FINDING AN UPPER BOUND TO THE ORDER OF PERMUTATION GROUPS USING THE SIZE OF THE LARGEST CONJUGACY CLASS

by

Lino Raul Guajardo, B.S.

A thesis submitted to the Graduate Council of
Texas State University in partial fulfillment
of the requirements for the degree of
Master of Science
with a Major in Mathematics
May 2020

Committee Members:

Thomas M. Keller, Chair

Maria T. Acosta

Yong Yang

ACKNOWLEDGMENTS

I would like to thank my committee first, without them this document would not have been finished.

Dr. Keller for all of your help and guidance that you provided. Never losing patience with me even as I struggled finding anything in the literature on the alternating groups. Dr. Yang for the training I received to obtain the skills to complete this thesis. And Dr. Acosta for the feedback and support in creating this document.

I want to thank my fellow graduate students and math faculty for the undying support during the creation of this thesis.

Without the support of these graduate students, my committee, or the faculty in the mathematics department that encouraged me to continue, I do not know if I would have finished. Thank you to all of you for your support and guidance.

TABLE OF CONTENTS

I. INTRODUCTION

In this thesis, we will be studying primarily permutation groups. We will consider many different permutation groups and a parameter defined by Harrison [6] in his thesis. Harrison used this parameter to bound the order of a group. We will be observing the relationship between the order of different types of permutation groups and their respective parameter. We will also be looking at special types of p-groups, which are not permutation groups but interesting findings arise. We will examine the relationship with these p-groups and their respective parameters. We will also test to see if it is possible to improve the bound discussed by Harrison, specifically in cases where our specific p-groups have a large derived length. More will be explained about this parameter later in this chapter.

Important Definitions

First, we would like to remind the reader that a group is a set of objects under a binary operation. This set must also meet the following requirements: the set must be closed under the binary operation, the set must contain an identity element and inverses of all elements, and the operation must follow the associative law. Before we can look at the permutation groups and the parameter, let us first look at some essential definitions. For this chapter, we will let G denote a group.

Definition 1. The *center* of a group is the set of elements of G that commutes with all other elements. We denote this subgroup as $\mathbf{Z}(G)$.

Definition 2. Let $x \in G$. We say that $\mathbf{C}_G(x)$, the *centralizer* of x, is the subgroup of G containing all of the elements of G that commute with x.

Definition 3. Let N be a subgroup of G. We say that N is *normal* in G if for every element $g \in G$, $g^{-1}Ng = N$. We denote a normal subgroup N of G as $N \lhd G$.

We would like to remind the reader that for any two elements $x, g \in G$, $g^{-1}xg$ is the conjugate of x with respect to g. It can also be denoted as x^g.

Definition 4. Let $x \in G$. Then the *conjugacy class* of x is the subset of G containing the elements x^g, for all $g \in G$.

For the rest of this thesis, we shall denote the conjugacy class of an element $x \in G$ as $k_G(x)$.

For the remaining definitions, we let Ω be a nonempty finite set.

Definition 5. We say that G *acts on* Ω under the action $(\cdot)$ if the two following conditions hold:

1. $\alpha \cdot 1 = \alpha$, for all $\alpha \in \Omega$.

2. $(\alpha \cdot g) \cdot h = \alpha \cdot gh$, for all $\alpha \in \Omega$ and $g, h \in G$.

This is also known as a *group action*.

Definition 6. An *orbit* of a group action is the set of elements $\alpha \cdot g$ for a set element $\alpha \in \Omega$ and for all $g \in G$. We denote this set as $\mathcal{O}_\alpha$.

When G acts on itself under the conjugation action, a conjugacy class is an orbit.

Definition 7. The *stabilizer* of an element $\alpha \in \Omega$ is the set of elements $g \in G$, such that $\alpha \cdot g = \alpha$. We denote this subgroup of G as G_α.

This can also be called a *point stabilizer*.

Theorem 1.1 (Fundamental Counting Principle). Let G be a group that acts on Ω. and $\mathcal{O}_\alpha$ be an orbit of Ω containing $\alpha \in \Omega$. Let $H = G_\alpha$ and $\Delta = \{Hx \mid x \in G\}$ be the set of right cosets of H in G. Then there exists a bijection $\theta : \Delta \to \mathcal{O}_\alpha$ such that $\theta(Hg) = \alpha \cdot g$. So, $|\mathcal{O}_\alpha| = |G : G_\alpha|$.

A proof of this theorem can be found in [10], Chapter 1 Section A Theorem 1.4.

From the FCP, we can see that if G acts on itself under the conjugation action, then $|k_G(x)| = \frac{|G|}{|\mathbf{C}_G(x)|}$.

Definition 8. Let G act on Ω. We say that the action is *faithful* if $\alpha \cdot g = \alpha$ only when g is the identity in G.

Definition 9. A *permutation group* is group G that acts faithfully on the set Ω.

Another way to think of this, is let $g \in G$ and $\sigma_g : \Omega \to \Omega$, such that $\sigma_g(\alpha) = \alpha \cdot g$, for all $\alpha \in \Omega$. Now we can create a homomorphism $\theta : G \to \Omega$ such that $\theta(g) = \sigma_g$. This homomorphism is known as a *permutation representation* and a group G that acts on a set Ω is a permutation group if its permutation representation is an injective homomorphism.

Parameter e

In 2008, Snyder [16] bounded the order a group by e, where his e used representation theory. Snyder used that fact that if G has order n, then $n = d(d+e)$ where d is a character degree of G and e is some non-negative integer. Snyder then proved his main result in [16] where he created his upper bound of the order of G. We state the theorem without proof.

Theorem 1.2. Let G be a finite group of order n with a simple $\mathbb{C}[G]$-module V of dimension d and $d(d+e) = n$.

1. If $e = 0$, then G is trivial.
2. If $e = 1$, then G is a doubly transitive Frobenius group or a cyclic group with two elements.
3. If $e > 1$, then $n \leq ((2e)!)^2$.

Note that for this thesis, we are not concerned with (1) and (2) from this main result. We will also define what it means for a group to be a Frobenius group and doubly transitive in a later chapter.

With this upper bound on the order of a group, it became popular to attempt to improve this bound. It was in 2011, Isaacs [11] made an improvement to this bound on the group order. The main result is presented without proof.

Theorem 1.3. Let $|G| = d(d+e)$, where d is the degree of some irreducible character of G and $e > 1$. Then $|G| \leq Be^6$ for some universal constant B.

Later in 2011, Durfee and Jensen [4], two students of Isaacs, improved this bound further. We present their main result without proof.

Theorem 1.4. For $e > 1$ we have the following bounds on d and $|G|$ in terms of e.

1. If e is not a prime power then $d^2 < e$ and $|G| < e^4 + e^3$.
2. If e is a prime power then $d < e^3 - e$ and $|G| < e^6 - e^4$.
3. If e is a prime then $d < e^2$ and $|G| < e^4 + e^3$.

Recall that d is the degree of an irreducible character in G.

Because of formal parallels between character degrees and conjugacy class sizes, on the group theoretical side one can define a parameter in a similar fashion as one defines the representation theoretic e. We call this group theoretic parameter also e. This parameter was first studied by Harrison [6, 7]. We will now define e as Harrison did.

Definition 10. e shall be defined in the following way:

$$e = min(|\mathbf{C}_G(x)| - 1)\sqrt{|k_G(x)|} : x \in G.$$

From this, Harrison was able to deduce that the largest conjugacy class of G and its respective centralizer (which would be the smallest centralizer of G) can be used to define e instead. For the remainder of this thesis, we shall denote $\mathbf{C}_G(x)$, where $x \in G$ such that its centralizer is minimal in G, and the size of the largest conjugacy class in G as C_G and k_G, respectively. So. let us define the parameter e as such for the remainder of the thesis.

Definition 11. We shall define e as follows:

$$e = (C_G - 1)\sqrt{k_G}.$$

Harrison used this parameter e to prove a general bound for the order of the group. He proved the following theorem. We state this theorem without proof, if the reader would like to see the proof refer to [6, 7].

Theorem 1.5. Let G be a finite group. Then $|G| \leq 2e^2$.

For the remainder of this thesis, we shall denote our parameter e as e_G, where G is the group we are studying.

II. ALTERNATING GROUPS

The alternating group, denoted as A_n, is the proper subgroup of the symmetric group, S_n, where the index is two. A_n is also known as the proper subgroup of S_n containing all even permutations. Since A_n is a subgroup of S_n, the conjugacy classes of A_n depend on S_n. So, we will find what a conjugacy class in A_n will look like.

First, let us see how we can determine the size of conjugacy classes in S_n.

Theorem 2.1. Let $x \in S_n$, such that x is of cycle type $(m_1)(m_2)\cdots(m_r)$. Now, let j_i be the number of cycles of cycle length equal to m_i. Thus, we can say that

$$|k_{S_n}(x)| = \frac{n!}{\prod_{i=1}^{r}(m_i)^{j_i}(j_i!)}.$$

Reference to this can be found in [3] (Chapter 4, page 132, problem 33).

