COUNTING G-ORBITS ON THE INDUCED ACTION ON k-SUBSETS

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

2014

Paul Michael Bradley
School of Mathematics

Contents

Word count 22570

List of Tables

The University of Manchester

Paul Michael Bradley
Doctor of Philosophy
COUNTING G-ORBITS ON THE INDUCED ACTION ON k-SUBSETS
November 10, 2014

Let G be a finite permutation group acting on a finite set Ω. Then we denote by $\sigma_k(G, \Omega)$ the number of G-orbits on the set Ω_k, consisting of all k-subsets of Ω. In this thesis we develop methods for calculating the values for $\sigma_k(G, \Omega)$ and produce formulae for the cases that G is a doubly-transitive simple rank one Lie type group. That is $G \cong PSL(2, q), Sz(q), PSU(3, q)$ or $R(q)$. We also give reduced functions for the calculation of the number of orbits of these groups when $k = 3$ and go on to consider the numbers of orbits, when G is a finite abelian group in its regular representation.

We then consider orbit lengths and examine groups with "large" G-orbits on subsets of size 3.

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

Acknowledgements

I want to say thank you firstly to my supervisor, Peter Rowley. He has helped me immeasurably through the last four years and without his support I doubt very much I would have gotten here. I am also grateful that I was given the chance to work with some of the country's best PhD. students, many of them with no idea how talented they are.

The second person I want to thank is my wife, Lisa, who allowed me to leave my career as a teacher to pursue this PhD. an endeavour which appeared both futile and lacking in judgement in equal measure at times. However, she gave me the faith in myself and supported us both, almost entirely, financially throughout. It is with the upmost clarity that I say that everything I have achieved so far and will go on to achieve in the future is because of her support. Thank you.

Finally, Manchester University gave me a place to be between the hours of 9 and 5 on week days. I have no doubt that if had been there between the hours of 9 and 5 most week days I would have finished this earlier, but I wasn't, so I didn't, let's not live in the past.

Chapter 1

Introduction

When studying finite groups, it is clear that group actions are of great importance. Exploring how a group acts on a structure, be it a vector space, Steiner system or some other set can allow us to see links between the group and other areas of mathematics. In looking at these actions questions about orbit lengths and numbers of orbits arise naturally, and as such have been studied extensively, with two of the most well known results on the latter coming in the form of the Orbit Counting Lemma and the Livingstone-Wagner Theorem.

Viewing groups through their actions allows us to write abstract groups or matrix groups in terms of permutation groups, and we may use a faithful representation of our group G acting on Ω as a subgroup of $Sym(n)$ when $|\Omega| = n$ to answer some of the questions we have mentioned. This affords us the opportunity of not having to wade through abstract spaces and complex actions. A particular subset of finite groups of interest to us are the doubly transitive finite groups whose classification formed part of the Classification of Finite Simple groups. An excellent exposition of these groups is given in Dixon and Mortimer [10], (or see Passman [23]). We choose four infinite families of these finite simple groups and answer questions relating to the number of orbits these groups have when we consider their permutation representations and induced actions on k-subsets of their respective G-sets, we also consider bounds for numbers of orbits for finite abelian groups acting in their regular representations.

Before we discuss our results further, we outline some notation and discuss our main motivation. We begin by saying that G will usually, denote a finite permutation group of degree n acting on a set Ω. Our primary motivation is due to Livingstone and

Wagner [16] who in 1965 published their paper titled "Transitivity of finite permutation groups on unordered sets", in which they presented the following result relating to group actions on k-sets. Throughout we will make use of the notation used in Livingstone and Wagner's paper, which we recall below.

Definition 1. Let G be a group acting on a set Ω of cardinality n. Then the number of G-orbits on Ω_k, the set of k-subsets of Ω, is denoted by $\sigma_k(G, \Omega)$. If $\sigma_k(G, \Omega) = 1$ we say G is k-homogeneous.

Remark When G and Ω are understood, we may write σ_k.

Theorem 1.0.1. *[Livingstone Wagner [16]]*

If $2 \leq k \leq \frac{n}{2}$, then the number of group orbits on the set of k-subsets of n points is at least as great as the number of orbits on the set of $(k-1)$-subsets of n points. That is,

$$\sigma_k \geq \sigma_{k-1}.$$

This induced action has been the subject of numerous papers, including Nakashima [21], who was able to make some generalisations of the original theorem by introducing a comparison of the number of G-orbits on k-subsets with the number of G-orbits on ordered $(k-1)$-tuples of Ω. This paper followed on from Mnukhin and Siemons [20] who in 2004 presented a more general theorem relating to orbits on subsets, which contained the Livingstone-Wagner Theorem as a special case, but also gave information about orbit counts for simplicial complexes, sequences, graphs and amalgamation classes.

As a consequence of the Livingstone-Wagner Theorem, there arise questions about the cases when $\sigma_k = \sigma_{k-1}$. These were tackled in 2009 by Bundy and Hart [3] in their paper "The case of equality in the Livingstone-Wagner Theorem", where they proved, the following results.

Lemma 1.0.2. *[Bundy and Hart [3]] Let $H \leq G \leq S_n$ and $1 \leq k < (n-1)/2$. 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 equality in a subgroup implies equality in the group. This clearly allows for equality at any point as S_n always maintains this equality condition. The next result requires the following notation. Let G be a finite permutation group acting

on a set Ω of cardinality n. Then if $\Delta \subseteq \Omega$ is a G-orbit denote the action of G on the G-set Δ by G^{Δ}.

Proposition 1.0.3. *[Bundy and Hart [3]] Let $G \leq S_n$ and $1 \leq k < (n-1)/2$ with $\sigma_{k+1}(G) = \sigma_k(G)$. Let Δ be an orbit of G of length at least $n-k$. Then $\sigma_l(G^{\Delta}) = \sigma_{l+1}(G^{\Delta})$, for all $k-(n-|\Delta|) \leq l \leq min(k, |\Delta|-k-2)$.*

If we have a case of equality, then we can take an orbit of length greater than $n-k$ and restrict the action of G to this set. This will then give us cases of equality for all values of σ_l satisfying $k-(n-|\Delta|) \leq l \leq \min(k, |\Delta|-k-2)$.

Considering the number of G-orbits on two sets and two actions, was the focus of a 1993 paper of Evans and Siemons [11] with obvious links to the above problems, their main focus was on comparing the numbers of orbits of G and its subgroups H acting on two different G-sets.

We will make prolific use of the classical result the Orbit Counting Theorem, which we mentioned above and which appears in numerous places for example see [22]. Here we present the result using Livingstone and Wagner's notation.

Theorem 1.0.4. *[Neumann [22]] Let G be a group and Ω a G-set, then if σ is the number of G-orbits on Ω we have*

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

As we are concerned primarily with k-subsets of Ω we use

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

This thesis can be split into two main parts, the first of which is concerned with calculating values for $\sigma_k(G,\Omega)$, where G is a finite doubly-transitive simple group of Lie rank one and the second being a look at lengths of orbits. We begin with Chapter 2, where we take a direct hands on approach to calculating the number of and lengths of orbits for $G \cong PSL(2,q)$, $q = 7, 11$ acting on the $q+1$ points of the projective line. We do this by ascertaining the number of fixed points for the group elements and then utilising the Orbit Counting Theorem to determine our solutions, the chapter then concludes with a table giving the number of orbits and their lengths. These two examples are small, and yet the calculation required is quite lengthy. For large values

of q, computer power and memory can be easily exhausted by direct computation and so we are unable, due to practicality, to directly calculate sequences of values for σ_k for these groups. This process acts as a source of motivation for our third chapter.

In Chapter 3, we establish four main results for the values of $\sigma_k(G, \Omega)$. These results come in the form of formulae, which can be implemented by a computer without the need to construct the group G, and as such can be evaluated, without such large demands on memory and time. The formulae themselves are quite ungainly to look at, and so we include MAGMA code for the implementation of each. More formally the main results in this chapter are formulae for $\sigma_k(G, \Omega)$, when G is a rank one simple Lie-type group acting doubly-transitively on Ω. Thus if we set $q = p^a$ where p is a prime and $a \in \mathbb{N}$, then the possibilities for G are $PSL(2, q)$ $(q > 3)$, the 2-dimensional projective special linear groups, $Sz(q)$ $(q = 2^{2n+1} > 2)$, the Suzuki groups, $PSU(3, q)$ $(q > 2)$, the 3-dimensional projective special unitary groups and $R(q)$ $(q = 3^{2n+1} > 3)$, the Ree groups. The corresponding sets Ω are the projective line (with $|\Omega| = q + 1$), the Suzuki oval (with $|\Omega| = q^2 + 1$), the isotropic 1-spaces of a 3-dimensional unitary space (with $|\Omega| = q^3 + 1$) and the Steiner system $S(2, q+1, q^3+1)$ (with $|\Omega| = q^3 + 1$).

As stated in the introduction, we dedicate a portion of this thesis to calculation of numbers of orbits of $PSL(2, q)$, in its doubly transitive action on $(q + 1)$ points. We remark that a great deal of work has been done in solving this problem for this particular family of groups, notably Cameron, Maimani, Omidi and Tayfeh-Rezaie [5] in 2006 published "3-designs from $PSL(2, q)$", where they present a method for calculation of the number of orbits which requires the use of a table of formulae and summing over the various subgroups of $PSL(2, q)$. However, they only concerned themselves with the case $q \equiv 3 (\text{mod } 4)$ as their main objective was to find 3-designs for which $PSL(2, q)$ acted as an automorphism group and so restricted their attention to when $PSL(2, q)$ is 3-homogeneous. Shortly afterwards in 2006 Cameron, Omidi and Tayfeh-Rezaie [6] published a second paper, this time for the family $PGL(2, q)$ with the same objective. It was not until 2012, that Chen and Liu [8] successfully tackled the remaining cases, that is when $q \equiv 1 (\text{mod } 4)$, where they again searched for 3-designs. In their paper, however, they did not include any methods for counting the orbits in these instances.

After establishing our results for these families of groups, in Chapter 4 we show applications of the formulae from Chapter 3. We give alternate proofs of some known

results for $PSL(2,q)$ and then go on to describe smaller, special cases of the formulae for each of the families with the results reduced and simplified for the numbers of orbits when $k = 3$.

Corollary 1.0.5 (Corollary of Theorem 3.2.1)**.** *Let $\sigma_3(PSL(2,q))$, $q = p^a > 2$, where p is prime, $a \in \mathbb{N}$, be the number of orbits on 3-subsets of the $(q+1)$ points on which $PSL(2,q)$ acts.*

$$\sigma_3(PSL(2,q)) = \begin{cases} 2, & \text{if } q \equiv 1 \bmod 4 \\ 1, & \text{if } q \equiv 3 \bmod 4 \end{cases}.$$

Proposition 1.0.6. *Let $L_n = PSL(2,2^n)$ acting on the projective plane Ω_n, and put $a_n = \sigma_4(L_n, \Omega_n)$. Setting $a_1 = a_2 = 1$, for $n \geq 3$ we have*

$$a_n = a_{n-1} + 2a_{n-2}.$$

Alternatively

$$a_n = \frac{2^n + (-1)^{n-1}}{3}.$$

Proposition 1.0.7. *Let $a_n = \sigma_3(Sz(q))$, $q = 2^{2n+1}$, be the number of orbits on 3-subsets of the (q^2+1) points on which $Sz(q)$ acts. Then*

$$a_n = \frac{4^n + 2}{3}.$$

Proposition 1.0.8. *Let $a_n = \sigma_3(PSU(3,q))$, $q = 3^n$ be the number of orbits on 3-subsets of the (q^3+1) isotropic points on which $PSU(3,q)$ acts. Then*

$$a_n = \frac{3^n + 3}{2}.$$

Proposition 1.0.9. *Let $a_n = \sigma_3(R(q))$, $q = 3^{2n+1}$ be the number of orbits on 3-subsets of the q^3+1 points on which $R(q)$ acts. Then*

$$a_n = \frac{(3^{2n+1} + 3)^2}{6}.$$

In chapter 5 we calculate σ_k for finite abelian groups in their regular representations and compare values for non-isomorphic groups of equal order. With our main result being

Corollary 1.0.10 (Corollary of Theorem 5.1.7)**.** *Let*

$$H \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{(m_{n-1})(m_n)},$$

and let

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{(m_{n-1})} \times \mathbb{Z}_{(m_n)},$$

where $hcf(m_1, m_2, ..., m_n) = m_n$.

$$\textit{Then } \sigma_k(H) = \begin{cases} \sigma_k(G), & \textit{for all } k \textit{ where } (k, m_i) = 1 \textit{ for all } i \\ \leq \sigma_k(G), & \textit{for all } k \textit{ where } (k, m_i) \neq 1 \textit{ for some } i. \end{cases}$$

The secondary goal of this Thesis is to explore the relationship of G-orbit lengths for k and $(k+1)$-subsets of Ω. The starting point for this aspect for our investigation is the 1988 paper "On the relationship between the lengths of orbits on k-sets and $(k+1)$-sets" by Siemons and Wagner [27], where they discuss the relationship of the length of the orbit of a k-subset of Ω with the length of orbit of any $(k+1)$-subset of Ω containing it. We also note here that there is a paper discussing a bounding property in this case by Mnukhin [19] titled "Some relations for the lengths of orbits on k-sets and $(k-1)$-sets". Our focus is on results for when G and its G-set are both finite, but for the record, we remark there is a considerable literature concerning the infinite case; for a small selection see Cameron [7]. This secondary goal is approached in Chapter 6 where we consider the case when G is a permutation group acting on $n \geq 8$ points where a 3-subset has a larger orbit than any 4-subset containing it. We are able to show in Proposition 6.2.3 that if G is a primitive permutation group acting on a set Ω of cardinality $n \geq 8$ and if Δ is a 3-subset of Ω such that $|\Delta^G| > |\Sigma^G|$ for all 4-subsets Σ containing Δ. Then Δ^G is of maximal length of any orbit on 3-subsets. We then go on to classify all such groups when there is only one orbit on 3-subsets, with the following:

Theorem 1.0.11. *Let G be a 3-homogeneous permutation group acting on a G-set, Ω, of cardinality $n \geq 8$. If the orbit on 3-subsets has length strictly greater than the G-orbit of any 4-subset then $G \cong PSL(2,7)$ or $G \cong PGL(2,7)$.*

1.1 Notation

For the benefit of the reader we end this introduction by presenting a table of notation which will be used going forward throughout this thesis. Where we reassign notation for an alternate purpose, we will make it explicit at the time.

G	A finite permutation group.
Ω	A finite G-set.
n	$\lvert\Omega\rvert$.
Ω_k	The set of all k-subsets of Ω.
$\sigma_k(G,\Omega), \sigma_k(G), \sigma_k$	The number of G-orbits on Ω_k.
G^{Δ}	The action of G restricted to G-set $\Delta \subset \Omega_k$ for some $k \in \mathbb{N}$.
$PSL(2,q)$	Projective special linear group type A_1.
$Sz(q)$	Suzuki group type ${}^2\mathrm{B}_2$.
$PSU(3,q)$	Projective special unitary group type ${}^2\mathrm{A}_2$.
$R(q)$	Ree group of type ${}^2\mathrm{G}_2$.
$S(a,c,b)$	Steiner system.
ϕ	Euler's ϕ function.
$\mathcal{D}(\ell)$	The set of divisors of $\ell \in \mathbb{N}$.
$\mathcal{D}^*(\ell)$	$\mathcal{D}(\ell) \setminus \{1\}$
$\pi = \lambda_1\lambda_2...\lambda_r$	A partition of n.
π_g	The cycle type of an element $g \in G$.
η_k	The number of subsequences $\lambda_{i_1}, \lambda_{i_2}, ..., \lambda_{i_l}$ of $\lambda_1, ..., \lambda_r$ which form a partition of k.
$\mathfrak{O}_{(m)}(G)$	The number of elements in G with order m.

Table 1.1: Notation

Chapter 2

Calculating σ_k

This chapter contains detailed examples of calculating the values of σ_k for two particular groups in the family of $PSL(2, q)$, the projective special linear groups over the field $\mathbb{F}_q$, where q is a power of a prime p. We lead with a brief discussion about these groups and their actions on the projective line before moving on to our two specific examples. We have chosen these two groups to tackle in detail as, apart from being small enough to manage, they both have a particular property relating to lengths of their orbits, which we highlight at the end of this chapter and discuss in greater detail in Chapter 6.

2.1 Examples for σ_k for $PSL(2, q)$

2.1.1 The Projective Line over $\mathbb{F}_q$

The projective line is the set of coordinate representatives on a line which can be used to express all points in the two dimensional space.

We form these representatives by projecting all points along a line down to a single point. This means we can deal with a single coordinate from the set rather than considering all possible points in the 2-dimensional plane, effectively identifying scalar multiples of our representative.

The projective line over $\mathbb{F}_q$ contains $q + 1$ points. The composition of these points and their representatives for $\mathbb{F}_p$ for some prime p is as given in table 2.1. More generally the points are $(1, x)$ for x in the field and $(0, 1)$.

Code	Span of
0	$(1,0)$
1	$(1,1)$
$\vdots$	$\vdots$
$p-1$	$(1,p-1)$
∞	$(0,1)$

Table 2.1: Elements of Projective Line over $\mathbb{F}_p$

We have a few well known facts regarding $PSL(2,q)$ which can be found in Huppert [13], and are collated in the following Lemma.

Lemma 2.1.1. *For $G \cong PSL(2,q)$, $q = p^a$, acting on the projective line Ω and letting $d = gcd(2, q-1)$. we have*

(i) $|G| = \frac{q(q+1)(q-1)}{d}$.

(ii) *G acts 2-transitively on Ω.*

(iii) *G contains cyclic subgroups $H_- = \langle h_- \rangle$ and $H_+ = \langle h_+ \rangle$ where $|H_-| = \frac{q-1}{d}$ and $|H_+| = \frac{q+1}{d}$.*

Let $P \in Syl_pG$, and set $\mathcal{S} = \{P^g, H_-^g, H_+^g \mid g \in G\}$. Then every non-identity element of G belongs to a unique subgroup in $\mathcal{S}$.

(iv) *h_- has cycle type $\left(\frac{q-1}{d}\right)^d$ on Ω and h_+ has cycle type $\left(\frac{q+1}{d}\right)^d$ on Ω. For $1 \neq x \in P$, x has cycle type $p^{p^{a-1}}$ on Ω.*

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

(vi) $[G : N_G(H_-)] = \frac{q(q+1)}{2}$ *and* $[G : N_G(H_+)] = \frac{q(q-1)}{2}$.

Proof. For parts $(i) - (iv)$ see 8.1 Hilfssatz and for (iii), (iv) and (vi) consult 8.3, 8.4, 8.5 Satz of [13]. Part (v) is given in 8.2 Satz (b) and (c) of [13]. □

We will also make use of the fact the $PSL(2,q)$ is 3-homogeneous if and only if $q \equiv 3 \bmod 4$. This is another standard result and can be found in many texts for example see [5], however we do not include a proof of it here as we derive a new proof later in Corollary 4.1.3.

2.2 $PSL(2,7)$

We begin be defining explicitly all the images on the projective line in this case.

Code	Representative	Projective line points
0	$\langle(1,0)\rangle$	$\{(1,0),(2,0),(3,0),(4,0),(5,0),(6,0)\}$
1	$\langle(1,1)\rangle$	$\{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6)\}$
2	$\langle(1,2)\rangle$	$\{(1,2),(2,4),(3,6),(4,1),(5,3),(6,5)\}$
3	$\langle(1,3)\rangle$	$\{(1,3),(2,6),(3,2),(4,5),(5,1),(6,4)\}$
4	$\langle(1,4)\rangle$	$\{(1,4),(2,1),(3,5),(4,2),(5,6),(6,3)\}$
5	$\langle(1,5)\rangle$	$\{(1,5),(2,3),(3,1),(4,6),(5,4),(6,2)\}$
6	$\langle(1,6)\rangle$	$\{(1,6),(2,5),(3,4),(4,3),(5,2),(6,1)\}$
∞	$\langle(0,1)\rangle$	$\{(0,1),(0,2),(0,3),(0,4),(0,5),(0,6)\}$

Table 2.2: Elements of Projective Line over $\mathbb{F}_7$

So we have the G-set

$$\begin{aligned}\Omega &= \{\langle(1,0)\rangle, \langle(1,1)\rangle, \langle(1,2)\rangle, \langle(1,3)\rangle, \langle(1,4)\rangle, \langle(1,5)\rangle, \langle(1,6)\rangle, \langle(0,1)\rangle\} \\ &= \{0,1,2,3,4,5,6,\infty\}.\end{aligned}$$

By coding the elements we can easily determine the $\binom{8}{3} = 56$ unordered subsets which make up Ω_3.

We begin by constructing $SL(2,7)$ as a subgroup of the General Linear Group $GL(2,7)$.

$$|GL(2,7)| = (7^2-1)(7^2-7) = 1968,$$

Only taking the elements of $GL(2,7)$ with determinant 1, we have $SL(2,7)$.

$$|SL(2,7)| = 336.$$

The elements of the centre ($Z(SL(2,7))$) are the matrices $\pm I$. The factor group $\frac{SL(2,7))}{Z(SL(2,7))}$ is called $PSL(2,7)$ and this group acts upon the 8 points of Ω by multiplication.

$$|PSL(2,7)| = \frac{|SL(2,7)|}{|Z(SL(2,7))|} = \frac{336}{2} = 168 = 2^3.3.7.$$

2.2.1 Number of Orbits when $k = 3$

As $q \equiv 3 \bmod 4$ we know that $PSL(2,7)$ is 3-homogeneous on 8 points and so $\sigma_1 = \sigma_2 = \sigma_3 = 1$.

However we pursue a more practical approach to determine a more general solution, but we also wish to deal with the two groups $PSL(2,7)$ and $PSL(2,11)$ in a more detailed way to gain further understanding of them.

We start by letting $G \cong PSL(2,7)$, we know that $3|168$ and so by Cauchy's Theorem there exists a $g \in G$ such that $H = \langle g \rangle$ and $|H| = 3$.

We know that G is 2 transitive on Ω and so for $\alpha, \beta \in \Omega$ $(\alpha \neq \beta)$ the H orbit of

$$(\alpha, \beta)^H = \{(\alpha, \beta), (\alpha', \beta'), (\alpha'', \beta'')\},$$

if all these elements are all different from each other, then we have H fixing 2 of the 8 elements of Ω. That is $|\text{fix}_\Omega(g)| \geq 2$, we know however that if $|\text{fix}_\Omega(g)| > 2$ then g cannot have order 3 so $|\text{fix}_\Omega(g)| = 2$.

Choosing an element of order 2 we can see that all the involutions are in the conjugates of subgroup H_+ described in Lemma 2.1.1 meaning all such elements have cycle type 2^4 and hence no element of order 2 can stabilize a 3 point set. We remark also that no element of order 7 can stabilize a 3-subset.

We now know that $Stab_G\{\alpha, \beta, \gamma\}$ contains elements of order 3 but no element of order 2 or 7 so $|Stab_G\{\alpha, \beta, \gamma\}| = 3$. Then by the Orbit Stabilizer Theorem the length of orbit is $\frac{168}{3} = 56 = \binom{8}{3}$, as required and $PSL(2,7)$ is 3-homogeneous.

2.2.2 Number of Orbits when $k = 4$

We know from the Livingstone-Wagner Theorem that we will have at least as many orbits for 4 subsets as we had for 3, this is clear as for $k = 3$ we only obtained one orbit, however if recall Ω_4 denotes the set of all 4-subsets of Ω, we can see that $|\Omega_4| = \binom{8}{4} = 70$ and as this is not a divisor of $|G|$ we certainly cannot have a single orbit.

If we let $\Delta_1 = \{\alpha, \beta, \gamma, \delta\}$ with $\alpha, \beta, \gamma, \delta \in \Omega$ then we denote the orbit containing Δ_1 by Δ_1^G. We wish to calculate $|\Delta_1^G|$ and so we use the Orbit Stabilizer Theorem and calculate $|G_{\Delta_1}|$.

Clearly Δ_1^G has length less than 70, so we can begin by writing a list of divisors of $|G| = 168$ as potential orders of G_{Δ_1} noting that the order is necessarily greater than 2. This gives us the following possibilities

$$|G_{\Delta_1}| \in \{56, 42, 28, 24, 21, 14, 12, 8, 7, 6, 4, 3\}.$$

Elements of order 7

An element of order 7 does not fix all 8 points of Ω and so cannot stabilize any 4-subset of Ω. If G_{Δ_1} were a multiple of 7, then by Cayley's Theorem it would contain such an element, hence $7 \nmid |G_{\Delta_1}|$. So we have the following possibilities remaining,

$$|G_{\Delta_1}| \in \{24, 12, 8, 6, 4, 3\}.$$

Elements of order 3

Let $g \in G$ have order 3. Then $|\text{fix}_\Omega(g)| = 2$ and so we know the cycle structure of g is $(\alpha_1, \alpha_2, \alpha_3)(\alpha_4, \alpha_5, \alpha_6)(\alpha_7)(\alpha_8)$ with $\alpha_i \in \Omega$. Choosing $g = \begin{bmatrix} 2 & 0 \\ 4 & 4 \end{bmatrix}$ we have that g can be written as the permutation $(1, 3, \infty)(2, 5, 6)(0)(4)$.

Letting $\alpha = 2$, $\beta = 5$, $\gamma = 6$, and $\delta = 0$ in Δ_1, we can see that $g \in G_{\Delta_1}$ and so we have

$$|G_{\Delta_1}| \in \{24, 12, 6, 3\}.$$

Elements of order 2

As involutions in G transpose pairs of points in Ω we can write $h = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$ as the permutation $(1, 3)(0, 5)(4, \infty)(2, 6)$ and we can see that h stabilizes Δ_1 and so

$$|G_{\Delta_1}| \in \{24, 12, 6\}.$$

We now have some elements which we know are in the subgroup, G_α, and so we can use these to generate further elements. Indeed $\langle g, h \rangle$ expressed as permutations in $Sym(\Omega)$ subgroup is a subgroup with order 12, so

$$|G_{\Delta_1}| \in \{24, 12\}.$$

Sylow 2-subgroups

If $|G_{\Delta_1}| = 24$ then clearly $Syl_2 G_{\Delta_1} \subset Syl_2 G$. However the Sylow 2-subgroups of $SL(2, 7)$ are generalised quarternion groups

$$\left\langle x, y | x^8 = y^4 = 1, y^{-1}xy = x^{-1} \right\rangle.$$

However we have Sylow 2-subgroups of order 8 in $PSL(2,7)$ which are of the form

$$\left\langle x, y | x^4 = y^2 = 1, y^{-1}xy = x^{-1} \right\rangle,$$

which is the group D_8.

This group is transitive on Ω and as all Sylow 2-subgroups are conjugate we must have that for all $P \in Syl_2G$, $P \not\leq G_{\Delta_1}$ We must have it then that $8 \nmid |G_{\Delta_1}|$ and so $|G_{\Delta_1}| = 12$ and hence $|\Delta_1^G| = 14$.

A similar argument shows that for $\Delta_2 = \{2, 4, 5, 6\}$ we have that $|\Delta_2^G| = 14$ also. Calculating points in Δ_1^G and Δ_2^G shows these two orbits are disjoint.

If we take the point $\Delta_3 = \{0, 1, 2, 3\} \in \Omega_4$, it can be shown that none of the 56 elements of order 3 stabilize Δ_3.

This means that $|\Delta_3^G| \leq 70 - 28 = 42$, and also that $3 \nmid |G_{\Delta_3}|$ so we have the following choices,

$$|G_{\Delta_3}| \in \{56, 28, 14, 8, 7, 4\}.$$

We have seen that 7 and 8 cannot divide the order and so we have that

$$|G_{\Delta_3}| = 4.$$

This gives us that $|\Delta_3^G| = \frac{168}{4} = 42$.

Hence $PSL(2,7)$ has three orbits of length 14, 14 and 42 on Ω_4.

2.3 $PSL(2,11)$

Let $G = PSL(2,11)$ and as before we begin by outlining the representatives of the corresponding projective line, here over $\mathbb{F}_{11}$.

We have that $|PSL(2,11)| = \frac{(11^2-1)(11^2-11)}{2(11-1)} = \frac{120\times110}{20} = 660 = 11 \cdot 5 \cdot 3 \cdot 2 \cdot 2$

2.3.1 Number of orbits when $k = 3$

Note that $|\Omega_3| = \binom{12}{3} = 220$. Let Δ be an element of Ω_3.

Elements of order 11

An element of order 11 has cycle type 11^1 and so clearly cannot stabilize a point in Ω_3. So we must have, by Cauchy's Theorem, that $11 \nmid |G_\Delta|$.

Code	Rep	Projective line points
0	$\langle(1,0)\rangle$	$\{(1,0),(2,0),(3,0),(4,0),(5,0),(6,0),(7,0),(8,0),(9,0),(10,0)\}$
1	$\langle(1,1)\rangle$	$\{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6)(7,7),(8,8),(9,9),(10,10)\}$
2	$\langle(1,2)\rangle$	$\{(1,2),(2,4),(3,6),(4,8),(5,10),(6,1),(7,3),(8,5),(9,7),(10,9)\}$
3	$\langle(1,3)\rangle$	$\{(1,3),(2,6),(3,9),(4,1),(5,4),(6,7),(7,10),(8,2),(9,5),(10,8)\}$
4	$\langle(1,4)\rangle$	$\{(1,4),(2,8),(3,1),(4,5),(5,9),(6,2),(7,6),(8,10),(9,3),(10,7)\}$
5	$\langle(1,5)\rangle$	$\{(1,5),(2,10),(3,4),(4,9),(5,3),(6,8),(7,2),(8,7),(9,1),(10,6)\}$
6	$\langle(1,6)\rangle$	$\{(1,6),(2,1),(3,7),(4,2),(5,8),(6,3),(7,9),(8,4),(9,10),(10,5)\}$
7	$\langle(1,7)\rangle$	$\{(1,7),(2,3),(3,10),(4,6),(5,2),(6,9),(7,5),(8,1),(9,8),(10,4)\}$
8	$\langle(1,8)\rangle$	$\{(1,8),(2,5),(3,2),(4,10),(5,7),(6,4),(7,1),(8,9),(9,6),(10,3)\}$
9	$\langle(1,9)\rangle$	$\{(1,9),(2,7),(3,5),(4,3),(5,1),(6,10),(7,8),(8,6),(9,4),(10,2)\}$
10	$\langle(1,10)\rangle$	$\{(1,10),(2,9),(3,8),(4,7),(5,6),(6,5),(7,4),(8,3),(9,2),(10,1)\}$
∞	$\langle(0,1)\rangle$	$\{(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7),(0,8),(0,9),(0,10)\}$

Table 2.3: Elements of Projective Line over $\mathbb{F}_{11}$

Elements of order 5

Let $g \in G$ have order 5, then g contains two 5 cycles and fixes two points when acting on Ω (this follows from Lemma 2.1.1) and clearly it cannot stabilize Δ and hence $5 \nmid |G_\Delta|$.

