Idle Words:
Word Maps on Finite Groups

By

William Cocke

A dissertation submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN – MADISON

2019

Date of final oral examination: April 4, 2019

The dissertation is approved by the following members of the Final Oral Committee:

Professor N. Boston, Professor, Mathematics and ECE

Professor M. Matchett Wood, Professor, Mathematics

Professor T. Dymarz, Associate Professor, Mathematics

LTC Scott Cheney, Professor, Military Science

Abstract

In this dissertation, we present a number of results in the broad theory of word maps on groups. Many of these results were done with a variety of coauthors. Using ideas motivated by group theory we show how the structure of word maps on a group can be used to obtain bounds on the order of the group. These bounds include statements about the number of not-powers in a finite group and the number of not solutions to a word map.

In addition, we present an algorithm and results about conditions that determine when a group is chiral. We also present the smallest chiral groups and give a family of chiral groups. Using the concept of weakly chiral as defined by Gordeev et. al., we present a weakly chiral group that is not chiral. Moreover, we give a witness to the chirality of the Mathieu group of order 7920.

We show how the probability distributions induced by word maps can be used to verify the nilpotency of a finite group: a finite group is nilpotent if every surjective word map is uniform. We also provide a few other novel characterizations of nilpotency for finite groups.

For a fixed group, we present new bounds for the number of distinct word maps over the group and show that these bounds are tight for infinitely many groups. We then expand upon a theorem of Lubotsky dealing with the images of word maps in finite simple groups. Finally, we briefly touch upon the connection between word maps and character theory.

Acknowledgements

The present dissertation is the result of a finite number of hours spent by the author studying finite things. I have family, friends, and colleagues to whom I am deeply indebted. First and foremost, I owe a debt of eternal gratitude to my wife and best friend: Thank you Em for supporting me through these five crazy years. I would also be remiss if I did not thank the many small simians that have provided me with inspiration, entertainment, and boundless motivation: Thank you Maximus, Minnie, Pius, Constance, Primus, etc.

The job of a mathematician is not to produce mathematics, but to communicate mathematics. Equivalently, the job of a mathematician is to produce mathematical communication. Communication requires a sender and a receiver. The goal of a mathematician is to send a reliable message that enlightens the receiver. To that end, I believe that good mathematics is produced in communities. I wish to thank those who have helped me find my place within the mathematical community. I thank my advisers Nigel Boston and I. Martin Isaacs. I am very lucky to have found a community of collaborators throughout my mathematical career. Thank you to Steve Goldstein, Turbo Ho Meng-Che, I. Martin Isaacs, Sara Jensen, Sandro Mattarei, Dane Skabelund, Michael Stemper, and Geetha Venkataraman. Of course the graduate students at Wisconsin and previously at BYU are an integral part of my community.

My committee members are owed a debt of gratitude for giving feedback and guidance on the dissertation and future directions. Thank you to Tulia Dymarz, Melanie Matchett Wood, and Scott Cheney.

The Army ROTC program at UW-Madison, the Army Cyber Institute, and the Department of Mathematics at West Point have all proven supportive of my scholarly pursuits. While the organizations as a whole deserve my thanks, I would like to individually thank Paul Goethals and Christopher Hartley for their support.

For enlarging my scholarly community I would like to give a special thanks to the Center for South Asia for providing programming, awards, and fellowships throughout my studies. Special thanks to Tonia Mahnke and Lalita du Perron for their work with the Center.

Eritis sicut Deus, scientes bonum et malum

List of Tables

Contents

Chapter 1

Introduction.

1.1 Introduction.

The title of this dissertation is "Idle Words: Word Maps on Finite Groups". We will assume that the reader is familiar with the concept of a group, but perhaps unfamiliar with the study of word maps on groups. The present chapter provides an overview of the author's work in the area. The theorems presented have been chosen to convey not only the breadth, but some of the depth of the theory. Within this chapter we will only state the theorems, but proofs of all main results appear in the later chapters. The theorems presented were all proven by the author, many times with various coauthors. The original works containing the results are cited whenever applicable, although many of the results are still in preparation; if however, the result includes a coauthor, then a citation is given to acknowledge the collaborative effort. The other references are from a variety of authors in the area of word maps. Currently, the study of word maps continues to incorporate new areas of mathematics, so much so that many of the authors of the works cited would be surprised to find their work included in a dissertation on word maps. We hope the present work helps to enlarge the community of researchers engaged in the study of word maps.

A word w is an element of the free group $\mathbf{F}_n\langle x_1, \ldots, x_n\rangle$. We will say that w is an

n-variable word, even when all of the x_i do not appear in w [95]. The word w can also be described in the following way, let $\Sigma = \{x_1, \ldots, x_n\}$. We call Σ an alphabet. Words over Σ consist of strings of elements of Σ together with their inverses [12]. We note that there is a possibility of confusion regarding the potential difference between the words x_1 and $x_1 x_1^{-1} x_1$. One can restrict to studying only reduced words, but because we are ultimately interested in the maps corresponding to the words, such semantic differences are of no consequence. The author's favorite way to define a word w is that w occurs as an element of the algebra of terms in the language $\mathcal{L} = \{1, *, ^{-1}\}$, the language of groups. An n-variable word occurs as an element in the algebra of terms restricted to only using n variables [66].

Given a group G, not necessarily finite, and a word $w \in \mathbf{F}_n$, there is a map, which by abuse of notation we write as w from G^n to G defined by:

$$w : (g_1, \ldots, g_n) \longrightarrow w(g_1, \ldots, g_n).$$

That is $w(g_1, \ldots, g_n)$ is the evaluation of w replacing $x_1, \ldots, x_n$ with $g_1, \ldots, g_n$. We will write $w(G)$ for the image of w in G. We will **not assume** that $w(G)$ is closed under inverses, in contrast to some other conventions. The reason for this distinction will be made clear in Chapter 5. In general $w(G)$ is not a subgroup of G. For example, there are groups of order 96 such that for the word $w = [x, y] = x^{-1}y^{-1}xy$, the set $w(G)$ is not a group [34].

The first interest in words as maps is attributed to Ore with his observation that every element of an alternating group occurs as a commutator [88]. Ore's original observation led to the Ore conjecture: given a finite nonabelian simple group G and $g \in G$, there are $a, b \in G$ such that $g = [a, b] = a^{-1}b^{-1}ab$, i.e., the image $w(G) = G$ for the word

$w = [x, y]$. The Ore conjecture was recently proven by Liebeck, O'Brien, Shalev, and Tiep; their work utilized the connection between character tables and the image of the commutator map, along with the classification of finite simple groups [67]. Various generalizations of the Ore conjecture have been proven using different words w. Many of these generalizations utilize character theory. We will discuss the connection between words and character tables in Chapter 9.

The author's own interest in word maps began with a question about the number of elements of a finite group G that do not occur as a square in G, i.e., the subset $G \setminus w(G)$ where $w = x^2$. Surprisingly the case for x^2 provides general insight for words of the form x^k. For any positive integer k let $n_k(G)$ be the number of elements of G that are not k-th powers in G, i.e., if $w = x^k$, then $n_k(G) = |G| - |w(G)|$; we will also write $\mathcal{N}_k(G)$ for $G \setminus w(G)$. The author, together with Marty Isaacs and Dane Skabelund proved the following theorem [18].

Theorem A. *[18, Theorem B] Let G be a finite group, and write $n = n_k(G)$. If $n > 0$, then $|G| \leq n(n+1)$ and in fact $|G| \leq n^2$, except in the case where G is a Frobenius group with kernel of order $n+1$ and $\mathcal{N}_k(G)$ is the set of nonidentity elements of the Frobenius kernel.*

Surprisingly the bound in Theorem A is entirely independent of k. A slightly looser bound was given previously by Bannai et al. [4] and by Lévai and Pyber [64]. More recently, Lucido and Pournaki [70, 71] investigated the proportion of elements of G that are squares, and provided another proof that $n_2(G) \geq \lfloor \sqrt{G} \rfloor$. Moreover, the finiteness in Theorem A can be relaxed to other finite-like conditions. For example, if the group G is residually finite and the number of not k-th powers in G is a positive integer, then

G is actually finite. However, independent constructions of Pálfy and Ivanov produce an infinite group with exactly $p-1$ not p-th powers [51]. In Chapter 3 we will prove Theorem A and some interesting results about the sequence of not powers of a group. We next turn to related questions about the word w as a map from G^n to G.

For any word the size of $w(G)$ does not bound the order of G, but for words of the form $w = x^k$, we have that $|G \setminus w(G)|$ can bound the size of G. A "dual" question of sorts relates

$$|\{(g_1, \ldots, g_n) \in G^n : w(g_1, \ldots, g_n) \neq 1\}|$$

and $|G|$. The author and Sara Jensen showed the following. [19].

Theorem B. *[19, Theorem A] Let G be a group, and let w be a word. Let*

$$k = |\{(g_1, \ldots, g_n) : w(g_1, \ldots, g_n) \neq 1\}|.$$

If $k > 0$, then $|G| \leq 2k^2$. Moreover, if $n > 1$, then $|G| \leq k^2$. In particular if k is finite, then G is finite.

As before, the bound in Theorem B is sharp. Moreover, unlike Theorem A the bound in Theorem B holds for all groups G. Along with the proof of Theorem B, Chapter 4 will contain a discussion about the differences between Theorem A and Theorem B; namely why does one bound require some finiteness property while the other does not. Regardless, both theorems are related by the following idea. Choose any property $\mathcal{P}$ of a group element x that somehow "propagates" through the centralizer of x. Then the number of elements of G that satisfy property $\mathcal{P}$ can be used to bound the order of a group G. As another example, we will mention the work of the author and Geetha Venkataraman wherein we show that the number of elements of maximal order in a group can be used to bound the order of the group [21].

Motivated by the connection between word maps and first-order properties of a group, the author asked the following vague question: "In what ways can a group distinguish between g and g^{-1}?" While inversion is not in general an automorphism of a group G, is it the case that there could be an "orientation" to the set $\{g, g^{-1}\}$ for a given group G and $g \in G$? In particular, the author and "Turbo" Ho Meng-che defined the following property.

Definition 1.1. A group G is **chiral** is there is a word w and an element $g \in G$ such that $g \in w(G)$ and $g^{-1} \notin w(G)$. We will call (G, w) a chiral pair. If G is not chiral, then we say that G is **achiral**.

We found families of chiral groups. Our main results about chirality include the following two theorems.

Theorem C. *[16, Theorem A] The only chiral groups with order less than 108 are SmallGroups* $(63, 1)$ *and* $(80, 3)$.

Theorem D. *[16, Theorem C] The free nilpotent group of class* ≥ 3 *is chiral and the free nilpotent group of rank 3 and class 2 is achiral.*

Gordeev, Kunyavskiĭ, and Plotkin extend the concept of chiral to weakly chiral in [30]. In Chapter 5 we prove Theorems C and D as well as provide some explicit examples motivated by questions of Gordeev et. al. It should be noted that Ashurst independently formulated some questions about chirality in her dissertation, although she gave no examples of chiral or weakly chiral groups [3].

We will also look at how word maps can be used to define various classes of groups. In general the collection of groups defined by the vanishing of certain words is called a

variety [84]. We want to examine some other ways that word maps can characterize a group, in particular how the probability function associated to a word can be used to derive information about the group. Formally, let w be a word. If G is finite then the word map w induces a probability distribution on G where

$$\mu_{w,G}(g) = \frac{|\{(\overline{g} \in G^n : w(\overline{g}) = g\}|}{|G|^n}.$$

Often information about G can be obtained from the function $\mu_{w,G}$, or from the collection of functions $\mu_{w,G}$ as w varies. For example, as a combination of results by Abért [1] and Nikolov and Segal [87], a finite group is solvable if and only if there is some $\epsilon > 0$ so that for all words w we have $\mu_{w,G}(1) \geq \epsilon$.

Restricting to words on 2 variables we have the following. For $w \in \mathbf{F}_2$ and a group G we can define a structure $(G, *_w)$ where G is the set G and $*_w$ is the binary operation $x *_w y = w(x, y)$. In general, we do not expect the structure $(G, *_w)$ to have interesting mathematical properties. However, let $\mathcal{P}$ be the set of all words in $\mathbf{F}_2$ for which the total number of times x and y each appear up to multiplicity is ± 1. For example xy and $x^{-1}yx^2$ are both in $\mathcal{P}$. Then $\mathcal{P}$ can be described using nilpotent groups, i.e., $w \in \mathcal{P}$ if and only if $(G, *_w)$ is a quasigroup for every nilpotent group G. Moreover, we can describe finite nilpotent groups using $\mathcal{P}$ as follows.

Theorem E. *[13, Theorem C] A finite group G is nilpotent if and only if for all w in $\mathcal{P}$ with length less than $4|G|$, we have $\mu_{G,w}(1) = \frac{1}{|G|}$.*

It turns out that the set $\mathcal{P}$ can be defined using nilpotent groups in a similar manner. In our proof of Theorem E we will utilize the following novel result of the author's which has interest independent of the study of word maps.

Theorem F. *[13, Theorem A] Let G be a finite group and p a prime. Then G is not p-nilpotent if and only if there are two elements $g, h \in G$ with $o(g) = o(h) = q^k$ for some prime $q \neq p$ and $o(gh) = p$ or possibly 4 when $p = 2$.*

A generalization of Theorem E appeared in [17] and we include it here.

Theorem G. *[17, Theorem B] Let G be a finite group. Then G is nilpotent if and only if for every surjective word map w, the distribution $\mu_{G,w}$ is uniform.*

Theorems E, F, and G appear in Chapter 6. We also discuss an interesting avenue of research in the broad category of word maps undertaken by Bastos and Shumyatsky regarding the nilpotency of the commutator subgroup [6].

We now turn to consider the collection of all n-variable word maps on a group G. The collection of word maps on n variables on a group G defines a group where

$$(v \cdot w)(g_1, \ldots, g_n) = v(g_1, \ldots, g_n) \cdot w(g_1, \ldots, g_n).$$

We will write the set of all word maps from $G^{(n)}$ to G as $\mathbf{F}_n(G)$. It is not hard to see that $\mathbf{F}_n(G)$ is a group under the action of point-wise multiplication. As noted in [16], for a finite group G, the group $\mathbf{F}_n(G)$ can be explicitly computed.

In their work, Amit and Vishne [2] define $\mathbf{F}_n(G)$ as follows: Let

$$K(G) = \bigcap_{\alpha:\mathbf{F}_n \to G} \ker(\alpha).$$

Then $\mathbf{F}_n(G)$ is the quotient $\mathbf{F}_n/K(G)$. The two formulations of $\mathbf{F}_n(G)$ are equivalent. The group $\mathbf{F}_n(G)$ is also the rank n free group in the variety generated by G [84], and is called the reduced free group on d variables of G.

To familiarize the reader with word maps, we now discuss the example of the two-variable word maps and probability distributions on the quaternion group $G = Q_8$. There are 32 two-variable word maps on G; this means that there are 32 maps

$$f_i : G \times G \mapsto G, \quad i \in \{1, \ldots, 32\}$$

such that for any element $w \in \mathbf{F}_2$, the map

$$w : G \times G \mapsto G,$$

is in $\{f_i : 1 \leq i \leq 32\}$; equivalently, the order of $\mathbf{F}_2(G)$ is 32. The following set of 32 words give the 32 distinct word maps:

$$\{w = x^i y^j [x, y]^k : i, j \in \{1, \ldots, 4\}, k \in \{0, 1\}.\}$$

Any of the word maps f_i can be induced by multiple elements of $\mathbf{F}_2$, i.e., every word determines a word map, but for every word map there are multiple words corresponding to it. Consider, for example, the following two words x^4 and 1 (the empty word). Over any 2-tuple $(g, h) \in G \times G$, these maps evaluate to g^4 and 1. Since G has exponent 4, we conclude that the word maps x^4 and 1 are equal, that is to say that the words induce the same map.

Fix 32 words $w_1, \ldots, w_{32} \in \mathbf{F}_2$ such that the word map of each w_i is f_i. While each w_i induces a unique word map, the probability distributions μ_{G,w_i} are not distinct. In fact there are only 4 distinct probability distributions induced by the w_i. In Table 1, we give the four distributions, $\mu_1, \ldots, \mu_4$ over G, where the μ_i row and the g_j-column intersect to give $\mu_i(g_j)$.

We will now examine certain computational questions regarding word maps in finite groups. Many of the theorems above were motivated by computations. Some of our early

Table 1: The Probability Distributions of Word Maps of Q_8.

	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
μ_1	1/8	1/8	1/8	1/8	1/8	1/8	1/8	1/8
μ_2	1	0	0	0	0	0	0	0
μ_3	5/8	3/8	0	0	0	0	0	0
μ_4	1/4	3/4	0	0	0	0	0	0

computations involving word maps failed simply because the number of word maps for a finite group G, even when G has relatively small order, can be quite large. For example, when G is the group of affine transformations of the field with 5 elements, the order of G is 20, but

$$|\mathbf{F}_2(G)| = 12207031250000.$$

An even more extreme example occurs when G is the alternating group on 5 symbols, i.e., $G = A_5$. We will prove that

$$|\mathbf{F}_2(A_5)| = 47383813383216168960000000000000000000000000.$$

The next few theorems verify these numbers and demonstrate a remarkable bound on $\mathbf{F}_n(G)$.

Theorem H. *Let G be a finite group with exponent e. Let Ω be a set of orbit representatives of the diagonal action of* $\mathrm{Aut}(G)$ *on the set of n-tuples $(g_1, \ldots, g_n)$ of G such that $\langle g_1, \ldots, g_n \rangle$ is not abelian. Then*

$$|\boldsymbol{F}_n(G)| \leq e^n \prod_{(x_1,\ldots,x_n)\in\Omega} |\langle x_1, \ldots, x_n \rangle'|.$$

We will show that the bound in Theorem H is sharp. In particular we have the following theorem.

Theorem I. *Let C_p be the cyclic group of order p, where p is prime. Let $G = C_p \rtimes \mathrm{Aut}(C_p)$ then*

$$|F_2(G)| = (p-1)^2 p^{2+p(p-2)},$$

and

$$F_2(G)' = (C_p)^{p(p-2)}.$$

We can also show via computation that Theorem H is sharp for the group A_5.

Theorem J. *Let $G = A_5$. Then*

$$|\boldsymbol{F}_2(G)| = 30^2 3^3 4^4 5^3 60^{19}$$

and

$$\boldsymbol{F}_2(G)' = (C_3)^3 \times (K_4)^4 \times (C_5)^3 \times (A_5)^{19}$$

As a corollary to Theorem J we see something very interesting about word maps over A_5, namely that for any subset A of A_5 that is closed under automorphisms of A_5 and contains 1, there is a commutator word w with $w(A_5) = A$. Lubotzky showed that for any simple group G and subset A of G closed under automorphisms and containing 1, there is a word w such that $w(G) = A$ [69]. The author and Turbo Ho observed the following improvement.

Theorem K. *[15] Let G be a finite simple group, $n > 1$, and $A \subseteq G$ such that A is closed under automorphisms and $1 \in A$. Assume that $v \in \boldsymbol{F}_n$ is not a law on G. Then there is a word $w \in \langle v(\boldsymbol{F}_n) \rangle$ such that $A = w(G)$.*

While Theorem K is effective, it is not efficient. However, in certain circumstances we can find relatively short words.

We conclude by mentioning some other results connecting word maps and character theory. These results are largely observations that came from a database of finite groups with the same character table. The author together with Steve Goldstein and Michael Stemper constructed the database using a large distributed computing network. The following is included among our results.

Theorem L. *[14] Let w be the word x^2. There are finite groups G and H of order 64 such that G and H have the same character table, but $|w(G)| \neq |w(H)|$.*

It should be noted that in contrast to Theorem L it is well-known that for two groups G and H with the same character table with $w = x^2y^2$ then $|w(G)| = |w(H)|$. This means that for the word $w = x^2$ the character table of G can determine the characteristic subgroup $\langle w(G)\rangle$, but not the subset x^2. Squares here are interesting, in that the character table of a group G cannot determine $\langle w(G)\rangle$ for $w = x^p$ for any prime $p > 2$.

1.2 Outline.

The dissertation is divided into a number of chapters. Most chapters can be read independently of the rest, although Chapters 3 and 4 are best read together. The preliminary results in Chapter 2 will be used throughout the dissertation, but can be referenced if needed. The rest of the dissertation proceeds as follows:

Chapter 2 contains many results that will be utilized throughout the dissertation. This Chapter concludes with a negative answer to a question of Amit and Vishne [2].

Results about the not images of a word map are explored in Chapter 3. Chapter 4 contains the proof of Theorem B, which deals with the number of not solutions to a

word map. At the end of Chapter 4 we discuss the differences between Theorems A and B.

Chapter 5 presents some of the author's work on chirality; in particular the existence of families of chiral groups is noted and Theorems C and D are proved. As Theorem C is based on a computation, the relevant code can be found in Appendix A. Within this chapter, we present a word that witnesses the chirality of the Mathieu group M_{11}. There is also an example of a weakly chiral group, answering a question of Gordeev et. al. [30].

In Chapter 6 we examine some of the author's characterizations of nilpotent groups including Theorems E, F, and G.

Chapter 7 contains work on the free groups in the varieties generated by a finite group and contains proofs of Theorems H, I, and J.

In Chapter 8 we review some of the work done on word maps in finite simple groups and prove Theorem K.

Chapter 9 focuses on the connections between character tables and word maps in finite groups. We prove Theorem L and mention some other observations from our database of small groups with the same character table.

The dissertation concludes in Chapter 10, which includes some open questions and directions for the study of word maps on finite groups.

Chapter 2

The Study of Word Maps.

In general the study of word maps in groups has focused on three areas which we broadly classify as

(1) Results about specific words, e.g., the commutator word $w = [x, y] = x^{-1}y^{-1}xy$.

(2) Results about certain families of groups, e.g., varieties of groups, finite simple groups.

(3) Asymptotic results, e.g., length of laws, diameter of Cayley graphs, growth, etc.

We note that the categories above are not all inclusive, nor are they mutually disjoint. The present dissertation deals primarily with results about abstract words in finite groups. However, many of our results can be placed in one or more of the categories above. We recommend [95] as a general reference for asymptotic results and Shalev [96] for a survey on progress regarding finite simple groups.

The results of this chapter will be used repeated throughout the dissertation. We will first show that all word maps are essentially power maps times some element of the commutator subgroup.

Lemma 2.1. *Let $w \in \boldsymbol{F}_n$. Then for some integers $e_1, \ldots, e_n$ and a suitably chosen $c \in \boldsymbol{F}_n'$ we can write*

$$w = x_1^{e_1} \ldots x_n^{e_n} \cdot c.$$

Proof. Similar to the proof of Dietzmann's theorem in Isaacs [48, Theorem 5.10] we will collect copies of x_1 towards the front of w. Suppose that $w = ux_1v$ for some words u and v where we assume that x_1 only appears in u as part of a commutator. Then

$$w = xuu^{-1}x^{-1}uvx = xu[u, x]v.$$

Iterating this processes we can write $w = x_1^{e_1}v$ where all copies of x_1 in v occur inside commutators. Continuing in this manner we can write w in the prescribed form. □

We note that the numbers $e_1, \ldots, e_n$ in the above theorem are unique, since the total number of times a variable can appear up to multiplicity is an invariant of w. We will call the total number of times a variable x appears in w the total degree of x and will write this as $\mathrm{Tot}_x(w)$. Define the weight of $w \in \mathbf{F}_n$ to be

$$\mathbf{weight}(w) = (\mathrm{Tot}_{x_1}(w), \mathrm{Tot}_{x_2}(w), \ldots, \mathrm{Tot}_{x_n}(x)).$$

Hence the e_i in the above lemma are exactly the values of $\mathrm{Tot}_{x_i}(w)$.

Since the weight of a word is invariant, we have the following corollary to the above lemma:

Corollary 2.2. *Let $w \in \boldsymbol{F}_n$. Then w is in $\boldsymbol{F}_n'$ if and only if $\boldsymbol{weight}(w) = (0, 0, \ldots, 0)$.*

Recall the following well-known theorem about $\mathrm{Aut}(\mathbf{F}_n)$.

Theorem 2.3. *[85] The group $\mathrm{Aut}(\boldsymbol{F}_n)$ is generated by the following types of automorphisms where one changes a word w to a word $\tilde{w}$ as described below:*

(1) Switch the variables x_i and x_j.

(2) Replace x_i with x_i^{-1}.

(3) Replace x_i with $x_i x_j$.

A proof of the above theorem can be found in Lyndon and Schupp [73], although their argument is more modern than Nielsen's original argument.

We can now prove that any word is equivalent up to automorphism to a power word times an element of the commutator subgroup.

Lemma 2.4. *Let $w \in \boldsymbol{F}_n$. Write $w = x_1^{e_1} \dots x_n^{e_n} \cdot c$ where c is in $\boldsymbol{F}'_n$. Then there is an automorphism σ of $(\boldsymbol{F}_n)$ such that $\sigma(w) = x_1^d \cdot c'$ where c' is in $\boldsymbol{F}'_n$ and $d = \boldsymbol{gcd}(e_1, \dots, e_n)$.*

Proof. There is a Nielsen transformation taking $w(x_1, \dots, x_n)$ to $w(x_1 x_i, \dots, x_n)$. Such a transformation changes the weight of w as follows.

$$\textbf{weight}(w(x_1, \dots, x_n)) = (a_1, \dots, a_n) \to \textbf{weight}(w(x_1 x_i, \dots, x_n) = (a_1 + a_i, a_2, \dots, a_n).$$

Swapping variables will naturally swap their place in the Nielsen transformation as well. Hence by applying the appropriate Nielsen transformations we can run the Euclidean algorithm on the weight of w until we arrive at a word v with $\textbf{weight}(v) = (d, 0, 0, \dots, 0)$. The combination of the transformations gives us a $\sigma \in \mathrm{Aut}(\mathbf{F}_n)$ such that $\sigma(w) = x_1^d c'$ where c' is in $\mathbf{F}'_n$. □

Corollary 2.5. *Let G be a finite group and suppose that $(|G|, p) = 1$. Then for $w = x^p$ we have that $w(G) = G$.*

Lemma 2.6. *Let F_n be the free group on the symbols $x_1, \dots, x_n$ and let $w \in F_n$ be a word. Let $\sigma \in Aut(F_n)$ and $u = \sigma(w)$. Then for any group G, $w(G) = u(G)$.*

Proof. The elementary Nielsen transformations do not change the image of a word map in a group. □

Recall that $K(G)$ is the set of all words in $\mathbf{F}_n$ that are laws on G, i.e., that as maps evaluate to the identity for any n-tuple of elements of G. More precisely

$$K(G) = \bigcap_{\alpha:\mathbf{F}_n \to G} \ker(\alpha).$$

We now present the following lemma, which has some surprisingly powerful applications.

Lemma 2.7. *Let $w \in \boldsymbol{F}_n$ and let G be a group. Suppose that σ is an automorphism of $\boldsymbol{F}_n$. Let*

$$\sigma(w) = w' = x_1^d c, \text{ where } c \in \boldsymbol{F}_n'.$$

Then $w \in K(G)$ if and only if $x_1^d \in K(G)$ and $c \in K(G)$.

Proof. Clearly, if x_1^d and c are both in $K(G)$ then w' and w are too. Suppose that $w' \in K(G)$. Then as a map $w'(g_1, \ldots, g_n) = 1$ for all $g_1, \ldots, g_n \in G$. So $w'(g, 1, \ldots, 1) = g^d = 1$ for all $g \in G$, i.e., $x_1^d \in K(G)$. Equivalently, $x_1^{-d} \in K(G)$ and we see that $c \in K(G)$ as well. □

Corollary 2.8. *Let G be a group with finite exponent. Let $w = x_1^{e_1} \ldots x_n^{n_n} c$, where c is in $\boldsymbol{F}_n'$. Then the word map w is in $\boldsymbol{F}_n(G)'$ if and only if the exponent of G divides* $\gcd(e_1, \ldots, e_n)$.