Let $k_{S_n}(x)$ be a conjugacy class of $x \in S_n$, where x is an even permutation. Then, either $k_{S_n}(x)$ splits or it does not split as a conjugacy class of x in A_n. If $k_{S_n}(x)$ splits, then $|k_{S_n}(x)| = 2|k_{A_n}(x)|$, where $k_{A_n}(x)$ is the conjugacy class of $x \in A_n$. If $k_{S_n}(x)$ does not split, then it is also the conjugacy class to $x \in A_n$.

The criteria to determine if $k_{S_n}(x)$ splits in A_n or does not split in A_n are the following:

- $k_{S_n}(x)$ splits if it is made up of permutations with distinct cycles of odd length.
- $k_{S_n}(x)$ does not split if it is made up of permutations that have a cycle of even length or two cycles of equal length.

The splitting criteria and what it means for a conjugacy class in S_n to split in A_n can be found in Scott's book [15].

From this, we shall be able to observe that the largest conjugacy class of the symmetric group is not the largest in the alternating group.

Theorem 2.2. Let $n \in \mathbb{N}$, where $n > 4$ and n is even. If x is a $(n-1)$-cycle in A_n, then there exists a $y \in A_n$, where y is not a $(n-1)$-cycle, such that $|k_{A_n}(x)| < |k_{A_n}(y)|$.

Proof. By the splitting criteria above, it can be noticed that $k_{S_n}(x)$ splits in A_n. Since $|k_{S_n}(x)| = \frac{n!}{n-1}$, then, $|k_{A_n}(x)| = \frac{n!}{2(n-1)}$.

Let $y \in S_n$, such that y is a $(n-2)(2)$-cycle. Notice that $y \in A_n$ and that the conjugacy class, $k_{S_n}(y)$, containing y does not split. Now, notice that $|k_{S_n}(y)| = |k_{A_n}(y)| = \frac{n!}{2(n-2)}$. We shall now compare the denominators of $|k_{A_n}(x)|$ and $|k_{A_n}(y)|$ since they share the same numerators. Notice that $2(n-1) > 2(n-2)$. Thus, $|k_{A_n}(x)| < |k_{A_n}(y)|$.

Therefore, we have shown that there exists a conjugacy class $k_{A_n}(y)$, for some $y \in A_n$ where y is not a $(n-1)$-cycle, whose size is larger than the size of $k_{A_n}(x)$.

□

Notice, if $n = 3$ the largest conjugacy class size of A_3 is 1 and when $n = 4$, the largest conjugacy class size of A_4 is four. So, for the rest of this section, we will assume $n > 4$.

We would like to inform the reader that we found our parameter e for some alternating groups by using the group theory program GAP. We shall now discuss our findings with GAP.

Using GAP

Notice that as n gets larger then the order of A_n and S_n become unmanageable. So, we use the group theory coding system GAP. With GAP, we can find the largest conjugacy class of A_n for a large n. Although we can use GAP for a large n, of course we can only check for as big of an n as GAP's system will allow. The information presented in this section was checked and confirmed for $n = 8, 9, ..., 20$ and for $n = 40$. We would like to note that $n = 45$ and $n = 50$ was attempted, but the computing size was too big for GAP's memory to handle. Now, we must consider two cases; when n is even and when n is odd. To help determine the largest conjugacy class in A_n, we must first look at S_n. Using GAP, we can see that the largest four conjugacy classes in S_n, respectively, are the conjugacy classes made up of $(n-1), (n), (n-3)(2), (n-2)(2)$ and $(n-2)$-cycles, with the $(n-2)$-cycle and the cycle type $(n-2)(2)$ having equal conjugacy classes sizes. Now we shall observe the two cases. We would like to note that the code we used to find the largest conjugacy class of A_n and the largest four conjugacy classes of S_n can be found in Appendix A.

Theorem 2.3. For the values of n tested above, the largest conjugacy class of A_n is either made up of elements of cycle type $(n-2)(2)$ or $(n-3)(2)$.

Proof. Case 1: n is even.

From Theorem 2.1 the conjugacy classes made up of $(n-1)$-cycles will have a smaller conjugacy class sizes than the conjugacy class made up of elements of cycle type $(n-2)(2)$. Also, the conjugacy classes made up of (n), $(n-2)$-cycles, and of cycle type $(n-3)(2)$, respectively, will not be contained in A_n. Thus the conjugacy class made up of elements of cycle type $(n-2)(2)$ is the largest in A_n.

Case 2: n is odd.

Notice that $(n-1)$-cycles are not in A_n. Now, observe that the conjugacy class made up of (n)-cycles splits. So, $\frac{n!}{2n} < \frac{n!}{2(n-2)}$. Thus, the largest conjugacy class in A_n is the one made up of $(n-3)(2)$-cycles.

Thus, we an see that the largest conjugacy class is made up of either elements with cycle type $(n-2)(2)$ or $(n-3)(2)$.

$\square$

Parameter e for A_n using GAP

Let us first consider the case where n is even.

Since the largest conjugacy class is made up of elements with cycle type $(n-2)(2)$, then

$$e_{A_n} = (n-2-1)\sqrt{\frac{n!}{2(n-2)}}.$$

Now we will consider $e^2_{A_n}$.

$$e^2_{A_n} = (n-3)^2 \frac{n!}{2(n-2)}$$

$$= \frac{n!}{2}\left[\frac{((n-3)^2}{n-2}\right]$$

$$= \frac{n!}{2}\left[\frac{n^2-6n+9}{n-2}\right]$$

Now, to show that $e^2_{A_n} \geq |A_n|$, we must show that $\frac{n^2-6n+9}{n-2} > 1$. By simple algebra, this can be shown to be true when $n > 4$ and since our $n > 4$, we can conclude that $e^2_{A_n} \geq |A_n|$ is true.

Thus, if n is even and $n > 4$, then $e^2_{A_n} \geq |A_n|$.

Now we shall consider the case when n is odd.

Since the largest conjugacy class is made up of elements with cycle type $(n-3)(2)$, then

$$e_{A_n} = (n-4)\sqrt{\frac{n!}{2(n-3)}}.$$

Now we will consider $e^2_{A_n}$.

$$e^2_{A_n} = (n-4)^2\left[\frac{n!}{2(n-3)}\right]$$

$$= \frac{n!}{2}\left[\frac{(n-4)^2}{n-3}\right]$$

$$= \frac{n!}{2}\left[\frac{n^2-8n+16}{n-3}\right]$$

Now, to show that $e_{A_n}^2 > |A_n|$, we must show that $\frac{n^2-8n+16}{n-3} > 1$. By simple algebra, this can be shown to be true when $n > 5$.

In the case when $n = 5$, we get that the largest conjugacy class is not made up of permutations of cycle type $(n-3)(2)$. Instead, the largest conjugcay class is made up of $(n-2)$-cycles. Now, with $n = 5$, we see that permutations made up of $(n-3)(2)$ are going to be of cycle type $(2)(2)(1)$. With this, it alters our arbitrary class size from $\frac{n!}{2(n-3)}$ to $\frac{n!}{(2^2)(2!)}$. The cycles are no longer of separate length, meaning $n-3$ is no longer different from 2, so we find that the largest conjugacy class is made up of permutations of $(n-2)$-cycles. When $n = 5$, these cycles become (3)-cycles. So, in the case of when $n = 5$, we get our largest conjugacy class to have size $\frac{5!}{(3)(2!)} = 20$ and with smallest centralizer size 3. So, we get

$$e_{A_5} = (3-1)\sqrt{20} = 2\sqrt{20}$$

and

$$e_{A_5}^2 = 80.$$

Thus, we can see that $e_{A_5}^2 \leq |A_5|$.

Thus, in both cases for even and odd n, we can increase the accuracy of our bound to $e_{A_n}^2 \geq |A_n|$, with $n \geq 5$.

III. MATHIEU GROUPS

In this chapter, we will be discussing the five Mathieu Groups. Note the information presented about the Mathieu groups was obtained and can be further investigated in [2]. Before we do, we will first define relevant information about the Mathieu Groups. First of which is the group $\mathrm{PSL}(n,q)$, where $n \geq 2$ and q is a prime power. To understand what this group is, we must first let F be a field of order q. With n and q, we can construct the general linear group $\mathrm{GL}(n,q)$, which is the group of invertible $n \times n$ matrices over the field F. Defining $\mathrm{SL}(n,q)$ to be the normal subgroup of $\mathrm{GL}(n,q)$, whose elements have determinant 1. The center of $\mathrm{SL}(n,q)$, we shall denote as Z. The center of this group is exactly all of the scalar matrices with determinant 1. So, we can now define $\mathrm{PSL}(n,q) = \mathrm{SL}(n,q)/Z$. We will also define Steiner systems.

