q-1}{4}$, with sizes $q^3(q-1)(q^2+1)$ in $PSp_4(q)$.

(2.6.2) Case 2 : If $q = 4k+3$, then the canonical image $\overline{B}(\frac{q+1}{4})$ of the class $B_6(\frac{q+1}{4})$ has the size $\frac{q^3(q-1)(q^2+1)}{2}$ under the canonical homomorphism. From $\frac{q-3}{2}$ the remaining classes, half of them merge with another half, resulting in $\frac{q-3}{4}$ classes $\overline{B_6}(i)$, where $i = 1, 2, \cdots, \frac{q-3}{4}$ with the sizes $q^3(q-1)(q^2+1)$ in $PSp_4(q)$.

(2.7) Families of the classes B_8 :

$$B_8(i) = Diag(\gamma^i, \gamma^{-i}, \gamma^i, \gamma^{-i}),\ i \in T_1 \text{ with } \gamma^{q-1} = 1.$$

This follows a similar argument as for $B_6(i)$.
There are two cases:

(2.7.1) Case 1 : If $q = 4k+1$, then the classes $B_8(\frac{q-1}{4})$ gives rise to a class $\overline{B_8}(\frac{q-1}{4})$ with size $q^3(q+1)(q^2+1)$ in $PSp_4(q)$. From the remaining classes, we obtain classes $\overline{B_8}(i)$, where $i = 1, 2, \cdots, \frac{q-5}{4}$, each also having size $q^3(q+1)(q^2+1)$ in $PSp_4(q)$.

(2.7.2) Case 2 : If $q = 4k+3$, then from the family of classes $B_8(i)$, we obtain $\frac{q-3}{4}$ classes $\overline{B_8}(i)$, where $i = 1, 2, \cdots, \frac{q-3}{4}$ each with size $q^3(q+1)(q^2+1)$ in $PSp_4(q)$.

(2.8) Families of the classes B_7 :
To determine the canonical image of $B_7(i)$ with $i \in T_2$ in $PSp_4(q)$, we consider the values of the irreducible characters of $Sp_4(q)$ in $B_7(i)$ that have equal values at $\pm I$ [50]. These values also correspond to irreducible characters of $PSp_4(q)$.
There are two cases to consider:

(2.8.1) Case 1 : If $q = 4k+1$, then the irreducible characters that have equal values at $\pm I$ also have equal in $B_7(i)$ and $B_7(\frac{q+1}{2} - i)$. The values of these irreducible characters in this family are determined by $\beta_{ik} = (\overline{\eta})^{ik} + (\overline{\eta})^{-ik}$. Since $\eta^{\frac{q+1}{2}} = -1$, we have $\beta_{\frac{q+1}{2}-i} = (-1)^k \beta_{ik}$. In irreducible characters, the factor $(-1)^k$ vanishes. For an example, the value of the irreducible characters

$\xi'_{21}(k)$ (where k is odd) in $B_7(i)$ is equal to $(-1)^i\beta_{ik}$ while in $B_7(\frac{q+1}{2}-i)$ it is equal to

$$(-1)^{\frac{q+1}{2}-i}\beta_{(\frac{q+1}{2}-i)k} = (-1)^{\frac{q+1}{2}}(-1)^k(-1)^i\beta_{ik} = (-1)^i\beta_{ik}.$$

Since k and $\frac{q+1}{2}$ are both odd, the canonical images of these classes coincide in $PSp_4(q)$. Thus, in $PSp_4(q)$, we have $\frac{q-1}{4}$ classes $\overline{B_7}(i)$ with size $q^3(q-1)(q^4-1)$, where $i = 1, 2, \cdots, \frac{q-1}{4}$.

(2.8.2) Case 2 : If $q = 4k+3$, then all of the classes $B_7(i)$ are distinguished by some of the mentioned irreducible characters. For example, as noted in (3.5), the values $\xi'_{21}(k)$ in $B_7(i)$ and $B_7(\frac{q+1}{2}-i)$ are $(-1)^i\beta_{ik}$ and $-(-1)^i\beta_{ik}$, respectively. Therefore, there are $\frac{q-1}{2}$ classes $\overline{B_7}(i)$ with size $\frac{q^3(q-1)(q^4-1)}{2}$ in $PSp_4(q)$.

(2.9) Families of the classes B_9 :

By a similar argument as for $B_7(i)$, consider the character table of $Sp_4(q)$. For $i \in T_1$, the classes $B_9(i)$ and $B_9(\frac{q-1}{2}-i)$ have the same values in all corresponding irreducible characters of $Sp_4(q)$, thus, their canonical images coincide in $PSp_4(q)$. There are two cases to consider:

(2.9.1) Case 1 : If $q = 4k+1$, then we obtain $\frac{q-1}{4}$ classes $\overline{B_9}(i)$ with $i = 1, 2, \cdots, \frac{q-1}{4}$ each has size $q^3(q+1)(q^4-1)$. Additionally, there is one class $\overline{B_7}(\frac{q-1}{4})$ with size $\frac{q^3(q+1)(q^4-1)}{2}$ in $PSp_4(q)$.

(2.9.2) Case 2 : If $q = 4k+3$, then in $PSp_4(q)$, we have $\frac{q-3}{2}$ classes $\overline{B_9}(i)$, where $i = 1, 2, \cdots, \frac{q-3}{4}$ each with size $q^3(q-1)(q^4-1)$.

(3) Families of the classes C and C' :

For any classes $C_1(i)$, with $i \in T_2$ in the family C_1, the classes,

$C_1(i)$ correspond to classes $C'_1(j)$, where $j \in T_2$ of the family C'_1, although i and j are not necessarily equal. Hence, the canonical images of the elements in these family of classes are pairwise distinct in $PSp_4(q)$. Therefore, these families give rise to $\frac{q-1}{2}$ classes $\overline{C_1}(i)$, with $i \in T_2$ and each having size $q^3(q-1)(q^2+1)$ in $PSp_4(q)$.

By a similar argument, there are collections of classes in $PSp_4(q)$ given by:

$$\{\overline{C_{21}}(i) : i \in T_2\}, \quad |\overline{C_{21}}(i)| = \frac{q^3(q-1)(q^4-1)}{2};$$
$$\{\overline{C_{22}}(i) : i \in T_2\}, \quad |\overline{C_{22}}(i)| = \frac{q^3(q-1)(q^4-1)}{2};$$
$$\{\overline{C_3}(i) : i \in T_2\}, \quad |\overline{C_3}(i)| = \frac{q^3(q+1)(q^4+1)}{2};$$
$$\{\overline{C_{41}}(i) : i \in T_2\}, \quad |\overline{C_{41}}(i)| = \frac{q^3(q+1)(q^4-1)}{2};$$
$$\{\overline{C_{42}}(i) : i \in T_2\}, \quad |\{\overline{C_{42}}(i)| = \frac{q^3(q+1)(q^4-1)}{2}.$$

(4) Family of the classes D :

The additive inverse of each element D_1 is also in D_1. The representative of D_1 in $Sp_4(q)$ is $Diag(1, 1, -1, -1)$, with $ED_1E = -D_1$ (refer to $B_3(i, j)$ for E).
By considering the character table and the conjugacy classes of $Sp_4(q)$ in [50], the pairs of classes (D_{21}, D_{23}) and (D_{22}, D_{24}) are additive inverses of each other. The irreducible characters of $Sp_4(q)$ corresponding to the irreducible characters of $PSp_4(q)$ have equal values in D_{32} and D_{33}, but in the classes D_{31} and D_{34}, these characters are distinct. Note that the differences lie in ξ and ξ', which occur in the values of some characters. Therefore, the following classes must be added to the conjugacy classes of $PSp_4(q)$:

$$|\overline{D_1}| = \frac{q^2(q^2+1)}{2},$$
$$|\overline{D_{21}}| = \frac{q^4(q^4-1)}{2},$$
$$|\overline{D_{22}}| = \frac{q^2(q^4-1)}{2},$$
$$|\overline{D_{31}}| = \frac{q^2(q^2-1)(q^4-1)}{8},$$
$$|\overline{D_{32}}| = \frac{q^2(q^2-1)(q^4-1)}{4},$$
$$|\overline{D_{34}}| = \frac{q^2(q^2-1)(q^4-1)}{8}.$$

For Table 3.2 and 3.3, refer to Table 3.1 for the class representatives of the conjugacy classes $\overline{A_1}$ to $\overline{D_{34}}$.

Table 3.2: $PSp_4(q),\ q = 4k+1$

Conjugacy class Class representative	No. of classes	Order of centralizer	$[G : C_G(g)]$ $= \lvert nX \rvert$
$\overline{A_1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1	$\frac{q^4(q^4-1)(q^2-1)}{2}$	1
$\overline{A_{21}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1	$q^4(q^2-1)$	$\frac{q^4-1}{2}$
$\overline{A_{22}} = \begin{bmatrix} 1 & \gamma & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1	$q^4(q^2-1)$	$\frac{q^4-1}{2}$
$\overline{A_{31}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1	$q^3(q-1)$	$\frac{q(q^4-1)(q+1)}{2}$
$\overline{A_{32}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -\gamma \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1	$q^3(q+1)$	$\frac{q(q^4-1)(q-1)}{2}$
$\overline{A_{41}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1	q^2	$\frac{q^2(q^4-1)(q^2-1)}{2}$
$\overline{A_{42}} = \begin{bmatrix} 1 & \gamma & 0 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1	q^2	$\frac{q^2(q^4-1)(q^2-1)}{2}$

Table 3.2 continued:

Conjugacy class Class representative	No. of classes	Order of centralizer	$[G : C_G(g)]$ $= \lvert nX \rvert$
$\overline{B_1}(i) = \begin{bmatrix} \zeta^i & 0 & 0 & 0 \\ 0 & \zeta^{-i} & 0 & 0 \\ 0 & 0 & \zeta^{qi} & 0 \\ 0 & 0 & 0 & \zeta^{-qi} \end{bmatrix}$	$\frac{q^2-1}{8}$ $i \in R_1$, i *even*	$\frac{q^2+1}{2}$	$q^4(q^2-1)^2$
$\overline{B_2}(i) = \begin{bmatrix} \theta^i & 0 & 0 & 0 \\ 0 & \theta^{-i} & 0 & 0 \\ 0 & 0 & \theta^{qi} & 0 \\ 0 & 0 & 0 & \theta^{-qi} \end{bmatrix}$	$\frac{(q-1)^2}{2}$ $i \in R_2'$	q^2-1	$\frac{q^4(q^4-1)}{2}$
$\overline{B_2}(i)$	$\frac{(q-1)(q-3)}{2}$ $i \in R_2''$	$\frac{q^2-1}{2}$	$q^4(q^4-1)$
$\overline{B_3}(i,j) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & \gamma^j & 0 \\ 0 & 0 & 0 & \gamma^{-j} \end{bmatrix}$	$\frac{q-5}{4}$ $1 \le i \le \frac{q-5}{4}$ $j = \frac{q-1}{2} - i$	$(q-1)^2$	$\frac{q^4(q^2+1)(q+1)^2}{2}$
$\overline{B_3}(i,j)$	$\frac{(q-5)^2}{16}$ $1 \le i \le \frac{q-5}{4}$ $i < j \le \frac{q-3}{2} - i$	$\frac{(q-1)^2}{2}$	$q^4(q^2+1)(q+1)^2$
$\overline{B_4}(i,j) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & \eta^j & 0 \\ 0 & 0 & 0 & \eta^{-j} \end{bmatrix}$	$\frac{q-1}{4}$ $1 \le i \le \frac{q-1}{4}$ $j = \frac{q+1}{2} - i$	$(q+1)^2$	$\frac{q^4(q^2+1)(q-1)^2}{2}$
$\overline{B_4}(i,j)$	$\frac{(q-1)(q-5)}{16}$ $1 \le i \le \frac{q-5}{4}$ $i < j \le \frac{q-1}{2} - i$	$\frac{(q+1)^2}{2}$	$q^4(q^2+1)(q-1)^2$
$\overline{B_5}(i,j) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & \gamma^j & 0 \\ 0 & 0 & 0 & \gamma^{-j} \end{bmatrix}$	$\frac{(q-1)(q-3)}{8}$ $1 \le i \le \frac{q-1}{4}$ $i < j \le \frac{q-3}{2} - i$	$\frac{q^2-1}{2}$	$q^4(q^4-1)$
$\overline{B_6}(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & \eta^i & 0 \\ 0 & 0 & 0 & \eta^{-i} \end{bmatrix}$	$\frac{(q-1)}{4}$ $1 \le i \le \frac{q-1}{4}$	$q(q+1)(q^2-1)$	$q^3(q^2+1)(q-1)$

Table 3.2 continued:

Conjugacy class Class representative	No. of classes	Order of centralizer	$[G : C_G(g)]$ $= \lvert nX \rvert$
$\overline{B_7}(i) = \begin{bmatrix} \eta^i & 0 & 1 & 0 \\ 0 & \eta^{-i} & 0 & 1 \\ 0 & 0 & \eta^i & 0 \\ 0 & 0 & 0 & \eta^{-i} \end{bmatrix}$	$\frac{(q-1)}{4}$ $1 \leq i \leq \frac{q-1}{4}$	$\frac{q(q+1)(q^2+1)}{2}$	$q^3(q^4-1)(q-1)$
$\overline{B_8}(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & \gamma^i & 0 \\ 0 & 0 & 0 & \gamma^{-i} \end{bmatrix}$	$\frac{(q-5)}{4}$ $1 \leq i \leq \frac{q-5}{4}$	$\frac{q(q-1)(q^2-1)}{2}$	$q^3(q^2+1)(q+1)$
$\overline{B_8}(i)$	1 $i = \frac{q-1}{2}$	$q(q-1)(q^2-1)$	$\frac{q^3(q^2+1)(q+1)}{2}$
$\overline{B_9}(i) = \begin{bmatrix} \gamma^i & 0 & 1 & 0 \\ 0 & \gamma^{-i} & 0 & 1 \\ 0 & 0 & \gamma^i & 0 \\ 0 & 0 & 0 & \gamma^{-i} \end{bmatrix}$	$\frac{q-5}{4}$ $1 \leq i \leq \frac{q-5}{4}$	$\frac{q(q-1)}{2}$	$q^3(q^4-1)(q+1)$
$\overline{B_9}(i)$	1 $i = \frac{q-1}{4}$	$q(q-1)$	$\frac{q^3(q^4-1)(q+1)}{2}$
$\overline{C_1}(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	$\frac{(q-1)}{2}$ $i \in T_2$	$\frac{q(q-1)(q^2-1)}{2}$	$q^3(q^2+1)(q-1)$
$\overline{C_{21}}(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	$\frac{(q-1)}{2}$ $i \in T_2$	$q(q+1)$	$\frac{q^3(q^4-1)(q-1)}{2}$
$\overline{C_{22}}(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & 1 & \gamma \\ 0 & 0 & 0 & 1 \end{bmatrix}$	$\frac{(q-1)}{2}$ $i \in T_2$	$q(q+1)$	$\frac{q^3(q^4-1)(q-1)}{2}$
$\overline{C_3}(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	$\frac{(q-3)}{2}$ $i \in T_1$	$q(q^2-1)(q-1)$	$q^3(q^2+1)(q+1)$

Table 3.2 continued:

Conjugacy class Class representative	No. of classes	Order of centralizer	$[G : C_G(g)]$ $= \lvert nX \rvert$
$\overline{C_{41}}(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	$\frac{(q-3)}{2}$ $i \in T_1$	$q(q-1)$	$\frac{q^3(q^4-1)(q+1)}{2}$
$\overline{C_{42}}(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & 1 & \gamma \\ 0 & 0 & 0 & 1 \end{bmatrix}$	$\frac{q-3}{2}$ $i \in T_1$	$q(q-1)$	$\frac{q^3(q^4-1)(q+1)}{2}$
$\overline{D_1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1	$q^2(q^2-1)^2$	$\frac{q^2(q^2+1)}{2}$
$\overline{D_{21}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1	$q^2(q^2-1)$	$\frac{q^2(q^2+1)(q^2-1)}{2}$
$\overline{D_{22}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -\gamma \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1	$q^2(q^2-1)$	$\frac{q^2(q^2+1)(q^2-1)}{2}$
$\overline{D_{31}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1	$2q^2$	$\frac{q^2(q^4-1)(q^2-1)}{4}$
$\overline{D_{32}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -\gamma \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1	$4q^2$	$\frac{q^2(q^4-1)(q^2-1)}{8}$
$\overline{D_{34}} = \begin{bmatrix} 1 & \gamma & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -\gamma \\ 0 & 0 & 0 & -1 \end{bmatrix}$	1	$4q^2$	$\frac{q^2(q^4-1)(q^2-1)}{8}$

Table 3.3: $PSp_4(q),\ q = 4k+3$

Conjugacy class Class representative	No. of classes	Order of centralizer	$[G : C_G(g)]$ $= \lvert nX \rvert$
$\overline{B_6}(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & \eta^i & 0 \\ 0 & 0 & 0 & \eta^{-i} \end{bmatrix}$	1 $i = \frac{q+1}{4}$	$q(q-1)(q+1)^2$	$\frac{q^3(q^2+1)(q-1)}{2}$
$\overline{B_6}(i)$	$\frac{(q-1)}{4}$ $1 \leq i \leq \frac{q-1}{4}$	$\frac{q(q-1)(q+1)^2}{2}$	$q^3(q^2+1)(q-1)$
$\overline{B_7}(i) = \begin{bmatrix} \eta^i & 0 & 1 & 0 \\ 0 & \eta^{-i} & 0 & 1 \\ 0 & 0 & \eta^i & 0 \\ 0 & 0 & 0 & \eta^{-i} \end{bmatrix}$	$\frac{(q-1)}{2}$ $1 \leq i \leq \frac{q-1}{2}$	$q(q-1)$	$\frac{q^3(q^4-1)(q-1)}{2}$
$\overline{B_8}(i) = \begin{bmatrix} \gamma^i & 0 & 0 & 0 \\ 0 & \gamma^{-i} & 0 & 0 \\ 0 & 0 & \gamma^i & 0 \\ 0 & 0 & 0 & \gamma^{-i} \end{bmatrix}$	$\frac{q-3}{4}$ $1 \leq i \leq \frac{q-3}{4}$	$\frac{q(q-1)(q^2-1)}{2}$	$q^3(q^2+1)(q+1)$
$\overline{B_9}(i) = \begin{bmatrix} \gamma^i & 0 & 1 & 0 \\ 0 & \gamma^{-i} & 0 & 1 \\ 0 & 0 & \gamma^i & 0 \\ 0 & 0 & 0 & \gamma^{-i} \end{bmatrix}$	$\frac{q-3}{4}$ $1 \leq i \leq \frac{q-3}{4}$	$\frac{q(q-1)}{2}$	$q^3(q^4-1)(q+1)$

Remark 3.5.4. *Tables 3.2 and 3.3 together provide the conjugacy classes of $PSp_4(q)$ for q an odd prime power.*