As another corollary to Lemma 7.1 we can answer a question of Amit and Vishne in the negative. Regarding the probability distributions of word maps, Amit and Vishne asked the following two questions. Let $N_{G,w}(g) = |\{(\overline{g} \in G^n : w(\overline{g}) = g\}|$. Their $N_{w,G}(g)$ is simply the counting version of our $\mu_{w,G}$, the probability distribution on G induced by w. Thus, $N_{w,G} = N_{w',G}$ if and only if $\mu_{w,G} = \mu_{w',G}$ and w and w' have the same number of variables. Amit and Vishne asked [2]:

Question 2.9. Suppose $N_{w,G} = N_{w',G}$ for every finite group G. Does it follow that w' is mapped to w by some automorphism of $\mathbf{F}_n$?

Question 2.10. Suppose $N_{w,G} = N_{w',G}$ for a fixed group G. Does it follow that w can be mapped by an automorphism of $\mathbf{F}_n$ to some w'', such that w'' is equivalent to w' modulo $K(G)$, i.e., such that w'' induces the same word map as w'.

We will answer Question 2.10 in the negative in Example 2.11 below. A work by Puder and Parzanchevski has shown that in certain situations Question 2.9 is true: if $N_{w,G}$ and $N_{w',G}$ are uniform for all groups G, then there is some automorphism of $\mathbf{F}_n$ taking w' to w [93]. It is unknown whether Question 2.9 holds in general. The following example is the **answer in the negative** to Question 2.10 of Amit and Vishne:

Example 2.11. [17, Example 5] There are word maps w and v over $G = S_3$, the symmetric group on 3 symbols, that induce the same probability distribution on G but no automorphism of $\mathbf{F}_2(S_3)$ maps w to v. Consider the words $w = x^2$ and $v = [x, yx^2y^2]$ as elements of $\mathbf{F}_2$. The corresponding word maps induce the same probability distribution on G.

We will write $\overline{w}$ and $\overline{v}$ for the word maps on G associated to w and v respectively. Suppose, by way of contradiction, that there were such an automorphism σ of $\mathbf{F}_2$, such that $\overline{\sigma(w)} = \overline{v}$. Hence, $\overline{x^2} = \overline{\sigma^{-1}(v)}$. Equivalently, the word $x^2\sigma^{-1}(v^{-1})$ is a law on G. So on G, the word x^2c would be a law for some $c \in \mathbf{F}_2'$. By Lemma 7.1 the word x^2 would be a law of G, a contradiction.

Even restricting to nilpotent groups, the author and Turbo Ho have found that there are 5 automorphism classes of word maps in $\mathbf{F}_2(Q_8)$, but only 4 probability distributions over Q_8. Hence it must be the case that there are two word maps w and v over Q_8 that

induce the same probability distribution, such that no element of $\mathrm{Aut}(\mathbf{F}_2)$ maps $\overline{w}$ to $\overline{v}$, where $\overline{w}$ and $\overline{v}$ are the images of w and v in $\mathbf{F}_2(Q_8)$.

We conclude this chapter by noting some elementary observations.

Lemma 2.12. *Let G be a group and let $w \in \boldsymbol{F}_n$. Then for $H \leq G$ we have that $w(H) \leq H$.*

Lemma 2.13. *Let G be a group and $w \in \boldsymbol{F}_n$. The set $w(G)$ is a union of conjugacy classes of G.*

The following theorem will be used in a few places. It was a conjecture of Frobenius and proven by Iliyori and Yamaki using the classification of finite simple groups [46]. We will refer to it in the text as the Frobenius solution theorem.

Theorem 2.14 (Frobenius)**.** *Let G be a finite group and let $X(d) = \{x \in G : x^d = 1\}$. If $|X(d)| = d$ then X is a normal subgroup of G.*

A weaker, but more natural version of Frobenius's theorem will suffice in many cases.

Lemma 2.15. *If m divides $|G|$, then m divides*

$$|\{x \in G : x^m = 1\}|.$$

A nice, self-contained proof can be found in a note by Isaacs and Robinson [50].

Chapter 3

The Not Images of Power Maps.

3.1 Power maps on groups.

The simplest words to investigate are those contained in $\mathbf{F}_1$. These words look like x^k for some integer k. We will call the words x^k power words and refer to the induced map from G to G as a power map. For the power word $w = x^k$ we will write $n_k(G) = |G| \setminus |w(G)|$ and $\mathcal{N}_k(G) = G \setminus w(G)$.

Many mathematicians have looked at power maps on a finite group. Miller [79] showed that the map $w = x^2$ is a law on a group G if at least $\frac{3}{4}|G|$ elements in G are solutions to it, i.e., if $\mu_{w,G}(1) \geq \frac{3}{4}$ then $\mu_{w,G}(1) = 1$.

Recall Theorem A, restated below.

Theorem A. *[18, Theorem B] Let G be a finite group, and write $n = n_k(G)$. If $n > 0$, then $|G| \leq n(n+1)$ and in fact $|G| \leq n^2$, except in the case where G is a Frobenius group with kernel of order $n+1$ and $\mathcal{N}_k(G)$ is the set of nonidentity elements of the Frobenius kernel.*

We will show that the bound in Theorem A is strict.

As mentioned in Chapter 1, Lucido and Pournaki [70, 71] investigated the proportion of elements of a finite group G that are squares. They showed that $n_2(G) \geq \lfloor \sqrt{G} \rfloor$ and noted that unless G is one of the exceptional groups in Theorem A then $|G| \leq n_2(G)^2$

is tight as exhibited by the cyclic group of order 4. After proving Theorem A, we will show that this example is unique, i.e., that if G is a finite group and $n = n_k(G)$, then $|G| = n^2$ if and only if G is the cyclic group of order 4. We will also show that Theorem A can be improved in the case that k is assumed to be odd.

Prior to Luicido and Pournaki, Bannai et al. [4] proved that $n_k(G) \geq \lfloor \sqrt{G} \rfloor$ using the classification of finite simple groups. Lévai and Pyber [64] later produced a classification-free proof of that result. The proof we present is elementary.

The chapter proceeds as follows. In section 3.2 we prove Theorem A. In section 3.3 we present some interesting refinements of Theorem A. Then we briefly recall the case for infinite groups in section 3.4. Finally we conclude in section 3.5 with a result of the author and Sara Jensen about what the sequence of not powers tells us about a group G.

We now proceed with our proof of Theorem A.

3.2 Proof of Theorem A.

We will first prove Theorem A in the case where k is a prime number. We will then show how the general case reduces to this case. Recall that for a prime p, an element g of a group is called p-regular if $o(g)$ is finite and not divisible by p; if $o(g)$ is finite and divisible by p we say that p is p-singular. Variations of all the theorems in this section can be found in [18, Section 2].

We have the following observation.

Lemma 3.1. *Let $x \in G$, and let p be a prime. Let $w = x^p$. Then $x \notin w(G)$ if and only if x is not p-regular and the cyclic group $\langle x \rangle$ does not have index p in any cyclic*

subgroup of G.

Proof. All p-regular elements are p-th powers, since $w(G) = G$ by Corollary 2.5. If x has infinite order and the cyclic group $\langle x \rangle$ has index p in the cyclic group Y, then $x \in \langle x \rangle = Y^p$, a contradiction to $x \notin w(G)$. □

The next lemma is rather surprising. It states that the number of not images of the word x^k decreases when the map is restricted to subgroups.

Lemma 3.2. *Let G be a finite group and let $H \leq G$. Let $w = x^p$. Then $n_p(H) \leq n_p(G)$.*

Proof. We will write w for the map $G \to G$ defined by w and w_H for the map $H \to H$ defined by w. We note the following

$$\begin{aligned} n_p(G) &= |G| \setminus w(G) \\ &= \sum_{x \in w(G)} \big(|w^{-1}(x)| - 1\big) \\ &\geq \sum_{x \in w_H(H)} \big(|w^{-1}(x)| - 1\big) \\ &\geq \sum_{x \in w_H(H)} \big(|w_H^{-1}(x)| - 1\big) \\ &= n_p(H). \end{aligned}$$

The first inequality holds because each summand is nonnegative. □

Lemma 3.3. *Let G be finite, and suppose that p divides $|\boldsymbol{Z}(G)|$, where p is prime. Then $|G| \leq 2n_p(G)$.*

Proof. Let $Z \subseteq \mathbf{Z}(G)$ with $|Z| = p$. Since all elements in each coset of Z in G have the same pth power, it follows that $|w(G)|$ is at most the number of cosets which is $|G|/p$.

Then

$$n_p(G) = |G| - |G^p| \geq |G| - \frac{|G|}{p} = \frac{p-1}{p}|G| \geq \frac{|G|}{2}.$$

□

We will use the following characterization of Frobenius groups to establish when the bound in Theorem A is obtained.

Theorem 3.4. *[48, Theorem 6.4] Let N be a normal subgroup of a finite group G, and suppose that A is a complement for N in G. The following are equivalent.*

(1) The conjugation action of A on N is fixed point free.

(2) $A \cap A^g = 1$ for all $g \in G \setminus A$.

(3) $\boldsymbol{C}_G(a) \leq A$ for all nonidentity elements $a \in A$.

(4) $\boldsymbol{C}_G(n) \leq N$ for all nonidentity elements $n \in N$.

When a group G has a normal subgroup N with complement A such that the conjugation action of A on N is fixed point free, we say G is a Frobenius group and call N the Frobenius kernel of G.

We can now prove a variant of Theorem A when k is prime.

Theorem 3.5. *Let G be a finite group and let p be a prime. Write $n = n_p(G)$. If $n > 0$, then $|G| \leq n(n+1)$ and in fact $|G| \leq n^2$, except in the case where G is a Frobenius group with kernel of order $n+1$ and $\mathcal{N}_k(G)$ is the set of nonidentity elements of the Frobenius kernel.*

Proof. Since $w(G)$ is a union of conjugacy classes, so is $G \setminus w(G)$. Suppose that $G \setminus w(G)$ is not a single conjugacy class; then some class contained in it has size at most $\frac{n}{2}$. Let

x be a member of this class, and write $C = \mathbf{C}_G(x)$, so $|G : C| \leq \frac{n}{2}$. Since $x \in G \setminus w(G)$, we see that x is p-singular and thus p divides $|\mathbf{Z}(C)|$. Hence $|C| \leq 2n_p(C)$ by Lemma 3.3. By Lemma 3.2 we know that $n_p(C) \leq n$. We thus have

$$|G| = |C||x^G| \leq 2n|x^G| \leq n^2.$$

Now suppose that $G \setminus w(G)$ is a single class x^G. We know that x is p-singular. Let A be a cyclic p-subgroup of G having largest possible order. Then $1 < A$ and each generator of A has order equal to $|A| > 1$. Moreover, A does not have index p in a larger cyclic subgroup. Therefore the generators of A are in $G \setminus w(G)$. Moreover, the order of x is $|A|$.

Suppose that $|A| > p$. Then the pth powers of elements of x^G form a conjugacy class $(x^p)^G$ with elements having order divisible by p. Moreover, the map $x^G \to (x^p)^G$ is not injective, so $|(x^p)^G| < n$. Write $C = \mathbf{C}_G(x^p)$. Then $|G : C| < n$, and since $\mathbf{C}_G(x) \leq C$ it follows that $|G : C|$ divides $|G : \mathbf{C}_G(x)| = n$. Therefore, $|G : C| \leq \frac{n}{2}$. As before $x^p \in \mathbf{Z}(C)$ and thus p divides the order of $\mathbf{Z}(C)$. We can apply Lemmas 3.2 and 3.3 to obtain

$$|G| = |(x^p)^G||G : C| \leq \frac{n}{2}2n = n^2.$$

We can now assume that $G \setminus w(G)$ is a single conjugacy class x^G and that $o(x)$ is p. Let y be a p-singular element of G and let B be maximal among cyclic subgroups of G containing y. Then B does not have index p in a larger cyclic subgroup, and p divides $|B|$. Therefore, the generators of B are in $G \setminus w(G)$. Hence, it must be the case that $|B| = p$. So $G \setminus w(G)$ is exactly the set of p-singular elements of G; moreover, all such elements have order exactly p.

We note that all elements of $C = \mathbf{C}_G(x)$ must have order p or 1. Otherwise, we could

generate a p-singular element with order greater than p. Hence all nonidentity elements of C have order p and are thus contained in $G \setminus w(G)$. It follows that $|C| \leq n+1$. If the inequality is strict, then $|G| = |x^G||C| \leq n^2$. We can now assume that $|C| = n+1$, so $|G| = n(n+1)$. In this case $C = \{1\} \cup (G \setminus w(G))$, so $C \lhd G$, and thus $C = \mathbf{C}_G(y)$ for all $y \in x^G$. Thus G is a Frobenius group with kernel C. □

Many of the inequalities we used above can be tightened, and the object of section 3.3 is to demonstrate some refinements of Theorem A that are obtained by examining the inequalities in greater detail.

The next lemma will be used to show how the general case of Theorem A follows from Theorem 3.5.

Lemma 3.6. *Let G be a group, and suppose that $0 < n_k(G) < \infty$. Then there exists a prime p dividing k such that $0 < n_p(G) \leq n_k(G)$.*

Proof. We proceed by induction on k. Since $n_k(G) > 0$, some element of G is not a kth power, and thus $k > 1$. If k is prime, there is nothing to prove, so assume that $k = ab$, where $a > 1$ and $b > 1$, and thus $a < k$ and $b < k$. Now write $w = x^k, v = x^a, u = x^b$. So $w(G) \subseteq u(G) \cap v(G)$, so $n_a(G), n_b(G) \leq n_k(G)$. We note that $n_a(G)$ and $n_b(G)$ cannot both be 0, i.e., we cannot have $u(G) = v(G) = G$, because if $u(G) = v(G) = G$ then the map $w(G) = v(u(G)) = G$, a contradiction. So one of $n_a(G)$ or $n_b(G) \leq n_k(G)$. By induction there is some prime p with $0 < n_p(G) \leq n_k(G)$. □

We now prove Theorem A.

Proof. **Proof of Theorem A.** From the lemma above, we can choose a prime p dividing k such that $0 < n_p(G) \leq n$. By Theorem 3.5 we have that $|G| \leq n_p(G)(n_p(G)+1)$ so

if $n_p(G) < n$, then $|G| < n^2$. Assume now that $n_p(G) = n$. Let $w = x^k$ and let $u = x^p$. Since p divides k we have that $w(G) \subseteq u(G)$, and since $n_p(G) = n$ we see that $w(G) = u(G)$. Hence $|G| \leq n(n+1)$ by Theorem 3.5, and in fact $|G| \leq n^2$ unless $|G| = n(n+1)$, in which case G is a Frobenius group and $G \setminus w(G)$ is exactly the set of nonidentity elements of the Frobenius kernel. □

3.3 Some refinements of Theorem A.

As mentioned in section 3.2, the inequalities used to prove Theorem A can often be sharpened if G has certain nice structural properties. In this section we examine some of refinements of Theorem A. For convenience we will write $\mathcal{N}_p(G) = G \setminus w(G)$, where w is x^p.

It was noted in the work of Lucido and Pournaki [71] that if G is not one of the exceptional cases to Theorem A, then the bound $|G| \leq n_2(G)^2$ is tight as exhibited by the cyclic group of order 4. In this note, we prove this example is unique:

Theorem 3.7. *If G is a finite group and $|G| = n_k(G)^2$ for some k, then $k \equiv 2 \pmod 4$ and $G \cong C_4$.*

Restricting our attention to odd primes, we also prove the following specialized version of Theorem A.

Theorem 3.8. *Let G be a finite group, and write $n = n_p(G)$, where p is an odd prime dividing $|G|$. Then G satisfies one of the following statements:*

(1) $|G| = n(n+1)$ *and G is a Frobenius group as in Theorem A.*

(2) $|G| = \frac{n}{2}(n+2)$ *and G is a central extension of a Frobenius group of order $\frac{n}{2}\left(\frac{n}{2}+1\right)$ by C_2.*

(3) $|G| = \frac{n}{2}(n+1)$ *and G is a Frobenius group with kernel of order $n+1$, and $\mathcal{N}_p(G)$ is the set of nonidentity elements of the Frobenius kernel.*

(4) $|G| \leq \frac{n^2}{2}$.

We note that when $|G| = \frac{n}{2}(n+2)$, then G is a central extension of one of the exceptional groups in Theorem A by C_2.

In section 3.3.1 we will examine various inequalities regarding $n_k(G)$. Sections 3.3.2 and 3.3.3 contain the proofs of Theorem 3.7 and Theorem 3.8 respectively.

3.3.1 Inequalities involving $n_k(G)$.

The next lemma follows from the fact that if $\langle x \rangle = \langle y \rangle$ then $x \in \mathcal{N}_k(G)$ if and only if $y \in \mathcal{N}_k(G)$.

Lemma 3.9. *Let p be a prime. If $n = n_p(G)$ for a finite group G, then $p-1$ divides n.*

Proof. Let $\sim$ be the equivalence relation $x \sim y$ iff $\langle x \rangle = \langle y \rangle$. We can partition $\mathcal{N}_p(G)$ into equivalence clases under $\sim$. Each such equivalence class has size divisible by $p-1$ and thus $n = |\mathcal{N}_p(G)|$ is divisible by $p-1$. □

The following lemma is merely the strengthening of the one we used to prove Theorem A. Let p be a prime. For $H \leq G$ the set $\mathcal{N}_p(H)$ is not always a subset of $\mathcal{N}_p(G)$. However $n_p(H) \leq n_p(H)$.

Lemma 3.10. *Let G be a finite group and H be a subgroup of G. Let p be a prime. Then $n_p(H) \leq n_p(G)$. Moreover $n_p(H) = n_p(G)$ if and only if $\mathcal{N}_p(H) = \mathcal{N}_p(G)$.*

Proof. For $x \in G^p$, write $\theta(x) = \{y \in G : y^p = x\}$, and note that by assumption the sets $\theta(x)$ are nonempty and disjoint, and their union is the whole group G. It follows that

$$n_p(G) = |G| - |G^p| = \left(\sum_{x \in G^p} |\theta(x)| \right) - |G^p| = \sum_{x \in G^p} (|\theta(x)| - 1).$$

Similarly, if $x \in H^p$, we write $\varphi(x) = \{y \in H : y^p = x\}$. Then

$$n_p(H) = \sum_{x \in H^p} (|\varphi(x)| - 1).$$

Now $H^p \subseteq G^p$ and for $x \in H^p$ we have $\varphi(x) = H \cap \theta(x)$, so $|\varphi(x)| \leq |\theta(x)|$. Noting that the terms $|\theta(x)| - 1$ are nonnegative for $x \in G^p \setminus H^p$ we have:

$$n_p(G) - n_p(H) \geq \sum_{x \in H^p} (|\theta(x)| - |\varphi(x)|) \geq 0. \tag{3.1}$$

Hence $n_p(H) \leq n_p(G)$. If $n_p(H) = n_p(G)$, then both

$$\sum_{\substack{x \in G^p \\ x \notin H^p}} |\theta(x)| - 1 = 0 \quad \text{and} \quad \sum_{x \in H^p} (|\theta(x)| - |\varphi(x)|) = 0.$$

Thus every element of H^p has the same number of pth roots in H as it does in G and all elements of G^p that are not in H^p have order not divisible by p.

If $n_p(G) = n_p(H)$ then $x \in \mathcal{N}_p(H)$ implies that $x \in \mathcal{N}_p(G)$ and thus $\mathcal{N}_p(G) = \mathcal{N}_p(H)$. □

The following corollaries demonstrate some implications of $n_p(H) = n_p(G)$ for $H \subseteq G$ and G finite:

Corollary 3.11. *Let p be a prime and let G be a finite group. Suppose $H < G$ with $n_p(H) = n_p(G)$. Then $\boldsymbol{O}^{p'}(G) \subseteq H$; in particular every Sylow p-subgroup of G is contained in H.*

Proof. The set $X = \{x \in G : o(x) = p^k, k \in \mathbb{N}\}$ generates $\mathbf{O}^{p'}(G)$. Since every element of order p^k is contained in $\langle y \rangle$ for some $y \in \mathcal{N}_p(G)$, we conclude that

$$\mathbf{O}^{p'}(G) = \langle X \rangle \subseteq \langle \mathcal{N}_p(G) \rangle = \langle \mathcal{N}_p(H) \rangle \subseteq H.$$

If $S \in \mathrm{Syl}_p(G)$ then $S \subseteq \mathbf{O}^{p'}(G)$. □

Lemma 3.12. *Let G be a finite group, and suppose that p divides $|\boldsymbol{Z}(G)|$, where p is a prime. Then*

$$|G| \leq \frac{p\, n_p(G)}{p-1},$$

and if equality holds, then G has a normal cyclic Sylow p-subgroup.

Proof. Let $Z \subset \mathbf{Z}(G)$ have order p. Since all elements in each coset of Z in G have the same pth power, it follows that $|G^p|$ is at most the number of cosets of Z in G, i.e., $|G : Z| = |G|/p$. Then

$$n_p(G) = |G| - |G^p| \geq |G| - \frac{|G|}{p} = \frac{p-1}{p}|G|.$$

If $n_p(G) = \frac{p-1}{p}|G|$, then every coset of Z has a unique pth power. As in the proof of Lemma 3.10, for $x \in G^p$ write $\theta(x) = \{y \in G : y^p = x\}$. If $n_p(G) = \frac{p-1}{p}|G|$, then $\theta(x)$ is a single coset of Z, and thus $|\theta(x)| = p$ for all $x \in G^p$.

Consider the set

$$S = \{x \in G : o(x) = p^k, k \in \mathbb{Z}\}.$$

We claim S is a normal cyclic Sylow p-subgroup of G. Let $s \in S$ have maximum order. We claim that $S = \langle s \rangle$. Suppose that $x \in S$ has minimal order such that $x \notin \langle s \rangle$. Then $x^p \in \langle s \rangle$ and $|\langle s \rangle \cap \theta(x^p)| = p$. But, $|\theta(x^p)| = p$. Hence $x \in \theta(x^p) \subseteq \langle s \rangle$.

Therefore $S = \langle s \rangle$. □

As part of our proof of Theorem 3.7 we will see that the proportion of non-kth-powers under the action of taking quotients behave nicely:

Lemma 3.13. *Let G be a finite group. If $k > 0$ and N is a normal subgroup of G then*

$$\frac{n_k(G/N)}{|G/N|} \leq \frac{n_k(G)}{|G|},$$

with equality if and only if for all $x \in G$ every coset representative of $x^k N$ is in $G \backslash \mathcal{N}_k(G)$.

We now return our attention, for the moment, to the case $k = p$.

Theorem 3.14. *Let G be a finite p-group of order p^m, and write $n = n_p(G)$. If G is cyclic then $n = p^m - p^{m-1}$. Otherwise $n \geq p^m - p^{m-2}$.*

Proof. If G is cyclic, then the only elements of G in $\mathcal{N}_p(G)$ are the elements with order equal to $|G|$. Hence $n = \varphi(p^m) = p^m - p^{m-1}$.

If G is not cyclic then $G/\Phi(G)$ is not cyclic and G has a normal subgroup F such that G/F is elementary abelian of rank 2. By Lemma 3.13 we see that

$$\frac{n}{|G|} \geq \frac{n_p(G/F)}{|G : F|} = \frac{n_p(C_p \times C_p)}{p^2} = \frac{p^2 - 1}{p^2}.$$

Hence $n \geq p^m - p^{m-2}$. □

We will now introduce some notation. For a prime p, the set $\mathcal{N}_p(G)$ of non-p-th powers of G is a union of conjugacy classes of G. Write

$$\mathcal{N}_p(G) = x_1^G \cup \cdots \cup x_m^G.$$

Without loss of generality, we will assume that the listing of conjugady classes is ordered so that $o(x_i) \leq o(x_j)$ whenever $i \leq j$. The **type** of $\mathcal{N}_p(G)$ is the m-tuple $(o(x_1), \ldots, o(x_m))$. We will refer to m as the **length** of $\mathcal{N}_p(G)$.

Recall that an element y of a group G is said to be p-singular if p divides the order of y.

Lemma 3.15. *Let G be a finite group. Let m be the length of $\mathcal{N}_p(G)$. Let Y denote the set of orders of p-singular elements of G. Let X be the set of integers j such that $p^k j \in Y$ and $\gcd(j,p) = 1$. Then $|X| \leq m$.*

Proof. We know that for each $a \in X$ there is an element $y \in G$ such that $o(y) = j$. Let $z \in \mathcal{N}_p(G)$ such that $z^{p^k} = y$, with k minimal. Then $o(z) = p^k \cdot j$. Since z depends on j, we conclude that distinct $i, j \in X$ will yield distinct elements z_j, z_i. Since $o(z_j) \neq o(z_i)$ we conclude that $z_j^G \neq z_i^G$. □

We will use Lemma 3.15 to analyze groups for which the length of $\mathcal{N}_p(G)$ is small.

3.3.2 Proof of Theorem 3.7.

In this section, we will prove that the only group G for which there is an integer k such that $|G| = n_k(G)^2$ is C_4. Recall the following lemma:

Lemma 3.16 (Lemma 2.5 [18])**.** *Let G be a group with $0 < n_k(G) < \infty$. Then there exists a prime p dividing k such that $0 < n_p(G) \leq n_k(G)$.*

We immediately have:

Corollary 3.17. *If $|G| = n_k(G)^2$ and G is finite, then $|G| = n_p(G)^2$ for some prime p dividing k.*

In the rest of the section we will prove that $|G| = n_p(G)^2$ for a prime p, if and only if $p = 2$ and $G \cong C_4$.

Lemma 3.18. *Let G be a finite group and write $n = n_p(G)$ for a prime p. If $|G| = n^2$ and m is the length of $\mathcal{N}_p(G)$, then one of the following holds:*

(1): $m = 1$.

(2): $p = 2$ and $m = 2$.

Proof. There is some $x \in \mathcal{N}_p(G)$ with $|x^G| \leq n_p(G)/m$. Moreover, $x \in \mathbf{Z}(\mathbf{C}_G(x))$ and p divides $o(x)$. We conclude that

$$n_p(G)^2 = |G| = |x^G||\mathbf{C}_G(x)| \leq \frac{n_p(G)}{m}\frac{p}{p-1}n_p(G).$$

Hence $(p-1)m \leq p$ and we conclude that either $m = 1$; or $p = 2$ and $m = 2$. □

Theorem 3.19. *Let G be a finite group with $n = n_p(G) > 0$. If $\mathcal{N}_p(G)$ has length 1, then $|G| \neq n^2$.*

Proof. We first note that n must be greater than 1, since $n = 1$ implies that $G = C_2$ by Theorem A.

By way of contradiction assume that $|G| = n^2$. There is an $x \in \mathcal{N}_p(G)$ of order p^k, for some positive integer k. Since the length of $\mathcal{N}_p(G)$ is 1 we conclude that all non-pth powers in G have order p^k. Consider $C = \mathbf{C}_G(x)$. Lemma 3.15 shows that C is

a p-group, or else the length of $\mathcal{N}_p(G)$ would be greater than 1. Let $|C| = p^j$ for some $j \geq k \geq 1$.

We now have that $|G| = n^2 = |x^G| \cdot |C| = n \cdot p^j$. Hence $n = p^j$ and G is a p-group of order p^{2j}. Theorem 3.14, gives us

$$p^j = n \geq (p^2 - 1)p^{2j-2}.$$

Dividing both sides by p^j gives us

$$1 \geq (p^2 - 1)p^{j-2},$$

and thus $j = 1$ and we conclude that $|G| = p^2$. A contradiction to $|x^G| = n > 1$. □

We can now prove Theorem 3.7.