Elements of order 3

Clearly in the case of g having order 3 we must have g containing four 3-cycles. Choosing $g = \begin{bmatrix} 2 & 2 \\ 4 & 10 \end{bmatrix}$ we can see that as a permutation on Ω,

$$g = (0,1,2)(3,7,9)(4,6,10)(5,\infty,8).$$

Hence we can define $\Delta = \{0,1,2\}$ and so $g \in G_\Delta$ and so $3 \big| |G_\Delta|$.

Elements of order 2

An element of order 2 has cycle type 2^6 on Ω and so cannot stabilize a 3-subset. Hence $2 \nmid |G_\Delta|$.

We have then that $|G_\Delta| = 3$ and so $|\Delta^G| = 220$ and $PSL(2,11)$ is 3-homogeneous as expected.

2.3.2 Number of Orbits when $k = 4$

Let $\Delta_1 = \{\alpha, \beta, \gamma, \delta\}$ where $\alpha, \beta, \gamma, \delta \in \Omega$.

Here we allow $PSL(2,11)$ to act on Ω_4, where $|\Omega_4| = \binom{12}{4} = \frac{11880}{24} = 495$.

Elements of order 11, 5 **or** 3

We have seen the cycle structure of these elements and clearly no such element can stabilize Δ_1 and hence none of 3, 5, and 11 can divide $|G_{\Delta_1}|$.

Elements of order 2

Clearly 2 must divide the order of the stabilizer, otherwise then we would have the contradiction that $|\Delta_1^G| > |\Omega_4|$.

If 4 divides the order of the stabilizer then G_{Δ_1} contains a Sylow 2-subgroup, P with order 4, however $PSL(2,11)$ does not contain an element of order 4 by Lemma 2.1.1 and so P must be a Klien 4 group.

Taking the matrix representations of elements $g = \begin{bmatrix} 0 & 1 \\ 10 & 0 \end{bmatrix}$ and $h = \begin{bmatrix} 1 & 8 \\ 8 & 10 \end{bmatrix}$, we can see that g and h are commuting involutions in $PSL(2,11)$. Therefore they generate a Sylow 2-subgroup of G.

Writing each as a permutation, we see that $g = (0,\infty)(1,10)(2,5)(3,7)(4,8)(6,9)$ and $h = (0,8)(1,2)(3,9)(4,\infty)(5,10)(6,7)$ and so g and h stabilize the set $\Delta_1 = \{0,4,8,\infty\}$. Hence $4\big||G_{\Delta_1}|$ and so $|G_{\Delta_1}| = 4$, giving $|\Delta_1^G| = \frac{660}{4} = 165$.

The above argument tells us that the size of the stabilizer for any element of Ω_4 can only be either 2 or 4. It follows that we have only two possibilities for the orbit lengths, that is 165 or 330. Hence, this leaves only two possible partitions of Ω_4, that is Ω_4 is the disjoint union of two orbits of length 165 and 330, or Ω_4 is the disjoint union of three orbits all of length 165.

Using the Orbit-Counting Theorem (1.0.4) we have either

$$2|G| = 1320 = \sum_{g\in G} |\mathrm{fix}_{\Omega_4}(g)| \qquad \text{or} \qquad 3|G| = 1980 = \sum_{g\in G} |\mathrm{fix}_{\Omega_4}(g)|.$$

Now, by the above we know that the only elements of G to fix points in Ω_4 are the identity and involutions. The identity fixes all 495 points and any involution will fix $\binom{6}{2} = 15$ subsets.

Using Lemma 2.1.1(iii) and (v) we can determine there are 55 involutions stabilizing the maximum number of subsets and so we have $\sum_{g\in G} |\mathrm{fix}_{\Omega_4}(g)| = (55\times 15)+495 =$

1320. Moreover we have that $PSL(2,11)$ has precisely two orbits on 4-subsets, one of length 165 and one of length 330.

2.3.3 Number of orbits when $k = 5$

Let $\Delta_1 = \{\alpha, \beta, \gamma, \delta, \epsilon\}$ where $\alpha, \beta, \gamma, \delta, \epsilon \in \Omega$.

Here we allow $G = PSL(2,11)$ to act on Ω_5, where $|\Omega_5| = \binom{12}{5} = \frac{95040}{120} = 792 = 2^3 \cdot 3^2 \cdot 11$.

Elements of prime order

We have seen the cycle structures of the elements of order, 11, 3 and 2 and we can clearly see that these group elements cannot stabilize Δ_1.

We must have then that $|G_{\Delta_1}| = 5$, for some choice of Δ_1 as elements of order 5 exist and trivially must fix two points in Ω_5.

$$|\Delta_1^G| = \frac{660}{5} = 132$$

for some $\Delta_1 \in \Omega_5$.

Now we can calculate the number of elements of order 5. Using Sylow's Theorems we can quickly determine the number of Sylow 5-subgroups is either 6, 11 or 66. Now each $P \in Syl_5(G)$ contains 4 non-identity elements. We know at that each will fix 2 points in Ω_5, that is $\sum_{g \in P^\#} |\mathrm{fix}_\Omega(g)| = 8$ but we have 132 points with such a stabilizer. It follows that if the number of Sylow 5 subgroups is 6 or 11, then we could only have

$$\sum_{P \in Syl_5(G)} \sum_{g \in P^\#} |\mathrm{fix}_\Omega(g)|$$

equal to 48 or 88 respectively. It must be then that $PSL(2,11)$ has 264 elements of order 5, each stabilizing two 5 subsets. Therefore the number of 5-subsets that can be stabilized by these elements is 528. As there are 792 choices for Δ, there must exist an element which is not stabilized by any non identity element and hence has a regular orbit of length $|G| = 660$. This gives us two orbits with sizes $660 + 132 = 792$ and so there are no more orbits.

We collate the results of this chapter in the following table, with the addition of calculations for $\sigma_6(PSL(2,11))$ and $\sigma_k(PSL(2,13))$ which were determined by MAGMA.

k	$PSL(2,7)$	$PSL(2,11)$	$PSL(2,13)$
1	8	12	14
2	28	66	91
3	56	220	182, 182
4	14, 14, 42	165, 330	91, 91, 273, 546
5		132, 660	182, 182, 546, 546, 546
6		110, 110, 110, 132, 132, 330	91,91,91,546,546,546,1092
7			78,78,182,182,364,364,546,546,546,546

Table 2.4: Length of Orbits

As q increases the amount of time taken to calculate the number of orbits increases dramatically and so relying on computer programmes to give an answer is necessary. However due to the size of the group this is also a short term solution as computer memory is quickly used when performing direct calculation on constructions of these groups. We therefore pursue a formula which will allow us to find the value of σ_k given only the values of q and k. This gives the motivation for the next chapter.

We notice from the results in Table 2.4 that the three groups $PSL(2,7)$, $PSL(2,11)$ and $PSL(2,13)$ all have a k-subset of their respective G sets which have larger orbits that any $(k+1)-$subset containing it, this happens at respectively $k = 3, 5, 6$. This is a characteristic discussed by Siemons and Wagner [27] in their 1988 paper "On the relationship between the lengths of orbits on k-sets and $(k+1)$-sets", where they discuss the Livingstone Wagner Theorem and explore the notion that a similar relationship is likely when considering lengths of orbits as opposed to the number of orbits.

They hypothesised that the property mentioned on orbit lengths is rare and went on to classify groups where this occurred for $k = 2$.

Chapter 3

Finite simple groups of Lie Rank one

It is well known which groups fall into the category of being rank 1 simple groups of Lie type, these are classified via their Dynkin diagrams into one of four possible families. Wilson gives each of these types an excellent introduction in "The Finite Simple Groups" [37].

We begin this chapter with a lemma which will serve us well throughout our calculations and will allow us to determine the number of elements of a given order in a cyclic group.

3.1 Preliminary Results

Lemma 3.1.1. *Let $m, n \in \mathbb{N}$, $m \neq 1$, be such that $m \mid n$ and let $H \cong \mathbb{Z}_n$. If $p_1, p_2, ..., p_r$ are the distinct prime divisors of m, then the number of elements in H of order m is*

$$\phi(m) = \frac{m}{p_1 p_2 ... p_r}(p_1 - 1)(p_2 - 1)...(p_r - 1).$$

Proof. Since H contains a unique cyclic subgroup H_0 of order m, all elements of order m in H will be contained in H_0. The number of elements of order m in H_0 is the number of $\ell \in \{1, 2, ..., m\}$ which are coprime to m and this, by definition, is Euler's function, $\phi(m)$. The stated formula for $\phi(m)$ is given as Theorem 7.5 in [26]. □

Before stating our main results we must introduce some notation. For $b, c \in \mathbb{N}$, we

use (b, c) to denote the greatest common divisor of b and c. Put $q = p^a$ where p is a prime and $a \in \mathbb{N}$. For $\ell \in \mathbb{N}$ we let

$$\mathcal{D}(\ell) = \{n \in \mathbb{N} |\ n \text{ divides } \ell\}$$

and write $\mathcal{D}^*(\ell) = \mathcal{D}(\ell) \setminus \{1\}$. Also due to Lemma 3.1.1 Euler's phi function ϕ (see [26]) will feature in our results. Our final piece of notation concerns partitions. Let $n \in \mathbb{N}$, and let $\pi = \lambda_1\lambda_2...\lambda_r$ where $\lambda_1 \leq \lambda_2 \leq ... \leq \lambda_r$ and $\sum_{i=1}^{r} \lambda_i = n$. Though we will frequently use the more compressed notation $\pi = \mu_1^{a_1}\mu_2^{a_2}...$ where $\mu_1 < \mu_2 < ...$ (a_i being the multiplicity of μ_i). For $k \in \mathbb{N}$, $\eta_k(\pi)$ is defined to be the number of subsequences $\lambda_{i_1}, \lambda_{i_2}, ..., \lambda_{i_l}$ of $\lambda_1, ..., \lambda_r$ which form a partition of k.

As an example consider $\pi = 1\ 1\ 4\ 4\ 4$ ($= 1^2 4^3$ in compressed form), a partition of $n = 14$. Then $\eta_5(\pi) = 6$, $\eta_6(\pi) = 3$, $\eta_7(\pi) = 0$ and $\eta_8(\pi) = 3$. Our interest in $\eta_k(\pi)$ is because of the following two simple lemmas.

Lemma 3.1.2. *Suppose $g \in Sym(\Omega)$ where $|\Omega| = n$, and let $k \in \mathbb{N}$. If g has cycle structure π on Ω (viewed as a partition of n), then g fixes $\eta_k(\pi)$ k-subsets of Ω.*

Lemma 3.1.3. *Let $\pi = \mu_1^{a_1}\mu_2^{a_2}...\mu_s^{a_s}$ be a partition of n (in compressed form). Then*

$$\eta_k(\pi) = \prod_{(k_1,k_2,...,k_s)} \binom{a_1}{k_1}\binom{a_2}{k_2}...\binom{a_s}{k_s},$$

running over all s-tuples $(k_1, k_2, ..., k_s)$ with $k_i \geq 0$ and $\mu_1 k_1 + \mu_2 k_2 ... + \mu_s k_s = k$.

We will freely identify a cycle type of an element with a partition of n. When we wish to emphasise the element used we may write π_g for $g \in G$.

3.2 Projective Special Linear Groups $PSL(2, q)$

The first family of doubly-transitive rank one simple groups of Lie type we are concerned with are projective special linear groups, $PSL(2, q)$, which are of type A_1. We now recall some of our notation for ease of reference.

We note that G acts upon $\Omega = PG(1, q)$, the projective line, and for $k \in \mathbb{N}$ we let $\sigma_k(G, \Omega)$ denote the number of orbits G has upon Ω_k, the set of all k element subsets of Ω.

Suppose that $q = p^a$ where p is a prime and $a \in \mathbb{N}$. Let $G = PSL(2,q)$, the two dimensional projective special linear group over $\mathbb{F}_q$. Set d to be the greatest common divisor of 2 and $q-1$. So $d = 1$ if q is even and $d = 2$ if q is odd.

We recall Lemma 2.1.1 below as it is used heavily in the proof of our next Theorem.

Lemma 2.1.2 *For $G \cong PSL(2,q)$ acting on the projective line, Ω, we have*

(i) $|G| = \frac{q(q+1)(q-1)}{d}$ *where* $d = (2, q-1)$.

(ii) *G acts 2 transitively on Ω.*

(iii) *G contains cyclic subgroups $H_- = \langle h_- \rangle$ and $H_+ = \langle h_+ \rangle$ where $|H_-| = \frac{q-1}{d}$ and $|H_+| = \frac{q+1}{d}$.*

Let $P \in Syl_p G$, and set $\mathcal{S} = \{P^g, H_-^g, H_+^g \mid g \in G\}$. Then every non-identity element of G belongs to a unique subgroup in $\mathcal{S}$.

(iv) *h_- has cycle type $\left(\frac{q-1}{d}\right)^d$ on Ω and h_+ has cycle type $\left(\frac{q+1}{d}\right)^d$ on Ω. For $1 \neq x \in P$, x has cycle type $p^{p^{a-1}}$ on Ω.*

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

(vi) $[G : N_G(H_-)] = \frac{q(q+1)}{2}$ *and* $[G : N_G(H_+)] = \frac{q(q-1)}{2}$.

Theorem 3.2.1. *Suppose that $G \cong PSL(2,q)$ $(q > 3)$ acts upon the projective line Ω, and let $k \in \mathbb{N}$ with $k \geq 3$. Set $d = (2, q-1)$. Then*

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

Remark Since G acts 2-transitively on Ω, $\sigma_1(G,\Omega) = \sigma_2(G,\Omega) = 1$.

Proof. Let Ω_k be the set of all k-subsets of Ω. Suppose $k \in \mathbb{N}$ with $k \geq 3$, and let $1 \neq g \in G$ $(\cong PSL(2,q))$ be an element of order m. Then by Lemma 2.1.1 *(iii)* g

must be contained (uniquely) in a conjugate of one of P, H_- and H_+. Since we seek to determine $|\mathrm{fix}_{\Omega_k}(g)|$ we may suppose that g is contained in one of P, H_- and H_+.

First we consider the case when $g \in H_+$. Since g is some power of h_+, by Lemma 2.1.1 (iv), g has cycle type $m^{\frac{q+1}{m}}$. By Lemmas 3.1.1 and 2.1.1 (vi) H_+ contains $\phi(m)$ elements of order m and there are $\frac{q(q-1)}{2}$ conjugates of H_+, hence these elements contribute

$$\frac{q(q-1)}{2} \sum_{m \in \mathcal{D}^*(\frac{q+1}{d})} \phi(m)\eta_k\left(m^{\frac{q+1}{m}}\right)$$

to the sum $\sum_{g\in G} |\mathrm{fix}_{\Omega_k}(g)|$. Now consider the case when $g \in H_-$. As g is a power of h_-, by Lemma 2.1.1 (iv), g has cycle type $1^2 m^{\frac{q-1}{m}}$. Employing Lemmas 3.1.1 and 2.1.1 (vi) we obtain

$$\frac{q(q+1)}{2} \sum_{m \in \mathcal{D}^*(\frac{q-1}{d})} \phi(m)\eta_k\left(1^2 m^{\frac{q-1}{m}}\right),$$

in the sum $\sum_{g\in G} |\mathrm{fix}_{\Omega_k}(g)|$. Similar considerations for $g \in P$, using Lemma 2.1.1, yield

$$(q-1)(q+1)\eta_k(1^1 p^{\frac{q}{p}}).$$

Combining the above with Lemmas 1.0.4 and 2.1.1 (i) we obtain the expression for $\sigma_k(G, \Omega)$. □

For the benefit of the reader we present here MAGMA code for this formula,

```
PSLsig:=procedure(q,k,~sigma);
Z:=Integers();d:=GreatestCommonDivisor(q-1,2);
P:=PrimeDivisors(q);p:=P[1];sig:=0;
I:=(d/(q*(q+1)*(q-1)))*Binomial(Z!(q+1),k);
CC:=[]; Append(~CC,[<(d/q),1>,<p,Z!(q/p)>,<1,1>]);
for m in Divisors(Z!((q+1)/d)) do if m ne 1 then
Append(~CC,[<(d/(2*(q+1))),EulerPhi(m)>,<m,Z!((q+1)/m)>]);
end if;end for;
for m in Divisors(Z!((q-1)/d)) do if m ne 1 then
Append(~CC,[<(d/(2*(q-1))),EulerPhi(m)>,<m,Z!((q-1)/m)>,<1,2>]);
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;end procedure;
```

This is repeated in the Appendix (along with the other formulae) for ease of reference.

We now move on from $PSL(2,q)$ and look at applying our methods to the second family of groups on our list.

3.3 Suzuki Groups $Sz(q)$

The second family of doubly-transitive rank one simple groups of Lie type we are concerned with are the Suzuki groups, $Sz(q)$, which are the first of our three families of "twisted" type and are classified as ${}^2B_2$.

Suppose $q = 2^{2n+1}$, $n \in \mathbb{N}$. Let $G = Sz(q)$, one of the family of Suzuki groups which acts upon Ω, an ellipse in 3-dimensional projective space over $GF(q)$ consisting of q^2+1 points. Let r be such that $r^2 = 2q$, then the following Lemma comes from Suzuki [33].

Lemma 3.3.1. *(i)* $|G| = q^2(q-1)(q^2+1)$.

(ii) Only the identity fixes three points.

(iii) G acts 2 transitively on Ω.

(iv) G contains cyclic subgroups $H_0 = \langle h_0 \rangle$, $H_- = \langle h_- \rangle$ and $H_+ = \langle h_+ \rangle$ where $|H_0| = q-1$, $|H_-| = q-r+1$ and $|H_+| = q+r+1$.

Let $P \in Syl_2 G$, and set $\mathcal{S} = \{P^g, H_0^g, H_-^g, H_+^g \mid g \in G\}$. Then every non-identity element of G belongs to a unique subgroup in $\mathcal{S}$.

(v) $|N_G(H_0)| = 2(q-1)$, $|N_G(H_-)| = 4(q-r+1)$ *and* $|N_G(H_+)| = 4(q+r+1)$.

(vi) $|N_G(P)| = q^2(q-1)$ *and* P *contains* $q-1$ *elements of order* 2 *and* q^2-q *elements of order* 4.

Theorem 3.3.2. *Suppose* $G \cong Sz(q)$ $(q = 2^{2n+1} > 2)$, $n \in \mathbb{N}$, *acts upon the Suzuki oval* Ω. *Let* $r \in \mathbb{N}$ *be such that* $r^2 = 2q$, *and let* $k \in \mathbb{N}$ *with* $k \geq 3$. *Then*

$$\begin{aligned}\sigma(G,\Omega) &= \frac{1}{q^2(q-1)(q^2+1)}\eta_k(1^{q^2+1}) + \frac{1}{q^2}\eta_k(1^1 2^{\frac{q^2}{2}}) \\ &\quad + \frac{1}{q}\eta_k(1^1 4^{\frac{q^2}{4}}) + \frac{1}{2(q-1)} \sum_{m \in \mathcal{D}^*(q-1)} \phi(m)\eta_k(1^2 m^{\frac{q^2-1}{m}}) \\ &\quad + \frac{1}{4(q+r+1)} \sum_{m \in \mathcal{D}^*(q+r+1)} \phi(m)\eta_k(m^{\frac{q^2+1}{m}}) \\ &\quad + \frac{1}{4(q-r+1)} \sum_{m \in \mathcal{D}^*(q-r+1)} \phi(m)\eta_k(m^{\frac{q^2+1}{m}}).\end{aligned}$$

Proof. We establish the formula by considering the cycle types of all elements $g \in G$ and then calculating $|\mathrm{fix}_{\Omega_k}(g)| = \eta(\pi_g)$ we substitute the values into Theorem 1.0.4 to resolve our count.

Let Ω_k denote the set of all k-element subsets of Ω. Suppose $3 \leq k \leq \frac{\Omega}{2}$. Let $g \in G^*$ have order m, then by Lemma 3.3.1 we have that g will belong to a unique conjugate of one of P, H_0, H_- or H_+. Since we wish to determine $\eta_k(\pi_g)$, where π_g is the cycle type of g, we may assume that g is contained in one of the given subgroups.

If $g \in H_+$, then as g is some power of h_+, g has cycle type $m^{\frac{q^2+1}{m}}$, where $m \in \mathcal{D}(2^{2n+1}+r+1)$. This can be seen as only the identity fixes three points and $|H_+|\big|q^2+1$ $(2^{4n+2}+1 = (2^{2n+1}+2^{n+1}+1)(2^{2n+1}-2^{n+1}+1))$. We now have that such elements together with their conjugates will contribute

$$\frac{1}{4(q+r+1)} \sum_{m \in \mathcal{D}^*(q+r+1)} \phi(m)\eta_k(m^{\frac{q^2+1}{m}})$$

to the total by Lemma 3.3.1. Similarly if $g \in H_-$ we have an identical argument that g will have cycle type $m^{\frac{q^2+1}{m}}$, where $m \in \mathcal{D}(2^{2n+1}-r+1)$, and so these elements and their conjugates will contribute

$$\frac{1}{4(q-r+1)} \sum_{m \in \mathcal{D}^*(q-r+1)} \phi(m)\eta_k(m^{\frac{q^2+1}{m}})$$

to our count.

Next we consider $g \in H_0$, then g is a power of h_0 which has odd order $q-1$. However as $q-1 \big| q^2-1$ we necessarily must have two fixed point of Ω for each power of h_0. This implies the cycle type of $g \in H_0$, where g has order m, is $m^{\frac{q^2-1}{m}}1^2$. Again we use Lemma 3.3.1, to show that such elements together with their conjugates will contribute

$$\frac{1}{2(q-1)} \sum_{m \in \mathcal{D}^*(q-1)} \phi(m)\eta_k(1^2 m^{\frac{q^2-1}{m}})$$

to our count.

This leaves us with the possibility $g \in P$, and so will have order either 4 or 2, we note that neither 4 nor 2 will divide $2^{2n+1}+1$ and so we must have elements with fixed points. Clearly elements of order 4 will square to involutions and so this dictates they can only have one fixed point in Ω and the remaining cycles must all be of length 4 giving us cycle type $4^{\frac{q^2}{4}}1^1$, similarly if g has order 2, then it must have at least one fixed point in Ω. However g cannot have 2 fixed points as $2 \nmid q^2-1$, hence these elements must have cycle type $2^{\frac{q^2}{2}}1^1$.

Combining these with the number of such elements and the information in Lemma 3.3.1 these two types of elements will give a contribution of $\frac{1}{q^2}\eta_k(1^1 2^{\frac{q^2}{2}})$ and $\frac{1}{q}\eta_k(1^1 4^{\frac{q^2}{4}})$ to the count.

Finally we include the number of k-subsets fixed by the identity and divide this by $|G|$ to complete the proof. □

Again we include the MAGMA code for implementing Theorem 3.3.2.

```
Suzsig:=procedure(q,k,~sigma);
Z:=Integers();R:=2*q;r:=SquareRoot(R);
sig:=0;
CC:=[]; I:=(1/(q^2*(q^2+1)*(q-1)))*Binomial(Z!(q^2+1),k);
 Append(~CC,[<(1/q^2),1>,<2,Z!(q^2/2)>,<1,1>]);
 Append(~CC,[<(1/q),1>,<4,Z!(q^2/4)>,<1,1>]);
 for m in Divisors(Z!((q-1))) do if m ne 1 then
 Append(~CC,[<(1/(2*(q-1))),EulerPhi(m)>,<m,Z!((q^2-1)/m)>,<1,2>]);
 end if;end for;t1:=Z!(q+r+1);t2:=Z!(q-r+1);
for m in Divisors(Z!((q+r+1))) do if m ne 1 then
Append(~CC,[<1/(4*t1),EulerPhi(m)>,<m,Z!((q^2+1)/m)>]);
```

```
end if;end for;
for m in Divisors(Z!((q-r+1))) do if m ne 1 then
Append(~CC,[<1/(4*t2),EulerPhi(m)>,<m,Z!((q^2+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;end procedure;
```

3.4 Projective Special Unitary Groups $PSU(3,q)$

The third family of doubly-transitive rank one simple groups of Lie type we are concerned with are the projective special unitary groups, $PSU(3,q)$, which are the second of our three families of "twisted" type and are classified as ${}^2A_2$.

We commence this section with a short expository account of this family of groups which can be found in Dixon and Mortimer [10] (or Wilson [37]). We let $q = p^a$ for some prime p and $a \in \mathbb{N}$. We also let $K = \mathbb{F}_{q^2}$ and V be the 3-dimensional vector space over K. Letting τ be the automorphism of K such that $\alpha^\tau = \alpha^q$ for $\alpha \in K$, we have that $\tau^2 = 1$.

We may use τ and a scalar product $(\cdot,\cdot)$ to define a Hermitian form $\phi : V \times V \mapsto K$, $\alpha, \beta \in K$ and $u, v \in V$ such that

$$\phi(\alpha u, \beta v) = \alpha\beta^q(u,v)$$

and

$$(u,v) = (v,u)^q.$$

We may then define the unitary group $GU(3,q)$ to be a subgroup of $GL(3,q^2)$ where for $g \in GL(3,q^2)$ we have $g \in GU(3,q)$ if and only if $\phi(u,v) = \phi(u^g, v^g)$ for all $u, v \in V$.

Taking the induced action on 1-dimensional subspaces of V we have $PGU(3,q)$, with the intersection $PGU(3,q) \cap PSL(3,q^2)$ being $PSU(3,q)$. If we take our Hermitian form ϕ and consider the isotropic points, that is the vectors $u \in V$ such that $\phi(u,u) = 0$, then by the definition of $PSU(3,q)$ we have that these form an invariant set, Ω, under the action of $PSU(3,q)$.

There are q^3+1 isotropic vectors in Ω and $PSU(3,q)$ acts 2-transitively on them.

We also mention that these points may be used to form an $S(2,q+1,q^3+1)$ Steiner system on which $PSU(3,q)$ acts as an automorphism group.

We present some facts about the group $PSU(3,q)$ which have been compiled mainly from Suzuki [34] and Huppert [13].

Lemma 3.4.1. *Let $q = p^a > 2$ where p is a prime and $a \in \mathbb{N}$, and suppose $G \cong PSU(3,q)$. Let $P \in Syl_p G$ and set $d = (q+1,3)$.*

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

(ii) *G acts 2-transitively on Ω, the set of isotropic 1-spaces of a unitary 3-space, $|\Omega| = q^3+1$ and $G_\alpha = N_G(P)$ for some $\alpha \in \Omega$. Further for $\beta \in \Omega \setminus \{\alpha\}$, $N_G(P) = PG_{\alpha,\beta}$ with $G_{\alpha,\beta}$ cyclic of order $\frac{q^2-1}{d}$ and $|C_{G_{\alpha,\beta}}(Z(P))| = \frac{(q+1)}{d}$.*

(iii) *P has class 2 with $|Z(P)| = q$. If p is odd, then P has exponent p and if $p = 2$ then P has exponent 4 with the set of involutions of P being $Z(P)^\#$.*

Let $\hat{}$ denote the image of subgroups of $SU(3,q)$ in $PSU(3,q)$ ($\cong G$).

(iv) *G has a maximal subgroup M isomorphic to $\hat{}GU(2,q)$.*

(v) *M has a subgroup E_0 of shape $\hat{}(q+1)^2$ for which $N_G(E_0) \sim \hat{}(q+1)^2 Sym(3)$ and any subgroup of G of shape $\hat{}(q+1)^2 Sym(3)$ is conjugate to $N_G(E_0)$*

(vi) *G has a cyclic subgroup C of order $\frac{q^2-q+1}{d}$ for which $N_G(C) \sim C.3$ is a Frobenius group.*

Proof. For parts (i) to (iii) see Suzuki [33] and Huppert [13]. Part (iv) follows from Mitchell [18] (or Bray, Holt, Roney-Dougal [2]). Also from either [2] or [18] G has one conjugacy class of maximal subgroups of shape $\hat{}(q+1)^2 Sym(3)$ (except when $q = 5$)

and (vi) holds (except when $q = 3, 5$). Using the Atlas [9] for these exceptional cases we obtain (v) and (vi). □

The character table for $PSU(3, q)$ was given by Simpson and Frame [28]. We are able to collate the information relating to the conjugacy class structure of $PSU(3, q)$ into Table 3.1, however we maintain the notation they present there. In the table we have $\omega^3 = 1$, $\rho^{q+1} = 1$, $\sigma^{q-1} = \rho$ and $\tau^{q^2-q+1} = 1$.

Label	Canonical Representation
$\mathcal{C}_1$	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$
$\mathcal{C}_2$	$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$
$\mathcal{C}_3^{(l)}$	$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$
$\mathcal{C}_4^{(k)}$	$\begin{bmatrix} \rho^{(k)} & 0 & 0 \\ 0 & \rho^{(k)} & 0 \\ 0 & 0 & \rho^{(-2k)} \end{bmatrix}$
$\mathcal{C}_5^{(l)}$	$\begin{bmatrix} \rho^{(k)} & 0 & 0 \\ 1 & \rho^{(k)} & 0 \\ 0 & 0 & \rho^{(-2k)} \end{bmatrix}$
$\mathcal{C}_6'$	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}$
$\mathcal{C}_6^{(k,l,m)}$	$\begin{bmatrix} \rho^{(k)} & 0 & 0 \\ 0 & \rho^{(l)} & 0 \\ 0 & 0 & \rho^{(m)} \end{bmatrix}$
$\mathcal{C}_7^{(k)}$	$\begin{bmatrix} \rho^{(k)} & 0 & 0 \\ 0 & \sigma^{(-\delta k)} & 0 \\ 0 & 0 & \sigma^{(-qk)} \end{bmatrix}$
$\mathcal{C}_8^{(k)}$	$\begin{bmatrix} \tau^{(k)} & 0 & 0 \\ 0 & \tau^{\delta kg} & 0 \\ 0 & 0 & \tau^{kg^2} \end{bmatrix}$

Table 3.1: Conjugacy class canonical representatives for $PSU(3, q)$

Theorem 3.4.2. *Suppose $G \cong U_3(q)$ $(q > 2)$ acts upon Ω, the set of isotropic points of a 3-dimensional unitary space. Let $k \in \mathbb{N}$ with $k \geq 3$, and set $d = (3, q+1)$ and $\ell = \frac{q+1}{d}$. Then*

$$\begin{aligned}\sigma_k(G,\Omega) &= \frac{d(\eta_k(\pi_1)+\mu_k)}{q^3(q^3+1)(q^2-1)} + \frac{d}{q(q+1)(q^2-1)} \sum_{m\in\mathcal{D}^*(\ell)} \phi(m)\eta_k(\pi_4^{(m)}) \\ &+ \frac{d}{q(q+1)(p-1)} \left(\sum_{\substack{m=pj \\ j\in\mathcal{D}^*(\ell)}} \phi(m)\eta_k(\pi_5^{(m)}) \right) + \frac{d\varepsilon_k(E_0^*,\Omega)}{6(q+1)^2} \\ &+ \frac{d}{2(q^2-1)} \sum_{\substack{m\in\mathcal{D}(\frac{q^2-1}{d}) \\ m\notin\mathcal{D}(\ell)}} \phi(m)\eta_k(\pi_7^{(m)}) \\ &+ \frac{d(q+1)}{3(q^3+1)} \sum_{m\in\mathcal{D}^*(\frac{q^2-q+1}{d})} \phi(m)\eta_k(\pi_8^{(m)}).\end{aligned}$$

Before we can introduce μ_k, ε_k and π_i we require a system of notation associated with pairs of natural numbers dividing ℓ $(= \frac{q+1}{d})$. So let

$$(\ell_1, \ell_2) \in \mathcal{D}(\ell) \times \mathcal{D}(\ell),$$

and let $p_1, .., p_r$ be prime numbers such that $\ell_1 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ and $\ell_2 = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r}$ where for $i = 1, ..., r$ at least one of the α_i and β_i is non-zero. If $\alpha_i \neq \beta_i$, then define $\gamma_i = max\{\alpha_i, \beta_i\}$. Without loss of generality we shall assume that $\alpha_i = \beta_i$ for $1 \leq i \leq s$ and $\alpha_i \neq \beta_i$ for $s < i \leq r$. Set

$$\begin{aligned}\ell_0 &= p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s} \ (= p_1^{\beta_1} p_2^{\beta_2} ... p_s^{\beta_s}) \\ m_1 &= p_{s+1}^{\alpha_{s+1}} p_{s+2}^{\alpha_{s+2}} ... p_r^{\alpha_r} \\ m_2 &= p_{s+1}^{\beta_{s+1}} p_{s+2}^{\beta_{s+2}} ... p_r^{\beta_r}.\end{aligned}$$

Also set $\ell_* = p_{s+1}^{\gamma_{s+1}} p_{s+2}^{\gamma_{s+2}} ... p_r^{\gamma_r}$ and note that $\ell_1 = \ell_0 m_1$ and $\ell_2 = \ell_0 m_2$. We remark that we do not exclude the possibilities $\ell_1 = \ell_0 = \ell_2$ or $\ell_1 = m_1$ and $\ell_2 = m_2$. Put $\ell_{12} = lcm\{\ell_1, \ell_2\}$. If $\ell_i = 1$ then $\ell_0 = 1 = m_i$ and if $\ell_1 = \ell_2 = 1$, then we set $\ell_* = 1$.

