APPROVAL PAGE FOR GRADUATE THESIS OR PROJECT

GS-13

SUBMITTED IN PARTIAL FULFILLMENT OF REQUIREMENTS FOR DEGREE OF MASTER OF SCIENCE AT CALIFORNIA STATE UNIVERSITY, LOS ANGELES BY

Ezekiel D. Golvin
Candidate

Mathematics
Department

TITLE: **LOWER BOUNDS ON THE ORDERS OF THE TERMS OF THE DERIVED SERIES OF FINITE 2-GROUPS OF DERIVED LENGTH 3**

APPROVED:

Dr. Mike Krebs Committee Chairperson	Signature
Dr. Gary Brookfield Faculty Member	Signature
Dr. Kristin Webster Faculty Member	Signature
Dr. Grant Fraser Department Chairperson	Signature

DATE: **June 9, 2014**

LOWER BOUNDS ON THE ORDERS OF THE TERMS OF THE DERIVED SERIES OF FINITE 2-GROUPS OF DERIVED LENGTH 3

A Thesis

Presented to

The Faculty of the Department of Mathematics

California State University, Los Angeles

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Mathematics

By

Ezekiel D. Golvin

June 2014

ACKNOWLEDGMENTS

Thank you to Dr. Mike Krebs, without whom this thesis would not exist. In addition, thank you to my thesis committee, and the entirety of the math department at Cal State LA.

ABSTRACT

Lower Bounds On The Orders Of The Terms

Of The Derived Series Of Finite 2-groups Of Derived Length 3

By

Ezekiel D. Golvin

Let G be a finite group with derived length three, such that the number of elements in G is a power of 2, and G, G', and G'' form the derived (commutator subgroup) series of G, where G''' is the trivial group. Let the order of G/G' be 2^a, and the order of G'/G'' be 2^b. Then, $a \geq 3$ and $b \geq 3$. This result comes from the work of P. Hall and D. Gorenstein. In a companion thesis [1], A. Al-Fares proves a partial converse of this statement.

TABLE OF CONTENTS

CHAPTER 1

A Motivating Problem

The research for thesis began with a short, but complex, question: Can we construct an expander family? This turned out to be too broad. After much work, the research came to be directed upon commutator subgroups of nonabelian 2-groups, the basis by which we attempted to construct an expander family initially. The pages that follow are an attempt to find bounds for the orders of quotient groups in the derived series of such groups, given that their derived length is short (in this paper, derived length 3). We will prove that, if G is a finite nonabelian 2-group of derived length 3, then the first two quotients of terms in the derived series must have order at least 8.

This section will serve to introduce nomenclature that drove the research, as well as introduce the motivation for this work. Much of the foundational elements for the group theoretic material can be found in [2]; this paper will assume some familiarity with topics in group theory. To make some notation precise, if we have G a group and H a subgroup of G, we write $H \leq G$. If H is a proper subgroup, we make this "strict," and say $H < G$. The usage of capital letters will almost always refer to a group, whereas lowercase letters will almost always refer to elements of a group.

In addition, if H and K are subgroups of G, then $H \cap K$ and (if H or K is normal in G) $HK = \{hk \mid h \in H,\, k \in K\}$ are also subgroups of G, and HK is called

the join of H and K. Other concepts in group theory will appear later, but most will be made explicit as they appear.

Now, we may focus our attention on the graph theoretic question that drives this thesis. Drawing on the work found in [5], we provide a number of definitions and statements about graphs, leading up to a notion of an expander family. These definitions and results come directly from [5] and are presented with minor revisions below.

Definition 1.1. *Let $X = (V, E)$ be a graph and $F \subset V$. The* **boundary** *of F is defined to be the set of edges with one endpoint in F and one endpoint in $V \setminus F$, and is denoted by ∂F. That is, ∂F is the set of edges connecting F to $V \setminus F$.*

Definition 1.2. *The* **isoperimetric constant**, *or* **edge expansion constant** *of a graph $X = (V, E)$ is defined as*

$$h(X) = \min \left\{ \frac{|\partial F|}{|F|} \;\middle|\; F \subset V \text{ and } 0 < |F| \leq \frac{|V|}{2} \right\}.$$