Table 3.4: Character Table of $PSp_4(q),\ q = 4k+1$

Character	$\chi_1(j)$	$\chi_2(j)$	$\chi_3(k,r)$	$\chi_4(k,r)$	$\chi_5(k,r)$	$\chi_6(k)$	$\chi_7(k)$	$\chi_8(k)$	$\chi_9(k)$
irreducible	$j \in R_1$	$j \in R_2$	$k,r \in T_1, k \neq r$	$k,r \in T_2, k \neq r$	$k \in T_2, r \in T_1$	$k \in T_2$	$k \in T_2$	$k \in T_1$	$k \in T_1$
	j even	j even	$k+r$ even	$k+r$ even	$k+r$ even				
A_1	$(q^2-1)^2$	q^4-1	$(q+1)^2(q^2+1)$	$(q-1)^2(q^2+1)$	q^4-1	$(q-1)(q^2+1)$	$q(q-1)(q^2+1)$	$(q+1)(q^2+1)$	$q(q+1)(q^2+1)$
A_{21}	$1-q^2$	$1-q^2$	$(1+q)^2$	$(1-q)^2$	$1+q^2$	$q-1$	$q(1-q)$	$q+1$	$q(q+1)$
A_{31}	$1-q$	$1+q$	$1+3q$	$1-q$	$1-q$	-1	$-q$	$(1+2q)$	q
A_{32}	$1+q$	$1-q$	$1+q$	$1-3q$	$1+q$	$1-2q$	$-q$	1	q
A_{41}	1	1	1	1	1	1		1	
$B_1(i)$	$\tilde{\zeta}^{ij}+\tilde{\zeta}^{-ij}+\tilde{\zeta}^{qij}+\tilde{\zeta}^{-qij}$								
$B_2(i)$		$\tilde{\theta}^{ij}+\tilde{\theta}^{-ij}+\tilde{\theta}^{qij}+\tilde{\theta}^{-qij}$				β_{ik}	$-\beta_{ik}$	α_{lk}	$-\alpha_{lk}$
$B_3(i,j)$			$\alpha_{ik}\alpha_{jr}+\alpha_{jk}\alpha_{ir}$					$\alpha_{ik}\alpha_{jk}$	$\alpha_{ik}\alpha_{jk}$
$B_4(i,j)$				$\beta_{ik}\beta_{jr}+\beta_{jk}\beta_{ir}$		$\beta_{ik}\beta_{jk}$	$\beta_{ik}\beta_{jk}$		
$B_5(i,j)$					$\beta_{ik}\alpha_{jr}$				
$B_6(i)$		$(1+q)\beta_{ij}$		$(1-q)\beta_{ik}\beta_{ir}$		$\beta_{2ik}+1-q$	$-q\beta_{2ik}+1-q$	$1+q$	$-(1+q)$
$B_7(i)$		β_{ij}		$\beta_{ik}\beta_{ir}$		$\beta_{2ik}+1$	1	1	-1
$B_8(i)$		$(1-q)\alpha_{ij}$	$(1+q)\alpha_{ik}\alpha_{ir}$			$1-q$	$-(1-q)$	$\alpha_{2ik}+1+q$	$q\alpha_{2ik}+1+q$
$B_9(i)$		α_{ij}	$\alpha_{ik}\alpha_{ir}$			-1	1	$\alpha_{2ik}+1$	1
$C_1(i)$				$(1-q)(\beta_{ik}+\beta_{ir})$	$(1+q)\beta_{ik}$	$(1-q)\beta_{ik}$	$\beta_{ik}(1-q)$		
$C_{21}(i)$				$(\beta_{ik}+\beta_{ir})$	β_{ik}	β_{ik}	β_{ik}		
$C_3(i)$			$(1+q)(\alpha_{ik}+\alpha_{ir})$		$(1-q)\alpha_{ir}$			$(1+q)\alpha_{ik}$	$(1+q)\alpha_{ik}$
$C_{41}(i)$			$(\alpha_{ik}+\alpha_{ir})$		α_{ir}			α_{ik}	α_{ik}
D_1			$2(-1)^k(1+q)^2$	$2(-1)^k(1-q)^2$	$2(-1)^k(1+q^2)$	$(-1)^k(1-q)^2$	$(-1)^k(1-q)^2$	$(-1)^k(1+q)^2$	$(-1)^k(1+q)^2$
D_{21}			$2(-1)^k(1+q)$	$2(-1)^k(1-q)$	$2(-1)^k$	$(-1)^k(1-q)$	$(-1)^k(1-q)$	$(-1)^k(1+q)$	$(-1)^k(1+q)$
D_{31}			$2(-1)^k$	$2(-1)^k$	$2(-1)^k$	$(-1)^k$	$(-1)^k$	$(-1)^k$	$(-1)^k$
D_{32}			$2(-1)^k$	$2(-1)^k$	$2(-1)^k$	$(-1)^k$	$(-1)^k$	$(-1)^k$	$(-1)^k$

Table 3.4 continued:

Character	$\xi_1(k)$	$\xi_1'(k)$	$\xi_3(k)$	$\xi_3'(k)$	$\xi_{21}(k)$	$\xi_{21}'(k)$	$\xi_{41}(k)$	$\xi_{41}'(k)$
irreducible	$k \in T_2$	$k \in T_2$	$k \in T_1$	$k \in T_1$	$k \in T_2$	$k \in T_2$	$k \in T_1$	$k \in T_1$
	k even	k even	k even	k even	k even	k odd	k even	k odd
A_1	$(q-1)(q^2+1)$	$q(q-1)(q^2+1)$	$(q+1)(q^2+1)$	$q(q+1)(q^2+1)$	$\frac{q^4-1}{2}$	$\frac{(q-1)^2(q^2+1)}{2}$	$\frac{(q+1)^2(q^2+1)}{2}$	$\frac{q^4+1}{2}$
A_{21}	$1+q^2-q$	q	$1+q+q^2$	q	$\frac{1+q}{2}+q(1-q)\tilde{\varepsilon}$	$\frac{1-q}{2}+q(1-q)\tilde{\varepsilon}$	$\frac{1+q}{2}-q(1+q)\tilde{\varepsilon}$	$\frac{1-q}{2}-q(1+q)\tilde{\varepsilon}$
A_{31}	$1-q$		$1+q$	$2q$	$\frac{1-q}{2}$	$\frac{1-q}{2}$	$\frac{1+3q}{2}$	$\frac{1-q}{2}$
A_{32}	$1-q$	$2q$	$1+q$		$\frac{1+q}{2}$	$\frac{1-3q}{2}$	$\frac{1+q}{2}$	$\frac{1+q}{2}$
A_{41}	1		1		$-\tilde{\varepsilon}'$	$-\tilde{\varepsilon}'$	$-\tilde{\varepsilon}$	$-\tilde{\varepsilon}$
$B_1(i)$								
$B_2(i)$								
$B_3(i,j)$			$\alpha_{ik}+\alpha_{jk}$	$\alpha_{ik}+\alpha_{jk}$			$(-1)^j\alpha_{ik}+(-1)^i\alpha_{jk}$	
$B_4(i,j)$	$\beta_{ik}+\beta_{jk}$	$-\beta_{ik}-\beta_{jk}$				$(-1)^i(1-q)\beta_{jk}$		
$B_5(i,j)$	β_{ik}	β_{ik}	α_{jk}	$-\alpha_{jk}$	$(-1)^j\beta_{ik}$			$(-1)^i\alpha_{jk}$
$B_6(i)$	$(1-q)\beta_{ik}$	$-(1-q)\beta_{ik}$				$(-1)^i(1-q)\beta_{ik}$		
$B_7(i)$	β_{ik}	$-\beta_{ik}$				$(-1)^i\beta_{ik}$		
$B_8(i)$			$(1+q)\alpha_{ik}$	$(1+q)\alpha_{ik}$			$(-1)^i(1+q)\alpha_{ik}$	
$B_9(i)$			α_{ik}	α_{ik}			$(-1)^i\alpha_{ik}$	
$C_1(i)$	$1-q+\beta_{ik}$	$q-1+q\beta_{ik}$	$1+q$	$-(1+q)$	$\frac{(1+q)\beta_{ik}}{2}$	$(-1)^i(1-q)+\frac{(1-q)\beta_{ik}}{2}$		$(-1)^i(1+q)$
$C_{21}(i)$	$1+\beta_{ik}$	-1	$1+q$	1	-1	$\beta_{ik}\tilde{\varepsilon}$	$(-1)^i-\beta_{ik}\tilde{\varepsilon}$	$(-1)^i$
$C_3(i)$	$1-q$	$1-q$	$1+q+\alpha_{ik}$	$1+q+q\alpha_{ik}$	$(-1)^i(1-q)$		$(-1)^i(1+q)+\frac{(1+q)\alpha_{ik}}{2}$	$\frac{(1-q)\alpha_{ik}}{2}$
$C_{41}(i)$	1	1	$1+\alpha_{ik}$	1	$(-1)^i$		$(-1)^i-\alpha_{ik}\tilde{\varepsilon}$	$-\alpha_{ik}\tilde{\varepsilon}$
D_1	$2(1-q)$	$2q(1-q)$	$2(1+q)$	$2q(1+q)$	$1-q^2$	$-(1-q)^2$	$(1+q)^2$	$-(1-q)^2$
D_{21}	$2-q$	q	$2+q$	q	$\frac{1+q}{2}-(1-q)\tilde{\varepsilon}$	$-\frac{1-q}{2}+(1-q)\tilde{\varepsilon}$	$\frac{1+q}{2}-(1+q)\tilde{\varepsilon}$	$-\frac{1-q}{2}+(1+q)\tilde{\varepsilon}$
D_{31}	2		2		$-2\tilde{\varepsilon}$	$2\tilde{\varepsilon}$	$-2\tilde{\varepsilon}$	$2\tilde{\varepsilon}$
D_{32}	2		2		$-\tilde{\varepsilon}-\tilde{\varepsilon}'$	$\tilde{\varepsilon}+\tilde{\varepsilon}'$	$-\tilde{\varepsilon}-\tilde{\varepsilon}'$	$\tilde{\varepsilon}+\tilde{\varepsilon}'$

Table 3.4 continued:

Character	Φ_5	Φ_7	Φ_9
A_1	$\frac{(1+q)(q^2+1)}{2}$	$\frac{(1+q)(q^2+1)}{2}$	$q(q^2+1)$
A_{21}	$\frac{(1+q)^2}{2} + q\tilde{\varepsilon}'$	$\frac{q(1+q)}{2} + q^2\tilde{\varepsilon}'$	q
A_{31}	$\frac{1+q}{2}$	q	q
A_{32}	$\frac{1+q}{2}$		q
A_{41}	$-\tilde{\varepsilon}$		
$B_1(i)$			
$B_2(i)$			1
$B_3(i,j)$	$(-1)^i + (-1)^j$	$(-1)^i + (-1)^j$	$2(-1)^{i+j}$
$B_4(i,j)$			$2(-1)^{i+j+1}$
$B_5(i)$	$(-1)^j$	$(-1)^{j+1}$	
$B_6(i)$			$q-1$
$B_7(i)$			-1
$B_8(i)$	$(-1)^i(1+q)$	$(-1)^i(1+q)$	$q+1$
$B_9(i)$	$(-1)^i$	$(-1)^i$	1
$C_1(i)$	$\frac{1+q}{2}$	$-\frac{1+q}{2}$	
$C_{21}(i)$	$-\tilde{\varepsilon}'$	$\tilde{\varepsilon}'$	$(-1)^{i+1}$
$C_3(i)$	$(-1)^i + \frac{1-q}{2}$	$q(-1)^i + \frac{1-q}{2}$	$(-1)^i(q+1)$
$C_{41}(i)$	$(1)^i - \tilde{\varepsilon}'$	$-\tilde{\varepsilon}$	$(-1)^i$
D_1	$1+q$	$q(1+q)$	q^2+1
D_{21}	$(1+q) + q\tilde{\varepsilon}'$	$\frac{1+q}{2} + \tilde{\varepsilon}'$	1
D_{31}	1	$\tilde{\varepsilon}' - \tilde{\varepsilon}$	-1
D_{32}	1		1

Table 3.4 continued:

Character	θ_1	θ_3	θ_9	θ_{10}	θ_{11}	θ_{12}	θ_{13}
A_1	$\frac{q^2(q^2+1)}{2}$	$\frac{q^2+1}{2}$	$\frac{q(q+1)^2}{2}$	$\frac{q(q-1)^2}{2}$	$\frac{q(q^2+1)}{2}$	$\frac{q(q^2+1)}{2}$	q^4
A_{21}	$-q^2\tilde{\varepsilon}$	$\frac{q+1}{2}+q\tilde{\varepsilon}$	$\frac{q(q+1)}{2}$	$\frac{q(q-1)}{2}$	$\frac{q(q-1)}{2}$	$\frac{q(q-1)}{2}$	
A_{31}		$\frac{q+1}{2}$	q		q		
A_{32}		$\frac{1-q}{2}$		q		q	
A_{41}		$-\tilde{\varepsilon}'$					
$B_1(i)$			-1	1			1
$B_2(i)$	$(-1)^{i+1}$	$(-1)^i$			1	-1	-1
$B_3(i,j)$	$(-1)^{i+j}$	$(-1)^{i+j}$	2		1	1	1
$B_4(i,j)$	$(-1)^{i+j}$	$(-1)^{i+j}$		-2	-1	-1	1
$B_5(i,j)$					-1	1	-1
$B_6(i)$	$-q$	1		$q-1$	q	-1	$-q$
$B_7(i)$		1		-1		-1	
$B_8(i)$	q	1	$q+1$		1	q	q
$B_9(i)$		1	1		1		
$C_1(i)$	$\frac{(-1)^i(1-q)}{2}$	$\frac{(-1)^i(1-q)}{2}$		$q-1$	-1	q	$-q$
$C_{21}(i)$	$(-1)^{i+1}\tilde{\varepsilon}$	$(-1)^{i+1}\tilde{\varepsilon}$		-1	-1		
$C_3(i)$	$\frac{(-1)^i(q+1)}{2}$	$\frac{(-1)^i(q+1)}{2}$	$q+1$		q	1	q
$C_{41}(i)$	$(-1)^{i+1}\tilde{\varepsilon}$	$(-1)^{i+1}\tilde{\varepsilon}'$	1			1	
D_1	q	q	$\frac{(q+1)^2}{2}$	$-\frac{(1-q)^2}{2}$	$\frac{(q^2-1)}{2}+q$	$\frac{1+2q-q^2}{2}$	q^2
D_{21}	$-q\tilde{\varepsilon}$	$\tilde{\varepsilon}+\frac{q+1}{2}$	$\frac{q+1}{2}$	$\frac{q-1}{2}$	$\frac{q-1}{2}$	$\frac{q+1}{2}$	
D_{31}		$-\tilde{\varepsilon}'+\tilde{\varepsilon}$	$\frac{q-1}{2}$	$\frac{1-q}{2}$	$-\frac{q+1}{2}$	$\frac{1-q}{2}$	
D_{32}			$\frac{q+1}{2}$	$-\frac{q+1}{2}$	$\frac{q-1}{2}$	$\frac{q+1}{2}$	

Table 3.5: Character Table of $PSp_4(q)$, $q = 4k+3$

Character	$\xi_{21}(k)$	$\xi'_{21}(k)$	$\xi_{41}(k)$	$\xi'_{41}(k)$	Φ_1	Φ_3	Φ_9	θ_1	θ_3	θ_{10}
irreducible	$k\in T_2$ k odd	$k\in T_2$ k odd	$k\in T_1$ k even	$k\in T_1$ k odd						
D_1	q^2-1	$(1-q)^2$	$-(1+q)^2$	$(1-q)^2$	$1-q$	$1-q$	$-(q^2+1)$	$-q$	$-q$	$-\frac{(1-q)^2}{2}$
D_{21}	$-\frac{1+q}{2}+(1-q)\tilde{\varepsilon}$	$\frac{1-q}{2}-(1-q)\tilde{\varepsilon}$	$-\frac{1+q}{2}+(1+q)\tilde{\varepsilon}$	$\frac{1-q}{2}-(1+q)\tilde{\varepsilon}$	$(1-q)-q\tilde{\varepsilon}'$	$-\frac{1-q}{2}-\tilde{\varepsilon}'$	-1	$q\tilde{\varepsilon}$	$-\tilde{\varepsilon}-\frac{q+1}{2}$	$\frac{q-1}{2}$
D_{31}	$2\tilde{\varepsilon}$	$-2\tilde{\varepsilon}$	$2\tilde{\varepsilon}$	$-2\tilde{\varepsilon}$	1	$\tilde{\varepsilon}'-\tilde{\varepsilon}$	-1		$\tilde{\varepsilon}'-\tilde{\varepsilon}$	$\frac{q-1}{2}$
D_{32}	$\tilde{\varepsilon}+\tilde{\varepsilon}'$	$-\tilde{\varepsilon}-\tilde{\varepsilon}'$	$\tilde{\varepsilon}+\tilde{\varepsilon}'$	$-\tilde{\varepsilon}-\tilde{\varepsilon}'$	1		-1			$-\frac{q+1}{2}$

Table 3.5 provides a few cases where the table for $q = 4k+3$ differs from that for $q = 4k+1$.

Remark 3.5.5. *Tables 3.4 and 3.5 together provide the character table of $PSp_4(q)$ for q an odd prime power.*

3.6 Irreducible characters of $PSp_4(q)$

In this section, we discuss the irreducible characters of $PSp_4(q)$, where q is an odd prime power. Suppose that we let the following represent the irreducible characters of $Sp_4(q)$:

$$\delta = \begin{bmatrix} \gamma^{-1} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \gamma^{-1} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then $\delta J \delta^T = \gamma^{-1} J$, where J is defined in section 3.4, so $\delta \in Z(Sp_4(q))$. All diagonal automorphisms of $Sp_4(q)$ are induced by conjugation by powers of δ. For $A \in Sp_4(q)$, $A^{\delta^2} = \imath^{-1} A \imath$, where:

$$\imath = \begin{bmatrix} \gamma^{-1} & 0 & 0 & 0 \\ 0 & \gamma & 0 & 0 \\ 0 & 0 & \gamma^{-1} & 0 \\ 0 & 0 & 0 & \gamma \end{bmatrix}.$$

But $\imath \in Sp_4(q)$ such that $\bar{\imath} \in PSp_4(q)$. Therefore, conjugation by δ^2 is an inner automorphism of $PSp_4(q)$. Thus, modulo inner automorphisms, conjugation by δ is of order 2. The element α can be expressed as a composition of diagonal and field automorphisms, given by $\alpha = \phi^k \delta^t$, where $0 \leq k \leq n-1$ and $t = 0$ or $t = 1$.

Observe that the conjugacy class representatives A_{21} and A_{22}, satisfy $(A_{21})^\delta = A_{22}$ and $(A_{22})^\delta = A_{21}^\imath$. Since $\bar{\imath} \in PSp_4(q)$, δ interchanges the conjugacy classes A_{21} and A_{22}. For q odd, γ^{p^k} is not a square, so the field automorphisms ϕ^k leave A_{21} and A_{22} fixed. Again, by examining the pairs of conjugacy classes A_{41} and A_{42}, C_{21} and C_{22}, and D_{21} and D_{22}, we find that δ interchanges the classes in each pair, while the remain classes are fixed under field automorphisms. If $\alpha = \phi^k \delta$ where $0 \leq k \leq n-1$, then α does not fix the conjugacy classes $A_{21}, A_{22}, A_{41}, A_{42}, C_{21}, C_{22}, D_{21}$ and D_{22}.

By examining the character table of $PSp_4(q)$, we see that it contains characters θ_1 and θ_2 which are not fixed by α and must fuse in $Sp_4(q)$. In particular, the stabilizer of θ_1 is $PSp_4(q) < \phi >$. Hence, $I_G(\theta_1)/PSp_4(q)$ is cyclic of order n. In [53], θ_1 extends to $I_G(\theta_1)$ and then induces irreducibly to $Sp_4(q)$. Since $Sp_4(q)$ contains α, it follows that $Sp_4(q) \neq I_G(\theta_1)$. Let $\psi \in Irr(G)$ such that $[\psi_{PSp_4(q)}, \theta_1] > 0$. Then $\psi(1) = r\theta_1(1)$ where $r > 1$ and $r | 2n$. However, θ_1 has degree $\frac{q^2(1+q^2)}{2}$, and no proper multiple of

$\theta_1(1)$ is a degree of $Sp_4(q)$. Hence, we reach a contradiction. Thus, $\alpha = \phi^k$ where $1 \leq k \leq n-1$.