Next, we give our partitions of $(q^3 + 1)$ which appear in Theorem 3.4.2.

Definition 2. (i) $\pi_1 = 1^{q^3+1}$.

(ii) $\pi_2 = 1^1 p^{\frac{q^3}{p}}$.

(iii) $\pi_3 = 1^1 4^{\frac{q^3}{4}}$ (only defined for $p = 2$).

(iv) $\pi_4^{(m)} = 1^{q+1} m^{\frac{q^3-q}{m}}$ where $m \in \mathcal{D}^*(\ell)$.

(v) $\pi_5^{(m)} = 1^1 p^{\frac{q}{p}} m^{\frac{q^3-q}{m}}$ where $m = px$ and $x \in \mathcal{D}^*(\ell)$.

(vi) $\pi_6^{(\ell_1,\ell_2,n)} = \ell_1^{\frac{q+1}{\ell_1}} \ell_2^{\frac{q+1}{\ell_2}} n^{\frac{q+1}{n}} \ell_{12}^{\frac{q^3-3q-2}{\ell_{12}}}$ where $(\ell_1, \ell_2) \in \mathcal{D}^*(\ell) \times \mathcal{D}^*(\ell)$ and $n = n_*\ell_*$, $n_* \in \mathcal{D}(\ell_0)$.

(vii) $\pi_7^{(m)} = 1^2 j^{\frac{q-1}{j}} m^{\frac{q^3-q}{m}}$ where $m \in \mathcal{D}(\frac{q^2-1}{d})$, $m \notin \mathcal{D}(\ell)$, $j = \frac{m}{(m,\ell)}$.

(viii) $\pi_8 = m^{\frac{q^3+1}{m}}$ where $m \in \mathcal{D}^*(q^2 - q + 1)$.

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

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

where $(\ell_1, \ell_2) \in \mathcal{D}(\ell) \times \mathcal{D}(\ell)$ and $n = n_*\ell_*$, $n_* \in \mathcal{D}(\ell_0)$.

The two terms μ_k and $\varepsilon_k(E_0^*, \Omega)$ appearing in Theorem 3.4.2 $\sigma_k(G, \Omega)$ are now defined.

Definition 3.

$$\mu_k = (q^3 + 1)(q^3 - 1)\eta_k(\pi_2)$$

if $p \neq 2$ and

$$\mu_k = (q^3 + 1)((q - 1)\eta_k(\pi_2) + (q^3 - q)\eta_k(\pi_3))$$

if $p = 2$.

Definition 4. Let $k \in \mathbb{N}$ and continue to set $\ell = \frac{q+1}{d}$, $(d = (q + 1, 3))$.For $(\ell_1, \ell_2) \in \mathcal{D}(\ell) \times \mathcal{D}(\ell)$ we use the notation ℓ_0, m_1, m_2, ℓ_* as defined earlier, let 3^a be the largest power of 3 dividing $q + 1$.

(i) Let $(\ell_1, \ell_2) \in \mathcal{D}(\ell) \times \mathcal{D}(\ell)$, and $n = \ell_* n_*$ with $n_* \in \mathcal{D}(\ell_0)$ and $n_* = p_1^{\delta_1} p_2^{\delta_2} ... p_s^{\delta_s}$. If $\ell_0 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s}$, then we define

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

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

(iii) For $\ell' \in \mathcal{D}^*(q+1)$ and $i \in \mathbb{N}$ such that $3^i|\ell'$ set
$$\lambda_k(\ell',\ell';i) = \sum_{(\ell_1,\ell_2)\in\mathcal{D}(\ell')\times\mathcal{D}(\ell')} \sum_{\substack{n=\ell_* n_* \\ n_*\in\mathcal{D}(\ell_0)}} f(\ell_1,\ell_2,n)\eta_k(3^i\pi_6^{(\ell_1,\ell_2,n)}).$$

(iv) $\varepsilon_k(E_0^*,\Omega) = \lambda_k^*(\ell,\ell) + \left(\frac{d-1}{2}\right) 9^{a-1}\left(\lambda_k(\frac{q+1}{3^a},\frac{q+1}{3^a},a)\right)$.

Definition 5. Let E_0 be an abelian subgroup of G isomorphic to the direct product of cyclic groups of order $\frac{(q+1)}{d}$ and $(q+1)$ with $N_G(E_0) \cong \frac{(q+1)}{d}(q+1).Sym(3)$. Subgroups such as E_0 exist by Lemma 3.4.1(v) Put $E_0^* = (\mathcal{C}_6 \cup \mathcal{C}_6') \cap E_0$, and define
$$\varepsilon_k(E_0^*,\Omega) = \sum_{g\in E_0^*} |\mathrm{fix}_{\Omega_k}(g)|.$$

Furthermore, when discussing a cyclic group H of order $m \in \mathbb{N}$ we will sometimes use the shorthand notation of $H \cong m$.

Remark Here $\varepsilon_k(E_0^*,\Omega)$ is the contribution of E_0^* to the sum $\sum_{g\in G}|\mathrm{fix}_{\Omega_k}(g)|$. This will coincide with the counting formula given in the previous definition.

In order to the count fixed subsets, we need to ascertain cycle types of elements in each of the 8 conjugacy class types described in [28] and shown in Table 3.1, we do this in the following section.

3.4.1 Determining Fixed Subsets in $PSU(3,q)$

We begin by expanding on the information we have about the conjugacy class types of $PSU(3,q)$.

Lemma 3.4.3. *The number of fixed points, number of classes of a given type and the orders of the centralizers of conjugacy classes for each class of type $\mathcal{C}_1,...,\mathcal{C}_8$ of $G \cong PSU(3,q)$, are given in Table 3.2.*

Class Type	Number of Classes of each Type	Centralizer Order	$\lvert\mathrm{fix}_\Omega(g)\rvert$, $g^G \in \mathcal{C}_i$
$\mathcal{C}_1$	1	$\lvert G\rvert$	q^3+1
$\mathcal{C}_2$	1	$\frac{q^3(q+1)}{d}$	1
$\mathcal{C}_3$	d	q^2	1
$\mathcal{C}_4$	$\ell-1$	$\frac{q(q+1)(q^2-1)}{d}$	$q+1$
$\mathcal{C}_5$	$\ell-1$	$\frac{q(q+1)}{d}$	1
$\mathcal{C}_6$	$\frac{q^2-q+1-d}{6d}$	$\frac{(q+1)^2}{d}$	0
$\mathcal{C}_6'$	0 if $d=1$, 1 if $d=3$	$(q+1)^2$	0
$\mathcal{C}_7$	$\frac{q^2-q-2}{2d}$	$\frac{q^2-1}{d}$	2
$\mathcal{C}_8$	$\frac{q^2-q+1-d}{3d}$	$\frac{q^2-q+1}{d}$	0

Table 3.2: Number of conjugacy classes of $PSU(3,q)$

Proof. From Table 2 in [28] we can extract details of the conjugacy classes of $G = PSU(3,q)$ as well as some supplementary information which we display in Table 3.2. Note that $d=(3,q+1), \ell=\frac{q+1}{d}$ and Ω is as in Lemma 3.4.1 (ii).

We have used the same notation for the classes as in [28] except we have omitted the superscripts used there as they are of no importance here. Because $PSU(3,q)$ acts 2-transitively on Ω, by page 69 of [14] the permutation character must be $\chi_1+\chi_{q^3}$ (as in Table 2 of [28]) which then yields the final column of Table 3.2.

□

Lemma 3.4.4. *The cycle type for elements in the classes of type $\mathcal{C}_i$ for $i \neq 6$ are given in Table 3.3*

Class Type	Order of g	Cycle type of g
$\mathcal{C}_1$	1	π_1
$\mathcal{C}_2$	p	π_2
$\mathcal{C}_3$	4, $(p=2)$ p, $(p\neq 2)$	π_3 π_2
$\mathcal{C}_4$	m, $(m\in\mathcal{D}^*(\ell))$	$\pi_4^{(m)}$
$\mathcal{C}_5$	px, $(x\in\mathcal{D}^*(\ell))$	$\pi_5^{(m)}$
$\mathcal{C}_7$	$m=js$, $(j\in\mathcal{D}*(q-1)$, $s\in\mathcal{D}(\ell))$	$\pi_7^{(m)}$
$\mathcal{C}_8$	m, $(m\in\mathcal{D}^*(q^2-q+1))$	π_8

Table 3.3: Cycle Types

Proof. Let $X = g^G$ be a conjugacy class of type $\mathcal{C}_i$, $i \in \{1,...,8\}\setminus\{6\}$, and let

$P \in Syl_p(G)$. If $i = 1$, then clearly $g = 1$. From the centralizer sizes in Table 3.2, for $i = 2$ we must have X is the conjugacy class containing $Z(P)^\#$, this can be seen from Lemma 3.4.1(ii), while classes of type $\mathcal{C}_3$ are the conjugacy classes of elements in $P \setminus Z(P)$. If p is odd, we note that P has class 2 and so the order of the centralizer of $x \in P \setminus Z(P)$ is equal to the order of $P/Z(P)$ which is q^2. Then by Lemma 3.4.1(iii) the elements in classes of type $\mathcal{C}_3$ all have order p whence, as elements in classes of types $\mathcal{C}_2$ and $\mathcal{C}_3$ fix just one element of Ω, their cycle type is π_2. If $p = 2$, then for $i = 2$, we also have cycle type π_2 and for $i = 3$ as the non-central elements of P must have order 4, due to the exponent, their cycle type must be π_3.

From Lemma 3.4.1(iv) G possesses a maximal subgroup $M \cong \hat{}GU(2, q)$. Furthermore $Z(M)$ is cyclic of order $\ell = \frac{q+1}{d}$. It is straightforward to check that no two elements in $Z(M)^\#$ are G-conjugate, indeed by maximality of M we have $N_G(Z(M)) = M$. We note that $|GU(2, q)| = q(q + 1)(q^2 - 1)$, so we see, using the centralizer sizes in Table 3.2, $Z(M)^\#$ supplies representatives for all the conjugacy classes of type $\mathcal{C}_4$. Choose h to be an element of order p in M (in fact h is G-conjugate to an element in $Z(P)$). By the structure of M, for any $h' \in Z(M)^\#$, $|C_G(hh')| = \frac{q(q+1)}{d}$, ($h \in Z(P)$ and $|Z(M)| = \frac{q+1}{d}$). Also for $h', h'' \in Z(M)^\#$ with $h' \neq h''$ we see that hh' and hh'' are not G-conjugate. Otherwise,

$$\begin{aligned} (hh')^g &= hh'' \\ h^g h'^g &= hh'' \end{aligned}$$

then taking the p^{th} power of $h^g h'^g$ and hh'' (note that h' and h'' have orders not divisible by p and h^g commutes with h'^g) we have

$$(h^p)'^g = (h^p)''$$

but h'' and h' are both in $Z(M)$ when raised to their p^{th} powers, so as they cannot be G-conjugate, we must have that these powers are equal, but $p \nmid |Z(M)|$ and so $h' = h''$, which is a contradiction. Therefore $\{hh' \mid h' \in Z(M)^\#\}$ gives representatives for all conjugacy classes of type $\mathcal{C}_5$. Now $|\mathrm{fix}_\Omega(g')| = q + 1$ for all $g' \in Z(M)^\#$. So for $h' \in Z(M)^\#$ of order m, h' will have cycle type $\pi_4^{(m)}$ on Ω. Similarly for hh', $h' \in Z(M)^\#$ with h' of order m, as $|\mathrm{fix}_\Omega(h)| = 1$, we infer that hh' has cycle type $\pi_5^{(m)}$. So we have dealt with classes of type $\mathcal{C}_4$ and $\mathcal{C}_5$.

Next we look at classes of type $\mathcal{C}_7$. Since $|\mathrm{fix}_\Omega(g)| = 2$, we may suppose $g \in G_{\alpha,\beta}$ ($\cong \frac{q^2-1}{d}$), where $\alpha, \beta \in \Omega$, $\alpha \neq \beta$. We may also suppose $Z(M)(\cong \frac{q+1}{d}) \leq G_{\alpha,\beta}$ where M is a maximal subgroup of G isomorphic to $\hat{}GU_2(q)$. Since $|\mathrm{fix}_\Omega(g')| = q+1$ for all $g' \in Z(M)^\#$, $g \in G_{\alpha,\beta} \setminus Z(M)$. Let g have order m and let j be the smallest natural number such that $g^j \in Z(M)$. Then $m = (m,\ell)j$ where $j \in \mathcal{D}^*(q-1)$ (note that if $j = 1$, then as $G_{\alpha,\beta} \cong \frac{(q+1)}{d}$ contains a unique subgroup $Z(M)$ of order $\frac{q+1}{d} = \ell$, would would have that $g \in Z(M)$ which we have already counted). So $j = \frac{m}{(m,\ell)}$ and hence g has cycle type $\pi_7^{(m)}$.

Finally we look at those of type $\mathcal{C}_8$. From Lemma 3.4.1(vi) G has a cyclic subgroup $C \cong \frac{(q^2-q+1)}{d}$ with $N_G(C) \sim C.3$ being a Frobenius group. Now $C^\#$ has $(|C|-1)/3$ $N_G(C)$-conjugacy classes and it can be seen that no two of these are G-conjugate. Hence we have that the $N_G(C)$-conjugacy class representatives of $C^\#$ give us representatives for all of the classes of type $\mathcal{C}_8$. So, as $|\mathrm{fix}_\Omega(h)| = 0$ for all $h \in C^\#$, the elements in $C^\#$ have cycle type π_8 on Ω, which completes the proof of Lemma 3.4.4.

□

We consider the cycle structures for $\mathcal{C}_6 \cup \mathcal{C}_6'$ separately in Lemma 3.4.7, we do this due to the complexity and variety of these cycle types (see the example in Table 3.4).

Cycle Type of Conjugacy Class Representative	Number of Classes	Cycle Type of Conjugacy Class Representative	Number of Classes
$2^{36}4^{89460}$	1	$6^{12}12^{29820}$	2
$2^{36}8^{44730}$	2	$6^{12}24^{14910}$	4
$2^{36}12^{29820}$	2	$6^{12}8^{9}24^{14907}$	8
$2^{36}24^{14910}$	4	$8^{9}12^{6}24^{14907}$	16
$2^{36}3^{24}6^{59628}$	2	9^{39768}	3
$3^{24}6^{59640}$	1	$9^{8}18^{19880}$	9
$3^{24}12^{29820}$	2	$9^{8}36^{9940}$	18
$3^{24}24^{14910}$	4	$9^{8}72^{4970}$	36
$3^{24}4^{18}12^{29814}$	4	$12^{6}24^{14910}$	8
$3^{24}8^{9}24^{14907}$	8	$18^{4}36^{9940}$	18
$4^{18}8^{44730}$	4	$18^{4}72^{4970}$	36
$4^{18}24^{14910}$	8	$36^{2}72^{4970}$	72
$4^{18}6^{12}12^{29814}$	4	3^{119304}	1

Table 3.4: Cycle types for $\mathcal{C}_6 \cup \mathcal{C}_6'$ class types in $U_3(71)$

As a result, these classes require more groundwork than those seen previously.

Lemma 3.4.5. *Suppose $A \cong \mathbb{Z}_e \times \mathbb{Z}_e$ with A containing three subgroups $A_i \cong \mathbb{Z}_e$ with $i = 1, 2, 3$, such that $A_i \cap A_j = 1$ for $i \neq j$. Then there exists $a_1 \in A_1$, $a_2 \in A_2$ such that $A_1 = \langle a_1 \rangle$, $A_2 = \langle a_2 \rangle$ and $A_3 = \langle a_1 a_2 \rangle$.*

Proof. Since $A_1 \cap A_2 = 1$ and $A_1 \cong \mathbb{Z}_e$, $A = A_1 A_2$. Let $A_3 = \langle c \rangle$. Then $c = a_1 a_2$ where $a_i \in A_i$, $i = 1, 2$. Suppose a_i has order e_i and, without loss, $e_1 \leq e_2$. Then $c^{e_1} = a_1^{e_1} a_2^{e_1} = a_2^{e_1} \in A_2 \cap A_3 = 1$. So $e_2 \leq e_1$ and hence $e_1 = e_2$. Since $c = a_1 a_2$ has order e, we must have that $e_1 = e_2 = e$, so proving the lemma. □

Hypothesis 3.4.6. *Suppose that A_0 is an abelian group containing a subgroup A with $[A_0 : A] = 1$ or 3. Also suppose that A has order e^2 and contains three subgroups A_1, A_2, A_3 with $A_i \cong \mathbb{Z}_e$ $(i = 1, 2, 3)$.*

Further suppose that Ω is an A_0-set such that

(i) for $1 \neq g \in A_0$, $\mathrm{fix}_\Omega(g) = \emptyset$ if $g \notin A_1 \cup A_2 \cup A_3$ and $\mathrm{fix}_\Omega(g) = \mathrm{fix}_\Omega(A_i)$ if $g \in A_i$;

(ii) $\mathrm{fix}_\Omega(A_i) \cap \mathrm{fix}_\Omega(A_j) = \emptyset$ for $1 \leq i \neq j \leq 3$; and

(iii) for $i = 1, 2, 3$, $|\mathrm{fix}_\Omega(A_i)| = q + 1$.

Set $\Lambda_i = \mathrm{fix}_\Omega(A_i)$ for $i = 1, 2, 3$ and $\Lambda = \Omega \setminus (\mathrm{fix}_\Omega(A_1) \cup \mathrm{fix}_\Omega(A_2) \cup \mathrm{fix}_\Omega(A_3))$ and so, by (ii), Ω is the disjoint union

$$\Lambda_1 \cup \Lambda_2 \cup \Lambda_3 \cup \Lambda.$$

Moreover, by (i), A_0 acts regularly on Λ and for $i = 1, 2, 3$, A_0/A_i acts regularly on Λ_i.

We shall encounter Hypothesis 3.4.6 both in a recursive setting and in the group $A_0 = \mathbb{Z}_{q+1} \times \mathbb{Z}_\ell$ (where $\ell = \frac{q+1}{d}$, $d = (3, q+1)$). For this A_0 we have $e = \ell$ and A would be the subgroup of A_0 generated by the elements of A_0 of order ℓ, then $[A_0 : A] = d$.

Lemma 3.4.7. *Assume Hypothesis 3.4.6 holds and use the notation A_0, A and A_i in the hypothesis. Let $(\ell_1, \ell_2) \in \mathcal{D}(e) \times \mathcal{D}(e)$ with $e \in \mathcal{D}(\ell)$. The cycle structure on Ω of the elements $g = g_1 g_2 \in A$ where $g_i \in A_i$ $(i = 1, 2)$ with g_i of order ℓ_i is*

$$(\ell_1)^{\frac{q+1}{\ell_1}} (\ell_2)^{\frac{q+1}{\ell_2}} (n)^{\frac{q+1}{n}} (\ell_{12})^{\frac{|\Lambda|}{\ell_{12}}},$$

where $n = \ell_* n_*$ *with* $n_* \in \mathcal{D}(\ell_0)$ *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*

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

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

Proof. By Hypothesis 3.4.6 (i) and (ii) $A_i \cap A_j = 1$ for $i \neq j$. Hence, by Lemma 3.4.5 we may select $a_1 \in A_1$, $a_2 \in A_2$ so as to have $A_1 = \langle a_1 \rangle$, $A_2 = \langle a_2 \rangle$ and $A_3 = \langle a_1 a_2 \rangle$. Additionally we may identify A with $A_1 A_2$. Let $g = g_1 g_2$ where $g_i \in A_i$ and g_i has order ℓ_i, $i = 1, 2$. The smallest $k \in \mathbb{N}$ such that $g^k \in A_2$ is clearly ℓ_1 and, likewise, the smallest $k \in \mathbb{N}$ such that $g^k \in A_1$ is clearly ℓ_2. Hence, as A/A_2 acts regularly on Λ_2, g in its action on Λ_2 must be the product of disjoint cycles of length ℓ_1. Similarly g acts upon Λ_1 as a product of disjoint cycles each of length ℓ_2. Concerning the action of g on Λ, as A_0 acts regularly on Λ and $\ell_{12} = lcm\{\ell_1, \ell_2\}$ is the order of g, Λ is a disjoint union of $\frac{|\Lambda|}{\ell_{12}}$ length cycles of g.

Since $A_3 = \langle a_1 a_2 \rangle$ to find the lengths of g's cycles on Λ_3, we must determine the smallest $k \in \mathbb{N}$ such that $g^k \in \langle a_1 a_2 \rangle$. For $i = 1, 2$ let $k_i \in \mathbb{N}$ with $k_i \le e$ be such that $g_i = a_i^{k_i}$. So $g = a_1^{k_1} a_2^{k_2}$ and, we recall, $\ell_i = e/(e, k_i)$ for $i = 1, 2$. Thus we seek the smallest $k \in \mathbb{N}$ for which

$$g^k = (a_1^{k_1} a_2^{k_2})^k = a_1^{k_1 k} a_2^{k_2 k} = (a_1 a_2)^j$$

for some j, $0 \le j < e$. This is the smallest $k \in \mathbb{N}$ such that $k_1 k \equiv k_2 k \bmod e$ which is $k = \frac{e}{(k_1 - k_2, e)}$.

Let C be a cyclic group isomorphic to $\mathbb{Z}_e$ with generator c. Now for $i = 1, 2$ the order of c^{k_i} is $\frac{e}{(e,k_i)} = \ell_i$ and the order of $c^{k_1}(c^{k_2})^{-1}$ is k. Thus to enumerate the possibilities for k (recall (ℓ_1, ℓ_2) is a fixed ordered pair) we look at the order of $c^{k_1}(c^{k_2})^{-1}$ as we run through the ordered pairs (c^{k_1}, c^{k_2}) of elements of C of order, respectively, ℓ_1 and ℓ_2. In doing this there no loss in supposing $C = \langle c \rangle$ has order $lcm\{\ell_1, \ell_2\}$.

For $i = 1, ..., r$, let $P_i \in Syl_{p_i}(C)$. Since the order of elements in C is the product of their orders in the projections into P_i for $i = 1, ..., r$, we first consider the special case when $C = P_i \neq 1$, for some $i \in \{1, ..., r\}$. So $\ell_1 = p_i^{\alpha_i}$ and $\ell_2 = p_i^{\beta_i}$.

(3.4.7.1) If $\alpha_i \neq \beta_i$, then for all choices of (c^{k_1}, c^{k_2}), of which there are $\phi(p_i^{\alpha_i})\phi(p_i^{\beta_i})$, the order of $c^{k_1}(c^{k_2})^{-1}$ is $p_i^{\gamma_i}$.

Recalling that by definition $\gamma_i = max\{\alpha_i, \beta_i\}$ we see that the order of $c^{k_1}(c^{k_2})^{-1}$ is $p_i^{\gamma_i}$ as asserted.

Now we turn to the case when $\alpha_i = \beta_i$. Here we have $\phi(p_i^{\alpha_i})^2$ possible choices for (c^{k_1}, c^{k_2}). Let C_1 be the unique subgroup of C of order $p_i^{\alpha_i - 1}$ (and note c^{k_1} and c^{k_2} are in $C \setminus C_1$). Should c^{k_1} and c^{k_2} be in different C_1 cosets of C, then $c^{k_1}(c^{k_2})^{-1}$ is not in C_1 whence $c^{k_1}(c^{k_2})^{-1}$ has order $p_i^{\alpha_i}$. This will happen $\phi(p_i^{\alpha_i})p_i^{\alpha_i - 1}(p_i - 2)$ times. The number of ordered pairs (c^{k_1}, c^{k_2}) for which c^{k_1} and c^{k_2} are in the same C_1 coset of C is $\phi(p_i^{\alpha_i})p_i^{\alpha_i - 1}$. In this situation, for a fixed c^{k_1}, $c^{k_1}(c^{k_2})^{-1}$ runs through all the elements of C_1 thus yielding $\phi(p_i^{\alpha_i - 1})$ of order $p_i^{\alpha_i - 1}$, $\phi(p_i^{\alpha_i - 2})$ of order $p_i^{\alpha_i - 2}$, and so on. To summarize we have the following.

(3.4.7.2) Suppose $\alpha_i = \beta_i$. Then for $\phi(p_i^{\alpha_i})p_i^{\alpha_i - 1}(p_i - 2)$ of the ordered pairs (c^{k_1}, c^{k_2}) the order of $c^{k_1}(c^{k_2})^{-1}$ is $p_i^{\alpha_i}$ and, for $j = 1, ..., \alpha_i$, $\phi(p_i^{\alpha_i})\phi(p_i^{\alpha_i - j})$ of the ordered pairs (c^{k_1}, c^{k_2}) the order of $c^{k_1}(c^{k_2})^{-1}$ is $p_i^{\alpha_i - j}$.

We now consider the general situation for $\ell_1 = p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$ and $\ell_2 = p_1^{\beta_1}p_1^{\beta_2}...p_r^{\beta_r}$. Looking at all those i for which $\alpha_i \neq \beta_i$ (just for the moment considering the projections onto $P_{s+1}, ..., P_r$) we obtain that $c^{k_1}(c^{k_2})^{-1}$ has order $p_{s+1}^{\gamma_{s+1}}...p_r^{\gamma_r} = \ell_*$ for

$$\prod_{i=s+1}^{r} \phi(p_i^{\alpha_i})\phi(p_i^{\beta_i}) = \phi(m_1)\phi(m_2)$$

pairs (c^{k_1}, c^{k_2}) by (3.4.7.1) We now wish to enumerate the pairs (c^{k_1}, c^{k_2}) for which the order of $c^{k_1}(c^{k_2})^{-1}$ is n, where $n = \ell_* n_*$, $n_* \in \mathcal{D}(\ell_0)$ and $n_* = p_1^{\delta_1}p_2^{\delta_2}...p_s^{\delta_s}$. Using (3.4.7.2) and by just considering the projections on $P_1, ..., P_s$ we see this occurs for

$$\begin{aligned}
&\prod_{\alpha_i = \delta_i} \phi(p_i^{\alpha_i})p_i^{\alpha_i - 1}(p_i - 2) \prod_{\alpha_i \neq \delta_i} \phi(p_i^{\alpha_i})\phi(p_i^{\delta_i}) \\
&= \prod_{1 \leq i \leq s} \phi(p_i^{\alpha_i}) \prod_{\alpha_i = \delta_i} p_i^{\alpha_i - 1}(p_i - 2) \prod_{\alpha_i \neq \delta_i} \phi(p_i^{\delta_i}) \\
&= \phi(\ell_0) \prod_{\alpha_i = \delta_i} p^{\alpha_i - 1}(p_i - 2)\phi\left(\prod_{\alpha_i \neq \delta_i} p_i^{\delta_i}\right)
\end{aligned}$$

pairs. Combining this with the projection onto $P_{s+1}, ..., P_r$ yields Lemma 3.4.7. □

Lemma 3.4.8. *Let E_0 be an abelian subgroup of G isomorphic to the direct product of two cyclic groups of order $\frac{(q+1)}{d}$ and $(q+1)$ with $N_G(E_0) \sim \frac{(q+1)}{d}(q+1).Sym(3)$. Also let E be the subgroup of E_0 generated by the elements of E_0 of order $\ell = \frac{(q+1)}{d}$. Then*

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

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

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

Where $\lambda_k^*(\ell, \ell)$ *is given in Definition 4.*

Proof. By Lemma 3.4.1(iv),(v) G contains a subgroup M with $M \sim \hat{} GU_2(q)$ and $E_0 \leq M$. From the structure of $N_G(E_0)$ and $\hat{} GU_2(q)$, $Z(M) \leq E_0$ with $Z(M) \cong \frac{q+1}{d} (= \ell)$. Let $h \in N_G(E_0)$ be an element of order 3. Because $[N_M(E_0) : E_0] = 2$, $h \notin M = N_G(Z(M))$. In order to key in with the notation of Hypothesis 3.4.6, principally as we shall employ Lemma 3.4.7, we set $A_0 = E_0$ and $A = E$. Further, we set $A_1 = Z(M)$, $A_2 = Z(M)^h$ and $A_3 = Z(M)^{h^2}$. Since $\mathrm{fix}_\Omega(h) = \mathrm{fix}_\Omega(Z(M))$ for all $h \in Z(M)^\#$, it follows that $\mathrm{fix}_\Omega(A_i) \cap \mathrm{fix}_\Omega(A_j) = \emptyset$ for $1 \leq i \neq j \leq 3$. We also have $|\mathrm{fix}_\Omega(A_i)| = q + 1$ and, by Table 3.2, $\mathrm{fix}_\Omega(g) = \emptyset$ if $g \in A_0 \setminus (A_1 \cup A_2 \cup A_3)$. Now A is the subgroup of A_0 generated by the elements of A_0 of order ℓ and $A_i \cong \ell$. So we have $A_i \leq A$, $i = 1, 2, 3$ and $[A : A_0] = d$ $(= 1$ and $3)$. Hence Hypothesis 3.4.6 holds with $e = \ell$.