Definition 12. A *Steiner system* is defined as $S = S(\Omega, \mathcal{B})$, where Ω is a finite set of points, and $\mathcal{B}$ is set of subsets of Ω, which are called blocks. We say for some integers t and λ, where t is the size of a subset of Ω and λ is the size of each block, every t points are contained in exactly one block. We also say that an automorphism of $S(\Omega, \lambda)$ is a permutation over Ω that also permutes the blocks amongst themselves as well.

More can be found about Steiner systems through [2], Chapter 6 Section 6.2.

The Mathieu groups were first discovered by Emile Mathieu between 1861-1873. These permutation groups are the first five of 26 sporadic simple groups. Meaning they are simple groups not belonging to an infinite family. The Mathieu groups will be denoted as M_{11}, M_{12}, M_{22}, M_{23}, and M_{24}, where the index is the number of items being permuted. Each $M_i \subset M_{24}$, where $i = 11, 12, 22, 23$. These groups are the automorphism groups of Steiner systems.

We shall discuss further theses groups, but first need to establish these definitions.

Definition 13. Let G act on Ω and $|\Omega| = n$. Then, we say that the *degree* of G is n.

Definition 14. Let G act on Ω. If for each $\alpha, \beta \in \Omega$, there exists a $g \in G$ such that $\alpha \cdot g = \beta$, then G is *transitive* on Ω.

Definition 15. Let G transitively act on Ω. If for each $\alpha, \beta \in \Omega$ there exists a unique $g \in G$, such that $\alpha \cdot g = \beta$, then G is *regular* on Ω.

We can also say that G is *sharply transitive* on Ω.

Definition 16. Let G act on Ω. Let $\mathcal{O}_k(\Omega)$ be the set of k-tuples, i.e. of elements $(\alpha_1, \alpha_2, \cdots, \alpha_k)$, where each $\alpha_i \in \Omega$. Then G is *k-transitive* on Ω, if for each $(\alpha_1, \alpha_2, \cdots, \alpha_k)$ and $(\beta_1, \beta_2, \cdots, \beta_k)$, there exists a $g \in G$ such that

$$(\alpha_1, \alpha_2, \cdots, \alpha_k) \cdot g = (\alpha_1 \cdot g, \alpha_2 \cdot g, \cdots, \alpha_k \cdot g) = (\beta_1, \beta_2, \cdots, \beta_k)$$

We can also say that G is *multiply transitive* on Ω.

Small Mathieu Groups

The small Mathieu groups are M_{11}, M_{12}. The group M_{11} is a subset of M_{12} and is a point stabilizer of M_{12}. While the group M_{12} is regular 5-transitive of degree 12. So, any 5-point stabilizer in the group, must be the identity. Thus, we can say that M_{11} is sharply 4-transitive on 11 points. M_{11} has a 3-transitive action on 12 points such that the point stabilizers are isomorphic to $\mathrm{PSL}(2,11)$. So, it can be seen that $\mathrm{PSL}(2,11)$ is both the natural 2-transitive action of degree 12 and an exceptional 2-transitive action of degree 11.

Large Mathieu Groups

The large Mathieu groups consist of M_{22}, M_{23}, and M_{24}. The largest of the three being M_{24}, which is 5-transitive of degree 24. Each of M_{23} and M_{22} are one-point and two-point stabilizers, respectively. The group PSL$(3, 4)$ is isomorphic to the point stabilizers in M_{22} in its natural 2-transitive action on PSL$(3, 4)$.

Parameter e for Mathieu Groups

We shall now explore the parameter e discussed by Harrison. Note the information collected in this section was with the help of the ATLAS [1]. First, we need to know the order and largest conjugacy class size for each group. We shall denote the size of the largest conjugacy class of each group as k_{M_i}, where i is the index to its respective Mathieu group. $|M_{11}| = 2^4 \cdot 3^2 \cdot 5 \cdot 11$, with $k_{M_{11}} = 2^4 \cdot 3^2 \cdot 11$. $|M_{12}| = 2^6 \cdot 3^2 \cdot 5 \cdot 11$, with $k_{M_{12}} = 2^5 \cdot 3 \cdot 5 \cdot 11$. $|M_{22}| = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$, with $k_{M_{22}} = 2^7 \cdot 3^2 \cdot 7 \cdot 11$. $|M_{23}| = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$, with $k_{M_{23}} = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$. $|M_{24}| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$, with $k_{M_{24}} = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 23$.

We shall denote the size of the centralizer pertaining to a representative of the largest conjugacy class as C_{M_i}, where i pertains to their respective Mathieu group. So, $C_{M_{11}} = 5$, $C_{M_{12}} = 2 \cdot 3 = 6$, $C_{M_{22}} = 5$, $C_{M_{23}} = 2^3 = 8$, and $C_{M_{24}} = 11$. We shall also denote the parameter e to be e_{M_i}, where i is the index to its respective Mathieu group.

Recall that $e = (C_G - 1) \cdot \sqrt{k_G}$, where C_G and k_G is the size of the smallest centralizer and largest conjugacy class of the group, respectively. So,

$$e_{M_{11}} = (5-1)\sqrt{2^4 \cdot 3^2 \cdot 11} = 2^4 \cdot 3 \cdot \sqrt{11}$$

$$e_{M_{12}} = (6-1)\sqrt{2^5 \cdot 3 \cdot 5 \cdot 11} = 2^2 \cdot 5 \cdot \sqrt{2 \cdot 3 \cdot 5 \cdot 11}$$

$$e_{M_{22}} = (5-1)\sqrt{2^7 \cdot 3^2 \cdot 7 \cdot 11} = 2^5 \cdot 3 \cdot \sqrt{2 \cdot 7 \cdot 11}$$

$$e_{M_{23}} = (8-1)\sqrt{2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23} = 2^2 \cdot 3 \cdot 7 \cdot \sqrt{5 \cdot 7 \cdot 11 \cdot 23}$$

$$e_{M_{24}} = (11-1)\sqrt{2^10 \cdot 3^3 \cdot 5 \cdot 7 \cdot 23} = 2^5 \cdot 3 \cdot \sqrt{3 \cdot 5 \cdot 7 \cdot 11 \cdot 23}$$

If we write the order of each Mathieu group in terms of their respective e, we see

$$|M_{11}| = \frac{5}{24}e^2_{M_{11}}$$

$$|M_{12}| = \frac{6}{25}e^2_{M_{12}}$$

$$|M_{22}| = \frac{5}{24}e^2_{M_{22}}$$

$$|M_{23}| = (\frac{5}{24}e_{M_{23}})^2$$

$$|M_{24}| = e^2_{M_{24}}.$$

From this, we can improve the bound in respect to Mathieu groups. It can be seen that for any Mathieu group, M, $|M| \leq e^2$.

IV. p-GROUPS OF MAXIMAL CLASS

In this section we shall discuss the parameter e for p-groups with maximal class. First we shall discuss information about p-groups.

p-Groups

Let p be a prime. We say that P is a p-group if $|P| = p^a$, where $a \in \mathbb{N}$. We shall now present some theorems about p-groups.

Theorem 4.1. Let P be a finite p-group. Suppose that N is a nontrivial normal subgroup of P. Then, $N \cap \mathbf{Z}(P) > 1$.

Proof. Let us look at the conjugation action from P on N. Then, the total set of fixed points from this action is $N \cap \mathbf{Z}(P)$. This tells us that every element in $N \cap \mathbf{Z}(P)$ will be in an orbit of size 1. Recall that from the Fundamental Counting Principal, that all non trivial orbits must have an order that divides the order of the group. So, all nontrivial orbits are made up from elements in $N - N \cap \mathbf{Z}(P)$ and will have an order that divides p. So, it must be that $|N - N \cap \mathbf{Z}(P)|$ divides p. Thus, $|N \cap \mathbf{Z}(P)| \equiv |N| \bmod p$. Now since we defined N to be a nontrivial p-group, then $|N| \equiv 0 \bmod p$. Thus, $|N \cap \mathbf{Z}(P)| \equiv |N| \bmod p \equiv 0 \bmod p$. Since $N \cap \mathbf{Z}(P) \neq 1$, then $N \cap \mathbf{Z}(P) > 1$.

So, we have shown that if P has a nontrivial normal subgroup, then the center of P is also nontrivial.

□

Definition 17. Let G be a group. Then, G is said to be *nilpotent*, if there exists a finite collection of normal subgroups of G, $G_0, G_1, G_2, ..., G_n$, where

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq ... \subseteq G_n = G,$$

such that

$$G_{i+1}/G_i \subseteq \mathbf{Z}(G/G_i)$$

for $i \in \{0, 1, 2, ..., n\}$

Definition 18. Let G be a group. G is to have a *central series* if there exists a a set $\{N_i\}_{i=0}^{n}$ of normal subgroups of G, such that

$$N_0 \subseteq N_1 \subseteq \cdots \subseteq N_n$$

and $N_{i+1}/N_i \subseteq \mathbf{Z}(G/N_i)$

Note: 1 and G are included in the above series iff G is nilpotent. I.e. if the central series is

$$1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_n = G$$

then G is nilpotent.