Definition 1.3. *Let (a_n) be a sequence of positive real numbers. We say that (a_n) is* **bounded away from zero** *if there exists a real number $\epsilon > 0$ such that $a_n \geq \epsilon$ for all n.*

Definition 1.4. *Let (X_n) be a sequence of d-regular graphs for some fixed d such that $|X_n| \to \infty$ as $n \to \infty$. We say that (X_n) is a* **family of expanders** *if the sequence $(h(X_n))$ is bounded away from zero.*

Definition 1.5. *Let (G_n) be a sequence of finite groups, and take Γ_n to be a symmetric subset of G_n with $|\Gamma_n| = d$, generating a sequence of Cayley graphs $(Cay(G_n, \Gamma_n))$. If we can choose the symmetric subsets Γ_n so that $(Cay(G_n, \Gamma_n))$ is an expander family,*

then we say that (G_n) ***yields an expander family***.

Proposition 1.6. *No sequence of abelian groups yields an expander family.*

Proposition 1.7 (Subgroups Non-expansion Principle)**.** *Let* (G_n) *be a sequence of finite groups. Suppose that* (G_n) *admits* (H_n) *as a bounded-index sequence of subgroups. If* (H_n) *does not yield an expander family, then* (G_n) *does not yield an expander family.*

Proposition 1.8 (Quotients Non-expansion Principle)**.** *Let* $(G_n$ *be a sequence of finite groups. Suppose that* (G_n) *admits* (Q_n) *as a sequence of quotients. If* (Q_n) *does not yield an expander family, then* (G_n) *does not yield an expander family.*

The three above propositions, taken together, imply that if (G_n) yields an expander family, then for every fixed positive integer k, the sequence $|G_n^k/G_n^{k+1}|$ is bounded, where G_n^k is said to be the k^{th} derived group of G_n. In other words, a sequence of groups cannot yield an expander family if for any k, the sequence of orders of kth terms in the derived series goes to infinity.

Interestingly, this statement only holds in one direction. Taking the smallest nonableian simple group, the alternating group A_5, and taking n-fold direct products with itself will give a counterexample (see [5]). It also turns out that nonabelian simple groups will always yield expander families, and so our research turns to trying to find nonabelian nonsimple groups whose quotients are bounded for every fixed positive integer k.

Trying to find bounds for each term of quotients motivates the research found in this thesis. We focused on nonabelian nonsimple 2-groups, and focused on the first two quotients. This thesis will prove that, given a finite 2-group G of derived

length 3, then $|G/G^1| \geq 8$ and $|G^1/G^2| \geq 8$; the precise statement is found at the end of Chapter 3, in Corollary 3.12. In Chapter 2, we will find initial bounds using techniques of P. Hall taken from [4]; Chapter 3 will improve on the first of those bounds to achieve the desired result. Along the way, we will prove other statements that will perhaps motivate further research into groups of larger derived length, including a classification for all group that are of maximal class.

CHAPTER 2

A Theorem Of P. Hall

This section will begin the examination of 2-groups and their derived series. Our goal is to explicitly show that, given a finite 2-group G of derived length 3, then $|G/G^1| \geq 2^2$ and $|G^1/G^2| \geq 2^3$. It will be useful at this juncture to introduce notational elements relevant to this discussion (including a precise definition of what we mean by "derived series" above). For the most part, this thesis will deal with characteristic subgroups of finite 2-groups; we say a subgroup H of G is characteristic if any automorphism of G leaves H fixed. In addition, if K is a second characteristic subgroup of G, then $H \cap K$ and, if H or K is normal in G, HK are characteristic subgroups of G as well, as explained in [2]. Finally, note that because a characteristic subgroup is fixed under all automorphisms, it is fixed under all inner automorphisms, and therefore is normal.

Characteristic subgroups will form an important part of the research presented here. For instance, in this paper, the focus lies upon commutator subgroups, and it turns out that, given a group G, the subgroup generated by the set of all $x^{-1}y^{-1}xy$ for x, $y \in G$ forms a characteristic subgroup. Note that G is a characteristic subgroup of itself, as any automorphism maps G to itself in full, and note that if G is abelian, the commutator subgroup is trivial, and therefore is necessarily maintained under any automorphism. Here, given subgroups H and K of a group G, the subgroup denoted

$(H,\, K)$ is the subgroup generated by elements of the form

$$[h,\, k] = h^{-1}k^{-1}hk, \tag{2.1}$$

for all $h \in H$ and $k \in K$. The subgroup $(H,\, K)$ is called a commutator subgroup of G, and is a characteristic subgroup of G if H and K are characteristic subgroups.

