PERMUTATION GROUPS AND INDUCED ACTIONS ON k-SUBSETS

A thesis submitted to the University of Manchester
for the degree of Doctor of Philosophy
in the Faculty of Science and Engineering

2020

Awatef Hoidi Almotairi
School of Natural Science
Department of Mathematics

Contents

Abstract **7**

Declaration **8**

Copyright Statement **9**

Acknowledgements **10**

Group Notation **11**

1 Introduction **13**

2 Background Material **19**

2.1 General Notation 19

2.2 Group Action 20

2.3 The Induced Action on k-subsets 22

2.4 General Linear Groups 26

3 Number of G-orbits in $PSL(3,q)$ **28**

3.1 Background Material 28

3.2 The Projective Special Linear Group $PSL(3,q)$ 30

3.2.1 The Subgroups of $PSL(3,q)$ 30

3.2.2 Conjugacy Classes of $PSL(3,q)$ 31

3.3 Main Results 34

3.3.1 Number of fixed k-subsets by elements in $\mathcal{C}_6 \cup \mathcal{C}'_6$ 37

3.3.2 Proof of Theorem 3.3.1 43

4 Orbit Lengths **46**

4.1 Introduction 46

4.2 General Results 47

4.3 Orbit Lengths when $k = 3$, 4 or 5 52

4.3.1 $PSL(2, 11)$ 54

4.3.2 $PSL(2, 16)$ 55

4.4 Orbit Length of $PSL(2, 2^n)$ 58

4.4.1 Orbit Lengths when $k = 5$ 60

4.4.2 Orbit Length when $k = 6$ 62

4.4.3 Orbit Length when $k = 7$ 64

5 Counting G-Orbits of some primitive permutation groups of small degree **71**

5.1 Number and length of G-orbits of some finite primitive groups 72

5.1.1 $PSL(2, 7)$ of degree 7 74

5.1.2 $PSL(2, 7)$ of degree 8 74

5.1.3 Alt(6) of degree 10 75

5.1.4 $PSL(2, 11)$ of degree 11 76

5.1.5 $PSL(2, 11)$ of degree 12 77

5.1.6 M_{11} of degree 11 78

5.1.7 M_{11} of degree 12 79

5.1.8 M_{12} of degree 12 80

5.1.9 Alt(5) of degree 10 81

5.1.10 Alt(7) of degree 15 83

5.1.11 $PSL(2, 13)$ of degree 14 85

5.1.12 Alt(6) of degree 15 89

5.1.13 $ASL(2, 4)$ of degree 16 93

Bibliography **100**

A MAGMA codes of Chapter 2 **104**

B MAGMA codes of Chapter 3 **107**

C MAGMA codes of Chapter 4 **116**

D MAGMA codes of Chapter 5 **118**

E Tables for Chapter 5 **120**

E.0.1 Alt(5) of degree 10 120

E.0.2 Alt(7) of degree 15 121

E.0.3 $PSL(2, 13)$ of degree 13 123

List of Tables

3.1 Conjugacy classes of $PSL(3, q)$ . . . 32

3.2 Cycle types of elements in $PSL(3, q)$ . . . 35

3.3 Cycle types of elements of $\mathcal{C}_6 \cup \mathcal{C}'_6$ in $PSL(3, 73)$ . . . 37

4.1 Primitive permutation groups satisfying Hypothesis($*$) . . . 49

4.2 The non-zero values of $f_k(H)$ for some subgroups H of $PSL(2, q)$ . . . 51

4.3 Size of orbits on k-subsets . . . 52

4.4 Number and cycle structure of elements of $PSL(2, 16)$ . . . 55

4.5 Number and length of orbits of $PSL(2, 16)$ in its action on Ω_6 . . . 64

4.6 Number and length of orbits of $PSL(2, 16)$ in its action on Ω_8 . . . 66

5.1 G-orbits of Alt(6) on its action on a set of 15 points . . . 93

5.2 G-orbits of $ASL(2, 4)$ on its action on a set of 16 points . . . 99

B.1 $PSL(3, 7)$ . . . 113

B.2 $PSL(3, 8)$ . . . 114

B.3 $PSL(3, 9)$ . . . 115

E.1 G-orbits of Alt(5) on its action on a set of 10 points . . . 121

E.2 G-orbits of Alt(7) on its action on a set of 15 points . . . 122

E.3 G-orbits of $PSL(2, 13)$ on its action on a set of 14 points . . . 124

List of Figures

5.1 G-orbits of $PSL(2,7)$ on its action on a set of 7 points 74

5.2 G-orbits of $PSL(2,7)$ on its action on a set of 8 points 75

5.3 G-orbits of Alt(6) on its action on a set of 10 points 76

5.4 G-orbits of $PSL(2,11)$ on its action on a set of 11 points 77

5.5 G-orbits of $PSL(2,11)$ on its action on a set of 12 points 78

5.6 G-orbits of M_{11} on its action on a set of 11 points 79

5.7 G-orbits of M_{11} on its action on a set of 12 points 80

5.8 G-orbits of M_{12} on its action on a set of 12 points 81

5.9 G-orbits of Alt(5) on its action on a set of 10 points 82

5.10 G-orbits of Alt(7) on its action on a set of 15 points 84

5.11 G-orbits of $PSL(2,13)$ on its action on a set of 14 points 86

The University of Manchester

Awatef Hoidi Almotairi
Doctor of Philosophy
Permutation Groups and Induced Actions on k-subsets
February 13, 2020

Assume that G is a permutation group acting upon a set Ω of size n. Then a group action of G induces an action on Ω_k, the set of all k-subsets of Ω. In this thesis we derive a formulae to calculate the number of G-orbits on Ω_k, where $G \cong PSL(3, q)$ on its action upon $q^2 + q + 1$ points of the projective plane over $GF(q)$.

We investigate the situation when a G-orbit of a k-subset is of the maximal length $|G|$ and all $(k + 1)$-subsets encompassing it are of lengths less than $|G|$. We examine this case when $G \cong PSL(2, q)$ in its action on the projective line of $q + 1$ points.

We subsequently pay attention to count the G-orbits on Ω_k for several primitive groups of small degrees.

Declaration

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

Copyright Statement

i. The author of this thesis (including any appendices and/or schedules to this thesis) owns certain copyright or related rights in it (the "Copyright") and s/he has given The University of Manchester certain rights to use such Copyright, including for administrative purposes.

ii. Copies of this thesis, either in full or in extracts and whether in hard or electronic copy, may be made **only** in accordance with the Copyright, Designs and Patents Act 1988 (as amended) and regulations issued under it or, where appropriate, in accordance with licensing agreements which the University has from time to time. This page must form part of any such copies made.

iii. The ownership of certain Copyright, patents, designs, trade marks and other intellectual property (the "Intellectual Property") and any reproductions of copyright works in the thesis, for example graphs and tables ("Reproductions"), which may be described in this thesis, may not be owned by the author and may be owned by third parties. Such Intellectual Property and Reproductions cannot and must not be made available for use without the prior written permission of the owner(s) of the relevant Intellectual Property and/or Reproductions.

iv. Further information on the conditions under which disclosure, publication and commercialisation of this thesis, the Copyright and any Intellectual Property and/or Reproductions described in it may take place is available in the University IP Policy (see http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=487), in any relevant Thesis restriction declarations deposited in the University Library, The University Library's regulations (see http://www.manchester.ac.uk/library/aboutus/regulations) and in The University's Policy on Presentation of Theses.

Acknowledgements

First and foremost, great thanks and praise to ALLAH Almighty for granting me the strength and health to complete this thesis.

I would like to thank my supervisor Professor Peter Rowley for all his academic guidance, encouragement, and invaluable advice throughout the course of my PhD study. Without him I would never have accomplished the completion of this thesis.

My deepest thanks go to my parents for their endless prayers, love and support which I will not be able to repay even if I tried for the rest of my life. I extend my thanks to my brothers and sisters (the real joys in my life); words cannot express my great gratitude for their consistent, never-ending, support and encouragement.

Last but not least, I offer my sincerest thanks to my friends in Manchester and in my home country for their love, words of encouragement, and for being supportive throughout trying times.

Group Notation

C_n	Cyclic group of order n.
$\langle g \rangle$	A subgroup of G that generated by element g.
$\mathbb{Z}_n$	Integer modulo n, ($\mathbb{Z}_n$ isomorphic to C_n).
$H_1 \times H_2$	The direct product group of two groups H_1 and H_2.
$H : K$	Split extension of H by K.
$Aut(G)$	The automorphisms of G under composition.
$\mathrm{Sym}(n)$	Symmetric group (permutations of a set $\{1, 2, ..., n\}$ under composition).
$\mathrm{Alt}(n)$	Alternating group (subgroup of $Sym(n)$ consists of even permutations).
$\mathrm{Dih}(2n)$	Dihedral group of degree n and order $2n$ (the group of symmetries of a regular polygon of n vertices).
$GL(n, \mathbb{F})$	General linear group over a field $\mathbb{F}$ ($n \times n$ invertible matrices with entries in the field $\mathbb{F}$).
$SL(n, \mathbb{F})$	Special linear group over a field $\mathbb{F}$ (subgroup of $GL(n, \mathbb{F})$ whose elements have determinant 1).
$PGL(n, \mathbb{F})$	Projective general linear group over a field $\mathbb{F}$ (the quotient of $GL(n, \mathbb{F})$ by its center).
$PSL(n, \mathbb{F})$	Projective special linear group over a field $\mathbb{F}$ (the quotient of $SL(n, \mathbb{F})$ by its center).
$AGL(n, \mathbb{F})$	Affine general linear group over $\mathbb{F}$ (the semidirect product of the vector space $\mathbb{F}^n$ by $GL(n, \mathbb{F})$, acting by linear transformations).
$ASL(n, \mathbb{F})$	Affine special linear group over $\mathbb{F}$ (the semidirect product of the vector space $\mathbb{F}^n$ by $SL(n, \mathbb{F})$).

$\Gamma L(n, \mathbb{F})$	Semilinear group (the group of all invertible semilinear transformations on the vector space $\mathbb{F}^n$).
$P\Gamma L(n, \mathbb{F})$	Projective semilinear group (the quotient of $\Gamma L(n, \mathbb{F})$ by its center).
$A\Gamma L(n, \mathbb{F})$	Affine semilinear group (the semidirect product of the vector space $\mathbb{F}^n$ by $\Gamma L(n, \mathbb{F})$).
$PSU(n, \mathbb{F})$	Projective special unitary group (the quotient of the special unitary group $SU(n, \mathbb{F})$ by its center).
$M_{11}, ..., M_{24}$	Mathieu groups (simple groups and multiply transitive permutation groups on 11,12,22,23, and 24 points).
$Sz(q)$	Suzuki group (a simple group of order $q^2(q-1)(q^2+1)$, where $q = 2^{2n+1} > 2, n \in \mathbb{N}$).
$R(q)$	Ree group (a simple group of order $q^3(q-1)(q^3+1)$, where $q = 3^{2n+1} > 3, n \in \mathbb{N}$).

Chapter 1

Introduction

It is obvious that studying group actions plays an important role in investigating the structure of a group. Exploring the manner in which elements of a group act on some spaces, such as sets, vector spaces, topological spaces or some other spaces, may allow us to observe connections amid the group and different mathematical areas. Using group actions help us to write abstract groups in terms of permutation groups or matrix groups which can be used to explore deep results in many fields.

In this thesis, we concentrate our attention on studying the induced action on k-subsets. Let G be a finite group acting on a set Ω of n points. Then there is a natural action on Ω_k, the set of all k-subsets of Ω. The number of G-orbits on Ω_k is denoted by σ_k. If G acts transitively on Ω_k, then G is k-homogeneous.

Under consideration of this action, some progress has been made relating to questions regarding the lengths of orbits and the number of orbits. The motivation towards the interest on this topic is due to the pioneering work of Livingstone and Wagner [23], in which they presented the following results:

Theorem 1.0.1 *Let G be permutation group acting upon a set Ω of n points and $k \in \mathbb{N}$ such that $2 \leq k \leq \frac{n}{2}$. Then:*

(i) the number of G-orbits on Ω_k is greater than or equal to the number of G-orbits on Ω_{k-1}.

(ii) if G is k-homogeneous, then G is $(k-1)$-homogeneous.

(iii) if G is k-homogeneous, then G is $(k-1)$-transitive.

(iv) if $k \geq 5$ and G is k-homogeneous, then G is k-transitive.

Their proofs are based on the representation theory of symmetric groups. Soon afterwards, using number theoretic considerations Wielandt [32] gave an elementary proof for Theorem 1.0.1 (ii) under a weaker hypotheses, that is $|\Omega| \geq k + p^a - 1$ for all prime power $p^a|k$. A question arise as a consequence of Theorem 1.0.1 (iv), If $k < 5$, which groups are k-homogeneous but not k-transitive?. Kantor [18] in his paper "k-homogeneous groups" determined all groups that are k-homogeneous but not k-transitive for $k = 2, 3$ and 4. Cameron [6] extended the results of Livingstone-Wagner to an infinite set Ω using incidence matrices. In 2004, Mnukhin and Siemons [25] published their paper "On the Livingstone-Wagner theorem", in which they provided a broader hypothesis concerning number of orbits on subsets. Their general theorem comprised the Livingstone-Wagner Theorem 1.0.1 (i) as a special case and additionally provided information concerning orbits counts for simplicial complexes, sequences, graphs and amalgamation classes. Another generalization of Theorem 1.0.1 (i) is given by Nakashima [27], in which he conjectured that the number of G-orbits on k-subsets on Ω is at least as great as the number of G-orbits on k-tuples on Ω. He was able to prove his conjecture in the simplest case $k = 3$ with condition $|\Omega| > 11$.

Questions emerge as a result of the Livingstone-Wagner theorem (ii) regarding the instances where $\sigma_k = \sigma_{k-1}$. The cases of equality under the assumption that Ω is an infinite were discussed by Cameron [8], whereby he determined the groups that satisfy the equality. These cases were also addressed in 2009 in a paper by Bundy and Hart [4], in which they verified the following result when Ω is a finite set.

Theorem 1.0.2 *Let G be a permutation group and H be a subgroup of G. If $1 \leq k < \frac{(n-1)}{2}$, then $\sigma_{k+1}(G) - \sigma_k(G) \leq \sigma_{k+1}(H) - \sigma_k(H)$. In particular, if $\sigma_{k+1}(H) = \sigma_k(H)$, then $\sigma_{k+1}(G) = \sigma_k(G)$.*

This means that the instance of the equality of $\sigma_k(G)$ and $\sigma_{k+1}(G)$ depends on the equality of the subgroups.

Counting the number of G-orbits was the main topic of Bradley and Rowley's paper [2], they were able to produce four formulas for calculating values of $\sigma_k(G, \Omega)$ for the cases that G is a 2-transitive simple group of Lie rank one, that is $G \cong$

$PSL(2,q), PSU(3,q)$ or $R(q)$. These formulas can be implemented by MAGMA without the need to construct the group G.

On the other hand, the length of the orbit of such a group in its induced action on Ω_k has been studied by many people. In 1988, Siemons and Wagner [29] published their paper "On the relationship between the length of orbits on k-sets and $(k+1)$-sets", in which they studied the case when the orbit length of a k-set is greater than the orbit length of any $(k+1)$-sets containing it. In their paper, they concerned the groups that satisfy the following hypothesis:

$(*)$: Let G be a transitive permutation group on a finite set Ω of n points. Let $k < n$, there is some set $\Delta \subset \Omega$ of size k such that $|\Sigma^G| < |\Delta^G|$ for every set Σ of size $(k+1)$ containing Δ.

If a group G satisfies $(*)$, then the following inequality holds:

$$k+1 \geq |\Delta^{G_\Sigma}| > |\Sigma^{G_\Delta}| \geq 1.$$

Furthermore, they proved that if $k = 2$ and G is a primitive group, then $G \cong PSL(2,5)$ in its natural action on 6 points. The case when $k = 3$ was discussed by Bradley [3], in which he was able to classify all such groups when there is only one orbit on Ω_3.

Theorem 1.0.3 *Let G be a 3-homogeneous permutation groups acting on a set Ω of size $n \geq 8$. If the orbit on 3-subset of Ω has length strictly greater than the G-orbit of any 4-subset of Ω, then $G \cong PSL(2,7)$ or $G \cong PGL(2,7)$.*

Another result on this topic is from Mnukhin [26], in which he discussed a bounding property of the orbit length on k-sets and presented the following result.

Theorem 1.0.4 *Let G be a permutation group acting upon a finite set Ω and let Σ be a k-set, $k \geq 2$. Then there is a $(k-1)$-set Δ subsets of Σ such that*

$$|\Delta^G| \geq \frac{2}{k^2} \cdot |\Sigma^G|^{\frac{k-1}{k}}.$$

So, if Σ^G is a long orbit, then it contains at least one "quit long" sub orbit Δ^G also.

This thesis is devoted to investigating the G-orbits of some finite groups in the set Ω_k. The novel contributions of this thesis can be summarized in the following three points:

- Counting the number of G-orbits of the group $PSL(3, q)$ on Ω_k.
- Exploring the relationship between the length of G-orbits of k-subsets and the length of G-orbit of $(k + 1)$-subsets, where $G \cong PSL(2, 2^n)$ and $2 \leq k \leq 7$.
- Counting the G-orbits of 13 finite primitive groups of small degrees.

We begin Chapter 2 by introducing some of the notation that will be used throughout the thesis. In Section 2.2, we give a brief overview of some well-known results relating to group actions and to the induced actions on k-subsets. At the end of this chapter, we give a brief summary about linear groups, as we will use them extensively in this thesis.

Chapter 3 contains the first contribution of this thesis. Using Burnside's Lemma 2.2.6, we count the value of $\sigma_k(G, \Omega)$, where $G \cong PSL(3, q)$ on its action upon q^2+q+1 points of the projective plane over $GF(q)$. Our method is to find the number of k-subsets that are left fixed by the representatives of the conjugacy classes of G. To do so, we follow the following steps:

- Determining the cycle type for each representative.
- Using Lemma 3.1.1 and Lemma 3.1.2 to count the number of fixed k-subsets for each representative.
- Counting number of fixed k-subsets for each type of conjugacy classes by knowing the length and number of these classes (from Table 3.1).
- Counting the value of $\sigma_k(G, \Omega)$ using Burnside's Lemma.

A large part of this chapter deals with determining the cycle type of the representatives. Since G has eight types of conjugacy classes, we obtain the cycle type of seven of the eight representatives directly form Lemma 3.2.5 and Table 3.1. Classes of types $\mathcal{C}_6 \cup \mathcal{C}'_6$ are treated separately in Lemma 3.3.10, which is the most challenging point in this chapter. The main result in this chapter is as follows:

Theorem 1.0.5 *Suppose $G \cong PSL(3, q)$ acts upon the projective plane $\Omega = PG(2, q)$*

of q^2+q+1 *points and let* $k \in \mathbb{N}$ *with* $2 \le k \le \frac{q^2+q+1}{2}$. *Then*

$$\begin{aligned}\sigma_k(G,\Omega) =& \frac{d\eta_k(\pi_1)}{q^3(q^3-1)(q^2-1)} + \frac{d\eta_k(\pi_2)}{q^3(q-1)} + \frac{d\eta_k(\pi_3)}{q^2} \\ &+ \frac{d}{q(q^2-1)(q-1)} \sum_{x\in D^*(l)} \phi(x)\eta_k(\pi_4^{(x)}) \\ &+ \frac{d}{q(q-1)} \sum_{\substack{x\in D^*(l)\\ m=px}} \phi(x)\eta_k(\pi_5^{(m)}) + \frac{d\epsilon_k(E_0^*,\Omega)}{6(q-1)^2} \\ &+ \frac{d}{2(q^2-1)} \sum_{\substack{n\in D^*(q^2-1)\\ n\notin D(q-1)\\ j\in D^*(\frac{q-1}{d})}} \phi(n)\eta_k(\pi_7^{(n,j)}) \\ &+ \frac{d}{3(q^2+q+1)} \sum_{y\in D^*(\frac{q^2+q+1}{d})} \phi(y)\eta_k(\pi_8^{(y)}).\end{aligned}$$

From this formula, we implement a Magma code to count the value of σ_k. This code is included as an appendix at the end of this thesis.

Chapter 4 is devoted to investigating the relationship of the length of the G-orbit of a k-subset of Ω with the length of the G-orbits of $(k+1)$-subset containing it. In particular, it concerns groups that satisfy the hypothesis:

Hypothesis($*$): Let G be a transitive permutation group of n points and let $2 \le k \le \frac{n}{2}$. There is some k-subsets Δ of Ω in a G-regular orbit, an orbit of maximal length $|G|$, and $|\Sigma^G| < |G|$ for every $(k+1)$-sets Σ containing Δ.

From this hypothesis and Siemons-Wagner's results, we obtain an immediate corollary

Corollary 1.0.6 *Let* G *be a transitive group acting upon a set* Ω *of size* $n > 4$. *If* $k = 2$, *then there is no primitive group that satisfies Hypothesis*($*$).

By using the database of primitive groups in Magma, we obtain that there are only 6 primitive groups of a degree less than 25 that satisfy Hypothesis($*$). For groups of a large degree ($n > 25$) a memory problems happen. In Section 4.3, we consider $G \cong PSL(2,q)$ and discuss Hypothesis($*$) in the cases when $k = 3$ or 4. We set up the following result:

Theorem 1.0.7 *Let* $G \cong PSL(2,q)$ *acting on the projective line* Ω *of* $q+1$ *points. Let* $\Delta \subseteq \Omega$ *be a* k*-subset of* Ω, *then* $|\Delta^G| < |G|$ *for* $k = 3, 4$.

At the end of this section, by giving a detailed description of G-orbits, we show that the groups $PSL(2, 11)$ and $PSL(2, 16)$ satisfy Hypothesis($*$) when $k = 5$. Section 4.4 contains the main results in Chapter 4, which can be summarized in the following theorem:

Theorem 1.0.8 *Let $G \cong PSL(2, q)$, q is even, acts upon the projective line $\Omega = PG(1, q)$ of $q + 1$ points. If $2 \leq k \leq 7$, then there is no group G that satisfies Hypothesis($*$) except when $k = 5$ and $G \cong PSL(2, 16)$.*

Our method to prove this theorem is as follows:

- Take Δ to be a k-subset such that $|G_\Delta| = 1$, and let $M = \{\Sigma | \Delta \subseteq \Sigma \subseteq \Omega, |\Sigma| = k+1\}$, $|M| = q + 1 - k$.
- Let s be the maximum number of elements in M with non-trivial stabilizers.
- If $s < |M|$, then G does not satisfy Hypothesis($*$).

In the cases when $k = 2, 3$ or 4 the result follows from Corollary 1.0.4 and Theorem 1.0.5. We prove that G dose not satisfy Hypothesis($*$) for $k = 5, 6,$ or 7 separately in Theorem 4.4.10, Theorem 4.4.12, and Theorem 4.4.13.

In Chapter 5 we explore the link between the G-orbits of a k-subset of Ω and the G-orbits of a $(k + 1)$-subset of Ω containing it. This link can be expressed as follows: Let Δ be a k-subset of Ω and Σ be a $(k + 1)$-subset containing Δ. Suppose that r be the number of $(k + 1)$-subsets containing Δ which belong to the orbit Σ^G. Further suppose that s is the number of k-subsets of Σ which are contained in Δ^G. Then we have

$$r|\Delta^G| = s|\Sigma^G|.$$

In the rest of this chapter we calculate the G-orbits of 13 finite primitive groups of small degrees. All of our calculations are performed by MAGMA. The results obtained from these calculations are presented in diagrams, except the group Alt(6) in its action on 15 points and the group $ASL(2, 4)$ in its natural action on 16 points. As the results of our calculations of these two groups are extremely complicated, we prefer to present them in tables.

Chapter 2

Background Material

This chapter introduces general definitions and some well-known results associated to group actions. Most of this material is basic and we refer the reader to [12], [33], and [9] for more general definitions and results. We will begin this chapter by presenting some notation that will be used throughout this thesis.

2.1 General Notation

Throughout this thesis, unless stated otherwise, G is a finite group acting upon a set Ω of cardinality n. For the subgroup H of G and normal subgroup we will use $H \leqslant G$ and $H \trianglelefteq G$ respectively. We will use the notation $|G|$ for the order of G and $[G : H]$ for the index of the subgroup H in G. The trivial subgroup is denoted by 1, the cyclic group of order n is denoted by C_n, and the dihedral group of order $2n$ is denoted by $\mathrm{Dih}(2n)$. We will use $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ for the symmetric and alternating groups of degree n respectively.

For any elements $g, h \in G$ the conjugate of g by h is denoted by $g^h = h^{-1}gh$ and g^G is the G-conjugacy class of g. The centralizer of g in G is denoted by $C_G(g)$, and $N_G(H)$ is the normalizer of a subgroup H of G. We will use the notation π_g for the cycle type of an element $g \in G$.

2.2 Group Action

Let G be a finite permutation group acting on a set Ω, then for $\alpha \in \Omega$ and $g \in G$ the image of α under g will be denoted by αg. The main concepts relating to a group action are stabilizers and orbits which define as.

(i) The *orbit* of α under G is the subset $\alpha^G = \{\beta \in \Omega | \alpha g = \beta\}$.

(ii) Let $\alpha \in \Omega$, then the *stabilizer* of α in G is the subgroup $G_\alpha = \{g \in G | \alpha g = \alpha\}$.

Let G act on a set Ω, and $\Delta \subseteq \Omega$. Then the *pointwise stabilizer* of Δ in G is the subgroup

$$G_{(\Delta)} = \{x \in G | \delta x = \delta \text{ for all } \delta \in \Delta\}$$

and the *setwise stabilizer* of Δ in G is

$$G_\Delta = \{x \in G | \Delta x = \Delta\}.$$

Further, for $g \in G$, let $\mathrm{fix}_\Omega(g)$ be the subset of Ω which is fixed by g, that is $\mathrm{fix}_\Omega(g) = \{\alpha \in \Omega | \alpha g = \alpha\}$.

Definition 2.2.1 A group G is called *transitive* if it possesses only one orbit.

A group action on a set Ω induces an action of G on ordered pairs of distinct points given by $(\alpha, \beta)g = (\alpha', \beta')$, for $\alpha \neq \beta$ and $\alpha' \neq \beta'$. If this action is transitive, then G is said to be a *2-transitive* or *doubly-transitive* group. This lead us to more general action on n-tuples.

Definition 2.2.2 A finite group G is said to be k-transitive if for every k-tuple of distinct points $(\alpha_1, \alpha_2, ..., \alpha_k)$ and $(\beta_1, \beta_2, ..., \beta_k)$ there exist an element $g \in G$ such that $\alpha_i g = \beta_i$, $1 \leqslant i \leqslant k$.

In particular, a transitive group is 1-transitive.

Example 2.2.3 The symmetric group $\mathrm{Sym}(n)$ is k-transitive for all $k \leqslant n$ and the alternating group $\mathrm{Alt}(n)$ is k-transitive for all $k \leqslant n - 2$.

A transitive permutation group on a set Ω is said to be *regular* if $G_\alpha = 1$ for each $\alpha \in \Omega$. A G-orbit α^G on a group G is said to be *regular* if $|G| = |\alpha^G|$. The next theorem presents some properties related to k-transitive groups.

Theorem 2.2.4 *Let G be a group acting on a set Ω.*

(i) If G acts transitively on Ω, then the action of G is regular if and only if $|G| = |\Omega|$.

(ii) Let G be a transitive group on Ω. Suppose that $k > 1$, then G is a k-transitive if and only if G_α is $(k-1)$-transitive on the set $\Omega \setminus \{\alpha\}$ for all $\alpha \in \Omega$.

(iii) If G is k-transitive group on a set Ω and $\Delta \subseteq \Omega$ with $|\Delta| = d < k$. Then G_Δ is $(k-d)$-transitive on $\Omega - \Delta$.

The relationship between orbits and stabilizers has a wide range of applications in counting problems and combinatorics. The two fundamental results about this relationship will be relied on heavily in this thesis.

Theorem 2.2.5 *(The Orbit-Stabilizer Theorem) Let G be a group acting upon a finite set Ω. Then $|\alpha^G| = [G : G_\alpha]$ for all $\alpha \in \Omega$. In particular if G is finite, then $|\alpha^G| = |G| \cdot |G_\alpha|$.*

The relation between the number of orbits and the group order is given by the following theorem

Theorem 2.2.6 *(Burnside's Lemma)* [1] *Let G be a finite group acting on a set Ω. Then the number of orbits on Ω is given by $\sigma(G,\Omega) = \frac{1}{|G|}\sum_{g\in G} |fix_\Omega(g)|$.*

The action on the group G can be extended to a subset Δ of Ω as $\Delta g = \{\delta g | \delta \in \Delta\}$.

Definition 2.2.7 Let G be a transitive group and Δ be a non empty subset of Ω. Then we say that Δ is a *block* for G if for all $g \in G$ either $\Delta g = \Delta$ or $\Delta g \cap \Delta = \emptyset$.

Remark: The set Ω and the singletons $\{\delta\}$, where$(\delta \in \Omega)$ are called the *trivial* blocks for any group acting transitively on a set Ω. Any other blocks are called *non-trivial.*

[1] *This lemma was proved by Frobenius in (1887), however Burnside quoted and proved the lemma in the first edition(1897) of his book. So sometimes it is called the Cauchy-Frobenius Lemma or The Lemma that is not Burnside.*

Definition 2.2.8 The transitive group G on the set Ω is *primitive* if it has no non-trivial blocks on Ω, otherwise G is *imprimitive.*

Example 2.2.9 Taking $H \leq \text{Sym}(4)$ where $H = \langle (1,2)(3,4),(1,3)(2,4)\rangle$. Obviously H is transitive and preserves the blocks $\{1,3\}$ and $\{2,4\}$. Therefore H is imprimitive.

The next theorem provides some properties regarding primitive groups.

Theorem 2.2.10 *Let G be a group acting on a set Ω.*

(i) If G is a doubly transitive permutation group, then G is primitive.

(ii) Let G_α be the stabilizer of a point $\alpha \in \Omega$, $|\Omega| > 1$. Then the action of G on the set of right cosets of G_α is primitive if and only if G_α is maximal subgroup.

2.3 The Induced Action on k-subsets

Let Ω be a set of n elements and k be a positive number, then a *k-subset* is a subset of Ω containing k elements. The set of all k-subsets is denoted by Ω_k and $|\Omega_k|$ is given by $\binom{n}{k}$.

A group action of G on a set Ω induces an action of G on the set Ω_k for each $k \leq n = |\Omega|$ and given by

$$\Delta g = \{\alpha g | \alpha \in \Delta\},$$

where $\Delta \in \Omega_k$.

Definition 2.3.1 Let G be a group acting upon Ω_k. Then $\sigma_k(G, \Omega)$ denotes the number of G-orbits on Ω_k.

If G acts on Ω_k transitively, then G is *k-homogeneous*, that is $\sigma_k(G, \Omega) = 1$. Now we will review some of the results about k-homogeneous groups.

Lemma 2.3.2 *(i) If G is k-transitive, then G is k-homogeneous.*

(ii) If G is k-homogeneous of degree n, then G is $(n-k)$-homogeneous.

(iii) If G is 2-homogeneous and G has even order, then G is 2-transitive.

(iv) If G is non-trivial 2-homogeneous group, then G is primitive.

Proof See [16], p(366).

Lemma 2.3.3 (Wielandt) *Let G be a group acting on a set Ω of cardinality n. Suppose G is k-homogeneous group and $p^a + k - 1 \leq n$ for any prime power p^a dividing k, then G is $(k-1)$-homogeneous.*

Proof See [32]

Example 2.3.4 Suppose that G is the permutation group $PGL(2,8)$ of degree 9. Since G is 3-transitive, then G is 3-homogeneous and therefore, by Lemma 2.3.2 (*ii*) G is k-homogeneous for $k = \{6,7,8,9\}$. Since G is 6-homogeneous and $6+3-1 \leq n$, then by Lemma 2.3.3 G is 5-homogeneous. Similarly, G is 4-homogeneous.

Theorem 2.3.5 (Livingstone-Wagner) *[23] If G is a k-homogeneous group where $2 \leq k \leq \frac{n}{2}$, then G is $(k-1)$-homogeneous.*

Proof Let p^a be a prime power divides k, then $p^a + k - 1 \leq 2k - 1 \leq n$. Therefore, G is $(k-1)$-homogeneous by Lemma 2.3.3. $\diamond$

If G is k-transitive group, then G is k-homogeneous. The converse is not true except when $5 \leq k \leq \frac{n}{2}$, see (Livingstone, Wagner [23]).