Theorem 4.2 (Correspondence Theorem). Let $\varphi : G \to H$ be a surjective homomorphism and let N =ker(φ). Define the following sets of subgroups:

$$S = \{U \mid N \subseteq U \subseteq G\}$$

and

$$T = \{V \mid V \subseteq H\}.$$

Then φ and φ^{-1} are inverse bijections between S and T. Furthermore, these maps respect containment, indices, normality, and factor groups.

Note, proof of this theorem can be found in [9], Chapter 3 page 35.

Theorem 4.3. Let G be a finite group and M be a proper normal subgroup of G. If $\mathbf{Z}(G/M) > 1$ for all $M \triangleleft G$, then G is nilpotent.

Proof. Define $Z_0 = 1$, $Z_1 = \mathbf{Z}(G)$, and Z_i such that $Z_i/Z_{i-1} = \mathbf{Z}(G/Z_{i-1})$ for all $i \geq 2$.

Notice that by the Correspondence Theorem, this guarantees each of the Z_i's to be normal, for $i \geq 1$. Also notice that for each $i \in \mathbb{Z}$, we have $Z_{i+1} > Z_i$. So since G is finite, then there must exist an $n \in \mathbb{Z}$, such that $Z_n = G$. Thus we have created the central series

$$1 = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_n = G$$

So, by Definition 6, G is nilpotent.

Thus, we have shown that for all $M \lhd G$ and $\mathbf{Z}(G/M) > 1$, then G is nilpotent.

□

Theorem 4.4. A finite p-group is nilpotent.

Proof. By Theorem 4.1, we know that any nontrivial finite p-group has a nontrivial center. So, by Theorem 4.3 we have our desired result.

Thus a finite p-group is nilpotent.

□

Now we will define what it means for a p-group to have maximal class. First, we must define nilpotency class. To do this, we must first define a set of related definitions.

Let us define $Z_0(G) = 1$ and $Z_i(G)$ such that $Z_i(G)/Z_{i-1}(G) = \mathbf{Z}(G/Z_{i-1}(G))$ for $i > 0$.

So, we can define the *nilpotency class* of a group G to be the smallest integer n, such that $Z_n(G) = G$.

Thus we can now define what it means for a p-group to have a maximal class. We define a p-group P of order p^n to have *maximal class* if P has nilpotency class of $n-1$, where $n > 3$.

Any dihedral, semidihedral, and quaternion 2-groups are examples of p-groups of maximal class. A proof of these groups being of maximal class can be found in [12, 5].

Parameter e for p-Groups

For the rest of this section, let us denote G to be a p-group of maximal class of order p^n.

To be able to discuss the parameter e, we must find the largest conjugacy class of our group G. To do this, we must define uniform elements.

Definition 19. Let G be a p-group of order p^n of maximal class. Let us define $s \in G$ to be a *uniform element* if $s \notin \bigcup_{i=2}^{n-2} \mathbf{C}_G(G_i/G_{i+2})$.

With these elements we can find out the size of the largest conjugacy class of our group G. But we must first know if there exists uniform elements inside our group. Luckily, Burnside was able to achieve this. Firstly, he was able to show that p-groups of maximal class always contain uniform elements.

We will present Burnside's Theorem and the following Theorem 4.5 without proof. The proofs of these theorems can be found in [5].

Theorem 4.5. (Burnside's Theorem) Let G be a p-group of maximal class of order p^n. Then the following statements hold:

1. If $l(G) = 0$ then $p \geq 5$, n is even, and $6 \leq n \leq p+1$.

2. $l(G/Z(G)) \geq 1$.

3. G has uniform elements.

Here $l(G)$ is the degree of commutativity of G. We leave the reader to look into this if interested, as we will not be using this in this thesis. More information can be found in [5], Chapter 3 Section 3.2.

With this theorem, we know that a uniform element exists, so we can now find the largest conjugacy class of p-groups of maximal class.

Theorem 4.6. Let G be a p-group of maximal class of order p^n and let s be a uniform element of G. Then the following properties hold:

1. $\mathbf{C}_G(s) = \langle s \rangle Z(G)$.
2. $s^p \in Z(G)$ and consequently $o(s) \leq p^2$ and $|\mathbf{C}_G(s)| = p^2$.
3. The conjugates of s are exactly the elements in the cosset sG_2.
4. For $0 \leq t \leq m-4$, the subgroup $H = \langle s, G_{i+1} \rangle$ is a p-group of maximal class of order p^{m-t} and such that $H_i = G_{i+1}$ for every $i \geq 1$. Hence, either $l(H) = m-t-2$ or $l(H) \geq l(G)+t$.

By (2) in Theorem 4.5, we can see that if s is a uniform element of our group G then $|\mathbf{C}_G(s)| = p^2$ and by (3) in Burnside's Theorem, we see that G does have uniform elements. So, from these two properties the largest conjugacy class of G, $k_G(s)$, is of order p^{n-2}.

We shall denote the parameter e for our p-group G as e_p. Thus, we can see that

$$\begin{aligned} e_p &= (|\mathbf{C}_G(s)| - 1)\sqrt{|k_G(s)|} \\ &= (p^2-1)\sqrt{p^{n-2}} \\ &= \sqrt{p^n}(p - \frac{1}{p}) \end{aligned}$$

and

$$e_p^2 = p^n (p - \frac{1}{p})^2.$$

Notice that $(p-\frac{1}{p})^2 > 1$, so we can improve our upper bound of the order of G using our parameter from $|G| \leq 2e_p^2$ to $|G| \leq e_p^2$, where $|G| = \frac{e_p^2}{(p-\frac{1}{p})^2}$.

Now, notice that

$$e_p^2 = p^n (p - \frac{1}{p})^2 = |G|(p - \frac{1}{p})^2$$

$$\frac{e_p^2}{(p-\frac{1}{p})^2} = |G|$$

Let us now fix a $p > 1000$. Then, $(p - \frac{1}{p}) \approx p$. So, $\frac{e_p^2}{p^2} \approx |G|$. Now, since $|G| = p^n$, then $p^2 = |G|^{\frac{2}{n}}$.

So,

$$\frac{e_p^2}{p^2} \approx |G|$$

$$\frac{e_p^2}{|G|^{\frac{2}{n}}} \approx |G|$$

$$e_p^2 \approx |G|^{1+\frac{2}{n}}$$

$$e_p^{\frac{2}{1+\frac{2}{n}}} \approx |G|$$

Now, as $n \to \infty$, $1 + \frac{2}{n} \to 1$. So, as $n \to \infty$, $e_p^{\frac{2}{1+\frac{2}{n}}} \to e_p^2$. Thus, as $n \to \infty$, $e_p^2 \to |G|$.

Therefore, $\lim_{n\to\infty} e_p^2 \approx |G|$.

Derived Length of a p-Group and its Parameter e

In this section, we shall explore the conditions needed to decrease our upper bound of $|G|$ to be less than e_G^2. Before we can explore this, we must first note some definitions.

Definition 20. We say that G is *solvable* if there exists a finite collection of normal subgroups $G_0, G_1, \cdots, G_n$, such that

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

and G_{i+1}/G_i is abelian for all $i \in \{0, 1, \cdots, n-1\}$.

Definition 21. Let $x, y \in G$. We say the *commutator* of x and y is $x^{-1}y^{-1}xy$. We denote this as $[x, y]$.

Definition 22. Let G' be the set of commutators of x and y, for all $x, y \in G$. We say that G' is the *commutator subgroup* of G. This is also known as the *derived* subgroup of G.

Note, that G' is the smallest normal subgroup of G, such that G/G' is abelian. We can also denote $G' = [G, G]$.

From this derived subgroup, we can create G'' as the derived subgroup of G'. We can then create G''' to be the derived subgroup of G'' and can continue this process indefinitely. Lets write this series as $G^{(0)} = G, G^{(1)} = G', G^{(2)} = G'', \ldots, G^{(n)} = (G^{(n-1)})'$. Now, let us observe the following theorem:

Theorem 4.7. A group G is solvable if and only if $G^{(n)} = 1$, for some $n \in \mathbb{Z}$.

Proof. First let us assume G is solvable. Then there exists normal subgroups of G, $G_0, G_1, \ldots G_n$, such that

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

where G_{i+1}/G_i is abelian for all $i \in \{0, 1, \ldots, n-1\}$. Now since G' is the smallest normal subgroup of G and $G_{i+1} \triangleleft G_i$, then we can notice that $(G_{i+1})' \subseteq G_i$ for all $i \in \{0, 1, \ldots, n-1\}$. Notice that since $G_n = G$ and G' is the smallest normal subgroup of G with an abelian factor group, then $G' \subseteq G_{n-1}$. Now since $G^{(2)} = G'' = (G')'$ and $G' \subseteq G_{n-1}$, then $G^{(2)} \subseteq (G_{n-1})' \subseteq G_{n-2}$. So, $G^{(2)} \subseteq G_{n-2}$. If we continue this process, we can deduce that $G^{(k)} \subseteq G_{n-k}$, for all $0 \leq k \leq n$. From this, we can see that $G^{(n)} \subseteq G_0 = 1$. Thus, $G^{(n)} = 1$.