Note that in the discussion of groups, a commutator subgroup is denoted by the use of parenthesis $(H,\, K)$. In the case of the commutator of elements of groups, we will instead use brackets; that is, for $h,\, k \in G$, set $[h,\, k] = h^{-1}k^{-1}hk$. The small difference, alongside the difference in lowercase and uppercase letters, will help distinguish between elements and subgroups.

Now, with this notation, we arrive at the definition of a derived group, which then gives rise to the derived series. Given a group G, the derived group is the group $(G,\, G)$. From here, let

$$G^0 = G, \text{ and}$$

$$G^1 = (G,\, G);$$

then, the i^{th} derived group is defined by

$$G^i = (G^{i-1},\, G^{i-1}), \tag{2.2}$$

for i a positive integer. This series of derived groups is known as the derived series of G, and for any 2-group, the final iterate will be E, the trivial group, given by [4]. If G^n is trivial and G^{n-1} is not, then the derived series is said to have length n. Note that if the derived series is of length n, then there are $n+1$ groups in the series; the value n is also known as the derived length, in that case. In addition, we consider

the special case where G is the trivial group. If that is true, then G^0 is trivial, and it is said to be of derived length 0.

On occasion, it will be simpler to denote the first derived group, G^1, by G', and similarly, to denote the second and third derived groups, G^2 and G^3, by G'' and G''' respectively. This "prime" notation is simply easier to type and discuss, so it may appear as such later on in this paper.

With this in mind, a useful definition in the discussion of these 2-groups is that of a central series of a group G. This is a monotonic sequence of normal subgroups, beginning with $K^0 = E$ and ending with $K^n = G$, such that:

$$K^0 \leq K^1 \leq \ldots \leq K^{n-1} \leq K^n, \tag{2.3}$$

with the property that for any $i = 1, 2, \ldots, n$, the group

$$\langle k^{-1}x^{-1}kx \mid k \in K^i, x \in G \rangle = (K^i, G) \leq K^{i-1}. \tag{2.4}$$

To rephrase that, the commutator of any element of G with any element of K^i is an element of K^{i-1}; or, K^{i+1}/K^i is in the center of G/K^i.

We will now introduce two "types" of series: The lower central series, and upper central series. The lower central series of G is given by H^1, H^2, $H^3, \ldots$, where $H^i = H^i(G)$, $H^1 = G$, and

$$H^i = (H^{i-1}, G) \tag{2.5}$$

for i a positive integer. This series ends, like the derived series above, with the trivial group, and has length n if H^{n+1} is trivial and H^n is not. This small divergence from the notation above should be noted, as this central series begins with the index of 1

rather than 0. The length is called the class of G, and is denoted $\mathrm{cl}(G)$. The class of G can be thought of as a measure of how close it is to an abelian group in properties; a group is of class 1 if and only if it is abelian, and so a group with large class is fairly divergent from an abelian group.

The upper central series functions somewhat differently; it is said to ascend, as the starting term will be the trivial group. Here, the upper central series of G is represented by Z^0, Z^1, $Z^2, \ldots$, where $Z^0 = E$, $Z^1 = Z(G)$ (that is, the center of the group), and Z^i/Z^{i-1} is the center of G/Z^{i-1}. Another way to consider the next term Z^{i+1}, given Z^i, is by:

$$Z^{i+1} = \{x \in G \mid \forall y \in G, [x, y] \in Z^i\}. \tag{2.6}$$

In any finite 2-group, the lower central series will terminate in E, and the upper central series will terminate in G.

It will be enlightening to use an example to demonstrate the differences between these three series. Since finite abelian 2-groups are not particularly interesting, we will take G to be a nonabelian finite 2-group of small order; in this case, let

$$G = \langle r, s \mid r^4 = s^2 = e, sr = r^{-1}s \rangle,$$

the dihedral group of order 8. Beginning with the derived series, $G^0 = G$, and so:

$$G^1 = (G, G) = \{x \mid \exists\, g, h \in G :\ g^{-1}h^{-1}gh = x\}.$$

With some calculations, it turns out that $G^1 = \{e, r^2\}$, an abelian group of order 2.