The following theorem determines the groups which are k-homogeneous but not k-transitive on a finite set Ω, $k \leqslant \dfrac{n}{2}$, for the cases $k = 2, 3, 4$. This theorem completes Livingstone-Wagner's result.

Theorem 2.3.6 (Kantor) *[18] Let G be k-homogeneous but not k-transitive group on a finite set Ω of cardinality n. If $2 \leq k \leq \dfrac{n}{2}$, then one of the following holds:*

(i) $k = 2$ *and* $G \leq A\Gamma L(1,q)$ *with* $q \equiv 3$ *mod* 4*;*

(ii) $k = 3$ *and* $PSL(2,q) \leq G \leq P\Gamma L(2,q)$ *where* $q \equiv 3$ *mod* 4*;*

(iii) $k = 3$ *and* $G = AGL(1,8)$, $A\Gamma L(1,8)$, *or* $A\Gamma L(1,32)$*;*

(iv) $k = 4$ *and* $G = PSL(2,8)$, $P\Gamma L(2,8)$, *or* $P\Gamma L(2,32)$.

The next theorem is a preliminary result of Livingstone and Wagner [23] which asserts the relation between number of orbits on Ω_k and Ω_{k-1}.

Theorem 2.3.7 (Livingstone-Wagner) *[23] Let G be a group acting upon a finite set Ω of size n. If $2 \leq k \leq \frac{n}{2}$, then the number of group orbits on Ω_k is at least as great as the number of orbits on Ω_{k-1}. That is,*

$$\sigma_k(G, \Omega) \geqslant \sigma_{k-1}(G, \Omega).$$

The next theorem comprised Livingstone-Wagner Theorem 2.3.7 as a special case. But first we need to define some notation relating to this theorem.

Let S be a family of subsets of Ω and let $n_k(G, S) = |\{\Delta^G | \Delta \in \Omega_k \text{ and} \Delta \subseteq \Sigma$ for some $\Sigma \in S\}|$. Further, Σ is maximal in S if $\Sigma \subseteq \Sigma' \in S$ implies that $\Sigma = \Sigma'$. Also put $m(S) = min\{|\Sigma| : \Sigma \text{ is maximal}, \Sigma \in S\}$.

Theorem 2.3.8 *[25] Let G be a permutation group on a set Ω and let S be a family of subsets of Ω. If $s < t$ are integers with $s + t \leq m(S)$, then $n_s(G, S) \leq n_t(G, S)$.*

Clearly, the Livingstone-Wagner Theorem 2.3.7 is the particular case when $S = \Omega$.

In the rest of this chapter we present a number of results about the equality of Livingstone-Wagner Theorem.

Definition 2.3.9 [9] Let G be a permutation group on a finite set Ω of size n, where $n = 2k$. Then G is said to have the *interchange property* if, for every k-element subset Γ of Ω there is an element g in G which interchanges Γ with its complement $\overline{\Gamma}$.

Example 2.3.10 [9] The following groups have interchange property:

(i) $PSL(2, 11)$, M_{12}, M_{11}, for $n = 12$, $k = 6$;

(ii) $AGL(4, 2)$, for $n = 16$, $k = 8$;

(iii) M_{24}, for $n = 24$, $k = 12$.

Theorem 2.3.11 (P.Cameron, P. Neumann) *[9] A group G has the interchange property if and only if*

$$\sigma_t(G, \Omega) = \sigma_{t+1}(G, \Omega)$$

for all even number t with $0 \leq t \leq k - 1$.

Remark: From Example 2.3.10 and Theorem 2.3.11 if G is not $(k+1)$-homogeneous for $k < \frac{n-1}{2}$, then the following groups achieve the equality in the Livingstone-Wagner Theorem:

(i) $PSL(2,11)$, M_{11}, for $n = 12$, $k = 4$;

(ii) $AGL(4,2)$, for $n = 16$, $k = 4,6$;

(iii) M_{24}, for $n = 24$, $k = 6,8,10$.

Theorem 2.3.12 (P.Cameron, P. Neumann) *[9] Let G be a transitive permutation group acting upon a set Ω such that*

$$\sigma_2(G,\Omega) = \sigma_3(G,\Omega) < \infty$$

If $|\Omega| > 5$, then one of the following holds:

(i) G has 2 blocks of imprimitivity of size $\frac{|\Omega|}{2}$;

(ii) G has $\frac{|\Omega|}{2}$ blocks of imprimitivity of size 2; or

(iii) G is a 3-homogeneous on Ω.

Theorem 2.3.13 *[4] Let G be a permutation group and H be a subgroup of G. If $1 \leq k < \frac{(n-1)}{2}$, then $\sigma_{k+1}(G) - \sigma_k(G) \leq \sigma_{k+1}(H) - \sigma_k(H)$. In particular, if $\sigma_{k+1}(H) = \sigma_k(H)$, then $\sigma_{k+1}(G) = \sigma_k(G)$.*

Proposition 2.3.14 *Let G be a primitive permutation group acting on a set of size $n \leq 160$. Suppose that G is not $(k+1)$-homogeneous for some $2 \leq k \leq \frac{n}{2} - 1$. If $\sigma_k(G,\Omega) = \sigma_{k+1}(G,\Omega)$, then G is one of the following:*

(i) $AGL(m,2)$, for $m \geq 4$, $n = 2^m$, $k = 4$,

(ii) $ASL(2,3)$ or $AGL(2,3)$, for $n = 9$, $k = 3$,

(iii) $Sym(5)$, $Sym(6)$, $PGL(2,9)$ or $P\Gamma L(2,9)$, for $n = 10$, $k = 4$,

(iv) M_{11}, $PSL(2,11)$, $PGL(2,11)$, for $n = 12$, $k = 4$,

(v) $PSL(3,3)$, for $n = 13$, $k = 4$,

(vi) $PGL(2,13)$, for $n = 14$, $k = 4,6$,

(vii) $2^4 : Alt(6)$, $2^4 : Sym(6)$, $2^4 : Alt(7)$, $AGL(4, 2)$, *for* $n = 16$, $k = 6$,

(viii) $PGL(2, 17)$, *for* $n = 18$, $k = 6$ *or* 8,

(ix) M_{22}, $M_{22} : 2$, *for* $n = 22$, $k = 8$,

(x) $M_{22} : 2$, *for* $k = 22$, $k = 10$,

(xi) M_{23}, *for* $n = 23$, $k = 8, 9$,

(xii) M_{24}, *for* $n = 24$, $k = 6, 7, 9$ *or* 10,

(xiii) $ASL(5, 2)$, *for* $n = 32$, $k = 14$.

Proof Bundy and Hart [4] found this list by searching the database of primitive groups in GAP for degree up to 28.

We have checked this list using the database of primitive groups in Magma for degree up to 160. We only add the following four groups to this list

- $PGL(2, 13)$, for $n = 14$, $k = 6$,
- $AGL(4, 2)$ for $n = 16$ and $k = 6$,
- $M_{22} : 2$, for $k = 22$, $k = 10$,
- $ASL(5, 2)$, for $n = 32$, $k = 14$. $\diamond$

2.4 General Linear Groups

Let p a prime number and n be a positive integer, then there exist a finite field with $q = p^n$ elements. This field is called the *Galois field* and denoted by $GF(q)$ and sometimes $\mathbb{F}_q$. If q is prime, then $GF(q) \cong {}^{\mathbb{Z}}/_{q\mathbb{Z}}$. For convenience, we may write $GF(q) = F$ and $F^* = F \setminus \{0\}$.

Let V be a finite dimensional vector space over a field K. The group of all invertible linear transformations from V to itself is called the *general linear group* and denoted by $GL(V)$. Suppose that $\{e_1, e_2, ..., e_n\}$ is the basis of V, each $\alpha \in GL(v)$ can be represented as $n \times n$ invertible matrix. Hence, $GL(v) \cong GL(n, K)$ where $GL(n, K)$ is the multiplicative group of all $n \times n$ invertible matrices and also called the general linear group. In the case when $K = F$ we write $GL(n, q)$ for $GL(n, K)$.

The set of all non-zero matrices λI_n, where $\lambda \in F$ form the center, say Z, of $GL(n,q)$. The quotient group G/Z, is called the *projective general linear group* and denoted by $PGL(n,q)$. The homomorphism $det : GL(n,q) \to F^*$ maps $GL(n,q)$ onto the multiplicative group F^* and its kernel consists of all matrices of determinant 1. This kernel is called the *special linear group* $SL(n,q)$. Again the quotient of $SL(n,q)$ with its center form a group called *the projective special linear group* $PSL(n,q)$.

Theorem 2.4.1 *The number of elements in* $GL(n,q)$ *is* $(q^n-1)(q^n-q)(q^n-q^2)...(q^n-q^{n-1})$.

It is easy to show that $PGL(n,q)$ and $SL(n,q)$ have the same order and equal $\frac{|GL(n,q)|}{q-1}$.

Proposition 2.4.2 *The order of* $PSL(n,q)$ *is*

$$|PSL(n,q)| = \frac{1}{d} q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - 1)$$

, where d *is the greatest common divisor of* n *and* $q-1$.

The groups of $PSL(n,q)$ are all simple except for the cases $PSL(2,2) \cong \mathrm{Sym}(3)$ and $PSL(2,3) \cong \mathrm{Alt}(4)$.

Chapter 3

Number of G-orbits in $PSL(3, q)$

This chapter is devoted to counting the number of G-orbits on the set Ω_k, the set of all k-subsets of Ω. Our main motivation comes from Bradley-Rowley work (2014) [2]. As was alluded to in the first chapter of this thesis, the two cited authors established four formulas for the rank one doubly transitive group, that is, $G \cong PSL(2, q), Sz(q), PSU(3, q)$ or $R(q)$. Using their formulas, one can find the value of σ_k by knowing only the values of q and k. In this chapter, we aim to compile a similar result for the 3-dimensional projective special linear group $PSL(3, q)$.

We begin this chapter by providing background information about counting the number of fixed k-subsets by a group element g.

3.1 Background Material

Let G be a permutation group acting on the set Ω_k. We can then use Burnside's lemma to count the number of G-orbits on Ω_k

$$\sigma_k(G, \Omega) = \frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}_{\Omega_k}(g)|.$$

Where $|\mathrm{fix}_{\Omega_k}(g)|$ is the number of k-subsets left fixed by the elements of the group G. The number of fixed k-subsets can be easily determined from the cycle type of the group element g on the points of Ω.

Assume g is an element of G such that $g = c_k c_{k-1} ... c_1$, where c_i are the disjoint cycles of g, $1 \leq i \leq k$, and $|c_i| \geq 1$. We say that g is of the type $1^{\lambda_1} \cdot 2^{\lambda_2} \cdot ... m^{\lambda_m}$ (with $\sum_{i=1}^{m} i\lambda_i = n$) if g has λ_i cycles of length i. Note that some of the λ_i could be

0. When there is no ambiguity, we denote the cycle type of g by π_g.

Lemma 3.1.1 *Let Δ be a k-subset of Ω and $g \in Sym(\Omega)$, $|\Omega| = n$, with cycle type π_g. Then Δ is fixed by the element g if and only if Δ is the union of cycles of g.*

Lemma 3.1.2 *Suppose $g \in G$ with cycle type π_g and let $k \in \mathbb{N}$. Then the number of k-subsets fixed by g is given by*

$$\eta_k(\pi) = \sum_{(k_1,k_2,\ldots,k_m)} \prod_{i=1}^{m} \binom{\lambda_i}{k_i}$$

running over all the non-negative integer vectors $(k_1, k_2, \ldots, k_m)$ such that $\sum_{i=1}^{m} ik_i = k$.

In our calculations, we need to determine the number of elements of a given order in a finite cyclic subgroup of $PSL(3,q)$. For convenience, we present a crucial number theoretic function called Euler's totient function and denoted by $\phi(n)$. This function is defined as the number of positive integers less than n which are relatively prime to n. If the prime factorization of n is $n = p_1^{a_1} \cdot p_2^{a_2} \ldots p_s^{a_s}$, then the general formula for computing $\phi(n)$ is as follows:

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}).$$

Lemma 3.1.3 *Suppose that C_n is a cyclic group. Let $m|n$, then the number of elements of order m in C_n is $\phi(m)$.*

PROOF The cyclic subgroup C_n has exactly one subgroup $C_m = \langle a \rangle$ of order m. Then each element in C_m of order m is also a generator of C_m. Since an element a^k is a generator of C_m if and only if $(k, m) = 1$, then the number of such elements is the Euler's function $\phi(m)$.$\diamond$

The next definition presents the final piece of notation in this section.

Definition 3.1.4 For $m \in \mathbb{N}$ we let $D(m) = \{n \in \mathbb{N} | n \text{ divides } m\}$ and write $D^*(m) = D(m) \setminus \{1\}$.

3.2 The Projective Special Linear Group $PSL(3, q)$

In this chapter, we let G be the 3-dimensional projective special linear group $PSL(3, q)$ acting upon $q^2 + q + 1$ points of the projective plane over $GF(q)$. The order of the group G is $|G| = \frac{q^3(q^3-1)(q^2-1)}{d}$, where $d = (3, q - 1)$.

3.2.1 The Subgroups of $PSL(3, q)$

The first determination of the subgroups of $PSL(3, q)$ was given by Mitchell [24] for the case where q is odd. Mitchell's [24] determination uses geometric methods to establish the maximal subgroups of $PSL(3, q)$ and all other subgroups. Using similar geometric methods, Hartley [14] (Mitchell's student) determined the subgroups of $PSL(3, q)$ for the case where q is even. In 1968, Bloom [1] gave a new determination of the subgroups of $PSL(3, q)$, for odd q, by using group-theoretic methods.

The next theorem presents the maximal subgroups of $PSL(3, q)$. Note that ˆ denotes the image of subgroups of $SL(3, q)$ in $PSL(3, q)$ and $[x]$ is an arbitrary subgroup of order x.

Theorem 3.2.1 *[1], [14], [24] Let G be the group $PSL(3, q)$, and let M be a maximal subgroup of G, then M is one of the following list. (The first four subgroups are all maximal for $q \geq 5$).*

(i) $\hat{}[q^2] : GL(2, q)$, *the stabilizer of a point;*

(ii) $\hat{}[q^2] : GL(2, q)$, *the stabilizer of a line;*

(iii) $\hat{}(q - 1)^2 : Sym(3)$, *the stabilizer of a triangle;*

(iv) $\hat{}(q^2 + q + 1) : 3$, *one $PSL(3, q)$-conjugacy class;*

(v) $PSL(3, q_0).(q - 1, 3, b)$, *where $q = q_0^b$ and b is a prime;*

(vi) $PSU(3, q_0)$ *for $q = q_0^2$;*

(vii) $Alt(6)$ *when $q = 4$ or q is odd with $q \equiv 1$ or 19 mod 30 ;*

(viii) $3^2.SL(2, 3)$ *when q is odd and $9|q - 1$;*

(ix) $3^2.Q_8$ *when q is odd and $3|q - 1$;*

(x) $PGL(2,q)$ *when* q *is odd;*

(xi) $PSL(2,7)$ *when* q *is odd and* $q^3 \equiv 1 \bmod 7$.

Let M be the subgroup $\hat{\ }GL(2,q)$ and $D = Z(\hat{\ }GL(2,q))$. Then, D is the projective image of

$$\left\{ \begin{pmatrix} \frac{1}{a^2} & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} | a \in GF(q) \right\},$$

where a is a primitive element of $GF(q)$.

Next, we present two useful lemmas relating to the subgroup D.

Lemma 3.2.2 *The intersection of any* $PSL(3,q)$*-conjugate subgroups of* D *is trivial.*

Proof See [13].

Lemma 3.2.3 *Let* $N \cong \hat{\ }(q-1)^2 : Sym(3)$ *be a maximal subgroup of* G. *Then* N *contains only three conjugates of* D *generating by the projective images of the following matrices:*

$$\begin{pmatrix} \frac{1}{a^2} & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}, \begin{pmatrix} a & 0 & 0 \\ 0 & \frac{1}{a^2} & 0 \\ 0 & 0 & a \end{pmatrix}, \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & \frac{1}{a^2} \end{pmatrix}.$$

Proof See [13].

3.2.2 Conjugacy Classes of $PSL(3,q)$

In this section, we introduce some information relating to the conjugacy class structure of $PSL(3,q)$. To get this information, we rely on the work of Simpson and Frame [30] and Chapter XI of Dickson's book [11]. In their paper, "The character tables for $SL(3,q)$, $SU(3,q^2)$, $PSL(3,q)$, $PSU(3,q^2)$" Simpson and Frame [30] provided the character table of $PSL(3,q)$ and $PSU(3,q^2)$ (see Table (2) in [30]). From this table, we are able to collate some information about the classes of our group. In his investigation on the cyclic subgroups of $PSL(3,q)$, Dickson provided some details relating to the classes of $PSL(3,q)$.

Lemma 3.2.4 *Let* $G \cong PSL(3,q)$ *acts upon the projective plane* $\Omega = PG(2,q)$ *and* $\mathcal{C}_i$ *be the types of conjugacy classes of* G. *Then, the number of fixed points of each type are given in the following table.*

Conjugacy Class	Canonical Representation	Parameters	Number of classes of each type	$\|C_G(g)\|$, $g \in \mathcal{C}_i$	$\|g^G\|$	χ_1	χ_{qs}	$\|\mathrm{fix}_\Omega(g)\|$
$\mathcal{C}_1$	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$		1	$\|G\|$	1	1	$q(q+1)$	$\|\Omega\|$
$\mathcal{C}_2$	$\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}$		1	$q^3(\frac{q-1}{d})$	$(q^3-1)(q+1)$	1	q	$q+1$
$\mathcal{C}_3^{(l)}$	$\begin{pmatrix}1&0&0\\\theta^l&1&0\\0&\theta^l&1\end{pmatrix}$	$0 \le l \le d-1$	d	q^2	$\frac{q(q^3-1)(q^2-1)}{d}$	1	0	1
$\mathcal{C}_4^{(k)}$	$\begin{pmatrix}\rho^k&0&0\\0&\rho^k&0\\0&0&\rho^{-2k}\end{pmatrix}$	$1 \le k \le r^{'}-1$	$\frac{q-1}{d}-1$	$\frac{q(q-1)(q^2-1)}{d}$	$q^2(q^2+q+1)$	1	$q+1$	$q+2$
$\mathcal{C}_5^{(k)}$	$\begin{pmatrix}\rho^k&0&0\\1&\rho^k&0\\0&0&\rho^{-2k}\end{pmatrix}$	$1 \le k \le r'-1$	$\frac{q-1}{d}-1$	$\frac{q(q-1)}{d}$	$q^2(q^3-1)(q+1)$	1	1	2
$\mathcal{C}_6'$	$\begin{pmatrix}1&0&0\\0&\omega&0\\0&0&\omega^2\end{pmatrix}$		0 if $d=1$, 1 if $d=3$	$(q-1)^2$	$\frac{q^3(q^2+q+1)(q+1)}{d}$	1	2	3
$\mathcal{C}_6^{(k,l,m)}$	$\begin{pmatrix}\rho^k&0&0\\0&\rho^l&0\\0&0&\rho^m\end{pmatrix}$	$1 \le k < l \le r'$, $l < m \le q-1$	$\frac{q^2-5q+7-d}{6d}$	$\frac{(q-1)^2}{d}$	$q^3(q^2+q+1)(q+1)$	1	2	3
$\mathcal{C}_7^{(k)}$	$\begin{pmatrix}\rho^k&0&0\\0&\sigma^{-k}&0\\0&0&\sigma^{-qk}\end{pmatrix}$	$1 \le k \le r's$, $k \ne 0 \bmod s$, $\mathcal{C}^{(k)} = \mathcal{C}^{(kq)}$	$\frac{q(q-1)}{2d}$	$\frac{q^2-1}{d}$	$q^3(q^3-1)$	1	0	1
$\mathcal{C}_8^{(k)}$	$\begin{pmatrix}\tau^k&0&0\\0&\tau^{kg}&0\\0&0&\tau^{kg^2}\end{pmatrix}$	$1 \le k \le t'-1$, $\mathcal{C}^{(k)} = \mathcal{C}^{(kq)} = \mathcal{C}^{(kq^2)}$	$\frac{q^2+q+1-d}{3d}$	$\frac{q^2+q+1}{d}$	$q^3(q-1)^2(q+1)$	1	-1	0

Table 3.1: Conjugacy classes of $PSL(3,q)$

(Note: $d = (3, q-1)$, $r' = \frac{q-1}{d}$, $s = q+1$, $t' = \frac{q^2+q+1}{d}$, $\rho^{q-1} = 1$, $\sigma^{q+1} = \rho$, $\tau^{q^2+q+1} = 1$, $\omega^3 = 1$ and $\theta^3 \neq 1$).

Proof This table (except the last column) is an extract from Table (2) in [30], in which the authors provided considerable detail of the conjugacy classes of $PSL(3,q)$, as well as the irreducible characters. Since G is a 2-transitive group, according to Isaac [17] page 69, the permutation character can be determined as $\chi_1 + \chi_{qs}$, which gives the number of fixed points for each type. $\diamond$

Lemma 3.2.5 *[11] [Chapter XI]*

(i) G contains $\frac{d|G|}{q^3(q-1)}$ elements of order p, which fix $q+1$ points and all these elements are conjugate.

(ii) G contains $\frac{1}{3}[\frac{q^2+q+1}{d} - 1]$ sets of conjugate elements each with size $\frac{d|G|}{q^2+q+1}$. It follows that G contains in all $\frac{d|G|}{3(q^2+q+1)}[\frac{q^2+q+1}{d} - 1]$ elements that are not the identity and whose orders are factors of $\frac{q^2+q+1}{d}$.

(iii) G contains d conjugate sets each of size $\frac{|G|}{q^2}$. The elements of these sets are of order p or 4 respectively when $p > 2$ or $p = 2$.

(iv) G contains $(\frac{q-1}{d} - 1)(\frac{d|G|}{q(q-1)})$ elements each of which has order dividing $p\frac{q-1}{d}$ but not p or $q-1$ and each of these elements has two fixed points.

(v) G contains $\frac{q(q-1)}{2d}$ sets of conjugate elements with each set contains $\frac{d|G|}{q^2-1}$ distinct conjugate elements. Each of these elements has an order that is a factor of $\frac{q^2-1}{d}$ without being a factor of $\frac{q-1}{d}$ and hence $q-1$.

(vi) If $d = 1$, then G contains $\frac{q^2-5q+6}{6}$ sets of conjugate elements. One of these sets is of length $\frac{|G|}{(q-1)^2}$.
If $d = 3$, then G contains $1 + \frac{1}{3}(\frac{q^2-5q+4}{6})$ sets of conjugate elements. One of these sets is of length $\frac{|G|}{(q-1)^2}$. Each of the remaining sets is of length $\frac{3|G|}{(q-1)^2}$.
In both cases, each element has an order which is a divisor of $q-1$.

Remark: Although Table 3.1 and Lemma 3.2.5 contain similar information about the conjugacy classes of $PSL(3,q)$, Lemma 3.2.5 provides more details relating to representatives orders and their number of fixed points. These details will play a crucial role in our investigation into determining cycle types of elements in $PSL(3,q)$.

3.3 Main Results

The next theorem is the main results of this chapter in which we provide a formula to count the number of G-orbits for the group $PSL(3,q)$. The notation η_k, ϵ_k and π_i will be defined later in this chapter.

Theorem 3.3.1 *Suppose $G \cong PSL(3,q)$ acts upon the projective plane $\Omega = PG(2,q)$ of q^2+q+1 points and $d = (q-1,3)$. Let $k \in \mathbb{N}$ with $2 \leq k \leq \frac{q^2+q+1}{2}$. Then*

$$\begin{aligned}\sigma_k(G,\Omega) =& \frac{d\eta_k(\pi_1)}{q^3(q^3-1)(q^2-1)} + \frac{d\eta_k(\pi_2)}{q^3(q-1)} + \frac{d\eta_k(\pi_3)}{q^2} \\ &+ \frac{d}{q(q^2-1)(q-1)} \sum_{x\in D^*(\ell)} \phi(x)\eta_k(\pi_4^{(x)}) \\ &+ \frac{d}{q(q-1)} \sum_{\substack{x\in D^*(\ell)\\ m=px}} \phi(x)\eta_k(\pi_5^{(m)}) + \frac{d\epsilon_k(E_0^*,\Omega)}{6(q-1)^2} \\ &+ \frac{d}{2(q^2-1)} \sum_{\substack{n\in D^*(q^2-1)\\ n\notin D(q-1)\\ j\in D^*(\frac{q-1}{d})}} \phi(n)\eta_k(\pi_7^{(n,j)}) \\ &+ \frac{d}{3(q^2+q+1)} \sum_{y\in D^*(\frac{q^2+q+1}{d})} \phi(y)\eta_k(\pi_8^{(y)}).\end{aligned}$$

The proof of this theorem relies on Burnside's Lemma 2.2.6. Therefore, first we need to count the number of k-subsets fixed by elements of the group G. Before doing so, we have to determine the cycle types of elements in each of the eight conjugacy classes of G. Then, we can easily use Lemma 3.1.2 to count the number of fixed k-subsets.

Before beginning our investigation on the cycle types of elements of G, we have to define a number of notation that will be used throughout this section.

Definition 3.3.2 (i) $q = p^a$ where p is a prime number and $a \in \mathbb{N}$;

(ii) $d = (q-1,3)$;

(iii) $\ell = \frac{q-1}{d}$, $x \in D^*(\ell)$, $m = px$;

(iv) $n \in D^*(\frac{q^2-1}{d})$, $n \notin D^*(\ell)$, $j = \frac{n}{(n,\ell)}$;

(v) $y \in D^*(\frac{q^2+q+1}{d})$.

In the next lemma, we ascertain the cycle structure for seven of the eight representatives of conjugacy classes of $PSL(3,q)$. We will consider the cycle types of classes $\mathcal{C}_6$ and $\mathcal{C}_6'$ separately.

Lemma 3.3.3 *Let $g \in G$ and $g^G \in \mathcal{C}_i$, where $i \neq 6$. Then, the cycle type of element g is given in the following table*

$\mathcal{C}_i$	$\lvert g\rvert$, $g \in \mathcal{C}_i$	π_i
$\mathcal{C}_1$	1	1^{q^2+q+1}
$\mathcal{C}_2$	p	$p^{\frac{q^2}{p}}.1^{q+1}$
$\mathcal{C}_3$	4 (if $p=2$) p (if $p>2$)	$4^{\frac{q^2}{4}}.2^{\frac{q}{2}}.1^1$ $p^{\frac{q^2+q}{p}}.1^1$
$\mathcal{C}_4$	x	$x^{\frac{q^2-1}{x}}.1^{q+2}$
$\mathcal{C}_5$	m	$m^{\frac{q^2-q}{m}}.x^{\frac{q-1}{x}}.p^{\frac{q}{p}}.1^2$
$\mathcal{C}_7$	n	$n^{\frac{q^2-1}{n}}.j^{\frac{q+1}{j}}.1^1$
$\mathcal{C}_8$	y	$y^{\frac{q^2+q+1}{y}}$

Table 3.2: Cycle types of elements in $PSL(3,q)$

Proof Let $X = g^G$ be a conjugacy class of type $\mathcal{C}_i$, with $1 \leq i \leq 8$, $i \neq 6$. If $i=1$, then clearly $g=1$ and has cycle type 1^{q^2+q+1}.

Let $g \in X$ where X is a class of type $\mathcal{C}_2$. Then, from Table 3.1, g fixes $q+1$ points and has centralizer subgroup of order $q^3(\frac{q-1}{d})$. Therefore, from Lemma 3.2.5 (i), g has order p and hence has the cycle type $p^{\frac{q^2}{p}}.1^{q+1}$.

From Table 3.1, classes of type $\mathcal{C}_3$ have length $\frac{|G|}{q^2}$. Then, from Lemma 3.2.5 (iii), elements in these classes have order p if $p>2$ or 4 if $p=2$. Let $g \in X$, where X is a class of type $\mathcal{C}_3$. If $p>2$, then g has the cycle type $p^{\frac{q^2+q}{p}}.1^1$.
If $p=2$, then g has order 4 and fixes one point. Since $|g^2| = 2$ and fixes $q+1$ points, g^2 lies inside a class of type $\mathcal{C}_2$. Hence, g possesses $\frac{q}{2}$ cycles of length 2, and thus the cycle type of g is $4^{\frac{q^2}{4}}.2^{\frac{q}{2}}.1^1$.

From Lemma 3.2.1 (i) G contains a subgroup $M \cong \hat{\ }GL(2,q)$ and, clearly $Z(M)$ is a cyclic subgroup of order $\frac{q-1}{d}$. Let $g \in Z(M)$, then from the centralizer sizes in Table 3.1, $|C_G(g)| = \frac{q(q+1)(q^2-1)}{d}$. From Lemma 3.2.2, no two elements in $Z(M)$ are $PSL(3,q)$-conjugate, thus elements in $Z(M)^\#$ are representatives of classes of type $\mathcal{C}_4$. Therefore, these elements have orders that are factors of $\frac{q-1}{d}$ and fix $q+2$ points in Ω. It follows that they have the cycle type $x^{\frac{q^2-1}{x}}.1^{q+2}$.

Since classes of type $\mathcal{C}_7$ have length $\frac{d|G|}{q^2-1}$, from Lemma 3.2.5 (v), elements in these classes are of orders that are factors of $\frac{q^2-1}{d}$ but not factors of $\frac{q-1}{d}$. Let $g \in X$, where X is a class of type $\mathcal{C}_7$. Further suppose that $|g| = n$, where $n \in D^*(\frac{q^2-1}{d})$ and $n \notin D^*(\ell)$, where $\ell = \frac{q-1}{d}$. Since $n \nmid \ell$, let j be the smallest natural number such that $\frac{n}{(n,\ell)} = j$. If $j \neq 1$, then g^j has an order divides $\frac{q-1}{d}$, and then g^j is an element in a conjugacy class of type $\mathcal{C}_4$. It follows that g contains cycles of length j. Clearly, there are no other cycles in g of length j_1, where $j_1|j$, because in this case g^{j_1} is of order that divides $\frac{q^2-1}{d}$ with $|\text{fix}_\Omega(g)| > 1$ and this a contradiction. Hence, g has the cycle type $n^{\frac{q^2-1}{n}}.j^{\frac{q+1}{j}}.1^1$.

Clearly, from Table 3.1, classes of type $\mathcal{C}_8$ have lengths $\frac{d|G|}{q^2+q+1}$. From Lemma 3.2.5 (ii), if $g \in X$ where X is a class of type $\mathcal{C}_8$, then g has an order that is a factor of $\frac{q^2+q+1}{d}$. Since all elements having orders that are factors of $\frac{q^2+q+1}{d}$ lie in classes of type $\mathcal{C}_8$, g has the cycle type $y^{\frac{q^2+q+1}{y}}$.

From Lemma 3.2.5(vi) and Table 3.1, we can show that elements of classes of type $\mathcal{C}_6 \cup \mathcal{C}_6'$ have orders that are factors of $q-1$. Therefore, from the argument above and Lemma 3.2.5, classes of type $\mathcal{C}_5$ have elements with orders that are factors of $p\frac{q-1}{d}$ but not are factors of p or $q-1$. Let $g \in X$, where X is a class of type $\mathcal{C}_5$ and let $|g| = m$, where $m = px$, $x \in D^*(\frac{q-1}{d})$. Since g^x is an element of order p, it lies inside a class of type $\mathcal{C}_2$ and fixes $q+1$ points. Hence, g has the cycle type $m^{\frac{q^2-q}{m}}.x^{\frac{q-1}{x}}.p^{\frac{q}{p}}.1^2$ (it is obvious that g does not contain any cycle of length x_1, where $x_1|x$, because in this case g^{x_1} has order that is a factor of $p\frac{q-1}{d}$ with $|\text{fix}_\Omega(g)| > 2$ and this is impossible). $\diamond$

Remark: Elements in classes of type $\mathcal{C}_5$ are contained in cyclic subgroups of order $p(\frac{q-1}{d})$, however, no two elements in each of these subgroups are $PSL(3, q)$-conjugate. We can easily prove that by contradiction as follows. Let a be an element of order p and $h, h' \in Z(M)^{\#}$ where $h \neq h'$. Then, ah and ah' have orders that are factors of $p(\frac{q-1}{d})$. Now we prove by contradiction that ah and ah' are not G-conjugate. Suppose that ah and ah' are $PSL(3, q)$-conjugate, then $(ah)^g = ah'$. By taking the p^{th} power of both sides we get $(h^p)^g = h'^p$. Since $h, h' \in Z(M)^{\#}$, it also follows that $h^p, h'^p \in Z(M)^{\#}$. As h^p and h'^p are not G-conjugate, we must have that

$$h^p = h'^p = 1 \text{ or } h = h'$$

which is a contradiction since $p \nmid \frac{q-1}{d}$ and $h \neq h'$.