Proof. **of Theorem 3.7**. Let G be a finite group satisfying $|G| = n_k(G)^2$ for some k. Then $|G| = n_p(G)^2$ for some prime p dividing k by Corollary 3.17. Furthermore by Lemma 3.18 and Theorem 3.19, we may assume that the length of $\mathcal{N}_k(G)$ is exactly 2, and that $p = 2$. Let $n = n_2(G)$.

Let $x \in \mathcal{N}_2(G)$ such that $|x^G|$ is minimal, and write $C = \mathbf{C}_G(x)$. We have

$$n^2 = |G| = |x^G||C| \leq \frac{n}{2} 2n_2(C)) \leq n^2.$$

Therefore, we must have the following equalities: $|x^G| = \frac{n}{2}$, $n_2(C) = n$, and $|C| = 2n$ for any $x \in \mathcal{N}_2(G)$. By Lemma 3.10, we are guaranteed that $\mathcal{N}_2(C) = \mathcal{N}_2(G)$. Moreover, by Lemma 3.12, we know that the Sylow 2-subgroup of C is cyclic. Now, fix an $x \in \mathcal{N}_2(G)$ such that $o(x) = 2^j$. Because $o(x)$ is 2^j and x is not a square in C, we see that the Sylow 2-subgroup of C is generated by x and has order 2^j. By Corollary 3.11, $\langle x \rangle$ is a Sylow subgroup of G. Moreover, $\langle x \rangle$ is normal in G.

Lemma 3.15 further tells us that C can be divisible by at most one odd prime. Let $|C| = 2^j q^\ell$. Then $n = 2^{j-1}q^\ell$ and $|G| = 2^{2j-2}q^{2\ell}$. Since $\langle x \rangle$ is a Sylow 2-subgroup of G, we see that $2^{2j-2} = 2^j$ and thus $j = 2$; moreover, G has a cyclic Sylow 2-subgroup and thus has a normal 2-complement H. Since normal subgroups commute, $H \subset C = \mathbf{C}_G(x)$. We conclude that $\ell = 2\ell$. Hence $\ell = 0$ and we conclude that $|G| = 4$ and G is cyclic. $\square$

3.3.3 Proof of Theorem 3.8.

To prove Theorem 3.8 we will first examine how the type of $\mathcal{N}_p(G)$ gives a bound on the order of G.

Lemma 3.20. *Let G be a finite group and write $n = n_p(G)$ for a prime p. If $|G| > \frac{n^2}{2}$ and m is the length of $\mathcal{N}_p(G)$, then either $m \leq 2$ or $p = 2$ and $m = 3$.*

Proof. There is some $x \in \mathcal{N}_p(G)$ with $|x^G| \leq n_p(G)/m$. Moreover, $x \in \mathbf{Z}(\mathbf{C}_G(x))$ and p divides $o(x)$. We conclude that

$$\frac{n^2}{2} < |G| = |x^G||\mathbf{C}_G(x)| \leq \frac{n}{m}\frac{p}{p-1}n.$$

Hence $(p-1)m < 2p$ and we conclude that either $m \leq 2$; or $p = 2$ and $m = 3$. $\square$

Lemma 3.21. *Let G be a finite group and p a prime. If G contains an element of order p^k for $k > 1$, then $|G| \leq \frac{n_p(G)^2}{p^{k-2}(p-1)}$.*

Proof. Let S be a Sylow p-subgroup of G and let p^k be the exponent of S. Suppose that $k > 1$. We will show that $|G| \leq \frac{n_p(G)^2}{p^{k-2}(p-1)}$.

Let K be the set of all elements of G of order p^k. Then $K \subseteq \mathcal{N}_p(G)$ and is a normal subset of G. Consider the set $K^{p^{k-1}}$ of p^{k-1} powers of elements of K. Let $\mu : G \to G$

take $x \to x^{p^{k-1}}$. For an element $y \in K$, we see that $\mu(y) \in K^{p^{k-1}}$; moreover, μ is at least $p^{k-1} : 1$ from $\langle y \rangle$ to $y^{p^{k-1}}$. Hence $|K^{p^{k-1}}| \leq \frac{|K|}{p^{k-1}}$. Therefore

$$|G| = \left|(y^{p^{k-1}})^G\right| \cdot \left|\mathbf{C}_G(y^{p^{k-1}})\right| \leq \frac{|K|}{p^{k-1}} \frac{p}{p-1} n_p(G) \leq \frac{n_p(G)^2}{p^{k-2}(p-1)}.$$

□

As seen in both Lemma 3.20 and 3.21 the prime 2 is special and will often require a separate argument. Recall that the type of $\mathcal{N}_p(G)$ is a list of the orders of conjugacy classes in $\mathcal{N}_p(G)$. By combining Lemmas 3.20, 3.21, and 3.15 we can greatly restrict the type of $\mathcal{N}_p(G)$ in the case that p is an odd prime and $|G| > \frac{n_p(G)^2}{2}$.

Corollary 3.22. *Let G be a finite group and p an odd prime dividing $|G|$. Write $n = n_p(G)$ and let m be the number of conjugacy classes of G contained in $\mathcal{N}_p(G)$. If $|G| > \frac{n^2}{2}$, then the type of $\mathcal{N}_p(G)$ is either (p),(p,p) or (p,qp).*

Of course there is a corresponding classification for the case $p = 2$, but the parametrization of possible types is not as succinct.

If p is an odd prime then we have the following theorem classifying when the type of $\mathcal{N}_p(G)$ is (p) in Corollary 3.22:

Theorem 3.23. *Let G be a finite group and p an odd prime dividing the order of G. Write $n = n_p(G)$. If the type of $\mathcal{N}_p(G)$ is (p) and $|G| \neq n(n+1)$, then $|G| \leq \frac{n(n+1)}{3}$.*

Proof. Let $x \in \mathcal{N}_p(G)$. By Lemma 3.15, $\mathbf{C}_G(x)$ is a p-group and is contained in a Sylow p-subgroup of S. Since $\mathcal{N}_p(G)$ has type (p) we know that all nontrivial elements of S are in $\mathcal{N}_p(G)$ and hence conjugate to x. Let $y \in \mathbf{Z}(S) \setminus 1$. Let $C = \mathbf{C}_G(y)$. Since $y \in \mathcal{N}_p(G)$, we have that $C = S$. Let $|C| = |S| = p^k$. We know that p^k divides $|G|$. By the theorem

of Frobenius, $p^k|(n+1)$. We have

$$|G| = |x^G||C| = n \cdot p^k.$$

If $p^k = n+1$, then $|G| = n(n+1)$. Otherwise suppose $p^k = \frac{n+1}{2}$ and $n = 2p^k - 1$. By Lemma 3.9, we know that n is divisible by $p-1$ which is even since p is an odd prime; This contradicts $n = 2p^k - 1$. Therefore if $p^k \neq n+1$, then $p^k \leq \frac{n+1}{3}$. □

We note that

$$\frac{n(n+1)}{3} \leq \frac{n^2}{2},$$

when $n \geq 2$. When $n = 1$, $|G| \leq 2$ by Theorem A and hence no odd primes divide $|G|$.

We now handle the two remaining cases in Corollary 3.22.

Theorem 3.24. *Let G be a finite group and p an odd prime dividing the order of G. Write $n = n_p(G)$. Assume $\mathcal{N}_p(G)$ has length 2. If $|G| > \frac{n^2}{2}$ then one of the following happens:*

- *The type of $\mathcal{N}_p(G)$ is (p,p) and $|G| = \frac{n}{2}(n+1)$ and G is a Frobenius group.*
- *The type of $\mathcal{N}_p(G)$ is $(p,2p)$ and $|G| = \frac{n}{2}(n+2)$ and G is a central extension of a Frobenius group of order $\frac{n}{2}(\frac{n}{2}+1)$.*

Proof. By Corollary 3.22, we know that the type of $\mathcal{N}_p(G)$ is either (p,p) or (p,pq) for q a prime. We proceed by cases.

Suppose that the type of $\mathcal{N}_p(G)$ is (p,p). Let x, y be elements of $\mathcal{N}_p(G)$ in different conjugacy classes. Without loss of generality assume that $|x^G| \leq |y^G|$, so $|x^G| \leq \frac{n}{2}$. By Lemma 3.15, we know that $C = \mathbf{C}_G(x)$ is a p-group and thus $|C| \leq (n+1)$. Therefore:

$$|G| = |x^G||C| \leq |x^G|(1+n) \leq \frac{n}{2}(n+1).$$

If $|x^G| < \frac{n}{2}$, then since n is even by Lemma 3.9, we know that $|x^G| \leq \frac{n}{2} - 1$ and thus

$$|G| \leq (\frac{n}{2} - 1)(n+1) \leq \frac{n^2}{2}.$$

Suppose $|x| = \frac{n}{2}$ and that $|C| < (n+1)$. Then $|C| \leq n$ and

$$|G| \leq \frac{n^2}{2}.$$

Hence if the type of $\mathcal{N}_p(G)$ is (p,p) and $|G| > \frac{n^2}{2}$ then $|G| = \frac{n}{2}(n+1)$. If we have $|G| = \frac{n}{2}(n+1)$, then for all $x \in \mathcal{N}_p(G)$ we have $|x^G| = \frac{n}{2}$ and $C = \mathbf{C}_G(x)$ has order $n+1$. Moreover $C = \mathcal{N}_p(G) \cup 1$ is a normal subgroup of G. We further note that $n+1$ and $\frac{n}{2}$ are coprime, so by the Schur–Zassenhaus theorem C has a complement in G. Since the centralizer of any nontrivial element of C is contained in C, we see that G is a Frobenius group with Frobenius kernel C consisting of $\mathcal{N}_p(G)$ together with the identity.

Suppose that the type of $\mathcal{N}_p(G)$ is (p,pq) for some prime q. Let $x \in \mathcal{N}_p(G)$ have order p and $y \in \mathcal{N}_p(G)$ have order pq. We note that x^G contains all elements of G of order p. Hence $y^q \in x^G$. Moreover, every qth power of an element of y^G is in x^G. The qth power map from y^G to x^G is j to 1 for some positive integer j. Since $|y^G| + |x^G| = n$ we have

$$n = (j+1)|x^G| \quad \text{and} \quad |x^G| = \frac{n}{j+1}.$$

Now consider $C = \mathbf{C}_G(x)$. Every element of C has order $1, p, q$ or pq. We wish to bound the number of elements in C of each of order. We note that there are exactly j elements in C of order pq whose qth power is x^q. Moreover, any element $s \in C$ of order q will satisfy $(xs)^q = x^q$. Hence there are at most j elements $s \in C$ of order q. Since all elements of y^G that have x^q as their q-power commute with x, we conclude that there are exactly j elements of order q in C. We also know that there are at most n elements

total of orders p and pq in C. Hence $|C| \leq n + j + 1$. We thus have

$$|G| = |x^G||C| = \frac{n}{j+1}|C| \leq \frac{n}{j+1}(n + j + 1).$$

For $j > 1$ and $n > 8$, we have $\frac{n}{j+1}(n + j + 1) \leq \frac{n^2}{2}$. Therefore if $|G| > \frac{n^2}{2}$ and $|G| > 56$, we can assume that $j = 1$. (For groups with order less than or equal to 56, we verified the theorem directly in Magma [9].) Since the map qth power map from y^G to x^G is 1:1, we can assume that $q = 2$, otherwise C would contain more than j elements of order q. Hence the element of order 2 in C is central in C (since there is only one such element). Therefore the number of elements of G of order p and $2p$ are equal and thus n is even. Hence if $|C| < n + 2$, then $|C| \leq n$ (since $|C|$ is even) and we have that

$$|G| = |x^G|C| \leq \frac{n^2}{2}.$$

Therefore if $|G| > \frac{n^2}{2}$ and the type of $\mathcal{N}_p(G)$ is not (p, p) then the type of $\mathcal{N}_p(G)$ is $(p, 2p)$ and $|G| = \frac{n}{2}(n + 2)$. Suppose $|G| = \frac{n}{2}(n + 2)$ and let $x \in \mathcal{N}_p(G)$ satisfy $o(x) = p$. Let $C = \mathbf{C}_G(x)$. Then $|C| = n + 2$ and C contains a unique involution z. Moreover, C is normal, since it is generated by the normal set $\mathcal{N}_p(G)$. Hence z is central in G, being the unique element of order 2 in a normal subgroup of G.

We now ask about the group $\overline{G} = G/\langle z \rangle$. What is $n_p(\overline{G})$? It must be the case that $n_p(\overline{G}) \leq n/2$. By Theorem A, we are guaranteed that $n_p(\overline{G}) = \frac{n}{2}$ and $\overline{G}$ is a Frobenius group with kernel of order $\frac{n}{2} + 1$ and complement of order $\frac{n}{2}$. Hence G is a central extension of such a Frobenius group. □

We can now prove Theorem 3.8:

Proof. **of Theorem 3.8.** By Corollary 3.22 we can reduce to either the length of $\mathcal{N}_p(G)$ is 1 or 2. If the length of $\mathcal{N}_p(G)$ is 1, then Theorem 3.23 demonstrates that $|G| = n(n+1)$

or $|G| \leq \frac{n^2}{2}$. If the length of $\mathcal{N}_p(G)$ is 2, then by Theorem 3.24, either $|G| \leq \frac{n^2}{2}$ or G satisfies hypotheses (2) or (3) of the theorem. □

3.4 Infinite groups.

The finiteness in Theorem A can be relaxed to other finite-like conditions. In [18] the author, Marty Isaacs, and Dane Skabelund give the following theorem.

Theorem 3.25. *[18, Theorem C] Let G be a group, and assume that $0 < n_k(G) < \infty$. Suppose also that one of the followings holds.*

(1) G satisfies the maximal condition on cyclic subgroups.

(2) G has a finite-index nilpotent subgroup, i.e., G is virtually nilpotent.

(3) G is residually finite.

Then G is finite.

However, independent constructions of Pálfy and Ivanov [51] produce an infinite group G with $n_p(G) = p - 1$. We next turn to a question about the sequence of values $(n_k(G))_{k\in\mathbb{N}}$ tells us about a group G.

3.5 The sequence of not powers in a group.

In this section, we explore the connection, for a group G, between the sequence $(n_k(G) : k \in \mathbb{N})$, which we write $(n_k(G))$, and structural information about G. We will also mention a result about the set $\{n_k(G) : k \in \mathbb{N}\}$. The results in this section were joint work with Sara Jensen [20].

It should be noted, that the sequence $(n_k(G))$ bears resemblance to another arithmetic sequence of interest, namely the order type of G [97]. Recall that the order type of G is the sequence $(G(d) : d \in \mathbb{N})$ where

$$G(d) = |\{x \in G : o(x) = d\}|.$$

We will discuss this interesting relationship later in the section.

We will show that whether or not a group is nilpotent is determined by the sequence $(n_k(G))$. However, $(n_k(G))$ does not always determine G even for nice families of groups. Nevertheless $(n_k(G)$ conveys interesting information about a group G.

For a given group G, most of the properties we will discuss about $(n_k(G))$ are also true for the order type of G. For example, whether or not a finite group G is nilpotent can be deduced from either sequence. However, the two sequences are not equivalent, e.g.,

$$\underbrace{(Q_8(d)) \neq (D_8(d))}_{\text{order type}}, \text{ but } \underbrace{(n_k(Q_8)) = (n_k(D_8))}_{\text{not powers}}$$

and

$$((C_4 \times C_4)(d)) = ((Q_8 \times C_2)(d)), \text{ but } (n_k(C_4 \times C_4)) \neq (n_k(Q_8 \times C_2)).$$

Both sequences are ostensibly infinite. The sequence $(G(d))$ satisfies $G(d) = 0$ for all $d \geq |G|$. However, from the initial entries of the sequence it is impossible to determine $|G|$. For example, let G be a finite group and M the $|G|$-th prime number. Then $(G \times C_M)(d) = G(d)$ for all $d < M$. However any nonzero term of $(n_k(G))$ can be used to bound $|G|$ and thus calculate when the sequence effectively terminates. Specifically, for two groups if $n = n_k(G) = n_k(H) > 0$ then either $|G| = |H|$ or for some $j < n(n+1)$ we have $n_j(G) \neq n_j(H)$.

The following problem is called Thompson's problem and originated from correspondence between Thompson and Shi [97].

Question 3.26. Let G and H be finite groups with $(G(d)) = (H(d))$. If H is solvable must G be solvable?

The problem tries to understand how much information about a group is contained in the order type of G. It is still open, but is known to be true in a number of cases such as when G has exactly 30 elements of maximal order [11].

We have tested the analogous problem concerning $(n_k(G))$ for all groups with order up to 2000 and subsequently ask the following open question:

Question 3.27. Let G and H be finite groups with $(n_k(G)) = (n_k(H))$. If H is solvable must G be solvable?

Let G be a finite group and suppose that $|G| = mr$ where $(m, r) = 1$. A subgroup of G of order m is called a Hall m-subgroup of G. In general, a group G does not have Hall subgroups of every possible order; for example, A_5 has no subgroup of order 15 order 20. Moreover, unlike Sylow subgroups, two Hall subgroups of the same order do not have to be conjugate, or even isomorphic. However, a group G has exactly one Hall subgroup H of order m if and only if $H \lhd G$. The existence of a normal Hall subgroup of order m can be determined by examining $n_r(G)$.

Theorem 3.28. *Let G be a finite group of order mr, where $(m, r) = 1$. Then G has a normal Hall subgroup of order m if and only if*

$$n_r(G) = (r - 1)m.$$

Proof. Note that since m and r are coprime, an element $x \in G$ is an rth power if and only if $o(x)$ divides m. Hence $\mathcal{N}_r(G)$ consists precisely of those elements whose order does not divide m.

Suppose that G has a normal Hall subgroup of order m. Then there are exactly m elements in G with order dividing m. Equivalently, there are exactly $|G| - m = (r-1)m$ elements of G with order not dividing m. These $(r-1)m$ elements of G are precisely the elements of $\mathcal{N}_r(G)$.

Now suppose that $n_r(G) = (r-1)m$. Then the number of elements in G with order dividing m is exactly m and by the Frobenuis solution theorem we see that G has a normal Hall subgroup of order m. □

The next few results serve as observations that will help us obtain information about subgroups of G from the sequence $(n_k(G))$.

Lemma 3.29. *Let G be a finite group with exponent e. Then the sequence $(n_k(G))$ is periodic of period e. Further, $n_k(G) \leq |G| - 1$ with equality if and only if e divides k.*

Proof. Since $x^{k+e} = x^k$ for all $x \in G$ and all positive integers k, we see that $G^k = G^{k+e}$ and therefore $n_k(G) = n_{k+e}(G)$ for all k. It follows that the sequence $(n_k(G))$ is periodic with period at most e.

Let k be arbitrary with $k > 0$. As $n_k(G) = |G| - |G^k|$ and $1 \in G^k$ for all k, we have that $n_k(G)$ is at most $|G| - 1$. Equality holds if and only if $x^k = 1$ for all $x \in G$; that is, if e divides k. This shows that $|G| - 1$ is a value in the sequence $(n_k(G))$ that does not appear in the sequence until $k = e$; hence the period of the sequence is at least e. □

A direct consequence of Lemma 3.29 is that $|G|$ is determined both by $(n_k(G))$ and $\{n_k(G)\}$. The sequence $(n_k(G))$ also determines the exponent of G.

Corollary 3.30. *If H is a finite cyclic group, then $(n_k(H)) = (n_k(G))$ if and only if G is isomorphic to H.*

Proof. If G is isomorphic to H then it is clear that $(n_k(H)) = (n_k(G))$. Both $|G|$ and the exponent of G are determined from $(n_k(G))$, by Lemma 3.29, we have the converse. □

Although the period of $(n_k(G))$ is the exponent of G by Lemma 3.29, there are some values of $(n_k(G))$ that repeat earlier in the sequence, as shown in our next lemma.

Lemma 3.31. *Suppose G is a finite group of exponent e. Then $G^k = G^{(k,e)}$ for all $k \in \mathbb{N}$.*

Proof. Let $k \in \mathbb{N}$ be arbitrary, and write $d = (k, e)$. First, suppose $g \in G^k$, so that $g = x^k$ for some $x \in G$. As d divides k, there exists a positive integer q for which $k = qd$, and it follows that $g = x^k = x^{qd} = (x^q)^d$. This shows that $g \in G^d$, and therefore $G^k \subseteq G^d$.

Now suppose that $g \in G^d$, so that $g = x^d$ for some $x \in G$. Write $d = sk + et$, where $s, t \in \mathbb{Z}$. We compute that

$$g = x^d = x^{sk+et} = (x^s)^k (x^e)^t = (x^s)^k \ ,$$

where the ultimate equality follows from the fact that e is the exponent of G. We conclude that $g \in G^k$, establishing that $G^d \subseteq G^k$. □

Returning to Theorem 3.28, we note that in general $(n_k(G))$ cannot determine the isomorphism type of a Hall m-subgroup of G. However, some properties of a Hall subgroup of G can be determined from $(n_k(G))$. These next results discuss the relationship between $(n_k(G))$ and Sylow subgroups of G.

Lemma 3.32. *Let G be a finite group with p prime. If G has a normal nontrivial Sylow p-subgroup P, then $(n_k(G))$ determines the sequence $(n_k(P))$.*

Proof. Write $|G| = p^a r$ where $(p, r) = 1$. Let $q = p^j$ for some $j \leq a$. We claim that $g \in G^{qr}$ if and only if $g \in P^q$. To see this, first suppose $g \in G^{qr}$, so that there exists some $x \in G$ for which $g = x^{qr}$. We claim that $x^r \in P$ and hence $g = (x^r)^q$ belongs to P^q. To see this, note that $(x^r)^{p^a} = x^{p^a r} = 1$, and therefore $o(x^r)$ is a p-power. It follows that x^r belongs to the unique Sylow p-subgroup of G and that g belongs to P^q. Conversely, suppose $g \in P^q$. Because $q = (q, qr)$, Lemma 3.31 implies that $P^q = P^{qr}$. As $P^{qr} \subseteq G^{qr}$, the converse is established.

Finally, we establish that $(n_k(P))$ is determined by $(n_k(G))$. Let i be an arbitrary positive integer and let q be the p-part of i. As $n_i(P) = n_q(P)$ by Lemma 3.31, it is without loss that we assume that i is a power of p. Now $n_q(P) = |P| - |P^q|$, and we claim that both $|P|$ and $|P^q|$ are determined by $(n_k(G))$. By the previous paragraph, $|P^q| = |G^{qr}|$, and $|G^{qr}| = |G| - n_{qr}(G)$. It follows from Lemma 3.29 that $|G|$ and therefore $|P|$ can be determined from $(n_k(G))$, and the result holds. □

Lemma 3.33. *Let G be a finite nonabelian nilpotent group of odd order with nilpotency class 2. Then there is an abelian group H such that $(n_k(G)) = (n_k(H))$ and $G(d) = H(d)$ for all d.*

Proof. This follows immediately from the Baer trick, see Isaacs [48, **4.37**]. □

The lemma above together with Theorem 3.35 gives the following corollary:

Corollary 3.34. *Let G be a finite nilpotent group of odd order with nilpotency class 2. Then the set $\{n_k(G)\}$ determines both $(n_k(G))$ and $G(d)$ for all d.*

We conclude by mentioning the following theorem from the authors work with Sara Jensen [20].

Theorem 3.35. *[20, Theorem C] Suppose G and H are abelian groups. Then the sets $\{n_k(G)\}$ and $\{n_k(H)\}$ are equal if and only if G and H are isomorphic.*

A few remarks about Theorem 3.35 are in order. It should be noted that D_8 and Q_8 are groups with $n_k(D_8) = n_k(Q_8)$ for all positive integers k, so Theorem 3.35 cannot be improved to yield the same result under the assumption that G and H are nilpotent. Similarly, $G = C_4 \times C_2$ satisfies $n_k(G) = n_k(D_8)$ for all positive integers k, so knowing that G is abelian and $n_k(H) = n_k(G)$ for all k does not imply that H is abelian.

Chapter 4

The Not Solutions of a Word.

In this chapter we examine a sort of dual to Theorem A. The work in this chapter is joint work with Sara Jensen [19]. In Chapter 3 we showed that for a power word w the number of elements of a group G not contained in $w(G)$ can be used to bound $|G|$. However, the order of $w(G)$ can always be arbitrarily small compared to $|G|$. Another property of the word map w of interest is the number of solutions to w, i.e., the number of $g \in G$ such that $w(g) = 1$. It turns out that this number can also be made arbitrarily small compared to $|G|$.

Example 4.1. Let $w = x^k$. Consider the group $G = C_k \times H$ where H has order coprime to k. Then there are exactly k elements of G that are solutions to w. In particular, for any group of odd order, the number of solutions to $x^2 = 1$ is always 1.

Much like the case for the image of w, i.e., $w(G)$, it turns out that the number of not solutions to w, i.e., the number of $g \in G$ such that $w(g) \neq 1$ can be used to bound the order of G.

Theorem B. *[19, Theorem A] Let G be a group, and let w be a word. Let*

$$k = |\{(g_1, \ldots, g_n) : w(g_1, \ldots, g_n) \neq 1\}|.$$

If $k > 0$, then $|G| \leq 2k^2$. Moreover, if $n > 1$, then $|G| \leq k^2$. In particular if k is finite, then G is finite.

Note that Theorem B differs from Theorem A in two strong ways. First, the hypotheses of Theorem B hold for any word G. Second, as long as k is finite, we do not need to presuppose a finite-like condition on G to bound the order of G. We will show that the bound in Theorem B is obtained by infinitely many groups G for appropriate words w.

4.1 History of the not solutions of word maps.

Our Theorem B was motivated by work on the the number of elements of maximal order in a group and some well-known results about the probability that two elements of a group commute. The author and Geetha Venkataraman showed the following somewhat surprising result [21]. Consider a group G with finite exponent and let m be the largest order of an element of G. Then one of the follow holds:

- There are infinitely elements in G of order m.
- The group G is finite.

In our notation, the result above says that if x^m has only finitely many not-solutions in G then G is finite. More famously, if $w = [x, y]$ then the number k of not solutions to w in a group G, if nonzero, bounds the order of G by

$$|G|^2 \leq \frac{8k}{3}.$$

A similar bound is known when $w = x^2$. Let k be the number of not solutions to w in a group G, then

$$|G| \leq 4k.$$

Less well-known is the case when $w = x^3$. Let k be the number of not solutions to w in a group G, then Laffey has shown the following bound [58, 57].

$$|G| \leq \frac{9k}{2}.$$

Returning to the case $w = x^2$ we see an interesting connection between the study of word maps and the study of other functions on a group. Tărnăuceanu in [100] first considered the following problem, which appears seemingly unrelated to word maps. Let $C(G)$ denote the set of cyclic subgroups of G, and let $\Delta(G) = |G| - |C(G)|$. Can all groups with $\Delta(G) = d$ be classified? In [100] and [101], Tărnăuceanu classified all groups that occur when d is 1 and 2. Belshoff, Dillstrom, and Reid were able to extend this result to classify all groups that have $\Delta(G)$ as $3, 4$, and 5 in [8]. A later addendum to [8] by Belshoff, Dillstrom, and Reid showed that if $\delta = \Delta(G)$ then $|G| \leq 8\delta$, allowing them to use GAP to classify all groups with $\Delta(G)$ values in the range of 1 to 32. We present our proof of their result now.

Theorem 4.2. *Let G be a finite group with $\Delta(G) = \delta$. Then $|G| \leq 8\delta$.*

Proof. We want to count the number of cyclic subgroups of G by taking a weighted sum over elements of G. For any $g \in G$, assign the weight $\frac{1}{\varphi(o(g))}$, i.e., the number of generators of $\langle g \rangle$. Then

$$\sum_{g \in G} \frac{1}{\varphi(o(g))} = |C(G)|,$$

and

$$\sum_{g \in G} 1 - \frac{1}{\varphi(o(g))} = |G| - |C(G)| = \delta.$$

The only elements in g with $\varphi(o(g)) = 1$ are solutions to the equation $x^2 = 1$ in G. Let $X = \{g \in G : g^2 = 1.\}$. Then $\sum_{g \in G \setminus X} 1 - \frac{1}{\varphi(o(g))} = \delta$ and we conclude that $|G| - |X| \leq 2\delta$, i.e., that the number of elements of G that do not satisfy $g^2 = 1$ is at most 2δ. By the result above about not solutions to the word x^2, we conclude that $|G| \leq 8\delta$. □

In [19], we extrapolate the relationship between $\Delta(G)$ and the map x^2 to obtain the following theorem.