Consider the conjugacy class $B_6(1)$ of $PSp_4(q)$. We claim that $B_6(1)$ is moved by α. A class representative:

$$B_6(i) = \begin{bmatrix} \eta^i & 0 & 0 & 0 \\ 0 & \eta^{-i} & 0 & 0 \\ 0 & 0 & \eta^i & 0 \\ 0 & 0 & 0 & \eta^{-i} \end{bmatrix}, \quad i \in T_2.$$

Hence, if $i = 1$, we have:

$$B_6(1) = \begin{bmatrix} \eta^1 & 0 & 0 & 0 \\ 0 & \eta^{-1} & 0 & 0 \\ 0 & 0 & \eta^1 & 0 \\ 0 & 0 & 0 & \eta^{-1} \end{bmatrix}.$$

Observe:

$$(B_6(1))^{\phi^k} = \begin{bmatrix} \eta^1 & 0 & 0 & 0 \\ 0 & \eta^{-1} & 0 & 0 \\ 0 & 0 & \eta^1 & 0 \\ 0 & 0 & 0 & \eta^{-1} \end{bmatrix}^{\phi^k} = \begin{bmatrix} \eta^{p^k} & 0 & 0 & 0 \\ 0 & \eta^{-p^k} & 0 & 0 \\ 0 & 0 & \eta^{p^k} & 0 \\ 0 & 0 & 0 & \eta^{-p^k} \end{bmatrix}.$$

If $B_6(1)$ is fixed by α, then $1 \equiv \pm p^k \, mod(q+1)$. For $q = p^n$, this implies that $p^n + 1 \,|\, p^k + 1$ or $p^n + 1 \,|\, p^k - 1$. Since $n > k$, it follows that $p^n + 1 > p^k \pm 1$. Hence, $p^n + 1 \nmid p^k \pm 1$. Therefore, $B_6(1)$ is moved by α to another class of the form $B_6(i)$, where $i \neq 1$.

By [53], the irreducible character $\chi_2(2)$ is not fixed by α^{-1}. On the class $B_6(1)$, this character has value $(1+q)\beta_2$, where $\beta_i = \eta^i + \eta^{-i}$. If $\chi_2(2) = \chi_2(2)^{\alpha^{-1}}$, then:

$$\begin{aligned} (\chi_2(2))^{\alpha^{-1}}(B_6(1)) &= \chi_2(2)((B_6(1))^{\phi^k}) \\ &= \chi_2(2)(B_6(i)) \quad \text{for some } i \neq 1 \\ &= (1+q)\beta_{2i} \\ &= (1+q)(\eta^{2i} + \eta^{-2i}), \end{aligned}$$

this implies that,

$$(1+q)(\eta^2+\eta^{-2}) = (1+q)(\eta^{2i}+\eta^{-2i}).$$

Hence,

$$\eta^2+\eta^{-2} = \eta^{2i}+\eta^{-2i}$$

implies $p^n+1 \,|\, 2(p^k+1)$ or $p^n+1 \,|\, 2(p^k-1)$. Thus, $p^n+1 \leq 2(p^k+1) \leq 2p^{n-1}+2$. Hence, we have:

$$p^n - 2p^{n-1} \leq 1$$

which leads to $p^{n-1}(p-2) \leq 1$. However, if $p \geq 3$ and $n \geq 2$, then $p^{n-1}(p-2) \geq p \geq 3$, resulting in a contradiction. Therefore, $\chi_2(2)$ is not fixed by α^{-1}.

Now, δ, the diagonal automorphism of $PSp_4(q)$, fixes the conjugacy classes on which $\chi_2(2)$ is non-zero. In particular, the stabilizer of $\chi_2(2)$ is $PSp_4(q) < \delta >$, where δ is the diagonal automorphism. Hence, $I_G(\chi_2(2))/PSp_4(q)$ is cyclic of order 2.

By [50, 51], $\chi_2(2)$ extends to $I_G(\chi_2(2))$ and then induces irreducibly to $Sp_4(q)$. Since $Sp_4(q)$ contains α, it follows that $Sp_4(q) \neq I_G(\chi_2(2))$.

Let $\chi \in Irr(G)$ such that $[\psi_{PSp_4(q)}, \chi_2(2)] > 0$. Then $\psi(1) = r\chi_2(1)$, where $r > 1$ and $r \,|\, 2n$ since $|Out(PSp_4(q))| = 2n$. However, $\chi_2(2)$ has degree q^4-1, and no proper multiple of $\chi_2(1)$ is a degree of $Sp_4(q)$. Hence, this leads to a contradiction.

Therefore, $Sp_4(q) = PSp_4(q) \times C_{S_{p_4(q)}}(PSp_4(q))$.

The following are the permutation character degrees of $PSp_4(q)$ [50, 51], denoted by $cd(PSp_4(q))$. For further details refer to [53].

Theorem 3.6.1. *Let $G = PSp(4,q)$. If q is even, then the set $cd(G)$ of character degrees of G is given as:*

$$\{1, \frac{q(q^2+1)}{2}, \frac{q(q+1)^2}{2}, q^4, \frac{q(q^2-1)}{2}, q^4-1, (q-1)^2(q^2+1), (q^2-1)^2,$$
$$(q+1)(q^2+1), (q-1)(q^2+1), q(q+1)(q^2+1), q(q-1)(q^2+1), (q+1)^2(q^2+1)\},$$

where the last degree appears only for $q > 4$. If q is odd and $q > 7$, we have the following additional degrees:

$$\{\frac{(q^4-1)}{2}, q(q^2+1), \frac{(q^2+1)}{2}, \frac{q^2(q^2+1)}{2}, \frac{(q-1)^2(q^2+1)}{2},$$
$$(q-1)^2(q^2+1), \frac{(q+1)^2(q^2+1)}{2}, \frac{(q+\epsilon)(q^2+1)}{2}, \frac{q(q+\epsilon)(q^2+1)}{2}\}$$

where $\epsilon = (-1)^{\frac{q-1}{2}}$.

3.7 Maximal subgroups

In this section, we present the maximal subgroups of the projective symplectic group $PSp_{2m}(q)$. We then use the primitive permutation representation of the group $PSp_4(q)$ to construct symmetric 1-designs. First, we provide some exceptional isomorphisms and discuss the Klein quadric to extend our understanding of $PSp_4(q)$.

3.7.1 Klein quadric and exceptional isomorphisms

In this subsection, we discuss the Klein quadric and exceptional isomorphisms, and we also refer the reader to [29].

In the Grassmannian of lines, lines in $PG(3,q)$ are represented as points in $PG(5,q)$. This representation can be explicitly given using Plücker coordinates. By choosing two points on a given line, the values $P_{ij} = x_iy_j - x_jy_i$ can be calculated. These points lie on the quadratic K defined by $X_0X_5 + X_1X_4 + X_2X_3 = 0$. The fundamental property of this representation is that two lines intersect if and only if their corresponding points lie on a line on K. A plane on K corresponds to either the set of lines passing through a point or the set of lines lying on a plane in $PG(3,q)$. There are two families of planes on K, where planes within a family are either equal or meet at a point, and planes from different families are either disjoint or meet in a line. A line on K corresponds to the set of lines lying on a plane and passing through a common point.

The Plücker coordinate construction in $PG(3,q)$ corresponds to points of K in a non-isotropic hyperplane in $PG(5,q)$. This leads to an isomorphism between $PSp_4(q)$ and $P(5,q)$ for odd q. When q is an odd number in the context of $PG(3,q)$, a regulus R is considered along with its opposite regulus $R^\perp$. The lines in R correspond to $q+1$ points on K that are not orthogonal to each other, but are all orthogonal to the $q+1$ points corresponding to the lines in R'. As a result, R and R' determine orthogonal and non-degenerate planes π and π' of $PG(5,q)$.

Assume that P is the point in $PG(3,q)\backslash K$, where $P^\perp$ is the hyperplane. Then $T_4 = P^\perp \cap K$ represents a parabolic quadric. The set of lines in $PG(3,q)$ that correspond to the points of T_4 polar to a point of T_4 is known as a parabolic congruence. We consider a point $R \notin K$ such that PR is non-isotropic. Two non-polar points of K that are not in T_4 can be found on PR if it is a secant line. The points of $T_4 \cap R^\perp$ are polar to both points of PR, and corresponding lines in $PG(3,q)$ form a hyperbolic congruence.

These lines correspond to polar non-isotropic lines in $PG(3,q)$.
If ℓ is a secant line in $P^\perp$, then $\ell^\perp \cap Q_4$ consist of $q+1$ points of a conic, each polar to the two points of Q_4 lying in ℓ. Thus, they correspond to $q+1$ self-polar lines of $PG(3,q)$; each meeting a pair of skew self-polar lines. The $q+3$ lines described all lies on a quadric in $PG(3,q)$. If ℓ is an external line in $P^\perp$, then $\ell^\perp \cap Q_4$ again consists of $q+1$ points of a conic, but these are no longer polar to a pair of points in Q_4. However, if we work over $GF(q^2)$, it would be possible to see these points as corresponding to lines on a quadric in $PG(3,q^2)$, such that in a certain sense, in which the stabilizer in $PSp_4(q)$ of this set of lines stabilizes a quadric.

Theorem 3.7.1. [29] *Assume that $p > 2$. The maximal subgroups of $PSp_4(q)$, up to conjugation, are as follows:*

1. *$PSp_4(q_0)$, where q is an odd prime power of q_0;*
2. *$PGSp_4(q_0)$, where $q = q_0^2$;*
3. *The stabilizer of a point and plane, having index q^3+q^2+q+1 (one class, say M_1 for both odd and even q);*
4. *The stabilizer of a parabolic congruence, having index q^3+q^2+q+1 (one class, say M_2 for both odd and even q);*
5. *The stabilizer of a hyperbolic congruence, having index $\frac{q^2(q^2+1)}{2}$ (one class for q odd and two classes for q even where $q > 2$, say M_3 and M_3');*
6. *The stabilizer of a elliptic congruence, having index $\frac{q^2(q^2-1)}{2}$ (one class for q odd and two classes for q even where $q > 2$, say M_4 and M_4');*
7. *The stabilizer of a quadratic congruence, having index $\frac{q^3(q^2+1)(q+1)}{2}$, (for $q > 3$) (one class, say M_5 for both odd and even q);*
8. *The stabilizer of a quadratic congruence, having index $\frac{q^3(q^2+1)(q-1)}{2}$, (for $q > 3$) (one class, say M_6 for both odd and even q);*
9. *The stabilizer of a twisted cubic, having index $q^3(q^4-1)$, (for $q > 3$, $q > 7$) (one class, say M_7 for both odd and even q);*

10. *groups of orders* 1920 *(for* $q \equiv \pm 1 (mod\, 8)$ *and prime),* 960 *(for* $q \equiv \pm 3 (mod\, 8)$ *and prime),* 920 *(for* $q \equiv \pm 1 (mod\, 12)$ *and prime),* 360 *(for* $q \equiv \pm 5 (mod\, 12)$ *and* $\neq 7$ *prime) and* 5520 *(for* $q = 7$*).*

3.7.2 Structures of maximal subgroups

In this subsection, we discuss the structures of some maximal subgroups of $PSp_4(q)$.

Stabilizer of points and plane maximal subgroup M_1 and Finite projective plane $PG_n(q)$

In this subsubsection, we discuss the structures of the stabilizers of points and the maximal subgroups of the plane, as well as the structure of the finite projective plane $PG_n(q)$.

Definition 3.7.2. [44] *A projective plane is a structure* $\mathcal{P} = (P, L, I)$*, where* P *is a set of points,* L *is a set of lines and* I *is a relation between points and lines called incident. If* $p \in P$ *and* $\ell \in L$*, the notation* $p \in \ell$ *means that point* p *is on line* ℓ*. The structure satisfies the following axioms:*

(i) Any two points lie on a unique line;

(ii) Any two lines intersect in a unique point;

(iii) There exist four points, no three on a line;

(iv) There exist four lines, no three through a common point.

Definition 3.7.3. *A homogeneous polynomial of degree* 1 *in* $\mathbb{P} = [X, Y, Z]$ *is of the form* $aX + bY + cZ$*, where at least one of* $a, b,$ *or* c *is non-zero. The zero set of such a polynomial is a projective line.*

Theorem 3.7.4. [3] *If* L_1 *and* L_2 *are distinct projective lines, then* $|L_1 \cap L_2| = 1$.

Remark 3.7.5. *All lines in the projective plane intersect with one another.*

Theorem 3.7.6. [3] *Let* $PG_3(q)$ *be a projective plane of dimension* 3*. Then:*

(i) If $p_1, p_2 \in PG_3(q)$ *are distinct points, then there is a unique line* L *with* p_1 *and* p_2 *lie on in* L*;*

(ii) *Let L_i be the line defined by the homogeneous equation $a_iX + b_iY + c_iZ = 0$ for $i = 1, 2$. Then the lines $L_1 = L_2$ are the same if and only if the coefficient (a_1, b_1, c_1) and (a_2, b_2, c_2) are proportional, denoted $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$;*

(iii) *Let $L_{a,b,c}$ be the line with the equation $aX+bY+cZ = 0$. The map $[a, b, c] \mapsto L_{a,b,c}$ establishes a bijective between the lines of $PG_3(q)$ and the points in the projective plane $PG_2(q)$, provided that not all of a, b, c are zero.*

Theorem 3.7.7. [44] *In a finite projective plane of order n:*

(i) *every line is incident with $n + 1$ points;*

(ii) *every point is incident with $n + 1$ lines;*

(iii) *there are $n^2 + n + 1$ points in P;*

(iv) *there are $n^2 + n + 1$ lines in L.*

Lines in $PG_3(q)$

Points in $PG_3(q)$ correspond to projective equivalence classes of non-zero vectors in $\mathbb{R}^4$. Specifically, the point in $PG_3(q)$ with homogeneous coordinates $[X : Y : Z : W]$ represents the line $[\mathbf{v}]$ spanned by the non-zero vector,

$$\mathbf{v} = \begin{bmatrix} X \\ Y \\ Z \\ W \end{bmatrix} \in \mathbb{R}^4.$$

Similarly, planes in $PG_3(q)$ correspond to projective equivalence classes of covectors:

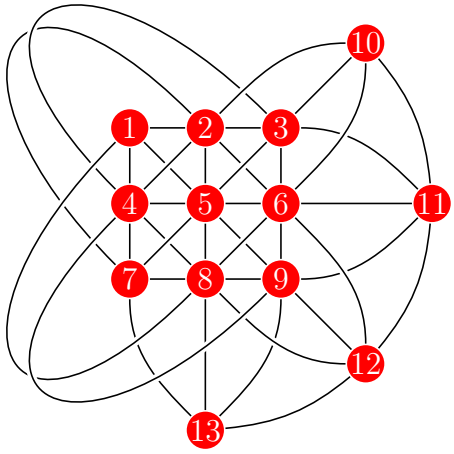
$$\phi : [a\ b\ c\ d] \in (\mathbb{R}^4)^*.$$

Where $[\phi] = [a : b : c : d]$ is the hyperplane defined in homogenous coordinates by $\phi(\mathbf{v}) = 0$, specifically given by the equation:

$$aX + bY + cZ + dW = 0. \tag{3.11}$$

We say that the point $[X : Y : Z : W]$ lies on the plane $[a : b : c : d]$ if and only if equation (3.11) is satisfied. Thus, lines and planes in $PG_3(q)$ are defined in

Figure 3.1: $PG_3(3)$



homogeneous coordinates by vectors in the vector space $V = \mathbb{R}^4$ and covectors in its dual vector space $V^* = (\mathbb{R})^*$. Moreover, the orthogonal complement $v^\perp$ of the line $\mathbb{R}v \in \mathbb{R}^4$ is the hyperplane in $\mathbb{R}^4$ defined by covector v^T, which is the transpose of v.

Example 3.7.8. *Projective space of dimension* 3 *over the finite field of order* 3*, denoted* $PG_3(3)$*, is illustrated in Figure* 3.1.

Stabilizer of parabolic maximal subgroup M_2

In this subsection, we discuss the structure of the stabilizer of a parabolic maximal subgroup.

Theorem 3.7.9. [55] *The stabilizer of totally isotropic subspaces is a parabolic maximal subgroup.*

Proof. Suppose that W is the stabilizer of $W^\perp$ and $W \cap W^\perp$. There is two cases: either $W \cap W^\perp = 0$ or $W \cap W^\perp = W$. This implies that W is a non-singular subspace or a totally isotropic subspace.
If the stabilizer of an isotropic subspace W of dimension k preserves the flag:

$$0 < W < W^\perp < V,$$

then $W^{\perp}/W$ induce a non-singular form. By Witt's lemma, we can choose a symplectic basis that spans W as $e_1, \cdots, e_k$ and $e_1, \cdots, e_m, f_{k+1}, \cdots, f_m$ that spans $W^{\perp}$, such that the basis for $W^{\perp}/W$ consists of the images of $e_{k+1}, \cdots, e_m, f_{k+1}, \cdots, f_m$.
Since the quotient group $Sp_{2m-2k}(q)$ acts on $W^{\perp}/W$, the a group $GL_k(q)$ also acts on W. This induce a dual action on $V/W^{\perp}$. A p-group of lower triangular matrices is generated by the following elements:

$$\begin{aligned} x_{ij} : f_i &\mapsto f_i + \lambda f_j \\ : e_j &\mapsto e_j - \lambda e_i \\ y_{ij} : f_i &\mapsto f_i + \lambda e_j \\ : f_j &\mapsto f_j + \lambda e_i \end{aligned}$$

By considering B to be the stabilizer of a maximal flag of shape:

$$0 < W_1 < \cdots < W_m = (W_m)^{\perp} = (W_{m-1})^{\perp} = (W_1)^{\perp} = V,$$

let $W_k = \langle e_1, \cdots, e_k \rangle$ and $e_1, \cdots, e_k,\ f_m, \cdots, f_1$ form a flag structure such that for all $i < j \leq m$ and for all $\lambda \in \mathbb{F}_q$. Define the maps on x_{ij} and y_{ij} that fix the basis except for e_k and f_k.
Then, a unitriangular subgroup U is generated by this map together with symplectic transvection given by:

$$T_{e_i}(-\lambda) : f_i \mapsto f_i + \lambda e_i,$$

such that $|U| = q^{m^2}$ and U is a Sylow p-subgroup.
Therefore, x_{ij} and y_{ij} generate a non-abelian group A such that $Z(A) = \Phi(A) = A'$, where $\Phi(A)$ denotes the Frattini subgroup, which is an elementary abelian group of order $q^{\frac{k(k+1)}{2}}$ and A/A' is an abelian group of order $q^{2k(m-k)}$.
The full stabilizer is of the shape:

$$q^{\frac{k(k+1)}{2}} \cdot q^{2k(m-k)} : (Sp_{2m-2k}(q) \times GL_k(q))$$

In the case $m = k$, we have:

$$q^{\frac{m(m+1)}{2}} : GL_m(q).$$

□

Remark 3.7.10. *These stabilizers are the maximal parabolic subgroups. In the Dynkin diagram, the k^{th} node of the diagram C_m corresponds to a totally isotropic k-dimension subspace. By deleting this node, we obtain the Levi complement $Sp_{2m-2k}(q) \times GL_k(q)$ of the subspace stabilizer.*

Proposition 3.7.11. *For $q = 3$, $|PSp_4(3)| = 25920 = 2^6.3^4.5$, which has 5 maximal subgroups.*

1. *The stabilizer of a point and plane, having index (length)* 40*;*
2. *The stabilizer of a parabolic congruence, having index (length)* 40*;*
3. *The stabilizer of a hyperbolic congruence, having index (length)* 45*;*
4. *The stabilizer of a elliptic congruence (structure: S_6), having index (length)* 36*;*
5. *Symplectic type with $M = (C_2)^4{:}A_5$, having index (length)* 27*.*

Number of points	*Suborbits*	*Rank*	*Point stabiliser*
27	*1, 10, 16*	3	$2^4 : A_5$
36	*1, 15, 20*	3	S_6
40	*1, 12, 27*	3	$3^{1+2} : 2A_4$
40	*1, 12, 27*	3	$3^3 : S_4$
45	*1, 12, 32*	3	$2.(A_4 \times A_4).2$

Proposition 3.7.12. *For $q = 5$, $|PSp_4(5)| = 4680000 = 2^6.3^2.5^4.13$, which has 8 maximal subgroups.*

1. *The stabilizer of a point and plane, having index (length)* 156*;*
2. *The stabilizer of a parabolic congruence, having index (length)* 156*;*
3. *The stabilizer of a hyperbolic congruence (order 1440), having index (length)* 325*;*
4. *The stabilizer of a elliptic congruence (order 15600), having index (length)* 300*;*
5. *Order* 360 *($q \equiv \pm 5\,(mod 12) \cong A_6$);*
6. *Order* 720 *(structure: $M = S_5 \times S_3$), length* 6500*;*

7. *Order* 480 *(structure:* $M = C_2 \times C_2 \times A_5{:}C_2$*), length* 9750*;*

8. *Order* 960 *(*$q \equiv \pm -3(mod 8)$*) length* 9750*.*

Number of points	*Suborbits*	*Rank*
156	*1, 30, 125*	3
156	*1, 30, 125*	3
300	*1, 65, 104, 130*	4
325	*1, 60, 120, 144*	4

Proposition 3.7.13. *For* $q = 7$, $|PSp_4(7)| = 138297600 = 2^8.3^2.5^2.7^4$, *which has* 9 *maximal subgroups.*

Number of points	*Suborbits*	*Rank*
400	*1, 56, 343*	3
400	*1, 56, 343*	3
1176	*1, 175, 300,* 350^2	5
1225	*1, 168,* 336^2*, 384*	5

Stabilizer of hyperbolic maximal subgroup M_3

In this subsection, we discuss the structure of the stabilizer of a hyperbolic maximal subgroup.