3.3.1 Number of fixed k-subsets by elements in $\mathcal{C}_6 \cup \mathcal{C}_6'$

From Lemma 3.2.5 (vi) and Table 3.1, there is a little known about classes of type $\mathcal{C}_6 \cup \mathcal{C}_6'$. However, our calculations (using MAGMA) indicate that elements of these classes have complicated cycle types. The next example shows that the cycle types of representatives of $\mathcal{C}_6$ and $\mathcal{C}_6'$ when $G \cong PSL(3, 73)$.

Example 3.3.4 Let $G \cong PSL(3, 73)$ and let g be a representative of a class of type $\mathcal{C}_6$ or $\mathcal{C}_6'$. As $q - 1 = 72$, then from Lemma 3.2.5 (vi), g has order that is a factor of 72. Using MAGMA, we can calculate the elements in $\mathcal{C}_6 \cup \mathcal{C}_6'$ and their cycle types as shown in the following table:

Cycle type of g	$\lvert g \rvert$	Number of classes
$3^{1800} \cdot 1^3$	3	1
$4^{1332} \cdot 2^{36} \cdot 1^3$	4	1
$6^{888} \cdot 3^{24} \cdot 1^3$	6	1
$6^{876} \cdot 3^{24} \cdot 2^{36} \cdot 1^3$	6	2
$8^{666} \cdot 4^{18} \cdot 1^3$	8	4
$8^{666} \cdot 2^{36} \cdot 1^3$	8	2
$9^{600} \cdot 1^3$	9	3
$12^{444} \cdot 3^{24} \cdot 1^3$	12	2
$12^{444} \cdot 6^{12} \cdot 1^3$	12	2
$12^{444} \cdot 2^{36} \cdot 1^3$	12	2
$12^{438} \cdot 6^{12} \cdot 4^{18} \cdot 1^3$	12	4
$12^{438} \cdot 4^{18} \cdot 3^{24} \cdot 1^3$	12	4
$18^{296} \cdot 9^8 \cdot 1^3$	18	9
$24^{222} \cdot 6^{12} \cdot 1^3$	24	4
$24^{222} \cdot 12^6 \cdot 1^3$	24	8
$24^{222} \cdot 4^{18} \cdot 1^3$	24	8
$24^{222} \cdot 3^{24} \cdot 1^3$	24	4
$24^{222} \cdot 2^{36} \cdot 1^3$	24	4
$24^{219} \cdot 12^6 \cdot 8^9 \cdot 1^3$	24	16
$24^{219} \cdot 8^9 \cdot 3^{24} \cdot 1^3$	24	8
$24^{219} \cdot 8^9 \cdot 6^{12} \cdot 1^3$	24	8
$36^{148} \cdot 9^8 \cdot 1^3$	36	18
$36^{148} \cdot 18^4 \cdot 1^3$	36	18
$72^{74} \cdot 9^8 \cdot 1^3$	72	36
$72^{74} \cdot 36^2 \cdot 1^3$	72	72
$72^{74} \cdot 18^4 \cdot 1^3$	72	36

Table 3.3: Cycle types of elements of $\mathcal{C}_6 \cup \mathcal{C}_6'$ in $PSL(3, 73)$

Bradley and Rowley [2] provided an example of the cycle structure of elements in

$PSU(3, 71)$ which occur in classes of type $\mathcal{C}_6 \cup \mathcal{C}_6'$ (see Table (1) in [2]). These elements are contained in cyclic subgroups of orders that are factors of $q + 1 = 71 + 1 = 72$. Comparing Table 3.3 and Table (1) in [2], we show that, after excluding the fixed points, elements of the same order in both groups have the same cycle lengths as well as the same number of classes. Therefore, the proof of the cycle types of elements of $PSL(3, q)$ which lie in $\mathcal{C}_6 \cup \mathcal{C}_6'$ will be probably very similar to that for $PSU(3, q)$.

Throughout, we will make use of the notation used in [2] and we start by letting $\ell = \frac{q-1}{d}$ and $\ell' \in D(\ell)$. Set $(\ell_1, \ell_2) \in D(\ell') \times D(\ell')$ and assume that the prime factorization of ℓ_1 and ℓ_2 are as follows:

$$\ell_1 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$$

$$\ell_2 = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r},$$

where at least one of α_i and β_i is non-zero for $1 \leq i \leq r$. Put $\ell_{12} = lcm\{\ell_1, \ell_2\}$. If $\alpha_i \neq \beta_i$, then define $\gamma_i = max\{\alpha_i, \beta_i\}$. Suppose that $\alpha_i = \beta_i$ for $1 \leq i \leq s$ and $\alpha_i \neq \beta_i$ for $s + 1 \leq i \leq r$. Then we can define ℓ_0, m_1, m_2 and ℓ_* as follows:

$$\ell_0 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s},$$

$$m_1 = p_{s+1}^{\alpha_{s+1}} p_{s+2}^{\alpha_{s+2}} ... p_r^{\alpha_r},$$

$$m_2 = p_{s+1}^{\beta_{s+1}} p_{s+2}^{\beta_{s+2}} ... p_r^{\beta_r} \text{ and}$$

$$\ell_* = p_{s+1}^{\gamma_{s+1}} p_{s+2}^{\gamma_{s+2}} ... p_r^{\gamma_r}.$$

Definition 3.3.5 We continue to use the notation given above. Let $k \in \mathbb{N}$ and $n = n_* \ell_*$, where $n_* \in D(\ell_0)$ and $n_* = p_1^{\delta_1} p_2^{\delta_2} ... p_s^{\delta_s}$. Further suppose that 3^a is the largest power of 3 dividing $q - 1$.

(i) $\pi_6^{(\ell_1, \ell_2, n)} = \ell_{12}^{\frac{(q^2-2q+1)}{\ell_{12}}} \cdot \ell_1^{\frac{q-1}{\ell_1}} \cdot \ell_2^{\frac{q-1}{\ell_2}} \cdot n^{\frac{q-1}{n}} \cdot 1^3$, where $(\ell_1, \ell_2) \in D^*(\ell) \times D^*(\ell)$.

(ii) When $3^i | q - 1$ with $i \in \mathbb{N}$,

$$3^i \pi_6^{(\ell_1, \ell_2, n)} = (3^i \ell_{12})^{\frac{(q^2-2q+1)}{3^i \ell_{12}}} \cdot (3^i \ell_1)^{\frac{q-1}{3^i \ell_1}} \cdot (3^i \ell_2)^{\frac{q-1}{3^i \ell_2}} \cdot (3^i n)^{\frac{q-1}{3^i n}} \cdot 1^3,$$

where $(\ell_1, \ell_2) \in D(\ell) \times D(\ell)$.

(iii)

$$f(\ell_1,\ell_2,n)=\phi(m_1)\phi(m_2)\phi(\ell_0)\prod_{\substack{\alpha_j=\delta_j\\1\le j\le s}} p_j^{\alpha_j-1}(p_j-2)\phi\Big(\prod_{\substack{\alpha_j\ne\delta_j\\1\le j\le s}} p_j^{\delta_j}\Big).$$

(iv)

$$\lambda_k^*(\ell,\ell)=\sum_{(\ell_1,\ell_2)\in D^*(\ell)\times D^*(\ell)}\ \sum_{\substack{1\ne n=\ell_* n_*\\ n_*\in D(\ell_0)}} f(\ell_1,\ell_2,n)\eta_k(\pi_6^{(\ell_1,\ell_2,n)}).$$

(v) Let $\ell'\in D^*(q-1)$ and $3^i|\ell'$ for some $i\in\mathbb{N}$,

$$\lambda_k(\ell',\ell';i)=\sum_{(\ell_1,\ell_2)\in D(\ell')\times D(\ell')}\ \sum_{\substack{n=\ell_* n_*\\ n_*\in D(\ell_0)}} f(\ell_1,\ell_2,n)\eta_k(3^i\pi_6^{(\ell_1,\ell_2,n)}).$$

Hypothesis 3.3.6 *Suppose that A_0 is an abelian group acting upon a set Ω, and A_0 has a subgroup $A\cong\mathbb{Z}_e\times\mathbb{Z}_e$ of index 3 or 1. Further suppose that A has order e^2 and contains three cyclic subgroups A_i of order e, $1\le i\le 3$ such that*

(i) $fix_\Omega(A_i)\cap fix_\Omega(A_j)=\emptyset$ for $1\le i\ne j\le 3$;

(ii) $|fix_\Omega(A_i)|=q-1$ for $i=1,2,3$; and

(iii) for $1\ne g\in A_0$, $fix_\Omega(g)=\emptyset$ if $g\notin\cup_{i=1}^3 A_i$ and $fix_\Omega(g)=fix_\Omega(A_i)$ if $g\in A_i$.

Set $\Lambda_i=fix_\Omega(A_i)$ for $i=1,2,3$ and $\Lambda=\Omega\backslash(fix_\Omega(A_1)\cup fix_\Omega(A_2)\cup fix_\Omega(A_3))$. Clearly, $\Omega=\Lambda_1\cup\Lambda_2\cup\Lambda_3\cup\Lambda$.

Lemma 3.3.7 *Suppose Hypothesis 3.3.6 holds and use the notation A_0, A, and A_i from the hypothesis. Let $(\ell_1,\ell_2)\in D(e)\times D(e)$, with $e\in D(\ell)$. The cycle structure on Ω of the elements $g=g_1g_2\in A$, where $g_i\in A_i$ $(i=1,2)$, with g_i of order ℓ_i is*

$$\pi_6^{*(\ell_1,\ell_2,n)}=(\ell_{12})^{\frac{|\Lambda|}{\ell_{12}}}\cdot(\ell_1)^{\frac{q-1}{\ell_1}}\cdot(\ell_2)^{\frac{q-1}{\ell_2}}\cdot(n)^{\frac{q-1}{n}},$$

where $n=\ell_* n_*$, with $n_*\in D(\ell_0)$ and $\ell_{12}=lcm(\ell_1,\ell_2)$. This cycle structure, as g_1 and g_2 range over the elements of order (respectively) ℓ_1 and ℓ_2, occurs

$$\phi(m_1)\phi(m_2)\phi(\ell_0)\prod_{\substack{\alpha_j=\delta_j\\1\le j\le s}} p_j^{\alpha_j-1}(p_j-2)\phi\Big(\prod_{\substack{\alpha_j\ne\delta_j\\1\le j\le s}} p_j^{\delta_j}\Big)$$

times, where $n_*=p_1^{\delta_1}...p_s^{\delta_s}$.

PROOF The proof of this lemma is very similar to the proof of Lemma (3.8) in [2]. ⋄

From Lemma 3.2.1 G contains a subgroup M isomorphic to the projective image of $GL(2,q)$. The subgroup M has a subgroup E_0 of the form $\hat{}(q-1)^2 \cong \mathbb{Z}_{q-1} \times \mathbb{Z}_\ell$, where $\ell = \frac{q-1}{d}$, with $N_G(E_0)$ isomorphic to the maximal subgroup of G, $\hat{}(q-1)^2 : \mathrm{Sym}(3)$.

Lemma 3.3.8 *Let $E_0 \cong \mathbb{Z}_{q-1} \times \mathbb{Z}_\ell$ with $\ell = \frac{q-1}{d}$. Then $|fix_\Omega(E_0)| = 3$.*

Proof We give an elementary proof of this lemma. Let $\mathbb{Z}_{q-1} = \langle a \rangle$. From Lemma 3.2.5 (vi) and Table 3.1, a is an element of a class of type $\mathcal{C}_6$ and $|\mathrm{fix}_\Omega(a)| = |\mathrm{fix}_\Omega(\mathbb{Z}_{q-1})| = 3$. Similarly, let $\mathbb{Z}_\ell = \langle b \rangle$, then from Lemma 3.3.3, b is an element of a class of type $\mathcal{C}_4$ and $|\mathrm{fix}_\Omega(b)| = |\mathrm{fix}_\Omega(\mathbb{Z}_\ell)| = q+2$.

We shall prove by contradiction that $\mathrm{fix}_\Omega(\mathbb{Z}_{q-1}) \cap \mathrm{fix}_\Omega(\mathbb{Z}_\ell) = \mathrm{fix}_\Omega(\mathbb{Z}_{q-1})$. Let $g \in E_0$, then $g = g_1 g_2$ where $g_1 \in \mathbb{Z}_{q-1}$ and $g_2 \in \mathbb{Z}_\ell$. Suppose that $\mathrm{fix}_\Omega(\mathbb{Z}_{q-1}) \cap \mathrm{fix}_\Omega(\mathbb{Z}_\ell) \neq \mathrm{fix}_\Omega(\mathbb{Z}_{q-1})$. Then there is a point $\beta \in \Omega \setminus \mathrm{fix}_\Omega(\mathbb{Z}_{q-1})$ such that $\alpha g = \beta$, where $\alpha \in \mathrm{fix}_\Omega(\mathbb{Z}_{q-1})$. It follows that $\alpha(g_1 g_2) = \beta$. Since $\alpha \in \mathrm{fix}_\Omega(g_1)$, $\alpha g_2 = \beta$. As E_0 is abelian subgroup, then $\alpha(g_2 g_1) = \beta$. Hence, we have that $\beta g_1 = \beta$. Therefore, $\beta \in \mathrm{fix}_\Omega(\mathbb{Z}_{q-1})$, which is impossible. $\diamond$

Definition 3.3.9 Let E_0 be as defined above and put $E_0^* = (\mathcal{C}_6 \cup \mathcal{C}_6') \cap E_0$. Then the number of fixed k-subsets by elements in E_0^* is denoted by

$$\epsilon_k(E_0^*, \Omega) = \sum_{g \in E_0^*} |\mathrm{fix}_{\Omega_k}(g)|.$$

Lemma 3.3.10 *Let E_0 be an abelian subgroup of G such that $E_0 \cong \mathbb{Z}_{q-1} \times \mathbb{Z}_\ell$, with $N_G(E_0) \cong \hat{}(q-1)^2 : Sym(3)$. Further suppose that E is the subgroup generated by elements of E_0 of order $\ell = \frac{q-1}{d}$. Then*

(i) if $d = 1$, then $\epsilon_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell)$;

(ii) if $d = 3$ and $3 \nmid |E|$, then $\epsilon_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell) + 2\lambda_k(\ell, \ell; 1)$;

(iii) if $d = 3$ and $3 || E|$, then $\epsilon_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell) + 2 \cdot 9^{b-1} \lambda_k(\frac{q-1}{3^b}, \frac{q-1}{3^b}; b)$ where 3^b is the largest power of 3 dividing $q-1$.

Proof From Lemma 3.2.1(i), we know that $\hat{}GL(2,q)$ is a subgroup of G. Let $M \cong \hat{}GL(2,q)$. Then M contains a subgroup E_0 of order $\frac{(q-1)^2}{d}$ such that $E_0 \cong \mathbb{Z}_{q-1} \times \mathbb{Z}_{\frac{q-1}{d}}$. Let $D \cong Z(M)$, then from the structure of E_0, we have $D \leqslant E_0$ with $D \cong \mathbb{Z}_{\frac{q-1}{d}}$. Let N be the maximal subgroup $\hat{}(q-1)^2 : \mathrm{Sym}(3)$. Then, from Lemma 3.2.3 N contains only three conjugate subgroups of D. There exists an element $g \in N$ of order three such that $A_1 = D$, $A_2 = D^g$, and $A_3 = D^{g^2}$. Since elements of D lie in $\mathcal{C}_4$, from Table 3.1 $|\text{fix}_\Omega(A_i)| = q+2$.

As we saw in Lemma 3.3.8, E_0 fixes three points in Ω, so we may take $\Sigma = \Omega \setminus \text{fix}_\Omega(E_0)$. In order to show that E_0 satisfies Hypothesis 3.3.6 and then Lemma 3.3.7, we let E_0 be acting upon the set Σ. Therefore, we have $|\text{fix}_\Sigma(E_0)| = 0$ and $|\text{fix}_\Sigma(A_i)| = q-1$, for $i = 1,2,3$. Let $h \in E_0 \setminus (\cup_i A_i)$, then from Table 3.1, $\text{fix}_\Sigma(h) = \emptyset$. Now let E be the subgroup of E_0 generated by elements of order $\frac{q-1}{d}$. It follows that $[E_0 : E] = d$ and $E = A_iA_j, 1 \leq i \neq j \leq 3$. As $\text{fix}_\Sigma(h) = \emptyset$ if $h \in E \setminus (\cup_i A_i)$, it holds that $\text{fix}_\Sigma(A_i) \cap \text{fix}_\Sigma(A_j) = \emptyset$ for $1 \leq i \neq j \leq 3$. Thus, Hypothesis 3.3.6 hold with $e = \ell$.

Suppose that $d = 1$, then $E_0 = E$. By Lemma 3.3.7, elements in E_0 (in its action on Σ) have the cycle structure $\pi_6^{*(\ell_1,\ell_2,n)}$. As each of these elements fixes three points in Ω, then they have the cycle structure $\pi_6^{(\ell_1,\ell_2,n)}$ on the set Ω. Thus, from Lemma 3.3.7, we have $\epsilon_k(E_0^*, \Omega) = \lambda^*(\ell,\ell)$.

Suppose that $d = 3$, then $[E_0 : E] = 3$. Let $\theta : E_0 \longrightarrow E_0$ be a map given by $\theta(g) = g^3$ for all $g \in E_0$. Since E_0 is abelian, θ is a homomorphism, with $im\theta \leqslant E$ and $ker\theta = \{x \in E_0 |\ |x| = 3 \text{ or } 1\}$.

Now suppose that $d = 3$ and $3 \nmid \ell$. We may take E_0 acting upon the set Σ. As $|E| = \ell^2$, then $3 \nmid |E|$. It follows that $|ker\theta| = 3$ and $|im\theta| = |E|$. Let $g \in E_0$, then there exists an element $h \in E$ such that $\theta(g) = g^3 = h$. Note that $|\theta^{-1}(\{h\})| = 3$. Due to the fact that $3 \nmid |E|$, θ restricted to E is one-to-one map. Then elements in E have cycle type $\pi_6^{*(\ell_1,\ell_2,n)}$. Hence, elements of $E \setminus (\cup_i A_i)$ in its action on Ω contribute $\lambda^*(\ell,\ell)$ to $\epsilon(E_0^*, \Omega)$. For every $g \in E_0 \setminus E$, the smallest power of g contained in A_i will be three times the corresponding power for $h = g^3 = \theta(g)$. Hence, the inverse image of h contains two elements of $E_0 \setminus E$. Then we must multiply the cycle length of h by 3. It follows that elements in $E_0 \setminus E$ in its action on Ω have cycle type $3\pi_6^{(\ell_1,\ell_2,n)}$. From Lemma 3.3.7, elements in $E_0 \setminus E$ contribute $2\lambda(\ell,\ell;1)$ to $\epsilon_k(E_0^*, \Omega)$. Thus, $\epsilon_k(E_0^*, \Omega) = \lambda^*(\ell,\ell) + 2\lambda(\ell,\ell;1)$.

Finally, assume that $d = 3$ and $3|\ell$. Then $|ker\theta| = 3^2$ and it follows that $[E : im\theta] = 3$. We continue to let E_0 acting on the set Σ. Let $A_i^{(3)}$ be the unique subgroup of A_i of index 3. Let B be a subgroup of E generated by the elements of order $\frac{\ell}{3}$ in E. It follows that $B = A_i^{(3)}A_j^{(3)}$, for $1 \leq i \neq j \leq 3$, with $[E : B] = 3^2$. Note that B is a subgroup of $im\theta$ with $[im\theta : B] = 3$. As remarked above, A_1 has only three conjugate subgroups $\{A_1, A_2, A_3\}$ in N. Therefore, N normalizes B and the N-conjugate class of A_1B is $\{A_1B, A_2B, A_3B\}$, with $[E : A_iB] = 3$. Since $A_i \neq A_j$, for $1 \leq i \neq j \leq 3$, $A_iB \neq A_jB$. Also observe that $im\theta$ is a normal subgroup of N. Then, N has four normal subgroups of E of index 3 which contain B. Note that the inverse image under θ of B is E. Following from that and from Lemma 3.3.7, elements in E in its action on Ω contribute $\lambda^*(\ell, \ell)$ to the count of $\epsilon_k(E_0^*, \Omega)$.

Now we are looking to determine the contribution of elements in $E_0 \setminus E$. Let $h \in im\theta \setminus B$, then $\theta^{-1}(\{h\}) \subseteq E_0 \setminus E$ and $|\theta^{-1}(\{h\})| = 9$. For $g \in \theta^{-1}(\{h\})$, $h = g^3$. To count the contribution of $\theta^{-1}(\{h\})$, we must multiply the cycle lengths of h by 3 and the multiplicity by 9.

Since $B = A_i^{(3)}A_j^{(3)}$, $1 \leq i \neq j \leq 3$, is a subgroup of $im\theta$ of index 3, $A_i^{(3)}$ is a subgroup of $im\theta \cap A_i$. Now, if $im\theta \cap A_i \neq A_i^{(3)}$, then $im\theta \cap A_i = A_i$ as $[A_i : A_i^{(3)}] = 3$. Since $A_j^{(3)} \leqslant im\theta$, then

$$im\theta \geqslant A_iA_j^{(3)} = A_iA_i^{(3)}A_j^{(3)} = A_iB.$$

This is impossible as $A_iB \neq im\theta$. Hence, $A_i \cap im\theta = A_i^{(3)}$ for $1 \leq i \neq j \leq 3$. Then, we have that $im\theta \cong \mathbb{Z}_{\frac{q-1}{3}} \times \mathbb{Z}_{\frac{q-1}{3^2}}$ and it satisfies Hypothesis 3.3.6 with $B \cong \mathbb{Z}_{\frac{q-1}{3^2}} \times \mathbb{Z}_{\frac{q-1}{3^2}}$ playing the role of E and $im\theta \cap A_i$ the role of A_i $(1 \leq i \leq 3)$. Moreover, B satisfies Hypothesis 3.3.6, with B playing the role of E and $A_i^{(3)}$ the role of A_i $(1 \leq i \leq 3)$. In this case we multiply the cycle lengths of elements in $im\theta \setminus B$ by 3 and the multiplicity by 9. We may repeat this process for $im(\theta^2) \setminus B^2$ (where B^2 is a subgroup of $im(\theta^2)$ of index 3), each time multiplying cycle lengths by 3 and the multiplicity by 9. In the end, we arrive at the subgroup $im(\theta^{b-1}) \cong \mathbb{Z}_{\frac{q-1}{3^{b-1}}} \times \mathbb{Z}_{\frac{q-1}{3^b}}$, containing the subgroup group $B^* \cong \mathbb{Z}_{\frac{q-1}{3^b}} \times \mathbb{Z}_{\frac{q-1}{3^b}}$ of index 3 and $3 \nmid \frac{q-1}{3^b}$. The count of this subgroup is given by part (ii) (with $\ell = \frac{q-1}{3^{b-1}}$) and the count for B^* (with $\ell = \frac{q-1}{3^b}$). Now by following the changes in cycle length and multiplicity, we obtain

$$9^{b-1}(\lambda_k^*(\frac{q-1}{3^{b-1}}, \frac{q-1}{3^{b-1}}) + 2\lambda_k(\frac{q-1}{3^b}, \frac{q-1}{3^b}; b) - \lambda_k^*(\frac{q-1}{3^{b-1}}, \frac{q-1}{3^{b-1}})).$$

Thus, the contribution of $E_0 \setminus E$ in its action on the set Ω is $2 \cdot 9^{b-1}\lambda_k(\frac{q-1}{3^b}, \frac{q-1}{3^b}; b)$. It follows that

$$\epsilon_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell) + 2 \cdot 9^{b-1}\lambda_k(\frac{q-1}{3^b}, \frac{q-1}{3^b}; b),$$

which completes the proof. $\diamond$

Remark: We can combine the three equations of $\epsilon_k(E_0^*,\Omega)$ given in Lemma 3.3.10 into a single equation given as follows:

$$\epsilon_k(E_0^*,\Omega) = \lambda_k^*(\ell,\ell) + (\frac{d-1}{2})2\cdot 9^{b-1}(\frac{q-1}{3^b},\frac{q-1}{3^b};b),$$

where 3^b is the largest power of 3 dividing $q-1$. Note that, in the case where $b=1$, part (ii) and part (iii) are equal.

3.3.2 Proof of Theorem 3.3.1

Now we are in a position to prove Theorem 3.3.1.

Proof In order to employ Burnside's Lemma, we first count the number of fixed k-subsets for each conjugacy class type.

Let $g \in G$ such that $g \in X$, where X is a conjugacy class of type $\mathcal{C}_i$, $1 \le i \le 8$. Let X is a class of type $\mathcal{C}_1$. Then g is the identity element and $|\mathrm{fix}_{\Omega_k}| = \eta_k(\pi_1)$. Hence, the contribution from this class is

$$\frac{\eta_k(\pi_1)}{|G|} = \frac{d\eta_k(\pi_1)}{q^3(q^3-1)(q^2-1)}.$$

Let X be a class of type $\mathcal{C}_2$. From Lemma 3.3.3, g is an element of order p and hence, $|\mathrm{fix}_{\Omega_k}(g)| = \eta_k(\pi_2)$. From Table 3.2, we can see that there is only one class of type $\mathcal{C}_2$ and has length $(q^3-1)(q+1)$. Then $\mathcal{C}_2$ will contributes $\frac{d}{q^3(q-1)}\eta_k(\pi_2)$ to the total.

Similarly, from Table 3.2 and Lemma 3.3.3, elements in classes of type $\mathcal{C}_3$ fix $q(q^3-1)(q^2-1)\eta_k(\pi_3)$ k-subsets. Then, we have a total contribution of

$$\frac{d\eta_k(\pi_3)}{q^2}.$$

Let X be a class of type $\mathcal{C}_4$. Then from Lemma 3.3.3, each element in these classes fixes $\eta_k(\pi_4^{(x)})$ k-subsets. The representatives of these classes are contained in cyclic subgroups of orders that are factors of $\frac{q-1}{d}$. Since elements in each of these cyclic subgroups are not G-conjugate, the summation over $D^*(\ell)$ is enough. Hence, elements in $\mathcal{C}_4$ contribute

$$\frac{d}{q(q^2-1)(q-1)}\sum_{x\in D^*(\ell)}\phi(x)\eta_k(\pi_4^{(x)})$$

to the total.

Now let X be a class of type $\mathcal{C}_5$. Then each element in X fixes $\eta_k(\pi_5^{(m)})$ k-subsets. These elements are contained in cyclic subgroups of orders that are factors of $p\frac{q-1}{d}$. Elements in each of these cyclic subgroups are not G-conjugate, then we only need to sum these elements over $D^*(\ell)$. Therefore, the total contribution from elements in $\mathcal{C}_5$ will be

$$\frac{d}{q(q-1)} \sum_{\substack{x \in D^*(\ell) \\ m=px}} \phi(x)\eta_k(\pi_5^{(m)}).$$

From Lemma 3.3.10, elements in classes of type $\mathcal{C}_6$ are contained in subgroups of the shape $\hat{}(q-1)^2$. Elements in these subgroups are normalized by Sym(3), therefore, to establish the contribution of these classes, we take our centralizer order from Table 3.1, and divide the total by 6. Then, the final contribution from these classes is

$$\frac{d\epsilon_k(E_0, \Omega)}{6(q-1)^2}.$$

From Table 3.1, we show the class of type $\mathcal{C}_6'$ only appears when $d = 3$. In this case, there is only one class of this type and it consists of elements of order 3. We include this class with other classes of type $\mathcal{C}_6$ in $\epsilon_k(E_0, \Omega)$. Observe that, in this case $\ell_1 = \ell_2 = n = 3$ and hence $f(3,3,3) = 2$. Since the total count is divided by 6, this corrects the size of this class in our count.

Let X be a class of type $\mathcal{C}_7$. Then elements in X have cycle type $\pi_7^{(n,j)}$ and each element fixes $\eta_k(\pi_7^{(n,j)})$ k-subsets. These elements are found in cyclic subgroups of orders that are factors of $\frac{q^2-1}{d}$ but not $\frac{q-1}{d}$, so all elements of orders that are factors of $\frac{q-1}{d}$ which lie in classes of type $\mathcal{C}_4$ are excluded. According to Table 3.1 and [1], the generators of these subgroups are conjugate to their q^{th} power. Hence, each subgroup contains two representatives of the class $\mathcal{C}_7$. Then, elements in $\mathcal{C}_7$ contribute

$$\frac{d}{2(q^2-1)} \sum_{\substack{n \in D^*(q^2-1) \\ n \notin D(q-1) \\ j \in D^*(\frac{q-1}{d})}} \phi(n)\eta_k(\pi_7^{(n,j)}).$$

Finally, elements in classes of type $\mathcal{C}_8$ have cycle type $\pi_8^{(y)}$ and are contained in subgroups of orders that are factors of $\frac{q^2+q+1}{d}$. Let $H = \langle g \rangle$ be a cyclic subgroup of an order divides $\frac{q^2+q+1}{d}$, such that g is a representative of a class of type $\mathcal{C}_8$. From Table 3.1 and [1], g is conjugate to g^q and g^{q^2}. Thus, each classes contains three representatives from H. Hence, we divide our count by 3 and then the final contribution is

$$\frac{d}{3(q^2+q+1)} \sum_{y \in D^*(\frac{q^2+q+1}{d})} \phi(y)\eta_k(\pi_8^{(y)}).$$

By summing all these contributions, we obtain the formula for $\sigma_k(G,\Omega)$. $\diamond$

As the formula of counting $\sigma_k(G,\Omega)$ is slightly complicated, we provide a Magma code to count the value of $\sigma_k(G,\Omega)$. Due to the length of this code, we include it as appendix at the end of this thesis.

Chapter 4

Orbit Lengths

4.1 Introduction

In this chapter we are interested in the lengths of G-orbits of such a group G acting on Ω_k, the set of all k-subsets of a set Ω. There has been much research devoted to the question of what the link is between the orbit length of a k-set Δ and the orbit length of a $(k+1)$-set Σ containing Δ.

In 1997 Mnukhin [26] published his paper "Some relations for the lengths of orbits on k-sets and $(k-1)$-sets", in which he was able to provide a bounding property of the orbits' length on k-sets (see Theorem(B)[26]). Although the result is given in general, it is not strong enough and this is clear from the example provided in his paper.

In 1988 Siemons and Wagner [29] studied the relation between the length of orbits of k-sets and $(k+1)$-sets in their paper "On the relationship between the lengths of orbits on k-sets and $(k+1)$-sets". They discussed both cases where G is a primitive or an imprimitive group and stated the following theorems.

Theorem 4.1.1 *Let G be a transitive permutation group on a finite set Ω and let Δ be a given subset of Ω of cardinality $k < |\Omega|$. Suppose that $|\Sigma^G| < |\Delta^G|$ for every set $\Sigma \supset \Delta$ of cardinality $k+1$. Then*

$$k + 1 \geqslant |\Delta^{G_\Sigma}| > |\Sigma^{G_\Delta}| \geqslant 1$$

If furthermore $k \geqslant 2$, then either

(i) every 2-element subset of Ω is contained in some G-image of Δ, or

(ii) G is imprimitive with blocks of imprimitivity $\Omega_1, ..., \Omega_r$ $(1 < |\Omega_i| < |\Omega|)$ each intersecting Δ in at most 1 point such that every 2-element subset of the form α_i, α_j with $\alpha_i \in \Omega_i \neq \Omega_j \ni \alpha_j$ is contained in some G-image of Δ.

In the following theorem they classified all exceptions when $k = 2$.

Theorem 4.1.2 *Let G be a transitive group of degree $n > 4$. Suppose there is some 2-element subset Δ such that $|\Delta^G| > |\Sigma^G|$ for every 3-element subset Σ containing Δ. If G is primitive, then $G = PSL(2,5)$ in its natural action on six points. Otherwise, G has three blocks of imprimitivity Ω_1,Ω_2 and Ω_3 with $|\Omega_i|$ a power of 2. Furthermore, $\Delta^G = \{\{\alpha, \beta\} | \alpha \in \Omega_i \neq \Omega_j \ni \beta\}$ and G has order $3 \cdot |\Omega_i|^2 \cdot |G_\Delta|$ with $|G_\Delta| \leq 2$.*

This chapter is devoted to investigating the relationship between the orbit length of k-sets and $(k+1)$-sets of the group $PSL(2, q)$, $q = p^a$, acting on the projective line of $q + 1$ points. The structure of this chapter is as follows. In the first section, we define the main hypothesis of our work and then we provide background information about $PSL(2, q)$. In the second section, we study the orbit lengths of $PSL(2, q)$ when $k = 3, 4$ and 5. In the last section, we let $G \cong PSL(2, 2^n)$ and investigate the cases when $k = 5, 6$, and 7.