Suppose $d = 1$. Then $A = A_0$. Using Lemma 3.4.7 and Definition 4(ii) we obtain $\sigma_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell)$. (Note the condition in Definition 4(ii) on the outer sum that $(\ell_1, \ell_2) \in \mathcal{D}^*(\ell) \times \mathcal{D}^*(\ell)$ and on the inner sum that $n \neq 1$ prevents the counting of elements in $\mathcal{C}_4$.) So Lemma 3.4.8 holds in this case.

So we now investigate the case when $d = 3$. Hence $[A_0 : A] = 3$. Let $\theta : A_0 \mapsto A_0$ be defined by $\theta : g \mapsto g^3$. Then, as A_0 is abelian, θ is a homomorphism with $im\theta \leq A$ and $ker\theta = \{x \in A_0 |$ order of x is 1 or 3$\}$.

Further assume that $3 \nmid |E|$ (so $3 \nmid \ell$). Then, as $|A| = \ell^2$, $3 \nmid |A|$. Also we have $|ker\theta| = 3$ and therefore, by orders, $im\theta = A$. For every $g \in A_0 \setminus A$, the smallest power of g contained in A_i $(i = 1, 2, 3)$ will be three times the corresponding power for $h = g^3 = \theta(g)$. Now $3 \nmid |A|$ means that θ restricted to A is a one-to-one map, and so the inverse image of h contains two elements of $A_0 \setminus A$. Hence, using Lemma 3.4.7, the elements of $A_0 \setminus A$ contribute $2\lambda_k(\ell, \ell, 1)$ to the sum $\sum_{g \in G} |\mathrm{fix}_{\Omega_k}(g)|$. Thus, using Lemma 3.4.7 again, $\sigma_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell) + 2\lambda_k(\ell, \ell; 1)$, as stated.

The last case to be considered is when, as well as $d = 3$, we have $3\big||E|$. So $3|\ell$. As a consequence $|ker\theta| = 3^2$ and thus $[A : im\theta] = 3$. We seek to pinpoint $im\theta$. Now let A_i^3 denote the unique subgroup of A_i of index 3 ($i = 1, 2, 3$). Let B be the subgroup of A generated by the elements of A of order $\ell/3$. Then $[A : B] = 3^2$ and, for $1 \leq i < j \leq 3$, $B = A_i^3 A_j^3$. Also observe that $im\theta \geq B$. Set $N = N_G(A_0)$, and recall that $N \sim (\frac{q+1}{d}(q+1)).Sym(3)$. Also the N-conjugacy class of A_1 is $\{A_1, A_2, A_3\}$. Hence N normalizes B $(= A_i^3 A_j^3, 1 \leq i < j \leq 3)$ and the N-conjugacy of $A_1 B$ is $\{A_1B, A_2B, A_3B\}$. Moreover $A_iB \neq A_jB$ for $1 \leq i < j \leq 3$ (as $A = A_iA_j$). Evidently $im\theta$ is a normal subgroup of N and therefore $\{im\theta, A_1B, A_2B, A_3B\}$ comprise the four subgroups of index 3 in A which contain B. Observe that the inverse image under θ of B is A. Since, by Lemma 3.4.7, $\lambda_k^*(\ell, \ell)$ is the count for the contribution of elements in A, we are looking to determine the contribution from the elements in $A_0 \setminus A$. Thus for $h \in im\theta \setminus B$, $\theta^{-1}(\{h\}) \subseteq A_0 \setminus A$ with $|\theta^{-1}(\{h\})| = 9$. For $g \in \theta^{-1}(\{h\})$, $h = g^3 \in im\theta$ and so we must multiply the cycle lengths of h by 3 and their multiplicities by 9 to count the contribution of $\theta^{-1}(\{h\})$.

Now $im\theta$ contains $B = A_i^{(3)} A_j^{(3)}$ $(1 \leq i \neq j \leq 3)$ as a subgroup of index 3, and clearly $A_i \cap im\theta \geq A_i^{(3)}$, $(1 \leq i \leq 3)$. If $A_i \cap im\theta \neq A_i^{(3)}$, then, as $[A_i : A_i^{(3)}] = 3$, we get $A_i \leq im\theta$. But then

$$im\theta \geq A_i A_j^{(3)} = A_i A_i^{(3)} A_j^{(3)} = A_i B$$

whence $im\theta = A_iB$. This is impossible as $im\theta \neq A_iB$ and so we conclude that $A_i \cap im\theta = A_i^{(3)}$ for $1 \leq i \leq 3$. Hence we have that $im\theta$ satisfies Hypothesis 3.4.6 with B playing the role of A and $A_i \cap im\theta$ $(1 \leq i \leq 3)$ the role of the A_i. Further B itself satisfies Hypothesis 3.4.6 with B playing the role also of A and the $A_i^{(3)}$ $(1 \leq i \leq 3)$ the role of the A_i. We may repeat this process for $im\theta \setminus B$ (note $s \geq 2$ in this case), each time we multiply cycle lengths by 3 and the multiplicity by 9. Eventually we arrive at $im(\theta^{s-1})$, containing a subgroup B^* of index 3. Observe that the count for $im(\theta^{s-1}) \cong \frac{q+1}{3^{s-1}} \times \frac{q+1}{3^s}$ is given by part (ii) (with $\ell = \frac{q+1}{3^{s-1}}$) and the count for $B^* \cong \frac{q+1}{3^s} \times \frac{q+1}{3^s}$ with $(\ell = \frac{q+1}{3^s})$. Keeping track of changes in cycle length and multiplicity we obtain

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

$$= 2.9^{s-1}\lambda_k(\frac{q+1}{3^s}, \frac{q+1}{3^s}; s)$$

which is the contribution for $A_0 \setminus A$. Consequently

$$\sigma_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell) + 2.9^{s-1}\lambda_k(\frac{q+1}{3^s}, \frac{q+1}{3^s}; s),$$

and the proof of Lemma 3.4.8 is complete. □

We note that in Lemma 3.4.8 if $a = 1$ then parts (ii) and (iii) are equal and we use this to combine the three equations for $\varepsilon(E_0^*, \Omega)$ given in the statement of Lemma 3.4.8 into the single value given in Definition 4.

We are now in a position to prove Theorem 3.4.2.

Proof of Theorem 3.4.2. We proceed in much the same vein as in previous proofs of such theorems, that is by counting the number of fixed subsets for $g \in G$ and applying Theorem 1.0.4. The first class type is the identity element contributing

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

We next consider the elements in classes of type $\mathcal{C}_2$ and $\mathcal{C}_3$. These elements will have cycle types, respectively, π_2 and π_3. Using Table 3.1 we are able to determine their combined contribution, which is $\mu_k(q)$ as described above, this is then divided by $|G|$.

The elements in classes of type $\mathcal{C}_4$ all have cycle type $\pi_4^{(m)}$ and we have seen in the proof of Lemma 3.4.4 that we only need sum our elements over $\mathcal{D}^*(\ell)$, combining this with the centralizer orders given in Table 3.2 we have a total contribution from these elements of

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

Elements in class type $\mathcal{C}_5$, have cycle type $\pi_5^{(m)}$, and we again use the proof of Lemma 3.4.4 to see that summing over the elements of $\mathcal{D}^*(\ell)$ is enough, again taking the centralizer order from Table 3.2 we have

$$\frac{d}{q(q+1)} \left(\sum_{\substack{m=pj \\ j \in \mathcal{D}^*(\ell)}} \phi(j)\eta_k(\pi_5^{(m)}) \right).$$

We now apply Lemma 3.4.8 to determine the value from the elements of class type $\mathcal{C}_6$ (and $\mathcal{C}_6'$). We take the centralizer orders from Table 3.2, this total is then divided

by 6 to compensate for the Normalizer of these classes as shown in Lemma 3.4.1 and discussed in the proof of Lemma 3.4.8. We are then able to reduce the formulae for $\varepsilon_k(E_0^*, \Omega)$ given in Lemma 3.4.8 into the reduced form to the expression given in Definition 4(iv).

We note that the type $\mathcal{C}_6'$ classes only arise when $d = 3$ (and then there is only one conjugacy class of this type) and consists of elements of order 3 with no fixed points, and is one third the size of the type $\mathcal{C}_6$ classes. When $d = 3$ we include this class along with the other type $\mathcal{C}_6$ classes in $\varepsilon_k(E_0^*, \Omega)$. It occurs as the case $\ell_1 = \ell_2 = n = 3$ and appears $f(3, 3, 3) = 2$ times. As the size of this class is divided by 6, this corrects the size of this class in our count.

Classes of type $\mathcal{C}_7$ have cycle type $\pi_7^{(m)}$ and are found in the subgroup isomorphic to $\mathbb{Z}_{\frac{q^2-1}{d}}$. However, there are only $\frac{q^2-q-1}{2d}$ such classes, as shown in Table 3.2. We note that we are excluding from our count the $\frac{q+1}{d}$ elements in this subgroup which lay inside classes $\mathcal{C}_4$, of which there are $\frac{q+1}{d}$, this leaves us with $\frac{q^2-q-1}{2d}$ class representatives. Now using a result in Suzuki [34] we know that such elements are conjugate to their q^{th} power and so we have two representatives for each class, so we divide our count by 2, leaving us with a contribution of

$$\frac{1}{2(q^2-1)} \sum_{\substack{m=js \\ j\in\mathcal{D}^*(q-1) \\ s\in\mathcal{D}(\ell)}} \phi(m)\eta_k(\pi_7^{(m,j)}).$$

Finally we consider the contribution of $\mathcal{C}_8$, the representatives will have cycle type $\pi_8^{(m)}$ and are normalized by an element of order 3, which we have seen in the proof of Lemma 3.4.4. We then take our centralizer orders from Table 3.2 as our scalar and upon division by 3, as we will have three representatives for each class, we have a final contribution of

$$\frac{d(q+1)}{3(q^3+1)} \sum_{m\in\mathcal{D}^*(\frac{q^2-q+1}{d})\setminus\{2\}} \phi(m)\eta_k(\pi_8^{(m)})$$

to the total.

By summing all these individual contributions we have the value of $\sigma_k(G, \Omega)$ as stated.

□

Due to the length of the MAGMA implementation code we include it as an appendix

only (see Appendix A.3).

3.5 The Small Ree Groups $R(q)$

We conclude this investigation of finite simple groups of Lie rank one by considering the final family of doubly-transitive rank one simple groups of Lie type, those of type ${}^2\mathrm{G}_2$, the Ree groups $R(q)$ where $q = 3^{2s+1}$ and $|R(q)| = q^3(q^3+1)(q-1)$. We consider their action on k-subsets of Ω, where $|\Omega| = q^3 + 1$. This family of Ree groups act 2-transitively as an automorphism group for a Steiner system $S(2, q+1, q^3+1)$. For an introduction to these groups see Dixon and Mortimer [10].

Much of this section is compiled from results in Ward [36] and Rainbolt and Sheth [24]. We also use the notation from Ward's paper for the conjugacy class types.

In keeping with the previous results in this chapter we begin by outlining useful facts regarding the structure of $R(q)$.

Lemma 3.5.1. *Let G be the small Ree Group $R(q)$, $q = 3^{2s+1} > 3$ acting on Ω of cardinality $q^3 + 1$ and $q \equiv 3$ mod 8. Then*

(i) G has a total of $q + 8$ conjugacy classes.

(ii) the group G contains only one class of involutions, denoted be representative J. We also have that $C_G(J) = \langle J \rangle \times PSL(2, q)$ and $C_G(J)$ is a maximal subgroup of G.

(iii) there are two cyclic Hall subgroups M^+ and M^- with orders, respectively, $q + 1 + \sqrt{3q}$ and $q + 1 - \sqrt{3q}$ which have trivial intersection with their conjugates. These have their class representatives denoted by W and V respectively. The normalizers of these subgroups in G are $M^+ \times \langle t^+ \rangle$ and $M^- \times \langle t^- \rangle$ where t^+, t^- are both elements of order 6.

(iv) G contains a cyclic subgroup $\langle R \rangle$ of order $\frac{(q-1)}{2}$ where $\langle R \rangle \leq PSL(2, q) \leq C_G(J)$, and R^a is conjugate to R^{-a} and no other power.

(v) G contains a cyclic subgroup $\langle S \rangle$ of order $\frac{(q+1)}{4}$ where $\langle S \rangle \leq PSL(2, q) \leq C_G(J)$, and $|N_G(\langle S \rangle)| = 6|\langle S \rangle|$, also S and S^{-1} are $C_G(J)$-conjugate.

(vi) *G contains two non-conjugate elements T and T^{-1} which have order 3.*

(vii) *G contains three elements of order 9, which are not conjugate, Y, YT, and YT^{-1}.*

(viii) *there exists a conjugacy class, X, of elements which are contained in the center of a Sylow 3-subgroup of G. These elements have order 3.*

Proof. (i) see Ward [36] (VI-8)[36].

(ii) see Ward [36] (Introduction), Rainbolt and Sheth [24] (p1264) and Wilson [37] (p138).

(iii) see Ward [36] (Thm I and IV-1) and Wilson [37] (Thm 4.2).

(iv) see Ward [36] (Introduction), Rainbolt and Sheth [24] (p1263).

(v) see Ward [36] (Introduction and II-5) Rainbolt and Sheth [24] (p1263).

(vi) see Ward [36] Rainbolt and Sheth [24] (p1263).

(vii) see Ward [36] (III-11)

(viii) see Ward [36] (III-3).

□

Lemma 3.5.2. *Let $G \cong R(q)$, $q = 3^{2s+1}$, $q > 3$, let G act on Ω of cardinality $q^3 + 1$, then G has 16 conjugacy class types, with the number of classes, order of centralizers of each class and the number of fixed points of each type given in Table 3.5*

Proof. For the class types and centralizer orders these are given in Ward [36]. The number of classes of each type is given explicitly in Rainbolt and Sheth [24]. The number of fixed points can be determined from the conjugacy class table presented in [36], as G acts doubly-transitively on Ω, by Isaac [14] (p69) the permutation character can be determined as the character sum $\xi_1 + \xi_3$ given in Ward [36]. □

We now outline the partitions of $q^3 + 1$ which will be used in Theorem 3.5.4.

Definition 6. (i) $\pi_1(q) = 1^{q^3+1}$,

(ii) $\pi_J(q) = 1^{q+1}2^{\frac{q^3-q}{2}}$,

Class Type	$\lvert fix_G\Omega\rvert$	$\lvert C_G(g)\rvert$	Number of Classes
1	q^3+1	$\lvert G\rvert$	1
J	$q+1$	$q(q+1)(q-1)$	1
X	1	q^3	1
Y	1	$3q$	1
T	1	$2q^2$	1
T^{-1}	1	$2q^2$	1
YT	1	$3q$	1
YT^{-1}	1	$3q$	1
JT	1	$2q$	1
JT^{-1}	1	$2q$	1
$R^a \neq 1$	2	$q-1$	$\frac{q-3}{4}$
$S^a \neq 1$	0	$q+1$	$\frac{q-3}{24}$
$JR^a \neq R^a$	2	$q-1$	$\frac{q-3}{4}$
$JS^a \neq S^a$	0	$q+1$	$\frac{q-3}{8}$
V	0	$q+1-\sqrt{3q}$	$\frac{q-\sqrt{3q}}{6}$
W	0	$q+1+\sqrt{3q}$	$\frac{q+\sqrt{3q}}{6}$

Table 3.5: Number of Fixed points and Centralizer sizes for small Ree Groups

(iii) $\pi_X(q) = \pi_T(q) = \pi_{T^{-1}}(q) = 1^1 3^{\frac{q^3}{3}}$,

(iv) $\pi_Y(q) = \pi_{YT}(q) = \pi_{YT^{-1}}(q) 1^1 9^{\frac{q^3}{9}}$,

(v) $\pi^{(m)}_{R^a}(q) = 1^2 m^{\frac{q^3-1}{m}}$, $m \in \mathcal{D}^*(\frac{q-1}{2})$,

(vi) $\pi^{(m)}_{S^a}(q) = m^{\frac{q^3+1}{m}}$, $m \in \mathcal{D}^*(\frac{q+1}{4})$,

(vii) $\pi^{(m)}_{JR^a}(q) = 1^2 m^{\frac{q-1}{m}} 2m^{\frac{q^3-q}{2m}}$, $m \in \mathcal{D}^*(\frac{q-1}{2})$,

(viii) $\pi^{(m)}_{JS^a}(q) = m^{\frac{q+1}{m}} 2m^{\frac{q^3-q}{2m}}$, $m \in \mathcal{D}^*(\frac{q+1}{4})$,

(ix) $\pi_{JT}(q) = \pi_{JT^{-1}} = 1^1 3^{\frac{q}{3}} 6^{\frac{q^3-q}{6}}$,

(x) $\pi^{(m)}_V(q) = m^{\frac{q^3+1}{m}}$, $m \in \mathcal{D}^*(q+1-\sqrt{3q})$,

(xi) $\pi^{(m)}_W(q) = m^{\frac{q^3+1}{m}}$, $m \in \mathcal{D}^*(q+1+\sqrt{3q})$.

Proposition 3.5.3. *Let H be a conjugacy class type of $G \cong R(q)$, $q = 3^{2s+1} > 3$, as denoted in Lemma 3.5.2, let G act doubly transitively on Ω, where $|\Omega| = q^3+1$. Then for $g \in H$, g has cycle type $\pi_H(q)$ or when appropriate $\pi^{(m)}_H(q)$, as defined above.*

Proof. Let $g \in G$, then we consider g in each conjugacy class type in turn and determine the cycle type of g. Firstly let g be of type 1. Then g is the identity class and so fixes all q^3+1 points of Ω, and so g has cycle type $\pi_1(q)$.

For $g \in G^{\#}$ it is clear that g lies in one of the remaining fifteen non-identity conjugacy class types. As we have seen in Lemma 3.5.2 each class type is denoted by some known subgroup identified in Lemma 3.5.1, which contains representatives of all conjugacy classes of the given type, as we are only interested in cycle types we may assume without loss that g is an element of the denoted subgroup.

Let $g \in J$, then g is an involution and fixes $q+1$ points in Ω, hence g has cycle type $\pi_J(q)$.

If g is an element of type X, T or T^{-1}, then by Lemma 3.5.1 g has order 3 and by Lemma 3.5.2 fixes one point in Ω giving us cycle type π_X. If g is of type Y, YT or YT^{-1}, then by Lemma 3.5.1 g is of order 9 and by Table 3.5 g fixes a single point. Now if g contained any cycles of length three, then g^3 would contain at least four fixed points. This contradicts Table 3.5 which shows the only non-trivial element to fix three points is an involution, hence g has cycle type $\pi_Y(q)$.

Assume now that g is of type $R^a \neq 1$, then (by Lemma 3.5.1 and Table 3.5) g lies in a cyclic subgroup of order $\frac{(q-1)}{2}$ and fixes two points. We note that for $q \equiv 3 \bmod 8$, $\frac{(q-1)}{2}$ is odd. This implies that all cycles of length greater than one must be of equal length, moreover g must have order $m|\frac{(q-1)}{2}$, hence g has cycle type $\pi^{(m)}_{R^a}(q)$.

Similarly if g is of type $S^a \neq 1$, then g lies in a cyclic subgroup of order $\frac{(q+1)}{4}$, which we note is odd for $q \equiv 3 \bmod 8$ and as g will fix no points of Ω (by Lemma 3.5.1 and Table 3.5), g has cycle type $\pi^{(m)}_{S^a}(q)$.

Next we consider when g is of type $JR^a \neq R^a$ or $JS^a \neq S^a$, by Lemma 3.5.1, both of these subgroups are contained in $C_G(J)$, and have orders, respectively, $q-1$ and $\frac{(q+1)}{2}$. In the case $g \in JR^a \setminus R^a$, then $g^2 \in R^a$, however, g has even order and so some power of g will be an involution, and will have cycle type π_J. This restriction implies that a generator for JR^a (note this is a cyclic subgroup) must contain cycles of length $q-1$ and by Table 3.5 two fixed points, but also two cycles of length $\frac{(q-1)}{2}$, therefore g will have order $2m$ where $m|\frac{(q-1)}{2}$ (we phrase the order in this way to emphasize the link to R^a), giving g cycle type $\pi^{(m)}_{JR^a}(q)$. An almost identical argument with g of type JS^a leads to g having cycle type $\pi^{(m)}_{JS^a}(q)$.

If g is of type JT or JT^{-1}, then, as T and T^{-1} are centralized by some involution, J (note that $|C_G(T)|$ is even), we apply a similar argument to that given above to show g has cycle type π_{JT}.

Finally we assume that g is of type W (or V), then by Lemmas 3.5.1 and 3.5.2 g is contained in a cyclic subgroup of order $q+1+\sqrt{3q}$ (or $q+1-\sqrt{3q}$) and fixes no points of Ω. We also note that $q+1\pm\sqrt{3q}$ is odd and so g will have order $m \mid q+1+\sqrt{3q}$, (or $m \mid q+1-\sqrt{3q}$) and so will have cycle type $\pi_W^{(m)}(q)$, (or $\pi_V^{(m)}(q)$) as required, thus proving the result. □

Theorem 3.5.4. *Suppose $G \cong R(q)$ the small Ree group acts as an automorphism group for a Steiner system $S(2, q+1, q^3+1)$. Let $k \in \mathbb{N}$. Then*

$$\begin{aligned}
\sigma_k(G,\Omega) &= \frac{1}{q^3(q^3+1)(q-1)}\eta_k(\pi_1(q)) + \frac{1}{q^3-q}\eta_k(\pi_J(q)) \\
&+\frac{(q+1)}{q^3}\eta_k(\pi_T(q)) + \frac{1}{q}\eta_k(\pi_Y(q)) + \frac{1}{q}\eta_k(\pi_{JT}(q)) \\
&+\frac{1}{2(q-1)}\sum_{m\in\mathcal{D}^*(\frac{q-1}{2})}\phi(m)\eta_k(\pi_{R^a}^{(m)}(q)) \\
&+\frac{1}{6(q+1)}\sum_{m\in\mathcal{D}^*(\frac{q+1}{4})}\phi(m)\eta_k(\pi_{S^a}^{(m)}(q)) \\
&+\frac{1}{2(q-1)}\sum_{m\in\mathcal{D}^*(\frac{q-1}{2})}\phi(m)\eta_k(\pi_{JR^a}^{(m)}(q)) \\
&+\frac{1}{2(q+1)}\sum_{m\in\mathcal{D}^*(\frac{q+1}{4})}\phi(m)\eta_k(\pi_{JS^a}^{(m)}(q)) \\
&+\frac{1}{6(q+1+\sqrt{3q})}\sum_{m\in\mathcal{D}^*(q+1+\sqrt{3q})}\phi(m)\eta_k(\pi_W^{(m)}(q)) \\
&+\frac{1}{6(q+1-\sqrt{3q})}\sum_{m\in\mathcal{D}^*(q+1-\sqrt{3q})}\phi(m)\eta_k(\pi_V^{(m)}(q)).
\end{aligned}$$

Proof. As in previous results of this type, we count the number of k-subsets fixed by an element $g \in G$ and substitute this information into Lemma 1.0.4. We note that when we use centralizer orders, these are all found in Table 3.5.

Clearly, the identity class will contribute

$$\frac{1}{q^3(q^3+1)(q-1)}\eta_k(\pi_1(q))$$

to the total. Similarly if g is an involution, then g will fix $\eta_k(\pi_J)(q)$ k-subsets. As there is only a single class of involutions, with centralizer order $q(q+1)(q-1)$, these contribute

$$\frac{1}{(q^3-q)}\eta_k(\pi_J)(q).$$

The next class type of g we consider are those of type X, T and T^{-1}. As each element in these classes has an identical cycle type we may count these together. Each element will fix $\eta_k(\pi_T(q))$ k-subsets, as the centralizers of these elements are, respectively, q^3, $2q^2$ and $2q^2$, summing these gives us a total contribution from these three classes of elements of

$$\frac{(q+1)}{q^3}\eta_k(\pi_T(q)).$$

Similarly we can consider the class types Y, YT and YT^{-1} together, as these elements all have identical cycle type $\pi_Y(q)$, hence such elements will each fix $\eta_k(\pi_Y(q))$ k-subsets. All of these elements have centralizers of order $3q$, hence the total contribution of these elements will be

$$\frac{1}{q}\eta_k(\pi_Y(q)).$$

We now consider the contributions of classes of type JT and JT^{-1}. As we have seen, we can count these two classes together as each element will fix $\pi_{JT}(q)$ k-subsets. As both of these classes have centralizers with orders $2q$, we have a total contribution of

$$\frac{1}{q}\eta_k(\pi_{JT}(q)).$$

So far, we have only dealt with those conjugacy class types which contain a single conjugacy class. As the remaining class types are represented by cyclic subgroups of G, we recall Lemma 3.1.1, which states that in a cyclic subgroup, H, if $h \in H$ has order m, then $m\big||H|$ and H contains $\phi(m)$ elements of order m. As we are now considering representatives as elements of subgroups rather than single elements, as above, we need also consider the normalizers of these subgroups to determine the number of distinct classes we actually obtain from the elements of each subgroup.

We begin with class type $R^a \neq 1$. These classes have representatives in a cyclic subgroup and the elements have orders $m \in \mathcal{D}^*(\frac{q-1}{2})$. Hence we have $\frac{q-3}{2}$ non-identity class representatives, however Lemma 3.5.1(iv) tells us that inverses in this class are conjugate, hence we have two representatives for all $\frac{q-3}{4}$ classes. Each representative will contribute $\frac{1}{q-1}\eta_k(\pi^{(m)}_{R^a}(q))$ to the count, summing these and division by 2, to allow for the over count gives us a total contribution from these classes of

$$\frac{1}{2(q-1)}\sum_{m\in\mathcal{D}^*(\frac{q-1}{2})}\phi(m)\eta_k(\pi^{(m)}_{R^a})(q).$$

Similarly for classes of type $S^a \neq 1$, these classes have representatives in a cyclic subgroup of order $\frac{q+1}{4}$, giving us $\frac{q-3}{4}$ non identity elements to consider, where each class will contain elements of order $m \in \mathcal{D}^*(\frac{q+1}{4})$ and will contribute $\frac{1}{q+1}\eta_k(\pi^{(m)}_{S^a}(q))$ to the count. However, by Lemma 3.5.1(v) we have that $|N_G(S^a)| = 6|S^a|$ meaning we will have 6 representatives for each class of type $S^a \neq 1$ in the subgroup S^a, therefore we divide our count by six and have accounted for all $\frac{q-3}{24}$ such classes. Summing our count we see that we have a total contribution from the classes of

$$\frac{1}{6(q+1)} \sum_{m \in \mathcal{D}^*(\frac{q+1}{4})} \phi(m)\eta_k(\pi^{(m)}_{S^a}(q)).$$

For elements of classes of type $JR^a \neq R^a$, this subgroup behaves as described in the proof of Proposition 3.5.3. We note that $|JR^a| = 2|R^a|$ and so the elements we wish to use as representative for the classes of this type are located in $JR^a \setminus \{R^a \cup J\}$, where there will be representatives for all $\frac{q+3}{4}$ classes of this type. This gives us a total contribution of

$$\frac{1}{2(q-1)} \sum_{m \in \mathcal{D}^*(\frac{q-1}{2})} \phi(m)\eta_k(\pi^{(m)}_{JR^a}(q)).$$

We note that these elements will have order $2m$ rather than m, however as $(2, m) = 1$ in this case, $\phi(2m) = \phi(2)\phi(m) = \phi(m)$.

Dealing with classes of type JS^a similarly we see that the elements in $JS^a \setminus \{S^a \cup J\}$ will total $\frac{q-3}{4}$, however, unlike elements in S^a these are not normalized by an element of order 3, but inverses are still conjugate in this subgroup, therefore we divide our total by 2 ensuring we have representatives for all the required $\frac{q-3}{8}$ classes. Hence we have a total contribution of these classes of

$$\frac{1}{2(q+1)} \sum_{m \in \mathcal{D}^*(\frac{q+1}{4})} \phi(m)\eta_k(\pi^{(m)}_{JS^a}(q)).$$

Finally we deal with classes of type W (and V). These classes have representatives in the cyclic subgroups M^+ (and M^-). The non-identity elements of these subgroups giving us $q+\sqrt{3q}$ (and $q-\sqrt{3q}$) class representatives, these elements will have order $m \in \mathcal{D}^*(q+\sqrt{3q}+1)$ (and $m \in \mathcal{D}^*(q-\sqrt{3q}+1)$) and so will fix $\eta_k(\pi^{(m)}_W(q))$ (and $\eta_k(\pi^{(m)}_V(q))$) k-subsets. The normalizers of these two subgroups are given in Lemma 3.5.1 and so we will have six representatives from each class. Hence by dividing by 6 and utilizing the orders of the centralizers of these two subgroups given in Lemma 3.5.2 we have

contributions of

$$\frac{1}{6(q+1+\sqrt{3q})} \sum_{m \in \mathcal{D}^*(q+1+\sqrt{3q})} \phi(m)\eta_k(\pi_W^{(m)}(q))$$

for type W and

$$\frac{1}{6(q+1-\sqrt{3q})} \sum_{m \in \mathcal{D}^*(q+1-\sqrt{3q})} \phi(m)\eta_k(\pi_V^{(m)}(q))$$

for type V.

Summing all these contributions gives us $\sigma_k(G, \Omega)$. □

Due to the length of the MAGMA implementation code we include it as an appendix only. See Appendix A.4.

Remark We note that in the main results of this chapter we encounter cyclic groups with element cycle types $m^{\frac{|\Omega|}{m}}$. Clearly to determine the value of η_k for such elements we lose nothing by restricting the values from $\Sigma_{m \in \mathcal{D}(m)}$ to $\Sigma_{m \in \mathcal{D}((m,k))}$ and only consider common divisors of m and k. Summing over the smaller set may reduce the length of time required to compute the values. Indeed we will make use of this in the next chapter.

We do however make note of the limitations of the MAGMA implementation provided as we calculate η_k using the built in command

```
RestrictedPartitions(a,S)
```

this command partitions value a using integers given in the set S. The values of a the command can cope with is quite small, moreover this will cause error messages when using the functions for large examples. Using Binomial methods, some of which are described in the next chapter does allow the function to be used for larger values.

Chapter 4

Subsequent Results

This short chapter presents results which are derived from the formulae in Chapter 3, as well as a supplementary formula for $PGL(2,q)$ to sit alongside the $PSL(2,q)$ result already given. We use this opportunity to highlight some methods and approaches to reducing the given formulae to more manageable states when looking at specific instances, we discuss the results for numbers of orbits of the 2-transitive groups we have considered when they act on 3-subsets and provide reduced functions for these values. We recall the notation used previously of (a,b) to the greatest common divisor of $a,b \in \mathbb{N}$, as well as $\mathcal{D}(a)$ to denote the set of divisors of $a \in \mathbb{N}$ and $\mathcal{D}^*(a) = \mathcal{D}(a)\backslash\{1\}$.