Now, assume that $G^{(n)} = 1$, for some $n \in \mathbb{Z}$. This thus implies that

$$1 = G^{(n)} \subseteq G^{(n-1)} \subseteq \cdots \subseteq G^{(1)} \subseteq G^{(0)} = G.$$

Since, for all $0 \leq k \leq n$, $G^{(k)} \triangleleft G$, then G is solvable.

Thus, G is solvable if and only if $G^{(n)} = 1$, for some $n \in \mathbb{Z}$.

□

This theorem helps confirm, that if G is solvable, then there is a derived series of G such that $G^{(0)} = G$ and $G^{(n)} = 1$. This smallest integer n such that $G^{(n)} = 1$ is called the *derived length* of G, denoted as $dl(G)$.

With this information of a derived length, we are able to place an upper bound on the derived length using the group's nilpotency class. We present the following theorem without proof. The reader can find the proof in [9], Chapter 8 Theorem 8.30.

Theorem 4.8. Let G be nilpotent with derived length d and nilpotency class c. Then

$$d < 1 + log_2(c+1).$$

We will be presenting a theorem without proof, the proof can be found in [12], Chapter 3 Section 3.4 Corollary 3.4.13. We would like to note that (1) of the theorem is unneccessary for this thesis and interested readers should look at Leedham-Green and McKay's book [12] for further information.

Theorem 4.9. Let G be a p-group of maximal class $p \geq 5$.

1. If $|G| \geq p^{6p-23}$ then P_1 is nilpotent of class at most 3.

2. If $|G| \geq p^{6p-35}$ then G has derived length at most 3.

Now, suppose our p-group G, with $p \geq 5$ and maximal class has a large derived length. From Theorem 4.9, it implies that if G has a large derived length, then $|G| \approx p^p$. Now recall from the previous section that $e_p = \sqrt{p^n}(p - \frac{1}{p})$. So, in this case $e_p = \sqrt{p^p}(p - \frac{1}{p})$. For any $p > 2$, $(p - \frac{1}{p}) \approx p$. Since $|G| \approx p^p$, then $p \approx |G|^{\frac{1}{p}}$. So, $(p - \frac{1}{p})^2 \approx p^2 \approx |G|^{\frac{2}{p}}$.

Thus, we can see that

$$p^p p^2 \approx e_p^2.$$

Recall that $|G| \approx p^p$, so

$$|G|^{1+\frac{2}{p}} \approx e_p^2.$$

$$|G| \approx e_p^{\frac{2}{1+\frac{2}{p}}}$$

$$|G| \approx e_p^{\frac{2p}{p+2}}.$$

Thus, as we can see in this case we are actually able to improve the upper bound of the group order from $|G| \leq 2e_p^2$ to approximately $|G| \leq e_p^{\frac{2p}{p+2}}$.

Since our discussion requires us to approximate from $(p - \frac{1}{p})$ to p our upper bound is not fully accurate, as it depends on an approximation where$(p-\frac{1}{p}) < p$. We shall instead get rid of our approximation and use a number greater than $(p - \frac{1}{p})^2$.

We still use the assumption that a p-group with maximal class and a large derived length has size approximate to p^p. Now, notice that $(p - \frac{1}{p})^2 = p^2 - 2 + \frac{1}{p^2} > p^2 - 2 \geq \frac{1}{2}p^2$. Thus, we can see that

$$p^p(\frac{1}{2}p^2) \leq p^p(p^2 - 2) < p^p(p - \frac{1}{p})^2 = e_p^2.$$

Now we can deduce the following,

$$\frac{1}{2}p^{p+2} < e_p^2$$

$$p^{p+2} < e_p^2$$

$$|G|^{\frac{p+2}{p}} < 2e_p^2$$

$$|G| < (2e_p^2)^{\frac{p}{p+2}}$$

Now we need to show that this new upper bound is less than our upper bound for arbitrary p-groups with maximal class, e_p^2.

To show this, we shall look at for what values of p does the following hold:

$(2e_p^2)^{\frac{p}{p+2}} < e_p^2$. This means that we must check if $2 < (e_p{}^2)^{\frac{2}{p}}$. From this, since $e_p = \sqrt{p^p}(p - \frac{1}{p})$, it follows that one has to show that

$$2 < [p^{p+2} - 2p^p + p^{p-2}]^{\frac{2}{p}},$$

which is true for all values of p. Thus, when the derived length of a p-group of maximal class is large $|G| < (2e^2)^{\frac{p}{p+2}}$, a smaller upper bound.

We would like to remind the reader then, that what was just discussed in this section of this chapter works for p-groups of maximal class of order p^p. Roughly speaking, from the results on p-groups of maximal class mentioned earlier one can say that if a p-group of maximal length has large derived length, then its order is, more or less, equal to p^p, so that the discussion above applies. A little more work would be needed to make this latter statement fully precise, but here we just wanted to discuss the main idea.

V. FROBENIUS GROUPS

One type of permutation group is called a Frobenius group. To define a Frobenius group F, we must first define what it means for a group to be a complement of another and some information about a subgroup and its complement.

Definition 23. Let $N \lhd F$ and $H \subseteq F$. We say that H is a *complement* for N if $NH = F$ and $N \bigcap H = 1$.

Theorem 5.1. Let $N \lhd F$ be a normal subgroup of F and H be a complement for N in F. Then the following are equivalent:

1. The conjugation action of H on N is Frobenius.

2. $H \bigcap H^f = 1$, for all elements $f \in F \setminus H$.

3. $\mathbf{C}_F(h) \subseteq H$, for all $1 \neq h \in H$.

4. $\mathbf{C}_F(n) \subseteq N$, for all $1 \neq n \in N$.

Note that if H acts on N, then the action is said to be *Frobenius* if for all $1 \neq h \in H$ and $n \in N$, then $n \cdot h \neq h$, under the conjugation action.

The reader can find proof of Theorem 5.1 in [10], Chapter 6 Section A Theorem 6.4. Now let us define a Frobenius group.

Definition 24. Let H, N be groups such that H acts on via automorphisms N, denoted as $(\cdot)$. We say that G is the *semidirect product* of N by H, denoted as $F = N \rtimes H$. Such that if $n_0 \in N$ and $h_0 \in H$, then for all $n \in N$ and $h \in H$

$$(n_0, h_0)(n, h) = (n_0 n \cdot {h_0}^{-1}), h_0 h).$$

From this definition, F is Frobenius group if the action in the semidirect product is Frobenius. Although this is a definition of a Frobenius group, we can also say that F is a Frobenius group in the following way.

Definition 25. Let F be a finite group. We say that F is a *Frobenius* group if there exists a normal subgroup $N \lhd F$ and subgroup $H \subseteq F$, such that H is a complement for N where the information in Theorem 5.1 is true.

Parameter e for an Arbitrary Frobenius Group

Now, we will look at the parameter e of our Frobenius group. Let us denote the parameter as e_F for this specific type of group.

Before we can discuss, e_F, we need the following theorem.

Theorem 5.2. Let $H, K \subseteq G$ be subgroups of G. Then

$$|HK| = \frac{|H||K|}{|H \bigcap K|}.$$

Proof. Let $\Omega = \{Hx \mid x \in G$ and K act on Ω by right multiplication. Notice,

$$HK = \bigcup_{k \in K} Hk.$$

Since $Hk = H \cdot k$, then HK must be in the in the orbit $\mathcal{O}$ that contains H. In other words, $\mathcal{O} = \{Hk \mid k \in K\}$. Now, since each coset in $\mathcal{O}$ is disjoint, then they all have size $|H|$. So we can see that $|HK| = |H||\mathcal{O}|$. Note that the stabilizer of H is $H \bigcap K$. Now, by Theorem 1.1 (Fundamental Counting Principle), we can see that

$$|HK| = \frac{|H||K|}{|H \bigcap K|},$$

as desired.

□

Let us fix an arbitrary $n \in N$ and $h \in H$.

Now, since from Theorem 5.1 part (3), we see that $\mathbf{C}_F(h) \subseteq H$, then $|\mathbf{C}_F(h)| \leq |H|$. Since $F = NH$ and $N \cap H = 1$, then from Theorem 5.2, we can see that $|F| = |N||H|$. So,

$$|N| = \frac{|F|}{|H|}$$

and

$$|H| = \frac{|F|}{|N|}.$$

Thus, it can be see that

$$|k_F(h)| = \frac{|F|}{|\mathbf{C}_F(h)|} \geq \frac{|F|}{|H|} = |N|.$$

Similar steps can be made for $\mathbf{C}_F(n)$ to show

$$|k_F(n)| = \frac{|F|}{|\mathbf{C}_F(n)|} \geq \frac{|F|}{|N|} = |H|.$$

Also, since $N \triangleleft F$, then it must be that $k_F(n) \subseteq N$. So, $|k_F(n)| \leq |N|$. From these inequalities, we can deduce that $|k_F(n)| \leq |k_F(h)|$. Thus, if we are trying to find our e_F, we only need to look at the elements in H, as they will produce the largest conjugacy class and smallest centralizer. So, we shall write $e_F = (C_F - 1)\sqrt{k_F}$, where C_F and k_F are the sizes of the smallest centralizer and largest conjugacy class, respectively, in H.