Throughout this chapter we use upper case Greek letters to denote the subsets of size k and we use the lower case Greek letters to denote points of those subsets.

4.2 General Results

In this chapter we concentrate on a similar hypothesis to that in Siemons and Wagner's Theorem. In particular, we focus on groups that satisfy the following hypothesis:

Hypothesis($*$): Let G be a transitive permutation group of n points and let $2 \leq k \leq \frac{n}{2}$. There is some k-subset Δ of Ω in a G-regular orbit, an orbit of the maximal length $|G|$, and $|\Sigma^G| < |G|$ for every $(k+1)$-sets Σ containing Δ.

Corollary 4.2.1 *Let G be a transitive group acting upon a set Ω of size $n > 4$. If $k = 2$, then there is no primitive group that satisfies Hypothesis($*$).*

PROOF The result follows from Theorem 4.1.2 together with the fact that $PSL(2, 5)$ has no G-regular orbit on its action on Ω_2. $\diamond$

The primitive groups satisfying Hypothesis($*$) are few, so relying on a computer software to determine these groups is necessary. Bradley [3] in his thesis created a MAGMA code to find all instances of primitive groups satisfying the Siemons-Wagner assumption, when the degree is less than 25. In our work, we modify his code to find primitive groups that satisfy Hypothesis($*$), where $n \leq 25$.

```
Z:=Integers();
SizeofOrbsPRIMk:=procedure(G,k,~a);
S:={}; K:={}; D:={1..Degree(G)}; kD:=Subsets(D,k);a:={};
Omega:=GSet(G,kD); O:=Orbits(G,Omega);
for Orbs in O do T:=Random(Orbs);Include(~K,T);end for;
V:={};
for T in K do;N:=Z!(#G/#Stabilizer(G,T));
if N eq #G then P:=D diff T; for b in P do;
Include(~V, #Stabilizer(G, T join{b}));
end for;
S:=Min(V);L:= Z!(#G/S);
if N gt L then Include(~a,<N,T>);
end if;end if;end for;
end procedure;
```

Letting D be the degree

```
for k in [2..Z!(Floor(D/2)-1)] do
for I:=1 to (Z!(NumberOfPrimitiveGroups(D)-2))do
SizeofOrbsPRIMk(PrimitiveGroup(D, I),k,~T);
if #T ge 1 then <D,I,T>;
end if;end for;end for;
```

The primitive groups of degree less than 25 satisfying Hypothesis($*$) are given on Table 4.1.

Table 4.1: Primitive permutation groups satisfying Hypothesis($*$)

Group	Degree	k
$PSL(2,11)$	12	5
$PSL(2,13)$	14	6
Alt(7)	15	6
$ASL(2,4)$	16	6
$PSL(2,16)$	17	5
$PSL(3,4)$	21	6

In the later arguments, we restrict our attention to studying the family of simple groups $PSL(2,q)$. Our aim is to find groups of $PSL(2,q)$ which satisfy our hypothesis for different instances of k.

In order to find groups that satisfy Hypothesis($*$) we will present some well-known facts regarding $PSL(2,q)$ in Lemma 4.2.2

Lemma 4.2.2 *Let $G \cong PSL(2,q)$, $q = p^a$, acting on the projective line Ω of $q+1$ points, and let $d = (2, q-1)$. Then*

(i) $|G| = \dfrac{q(q+1)(q-1)}{d}$;

(ii) G contains exactly $\dfrac{q(q+1)}{2}$ *cyclic subgroups of order* $\dfrac{q-1}{d}$;

(iii) G contains exactly $\dfrac{q(q-1)}{2}$ *cyclic subgroups of order* $\dfrac{q+1}{d}$;

(iv) G contains exactly $q+1$ elementary abelian p-subgroups of order q, and each contains $\frac{(q-1)(q-p)(q-p^2)...(q-p^{a-1})}{(p^a-1)(p^a-p)(p^a-p^2)...(p^a-p^{a-1})}$ *distinct abelian subgroups of order p^a, $a \leq n$;*

(v) for q is odd and $q \equiv 3 \bmod 4$, G has a single class of $\frac{q(q^2-1)}{4m}$ *dihedral subgroups $Dih(2m)$ of order $2m$ where $m|q \pm 1$ and $m > 2$ and* $\frac{q(q^2-1)}{24}$ *subgroups $Dih(4)$;*

(vi) for q is odd and $q \equiv 1 \bmod 4$, G has two classes each of $\frac{q(q^2-1)}{8m}$ *dihedral subgroups $Dih(2m)$ of order $2m$ where $m|q \pm 1$ and $m > 2$ and two classes each of* $\frac{q(q^2-1)}{48}$ *subgroups $Dih(4)$;*

(vii) for q is even, G has a single class of $\frac{q(q^2-1)}{2m}$ *dihedral subgroups $Dih(2m)$ of order $2m$ where $m|q \pm 1$; and*

(viii) The number of elements of order p is $(q-1)(q+1)$.

PROOF See Huppert [15] Chapter II,§ 8, and Dickson [11] Chapter XII. $\diamond$

Corollary 4.2.3 *Elements in $PSL(2,q)$ have orders either dividing p, $\frac{q-1}{d}$, or $\frac{q+1}{d}$.*

PROOF The results follows from Lemma 4.2.2 (ii), (iii), and (iv). $\diamond$

The number of fixed points of elements in $PSL(2,q)$ is given by the following lemma.

Lemma 4.2.4 *Let $g \in PSL(2,q)$, $q = p^n$, then the number of fixed points of g in Ω is as follows:*

(i) if $|g| | \frac{q-1}{2}$, $fix_\Omega(g) = 2$;

(ii) if $|g| | \frac{q+1}{2}$, $fix_\Omega(g) = 0$;

(iii) if $|g| | p$, $fix_\Omega(g) = 1$.

Let $G \cong PSL(2,q)$ and let H be a subgroup of G, we define $f_k(H)$ and $g_k(H)$ as follows:

$f_k(H)$ is the number of k-subsets fixed by H.

$g_k(H)$ is the number of k-subsets with stabilizer group precisely H.

As we are concerned with calculating the number and length of G-orbits of $PSL(2,q)$, we will use the results of Cameron, Maimani, Omidi, and Tayfeh-Rezaie [5]. In their paper they present a method for calculating the number of orbits of the group $PSL(2,q)$ in the case when $q \equiv 3 \bmod 4$. This method requires the use of a table of the numbers of k-subsets fixed by a subgroup H of $PSL(2,q)$ and numbers of formulae to determine $g_k(H)$ for subgroups H.

Moreover, we will make use of the subgroup structure of $PSL(2,q)$ to find stabilizer subgroups of k-subsets in $PSL(2,q)$. King [20] in his paper titled "The subgroup structure of finite classical groups in terms of geometric configurations" gives a good description of the subgroups of $PSL(2,q)$ based on L.E. Dickson's book [11].

Suppose that H is a subgroup of $PSL(2,q)$ and let $f_k(H)$ be the number of k-subsets fixed by H. Then we can calculate $f_k(H)$ for any subgroup H and $1 \leq k \leq q+1$. Assume that H has r_i orbits of size l_i, $1 \leq i \leq s$, then

$$f_k(H) = \sum_{\sum_{i=1}^{s} m_i l_i = k} \left(\prod_{i=1}^{s} \binom{r_i}{m_i} \right). \tag{4.1}$$

For more details about the determination of f_k we refer the reader to [5].

The next table (Table 4.2) is a part of Table (2) in [5] in which the authors present the number of fixed k-subsets by a subgroup H of $PSL(2,q)$, where $q \equiv 3 \bmod 4$. In our calculations we need only to know $f_k(H)$ for H is a cyclic or dihedral subgroup of $PSL(2,q)$.

Table 4.2: The non-zero values of $f_k(H)$ for some subgroups H of $PSL(2,q)$

H	Condition on m	$l \equiv k \bmod (\lvert H\rvert)$	$f_k(H)$
1		0	$\binom{q+1}{k}$
C_m	$m \mid \frac{q+1}{2}$	0	$\binom{(q+1)/m}{(k-l)/m}$
C_m	$m \mid \frac{q-1}{2}$	0,2	$\binom{(q-1)/m}{(k-l)/m}$
C_m	$m \mid \frac{q-1}{2}$	1	$2\binom{(q-1)/m}{(k-l)/m}$
Dih$(2m)$	$m \mid \frac{q+1}{2}$	0	$\binom{(q+1)/2m}{(k-l)/2m}$
Dih$(2m)$	$m \mid \frac{q-1}{2}$	0,2	$\binom{(q-1)/2m}{(k-l)/2m}$

Where $l \cong k \bmod (|H|)$, $l < |H|$ and l is either a sum of non-regular orbit sizes of H (if H has no two non-regular orbits of size l), or it is a size of non-regular orbit of H (if H has two non-regular orbits each of size l).

Theorem 4.2.5 *[5] Let $G \cong PSL(2,q)$, $q \equiv 3 \bmod 4$, acting on the projective line Ω. Then the number of of k-subsets with trivial stabilizer is given by*

$$g_k(1) = f_k(1) + \frac{q(q^2-1)}{12}(2f_k(Alt(4)) - 6f_k(Sym(4)) - 12f_k(Alt(5)) + f_k(Dih(4))$$
$$+ \sum_{l>1, l \mid (q\pm 1)/2} \frac{q(q\mp 1)}{2}\mu(l) f_k(C_l) - \frac{q(q^2-1)}{4} \sum_{l>2, l \mid (q\pm 1)/2} \mu(l) f_k(Dih(2l)).$$

Remark: In Theorem 4.2.5 $\mu(l)$ is the Möbius function of the lattice subgroup of $PSL(2,q)$. For more details we refer the reader to [5].

Table 4.3: Size of orbits on k-subsets

Orbit size	$\|G\|$	$\frac{\|G\|}{4}$	$\frac{\|G\|}{12}$	$\frac{\|G\|}{24}$	$\frac{\|G\|}{60}$	$\frac{\|G\|}{m}$	$\frac{\|G\|}{2m}(m > 2)$
Number of orbits	$\frac{2g_k(1)}{q^3-q}$	$\frac{g_k(\mathrm{Dih}(4)}{3}$	$g_k(\mathrm{Alt}(4))$	$2g_k(\mathrm{Sym}(4))$	$2g_k(\mathrm{Alt}(5))$	$\frac{mg_k(C_m)}{q\pm1}$	$g_k(\mathrm{Dih}(2m))$

Theorem 4.2.6 *[5] Let $1 \leq k \leq q+1$ and $k \not\equiv 0, 1 mod\ p$. Then the number and size of orbits of $PSL(2, q)$ on k-subsets are as in Table 4.3, where $m | \frac{q\pm1}{2}$ and $m > 1$.*

In 2014 Bradley and Rowley established a formulae to count the number of G-orbits in Ω_k where G is $PSL(2, q)$. We will use their result to find $\sigma_k(G, \Omega)$ for some $PSL(2, q)$.

Theorem 4.2.7 (Bradley-Rowley) *[2] Let $G \cong PSL(2, q)$, where $q > 3$, act upon the projective line Ω, and let $k \in \mathbb{N}$ with $k \geq 3$. Set $d = (2, q-1)$. Then*

$$\begin{aligned}\sigma_k(G, \Omega) = \quad & \frac{d}{q(q+1)(q-1)}\eta_k(1^{q+1}) + \frac{d}{q}\eta_k(1^1 p^{\frac{q}{p}}) \\ & + \frac{d}{2(q+1)} \sum_{m \in D^*(\frac{q+1}{d})} \phi(m)\eta_k(m^{\frac{q+1}{m}}) \\ & + \frac{d}{2(q-1)} \sum_{m \in D^*(\frac{q-1}{d})} \phi(m)\eta_k(1^2 m^{\frac{q-1}{m}}).\end{aligned} \tag{4.2}$$

The notation η_k, $\phi(m)$, and D^* are as defined in Chapter 3.

4.3 Orbit Lengths when $k = 3$, 4 or 5

Lemma 4.3.1 *Let $G \cong PSL(2, 2^n)$, $n \in \mathbb{N}$, acting on the projective line Ω over $GF(q)$. Then for any 4-subset Δ of Ω there is a unique $Dih(4)$ such that $Dih(4) \leqslant G_\Delta$.*

PROOF Let $\Delta = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ be any 4-subset of Ω. The group G is 3-transitive, so there exist an element $g \in G$ such that $\alpha_1 g = \alpha_2$, $\alpha_2 g = \alpha_1$, and $\alpha_3 g = \alpha_4$. Then g contains the 2-cycle (α_1, α_2), it follows that g has even order. By Corollary 4.2.3 only elements of order 2 have even orders, hence $|g| = 2$. Then the action of G_Δ restricted to Δ-set contains all even involution on $\mathrm{Sym}(\Delta)$. Hence, $\mathrm{Dih}(4) \leqslant G_\Delta$. $\diamond$

We will use formula (4.1) to prove the next lemma.

Lemma 4.3.2 *Let $G \cong PSL(2, q)$, acting on the projective line Ω. Then the number of 4-subsets fixed by $Dih(4)$ is as follows* *(i) if q is odd and $q \equiv 1 \bmod 4$, then Dih(4) fixes $\frac{q+7}{4}$ 4-subsets;*

(ii) if q is odd and $q \equiv 3 \bmod 4$, then Dih(4) fixes $\frac{q+1}{4}$ 4-subsets;

(iii) if q is even, then Dih(4) fixes $\frac{q}{4}$ 4-subsets.

PROOF :

(i) Let H be a dihedral subgroup of order 4. In the case of $q \equiv 1 \bmod 4$ each element of order 2 fixes two points in Ω (see Lemma 4.2.4), therefore $\sum_{h\in H} \mathrm{fix}(h) = q+1+6 = q+7$ points. Then by Burnside's Lemma H has $\dfrac{q+7}{4}$ orbits, three of which have size 2 and the others are regular. Therefore, the number of 4-subsets fixed by Dih(4) is given by (4.1) as follows $f_4(H) = \binom{3}{2} + \binom{(q-5)/4}{1} = 3 + \frac{q-5}{4} = \frac{q+7}{4}$.

A similar argument applies to (ii) and (iii). $\diamond$

Theorem 4.3.3 *Let $G \cong PSL(2,q)$ acting on the projective line Ω of $q+1$ points. Let $\Delta \subseteq \Omega$ be a k-subset of Ω, then $|\Delta^G| < |G|$ for $k = 3, 4$*

PROOF :

For $k = 3$. Since $|G| = \dfrac{q(q+1)(q-1)}{d}$, $d = (2, q-1)$ and $|\Omega_3| = \binom{q+1}{3} = \dfrac{q(q+1)(q-1)}{6}$, then $|G| > |\Omega_3|$. Hence there is no orbit Δ^G of the maximal length $|G|$.

For $k = 4$. Since $|\Omega_4| = \dfrac{q(q+1)(q-1)(q-2)}{4!}$ by comparing the order of G to the total number of 4-subsets shows that q must be at least 17. We split our investigation into three cases.

Case 1: q is even. Let $\Delta \subseteq \Omega$ be a 4-subset of Ω. From Lemma 4.3.1 the dihedral subgroup Dih(4) is contained in G_Δ. Hence, from Orbit-Stabilizer Theorem $|\Delta^G| < |G|$.

Case 2: q is odd and $q \equiv 3 \bmod 4$. In this case, G contains $\frac{q(q-1)}{2}$ elements of order 2 and by Table 4.2 each of them fixes $\frac{(q+1)(q-1)}{8}$ subsets of size 4. It is not difficult to count $a = |\{(\Delta, g) | g \in G_\Delta, |g| = 2\}| = \frac{q(q+1)(q-1)^2}{16}$. Then from Lemma 4.2.2$(v)$, G contains $\frac{q(q^2-1)}{24}$ dihedral subgroups of order 4 and by Lemma 4.3.2(ii) each of them fix $\frac{q+1}{4}$ subsets of size 4. Thus, the total number of 4-subsets which are fixed by Dih(4) is $\frac{q+1}{4} \times \frac{q(q^2-1)}{24} = \frac{q(q+1)(q^2-1)}{96}$. Now each Dih(4) contains 3 elements of order 2 leaving the same $\frac{q+1}{4}$ 4-subsets invariant. Then there are $3 \times \frac{q+1}{4} \times \frac{q(q^2-1)}{24} = \frac{q(q+1)(q^2-1)}{32}$ duplicate

4-subsets in a. To avoid double counting we rule out all duplicates 4-subsets from a, that is, $a - \frac{q(q^2-1)(q+1)}{32} = \frac{q(q^2-1)(q-3)}{32}$. Hence elements of order two fix

$$\frac{q(q^2-1)(q-3)}{32} + \frac{q(q^2-1)(q+1)}{96} = \frac{q(q+1)(q-1)(q-2)}{4!} = \Omega_4$$

subsets of size 4. Then the stabilizer for any 4-subsets Δ is non-trivial.

Case 3: q is odd and $q \equiv 1 \mod 4$. The result follows by using Lemma 4.3.2 (i) and a similar argument to case 2. $\diamond$

As we saw in Table 4.1 $PSL(2, 11)$ and $PSL(2, 16)$ satisfy Hypothesis($*$) when $k = 5$. Next, we will give detailed calculations about their number and length of G-orbits on their action on Ω_5.

4.3.1 $PSL(2, 11)$

Let $G \cong PSL(2, 11)$ the 2-dimensional projective special linear group of order $|PSL(2, 11)| = 660$. Since G is 3-homogeneous, we can use the results in [5] to compare between the number of regular orbits when $k = 5$ and $k = 6$.

Regular orbits when $k = 5$

Let Δ be a subset of size 5. From Table 4.2 one can obtain that the stabilizer subgroup for any 5-subset Δ is the cyclic subgroup C_5 or the trivial subgroup. Therefore, the number of 5-subsets fixed by C_5 is

$$f_5(C_5) = \binom{(11-1)/5}{5/5} = 2$$

Then, by using Theorem 4.2.5 we can count the number of 5-subsets with trivial stabilizer as follows

$$g_5(1) = \binom{12}{5} + \frac{11 \times 12}{2} \times (-1) \times 2 = 660$$

Thus, Theorem 4.2.6 tells us that G contains $\frac{2 \times 660}{11^3 - 11} = 1$ regular G-orbit.

Regular orbits when $k = 6$

Let Δ be a subset of size 6. Then, by Table 4.2, the numbers of fixed 6-subsets by subgroups H are as follows:

(i) $f_6(C_2) = \binom{6}{3} = 20$;

(ii) $f_6(C_3) = \binom{4}{2} = 6$;

(iii) $f_6(C_5) = 2 \cdot \binom{2}{1} = 4$;

(iv) $f_6(C_6) = \binom{2}{1} = 2$;

(v) $f_6(\text{Dih}(6)) = \binom{2}{1} = 2$.

Therefore by using Theorem 4.2.5, the number of 6-subsets with trivial stabilizer is

$$\begin{aligned} g_6(1) &= \binom{12}{6} + (\frac{11 \times 10}{2} \times (1) \times 20 + \frac{11 \times 10}{2} \times (-1) \times 6 + \frac{11 \times 12}{2} \times (-1) \times 4 \\ &\quad + \frac{11 \times 10}{2} \times 1 \times 2) - \frac{11 \times (11^2 - 1)}{4} \times (-1) \times 2 = 0 \end{aligned}$$

Hence, from Theorem 4.2.6 G does not contain any regular G-orbit in its action on Ω_6.

From the two cases above we can deduce that $G \cong PSL(2, 11)$ satisfies Hypothesis($*$).

4.3.2 $PSL(2, 16)$

Let $G \cong PSL(2, 16)$ be the 2-dimensional projective special linear group of order $|G| = 4080$. Since $q = 16$, by Lemma 4.2.2 the group G contains elements of order 2,3,5,15, and 17. Table 4.4 presents the number and cycle structure of these elements.

Table 4.4: Number and cycle structure of elements of $PSL(2, 16)$

Order of element	Number of elements	Cycle structure
2	255	$2^8 \cdot 1^1$
3	272	$3^5 \cdot 1^2$
5	544	$5^3 \cdot 1^2$
15	1088	$15^1 \cdot 1^2$
17	1920	17^1

The aim of this section is to compute the number and lengths of G-orbits when $k = 5$ and $k = 6$. Therefore, we need to determine the stabilizer subgroups in each case.

Orbit lengths when $k = 5$

Let G act upon the set Ω_5, where $|\Omega_5| = 6188$. The number of G-orbits on Ω_5 can be counted by using Theorem 4.2.7. First, we need to count $\eta_5(\pi_g)$, the number of 5-subsets fixed by elements $g \in G$.

(i) $\eta_5(1^{17}) = \binom{17}{5} = 6188$;

(ii) $\eta_5(1^1 \cdot 2^8) = \binom{1}{1}\binom{8}{2} = 28$;

(iii) $\eta_5(1^2 \cdot 3^5) = \binom{2}{2}\binom{5}{1} = 5$;

(iv) $\eta_5(1^2 \cdot 5^3) = \binom{2}{0}\binom{3}{1} = 3$;

(v) $\eta_5(17^1) = 0$.

Applying formulae (4.2) in Theorem 4.2.7 to find the number of G-orbits in Ω_5

$$\sigma_5(G,\Omega) = \frac{1}{16 \times 17 \times 15} \times 6188 + \frac{1}{16} \times 28 + \frac{1}{2 \times 17} \times 0 + \frac{1}{2 \times 15}(2 \times 5 + 4 \times 3) = 4.$$

We know from Corollary 2.2 [20] that $H \cong PSL(2,4)$ is a maximal subgroup of $PSL(2,16)$ and that H stabilizes a sub-line of 5 point of the projective line $\Omega = PG(1,16)$. Hence, there exist a G-orbit of length $\frac{|G|}{60} = 68$.

Suppose that Γ is a 4-subsets of Ω, by Lemma 4.3.1 there is a dihedral subgroup $K \cong \text{Dih}(4)$ fixes Γ. Since K fixes one point, say α, in Ω, then K fixes also the 5-subset $\Delta = \Gamma \cup \{\alpha\}$. From Lemma 4.3.2 (iii), every subgroup Dih(4) fixes 4 subsets of size 4; it follows that it fixes also 4 subsets of size 5. Let V be a dihedral subgroup Dih(4) and Δ be a 5-subset of Ω. Assume A to be the set $\{(V,\Delta)|\Delta \in \Omega_5, V \cong \text{Dih}(4)$ and $V \leqslant G_\Delta\}$, we know from Lemma 4.2.2 (iv) G contains 595 Dih(4) subgroups, then $|A| = 595 \times 4 = 2380$. The subgroup $PSL(2,4)$ of G has 5 Dih(4) subgroups and all of them leave the same 5-subset invariant. Since G contains 68 $PSL(2,4)$ subgroups, it follows that A contains $68 \times 5 = 340$ duplicate 5-subsets. To avoid double counting we exclude all duplicate 5-subsets from A, hence there are $|A| - 340 = 2040$ 5-subsets having stabilizers divided by 4.

From the above argument, as there are 4 G-orbits and one of them of size $\frac{|G|}{60}$, then the only possible lengths for the other orbits are: two orbits of length $\frac{|G|}{4}$ and one regular orbit.

Orbit length when $k = 6$

Let G act upon the set of all 6-subsets of Ω, where $|\Omega_6| = 12376$. From Theorem 4.2.7 the number of G-orbits on Ω_6 is given as follows.

(i) $\eta_5(1^{17}) = \binom{17}{6} = 12376$;

(ii) $\eta_5(1^1 \cdot 2^8) = \binom{1}{0}\binom{8}{3} = 56$;

(iii) $\eta_5(1^2 \cdot 3^5) = \binom{2}{0}\binom{5}{2} = 10$;

(iv) $\eta_5(1^2 \cdot 5^3) = \binom{2}{1}\binom{3}{1} = 6$;

(v) $\eta_5(17^1) = 0$.

Therefore,

$$\sigma_5(G, \Omega) = \frac{1}{16 \times 17 \times 15} \times 12376 + \frac{1}{16} \times 56 + \frac{1}{2 \times 17} \times 0 + \frac{1}{2 \times 15}(2 \times 10 + 4 \times 6) = 8.$$

From Table 4.4 only elements of order 2,3 and 5 can fix a set of size 6. First, we will count all 6-subsets with stabilizers isomorphic to Dih(4), Dih(6), Dih(10), or C_2. From Lemma 4.2.2 $(viii)$ G contains $17 \times 15 = 255$ element of order 2 and each of them fixes $\binom{\frac{16}{2}}{3} = 56$ sets of size 6. We may take $A = \{(C_2, \Delta) | \Delta \in \Omega_6 \text{ and } C_2 \leqslant G_\Delta\}$, then $|A| = 255 \times 56 = 14280$.

Obviously, dihedral subgroups of order 4 cannot stabilize any set of size 6, so for any 6-subset Δ we have $4 \nmid |G_\Delta|$. However, by formula (4.1) we can calculate the number of fixed 6-subsets by the dihedral subgroup Dih(6) and it is easy to show that each Dih(6) fixes two subsets of size 6. Since G contains 680 dihedral subgroups Dih(6), then the number of fixed 6-subsets by these groups is 1360. Therefore, we have two orbits of length equal to $\frac{|G|}{6}$. Again formula (4.1) shows that the dihedral subgroups Dih(10) cannot stabilize any subset of size 6.

Since each Dih(6) contains 3 involution leaving the same 6-subsets invariant, the number of 6-subsets with stabilizers isomorphic to C_2 is equal to $|A| - 2 \times 3 \times 680 = 120200$ 6-subsets. Therefore, G must contain 5 orbits of length $\frac{|G|}{2}$. Since G has 8 orbits in its action on Ω_6, the only possible length for the last orbit is $\frac{|G|}{5}$.

As all orbits of the group G in its action on Ω_6 are non-regular and G contains a regular orbit on its action on Ω_5, then G satisfies Hypothesis$(*)$.

4.4 Orbit Length of $PSL(2, 2^n)$

Let $G \cong PSL(2, q)$, where $q = 2^n$ and $n \in \mathbb{N}$. A group G is a 3-transitive on the projective line $\Omega = PG(1, q)$ of $q + 1$ points [12] P(245).

Lemma 4.4.1 *[11] The subgroups of G are as follows:*

(i) Elementary abelian groups of order 2^m, where $m \leq n$;

(ii) Cyclic subgroups of order d where $d|(q \mp 1)$;

(iii) Dihedral subgroups $Dih(2d)$ for $d|(q \mp 1)$;

(iv) Subgroups of order $2^m d$ each of which the semidirect product of an elementary abelian group P_i of order 2^m and a cyclic group of order d, where $d|(q-1)$. Each stabilizes a point;

(v) Subgroups isomorphic with $PSL(2, 2^k)$ where k is a divisor of n;

(vi) Alternating groups $Alt(4)$.

The following lemma determines the stabilizer subgroups for any 5-subset of Ω.

Lemma 4.4.2 *Let Σ be a 5-subset of Ω and G_Σ be the stabilizer of Σ in G. Then*

(i) If $2||G_\Sigma|$, then $4||G_\Sigma|$;

(ii) $3||G_\Sigma|$ if and only if $5||G_\Sigma|$;

(iii) If $3||G_\Sigma|$, then $60||G_\Sigma|$.

Proof See [19].

In 2008 Li and Shen in their papers [21], [22] studied a simple 3-design of $PSL(2, 2^n)$ with blocks of size 6 and 7. In their papers they investigated stabilizers of subsets of sizes 6 and 7 in considerable detail. Their results are summarized in the following two lemmas.

Lemma 4.4.3 *Let Σ be a 6-set of Ω and G_Σ be the stabilizer of Σ in G. Then:*

(i) If $5||G_\Sigma|$, then $2 \nmid |G_\Sigma|$;

(ii) If $3||G_\Sigma|$*, then* $2||G_\Sigma|$ *and* $|G_\Sigma| \neq 12$ *or* 24*;*

(iii) If $2||G_\Sigma|$*, then* $|G_\Sigma| \neq 4$ *or* 8*;*

(iv) If $5||G_\Sigma|$*, then* $|G_\Sigma| = 5$*. If* $3||G_\Sigma|$*, then* $|G_\Sigma| = 6$*.*

Proof See [21].

Lemma 4.4.4 *[22] Let* Σ *be a 7-set of* Ω *and* G_Σ *be the stabilizer of* Σ *in* G*. Then:*

(i) If $7||G_\Sigma|$*, then* $2||G_\Sigma|$ *and* Σ^G *is the unique orbit such that* $7||G_\Sigma|$*.*

(ii) If $5||G_\Sigma|$*, then* $2||G_\Sigma|$ *and* Σ^G *is the unique orbit such that* $5||G_\Sigma|$*.*

(iii) If $3||G_\Sigma|$*, then* $2 \nmid |G_\Sigma|$*.*

Proof See [22].

Lemma 4.4.5 *Let* G *be a transitive permutation group on a finite set* Ω *and let* Δ *be a given subset of* Ω *of size* $k < |\Omega|$*. Suppose that* $|\Delta^G| = |G|$ *and* $|\Sigma^G| < |\Delta^G|$*, where* Σ *is* $(k+1)$*-subset containing* Δ*, then* $|G_\Sigma| \leq k+1$*.*

Proof Since the G-orbit of Δ is regular, then $G_\Delta = 1$. Applying the Orbit-Stabilizer Theorem, we have $|G| = |\Delta^G| = |\Sigma^G| \cdot |G_\Sigma| = |\Sigma^G| \cdot |\Delta^{G_\Sigma}| \cdot |(G_\Sigma)_\Delta|$. As $|G_\Delta| = 1$, then $|(G_\Sigma)_\Delta| = 1$ and therefore $|G_\Sigma| = |\Delta^{G_\Sigma}|$. Clearly, $|\Delta^{G_\Sigma}| \leq k+1$, it follows that $|G_\Sigma| \leq k+1$. $\diamond$

Lemma 4.4.6 *[19] Let* $fix_{\Omega_k}(g)$ *be the number of* k*-subsets of* Ω *fixed by* $g \in G$*, then* $fix_{\Omega_1}(g) = fix_\Omega(g)$*. If* $g \in G$ *is of order* $m > 1$*, then* g *has* $a = fix_\Omega(g) \leq 2$ *fixed points and* $b = \frac{(2^n+1-a)}{m}$ m*-cycles. Thus the number of* k*-subsets of* Ω *fixed by* g *is*

$$fix_{\Omega_k}(g) = \binom{a}{r}\binom{b}{s},$$

where $k = ms + r$*,* $0 \leq r < m$*.*

Remark: If Δ be a k-subset of Ω and g be an element of order m, then $g \in G_\Delta$ if and only if Δ consists of s m-cycle and r fixed points of g, where $k = sm + r$, $0 \leq r < m$.

Lemma 4.4.7 *[22] Suppose* p *is an odd prime such that* $p|2^n - 1$*, if* $p \leq k \leq p+2$*, then there exists a unique orbit* $\Gamma = A^G$ *such that* $p||G_A|$*, where* A *is a* k*-subset of* Ω*. Moreover,* $2||G_A|$ *if* k *is odd.*

We have the following immediate corollary to Lemmas 4.4.5 and 4.4.7

Corollary 4.4.8 *Let* Δ *be a* k*-subset of* Ω *such that* $|G_\Delta| = 1$ *and* $\Sigma = \Delta \cup \{\beta\}$, $\beta \in \Omega \setminus \Delta$. *Suppose that* p *is an odd prime such that* $p|2^n - 1$, *if* $p \leq k+1 \leq p+2$, *where* $k+1$ *is odd, then there are no elements of order* p *that can fix any set* Σ.

Proof The conclusion follows from Lemma 4.4.5 and 4.4.7. $\diamond$

Main Results

Theorem 4.4.9 *Let* $G \cong PSL(2,q)$, *q is even, act upon the projective line* $\Omega = PG(1,q)$ *of* $q+1$ *points. If* $2 \leq k \leq 7$, *then there is no group* G *that satisfies Hypothesis*$(*)$ *except when* $k = 5$ *and* $G \cong PSL(2,16)$.

Due to Corollary 4.2.1 if $k = 2$, then Theorem 4.4.9 holds. Also, we have already proved that the result is true when $k = 3$ or 4 in Theorem 4.3.3.

Suppose that Δ be a k-subset of Ω where $|\Omega| = q+1$. Further suppose that $M = \{\Sigma | \Delta \subseteq \Sigma \subseteq \Omega \text{ and } |\Sigma| = k+1\}$, clearly $|M| = q+1-k$. We let Δ^G be a regular orbit and count the maximum number of elements in M with a non-trivial stabilizer subgroups. If this number is less than $q+1-k$, then there is no group G that satisfies Hypothesis$(*)$.