Theorem 4.3. *[19] Suppose G is a finite group with $\delta = \Delta(G)$, where $\delta \geq 1$. Suppose further that $|G| = 2^n \cdot m$ where $(2, m) = 1$ and $m > 1$. Then one of the following holds.*

(a) If $|G| = 6\delta$ then $m = 3$ and $G \cong S_3 \times E$ where E is an elementary abelian 2-group of order 2^{n-1}.

(b) If $m \geq 5$, then $|G| \leq 5\delta$.

We note that Edmonds proves something similar to our part (a) above, but the proof involves many different case analyses [23]. Our proof is an independent simplification.

4.2 Proof of Theorem B.

Proof of Theorem B. Consider the set of n-tuples G^n. The group G acts on these tuples diagonally, i.e.,

$$(g_1, \ldots, g_n)^g = (g_1^g, \ldots, g_n^g).$$

(Note we are **acting on the right** so conjugation behaves appropriately.) We see that $w(g_1, \ldots, g_n)^g = w(g_1^g, \ldots, g_n^g)$. Hence if $w(g_1, \ldots, g_n) \neq 1$, then $w(g_1^g, \ldots, g_n^g) \neq 1$. Now

let

$$N = \{(g_1, \ldots, g_n) : w(g_1, \ldots, g_n) \neq 1.\}$$

We can partition N into a number of orbits under the action of G.

Fix $\gamma = (h_1, \ldots, h_n)$ an element of N and let X be its orbit under the action of G. Let G_γ be the stabilizer of γ. Then $|G| = |X| \cdot |G_\gamma|$. By hypothesis we have that $|X| \leq k$. We will show that $|G_\gamma| \leq 2k$.

Let $s \in G_\gamma$. Now $\gamma^s = \gamma$ and we have that $h_i^s = h_i$ for all i. Equivalently s commutes with all of the h_i, we have the equality

$$w(h_1 s, h_2 s, \ldots, h_n s) = w(h_1, \ldots, h_n) w(s, \ldots, s).$$

Since $\gamma \in N$ we know that either $(h_1 s, \ldots, h_n s)$ or $(s, \ldots, s)$ must be in N. We can define a map $f_\gamma : G_\gamma \to N$, where

$$f(s) = \begin{cases} \tilde{s} & \text{if } (s, \ldots, s) \in N \\ (h_1 s, \ldots, h_n s) & \text{otherwise.} \end{cases}$$

Note that the map f is only a map on sets. We will show that for any $\eta \in N$ the fibre $f_\gamma^{-1}(\eta)$ has size at most 2. Suppose that for distinct $s, t \in G_\gamma$ we have that $f_\gamma(s) = f_\gamma(t)$. If $(s, \ldots, s) \in N$, equivalently $f_\gamma(s) = \tilde{s}$, then $f_\gamma(t) = (h_1 t, \ldots, h_n t)$. If $(s, \ldots, s) \notin N$, then $f_\gamma(s) = (h_1 s, \ldots, h_n s)$ and $f_\gamma(t) = (t, \ldots, t)$. Hence, for any $\eta \in N$, the fibre $f_\gamma^{-1}(\eta)$ has size at most 2. We conclude that $|G_\gamma| \leq 2k$. Hence $|G| \leq 2k^2$.

If there is more than one orbit of N under the action of G, then one of orbits has size less than or equal to $k/2$ and we conclude that $|G| \leq k^2$. Assume that $n > 1$ and that we have fixed a $\gamma = (h_1, \ldots, h_n)$ and that N is the orbit of γ under the action of G. Either $\gamma = (h, \ldots, h)$ or for all $s \in G_\gamma$ we have that $(s, \ldots, s) \notin N$. But, if $(s, \ldots, s)$ is

not in N for all $s \in G_\gamma$, then f_γ is bijective and we conclude that $|G_\gamma| \leq k$ and $|G| \leq k^2$. Suppose by way of contradiction that $\gamma = \tilde{h}$ and $n > 1$.

Recall that for any word w, there is an automorphism σ of $\mathbf{F}_n$ such that $\sigma(w) = x^k c$ where $c \in \mathbf{F}_n'$. It must be the case that x^k is a law on G, otherwise

$$w(h, 1, 1, \ldots, 1) = w(h, \ldots, h),$$

but $(h, 1, \ldots, 1)$ is in a different orbit than γ under the action of G. But, then $\sigma(w) = c$ and $c(h, \ldots, h) = 1$; this contradicts the assumption that N was the orbit of γ and that $\gamma = (h, \ldots, h)$. □

We now show that the bound in Theorem B is obtained infinitely often. Let H be the cyclic group of order 2^m. Let G be the holomorph of H, i.e.,

$$G = \mathrm{Hol}(H) = H \rtimes \mathrm{Aut}(H).$$

Then $|G| = 2^m(2^{m-1})$. Let w be the word $x^{2^{m-1}}$. Then there are exactly $k = 2^{m-1}$ tuples in G that are not solutions to w. Hence, $|G| = 2^m k = 2k^2$. This also shows that the bound obtained by the author and Geetha Venkataraman involving the number of elements of maximal order is tight for another infinite family of groups [21, Theorem A]. We examine this bound in section 4.4 as an example of the ideas discussed in section 4.3 below.

4.3 General bounding statements.

Theorems B and A are remarkable similarly in structure. Broadly speaking they have the following form which we will not make precise at this time.

Theorem: Let P be a property of group elements definable by a sentence in the language of groups. Let G be a finite group and let $g \in G$ have property P. If P "propagates" through $\mathbf{C}_G(g)$, then we use the number of elements in G having property P to bound the order of G.

Theorem A does not actually have this form, but a close counterfeit form. In Theorem A, the property of not being in $w(G)$ did not propagate through $\mathbf{C}_G(g)$, instead we showed that on $\mathbf{C}_G(g)$ the map $w(g)$ was many-to-one and hence could not be very surjective. The assumption that very injective and very surjective are correlated depends on some form of finiteness. In contrast, in the proof of Theorem A we actually constructed new elements that were not solutions to the word w.

We give the following toy example of a first order property that can be used to bound the order of G.

Example 4.4. Let G be a group. We say that property P holds on $g \in G$ if and only if $\mathbf{C}_G(g)$ has order 7. Suppose that exactly n elements of G satisfy property P where $0 < n < \infty$. Let $x \in G$ have property P. Then all elements of x^G have property P and hence $|x^G| \leq n$. Moreover, $|\mathbf{C}_G(x)|| = 7$ and thus $|G| = 7n$.

It is easy to construct more complicated, but equally trivial examples. The following section discusses an example that is deeply related to Theorem B, but appeared in previous work of the author and Geetha Venkataraman.

4.4 The number of elements of maximal order in a group.

In this section we present an example of a property of group elements that propagates through the center of G. We note that our example can be viewed as a special case of Theorem B, however we feel the exposition warrants its inclusion. The work in this section was joint work with Geetha Venkataraman and the author wishes to once again thank the Center for South Asia for a travel award in support of this research.

In this note we investigate how the number of elements of maximal order in a group affects the order of the group. We show that if a group has only finitely many elements of maximal order, then the group itself is finite. This is a surprising result: if G is a group and m is the maximal order of an element G, then either there are infinitely many elements of order m, of G is finite. We note that a group with finitely many elements of maximal order cannot have any elements of infinite order, since a group having one element of infinite order must have infinitely many elements of infinite order. Moreover, we then give a few explicit bounds for the order of a group in terms of the number of elements of maximal order. The first of these bounds is attained infinitely often by the holomorphs of cyclic groups of prime order, i.e., $C_p \rtimes C_{p-1}$.

There has been interest in studying groups with a certain fixed number of elements of maximal order; for example, see [11, 38, 39, 40, 52, 102]. These papers investigate the structure of finite groups with a stated number of elements of maximal order, often an explicit integer such as 24 or 42. By Theorem 4.5 below, groups with a fixed number of elements of maximal order are necessarily finite, hence the restriction to finite groups in the titles is superfluous.

For a group G, and $x \in G$, we will denote the order of x as $o(x)$. We will also denote the Euler totient function as $\varphi(n)$. We show the following.

Theorem 4.5. *Let G be a group. If $m = \max\{o(g) : g \in G\}$ is finite, and exactly k elements of G have order m, where $k < \infty$, then G is finite and*

$$|G| \leq \frac{mk^2}{\varphi(m)}.$$

Using the notation of Theorem 4.5, we note that if G has exactly $k < \infty$ elements of maximum order, then there are only finitely many possibilities for m since $\varphi(m)$ divides k. In fact, $k = \varphi(m) \cdot n$, where n is the number of cyclic subgroups of order m in G. For a given k, the set of y where $\varphi(y)$ divides k is bounded, since by using properties of φ one can show that such y cannot be divisible by large primes, or by large powers of smaller primes. We write $\theta(k)$ to denote the largest integer y such that $\varphi(y)$ divides k. We have the following Corollary to Theorem 4.5.

Corollary 4.6. *Let G be a group. If $m = \max\{o(g) : g \in G\}$ is finite, and exactly k elements of G have order m, where $k < \infty$, then G is finite and*

$$|G| \leq \theta(k)k^2.$$

Proof. Since $\varphi(m)$ divides k, we have that $m \leq \theta(k)$. Hence Theorem 4.5 implies

$$|G| \leq \frac{mk^2}{\varphi(m)} \leq mk^2 \leq \theta(k)k^2.$$

□

As part of our proof of Theorem 4.5 we will show the following.

Theorem 4.7. *Let G be a group and let*

$$X = \{x : x \in G \text{ and } o(x) < \infty\}.$$

Suppose that $m = \max\{o(x) : x \in X\}$ is finite and exactly k elements of G have order m, where $k < \infty$. Suppose for some $g \in Z(G)$, we have that $o(g) = m$. Then X is a finite characteristic subgroup of G and

$$|X| \leq \frac{mk}{\varphi(m)}.$$

The proof of Theorem 4.7 will utilize a theorem of Dietzmann's. Dietzmann showed that given a group G and a finite subset X of G, if every element of X has finite order and X is closed under conjugation, then $\langle X \rangle$ is finite.

4.4.1 Proofs of Theorems 4.5 and 4.7.

In general, "x has order n" is not a well-behaved property on a group G because the order function behaves very erratically. For example, knowing $o(x)$ and $o(y)$ tells us nothing about $o(xy)$. Even when x and y commute, the order of the product is not determined. Recall the following lemma.

Lemma 4.8. *Let G be a group and n and m be positive integers. For $x, y \in G$, if $o(x) = n$, $o(y) = m$, and x and y commute, then there is an element of $\langle x, y \rangle$ with order equal to the least common multiple of m and n.*

Proof. Let d be the least common multiple of m and n. For a prime p, if p^e is the largest power of p that divides d, then p^e divides either m or n. Hence the abelian group $\langle x, y \rangle$ has an element of order p^e. The product of these elements for the various primes dividing d will have order d. □

Hence, for a group G, if $x \in G$ has maximal order, and $y \in G$ commutes with x, then $o(y)$ must divide $o(x)$. In this sense, "having maximal order" is a very well-behaved property as demonstrated below.

Lemma 4.9. *Let G be a group, and m and n be positive integers such that n divides m. Let $x, y \in G$ such that $o(x) = m$ and $o(y) = n$, and x and y commute. Write $X = \langle x \rangle$ and $Y = \langle y \rangle$. Then the coset Xy has at least $\varphi(m)$ elements of order m. Hence $H = XY$ has at least $\varphi(m)t$ elements of order m, where $t = |Y : X \cap Y|$.*

Proof. We will show that X has a complement in the abelian group H. It suffices to show for each prime p that the Sylow p-subgroup of X has a complement in the Sylow p-subgroup of H. Let p be a prime dividing $|H|$. Let P be the Sylow p-subgroup of X and let S be the Sylow p-subgroup of H. To show that P has a complement in S, we appeal to the following result used in one of the standard proofs of the fundamental theorem of finite abelian groups (see, for example, **7.12** of [49]), i.e., in an abelian group a cyclic subgroup of maximal possible order has a complement. Since n divides m, P is a cyclic subgroup of maximal order in S, and we conclude that P has a complement in S. Since X is a direct product of its Sylow p-subgroups, all of which have a complement in H, we conclude that X has a complement in H.

Hence H is of the form $X \times K$ for some subgroup K in H of order t. It follows that the coset Xy has at least $\varphi(m)$ elements of order m. □

Note: In the notation of Lemma 4.9, it is **not necessarily the case** that the element xy has order m. Consider, $C_6 \times C_2$ where $C_6 = \langle a \rangle$ and $C_2 = \langle b \rangle$, and let $x = (a^2, b)$ and $y = (1, b)$. So $o(x) = 6$ and $o(y) = 2$, but $o(xy) = 3$. However, $o(x^2y) = 6$.

Our proof of Theorem 4.7 will use a remarkable theorem of Dietzmann.

Theorem 4.10 (Dietzmann)**.** *Let G be a group, and let $X = \{x_1, \ldots, x_k\}$ be a finite subset of G that is closed under conjugation. If there is a positive integer n such that $x^n = 1$ for all $x \in X$, then $\langle X \rangle$ is a finite subgroup of G.*

Dietzmann's theorem appears as Exercise 6.15 in Lam [59] and Theorem 5.10 in Isaacs [48]. The theorem follows since any product of at least $(n-1)|X| + 1$ elements of X is equal to a product of a smaller number of elements of X. Hence, the subgroup generated by X has bounded size. Note that any product of elements of X can be conjugated by an element of X and remains a product of elements of X. Hence, if a product of elements of X contains n copies of the same element, conjugating the product can allow one to combine and eliminate them, since $x^n = 1$ for all $x \in X$.

We now prove Theorem 4.7.

Proof. Let $Z = \langle g \rangle$. We note that Z acts by multiplication on X, so X is a disjoint union of $|X|/m$ distinct cosets of Z. Since g has maximal order in X and is central, every element of X has order dividing m. By Lemma 4.9, every coset of Z contains at least $\varphi(m)$ elements of order m. Hence X contains at least $\frac{|X|}{m}\varphi(m)$ elements of order m, and so

$$k \geq \frac{|X|\varphi(m)}{m}.$$

Since m is finite, every element x of X satisfies $x^{m!} = 1$. We also know that X is closed under conjugation and, from above, finite. Applying Dietzmann's theorem shows that $\langle X \rangle$ is a finite subgroup of G. As the set of torsion elements of G, we see that X is in fact a characteristic subgroup of G. □

We now prove Theorem 4.5.

Proof. The group G must be a torsion group with m being the maximum order of any element of G.

Let $g \in G$ have order m. Write $C = \mathbf{C}_G(g)$. Since every conjugate of g has order m, we have that $|g^G| \leq k$. Applying Theorem 4.7 to the group C, if follows that

$$|G| = |g^G| \cdot |C| \leq k|C| \leq k\left(\frac{mk}{\varphi(m)}\right).$$

□

As mentioned at the end of section 4.2 the bound in Theorem 4.5 is sharp and obtained infinitely often.

Chapter 5

Chirality in word maps.

The material in this chapter is joint work with Turbo Ho [16].

In this chapter we consider subsets of a group that arise as the realizations of a word. The most famous example of such a subset is the set of commutators $[x, y]$, the realizations of the word $x^{-1}y^{-1}xy$, within a group. It is a basic property of commutators that $[x, y]^{-1} = [y, x]$, and hence the set of commutators in any group G is closed under inverses in G. We investigate groups and words whose corresponding sets are not closed under inversion.

In Segal's *Words* [95] the set $w(G)$ has a slightly different definition than the one we use. Segal sets $w(G)$ to be the image of the map w together with the image of the map w^{-1}.We **do not** assume that $w(G)$ is closed under inverses and instead we investigate the following property:

Definition 5.1. A pair (G, w), where G is a group and w is a word, is called *chiral* if $w(G) \neq w^{-1}(G)$. Equivalently, the pair $w(G)$ is chiral if the set $w(G)^{-1}$, the inverses of elements of $w(G)$, does not equal $w(G)$. We say G is *chiral* if $w(G)$ is chiral for some w. Otherwise G is *achiral*. We say $x \in G$ witnesses the chirality of G if $x \in w(G)$ and $x^{-1} \notin w(G)$ for some w.

The existence of chiral groups can be shown from a result of Lubotzky [69]: In a finite simple group G the images of word maps are exactly the subsets of G closed under

automorphisms and containing the identity. Consider $G = M_{11}$, the Mathieu group of order 7920. G is chiral since an element of order 11 is not conjugate to its inverse and $\mathrm{Out}(G)$ is trivial. Using Lubotzky's result, it is easy to verify that M_{11} is the smallest chiral simple group. In section 5.5 we present a calculation giving an explicit example of a word w that witnesses the chirality of M_{11}; we also show the existence of a weakly chiral group that is not chiral, answering a question of Gordeev et. al. [30] inspired by the chirality of M_{11}.

In this chapter we begin the process of classifying all finite chiral groups. We will prove

Theorem C. *[16, Theorem A] The only chiral groups with order less than 108 are SmallGroups* $(63, 1)$ *and* $(80, 3)$*.*

Theorem D. *[16, Theorem C] The free nilpotent groups of class* ≥ 3 *is chiral and the free nilpotent groups of rank 3 and class 2 is achiral.*

Section 5.1 demonstrates how structural information about a group can force achirality of the group; for example finite Frobenius groups with abelian kernel and achiral complement are achiral.

In section 5.2 we recall an algorithm of Neumann [83], for constructing all word maps on a finite group with a given number of variables. We prove the following theorem:

Theorem 5.2. *If a group G is generated by d elements, then G is chiral if and only if there is a word w on d variables such that (G, w) is chiral.*

Hence the chirality of a finite group is recursive. In section 5.3 we give an explicit infinite family of pairs of finite groups and words that have no nontrivial chiral quotient

groups. Interestingly both chiral groups in Theorem C are in this infinite family. In section 5.4 we turn our attention to nilpotent groups and prove Theorem D.

5.1 Properties of Chirality.

Most of our results about achirality come from the following line of reasoning: a group G is chiral if and only if there is a word w such that (G, w) is chiral. (G, w) is chiral if and only if some element $x \in G$ that witnesses the chirality of (G, w). If no element x can be a witness of the chirality of (G, w) for any w, then G is achiral.

For a group G, and $x, y \in G$ we say x is *automorphic* to y if there is an automorphism σ of G such that $\sigma(x) = y$. We likewise will say that x is homomorphic to y if there is a homomorphism ϕ from G to G such that $\phi(x) = y$. Clearly, an element $x \in G$ cannot be a witness to chirality if x is homomorphic to x^{-1}. This gives us the following simple observation:

Lemma 5.3. *Let G be a group with the property that for every $x \in G$ there is a ϕ, a homomorphism of G (dependent on x), such that $\phi(x) = x^{-1}$. Then G is achiral.*

The following lemmas will be useful in developing a computational test for chirality. The first lemma shows that $w(G)$ depends only on the equivalence class of w via automorphisms in a free group containing w. This lemma was first observed via examples using the automated proof software Prover9 [77]. Using Prover9 the authors found automorphisms taking the 2-Engel word $[x, y, y]$ and the 3-Engel word $[x, y, y, y]$ to their inverses respectively, thus showing that the images of maps associated with each of them are closed under inversion in all groups. For n greater than 3, we do not know whether the image of the n-Engel word is closed under inversion for all groups.

It is worth noting that for a $w \in \mathbf{F}_n$, $w(G) = w^{-1}(G)$ for all groups G if and only if there is a *homomorphism* of $\mathbf{F}_n$ taking w to w^{-1}. However, we do not know if it is necessary that there is an automorphism in this case.

We can use Nielsen transformations to show that for a group G and a word w (G, w) is chiral if and only if (G, v) is chiral for a word v of specified form:

Theorem 5.4. *A group G with exponent e is chiral if and only if (G, w) is chiral for some word $w = x^k c$ where k divides e and c is a product of commutators.*

Proof. Let $\sigma \in \mathrm{Aut}(\mathbf{F}_n)$. Then $w(G) = \sigma(w(G))$. Since w is automorphic to a word of the $x^d c$ where $c \in \mathbf{F}'_n$, we see that over G, w is automorphic to a word map of the form $x^k c$ where k has the desired form. □

We will use the above theorem to prove the following:

Corollary 5.5. *Let G be a group with finite exponent e. Let G^k be the set of kth powers in G. If for every k dividing e, every element of $G^k G' \setminus G^k$ is not a witness of chirality, then G is achiral.*

Proof. Consider a word w of the form $x^k c$. Clearly, the image of w is inside $G^k G'$. Suppose by way of contradiction that (G, w) is chiral as witnessed by $g \in G$. Then $g \in G^k G'$ and by hypothesis $g \in G^k$. Let $g = h^k$ for some $h \in G$. Hence $w(h, 1, \ldots, 1) = g$. But, then $g^{-1} = h^{-k}$ and $w(h^{-1}, 1, \ldots, 1) = g^{-1}$, contradicting g as a witness to the chirality of (G, w). Therefore G is achiral. □

The next few results show how the structure of a group G limits the potential witnesses to the chirality of G.

Lemma 5.6. *Let N be an abelian group. Suppose another group H acts on N via automorphisms and consider $G = N \rtimes H$. Then there is an automorphism of G that acts as inversion on N and fixes H pointwise.*

Proof. Let σ be a set map that inverts N and fixes H point-wise. We will show that σ is a homomorphism of G. We will denote the action of h on n via n^h. Let $n, m \in N$ and $h, j \in H$ then

$$\begin{aligned}(nhmj)^\sigma &= (nm^{h^{-1}}hj)^\sigma \\ &= (m^{h^{-1}})^{-1}n^{-1}hj \\ &= n^{-1}hm^{-1}j \\ &= (nh)^\sigma(mj)^\sigma.\end{aligned}$$

Hence σ is a homomorphism. It is clearly surjective and injective, thus an automorphism. □

Lemma 5.7. *Let G be a group with a normal subgroup N, such that N is complemented in G by H. Let w be a word on d variables. Suppose $w(g_1, \ldots, g_d) = h \in H$ for some $g_1, \ldots, g_d \in G$. Write $g_i = n_i h_i$. Then $w(h_1, \ldots, h_d) = h$.*

Proof. By considering the action of H on N, $w(g_1, \ldots, g_d)$ can be written as $n \cdot w(h_1, \ldots, h_d)$ for some $n \in N$. Since $N \cap H = 1$ we conclude that $n = 1$ and $w(h_1, \ldots, h_d) = h$. □

Corollary 5.8. *Let N and H be groups and $G = N \rtimes H$. If H is achiral, then no element of H can witness the chirality of G.*

Proof. For a group $G = N \rtimes H$, $h \in H$ is a witness to the chirality of (G, w) if and only if $h \in H$ is a witness to the chirality of (H, w). □

Theorem 5.9. *Let N be an abelian group and H be an achiral group with $G = N \rtimes H$. No witness of the chirality of G can be automorphic to an element of N or H.*

Proof. From Lemma 5.6 there is an automorphism σ of G that acts as inversion on N and fixes H. If $g \in G$ is automorphic to an element of N, then g is automorphic to its own inverse, and thus not a witness to the chirality of G.

Corollary 5.8 states that no element of H can witness the chirality of (G, w), and hence there are no witnesses of the chirality of G automorphic to an element of H. □

We have the immediate corolloary:

Corollary 5.10. *Let N be an abelian group and H be an achiral group with $G = N \rtimes H$. If every element of G is automorphic to an element of either N or H, then G is achiral.*

5.2 The Computability of Chirality.

We will give an algorithm that determines if a given finite group is chiral. As part of our algorithm, we will calculate for all words on some specified number of variables all of the sets $w(G)$; this part of our algorithm is similar to an algorithm originally discovered by Neumann in [83]. We start by proving the following lemma, which says that the chirality of a finitely generated group is only dependent on words of a given number of variables.

Lemma 5.11. *If a group G is generated by d elements, then G is chiral if and only if there is a word w on d variables such that (G, w) is chiral.*

Proof. We need only to show that if G is chiral, then there is a word w on d variables that witnesses the chirality of G.

Fix a generating set $g_1, g_2, \ldots, g_d$ of G, and fix d-variables words $u_1, u_2, \ldots, u_{|G|}$, such that $u_i(\overline{g})$ enumerates G. Let v be a word with k variables. Then

$$v(u_{i_1}, u_{i_2}, \ldots, u_{i_k})(G^{(d)}) \subseteq v(G^{(k)}).$$

On the other hand, every k-tuple from G can be written as $(u_{i_1}(\overline{g}), \ldots, u_{i_k}(\overline{g}))$, so we have

$$\bigcup_{1 \leq i_j \leq |G|} v(u_{i_1}, u_{i_2}, \ldots, u_{i_k})(G^{(d)}) = v(G^{(k)})$$

Now, if (G, v) is chiral, then $v(G^{(k)})$ is not closed under inverse for some v, thus there are some $\overline{i}$ such that $w = v(u_{i_1}, u_{i_2}, \ldots, u_{i_k})$ witnesses the chirality of G. □

To check chirality, it suffices to check the d-variable words. We are now ready to state our variant of Neumann's algorithm:

Theorem 5.12. *There is an algorithm, when given a finite group as input, outputs whether G is chiral.*

Proof. Let G be d-generated. We first build the Cayley graph of $\mathbf{F}_d(G)$. For a vertex with label w, a word in $\mathbf{F}_d$, there is an outward edge labeled x_i that connects to a vertex labeled by the word map wx_i. We then check if this (as a map) is equal to some existing vertex. For every existing vertex, the check is finite since the group is finite, and there are only finitely many existing vertices. This process terminates since $\mathbf{F}_d(G)$, being a subgroup of $G^{(d)}$, is finite. Now for each vertex, we check if the (finite) image of the map is chiral. If it is chiral for any word map, we return *chiral*, otherwise we return *achiral*. □

This construction is actually related to the theory of varieties of groups.

Note that this also shows once again that for a finite group G, $\mathbf{F}_d(G)$ is finite, since $\mathbf{F}_d(G) \subseteq G^{(d)}$ is finite. Furthermore, the algorithm actually builds the group $\mathbf{F}_d(G)$, and in particular, enumerates all the d-variable laws satisfied by G. In [83], it was pointed out that this can be used to find all laws satisfied by G with a bounded number of variables, but does not give a finite process to find *all* laws. In our case, since chirality can be reduced to a property on words with a bounded number of variables, it suffices to stop at a finite stage, hence yielding an algorithm.

In practice, Neumann's algorithm and our implementation of it are time and memory intensive and do not yield a practical method for determining if a finite group is chiral. For example, $\mathbf{F}_2(S_3)$ has order 972. By Theorem I we see that if G is $C_5 \rtimes C_4$, where the action is faithful, then

$$|\mathbf{F}_2(G) = 122070317250000.|$$

As this section contained an algorithm to determine whether a finite group G is chiral, we present an interesting variation of chirality below. We will say that a word w is chiral if there is some group for which (G, w) is chiral. The chirality of a word is decidable, i.e., there is an algorithm, when input a word, outputs whether the word is chiral or not. Indeed, Given a word w, the word is chiral if and only if it is chiral in some free group, which is equivalent to saying the free group does not satisfy the first-order sentence $\forall\overline{x}\exists\overline{y}w(\overline{x})\cdot w(\overline{y}) = 1$. This is a sentence in the positive theory of the free group, which coincides for all nonabelian free groups [78] and is decidable [74].