Because the elements of Frobenius groups differ between groups, we cannot go further in specifying what the value of e_F will be. So, in this next section we will look at multiple examples of Frobenius groups.

Examples of Frobenius Groups and their Respective Parameter e

The Frobenius groups we will be looking at are taken from Perumal's thesis [14]. First, let us look at the dihedral group of order $2n$, where n is an odd integer.

We would first like to remind the reader that the dihedral group of order $2n$, denoted D_{2n}, is the group made up of rotations and turns on some geometric shape. For all $n \in \mathbb{N}$, we can write $D_{2n} = \{r^l t^k | 0 \leq l \leq 2 \text{ and } 0 \leq k \leq n\}$, where r is a rotation and t is a turn. Also, we would like to remind the reader that $r^2 = t^n = 1$.

Perumal, shows that the Frobenius complement of the Frobenius group D_{2n} is $H = \{1, r\}$. Now from this, we can see that $k_{D_{2n}}(1) = \{1\}$. So, we are interested in the size of $k_{D_{2n}}(r)$. Thus, we shall show all types of conjugacy classes of D_{2n}.

Theorem 5.3. Let D_{2n} be the dihedral group of order $2n$, where n is odd. Then the conjugacy classes are $\{1\}$, $\{t^k, t^{-k}\}$ for all $1 \leq k < n$, and $\{rt^k | 1 \leq k \leq n\}$.

Proof. Clearly 1 is in a conjugacy class of its own. Now, let $t^k \in D_{2n}$, for some $k \in \{1, \cdots, n\}$. Note, that we only need to check the conjugate action of rt^l on t^k, for some $l \in \{1, \cdots, n-1\}$, since $r^2 = 1$. Which means that $t^{-1} t^k t^l = t^k$. So,

$$(rt^l)^{-1} t^k (rt^l) = t^{-l} r t^k r t^l = t^{-l} t^{-k} t^l = t^{-l+(-k)+l} = t^{-k},$$

for some $l \in \{1, \cdots, n-1\}$. Thus, $\{t^k, t^{-k}\}$ is a conjugacy class for all $1 \leq k < n$.

Now we shall look at the conjugacy class of r. So,

$$(rt^l)^{-1} r (rt^l) = t^{-l} r r r t^l = t^{-l} r t^l.$$

Now, since $rt^{-k} r = t^k$, then

$$rt^{-k} r t^k = t^{2k} t^{-k} r t^k = rt^{2k}.$$

So,

$$t^{-l}rt^{l} = rt^{2l},$$

for all $l \in \{1, \cdots, n\}$. Now, since we l is arbitrary, we can generate the conjugacy class $\{rt^k | 1 \leq k \leq n\}$.

Notice, that since n is odd, then $n = 2m + 1$. Now, then the total size of each conjugacy class should equal the group order. Then,

$$|\{1\}| + |\{b, b^{-1}\}| + \cdots + |\{b^m, b^{-m}\}| + |\{rt^k | 1 \leq k \leq n\}|$$

$$= 1 + 2 + \cdots + 2 + n = 2n$$

Thus, we have found all conjugacy class of D_{2n}, where n is odd.

□

So, from this, we can see that

$$e_{D_{2n}} = (2-1)\sqrt{n} = \sqrt{n}$$

Now, since $|D_{2n}| = 2n$, then $|D_{2n}| = 2e^2_{D_{2n}}$.

Definition 26. Let G be a group and p be a prime. A *Sylow p-subgroup* of G is a subgroup, S, such that $|S| = p^a$, where a is the largest integer such that $|G| = p^a m$, for some $m \in \mathbb{N}$ not divisible by p. We denote the set of all Sylow p-subgroups of G as $\mathrm{Syl}_p(G)$.

Another example we see of a Frobenius group from Perumal [14] is a nonabelian group G of order pq, where p and q are primes with $p > q > 2$, such that the Sylow p-subgroup $P \triangleleft G$ is normal in G and the Sylow q-subgroup Q is not normal in G. Now, we shall present a theorem, its proof can be found in [14].

Theorem 5.4. Suppose that G is Frobenius with complement H. Then, if $P \in$

$\mathrm{Syl}_p(H)$, then

1. if $p = 2$, then P is cyclic or generalized quaternion.

2. if $p \neq 2$, then P is cyclic.

Notice that Q is the Frobenius complement in G. Now, since Q is its own Sylow q-subgroup, then Q is cyclic. Since Q is cyclic. Then Q is abelian. So, we can say that $|\mathbf{C}_G(x)| \geq |Q|$, for all $x \in Q$. This also implies that $|k_G(x)| \leq |P|$, for all $x \in Q$. Since G is Frobenius, then we know that $C_G = |Q|$ and $k_G = |P|$. So,

$$e_G = (|Q| - 1)\sqrt{|P|} = (q-1)\sqrt{p}.$$

Now, we can also see that

$$e_G^2 = (q-1)^2 p.$$

So, $|G| \leq e_G^2$.

Recall that $\mathrm{SL}(n,q)$ is the normal subgroup of $\mathrm{GL}(n,q)$, where each element has determinant of 1. Now, we will look at the example in [14] $29^2 \rtimes \mathrm{SL}(2,5)$, where 29^2 is a group of order 29^2. We shall denote this group as G.

From Perumal, we can see that the size of this group is $29^2 \cdot 120$, the largest conjugacy class is of size $29^2 \cdot 30$, and its respective centralizer is of size 4. So,

$$e_G = (4-1)\sqrt{29^2 \cdot 30} = 87\sqrt{30}.$$

Thus, we can see $e_G^2 = (87^2)(30)$. So, $|G| \leq e_G^2$.

VI. SOLVABLE DOUBLY TRANSITIVE PERMUTATION GROUPS

It is known that in the 1950s, Betram Huppert classified all of the solvable doubly transitive permutation groups. We will be looking at a theorem prior to Huppert's discussed in [13]. Before we show the theorem, we would first like to discuss some essential definitions.

First we would like the reader to recall the meaning of solvable, k-transitivity, where $k = 2$ (doubly transitive), and the group $\mathrm{GL}(n, q)$ of $n \times n$ matrices over a field F of order q. Note that F can also be called a Galois field, denoted $\mathrm{GF}(q)$.

Let V be a vector space of dimension n over the field F of order q. Then, V is a field of degree q^n. Also, let H be the multiplicative group of V. This group is also known as V^*. Now, let H act on V by multiplication. Let us define $\varphi : V \to V$ such that $\varphi(v) = v^q$. Now, we shall let the group generated by $\langle\varphi\rangle$ act on the semi-direct product of $V \rtimes H$. Thus, the group known as the semi-linear group $\Gamma(q^n) = (V \rtimes H) \rtimes \langle\varphi\rangle$.

Lastly, we shall define the fitting subgroup. We say that the *fitting subgroup* of G is the largest normal nilpotent subgroup of G, denoted $\mathbf{F}(G)$. From this we can derive a series of subgroups

$$F_1(G) \leq F_2(G) \leq \dots$$

such that $\mathbf{F}(G) = F_1(G)$ and $F_{i+1}/F_i = \mathbf{F}(G/F_i(G))$.

We now present the theorem in [13], chapter 2 section 6, without proof.

Theorem 6.1. Let V be a vector space of dimension n over $\mathrm{GF}(q)$, where q is a prime power. Suppose that $G \leq \mathrm{GL}(V)$ be a solvable subgroup that is transitive on V^*. Then $G \leq \Gamma(q^n)$, or one of the following occurs:

1. $q^n = 3^4$, $\mathbf{F}(G)$ is extra-special of order 2^5, $|F_2(G)/\mathbf{F}(G)| = 5$ and $G/F_2(G) \leq$

$\mathbb{Z}_4$.

2. $q^n = 3^2,\ 5^2,\ 7^2,\ 11^2$, or 23^2. Here $\mathbf{F}(G) = QT$, where $T = \mathbf{Z}(G) \le \mathbf{Z}(\mathrm{GL}(V))$ is cyclic, $Q_8 \cong Q \lhd G$, $T \bigcap Q = \mathbf{Z}(Q)$ and $Q/\mathbf{Z}(Q) \cong \mathbf{F}(G)/T$ is a faithful irreducible $G/\mathbf{F}(G)$-module. We also have one of the following entries:

q^n	$\|T\|$	$G/\mathbf{F}(G)$
3^2	2	$\mathbb{Z}_3$ or S_3
5^2	2 or 4	$\mathbb{Z}_3$
5^2	4	S_3
7^2	2 or 6	S_3
11^2	10	$\mathbb{Z}_3$ or S_3
23^2	22	S_3

We would like to note that the G in Theorem 6.1 is not doubly transitive. Instead it is a solvable transitive subgroup of the general linear group of dimension n over a field of order q. In order to obtain our solvable doubly transitive permutation group, we must take the semi-direct product of our found group and its respective vector space V of size q^n. More about this can be found in [13] at the beginning of chapter 2 section 6.