4.1 $PSL(2,q)$

Our first result is a restatement of Propositions 4.1.3 and 4.1.4.

Proposition 4.1.1. *Let $G = PSL(2,q)$ act on 3-subsets of $\Omega = PG(1,q)$, $q = p^a > 2$, where p is prime, $a \in \mathbb{N}$. Then if σ_3 is the number of orbits of G on the set Ω_3 we have*

$$\sigma_3 = \begin{cases} 2, & \text{if } q \equiv 1 \text{ mod } 4 \\ 1, & \text{otherwise.} \end{cases}$$

Lemma 4.1.2. *Let $q = p^a$, where p is a prime greater than 3, $a \in \mathbb{N}$. Then either*

$$(3, \frac{q+1}{2}) = 3 \text{ and } (3, \frac{q-1}{2}) = 1$$

or

$$(3, \frac{q+1}{2}) = 1 \text{ and } (3, \frac{q-1}{2}) = 3.$$

Proof. Let $m = (3, \frac{q+1}{2}) = 3$, then $\frac{q+1}{2} \equiv 0 \bmod 3$ and $\frac{q-1}{2} = \frac{q+1}{2} - 1 \equiv 2 \bmod 3$. Hence $(3, \frac{q-1}{2}) = 1$.

Now let $m = (3, \frac{q+1}{2}) = 1$, then

$$\begin{aligned} \frac{q+1}{2} &\equiv 1 \text{ or } 2 \bmod 3, \\ q+1 &\equiv 1 \text{ or } 2 \bmod 3, \\ q &\equiv 0 \text{ or } 1 \bmod 3, \text{ as } p \neq 3. \\ q &\equiv 1 \bmod 3. \end{aligned}$$

Hence $\frac{q-1}{2} \equiv 0 \bmod 3$ and so $(3, \frac{q-1}{2}) = 3$.

□

We make use of this in the establishment of an alternative combinatorial proof of $PSL(2,q)$ being 3-homogeneous if and only if $q = p^a$ where p is a prime congruent to 3 mod 4 and a is odd.

Proposition 4.1.3. *Let $G = PSL(2,q)$ act on 3-subsets of $\Omega = PG(1,q)$, $q = p^a > 2$, where p is prime, $a \in \mathbb{N}$. Then if σ_3 is the number of orbits of G on the set Ω_3 we have*

$$\sigma_3 = \begin{cases} 2, & \text{if } q \equiv 1 \text{ mod } 4 \\ 1, & \text{if } q \equiv 3 \text{ mod } 4 \end{cases}.$$

Proof. We prove this by dealing with the equation in Theorem 3.2.1 in five parts, denoted using $\mathbf{I}$, $\mathbf{P}$, $\mathbf{H}_+$, $\mathbf{H}_-^{\mathbf{i}}$ $i = 0, 1, 2$ (see Table 4.1). We will then sum the contribution of each of these parts to give a total value for σ_3. We also consider the case for $p = 3$ separately.

First note that here $d = 2$ and $k = 3$, and we initially wish to write the formula without the η_k notation. Using the proof of Theorem 3.2.1 and by defining $l_0 = 1$, $l_1 = 2$ and $l_2 = 1$, we are able to remove the η_k notation from the statement of Theorem 3.2.1 for clarity as this notation requires calculations to be performed.

We begin by replacing $\eta_k(1^{q+1})$ with $\binom{q+1}{k}$ which is clear. Next we consider $\eta_k(1^1 p^{q/p})$, this is the number of k-subsets fixed by an element of cycle type $1^1 p^{q/p}$. This value is determined by whether or not $p|k$ or, due to the presence of a fixed point, $p|(k-1)$, hence

$$\eta_k(1^1 p^{q/p}) = \sum_{i=0}^{1} \sum_{m \in \mathcal{D}^*((k-i,p))} \binom{p^{a-1}}{\frac{k-i}{p}}.$$

We deal with $\eta_k\left(m^{\frac{q+1}{m}}\right)$ in a similar way as the number of k-subsets fixed by an element of this cycle type would be $\binom{\frac{q+1}{m}}{\frac{k}{m}}$. Finally we replace $\eta_k(1^2m^{\frac{q-1}{m}})$ by the number of k-subsets fixed by the given cycle type, which will be non zero if $m|(k-i)$ for $i=0,1,2$ due to the two fixed points. Hence we have $\eta_k(1^2m^{\frac{q-1}{m}}) = \sum_{i=0}^{2} l_i\phi(m)\binom{\frac{q-1}{m}}{\frac{k-i}{m}}$.

$$\begin{aligned}\sigma_k(G,\Omega) &= \frac{d}{q(q+1)(q-1)}\binom{q+1}{k} + \frac{d}{q}\sum_{i=0}^{1}\sum_{m\in\mathcal{D}^*((k-i,p))}\binom{p^{a-1}}{\frac{k-i}{p}} \\ &+ \frac{d}{2(q+1)}\sum_{m\in\mathcal{D}^*((k,\frac{q+1}{d}))}\phi(m)\binom{\frac{q+1}{m}}{\frac{k}{m}} \\ &+ \frac{d}{2(q-1)}\sum_{i=0}^{2}\sum_{m\in\mathcal{D}^*((k-i,\frac{q-1}{d}))} l_i\phi(m)\binom{\frac{q-1}{m}}{\frac{k-i}{m}}.\end{aligned}$$

Let

$$\mathbf{I} = \frac{d}{q(q+1)(q-1)}\binom{q+1}{k}$$

substituting gives

$$\begin{aligned}\mathbf{I} &= \frac{2}{(q+1)(q)(q-1)}\left(\frac{(q+1)!}{3!(q-2)!}\right), \\ &= \frac{2}{3!}, \\ &= \frac{1}{3},\end{aligned}$$

for all q.

Let

$$\mathbf{P} = \frac{d}{q}\sum_{i=0}^{1}\sum_{m\in\mathcal{D}^*((k-i,p))}\binom{p^{a-1}}{\frac{k-i}{p}}.$$

Clearly for $p\neq 3$, $(3,p)=(2,p)=1$. Hence $\mathbf{P}=0$. for all $p\neq 3$ and all a.

By applying Lemma 4.1.2 we can combine

$$\mathbf{H}_+ = \frac{d}{2(q+1)}\sum_{m\in\mathcal{D}^*((k,\frac{q+1}{d}))}\phi(m)\binom{\frac{q+1}{m}}{\frac{k}{m}}$$

and

$$\mathbf{H}_-^{\mathbf{i}} = \frac{d}{2(q-1)}\sum_{i=0}^{2}\sum_{m|(k-i,\frac{q-1}{d})m\neq 1} l_i\phi(m)\binom{\frac{q-1}{m}}{\frac{k-i}{m}}$$

for $i=0$.

Let p be such that $(3, \frac{q+1}{2}) = 1$ then we have that $(3, \frac{q-1}{2}) = 3$ and so

$$\mathbf{H}_+ = 0$$

and

$$\mathbf{H}_-^{\mathbf{0}} = \frac{2}{2(q-1)}(2)\binom{\frac{q-1}{3}}{\frac{3}{3}} = (\frac{q-1}{3})(\frac{2}{q-1}) = \frac{2}{3}.$$

Now let p be such that $(3, \frac{q+1}{2}) = 3$ then we have that $(3, \frac{q-1}{2}) = 1$ and so

$$\mathbf{H}_+ = \frac{2}{2(q+1)}(2)\binom{\frac{q+1}{3}}{\frac{3}{3}} = (\frac{q+1}{3})(\frac{2}{q+1}) = \frac{2}{3},$$

and

$$\mathbf{H}_-^{\mathbf{0}} = 0.$$

Hence $\mathbf{H}_+ + \mathbf{H}_-^{\mathbf{0}} = \frac{2}{3}$ for all $p \neq 3$, all a.

For $\mathbf{H}_-^{\mathbf{2}}$, as $(1, \frac{q-1}{2}) = 1$ for all q, we have $\mathbf{H}_-^{\mathbf{2}} = 0$.

For the case $\mathbf{H}_-^{\mathbf{1}}$ we first consider $q = p^a$ where a is even.

Let $m = (2, \frac{q-1}{2})$, then $m = 2$ otherwise we have

$$\begin{aligned} \frac{q-1}{2} &\equiv 1 \bmod 2 \\ \frac{q-1}{2} &\equiv 1 \text{ or } 3 \bmod 4 \\ q-1 &\equiv 2 \bmod 4 \\ q &\equiv 3 \bmod 4 \end{aligned}$$

which contradicts q being a square.

Now substituting $m = 2$ we have

$$\mathbf{H}_-^{\mathbf{1}} = \frac{2}{2(q-1)}(2)(1)\binom{\frac{q-1}{2}}{1} = (\frac{2}{q-1})(\frac{q-1}{2}) = 1.$$

for all even powers of p.

For odd powers of p where $p \equiv 1 \bmod 4$, we have that $q \equiv 1 \bmod 4$, hence $m = (2, \frac{q-1}{2}) = 2$, otherwise $\frac{q-1}{2} \equiv 1 \bmod 2$ and the above argument yields the contradiction $q \equiv 3 \bmod 4$. Hence

$$\mathbf{H}_-^{\mathbf{1}} = \frac{2}{2(q-1)}(2)(1)\binom{\frac{q-1}{2}}{1} = 1,$$

for $p \equiv 1 \bmod 4$ and a even.

For odd powers of p where $p \equiv 3 \bmod 4$, we have that $q \equiv 3 \bmod 4$, hence $m = (2, \frac{q-1}{2}) = 1$, otherwise, by a similar argument to that above we get the contradiction that $q \equiv 1 \bmod 4$. Substituting $m = 1$ gives

$$\mathbf{H}_{-}^{\mathbf{1}} = 0$$

for odd powers of p where $p \equiv 3 \bmod 4$.

When $p = 3$ the arguments for $\mathbf{I}, \mathbf{H}_{-}^{\mathbf{1}}, \mathbf{H}_{-}^{\mathbf{2}}$ hold true. However for $\mathbf{P}$ we have

$$\frac{2}{q}\binom{p^{a-1}}{1} = \frac{2p^{a-1}}{p^a} = \frac{2}{3}.$$

Also we have that $\mathbf{H}_{+} + \mathbf{H}_{-}^{\mathbf{0}} = 0$ as $(3, \frac{q+1}{2}) = 1$ and $(3, \frac{q-1}{2}) = 1$, otherwise $(3, \frac{q+1}{2}) \equiv 0 \bmod 3 \Rightarrow\ 3^a \equiv 2 \bmod 3$ or $(3, \frac{q-1}{2}) \equiv 0 \bmod 3 \Rightarrow\ 3^a \equiv 1 \bmod 3$.

Hence we have the following table of results for all cases.

		$\mathbf{I}$	$\mathbf{P}$	$\mathbf{H}_{+} + \mathbf{H}_{-}^{\mathbf{0}}$	$\mathbf{H}_{-}^{\mathbf{1}}$	$\mathbf{H}_{-}^{\mathbf{2}}$	σ_3
$p \equiv 1 \bmod 4$	a even	$\frac{1}{3}$	0	$\frac{2}{3}$	1	0	2
	a odd	$\frac{1}{3}$	0	$\frac{2}{3}$	1	0	2
$p \equiv 3 \bmod 4$	a even	$\frac{1}{3}$	0	$\frac{2}{3}$	1	0	2
	a odd	$\frac{1}{3}$	0	$\frac{2}{3}$	0	0	1
$p = 3$	a even	$\frac{1}{3}$	0	$\frac{2}{3}$	1	0	2
	a odd	$\frac{1}{3}$	$\frac{2}{3}$	0	0	0	1

Table 4.1: σ_3 for $q = p^a$

which proves the result. □

Proposition 4.1.4. *Let $G = PSL(2, q)$ act on 3-subsets of $\Omega = PG(1, q)$, $q = 2^a$, where $a > 1$, $a \in \mathbb{N}$. Then if σ_3 is the number of orbits of G on the set Ω_3 we have $\sigma_3 = 1$.*

Proof. We prove this by substituting $k = 3$, $q = 2^a$ and $d = 1$ into the formula in Theorem 3.2.1, we also note that $\phi(3) = 2$. It is straightforward for us to determine the values of η_3 for the first two terms of the sequence, these become

$$\frac{1}{q(q+1)(q-1)}\binom{q+1}{3} = \frac{1}{6},$$

and

$$\frac{1}{q}\left(\frac{q}{2}\right) = \frac{1}{2}.$$

Now the final two terms depend on whether or not 3 divides $(q+1)$ or $(q-1)$, as 3 does not divide $2^a = q$ we have that 3 must divide exactly one of $(q+1)$ or $(q-1)$. So if we assume 3 divides $(q+1)$ then the final two terms become, respectively,

$$\frac{1}{2(q+1)}\phi(3)\left(\frac{q+1}{3}\right) = \frac{1}{3}$$

and 0. Now if we assume 3 divides $(q-1)$ then the final two terms become, respectively, 0 and

$$\frac{1}{2(q-1)}\phi(3)\left(\frac{q-1}{3}\right) = \frac{1}{3}$$

giving us a total value in either case for σ_3 of $\frac{1}{6}+\frac{1}{2}+\frac{1}{3} = 1$, as required. □

We can also prove a result regarding the lengths of orbits of $PSL(2,q)$ on subsets of size three.

Proposition 4.1.5. *Let $G \cong PSL(2,q)$ act on a G-set, Ω, of cardinality n. Then for $\Delta \subset \Omega$ of cardinality 3, we have* $|\Delta^G| = \begin{cases} \binom{q+1}{3}, & \text{if } q \equiv 3 \text{ or } 0 \bmod 4 \\ \frac{1}{2}\binom{q+1}{3}, & \text{if } q \equiv 1 \bmod 4 \end{cases}$.

Proof. In the cases of $q \equiv 3 \bmod 4$ and $q \equiv 0 \bmod 4$ this is clear as there is only one orbit in these instances, so assume that $q \equiv 1 \bmod 4$ We define a homomorphism $\theta : G_\Delta \to S_3$ and note that as only the identity element fixes three points of Ω pointwise, the $ker(\theta)$ is trivial and so θ is injective and moreover $|G_\Delta|\big|6$.

If $|G_\Delta| = 1$ or 2 then we quickly have the contradiction that $|\Delta^G| > \binom{q+1}{3}$, if $|G_\Delta| = 3$ then we have $|\Delta^G| = \binom{q+1}{3}$ contradicting Proposition 4.1.3. Hence $|G_\Delta| = 6$ and so by the Orbit Stabilizer Theorem

$$|\Delta^G| = \frac{q(q+1)(q-1)}{2\cdot 6} = \frac{1}{2}\frac{q(q+1)(q-1)}{6} = \frac{1}{2}\binom{q+1}{3}$$

giving the result. □

4.2 Sequences

The next results all follow the same theme, we prove the existence of certain interesting sequences in the values of $\sigma_k(G,\Omega)$ for $G \cong PSL(2,q)$, $Sz(q)$, $PSU(3,q)$ and $R(q)$.

As we have seen in the previous section, there is very little variety in what happens to $\sigma_3(PSL(2,q))$, so here we consider σ_4 to be the first non-trivial case.

Proposition 4.2.1. *Let $L_n = PSL(2, 2^n)$ acting on the projective plane Ω_n, and put $a_n = \sigma_4(L_n, \Omega_n)$. Setting $a_1 = a_2 = 1$, for $n \geq 3$ we have*

$$a_n = a_{n-1} + 2a_{n-2}.$$

Alternatively

$$a_n = \frac{2^n + (-1)^{n-1}}{3}.$$

Proof. We substitute $d = 1$, $q = 2^n$, $p = 2$ and $k = 4$ into Theorem 3.2.1 and simplify. Using the same statement of the formula as in the proof of Proposition 4.1.3, we can see that

$$\frac{1}{q(q+1)(q-1)}\binom{q+1}{4} = \frac{q-2}{4!}$$

and

$$\begin{aligned}\frac{d}{q}\sum_{i=0}^{1}\sum_{m\in\mathcal{D}^*((k-i,p))}\binom{p^{a-1}}{\frac{k-i}{p}} &= \frac{1}{2^n}\binom{2^{n-1}}{2} \\ &= \frac{2^{n-1}-1}{2^2}.\end{aligned}$$

Now, as $q+1$ is odd, it is clear that

$$\frac{d}{2(q+1)}\sum_{m\in\mathcal{D}^*((k,\frac{q+1}{d}))}\phi(m)\binom{\frac{q+1}{m}}{\frac{k}{m}} = 0$$

for our values.

This brings us to the final part of the formula, here we notice that $2 \equiv -1 \bmod 3$, and so for 4-subsets to be fixed by such elements as we see here, we need $m = 3$ to be a possibility (note again that $m = 4$ or $m = 2$ cannot occur). We must then split our consideration of this part of the formula to account for whether or not q is an even power of 2. If not, then $q - 1 \not\equiv 0 \bmod 3$ and we have a total of 0 for this part. However, if q is an even power of 2, we have

$$\frac{1}{2(q-1)}\phi(3)(2)\binom{\frac{q-1}{3}}{1} = \frac{2}{3}.$$

This gives us two cases for values of a_n,

$$a_n = \frac{2^n-2}{4!} + \frac{2^{n-1}-1}{2^2} + \frac{2}{3}$$

for n even and

$$a_n = \frac{2^n-2}{4!} + \frac{2^{n-1}-1}{2^2}$$

for n odd.

Here we deal with the case when n is even. So substituting a_{n-1} and a_{n-2} into the appropriate formulae above we have

$$a_{n-1} = \frac{2^{n-1}-2}{4!} + \frac{2^{n-2}-1}{2^2}$$

and

$$2a_{n-2} = \frac{2^{n-1}-4}{4!} + \frac{2^{n-2}-2}{2^2} + \frac{4}{3}.$$

We can see that $a_n = a_{n-1} + 2a_{n-2}$ in this case, as required. Similarly we can show that the result holds for n odd. The second expression of a_n follows.

□

This recursive formula generates the sequence $1, 1, 3, 5, 11, 21, 43, 85, 341, ...$ known as the Jacobsthal sequence [31].

Next, we follow the same process as above but for the Suzuki groups and obtain another sequence.

Proposition 4.2.2. *Let $a_n = \sigma_3(Sz(q))$, $q = 2^{2n+1}$, be the number of orbits on 3-subsets of the (q^2+1) points on which $Sz(q)$ acts. Then*

$$a_n = \frac{4^n + 2}{3}.$$

Proof. We substitute the values $q = 2^{2n+1}$, $k = 3$ and $r = 2^{n+1}$ into Theorem 3.3.2 and reduce. We note that as $2 \equiv -1 \bmod 3$, even powers of $2 \equiv 1 \bmod 3$.

We begin by determining the values for $\eta_k(1^{q^2+1})$ and $\eta_k(1^1 2^{\frac{q^2}{2}})$. It is clear that, respectively, these equal $\binom{q^2+1}{3}$ and $\frac{q^2}{2}$. It is also clear that $\eta_k(1^1 4^{\frac{q^2}{4}}) = 0$ when $k = 3$. For the remaining parts of the formula, m cannot equal 1, so for $\eta_k(1^2 m^{\frac{q^2-1}{m}})$ to be non-zero m would have to equal 2 or 3, as neither of these divide $(q-1)$, ($q - 1 \equiv 1 \bmod 2$ and $q - 1 \equiv 1 \bmod 3$), we have $\eta_k(1^2 m^{\frac{q^2-1}{m}}) = 0$. For $\eta_k(m^{\frac{q^2+1}{m}})$ to be non-zero, m would have to equal 3. Again this cannot happen as $m \in \mathcal{D}^*(q \pm r + 1)$ and we can see that $q + 1 \equiv 0 \bmod 3$ and $3 \nmid r$, hence the final two summations equal 0.

This gives us a total value for

$$\begin{aligned} a_n &= \frac{1}{q^2(q-1)(q^2+1)}\binom{q^2+1}{3} + \frac{1}{q^2}\binom{q^2}{2} \\ &= \frac{(q^2+1)(q^2)(q^2-1)}{6q^2(q-1)(q^2+1)} + \frac{1}{2} \\ &= \frac{q+4}{6} \\ &= \frac{2^{2n}+2}{3} = \frac{4^n+2}{3}, \end{aligned}$$

as required.

□

The first few terms of this sequence are 2, 6, 22, 86, 342 and 1366.

Next we highlight a sequence which occurs in the values of $\sigma_3(PSU(3,q))$ using Theorem 3.4.2.

Proposition 4.2.3. *Let $a_n = \sigma_3(PSU(3,3^n))$ be the number of orbits on 3-subsets of the $(3^{3n}+1)$ isotropic points on which $PSU(3,3^n)$ acts. Then*

$$a_n = \frac{3^n+3}{2}.$$

Proof. We prove the result by substituting the values $p=3$, $q=3^n$, $k=3$ and $d=1$ into the formula in Theorem 3.4.2.

Ignoring the coefficients for the moment, we wish to evaluate the contributions of each class type individually. That is calculate the values of each summation in turn.

Clearly $\eta_k(\pi_1) = \binom{q^3+1}{3}$, and $\mu_k = (q^3+1)(q^3-1)(\eta_k(\pi_2)) = (q^3+1)(q^3-1)(\frac{q^3}{p})$.

Now, $\sum_{m\in\mathcal{D}^*(\ell)} \phi(m)\eta_k(\pi_4^{(m)})$ is non zero for all values of m as each element will have $q+1$ fixed points, hence each will fix $\binom{q+1}{3}$ 3-subsets. As $\sum \phi(m) = \ell - 1$ in this instance, we have a q such elements. We also need consider the case $m=2$, ($q+1$ is even) as then we can construct 3-subsets from one of the fixed points and a cycle of length 2, this combines with the above to give a contribution to the total of

$$q\binom{q+1}{3} + \frac{q^3-q}{2}(q+1).$$

The value of

$$\sum_{\substack{m=pj \\ j\in\mathcal{D}^*(\ell)}} \phi(m)\eta_k(\pi_5^{(m)})$$

is slightly more subtle, we first note that the value of $\phi(m) = \phi(pj) = \phi(p)\phi(j) = 2\phi(j)$. These classes will all fix $\frac{q}{p}$ 3-subsets. As the sum of the $\phi(j)$s will total q, we have a contribution of $2q\frac{q}{p}$ (note that m cannot equal 2).

The value of $\varepsilon_k(E_0^*, \Omega)$ is zero as these elements all have cycles of lengths greater than 1 but dividing $q+1$, which 3 clearly does not.

Similarly the count for

$$\sum_{m \in \mathcal{D}^*(\frac{q^2-q+1}{d})} \phi(m)\eta_k(\pi_8^{(m)})$$

is zero, as again 3 is not a divisor of $q^2 - q + 1$.

Finally, we address the value of

$$\sum_{\substack{m \in \mathcal{D}(\frac{q^2-1}{d}) \\ m \notin \mathcal{D}(\ell)}} \phi(m)\eta_k(\pi_7^{(m)}).$$

We redefine $j = \frac{m}{(m,\ell)}$ as $j = \frac{q-1}{(\frac{q^2-1}{m}, q-1)}$, (we can see that these are identical in this case as $d = 1$ and so division of these two expressions gives the value 1). As for this summation, we will only obtain non-zero values for $\eta_k(\pi_7)$ when the greatest common divisor of $(\frac{q^2-1}{m}, q-1) = \frac{q-1}{2}$, we need understand this case and so take a generator of the subgroup of order $q^2 - 1$ and raise it to an appropriate power to obtain a cycle type containing cycles of length 2. This is equivalent to choosing m dividing $q^2 - 1$ such that the above condition on j is satisfied, and hence letting $m = 2(q+1)$ gives us an element of largest order in this subgroup with cycles of length 2. We denote such an element by h (where h has cycle type $\pi_7(m) = (2(q+1))^{\frac{q^3-q}{2(q+1)}} 2^{\frac{q-1}{2}} 1^2$) and know that all elements which fix 3-subsets will appear in $\langle h \rangle$, where $|\langle h \rangle| = 2(q+1)$. As the elements of $\langle h \rangle$ will have $(q+1)$ fixed points for even powers of h we must exclude these and only count the remaining $(q+1)$ relevant elements, each of which will fix $2^{\frac{q-1}{2}}$ 3-subsets. This gives us a total contribution of $(q+1)(q-1)$ fixed subsets.

Now we have values for each summation, we place these directly into the formula

as given and so

$$\begin{aligned} a_n &= \frac{1}{q^3(q^3+1)(q^2-1)}\left(\binom{q^3+1}{3} + (q^3+1)(q^3-1)(\frac{q^3}{3})\right), \\ &+\frac{1}{q^3(q^3+1)(q^2-1)}\left((q^4-q^3+q^2)(q\binom{q+1}{3} + \frac{q^3-q}{2}(q+1))\right), \\ &+\frac{1}{q(q+1)(2)}2q\frac{q}{3} + \frac{1}{2(q^2-1)}(q+1)(q-1). \end{aligned}$$

After much simplification

$$\begin{aligned} a_n &= \frac{q^3-1}{6(q^2-1)} + \frac{q^3-1}{3(q^2-1)} + \frac{4q+3}{6(q+1)} + \frac{q}{3(q+1)} + \frac{1}{2}, \\ &= \frac{q^2+q+1+2q^2+2q+2+4q+3+2q+3(q+1)}{6(q+1)}, \\ &= \frac{3q^2+12q+9}{6(q+1)}, \\ &= \frac{q^2+4q+3}{2(q+1)}, \\ &= \frac{q+3}{2}, \end{aligned}$$

as required. □

The sequence a_n given in Proposition 4.2.3 is also associated to Sierpinski's Triangle, see [32]. In that case the sequence determines the number of points in the n^{th} iteration of the fractal, the first few terms in this sequence are 3, 6, 15, 42, 123, and 366.

Proposition 4.2.4. *Let $a_n = \sigma_3(R(3^{2n+1}))$ be the number of orbits on 3-subsets of the q^3+1 points on which $R(q)$ acts. Then*

$$a_n = \frac{(3^{2n+1}+3)^2}{6}.$$

Proof. We substitute the value $k = 3$ into Theorem 3.5.4 and simplify. From the definitions, we can easily determine that η_k will be non-zero only for cycle types π_1, π_J, π_T and π_{JT}. It follows then that we need only consider these four parts of the formula and determine the η_3 values. This is straightforward in these cases,

$$\begin{aligned}
\eta_3(\pi_1(q)) &= \binom{q^3+1}{3}, \\
\eta_3(\pi_J(q)) &= \frac{q^3-q}{2}(q+1) + \binom{q+1}{3}, \\
\eta_3(\pi_T(q)) &= \frac{q}{3}, \\
\eta_3(\pi_{JT}(q)) &= \frac{q^3}{3}.
\end{aligned}$$

This gives us a value for $\sigma_3(R(q))$ of

$$\sigma_3(R(q)) = \frac{q^3(q^3+1)(q^3-1)}{6q^3(q^3+1)(q-1)} + \frac{(q^3-q)(q+1)}{2(q^3-q)} + \frac{q^3-q}{q(q^3-q)} + \frac{q(q+1)}{3q^3} + \frac{q}{3q},$$

which simplifies to

$$\sigma_3(R(q)) = \frac{q^2+6q+9}{6} = \frac{(q+3)^2}{6},$$

as required.

□

The first terms of this sequence are 150, 10086, 799350, 64589766 and 5230353750.

4.3 $PGL(2,q)$ Formula

We end this chapter with a look at establishing a more general formula for $\sigma_k(PGL(2,q))$. We replicate some of the methods used above whilst using a mixture of conjugacy classes and conjugate subgroups to form our partition.

Lemma 4.3.1. *Let $G \cong PGL(2,q)$ where q is a power of an odd prime, and let Ω be the projective line over $\mathbb{F}_q$ so that $|\Omega| = q+1$. Then*

(i) $|G| = q(q+1)(q-1)$,

(ii) there are q^2-1 elements of order p with cycle structure $1^1 p^{\frac{q}{p}}$ on Ω,

(iii) there exists a unique conjugacy class of cyclic subgroups H_+ such that $|H_+| = q+1$ with non trivial elements having cycle structure $m^{\frac{q+1}{m}}$ and $N_G(H_+)/H_+ \cong C_2$,

(iv) there exists a unique conjugacy class of cyclic subgroups H_- such that $|H_-| = q-1$ with non trivial elements having cycle structure $1^2, m^{\frac{q-1}{m}}$ and $N_G(H_-)/H_- \cong C_2$,

(v) G has $q+2$ conjugacy classes,

(vi) Let $P \in Syl_pG$, and set $\mathcal{S} = \{P^g, H_-^g, H_+^g \mid g \in G\}$. Then every non-identity element of G belongs to a unique subgroup in $\mathcal{S}$.

Proof. For (i) and (ii) see Huppert [13], for (iii) and (iv) see Huppert [13] and Faber [12] for (v) see Macdonald [17]. We show (v) by counting the number of classes contributed by the subgroups and noting that they sum to $q+2$. It is clear that the identity class and $P^{\#}$ both contribute a single conjugacy class each. The subgroups H_+ and H_- will contribute $\frac{q-1}{2}$ and $\frac{q-3}{2}$ classes from the elements of order greater than 2 respectively, with both cyclic subgroups contributing a further class of involutions each. This gives us $4 + \frac{q-1}{2} + \frac{q-3}{2} = q+2$ class representatives. We observe that the differing number of fixed points of Ω for each of these subgroups ensures they pairwise intersect trivially. □

Theorem 4.3.2. *Let $G = PGL(2,q)$, where $q = p^a$ for odd prime p, act on k-subsets of $\Omega = PG(1,q)$, the projective line with p and odd prime. Now let $\sigma_k(G,\Omega)$ denote the number of orbits G has on the set Ω_k.*

$$\begin{aligned}\sigma_k(G,\Omega) &= \frac{1}{q(q+1)(q-1)}\eta_k(1^{q+1}) + \frac{1}{q}\eta_k(1^1 p^{\frac{q}{p}}) \\ &+ \frac{1}{2(q+1)} \sum_{m \in \mathcal{D}^*((k,q+1))} \phi(m)\eta_k\left(m^{\frac{q+1}{m}}\right) \\ &+ \frac{1}{2(q-1)} \sum_{m \in \mathcal{D}^*(q-1)} \phi(m)\eta_k\left(1^2 m^{\frac{q-1}{m}}\right).\end{aligned}$$

Remark Since G acts 3-transitively on Ω, $\sigma_1(G,\Omega) = \sigma_2(G,\Omega) = \sigma_3(G,\Omega) = 1$.

Proof. This follows the proof of Theorem 3.2.1 almost identically. □

This result is in line with our previous result for $PSL(2,q)$, allowing us to use the same formula for both families of groups, setting the variable d equal to 1 in Theorem 3.2.1 when wishing to evaluate σ_k for $PGL(2,q)$.