5.3 An Infinite Family of Minimal Chiral Groups.

We first note that achirality is preserved under quotienting:

Lemma 5.13. *Let H be a homomorphic image of G. If H is chiral, then G is also chiral.*

Proof. Let ϕ be the epimorphism taking G onto H. Let w be a word witnessing the chirality of H, i.e. there is $h \in w(H)$ with $h^{-1} \notin w(H)$. Suppose $w(\overline{y}) = h$ for $\overline{y} \in H$. Let $\overline{x} \in G$ be such that $\phi(\overline{x}) = \overline{y}$, and we have $\phi(w(\overline{x})) = h$. Write $g = w(\overline{x})$.

Now we claim that $g^{-1} \notin w(G)$. If not, let $w(\overline{x}') = g^{-1}$. Then $h^{-1} = \phi(g^{-1}) = \phi(w(\overline{x}')) = w(\phi(\overline{x}')) \in w(H)$, a contradiction. Thus G is also achiral as witnessed by w and g. □

Hence a classification of all finite chiral groups depends only on classifying those that do not have a proper chiral quotient. We call such groups *minimal chiral*. The next theorem shows the existence of an infinite family of minimal chiral groups. Moreover, both SmallGroup(63,1) and SmallGroup(80,3) are part of in this family.

Lemma 5.14. *Let p and q be primes. Let $\mathbb{Z}_p$ act on $\mathbb{Z}_q$ by multiplication by ϕ, and assume that ϕ has order p and $\phi - 1$, $\phi + 1$ are both coprime to q. Then for $p \mid r$, the group $\mathbb{Z}_q \rtimes \mathbb{Z}_{pr}$, where the action is multiplying by ϕ, is chiral as witnessed by the word $w = a^p[a, b][a^{-1}, b]^\phi$.*

Proof. Write $a = (x, n)$ and $b = (y, m)$ in $\mathbb{Z}_{pr} \ltimes \mathbb{Z}_q$. We compute:

$$a^p = (px, n + \phi^x n + \cdots + \phi^{x(p-1)} n)$$

$$[a, b] = (0, -n - \phi^x m + \phi^y n + m)$$

$$[a^{-1}, b] = (0, \phi^{-x} n - \phi^{-x} m - \phi^{y-x} n + m)$$

Note that when $x = 1$, $a^p = (p, 0)$ since $\gcd(\phi - 1, q) = 1$ implies $1 + \phi + \cdots + \phi^{p-1} \equiv 0(q)$.

Note that the first coordinate of w is p if and only if $px = p(pr)$, thus $x = 1(r)$. Note that $\phi^r = 1(q)$ since the action has order $p \mid r$. Thus, when $x = 1(r)$, we have:

$$a^p = (p, 0)$$

$$[a, b] = (0, -n - \phi m + \phi^y n + m)$$

$$[a^{-1}, b] = (0, \phi^{-1} n - \phi^{-1} m - \phi^{y-1} n + m)$$

Thus, $a^p[a, b][a^{-1}, b]^\phi = (p, 0)$ if the first coordinate is p.

Now consider when the first coordinate is $-p$. Again, this happens if and only if $x = -1(r)$. We again compute:

$$a^p = (-p, 0)$$

$$[a, b] = (0, -n - \phi^{-1} m + \phi^y n + m)$$

$$[a^{-1}, b] = (0, \phi n - \phi m - \phi^{y+1} n + m)$$

And

$$\begin{aligned} a^p[a, b][a^{-1}, b]^\phi &= (-p, -n - \phi^{-1} m + \phi^y n + m + \phi^2 n - \phi^2 m - \phi^{y+2} n + \phi m) \\ &= (-p, (\phi + 1)(\phi - 1)(1 - \phi^y) n + (1 + \phi)(1 - \phi)(1 - \phi^{-1}) m) \end{aligned}$$

Since $\phi - 1$ and $\phi + 1$ are both coprime to q, as n, m, y ranges over various values, this ranges over the coset $(-p, 0)C_q$. The inverse of the coset $(-p, 0)C_q$ is $(p, 0)C_q$, but the image of the word does not include any elements of the form $(p, 0)C_q$ except for $(p, 0)$. Therefore, (G, w) is chiral.

□

Hence we have shown that SmallGroup$(63, 1)$ and SmallGroup$(80, 3)$ are achiral. We can now prove Theorem C, i.e., that the only chiral groups with order less than 108 are SmallGroup $(63, 1)$ and SmallGroup $(80, 3)$.

Proof of Theorem C. Recall that any chiral group must have an element $x \in G$ such that $\sigma(x) \neq x^{-1}$ for all automorphisms σ of G. There are only 44 groups with this property of order less than 108. Of those 44 groups, only SmallGroup $(63, 1)$, SmallGroup$(80, 3)$, and SmallGroup$(81, 10)$ are not shown to be achiral by Corollary 5.5 as tested using Magma [9]. From the above we know that SmallGroup$(63, 1)$ and smallGroup$(80, 3)$ are chiral.

To show that SmallGroup$(81, 10)$ is achiral, we performed a search in Magma over the Mal'cev coordinates of all possible words over SmallGroup(81,10). This is possible, since SmallGroup(81,10) is nilpotent. Any word over SmallGroup(81,10) has a unique Mal'cev coordinate, and there are only finitely many such coordinates. □

5.4 Nilpotent Groups.

It is clear that every abelian group is achiral. In this section we will see that there are chiral nilpotent groups and prove Theorem D.

Lemma 5.15. *A reduced free group G is achiral if and only if every element is homomorphic to its inverse.*

Proof. Suppose first every element in G is homomorphic to its inverse. Then if $g \in w(G)$ for some word map w and $g \in G$, we have $w(\overline{a}) = g$ for some $\overline{a} \in G$ and the homomorphism ϕ sending g to g^{-1} gives $w(\phi(\overline{a})) = g^{-1}$, so $g^{-1} \in w(G)$. Thus G is achiral.

Now suppose G is achiral and let $g \in G$. Fix a generating set S of G and write g as a word w in S. Considering w as a word map, we see $g \in w(G)$ by evaluating on S. By achirality of G, we have $g^{-1} \in w(G)$, say by evaluating on T. Consider the map that

maps elements of S to corresponding elements of T. Since G is a reduced free group, this map can be extended to an homomorphism on G, and it maps g to g^{-1}. □

Theorem 5.16. *The class 2 rank 3 free nilpotent group $N = N_{2,3}$ is achiral. As a result, every class 2 rank 3 nilpotent group is achiral.*

Proof. Write the generators of N to be a, b, c and the commutators to be $d = [a, b]$, $e = [a, c]$, $f = [b, c]$. Since every element in N is automorphic to some element of the form $a^*d^*e^*f^*$, it suffices to show that elements of this form is homomorphic to its inverse.

Fix $g = a^i d^j e^k f^l \in N$. Consider the homomorphism ϕ with $\phi(a) = a^{-1}$, $\phi(b) = b^x c^y$, and $\phi(c) = b^z c^w$. We have $\phi(d) = d^{-x}e^{-y}$, $\phi(e) = d^{-z}e^{-w}$, and $\phi(f) = f^{xw-zy}$. Thus, to have $\phi(g) = g^{-1}$, we need

$$a^{-i}d^{-j}e^{-k}f^{-l} = (a^{-1})^i(d^{-x}e^{-y})^j(d^{-z}e^{-w})^k(f^{xw-zy})^l,$$

which is equivalent to the following system of equations:

$$\begin{cases} xj + zk = j \\ yj + wk = k \\ xw - zy = -1. \end{cases}$$

However, this is again equivalent to finding an integer matrix $M = \begin{pmatrix} x & z \\ y & w \end{pmatrix}$ such that its determinant is -1 and the vector $\begin{pmatrix} j \\ k \end{pmatrix}$ is its eigenvector with eigenvalue 1. This matrix can be found by starting with the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and do a change of bases such that

$(\gcd(j,k),0)$ gets mapped to (j,k). Thus, we see that every $g \in N$ is homomorphic to its inverse, and thus N is achiral by the previous lemma.

□

Theorem 5.17. *Let $N_{3,2} = \langle a, b\rangle$ be the free nilpotent group of class 3, rank 2, and let $c = [a,b]$, $d = [c,a]$, and $e = [c,b]$ be the standard Mal'cev basis of $N_{3,2}$. Then for any odd prime p, the element $g = a^{p^2}c^p d$ is not homomorphic to its inverse. Thus, $N_{3,2}$ is chiral.*

Proof. Suppose ϕ is an automorphism such that $\phi(g) = g^{-1} = a^{-p^2}c^{-p}d^{p^3-1}$. For simplicity, we will use $*$ to denote unknown (possibly different for different $*$'s) integers, and $n*$ to denote integers divisible by n. By considering the power of a in $\phi(g)$, we see $\phi(a)$ must have the form $a^{-1}c^*d^*e^*$. Suppose $\phi(b) = a^*b^xc^*d^*e^*$. Thus, $\phi(c) = c^{-x}d^*e^*$ and $\phi(d) = d^x$.

We then compute

$$\begin{aligned}\phi(g) &= (a^{-1}c^*d^*e^*)^{p^2}(c^{-x}d^*e^*)^p(d^x)\\ &= (a^{-p^2}c^{p^2*}d^{-\frac{p^2(p^2-1)}{2}*+p^2*}e^{p^2*})(c^{-px}d^{p*}e^{p*})(d^x)\\ &= (a^{-p^2}c^{p^2*-px}d^{p*+x}e^{p*})\end{aligned}$$

By considering the exponent of c modulo p^2, we see $-px \equiv -p$ modulo p^2, so $x \equiv 1$ modulo p. However, considering the exponent of d modulo p, we get $x \equiv -1$ modulo p, a contradiction. Thus the theorem follows. □

The previous argument and hence chirality still holds for (finite) quotients of the free nilpotent group with the order of a being infinity or divisible by p^3, order of b being infinity or divisible by p^2, and order of c being infinity or divisible by p.

5.5 Weakly chiral groups and the chirality of M_{11}.

Gordeev et. al. defined the following concept, which they call weakly chiral [30].

Definition 5.18. A group G is weakly chiral, if for some word w and $g \in G$ we have that $0 < \mu_{w,G}(g) < \mu_{w,G}(g^{-1})$. The pair (G, w) is called a weakly chiral pair.

The above definition was motivated by an observation of Elkies that for the Mathieu group of $G = M_{11}$ and the word $w = xy^2xy^3x^3$ the pair (G, w) is weakly chiral, while words v such (G, v) is chiral were unknown [24]. In this section we give a word w so that (M_{11}, w) is a chiral pair. Moreover, we answer a question of Gordeev et. al. by providing an example of a weakly chiral group G that is not chiral.

Theorem 5.19. *Let G be the Mathieu Group M_{11} and let w be the word*

$$[x^{-440}(x^{-440})^{(y^{-440})}x^{-440}, (y^{-440})^{(x^{-440}y^{-440})}y^{-440}].$$

Then $w(G)$ contains an element g such that $o(g) = 11$ and $g^{-1} \notin w(G)$, i.e., the word w witnesses the chirality of G.

Proof. All elements of M_{11} have order either $1, 2, 3, 4, 5, 6, 8$, or 11. For an element g of M_{11} we have

$$g^{-440} = \begin{cases} 1 & \text{if } o(g) \notin \{3, 6\}, \\ g & \text{if } o(g) = 3, \\ g^4 & \text{if } o(g) = 6. \end{cases}$$

If $a \in G$ does not have order 3 or 6, then $w(a, b) = w(1, b) = 1$ for all $a \in G$, since w is a commutator. Similarly, if $b \in G$ does not have order 3 or 6, then $w(a, b) = w(a, 1) = 1$ for all $a \in G$. Moreover, $w(a, b) = w(a^4, b^4)$ for all $a, b \in G$. Hence to determine $w(G)$

we need to determine $w(a, b)$ where both a and b have order 3. There are 93600 such tuples from G. Let $X = \{a \in G : o(a) = 3.\}$

Let $v = [x(x^y)x, y^{(xy)}y]$. Using Magma it is easy to compute the value of w on all $a, b \in X$, by noting that $w(a, b) = v(a, b)$ [9]. Computing the value of $w(a, b)$ for all $a, b \in X$, there are elements of order 1,2,4,5,6, and 11. However, all of the elements of order 11 that occur in the image of w are conjugate. For $g \in M_{11}$ with $o(g) = 11$ we have that $g^{-1} \notin g^G$. We conclude that w witnesses the chirality of M_{11}. □

We note that w has length equal to 9680 =(440)(22), and is a relatively short straight-line program.

We now turn to the question of whether there is an achiral group that is weakly chiral. Using Magma [9] we can verify the following theorem. The relevant Magma code can be found in Appendix A.

Theorem 5.20. *Let* $G = \langle N_{2,3} \mid a^{3^2} = d, b^{3^2} = 1, c^3 = d^{-1}, d^3 = 1, e = 1\rangle$ *with* $c = [b, a]$, $d = [c, a]$, $e = [c, b]$. *Then* G *is weakly chiral with witness* d *and* $w = x^{3^2}[x, y]^3[x, y, x]$. *Moreover, we can computationally show that* G *is not chiral.*

Proof. An exhaustive Magma-aided search shows that G is not chiral. Using Magma we directly calculate the fiber sizes and we see that there are $w^{-1}(a^{20}) = 255879$ and $w^{-1}(a^{-20}) = 78732$. □

Chapter 6

Verbal descriptions of finite nilpotent groups.

In this chapter we investigate conditions on a finite group G that ensure G is nilpotent. For example, Baumslag and Wiegold [7], showed that a finite group is nilpotent if and only the product of elements of coprime order m and n has order mn.

Recall that Nikolov and Segal [87] have shown the following:

Theorem 6.1. *A finite G is solvable if and only if $\mu_{G,w}(1)$ is bounded away from zero as w ranges over all words.*

Work by Bray et. al. [10] described a sequence of words that can identify when a finite group G is solvable. In this note, we do likewise for nilpotent groups, giving yet another characterization of finite nilpotent groups. We note that the Engel words can also be used to determine when a finite group is nilpotent. Our result seems independent of this fact.

Recall the following from Chapter 1. For $w \in \mathbf{F}_2$ and a group G, define the structure $(G, *_w)$ where G is the set G and $*_w$ is the binary operation $x *_w y = w(x, y)$. In general, we do not expect the structure $(G, *_w)$ to have interesting mathematical properties. However, let $\mathcal{P}$ be the set of all words in $\mathbf{F}_2$ for which the total number of times x and y each appear up to multiplicity is ± 1. We will see that membership in $\mathcal{P}$ can

be determined using the structure $(G, *_w)$ where G ranges over a set of abelian groups. Moreover, we can describe finite nilpotent groups using $\mathcal{P}$ as follows.

Theorem E. *[13, Theorem C] A finite group G is nilpotent if and only if for all w in $\mathcal{P}$ with length less than $4|G|$, we have $\mu_{G,w}(1) = \frac{1}{|G|}$.*

It turns out that the set $\mathcal{P}$ can be defined using nilpotent groups in a similar manner. In our proof of Theorem E we will utilize the following novel result of the author's which has interest independent of the study of word maps.

Theorem F. *[13, Theorem A] Let G be a finite group and p a prime. Then G is not p-nilpotent if and only if there are two elements $g, h \in G$ with $o(g) = o(h) = q^k$ for some prime $q \neq p$ and $o(gh) = p$ or possibly 4 when $p = 2$.*

By extending the the techniques used to prove Theorem E, the author and Turbo Ho were able to prove the following characterization of finite nilpotent groups.

Theorem G. *[17, Theorem B] Let G be a finite group. Then G is nilpotent if and only if for every surjective word map w, the distribution $\mu_{G,w}$ is uniform.*

We start by proving Theorem F in Section 6.1 and then proving Theorems E and G in Sections 6.2 and 6.3 respectively. In Section 6.4, motivated by Bastos and Shumyatsky [6] we demonstrate an application of Theorem F to determining whether or not the derived subgroup of a group is nilpotent.

6.1 Normal p-complements.

Recall, that a finite group is nilpotent if and only if it has a normal p-complement for every prime p dividing the order of G. If G has a normal p-complement for a prime p,

then we say that G is p-nilpotent. We will use the Frobenius Complement Theorem as found in Isaacs [48]:

Theorem 6.2. *Let G be a finite group, and suppose p is a prime. Then the following are equivalent:*

(1) G is p-nilpotent.

(2) $\boldsymbol{N}_G(X)$ is p-nilpotent for every nonidentity p-subgroup $X \subseteq G$.

(3) $\boldsymbol{N}_G(X)/\boldsymbol{C}_G(X)$ is a p-group for every p-subgroup $X \subseteq G$.

We will also use the following Lemma, taken from an exercise in Isaacs.

Lemma 6.3 (Exercise **4D.4** [48])**.** *Let A act via automorphisms on G, where $(|G|, |A|) = 1$ and G is a p-group. Suppose that A acts trivially on every A-invariant proper subgroup of G, but that the action of A on G is nontrivial. Then the exponent of G is p or 4.*

We can now prove Theorem F

Proof of Theorem F. Since G does not have a normal p-complement for the prime p, by the Frobenius Complement Theorem, there is a p-subgroup $H < G$, such that $|\mathbf{N}_G(H) : \mathbf{C}_G(H)|$ is divisible by q for a prime q. We can assume H is minimal with this property, i.e., for all p-subgroups $K < H$, the groups $\mathbf{N}_G(K)/\mathbf{C}_G(K)$ are p-groups. Let Q be a Sylow q-subgroup of $\mathbf{N}_G(H)$. Then Q acts on H via automorphisms non-trivially, and by the minimality of H, we see that Q centralizes every Q-invariant subgroup of H. By Lemma 6.3 the exponent of H is either p or 4.

Let $x \in H$ such that for some $t \in G$ we have $x^t \neq x$. Then

$$x^t x^{-1} = t^{-1}xtx^{-1} = t^{-1}(xtx^{-1}).$$

The order of $x^t x^{-1}$ is either p or 4 and $o(t^{-1}) = o(xtx^{-1}) = q^k$. □

6.2 Proof of Theorem E.

The following lemmas will help prove Theorem E.

Lemma 6.4. *Let G be a group and let $Z = \boldsymbol{Z}(G)$. Let $w \in \mathcal{P}$. The structure $(G, *_w)$ is a quasigroup if and only if $(G/Z, *_w)$ is a quasigroup.*

Proof. Suppose that $(G, *_w)$ is a quasigroup. Then $w(a, b) = w(a, c)$ implies $b = c$. Use the "overbar notation" and suppose $w(\overline{a}, \overline{b}) = w(\overline{a}, \overline{c})$. Then $\overline{w(a, b)} = \overline{w(a, c)}$ and we conclude that $w(a, b) = w(a, c)z$ for some $z \in Z$. Since $w \in \mathcal{P}$, we see that $w(a, c) = w(a, cz^{\pm 1})$ and thus $\overline{b} = \overline{c}$. By symmetry, $w(\overline{a}, \overline{b}) = w(\overline{c}, \overline{b})$ implies that $\overline{b} = \overline{a}$ and $(G/Z, *_w)$ is a quasigroup.

Suppose that $(G/Z, *_w)$ is a quasigroup and $w(a, b) = w(a, c)$. Then as before $\overline{b} = \overline{c}$ and we conclude that $c = bz$ for some $z \in Z$. But, $w(a, c) = w(a, bz) = w(a, b)z^{\pm 1} = w(a, b)$ and we conclude that $z = 1$ and thus $c = b$. By symmetry, we see that $(G, *_w)$ is a quasigroup. □

Iterating Lemma 6.4 we have

Corollary 6.5. *Let G be a nilpotent group and let $w \in \mathcal{P}$. Then $(G, *_w)$ is a quasigroup.*

Proof. Observe that in an abelian group H, the action $x *_w y$ is $x^{\pm 1}y^{\pm 1}$. □

We now proof that membership in $\mathcal{P}$ can be determined by examining nilpotent groups.

Theorem 6.6. *A word $w \in \boldsymbol{F}_2$ is in $\mathcal{P}$ if and only if the length of w is greater than 1 and for any nilpotent group G with order less than the length of w, the structure $(G, *_w)$ is a quasigroup.*

Proof. By Lemma 6.4 and its corollary we see that $w \in \mathcal{P}$ only if for any nilpotent group G the structure $(G, *_w)$ is a quasigroup.

Now suppose that w is not in $\mathcal{P}$ and the length or w is greater than 1. Without loss of generality, either the degree of x in w is 0 or there is a prime p that divides the degree of x. If the degree of x in w is 0, then for any abelian group $g * 1 = 1$ for all $g \in G$. Suppose the degree of x is nonzero and let p divides the degree of x. Then consider C_p, the cyclic group of order p and note that $g * 1 = 1$ for all $g \in G$. Note that either the total number of times y appears is 0 or p is less than the length of w. □

We now prove Theorem E.

Proof of Theorem E. By Lemma 6.4 and its corollary we know that for a nilpotent group G, the structure $(G, *_w)$ is a quasigroup; therefore $\mu_{G,w}(g) = \frac{1}{|G|}$. for all $g \in G$.

Suppose that G is not nilpotent. We will construct a word w, so that $(G, *_w)$ is not a quasigroup. In particular, let G fail to be p-nilpotent. Then by Theorem F there are two elements g and h in G of order q^k such that $o(gh) = p$ or 4. Let $0 < a < q^k$ be an inverse of p modulo q^k, that is $ap \equiv 1 \pmod{q^k}$. Since $(a, q^k) = 1$, there are unique $\widehat{g}$ and $\widehat{h}$ such that $\widehat{g}^a = g$ and $\widehat{h}^a = h$. Moreover, $o(\widehat{g}) = o(\widehat{h}) = q^k$. Let b satisfy $ap - bq^k = 1$.

If $o(gh) = p$, consider the word:

$$w(x, y) = (x^a y^a)^{p-1}(x^{a-bq^k} y^{a-bq^k}).$$

Then

$$w(\widehat{g}, \widehat{h}) = (gh)^{p-1}(\widehat{g}^{a-bq^k}\widehat{h}^{a-bq^k}) = (gh)^p = 1.$$

By construction the degree of both x and y is $ap - bq^k = 1$. Hence $w(k, k^{-1}) = 1$ for all $k \in G$. Therefore $\mu_{G,w}(1) > \frac{1}{|G|}$. The length of w is $2(ap + bq^k)$. We note that $a < q^k$ and $bq^k = ap - 1 < |G|$. Hence the length of w is less than $4|G|$.

The construction of w works *mutatis mutandis* when $o(gh) = 4$. □

We remark, that the theorem is still true if $\mathcal{P}$ is replaced with the subset of all words w with total degree of x and y both being 1. Such words will generate a loop on every nilpotent group.

6.3 Proof of Theorem G.

The arguments used to prove Theorem E can be generalized to prove Theorem G, i.e., that a finite group G is nilpotent if and only if every surjective word map induced the uniform distribution on G. What's more, using Theorem F we see that for non-nilpotent groups G we can construct a surjective word w that fails to induce a uniform distribution. The work in this section was joint work with Turbo Ho [17]. The authors were interested in the follow question.

Question 6.7. Fix $n \in \mathbb{N}$, a finite group G, and an enumeration of the elements of G. Let g_i be the i-th element of G. Consider the probability distribution of the word map w as a function $f_w : \{1, 2, \cdots, |G|\} \to \mathbb{Q}$ where

$$f_w(i) = \mu_{G,w}(g_i).$$

The functions f_w and $\mu_{G,w}$ differ in their domains of definition, an important, if somewhat pedantic, distinction. Given the distributions of all n-variable word maps of G as a set, what information can be recovered about G?

In addition to Theorem F, in this section we will show the following:

Theorem 6.8. *For all $n \in \mathbb{N}$, we can identify when a finite group G is nilpotent from the set of distributions of all n-variable word maps on G.*

Theorem 6.9. *For $n > 1$, the set of distributions of all n-variable word maps on G can be used to identify whether G is abelian; moreover, if G is abelian, then the set of distributions identifies G up to isomorphism.*

For a word w, we will use the notation $w(\overline{x}; \overline{g})$ to refer to $w(x_1, \ldots, x_n; g_1, \ldots, g_m)$, the word w now taken to include parameters $g_1, \ldots, g_m$ in some group N. Klyachko and Mkrtchyan [55] call the elements of $\overline{g}$ the coefficients of w.

Lemma 6.10. *Let N be a finite nilpotent group, and $w(\overline{x}; \overline{g})$ be a word with parameters $\overline{g} \in N$. Then the following are equivalent:*

1. *$w(\overline{x}; \overline{g})$ has uniform fiber size over N.*
2. *$w(\overline{x}; \overline{g})$ is surjective.*
3. *The greatest common divisor of the exponents of variables in $\overline{x}$ in $w(\overline{x}; \overline{g})$ together with the exponent of N is 1.*

Proof. (1) $\rightarrow$ (2) is obvious.

(2) $\rightarrow$ (3): Suppose (2) holds, but the greatest common divisor of the exponents of variables in $\overline{x}$ in $w(\overline{x}; \overline{g})$ together with the exponent of N is $d > 1$. Let p be a prime divisor of d. Then p divides the exponent of the abelianization N/N'. In N/N', the image of $w(\overline{x}; \overline{g})$ is a coset of $w(\overline{x}; \overline{1})$. However, if p divides the greatest common divisor of the exponents of $\overline{x}$ in w, we have that $w(N/N'; \overline{1}) \subseteq (N/N')^p$, which is strictly smaller than N/N' since p divides the exponent of N/N'.

(3) $\rightarrow$ (1): Suppose (3) holds, then w has uniform fiber size over N if and only if any element u in the orbit of w under the action of automorphisms of $\mathbf{F}_m(N)$ has uniform fiber size over N. By (3), we have an automorphism of the $\mathbf{F}_m(N)/\mathbf{F}_m(N)'$ that maps

the abelianization of w to the product of a generator and some parametes. Hence, by lifiting this autormophism to an automorphism of $\mathbf{F}_m(N)$, we can assume that w has the form x_1hc where h is a word in $\overline{g}$ and c is a commutator word in the variables $\overline{x}$ and parameters $\overline{g}$. It is clear that this has uniform fiber size over an abelian group.

We now induct on the nilpotency class of N. Let $Z(N)$ be the center of Z. By the induction hypothesis, $w(\overline{x};\overline{g})$ has uniform fiber size over $N/Z(N)$, after replacing the parameters by their canonical image. Thus, it suffices to show that for every $a, b \in N$ such that $a^{-1}b \in Z(N)$, w has the same fiber size over a and b. However, we have the bijection $(x_1, x_2, x_3, \cdots) \to (x_1a^{-1}b, x_2, x_3, \cdots)$ between the fibers of a and b. Indeed, suppose that $w(x_1, x_2, \cdots) = a$. As $a^{-1}b$ is in the center and c is a commutator word, we have $c(x_1a^{-1}b, x_2, \cdots) = c(x_1, x_2, \cdots)$, thus $w(x_1a^{-1}b, x_2, \cdots) = x_1a^{-1}bhc(x_1a^{-1}b, x_2, \cdots) = (a^{-1}b)(x_1hc(x_1, x_2, \cdots)) = a^{-1}ba = b$. The other implication can be established similarly. So w has uniform fiber size over N, completing the proof. □

We now prove a slightly stronger version of Theorem G.

Theorem 6.11. *Let G be a finite group. Then the following are equivalent:*

1. *G is nilpotent.*
2. *For every surjective word map w, the distribution $\mu_{G,w}$ is uniform.*
3. *There is some $n > 1$ such that for every n-variable surjective word map w, the distribution $\mu_{G,w}$ is uniform.*

Proof. (1) → (2) We first suppose that G is nilpotent. Then by the previous lemma, if a word map is surjective, then is has uniform fiber size.

(2) → (3) is obvious.