4.4.1 Orbit Lengths when $k = 5$

In this section we let $k = 5$ and $|\Omega| \geq 12$. Further suppose that Δ be a 5-subset of Ω such that $|G_\Delta| = 1$ and let Σ is a 6-subset containing Δ. In Theorem 4.4.10 we count the maximal number of 6-subsets Σ having non-trivial stabilizers.

Theorem 4.4.10 *Let* $G \cong PSL(2,q)$, *where* q *is even, act upon the projective line* Ω *of* $q+1$ *points. If* G *satisfies Hypothesis*$(*)$, *then* $G \cong PSL(2,16)$.

Proof We have already shown that $PSL(2,16)$ satisfies Hypothesis$(*)$ (see Section 4.3.2), so we need only to prove there are no other groups satisfying Hypothesis$(*)$ when $q > 16$.

Let $\Delta = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ be a 5-subset of Ω with a trivial stabilizer and let $\Sigma_i = \Delta \cup \{\beta_i\}$, where $\beta_i \in \Omega \setminus \Delta, 1 \leq i \leq q-4$ be a 6-subset of Ω. In this proof we aim to show that not all 6-sets Σ_i have a non-trivial stabilizer. The group G has no element of order 4, then only elements of order 1,2,3, or 5 can fix a subset of size 6.

Elements of order 2:

Since q is even, every element of order 2 fixes one point in Ω. From Lemma 4.3.2 (*iii*) every dihedral subgroup Dih(4) stabilizes $\frac{q}{4}$ subsets of size 4 and it also fixes one point in Ω, then Dih(4) stabilizes $\frac{q}{4}$ subsets of size 5.

Let $g \in G$ be an element of order 2 and $g \in G_{\Sigma_1}$. As $G_\Delta = 1$, then, without loss of generality, g must be of the form $g = (\alpha_1, \alpha_2)(\alpha_3, \alpha_4)(\alpha_5, \beta_1)(\beta_2, \beta_3)...$, $\beta_i \in \Omega \setminus \Delta$. From Lemma 4.3.1, g belongs to Dih(4), that stabilizes the 4-subset $\varepsilon_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and then there exist suitable β_i such that it also stabilizes $\varepsilon_2 = \{\alpha_5, \beta_1, \beta_2, \beta_3\}$. Hence, each involution in Dih(4) contains one of the 2-cycles (α_5, β_i), $i = 1, 2, 3$ and it follows that each involution fixes a 6-subset Σ_i, $i = 1, 2, 3$.

By replacing α_5 with α_i, $1 \leq i \leq 4$, thus we have at most 15 subsets Σ that are fixed by elements of order 2.

Elements of order 3:

Let $g \in G$ be an element of order 3 such that $g \in G_{\Sigma_1}$. From Lemma 4.4.3 (*ii*) $2||G_{\Sigma_1}|$. Therefore, the subsets Σ_i that are fixed by elements of order 3 are already counted with those fixed by elements of order 2.

Elements of order 5:

Elements of order 5 can stabilize a set of size 6 only if $5|(q-1)$; in this case each element of order 5 fixes 2 points in Ω. Suppose that $g \in G$ is an element of order 5 and $g \in G_{\Sigma_1}$, then, without loss of generality, g must be of the form $g = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_1)...(\alpha_5)(\gamma_1)$, where $\gamma_1 \in \Omega \setminus \Delta$. Using contradiction we will prove that if g_1 is an element of order 5 such that $\alpha_5 \in \text{fix}_\Omega(g_1)$ and $g_1 \in G_{\Sigma_2}$, where $\Sigma_2 = \Delta \cup \beta_2$, then $\Sigma_1 = \Sigma_2$. Clearly, $g \in G_{\Delta_1}$, where $\Delta_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_1\}$. From Lemma 4.4.7, $g \in \text{Dih}(10) \leqslant G_{\Delta_1}$, then G_{Δ_1} has an element of order 2, say h_1, fixes the 4-subset $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and $\beta_1 \in \text{fix}_\Omega(h_1)$ (as each involution in Dih(10) fixes one point in Δ_1).

Suppose that there exist an element of order 5 $g_1 \in G_{\Sigma_2}$, where $\Sigma_1 \neq \Sigma_2$, and let $\alpha_5 \in \mathrm{fix}_\Omega(g_1)$. Therefore, g_1 must contains a 5-cycle which fixes the 5-subset $\Delta_2 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_2\}$ and hence $g_1 \in \mathrm{Dih}(10) \leqslant G_{\Delta_2}$. Then G_{Δ_2} has an element h_2 of order 2 stabilizes the 4-subset $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and $\beta_2 \in \mathrm{fix}_\Omega(h_2)$.

Therefore, $h_1, h_2 \in \mathrm{Dih}(4) \leqslant G_{\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}}$. But every Dih(4) fixes only one point in Ω, then $\beta_1 = \beta_2$ which is impossible. Thus, if α_5 is a fixed point, then there is only one 6-subset containing Δ can be fixed by elements of order 5.

By replacing α_5 by α_i, $1 \leq i \leq 4$, we have at most 5 sets of size 6 containing Δ with stabilizers of order 5.

Therefore, we have at most 20 sets of size 6 containing Δ with non-trivial stabilizers. It follows that, some 6-subsets Σ_i have a trivial stabilizer and so Hypothesis($*$) it does not hold. $\diamond$

4.4.2 Orbit Length when $k = 6$

Let $G \cong PSL(2, q)$ acting on the projective line Ω, where $|\Omega| \geq 14$. In this section we let Δ be a 6-subset such that $|G_\Delta| = 1$ and Σ is 7-subset containing Δ.

The Next lemma is an immediate corollary of Lemmas 4.4.5 and 4.4.4.

Lemma 4.4.11 *Let $G \cong PSL(2, q)$, where q is even, acts upon a set Ω of $q+1$ points. Suppose that $|\Delta^G| = |G|$ where Δ is a subset of size 6, then only elements of order 1,2, or 3 can stabilize a set Σ of size 7 where $\Sigma \supset \Delta$.*

Proof Assume that $g \in G_\Sigma$, where Σ is a 7-subset of Ω, then $|g| = \{1, 2, 3, 5, 7\}$. Hence, the result follows from Lemma 4.4.5 and Lemma 4.4.4 (i),(ii). $\diamond$

Remark: In Section 4.3.2 we have already proved that there is no regular G-orbit for any subset of size 6 when $q = 16$.

Theorem 4.4.12 *Let $G \cong PSL(2, q)$, where q is even, acts upon a set Ω of $q + 1$ points. If $q > 16$, then there is no group G that satisfies Hypothesis($*$).*

Proof Let $\Delta = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$ be a 6-subset of Ω with a trivial stabilizer and let $\Sigma_i = \Delta \cup \{\beta_i\}$, where $\beta_i \in \Omega \setminus \Delta, 1 \leq i \leq q - 5$, be a 7-subset of Ω. In this proof we aim to show that not all 7-subsets Σ_i have non-trivial stabilizers. Let $g \in G$, then by Lemma 4.4.11 we know that $g \in G_{\Sigma_i}$ only when $|g| = \{1, 2, 3\}$.

Elements of order 2:

From our assumption that q is even, then every element of order 2 fixes one point in Ω. Let $g \in G$ be an element of order 2 and $g \in G_{\Sigma_1}$, then, without loss of generality, g must be of the form $g = (\alpha_1, \alpha_2)(\alpha_3, \alpha_4)(\alpha_5, \beta_1)(\beta_2, \beta_3)...(\alpha_6)$, $\beta_i \in \Omega \setminus \Delta$. Since g belongs to Dih(4), which stabilizes the 4-subsets $\varepsilon_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and $\varepsilon_2 = \{\alpha_5, \beta_1, \beta_2, \beta_3\}$, then each element of order 2 in Dih(4) fixes one 7-subset Σ_i, where $\Sigma_i = \Delta \cup \beta_i, 1 \leq i \leq 3$. Now replacing α_5 by any points α_i, where $1 \leq i \leq 4$, then we have an element $g_1 \in G_{\Sigma_4}$ of the form, without loss of generality, $g_1 = (\alpha_1, \alpha_5)(\alpha_3, \alpha_4)(\alpha_2, \beta_4)...(\alpha_6)$. Since $g, g_1 \in G_{\{\alpha_3,\alpha_4\}}$, it follows that $g \cdot g_1 \in G_{\alpha_3,\alpha_4}$. Therefore $|\text{fix}(g \cdot g_1)| \geq 3$ and that is a contradiction by Lemma 4.4.6.

By replacing α_6 with α_i, $1 \leq i \leq 5$, clearly we have at most 18 sets Σ_i that are fixed by elements of order 2.

Elements of order 3:

Elements of order 3 can stabilize a subset of size 7 only if $3|(q-1)$; in this case, $q \geq 64$ and each element of order 3 fixes 2 points in Ω. Suppose that $q \geq 64$ and let $g \in G_{\Sigma_1}$ be an element of order 3. Clearly, an elements of order 3 fixes a 7-subset Σ only if Σ is the union of points of two 3-cycles and one fixed points. As $G_\Delta = 1$, then, without loss of generality, g must be of the form

$$g = (\alpha_1, \alpha_2, \alpha_3)(\alpha_4, \alpha_5, \beta_1)...(\alpha_6)(\gamma),\ \ \beta_1, \gamma \in \Omega \setminus \Delta.$$

Due to the fact that G is a 3-transitive, then the stabilizer for any 3-subset of Ω is of order 6. Hence, there is a unique cyclic subgroup of order 3, say H, such that $H < G_{\{\alpha_1,\alpha_2,\alpha_3\}}$. It follows that H fixes at most one subset of size 7 containing Δ.

Since Δ contains $\binom{6}{3} = 20$ subsets of size 3 and each of them is fixed by only one cyclic subgroup of order 3, there are at most 20 subsets of size 7 containing Δ with $3||G_\Sigma|$.

Therefore, if $q \geq 64$, we have at most 38 sets of size 7 containing Δ with non-trivial stabilizer subgroups. This means there are some 7-subsets containing Δ having a trivial stabilizer. Hence, the result holds. $\diamond$

4.4.3 Orbit Length when $k = 7$

In this section we discuss the Hypothesis($*$) when $k = 7$ and $|\Omega| \geq 16$. Theorem 4.4.13 is the main result in this case.

Theorem 4.4.13 *Let $G \cong PSL(2, q)$, where q is even, act upon the projective line Ω of $q + 1$ points. If $q \geq 16$, then there is no group G that satisfies Hypothesis($*$).*

The proof of this theorem will be separated into two cases; the first one when $q > 16$ and the second when $q = 16$. Before we get start our proof, we need to make some preparations.

Remark: We have already counted the number and lengths of orbits of $PSL(2, 16)$ in its action on Ω_6 in Section 4.3.2 and they are as follows:

Table 4.5: Number and length of orbits of $PSL(2, 16)$ in its action on Ω_6

Length of orbits	Number of orbits
$\frac{\lvert G\rvert}{6}$	2
$\frac{\lvert G\rvert}{5}$	1
$\frac{\lvert G\rvert}{2}$	5

Lemma 4.4.14 *Let G be a permutation group $PSL(2, 16)$ of degree 17 on Ω. Let Δ be a 7-subset of Ω such that $|\Delta^G| = |G|$.*

(i) If Γ be any 5-subset of Δ, then $5 \nmid |G_\Gamma|$.

(ii) If $\Delta_1 \neq \Delta_2$ be any two 6-subsets of Δ, then $\Delta_1^G \neq \Delta_2^G$. Moreover, $|G_{\Delta_i}| = 2$ or 6, $1 \leq i \leq 7$.

Proof Suppose that $\Delta = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7\}$ is a subset of Ω of size 7 and $|G_\Delta| = 1$.

(i) Suppose that Γ be a subset of size 5 of Δ, there are $\binom{12}{2} = 66$ subsets of Ω of size 7 containing Γ. We claim that if $5 \| G_\Gamma|$, then all 7-subsets containing Γ have non-trivial stabilizers. To see that, suppose that there exist an element g of order 5 such that $g \in G_\Gamma$. From Lemma 4.4.2 (iii) $60 \| G_\Gamma|$ and then $G_\Gamma \cong PSL(2, 4)$ as $PSL(2, 4)$ is a maximal in G. The subgroup $PSL(2, 4)$ contains 15 elements of order 2, each of them fixes 6 different 7-subsets containing Γ (as Γ is the union of points of two 2-cycles and one fixed point). Let $A = \{(\Sigma, g) | |g| = 2, \Gamma \subseteq \Sigma \subseteq \Omega,\ g \in G_\Sigma \text{ and } |\Sigma| = 7\} = 15 \times 6 = 90$. However, G_Γ contains 6 Dih(10) subgroups each of them fixes a 7-subset containing Γ. Then the number of duplicate 7-subsets that are fixed by elements of order 2 in Dih(10) is $6 \times 5 = 30$ subsets.

Thus, the number of 7-subsets containing Γ with stabilizer isomorphic to C_2 is 60 and the number of 7-subsets containing Γ with stabilizer isomorphic to Dih(10) is 6. Therefore, all 7-subsets containing Γ have non-trivial stabilizer. Hence, $|G_\Delta| \neq 1$ and this is impossible.

(ii) Let $\Delta_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$ and $\Delta_2 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_7\}$ be 6-subsets of Δ such that ${\Delta_1}^G = {\Delta_2}^G$ and $\Delta_1 \neq \Delta_2$. Then there exists an element $g \in G$ such that g maps Δ_1 to Δ_2. Since $\alpha_6 \notin \Delta_2$, g cannot map points of the set $\Gamma = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ to α_6, $\alpha_6 \notin \text{fix}(g)$, and cannot map α_6 to any points out of Δ_2.

Let g is of order 2, then g contains the 2-cycle (α_6, α_7) and maps Γ to itself. Hence, $g \in G_\Delta$ which is a contradiction.

Suppose that g is of order 5, then g has the form $g = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)(\alpha_6, \alpha_7, ...)....$ Then $g \in G_\Gamma$ which is impossible from *(i)*.

Let g of order 3, then g has the form $g = (\alpha_1, \alpha_2, \alpha_3)(\alpha_6, \alpha_7, \beta)...(\alpha_4)(\alpha_5)$, $\beta \in \Omega \backslash \Delta$. Clearly, $g \in G_\Gamma$, however by Lemma 4.4.2 *(ii)* $5 | |G_\Gamma|$. A contradiction by *(i)*.

Suppose that g is of order 15, then g has the form $g = (..., \alpha_6, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_7, ...)$. Since $g \in C_{15} \leqslant \text{Dih}(30)$, then there exist an element of order 2, say h, in Dih(30) of the form $h = (\alpha_1, \alpha_5)(\alpha_2, \alpha_4)(\alpha_6, \alpha_7)...(\alpha_3)$, (as $g, h \in \text{Dih}(30)$ we can see that $g^h = hgh^{-1} = (..., \alpha_7, \alpha_5, \alpha_4, \alpha_3, \alpha_2, \alpha_1, \alpha_6, ...) = g^{-1}$). Therefore, $h \in G_\Delta$ which is a contradiction. For a similar reason g cannot be of order 17.

Therefore, from the above arguments we deduce that if $\Delta_1 \neq \Delta_2$, then $\Delta_1^G \neq \Delta_2^G$.

Finally, let $5 | |G_{\Delta_i}|$, then there exist an element of order 5, $g \in G_{\Delta_i}$ of the form $g = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)...(\alpha_6)(\beta)$, $\beta \in \Omega \setminus \Delta$. Then $g \in G_\Gamma$ which is impossible from *(i)*. Hence, from Lemma 4.4.3 and Table 4.5 $|G_{\Delta_i}| = 2$ or 6. $\diamond$

Lemma 4.4.15 *Let G be a permutation group $PSL(2, 16)$ acting upon a set Ω of size 17. Then the number and length of orbits of G in its action on Ω_8 are given in the following table:*

Table 4.6: Number and length of orbits of $PSL(2,16)$ in its action on Ω_8

Length of orbits	Number of orbits
$\frac{\lvert G\rvert}{8}$	1
$\frac{\lvert G\rvert}{6}$	2
$\frac{\lvert G\rvert}{2}$	5
$\lvert G\rvert$	3

Proof Suppose that G acts upon the set Ω_8 where $|\Omega_8| = 24310$. We can count the number of G-orbits when $k = 8$ by Theorem 4.2.7 as follows

(i) $\eta_8(1^{17}) = \binom{17}{8} = 24310$;

(ii) $\eta_8(1^1 \cdot 2^8) = \binom{1}{0}\binom{8}{4} = 70$;

(iii) $\eta_8(1^2 \cdot 3^5) = \binom{2}{2}\binom{5}{2} = 10$;

(iv) $\eta_8(1^2 \cdot 5^3) = 0$;

(v) $\eta_8(17^1) = 0$.

Therefore,

$$\sigma_8(G,\Omega) = \frac{1}{16 \times 17 \times 15} \times 24310 + \frac{1}{16} \times 70 + \frac{1}{2 \times 17} \times 0 + \frac{1}{2 \times 15}(2 \times 10 + 4 \times 0) = 11$$

From the cycle structure of elements in $PSL(2,16)$ in Table 4.4, only elements of order 2 and 3 can stabilize a set of size 8. Let Σ be a set of size 8, then we can determine the orbit lengths of G as follows.

Elements of order 3:

Let $\Sigma = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\, \alpha_7, \alpha_8\}$ be 8-subset of Ω and let $g \in G_\Sigma$ be an element of order 3. Then, without loss of generality, g has the form

$$g = (\alpha_1, \alpha_2, \alpha_3)(\alpha_4, \alpha_5, \alpha_6)...(\alpha_7)(\alpha_8).$$

From Lemma 4.4.3 $(ii), (iv)$ $g \in \mathrm{Dih}(6) \cong G_\Gamma$, where $\Gamma = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$. Since elements of order 2 in Dih(6) interchange $\{\alpha_7, \alpha_8\}$, then $\mathrm{Dih}(6) \cong G_\Sigma$. Using formulae (4.1) Dih(6) fixes two subsets of size 8. From Lemma 4.2.2 (vii) G contains 680 dihedral subgroups, then the number of 8-subsets which are fixed by these groups is

$2 \times 680 = 1360$. Hence, G has two orbits each of size $\frac{|G|}{6}$.

Elements of order 2:

Each elements of order 2 fixes $\binom{8}{4} = 70$ subsets of size 8. We may assume that $A = \{(g, \Sigma) | g \in G_\Sigma, |g| = 2\}$ where Σ is 8-subsets. By Lemma 4.2.2 $(viii)$ G has 255 elements of order 2, then $|A| = 17850$. To avoid double counting we have to count the number of fixed 8-subsets by elementary abelian 2-subgroups of G. Suppose that P is an elementary abelian subgroup of G of order $2^m, m \leq n$. By Burnside's Lemma, the number of orbits of each of these subgroups is $\frac{2^n+1+2^m-1}{2^m} = 2^{n-m} + 1$. Clearly, one of these orbits has size 1 and all other orbits are regular. By formulae (4.1) we can show that if $|P| = 16$, then P cannot stabilize any set of size 8, if $|P| = 8$, then P fixes 2 subsets of size 8, and if $|P| = 4$, then P fixes 6 subsets of size 8. As G contains 255 elementary abelian subgroup of order 8 (Lemma 4.2.2 (iv)) each of them fixes 2 subsets of size 8, then G has one orbit of size $255 \times 2 = 510 = \frac{|G|}{8}$ on 8-subsets. Let $B = \{(g, \Sigma) || g| = 2, g \in G_\Sigma$ and $g \in P \vee g \in D_6\} \subseteq A$, clearly from the above calculations $|B| = 7 \times \frac{|G|}{8} + 2 \times 3 \times \frac{|G|}{6} = 7650$. Now the number of 8-subsets which are fixed by cyclic subgroups of order 2 is equal to $|A| - 7650 = 10200$. Then there are 5 orbits of size $\frac{|G|}{2}$.

From the above argument we count the number of all 8-subsets which are fixed by elements of order 2 and 3. Then the possible size for the last 3 orbits is $|G|$.$\diamond$

Now we are on the position to prove Theorem 4.4.13.

Proof of Theorem 4.4.13

We may take $\Delta = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7\}$ be a 7-subset of Ω with a trivial stabilizer and let $\Sigma_i = \Delta \cup \{\beta_i\}$, where $\beta_i \in \Omega \setminus \Delta, 1 \leq i \leq q-6$, be an 8-subsets. We aim to count the maximum number of all 8-subsets Σ_i with non-trivial stabilizers.

Case1: $q > 16$

Let $g \in G$, then $g \in G_{\Sigma_1}$ only when $|g| = \{1, 2, 3, 7\}$.

Elements of order 2:

Let $g \in G$ be an element of order 2 and $g \in G_{\Sigma_1}$, then, without loss of generality, g has the form

$$g = (\alpha_1, \alpha_2)(\alpha_3, \alpha_4)(\alpha_5, \alpha_6)(\alpha_7, \beta_1)...(\gamma),\ \gamma \in \Omega \setminus \Delta.$$

Suppose that $\Gamma = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$ be a 6-subset of Δ. Since $g \in G_\Gamma$, then $2||G_\Gamma|$ and by Lemma 4.4.3, we can see that $|G_\Gamma| = 2$ or 6. This leads us to two cases:

Case (a): $|G_\Gamma| = 2$

In this case there is only one cyclic subgroup C_2 can stabilize the set Γ, then C_2 also stabilizes the 8-subset Σ_1. By replacing α_7 with α_i, $1 \leq i \leq 6$, there are at most 7 subsets Σ with $2||G_\Sigma|$.

Case (b): $|G_\Gamma| = 6$

Suppose that $g \in G_\Gamma \cong \mathrm{Dih}(6)$ is an element of order 2. Elements of order 2 in Dih(6) fix the set Γ and interchange α_7 with β_i, where $\beta_i \in \Omega \setminus \Delta, 1 \leq i \leq 3$. Then G_Γ contains three involution each of them fixes one 8-subset Σ_i. Now by replacing α_7 with α_i, $1 \leq i \leq 6$, then the maximum number of all subsets Σ_i with $2||G_\Sigma|$ is less than or equal to 21.

Elements of order 3:

Elements of order 3 can stabilize a set of size 8 only if $3|(q-1)$; in this case, each element of order 3 fixes 2 points in Ω and $q \geq 64$. Suppose that $3||G_{\Sigma_1}|$, then there exists an element $g \in G_{\Sigma_1}$ such that $|g| = 3$. Let $(\alpha_1, \alpha_2, \alpha_3)$ and $(\alpha_4, \alpha_5, \beta_1)$ be 3-cycles of g and $\{\alpha_6, \alpha_7\} \in \mathrm{fix}_\Omega(g)$. We may take $\Gamma = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \beta_1\}$ as a set of size 6, since $g \in G_\Gamma$, then by Lemma 4.4.3 (iv) $G_\Gamma \cong \mathrm{Dih}(6)$. As elements of order 2 in G_Γ interchange $\{\alpha_6, \alpha_7\}$, then they fix also the subset Σ_1. Therefore, if $3||G_{\Sigma_1}|$, then $2||G_{\Sigma_1}|$. Hence, 8-subsets Σ_i which are fixed by elements of order 3 are already counted with those fixed by elements of order 2.

Elements of order 7:

Elements of order 7 can stabilize a set of size 8 only if $7|(q-1)$; in this case, each element of order 7 fixes 2 points in Ω and $q \geq 64$. Let G be an element of order 7 and $g \in G_{\Sigma_1}$. As $G_\Delta = 1$, then, without loss of generality, g has the form

$$g = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \beta_1)...(\alpha_7)(\beta_2), \ \beta_1, \beta_2 \in \Omega \setminus \Delta.$$

Let $\Gamma = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \beta_1\}$ be a set of size 7, then $g \in G_\Gamma$. By Lemma 4.4.4 (i) we have $2||G_\Gamma|$ and then $g \in \mathrm{Dih}(14) \leqslant G_\Gamma$. As elements of order 2 interchange α_7 and β_2, then there exists an element of order 2, say h, of the form $h = (\alpha_1, \alpha_6)(\alpha_2, \alpha_5)(\alpha_3, \alpha_4)(\alpha_7, \beta_2)...(\beta_1)$, then h stabilizes the set Σ_2. Therefore, if

$7||G_{\Sigma_1}|$, then there is an element of order 2 fixes a subset of size 8 Σ_2, where $\Sigma_1 \neq \Sigma_2$. As a result, the number of 8-subsets Σ with $7||G_\Sigma|$ is less than or equal to the number of 8-subsets Σ with $2||G_\Sigma|$.

From the above argument we deduce that the maximum number of 8-subsets Σ with a non-trivial stabilizers is 42. Therefore, there are 8-subsets containing Δ have a trivial stabilizer and so G does not satisfy Hypothesis(∗).

Case2: $q = 16$

Suppose that $|\Delta^G| = |G|$ where $\Delta = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7\}$ is a 7-subset of Ω and let $\Sigma_i = \Delta \cup \{\beta_i\}$, where $\beta_i \in \Omega \setminus \Delta, 1 \leq i \leq 10$. Suppose that $G_{\Sigma_1} \neq 1$, then by Lemma 4.4.15, $2||G_{\Sigma_1}|$. Let $1 \neq g \in G_{\Sigma_1}$ be an element of order 2, then, without loss of generality, g must be of the form:

$$g = (\alpha_1, \alpha_2)(\alpha_3, \alpha_4)(\alpha_5, \alpha_6)(\alpha_7, \beta_1)....$$

Thus, g fixes also a 6-subset of Δ. Therefore, by looking at the stabilizers of 6-subsets of Δ we can count the number of 8-subsets containing Δ with non-trivial stabilizers. Let Δ_i be a 6-subset of Δ, where $1 \leq i \leq 7$. Clearly, by Lemma 4.4.14 and Table 4.5, as $G_\Delta = 1$, then Δ contains 7 subsets of size 6; two of them have stabilizers isomorphic to Dih(6) and all other subsets have stabilizers isomorphic to C_2.

Assume that Δ_1 and Δ_2 be 6-subsets of Δ such that $\Delta_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$ and $\Delta_2 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_7\}$ with $|G_{\Delta_i}| = 6$, $i = 1, 2$. As $G_{\Delta_1} \cong \mathrm{Dih}(6)$, then without loss of generality we may take $G_{\Delta_1} = \langle g_1, h_1\rangle$ such that $g_1 = (\alpha_1, \alpha_2, \alpha_3)(\alpha_4, \alpha_5, \alpha_6)....$ Therefore, G_{Δ_1} contains the following elements of order 2:

$$h_1 = (\alpha_1, \alpha_4)(\alpha_2, \alpha_6)(\alpha_3, \alpha_5)(\alpha_7, \beta_1)...(\gamma_1);$$

$$h_2 = (\alpha_1, \alpha_6)(\alpha_2, \alpha_5)(\alpha_3, \alpha_4)(\alpha_7, \beta_2)...(\gamma_2);$$

$$h_3 = (\alpha_1, \alpha_5)(\alpha_2, \alpha_4)(\alpha_3, \alpha_6)(\alpha_7, \beta_3)...(\gamma_3).$$

Since $\Delta_1 \cap \Delta_2 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$, there are 5 subsets of size 4 of $\Delta_1 \cap \Delta_2$ and by Lemma 4.3.1 each of them is fixed by only one Dih(4). Note that any 4-subsets of Ω cannot be fixed by Dih(6) (because, if elements of order 3 in Dih(6) fix a 4-subset Γ of Ω, then Γ is the union of the points of a 3-cycle and one fixed point, however, elements of order 2 interchange the two fixed points). It follows that the three involution in

G_{Δ_1} fix three different 4-subsets of $\Delta_1 \cap \Delta_2$, and the same argument applies for the involution in G_{Δ_2}. Therefore, there is at least one 4-subset of $\Delta_1 \cap \Delta_2$ fixed by an involution of G_{Δ_1} and also by an involution of G_{Δ_2}. Let $h_1 \in G_{\Delta_1}$ and $y_1 \in G_{\Delta_2}$ fix the same 4-subset, say $\{\alpha_1, \alpha_3, \alpha_4, \alpha_5\}$. As h_1 possesses the 2-cycle (α_2, α_6) and y_1 must contain the 2-cycle (α_2, α_7), then h_1 and y_1 fix also the 4-subset $\{\alpha_2, \alpha_6, \alpha_7, \beta_1\}$. As h_1 and y_1 commute, then by Lemma 4.4.15 $h_1, y_1 \in P \cong G_{\Sigma_1}$, where P is an elementary abelian subgroup of order 8.

Now, if Δ_i is a 6-subset of Δ and $|G_{\Delta_i}| = 2$, then all involution which stabilize these subsets are contained in P. Consequently, there are at most two involution in G_{Δ_1} or two involution in G_{Δ_2} that can fix 8-subsets containing Δ. Hence, if Δ has a trivial stabilizer, then there are at most 5 subsets of size 8 containing Δ with non-trivial stabilizers. It follows that, there are 8-subsets with trivial stabilizer, and so Hypothesis($*$) does not hold. $\diamond$

Chapter 5

Counting G-Orbits of some primitive permutation groups of small degree

This chapter is devoted to investigating the G-orbits of some finite primitive groups and their action on Ω_k. In particular, we concentrate our effort on exploring the relationship between the G-orbits on Ω_k and Ω_{k+1} for $1 \leq k \leq \frac{n}{2}$. We will consider the group action on Ω_k for 13 primitive groups,

- $PSL(2,7)$ on its action on 7 points;
- $PSL(2,7)$ on its natural action on 8 points;
- Alt(6) on its action on 10 points;
- $PSL(2,11)$ on its action on 11 points;
- $PSL(2,11)$ on its natural action on 12 points;
- M_{11} on its natural action on 11 points;
- M_{11} on its action on 12 points;
- M_{12} on its natural action on 12 points;
- Alt(5) on its action on 10 points;
- Alt(7) on its action on 15 points;

- $PSL(2,13)$ on its natural action on 14 points;
- Alt(6) on its action on 15 points;
- $ASL(2,4)$ on its natural action on 16 points.

The results of our calculations will be represented in diagrams except the group Alt(6) in its action on 15 points and $ASL(2,4)$ in its natural action on 16 points. These two groups will be represented in a different way which will be illustrated later.

Let G be a primitive group and H be a maximal subgroup of G. One can obtain a permutation action of G on the right cosets of H, where $[G:H]=n$, by numbering these cosets from 1 to n. In order to construct this permutation representation we will use the following Magma code:

```
CosetImage(G,H);
```

In this chapter we study some primitive groups in their natural representation or in their action on the cosets of a maximal subgroup.

5.1 Number and length of G-orbits of some finite primitive groups

In this section we consider the action of G on Ω_k of size $\binom{n}{k}$ where $1 \le k \le \frac{n}{2}$. Suppose that G has m orbits in its action on Ω_k, each of these orbits is denoted by Ω_k^i, for $1 \le i \le m$. Let Δ be a k-subset of Ω with $\Delta \in \Omega_k^i$. Then there are $n-k$ subsets Σ of size $k+1$ such that $\Sigma = \Delta \cup \{\alpha\}$ where $\alpha \in \Omega \setminus \Delta$. Let a_k^j be the number of sets Σ which belong to the G-orbit Ω_{k+1}^j, where $1 \le j \le s$ and s is the number of G-orbits on Ω_{k+1}. Indeed we have that

$$\sum_j a_k^j = n-k.$$

Now suppose that Σ be a subset of Ω of size $k+1$ such that $\Sigma \in \Omega_{k+1}^j$. Then there are $k+1$ subsets Δ of Σ each of size k. The number of subsets Δ which belong to the G-orbit Ω_k^i is denoted by b_{k+1}^i and clearly we have that

$$\sum_i b_{k+1}^i = k+1.$$

The relation between a_k^j and b_{k+1}^i is given by

$$|\Omega_k^i|a_k^j = |\Omega_{k+1}^j|b_{k+1}^i. \tag{5.1}$$

The following corollary is an immediate result of equation (5.1).

Corollary 5.1.1 *Let G be a permutation group acting upon a set Ω of size n. Suppose that Δ is a k-subset of Ω and Σ is $(k+1)$-subsets of Ω containing Δ. Further suppose that $s = |\{\beta \in \Omega | \Delta \cup \beta \in \Sigma^G\}|$ and $r = |\{\alpha \in \Sigma | \Sigma \setminus \alpha \in \Delta^G\}|$. Then*

$$\frac{|\Sigma^G|}{n-k} \leq |\Delta^G| \leq (k+1)|\Sigma^G|.$$

PROOF Since $1 \leq s \leq n-k$ and $1 \leq r \leq k+1$, hence the result follows from (5.1). ⋄

As we mentioned in Chapter 1 of this thesis, Mnukhin [26] in Theorem 1.0.4 was able to provide a bounding property for the maximal possible length of G-orbits on k-subsets. In Corollary 5.1.1 we obtain another lower bound for this case.