Chapter 5

Discussion of Number of Orbit Tables

In the appendices, we include a number of tables of values for differing representations of some finite groups. One of the more interesting sections is the orbit counts for finite abelian groups, where we compare the values of σ_k for non-isomorphic finite abelian groups of equal order, acting in their regular representations. We then go on to show the lower bound for $\sigma_k(G)$ for such groups is attained when G is cyclic.

5.1 Cyclic Groups

Many of the results in this Chapter rely upon being able to write finite abelian groups as a product of cyclic groups where subsequent torsion coefficients divide the previous ones. This is due to the Classification of finitely generated abelian groups, which we repeat here.

Theorem 5.1.1. *[Classification of finite abelian groups] Any finite abelian group G is isomorphic to a direct product of cyclic groups*

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} ... \times \mathbb{Z}_{m_s},$$

where $m_1|m_2$, $m_2|m_3$,..., $m_{s-1}|m_s$ ($m_1 > 1$). The values m_i are called the torsion coefficients of G.

For further details of this see for example [35].

We now state a result we used implicitly in Chapter 3.

Proposition 5.1.2. *Let G be a cyclic permutation group of order n acting regularly on a set Ω of size n. Then for $k \leq n$ we have*

$$\sigma_k = \frac{1}{n} \sum_{m \in \mathcal{D}(n)} \phi(m)\eta_k(m^{\frac{n}{m}}).$$

Proof. We count the number of fixed points in the G-action on k-subsets of Ω for an element of G with order m, this is given by $\eta_k(m^{\frac{n}{m}})$ as any such element will have cycle type $m^{\frac{n}{m}}$, by Lemma 3.1.1 there will be $\phi(m)$ such elements in G. Substitution into Theorem 1.0.4, gives the result. □

Proposition 5.1.3. *Let G be a cyclic permutation group of order n acting regularly on a set Ω of size n. Then for $k \leq n$ such that $(n, k) = 1$ we have all orbits are regular and*

$$\sigma_k = \frac{\binom{n}{k}}{n}.$$

Proof. As G is regular cyclic, we have that elements in G of order m will have cycle structure $m^{\frac{n}{m}}$ where m is a divisor of n, moreover for a k-subset to be stabilized by some non-trivial group element there must exist m dividing k. Therefore we are only concerned with elements of orders dividing $(k, n) = 1$. Hence no such k-subset can have a non-trivial stabilizer. □

Definition 7. Let G be a group. Then for m dividing $|G|$ we denote the number of elements of G with order m by $\mathfrak{O}_m(G)$.

Lemma 5.1.4. *Let G be an abelian group of order n and let m be a divisor of n where $m = p_1^{a_1}, ..., p_s^{a_s}$, for distinct primes p_i. Then*

$$\mathfrak{O}_m(G) = \prod_{i=1}^{s} \mathfrak{O}_{p_i{}^{a_i}}(G).$$

Proof. For $m = p_1^{a_1}$ we clearly have that $\mathfrak{O}_m(G) = \mathfrak{O}_{p_1{}^{a_1}}(G)$.

Now assume the statement for all $i \leq t$. We now count the number of elements of order $p_1^{a_1}...p_{t+1}^{a_{t+1}}$. As G is abelian such elements are of the form gh where $g \in G$ and has order $p_1^{a_1}...p_t^{a_t} = m_1$ and $h \in G$ with order $p_{t+1}^{a_{t+1}} = m_2$, note that m_1 and m_2 are coprime ($(gh)^{m_1} = h$ and $(gh)^{m_2} = g$). By induction there are $\mathfrak{O}_{m_1}(G)$ choices for g and $\mathfrak{O}_{m_2}(G)$ choices for h giving us

$$\mathfrak{O}_{m_2}(G) \times \mathfrak{O}_{m_1}(G) = \prod_{i=1}^{t+1} \mathfrak{O}_{p_i{}^{a_i}}(G)$$

as required. □

Proposition 5.1.5. *Let $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, such that $n_2 \mid n_1$. Then denote n_2 by its product of prime factors, $p^a p_1^{a_1} ... p_s^{a_s}$ for primes p and p_i, $a_i \in \mathbb{N}$ $i = 1...s$ $a \in \mathbb{N} \cup \{0\}$. Then for a prime power $p^x \mid n_1$ we have*

$$\mathfrak{O}_{p^x}(G) = \begin{cases} \phi(p^x) \sum_{i=0}^{a} \phi(p^{a_i}), & \text{if } p^x \nmid n_2 \\ \phi(p^x) \left(\phi(p^x) + 2 \sum_{i=0}^{x-1} \phi(p^{a_i}) \right), & \text{if } p^x \mid n_2 \end{cases}$$

Proof. We begin by recalling the notation of $\mathcal{D}(s)$ to be the set of divisors of $s \in \mathbb{N}$. We need to enumerate the number of pairs of elements $x \in \mathbb{Z}_{n_1}$ and $y \in \mathbb{Z}_{n_2}$ with orders denoted $o(a, b) \in \mathcal{D} = \mathcal{D}(n_1) \times \mathcal{D}(n_2)$ with lowest common multiple of a and b equal to p^x. We will use Lemma 3.1.1 to infer that for a pair of divisors $o(a, b) \in \mathcal{D}$ there are $\phi(a)\phi(b)$ choices for elements in G.

We first consider the case when $p^x \nmid n_2$, then we need to count the pairs in $\mathcal{D}$ with lowest common multiple p^x. That is pairs of the form $o(p^x, 1), o(p^x, p), ..., o(p^x, p^a)$ of which there are

$$\phi(p^x)\phi(p^0) + ... + \phi(p^x)\phi(p^a) = \phi(p^x) \sum_{i=0}^{a} \phi(p^i)$$

such elements in G.

Secondly we consider when $p^x \mid n_2$, then we need pairs in $\mathcal{D}$ of the form

$$o(p^x, 1), o(p^x, p), ..., o(p^x, p^x), o(p^{x-1}, p^x), ..., o(p^0, p^x)$$

of which there are

$$\phi(p^x)\phi(p^0)+...+\phi(p^x)\phi(p^x)+\phi(p^{x-1})\phi(p^x)+...+\phi(p^0)\phi(p^x) = \phi(p^x) \left(\phi(p^x) + 2 \sum_{i=0}^{x-1} \phi(p^i) \right)$$

such elements.

□

Remark The above two results allow us to count the number of elements of a given order in a direct product of two cyclic groups, but also we see that the orders and number of elements with any such order is entirely defined by the number of elements with prime power order.

Definition 8. Let G be a finite group. Then denote by O_G the monotonic increasing sequence $(m_i)_{i=1}^{|G|}$ where m_i is the order of element $g_i \in G$ where $g_i \neq g_j$ for $i \neq j$ and $1 \leq i \leq |G|$. Then let P_G be the subsequence of O_G containing only those terms which equal a prime power.

Proposition 5.1.6. *Let $G \cong \mathbb{Z}_n$ and $H \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ with $n_2 \mid n_1$ and $n = n_1 n_2$. Then we can define an one-to-one correspondence $\rho : O_G \to O_H$ such that $\rho(g_i) \mid g_i$ for all $1 \leq i \leq n$.*

Proof. As the terms in the sequences O_G and O_H are element orders of abelian groups we can apply Lemmas 5.1.4 and 5.1.5 to calculate the multiplicity of each value in either sequence. As this is entirely defined by the terms of O_G and O_H which are prime powers, we first define a map $\rho_p : P_G \to P_H$ on the subsequences of O_G and O_H consisting of all values which are prime powers. Then by showing this is one to one we can then extend ρ_p to ρ by $\rho(p_1^{a_1}...p_s^{a_s}) = \rho_p(p_1^{a_1})...\rho_p(p_s^{a_s})$ where p_i are distinct primes dividing g_i, $a_i \in \mathbb{N}$.

We define ρ_p as follows, let p be a prime dividing n and let p^c be the largest power of p dividing n_2. Then for a prime power $p^x \mid n$ we have

$$\rho_p(p^x) = \begin{cases} p^x, & \text{if } p \nmid n_2 \\ p^{x/2}, & \text{if } x \text{ is even and } x \leq 2c \\ p^{(x+1)/2}, & \text{if } x \text{ is odd and } x \leq 2c \\ p^{x-c} & \text{if } x > 2c. \end{cases}$$

We note that this covers all possible values of p^x in both P_G and P_H. Next we show this is an injective mapping by demonstrating equality in the multiplicities. In the first case we have $p \nmid n_2$, it follows then that for such a value all the elements of G with the order p^x are contained in the unique cyclic subgroup of G with order p^x and as such there are $\phi(p^x)$ such elements in G and hence there are $\phi(p^x)$ such terms in P_G. Similarly as $p \nmid n_2$ all such elements in H are contained in the cyclic subgroup $\mathbb{Z}_{p^x} \times 1$ and so we have $\phi(p^x)$ such elements and hence terms in P_H giving us a one to one correspondence for these elements.

For the second and third cases we will let $p^x = p^{2k}$ and $p^x = p^{2k-1}$ when x is even and odd respectively. Now in order to show that ρ_p maintains a one to one correspondence it is enough to show that

$$\mathfrak{O}_{p^{2k}}(G) + \mathfrak{O}_{p^{2k-1}}(G) = \mathfrak{O}_{p^k}(H) \tag{5.1}$$

for $p^k \mid n_2$, this is due to both these values in P_G being mapped to terms with equal value in P_H.

As G is cyclic and by recalling that $\phi(p^a) = p^{a-1}(p-1)$ we can easily determine the left hand side of equation (5.1),

$$\begin{aligned}\phi(p^{2k}) + \phi(p^{2k-1}) &= p^{2k-1}(p-1) + p^{2k-2}(p-1)\\ &= p^{2k} - p^{2k-1} + p^{2k-1} - p^{2k-2}\\ &= p^{2k} - p^{2k-2}.\end{aligned}$$

Hence there are $p^{2k} - p^{2k-2}$ terms in P_G equal to either p^{2k} or p^{2k-1}. For the right hand side of equation (5.1) we use Proposition 5.1.5 and so we have

$$\begin{aligned}\mathfrak{O}_{p^k}(H) &= \phi(p^k)\left(\phi(p^k) + 2\sum_{i=0}^{k-1}\phi(p^i)\right),\\ &= \phi(p^x)(\phi(p^x) + 2(1 + (p-1) + p(p-1) + ... + p^{k-1}(p-1))),\\ &= \phi(p^x)(\phi(p^x) + 2 + 2((p-1) + p(p-1) + ... + p^{k-1}(p-1))),\\ &= \phi(p^x)(\phi(p^x) + 2 + 2\left(\frac{(p-1)(p^{k-1}-1)}{(p-1)}\right)),\\ &= \phi(p^x)(\phi(p^x) + 2 + 2(p^{k-1} - 1)),\\ &= p^{k-1}(p-1)(p^{k-1}(p-1) + 2p^{k-1}),\\ &= p^{2k-2}(p^2 - 2p + 1) + 2p^{2k-1} - 2p^{2k-2},\\ &= p^{2k} - 2p^{2k-1} + p^{2k-2} + 2p^{2k-1} - 2p^{2k-1},\\ &= p^{2k} - p^{2k-2}.\end{aligned}$$

Hence these terms are in a one to one correspondence also.

Finally we show that for $p^x > p^{2c}$, we have $\mathfrak{O}_{p^x}(G) = \mathfrak{O}_{p^{x-c}}(H)$. Starting with the right side of the equation and using Proposition 5.1.5, whilst noting that as $x > 2c$ we have $x - c > c$ and so $p^{x-c} \nmid n_2$, we have

$$\begin{aligned}\mathfrak{O}_{p^{x-c}}(H) &= \phi(p^{x-c})\sum_{i=0}^{c}\phi(p^i),\\ &= \phi(p^{x-c})(1 + (p-1) + p(p-1) + ... + p^{c-1}(p-1)),\\ &= \phi(p^{x-c})\left(\frac{(p-1)(p^c-1)}{(p-1)}\right),\\ &= p^{x-c-1}(p-1)(1 + (p^c - 1)),\\ &= (p^{x-c} - p^{x-c-1})(p^c),\\ &= p^x - p^{x-1},\\ &= p^{x-1}(p-1) = \phi(p^x) = \mathfrak{O}_{p^x}(G)\end{aligned}$$

as required. Hence ρ_p is a one to one correspondence and so by Proposition 5.1.4 ρ is also.

Now as ρ_p is such that $\rho_p(g_i) \mid g_i$ it follows that $\rho(g_i) \mid g_i$ for all i also.

□

Remark We note that the mapping is such that $\rho(m) = m$ if and only if $gcd(m, n_2) = 1$ and $\rho(m) \mid m$ otherwise. This can be seen from the definition of ρ_p given in the proof of Proposition 5.1.6.

Example Let $G \cong \mathbb{Z}_{48}$ and $H \cong \mathbb{Z}_{12} \times \mathbb{Z}_4$. Then we have the following table

m (Order of $g \in G$)	$\phi(m) = \mathfrak{O}_m(G)$	$\rho(m)$	$\mathfrak{O}_m(H)$
1	1	1	1
2	1	2	3
3	2	3	2
4	2	2	12
6	2	6	6
8	4	4	24
12	4	6	0
16	8	4	0
24	8	12	0
48	16	12	0

With the above remark in mind we present the following Theorem.

Theorem 5.1.7. *Let $G = \mathbb{Z}_n$ and $H = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ such that $n_2 \mid n_1$ and $n = n_1 n_2$. Let G and H act in their regular representations on n points. Then for k-subsets we have*

$$\sigma_k(G) \begin{cases} = \sigma_k(H), & \text{for all } k \text{ such that } (n_2, k) = 1 \\ \leq \sigma_k(H), & \text{for all } k \text{ such that } (n_2, k) \neq 1. \end{cases}$$

Proof. Let K_G be the subsequence of O_G containing all terms which divide $gcd(k, n)$. Then to count the number of G-orbits we need only calculate

$$n\sigma_k(G) = \sum_{i=1}^{|K_G|} \binom{\frac{n}{g_i}}{\frac{k}{g_i}}.$$

Now if we compare K_G to the subsequence of O_H containing all terms dividing $gcd(k, n)$ then this subsequence equals $\rho(K_G)$, and so we have a subsequence of O_H of length $|K_G|$ containing only terms with the property that $\rho(g_i) \mid g_i$ for all $1 \leq i \leq |K_G|$.

Now for a given k, if $gcd(k, n_2) = 1$ then for all i we have $\rho(g_i) = g_i$. Furthermore this gives

$$n\sigma_k(G) = \sum_{i=1}^{|K_G|} \binom{\frac{n}{g_i}}{\frac{k}{g_i}} = \sum_{i=1}^{|K_G|} \binom{\frac{n}{\rho(g_i)}}{\frac{k}{\rho(g_i)}} = n\sigma_k(H).$$

However if $gcd(k, n_2) > 1$ then there exists some $g_i \mid gcd(k, n)$ such that $\rho(g_i) \leq (g_i)$ and so

$$n\sigma_k(G) = \sum_{i=1}^{|K_G|} \binom{\frac{n}{g_i}}{\frac{k}{g_i}} \leq \sum_{i=1}^{|K_G|} \binom{\frac{n}{\rho(g_i)}}{\frac{k}{\rho(g_i)}} = n\sigma_k(H).$$

□

Corollary 5.1.8. *Let*

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{(m_{n-1})(m_n)},$$

and let

$$H \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{(m_{n-1})} \times \mathbb{Z}_{(m_n)},$$

where $hcf(m_1, m_2, ..., m_n) = m_n$.

$$\textit{Then } \sigma_k(G) = \begin{cases} \sigma_k(H), & \textit{for all } k \textit{ where } (k, m_i) = 1 \textit{ for all } i \\ \leq \sigma_k(H), & \textit{for all } k \textit{ where } (k, m_i) \neq 1 \textit{ for some } i. \end{cases}$$

Proof. We can apply the map ρ from Proposition 5.1.6 to the $\mathbb{Z}_{(m_{n-1})(m_n)}$ component of G with image the $\mathbb{Z}_{(m_{n-1})} \times \mathbb{Z}_{(m_n)}$ component of H. We can determine the orders of elements of G by using the lowest common multiple of the $n-1$-tuple of the element orders from each product. We then construct a mapping from G to H by applying the map ρ_n to these $(n-1)$-tuples where ρ_n fixes all coordinate points $i = 1...n-2$ and applies the mapping ρ from Proposition 5.1.6 to the $(n-1)^{th}$ position to obtain an n-tuple. It is clear then that we have a one to one mapping from the sequence of element orders of G to the sequence of element orders of H where the order of $\rho_n(g)$ divides the order of g for all $n-1$-tuples representing elements of G.

□

Theorem 5.1.9. *Let G and H be groups of order n acting in their regular representations on k-subsets of group elements. If $\mathfrak{O}_m(G)$ denotes the number of elements of G of order m then*

$$\sigma_i(G) = \sigma_i(H) \textit{ for all } 1 \leq i \leq n \iff \mathfrak{O}_j(G) = \mathfrak{O}_j(H) \textit{ for all } 1 \leq j \leq n.$$

Proof. In the regular representation we have that only the identity fixes any single point and every other element can be expressed as disjoint cycles of length equal to the order of the element.

Clearly if $\mathfrak{O}_j(G) = \mathfrak{O}_j(H)$ for all $1 \leq j \leq n$ then counting the number of fixed points will be determined by the cycle types and hence the orders of the elements of each group, as each group has an equal number of elements of a given order the number of fixed k-sets will be equal, hence by the Orbit Stabilizer Theorem we have $\sigma_i(G) = \sigma_i(H)$ for all $1 \leq i \leq n$.

If we have that $\sigma_i(G) = \sigma_i(H)$ for all $1 \leq i \leq n$ then for $\Delta \subseteq \Omega$, with $g \in G$ stabilizing Δ with the order of g being such that $\langle g \rangle$ is not contained in any other cyclic subgroup of G_Δ then we must have that Δ is the disjoint union of g-cycles and so Δ is stabilized by all $g' \in \langle g \rangle$.

Now choose $h \in G \setminus \langle g \rangle$, if such an element exists, where $h \in G_{\{\Delta\}}$, then no h-cycle can intersect any g cycle in more than one point. Otherwise for some α and β if $\alpha g^x = \beta$ and $\alpha h = \beta$ then we have $g^x = h$, contradicting our choice of h. It follows then that Δ can only be stabilized by cyclic subgroups with trivial pairwise intersection. Hence for the count of fixed points to be equal for all i, we must have that both G and H have a one to one correspondence between elements of a given order, and so $\mathfrak{O}_j(G) = \mathfrak{O}_j(H)$ for all $1 \leq j \leq n$.

□

Remark This result does not imply isomorphism. For example the group of upper triangular 3×3 unipotent matrices over $\mathbb{F}_p$ and the group $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$, will both have one element of order 1 and $p^3 - 1$ elements of order p. However these two groups are not isomorphic.

5.2 Non-regular representation

After considering direct products of groups, it makes sense to return to our motivation of the Livingstone-Wagner Theorem, and the question as to cases of equality. In this section we show how we can create a group with arbitrary lengths of equality in the Livingstone-Wagner Theorem and with a determined value of σ for these lengths. We attack this by making use of specific induced actions of some intransitive groups.

Let G_1 and G_2 be groups acting on the sets Ω_1 and Ω_2 respectively. Then define $\Omega = \Omega_1 \cup \Omega_2$ and define an action from $G = G_1 \times G_2$ on Ω, such that for $\alpha \in \Omega$, $(g, h) \in G$ we have $\alpha^{(g,h)} = \alpha^g$ if $\alpha \in \Omega_1$, and $\alpha^{(g,h)} = \alpha^h$ if $\alpha \in \Omega_2$.

Lemma 5.2.1. *Let $G = G_1 \times G_2$, for groups G_1 and G_2, where G_1 and G_2 act on sets Ω_1 and Ω_2 respectively and G acts on $\Omega = \Omega_1 \cup \Omega_2$ as described above. Let σ_i^1 be the number of G_1-orbits on i-subsets on Ω_1, and σ_i^2 be the number of G_2-orbits on i subsets of Ω_2. Then if σ_k is the number of G-orbits on k-subsets of Ω, we have*

$$\sigma_k = \sum_{i=0}^{k} \sigma_i^1 \sigma_{k-i}^2.$$

Proof. This follows from the k-sets being constructed from disjoint unions of G_1 i-sets and G_2 $(k-i)$-sets. □

Definition 9. We say the increasing sequence σ_n stutters from a to b for $a, b \in \mathbb{N}$ if $\sigma_a = \sigma_i$ for all $a \leq i \leq b$.

Proposition 5.2.2. *Let G, G_1, G_2, Ω, Ω_1 and Ω_2 be as in Lemma 5.2.1. Suppose that $|\Omega_1| = m_1$, G_1 is j-homogeneous for all values $1 \leq j \leq m_1$ and G_2 is m_2-homogeneous for $m_1 \leq m_2 \in \mathbb{N}$. Then the sequence $\sigma_i(G, \Omega)$, $1 \leq i \leq |\Omega|$ will stutter from m_1 to m_2 and have the value $m_1 + 1$.*

Proof. This follows from Lemma 5.2.1, we note that as G_1 will have no orbits on k-subsets for $k > m_1$, the value of σ_k^1 will be zero for such k. □

We give examples of Proposition 5.2.2 using Lemma 5.2.1 to evaluate σ_k. Letting G_1 and G_2 be highly transitive (or homogeneous) we can build a sequence of values for $\sigma_k(G)$ which will stabilize at a given value.

Example We begin with letting $G_1 = A_4$ be the alternating group on 4 points and $G_2 = A_6$ the alternating group on 6 points. Then $\Omega = \{1, ..., 10\}$, with G_1 acting on $\{1, 2, 3, 4\}$ and G_2 acting on $\{5, 6, 7, 8, 9, 10\}$. Then $G = G_1 \times G_2$ acts on Ω as described above. Hence

$\sigma_1(G) = 1 + 1 = 2,$

$\sigma_2(G) = 1 + (1 \times 1) + 1 = 3,$

$\sigma_3(G) = 1 + (1 \times 1) + (1 \times 1) + 1 = 4,$

$\sigma_4(G) = 1 + (1 \times 1) + (1 \times 1) + (1 \times 1) + 1 = 5,$

$\sigma_5(G) = 0 + (1 \times 1) + (1 \times 1) + (1 \times 1) + (1 \times 1) + 1 = 5.$

We can show this in the general setting with the next example.

Example Letting $G_1 = A_i$ be the alternating group on i points and $G_2 = A_n$ the alternating group on n points, for n large enough to produce the length of stutter you require, we can generate a set of results for values of i.

$i =$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	σ_9	
1	2	2	2	2	2	2	2	2	2	$\cdots$
2	2	3	3	3	3	3	3	3	3	$\cdots$
3	2	3	4	4	4	4	4	4	4	$\cdots$
4	2	3	4	5	5	5	5	5	5	$\cdots$
5	2	3	4	5	6	6	6	6	6	$\cdots$
6	2	3	4	5	6	7	7	7	7	$\cdots$
7	2	3	4	5	6	7	8	8	8	$\cdots$
8	2	3	4	5	6	7	8	9	9	$\cdots$
9	2	3	4	5	6	7	8	9	10	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 5.1: Number of Orbits for $G = A_i \times A_n$

Next we consider an example where $G = PSL(2,7) \times PSL(2,11)$.

Example We begin with letting $G_1 = PSL(2,7)$ act on 8 points and $G_2 = PSL(2,11)$ act on 12 points. Then $\Omega = \{1, ..., 20\}$, with G_1 acting on $\{1,2,3,4,5,6,7,8\}$ and G_2 acting on $\{9,10,11,12,13,14,15,16,17,18,19,20\}$. Then $G = G_1 \times G_2$ acts on Ω as described above. Hence using the results in Table 2.4 we have the following

$\sigma_1(G) = 1 + 1 = 2,$

$\sigma_2(G) = 1 + (1 \times 1) + 1 = 3,$

$\sigma_3(G) = 1 + (1 \times 1) + (1 \times 1) + 1 = 4,$

$\sigma_4(G) = 3 + (1 \times 1) + (1 \times 1) + (1 \times 1) + 2 = 8,$

$\sigma_5(G) = 3 + (3 \times 2) + (1 \times 1) + (1 \times 1) + (1 \times 2) + 2 = 15,$

$\sigma_6(G) = 1 + (3 \times 1) + (3 \times 1) + (1 \times 1) + (1 \times 2) + (1 \times 2) + 6 = 18,$

$\sigma_7(G) = 18,$

$\sigma_8(G) = 22,$

$\sigma_9(G) = 22,$

$\sigma_{10}(G) = 30.$

Chapter 6

Orbit Lengths

Here, we look at the lengths of G-orbits of a permutation group, G, acting on Ω_k, the set of k subsets of a G-set Ω. We take a general view of this initially and later in the chapter we move towards a particular question, which was highlighted by Siemons and Wagner [27] in 1988.

It would be preferable for there to be an analogous result to the Livingstone-Wagner Theorem but relating to orbit lengths. Something along the lines of when we consider the action on k-subsets, when we reach a value of k for which there appears a regular orbit we always have a regular orbit for all values $(k+i) < n/2$, but we can see that $PSL(2,11)$ is a counter example for $k = 5$. Even a result about the minimum length of an orbit increasing does not hold, again we can cite $PSL(2,11)$ as a counterexample (see Table 2.4).

6.1 General Results

We know from classical results that for a finite group G acting on Ω, the length of any G-orbit of $\alpha \in \Omega$ satisfies $|\alpha^G| = \frac{|G|}{|G_\alpha|}$. There has been some work on calculating the lengths of orbits when G acts on k-subsets of a G-set Ω. Specifically a search for results linking the length of an orbit of a k-set Δ, with that of the length of the orbit of a $(k+1)$-set Σ containing Δ. Throughout this chapter we denote the setwise stabilizer of Δ in G by G_Δ, and the pointwise stabilizer of Δ in G by $G_{(\Delta)}$.

In 1997 Mnukhin looked at bounding the possible lengths of orbits when you increase the value of k and presented the following result in his paper titled "Some

relations for the lengths of orbits on k-sets and $(k-1)$-sets".

Theorem 6.1.1. *[Mnukhin [19]]*

Let G be a permutation group on the set Ω and let $\Sigma \subseteq \Omega$ be a k-set, $k \geq 2$. Then there is a $(k-1)$-subset, $\Delta \subset \Sigma$ such that

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

Although this is a bounding property it is not particularly strong, indeed the example given in the paper demonstrates this.

Example For $G \cong PSL(2,29)$, every 5-orbit of length 24360 contains a sub-orbit of length greater than 280. We will compare this to a second lower bound established for this case after Lemma 6.1.4.

We can add the following simple Lemma.

Lemma 6.1.2. *Let G be a permutation group acting on a set Ω of cardinality n, and let Σ be a k subset of Ω. Then denote the G-orbit of Σ by Σ^G. Let Δ be a $(k-1)$-subset of Σ and denote its G-orbit by Δ^G, then*

$$|\Delta^G| \leq k|\Sigma^G|,$$

for all $2 \leq k \leq n/2$.

Proof. Let $\Sigma = \{\alpha_1, \alpha_2, ..., \alpha_k\}$, then for a fixed group element $g \in G$ we have $\Sigma^g = \{\alpha_1^g, \alpha_2^g, ..., \alpha_k^g\} = \{\beta_1, \beta_2, ..., \beta_k\}$, where $\beta_i \in \Omega$. Now let H be the subset of G containing only elements of G which map Σ to Σ^g.

Take a $(k-1)$ element subset, $\Delta \subset \Sigma$ where, without loss of generality, $\Delta = \{\alpha_1, \alpha_2, ..., \alpha_{k-1}\}$. Then $\Delta^h \subset \Sigma^g$ for all $h \in H$.

Clearly there are at most k possible images for Δ under the action of elements in H. As this holds for any image of Σ in Σ^G we have the required inequality. □

Corollary 6.1.3. *Let G be a permutation group on the set Ω and let $\Sigma \subseteq \Omega$ be a k-set, $k \geq 2$. Then there is a $(k-1)$-subset, $\Delta \subset \Sigma$ such that*

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

For example, if G is a permutation group acting on a set and it has only one orbit of length 56 on 3-subsets, then every orbit of 4-subsets must be of length at least 14. This example is obtained for $G = PSL(2, 7)$ can be seen Table 2.4.

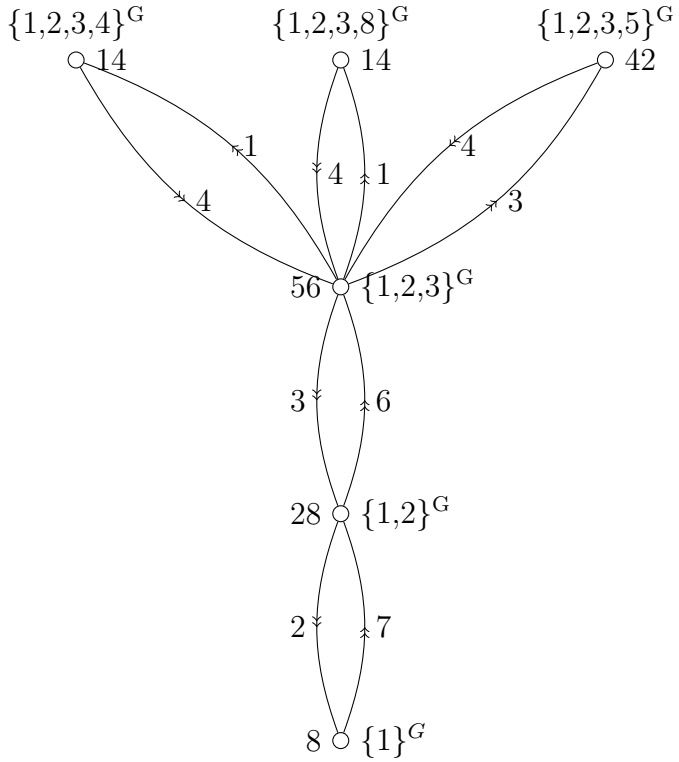
We will make use of the following simple Lemma.

Lemma 6.1.4. *Let G be a permutation group acting on n points, let Σ^G be an G-orbit of a $(k+1)$-subset and Δ^G and G-orbit of a k-subset Δ with $\Sigma \supset \Delta$. Then letting $d = |\{\alpha \in \Sigma \mid \Sigma \setminus \{\alpha\} \in \Delta^G\}|$ and $u = |\{\beta \in \Omega \mid \Delta \cup \{\beta\} \in \Sigma^G\}|$ then*

$$d|\Sigma^G| = u|\Delta^G|.$$

Proof. We form a graph with vertex set the elements of Σ^G and Δ^G, then we draw edge (s, t) if and only if $t \subset s$. Then the number of edges is equal to $d|\Sigma^G|$ and $u|\Delta^G|$. □

We use $PSL(2, 7)$ in its doubly-transitive action on 8 points (see Chapter 2) as an example of this Lemma we draw the diagram below. Here the numbers on upward arrows denote u and numbers on downward arrows denote d, the nodes represent G-orbits and are labelled with an orbit representatives and the length of the orbit.