(3) $\rightarrow$ (1) Now suppose that $n > 1$ and every n-variable surjective word map on G induces the uniform distribution. We will show G is p-nilpotent for every prime p. Suppose by way of contradiction that G is not p-nilpotent for the prime p. Then by Theorem F there are two elements a, b of G, such that $o(a) = o(b) = q^k$ and

$$o(ab) \begin{cases} = p & \text{for } p \text{ an odd prime} \\ \in \{2, 4\} & \text{for } p{=}2. \end{cases}$$

Since p and q are coprime there are $r, s \in \mathbb{Z}$ such that $rp + sq^k = 1$; (in the event $o(ab) = 4$ we will assume that $4r + sq^k = 1$). Consider the n-variable word

$$w(\overline{x}) = x_1^{sq^k} x_2^{sq^k} (x_1 x_2)^{rp},$$

(if necessary let $p = 4$). We have the following facts about w:

(a) For any $g \in G$, we have $w(\overline{x}) = g$ if $x_1 = g$ and $x_2 = 1$.

(b) For any $g \in G$, we have $w(\overline{x}) = 1$ if $x_1 = g$ and $x_2 = g^{-1}$.

(c) If $x_1 = a$ and $x_2 = b$, we have

$$w(a, b) = a^{sq^k} b^{sq^k} (ab)^{rp} = 1.$$

By (a), w is surjective. By (b) and (c), there are at least $(|G| + 1) \cdot |G|^{n-2}$ tuples in G^n that map to the identity. So w is a surjective word map on G that does not induce the uniform distribution. We conclude that if every n-variable surjective word map on G induces the uniform distribution, then G is p-nilpotent for every prime p, and hence nilpotent. $\square$

Recall that a word c is a commutator if the total degree of any variable that appears in c is 0. Equivalently, c is in the commutator subgroup of the appropriate free group.

Corollary 6.12. *In a finite nilpotent group G, the equation $x = c(x, y)$, where c is a commutator word in x, y, has exactly $|G|$ solutions; moreover, the solution set is exactly the two-tuples in the set $\{(1, g) : g \in G\}$.*

Proof. We note that a solution (a, b) to $x = c(x, y)$ is also a solution to $w(x, y) = 1$ where $w = x^{-1}c(x, y)$. Since G is nilpotent and w is surjective, we see that there are exactly $|G|$ such solutions. Clearly, $(1, g)$ is a solution for all $g \in G$. □

The above corollary can easily be generalized to the following:

Corollary 6.13. *In a finite nilpotent group G, the equation $w(\overline{x}) = c(\overline{x})$, where c is a commutator word in $\overline{x}$ and w is a surjective word map on G, has exactly $|G|^{|\overline{x}|-1}$ solutions.*

Proof. By Theorem 6.10, the greatest common divisor of the exponents of variables in $\overline{x}$ in $w(\overline{x})$ together with the exponent of N is 1. However, as c is a commutator word, this is also true for wc^{-1}. Thus, again by Theorem 6.10, wc^{-1} has uniform fiber size over N. Hence, there are exactly $|G|^{|\overline{x}|-1}$ solutions to $wc^{-1}(\overline{x}) = 1$ and these are exactly the solutions to $w(\overline{x}) = c(\overline{x})$. □

It is natural to ask about the generalization of Corollary 6.13 to the equation $w(\overline{x}) = v(\overline{x})$, without any restriction on w or v, which is equivalent to considering the equation $w(\overline{x}) = 1$. The following conjecture is attributed to Amit in [86, Question 24]:

Conjecture 6.14 (Amit)**.** *For every word map $w(\overline{x})$ on a finite nilpotent group G,*

$$\mu_{G,w}(1) \geq \frac{1}{|G|},$$

i.e., the number of solutions to $w(\overline{x}) = 1$ *is greater than or equal to* $|G|^{|\overline{x}|-1}$.

There are only some partial results in this direction. Levy [65] has shown that when G has nilpotent class 2, then for any word w we have $\mu_{G,w}(1) \geq \frac{1}{|G|}$; showing that Amit's Conjecture holds for class 2 groups. Iñiguez and Sangroniz [45] have shown the stronger condition that for free p-groups of nilpotency class 2 and exponent 2, it is true that $\mu_{G,w}(g) \geq \frac{1}{|G|}$. Solomon [99] showed that for any finite group G and $w \in \mathbf{F}_2$, we have $\mu_{G,w}(1) \geq \frac{1}{|G|}$.

We are also interested in understanding the information content of the distributions of word maps of a group. Recall that we are interested in the following question:

Fix $n \in \mathbb{N}$, a finite group G, and an enumeration of the elements of G. Let g_i be the i-th element of G. Consider the probability distribution of the word map w as a function $f_w : |G| \to \mathbb{N}$ where $f_w(i) = |w^{-1}(g_i)|$. Given the distributions of all n-variable word maps of G as a set, what information can be recovered about G?

A priori, the answer of the question depends on n. We ask:

Question 6.15. Do we get more information as n gets larger?

From the distributions of word maps we can easily read off the size of the group. Moreover, we can identify the identity element in G as it is the image of the only word map (the identity map) that has an image of size 1.

We mention the following example:

Example 6.16. The dihedral group of order 8, which we write as D_8, and Q_8 have the same reduced free group on two variables, i.e.,

$$\mathbf{F}_2(D_8) \cong \mathbf{F}_2(Q_8).$$

However using Magma [9] we find that they have different sets of distributions of 2-variable word maps.

6.3.1 $n = 1$: words with a single variable.

When $n = 1$, the images of the word maps are exactly the sets $G^k = \{g^k \mid g \in G\}$.

Example 6.17. The distribution of 1-variable word maps does not determine even nilpotent groups up to isomorphism. Consider any nonabelian group of exponent p, for $p \geq 3$ a prime. When looking at word maps on 1-variable, such a group is indistinguishable from an elementary abelian group of the same order. For example, the Heisenberg group $H_3(\mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$ over the field of p elements is a non-abelian group of exponent p and order p^3, and it cannot be distinguished by its 1-variable word maps from the elementary abelian group of order p^3.

Using the Frobenius Solutions Theorem we can now show:

Theorem 6.18. *The distributions of 1-variable word maps on a finite group G determine whether or not G is nilpotent.*

Proof. We first note that the identity element is always determined by the set of distributions, i.e., the only element for which there is a distribution mapping entirely onto it.

Let $|G| = p^k m$ where $\gcd(p, m) = 1$ and $k \geq 1$. Then, if G is nilpotent, there are exactly p^k solutions to the equation $x^{p^k} = 1$. Moreover, letting $w = x^{p^k}$, we see that for every $g \in w(G)$ there are exactly p^k preimages in G and $|w(G)| = m$.

Now suppose G is a group of order $p^k m$, where $(p, m) = 1$, and $w = x^d$ such that the following hold:

- For every $g \in w(G)$ there are exactly p^k preimages in G.
- $|w(G)| = m$.

We claim G must have a normal Sylow p-subgroup. Note that by the Frobenius Solutions Theorem the number d is a p-th power.

Let $X(m)$ be the solutions to the equation $x^m = 1$. Also by the Frobenius Solutions Theorem, $|X(m)| \geq m$. But every element of $X(m)$ is a solution to $x^m = 1$, hence they have order coprime to p. Since $w = x^{p^j}$ for some $j \geq 1$ and $\gcd(p^j, m) = 1$, the elements in $X(m)$ must also be in $w(G)$. But, $|w(G)| = m$ and we conclude that $w(G) = X(m)$ and contains no elements of order p. Hence every element whose order is a power of p is a solution to w. Thus, G has a normal Sylow p-subgroup. Then G is nilpotent if and only if there is such a w for all p dividing $|G|$. □

6.3.2 $n > 1$: words with more than one variable.

From Theorem 6.11, we see that for $n > 1$, the set of all distributions of n-variable word maps on G is enough to determine whether or not G is nilpotent, i.e., a finite group G is not nilpotent if and only if there is some n-variable surjective map that is not uniform. This, together with Theorem 6.18, proves Theorem 6.8.

Interestingly enough the set of all distributions of n-variable word maps can also identify commutativity:

Lemma 6.19. *For any $n > 1$, a finite group G is abelian if and only if the distribution of every n-variable word map is uniform over its image.*

Proof. If G is abelian, then for every word map w, $w^{-1}(0)$ is a subgroup of G^k, and $w^{-1}(g)$ is either a coset of it or empty. Thus every word map is uniform over its image.

If G is not abelian, then as shown by Ashurst, for $w = [x, y]$, we have that $\mu_{G,w}(1) > \mu_{G,w}(g)$ for all $g \in G$ [3, Lemma 2.2.8]. Also, as G is not abelian, $\mu_{G,w}(g)$ is not all zero for $g \neq 1$. If we regard w as an n-variable word, then $\mu_{G,w}$ is not uniform over its image. □

We now prove Theorem 6.9.

Proof of Theorem 6.9. In an abelian group, every word is automorphic to a power word, as can be seen by using a series of Nielsen transformation to cancel out all but a single variable. Since the number of non k-powers in G is determined by the word map x^k, the set of distributions of word maps on G for any number of variables determines the set of natural numbers m such that there exists a k so that the word $w = x^k$ satisfies $|G| - |w(G)| = m$. If we are looking at all distributions induced by n-variable word maps where $n > 1$, then we can determine if G is abelian. If G is abelian, then by Theorem B above we have determined G up to isomorphism. □

Remark 6.20. *Note that as shown in Example 6.17, the distribution of 1-variable word maps is not enough to identify whether a group is abelian. However, if in addition to knowing that the distribution of 1-variable word maps, we also assume that G is abelian, then Theorem B applies and we can still identify G up to isomorphism.*

The reduced free group of a nilpotent group is the direct product of the reduced free groups of its Sylow subgroups [84, p. 41]. We show that without the group structure, the distributions of word maps of a nilpotent group determine the distributions of word

maps of its Sylow subgroups, and similarly the distributions of word maps of all the Sylow subgroups determine the distributions of word maps of G.

Theorem 6.21. *The distributions of word maps of a nilpotent group uniquely determine the distributions of word maps of its Sylow p-subgroups for all p, and vice versa.*

Proof. Given the distributions of word maps of a finite group G, we will show how to identify the sub-lists of the enumerated list G that correspond to the Sylow p-subgroups. First, we note that from the distributions of word maps of G we can determine the order of G. Write $|G| = p^n k$ such that $p \nmid k$. Then the word map x^k is uniformly distributed on its image, the Sylow p-subgroup. Since G is nilpotent, we have $G = PK$ where $|P| = p^n$ and $|K| = k$. Then the following holds for every word map w and $g \in P$, $h \in K$:

$$w_G^{-1}(gh) = w_P^{-1}(g) w_K^{-1}(h).$$

Suppose w have image of size p^n and is uniform. Then it is uniform when projected to both P and K. However, this means that the size of the image in K must divide $|K|^2 = k^2$. But k and p are co-prime, so the size of the image of w in K is 1. Thus, the image of w in G must be P. This allows us to identify the Sylow p-subgroups. For every word map, we may find its distribution as a word map on P by looking at its distribution on P and scale accordingly.

For the backward direction, if we enumerate elements in G as the Cartesian product of the elements in the Sylow p-subgroups, then from the above discussion we have that any distribution on G is a product of distributions on the Sylow subgroups in the sense that

$$w_G^{-1}(g_1 \cdots g_\ell) = w_{P_1}^{-1}(g_1) \cdots w_{P_\ell}^{-1}(g_\ell).$$

Thus, we only need to show that the products of distributions on the Sylow subgroups are actually realized as the distribution of some word map on G. Let P be a Sylow p-subgroup, and K be its complement. Suppose $|P| = p^n$ and $|K| = k$, and $rp^n + sk = 1$. Then for any word w, define $\hat{w}_p(x_1, x_2, \cdots) = w(x_1^{sk}, x_2^{sk}, \cdots)$. Then $w = \hat{w}_p$ in P, and $\hat{w}_p$ is a law on K. Thus, the product of distributions on the Sylow subgroups are realized by the product of the $\hat{w}_p$ as a word map in G. □

6.4 The nilpotency of commutator subgroups.

An interesting line of study has emerged following the observation of Baumslag and Wiegold [7] that a finite group is nilpotent if and only the product of elements of coprime order m and n has order mn. Bastos and Shumyatsky showed a similar condition on commutators was sufficient to guarantee that the commutator subgroup is nilpotent. In this section, we will say that an element g of a group G is a commutator if there are $a, b \in G$ such that $[a, b] = g$.

Bastos and Shumyatsky showed the following.

Theorem 6.22. *[6] Let G be a finite group. If for all commutators $g, h \in G$ of coprime order $o(g)o(h) = o(gh)$, then G' is nilpotent.*

Bastos et. al. [5] extended that result to metanilpotency and Freitas de Andrade and Carrazedo Dantas [27] showed a similar result regarding the nilpotency of the nilpotent residue. We also note that Monakhov has done related work using just commutators of prime power order [81, 80].

In the present section we show that Theorem F can be used to derive another test for the nilpotency of the commutator subgroup.

Theorem 6.23. *Let G be a finite group. The following are equivalent:*

(1) The group G' is nilpotent.

(2) For any prime p and two commutators x and y of order p^k, the element xy does not have order $q^j > 1$ for q a prime different than p.

(3) For any prime p and any commutator x of order p^k and an arbitrary $y \in G$, the element $x^{-1}x^y$ does not have order $q^j > 1$ for q a prime different than p.

Lemma 6.24. *Let G be a finite group and let H be a q-subgroup of G. Let p and q be distinct primes dividing the order of G. Assume that for all commutators x in G of order p^k, there is no nontrivial commutator z of order q^j such that the product of x and z is conjugate to x. Then, if $x \in \boldsymbol{N}_G(H)$ then $x \in \boldsymbol{C}_G(H)$.*

Proof. Let $x \in \mathbf{N}_G(H)$ and let $y \in H$. Consider $[x, y]$. We claim that $[x, y] = 1$. To see this, consider

$$x \underbrace{[x, y]}_{\in H} = xx^{-1}y^{-1}xy = x^y.$$

By assumption we must have that $[x, y] = 1$. Hence $x \in \mathbf{C}_G(H)$. □

Theorem 6.25. *Let G be a finite solvable group. If for any prime p and any commutator x of order p^k and an arbitrary $y \in G$, the element $x^{-1}x^y$ does not have order $q^j > 1$ for q a prime different than p, then G' is nilpotent.*

Proof. Look at $G'' > 1$. Consider any Sylow subgroup S of G' and a different Sylow subgroup T of G''. Then ST is a characteristic subgroup of G' and hence normal in G. We note that S is generated by commutators. Moreover, for each commutator g that is in S, we have that $[g, T] = 1$ since T is a normal subgroup of G'. Hence, $[S, T] = 1$

and we conclude that S is characteristic in ST and thus normal in G. Therefore G' is nilpotent. □

We can prove the general case, using the proven Ore Conjecture [67].

Proof of Theorem 6.23. (1) → (2) follows since every Sylow subgroup of G is normal.

(2) → (3) This is a tautological weakening.

(3) → (1) Assume that G is a minimal counterexample to the implication (3) → (1), i.e., that for any x of order p^k and any y, the product $x^{-1}x^y$ does not have nontrivial q-power order; but, G' is not nilpotent. From Theorem 6.25, we see that G is not a solvable group, and by induction we can assume that every subgroup H of G satisfies H' is nilpotent. Hence every subgroup of H is meta-nilpotent and thus solvable. Therefore, G is either solvable or a minimal simple group. If G is solvable then from Theorem 6.25 we see that G' is nilpotent. If G is simple, then by combining the Ore Conjecture and Theorem F we see that G contains a commutator of order p^k and an element $y \in G$ such that $x^{-1}x^y$ nontrivial q-power order. □

Chapter 7

The number of word maps on a finite group.

In this chapter we return to examining the group of word maps on a group G. This group $\mathbf{F}_n(G)$ shares many of the interesting properties of the group $\mathbf{F}_n$. The notation is in part inspired by the fact that $\mathbf{F}_n(G)$ is the rank n-free group in the variety generated by G [84]. All characteristic subgroups of $\mathbf{F}_n(G)$ are verbal, moreover any characteristic subgroup is generated by a single word w, although w might be a word on more than n variables. We can also formulate $\mathbf{F}_n(G)$ as the following quotient of $\mathbf{F}_n$:

Let

$$K(G) = \{w \in \mathbf{F}_n : w(G) = 1\}.$$

The group K is called the set of n-variable laws on G. Then

$$\mathbf{F}_n(G) = \mathbf{F}_n/K(G).$$

It should be noted that $\mathbf{F}_n(G)$ is a subgroup of the group of all maps from $G^n \to G$. Hence when G is finite it has order dividing $|G|^{|G|^n}$. However, it is easy to show that when $|G| > 1$ this bound is not sharp. Finding explicit formulas for $|\mathbf{F}_n(G)|$ for specific groups has been a matter of some interest.

Several authors have worked on bounding the order of $\mathbf{F}_n(G)$ including the following:

The observation that $|\mathbf{F}_n(G)|$ divides $|G|^{|G|^n}$ was originally made by Neumann in [83]. Restricting to dihedral groups, Fine gave a much tigher bound [25], which prompted Kovács to announce a general formula for $|\mathbf{F}_n(D_m)|$ where D_m is the dihedral group of order $2m$ [56]. However, it is known that his result is written incorrectly for the cases where m is odd. A corrected formula previously appeared on Kovács website [53]. We will give an explicit example showing the error in Kovács' formula in Section I.

In this note we provide a new bound on $\mathbf{F}_n(G)$, motivated in large part by the desire to determine the size of the reduced free group on two variables in the variety generated by the alternating group on 5 elements, i.e., we want to find $|\mathbf{F}_2(A_5)|$. As will we see in Theorem J,

$$|\mathbf{F}_2(A_5)| = 47383813383216168960000000000000000000000000.$$

Our new bound for general groups G is stated in the following theorem.

Theorem H. *Let G be a finite group with exponent e. Let Ω be a set of orbit representatives of the diagonal action of $\mathrm{Aut}(G)$ on the set of n-tuples $(g_1, \ldots, g_n)$ of G such that $\langle g_1, \ldots, g_n \rangle$ is not abelian. Then*

$$|\boldsymbol{F}_n(G)| \leq e^n \prod_{(x_1,\ldots,x_n)\in\Omega} |\langle x_1, \ldots, x_n \rangle'|.$$

We will show that the bound in Theorem H is sharp. In particular we have the following theorem:

Theorem I. *Let C_p be the cyclic group of order p, where p is prime. Let $G = C_p \rtimes \mathrm{Aut}(C_p)$ then*

$$|F_2(G)| = (p-1)^2 p^{2+p(p-2)},$$

and

$$F_2(G)' = (C_p)^{p(p-2)}\,.$$

It is worth noting that in our proof of Theorem I we have the following lemma, which while elementary is nonetheless interesting and is related to the matrix examined in Section 2 of [94] :

Let z be a primitive root of unity modulo p. Let M be the $p-2$-by-$p-2$ matrix defined by $(z^{ij}-1)$. Then $M^4 = I$.

Returning to the group A_5, we used Magma [9] to perform calculations necessary to verifiy the order of $|F_2(A_5)|$. We also determined the structure of $F_2(A_5)'$.

Theorem J. *Let $G = A_5$. Then*

$$|\boldsymbol{F}_2(G)| = 30^2 3^3 4^4 5^3 60^{19}$$

and

$$\boldsymbol{F}_2(G)' = (C_3)^3 \times (K_4)^4 \times (C_5)^3 \times (A_5)^{19}$$

The rest of the note consists of Sections 7.1, 7.2, and 7.3, where we prove Theorems H, I, and J respectively.

7.1 Proof of Theorem H.

Recall that any word $w(x_1, \ldots, x_n)$ can be written in the form

$$w = x_1^{k_1} \ldots x_n^{k_n} v(x_1, \ldots, x_n), \text{ where } v \in \mathbf{F}'_n.$$

By applying Nielson transformation to w, we see that w is automorphic to a word $w' = x_1^k c$ where k is $\mathbf{gcd}(k_1, \ldots, k_n)$ and $c \in \mathbf{F}'_n$. For a group G, the subgroup $K(G) \leq$

$\mathbf{F}_n(G)$ is characteristic, and hence $w \in K(G)$ if and only if $w' \in K(G)$. Equivalently, w is a law on G if and only if w' is a law on G. We have the following lemma:

Lemma 7.1. *Let $w \in \boldsymbol{F}_n$ and let G be a group. Suppose that σ is an automorphism of $\boldsymbol{F}_n$. Let*

$$\sigma(w) = w' = x_1^k c, \text{ where } c \in \boldsymbol{F}_n'.$$

Then $w \in K(G)$ if and only if $x_1^k \in K(G)$ and $c \in K(G)$.

Proof. Clearly, if x_1^k and c are both in $K(G)$ then w' and w are too. Suppose that $w' \in K(G)$. Then as a map $w'(g_1, \ldots, g_n) = 1$ for all $g_1, \ldots, g_n \in G$. So $w'(g, 1, \ldots, 1) = g^k = 1$ for all $g \in G$, i.e., $x_1^k \in K(G)$. Equivalently, $x_1^{-k} \in K(G)$ and we see that $c \in K(G)$ as well. □

From Lemma 7.1 we deduce the following corollary:

Corollary 7.2. *Let G be a group. The exponent of G is e if and only if*

$$|\boldsymbol{F}_n(G) : \boldsymbol{F}_n(G)'| = e^n.$$

Proof. The word maps $x_1^{e_1} \ldots x_n^{e_n}$ for $e_1, \ldots, e_n$ in $\{1..e\}$ give a unique set of coset representatives of $\mathrm{F}_n(G)'$ in $\mathrm{F}_n(G)$. □

Theorem H follows as a Corollary to the below theorem and an application of Lemma 7.1:

Theorem 7.3. *Let G be a finite group with exponent e. Let Ω be a set of orbits of representatives of the diagonal action of $\mathrm{Aut}(G)$ on the set of n-tuples of G such that $\langle g_1, \ldots, g_n \rangle$ is not abelian. Then*

$$|\boldsymbol{F}_n(G)'| \leq \prod_{(x_1,\ldots,x_n)\in\Omega} |\langle x_1, \ldots, x_n \rangle|'.$$

Proof. Let $w \in \mathbf{F}_n(G)'$. The word map w is determined by its value on the set of n-tuples of G such that $\langle g_1, \ldots, g_n \rangle$ is not abelian. Moreover, if for some $\sigma \in \mathrm{Aut}(G)$ and $(g_1, \ldots, g_n)$ and $(h_1, \ldots, h_n)$ we have that $\sigma(g_i) = h_i$ for all i, then

$$\sigma(w(g_1, \ldots, g_n)) = w(\sigma(g_1), \ldots, \sigma(g_n)).$$

Hence, knowing the value of $w(g_1, \ldots, g_n)$ determines the value of $w(h_1, \ldots, h_n)$. By assumption $w(g_1, \ldots, g_n) \in \langle g_1, \ldots, g_n \rangle'$. Hence, there are at most

$$\prod_{(x_1,\ldots,x_n)\in\Omega} |\langle x_1, \ldots, x_n \rangle|'$$

commutator maps on G. □

We note that the bound obtain in Theorem 7.3 is not strict. For example, let G be the dihedral group of order 8. Applying Theorem 7.3 we see that $|\mathbf{F}_2(G)'| \leq 8$; but, in fact $|\mathbf{F}_2(G)'| = 2$, as seen by running an algorithm that calculates $\mathbf{F}_2(G)$ [16, Theorem 3.3]. However, there is one family of groups where we obtain equality in Theorem H when $n = 2$. In the next section we prove that Theorem H is sharp for the number of 2 variable word maps on the holomorphs of cyclic groups of order p, where p is prime.

7.2 Proof of Theorem I.

Let C_p be the cyclic group of order p, where p is prime. Let $G = C_p \rtimes \mathrm{Aut}(C_p)$ then We will first show that when $p = 3$, we have $C_3 \rtimes C_2 = S_3$ and

$$|\mathbf{F}_2(S_3)| = 972.$$

The techniques and ideas used in the proof for $p = 3$ will carry directly over to our

proof of Theorem I. As promised, the example of $|\mathbf{F}_2(S_3)| = 972$ contradicts the formula originally given by Kovács [56].

7.2.1 The case $G = S_3$.

Let $G = S_3 = \mathrm{Hol}(C_3)$. By Theorem 7.3 we see that $|\mathbf{F}_2(G)| = 972$ if and only if $|\mathbf{F}_2(G)'| = 27$. To determine the number of commutator word maps on G, we first compute the number of noncommuting 2-tuples of G; in this case there 18 noncommuting 2-tuples. The automorphism group of S_3 is S_3 and under the diagonal action of S_3 there are exactly 3 orbits. Our choice of orbit representatives is:

- $A = ((123), (12))$;
- $B = ((12), (123))$;
- $C = ((12), (13))$.

Hence any commutator word map is determined entirely by its values on A, B, and C. Consider the maps corresponding to $[x^3, y^3], [x, y^2]$, and $[x^2, y]$. Since G' is a group of order 3, the group $\mathbf{F}_2(G)'$ is a vector space over $G = \mathbb{F}_3$, the field with 3 elements. By choosing a generator of G', we can evaluate commutator word maps on A, B, and C to get vectors in $\mathbb{F}_3^3$, where each coordinate corresponds to the value over one of A, B or C . Explicitly, let $(123) \to 1$. Then

$$[x, y](A) = [(123), (12)] = (132)(12)(123)(12) = (123) \to 1.$$

We construct a matrix M to manipulate the values of the various commutator maps on A, B, and C. We note that given two commutator words w and v, the product map

wv is also a commutator map and will correspond to adding the appropriate rows of the matrix. Moreover, the evaluation of wv is the product of the evaluation map on w and v.

$$M = \begin{pmatrix} [x^3,y^3](A) & [x^3,y^3](B) & [x^3,y^3](C) \\ [x,y^2](A) & [x,y^2](B) & [x,y^2](C) \\ [x^2,y](A) & [x^2,y](B) & [x^2,y](C) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \end{pmatrix}.$$

Hence, by using products of $[x^3,y^3],[x,y^2]$, and $[x^2,y]$ we could get any of the 27 vectors in $\mathbb{F}_3$ to occur as the values of a commutator word map on A, B, and C. We conclude that $\mathbf{F}_2(G)'$ has order 27. In the present case it was a fortunate stroke of serendipity that the commutator maps in questions are clearly independent as vectors over $\mathbb{F}_3$. In general, we will need to demonstrate that some system of commutators produces a non-singular matrix to show independence over $\mathbb{F}_p$.

7.2.2 The general case.

For the general case we need to first determine the number of orbits of noncommuting pairs of elements of $G = \mathrm{Hol}(C_p) = C_p \rtimes C_{p-1}$. We note that Out(G) is trivial. We will first give a set of $p(p-2)$ elements that are a set of orbit representatives of the action of $\mathrm{Aut}(G)$ on the set of noncommuting pairs of elements of G. Let z be a primitive p-th root of unity. Let $G = \langle a,b : a^p, b^{p-1}, a^b = a^z \rangle = \mathrm{Hol}(C_p)$. Let

$$X = \{(a,b^j) : \text{ and } j \in \{1..p-2\}\},$$

$$Y = \{(b^j,a) : \text{ and } j \in \{1..p-2\}\},$$

$$Z = \{(b^i,(b^j)^a) : i,j \in \{1..p-2\}\}.$$

Lemma 7.4. *With the notation defined above, the set $X \cup Y \cup Z$ is a set of orbit representatives of noncommuting pairs of elements of G and $|X \cup Y \cup Z| = p(p-2)$.*

Proof. By construction $|X| = |Y| = p-2$ and $|Z| = (p-2)^2$. Hence $|X \cup Y \cup Z| = p(p-2)$. We need to show that given $s, t \in X \cup Y \cup Z$ there is no automorphism of G that takes s to t.