Example 5.1.2 Let $G \cong PGL(2, 25)$ acting upon the projective line $\Omega = PG(1, 25)$ of 26 points. Let Σ be a 5-subset of Ω and Σ^G is of the maximal length 19656. Then by Corollary 5.1.1 the minimum bound for any sub orbit length of Σ is 819. However, from Mnukhin's result Σ must contain a sub orbit longer than 234.

We are mostly interested in drawing diagrams for the G-orbits on Ω_k which help us to obtain much information about the number and lengths of these orbits. These diagrams are consisting of nodes representing the m G-orbits Ω_k^i joined by edges which are labelled with a_k^j and b_{k+1}^i. The numbers on upward arrows denote a_k^j and the numbers on downward arrows denote b_{k+1}^i.

As the amount of time to calculate the number and the length of G-orbits is too long, all our calculations are performed using MAGMA. Our method to accomplish these calculations is as follows. Let G be a primitive group of degree n and Ω be the set $\{1, 2, ..., n\}$. For $1 \leq k \leq \frac{n}{2}$, the set Ω_k can be easily determined by the MAGMA command `Subsets(Omega,k)`. The first step is to count the number of G-orbits on Ω_k.

- For $1 \leq k \leq \frac{n}{2}$, we can construct the action of the group G on the set Ω_k by using the command `GSet(G,Omega-k)`. Now it is not difficult to find the G-orbits on Ω_k by the command `Orbits`. From this step we can determine the number and lengths of all G-orbits on Ω_k for all k.

- For every A_i as a G-orbit in Ω_k, pick a random elements in A_i, say t, and let $Q = \Omega \setminus t$. Take $\Sigma = t \cup \{q\}$ for every $q \in Q$ and let B_i be a G-orbit on Ω_{k+1}. Next check whether or not Σ in B_i for all orbits B_i in Ω_{k+1}.

- Let $t \in A_i$ be as mentioned above. Let S be the set of all $(k-1)$-subsets of t and C_i be a G-orbit on Ω_{k-1}. Now for every $\Delta \in S$ we check whether or not $\Delta \in C_i$ for all G-orbits C_i.

5.1.1 $PSL(2, 7)$ of degree 7

Let G be the group $PSL(2, 7)$ in its action on the right cosets of a subgroup isomorphic to Sym(4). In this case, G acts upon a set Ω of 7 points and then we can construct the G-orbits on Ω_k for $k = 1, 2, 3$. The following diagram shows the number and lengths of G-orbits on Ω_k.

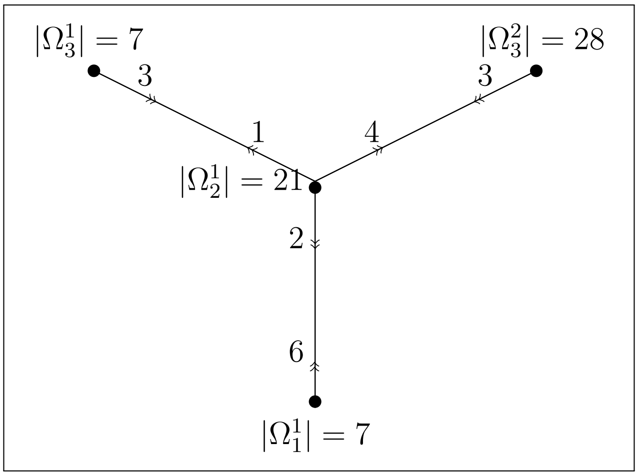

Figure 5.1: G-orbits of $PSL(2, 7)$ on its action on a set of 7 points

5.1.2 $PSL(2, 7)$ of degree 8

Let G is the 2-dimensional projective special linear group $PSL(2, 7)$ acting upon the projective line $\Omega = PG(1, 7)$ of 8 points. The number and length of G-orbits on Ω_k, where $1 \leq k \leq 4$, are given in Figure 5.2.

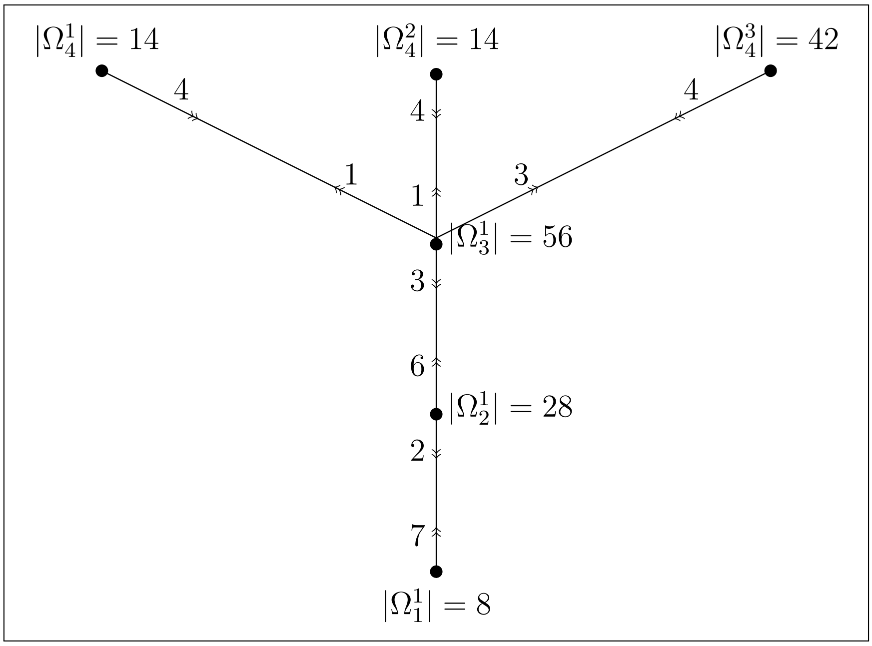

Figure 5.2: G-orbits of $PSL(2,7)$ on its action on a set of 8 points

5.1.3 Alt(6) of degree 10

Consider G is the group Alt(6) in its action on the right cosets of the maximal subgroup $H \cong 3^2 : 4$. As $[G : H] = 10$, then Ω is of size 10. Using Magma, we calculate the number and lengths of G-orbits under the action upon Ω_k, where $1 \leq k \leq 5$. The results of our calculations are presented in Figure 5.3.

Figure 5.3 shows that G satisfies the Siemons-Wagner property in Theorem 4.1.2. Take Δ to be a 4-subset in Ω_4^3; we can show that all 5-subsets containing Δ belong to G-orbits of a length less than the length of Ω_4^3.

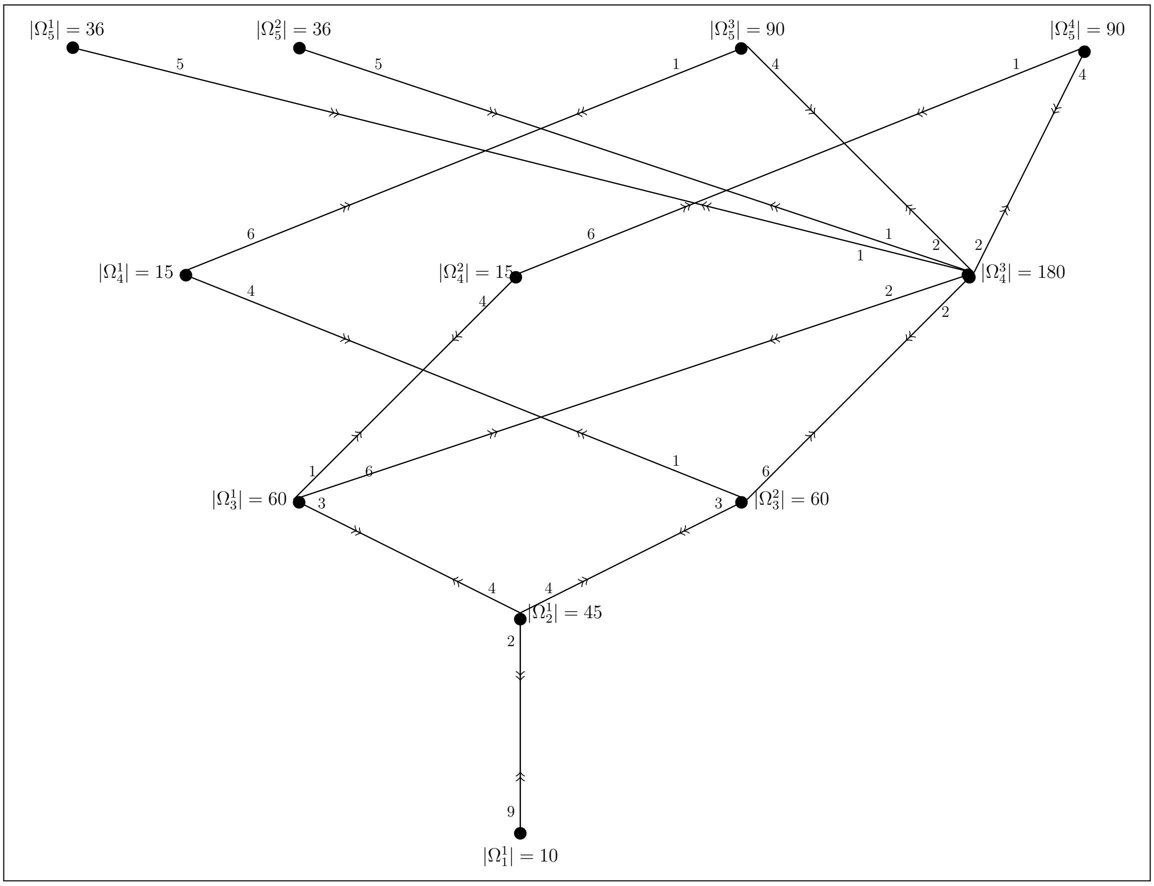

Figure 5.3: G-orbits of Alt(6) on its action on a set of 10 points

5.1.4 $PSL(2, 11)$ of degree 11

Let $G \cong PSL(2, 11)$ act on the right cosets of the maximal subgroup Alt(5). Since $[G : \text{Alt}(5)] = 11$, Ω has size 11. The number and lengths of G-orbits on Ω_k, $1 \leq k \leq 5$ are illustrated in Figure 5.4

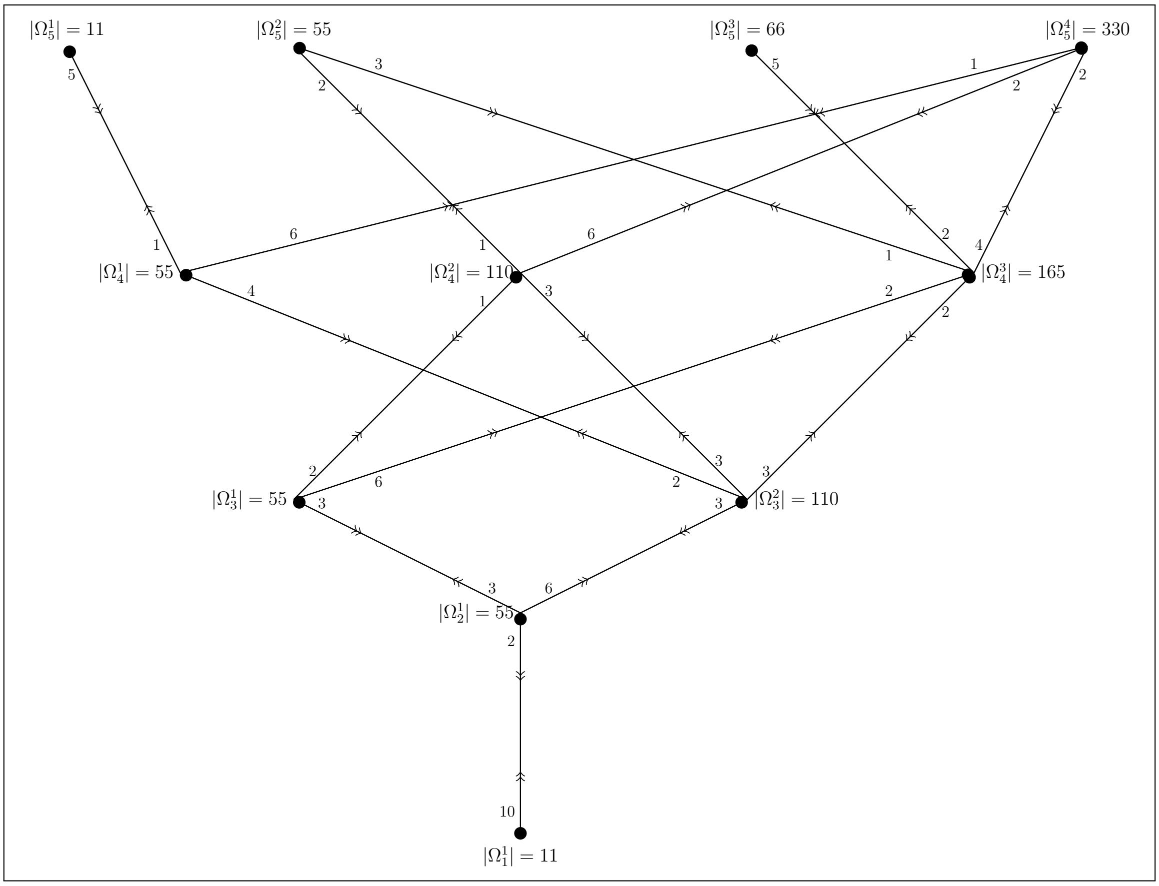

Figure 5.4: G-orbits of $PSL(2, 11)$ on its action on a set of 11 points

5.1.5 $PSL(2, 11)$ of degree 12

Let $G \cong PSL(2, 11)$ the 2-dimensional projective special linear group of order 660. This group acts upon the projective line $\Omega = PG(1, 11)$ of 12 points. The number and lengths of G-orbits of $PSL(2, 11)$ are illustrated in Figure 5.5.

Figure 5.5 shows that G satisfies the following properties:

- Group G satisfies Hypothesis($*$) in Chapter 4. Take Δ to be a 5-subset in Ω_5^2, where Ω_5^2 is a regular orbit. Clearly all G-orbits in Ω_6 have lengths less than the order of G. We discussed this case in considerable detail in Section 4.3.1.

- Group G satisfies the equality in the Livingstone-Wagner Theorem 2.3.7, as $\sigma_4(\Omega) = \sigma_5(\Omega) = 2$.

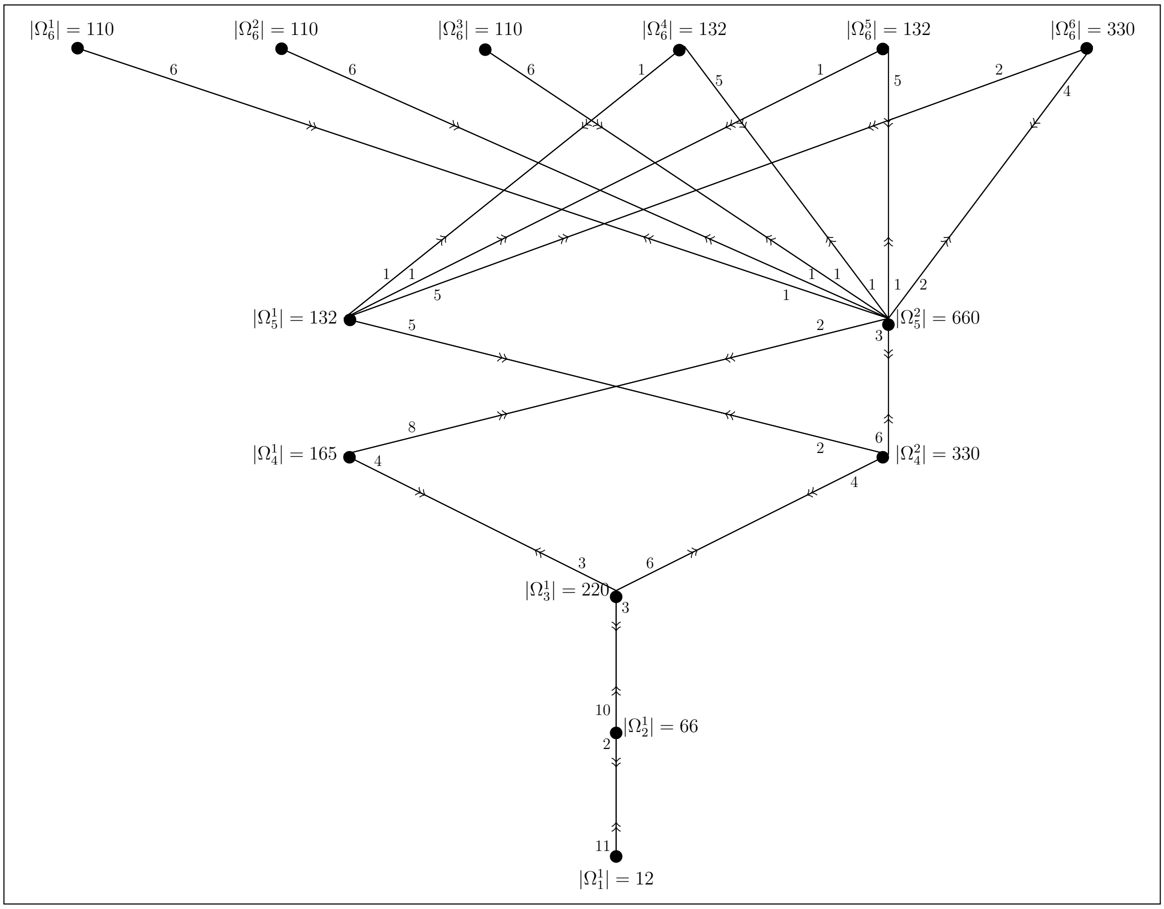

Figure 5.5: G-orbits of $PSL(2, 11)$ on its action on a set of 12 points

5.1.6 M_{11} of degree 11

Let G be the Mathieu group M_{11} in its 4-transitive action on a set Ω of 11 points. Figure 5.6 illustrate the number and length of G-orbits on Ω_k.

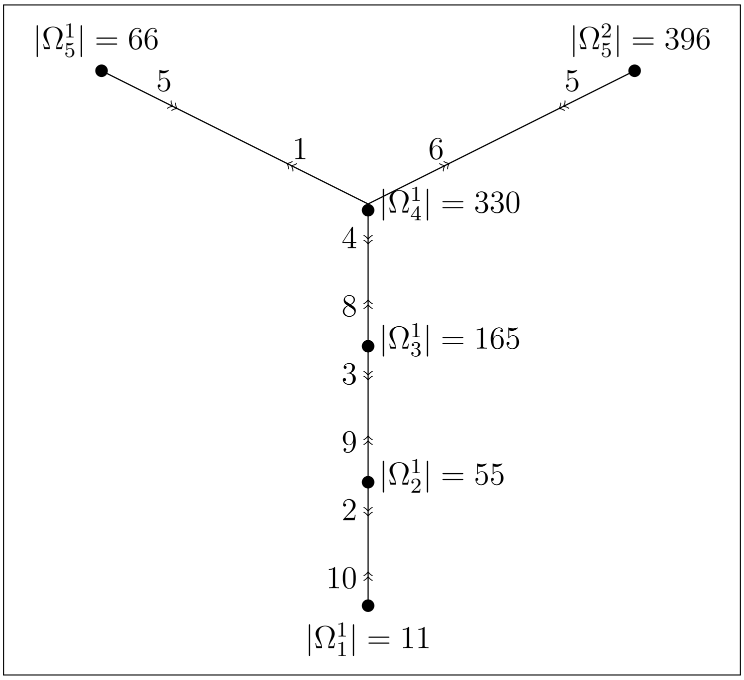

Figure 5.6: G-orbits of M_{11} on its action on a set of 11 points

5.1.7 M_{11} of degree 12

Consider G to be the group M_{11} in its action on the right cosets of a subgroup isomorphic with $PSL(2, 11)$. In this case, G acts upon a set Ω of size 12. The number and the lengths of G-orbits are given in Figure 5.7.

In Section 5.1.5 we saw that $PSL(2, 11)$ in its natural action on 12 points satisfies the equality of the Livingstone and Wagner Theorem 2.3.7 when $k = 4$. Since $PSL(2, 11)$ is a subgroup of M_{11}, from Lemma 2.3.13, $\sigma_4(M_{11}, \Omega) = \sigma_5(M_{11}, \Omega)$ and this is also obvious in Figure 5.7.

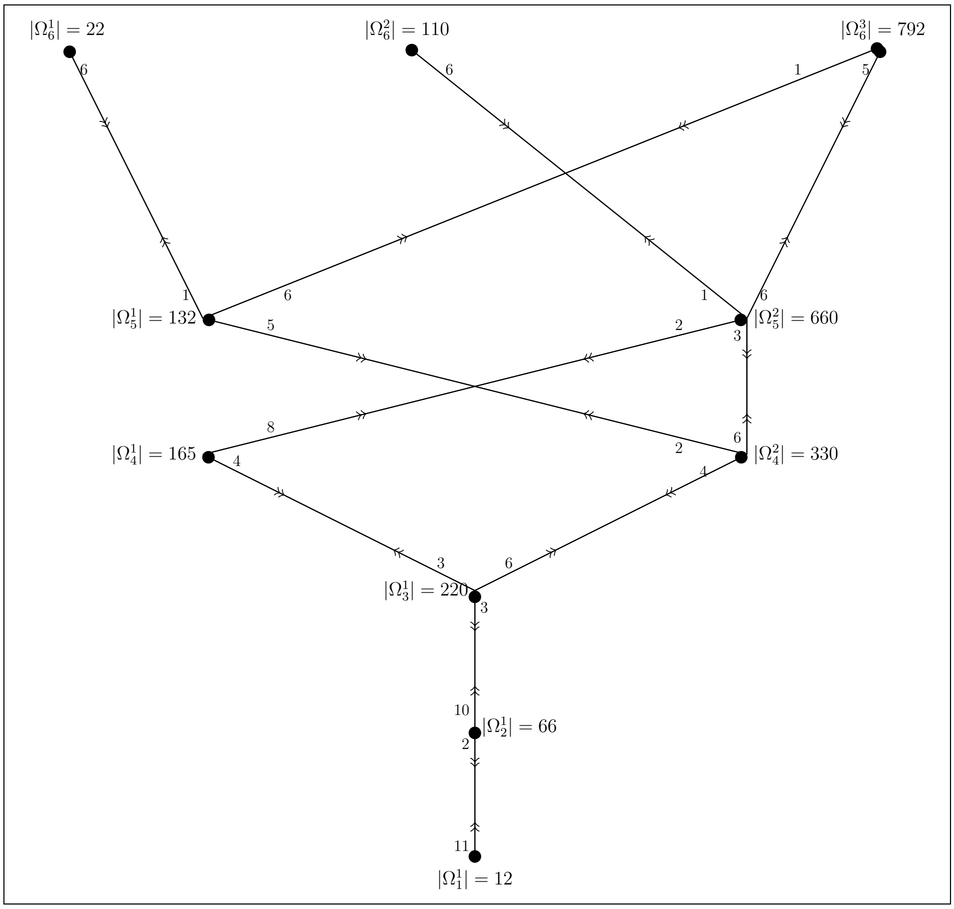

Figure 5.7: G-orbits of M_{11} on its action on a set of 12 points

5.1.8 M_{12} of degree 12

Consider G to be the Mathieu group M_{12} on its 5-transitive action on a set Ω of 12 points. The number and lengths of G-orbits in Ω_k, when $1 \leq k \leq 6$, are illustrated in Figure 5.8.

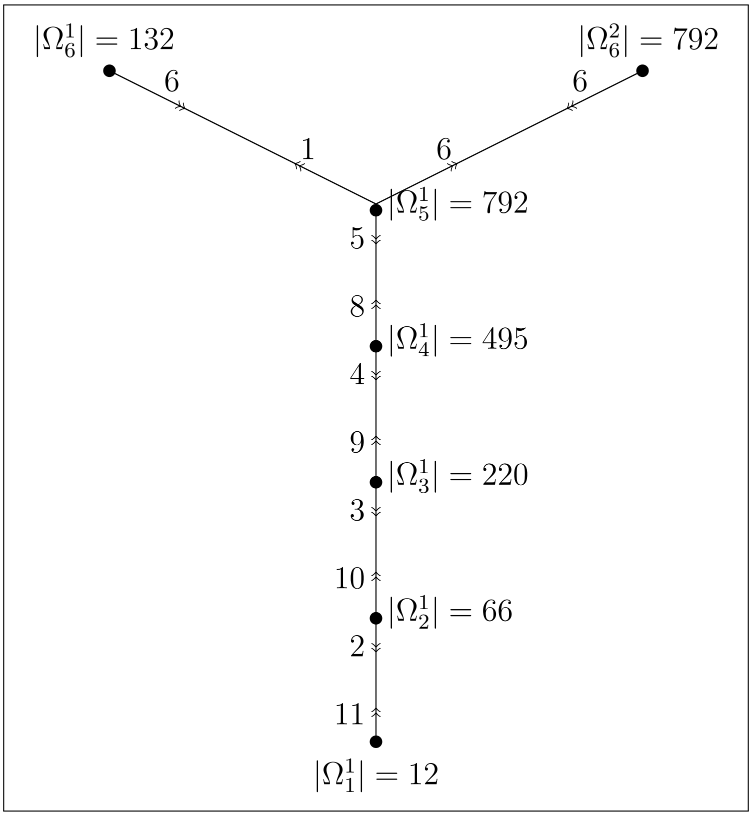

Figure 5.8: G-orbits of M_{12} on its action on a set of 12 points

5.1.9 **Alt**(5) **of degree** 10

Let G be the group Alt(5) in its action on the right cosets of a maximal subgroup isomorphic to Sym(3). In this case, G is a transitive group that acts on a set Ω of size 10.

Figure 5.9 shows the number and the length of G-orbits of Alt(5), where $1 \leq k \leq 5$.

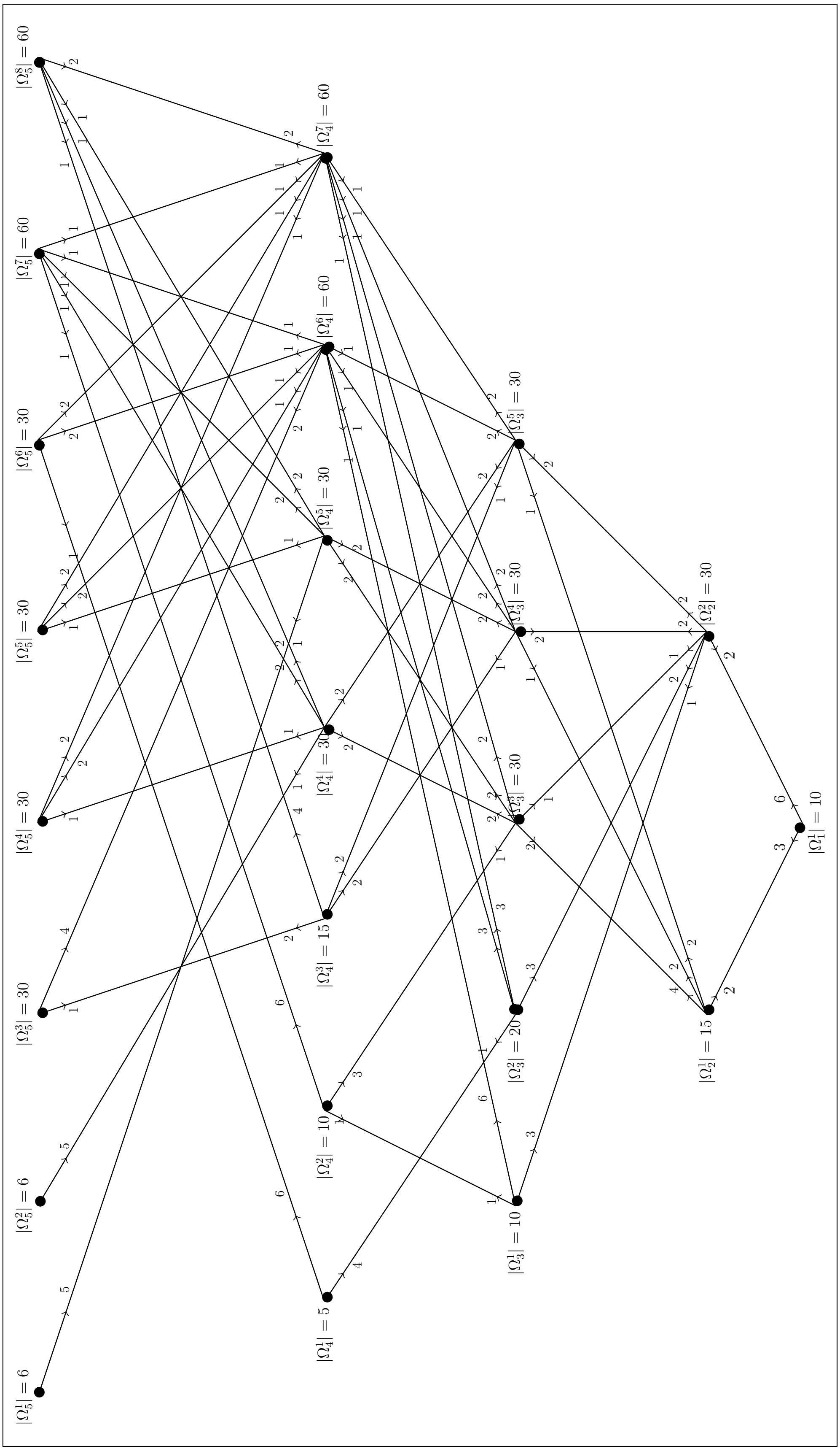

Figure 5.9: G-orbits of Alt(5) on its action on a set of 10 points

5.1.10 Alt(7) of degree 15

Let $G \cong \text{Alt}(7)$ the alternating group of order 2520. Suppose G acts upon the right cosets of its maximal subgroup $PSL(2,7)$ of index 15. Then Ω is of size 15.

Figure 5.10 shows that G satisfies Hypothesis($*$) in Chapter 4. Let Δ be a 6-subset in Ω_6^7. Clearly, $\Delta^G = \Omega_6^7$ is a regular orbit and all 7-subsets containing Δ belong to orbits of a length less than the order of G.

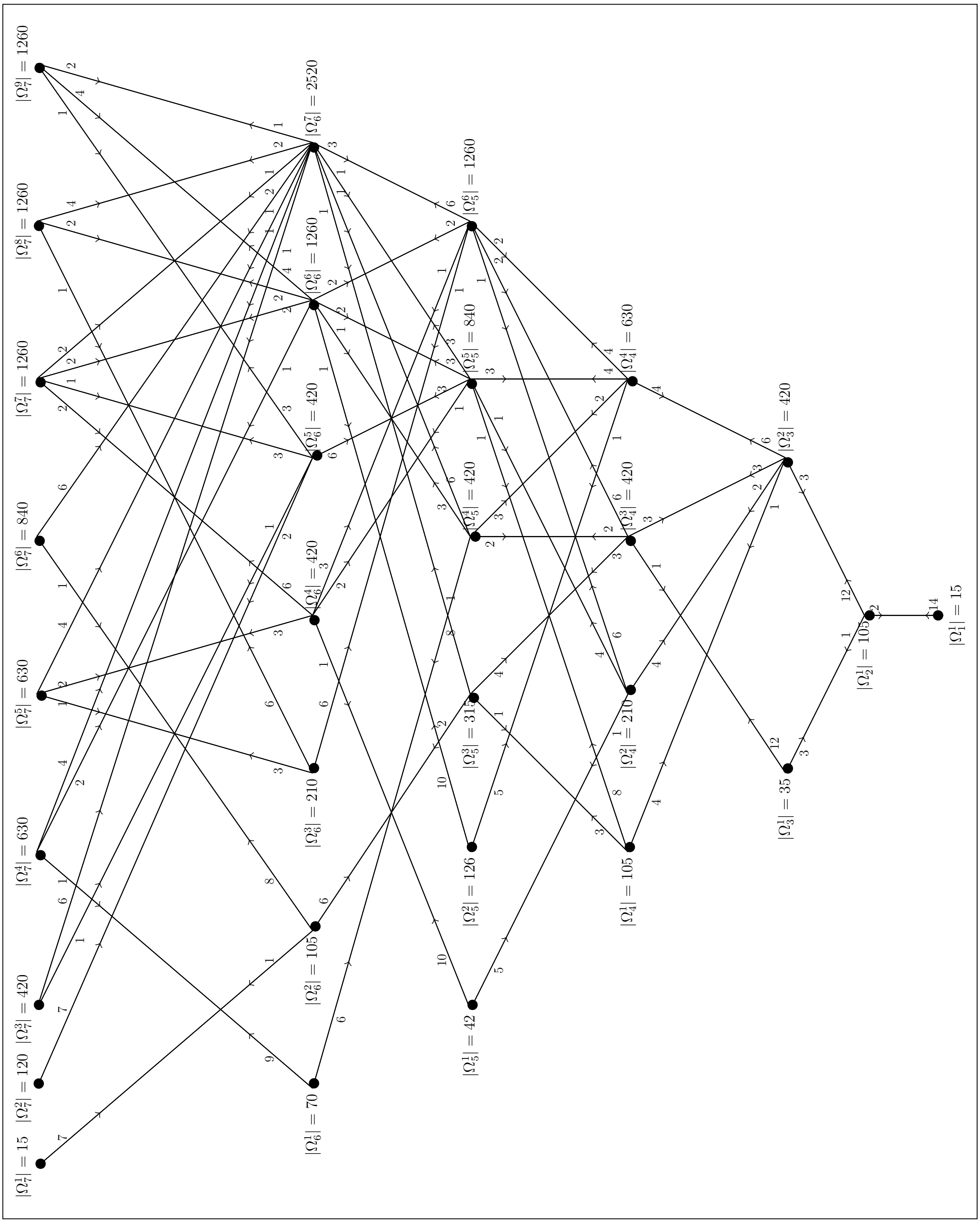

Figure 5.10: G-orbits of Alt(7) on its action on a set of 15 points

5.1.11 $PSL(2, 13)$ of degree 14

Let $G \cong PSL(2, 13)$ the 2-dimensional projetive special linear group acting upon the projective line $\Omega = PG(1, 13)$ of size 14. Group G is generated by two elements a and b, where a is of order 2, b of order 3, and ab of order 13.