We now revisit the example in Mnukhin's paper and by applying Lemma 6.1.4 we see that the minimum bound for the sub orbit length is actually 1015.

In 1988 Siemons and Wagner [27] published an interesting paper which looked at cases where the length of a k-subset orbit is longer than that the orbit of any $(k+1)$ overset. They obtained some examples of groups where this phenomenon is observed and classified all instances when $k = 2$.

Theorem 6.1.5. *[Siemons and Wagner [27]]*

Let G be a transitive permutation group of degree $n > 4$ acting on a set Ω. 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 $G \cong PSL(2,5)$ acting on 6 points. Otherwise G has three blocks of imprimitivity Ω^1, Ω^2 and Ω^3 with $|\Omega^i|$ a power of 2. Furthermore $\Delta^G = \{\{\alpha, \beta\} \mid \alpha \in \Omega^i \neq \Omega^j \ni \beta\}$ and G has order $3 \cdot |\Omega^i|^2 \cdot |G_\Delta|$ with $|G_\Delta| \leq 2$.

They also presented a result which is more general

Theorem 6.1.6. *[Siemons and Wagner [27]]*

Let G be a transitive permutation group on a finite set Ω and let Δ be a subset of Ω of cardinality k such that $|\Delta^G| > |\Sigma^G|$ for every subset Σ containing Δ of cardinality $k+1$. Then

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

Furthermore, if $k \geq 2$ 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 $\{\alpha_i, \alpha_j\}$ with $\alpha_i \in \Omega^i \neq \Omega^j \ni \alpha_j$ is contained in some G image of Δ.

It is suggested, by calculation, that this behaviour is rare and we can classify all instances in primitive groups when the degree is less than 25.

Proposition 6.1.7. *Let G be a primitive permutation group acting on a set of degree $n \leq 25$. Suppose that there exists a k-subset, $\Delta \subset \Omega$ such that $|\Delta^G| > |\Sigma^G|$ for any $(k+1)$-subset $\Sigma \subset \Omega$. Then G appears in Table 6.1.*

Proof. This list was compiled by direct calculation in Magma on the 183 primitive permutation groups of degree less than 25. The following code was used to check for the Siemons Wagner property, out putting the primitive groups satisfying the criteria and an example of such a k-subset.

Group	Degree	k
$PSL(2,5)$	6	2
$PSL(2,7)$	8	3
$PGL(2,7)$	8	3
$PSL(2,9)$	10	4
$Sym(6)$	10	4
$PSL(2,11)$	12	5
$PGL(2,11)$	12	5
$PSL(2,13)$	14	6
$Alt(7)$	15	6
$ASL(2,4)$	16	6
$Alt(7) \ltimes (\mathbb{Z}_2)^4$	16	7
$PSL(2,16)$	17	5
$PSL(3,4)$	21	6
$M(22)$	22	10
$M(23)$	23	10
$M(24)$	24	11

Table 6.1: Primitive permutation groups satisfying Siemons-Wagner property

```
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)); 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 for;
end procedure;
```

Letting D be the degree.

```
for k in [3..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;
```

□

Remark We note that the database of primitive groups used in the MAGMA calculations was produced by Roney-Dougal in [25] and Sims [30].

Example Here we demonstrate the above MAGMA code checking primitive groups of degrees between 6 and 10.

```
for D in [6..10] do
for> for k in [2..Z!(Floor(D/2)-1)] do
for|for> 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;end for;
<6, 1, {<15, { 1, 5 }>}>
<8, 4, {<56, { 4, 6, 7 }>}>
<8, 5, {<56, { 5, 6, 7 }>}>
<10, 3, {<180, { 1, 4, 5, 8 }>}>
<10, 4, {<180, { 3, 5, 9, 10 }>}>
```

6.2 Siemons-Wagner Property when $k = 3$

Taking our lead from Siemons and Wagner we consider the next value for k. That is when we have a 3-subset, Δ, with orbit of greater length than the orbit of any 4-subset Σ containing Δ. We have seen examples of this in $PSL(2,7)$ and $PGL(2,7)$ in Proposition 6.1.7, however, further calculation shows these are the only examples of degree $n \leq 200$. Furthermore we split Theorem 6.1.6 into two parts and here we are only concerned with accounting for primitive groups satisfying condition (i) of Theorem 6.1.6.

We present here, a list of results about the possible structure of such a group as well as some information on the relative sizes of the orbits, including Proposition 6.2.3 which states that the orbit of Δ is of greatest length amongst all the orbits on 3-subsets, and conclude by classifying all examples where the group G is 3-homogeneous.

Definition 10. For this chapter we will say that a group G satisfies condition $(\star)$ if G is a transitive permutation group of degree $n \geq 8$, acting on a set Ω, and that there exists a 3-subset Δ such that $|\Delta^G| > |\Sigma^G|$ for every 4-subset Σ containing Δ.

Definition 11. Let G be a permutation group acting transitively on a set Ω. Let the number of G_α-orbits on Ω equal t. Then we say G has rank t.

Lemma 6.2.1. *Let G satisfy $(\star)$, denote the subset Δ by $\{\alpha, \beta, \gamma\}$. If G satisfies condition (i) of 6.1.6 and G_Δ is transitive on Δ then G is 2-homogeneous and either 2-transitive or has rank 3.*

Proof. By Theorem 6.1.6(i) every 2-subset of Ω can be mapped onto some 2-subset of Δ. As G_Δ is transitive on the 2-subsets of Δ we have that all 2-subsets of Ω are in a single orbit.

As G_Δ is transitive on Δ we have that for all $g \in G$ such that $\alpha^g \in \Delta$, there exists $h \in G_\Delta$ such that $(\alpha^g)^h = \alpha$.

We know that every 2-subset of Ω is contained in some G-image of Δ, so we choose a 2-subset $\{\alpha, \delta\}$ for $\alpha, \delta \in \Omega$ $\alpha \neq \delta$ and choose $g \in G$ such that $\{\alpha, \delta\}^g \subset \Delta$. As $\{\alpha, \delta\}^g = \{\alpha^g, \delta^g\}$ we may now choose our $h \in G_\Delta$ such that $(\alpha^g)^h = \alpha$ and so $(\delta^g)^h \in \{\beta, \gamma\}$. However, $gh \in G_\alpha$ and so G_α has at most two orbits on $\Omega \setminus \{\alpha\}$.

□

We use Lemma 6.2.1 to prove our first result about groups satisfying $(\star)$.

Theorem 6.2.2. *Let G be a permutation group satisfying $(\star)$ and condition (i) of 6.1.6. If G_Δ is transitive on Δ then G is 2-transitive.*

Proof. We begin by assuming G is not 2-transitive. By Proposition 6.2.1 we have that G_α has exactly two orbits on $\Omega \setminus \{\alpha\}$ for $\alpha \in \Omega$, hence, by a result by Sims [29] there are exactly two G-orbits on ordered pairs $(\alpha, \beta) \in \Omega \times \Omega$ with $\alpha \neq \beta$. We then choose any ordered pair from each of these orbits and denote them by (a, b) and (c, d). As G is 2-homogeneous (by Proposition 6.2.1), we may map both of the sets $\{a, b\}$ and $\{c, d\}$ to the set $\{\alpha, \beta\}$, as these two ordered pairs are in distinct orbits we must have, without loss, that $(a, b)^{g_1} = (\alpha, \beta)$ and $(c, d)^{g_2} = (\beta, \alpha)$. It follows then that any orbit containing a pair (α, β) cannot contain (β, α) for any $\alpha, \beta \in \Omega$, $\alpha \neq \beta$.

If the order of G is even then there will exist an element containing a product of 2-cycles, this element would then join the two orbits, as G is not 2-transitive we have that $|G|$ is odd.

We now recall Theorem 6.1.6 which states

$$4 \geq |\Delta^{G_\Sigma}| > |\Sigma^{G_\Delta}| \geq 1,$$

as G is not 2-transitive it follows that G is not 3-homogeneous (3-homogeneous implies 2-transitivity see Livingstone and Wagner [16]) and so there exists a 3-subset $P \notin \Delta^G$. As G is 2-homogeneous, we lose nothing by writing $\Delta = \{\alpha, \beta, \gamma\}$ and $P = \{\alpha, \beta, \delta\}$ and then we may take $\Sigma = \Delta \cup P = \{\alpha, \beta, \gamma, \delta\}$.

As G has odd order we have that G_Σ has odd order and so $|\Delta^{G_\Sigma}|$ is odd, and so equals 3 which implies that $|P^{G_\Sigma}| = 1$ and moreover that $G_\Sigma \leq G_P$. As G_Σ moves Δ to the three 3-subsets of Σ which are not P, we must have that there exists an element $h \in G_\Sigma$ which looks like $(\alpha, \beta, \delta)(\gamma)....$ Also we have that G_Δ is transitive on Δ and so must contain an element $g \in G_\Delta$ which looks like $(\alpha, \beta, \gamma)(\delta, ...,)....$

From above we have an orbit containing the ordered pair (α, γ) and a second orbit containing (γ, α). However, $(\alpha, \gamma)^{g^2} = (\gamma, \beta)$ but $(\gamma, \beta)^{h^2} = (\gamma, \alpha)$, which is a contradiction, therefore G is 2-transitive.

□

Proof. Clearly we have that $|G_\Delta| < |G_\Sigma|$, so we have the two cases of either $G_\Delta < G_\Sigma$ or $(G_\Delta \cap G_\Sigma) = H$. If $G_\Delta = H$ then we must have $2 \leq [G_\Sigma : H] \leq 4$, and H is a point stabilizer in G_Σ, then as G_Σ is transitive on Σ we have $[G_\Sigma : H] = 4$.

If we assume that $H \neq G_\Delta$ then, as $|G_\Delta| < |G_\Sigma|$, we have $2 \leq [G_\Delta : H] \leq 3$. □

Proposition 6.2.3. *Let G be a primitive permutation group acting on a set Ω of cardinality $n \geq 8$. Let Δ be a 3-subset of Ω such that $|\Delta^G| > |\Sigma^G|$ for all 4-subsets Σ containing Δ. Then Δ^G is of maximal length among G-orbits on 3-subsets.*

Proof. If G is 3-homogeneous we are done, so assume there exists a 3-subset P which is not in Δ^G. We wish to show that $|\Delta^G| \geq |P^G|$. Theorem 6.1.6 tells us that every 2-subset of Ω appears in the image of Δ, hence without loss we can assume that $|P \cap \Delta| = 2$ and so we can write $\Delta = \{1, 2, 3\}$, $P = \{1, 2, 4\}$. Choosing $\Sigma = \{1, 2, 3, 4\}$, we note now G_Σ is not transitive on Σ otherwise $P \in \Delta^G$, we also note that $|\Sigma^G| < |\Delta^G|$.

We now consider the possible structure of G_Σ as a subgroup of $Sym(4)$, we also have that

$$4 \geq |\Delta^{G_\Sigma}| > |\Sigma^{G_\Delta}| \geq 1,$$

so we have $|\Delta^{G_\Sigma}| > 1$.

Using Lemma 6.1.4 and $|\Sigma^G|$ as a fixed value we must have that $3 \geq |\Delta^{G_\Sigma}| \geq 2$. If $|\Delta^{G_\Sigma}| = 3$ then three of the four 3-subsets of Σ lie in Δ^G and so

$$3|\Sigma^G| = u|\Delta^G|,$$

where $u < 3$. Applying Lemma 6.1.4 again gives us $|\Sigma^G| = x|P^G|$ for some $x \geq 1$. It is clear from substitution that we have $|P^G| \leq |\Sigma^G| < |\Delta^G|$.

Similarly if $|\Delta^{G_\Sigma}| = 2$, then $2|\Sigma^G| = u|\Delta^G|$, however by assumption it must be that $u = 1$. Moreover $d|\Sigma^G| = x|P^G|$ where $1 \leq d \leq 2$ and $x \geq 1$. Again by substitution we have

$$\begin{aligned} \frac{|\Delta^G|}{2} &= |\Sigma^G| \\ \frac{d}{2}|\Delta^G| &= x|P^G| \\ |\Delta^G| &= \frac{2x}{d}|P^G|, \end{aligned}$$

where $2x \geq d$ and so $|\Delta^G| \geq |P^G|$ as required.

□

As is clear for a primitive group satisfying $(\star)$ we have $\sigma_2 \leq 3$ (all 2-subsets of Ω are conjugate to one of 3 possible 2-subsets of Δ) and so we next consider the case when $\sigma_2(G) = 3$.

Proposition 6.2.4. *Let G be a primitive permutation group acting on a set Ω of cardinality $n \geq 8$. Let Δ be a 3-subset of Ω such that $|\Delta^G| > |\Sigma^G|$ for all 4-subsets Σ containing Δ, suppose $\sigma_2(G) = 3$ and there exists a second orbit P^G on 3-subsets with length equal to $|\Delta^G|$. Then $G_\Delta = G_{(\Sigma)}$ and G_Δ fixes at least 4 points of Ω.*

Proof. We begin by choosing a 3-subset P which is not in Δ^G, but $|P^G| = |\Delta^G|$. We may also assume that $|P \cap \Delta| = 2$, by Theorem 6.1.6. Hence we denote $\Delta = \{1, 2, 3\}$, $P = \{1, 2, 4\}$ and $\Sigma = \{1, 2, 3, 4\}$. Note that $|P^G| > |\Sigma^G|$ and so we have $|P^{G_\Sigma}| > |\Sigma^{G_P}| \geq 1$ and $|\Delta^{G_\Sigma}| > |\Sigma^{G_\Delta}| \geq 1$, and so as $P \notin \Delta^G$ we have $|P^{G_\Sigma}| = |\Delta^{G_\Sigma}| = 2$ and so $|\Sigma^{G_P}| = |\Sigma^{G_\Delta}| = 1$. It follows that $G_\Sigma \supseteq G_\Delta \cup G_P$, and by the inequality of their sizes we have $G_\Sigma > G_\Delta$ and $G_\Sigma > G_P$.

Clearly $G_\Sigma \neq G_\Delta \cup G_P$, and furthermore we have an element $g \in G_\Sigma \setminus (G_\Delta \cup G_P)$. If $g = g|_\Sigma$ contains a cycle of length 4 on Σ, then G_Σ is transitive and $P \in \Delta^G$, however

we observe that g can have no fixed points in Σ as we only have two possibilities for the orbits of P and Δ under the action of G_Σ, namely

(i) $\Delta^{G_\Sigma} = \{\{1,2,3\},\{1,3,4\}\}$ and $P^{G_\Sigma} = \{\{1,2,4\},\{2,3,4\}\}$ or

(ii) $\Delta^{G_\Sigma} = \{\{1,2,3\},\{2,3,4\}\}$ and $P^{G_\Sigma} = \{\{1,2,4\},\{1,3,4\}\}$.

Therefore g has order 2 on Σ and so has cycle type 2^2. We lose no generality by assuming the orbits under g are those shown in (i). This restricts our options for a suitable element of $Sym(4)$ to $g = (1,3)(2,4)$ as g cannot stabilize $\{1,4\}$ or $\{1,2\}$.

It follows from Lemma 6.1.4 that $|\Delta^G| = 2|\Sigma^G| = |P^G|$ and as G_Δ and G_P are both subgroups of G_Σ we have that they both have index 2 in G_Σ. If $G_\Delta = G_P$ then these groups fix all 4 points of Σ. (Otherwise they contain the transposition $h = (1,2)(3)(4)$, which would be make G_Σ transitive on Σ by the existence of g above).

So assuming that these two subgroups are not equal, then there exists an element $p \in G_P \setminus G_\Delta$ such that $gp \in G_\Delta$. This leaves us with the options for p to be either $(1,4,2)$ or $(2,4)$, we note that if $p = (1,4,2)$ then $\langle g,p\rangle < G_\Sigma$ is transitive, and so $p = (2,4)$. Repeating this argument for $t \in G_\Delta \setminus G_P$ we have that $t = (1,3)$.

With this information we can construct the two possible structures for G_Σ as a subgroup of $Sym(4)$. That is either

Case 1 $G_\Sigma = \{(1),(1,3)(2,4)\}$ and so $G_\Delta = G_P = \{(1)\} = G_{(\Sigma)}$ the pointwise stabilizer of Σ, or

Case 2 $G_\Sigma = \{(1),(1,3),(2,4),(1,3)(2,4)\}$ with $G_\Delta = \{(1),(1,3)\}$ and $G_P = \{(1),(2,4)\}$.

We eliminate Case 2 by considering the three orbits on 2-subsets. We know that these orbits can be denoted by $\{1,2\}^G$, $\{1,3\}^G$ and $\{2,3\}^G$. Taking the three subsets of Δ^g above we see that $\{3,4\} \in \{1,2\}^G$ and $\{1,4\} \in \{2,3\}^G$. We also have that for non-identity h in G_Δ $\{3,4\}^h = \{1,4\}$ and so $\{1,2\} \in \{2,3\}^G$ giving $\sigma_2 \leq 2$ which is a contradiction. □

We are still some way from being able to say that a primitive group satisfying $(\star)$ is 3-homogeneous, but we have made some progress under other restrictions. Knowing that the orbit containing the 3-subset of interest is the largest, we assess the case when it is the only orbit on 3-subsets.

Theorem 6.2.5. *Let G be a 3-homogeneous permutation group acting on a G-set, Ω, of cardinality $n \geq 8$. If the orbit on 3-subsets of Ω has length strictly greater than the G-orbit of any 4-subset of Ω then $G \cong PSL(2,7)$ or $G \cong PGL(2,7)$.*

Proof. As G is 3-homogeneous we note that any group hoping to have the property we are searching for cannot have any regular orbits on 4-subsets and furthermore cannot be 4-homogeneous.

We begin by compiling a list of possible candidates from two results from Kantor [15] and Cameron [4] giving us M_{11}, M_{22}, $AGL(1,8)$, $A\Gamma L(1,8)$, $A\Gamma L(1,32)$ and $PSL(2,q)$ and a family of groups $PSL(2,q) \leq G \leq P\Gamma L(2,q)$, where $q \equiv 3 \bmod 4$.

Initially we can compute the groups M_{11}, M_{22}, $AGL(1,8)$, $A\Gamma L(1,8)$ and $A\Gamma L(1,32)$ and see that these do not satisfy the condition of having such a 3-subset of their respective G-sets.

We now eliminate the possibilities for q in the remaining families of groups. We first note that as all the groups which remain have $PSL(2,q)$ as their respective socles then as the G-sets of the over groups are the same as for their socles, we need only show that $PSL(2,q)$ does not satisfy the condition of having all 4-subsets with stabilizers of order greater than 2. This is due to the size of the orbit on 3-subsets being as large as possible but less than $\frac{|G|}{2}$ and so any over group cannot increase the length of this 3-orbit but can fuse two or more 4-orbits.

We do this by considering a specific subset of the projective line on which these groups act. We represent the span of vector in the usual way (see Table 2.1).

We begin by letting ω be a generator for the multiplicative field of q elements, that is $\omega^{q-1} = 1$. We choose $\Sigma = \{0, 1, \infty, \omega^a\}$ where $\omega^a \notin \{-1, 2, 2^{-1}\}$ and, $\omega^{2a} - \omega^a + 1 \neq 0$.

We can now make use of a result in [1] where we have that for such a set the size of the stabilizer in $PGL(2,q)$ is 4. We now show that this set must have a stabilizer in $PSL(2,q)$ with order less than 4 by giving an element of $PGL(2,q)_\Sigma$ which is not in $PSL(2,q)$.

$$A = \begin{bmatrix} 1 & \omega^a \\ -1 & -1 \end{bmatrix}.$$

It is easy to see that A will act on Σ with the cycles $(0, \omega^a)(1, \infty)$ and so $A \in PGL(2,q)_\Sigma$. However, the determinant of A is equal to $\omega^a - 1$ however, $\omega^a \neq 2$ by choice and so $A \notin PSL(2,q)$ as required. Hence the stabilizer of Σ in $PSL(2,q)$ must have order 1 or 2 and so the $PSL(2,q)$ orbit of Σ is greater than the total number of 3-subsets of Ω and hence such groups cannot have a large enough 3 orbit to satisfy our condition.

This has now reduced our problem to finding fields for which no such element ω^a exists. We also note that we are interested in $q \geq 7$. In fact $q = 7$ is the only such field in our range without such an element as a simple counting argument shows that any field with more than 8 elements must satisfy this requirement.

Finally we note that $PSL(2,7) < PGL(2,7) = P\Gamma L(2,7)$ and that Proposition 6.1.7 shows both of these groups satisfy the condition.

□

We continue with the assumption that our group G satisfying $(\star)$ is 2-transitive, but not 3-homogeneous, all such groups are known and we can find a classification in [4] and we have that G must contain one of the following groups T as its socle.

Group (T)	Degree	Notes
$PSL(2,q)$	$q+1$	$q \equiv 1 \bmod 4$
$PSU(3,q)$	q^3+1	
$PSL(d,q)$	$(q^d-1)/(q-1)$	$d > 2$
$Suz(q)$	q^2+1	
$R(q)$	q^3+1	
$PSp(2d,2)$	$2^{2d-1}+2^{d-1}$	$d > 2$
$PSp(2d,2)$	$2^{2d-1}-2^{d-1}$	$d > 2$
$PSL(2,11)$	11	
$PSL(2,8)$	28	
$Alt(7)$	15	
HS	176	
Co_3	276	

Table 6.2: 2-transitive, not 3-homogeneous group socles

Proposition 6.2.6. *Let G be a 2-transitive permutation group satisfying $(\star)$. If $T = Soc(G)$ then T is not $PSL(2,11)$, $PSL(2,8)$, $Alt(7)$, HS or Co_3 as described in Table 6.2.*

Proof. As G will be primitive and we have the given degree of G in the representation

in Table 6.2, we may us representations given in the MAGMA database of primitive groups.

Firstly we let $T \cong PSL(2,11)$ and G will act on 11 points. We can obtain this representation of T and see that T will have two orbits on 3-subsets, which we denote Δ_1^G and Δ_2^G, we see that without loss these T-orbits have length 110 and 55 respectively. We know that G could fuse these, but would then be 3-homogeneous which is a contradiction. By Proposition 6.2.3, we need only consider a 3-subset in Δ_1^G, and we can let $\Delta_1 = \{1,2,3\}$, however, letting $\Sigma = \{1,2,3,4\}$ we have that $|\Sigma^T| > |\Delta_1^T|$ and so G cannot have socle $PSL(2,11)$ on 11 points.

If $T \cong PSL(2,8)$ and G has degree 28, we know that G will be contained in the primitive groups of degree 28, checking these we see that none of these groups satisfy $(\star)$.

We use the MAGMA database and choose $T \cong Alt(7)$ on 15 points, (PrimitiveGroup(15,3)), we deal with this group similarly as the $PSL(2,11)$ case above. Here we again have that T has two orbits on 3-subsets which we denote Δ_1^G and Δ_2^G, we see that without loss these T-orbits have length 420 and 35 respectively. We know that G could fuse these, but would then be 3-homogeneous which is a contradiction. By Proposition 6.2.3, we need only consider a 3-subset in Δ_1^G, and we can let $\Delta_1 = \{1,2,3\}$, however, letting $\Sigma = \{1,2,3,4\}$ we have that $|\Sigma^T| > |\Delta_1^T|$ and so G cannot have socle $Alt(7)$ on 15 points.

Again we use the same method to eliminate $T \cong Co_3$ as a possibility, we are able to see that there are two orbits on 3-subsets, with the longest orbit having length 2049300. We then proceed as before and by careful choice of representatives, show $T \cong Co_3$ cannot be a socle of G.

Finally we eliminate any G which contains socle $T \cong HS$. Taking the permutation representation on 176 points from the online Atlas of finite groups, we see that T has three orbits on 3-subsets of $\Omega = \{1...176\}$, we denote these by representatives Δ_1, Δ_2 and Δ_3 which have T-orbit lengths respectively $462000, 369600$ and 61600. Now If G satisfies $(\star)$ then we know from Proposition 6.2.3 that the possible orbit lengths of G on 3-subsets which could contain an appropriate 3-subset will be the longest orbit.

The possible longest G-orbits will be $|\Delta_1^T| = 462000$, $|\Delta_1^T \cup \Delta_2^T| = 831600$ or $|\Delta_1^T \cup \Delta_3^T| = 523600$. Each of these will contain the 3-subset Δ_1. Using the representation we

have we determine that $\Delta_1 = \{1, 2, 6\}$ satisfies the conditions, however, $\Sigma = \{1, 2, 3, 6\}$ has T-orbit length 1108800 and so is longer than any G-orbit on 3-subsets containing Δ_1. This excludes $T \cong HS$ as a possible socle of G.

□

It was hoped that the initial results would allow us to infer that such a G would be 3-homogeneous, however this has not been the case so far, and we are left with the following open conjecture.

Conjecture 6.2.7. *Let G be a primitive permutation group acting on a G-set, Ω, of cardinality $n \geq 8$. If there exists a 3-subset $\Delta \subset \Omega$ such that $|\Delta^G| > |\Sigma^G|$ for any 4-subset Σ containing Δ, then $G \cong PSL(2, 7)$ or $G \cong PGL(2, 7)$.*

We have been pretty vocal on the case when G is primitive, as there are so few examples of such groups that we have found which satisfy the Livingstone Wagner property. However, imprimitive examples are much more common. We restrict our attention to a few imprimitive transitive groups, in all three of the following examples we keep $\Delta = \{1, 2, 3\}$.

Example 1 is a subgroup of $Sym(8)$ where

$$\begin{aligned} G_1 \quad \cong \quad & \langle (4,6), (1,2,5,3)(4,8)(6,7), (1,8)(4,6), (3,4,6), (1,7,8), (2,3)(4,6), \\ & (2,4)(3,6), (1,5)(7,8), (1,7)(5,8) \rangle. \end{aligned}$$

Here $|G_1| = 1152$ and $|\Delta^{G_1}| = 48$. This group satisfies the condition that every 2-subset appears in some G_1-image of Δ. The system of imprimitivity for G_1 is the set

$$\{\{1, 5, 7, 8\}, \{2, 3, 4, 6\}\}.$$

The σ_k values are $\sigma_1 = 1,\ \sigma_2 = 2,\ \sigma_3 = 2$ and $\sigma_4 = 3$.

It is also clear that there exists a 4-subset for which no G_1-image contains Δ as a subset (the system of imprimitivity is a single orbit) also we have $G_{1\Delta}$ is not transitive on Δ.

Example 2 is a subgroup of $Sym(9)$ where

$$G_2 \cong \langle (4,7)(5,9)(6,1), (8,9,5)(2,7,4)(3,1,6), (4,5,6)(7,1,9), (8,3,2)(7,1,9) \rangle.$$

Here $|G_2| = 54$ and $|\Delta^{G_2}| = 54$. This group satisfies the condition that every 2-subset appears in some G_2-image of Δ. The system of imprimitivity for G_2 is the set

$$\{\{1,7,9\},\{2,3,8\},\{4,5,6\}\}.$$

The σ_k values are $\sigma_1 = 1,\ \sigma_2 = 2,\ \sigma_3 = 5$ and $\sigma_4 = 5$. In this case Δ appears as a subset of a point in each G_2-orbit of subsets of size 4. Here we have $G_{2\Delta}$ is not transitive on Δ.

Example 3 is a subgroup of $Sym(16)$ where

$$\begin{aligned} G_3 \cong \langle &(1,12)(7,3)(11,8)(4,2)(5,10)(6,9)(13,15)(14,16),\\ &(1,8,6,14)(7,2,5,13)(11,9,16,12)(4,10,15,3),\\ &(1,14)(7,13)(11,12)(4,3)(5,2)(6,8)(9,16)(10,15),\\ &(1,6)(7,5)(11,15)(4,16)(2,14)(8,13)(9,12)(10,3),\\ &(1,16)(7,15)(11,6)(4,5)(2,3)(8,12)(9,14)(10,13),\\ &(7,8)(9,10)(3,12)(13,14),\\ &(11,4)(9,10)(3,12)(15,16),\\ &(1,7)(11,4)(5,6)(2,8)(9,10)(3,12)(13,14)(15,16)\rangle. \end{aligned}$$

Here $|G_3| = 256$ and $|\Delta^{G_3}| = 256$. This group does not satisfy the condition of every 2-subset being contained in some G_3-image of Δ. The σ_k values for G_3 are $\sigma_1 = 1$, $\sigma_2 = 6$, $\sigma_3 = 11$, $\sigma_4 = 35$, $\sigma_5 = 48$, $\sigma_6 = 91$, $\sigma_7 = 100$ and $\sigma_8 = 132$. Here we have three systems of imprimitivity $\{\{1,5\},\{2,14\},\{3,9\},\{4,16\},\{6,7\},\{8,13\},\{10,12\},\{11,15\}\}$,

$\{\{3,9,10,12\},\{1,5,6,7\},\{4,11,15,16\},\{2,8,13,14\}\}$

and $\{\{1,3,5,6,7,9,10,12\},\{2,4,8,11,13,14,15,16\}\}$.

It is also clear that there exists a 4-subset for which no G_3-image contains Δ as a subset (the system of imprimitivity is a single orbit). Again we have that the stabilizer in G_3 is not transitive on Δ.

What these examples suggest in relation to our conjecture is that if we are to progress towards a proof of it we need to use primitivity to imply such a group is 3-homogeneous, as we have examples of imprimitive groups, G_1 and G_2 above, where every 2-subset appears in some G-image of our chosen Δ. The equivalent 2-homogeneous

condition was achieved in the original paper by Siemons and Wagner by joining all pairs of points via an equivalence relation. However, so far we have been unable to do a similar thing for triples of points.

6.3 Further Work

Going forward from this thesis, we see that we have formulae for the rank one doubly transitive groups, it would be of interest to further these to compile equivalent results for all doubly transitive groups, and it may be possible to classify these from the orbit numbers on 3-sets.

Another avenue would be prove or disprove Conjecture 6.2.7, and if it is proven, possibly go on to determine if the list in Proposition 6.1.7 is a complete list of all primitive groups with the Siemons Wagner property. Certainly calculation with the list of primitive groups in the Magma database suggests these groups are rare.

Bibliography

[1] Beth, T.; Jungnickel, D.; Lenz, H. *Design theory. Vol. I. Second edition,* Encyclopedia of Mathematics and its Applications, 69. Cambridge University Press, Cambridge, 1999, 209.

[2] Bray, J. N.; Holt, D. F.; Roney-Dougal, C. M. *The maximal subgroups of the low-dimensional finite classical groups,* London Mathematical Society Lecture Note Series, 407. Cambridge University Press, Cambridge, 2013.

[3] Bundy, D.; Hart, S. *The case of equality in the Livingstone-Wagner theorem,* J. Algebraic Combin. 29, 2009, no. 2, 215–227.

[4] Cameron, P. J. *Finite permutation groups and finite simple groups,* Bull. London Math. Soc. 13, 1981, no. 1, 1–22.

[5] Cameron, P. J.; Maimani, H. R.; Omidi, G. R.; Tayfeh-Rezaie, B. *3-designs from PSL(2,q)*, Discrete Math. 306, 2006, no. 23, 3063–3073.