Let:

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

Definition 3.7.14. *The projective symplectic group* $PSp_4(q)$ *is the group of all* 4×4 *matrices* A *with coefficients in* $\mathbb{F}_q$ *such that* $A^T JA = J$*, where* A^T *denotes the transpose of* A *and* J *is a symplectic form. Let* M_3 *be the hyperbolic subgroup, which is the centralizer of the involution in* $PSp_4(q)$*.*

$$t = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix},$$

where I is the identity matrix of degree n. If M_3 is a maximal subgroup, it consists of all elements of the form,

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \text{ or } \begin{pmatrix} 0 & A \\ B & 0 \end{pmatrix},$$

where A and B are isomorphic to $SL_2(q)$. Setting,

$$L_1 = \{\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} | A = \begin{pmatrix} a & 0 \\ 0 & I \end{pmatrix} \cong SL_2(q)\}, \quad L_2 = \{\begin{pmatrix} I & 0 \\ 0 & B \end{pmatrix} | B = \begin{pmatrix} I & 0 \\ 0 & b \end{pmatrix} \cong SL_2(q)\}$$

$$u = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix},$$

$$L_1 L_2 = \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

Remark 3.7.15. *Let L_1 and L_2 be isomorphic to $SL_2(q)$. The elements of L_1 commute with the elements of L_2, such that $L_1 \cap L_2 =< t >$, $M_3 = L_1 L_2 < u >$, where $u^2 = 1$ and $L_1^u = L_2$. The center of M_3 is $Z =< t >$, which has order 2.*

Theorem 3.7.16. [56] *Let M_3 be a hyperbolic subgroup of $PSp_4(q)$. According to the Jordan-Hölder theorem, there are two composition series:*

$$1 \trianglelefteq Z \trianglelefteq L_1 \trianglelefteq H \trianglelefteq M_3,$$

$$1 \trianglelefteq Z \trianglelefteq L_2 \trianglelefteq H \trianglelefteq M_3,$$

1. *$H = N_{M_3(L_1)} = N_{M_3(L_2)}$, where $[M_3 : H] = 2$.*
2. *$H/L_1 \cong H/L_2 \cong PSL_2(q) \Rightarrow L_1 (or\ L_2) \trianglelefteq H$.*
3. *$L_1/Z \cong L_2/Z \cong PSL_2(q) \Rightarrow Z \trianglelefteq L_1 (or\ L_2)$.*
4. *$L_1 L_2 = H$, where $L_1 \cap L_2 = Z =< t >$.*
5. *$M_3 = H < u >$, where $|H| = \frac{L_1 L_2}{L_1 \cap L_2} = \frac{|M_3|}{2}$.*

Theorem 3.7.17. [56] *Let M_3 be a hyperbolic subgroup of $PSp_4(q)$. Then:*

1. *$|M_3| = q^2(q^2 - 1)^2$.*

2. *$M_3 = L_1 L_2 < u >$, where L_1 and L_2 are subgroups of M_3 such that:*

$$L_1 \cap L_2 =< t >, \qquad [L_1, L_2] = 1,$$

u is an involution, and there are isomorphisms:

$$x \to x_1, \qquad x \to x_2,$$

of $SL_2(q)$ on L_1 and L_2, respectively, such that:

$$x_1^u = x_2 \qquad \text{for all } x \in SL_2 q.$$

3. *If $a, b \in SL_2(q)$, then*

$$S =< a_1, b_1, a_2, b_2, u >,$$

is a $Syl_2(q)$ of C, $S = 2^{2n+1}$.

4. *$Z(M_3) = Z(S) =< t >$.*

5. *All involutions of $L_1, L_2 \backslash < t >$ are conjugate in M_3. All involutions of $M_3 \backslash L_1 L_2$ are conjugate in M_3 to u or tu.*

Lemma 3.7.18. [56] *The involutions of L_1 and $L_2 \backslash < t >$ are not conjugate in $PSp_4(q)$ to t.*

Chapter 4

Main results

In this chapter, we provide the design parameters obtained using Method 1 and Method 2, along with the corresponding codes for some maximal subgroups and conjugacy classes of $PSp_4(q)$.
Our goal is to determine the parameters of the designs and codes that remain invariant under the simple group G with respect to the maximal subgroups of $PSp_4(q)$. Moreover, we will apply the two methods discussed earlier, beginning with Method 1.

4.1 Designs from Method 1

In Method 1, we will use the primitive permutation representation of the $PSp_4(q)$ group to construct symmetric 1-designs.

Definition 4.1.1. [28] *The symplectic group $PSp_{2m}(q)$, where $m \geq 2$ and q is any prime power, acts as a primitive rank-3 group of degree $\frac{q^{2m}-1}{q-1}$ on the points of the projective $(2m-1)$-space $PG_{2m-1}(\mathbb{F}_q)$. The orbits of the stabilizer on points P consist of the single point $\{P\}$ one orbit of length $\frac{q^{2m-1}-1}{q-1}-1$ and another of length q^{2m-1}. The points P, together with the points from the orbit of length $\frac{q^{2m-1}-1}{q-1}-1$, form a hyperplane. In fact, the image of the absolute point P under the symplectic polarity is this hyperplane.*

Theorem 4.1.2. [19] *Let G be a transitive rank-3 permutation group such that the orbit lengths for the stabilizer G_α of a point α are 1, $q(q+1)$, and q^3, where $q > 2$. Suppose that G_α is not faithful on its orbit. Then:*

(i) There are at least q elements of G fixing a G_α-orbit of length $q(q+1)$ pointwise.

(ii) If $q = p^r$, where p is a prime and r is a power of 2, then G contains a normal subgroup isomorphic to $PSp_4(q)$. In particular, G is isomorphic to a group of symplectic collineations of projective 3-space over $\mathbb{F}_q$ contains all the symplectic elations.

Lemma 4.1.3. *If $W = W^\perp$ is a maximal isotropic subspace of dimension m, with a complement U that is also totally isotropic, then the stabiliser of the direct sum decomposition $V = W \oplus U$ is a maximal subgroup of $PSp_4(q)$. The order of this stabilizer is $q^3 + q^2 + q + 1$.*

Proof. Suppose that $W = W^\perp$ is a maximal isotropic subspace of dimension m. Choose a complement U that is also totally isotropic, such that the stabiliser of the direct sum decomposition $V = W \oplus U$ is $2{\cdot}GL_m(q)$. The elements that swap W and U induce the duality automorphism on $GL_m(q)$.
The stabilizer of the maximal parabolic subgroup for $PSp_4(q)$ is given by $q^3{:}GL_2(q)$.

$$\begin{aligned}|GL_m(q)| &= (q^m-1)(q^m-q)(q^m-q^2)\cdots(q^m-q^{m-1}) \\ &= q^{\frac{m(m-1)}{2}}(q-1)(q^2-1)\cdots(q^m-q^{m-1})\end{aligned}$$

For $m = 2$:

$$|GL_2(q)| = q(q-1)(q^2-1).$$

Let $|M|$ be defined as follows:

$$\begin{aligned}|M| = |q^3{:}2{\cdot}GL_2(q)| &= \frac{q(q-1)(q^2-1)}{2} \times q^3 \\ &= \frac{q^4(q-1)(q^2-1)}{2}.\end{aligned}$$

Now, we compute ratio:

$$\begin{aligned}\frac{|PSp_4(q)|}{|M|} &= \frac{\frac{q^4(q^4-1)(q^2-1)}{2}}{\frac{q^4(q-1)(q^2-1)}{2}} \\ &= \frac{q^4-1}{q-1} \ = (q+1)(q^2+1) \\ &= q^3+q^2+q+1\end{aligned}$$

□

Theorem 4.1.4. [40] *If the group G acts primitively on the points and blocks of a symmetric 1-design $\mathcal{D}$, then the design can be obtained by orbiting a union of orbits of a point-stabilizer.*

Proof. Let $\{M : |M \cap M^g|\}$ denote the sizes of the intersections of M with its conjugates in G.

$$
\begin{aligned}
|M \cap M^g| &\in \left\{1, \frac{q(q^{2m-2}-1)}{q-1}, q^{2m-1}\right\} \\
|M : |M \cap M^g|| &= \left\{\frac{|M|}{1}, \frac{|M|(q-1)}{q(q^{2m-2}-1)}, \frac{|M|}{q^{2m-1}}\right\} \\
\mathcal{A}_M &= \{|M \cap M^g| : g \in G\} \\
\frac{|M|}{n} &= \left\{\frac{|M|}{1}, \frac{|M|(q-1)}{q(q^{2m-2}-1)}, \frac{|M|}{q^{2m-1}}\right\}, \ n \in \mathcal{A}_M.
\end{aligned}
$$

If $m = 2$, then:

$$
\begin{aligned}
|M \cap M^g| &\in \left\{1, \frac{q(q^2-1)}{q-1}, q^3\right\} \\
&\in \left\{1, q(q+1), q^3\right\}
\end{aligned}
$$

□

Proposition 4.1.5. *Let M_1 and M_2 be defined in chapter 3. The parameters of designs constructed from $PSp_4(q)$ for all q by Method 1, with respect to M_1 and M_2 are as follows:*

1. $\mathcal{D}_1 = \left(\frac{q^4(q-1)^2(q+1)}{2}, \frac{q^3(q-1)^2}{2}, \frac{q^3(q-1)^2}{2}\right)$;
2. $\mathcal{D}_2 = \left(\frac{q^4(q-1)^2(q+1)}{2}, \frac{q^3(q-1)^2}{2}, \frac{q^3(q-1)^2}{2}\right)$;
3. $\mathcal{D}_3 = \left(\frac{q^4(q-1)^2(q+1)}{2}, \frac{q(q-1)^2(q+1)}{2}, \frac{q(q-1)^2(q+1)}{2}\right)$;
4. $\mathcal{D}_4 = \left(\frac{q^4(q-1)^2(q+1)}{2}, \frac{q(q-1)^2(q+1)}{2}, \frac{q(q-1)^2(q+1)}{2}\right)$.

Proof. We have M_1 and M_2 as maximal subgroups of $G = PSp_4(q)$, and $|G : M_1| = |G : M_2| = 1 + q + q^2 + q^3$. Our goal is to find the parameters of the designs invariant under the group G using Method 1.
Since the rank of G with respect to M_i $(i = 1, 2)$ is 3, the corresponding suborbits are $1, a_i, b_i$. Therefore, for each i, we can construct two non-trivial symmetric designs with parameters $1 - (v, a_i, a_i)$ and $1 - (v, b_i, b_i)$, where $v = 1 + q + q^2 + q^3$, and a_i, b_i are well-known according to the ATLAS.
See [28], Proposition 1, which suggests that a projective symplectic group $PSp_{2m}(q)$ acts as a primitive rank-3 group of degree $\frac{q^{2m}-1}{q-1}$. We have the designs $1-\left(\frac{q^{2m}-1}{q-1}, q^{2m-1}, q^{2m-1}\right)$ formed from the longer orbit of a point-stabilizer, and $1-\left(\frac{q^{2m}-1}{q-1}, \frac{q(q^{2m-2}-1)}{q-1}, \frac{q(q^{2m-2}-1)}{q-1}\right)$, which is formed from the other orbit. Therefore, when $m = 2$, the result follows. □

4.2 Designs from Method 2

In this section, we present the parameters of designs from $G = PSp_4(q)$ using Method 2, considering both maximal subgroups of index $q^3 + q^2 + q + 1$ and those with indices $\frac{q^2(q^2\pm1)}{2}$ for both even and odd prime powers of q.

4.2.1 Designs from subgroups of index $1 + q + q^2 + q^3$

In this section, we provide the parameters of designs from $G = PSp_4(q)$ using Method 2, with respect to maximal subgroups of index $q^3 + q^2 + q + 1$. These subgroups appear as two classes, denoted M_1 and M_2, under G for all q, as defined in chapter 3.

Theorem 4.2.1. *The parameters of designs from $G = PSp_4(q)$ using Method 2 with respect to M_1 and M_2 are fully provided in the following tables:*

1. *For even q, the parameters are provided fully in Table 4.1 and Table 4.2.*
2. *For odd q, the parameters are provided fully in Table 4.3 and Table 4.4, respectively.*

Proof. As in [29], let M_1 and M_2 be the stabilizers of rank-3 actions of G. By Theorem 1.5.39, we have $\chi_{M_i} = 1 + \psi_i + \chi_i$ (for $i = 1, 2$), where ψ_i and χ_i are irreducible characters of G and $\psi_1(1) + \psi_2(1) = q + q^2 + q^3$. According to the character table of

G, the group has a unique irreducible character θ_9 of degree $\frac{q(q+1)^2}{2}$ and exactly two irreducible characters θ_{11} and θ_{12}, both of degree $\frac{q(q^2+1)}{2}$. It is clear that

$$\theta_9 + \theta_{11} = \theta_9 + \theta_{12} = q + q^2 + q^3.$$

We claim that $1+\theta_9+\theta_{11}$ and $1+\theta_9+\theta_{12}$ are permutation characters of the rank-3 actions of G. In fact, a careful examination of the character degrees of G (Theorem 3.6.1) implies that there is no other possibility for the sum of the degrees of two irreducible characters of G to equal $q + q^2 + q^3$. Now, using the values of these two permutation characters given in Table **??**, we can determine the third parameters of each design. Notice that if $\chi_{M_i}(g) = 0$, then the conjugacy class of G does not intersect M_i (for $i = 1, 2$), so we exclude the conjugacy classes on which the permutation characters vanish. To find the second parameter of the design, we use Lemma 2.2.12. This completes the proof.

□

Table 4.1: Designs from G under M_1 (q even)

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_1}$
$\overline{A}_1$	1	1	$(q+1)(q^2+1)$
$\overline{A_{11}}$	$(q^2-1)(q^4-1)$	$(q^2-1)^2$	$q+1$
$\overline{A}_{21}$	q^4-1	$(q-1)(q^2+q+1)$	q^2+q+1
$\overline{A}_{22}$	q^4-1	q^2-1	$q+1$
$\overline{A}_{31}$	$q(q^4-1)(q+1)$	$q(q^2-1)(q+1)$	$q+1$
$\overline{A}_{32}$	$q(q^4-1)(q-1)$	$q(q^2-1)(q-1)$	$q+1$
$\overline{A}_{41}$	$q^2(q^4-1)(q^2-1)$	$q^2(q^2-1)(q-1)$	1
$\overline{A}_{42}$	$q^2(q^4-1)(q^2-1)$	$q^2(q^2-1)(q-1)$	1
$\overline{B}_2(i)$	$q^4(q^4-1)$	$2q^4(q-1)$	2
$\overline{B}_3(i,j)$	$q^4(q^2+1)(q+1)^2$	$4q^4(q+1)$	4
$\overline{B}_3(i,j)$	$q^4(q^2+1)(q+1)^2$	$4q^4(q+1)$	4
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^4(q-1)$	2
$\overline{B}_6(i)$	$q^3(q^2+1)(q-1)$	$q^3(q-1)$	$q+1$
$\overline{B}_8(i)$	$q^3(q^2+1)(q+1)$	$2q^3(q+1)$	$2(q+1)$
$\overline{B}_9(i)$	$q^3(q^4-1)(q+1)$	$2q^3(q^2-1)$	2
$\overline{C}_1(i)$	$q^3(q^2+1)(q-1)$	$q^3(q-1)$	$q+1$
$\overline{C}_{21}(i)$	$q^3(q^4-1)(q-1)$	$q^3(q-1)^2$	1
$\overline{C}_{22}(i)$	$q^3(q^4-1)(q-1)$	$q^3(q-1)^2$	1
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$q^3(q+3)$	$q+3$
$\overline{C}_{41}(i)$	$q^3(q^4-1)(q+1)$	$3q^3(q^2-1)$	3
$\overline{D}_1$	$q^2(q^2+1)$	$2q^2$	$2(q+1)$
$\overline{D}_{21}$	$q^2(q^2+1)(q^2-1)$	$q^2(q-1)(q+2)$	$q+2$
$\overline{D}_{22}$	$q^2(q^2+1)(q^2-1)$	$q^2(q-1)(q+2)$	$q+2$
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{2}$	$q^2(q-1)(q^2-1)$	1
$\overline{D}_{32}$	$\frac{q^2(q^4-1)(q^2-1)}{2}$	$\frac{q^2(q-1)(q^2-1)}{2}$	1
$\overline{D}_{34}$	$\frac{q^2(q^4-1)(q^2-1)}{4}$	$\frac{q^2(q-1)(q^2-1)}{2}$	2

Table 4.2: Designs from G under M_2 (q even)

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_2}$
$\overline{A}_1$	1	1	$(q+1)(q^2+1)$
$\overline{A_{11}}$	$(q^2-1)(q^4-1)$	$(q^2-1)^2$	$q+1$
$\overline{A}_{21}$	q^4-1	q^2-1	$q+1$
$\overline{A}_{22}$	q^4-1	q^2-1	$q+1$
$\overline{A}_{31}$	$q(q^4-1)(q+1)$	$q(q^2-1)(2q+1)$	$2q+1$
$\overline{A}_{32}$	$q(q^4-1)(q-1)$	$q(q-1)^2$	1
$\overline{A}_{41}$	$q^2(q^4-1)(q^2-1)$	$q^2(q^2-1)(q-1)$	1
$\overline{B}_2(i)$	$q^4(q^4-1)$	$2q^4(q-1)$	2
$\overline{B}_3(i,j)$	$q^4(q^2+1)(q+1)^2$	$4q^4(q+1)$	4
$\overline{B}_3(i,j)$	$q^4(q^2+1)(q+1)^2$	$4q^4(q+1)$	4
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^4(q-1)$	2
$\overline{B}_6(i)$	$q^3(q^2+1)(q-1)$	$q^3(q-1)$	$q+1$
$\overline{B}_7(i)$	$q^3(q^4-1)(q-1)$	$q^3(q-1)^2$	1
$\overline{B}_8(i)$	$q^3(q^2+1)(q+1)$	$q^3(q+3)$	$q+3$
$\overline{B}_8(i)$	$q^3(q^2+1)(q+1)$	$q^3(q+3)$	$q+3$
$\overline{B}_8(i)$	$q^3(q^2+1)(q+1)$	$2q^3(q+1)$	$2(q+1)$
$\overline{B}_9(i)$	$q^3(q^4-1)(q+1)$	$2q^3(q^2-1)$	2
$\overline{B}_9(i)$	$q^3(q^4-1)(q+1)$	$2q^3(q^2-1)$	2
$\overline{B}_9(i)$	$q^3(q^4-1)(q+1)$	$3q^3(q^2-1)$	3
$\overline{C}_{21}(i)$	$q^3(q^4-1)(q-1)$	$q^3(q-1)^2$	1
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$2q^3(q+1)$	$2(q+1)$
$\overline{C}_{41}(i)$	$q^3(q^4-1)(q+1)$	$2q^3(q^2-1)$	2
$\overline{D}_1$	$q^2(q^2+1)$	$q^2(q+1)$	$(q+1)^2$
$\overline{D}_{21}$	$q^2(q^2+1)(q^2-1)$	$q^2(q^2-1)$	$q+1$
$\overline{D}_{22}$	$q^2(q^2+1)(q^2-1)$	$q^2(q^2-1)$	$q+1$
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{2}$	$\frac{q^2(q-1)(q^2-1)}{2}$	1
$\overline{D}_{32}$	$\frac{q^2(q^4-1)(q^2-1)}{2}$	$\frac{q^2(q-1)(q^2-1)}{2}$	1
$\overline{D}_{34}$	$\frac{q^2(q^4-1)(q^2-1)}{4}$	$\frac{q^2(q-1)(q^2-1)}{4}$	1