The number and lengths of G-orbits in Ω_k, when $1 \leq k \leq 7$, are illustrated in Figure 5.11. In Figure 5.11, we show that G contains a regular orbit in its action upon Ω_6; however, all G-orbits in Ω_7 have a length less than the order G. Therefore, G satisfies Hypothesis($*$) in Chapter 4.

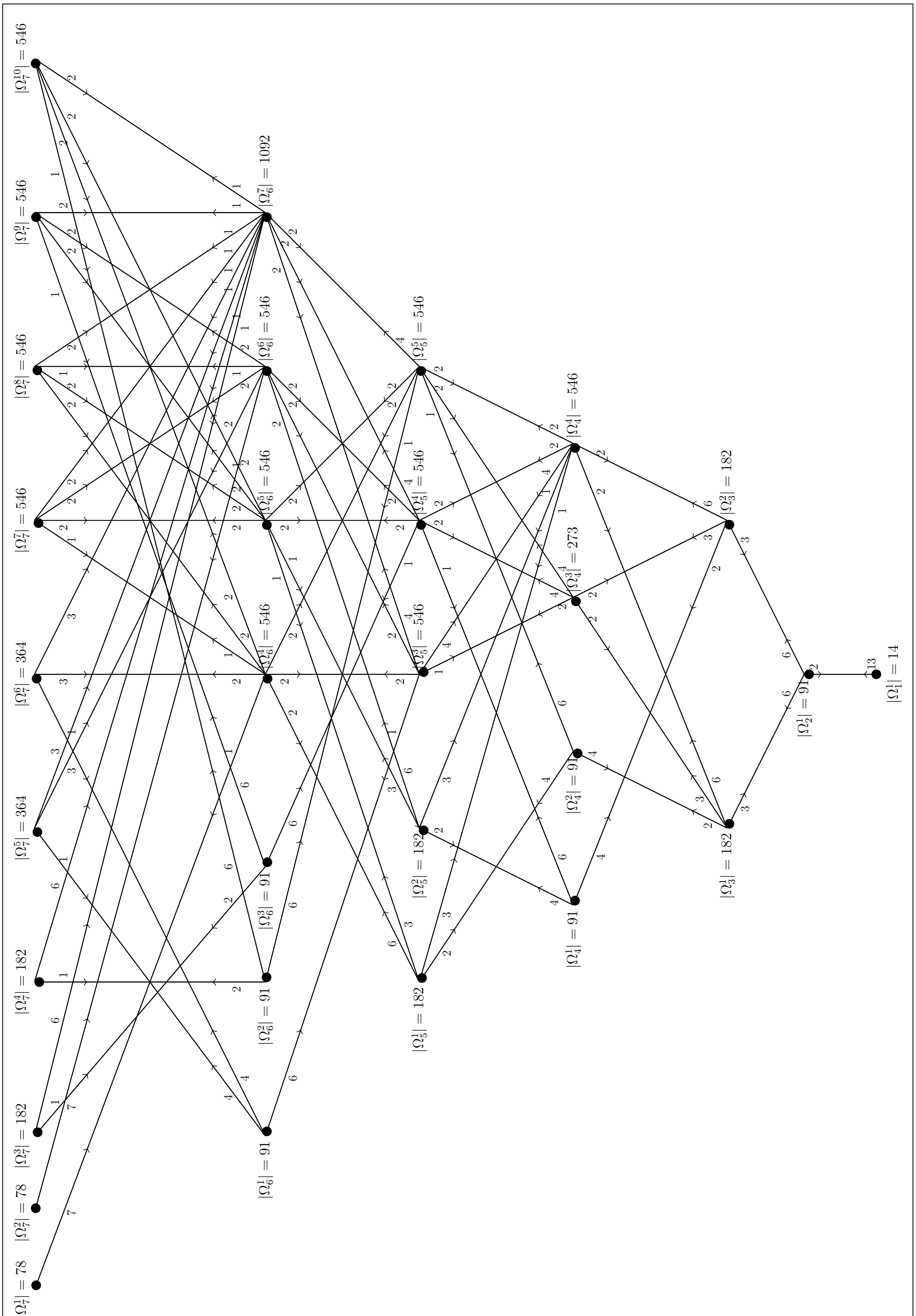

Figure 5.11: G-orbits of $PSL(2, 13)$ on its action on a set of 14 points

There are some groups where the number of G-orbits is too large to be presented by diagrams. In these cases, the number of nodes and the number of edges increase, and consequently, the diagrams will be extremely complicated. Therefore, we must use an alternative way to overcome this difficulty. In the rest of this chapter, we will use tables to present the results of our calculations. Before doing so, we must define the notation that will be used in these tables.

Let G act upon the set Ω_k and let $\Omega_k^1, \Omega_k^2, ..., \Omega_k^m$ be the G-orbits in Ω_k. Further suppose $\Sigma \in \Omega_k^i$, where Σ is a subset of Ω of size k, then

- c_i is the m-tuple $(|\Omega_k^1|, |\Omega_k^2|, ..., |\Omega_k^m|)$, each entry represents the length of G-orbit Ω_k^i, $1 \leq i \leq m$.

- u_i is the m-tuple $(A_1, A_2, ..., A_m)$ each entry A_i is a n-tuple $A_i = (n_1, n_2, ..., n_n)$, where n_i is the number of $(k+1)$-subsets containing Σ which locate in the orbit Ω_{k+1}^j for $1 \leq j \leq n$. Note that n is the number of G-orbits in Ω_{k+1}.

- d_i is the m-tuple $(B_1, B_2, ..., B_m)$ each entry B_i is the s-tuple $B_i = (s_1, s_2, ..., s_s)$, where s_i is the number of $(k-1)$-subsets of Σ which lie inside Ω_{k-1}^j. Note that s is the number of G-orbits in Ω_{k-1}

Indeed when $k = 1$, then d_1 is not counted. If $k = \frac{n}{2}$ (or $\frac{n}{2} - 1$ if n is odd), then $u_{\frac{n}{2}}$ (or $u_{\frac{n}{2}-1}$) is not counted as well.

To make these notation clearer, it would be beneficial to illustrate them in an example of a group of small degree.

Example 5.1.3 Let $G \cong PSL(2, 11)$ act on the right cosets of the maximal subgroup set Ω of 11 points. As we saw in Figure 5.4, G is a 2-homogeneous group, then $|\Omega_1^1| = 11$ and all 2-subsets are contained in the orbit Ω_2^1 of length 55. This means

$$c_1 = (11),$$
$$u_1 = ((10)).$$

Suppose that Σ is 2-subset of Ω, then there are 9 subsets of size 3 containing Σ; three of them lie in Ω_3^1 and the other 6 subsets lie in Ω_3^2. Clearly, Σ has two subsets of size 1 and they are contained in Ω_1^1. Then we have

$$c_2 = (55),$$
$$u_2 = ((3, 6)),$$
$$d_2 = ((2)).$$

Suppose that G acts on 3-subsets, then from Figure 5.4, G has two orbits on Ω_3, Ω_3^1 of length 55 and Ω_3^2 of length 110. Let $\Sigma_1 \in \Omega_3^1$, then there are 8 subsets of size 4 containing Σ_1, 6 of them lie inside Ω_4^3 and the other lie inside Ω_4^2. Hence, the first entry of u_3 is $(0, 2, 6)$. Also Σ_1 contains 3 subsets of size 2 and all of them are in the orbit Ω_2^1. Then, the first entry of d_3 is (3). Let $\Sigma_2 \in \Omega_3^2$, then from Figure 5.4 we see that the second entry of u_3 is $(2, 3, 3)$ and the second entry of d_3 is (3). It follows that:

$$c_3 = (55, 110),$$
$$u_3 = ((0, 2, 6), (2, 3, 3)),$$
$$d_3 = ((3), (3)).$$

Similarly, we can obtain c_k, u_k, and d_k for $k = 4, 5$ as follows

$$c_4 = (55, 110, 165),$$
$$u_4 = ((1, 0, 0, 6), (0, 1, 0, 6), (0, 1, 2, 4),$$
$$d_4 = ((0, 4), (1, 3), (2, 2)).$$

and

$$c_5 = (11, 55, 66, 330),$$
$$d_5 = ((5, 0, 0), (0, 2, 3), (0, 0, 5), (1, 2, 2)).$$

5.1.12 Alt(6) of degree 15

Let G be the group Alt(6) in its action on the right cosets of a maximal subgroup isomorphic to Sym(4) of index 15. Then Ω is of size 15.

The number and lengths of G-orbits on Ω_k, where $1 \leq k \leq 7$, are given in Table 5.1.

$c_1 =$ (15); $u_1 =$ ((6,8));
$c_2 =$ (45,60); $u_2 =$ ((1,0,0,4,8),(0,1,3,6,3)); $d_2 =$ ((2),(2)).
$c_3 =$ (15,20,60,180,180) $u_3 =$ ((0,0,0,0,0,0,12,0,0,0),(0,0,0,3,0,0,0,0,9,0),(2,0,1,0,0,0,0,0,3,6), (0,1,0,0,0,2,1,2,2,4),(0,0,1,1,2,2,2,2,0,2)); $d_3 =$ ((3,0),(0,3),(0,3),(1,2),(2,1)).
$c_4 =$ (30,45,60,60,90,180,180,180,180,360);

$u_4 =$ ((1,0,0,0,0,0,0,4,0,0,0,0,0,6,0,0,0,0),(0,0,0,1,0,2,0,0,0,0,0,0,0,0,0,8,0,0),
(0,0,0,0,0,0,0,2,0,0,3,0,0,0,0,0,0,6),(0,0,0,0,2,0,0,0,0,0,3,0,0,0,0,0,6,0),
(0,0,0,0,2,0,1,0,0,0,0,0,0,0,4,0,0,4),(0,1,0,0,0,0,0,0,0,1,0,1,0,0,2,2,2,2),
(0,0,0,1,0,0,0,0,0,0,2,2,2,0,4,0,0,0),(0,0,1,0,0,0,0,0,1,0,0,0,1,0,2,2,2,2),
(0,0,0,0,0,2,0,0,2,2,1,0,0,2,0,0,2,0),(0,0,0,0,0,0,1,1,1,1,0,1,1,1,0,2,1,1));

$d_4 =$ ((0,0,4,0,0),(0,0,0,4,0),(0,0,1,0,3),(0,1,0,0,3),(0,0,0,0,4),(0,0,0,2,2),
(1,0,0,1,2),(0,0,0,2,2),(0,1,1,2,0),(0,0,1,2,1);

$c_5 =$ (6,36,36,45,60,90,90,120,180,180,180,180,180,180,360,360,360,360);

$u_5 =$ ((0,0,0,10,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,5,0,5,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,5,0,0,0,5,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,8,0,0),
(1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3,0,0,6,0,0,0,0,0,0),
(0,1,0,0,0,0,0,1,0,0,0,0,0,0,0,0,4,0,0,0,0,0,0,0,4,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,4,0,0,0,4,0,0,0),
(0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,3,0,0,0,0,3,0,3,0,0,0),
(0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,2,0,0,0,0,2,0,2,2),
(0,0,0,0,0,1,0,0,0,0,1,0,0,0,0,0,2,0,0,0,2,2,0,2,0),
(0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,2,2,2,0,0,0,2),
(0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,2,0,2,0,0,2,0,2),
(0,0,1,0,0,0,0,0,0,0,0,0,0,1,0,0,0,2,0,2,2,0,2,0,0),
(0,0,0,1,0,0,0,0,1,0,0,0,0,0,0,0,4,0,0,2,0,2,0,0,0),
(0,0,0,0,1,0,0,0,0,0,0,0,1,1,0,0,0,1,2,0,1,0,2,0,1),
(0,0,0,0,0,0,1,0,0,1,1,1,0,0,1,0,1,2,0,0,0,0,1,1,0),
(0,0,0,0,0,0,0,0,1,1,1,0,0,0,0,1,0,0,1,1,1,0,0,2,1),
(0,0,0,0,0,0,0,0,0,0,0,2,1,1,1,1,0,0,1,0,1,1,0,0,1));

$d_5 =$ ((5,0,0,0,0,0,0,0,0,0,0),(0,0,0,0,0,5,0,0,0,0),

(0,0,0,0,0,0,0,5,0,0),(0,1,0,0,0,0,4,0,0,0),
(0,0,0,2,3,0,0,0,0,0),(0,1,0,0,0,0,0,0,4,0),
(0,0,0,0,1,0,0,0,0,4),(1,0,1,0,0,0,0,0,0,3),
(0,0,0,0,0,0,0,1,2,2), (0,0,0,0,0,1,0,0,2,2),
(0,0,1,1,0,0,2,0,1,0),(0,0,0,0,0,1,2,0,0,2),
(0,0,0,0,0,0,2,1,0,2),(1,0,0,0,0,0,0,0,2,2),
(0,0,0,0,1,1,2,1,0,0), (0,1,0,0,0,1,0,1,0,2),
(0,0,0,1,0,1,0,1,1,1),(0,0,1,0,1,1,0,1,0,1));

$c_6 =$ (10,15,60,60,60,60,60,90,90,180,180,180,180,180,180,180,360,360,360,
360,360,360,360,360,360);

$u_6 =$ ((0,0,9,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(1,0,0,0,0,8,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3,0,0,0,0,0,0,0,0,0,0,0,0,0,6),
(0,0,0,3,0,0,0,0,0,6,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,3,0,0,3,3,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3,0,0,6,0,0,0,0,0,0,0,0),
(0,1,0,0,2,0,0,0,0,0,3,0,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,4,0,0,0,4,0,0,0),
(0,0,0,1,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,4,0),
(0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,1,0,0,0,2,0,0,0,0,2,2,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,2,2,0,0,0,0,0,0,1,0,0,0,0,2,0,0,0,2,0,0),
(0,0,0,0,2,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,1,0,0,2,0,2,0,0,0,0),
(0,0,0,0,0,0,0,0,2,0,0,0,0,2,0,0,0,0,1,0,0,0,0,2,0,0,0,2,0,0),
(0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,1,2,0,0,0,0,0,0,0,2,2,0,0,0,0),
(0,0,0,0,2,0,1,0,0,1,0,0,0,0,1,0,0,0,0,0,0,0,0,0,2,0,0,2,0,0),
(0,0,1,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,2,0,0,2,0),
(0,1,0,0,0,1,0,0,0,1,0,1,0,0,0,0,0,0,0,1,1,1,1,0,0,0,0,0,0,1),
(0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,1,0,0,0,1,0,1,1,1,0,1,0,0),
(0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0,1,0,0,0,0,0,0,1,0,1,2,0,1,0),

(0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,2,0,1,0,0,1,1,1),
(0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,1,0,0,0,1,1,1,0,1,0,1,1),
(0,0,0,0,0,0,1,0,0,1,0,0,0,0,0,0,0,0,0,0,2,1,0,0,1,0,0,1,1,1),
(0,0,0,0,0,0,0,0,1,0,0,0,1,0,1,1,0,2,1,0,0,0,1,0,0,0,1,0,0,0),
(0,0,0,0,0,1,1,1,0,0,1,1,0,0,0,0,0,0,0,1,0,1,0,0,0,0,1,0,0,1),
(0,0,0,0,0,0,0,1,0,0,0,0,0,1,0,1,0,0,0,0,0,1,1,0,0,1,1,1,1,0));

$d_6 =$ ((0,0,0,0,6,0,0,0,0,0,0,0,0,0,0,0,0,0),(0,0,0,0,0,6,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,3,0,0,0,3,0,0,0,0,0),(1,0,0,0,0,0,0,2,0,0,0,0,0,3,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,6,0,0,0),(0,0,0,0,0,0,0,0,0,0,3,0,3,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,6,0,0),(0,0,0,1,0,1,0,0,0,0,4,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,4,0),(0,0,1,0,0,0,0,0,1,0,0,0,0,0,0,2,2,0),
(0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,2,2,0),(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,4),
(0,1,0,0,0,0,0,0,0,0,0,1,0,0,2,0,0,2),(0,0,1,0,0,0,0,0,0,0,0,0,1,0,2,0,0,2),
(0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,2,0,2),(0,0,0,0,1,0,1,0,0,0,0,0,0,0,0,0,2,2),
(0,0,0,0,0,1,0,0,1,1,0,0,0,2,0,1,0,0),(0,0,0,0,0,0,1,0,0,0,0,1,1,0,1,2,0,0),
(0,0,0,0,1,0,0,0,0,0,1,0,0,0,2,0,1,1),(0,0,0,0,0,0,0,1,0,0,1,1,1,1,0,0,1,0),
(0,0,0,0,0,0,0,0,0,1,1,0,1,0,1,0,1,1),(0,0,0,0,0,0,1,1,1,1,0,0,0,1,0,0,0,1),
(0,0,0,1,0,0,0,0,0,0,0,1,1,0,2,1,0,0),(0,0,0,0,0,1,0,0,1,1,0,0,0,0,0,1,2,0),
(0,0,0,0,0,0,0,0,1,0,1,1,0,0,1,0,1,1)).

$c_7 =$ (15,60,90,90,120,120,180,180,180,180,180,180,180,180,180,180,180,
180,180,180,180,360,360,360,360,360,360,360,360,360);

$d_7 =$ ((0,1,0,0,0,0,0,0,6,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,6,0,0,0,0,0,0,0,0),
(1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,4,0,0,0,0,0,0),
(0,0,0,2,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,4,0,0,0,0,0),
(0,0,0,0,0,0,1,0,0,0,0,3,0,0,3,0,0,0,0,0,0,0,0,0,0),
(0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3,0,0,0,0,0,0,3,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,2,0,0,0,0,0,2,0,2,0),

(0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,2,2),

(0,0,0,0,0,0,0,0,0,0,0,1,2,2,0,0,0,0,0,0,0,0,2,0,0),

(0,0,0,2,0,0,0,0,0,0,0,0,0,0,1,0,2,0,0,0,0,2,0,0,0),

(0,0,0,0,0,0,1,0,0,2,2,0,0,0,0,0,0,0,0,0,0,0,0,2,0),

(0,0,0,0,0,0,0,0,1,0,2,0,0,0,0,0,2,0,0,0,0,0,0,2,0),

(0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,4,0,0,0,0,2,0,0),

(0,0,0,0,1,0,0,0,0,0,0,0,2,0,0,0,0,0,2,0,0,0,0,0,2),

(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,2,2,0,0,2,0,0),

(0,0,1,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,2,0,2),

(0,0,0,0,1,0,0,0,0,0,0,0,2,0,0,0,0,2,0,2,0,0,0,0,0),

(0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,4,0,0),

(0,0,0,0,0,1,0,0,0,0,1,0,1,0,0,0,0,0,0,0,2,0,2,0,0),

(0,0,0,0,0,0,0,0,1,2,0,0,0,0,0,0,2,0,0,0,0,0,0,2,0),

(0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,2,0,0,0,0,4,0,0,0),

(0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0,1,0,1,0,1,1),

(0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,0,2,1,0,1,0,1),

(0,0,0,0,0,0,0,0,0,0,1,1,1,0,0,1,0,1,1,0,1,0,0,0,0),

(0,0,0,0,0,0,0,0,0,1,0,0,0,1,1,0,0,1,0,1,1,1,0,0,0),

(0,0,0,0,0,0,0,0,0,1,0,1,0,1,0,1,0,1,1,0,0,0,0,0,1),

(0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,2,0,1,0,1,1,1),

(0,0,0,0,0,0,0,0,0,0,1,0,1,0,1,0,0,1,0,1,0,1,0,0,1),

(0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,1,1,1,1,0,0,1),

(0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1,1,1,0,1,0).

Table 5.1: G-orbits of Alt(6) on its action on a set of 15 points

5.1.13 $ASL(2,4)$ of degree 16

Let G be the affine special linear group $ASL(2,4)$ acting upon the affine plane $\Omega = AG(2,4)$ of 16 points. The group G acts doubly transitively on the set Ω. The number and the lengths of G-orbits on Ω_k, where $1 \leq k \leq 8$, are given in Table 5.2.

Let Δ be a 6-subsets that lies inside the orbit Ω_6^{19}, where $|\Omega_6^{19}| = |G|$. One can show that from the 19^{th} entry of u_6 in Table 5.2, all 7-subsets which contain Δ lie in G-orbits of length less than the order of the group G. Hence, G satisfies Hypothesis($*$) in Chapter 4.

$c_1 =$ (16); $u_1 =$ (15);
$c_2 =$ (120); $u_2 =$ ((2,4,4,4)); $d_2 =$ ((2)).
$c_3 =$ (80,160,160,160) $u_3 =$ ((1,0,0,0,0,0,0,12),(0,1,0,0,0,3,3,6),(0,0,1,0,3,0,3,6),(0,0,0,1,3,3,0,6)); $d_3 =$ ((3),(3),(3),(3)).
$c_4 =$ (20,40,40,40,240,240,240,960); $u_4 =$ ((0,0,0,12,0,0,0,0,0,0,0),(0,0,0,0,0,0,12,0,0,0,0), (0,0,0,0,12,0,0,0,0,0,0),(0,0,0,0,0,12,0,0,0,0,0), (0,2,0,0,2,2,0,2,0,0,4),(2,0,0,0,0,2,2,0,2,0,4), (0,0,2,0,2,0,2,0,0,2,4),(0,0,0,1,1,1,1,2,2,2,2));

$d_4 =$ ((4,0,0,0),(0,4,0,0),(0,0,4,0),(0,0,0,4),(0,0,2,2),(0,2,0,2),(0,2,2,0),(1,1,1,1));

$c_5 =$ (96,96,96,240,480,480,480,480,480,480,960);

$u_5 =$ ((0,0,1,0,0,0,0,0,0,0,0,0,5,5,0,0,0,0,0,0,0,0),
(1,0,0,0,0,0,0,0,0,0,5,5,0,0,0,0,0,0,0,0,0,0),
(0,1,0,0,0,0,0,0,0,0,0,0,0,0,5,5,0,0,0,0,0,0),
(0,0,0,0,0,0,1,1,1,0,0,0,0,0,0,0,0,0,8,0,0),
(0,0,0,0,0,0,0,1,0,0,0,2,0,0,2,0,2,0,0,4,0),
(0,0,0,0,0,0,0,0,1,0,2,0,2,0,0,0,2,0,0,0,4),
(0,0,0,0,0,0,1,0,0,0,0,0,0,2,0,2,2,4,0,0,0),
(0,0,0,1,0,0,0,0,0,0,1,1,0,0,0,0,0,2,2,2,2),
(0,0,0,0,1,0,0,0,0,0,0,0,1,1,0,0,0,2,2,2,2),
(0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,0,2,2,2,2),
(0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,0,1,1,1,1));

$d_5 =$ ((0,0,0,0,0,5,0,0),(0,0,0,0,5,0,0,0),(0,0,0,0,0,0,5,0),
(1,0,0,0,0,0,0,4),(0,0,1,0,1,0,1,2), (0,0,0,1,1,1,0,2),
(0,1,0,0,0,1,1,2),(0,0,0,0,1,0,0,4),(0,0,0,0,0,1,0,4),
(0,0,0,0,0,0,1,4), (0,0,0,0,1,1,1,2));

$c_6 =$ (16,16,16,80,80,80,120,120,120,160,480,480,480,480,480,480,480,960
,960,960,960);

$u_6 =$ ((10,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(0,10,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,10,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) ,
(0,0,0,0,0,4,0,0,0,0,0,6,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,4,0,0,0,0,0,6,0,0,0,0,0,0,0,0,0,0,0,0) ,
(0,0,0,0,0,0,4,0,0,0,0,0,6,0,0,0,0,0,0,0,0,0,0,0,0,0),

(0,0,0,0,2,0,0,0,4,4,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,2,0,0,0,0,0,0,0,0,0,4,0,0,0,0,4,0,0,0,0),
(0,0,0,0,2,0,0,0,0,0,4,0,0,0,0,0,0,0,4,0,0,0,0,0),
(0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,3,3,3,0,0,0,0,0,0),
(1,0,0,0,0,0,0,0,0,0,1,2,0,0,0,2,0,0,0,0,2,0,0,2),
(1,0,0,0,0,0,0,0,0,0,0,1,0,0,2,0,0,2,0,0,2,0,0,2),
(0,0,1,0,0,0,0,0,0,0,0,0,0,1,0,2,0,0,2,0,0,2,0,2),
(0,0,1,0,0,0,0,0,2,0,0,0,0,1,0,0,2,0,0,0,0,2,0,2),
(0,1,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,2,0,2,2,2,0,0),
(0,1,0,0,0,0,0,0,0,2,0,0,1,0,0,0,2,0,0,0,2,2,0,0),
(0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,2,2,2),
(0,0,0,0,0,1,0,0,1,1,0,0,1,1,0,0,1,0,0,0,1,0,2,1),
(0,0,0,1,0,1,1,1,1,1,1,0,0,0,1,0,0,0,1,1,0,0,0,0),
(0,0,0,0,0,0,0,1,0,0,0,1,1,0,1,0,0,1,0,1,0,1,2,1),
(0,0,0,0,0,0,1,0,1,0,1,1,0,1,0,1,0,0,0,0,1,1,2,0));

$d_6 =$ ((0,6,0,0,0,0,0,0,0,0,0,0),(0,0,6,0,0,0,0,0,0,0,0,0),
(6,0,0,0,0,0,0,0,0,0,0,0), (0,0,0,0,0,0,0,6,0,0,0),
(0,0,0,0,0,0,0,0,6,0,0),(0,0,0,0,0,0,0,0,0,0,6,0),
(0,0,0,4,0,0,2,0,0,0,0,0), (0,0,0,2,4,0,0,0,0,0,0,0),
(0,0,0,2,0,4,0,0,0,0,0,0),(0,0,0,0,0,0,0,0,0,0,0,6),
(0,1,0,0,0,2,0,1,0,0,2), (0,1,0,0,2,0,0,1,0,0,2),
(1,0,0,0,0,2,0,0,1,0,2),(1,0,0,0,0,0,2,0,1,0,2),
(0,0,1,0,2,0,0,0,0,1,2), (0,0,1,0,0,0,2,0,0,1,2),
(0,0,0,0,2,2,2,0,0,0,0),(0,0,0,0,0,0,2,1,1,1,1),
(0,0,0,2,0,0,0,1,1,1,1), (0,0,0,0,2,0,0,1,1,1,1),
(0,0,0,0,0,2,0,1,1,1,1)).

$c_7 =$ (160,160,160,160,240,320,320,320,480,480,480,480,480,480,480,480,480,
480,480,480,960,960,960,960);

$u_7 =$ ((0,0,0,0,0,3,0,0,0,0,0,0,6,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,3,0,0,0,0,0,6,0,0,0,0,0,0,0,0,0,0),
(0,0,3,0,0,0,0,0,0,0,0,0,0,0,6,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,3,0,3,3,0,0,0,0,0,0,0,0,0,0),
(1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,4,4,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,3,0,0,0,3,3,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,3,0,0,3,0,0,0,3,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,3,0,0,0,0,0,0,3,0,0,3,0,0,0),
(0,0,1,0,1,0,0,1,0,0,0,0,0,2,0,0,0,0,0,2,0,2,0,0,0),
(0,0,0,0,0,0,1,1,1,0,0,0,0,2,0,0,0,0,0,0,2,2,0,0,0),
(0,0,0,1,0,1,1,0,0,0,0,0,0,0,2,0,0,0,2,2,0,0,0,0,0),
(0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,2,2,0,0,0,0,4,0),
(0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,2,0,0,4),
(0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,2,4,0,0),
(0,0,0,0,1,1,0,0,0,1,0,2,0,0,0,0,0,2,0,0,2,0,0,0,0),
(0,0,0,2,0,0,0,0,0,0,0,0,1,0,1,0,1,0,0,0,0,0,2,2,0),
(0,0,0,0,0,0,0,2,0,0,0,0,0,1,0,1,1,0,0,0,0,0,2,0,2),
(0,0,0,0,0,0,0,0,0,2,0,1,1,0,0,1,0,0,0,0,0,0,0,2,2),
(0,0,1,1,0,0,0,0,0,0,1,0,0,0,2,0,0,0,2,0,2,0,0,0,0),
(0,0,0,0,0,0,0,0,1,1,1,2,0,0,0,0,0,2,0,2,0,0,0,0,0),
(0,0,0,0,0,0,1,0,0,0,0,0,1,0,0,1,0,1,0,1,1,0,1,1,1),
(0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,1,1,0,0,1,1,1,1,1,1),
(0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1),
(0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,1,0,1,1,1,0,1,1,1))

$d_7 =$ ((1,0,0,0,0,0,0,0,0,0,3,3,0,0,0,0,0,0,0,0,0),
(0,1,0,0,0,0,0,0,0,0,0,0,0,0,3,3,0,0,0,0,0),
(0,0,1,0,0,0,0,0,0,0,0,0,3,3,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,6,0,0),
(0,0,0,0,0,0,1,1,1,0,0,0,0,0,0,0,4,0,0,0,0),
(0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,3,3,0,0),
(0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,3,0,3),

(0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,3,3,0),
(0,0,0,0,0,0,1,0,0,0,0,0,0,2,0,0,0,2,2,0,0),
(0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,2,2,0,0),
(0,0,0,0,0,0,0,0,1,0,2,0,0,0,0,0,0,0,2,0,2),
(0,0,0,1,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,2,2),
(0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,0,2,0,2,0),
(0,0,0,0,1,0,0,0,0,0,0,0,1,1,0,0,0,2,0,0,2),
(0,0,0,0,0,0,0,1,0,0,0,2,0,0,0,0,0,0,2,2,0),
(0,0,0,0,0,0,0,0,0,1,2,0,2,0,0,0,0,0,0,0,2),
(0,0,0,0,0,0,0,0,0,1,0,0,0,2,0,2,0,2,0,0,0),
(0,0,0,0,0,0,0,0,0,1,0,2,0,0,2,0,0,0,0,2,0),
(0,0,0,0,0,0,0,0,1,0,0,0,2,0,0,0,0,0,2,0,2),
(0,0,0,0,0,0,0,1,0,0,0,0,0,0,2,0,0,0,2,2,0),
(0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1,1,1,0,0,1),
(0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,0,0,1,1),
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,2,0,2,2),
(0,0,0,0,0,0,0,0,0,0,1,1,1,1,0,0,1,1,0,1,0)),

$c_8 =$ (30,120,240,240,240,240,240,240,240,240,240,480,480,480,480,480,480,
960,960,960,960,960,960,960,960);

$d_8 =$ ((0,0,0,0,8,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,8,0),
(0,0,2,0,0,0,0,0,2,0,0,0,0,2,0,0,0,0,2,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,4,0,0,2,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,4),
(2,0,0,0,0,0,0,0,0,0,2,2,0,0,2,0,0,0,0,0,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,2,2,0,0,0,0,0,0,0,0,0,4,0,0,0,0),
(0,0,0,0,0,0,0,0,2,2,0,0,0,0,0,0,4,0,0,0,0,0,0,0,0),
(0,2,0,0,0,0,0,0,0,2,0,0,2,0,0,0,0,0,0,2,0,0,0,0,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,4,0,2,0,0,0,0),

(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,2,0,4,0,0),
(0,0,0,1,0,0,0,2,0,0,0,0,0,0,2,0,0,1,0,2,0,0,0,0),
(2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,0,0,2,0,0,2),
(0,0,0,1,0,2,0,0,2,2,0,0,0,0,0,0,1,0,0,0,0,0,0,0),
(0,0,0,1,0,0,2,0,0,0,2,0,0,0,0,1,0,0,2,0,0,0,0,0),
(0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,2,2,0,0),
(0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,2,0,2),
(0,0,0,0,0,1,1,0,0,0,0,1,1,0,1,0,0,0,0,1,1,0,1,0),
(0,0,0,0,0,1,0,1,0,0,1,1,0,1,0,0,0,0,1,0,0,0,1,1),
(0,0,0,0,1,0,0,0,1,0,1,0,0,0,0,0,0,0,0,1,1,1,1,1),
(0,0,0,0,1,0,0,0,0,1,0,0,0,0,1,0,0,0,1,0,1,1,1,1),
(0,0,0,0,0,0,1,1,1,1,0,0,1,1,0,0,0,0,0,0,0,1,1,0),
(0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,1,1,0,0,0,1,1,1,1),
(0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,1,0,1,0,0,1,1,1,1),
(0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,1,1,0,0,1,1,1,1)).