Every automorphism of G is inner. Consider (a, b^j) in X. Let $g = a^n b^m \in G$. We have

$$(a, b^j)^g = (a^{(b^m)}(b^j)^g), (a^{(z^m)}, (b^j)^g).$$

Clearly, $(a, b^j)^g$ is not in Y, Z for any g. A similar result holds for (b^j, a) in Y. Therefore for $s, t \in X \cup Y \cup Z$ we see that $s^g = t$ if and only if s, t are in exactly one of X, Y, or Z. But, it is obvious that for $s, t \in X$ there is no $g \in G$ such that $s^g = t$; by symmetry the same holds for Y, and by exclusion the result holds for Z as well. Therefore, $X \cup Y \cup Z$ is a set of orbit representatives of the noncommuting pairs of elements of G. □

Hence any commutator word map on G is determined by its values on X, Y, and Z. Moreover, given a word $w(x, y) \in \mathbf{F}_2'$ we can construct a word $v_X(x, y) = w(x^{1-p}, y)$. We see immediately that v_X has the following properties:

- For all $(x, y) \in X$, we have the equality $w(x, y) = v_X(x, y)$.
- For all $(x, y) \in Y \cup Z$, we have that $v_X(x, y) = 1$.

Heuristically, v_X mimics w over the set X.

We can similarly construct $v_Y(x, y) = w(x, y^{1-p})$ and $v_Z = w(x^p, y^p)$. Thus for any word map $w \in \mathbf{F}_2(G)'$ we have $w = v_X v_Y v_Z$. Moreover, the words v_X, v_Y and v_Z pairwise commute. Hence, $\mathbf{F}_2(G)'$ decomposes as a direct product of words taking values over X,

Y, and Z. We will show that for any tuple in $X \cup Y \cup Z$ there is a commutator w that does not vanish on that tuple, but w does vanish on all other tuples in $X \cup Y \cup Z$, i.e., the word w isolates a single tuple.

7.2.3 Tuples in X and Y.

Consider the $p-2$ tuples of the form (a, b^j) where $1 \leq j \leq p-2$. Consider the words $w_i = [x, y^i]$ where $i \in \{1..p-2\}$. What is the value of $w_i(a, b^j)$? We compute

$$w_i(a, b^j) = a^{-1}b^{-ij}ab^{ij} = a^{(z^{ij}-1)}.$$

Let us fix a homomorphism $f : G' \to \mathbb{F}_p^+$ such that $f(a) = 1$. The words w_i on (a, b^j) give us the matrix

$$\Big(f(w_i(a, b^j))\Big) = \begin{pmatrix} z & z^2 & \dots & z^{p-2} \\ z^2 & z^4 & \dots & z^{2(p-2)} \\ \vdots & \vdots & \dots & \vdots \\ z^{p-2} & z^{2(p-2)} & \dots & z^{(p-2)^2} \end{pmatrix}.$$

We will show that the matrix above is invertible.

Lemma 7.5. *Let z be a primitive root of unity modulo p. Let M be the $p-2$-by-$p-2$ matrix defined by $(z^{ij} - 1)$. Then $M^4 = I$.*

Proof. Consider the ij-entry of M^2, which we write as $M^2(i, j)$. We have that

$$M^2(i, j) = \sum_{k=1}^{p-2}(z^{ik} - 1)(z^{kj} - 1) = \sum_{k=1}^{p-2} z^{ik+kj} - \sum_{k=1}^{p-2} z^{kj} - \sum_{k=1}^{p-2} z^{ij} + \sum_{k=1}^{p-2} 1.$$

We note that $\sum_{k=1}^{p-2} \zeta^k$ of any element of $\mathbb{F}_p$ is 0, unless $\zeta = 1$, in which case the summation comes out to -2. Hence we immediately have

$$M^2(i,j) = \begin{cases} -2 & \text{if } i+j \equiv -1 \pmod{p} \\ -1 & \text{otherwise.} \end{cases}$$

Hence

$$M^2 = \begin{pmatrix} -1 & -1 & -1 & \dots & -1 & -2 \\ -1 & -1 & -1 & \dots & -2 & -1 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ -2 & -1 & -1 & \dots & -1 & -1. \end{pmatrix}$$

Let $M^4(i,j)$ be the ij entry of M^4. We have that

$$M^4(i,j) = \begin{cases} p-3+4 & \text{if } i=j \\ p-4+4 & \text{otherwise.} \end{cases}$$

Since we are working over $\mathbb{F}_p$ we have

$$M^4(i,j) = \begin{cases} 1 & \text{if } i+j \equiv 0 \pmod{p} \\ 0 & \text{otherwise.} \end{cases}$$

□

So every tuple of X, and by symmetry Y, can be isolated by a commutator word map. We now need to show that for any of the $(p-2)^2$ tuples in Z there is a word map that vanishes on all but a single tuple. To do this, we will first show that there is an invertible matrix Q that corresponds to the values of well-chosen words on the right subsets of Z. We will use Q to construct an invertible $(p-2)^2$-by-$(p-2)^2$ matrix P over Z that corresponds to a choice of $(p-2)^2$ words.

7.2.4 Tuples in Z.

We will ultimately want to show that the values on tuples in Z of the words $[x^i, y^j]$ where i and j range from 1 to $p-2$ can be used to construct an invertible matrix P. However, such a direct approach might be unwise. We will instead show that P is the Kronecker product of two invertible matrices $(p-2)$-by-$(p-2)$ matrices.

We calculate the values of $(b, (b^j)^a)$ and (b^i, b^a) under the words $w_i(x,y) = [x, y^i]$ on $v_i(x,y) = [x^i, y]$.

We see that

$$w_i(b, (b^j)^a) = [b, a^{-1}b^{ij}a] = a^{1-z+z^{(ij+1)}-z^{(ij)}}, \tag{7.1}$$

and

$$v_i(b^j, b^a) = [b^{ij}, a^{-1}ba] = a^{1-z+z^{(ij+1)}-z^{(ij)}}. \tag{7.2}$$

Identifying a with 1 in $\mathbb{F}_p$ under the map f then equations (7.1) and (7.2) give us

$$f(w_i(b, (b^j)^a) = f(v_i(b^j, b^a)) = 1 - z + z^{(ij+1)} - z^{ij} = \left(z^{ij} - 1\right)(z-1) \tag{7.3}$$

As before, we will need to show that a particular matrix is invertible.

Lemma 7.6. *Let z be a primitive root of unity modulo p. Let Q be the $(p-2)$-by-$(p-2)$ matrix defined by $(z^{ij}-1)(z-1)$. Then Q is invertible.*

Proof. The matrix Q is $(z-1)$ times the matrix M defined in the previous section. Since M is invertible and $(z-1)$ is a unit, the matrix Q is invertible.

□

We now ask the question, what is the value of $[b^{i\alpha}, (b^a)^{j\beta}]$.

$$[b^i, (b^a)^j] = a^{-z^i + z^{i+j} - z^j + 1}. \tag{7.4}$$

Identifying a with 1 in $\mathbb{F}_p$ then equation (7.4) gives us

$$[b^i, (b^a)^j] \longrightarrow -z^i + z^{i+j} - z^j + 1 = \left(z^i - 1\right)\left(z^j - 1\right) \tag{7.5}$$

We note combine equations (7.3) and (7.5) to get

$$f([b^i, (b^a)^j]) = \left(z^i - 1\right)\left(z^j - 1\right) = \frac{f\left([b^i, b^a]\right) f\left([b, (b^a)^j]\right)}{(z-1)^2}. \tag{7.6}$$

What does equation (7.6) mean? We show below that $Q \otimes (z-1)^{-2}Q$ is the matrix P we wanted to construct. The following rather technical looking lemma, essentially makes note of the fact we observed above in equation (7.6). Once the observation relating $[b^i, (b^a)^j]$ and the values of $[b^i, b^a], [b, (b^a)^j]$ has been made, the rest of the proof is a game of tracking the right symbols to the right indexes.

Lemma 7.7. *Let α, β be in $\{1, \ldots, (p-2)^2\}$. Write $\alpha = (i-1)(p-2) + (j-1)\cdot 1$ where $j \leq p-2$ and $\beta = (k-1)(p-2) + (\ell - 1)\cdot 1$ where $\ell \leq p-2$. The α, β entry of the $(p-2)^2$-by-$(p-2)^2$ matrix $Q \otimes (z-1)^{-2}Q$ corresponds (under the mapping f) to the values of $w = [x^i, y^j]$ on $\left(b^k, (b^a)^\ell\right)$.*

Proof. Fix a $\beta = \left(b^k, (b^a)^\ell\right)$ and fix some $\alpha = (i, j)$. Then

$$\begin{aligned} f\left(w_\alpha(\beta)\right) &= f\left([b^{ik}, (b^a)^{j\ell}]\right) \\ &= \left(z^{ik} - 1\right)\left(z^{j\ell} - 1\right) \\ &= Q[ik, 1] \cdot (z-1)^{-2} Q[j\ell, 1] \\ &= Q[i, k] \cdot (z-1)^{-2} Q[j, \ell] \\ &= \left(Q \otimes (z-1)^{-2}\right)[\alpha, \beta]. \end{aligned}$$

□

7.2.5 Pulling it all together.

For the group $G = \mathrm{Hol}(C_p) = C_p \rtimes C_{p-1}$ we showed that there are exactly $p(p-2)$ orbits of noncommuting 2-tuples under the action of $\mathrm{Aut}(G)$. We classified these orbits into sets X, Y, and Z, and showed that for any tuple (g, h) of $X \cup Y \cup Z$ there is a word w such that $w(g, h) \neq 1$ and $w(g', h') = 1$ for all (g', h') in $X \cup Y \cup Z$ not equal to (g, h). Our proof is constructive, in that using linear algebra one could conjure up such a w directly.

Proof of Theorem I. In the notation established in this section, any tuple (g, h) $X \cup Y \cup Z$ can be isolated by a pure-commutator w. Hence for any possible map from $\varphi : G^2 \to G' = C_3$ that respects automorphisms of G and vanishes on commuting tuples, we can find a commutator word w that is identical, as a map, to φ. □

7.3 Proof of Theorem J.

By Corollary 7.2 we see that showing that

$$\mathbf{F}_2(G)' = (C_3)^3 \times (K_4)^4 \times (C_5)^3 \times (A_5)^{19}$$

immediately yields

$$|\mathbf{F}_2(G)| = 30^2 3^3 4^4 5^3 60^{19}.$$

As in the proof of Theorem I we want to show that all of the orbits of the action of $\mathrm{Aut}(G)$ on the noncommuting subset of G^n occur independently from one another. However, in the proof of Theorem I we utilized the fact that the commutator subgroup had prime order and hence commutator word maps could be realized as vectors over $\mathbb{F}_p$; this realization enabled us to utilize linear algebra to avoid explicitly finding words w that isolated each orbit. We cannot perform linear algebra over A_5 and instead proceed as follows.

There are 29 orbits of noncommutating 2-tuples over A_5. Moreover, each group appears the correct number of times. We will computational show that each orbit is independent of the others. To do this we first observe the following information about the orbits recorded in Table 2.

As seen in Table 2, the 29 orbits of noncommutating 2-tuples over A_5 can be grouped into 9 classes based on the orders of the first and second elements in the tuple. The group A_5 has the rather special property that all nontrivial elements of A_5 have prime order. This will allow us to work with each of the blocks independently from one another. We will call the set of elements (g, h) with $o(g) = p$ and $o(h) = q$ the (p, q)-block of A_5. This is a nonstandard notation that merely serves to incapsulate the blocks seen in Table 2.

Table 2: Orbit representatives of noncommuting 2-tuples of A_5 under $\mathrm{Aut}(A_5)$ showing the breakdown into blocks based on the orders of the elements in the tuple.

Orbit Rep. (g, h)	$(o(g), o(h))$	$\lvert\langle g, h\rangle'\rvert$.
((1, 2)(3, 4) , (1, 2)(4, 5))	(2 , 2)	3
((1, 2)(3, 4) , (1, 4)(2, 5))	(2 , 2)	5
((1, 2)(3, 4) , (1, 5, 2))	(2 , 3)	3
((1, 2)(3, 4) , (1, 3, 2))	(2 , 3)	4
((1, 2)(3, 4) , (1, 5, 3))	(2 , 3)	60
((1, 2)(3, 4) , (1, 5, 2, 4, 3))	(2 , 5)	5
((1, 2)(3, 4) , (1, 2, 5, 3, 4))	(2 , 5)	60
((1, 2)(3, 4) , (1, 4, 5, 2, 3))	(2 , 5)	60
((1, 2, 3) , (1, 2)(4, 5))	(3 , 2)	3
((1, 2, 3) , (1, 2)(3, 5))	(3 , 2)	4
((1, 2, 3) , (1, 4)(3, 5))	(3 , 2)	60
((1, 2, 3) , (1, 5, 2))	(3 , 3)	4
((1, 2, 3) , (1, 5, 3))	(3 , 3)	4
((1, 2, 3) , (1, 5, 4))	(3 , 3)	60
((1, 2, 3) , (1, 2, 5, 3, 4))	(3 , 5)	60
((1, 2, 3) , (1, 3, 2, 5, 4))	(3 , 5)	60
((1, 2, 3) , (1, 4, 3, 5, 2))	(3 , 5)	60
((1, 2, 3) , (1, 5, 4, 2, 3))	(3 , 5)	60
((1, 2, 3, 4, 5) , (1, 2)(3, 5))	(5 , 2)	5
((1, 2, 3, 4, 5) , (1, 2)(4, 5))	(5 , 2)	60
((1, 2, 3, 4, 5) , (1, 4)(2, 5))	(5 , 2)	60
((1, 2, 3, 4, 5) , (1, 4, 2))	(5 , 3)	60
((1, 2, 3, 4, 5) , (1, 4, 5))	(5 , 3)	60
((1, 2, 3, 4, 5) , (2, 3, 5))	(5 , 3)	60
((1, 2, 3, 4, 5) , (2, 4, 3))	(5 , 3)	60
((1, 2, 3, 4, 5) , (1, 2, 3, 5, 4))	(5 , 5)	60
((1, 2, 3, 4, 5) , (1, 3, 5, 4, 2))	(5 , 5)	60
((1, 2, 3, 4, 5) , (1, 4, 2, 3, 5))	(5 , 5)	60
((1, 2, 3, 4, 5) , (1, 4, 3, 2, 5))	(5 , 5)	60

Lemma 7.8. *For every commutator word w and noncommuting tuple (g,h) there is a commutator word v such that the following hold for $a,b \in G = A_5$:*

- *When $(o(a),o(b)) = (o(g),o(h))$ then $v(a,b) = w(a,b)$;*
- *If $(o(a),o(b)) \neq (o(g),o(h))$ then $v(a,b) = 1$.*

Proof. Let $o(g) = p$ and $o(h) = q$. Then consider the commutator word $v(x,y) = w\left(x^{(30/p)}, y^{(30/q)}\right)$. Then the following hold:

- If $(o(a),o(b)) = (p,q)$ then $v(a,b) = w(a,b)$.
- if $(o(a),o(b)) \neq (p,q)$ then either $a^{30/p}$ or $b^{30/q}$ is 1. Since w is a commutator, we conclude that $v(a,b) = 1$.

□

Corollary 7.9. *The group $\boldsymbol{F}_2(A_5)'$ is a direct product of 9 different groups $H_{(p,q)}$, where each $H_{(p,q)}$ corresponds to the set of commutator maps over the (p,q)-block.*

However, it is expected that there will be 60^4 commutator maps on the $(3,5)$-block, the $(5,3)$-block and the $(5,5)$-block. Rather than compute these directly, we utilize the the following lemma.

Lemma 7.10. *The group A_5^{19} occurs as a subgroup of $\boldsymbol{F}_2(A_5)'$. Hence $H_{(3,5)}, H_{(5,3)}$, and $H_{(5,5)} \cong A_5^4$.*

Proof. We note that A_5^{19} occurs as a quotient of $\mathbf{F}_2(A_5)'$. As observed in Theorem H, the group $\mathbf{F}_2(A_5)'$ is a subdirect product of subgroups of A_5. Hence, the only way to obtain A_5^{19} as a quotient of $\mathbf{F}_2(A_5)'$ is for it to occur as a subgroup. □

We now prove Theorem J.

Proof of Theorem J. Write

$$\mathbf{F}_2(A_5)' = \prod_{p,q\in\{2,3,5\}} H_{(p,q)}.$$

As noted in the above lemma, $H_{(3,5)}, H_{(5,3)}$ and $H_{(5,5)}$ are all isomorphic to A_5^4. Using Magma, we can calculate the following [9]:

- $H_{(2,2)} = C_3 \times C_5$.
- $H_{(2,3)} = H_{(3,2)} = C_3 \times C_4 \times A_5$.
- $H_{(2,5)} = H_{(5,2)} = C_5 \times A_5^2$.
- $H_{(3,3)} = K_4^2 \times A_5$.

□

Chapter 8

On the images of word maps on finite simple groups.

The image of various word maps in finite simple groups has been a topic of considerable interest. The now-proved Ore conjecture asked whether every element of a finite nonabelian simple group G is a commutator [67]. Recently, for any finite nonabelian simple group G, it was shown that if N is the product of two prime powers, then every element of G occurs as the product of two N-powers in G [36].

In examining word maps on finite simple groups, the question was asked at the conference 'Words and Growth' (Jerusalem, June 2012) if every subset of a finite simple group that is closed under endomorphisms of G occurs as the image of some word map. Lubotzky responded in the affirmative with the following theorem.

Theorem 8.1. *[69] Let G be a finite simple group, $n > 1$, and let $A \subseteq G$ such that A is closed under all endomorphisms of G, then there is a word $w \in \boldsymbol{F}_n$ such that $A = w(G)$.*

In the current section we extend Lubotzky's result by showing that the structure of w realizing A can be controlled in a very strong way; we also show that there are groups G and $A \subset G$ with A closed under endomorphisms such that A is not $w(G)$ for any w.

Theorem K. *Let G be a finite simple group, $n > 1$, and $A \subseteq G$ such that A is closed*

under automorphisms and $1 \in A$. *Assume that* $v \in \boldsymbol{F}_n$ *is not a law on* G. *Then there is a word* $w \in \langle v(\boldsymbol{F}_n)\rangle$ *such that* $A = w(G)$.

We note Theorem K shows that any subset of G that is closed under endomorphisms of G can occurs as the image of a word map w in $v(\mathbf{F}_n)$, it does not provide a description of w. However, it is possible in some cases to explicitly find w.

In the case of a general group G, one might ask if being closed under endomorphisms of G is a sufficient condition for a subset A to be $w(G)$ for some G. We will show this is false in Section 8.2, even in the case of abelian groups.

Theorem 8.2. *Let* G *be the cyclic group of order* 12. *Then*

$$A = \{x^2 : x \in G\} \cup \{x^3 : x \in G\},$$

is closed under endomorphisms of G, *but is not the image of any word map over* G.

8.1 Proof of Theorem K.

The group $\mathbf{F}_n(G)$ is the free group of rank n in the variety generated by G. In particular, any n-generated group in the variety generated by G occurs as a quotient of $\mathbf{F}_n(G)$. In H. Neumann's text *Varieties of Groups*, it is observed that for a finite simple group G, we have

$$\mathbf{F}_n(G) = G^{d(n)} \times \mathbf{F}_n(H)$$

where H is the direct product of all proper subgroups of G [84, pg 141] and $d(n)$ is the number of orbits of $\mathrm{Aut}(G)$ acting on the generating n-tuples of G. However, since this occurs without proof, we will prove a slightly weaker statement below, which will be

sufficient for our purposes. It is also the case that $G^{d(n)}$ is n-generated, but $G^{d(n)+1}$ is not [37].

Lemma 8.3. *Let G be a finite simple group. Then*

$$\boldsymbol{F}_n(G) = G^{d(n)} \times H,$$

for some group H.

Proof. Since a word map w respects endomorphisms of G, the map w is defined by its value on a set of representatives of the diagonal action of the automorphism groups of G on G^n. Moreover the number of possible values of w on an orbit representative $(\overline{g})$ is less than or equal to $|\langle\overline{g}\rangle|$, the size of the subgroup generated by the orbit. There are exactly $d(g)$ orbits of n-tuples corresponding to n-tuples that generate G, and some number of other orbits.

Therefore $\mathbf{F}_n(G)$ is a subgroup of the direct product $G^{d(n)} \times K$ where K is some direct product of proper subgroups of G. But, any group of rank n that satisfies the same laws as G occurs as a quotient of $\mathbf{F}_n(G)$. Hence $G^{d(n)}$ must occur as a quotient of $\mathbf{F}_n(G)$. □

Before proving Theorem K, we need the following lemma which follows from the work of Kantor and Guralnick, which depends heavily on the classification of finite simple groups [35, Corollary p. 745].

Lemma 8.4. *[35] For every nontrivial element g of a finite simple group G there is an $h \in G$ such that $G = \langle g, h\rangle$.*

In particular, it is the case that for any finite simple group G, the number $d(n)$ is greater than the number of conjugacy classes of G.

Proof of Theorem K. Since v is not a law on G, we know that $\langle v(G)\rangle = G$. By Lemma 8.3 we see that

$$\langle v\left(\mathbf{F}_n(G)\right)\rangle = \langle v(G^{d(n)})\rangle \times \langle v(H)\rangle = G^{d(n)} \times \langle v(H)\rangle,$$

for the appropriate group H.

Hence there is a word map $w \in v((\mathbf{F}_n(G))$ that is defined by its value on the generating tuples with a value from the group $G^{d(n)} \times v(H)$. Given A, we can write A as a union of $m \leq d(n)$ automorphism classes. There is a w so that on m different orbits of generating tuples of G, the value of w is one of the distinct automorphism classes in A and w vanishes elsewhere.

Now we need to find a word in $\langle v(\mathbf{F}_n)\rangle$ such that it induces the word map w on G. Consider the word maps induced by the words $x_1, \cdots, x_n$. These word maps generate $\mathbf{F}_n(G)$. Since $w \in \langle v(\mathbf{F}_n(G))\rangle$, we can write w as product of elements of the form $v(u_1, \cdots, u_n)$ such that each u_j is a product of $x_1, \cdots, x_n$. Consider this spelling of w in $x_1, \cdots, x_n$ as an element in $\mathbf{F}_n = \mathbf{F}(x_1, \cdots, x_n)$, we get a word in $\langle v(\mathbf{F}_n)\rangle$ that induces the word map w on G, which has image being A. □

8.2 Proof of Theorem 8.2.

Recall that any word $w(x_1, \ldots, x_n)$ can be written in the form

$$w = x_1^{k_1} \ldots x_n^{k_n} v(x_1, \ldots, x_n), \text{ where } v \in \mathbf{F}'_n.$$

By applying Nielson transformations to w, we see that w is automorphic to a word $w' = x_1^k c$ where k is $\mathbf{gcd}(k_1, \ldots, k_n)$ and $c \in \mathbf{F}'_n$. Moreover, w is a law on a group G if and only if w' is a law on G. Since automorphic words have the same image over a

group G, we see that $w(G) = w'(G)$. Hence for a finite abelian group the only images of word maps are exactly the images of the power maps, e.g., $\{x^k : x \in G\}$ for some k. We now prove Theorem 8.2 showing that not every subset of a group G that is closed under endomorphisms occurs as word map.

Proof of Theorem 8.2. Let $G = \langle a | a^{12} \rangle$ be the cyclic group of order 12, then the images of the power maps in G are exactly

$$1 = \{x^{12}\}, G = \{x^1\}, \{1, a^2, a^4, a^6, a^8, a^{10}\} = \{x^2\}, \{1, a^3, a^6, a^9\} = \{x^3\}$$

$$\{1, a^4, a^8\} = \{x^4\}, \{1, a^6\} = \{x^6\}.$$

Any union of subsets closed under endomorphisms is closed under endomorphisms. However, there is no power map, equivalently no word map, that has the set

$$\{1, a^2, a^3, a^4, a^6, a^8, a^9, a^{10}\}$$

as its image. □

Chapter 9

Word maps and character tables.

The connection between certain word maps and character tables has been a source for many new ideas and theorems, especially as it relates to the finite simple groups. In this section we present a tool, developed by the author with Steve Goldstein and Michael Stemper, to better understand this connection [14]. We also prove Theorem L.

Theorem L. *Let w be the word x^2. There are finite groups G and H of order 64 such that G and H have the same character table, but $|w(G)| \neq |w(H)|$.*

To prove that a property $\mathcal{P}$ of a group G cannot be determined from the character table of G, one is often forced to look for a group H such that H has the same character table as G, but H does not have property $\mathcal{P}$. To aid in this endeavor, the author with Steve Goldstein and Michael Stemper constructed a database of all finite groups with order less than 2000 (excluding 1024) that share a character table [14]. We mention that an earlier project was undertaken by Skrzipczyk in which she searched for a minimal example of Brauer pairs [98]. Our approaches for distinguishing tables are different; we are grateful to Gerhard Hiss for assisting us in obtaining copies of Skrzipczyk's work.

In addition the structure of the database itself is of some interest. For example, we can expand the table originally found in the book by Lux and Pahlings [72, Table 2.2 pg 136]:

Order	Number of Groups	Number of Tables
2	1	1
4	2	2
8	5	4
16	14	11
32	51	35
64	267	146
128	2328	904
256	56092	9501
512	10494213	360135

The chapter is slightly different from the rest of the dissertation. Sections 9.1 and 9.2 contain historical material and well-known properties of character tables; they are included for motivation. Section 9.3 contains some of our observations from the database about character tables and word maps including the example promised in Theorem L.

9.1 Definitions and Previous Results.

For a finite group G, write the character table of G as $CT(G)$. We note that in displaying $CT(G)$, we are forced to order the rows and columns. However, we adopt the convention that any rearrangement of the rows and columns of $CT(G)$ is still, as a character table, equal to $CT(G)$. Hence $CT(G) = CT(H)$ means that some permutation of the rows and columns of $CT(H)$ gives the table $CT(G)$. Let **Char** denote the class of finite groups determined by their character tables, i.e., $G \in$ **Char** means that G and H have the same character table if and only if $G \cong H$.

It is a standard fact that all finite abelian groups are in **Char**. There has been quite a bit of interest in showing that various other families of groups are subsets of **Char**. Since there appears to be no source compiling many of the early results we will do our best to provide a short history of the subject below. However, the uninterested reader can move directly to the next section.

In 1957, Nagao [82] showed that the symmetric groups are in **Char**. Oyama [89] was able to show that the alternating groups are in **Char** in 1964. In 1965, Yokonuma [103] also showed that the wreath products of the cyclic group of order p, for p a prime with symmetric groups are in **Char**. Yokonuma calls a group a *Nagao group* if $G \in$ **Char**.

Higman [43] gave an alternative proof that the alternating groups are in **Char**, and that the Janko group of order 175,560 was in **Char** in 1969. Of greater interest Higman observed, in the same paper, that from the character table of a group G one can read off the the primes divisors of the centralizer of the elements of a conjugacy class. In 1971, Pahlings [90] showed that the Weyl-Group of type F_4, was contained in **Char**. Shortly thereafter, through 1972-74, Lambert showed that the Suzuki groups, the groups $\mathrm{PSL}(2,q)$, and groups of Ree type [60], $\mathrm{PSL}(3,q)$ and $\mathrm{PSU}(3,q)$ [61], and $\mathrm{SL}(n,2)$ [62] are in **Char**. Klemm [54] proved many of the same results as Lambert, almost simultaneously in 1973. Pahlings [91] also showed that the finite groups in Fischer's [26] list of groups genenerated by 3-transpositions, are in **Char**, in 1974. In 1976, Pahlings proved that the Weyl groups $W(D_n)$ of the simple Lie algebras of type D_n [91], $\mathrm{Sp}(2n,2^k), \mathrm{PSU}(n,2^k)$, the orthogonal groups $\mathrm{O}^+(2n,2^k)$ and $\mathrm{O}^-(2n,2^k)$, and the orthogonal groups ${}^{\epsilon}\mathrm{O}^+(n,5)$ and ${}^{\epsilon}\mathrm{O}^-(n,5)$ are in **Char** [92]. In 1977 and 1979, Herzog and Wright showed that the groups $G_2(q)$ where q is coprime to 6 [41], and $G_2(q)$ where $q = 3^f$ [42] are in **Char**.