Table 4.3: Designs from G under M_1 (q odd)

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_1}$
$\overline{A}_1$	1	1	$(q+1)(q^2+1)$
$\overline{A}_{21}$	$\frac{q^4-1}{2}$	$\frac{(q-1)(q^2+q+1)}{2}$	q^2+q+1
$\overline{A}_{22}$	$\frac{q^4-1}{2}$	$\frac{(q-1)(q^2+q+1)}{2}$	q^2+q+1
$\overline{A}_{31}$	$\frac{q(q^4-1)(q+1)}{2}$	$\frac{q(q^2-1)(q+1)}{2}$	$q+1$
$\overline{A}_{32}$	$\frac{q(q^4-1)(q-1)}{2}$	$\frac{q(q^2-1)(q-1)}{2}$	$q+1$
$\overline{A}_{41}$	$\frac{q^2(q^4-1)(q^2-1)}{2}$	$\frac{q^2(q^2-1)(q-1)}{2}$	1
$\overline{A}_{42}$	$\frac{q^2(q^4-1)(q^2-1)}{2}$	$\frac{q^2(q^2-1)(q-1)}{2}$	1
$\overline{B}_2(i)\ \ i \in\ R_1''$	$q^4(q^4-1)$	$2q^4(q-1)$	2
$\overline{B}_3(i,j)\ \ j = \frac{q-1}{2} - i$	$\frac{q^4(q^2+1)(q+1)^2}{2}$	$2q^4(q+1)$	4
$\overline{B}_3(i,j)\ \ i < j \leq \frac{q-3}{2} - i$	$q^4(q^2+1)(q+1)^2$	$4q^4(q+1)$	4
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^4(q-1)$	2
$\overline{B}_7(i)$	$q^3(q^4-1)(q-1)$	$q^3(q-1)^2$	1
$\overline{B}_8(i)\ \ i = \frac{q-1}{2}$	$\frac{q^3(q^2+1)(q+1)}{2}$	$q^3(q+1)$	$2(q+1)$
$\overline{B}_9(i)\ \ i = \frac{q-1}{4}$	$\frac{q^3(q^4-1)(q+1)}{2}$	$q^3(q^2-1)$	2
$\overline{B}_9(i)\ \ 1 \leq i \leq \frac{q-3}{4}$	$\frac{q^3(q^4-1)(q+1)}{2}$	$\frac{3q^3(q^2-1)}{2}$	3
$\overline{C}_1(i)$	$q^3(q^2+1)(q-1)$	$q^3(q-1)$	$q+1$
$\overline{C}_{21}(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$\frac{q^3(q-1)^2}{2}$	1
$\overline{C}_{22}(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$\frac{q^3(q-1)^2}{2}$	1
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$q^3(q+3)$	$q+3$
$\overline{C}_{41}(i)$	$\frac{q^3(q^4-1)(q+1)}{2}$	$\frac{3q^3(q^2-1)}{2}$	3
$\overline{D}_1$	$\frac{q^2(q^2+1)}{2}$	q^2	$2(q+1)$
$\overline{D}_{21}$	$\frac{q^2(q^2+1)(q^2-1)}{2}$	$\frac{q^2(q-1)(q+2)}{2}$	$q+2$
$\overline{D}_{22}$	$\frac{q^2(q^2+1)(q^2-1)}{2}$	$\frac{q^2(q-1)(q+2)}{2}$	$q+2$
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{4}$	$\frac{q^2(q-1)(q^2-1)}{2}$	2
$\overline{D}_{32}$	$\frac{q^2(q^4-1)(q^2-1)}{8}$	$\frac{q^2(q-1)(q^2-1)}{4}$	2
$\overline{D}_{34}$	$\frac{q^2(q^4-1)(q^2-1)}{8}$	$\frac{q^2(q-1)(q^2-1)}{4}$	2

Table 4.4: Designs from G under M_2 (q odd)

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_2}$
$\overline{A}_1$	1	1	$(q+1)(q^2+1)$
$\overline{A}_{21}$	$\frac{q^4-1}{2}$	$\frac{q^2-1}{2}$	$q+1$
$\overline{A}_{22}$	$\frac{q^4-1}{2}$	$\frac{q^2-1}{2}$	$q+1$
$\overline{A}_{31}$	$\frac{q(q^4-1)(q+1)}{2}$	$\frac{q(q^2-1)(2q+1)}{2}$	$2q+1$
$\overline{A}_{32}$	$\frac{q(q^4-1)(q-1)}{2}$	$\frac{q(q-1)^2}{2}$	1
$\overline{A}_{41}$	$\frac{q^2(q^4-1)(q^2-1)}{2}$	$\frac{q^2(q^2-1)(q-1)}{2}$	1
$\overline{A}_{42}$	$\frac{q^2(q^4-1)(q^2-1)}{2}$	$\frac{q^2(q^2-1)(q-1)}{2}$	1
$\overline{B}_2(i) \;\; i \in \; R_1''$	$\frac{q^4(q^4-1)}{2}$	$q^4(q-1)$	2
$\overline{B}_2(i) \;\; i \in \; R_1''$	$\frac{q^4(q^4-1)}{2}$	$q^4(q-1)$	2
$\overline{B}_3(i,j) \;\; j = \frac{q-1}{2} - i$	$\frac{q^4(q^2+1)(q+1)^2}{2}$	$2q^4(q+1)$	4
$\overline{B}_3(i,j) \;\; i < j \leq \frac{q-3}{2} - i$	$q^4(q^2+1)(q+1)^2$	$4q^4(q+1)$	4
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^4(q-1)$	2
$\overline{B}_6(i)$	$q^3(q^2+1)(q-1)$	$q^3(q-1)$	$q+1$
$\overline{B}_6(i)$	$\frac{q^3(q^2+1)(q-1)}{2}$	$\frac{q^3(q-1)}{2}$	$q+1$
$\overline{B}_7(i)$	$q^3(q^4-1)(q-1)$	$q^3(q-1)^2$	1
$\overline{B}_7(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$\frac{q^3(q-1)^2}{2}$	1
$\overline{B}_8(i) \;\; i = \frac{q-1}{2}$	$\frac{q^3(q^2+1)(q+1)}{2}$	$\frac{q^3(q+3)}{2}$	$q+3$
$\overline{B}_8(i) \;\; 1 \leq i \leq \frac{q-3}{4}$	$q^3(q^2+1)(q+1)$	$q^3(q+3)$	$q+3$
$\overline{B}_8(i) \;\; 1 \leq i \leq \frac{q-5}{4}$	$q^3(q^2+1)(q+1)$	$2q^3(q+1)$	$2(q+1)$
$\overline{B}_9(i) \;\; i = \frac{q-1}{4}$	$\frac{q^3(q^4-1)(q+1)}{2}$	$q^3(q^2-1)$	2
$\overline{B}_9(i) \;\; 1 \leq i \leq \frac{q-5}{4}$	$q^3(q^4-1)(q+1)$	$2q^3(q^2-1)$	2
$\overline{B}_9(i) \;\; 1 \leq i \leq \frac{q-3}{4}$	$\frac{q^3(q^4-1)(q+1)}{2}$	$\frac{3q^3(q^2-1)}{2}$	3
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$2q^3(q+1)$	$2(q+1)$
$\overline{C}_{41}(i)$	$\frac{q^3(q^4-1)(q+1)}{2}$	$q^3(q^2-1)$	2
$\overline{D}_1$	$\frac{q^2(q^2+1)}{2}$	$\frac{q^2(q+1)}{2}$	$(q+1)^2$
$\overline{D}_{21}$	$\frac{q^2(q^2+1)(q^2-1)}{2}$	$\frac{q^2(q^2-1)}{2}$	$q+1$
$\overline{D}_{22}$	$\frac{q^2(q^2+1)(q^2-1)}{2}$	$\frac{q^2(q^2-1)}{2}$	$q+1$
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{4}$	$\frac{q^2(q-1)(q^2-1)}{4}$	1
$\overline{D}_{32}$	$\frac{q^2(q^4-1)(q^2-1)}{8}$	$\frac{q^2(q-1)(q^2-1)}{8}$	1
$\overline{D}_{34}$	$\frac{q^2(q^4-1)(q^2-1)}{8}$	$\frac{q^2(q-1)(q^2-1)}{8}$	1

4.2.2 Designs from subgroups of indices $\frac{q^2(q^2\pm1)}{2}$

In this section, we provide the parameters of designs from $G = PSp_4(q)$ using Method 2 with respect to maximal subgroups of index $\frac{q^2(q^2+1)}{2}$. These subgroups appear as one class for q odd and as two classes for q even, designated M_3 and M_3'. We also consider maximal subgroups of index $\frac{q^2(q^2-1)}{2}$, similarly which appear as one class for q odd and as two classes for q even, labeled M_4 and M_4'.

Theorem 4.2.2. *The parameters of designs from $G = PSp_4(q)$ (where $q > 2$ is even) using Method 2 are fully provided in Table 4.5 and Table 4.6 for the two classes of subgroups of index $\frac{q^2(q^2+1)}{2}$, and in Table 4.7 and Table 4.8 for the two classes of subgroups of index $\frac{q^2(q^2-1)}{2}$.*

Proof. According to Theorem 3.6.1, the degree of the permutation representation of M_3 is $\frac{q^2(q^2+1)}{2}$, which is a linear combination of some irreducible characters of G.
We claim that $1+\theta_9+\chi_3$ and $1+\theta_9'+\chi_3$ are permutation characters corresponding to specific actions of G. A careful examination of the character degrees of G (Theorem 3.6.1) suggests that these are the only combinations of irreducible character degrees that sum to $\frac{q^2(q^2+1)}{2}$.
Similarly, we claim that $1+\theta_{11}+\chi_8$ and $1+\theta_{12}+\chi_8$ are permutation characters corresponding to specific actions of G. A careful examination of the character degrees of G (Theorem 3.6.1) implies that there is no other combination of irreducible character degrees that sums to $\frac{q^2(q^2-1)}{2}$.
We need to find the permutation characters of the action in each case.

$$\frac{q^2(q^2+1)}{2} = 1+\theta_9(1)+\left(\frac{q-2}{2}\right)\chi_3(1) = 1+\theta_9'(1)+\left(\frac{q-2}{2}\right)\chi_3(1).$$

and

$$\frac{q^2(q^2-1)}{2} = 1+\theta_{11}(1)+\left(\frac{q-2}{2}\right)\chi_8(1) = 1+\theta_{12}(1)+\left(\frac{q-2}{2}\right)\chi_8(1).$$

We claim that the permutation characters for these two actions are:

$$1+\theta_9+\left(\frac{q-2}{2}\right)\chi_3, 1+\theta_9'+\left(\frac{q-2}{2}\right)\chi_3,$$

and

$$1+\theta_{11}+\left(\frac{q-2}{2}\right)\chi_8, 1+\theta_{12}+\left(\frac{q-2}{2}\right)\chi_8.$$

Now, using Maxima [33], we can verify that no other linear combinations of the character degrees of G sum to $\frac{q^2(q^2+1)}{2}$. A similar argument shows that the permutation characters of degree $\frac{q^2(q^2-1)}{2}$ are as follows:

$$1+\theta_9(1)+\left(\frac{q-2}{2}\right)\chi_3(1), 1+\theta'_9(1)+\left(\frac{q-2}{2}\right)\chi_3(1),$$

and

$$1+\theta_{11}(1)+\left(\frac{q-2}{2}\right)\chi_8(1), 1+\theta_{12}(1)+\left(\frac{q-2}{2}\right)\chi_8(1).$$

The proof is now complete.

□

Table 4.5: Designs under M_3 (q even)

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_3}$
$\overline{A}_1$	1	1	$\frac{q^2(q^2+1)}{2}$
$\overline{A}_{11}$	$(q^2-1)(q^4-1)$	$\frac{4(q^4-1)}{q}$	$2q$
$\overline{A}_{21}$	q^4-1	$2(q^2-1)$	q^2
$\overline{A}_{22}$	q^4-1	$4(q^2-1)$	$2q^2$
$\overline{B}_2(i)$	$q^4(q^4-1)$	$2q^2(q^2-1)$	1
$\overline{B}_4(i,j)$	$q^4(q^2+1)(q-1)^2$	$2q^2(q-1)^2$	1
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^2(q^2-1)$	1
$\overline{B}_6(i)$	$q^3(q^2+1)(q-1)$	$2q(q-1)(q+2)$	$q+2$
$\overline{B}_7(i)$	$q^3(q^4-1)(q-1)$	$4q(q-1)(q^2-1)$	2
$\overline{B}'_7(i)$	$q^3(q^4-1)(q-1)$	$4q(q-1)(q^2-1)$	2
$\overline{B}_8(i)$	$q^3(q^2+1)(q+1)$	$2q(q+1)$	1
$\overline{B}_9(i)$	$q^3(q^4-1)(q+1)$	$2q(q^2-1)(q+1)$	1
$\overline{C}_1(i)$	$q^3(q^2+1)(q-1)$	$2q(q-1)$	1
$\overline{C}_{21}(i)$	$q^3(q^4-1)(q-1)$	$2q(q^2-1)(q-1)$	1
$\overline{C}_{22}(i)$	$q^3(q^4-1)(q-1)$	$2q(q^2-1)(q-1)$	1
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$4q(q+1)^2$	$2(q+1)$
$\overline{C}_{41}(i)$	$q^3(q^4-1)(q+1)$	$4q(q^2-1)(q+1)$	2
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{2}$	$q(q^2-1)^2$	q

Table 4.6: Designs under M_3' (q even)

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_3'}$
$\overline{A}_1$	1	1	$\frac{q^2(q^2+1)}{2}$
$\overline{A}_{11}$	$(q^2-1)(q^4-1)$	$\frac{4(q^4-1)}{q}$	$2q$
$\overline{A}_{21}$	q^4-1	$2(q^2-1)$	q^2
$\overline{A}_{22}$	q^4-1	$4(q^2-1)$	$2q^2$
$\overline{B}_2(i)$	$q^4(q^4-1)$	$2q^2(q^2-1)$	1
$\overline{B}_4(i,j)$	$q^4(q^2+1)(q-1)^2$	$2q^2(q-1)^2$	1
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^2(q^2-1)$	1
$\overline{B}_6(i)$	$q^3(q^2+1)(q-1)$	$2q(q-1)(q+2)$	$q+2$
$\overline{B}_7(i)$	$q^3(q^4-1)(q-1)$	$4q(q-1)(q^2-1)$	2
$\overline{B}_7'(i)$	$q^3(q^4-1)(q-1)$	$4q(q-1)(q^2-1)$	2
$\overline{B}_8(i)$	$q^3(q^2+1)(q+1)$	$2q(q+1)$	1
$\overline{B}_9(i)$	$q^3(q^4-1)(q+1)$	$2q(q^2-1)(q+1)$	1
$\overline{C}_1(i)$	$q^3(q^2+1)(q-1)$	$2q(q-1)$	1
$\overline{C}_1'(i)$	$q^3(q^2+1)(q-1)$	$2q(q-1)$	1
$\overline{C}_{21}(i)$	$q^3(q^4-1)(q-1)$	$2q(q^2-1)(q-1)$	1
$\overline{C}_{22}(i)$	$q^3(q^4-1)(q-1)$	$2q(q^2-1)(q-1)$	1
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$4q(q+1)^2$	$2(q+1)$
$\overline{C}_{41}(i)$	$q^3(q^4-1)(q+1)$	$4q(q^2-1)(q+1)$	2
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{2}$	$q(q^2-1)^2$	q

Table 4.7: Designs under M_4 (q even)

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_4}$
$\overline{A}_1$	1	1	$\frac{q^2(q^2-1)}{2}$
$\overline{A}_{11}$	$(q^2-1)(q^4-1)$	$\frac{4(q^4-1)}{q}$	$2q$
$\overline{A}_{22}$	q^4-1	$4(q^2+1)$	$2q^2$
$\overline{B}_1(i)$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_1'(i)$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_1''(i)$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_1'''(i)$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_2(i)$	$q^4(q^4-1)$	$2q^2(q^2+1)$	1
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^2(q^2+1)$	1
$\overline{B}_6(i)$	$q^3(q^2+1)(q-1)$	$4q(q^2+1)$	$2(q+1)$
$\overline{B}_7(i)$	$q^3(q^4-1)(q-1)$	$4q(q^2+1)(q-1)$	2
$\overline{B}_7(i)$	$q^3(q^4-1)(q-1)$	$4q(q^2+1)(q-1)$	2
$\overline{B}_8(i)$	$q^3(q^2+1)(q+1)$	$\frac{2q(q^2+1)(q+2)}{q-1}$	$q+2$
$\overline{C}_1(i)$	$q^3(q^2+1)(q-1)$	$4q(q^2+1)$	$2(q+1)$
$\overline{C}_{21}(i)$	$q^3(q^4-1)(q-1)$	$4q(q^2+1)(q-1)$	2
$\overline{C}_{22}(i)$	$q^3(q^4-1)(q-1)$	$4q(q^2+1)(q-1)$	2
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$\frac{2q(q^2+1)(q+2)}{q-1}$	$q+2$
$\overline{C}_{41}(i)$	$q^3(q^4-1)(q+1)$	$4q(q^2+1)(q+1)$	2
$\overline{C}_{42}(i)$	$q^3(q^4-1)(q+1)$	$4q(q^2+1)(q+1)$	2
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{2}$	$q(q^4-1)$	q

Table 4.8: Designs under M_4' (q even)

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_4'}$
$\overline{A}_1$	1	1	$\frac{q^2(q^2-1)}{2}$
$\overline{A}_{11}$	$(q^2-1)(q^4-1)$	$\frac{4(q^4-1)}{q}$	$2q$
$\overline{A}_{22}$	q^4-1	$4(q^2+1)$	$2q^2$
$\overline{B}_1(i)$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_1(i)$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_1(i)$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_1(i)$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_2(i)$	$q^4(q^4-1)$	$2q^2(q^2+1)$	1
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^2(q^2+1)$	1
$\overline{B}_6(i)$	$q^3(q^2+1)(q-1)$	$4q(q^2+1)$	$2(q+1)$
$\overline{B}_7(i)$	$q^3(q^4-1)(q-1)$	$4q(q^2+1)(q-1)$	2
$\overline{B}_8(i)$	$q^3(q^2+1)(q+1)$	$\frac{2q(q^2+1)(q+2)}{q-1}$	$q+2$
$\overline{B}_9(i)$	$q^3(q^4-1)(q+1)$	$4q(q^2+1)(q+1)$	2
$\overline{C}_1(i)$	$q^3(q^2+1)(q-1)$	$4q(q^2+1)$	$2(q+1)$
$\overline{C}_{21}(i)$	$q^3(q^4-1)(q-1)$	$4q(q^2+1)(q-1)$	2
$\overline{C}_{22}(i)$	$q^3(q^4-1)(q-1)$	$4q(q^2+1)(q-1)$	2
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$\frac{2q(q^2+1)(q+2)}{q-1}$	$q+2$
$\overline{C}_{41}(i)$	$q^3(q^4-1)(q+1)$	$4q(q^2+1)(q+1)$	2
$\overline{C}_{42}(i)$	$q^3(q^4-1)(q+1)$	$4q(q^2+1)(q+1)$	2
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{2}$	$q(q^4-1)$	q

Theorem 4.2.3. *The parameters of designs from $G = PSp_4(q)$ (where $q > 2$ is odd) using Method 2 are fully provided in Table 4.9 and Table 4.10 for the two classes of subgroups of index $\frac{q^2(q^2+1)}{2}$, and in Table 4.11 and Table 4.12 for the two classes of subgroups of index $\frac{q^2(q^2-1)}{2}$.*

Proof. Based on Theorem 3.6.1, the degree of the permutation representation of $\frac{q^2(q^2+1)}{2}$, and it can be written as a linear combination of specific irreducible characters of G. We assert that the expressions $1+\theta_9+\chi_3$ and $1+\theta'_9+\chi_3$ serve as permutation characters for specific actions of the group G. A thorough analysis of the character degrees of G, as outlined in Theorem 3.6.1, indicates that these are the sole combinations of irreducible character degrees that sum to $\frac{q^2(q^2+1)}{2}$. This suggests that no other combinations can achieve this total.