[6] Cameron, P. J.; Omidi, G. R.; Tayfeh-Rezaie, B. *3-designs from PGL(2,q)*, Electron. J. Combin. 13, 2006, no. 1, Research Paper 50, 11.

[7] Cameron, P. J. *On an algebra related to orbit-counting,* J. Group Theory 1, 1998, no. 2, 173–179.

[8] Chen, J.; Liu, W. J. 3-*designs from* $PSL(2,q)$ *with* $q = 1(mod 4)$, Util. Math. 88, 2012, 211–222.

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

[10] Dixon, J. D.; Mortimer, B. *Permutation groups*, Graduate Texts in Mathematics, 163. Springer-Verlag, New York, 1996.

[11] Evans, D. M., Siemons, J. *On the number of orbits of a group in two permutation actions,* Arch. Math. (Basel) 60, 1993, no. 5, 420–424

[12] Faber, Xander *Finite p-Irregular Subgroups of $PGL(2, k)$,* arXiv:1112.1999 [math.NT]

[13] Huppert, B. *Endliche Gruppen I*, Springer-Verlag. Berlin, 1967, 185–193.

[14] Isaacs, I. M *Character theory of finite groups,* Academic Press Inc. (London), 1970, 69.

[15] Kantor, W. M. *k-homogeneous groups,* Math. Z. 124, 1972, 261–265.

[16] Livingstone, D.; Wagner, A. *Transitivity of finite permutation groups on unordered sets*, Math. Z. 90, 1965, 393–403.

[17] Macdonald, I. G. *Numbers of conjugacy classes in some finite classical groups*, Bull. Austral. Math. Soc. 23 , 1981, no. 1, 23–48.

[18] Mitchell, H. H. *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc 12, 1911, 207–242.

[19] Mnukhin, V. B. *Some relations for the lengths of orbits on k-sets and $(k-1)$-sets*, Arch. Math. (Basel) 69, 1997, no. 4, 275–278.

[20] Mnukhin, V. B., Siemons, I. J. *On the Livingstone-Wagner theorem,* Electron. J. Combin. 11, 2004, no. 1, Research Paper 29, 8.

[21] Nakashima, Y. *A partial generalization of the Livingstone-Wagner theorem*, (English summary) Ars Math. Contemp. 2, 2009, no. 2, 207–215.

[22] Neumann, P. M. *A lemma that is not Burnside's*, Math. Sci. 4, 1979, no. 2, 133–141.

[23] Passman, D. *Permutation Groups*, W. A. Benjamin, Inc., New York-Amsterdam, 1968, ix+310.

[24] Rainbolt, J. G., Sheth, J. K. *The multiplicity free permutation representations of the Ree groups ${}^2G_2(q)$, the Suzuki groups ${}^2B_2(q)$, and their automorphism groups*, Com. in Alg. Vol. 31, No. 3, (New York), 2003, 1253–1270.

[25] Roney-Dougal, Colva M. *The primitive permutation groups of degree less than* 2500, J. Algebra 292, 2003, no. 1, 154–183.

[26] Rosen, K. H. *Elementary number theory and its applications*, Second edition. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1988.

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

[28] Simpson, W. A.; Frame, J. S. *The character tables for $SL(3,q)$, $SU(3,q^2)$, $PSL(3,q)$, $PSU(3,q^2)$*, Can. J. Math, Vol. XXV, No.3, 1973, 486–494.

[29] Sims, C. C. *Graphs and finite permutation groups*, Math. Z. 95, 1967, 76–86.

[30] Sims. C.C. *Computational methods in the study of permutation groups*, Computational problems in abstract algebra, 1970, 169–183. Oxford - Pergamon.

[31] Sloane, N. J. A. *Jacobsthal sequence (or Jacobsthal numbers)*, Available: `https://oeis.org/search?q=1%2C1%2C3%2C5%2C11%2C21%2C43&language=english`. Last accessed 4th Jan 2012.

[32] Sloane, N. J. A. *Number of vertices in Sierpinski triangle of order n*, Available: `http://oeis.org/search?q=3%2C6%2C15%2C42%2C123%2C366&sort=&language=english` Last accessed 28th Nov 2013.

[33] Suzuki, M. *On a class of doubly transisitive groups*, Ann. of Math.(2) 75, 1962, 105–145.

[34] Suzuki, M. *A characterization of the* 3 *-dimensional projective unitary group over a finite field of odd characteristic*, J. Algebra 2, 1965, 1–14.

[35] Suzuki, M. *Group theory I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 247. Springer-Verlag, Berlin-New York, 1982, xiv+434.

[36] Ward, H. N. *On Ree's series of simple groups*, Bull. Amer. Math. Soc. 69, 1963, 113–114.

[37] Wilson, R. A. *The finite simple groups. Graduate Texts in Mathematics*, 251. Springer-Verlag London, Ltd., London, 2009.

Appendix A

Magma Code

A.1 $PSL(2, q)$

```
PSLsig:=procedure(q,k,~sigma);
Z:=Integers();d:=GreatestCommonDivisor(q-1,2);
P:=PrimeDivisors(q);p:=P[1];sig:=0;
I:=(d/(q*(q+1)*(q-1)))*Binomial(Z!(q+1),k);
CC:=[]; Append(~CC,[<(d/q),1>,<p,Z!(q/p)>,<1,1>]);
for m in Divisors(Z!((q+1)/d)) do if m ne 1 then
Append(~CC,[<(d/(2*(q+1))),EulerPhi(m)>,<m,Z!((q+1)/m)>]);
end if;end for;
for m in Divisors(Z!((q-1)/d)) do if m ne 1 then
Append(~CC,[<(d/(2*(q-1))),EulerPhi(m)>,<m,Z!((q-1)/m)>,<1,2>]);
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;end procedure;
```

A.2 $Sz(q)$

```
Suzsig:=procedure(q,k,~sigma);
Z:=Integers();R:=2*q;r:=SquareRoot(R);sig:=0;
CC:=[]; I:=(1/(q^2*(q^2+1)*(q-1)))*Binomial(Z!(q^2+1),k);
Append(~CC,[<(1/q^2),1>,<2,Z!(q^2/2)>,<1,1>]);
Append(~CC,[<(1/q),1>,<4,Z!(q^2/4)>,<1,1>]);
for m in Divisors(Z!((q-1))) do if m ne 1 then
Append(~CC,[<(1/(2*(q-1))),EulerPhi(m)>,<m,Z!((q^2-1)/m)>,<1,2>]);
end if;end for;t1:=Z!(q+r+1);t2:=Z!(q-r+1);
for m in Divisors(Z!((q+r+1))) do if m ne 1 then
Append(~CC,[<1/(4*t1),EulerPhi(m)>,<m,Z!((q^2+1)/m)>]);
end if;end for;
for m in Divisors(Z!((q-r+1))) do if m ne 1 then
Append(~CC,[<1/(4*t2),EulerPhi(m)>,<m,Z!((q^2+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;end procedure;
```

A.3 $PSU(3,q)$

```
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^3)/p)>,<1,1>]);
Append(~CC,[<Z!((q^3+1)*(q^3-q)),1>,
<4,Z!((q^3)/4)>,<1,1>]);end if;if p ne 2 then
Append(~CC,[<Z!((q^3+1)*(q^3-1)),1>,
<p,Z!((q^3)/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^3-3*q-2;
l12:=LCM(l1,l2);
Append(~CK,
[<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;

PI36:=function(PI,t);
X:=[[]]; for i:=1 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:=PI36(PI6(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;

PSUsig:=procedure(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^3+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^3-q)/m)>,<1,Z!(q+1)>]);end if;end for;
for j in D do m:=Z!(p*j);if j ne 1 then
Append(~CC,[<d/(q*(q+1)*(p-1)),EulerPhi(m)>,<p,Z!(q/p)>,
<m,Z!((q^3-q)/m)>,<1,1>]);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^3-1)/m)>,<1,2>]); elif j ne m then
Append(~CC,[<d/(2*(q^2-1)),EulerPhi(m)>,<j,Z!((q-1)/j)>,
<m,Z!((q^3-q)/m)>,<1,2>]);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*(q+1)/(3*(q^3+1)),EulerPhi(m)>,
<m,Z!((q^3+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;
```

A.4 $R(q)$

```
Z:=Integers();

E:=function(q);
p:=(q mod 8);
return Z!(p-4);
end function;

DM:=function(m);
return Z!(GCD(m,2)); 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;

etakphi2:=function(k,PI); ng:=0;sig:=0;
for i:=1 to #PI do Cg:=PI[i];
RPg:=RestrictedPartitions(k,{Cg[i][1]: i in [2..#Cg]});
ng:=0;
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;
ng:=(ng + np);
end for;
sig:=sig + ng*Cg[1][1];
end for;
sigma:=sig;return sigma;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;

PIJ:=function(q);
PI:=[[<2,Z!((q^3-q)/2)>,<1,Z!(q+1)>]];
return PI;
end function;

PIRa:=function(q);e:=E(q);
D:=Divisors(Z!((q+e)/2)); Exclude(~D,1);Exclude(~D,2);
CT:=[]; for m in D do;
Append(~CT,[<EulerPhi(m),1>,<1,2>,<m,Z!((q^3-1)/(m))>]);
end for;return CT; end function;

PISa:=function(q);e:=E(q);
D:=Divisors(Z!((q-e)/4)); Exclude(~D,1);
CT:=[]; for m in D do;
```

```
Append(~CT,[<EulerPhi(m),1>,<m,Z!((q^3-q)/(m))>,
<Z!(m/DM(m)),Z!(DM(m)*(q+1)/m)>]);
end for;CySt(CT,~CT);return CT; end function;

PIT:=function(q);
PI:=[[<3,Z!((q^3)/3)>,<1,1>]];
return PI;
end function;

PIJRa:=function(q);e:=E(q);
D:=Divisors(Z!((q+e)/2)); Exclude(~D,1);
CT:=[]; for m in D do;
Append(~CT,[<EulerPhi(m),1>,<Z!(2*m),Z!((q^3-q)/(2*m))>,
<Z!(m),Z!((q-1)/m)>,<1,2>]);
end for;CySt(CT,~CT);return CT; end function;

PIJSa:=function(q);e:=E(q);
D:=Divisors(Z!((q-e)/4)); Exclude(~D,1);
CT:=[]; for m in D do;
Append(~CT,[<EulerPhi(m),1>,<Z!(2*m),Z!((q^3-q)/(2*m))>,
<Z!(m),Z!((q+1)/m)>]);
end for;CySt(CT,~CT);return CT; end function;

PIJT:=function(q);
PI:=[[<6,Z!((q^3-q)/6)>,<3,Z!(q/3)>,<1,1>]];
return PI;
end function;

PIY:=function(q);
PI:=[[<9,Z!((q^3)/9)>,<1,1>]];
return PI;
end function;
```

```
PIX:=function(q);
PI:=[[<3,Z!((q^3)/3)>,<1,1>]];
return PI;
end function;

PIW:=function(q);M:=Sqrt(Z!(3*q));
D:=Divisors(Z!(q+1+M)); Exclude(~D,1);
CT:=[]; for m in D do;
Append(~CT,[<EulerPhi(m),1>,<m,Z!((q^3+1)/(m))>]);
end for;return CT;
end function;

PIV:=function(q);M:=Sqrt(Z!(3*q));
D:=Divisors(Z!(q+1-M)); Exclude(~D,1);
CT:=[]; for m in D do;
Append(~CT,[<EulerPhi(m),1>,<m,Z!((q^3+1)/(m))>]);
end for;return CT;
end function;

ID:=function(q,k);
return Binomial(q^3+1,k);
end function;

ClJ:=function(q,k);
x:=etak(k,PIJ(q));
return q^2*(q^2-q+1)*x; end function;

ClRa:=function(q,k);
x:=etakphi2(k,PIRa(q));
return (q^6+q^3)*x/2;
end function;
```

```
ClSa:=function(q,k);
x:=etakphi2(k,PISa(q));
return (q^3*(q-1)*(q^2-q+1)*x)/6;
end function;

ClT:=function(q,k);
x:=etak(k,PIT(q));
return q*(q-1)*(q^3+1)*x; end function;

ClJRa:=function(q,k);
x:=etakphi2(k,PIJRa(q));
return (q^6+q^3)*x/2;
end function;

ClJSa:=function(q,k);
x:=etakphi2(k,PIJSa(q));
return q^3*(q-1)*(q^2-q+1)*x/2;
end function;

ClJT:=function(q,k);
x:=etak(k,PIJT(q));
return q^2*(q-1)*(q^3+1)*x;
end function;

ClW:=function(q,k);
x:=etakphi2(k,PIW(q));
return (q^3)*(q^3+1)*(q-1)*x/((q+1+Z!(Sqrt(Z!(3*q))))*6);
end function;

ClV:=function(q,k);
x:=etakphi2(k,PIV(q));
```

```
return (q^3)*(q^3+1)*(q-1)*x/((q+1-(Z!(Sqrt(Z!(3*q)))))*6);
end function;

ClY:=function(q,k);
x:=etak(k,PIY(q));
return q^2*(q-1)*(q^3+1)*x;
end function;

ClX:=function(q,k);
x:=etak(k,PIX(q));
return (q-1)*(q^3+1)*x;
end function;

procedure SigmaRee(q,k,~sigma);
x:=ID(q,k)+ClJ(q,k)+ClRa(q,k)+ClSa(q,k)+ClT(q,k)+ClJRa(q,k)
+ClJSa(q,k)+ClJT(q,k)+ClW(q,k)+ClV(q,k)+ClY(q,k)+ClX(q,k);
sigma:=x/((q^3)*(q^3+1)*(q-1));
end procedure;
```

Appendix B

Number of Orbit Tables

We present here a list of finite groups and their values σ_k when considered in regular representations. For the abelian groups we let $(\alpha_1, \alpha_2, ..., \alpha_n)$ denote $\mathbb{Z}_{\alpha_1} \times \mathbb{Z}_{\alpha_2} ... \times \mathbb{Z}_{\alpha_n}$.

(2)

k	σ
1	1

(3)

k	σ
1	1
2	1

(4)

k	σ
1	1
2	2

(2, 2)

k	σ
1	1
2	3

(5)

k	σ
1	1
2	2
3	2

(6)

k	σ
1	1
2	3
3	4

(7)

k	σ
1	1
2	3
3	5

(8)

k	σ
1	1
2	4
3	7
4	10

(4, 2)

k	σ
1	1
2	5
3	7
4	12

(2, 2, 2)

k	σ
1	1
2	7
3	7
4	14

(9)

k	σ
1	1
2	4
3	10
4	14

(3, 3)

k	σ
1	1
2	4
3	12
4	14

(10)

k	σ
1	1
2	5
3	12
4	22
5	26

(11)

k	σ
1	1
2	5
3	15
4	30
5	42

(12)

k	σ
1	1
2	6
3	19
4	43
5	66
6	80

(6, 2)

k	σ
1	1
2	7
3	19
4	45
5	66
6	84

(13)

k	σ
1	1
2	6
3	22
4	55
5	99
6	132

(14)

k	σ
1	1
2	7
3	26
4	73
5	143
6	217
7	246

(15)

k	σ
1	1
2	7
3	31
4	91
5	201
6	335
7	429

(16)

k	σ
1	1
2	8
3	35
4	116
5	273
6	504
7	715
8	810

(8, 2)

k	σ
1	1
2	9
3	35
4	120
5	273
6	511
7	715
8	820

(4, 4)

k	σ
1	1
2	9
3	35
4	122
5	273
6	511
7	715
8	822

(4, 2, 2)

k	σ
1	1
2	11
3	35
4	128
5	273
6	525
7	715
8	838

(2, 2, 2, 2)

k	σ
1	1
2	15
3	35
4	140
5	273
6	553
7	715
8	870

(17)

k	σ
1	1
2	8
3	40
4	140
5	364
6	728
7	1144
8	1430

(18)

k	σ
1	1
2	9
3	46
4	172
5	476
6	1038
7	1768
8	2438
9	2704

(6, 3)

k	σ
1	1
2	9
3	48
4	172
5	476
6	1044
7	1768
8	2438
9	2710

(19)

k	σ
1	1
2	9
3	51
4	204
5	612
6	1428
7	2652
8	3978
9	4862

(20)

k	σ
1	1
2	10
3	57
4	245
5	776
6	1944
7	3876
8	6310
9	8398
10	9252

(10, 2)

k	σ
1	1
2	11
3	57
4	249
5	776
6	1956
7	3876
8	6330
9	8398
10	9278

(21)

k	σ
1	1
2	10
3	64
4	285
5	969
6	2586
7	5538
8	9690
9	14000
10	16796

(22)

k	σ
1	1
2	11
3	70
4	335
5	1197
6	3399
7	7752
8	14550
9	22610
10	29414
11	32066

(23)

k	σ
1	1
2	11
3	77
4	385
5	1463
6	4389
7	10659
8	21318
9	35530
10	49742
11	58786

(24)

k	σ
1	1
2	12
3	85
4	446
5	1771
6	5620
7	14421
8	30667
9	54484
10	81752
11	104006
12	112720

(64)

k	σ
1	1
2	32
3	651
4	9936
5	119133
6	1171552
7	9706503
8	69159400
9	430321633
10	2366772128
11	11618684091
12	51315868912
13	205263418941
14	747745364448
15	2492484372855
16	7633233556276
17	21552658988805
18	56276387797920
19	136248095712855
20	306558216362064
21	642312451217745
22	1255428883941600
23	2292522306124995
24	3916392276491800
25	6266227636741653
26	9399341460540192
27	13228702788676823
28	17480785835260912
29	21700285855317153
30	25317000173376096
31	27767032438524099
32	28634752211620266

(32, 2)

k	σ
1	1
2	33
3	651
4	9952
5	119133
6	1171707
7	9706503
8	69160528
9	430321633
10	2366778421
11	11618684091
12	51315897248
13	205263418941
14	747745469631
15	2492484372855
16	7633233885032
17	21552658988805
18	56276388674445
19	136248095712855
20	306558218378208
21	642312451217745
22	1255428887973615
23	2292522306124995
24	3916392283548080
25	6266227636741653
26	9399341471395617
27	13228702788676823
28	17480785849993632
29	21700285855317153
30	25317000191054931
31	27767032438524099
32	28634752230404436

(16,4)

k	σ
1	1
2	33
3	651
4	9954
5	119133
6	1171707
7	9706503
8	69160544
9	430321633
10	2366778421
11	11618684091
12	51315897318
13	205263418941
14	747745469631
15	2492484372855
16	7633233885264
17	21552658988805
18	56276388674445
19	136248095712855
20	306558218378754
21	642312451217745
22	1255428887973615
23	2292522306124995
24	3916392283549088
25	6266227636741653
26	9399341471395617
27	13228702788676823
28	17480785849995062
29	21700285855317153
30	25317000191054931
31	27767032438524099
32	28634752230406054

$(8,8)$

k	σ
1	1
2	33
3	651
4	9954
5	119133
6	1171707
7	9706503
8	69160548
9	430321633
10	2366778421
11	11618684091
12	51315897318
13	205263418941
14	747745469631
15	2492484372855
16	7633233885276
17	21552658988805
18	56276388674445
19	136248095712855
20	306558218378754
21	642312451217745
22	1255428887973615
23	2292522306124995
24	3916392283549116
25	6266227636741653
26	9399341471395617
27	13228702788676823
28	17480785849995062
29	21700285855317153
30	25317000191054931
31	27767032438524099
32	28634752230406086

$(16,2,2)$

k	σ
1	1
2	35
3	651
4	9984
5	119133
6	1172017
7	9706503
8	69162784
9	430321633
10	2366791007
11	11618684091
12	51315953920
13	205263418941
14	747745679997
15	2492484372855
16	7633234542544
17	21552658988805
18	56276390427495
19	136248095712855
20	306558222410496
21	642312451217745
22	1255428896037645
23	2292522306124995
24	3916392297660640
25	6266227636741653
26	9399341493106467
27	13228702788676823
28	17480785879459072
29	21700285855317153
30	25317000226412601
31	27767032438524099
32	28634752267972774

$(8,4,2)$

k	σ
1	1
2	35
3	651
4	9988
5	119133
6	1172017
7	9706503
8	69162816
9	430321633
10	2366791007
11	11618684091
12	51315954060
13	205263418941
14	747745679997
15	2492484372855
16	7633234543004
17	21552658988805
18	56276390427495
19	136248095712855
20	306558222411588
21	642312451217745
22	1255428896037645
23	2292522306124995
24	3916392297662656
25	6266227636741653
26	9399341493106467
27	13228702788676823
28	17480785879461932
29	21700285855317153
30	25317000226412601
31	27767032438524099
32	28634752267976006

$(4,4,4)$

k	σ
1	1
2	35
3	651
4	9996
5	119133
6	1172017
7	9706503
8	69162872
9	430321633
10	2366791007
11	11618684091
12	51315954340
13	205263418941
14	747745679997
15	2492484372855
16	7633234543900
17	21552658988805
18	56276390427495
19	136248095712855
20	306558222413772
21	642312451217745
22	1255428896037645
23	2292522306124995
24	3916392297666632
25	6266227636741653
26	9399341493106467
27	13228702788676823
28	17480785879467652
29	21700285855317153
30	25317000226412601
31	27767032438524099
32	28634752267982406

$(8,2,2,2)$

k	σ
1	1
2	39
3	651
4	10048
5	119133
6	1172637
7	9706503
8	69167296
9	430321633
10	2366816179
11	11618684091
12	51316067264
13	205263418941
14	747746100729
15	2492484372855
16	7633235857564
17	21552658988805
18	56276393933595
19	136248095712855
20	306558230475072
21	642312451217745
22	1255428912165705
23	2292522306124995
24	3916392325885760
25	6266227636741653
26	9399341536528167
27	13228702788676823
28	17480785938389952
29	21700285855317153
30	25317000297127941
31	27767032438524099
32	28634752343109446

$(4,4,2,2)$

k	σ
1	1
2	39
3	651
4	10056
5	119133
6	1172637
7	9706503
8	69167352
9	430321633
10	2366816179
11	11618684091
12	51316067544
13	205263418941
14	747746100729
15	2492484372855
16	7633235858460
17	21552658988805
18	56276393933595
19	136248095712855
20	306558230477256
21	642312451217745
22	1255428912165705
23	2292522306124995
24	3916392325889736
25	6266227636741653
26	9399341536528167
27	13228702788676823
28	17480785938395672
29	21700285855317153
30	25317000297127941
31	27767032438524099
32	28634752343115846

$(4,2,2,2,2)$

k	σ
1	1
2	47
3	651
4	10176
5	119133
6	1173877
7	9706503
8	69176312
9	430321633
10	2366866523
11	11618684091
12	51316293952
13	205263418941
14	747746942193
15	2492484372855
16	7633238487580
17	21552658988805
18	56276400945795
19	136248095712855
20	306558246604224
21	642312451217745
22	1255428944421825
23	2292522306124995
24	3916392382335944
25	6266227636741653
26	9399341623371567
27	13228702788676823
28	17480786056251712
29	21700285855317153
30	25317000438558621
31	27767032438524099
32	28634752493382726

$(2,2,2,2,2,2)$

k	σ
1	1
2	63
3	651
4	10416
5	119133
6	1176357
7	9706503
8	69194232
9	430321633
10	2366967211
11	11618684091
12	51316746768
13	205263418941
14	747748625121
15	2492484372855
16	7633243745820
17	21552658988805
18	56276414970195
19	136248095712855
20	306558278858160
21	642312451217745
22	1255429008934065
23	2292522306124995
24	3916392495228360
25	6266227636741653
26	9399341797058367
27	13228702788676823
28	17480786291963792
29	21700285855317153
30	25317000721419981
31	27767032438524099
32	28634752793916486

Appendix C

Dihedral Groups

In this section we will denote the Dihedral group D_n in its degree s representation as $D(n, s)$.

$D(4,4)$

k	σ
1	1
2	2

$D(4,8)$

k	σ
1	1
2	6
3	7
4	13

$D(5,5)$

k	σ
1	1
2	2

$D(5,10)$

k	σ
1	1
2	7
3	12
4	26
5	26

$D(6,6)$

k	σ
1	1
2	3
3	3

$D(6,12)$

k	σ
1	1
2	9
3	19
4	50
5	66
6	90

$D(7,7)$

k	σ
1	1
2	3
3	4

$D(7,14)$

k	σ
1	1
2	10
3	26
4	82
5	143
6	232
7	246

$D(8,8)$

k	σ
1	1
2	4
3	5
4	8

$D(8,16)$

k	σ
1	1
2	12
3	35
4	130
5	273
6	532
7	715
8	845

$D(9,9)$

k	σ
1	1
2	4
3	7
4	10

$D(9,18)$

k	σ
1	1
2	13
3	46
4	188
5	476
6	1075
7	1768
8	2494
9	2704

$D(10,10)$

k	σ
1	1
2	5
3	8
4	16
5	16

$D(10,20)$

k	σ
1	1
2	15
3	57
4	267
5	776
6	2004
7	3876
8	6414
9	8398
10	9378

$D(11,11)$

k	σ
1	1
2	5
3	10
4	20
5	26

$D(11,22)$

k	σ
1	1
2	16
3	70
4	360
5	1197
6	3474
7	7752
8	14700
9	22610
10	29624
11	32066

$D(12,12)$

k	σ
1	1
2	6
3	12
4	29
5	38
6	50

$D(12,24)$

k	σ
1	1
2	18
3	85
4	479
5	1771
6	5730
7	14421
8	30914
9	54484
10	82148
11	104006
12	113182

Appendix D

$PSL(2,q)$, $Sz(q)$ and $R(q)$

Is this section we give tables for values of σ_k for $PSL(2,q)$.

$PSL(2,2)$ $PSL(2,4)$ $PSL(2,8)$ $PSL(2,16)$

k	σ
1	1

k	σ
1	1
2	1
3	1

k	σ
1	1
2	1
3	1
4	1

k	σ
1	1
2	1
3	1
4	3
5	4
6	8
7	10
8	11

$PSL(2,32)$

k	σ
1	1
2	1
3	1
4	5
5	11
6	53
7	148
8	481
9	1240
10	2964
11	6049
12	11099
13	17759
14	25370
15	32054
16	36045

$PSL(2,64)$

k	σ
1	1
2	1
3	1
4	11
5	40
6	396
7	2741
8	19825
9	122557
10	686242
11	3418419
12	15382884
13	62671071
14	232777653
15	791317807
16	2472867747
17	7127366718
18	19006311249
19	47014965768
20	108134418184
21	231715458345
22	463430916690
23	866412564390
24	1516221987675
25	2486601803061
26	3825541228710
27	5525779362487
28	7499271994953
29	9568034643928
30	11481641572756
31	12963142575416
32	13773338980081

$PSL(2,3)$ $PSL(2,9)$ $PSL(2,27)$ $PSL(2,81)$

k	σ
1	1
2	1

k	σ
1	1
2	1
3	2
4	3
5	4

k	σ
1	1
2	1
3	1
4	6
5	10
6	54
7	124
8	352
9	709
10	1413
11	2185
12	3212
13	3820
14	4208

k	σ
1	1
2	1
3	2
4	18
5	124
6	1462
7	14566
8	135423
9	1105394
10	8061545
11	52721076
12	311892300
13	1679211364
14	8275918844
15	37516692764
16	157100387263
17	609916428107
18	2202473433337
19	7418849947652
20	23369369792992
21	68995262085052
22	191305025566124
23	499056543144016
24	1226847291938554
25	2846285627835338
26	6239933790333132
27	12942084742595510
28	25421952022430098
29	47337427663548448
30	83629455307070090
31	140281666642156042
32	223573905896345978
33	338748341886591892
34	488196139407869156
35	669526133664350820
36	874103563025840264
37	1086723348320185108
38	1286909227975019584
39	1451897590368099280
40	1560789909481571850
41	1598857956053790920

$Sz(2^3)$

k	σ_k
1	1
2	1
3	2
4	33
5	296
6	2914
7	23989
8	173915
9	1098340
10	6150614
11	30740406
12	138331897
13	563924722
14	2094577290
15	7121436602
16	22254489349
17	64144982995
18	171053287380
19	423131170290
20	973201692356

$Sz(2^5)$

k	σ_k
1	1
2	1
3	6
4	1541
5	287096
6	48803566
7	7101265092
8	903635983977
9	102110556557351
10	10374432546124066
11	957277159310463642
12	80889919961734264109
13	6303191453654698278859
14	455630696507039612200642
15	30709508944460592186709766

$R(3^3)$

k	σ
1	1
2	1
3	150
4	623428
5	2443427220
6	8013812054828
7	22527945403688618
8	55410297162241208130
9	121139222946638748437249
10	23834142114641690057862880 5
11	42628446542124586598106987 5960
12	69885785735267901539572563105 0206
13	10575332130647615437083530106454 39432
14	14859097024426374493089439529260505 90344
15	19485229231364452417136242047561322571 33808
16	23953435859481713412008928510037034092984 22692

$R(3^5)$

k	σ
1	1
2	1
3	10086
4	35451376171
5	101732489116660938
6	243291602002140809300534
7	49870962206991668235587933 0498
8	89449187435357931713797156487941 0236
9	14261082728791193501646484418721917006 24000
10	20463083570606922764431204526947087257413729 40222
11	26692972629101321167336342303697782324602292732727 86165

$R(3^7)$

k	σ
1	1
2	1
3	799350
4	2085602656334218
5	4363225346047096148780784
6	7606813034408617115798632828683512
7	1136713586443774831546824330381756459 5497220
8	1486303199753809489989217881754235850223056540 4935708

Appendix E

$A(n)$ and $S(n)$

A_4

k	σ
1	1
2	7
3	21
4	45
5	66
6	86

A_5

k	σ
1	1
2	37
3	577
4	8236
5	91030
6	835476
7	6436782
8	42650532
9	246386091
10	1256602779
11	5711668755
12	23322797475
13	86114390460
14	289098819780
15	886568158468
16	2493474394140
17	6453694644705
18	15417163018725
19	34080036632565
20	69864082608210
21	133074428781570
22	235904682814710
23	389755540347810
24	600873146368170
25	865257299572455
26	1164769471671687
27	1466746704458899
28	1728665795116244
29	1907493251046152
30	1971076398255692

S_4

k	σ
1	1
2	16
3	87
4	469
5	1771
6	5700
7	14421
8	30834
9	54498
10	82016
11	104006
12	113048

S_5

k	σ
1	1
2	72
3	2347
4	68831
5	1588155
6	30446808
7	495729741
8	7002284291
9	87138273898
10	967235959860
11	9672348219898
12	87857173443656
13	729890277209226
14	5578447199130288
15	39421026305381698
16	258700485661397901
17	1582638261961640247
18	9056207835416513832
19	48617536784119860921
20	245518560775512424479
21	1169136003618123572265
22	5261112016352937951960
23	22416912069373527176835
24	906016862806762183991 10
25	347910475316677141792980
26	127121135211970444793942 4
27	44256987814500383306663 08
28	14699642381248383747739468
29	46633348243948925575439764
30	14145448967332282315538869 2