Parameter e for Solvable Doubly Transitive Permutation Groups

To find the parameter e for each of the groups classified in Theorem 6.1 and the solvable doubly transitive groups, we used the computing system GAP. We found that we were able to compute all of the needed information for each of the values for q^n in (2) of Theorem 6.1 except for when $q^n = 23^2$ as their were too many subgroups of $\mathrm{GL}(2, 23)$ than GAP's memory could handle. We leave the code we used in Appendix B.

First, we shall discuss the parameter e in respect to (1) of Theorem 6.1.

Now, since $G/F_2(G) \le \mathbb{Z}_4$, then there are three possible choices for G, that is $G/F_2(G) \cong \langle 1 \rangle$, $G/F_2(G) \cong \mathbb{Z}_2$, or $G/F_2(G) \cong \mathbb{Z}_4$. So, let us denote the parameter e as e_{d1}, e_{d2}, e_{d3}, where the subscript pertains to each of the possible quotient groups, respectively. Our choice of subscript will be clear in respect to the doubly transitive groups. We shall show the size of the three possible groups G, its respective parameter, and the square of the parameter.

$$
\begin{array}{lll}
|G| = 160 & e_{d1} = 32 & e_{d1}^2 = 1024 \\
|G| = 320 & e_{d2} = 14\sqrt{(10)} & e_{d2}^2 = 1960 \\
|G| = 640 & e_{d3} = 28\sqrt{(5)} & e_{d3}^2 = 3920
\end{array}
$$

The three possible solvable doubly transitive groups G are also known as Bucht groups, denoted B_1, B_2, and B_3 respectively. More about Bucht groups can be found in [8], pages 385 and 386. So, let us denote the parameter e as e_1, e_2, e_3, where the subscript pertains to each Bucht group, respectively. So,

$$
\begin{array}{lll}
|B_1| = 12960 & e_1 = 324 & e_1^2 = 104976 \\
|B_2| = 25920 & e_2 = 126\sqrt{(10)} & e_2^2 = 158760 \\
|B_3| = 51840 & e_3 = 42\sqrt{(190)} & e_3^2 = 335160
\end{array}
$$

We shall look at the groups obtained in (2) of Theorem 6.1 and their respective parameter and its square. Since there are different values for q^n, the order of T, and what the group $G/\mathbf{F}(G)$ being isomorphic to, we shall denote our parameter as e_G. Here the first will pertain to the case where $q^n = 3^2$, $|T| = 2$, and $G/\mathbf{F}(G) \cong \mathbb{Z}$ and the second will pertain to the case where $q^n = 3^2$, $|T| = 2$, and $G/\mathbf{F}(G) \cong S_3$, continuing in this fashion. We present the size of each group and each parameter and its square below.

$$|G| = 24 \quad e_G = 3\sqrt(6) \quad e_G^2 = 54$$

$$|G| = 48 \quad e_G = 6\sqrt(3) \quad e_G^2 = 108$$

$$|G| = 24 \quad e_G = 3\sqrt(6) \quad e_G^2 = 54$$

$$|G| = 48 \quad e_G = 7\sqrt(6) \quad e_G^2 = 294$$

$$|G| = 96 \quad e_G = 14\sqrt(3) \quad e_G^2 = 588$$

$$|G| = 48 \quad e_G = 6\sqrt(3) \quad e_G^2 = 108$$

$$|G| = 144 \quad e_G = 22\sqrt(3) \quad e_G^2 = 1452$$

$$|G| = 120 \quad e_G = 19\sqrt(6) \quad e_G^2 = 2166$$

$$|G| = 240 \quad e_G = 38\sqrt(3) \quad e_G^2 = 4332$$

The size of the solvable doubly transitive groups, each of the parameters for their respective groups, and the parameter squared shall now be given. We shall use the same notation, e_G, but please note that these are not the same groups.

$$|G| = 216 \quad e_G = 9\sqrt(6) \quad e_G^2 = 486$$

$$|G| = 432 \quad e_G = 30\sqrt(2) \quad e_G^2 = 1800$$

$$|G| = 600 \quad e_G = 20\sqrt(6) \quad e_G^2 = 2400$$

$$|G| = 1200 \quad e_G = 35\sqrt(6) \quad e_G^2 = 7350$$

$$|G| = 2400 \quad e_G = 70\sqrt(3) \quad e_G^2 = 14700$$

$$|G| = 2352 \quad e_G = 42\sqrt(3) \quad e_G^2 = 5292$$

$$|G| = 7056 \quad e_G = 154\sqrt(3) \quad e_G^2 = 71148$$

$$|G| = 14520 \quad e_G = 209\sqrt(6) \quad e_G^2 = 262086$$

$$|G| = 29040 \quad e_G = 418\sqrt(3) \quad e_G^2 = 524172$$

In each one of these cases, we can see that $|G| \leq e_G^2$. Because of the large difference between most of the order of our found groups G and their parameter squared e_G^2, there may exist a universal constant B, such that $|G| \leq Be_G$ for all found solvable transitive permutation groups in (1) and (2) of Theorem 6.1, including their respective solvable doulby transitive permutation groups.

Now, we shall look at the subgroups G of $\Gamma(q^n)$. In [13], they have many theorems that help us find subgroups of the semi-linear group. In our case, we only needed the following.

Theorem 6.2. Let G be a solvable irreducible subgroup of $\mathrm{GL}(p,q)$ for primes p and q.

1. If $q = 2$, then $G \leq \Gamma(2^p)$.

2. If $q = p$, then $G \leq \Gamma(p^p)$ or $G \leq \mathbb{Z}_{p-1}\mathrm{wr}S$, where $\mathbb{Z}_p \leq S \leq \mathbb{Z}_p \cdot \mathbb{Z}_{p-1} \leq S_p$.

Proof of this theorem can be found in [13], chapter 1 section 2.

Theorem 6.3. Let G be a solvable irreducible subgroup of $\mathrm{GL}(pr,2)$ where p and r are primes not necessarily distinct. After possibly inter-changing p and r, one of the following occurs:

1. $G \leq \Gamma(2^p)\mathrm{wr}S$ where $\mathbb{Z}_r \leq S = \mathbb{Z}_r \cdot \mathbb{Z}_{r-1} \leq S_r$,

2. $G \leq \Gamma(2^{pr})$, or

3. $\mathbf{F}(G) = DT$ with $D, T < G$, $T = \mathbf{Z}(\mathbf{F}(G))$ is cyclic, D is extra-special of order p^3, $\mathbf{F}(G)/T \cong D/\mathbf{Z}(D)$ is a faithful irreducible $G/\mathbf{F}(G)$-module of order p^2. Furthermore, $|T| \mid 2^r - 1$ and $p \neq 2$.

Proof of this theorem can be found in [13], Chapter 1 Section 2.

With these theorems, we are able to find some semi-linear groups using GAP then find its respective parameter e. With the capabilities of GAP, the values for q and p we could compute are the following: 2^2, 2^3, 2^4, 3^3, 2^5, and 2^6. When presenting our information, we shall present in the order of value of q^n.

First, we found the parameter e for these subgroups then found the parameter e for their respective solvable doubly transitive permutation groups. We shall denote our parameter in both instances as e_G.

We obtained the following information.

$$|G| = 6 \qquad e_G = \sqrt(3) \qquad e_G^2 = 3$$
$$|G| = 21 \qquad e_G = 2\sqrt(7) \qquad e_G^2 = 28$$
$$|G| = 60 \qquad e_G = 3\sqrt(15) \qquad e_G^2 = 135$$
$$|G| = 78 \qquad e_G = 5\sqrt(13) \qquad e_G^2 = 325$$
$$|G| = 155 \qquad e_G = 4\sqrt(31) \qquad e_G^2 = 496$$
$$|G| = 378 \qquad e_G = 15\sqrt(7) \qquad e_G^2 = 1575$$

Here, one can notice that we are unable to lower our bound of $2e_G^2$ to e_G^2, since in the case where $q^n = 2^2$ our group G has order equal to $2e_G^2$. Now we present the solvable doubly transitive permutation group parameters in the same order.

$$|G| = 24 \qquad e_G = 4\sqrt(2) \qquad e_G^2 = 32$$
$$|G| = 168 \qquad e_G = 10\sqrt(7) \qquad e_G^2 = 700$$
$$|G| = 960 \qquad e_G = 20\sqrt(10) \qquad e_G^2 = 4000$$
$$|G| = 2106 \qquad e_G = 15\sqrt(39) \qquad e_G^2 = 8775$$
$$|G| = 4960 \qquad e_G = 32\sqrt(31) \qquad e_G^2 = 31744$$
$$|G| = 24192 \qquad e_G = 64\sqrt(42) \qquad e_G^2 = 172032$$

From these groups, we can see that we are able to lower our upper bound from $2e_G^2$ to e_G^2. Thus we can conclude that $|G| \leq e_G^2$, except for when $q^n = 2^2$. So, we are unable to generalize and improve our upper bound to e_G^2. We would like to note that each of these found groups were in the case when $G = \Gamma(q^n)$. This is because of the code we used for GAP, we were unable to find groups G that were proper subgroups of $\Gamma(q^n)$.