Similarly, we claim that $1+\theta_{11}+\chi_8$ and $1+\theta_{12}+\chi_8$ are permutation characters of the actions of G. A detailed analysis of the character degrees of G, as presented in Theorem 3.6.1, indicates that these are the only combinations of irreducible character degrees that sum to $\frac{q^2(q^2-1)}{2}$. This indicates that no alternative combinations can produce this sum.

Hence, we have:

$$1+\theta_9(1)+\left(\frac{q+2}{2}\right)\chi_3(1), 1+\theta'_9(1)+\left(\frac{q+2}{2}\right)\chi_3(1),$$

and

$$1+\theta_{11}(1)+\left(\frac{q+2}{2}\right)\chi_8(1), 1+\theta_{12}(1)+\left(\frac{q+2}{2}\right)\chi_8(1).$$

Now, using a similar argument to the proof of the previous theorem, we can find the corresponding permutation characters of G and the result follows.

□

Table 4.9: Designs under M_3 for $q = 4n - 1$, where $n \in \mathbb{N}$

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_3}$
$\overline{A}_1$	1	1	$\frac{q^2(q^2+1)}{2}$
$\overline{A}_{22}$	$\frac{q^4-1}{2}$	q^2-1	q^2
$\overline{A}_{31}$	$\frac{q(q^4-1)(q+1)}{2}$	$n(q+1)(q^2-1)$	qn
$\overline{A}_{32}$	$\frac{q(q^4-1)(q-1)}{2}$	$2n(q-1)(q^2-1)$	$2nq$
$\overline{B}_2(i) \;\; i \in \;\; R_1''$	$\frac{q^4(q^4-1)}{2}$	$q^2(q^2-1)$	1
$\overline{B}_6(i) \;\; i = \frac{q+1}{4}$	$q^3(q^2+1)(q-1)$	$2q(q-1)n$	n
$\overline{B}_6(i) \;\; i = \frac{q+1}{4}$	$\frac{q^3(q^2+1)(q-1)}{2}$	$q(q-1)(q+2)$	$q+2$
$\overline{B}_7(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$q(q-1)^2(q+1)$	1
$\overline{B}_8(i) \;\; i = \frac{q-1}{2}$	$\frac{q^3(q^2+1)(q+1)}{2}$	$q(q+1)n$	n
$\overline{C}_{21}(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$2q(q-1)^2(q+1)$	2
$\overline{C}_{22}(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$q(q^2-1)(q-1)$	1
$\overline{D}_1$	$\frac{q^2(q^2+1)}{2}$	$\frac{q^3-2q+(q+2n)}{2}$	$\frac{q^3-2q+(q+2n)}{2}$
$\overline{D}_{21}$	$\frac{q^2(q^4-1)}{2}$	$(q^2-1)n$	n
$\overline{D}_{22}$	$\frac{q^2(q^2+1)(q^2-1)}{2}$	$\frac{q^3-2q+(q+2n)}{2}$	$\frac{q^3-2q+(q+2n)}{2}$
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{4}$	$\frac{(q-1)(q^2-1)^2}{4}$	$\frac{q-1}{2}$
$\overline{D}_{32}$	$\frac{q^2(q^4-1)(q^2-1)}{8}$	$\frac{(q+n)(q^2-1)^2}{4}$	$q+n$
$\overline{D}_{34}$	$\frac{q^2(q^4-1)(q^2-1)}{8}$	$\frac{(q+n)(q^2-1)^2}{4}$	$q+n$

Table 4.10: Designs under M_3 for $q = 4n + 1$, where $n \in \mathbb{N}$.

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_3}$
$\overline{A}_1$	1	1	$\frac{q^2(q^2+1)}{2}$
$\overline{A}_{21}$	$\frac{q^4-1}{2}$	q^2-1	q^2
$\overline{A}_{22}$	$\frac{q^4-1}{2}$	q^2-1	q^2
$\overline{A}_{31}$	$\frac{q(q^4-1)(q+1)}{2}$	$2n(q+1)(q^2-1)$	$2nq$
$\overline{A}_{32}$	$\frac{q(q^4-1)(q-1)}{2}$	$(2n+1)(q-1)(q^2-1)$	$(2n+1)q$
$\overline{B}_2(i) \;\; i \in \; R_1''$	$\frac{q^4(q^4-1)}{2}$	$2q^2(q^2-1)$	2
$\overline{B}_2(i) \;\; i \in \; R_1''$	$\frac{q^4(q^4-1)}{2}$	$3q^2(q^2-1)$	3
$\overline{B}_4(i,j) \;\; i < j \leq \frac{q-3}{2} - i$	$\frac{q^4(q^2+1)(q-1)^2}{2}$	$q^2(q-n)(q-1)^2$	$q-n$
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^2(q^2-1)$	1
$\overline{B}_6(i) \;\; i = \frac{q+1}{4}$	$q^3(q^2+1)(q-1)$	$2q(q-1)$	1
$\overline{B}_6'(i) \;\; i = \frac{q+1}{4}$	$q^3(q^2+1)(q-1)$	$4q^2(q-1)$	$2q$
$\overline{B}_7(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$q(q-1)^2(q+1)$	1
$\overline{B}_8(i) \;\; i = \frac{q-1}{2}$	$\frac{q^3(q^2+1)(q+1)}{2}$	$q[(4n-1)q+2](q+1)$	$(4n-1)q+2$
$\overline{B}_9(i) \;\; i = \frac{q-1}{4}$	$\frac{q^3(q^4-1)(q+1)}{2}$	$2q(q^2-1)(q+1)$	2
$\overline{C}_1(i)$	$q^3(q^2+1)(q-1)$	$2q(q-1)$	1
$\overline{C}_{21}(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$q(q^2-1)(q-1)$	1
$\overline{C}_{22}(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$q(q^2-1)(q-1)$	1
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$2q(q+1)$	1
$\overline{C}_{41}(i)$	$\frac{q^3(q^4-1)(q+1)}{2}$	$q(q^2-1)(q+1)$	1
$\overline{C}_{42}(i)$	$\frac{q^3(q^4-1)(q+1)}{2}$	$q(q^2-1)(q+1)$	1
$\overline{D}_1$	$\frac{q^2(q^2+1)}{2}$	$\frac{q^3-2q+(q+2n)}{2}$	$\frac{q^3-2q+(q+2n)}{2}$
$\overline{D}_{21}$	$\frac{q^2(q^4-1)}{2}$	$n(q^2-1)$	n
$\overline{D}_{22}$	$\frac{q^2(q^4-1)}{2}$	$n(q^2-1)$	n
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{4}$	$\frac{n(q^2-1)^2}{2}$	n
$\overline{D}_{32}$	$\frac{q^2(q^4-1)(q^2-1)}{8}$	$\frac{(q+n)(q^2-1)^2}{4}$	$q+n$
$\overline{D}_{34}$	$\frac{q^2(q^4-1)(q^2-1)}{8}$	$\frac{(q+n)(q^2-1)^2}{4}$	$q+n$

Table 4.11: Designs under M_4 for $q = 4n - 1$, where $n \in \mathbb{N}$

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_4}$
$\overline{A}_1$	1	1	$\frac{q^2(q^2-1)}{2}$
$\overline{A}_{31}$	$\frac{q(q^4-1)(q+1)}{2}$	$n(q+1)(q^2+1)$	nq
$\overline{A}_{32}$	$\frac{q(q^4-1)(q-1)}{2}$	$2n(q-1)(q^2+1)$	$2nq$
$\overline{B}_1(i) \;\; i \in \; R_1''$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_2(i) \;\; i \in \; R_1''$	$\frac{q^4(q^4-1)}{2}$	$q^2(q^2+1)(q-1)$	$q-1$
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^2(q^2+1)$	1
$\overline{B}_6(i) \;\; i = \frac{q+1}{4}$	$\frac{q^3(q^2+1)(q-1)}{2}$	$2q(q^2+1)$	$2(q+1)$
$\overline{B}_7(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$q(q-1)(q^2+1)$	1
$\overline{C}_{21}(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$2q(q^2+1)(q-1)$	2
$\overline{D}_1$	$\frac{q^2(q^2+1)}{2}$	$\frac{q(q^2+1)}{q-1}$	$q(q+1)$
$\overline{D}_{21}$	$\frac{q^2(q^4-1)}{2}$	$(q^2+1)n$	n
$\overline{D}_{22}$	$\frac{q^2(q^2+1)(q^2-1)}{2}$	$\frac{q^3-2q+(q+2n)}{2}$	$\frac{q^3-2q+(q+2n)}{2}$
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{4}$	$\frac{q(q^4-1)}{2}$	q

Table 4.12: Designs under M_4 for $q = 4n + 1$, where $n \in \mathbb{N}$

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_4}$
$\overline{A}_1$	1	1	$\frac{q^2(q^2+1)}{2}$
$\overline{A}_{31}$	$\frac{q(q^4-1)(q+1)}{2}$	$2n(q+1)(q^2+1)$	$2nq$
$\overline{A}_{32}$	$\frac{q(q^4-1)(q-1)}{2}$	$(q^2+1)(q-1)(q-2n)$	$q(q-2n)$
$\overline{B}_1(i) \;\; i \in R_1''$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_1'(i) \;\; i \in R_1''$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_1''(i) \;\; i \in R_1''$	$q^4(q^2-1)^2$	$2q^2(q^2-1)$	1
$\overline{B}_2(i) \;\; i \in R_1''$	$\frac{q^4(q^4-1)}{2}$	$q^2(q^2+1)(q-1)$	$q-1$
$\overline{B}_4(i,j) \;\; i < j \leq \frac{q-3}{2} - i$	$\frac{q^4(q^2+1)(q-1)^2}{2}$	$\frac{q^2(q^2+1)(q-1)(q-2)}{q+1}$	$q-2$
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q^2(q^2+1)$	1
$\overline{B}_8(i) \;\; i = \frac{q-1}{2}$	$\frac{q^3(q^2+1)(q+1)}{2}$	$\frac{2q(q^2+1)(q+1)}{q-1}$	$2(q+1)$
$\overline{C}_1(i)$	$q^3(q^2+1)(q-1)$	$\frac{2q^2(q^2+1)(q-2)}{q+1}$	$q(q-2)$
$\overline{C}_{21}(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$q(q^2+1)(q-1)$	1
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$\frac{2q(q^2+1)(q-2n)}{q-1}$	$q-2n$
$\overline{C}_{41}(i)$	$\frac{q^3(q^4-1)(q+1)}{2}$	$2q(q^2+1)(q+1)$	2
$\overline{D}_1$	$\frac{q^2(q^2+1)}{2}$	$\frac{2q(q^2+1)}{q-1}$	$2q(q+1)$
$\overline{D}_{21}$	$\frac{q^2(q^4-1)}{2}$	$n(q^2-1)$	n
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{4}$	$\frac{(4n+1)(q^4-1)}{2}$	$4n+1$
$\overline{D}_{32}$	$\frac{q^2(q^4-1)(q^2-1)}{8}$	$\frac{(q+n)(q^4-1)}{4}$	$q+n$

4.2.3 Designs from subgroups of indices $\frac{q^3(q^2+1)(q\pm1)}{2}$

Theorem 4.2.4. *The parameters of designs from $G = PSp_4(q)$ (where $q > 3$) using Method 2 are fully provided in Table 4.13 and Table 4.14 for the two classes of subgroups of indices $\frac{q^3(q^2+1)(q+1)}{2}$ and $\frac{q^3(q^2+1)(q-1)}{2}$, as defined in Chapter 3.*

Proof. Using a similar argument to that in the proof of the previous theorem, we have:

$$1 + \theta_9(1) + \left(\frac{q+2}{2}\right)\chi_5(1) = 1 + \theta'_9(1) + \left(\frac{q+2}{2}\right)\chi_5(1),$$

and

$$1 + \theta_{11}(1) + \left(\frac{q+2}{2}\right)\chi_9(1) = 1 + \theta_{12}(1) + \left(\frac{q+2}{2}\right)\chi_9(1).$$

Thus, the result follows.

□

Table 4.13: Designs under M_5

Representative	$v = \lvert x^G\rvert$	$k = \lvert M \cap x^G\rvert$	$\lambda = \chi_{M_5}$
$\overline{A}_1$	1	1	$\frac{q^3(q^2+1)(q+1)}{2}$
$\overline{A}_{31}$	$\frac{q(q^4-1)(q+1)}{2}$	q^2-1	q^2
$\overline{B}_2(i)\ \ i \in R_1''$	$\frac{q^4(q^4-1)}{2}$	$\frac{q(q^2-1)}{2}$	$\frac{q+1}{2}$
$\overline{B}_2(i)\ \ i \in R_1''$	$\frac{q^4(q^4-1)}{2}$	$q(q-1)^2$	$q-1$
$\overline{B}_4(i)\ \ i \in R_1''$	$\frac{q^4(q^2+1)(q-1)^2}{2}$	$\frac{q(q-1)^2}{2}$	$\frac{q+1}{2}$
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q(q-1)$	1
$\overline{B}_6(i)\ \ i = \frac{q+1}{4}$	$q^3(q^2+1)(q-1)$	$\frac{6q(q-1)}{q+1}$	$3q$
$\overline{B}_8(i)$	$\frac{q^3(q^2+1)(q+1)}{2}$	$\frac{q^3+(q+2k)}{2}$	$\frac{q^3+(q+2k)}{2}$
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$2q(q+1)$	$q(q+1)$
$\overline{C}_{41}(i)$	$\frac{q^3(q^4-1)(q+1)}{2}$	q^2-1	1
$\overline{D}_1$	$\frac{q^2(q^2+1)}{2}$	$[(4k-1)q+2]q(q+1)$	$(4k-1)+2$
$\overline{D}_{22}$	$\frac{q^2(q^2+1)(q^2-1)}{2}$	$\frac{q^3-2q+(q+2k)}{2}$	$\frac{q^3-2q+(q+2k)}{2}$
$\overline{D}_{32}$	$\frac{q^2(q^2-1)(q^4-1)}{8}$	$\frac{(q-1)(q^2-1)}{4}$	q
$\overline{D}_{34}$	$\frac{q^2(q^2-1)(q^4-1)}{8}$	$\frac{(q-1)(q^2-1)}{4}$	q

Table 4.14: Designs under M_6

Representative	$v = \lvert x^G \rvert$	$k = \lvert M \cap x^G \rvert$	$\lambda = \chi_{M_6}$
$\overline{A}_1$	1	1	$\frac{q^3(q^2+1)(q-1)}{2}$
$\overline{A}_{32}$	$\frac{q(q^4-1)(q-1)}{2}$	q^2-1	q^2
$\overline{B}_2(i) \;\; i \in \;\; R_1''$	$\frac{q^4(q^4-1)}{2}$	$\frac{q(q+1)^2}{2}$	$\frac{q+1}{2}$
$\overline{B}_2(i) \;\; i \in \;\; R_1''$	$\frac{q^4(q^4-1)}{2}$	$q(q^2-1)$	$q-1$
$\overline{B}_4(i) \;\; i \in \;\; R_1''$	$\frac{q^4(q^2+1)(q-1)^2}{2}$	$q^2(q-1)$	q
$\overline{B}_5(i,j)$	$q^4(q^4-1)$	$2q(q+1)$	1
$\overline{B}_6(i) \;\; i = \frac{q+1}{4}$	$q^3(q^2+1)(q-1)$	$8q$	$4q$
$\overline{B}_6(i) \;\; i = \frac{q+1}{4}$	$q^3(q^2+1)(q-1)$	$8q$	$4q$
$\overline{B}_7(i)$	$\frac{q^3(q^4-1)(q-1)}{2}$	$2(q^2-1)$	1
$\overline{B}_8(i)$	$\frac{q^3(q^2+1)(q+1)}{2}$	$2(2q+1)$	$2q+1$
$\overline{C}_1(i)$	$q^3(q^2+1)(q+1)$	$2q(q+1)$	$q(q+1)$
$\overline{C}_3(i)$	$q^3(q^2+1)(q+1)$	$2q(q+1)$	$q(q+1)$
$\overline{C}_{41}(i)$	$\frac{q^3(q^4-1)(q+1)}{2}$	q^2-1	1
$\overline{D}_1$	$\frac{q^2(q^2+1)}{2}$	$\frac{q+1}{2}$	$\frac{q(q-1)(q^2+1)}{2}$
$\overline{D}_{31}$	$\frac{q^2(q^2-1)(q^4-1)}{4}$	$\frac{(q+1)(q^2-1)}{2}$	q
$\overline{D}_{34}$	$\frac{q^2(q^2-1)(q^4-1)}{8}$	$\frac{(q-1)(q^2-1)}{4}$	q

4.3 Codes from the simple group $PSp_4(3)$

In this section, we construct the code parameters from the finite simple group $PSp_4(3)$.

Proposition 4.3.1. *For $q = 3$, $|PSp_4(3)| = 25920 = 2^6.3^4.5$, and there are 5 maximal subgroups that appear:*

Table 4.15: Maximal Subgroups for $q = 3$

Degree	Suborbits	Rank	Group structures
27	1, 10, 16	3	$2^4 : A_5$
36	1, 15, 20	3	S_6
40	1, 12, 27	3	$3^{1+2} : 2A_4$
40	1, 12, 27	3	$3^3 : S_4$
45	1, 12, 32	3	$2^2.(A_4 \times A_4)$

The table 4.15, shows that the group has five classes of maximal subgroups up to conjugation [11]. For each maximal subgroup M_i (where $i = 1, 2, 3, 4, 5$), the action of G by conjugation on the set of conjugates of M_i gives a primitive action of degree $|G{:}M_i| \in \{27, 36, 40, 40, 45\}$. The elements of each degree generate a permutation module over $\mathbb{F}_2$. Every binary code of length $|G{:}M_i|$ that admits G as a primitive permutation group is a submodule of the permutation module of G with respect to the action of G.

Lemma 4.3.2. *Let C be the repetition code of length n over the finite field $\mathbb{F}_2$, and let $C^\perp$ denote the dual of C. If $C = [n, 1, n]$, then $C^\perp = [n, n-1, 2]$.*

Proof. If w is a non-zero codeword in C, then $w = (\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_n)$, where $\lambda \in \mathbb{F}$. Hence, the weight of w is n. From the definition of the dual of a code, we observe that the codeword $(1, |\mathbb{F}^*|, 0, \cdots, 0)$ is in $C^\perp$. Additionally, if $v = (v_1, v_2, v_3, \cdots, v_n)$ is a non-zero codeword of $C^\perp$, then $v_1 + v_2 + v_3 + \cdots + v_n = 0$. Therefore, no codewords of weight 1 exist, which implies that the minimum weight of $C^\perp$ is 2.

□

According to Lemma 4.3.2, the codes $[n, n, 1]$ and $[n, n-1, 2]$ correct fewer than 1 error, so they are of less interest.