From the classification of finite simple groups [22] and work by Landazuri and Seitz [63], all finite simple groups are in **Char**.

Recently, work of Humphries and Dane Skabelund [44] showed that all groups of square-free order are in **Char**.

With the restriction to groups of cube-free order, work by Gorenstein and Walter [31, 32, 33] establishes that the only finite simple groups of cube-free order are contained in the family $\mathrm{PSL}(2, p)$ and are all determined by their character tables.

9.2 Character-theoretic Properties of a Group.

If $\mathcal{P}$ is a group-theoretic property of G, then we will say that $CT(G)$ determines $\mathcal{P}$ if all groups with the same character table as G have property $\mathcal{P}$. Heuristically, properties $\mathcal{P}$ that are determined by $CT(G)$ are called character-theoretic. Many such properties can be found in Isaacs [47]. For example, for a finite group G, $CT(G)$ determines the following:

- The order of the derived subgroup G'.
- The order of the center $Z(G)$.
- The total number of normal subgroups of G, and their orders.
- Whether or not G is solvable.
- Whether or not G is nilpotent.

For a normal subgroup N of G identified as a union of conjugacy classes, $CT(G)$ determines $CT(G/N)$ ([47] 2.22). However, in general one cannot tell from $CT(G)$ the

isomorphism type of N. The lattice of normal subgroups of G, where each subgroup is identified as a union of conjugacy classes is determined by $CT(G)$, that is to say, from $CT(G)$ one can read off all of the normal subgroups of G, their orders, and all inclusion relations between them. The correspondence theorem holds over this action: if $\overline{M}$ is a normal subgroup of G/N identified as a union of conjugacy classes in $CT(G/N)$, then the normal subgroup M of G containing N and mapping to $\overline{M}$ can be identified as a union of conjugacy classes in $CT(G)$. We will find it useful to distinguish the difference between the phrases "$CT(G)$ determines the isomorphism type of N", and "$CT(G)$ determines the conjugacy classes contained in N". We will say that $CT(G)$ class-determines N, to mean that $CT(G)$ determines the conjugacy classes contained in N.

As stated above, $CT(G)$ always determines whether or not G is solvable. For a solvable group G, the derived length of G is not determined by $CT(G)$; this was noted by Mattarei [75, 76].

Garrison [29] showed that if G is not solvable, then $CT(G)$ does not class-determine $\Phi(G)$. He further showed that is G is solvable, then $CT(G)$ class-determines $\Phi(G)$. Hence $CT(G)$ determines $|\Phi(G)|$. If G has cube-free order, then not only does $CT(G)$ class-determine $\Phi(G)$, it determines the isomorphism type of $\Phi(G)$.

9.3 Applications and observations.

We highlight two interesting observations from our database, the existence of 2-groups G, H with different derived length and $CT(G) = CT(H)$, and that the image of the word x^2 is not determined from the character table.

9.3.1 Derived Length.

Using the character table of a finite group, one can determine if the group is solvable by constructing the lattice of normal subgroups of G and looking for a chain of normal subgroups such that the index of each subgroup in the next is a prime power. Moreover, the conjugacy classes contained in the derived subgroup can be readily identified from the character table, as can the commutators. However, the derived length of the group is not observable from the character table by itself.

Mattarei first observed that the derived lengths cannot be determined from the character table of a group; meaning that there are groups G and H with the same character table, but with different derived lengths [75]. In later work he produced p-groups G and H with the same character table, but different derived lengths [76]. However, for his p-group examples, Mattarei required that $p \geq 5$ and the groups themselves have order p^{11}. Using our database, we were able to identify the following examples of groups of order $512 = 2^9$ that have the same character table, but different derived lengths; moreover, we can easily verify that they are the smallest possible examples in terms of order.

Example 9.1. Search the database...

9.3.2 Character Theoretic Words.

It is well-known that the conjugacy classes of a group G whose elements occur as commutaters can be identified from the character table of G, i.e., looking at the character values over g we can tell if there is some $x, y \in G$ with $[x, y] = x^{-1}y^{-1}xy = g$. Explicitly, we have the following lemma, which is an exercise in [47, Exercise 3.10] and a lemma in [72, Lemma 2.6.4].

Lemma 9.2. *Let G be a finite group and let $g \in G$. There is some $x, y \in G$ with $g = [x, y]$ if and only if*

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0.$$

The character table can also be used to determine the number of ways g occurs as a commutator. The recently proven Ore conjecture asked whether every element of a finite nonabelian simple group G occured as a commutator. The proof of the Ore conjecture by Liebeck, O'Brien, Shalev, and Tiep utilized the character theoretic nature of the word $w = x^{-1}y^{-1}xy$ [67].There has been some interest over finite nonabelian simple groups of the probability that g occurs as a commutator [28]; this probability is also determined by the character table of G.

Besides $[x, y]$, there are results known for other words, for example $w = x^2y^2$. The word w is also character theoretic in that:

Lemma 9.3. *[68, Lemma 2.2] Let G be a finite group and $g \in G$. The number of ways g occurs as a product of two squares is*

$$|G| \cdot \sum_{\chi \in \mathrm{Irr}(G), \chi \mathrm{real}} \frac{\chi(g)}{\chi(1)}.$$

The same authors who proved the Ore conjecture also showed that every element of a finite nonabelian simple group is a product of two squares [68].

A natural question to ask is whether for every word w, there is some way to deduce from the character table of a group G whether or not an element $g \in G$ occurs in the image of w. As seen above when $w = [x, y]$ or $w = x^2y^2$ this is the case. However, when $w = x^p$ for p an odd prime, we note that the extraspecial groups of order p^3 share a character table. Because one of the extraspecial groups of order p^3 has exponent p and

one has exponent p^2, the image of w cannot be extracted from the character table by itself.

What about the word $w = x^2$. By using the character table database to look for groups G and H such G and H have the same character table, but the number of squares in G is different than the number in H we found the following example, which proves Theorem L.

Example 9.4. Let G be SmallGroup$(64, 100)$ and let H be SmallGroup$(64, 98)$. Then G and H share a character table. But, $|\{x^2 : x \in G\}| = 6$ and $|\{x^2 : x \in H\}| = 5$.

Hence the character table can determine the group generated by $w(G)$, but not $w(G)$ when $w = x^2$. The question of what words w have the property that $w(G)$ is determined from the character table, and what words w have the property that $\langle w(G) \rangle$ is open.

Chapter 10

Final Words.

Word maps continue to find interesting applications. The theorems we examined above do not represent the limit of the theory, but merely some of the work the author has done in his study. There are a number of interesting directions one could take the study of word maps. We mention some of these below.

In the spirit of Theorem A and B about the number of not images or not solutions of a word map, we ask the following vague question.

Question 10.1. What properties P of group elements can be used to bound the order of G in the following sense: if exactly n elements of G satisfy property P, then $|G| \leq f(n)$ for some function f.

Our Theorems C and D started the formal study of chirality. There are many open questions regarding chirality, weak chirality, and other properties of word maps. Originally the 2-Engel word was proposed as a potential example of a witness to the chirality of $\mathbf{F}_2$. The author and Turbo Ho utilized automated theorem proving software to see that the image of the 2-Engel word is always closed under inversion [16]. We ask the following question, which could be partially answered via computation.

Question 10.2. For n greater than 3, is the image of the n-Engel word closed under inversion for all groups.

Theorem G showed that the probability distributions induced by word maps can be used to determine whether or not a group is nilpotent. We ask:

Question 10.3. What other properties of a group can be determined from the probability distributions induced by word maps? Can the probability distributions determine whether or not a group is a Frobenius group?

Another interesting direction of study would be to understand how the structures G and $(G, *_w)$ relate for well-behaved words w.

Reduced free groups continue to attract attention due to their large number of automorphisms and nice properties. Extending the results of Theorems H, I, and J would surely prove interesting. The author's own hope is to use reduced free groups as platform groups for group-theoretic cryptography.

We note that the author is involved in a few projects aiming to provide a computational version of Theorem K.

In Chapter 9 we presented Theorem L, which shows that when $w = x^2$, the set $w(G)$ is not determined by the character table. In this vein we ask the following.

Question 10.4. What words w have the property that $w(G)$ is determined from the character table?

It would seem that there are many words left unsaid about word maps on groups. There are many other directions that one could investigate. The author welcomes friendly words and collaborations.

Appendix A

Calculating Chirality.

The following functions can be used to calculate the chirality of a given group. We used them to verify our claims about chirality.

```
Orb:=function(x,G,B,f)
Y:=[];
for g in B do
s:=g@@f;
Include(~Y,s(x));
end for;
return Y;
end function;

make_orbits:=function(G)
A:=AutomorphismGroup(G);
f,B:=PermutationRepresentation(A);
is_sym:=true;
X:={};
for x in ConjugacyClasses(G) do
include_x:=true;
```

```
for y in X do
if Order(y[1]) eq Order(x[3]) and x[3] in y then
include_x:=false;
break y;

end if;
end for;
if include_x then
Include(~X,Orb(x[3],G,B,f));
is_sym:=is_sym and x[3]^-1 in Orb(x[3],G,B,f);
end if;
end for;
return X, is_sym;
end function;

contains_witness:=function(G,r,g,Potential_Witnesses)
H:=sub<G|r,g>;
for x in Potential_Witnesses do
if x in H then
return true;
end if;
end for;
return false;
end function;
```

```
two_words_constructor_chirality:=function(G)
f,B:=PermutationRepresentation(AutomorphismGroup(G));
Orbits:={{(s@@f)(g): s in B}: g in G};
Orbits:=[O:O in Orbits];
Reps:=[Random(O): O in Orbits];
Potential_Witness_Indeces:=[i: i in [1..#Orbits] | not Reps[i]^-1 in Orbits[i]];
Orbit_Witness:=[];
for i in Potential_Witness_Indeces do
if not Orbits[i] in Orbit_Witness then
Append(~Orbit_Witness,Orbits[i]);
for j in Potential_Witness_Indeces do
if Reps[i]^-1 in Orbits[j]
then Append(~Orbit_Witness,Orbits[j]); break j; end if;
end for;
end if;
end for;
Potential_Witnesses:=[];
for i in [1..#Potential_Witness_Indeces] do
for x in Orbits[Potential_Witness_Indeces[i]] do
Append(~Potential_Witnesses,x);
end for;
end for;
Two_Orbits:={{[r,(s@@f)(g)]: s in B| (s@@f)(r) eq r}:
```

```
 r in Reps, g in G |(r,g) ne Id(G) and
 contains_witness(G,r,g,Potential_Witnesses) eq true};
M:=[Random(X):X in Two_Orbits];
//M:=[[g,h]:g,h in G |(g,h) ne Id(G)];
dum_N:=[];
for i in [1..#M] do
Append(~dum_N,Id(G));
end for;
Node_List:={dum_N};
New_Node_List:={dum_N};
COUNT:=0;
while #New_Node_List gt 0 do
COUNT+:=1;
dum_New_Node_List:={};
for N in New_Node_List do
R:=[];S:=[];
for i in [1..#M] do
Append(~R,N[i]*(M[i][1]));
Append(~S,N[i]*(M[i][2]));

end for;
if not R in Node_List then
     Node_List join:= {R};
     dum_New_Node_List join:={R};
```

```
end if;
if not S in Node_List then
   Node_List join:= {S};
   dum_New_Node_List join:={S};
end if;


end for;
New_Node_List:=dum_New_Node_List;
     //"************************";
//#Node_List;
//if #Node_List gt 100000 then
// return Node_List;
//%end if;
    //"************************";
end while;
Prob:={};
is_weakly_chiral:=false;
is_chiral:=false;
for N in Node_List do
Occurences:=[0:i in [1..#Potential_Witness_Indeces]];
for ii in [1..#N] do
for i in [1..#Potential_Witness_Indeces] do
if N[ii] in Orbit_Witness[i] then Occurences[i]+:=1;
//break i;
```

```
end if;
end for;
end for;
Include(~Prob,Occurences);
end for;
for P in Prob do
for i in [1..#P/2] do
if P[2*i] ne P[2*i-1] then
is_weakly_chiral:=true;
if P[2*i]*P[2*i-1] eq 0 then
is_chiral:=true;
end if;
end if;
end for;
end for;
return Prob,is_weakly_chiral,is_chiral;
end function;



test_powers_derived:=function(i,j)
/*Creates Orbits and checks if the
elements not isomorphic to their inverses are kth powers*/
G:=SmallGroup(i,j);
X,t:=make_orbits(G);
```

```
N:={x[1]: x in X | not x[1]^-1 in x};
if #N eq 0 then
return true; /*"G is automorphically achiral.";*/
end if;

D:=DerivedSubgroup(G);
for d in Divisors(Exponent(G)) do
H:=sub<G|{x^d: x in G},D>;
for n in N do
if n in H and not n in {x^d: x in G} then
return false;
end if;
end for;
end for;
return true;
end function;
```

Bibliography

[1] M. Abert, *On the probability of satisfying a word in a group*, J. Group Theory, 9 (2006), pp. 685–694.

[2] A. Amit and U. Vishne, *Characters and solutions to equations in finite groups*, J. Algebra Appl., 10 (2011), pp. 675–686.

[3] C. Ashurst, *Fibres of words in finite groups, a probabilistic approach*, 2012. Thesis (Ph.D.)–University of Bath.

[4] E. Bannai, M. Deza, P. Frankl, A. C. Kim, and M. Kiyota, *On the number of elements which are not nth powers in finite groups*, Comm. Algebra, 17 (1989), pp. 2865–2870.

[5] R. Bastos, C. Monetta, and P. Shumyatsky, *A criterion for metanilpotency of a finite group*, J. Group Theory, 21 (2018), pp. 713–718.

[6] R. Bastos and P. Shumyatskiĭ, *A sufficient condition for the nilpotency of a commutator subgroup*, Sibirsk. Mat. Zh., 57 (2016), pp. 978–980.

[7] B. Baumslag and J. Wiegold, *A sufficient condition for nilpotency in a finite group*. arXiv:1411.2886v1[math.GR].

[8] R. Belshoff, J. Dillstrom, and L. Reid, *Finite groups with a prescribed number of cyclic subgroups*, Communications in Algebra, (2018), pp. 1–14.

[9] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265. Computational algebra and number theory (London, 1993).

[10] J. N. Bray, J. S. Wilson, and R. A. Wilson, *A characterization of finite soluble groups by laws in two variables*, Bull. London Math. Soc., 37 (2005), pp. 179–186.

[11] G. Chen and W. Shi, *Finite groups with 30 elements of maximal order*, Appl. Categ. Structures, 16 (2008), pp. 239–247.

[12] I. Chiswell, *A course in formal languages, automata and groups*, Universitext, Springer-Verlag London, Ltd., London, 2009.

[13] W. Cocke, *Two characterizations of finite nilpotent groups*, J. Group Theory, 21 (2018), pp. 1111–1116.

[14] W. Cocke, S. Goldstein, and M. Stemper, *Determining groups with the same character table.* in preparation.

[15] W. Cocke and M.-C. Ho, *Word maps in finite simple groups.* submitted.

[16] ——, *On the symmetry of images of word maps in groups*, Comm. Algebra, 46 (2018), pp. 756–763.

[17] ——, *The probability distribution of word maps on finite groups*, J. Algebra, 518 (2019), pp. 440–452.

[18] W. Cocke, I. M. Isaacs, and D. Skabelund, *On the number of elements that are not kth powers in a group*, Arch. Math. (Basel), 105 (2015), pp. 529–538.

[19] W. Cocke and S. Jensen, *Not solutions to word maps.* submitted.

[20] W. Cocke and S. Jensen, *The sequence of non k-th powers of a finite group G*, Communications in Algebra, available online (2019), pp. 1–6.

[21] W. Cocke and G. Venkataraman, *On the number of elements of maximal order in a group*, The American Mathematical Monthly, 126 (2019), pp. 66–69.

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

[23] A. L. Edmonds, *The partition problem for equifacetal simplices*, Contributions to Algebra and Geometry, 50 (2009), pp. 195–213.

[24] N. Elkies, *Word evaluating to a group element and its inverse with different frequency.* MathOverflow. URL:https://mathoverflow.net/q/137802 (version: 2013-07-26).

[25] B. Fine, *The free groups in the dihedral variety*, Arch. Math. (Basel), 46 (1986), pp. 193–197.

[26] B. Fischer, *Finite groups generated by* 3*-transpositions. I*, Invent. Math., 13 (1971), pp. 232–246.

[27] A. Freitas de Andrade and A. Carrazedo Dantas, *A sufficient condition for nilpotency of the nilpotent residual of a finite group*, J. Group Theory, 21 (2018), pp. 289–293.

[28] S. Garion and A. Shalev, *Commutator maps, measure preservation, and T-systems*, Trans. Amer. Math. Soc., 361 (2009), pp. 4631–4651.

[29] S. Garrison, *Determining the Frattini subgroup from the character table*, Canad. J. Math., 28 (1976), pp. 560–567.

[30] N. L. Gordeev, B. E. Kunyavskiĭ, and E. B. Plotkin, *Geometry of word equations in simple algebraic groups over special fields*, Uspekhi Mat. Nauk, 73 (2018), pp. 3–52.

[31] D. Gorenstein and J. H. Walter, *The characterization of finite groups with dihedral Sylow 2-subgroups. I*, J. Algebra, 2 (1965), pp. 85–151.

[32] ——, *The characterization of finite groups with dihedral Sylow 2-subgroups. II*, J. Algebra, 2 (1965), pp. 218–270.

[33] ——, *The characterization of finite groups with dihedral Sylow 2-subgroups. III*, J. Algebra, 2 (1965), pp. 354–393.

[34] R. M. Guralnick, *Expressing group elements as commutators*, Rocky Mountain J. Math., 10 (1980), pp. 651–654.

[35] R. M. Guralnick and W. M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra, 234 (2000), pp. 743–792. Special issue in honor of Helmut Wielandt.

[36] R. M. Guralnick, M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep, *Surjective word maps and Burnside's p^aq^b theorem*, Invent. Math., 213 (2018), pp. 589–695.

[37] P. Hall, *The eulerian functions of a group*, The Quarterly Journal of Mathematics, os-7 (1936), pp. 134–151.

[38] Z. Han and R. Song, *Finite groups having exactly 44 elements of maximal order*, Adv. Math. (China), 45 (2016), pp. 61–66.

[39] Z. Han and L. Zhang, *Finite groups having exactly 42 elements of maximal order*, Ital. J. Pure Appl. Math., (2017), pp. 351–354.

[40] Z. J. Han and G. Y. Chen, *Solvability of finite groups with* $2pq$ *elements of maximal order*, Xinan Shifan Daxue Xuebao Ziran Kexue Ban, 29 (2004), pp. 198–200.

[41] M. Herzog and D. Wright, *Characterization of a family of simple groups by their character table*, J. Austral. Math. Soc. Ser. A, 24 (1977), pp. 296–304.

[42] ——, *Characterization of a family of simple groups by their character table. II*, J. Austral. Math. Soc. Ser. A, 30 (1980/81), pp. 168–170.

[43] G. Higman, *Construction of simple groups from character tables*, (1971), pp. 205–214.

[44] S. P. Humphries and D. C. Skabelund, *Character tables of metacyclic groups*, Glasg. Math. J., 57 (2015), pp. 387–400.

[45] A. Iñiguez and J. Sangroniz, *Words and characters in finite p-groups*, J. Algebra, 485 (2017), pp. 230–246.

[46] N. Iiyori and H. Yamaki, *On a conjecture of Frobenius*, Bull. Amer. Math. Soc. (N.S.), 25 (1991), pp. 413–416.

[47] I. M. Isaacs, *Character theory of finite groups*, AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].

[48] ——, *Finite group theory*, vol. 92 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2008.

[49] ——, *Algebra: a graduate course*, vol. 100 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2009. Reprint of the 1994 original.

[50] I. M. Isaacs and G. R. Robinson, *On a theorem of Frobenius: solutions of* $x^n = 1$ *in finite groups*, Amer. Math. Monthly, 99 (1992), pp. 352–354.

[51] S. V. Ivanov, *Infinite groups almost all of whose elements are prime powers*, arXiv preprint arXiv:1702.01378, (2017).

[52] Q. Jiang and C. Shao, *Finite groups with 24 elements of maximal order*, Front. Math. China, 5 (2010), pp. 665–678.

[53] K. Kearnes, *Relatively free groups in* $var(s_3)$. MathOverflow. URL:https://mathoverflow.net/q/310670 (version: 2018-09-16).

[54] M. Klemm, *Charakterisierung der Gruppen* PSL(2, p^f) *und* PSU(3, p^{2f}) *durch ihre Charaktertafel*, J. Algebra, 24 (1973), pp. 127–153.

[55] A. A. Klyachko and A. A. Mkrtchyan, *How many tuples of group elements have a given property?*, Internat. J. Algebra Comput., 24 (2014), pp. 413–428. With an appendix by Dmitrii V. Trushin.

[56] L. G. Kovács, *Free groups in a dihedral variety*, Proc. Roy. Irish Acad. Sect. A, 89 (1989), pp. 115–117.

[57] T. J. Laffey, *The number of solution of $x^p = 1$ in a finite group*, Math. Proc. Cambridge Philos. Soc., 80 (1976), pp. 229–231.

[58] ——, *The number of solutions of $x^3 = 1$ in a 3-group*, Math. Z., 149 (1976), pp. 43–45.

[59] T. Y. Lam, *A first course in noncommutative rings*, vol. 131 of Graduate Texts in Mathematics, Springer-Verlag, New York, second ed., 2001.

[60] P. J. Lambert, *Characterizing groups by their character tables. I*, Quart. J. Math. Oxford Ser. (2), 23 (1972), pp. 427–433.

[61] ——, *Characterizing groups by their character tables. II*, Quart. J. Math. Oxford Ser. (2), 24 (1973), pp. 223–240.

[62] ——, *Characterizing groups by their character tables. III*, Quart. J. Math. Oxford Ser. (2), 25 (1974), pp. 29–40.

[63] V. Landazuri and G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra, 32 (1974), pp. 418–443.

[64] L. Lévai and L. Pyber, *Profinite groups with many commuting pairs or involutions*, Arch. Math. (Basel), 75 (2000), pp. 1–7.

[65] M. Levy, *On the probability of satisfying a word in nilpotent groups of class 2*, arXiv preprint arXiv:1101.4286, (2011).

[66] L. Libkin, *Elements of finite model theory*, Texts in Theoretical Computer Science. An EATCS Series, Springer-Verlag, Berlin, 2004.

[67] M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep, *The Ore conjecture*, J. Eur. Math. Soc. (JEMS), 12 (2010), pp. 939–1008.

[68] ——, *Products of squares in finite simple groups*, Proc. Amer. Math. Soc., 140 (2012), pp. 21–33.

[69] A. Lubotzky, *Images of word maps in finite simple groups*, Glasg. Math. J., 56 (2014), pp. 465–469.

[70] M. S. Lucido and M. R. Pournaki, *Elements with square roots in finite groups*, Algebra Colloq., 12 (2005), pp. 677–690.

[71] ——, *Probability that an element of a finite group has a square root*, Colloq. Math., 112 (2008), pp. 147–155.

[72] K. Lux and H. Pahlings, *Representations of groups*, vol. 124 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2010. A computational approach.

[73] R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Classics in Mathematics, Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition.

[74] G. S. Makanin, *Decidability of the universal and positive theories of a free group*, Izv. Akad. Nauk SSSR Ser. Mat., 48 (1984), pp. 735–749.

[75] S. Mattarei, *Character tables and metabelian groups*, J. London Math. Soc. (2), 46 (1992), pp. 92–100.

[76] ——, *An example of p-groups with identical character tables and different derived lengths*, Arch. Math. (Basel), 62 (1994), pp. 12–20.

[77] W. McCune, *Prover9 and mace4*. `http://www.cs.unm.edu/~mccune/prover9/`, 2005–2010.

[78] J. I. Merzljakov, *Positive formulae on free groups*, Algebra i Logika Sem., 5 (1966), pp. 25–42.

[79] G. A. Miller, *Groups which admit automorphisms in which exactly three-fourths of the operators correspond to their inverses*, Bull. Amer. Math. Soc., 35 (1929), pp. 559–565.

[80] V. S. Monakhov, *A metanilpotency criterion for a finite solvable group*, Tr. Inst. Mat. Mekh., 23 (2017), pp. 253–256.

[81] ——, *The nilpotency criterion for the derived subgroup of a finite group*, Probl. Fiz. Mat. Tekh., (2017), pp. 58–60.

[82] H. Nagao, *On the groups with the same table of characters as symmetric groups*, J. Inst. Polytech. Osaka City Univ. Ser. A., 8 (1957), pp. 1–8.

[83] B. H. Neumann, *Identical relations in groups. I*, Math. Ann., 114 (1937), pp. 506–525.

[84] H. Neumann, *Varieties of groups*, Springer-Verlag New York, Inc., New York, 1967.

[85] J. Nielsen, *Die Isomorphismengruppe der freien Gruppen*, Math. Ann., 91 (1924), pp. 169–209.

[86] N. Nikolov, *Algebraic properties of profinite groups*, arXiv preprint arXiv:1108.5130, (2011).

[87] N. Nikolov and D. Segal, *A characterization of finite soluble groups*, Bull. Lond. Math. Soc., 39 (2007), pp. 209–213.

[88] O. Ore, *Some remarks on commutators*, Proc. Amer. Math. Soc., 2 (1951), pp. 307–314.

[89] T. Oyama, *On the groups with the same table of characters as alternating groups*, Osaka J. Math., 1 (1964), pp. 91–101.

[90] H. Pahlings, *Über die Charakterentafel der Weyl-Gruppe vom Typ* F_4, Mitt. Math. Sem. Giessen, (1971), pp. 115–119.

[91] H. Pahlings, *On the character tables of finite groups generated by* 3*-transpositions*, Comm. Algebra, 2 (1974), pp. 117–131.

[92] ——, *Characterization of groups by their character tables. I, II*, Comm. Algebra, 4 (1976), pp. 111–153; ibid. 4 (1976), no. 2, 155–178.

[93] D. Puder and O. Parzanchevski, *Measure preserving words are primitive*, J. Amer. Math. Soc., 28 (2015), pp. 63–97.

[94] M. Ram Murty and S. Pathak, *Evaluation of the quadratic Gauss sum*, Math. Student, 86 (2017), pp. 139–150.

[95] D. Segal, *Words: notes on verbal width in groups*, vol. 361 of London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 2009.

[96] A. Shalev, *Some results and problems in the theory of word maps*, in Erdös centennial, vol. 25 of Bolyai Soc. Math. Stud., János Bolyai Math. Soc., Budapest, 2013, pp. 611–649.

[97] W. J. Shi, *Arithmetical properties of finite groups*, in Groups St. Andrews 2005. Vol. 2, vol. 340 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 2007, pp. 646–653.

[98] E. Skrzipczyk, *Charaktertafeln von p-Gruppen.* Diplomarbeit, Lehrstuhl D für Mathematik, RWTH-Aachen, Aachen (1992).

[99] L. Solomon, *The solution of equations in groups*, Arch. Math. (Basel), 20 (1969), pp. 241–247.

[100] M. Tărnăuceanu, *Finite groups with a certain number of cyclic subgroups*, The American Mathematical Monthly, 122 (2015), pp. 275–276.

[101] ——, *Finite groups with a certain number of cyclic subgroups ii*, preprint, the arXiv, (2016).

[102] Y. Xu, J. Gao, and H. Hou, *Finite groups with $6PQ$ elements of the largest order*, Ital. J. Pure Appl. Math., (2013), pp. 277–284.

[103] T. Yokonuma, *On a property of some generalized symmetric groups*, J. Fac. Sci. Univ. Tokyo Sect. I, 12 (1965), pp. 193–211 (1965).