Table 5.2: G-orbits of $ASL(2,4)$ on its action on a set of 16 points

Bibliography

[1] David M. Bloom. The subgroups of PSL(3, q) for odd q. *Trans. Amer. Math. Soc.*, 127:150–178, 1967. https://doi.org/10.2307/1994638.

[2] Paul Bradley and Peter Rowley. Orbits on k-subsets of 2-transitive simple lie-type groups. *MIMS EPrint*, 2014. http://eprints.ma.man.ac.uk/2167/1/covered/MIMS_ep2014_42.pdf.

[3] Paul Michael Bradley. *Counting G-Orbits on the Induced Action on K-Subsets*. PhD thesis, The University of Manchester (United Kingdom), 2014. https://www.escholar.manchester.ac.uk/uk-ac-man-scw:239461.

[4] David Bundy and Sarah Hart. The case of equality in the Livingstone-Wagner theorem. *J. Algebraic Combin.*, 29(2):215–227, 2009. https://doi.org/10.1007/s10801-008-0130-7.

[5] P. J. Cameron, H. R. Maimani, G. R. Omidi, and B. Tayfeh-Rezaie. 3-designs from PSL$(2, q)$. *Discrete Math.*, 306(23):3063–3073, 2006. https://doi.org/10.1016/j.disc.2005.06.041.

[6] Peter J. Cameron. Transitivity of permutation groups on unordered sets. *Math. Z.*, 148(2):127–139, 1976. https://doi.org/10.1007/BF01214702.

[7] Peter J. Cameron. Permutation groups on unordered sets. In *Higher combinatorics (Proc. NATO Advanced Study Inst., Berlin, 1976)*, volume 31 of *NATO Adv. Study Inst. Ser., Ser. C: Math. Phys. Sci.*, pages 217–239. Reidel, Dordrecht-Boston, Mass., 1977.

[8] Peter J. Cameron. Orbits of permutation groups on unordered sets. *Journal of the*

London Mathematical Society, s2-17(3):410–414, 1978. https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms/s2-17.3.410.

[9] Peter J. Cameron, Peter M. Neumann, and Jan Saxl. An interchange property in finite permutation groups. *Bull. London Math. Soc.*, 11(2):161–169, 1979. https://doi.org/10.1112/blms/11.2.161.

[10] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups.* Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[11] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory.* with an introduction by W. Magnus. Dover Publications, Inc., New York, 1958.

[12] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1996.

[13] Nick Gill. $\mathrm{PSL}(3, q)$ and line-transitive linear spaces. *Beiträge Algebra Geom.*, 48(2):591–620, 2007.

[14] R. W. Hartley. Determination of the ternary collineation groups whose coefficients lie in the $\mathrm{GF}(2^n)$. *Ann. of Math. (2)*, 27(2):140–158, 1925. https://doi.org/10.2307/1967970.

[15] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967.

[16] Bertram Huppert and Norman Blackburn. *Finite groups. III*, volume 243 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin-New York, 1982.

[17] I. Martin Isaacs. *Character theory of finite groups.* Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976. Pure and Applied Mathematics, No. 69.

[18] William M. Kantor. k-homogeneous groups. *Math. Z.*, 124:261–265, 1972. https://doi.org/10.1007/BF01113919.

[19] M. S. Keranen and D. L. Kreher. 3-designs of $\mathrm{PSL}(2, 2^n)$ with block sizes 4 and 5. *J. Combin. Des.*, 12(2):103–111, 2004. https://doi.org/10.1002/jcd.10068.

[20] Oliver H. King. The subgroup structure of finite classical groups in terms of geometric configurations. In *Surveys in combinatorics 2005*, volume 327 of *London Math. Soc. Lecture Note Ser.*, pages 29–56. Cambridge Univ. Press, Cambridge, 2005. https://doi.org/10.1017/CBO9780511734885.003.

[21] Weixia Li and Hao Shen. Simple 3-designs of $\mathrm{PSL}(2,\ 2^n)$ with block size 6. *Discrete Mathematics*, 308(14):3061–3072, 2008.

[22] Weixia Li and Hao Shen. Simple 3-designs of $\mathrm{PSL}(2,\ 2^n)$ with block size 7. *Journal of Combinatorial Designs*, 16(1):1–17, 2008.

[23] Donald Livingstone and Ascher Wagner. Transitivity of finite permutation groups on unordered sets. *Math. Z.*, 90:393–403, 1965. https://doi.org/10.1007/BF01112361.

[24] Howard H. Mitchell. Determination of the ordinary and modular ternary linear groups. *Trans. Amer. Math. Soc.*, 12(2):207–242, 1911. https://doi.org/10.2307/1988576.

[25] V. B. Mnukhin and I. J. Siemons. On the Livingstone-Wagner theorem. *Electron. J. Combin.*, 11(1):Research Paper 29, 8, 2004. http://www.combinatorics.org/Volume_11/Abstracts/v11i1r29.html.

[26] Valery B. Mnukhin. Some relations for the lengths of orbits on k-sets and $(k-1)$-sets. *Arch. Math. (Basel)*, 69(4):275–278, 1997. https://doi.org/10.1007/s000130050121.

[27] Yasuhiro Nakashima. A partial generalization of the Livingstone-Wagner theorem. *Ars Math. Contemp.*, 2(2):207–215, 2009. https://doi.org/10.26493/1855-3974.92.46f.

[28] Peter Rowley. Magma code for counting number of G-orbits. Unpublished.

[29] J. Siemons and A. Wagner. On the relationship between the lengths of orbits on k-sets and $(k+1)$-sets. *Abh. Math. Sem. Univ. Hamburg*, 58:267–274, 1988. https://doi.org/10.1007/BF02941383.

[30] William A. Simpson and J. Sutherland Frame. The character tables for SL(3, q), SU(3, q^2), PSL(3, q), PSU(3, q^2). *Canadian J. Math.*, 25:486–494, 1973. https://doi.org/10.4153/CJM-1973-049-7.

[31] Helmut Wielandt. *Finite permutation groups.* Translated from the German by R. Bercov. Academic Press, New York-London, 1964.

[32] Helmut Wielandt. Endliche k-homogene Permutationsgruppen. *Math. Z.*, 101:142, 1967. https://doi.org/10.1007/BF01136031.

[33] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London, Ltd., London, 2009. https://doi.org/10.1007/978-1-84800-988-2.

Appendix A

MAGMA codes of Chapter 2

In Chapter 2 we use the data base of primitive groups in Magma to find primitive groups that satisfy the equality of Livingstone-Wagner Theorem 2.3.7. In order to do this, we use a Magma code which was implemented by Rowley [28] to count the number of G-orbits on Ω_k.

```
procedure NumberofOrbskSets(G,k,~sigma)
 Sig:=0;CC:=Classes(G);
 for i:=1 to #CC do g:=CC[i][3];
 Cg:=CycleStructure(g);
 RPg:=RestrictedPartitions(k,{Cg[i][1]: i in [1..#Cg]});
 ng:=0;
 for I:=1 to #RPg do p:=RPg[I];np:=1;
 for j:=1 to #Cg do
 pj:=#{m:m in [1..#p] |p[m] eq Cg[j][1]};
 np:=np*Binomial(Cg[j][2],pj);
 end for;
 ng:=ng+np;
 end for;
 Sig:=Sig+(ng*CC[i][2]);
 end for;
 sigma:=Sig/(#G);
 end procedure;
```

Let D be the degree of the primitive group and take $2 \leq D \leq 160$. Now we can compare between the number of G-orbits on Ω_k and Ω_{k+1} as follows

```
for D in [2..160] do
for k in [3..Z!(Floor(D/2)-1)] do
for I:=1 to (Z!(NumberOfPrimitiveGroups(D)-2)) do
NumberofOrbskSets(PrimitiveGroup(D, I),k,~sigma);
S1:=sigma;
NumberofOrbskSets(PrimitiveGroup(D, I),k+1,~sigma);
S2:=sigma;
if S1 eq S2 then <D,I,k>;
end if; end for; end for; end for;
```

Then we get the following groups

$< 9, 6, 3 >$

$< 9, 7, 3 >$

$< 9, 8, 3 >$

$< 9, 9, 3 >$

$< 10, 2, 4 >$

$< 10, 4, 4 >$

$< 10, 5, 4 >$

$< 10, 7, 4 >$

$< 11, 6, 3 >$

$< 12, 4, 3 >$

$< 12, 1, 4 >$

$< 12, 2, 4 >$

$< 12, 3, 4 >$

$< 12, 4, 4 >$

$< 13, 7, 4 >$

$< 14, 2, 4 >$

$< 14, 2, 6 >$

$< 16, 20, 4 >$

$< 16, 17, 6 >$

$< 16, 18, 6 >$

$< 16, 19, 6 >$

$< 16, 20, 6 >$

$< 18, 2, 6 >$

$< 18, 2, 8 >$

$< 22, 1, 8 >$

$< 22, 2, 8 >$

$< 22, 2, 10 >$

$< 23, 5, 3 >$

$< 23, 5, 8 >$

$< 23, 5, 9 >$

$< 24, 3, 3 >$

$< 24, 3, 4 >$

$< 24, 3, 6 >$

$< 24, 3, 8 >$

$< 24, 3, 9 >$

$< 24, 3, 10 >$

$< 32, 3, 4 >$

$< 32, 3, 14 >$

$< 33, 2, 3 >$

$< 64, 64, 4 >$

$< 128, 3, 4 >$

The highlighted groups are k-homogeneous, so they are excluded from our list.

Appendix B

MAGMA codes of Chapter 3

```
Z:=Integers();
muk:=function(q,k);
p:=Factorisation(q)[1,1];sig:=0;CC:=[];
if p eq 2 then
Append(~CC,[<Z!((q^3-1)*(q+1)),1>,
<p,Z!((q^2)/p)>,<1,Z!(q+1)>]);
Append(~CC,[<Z!((q^3-1)*(q^3-q)),1>,
<4,Z!((q^2)/4)>,<2,Z!((q)/2)>,<1,1>]);end if;
if p ne 2 then
Append(~CC,[<Z!((q^3-1)*(q+1)),1>,
<p,Z!((q^2)/p)>,<1,Z!(q+1)>]);
Append(~CC,[<Z!((q^3-1)*(q^3-q)),1>,
<p,Z!((q^2+q)/p)>,<1,1>]);end if; a:=0;
for i:=1 to #CC do Cg:=CC[i];
S:={Z!(Cg[i][1]): i in [2..#Cg]};
RPg:=RestrictedPartitions(k,S);
for l:=1 to #RPg do p:=RPg[l];np:=1;
for j:=2 to #Cg do
pj:=#{m:m in [1..#p] |p[m] eq Cg[j][1]};
np:=np*Binomial(Cg[j][2],pj);
end for;
a:=a + np*(Cg[1][1]*Cg[1][2]);end for;end for;
```

```
return a;end function;

Pro:=function(A,B);CH:=[];
for i:=1 to #A do;for j:=1 to #B do;
if A[i] eq B[j] then Append (~CH,A[i]);
end if; end for; end for;
return CH; end function;

NotPro:=function(A,B);CH:=[];
for i:=1 to #A do; if not A[i] in B then
Append (~CH,A[i]);end if; end for;
return CH; end function;

etak:=function(k,T); ng:=0;PI:=T[1];
for i:=1 to #PI do
RPg:=RestrictedPartitions(k,{PI[i][1]:
i in [1..#PI]});end for;
for l:=1 to #RPg do p:=RPg[l];np:=1;
for j:=1 to #PI do
pj:=#{m:m in [1..#p] |p[m] eq PI[j][1]};
np:=np*Binomial(Z!(PI[j][2]),pj);
end for;
ng:=ng + np;end for; sigma:=ng;
return sigma;end function;

eff:=function(l1,l2,n,q);np:=1;
p:=Factorisation(q)[1,1];l0:=1; pr:=1;np:=1;
T:=Pro(Factorisation(l1),Factorisation(l2));
if#T eq 1 then Append(~T,<1,1>);end if;
for i in [1..#T] do l0:=l0*(T[i][1]^T[i][2]); end for;
m1:=Z!(l1/l0); m2:=Z!(l2/l0);
lstar:=LCM(m1,m2);nstar:=(n/lstar);if nstar in Z then
```

```
Aj:=Factorization(l0); Dj:=Factorization(Z!nstar);
P:=Pro(Aj,Dj); NP:=NotPro(Dj,Aj);
if #NP ne 0 then for s:=1 to #NP do;
np:=np*NP[s][1]^(Z!(NP[s][2]));end for;end if;
if #P ne 0 then for t:=1 to #P do;
pr:=pr*(P[t][1])^(Z!(P[t][2]-1))
*(EulerPhi(Z!(np)))*(Z!(P[t][1]-2));end for;end if;
if #P eq 0 then pr:=EulerPhi(np); end if;end if;
if not n/lstar in Z then nstar:= 1;pr:=0; end if;
return EulerPhi(m1)*EulerPhi(m2)*EulerPhi(l0)*pr;
end function;

CyTy:=procedure(T,~T1);
for i:=1 to #T do for j in [2..#T[i]] do for k in {1..j-1} do;
v1:=T[i][j][1]; if v1 eq T[i][k][1] then
v2:=T[i][j][2]+T[i][k][2];T[i][k][2]:=v2;
Exclude(~T[i],T[i][j]);break j;
end if;end for; end for;end for;T1:=T; end procedure;
CySt:=procedure(T,~CC);
CyTy(T,~T1);CyTy(T1,~T2);CyTy(T2,~T3); CC:=T3; end procedure;

PI6:=function(l1,l2,n,q);CK:=[]; t:=q^2-2*q+1;
l12:=LCM(l1,l2);
Append(~CK,
[<1,3>,<l1,Z!((q-1)/l1)>,<l2,Z!((q-1)/l2)>,<n,Z!((q-1)/n)>,
<l12,Z!(t/l12)>]);
CySt(CK,~CK);return CK;end function;

PI7:=function(l1,l2,n,q,t);CK:=[]; b:=q^2-2*q+1;
l12:=LCM(l1,l2);
Append(~CK,
[<t*l1,Z!((q-1)/(t*l1))>,<t*l2,Z!((q-1)/(t*l2))>,
```

```
<t*n,Z!((q-1)/(t*n))>,<t*l12,Z!(b/(t*l12))>,<1,3>]);
CySt(CK,~CK);return CK;end function;

PI36:=function(PI,t);
X:=[[]]; for i:=2 to #PI[1] do
Append(~X[1],<t*PI[1][i][1],PI[1][i][2]/t>);
 end for; return X;
 end function;

lambdak:=function(q,k);sum:=0;
d:=GCD(q-1,3);l:=Z!((q-1)/d);
D:=Divisors(l);Exclude(~D,1);
DD:=CartesianProduct(D,D);
for x in DD do; l1:=x[1];l2:=x[2];
p:=Factorisation(q)[1,1];l0:=1; pr:=1;np:=1;
T:=Pro(Factorisation(l1),Factorisation(l2));
if #T eq 1 then Append(~T,<1,1>);end if;
for i in [1..#T] do l0:=l0*(T[i][1]^T[i][2]); end for;
m1:=Z!(l1/l0);m2:=Z!(l2/l0);
lstar:=LCM(m1,m2);Dlo:=Divisors(l0);
for nstar in Dlo do n:=nstar*lstar;
if n ne 1 then CT:=PI6(l1,l2,n,q);
sum:=sum +(eff(l1,l2,n,q)*etak(k,CT));
end if; end for; end for;return sum;
end function;

g:=function(q,k);
sum:=0;sum1:=0;S:=[];SS:=[];DD:={};t:=1;
d:=GCD(q-1,3);l:=Z!((q-1)/d);
X:=Factorization(Z!(q-1));
if X[1][1] eq 3 then t:=X[1][1]^(X[1][2]);
elif X[2][1] eq 3 then t:=X[2][1]^(X[2][2]); end if;
```

```
a:=Factorization(t)[1][2];
D:=Divisors((Z!((q-1)/t)));C:=CartesianProduct(D,D);
for a in C do Include(~DD,a); end for;for x in DD do;
l1:=x[1];l2:=x[2];if LCM(l1,l2) in D then
T:=Pro(Factorization(l1),Factorization(l2));
if #T eq 0 then Append(~T,<1,1>);end if;
l0:=1;for i in [1..#T] do l0:=l0*(T[i][1]^T[i][2]);end for;
m1:=Z!(l1/l0);m2:=Z!(l2/l0);
lstar:=LCM(m1,m2);Dlo:=Divisors(l0);
for nstar in Dlo do n:=nstar*lstar;
CT:=PI7(l1,l2,n,q,t);
Append(~S,(eff(l1,l2,n,q)*etak(k,CT)));
end for;end if;end for;for i:=1 to #S do
Append(~SS,S[i]);end for;
for i:=1 to #SS do sum:= sum+SS[i];end for;
return (sum)*9^(a-1)*2;
end function;

eps:=function(q,k);
x:=0;
d:=GCD(q-1,3);l:=Z!((q-1)/d);
if d eq 1 then x:=lambdak(q,k);end if;
if d eq 3 then x:=lambdak(q,k)+g(q,k);end if;
return x;  end function;

procedure PSLsig(q,k,~sigma);
Z:=Integers();d:=Gcd(q-1,3);
p:=Factorisation(q)[1,1];sig:=0;CC:=[];ell:=Z!((q-1)/d);
D:=Divisors(ell);
I:=(d/(q^3*(q^3-1)*(q^2-1)))*(Binomial(Z!(q^2+q+1),k)+muk(q,k));
J:=(d/(6*(q-1)^2))*eps(q,k);for m in D do if m ne 1 then
Append(~CC,[<d/(q*(q-1)*(q^2-1)),EulerPhi(m)>,
```

```
<m,Z!((q^2-1)/m)>,<1,Z!(q+2)>]);end if;end for;
for j in D do m:=Z!(p*j);if j ne 1 then
Append(~CC,[<d/(q*(q-1)),EulerPhi(j)>,<p,Z!(q/p)>,<j,Z!((q-1)/j)>,
<m,Z!((q^2-q)/m)>,<1,2>]);end if; end for;
for m in Divisors(Z!((q^2-1)/d)) do if m in D eq false then;
j:=Z!((m/Gcd(m,ell)));
if j eq m then
Append(~CC,[<d/(2*(q^2-1)),EulerPhi(m)>,
<m,Z!((q^2+q)/m)>,<1,1>]);
elif j ne m then
Append(~CC,[<d/(2*(q^2-1)),EulerPhi(m)>,<j,Z!((q+1)/j)>,
<m,Z!((q^2-1)/m)>,<1,1>]);end if;end if; end for;
for m in Divisors(Z!((q^2+q+1)/d)) do
if m ne 1 then
Append(~CC,[<d/(3*(q^2+q+1)),EulerPhi(m)>,
<m,Z!((q^2+q+1)/m)>]);
end if; end for;a:=0;
for i:=1 to #CC do Cg:=CC[i];S:={Z!(Cg[i][1]): i in [2..#Cg]};
RPg:=RestrictedPartitions(k,S);
for l:=1 to #RPg do p:=RPg[l];np:=1;for j:=2 to #Cg do
pj:=#{m:m in [1..#p] |p[m] eq Cg[j][1]};
np:=np*Binomial(Cg[j][2],pj);
end for;
a:=a + np*(Cg[1][1]*Cg[1][2]);end for;end for;
sigma:=a+I+J;
end procedure;
```

k	σ_k
3	2
4	6
5	13
6	51
7	226
8	1085
9	5281
10	24147
11	100690
12	381718
13	1313961
14	4117053
15	11782779
16	30901157
17	74484384
18	165464336
19	339564965
20	645082794
21	1136468332
22	1859559479
23	2829640958
24	4008536534
25	5291160113
26	6512106685
27	7476798482
28	8010824682

Table B.1: $PSL(3,7)$

k	σ_k
3	2
4	3
5	5
6	25
7	132
8	901
9	6155
10	38344
11	217432
12	1119290
13	5242484
14	22449375
15	88267837
16	319907830
17	1072522676
18	3336559726
19	9658168478
20	26076599606
21	65811704180
22	155553963224
23	344922652766
24	718587080682
25	1408428360846
26	2600172554746
27	4526222907944
28	7435933709098
29	11538513489266
30	16923148623132
31	23474040320930
32	30809673593361
33	38278681627549
34	45033740037278
35	50180451020258
36	52968252821940

Table B.2: $PSL(3, 8)$

k	σ_k
3	2
4	4
5	9
6	40
7	251
8	2179
9	19068
10	153107
11	1119490
12	7444639
13	45193018
14	251681833
15	1291732944
16	6135221339
17	27066109468
18	111269738050
19	427506100202
20	1539014685175
21	5203322444771
22	16556003538697
23	49667973112517
24	140725863194328
25	377145217789080
26	957368483960962
27	2304775764441529
28	5268058579909611
29	11444402688681292
30	23651764970160503
31	46540569006938438
32	87263565899333345
33	156016677200478970
34	266146094923567178
35	433437924293017177
36	674236769173734342
37	1002243843936415371
38	1424241249658381660
39	1935507336997433577
40	2516159535877523614
41	3129856981602024483
42	3726020214419475684
43	4245930010370281286
44	4631923646701731850
45	4837786919397985830

Table B.3: $PSL(3,9)$

Appendix C

MAGMA codes of Chapter 4

In Chapter 4 we use the following code to determine the primitive groups (of degree less than 25) that satisfy Hypothesis($*$).

```
Z:=Integers();
SizeofOrbsPRIMk:=procedure(G,k,~a);
S:={}; K:={}; D:={1..Degree(G)}; kD:=Subsets(D,k);a:={};
Omega:=GSet(G,kD); O:=Orbits(G,Omega);
for Orbs in O do T:=Random(Orbs);Include(~K,T);end for;
V:={};
for T in K do;N:=Z!(#G/#Stabilizer(G,T));
if N eq #G then P:=D diff T; for b in P do;
Include(~V, #Stabilizer(G, T join{b}));
end for;
S:=Min(V);L:= Z!(#G/S);
if N gt L then Include(~a,<N,T>);
end if;end if;end for;
end procedure;
```

Let D be the degree and take $3 \leq D \leq 25$.

```
for D in [3..25] do
for k in [2..Z!(Floor(D/2)-1)] do
for I:=1 to (Z!(NumberOfPrimitiveGroups(D)-2))do
```

```
SizeofOrbsPRIMk(PrimitiveGroup(D, I),k,~T);
if #T ge 1 then <D,I,T>;
end if;end for;end for;
```

Then the primitive groups that satisfy Hypothesis($*$) are as follows

```
<12, 1, {
    <660, { 1, 5, 8, 10, 12 }>}>


<14, 1, {
    <1092, { 6, 7, 10, 11, 12, 13 }>}>
<15, 3, {
    <2520, { 4, 7, 10, 11, 12, 13 }>}>
<16, 11, {
    <960, { 2, 4, 6, 7, 9, 12 }>}>
<17, 6, {
    <4080, { 6, 10, 11, 16, 17 }>}>
<21, 4, {
    <20160, { 2, 6, 8, 10, 11, 18 }>}>.
```

Appendix D

MAGMA codes of Chapter 5

The following two codes are used to check the results of our calculations in Chapter 5.

let G be a primitive group acting upon a set D and let $Omega = D_k$ and $Omega1 = D_{k+1}$. In the first code we take T to be an element in a G-orbit on $Omega$ and take N to be $(k+1)$-subset containing T. Then we we determine the G-orbit (on $Omega1$) which N belongs to.

```
D:={1..Degree(G)};
z:=Integers();
for k in [1..z!(Floor(Degree(G)/2)-1)] do
Omega:=Subsets(D,k); GS:=GSet(G,Omega); O:=Orbits(G,GS);
Omega1:=Subsets(D,k+1);
GS1:=GSet(G,Omega1); O1:=Orbits(G,GS1);
for i:=1 to #O do T:=Random(O[i]);
printf"i:=";i,"#O[i]:=",#O[i],"T:=",T;
P:=D diff T;
for b in P do N:=T join {b};
for j:=1 to #O1 do Oj:=O1[j];
if N in O1[j] then printf"#O[j]:=";#O1[j],"j=",j;
end if; end for; end for; end for;end for;
```

In the second code we take R to be an element of G-orbit on $Omega1$ and take y to be k-subset of y. Then we determine the G-orbit on $(Omega)$ which y belongs to.

```
D:={1..Degree(G)};
```

```
z:=Integers();
for k in [1..z!(Floor(Degree(G)/2)-1)] do
Omega:=Subsets(D,k); GS:=GSet(G,Omega); O:=Orbits(G,GS);
Omega1:=Subsets(D,k+1);
GS1:=GSet(G,Omega1); O1:=Orbits(G,GS1);
for s:=1 to #O1 do R:=Random(O1[s]);
printf"s:=";s,"#O1[s]:=",#O1[s],"R:=",R;
Y:=Subsets(R,k);
for y in Y do h:=y; for t:=1 to #O do Ot:=O[t];
if y in O[t] then printf"#O[t]:=";#O[t],"t=",t;
end if; end for; end for; end for;end for;
```

Appendix E

Tables for Chapter 5

As we saw in Chapter 5 the diagrams for the groups Alt(5) of degree 10, Alt(7) of degree 15, and $PSL(2,13)$ of degree 13 are slightly complicated. Therefore, it would be worth presenting them also in tables as follows.

E.0.1 Alt(5) of degree 10

$c_1 =$ (10); $u_1 =$ ((3,6));
$c_2 =$ (15,30); $u_2 =$ ((0,0,4,2,2),(1,2,1,2,2)); $d_2 =$ ((2),(2)).
$c_3 =$ (10,20,30,30,30) $u_3 =$ ((0,1,0,0,0,6,0),(1,0,0,0,0,3,3),(0,1,0,2,2,0,2),(0,0,1,0,2,2,2), (0,0,1,2,0,2,2)); $d_3 =$ ((0,3),(0,3),(2,1),(1,2),(1,2)).

$c_4 =$ (5,10,15,30,30,60,60);
$u_4 =$ ((0,0,0,0,0,6,0,0),(0,0,0,0,0,0,6,0),(0,0,2,0,0,0,0,4),
(0,1,0,1,0,0,2,2),(1,0,0,0,1,0,2,2), (0,0,2,1,1,1,1,0),
(0,0,0,1,1,1,1,2));
$d_4 =$ ((0,4,0,0,0),(1,0,3,0,0),(0,0,0,2,2),(0,0,2,0,2),(0,0,2,2,0),
(1,1,0,1,1),(0,1,1,1,1));

$c_5 =$ (6,6,30,30,30,30,60,60);
$d_5 =$ ((0,0,0,0,5,0,0),(0,0,0,5,0,0,0),(0,0,1,0,0,4,0),(0,0,0,1,0,2,2),
(0,0,0,0,1,2,2),(1,0,0,0,0,2,2), (0,1,0,1,1,1,1),(0,0,1,1,1,0,2));

Table E.1: G-orbits of Alt(5) on its action on a set of 10 points

E.0.2 Alt(7) of degree 15

$c_1 =$ (15);
$u_1 =$ ((14));

$c_2 =$ (105);
$u_2 =$ ((1,2));
$d_2 =$ ((2)).

$c_3 =$ (35,240)
$u_3 =$ ((0,0,12,0),(1,2,3,6));
$d_3 =$ ((3),(3)).

$c_4 =$ (105,210,420,630); $u_4 =$ ((0,0,3,0,8,0),(1,0,0,0,4,6),(0,0,3,2,0,6),(0,1,0,2,4,4)); $d_4 =$ ((0,4),(0,4),(1,3),(0,4));
$c_5 =$ (42,126,315,420,840,1260); $u_5 =$ ((0,0,0,10,0,0,0),(0,0,0,0,0,10,0),(0,2,0,0,0,0,8), (1,0,0,0,0,3,6),(0,0,0,1,3,3,3),(0,0,1,1,0,2,6)); $d_5 =$ ((0,5,0,0),(0,0,0,5),(1,0,4,0),(0,0,2,3),(1,1,0,3),(0,1,2,2));
$c_6 =$ (70,105,210,420,420,1260,2520); $u_6 =$ ((0,0,0,9,0,0,0,0,0),(1,0,0,0,0,8,0,0,0),(0,0,0,0,3,0,0,6,0), (0,0,0,0,3,0,6,0,0), (0,2,1,0,0,0,3,0,3),(0,0,0,1,0,0,2,2,4), (0,0,1,1,1,2,1,2,1)); $d_6 =$ ((0,0,0,6,0,0),(0,0,6,0,0,0),(0,0,0,0,0,6),(1,0,0,0,2,3), (0,0,0,0,6,0),(0,1,0,1,2,2), (0,0,1,1,1,3));
$c_7 =$ (15,120,420,630,630,840,1260,1260,1260); $d_7 =$ ((0,7,0,0,0,0,0),(0,0,0,0,7,0,0),(0,0,0,0,1,0,6), (1,0,0,0,0,2,5),(0,0,1,2,0,0,5),(0,1,0,0,0,0,6), (0,0,0,2,1,2,2),(0,0,1,0,0,2,4),(0,0,0,0,1,4,2));

Table E.2: G-orbits of Alt(7) on its action on a set of 15 points

E.0.3 $PSL(2, 13)$ of degree 13

$c_1 =$ (14); $u_1 =$ ((13));
$c_2 =$ (91); $u_2 =$ ((6,6)); $d_2 =$ ((2)).
$c_3 =$ (182,182) $u_3 =$ ((0,2,3,6),(2,0,3,6)); $d_3 =$ ((3),(3)).
$c_4 =$ (91,91,273,546); $u_4 =$ ((0,4,0,6,0),(4,0,0,0,6),(0,0,2,4,4),(1,1,4,2,2)); $d_4 =$ ((0,4),(4,0),(2,2),(2,2));
$c_5 =$ (182,182,546,546,546); $u_5 =$ ((0,0,0,3,6,0,0),(0,0,0,0,3,6,0),(1,0,0,2,0,2,4), (0,0,1,0,2,2,4),(0,1,0,2,2,0,4)); $d_5 =$ ((0,2,0,3),(2,0,0,3),(0,0,1,4),(1,0,2,2),(1,0,2,2),(0,1,2,2));
$c_6 =$ (91,91,91,546,546,546,1092); $u_6 =$ ((0,0,0,0,4,4,0,0,0,0,0),(0,0,0,2,0,0,0,0,0,6),(0,0,2,0,0,0,0,0,6,0), (1,0,0,0,0,2,1,2,0,2), (0,0,0,0,0,0,2,2,2,2),(0,1,0,0,2,0,2,1,2,0), (0,0,1,1,1,1,1,1,1,1));

$d_6 =$	((0,0,6,0,0),(0,0,0,0,6),(0,0,0,6,0),(2,0,2,0,2),(1,1,0,2,2), (0,2,2,2,0),(0,0,2,2,2));
$c_7 =$	(78,78,182,182,364,364,546,546,546,546);
$d_7 =$	((0,0,0,7,0,0,0),(0,0,0,0,0,7,0),(0,0,1,0,0,0,6),(0,1,0,0,0,0,6), (1,0,0,0,0,3,3),(1,0,0,3,0,0,3),(0,0,0,1,2,2,2),(0,0,0,2,1,2,2), (0,0,1,0,2,2,2),(0,1,0,2,2,0,2));

Table E.3: G-orbits of $PSL(2,13)$ on its action on a set of 14 points