Lemma 4.3.3. *Let C be a code of length n over a finite field $\mathbb{F}_q$, and let $C^{\perp}$ be the dual of C. Then all codewords c' lies in C if and only if q divides the sum of all coordinates of each $w \in C^{\perp}$. In particular, if $q = 2$, then $c' \in C$ if and only if $C^{\perp}$ is even.*

Proof. See ([13], Lemma 2) □

Proposition 4.3.4. *Let $G = PSp_4(3)$, the projective symplectic group. Then:*

1. *If M_1 is a primitive subgroup of degree 40, then a binary linear code $C_{12} = [40, 16, 8]$ is doubly even and irreducible, with a dual binary linear code $[40, 24, 6]$ of dimension 24 that is even and self-orthogonal.*

2. *If M_2 is a primitive subgroup of degree 40, then a binary linear code $C_{12} = [40, 10, 12]$ is doubly even and irreducible, with a dual binary linear code $[40, 30, 3]$ of dimension 30 that is even and self-orthogonal.*

3. *If M_3 is a primitive subgroup of degree 36, then a binary linear code $C_{20} = [36, 6, 16]$ is doubly even, with a dual binary linear code $[36, 30, 3]$ of dimension 30 that is even and self-orthogonal.*

4. *If M_4 is a primitive subgroup of degree 45, then a binary linear code $C_{32} = [45, 14, 12]$ is doubly even, with a dual binary linear code $[45, 31, 5]$ of dimension 31 that is even and self-orthogonal.*

5. *If M_5 is a primitive subgroup of degree 27, then a binary linear code $C_{16} = [27, 6, 12]$ is doubly even, with a dual binary linear code $[27, 21, 3]$ of dimension 21 that is even and self-orthogonal.*

Proof. Using MAGMA, the weight distributions of the codes under $PSp_4(3)$ are given in Table 4.16,
Since all the weights of these codes are divisible by 4, they are doubly even. The code $C_{12} = [40, 10, 12]$ has submodules other than the trivial submodule, hence it is irreducible, while the other codes are reducible.

□

Table 4.16: Codes

Name	Codes	Weight distribution	Design
C_{12}	$[40, 16, 8]$	$[0^1, 8^{45}, 12^{1120}, 16^{15570}, 20^{32064}, 24^{15570}, 28^{1120}, 32^{45}, 40^1]$	$1-(40, 12, 12)$
C_{12}	$[40, 10, 12]$	$[0^1, 12^{40}, 16^{135}, 20^{672}, 24^{135}, 28^{40}, 40^1]$	$1-(40, 12, 12)$
C_{20}	$[36, 6, 16]$	$[0^1, 16^{27}, 20^{36}]$	$1-(36, 20, 20)$
C_{32}	$[45, 14, 12]$	$[0^1, 12^{120}, 16^{810}, 20^{6768}, 24^{6120}, 28^{2520}, 32^{45}]$	$1-(45, 32, 32)$
C_{16}	$[27, 6, 12]$	$[0^1, 12^{36}, 16^{27}]$	$1-(27, 16, 16)$

4.3.1 Representation of degree 40

We consider a permutation group G acting on a set Ω of size 40. We identify a 40-dimensional permutation module that is invariant under the action of G. This module serves as our primary working module, and we proceed to examine all of its submodules. The permutation module decomposes into submodules with dimensions $0, 1, 15, 16, 24, 25, 39$, and 40. The composition series of the module is as follows:

$$V = 40 \supset 39 \supset 25 \supset 24 \supset 16 \supset 15 \supset 1 \supset 0.$$

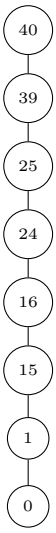
This demonstrates that the only irreducible submodule is the one of dimension 0. The non-trivial submodules have dimensions $1, 15, 16, 24, 25, 39$, and 40. Therefore, by Theorem 2.3.2, it is sufficient to find codes of dimensions $1, 15, 16, 24, 25, 39$, and 40. We will refer to these codes as:

1. $C_{40,1} = [40, 1, 40]$.
2. $C_{40,2} = [40, 15, 8]$.
3. $C_{40,3} = [40, 16, 8]$.
4. $C_{40,4} = [40, 24, 6]$.
5. $C_{40,5} = [40, 25, 4]$.
6. $C_{40,6} = [40, 39, 2]$.

Proposition 4.3.5. *$C_{40,1}$ is a repetition code, and $C_{40,6}$ is its dual code. They have minimum distances of 40 and 2, respectively. Moreover, $C_{40,1} \leq C_{40,6}$.*

Proof. The dimension of $C_{40,1}$ satisfies the definition of a repetition code. Moreover, $|P_1(2)| - 1 = 39$ by Proposition 2.3.3.
It follows that $C_{40,6}$ is the dual code of $C_{40,1}$. By Lemma 4.3.2, we have $C_{40,1} = [40, 1, 40]$ and $C_{40,6} = [40, 39, 2]$; hence, $C_{40,6}$ is the dual code of $C_{40,1}$. Since $Char(\mathbb{F}_2)$ divides the order of $|P_1(2)|$, we also have $C_{40,1} \leq C_{40,6}$ as proposed. □

Figure 4.1: Submodule lattice for a 40-dimensional representation.



Proposition 4.3.6. *1. $C_{40,2}$ is a code, and $C_{40,5}$ is its dual code; they have minimum distances of 8 and 4, respectively. Moreover, $C_{40,2} \leq C_{40,5}$.*

2. $C_{40,3}$ is a code, and $C_{40,4}$ is its dual code; they have minimum distances of 8 and 6, respectively. Moreover, $C_{40,3} \leq C_{40,4}$.

Proof. Same proof as Proposition 4.3.5. □

Using MAGMA, we find that the minimum distance of $C_{40,2}$ is 8 and the minimum distance of $C_{40,5}$ is 4. From the fact that if $C = [n, k, d]$ then $C^{\perp} = [n, n-k, d']$, we can conclude that $C_{40,2}$ and $C_{40,5}$ are each other's dual codes.
As for $C_{40,3}$, its minimum distance is 8 and the minimum distance of $C_{40,4}$ is 6, with $C_{40,3}$ and $C_{40,4}$ being each other's dual codes.

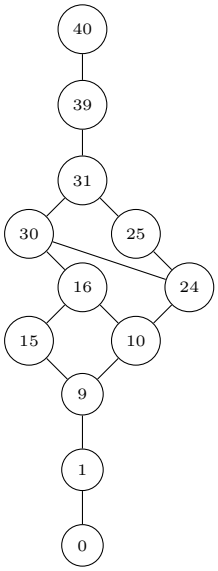
4.3.2 Representation of degree 40

For the maximal subgroup M_2 of a permutation group acting on a set Ω of size 40, we identify a 40-dimensional permutation module that is invariant under the action of G. This permutation module serves as our working module, and we proceed to analyze all of its submodules. The module decomposes into submodules with dimensions $0, 1, 9, 10, 15, 16, 24, 25, 30, 31, 39$, and 40.

This shows that the only irreducible submodule is of dimension 0. The non-trivial submodules have dimensions $1, 9, 10, 15, 16, 24, 25, 30, 31$, and 39. Therefore, according to Theorem 2.3.2, it suffices to find codes of dimensions $9, 10, 15, 16, 24, 25, 30$ and 31. We will denote these codes by:

1. $C_{40,1} = [40, 9, 16]$.
2. $C_{40,2} = [40, 10, 12]$.
3. $C_{40,3} = [40, 15, 10]$.
4. $C_{40,4} = [40, 16, 10]$.
5. $C_{40,5} = [40, 24, 6]$.
6. $C_{40,6} = [40, 25, 4]$.
7. $C_{40,7} = [40, 30, 4]$.
8. $C_{40,8} = [40, 31, 4]$.

Figure 4.2: Submodule lattice for a 40-dimensional representation.



Proposition 4.3.7. *$C_{40,1}$ is a code and $C_{40,8}$ is its dual code; they have minimum distances of 16 and 4, respectively. Moreover, $C_{40,1} \leq C_{40,8}$.*

Proof. Same proof as Proposition 4.3.5. □

Using MAGMA, we find that the minimum distance of $C_{40,2}$ is 12 and the minimum distance of $C_{40,7}$ is 4. From the fact that if $C = [n, k, d]$ then $C^{\perp} = [n, n-k, d']$, we can conclude that $C_{40,2}$ and $C_{40,7}$ are each other's dual codes.

Similarly, $C_{40,3}$ with minimum distance 10 and $C_{40,6}$ with minimum distance 4 are also each other's dual codes. We also find that the minimum distance of $C_{40,4}$ is 10, and the minimum distance of $C_{40,5}$ is 6; these codes are each other's dual codes as well.

4.3.3 Representation of degree 45

For the maximal subgroup M_3 of a permutation group acting on the set Ω of degree 45, we find a 45-dimensional permutation module invariant under G. We take this permutation module as our working module and identify all its submodules. This permutation module breaks into submodules of dimensions;
$0, 1, 14, 15^3, 16, 20, 21^3, 22, 23, 24^3, 25, 29, 30^3, 31, 44$, and 45.
This shows that the only irreducible submodule is of dimension 0. The non-trivial submodules have dimensions $1, 14, 15^3, 16, 20, 21^3, 22, 23, 24^3, 25, 29, 30^3, 31$, and 44. Therefore, according to Theorem 2.3.2, it suffices to find codes of dimensions
$14, 15^3, 16, 20, 21^3, 22, 23, 24^3, 25, 29, 30^3$, and 31. We will denote these codes by:

1. $C_{45,1} = [45, 14, 12]$.
2. $C_{45,2} = [45, 15, 9]$.
3. $C_{45,3} = [45, 15, 12]$.
4. $C_{45,4} = [45, 15, 12]$.
5. $C_{45,5} = [45, 16, 9]$.
6. $C_{45,6} = [45, 20, 8]$.
7. $C_{45,7} = [45, 21, 8]$.
8. $C_{45,8} = [45, 21, 8]$.
9. $C_{45,9} = [45, 21, 5]$.
10. $C_{45,10} = [45, 22, 5]$.
11. $C_{45,11} = [45, 23, 8]$.
12. $C_{45,12} = [45, 24, 6]$.
13. $C_{45,13} = [45, 24, 8]$.
14. $C_{45,14} = [45, 24, 8]$.
15. $C_{45,15} = [45, 25, 6]$.
16. $C_{45,16} = [45, 29, 6]$.
17. $C_{45,17} = [45, 30, 6]$.
18. $C_{45,18} = [45, 30, 5]$.
19. $C_{45,19} = [45, 30, 5]$.
20. $C_{45,20} = [45, 31, 5]$.

Proposition 4.3.8. *1. $C_{45,1}$ is a code, and $C_{45,20}$ is its dual code; they have minimum distances of 12 and 5, respectively. Moreover, $C_{45,1} \leq C_{45,20}$.*

2. $C_{45,2}$ *is a code, and* $C_{45,17}$ *is its dual code; they have minimum distances of* 9 *and* 6, *respectively. Moreover,* $C_{45,2} \leq C_{45,17}$.

3. *There are two isomorphic codes,* $C_{45,3}$ *and* $C_{45,4}$, *which are codes isomorphic to* $C_{45,18}$ *and* $C_{45,19}$ *such that they are each other's dual codes and have minimum distances of* 12 *and* 5, *respectively. Moreover,* $(C_{45,3}, C_{45,4}) \leq (C_{45,18}, C_{45,19})$.

4. $C_{45,5}$ *is a code, and* $C_{45,16}$ *is its dual code; they have minimum distances of* 9 *and* 6, *respectively. Moreover,* $C_{45,5} \leq C_{45,16}$.

5. $C_{45,6}$ *is a code, and* $C_{45,15}$ *is its dual code; they have minimum distances of* 8 *and* 6, *respectively. Moreover,* $C_{45,6} \leq C_{45,15}$.

6. *There are two isomorphic codes,* $C_{45,7}$ *and* $C_{45,8}$, *which are codes isomorphic to* $C_{45,14}$ *and* $C_{45,13}$ *such that they are each other's dual codes and have minimum distances of* 8 *and* 8, *respectively. Moreover,* $(C_{45,7}, C_{45,8}) \leq (C_{45,14}, C_{45,13})$.

7. $C_{45,9}$ *is a code, and* $C_{45,12}$ *is its dual code; they have minimum distances of* 5 *and* 6, *respectively. Moreover,* $C_{45,9} \leq C_{45,12}$.

8. $C_{45,10}$ *is a code, and* $C_{45,11}$ *is its dual code; they have minimum distances of* 5 *and* 8, *respectively. Moreover,* $C_{45,10} \leq C_{45,11}$.

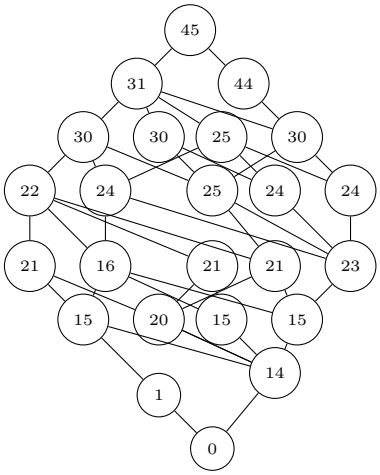
Proof. Same proof as Proposition 4.3.5. □

The submodule lattice of this representation as shown in Figure 4.3.

4.3.4 Representation of degree 36

For the maximal subgroup M_4 of a permutation group acting on the set Ω of degree 36, we find a 36-dimensional permutation module invariant under G. We take this permutation module as our working module and identify all submodules. This permutation module breaks into submodules of dimensions $0, 1, 6, 7, 15, 16, 20, 21, 29, 30, 35$, and 36. This shows that the only irreducible submodule is of dimension 0. The non-trivial submodules have dimensions $1, 6, 7, 15, 16, 20, 21, 29, 30$, and 35. Therefore, according to Theorem 2.3.2, it suffices to find codes of dimensions $6, 7, 15, 16, 20, 21, 29$ and 30. We will denote these codes by:

Figure 4.3: Submodule lattice for a 45-dimensional representation.



1. $C_{36,1} = [36, 6, 16]$.
2. $C_{36,2} = [36, 7, 16]$.
3. $C_{36,3} = [36, 15, 8]$.
4. $C_{36,4} = [36, 16, 8]$.
5. $C_{36,5} = [36, 20, 6]$.
6. $C_{36,6} = [36, 21, 6]$.
7. $C_{36,7} = [36, 29, 4]$.
8. $C_{36,8} = [36, 30, 3]$.

Proposition 4.3.9. *1. $C_{36,1}$ is a code, and $C_{36,8}$ is its dual code; they have minimum distances of* 16 *and* 3*, respectively. Moreover, $C_{36,1} \leq C_{36,8}$.*

2. $C_{36,2}$ is a code, and $C_{36,7}$ is its dual code; they have minimum distances of 16 *and* 4*, respectively. Moreover, $C_{36,2} \leq C_{36,7}$.*

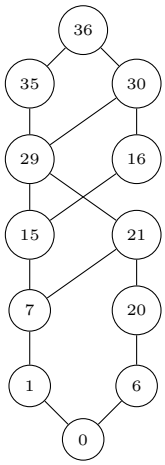
3. $C_{36,3}$ is a code, and $C_{36,6}$ is its dual code; they have minimum distances of 8 *and* 6*, respectively. Moreover, $C_{36,3} \leq C_{36,6}$.*

4. $C_{36,4}$ is a code, and $C_{36,5}$ is its dual code; they have minimum distances of 8 *and* 6*, respectively. Moreover, $C_{36,4} \leq C_{36,5}$.*

Proof. Same proof as Proposition 4.3.5. □

The submodule lattice of this representation as shown in Figure 4.4.

Figure 4.4: Submodule lattice for a 36-dimensional representation



4.3.5 Representation of degree 27

For the maximal subgroup M_5 of a permutation group acting on the set Ω of degree 27, we find a 27-dimensional permutation module invariant under G. We take this permutation module as our working module and identify all submodules. This permutation module breaks into submodules of dimensions $0, 1, 6, 7, 20, 21, 26$ and 27.
This shows that the only irreducible submodule is of dimension 0. The non-trivial submodules have dimensions $1, 6, 7, 20, 21, 26$ and 27. Therefore, according to Theorem 2.3.2, it suffices to find codes of dimensions $6, 7, 20, 21$, and 26. We will denote these codes by:

1. $C_{27,1} = [27, 6, 12]$.
2. $C_{27,2} = [27, 7, 11]$.
3. $C_{27,3} = [27, 20, 4]$.
4. $C_{27,4} = [27, 21, 3]$.

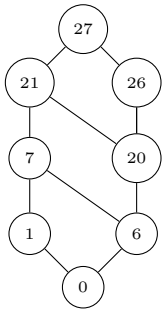
Proposition 4.3.10. *1. $C_{27,1}$ is a code, and $C_{27,4}$ is its dual code; they have minimum distances of 12 and 3, respectively. Moreover, $C_{27,1} \leq C_{27,4}$.*

2. A $C_{27,2}$ is a code, and $C_{27,3}$ is its dual code; they have minimum distances of 11 and 4, respectively. Moreover, $C_{27,2} \leq C_{27,3}$.

Proof. Same proof as Proposition 4.3.5. □

The submodule lattice of this representation as shown in Figure 4.5.

Figure 4.5: Submodule lattice for a 27-dimensional representation.



Non-binary codes

Proposition 4.3.11. *Let $G = PSp_4(3)$ be the projective symplectic group. Then:*

1. *If M_1 is a primitive subgroup of degree 40, then the ternary linear code $C_{27} = [40, 10, 18]$ is divisible by 3 and is irreducible. Its dual ternary linear code is $[40, 30, 4]$, with dimension 30. This dual code is also divisible by 3 and is self-orthogonal.*

2. *If M_2 is a primitive subgroup of degree 40, then the ternary linear code $C_{27} = [40, 16, 8]$ is divisible by 3. Its dual binary linear code is $[40, 24, 6]$, with dimension 24. This dual code is divisible by 3 and it is self-orthogonal.*

3. *If M_3 is a primitive subgroup of degree 36, then the ternary linear code $C_{15} = [36, 15, 9]$ is divisible by 3. Its dual binary linear code is $[36, 21, 6]$, with dimension 21. This dual code is divisible by 3 and is self-orthogonal.*

4. *If M_4 is a primitive subgroup of degree 45, then the ternary linear code $C_{12} = [45, 15, 12]$ is divisible by 3. Its dual binary linear code is $[45, 30, 6]$, with dimension 30. This dual code is divisible by 3 and it is self-orthogonal.*

Proof. Using MAGMA, the weight distributions of the codes under $PSp_4(3)$ are given in the Table 4.17.

□

Table 4.17: Codes

Name	Codes	Weight distribution	Design
C_{27}	$[40, 10, 18]$	$[0^1, 18^{1560}, 24^{21060}, 27^{18800}, 30^{16848}, 36^{780}]$	$1-(40, 27, 27)$
C_{27}	$[40, 14, 12]$	$[0^1, 12^{540}, 15^{3600}, 18^{39360}, 21^{305280}, 24^{1228320}, 27^{1982240}, 30^{1017648}, 33^{193680}, 36^{11580}, 39^{720}]$	$1-(40, 27, 27)$
C_{15}	$[36, 15, 9]$	$[0^1, 9^{80}, 12^{3240}, 15^{43632}, 18^{693600}, 21^{3355344}, 24^{5992110}, 27^{3654320}, 30^{587736}, 33^{18360}, 36^{484}]$	$1-(36, 15, 15)$
C_{12}	$[45, 15, 12]$	$[0^1, 12^{90}, 15^{11523}, 18^{8660}, 21^{92340}, 24^{952020}, 27^{3394640}, 30^{5270400}, 33^{3712770}, 36^{850170}, 39^{63360}, 42^{3060}, 45^{244}]$	$1-(45, 12, 12)$

Non-binary codes from representation of degree 40

For M_1, we are interested in constructing linear codes of length 40 over the finite field $\mathbb{F}_q$, where q is a prime factor of $|G|$. This method is particularly useful for constructing non-binary codes. In this section, we will focus on constructing codes of length 40 over $\mathbb{F}_3$, which are referred to as ternary codes.

In the field $\mathbb{F}_3$, the permutation module of degree 40 decomposes into submodules of the following dimensions: $0, 1, 10, 11, 15, 16, 25, 29, 30, 39$ and 40. These dimensions represent the distinct submodules that arise when the permutation module is decomposed. This decomposition is an essential part of understanding the structure of the codes, we aim to construct.