The code we used to find all of the subgroups G mentioned in [13], the solvable doubly transitive permutation groups from Huppert, and their respective parameter e's can be found in the Appendix A of this thesis.

VII. OPEN PROBLEMS

Throughout this thesis, we were unable to fully explore many different aspects of the groups we were studying. So, we leave here a list of open problems for those interesting in studying to attempt to answer.

- Finding the largest conjugacy class for the alternating group, A_n, for all $n \in \mathbb{N}$.

- Determining if the bound of the order of the alternating groups. for values of n not tested here ($20 < n < 40$ and for all $n > 40$), using Harrison's parameter.

- Proving or disproving that if P is a p-group of maximal class with large derived length, then the bound on the group's order using Harrison's parameter can be further improved to $|P| \leq (2e_P^2)^{\frac{p}{p+2}}$.

- Finding the parameter e for the solvable doubly transitive permutation groups and solvable transitive permutation groups when $q^n = 23^2$ in (2) of Theorem 6.1.

- Finding the parameter e for the solvable doubly transitive permutation groups and solvable transitive permutation groups for any $q^n \neq 2^2, 2^3, 2^4, 3^3, 2^5$, or 2^6 when $G \leq \Gamma(q^n)$.

- Finding the parameter e for the solvable doubly transitive permutation groups and solvable transitive permutation groups when $q^n = 2^2, 2^3, 2^4, 3^3, 2^5$, or 2^6 and $G < \Gamma(q^n)$.

- Finding if there exists a universal constant B, such that $|G| \leq Be_G$, for all G from (1) and (2) of Theorem 6.1

- Finding the general bound for solvable doubly transitive permutation groups and solvable transitive permutation groups.

APPENDIX SECTION

APPENDIX A: In this section we shall present the various codes used to find the largest conjugacy classes of the permutation groups we observed. And the code used to find the largest four conjugacy classes of S_n. We would like to note to the reader that text written within %% %% is not part of the code, but is an explanation of prior line of code.

We shall first present the main code used to find the largest conjugacy class of a group.

```
c := ConjugacyClasses(G);
nc := NrConjugacyClasses(G);
m := [];
for i in [1..nc] do
    m[i] := Size(c[i]);
od;
m;
```

We would like to note that the groups we dealt with were usually small enough for us to check manually which was the largest conjugacy class. This was not the case when dealing with A_n and S_n. So, we will append the extra bit of code needed to find the largest conjugacy class that was used when working with A_n and S_n.

```
k := 2;
j := 2;
repeat
    j := j + 1;
    if m[j] > m[k]
        then k := j;
```

```
        else k := k;
    fi;
until j > nr - 1;
k;
c[k];
```

Now we will show the code used to find the largest four conjugacy classes of S_n. This code is similar to the process of finding the largest conjugacy class in A_n.

```
k := 2;
j := 2;
repeat
    j := j + 1;
    if m[j] > m[k]
        then k := j;
        else k := k;
    fi;
until j > nr - (p + 1);
k;
c[k];
Remove(m,k);
```

We would like to make note that the final loop process is repeated until the user decides to stop. The p represents the number of elements removed from m prior to computing current loop. In our case, we would repeat this process until we obtained the desired cycle type of S_n. Recall that this cycle type was $(n-2)(2)$ for an even n and $(n-3)(2)$ for an odd n. While repeating this process, we would keep track of what cycle types we would be eliminating from l, which would help confirm our conjecture on what the four largest conjugacy classes are in S_n.

Now we shall present to code to find the subgroup G from Theorem 6.1 (1). Note, to do this for (1) we had to find the subgroup G of $\Gamma(3^4)$ that met the requirements presented in (1).

```
ni := NumberIrreducibleSolvableGroups(4,3);
l := [];
for i in [1..ni] do
    l[i] := IrreducibleSolvableGroupMS(4,3,i);
od;
k := [];
j := 0;
for i in [1..ni] do
    if Size(FittingSubgroup(l[i])) = 32 then
        j := j + 1;
    fi;
    if Size(FittingSubgroup(l[i])) = 32 then
        k[j] := l[i];
    fi;
od;
t := [];
for i in [1..j] do
    t[i] := FittingSubgroup(FactorGroup(k[i],
    FittingSubgroup(k[i])));
od;
y := [];
r := 0;
for i in [1..j] do
    if Size(t[i]) = 5 then
```

```
        r := r + 1;
    fi;
    if Size(t[i]) = 5 then
        y[r] := k[i];
    fi;
od;
```

After obtaining the three subgroups, we applied the code to find the largest conjugacy class to each.

Now, we shall present the code used to find the subgroups from Theorem 6.1 (2). Here, we checked for the subgroups that met the requirements of having the correct size for the group and its Fitting subgroup.

```
x := GL(n,q);
as := AllSubgroups(x);
ng := Size(as);
i := 2;
p := 0;
j := 0;
k := [];
repeat
    if Size(as[i]) = |G| then
        p := i;
    fi;
    if Size(as[i]) = |G| then
        j := j + 1;
    fi;
    if Size(as[i]) = |G| then
        k[j] := as[i];
```

```
    fi;
    i := i + 1;
until i > ng - 1;
l := [ ];
for i in [1..j] do
l[i] := Size(FittingSubgroup(as[p-j+i]));
od;
```

Now, we shall present the code used to find the various subgroups of $\Gamma(q^n)$ for the values of q and n we had chosen.

```
ni := NumberIrreducibleSolvableGroups(n,q);
irr := [];
for i in [1..ni] do
    irr[i] := IrreducibleSolvableGroupMS(n,q,i);
od;
l := [];
k := [];
j := 0;
for i in [1..ni] do
    k[i] := Size(irr[i]);
od;
```

With these codes and found subgroups, we will not present the code used to create the solvable doubly transitive permutation groups classified by Huppert.

```
g := SemidirectProduct(h,n);
N := Image(Embedding(g,2));;
Nelm := Elements(N);;
H := Image(Embedding(g,1));;
```

```
act1 := Action(H, Nelm, OnPoints);
act2 := Action(N, Nelm, OnRight);
G := ClosureGroup(act1,act2);
```

We would like to thank Professor Alexander Hulpke for his help in creating the following code. Without his help, we would have struggled finding out how to produce the desired groups.

REFERENCES

[1] J.H. Conway, S.P. Norton, R.A. Wilson, and R.A. Parker. *ATLAS of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups.* New York : Oxford University Press, 1985.

[2] J.D. Dixon and B. Mortimer. *Permutation Groups.* New York : Springer-Verlag New York, 1996.

[3] D.S. Dummit and R.M. Foote. *Abstract Algebra, 3rd edition.* New Jersey : John Wiley and Sons, Inc., 2004.

[4] C. Durfee and S. Jensen. A bound on the order of a group having a large character degree. *Journal of Algebra*, 338:197–206, 2011.

[5] G.A. Fernández-Alcober. An introduction to finite p-groups: regular p-groups and groups of maximal class. *Mathemática Contemporânea*, 20:155–226, 2001.

[6] A. Harrison. Bounding the order of a group with a large conjugacy class. Master's thesis, Texas State University, San Marcos, TX, 2013.

[7] A. Harrison. Bounding the order of a group with a large conjugacy class. *Journal of Group Theory*, 18:201–207, 2015.

[8] B. Huppert. *Character Theory of Finite Groups.* Berlin ; New York : de Gruyter, 1998.

[9] I.M. Isaacs. *Algebra: A Graduate Course.* Providence, Rhode Island : American Mathematical Society, 1994.

[10] I.M. Isaacs. *Finite Group Theory.* Providence, Rhode Island : American Mathematical Society, 2008.

[11] I.M. Isaacs. Bounding the order of a group with a large character degree. *Journal of Algebra*, 348:264–275, 2011.

[12] C.R. Leedham-Green and S. McKay. *The Structure of Groups of Prime Power Order.* Oxford, New York : Oxford University Press, 2002.

[13] O. Manz and T.R. Wolf. *Representations of Solvable Groups.* Cambridge : Cambridge University Press, 1993.

[14] P. Perumal. On the theory of the frobenius groups. Master's thesis, University of Kwa-Zulu Natal, Pietermaritzburg, 2012.

[15] W.R. Scott. *Group Theory.* Englewood Cliffs, N.J. : Prentice-Hall, 1964.

[16] N. Snyder. Groups with a large character degree. *Proceedings of the American Mathematical Society*, 136(6):1893–1903, 2008.