According to Theorem 2.3.2, it is sufficient to find codes with the specified dimensions. As a result, there are 8 non-trivial ternary codes that admit $PSp_4(3)$ as a primitive permutation group. We have already determined the lengths and dimensions of these ternary codes, and the remaining task is to determine their minimum distances in order to fully characterize the codes. Using MAGMA, we find the following non-trivial codes:

1. $C^*_{40,1} = [40, 10, 18]$.
2. $C^*_{40,2} = [40, 11, 13]$.
3. $C^*_{40,3} = [40, 15, 8]$.
4. $C^*_{40,4} = [40, 16, 8]$.
5. $C^*_{40,5} = [40, 24, 6]$.
6. $C^*_{40,6} = [40, 25, 4]$.
7. $C^*_{40,7} = [40, 29, 6]$.
8. $C^*_{40,8} = [40, 30, 4]$.

Proposition 4.3.12. *1. $C^*_{40,1}$ is a code and $C^*_{40,8}$ is its dual code, with minimum distances 18 and 4 respectively. Moreover, $C^*_{40,1} \leq C^*_{40,8}$.*

2. $C^*_{40,2}$ is a code and $C^*_{40,7}$ is its dual code, with minimum distances 13 and 6 respectively. Moreover, $C^*_{40,2} \leq C^*_{40,7}$.

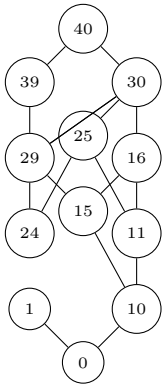
3. $C^*_{40,3}$ *is a code and* $C^*_{40,6}$ *is its dual code, with minimum distances* 8 *and* 4 *respectively. Moreover,* $C^*_{40,3} \leq C^*_{40,6}$.

4. $C^*_{40,4}$ *is a code and* $C^*_{40,5}$ *is its dual code, with minimum distances* 8 *and* 6 *respectively. Moreover,* $C^*_{40,4} \leq C^*_{40,5}$.

Proof. Same proof as Proposition 4.3.5. □

The submodule lattice is shown in Figure 4.6, which also indicates that the only irreducible code is of dimension 0.

Figure 4.6: Submodule lattice for a 40-dimensional representation in $\mathbb{F}_3$



Non-binary codes from representation of degree 45

For M_3, we aim to find linear codes of length 45 over $\mathbb{F}_q$, where q is a prime divisor of $|G|$. The method outlined here is applicable to constructing non-binary codes. In this case, we focus on finding codes of length 45 over $\mathbb{F}_3$.
In the field $\mathbb{F}_3$, the permutation module of degree 45 decomposes into submodules with dimensions $0, 1, 14, 15, 20, 21, 24, 25, 30, 31, 44$, and 45.
According to Theorem 2.3.2, it is sufficient to identify codes with the specified dimensions. As a result, there are 8 non-trivial ternary codes that have $PSp_4(3)$ as a primitive permutation group. We have already determined the lengths and dimensions of these ternary codes, and the next step is to calculate their minimum distances in order to fully characterize the codes. Using MAGMA, we find that the non-trivial codes are as follows:

1. $C^*_{45,1} = [45, 14, 15]$.
2. $C^*_{45,2} = [45, 15, 12]$.
3. $C^*_{45,3} = [45, 20, 8]$.
4. $C^*_{45,4} = [45, 21, 5]$.
5. $C^*_{45,5} = [45, 24, 6]$.
6. $C^*_{45,6} = [45, 25, 6]$.
7. $C^*_{45,7} = [45, 30, 6]$.
8. $C^*_{45,8} = [45, 31, 5]$.

Proposition 4.3.13. *1. $C^*_{45,1}$ is a code and $C^*_{45,8}$ is its dual code, with minimum distances 15 and 5, respectively. Moreover, $C^*_{45,1} \leq C^*_{45,8}$.*

2. $C^*_{45,2}$ is a code and $C^*_{45,7}$ is its dual code, with minimum distances 12 and 6, respectively. Moreover, $C^*_{45,2} \leq C^*_{45,7}$.

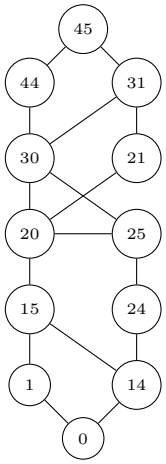
3. $C^*_{45,3}$ is a code and $C^*_{45,6}$ is its dual code, with minimum distances 8 and 6, respectively. Moreover, $C^*_{45,3} \leq C^*_{45,6}$.

4. $C^*_{45,4}$ is a code and $C^*_{45,5}$ is its dual code, with minimum distances 5 and 6, respectively. Moreover, $C^*_{45,4} \leq C^*_{45,5}$.

Proof. Same proof as Proposition 4.3.5. □

The submodule lattice of this representation as shown in Figure 4.7.

Figure 4.7: Submodule lattice for a 45-dimensional representation.



Non-binary codes from representation of degree 36

For M_4, we aim to find linear codes of length 36 over $\mathbb{F}_q$, where q is a prime factor of $|G|$. The method described here is applicable for constructing non-binary codes. Specifically, we will focus on finding codes of length 36 over $\mathbb{F}_3$.
In the field $\mathbb{F}_3$, the permutation module of degree 36 decomposes into submodules with dimensions $0, 1, 14, 15^4, 16, 20, 21^4, 22, 35$ and 36.

1. $C^*_{36,1} = [36, 14, 12]$.
2. $C^*_{36,2} = [36, 15, 11]$.
3. $C^*_{36,3} = [36, 15, 11]$.
4. $C^*_{36,4} = [36, 15, 8]$.
5. $C^*_{36,5} = [36, 15, 9]$.
6. $C^*_{36,6} = [36, 16, 8]$.
7. $C^*_{36,7} = [36, 20, 6]$.
8. $C^*_{36,8} = [36, 21, 6]$.
9. $C^*_{36,9} = [36, 21, 6]$.
10. $C^*_{36,10} = [36, 21, 6]$.
11. $C^*_{36,11} = [36, 21, 6]$.
12. $C^*_{36,12} = [36, 22, 6]$.

Proposition 4.3.14. *1. $C^*_{36,1}$ is a code and $C^*_{36,12}$ is its dual code, with minimum distances 12 and 6, respectively. Moreover, $C^*_{36,1} \leq C^*_{36,12}$.*

2. There are two equal codes, $C^*_{36,2}$ and $C^*_{36,3}$, with $C^*_{36,11}$ and $C^*_{36,10}$ such that their dual codes are also equal, and they have minimum distances 11 and 6, respectively. Moreover, $(C^*_{36,2}, C^*_{36,3}) \leq (C^*_{36,11}, C^*_{36,10})$.

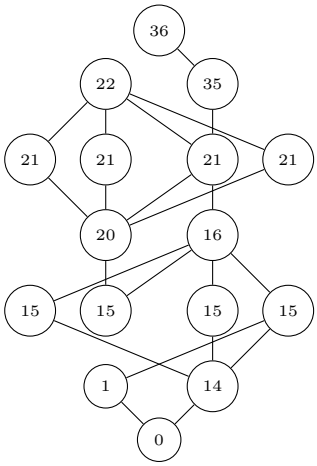
3. *There are two isomorphic codes,* $C^*_{36,4}$ *and* $C^*_{36,5}$*, with* $C^*_{36,9}$ *and* $C^*_{36,8}$ *such that they are isomorphic to their dual codes, and they have minimum distances* 8, 9, *and* 6, *respectively. Moreover,* $(C^*_{45,7}, C^*_{45,8}) \leq (C^*_{45,14}, C^*_{45,13})$.

4. $C^*_{36,6}$ *is a code and* $C^*_{36,7}$ *is its dual code, with minimum distances* 8 *and* 6, *respectively. Moreover,* $C^*_{36,6} \leq C^*_{36,7}$.

Proof. Same proof as Proposition 4.3.5. □

The submodule lattice of this representation is shown in Figure 4.8.

Figure 4.8: Submodule lattice for a 36-dimensional representation.



Non-binary codes from representation of degree 27

For M_5, we aim to find linear codes of length 27 over $\mathbb{F}_q$, where q is a prime divisor of $|G|$. The method presented here is applicable for constructing non-binary codes. Specifically, we focus on finding codes of length 27 over $\mathbb{F}_3$.

In the field $\mathbb{F}_3$, the permutation module of degree 27 decomposes into submodules with dimensions $0, 1, 6, 7, 20, 21, 26$, and 27.

According to Theorem 2.3.2, it is sufficient to identify codes with the specified dimensions. As a result, there are 4 non-trivial ternary codes that have $PSp_4(3)$ as a primitive permutation group. We have already determined the lengths and dimensions of these ternary codes, and the next step is to calculate their minimum distances in order to fully define the codes. Using MAGMA, we find the following non-trivial codes:

1. $C^*_{27,1} = [27, 6, 12]$.
2. $C^*_{27,2} = [27, 7, 11]$.
3. $C^*_{27,3} = [27, 20, 4]$.
4. $C^*_{27,4} = [27, 21, 3]$.

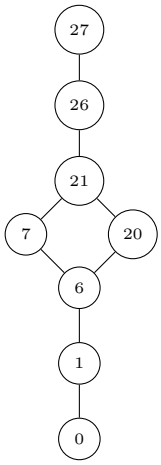
Proposition 4.3.15. *1. A code $C^*_{27,1}$ has a dual code $C^*_{27,4}$, and they have minimum distances 12 and 3, respectively. Moreover, $C^*_{27,1} \leq C^*_{27,4}$.*

2. A code $C^*_{27,2}$ has a dual code $C^*_{27,3}$, and they have minimum distances 11 and 4, respectively. Moreover, $C^*_{27,2} \leq C^*_{27,3}$.

Proof. Same proof as Proposition 4.3.5. □

The submodule lattice of this representation as shown in Figure 4.9.

Figure 4.9: Submodule lattice for a 27-dimensional representation



4.3.6 Conclusion

The primary aim of constructing codes from the group $PSp_4(3)$ was to explore the symmetries and structural properties of these codes within the framework of combinatorial designs and group theory. By leveraging the projective symplectic group $PSp_4(3)$, we were able to construct error-correcting codes that exhibit robust algebraic properties, such as invariance under the group action. These constructions not only deepen our understanding of the interaction between group actions and coding theory but also reveal the potential for applying these codes to various practical areas, including cryptography and communication systems.

Furthermore, the investigation into lattices provided valuable insights into the geometric structures associated with the codes, particularly in how these lattices reflect the symmetries of the group $PSp_4(3)$ The lattice theory approach helped in understanding the modular relationships between different code structures and their representation within a lattice framework. This comprehensive approach has the potential to inform the development of new coding schemes and combinatorial designs, contributing to both theoretical advancements and practical applications in fields reliant on error correction and information security.

In summary, the construction of codes from $PSp_4(3)$ and their connection to lattice theory not only fulfills the theoretical objectives but also paves the way for future research in the application of symmetries and group actions in coding theory.

Bibliography

[1] R. Allenby and E. Redfern, *Introduction to Number Theory with Computing*, 1989.

[2] J. L. Alperin and R. B. Bell, *Groups and Representations*, Springler, 1995.

[3] E. B. Al-Zagana, *Finite Projective Geometry and Its Application*, Mustansiriyah University, College of Science, Dept. of Math., 2016 – 2017.

[4] E. F. Assmus Jr. and J. D. Key, *Designs and Their codes*, Cambridge Tracts in Mathematics, Vol. 103, 1993.

[5] J. Baylis, *Error-correcting codes*, Department of Mathematics, Nottingham-Trent University, UK, Springer Dordrecht, 1998.

[6] L. Bolcar, *On the Weights of Linear Codes and Their Dual*, Digital commons, 2020.

[7] W. Bosma, J. Cannon, and C. Playoust, The MAGMA Algebra System I: *The User Language*, Journal of Symbolic Computation, 24(3-4), pp. 235 – 265, 1997.

[8] R. Brauer, *On Modular Characters of Groups*, Annals of mathematics 42, pp. 556 – 590, 1941.

[9] B. M. Burton, *Elementary Number Theory*, 6^{th} edition, Americas, New York, 2007.

[10] L. Chikamai, J. Moori, and B. G. Rodrigues, *Linear codes obtained from 2-Modular Representations of Some Finite Simple Groups*, Ph.D. thesis, University of Kwazulu Natal, 2012.

[11] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *An Atlas of Finite Groups*, Oxford University Press, 1985.

[12] M. R. Darafsheh, *Designs from the Group $PSL_2(q)$, q even*, Des. Codes Crypt., 39(3), pp. 15 – 168, 2006.

[13] M. R. Darafsheh, B. G. Rodrigues, and A. Saeidi, *On Codes and Designs Admitting the Mathieu group M_{11} as Permutation Automorphism Group*, Mathematical communication, 28 pp. 85 – 104, 2013.

[14] C. Ding and C. Tang, *Designs from Linear Codes*, Second Edition, World Scientific, 2022.

[15] D. S. Dummit and R. M. Foote, *Abstract Algebra*, John Wiley and Sons, Inc., 2004.

[16] M. Golay, *Notes on Digital Coding*, Proc. IRE, 37, pp. 657 – 662, 1948.

[17] R. W. Hamming, *Error Detecting and Correcting Codes*, Bell System Technical Journal, Vol. 26, No 2.

[18] A. S. Herbert, *Science of the Artificial*, Inc., 1969. Download: www.interaction-design.org, 2021.

[19] D. G. Higman, *Finite Permutation Groups of Rank*-3, Math. Zeitschr, 86, pp. 145 – 156, 1964.

[20] R. Hill, *A first course in Coding Theory*, Oxford Applied Mathematics and Computing Science Series, Oxford University Press Inc., New York, 1986.

[21] W. C. Huffman, *Codes and Groups* Handbook of Coding Theory, Vol. 2, Part 2, Chapter 17, Amsterdam, Elsevier, pp. 1345 – 1440, 1998.

[22] I. M. Isaacs, *The Character Theory of Groups*, Press, San Diego, 1976.

[23] D. C. Lay, S. R. Lay and J. J. McDonald, *Linear Algebra and Its Application*, Pearson, 2015.

[24] W. M. Kantor, *Permutation Representations of the Finite Classical Groups of Small Degree or Rank*, J. Algebra, 60, pp. 15 – 168, 1979.

[25] J. D. Key and E. F. *Assmus, Discrete Mathematics, Information Theory and Coding*, Recreational Mathematics, Cambridge University Press, 1992.

[26] J. D. Key and E. F. Assmus, *Designs and Their Codes*, Volume 103 of Cambridge Tracts in Mathematics, 1992.

[27] J. D. Key and J. Moori, *Designs, Codes and Graphs from Janko Group J_1 and J_2*, J. Combin. Math. Combin. Comput., 40, pp. 143 – 159, 2002.

[28] J. D. Key, J. Moori and B. G. Rodrigues, *On Some Designs and Codes from Primitive Representations of Some Finite Groups*, J. Combin. Math. Combin. Comput., 45, pp. 3 – 19, 2003.

[29] O. H. King, *The Subgroup Structure of Finite Classical Groups in Terms of Geometric Configuration*, Invent. Math, pp. 8 – 10.

[30] T. Lê and J. Moori, *On the Automorphisms of Designs Constructed from Finite Simple Groups*, *Springer Science+Business Media* (NY), 10 – 44 2014.

[31] Y. Lindell, *Introduction to Coding Theory*, Lecture Notes, Department of Computer Science, Bar-Ilan University, Israel. January 25, 2010.

[32] X. Mbaale, B. G. Rodrigues, and S. Zandi, *Design from Maximal Subgroups and Conjugacy Classes of $PSL_2(q)$*, AUT Journal of Mathematics and Computing, 4(1) pp. 47 – 55, 2023. https://doi.org/10.22060/AJMC.2022.21877.1117

[33] Maxima. (2023). *Maxima, a Computer Algebra System. Version 5.47.0*. Retrieved from `https://maxima.sourceforge.io/`

[34] J. Moori, *Finite Groups Designs, and Codes*, Information Security, Coding Theory and Related Combinatorics. NATO Science for Peace and Securiy Series D Information and Communication security, Vol. 29. Amsterdam, IOS, pp. 202 – 230, 2011.

[35] J. Moori, *Designs and codes from $PSL_2(q)$*, (English Summary), Group Theory, Combinatorics, and Computing, Contemporary Mathematics, Vol. 611. Providence, RI, American Mathematical Socity, pp. 143 – 159, 2014.

[36] J. Moori and A. Saeidi, *Some Designs and Codes Invariant under the Tits Group*, Math. Commun, 2016.

[37] J. Moori, *Designs and Codes from Fixed Points from Finite Group*, Communications in Algebra, 49(2), pp. 706 − 720, 2021.

[38] J. Moori and A. Saeidi, *Some Designs and codes Invariant Under the Tits Group*, Adv. Math. Commun., 11(1), pp. 77 − 82, 2017.

[39] J. Moori and A. Saeidi, *Constructing Some Designs Invariant Under $PSL_2(q)$, q even*, Communications in Algebra, 46(1), pp. 160 − 166, 2018.

[40] J. Moori and A. Saeidi, *Some Designs Invsriant Under the Suzuki Groups*, Util. Math., 109, pp. 105 − 114, 2018.

[41] J. Moori, *Designs and Codes from Finite Groups*, North-West Universty (Mafikeng Campus, South Africa), University of Birmingham (UK), 2020.

[42] J. Moori and B. G. Rodrigues, *A Self-orthogonal Doubly even Codes Invariant Under MCL:* 2, J. Combin. Theory Ser. A, 110(1), pp. 53 − 69, 2005.

[43] J. Moori, *Representation Theory*, Lecture Notes, Mathematical Sciences, North-West Universty, Mafikeng, 2011.

[44] A. Pascoe, *Affine and Projective planes*, MSU Graduate Thesis, 3233, 2018.

[45] R. Prag, *A Brief Summary of Modular Representation Theory*, Lecture notes, 2021.

[46] B. G. Rodrigues, *Codes of Designs and Graphs from Finite Simple Groups*, School of Mathematics, Statistics and Information Technology. University of Natal, Pietermaritzburg, 2002.

[47] B. G. Rodrigues, *Topics in Permutation Group Theory*, University of KwaZulu-Natal, December 09, 2019, Combin. Theory Ser., A, 110(1), pp. 53 − 69, 2005.

[48] A. Saeidi, *Group Structures*, Study Guide, *Faculty of Science and Agriculture,* University of Limpopo, January 2022.

[49] A. Saeidi, *Reduced Designs Constructed by Key-Moori Method* 2 *and Their Connection with Method* 3, School of Mathematical and Computer Sciences, University of Limpopo (Turfloop) Sovenga, South Africa. AUT J. Math. Com., 4(1), pp. 39 − 46, 2023. https://doi.org/10.22060/ajmc.2022.21378.1092

[50] M. A. Shahabi and H. Mohtadifar, *The Characters of Finite Projective Symplectic Group $PSp_4(q)$*, University Tabriz, Iran, 2018.

[51] B. Srinivasa, *The Characters of the Finite Symplectic Group $Sp(4,q)$*, Transactions of the American Mathematical Society, May, Vol. 131(2), pp. $488-525$, May 1968.

[52] J. A. Thas, *Symplectic spread in $PG_3(q)$*, Inversive Planes and Projective Planes, University of Gent, Krijgslaan, Belgium, 1994.

[53] T. P. Wakefield, *Verifyng Huppert's Conjecture for $PSp_4(q)$ when $q = 7$*, Springer Science, Business Media, 2010.

[54] S. H. Weintruab, *Representation Theory of Finite Group: Algebra and Arithmetic*, American Mathematics Society, 2003.

[55] R. A. Wilson, *The Finite Simple Groups*, Graduate Texts in Mathematics, Vol. 251, Springer-Verlag, London, 2009.

[56] W. J. Wong, A Characterization of the Finite Projective Symplectic Groups $PSp_4(q)$, National Science Foundation grant GP-6652, University of Notre Dame, 1967.