Therefore, the next iterate gives

$$\begin{aligned} G^2 &= (G^1, G^1) \\ &\cong (\mathbb{Z}_2, \mathbb{Z}_2) = E. \end{aligned}$$

Thus, G has derived length 2, as G^2 is trivial and G^1 is not. Turning to the lower central series, by definition we get that

$$\begin{aligned} H^1 &= G, \text{ and} \\ H^2 &= G^1 = \{e, r^2\} \end{aligned}$$

by above. The next term in the lower central series is then

$$\begin{aligned} H^3 &= (H^2, G) \\ &= (\{e, r^2\}, \langle r, s \rangle). \end{aligned}$$

Since r^2 commutes with both r and s, necessarily, for all $g \in G$, $r^2 g^{-1} r^2 g = e$. Therefore, $H^3 = E$ as well. In this case, the derived series and the lower central series are the same.

Finally, we examine the upper central series. Beginning with $Z^0 = E$, the next term will be

$$\begin{aligned} Z^1 &= Z(G) \\ &= \{x \mid g^{-1} x g = x \; \forall g \in G\} \\ &= \{e, r^2\}. \end{aligned}$$

The next term in the series must obey the relation that $Z^2/Z^1 = Z(G/Z^1)$. In other

words,

$$Z^2 = \{x \in G \mid \forall y \in G,\, [x,\, y] \in \{e,\, r^2\}\} = G,$$

as since for any $x,\, y \in G,\, [x,\, y] \in \{e,\, r^2\}$, it must be true for any fixed $x \in G$. Therefore, $Z^2 = G$, and the upper central series terminates here, as $Z^1 \neq G$.

Since the aim is to prove properties of finite 2-groups with series of these types, it will be a good idea to show that any 2-group has a central series. In fact, the construction of the upper central series above will always yield a central series for any finite 2-group G. If such a G is abelian, then clearly

$$Z^0 = E$$

and

$$\begin{aligned} Z^1 &= Z(G) \\ &= G, \end{aligned}$$

so the series exists and ends in G. If such a G is nonabelian, then an elementary result of [4] is that $Z(G)$ is nontrivial, and so the series has a length greater than 1.

Returning to the class of G, it was stated above that the class is given by the length of the lower central series. This will remain the case, but in fact, for any finite 2-group, the length of the lower central series and the length of the upper central series are the same.

Lemma 2.1. *If G is a finite 2-group, where H^a is trivial and H^{a-1} is not, and $Z^b = G$ and Z^{b-1} is proper, then $a - 1 = b$.*

Proof. Let K^0, K^1, ..., K^n be a central series of G. Clearly, for the upper central series Z^i,

$$K^0 = Z^0.$$

Take this to be the base case. Assume that for i,

$$K^i \leq Z^i.$$

By the definition of a central series, $(K^{i+1}, G) \leq K^i$, so every element of K^{i+1} corresponds in the homomorphism $G \to G/Z^i$ to an element of the center of G/Z^i; in other words,

$$K^{i+1} \leq Z^{i+1}.$$

By induction, then, $K^i \leq Z^i$ for all $i = 0, \ldots, b$.

Since the lower central series is a central series, by the above paragraph its length must be at least the length of the upper central series; that is, $a - 1 \geq b$. Assume that $H^i \leq Z^{b-i}$. Then $H^{i+1} \leq Z^{b-i-1}$, until

$$H^{i+1} \leq Z^{b-i-1}, \ldots, H^a \leq Z^0 = E.$$

If this were the case, then the length of the lower central series would be less than $a - 1$, which is a contradiction. Thus,

$$H^i > Z^{b-1}, \tag{2.7}$$

and so we conclude that the lengths of the lower and upper central series are the same for any finite 2-group. □

With some experience under our belt with these central series of finite 2-groups, our attention can now turn to the main goal of this chapter. Using characteristics of these central series, primarily the lower central series, we can arrive at a result that bounds the orders of quotient groups of the derived sequence of a finite 2-group G.

However, before arriving at this statement, there are many hurdles. In the interest of brevity, we will take but not prove a few statements from [4] that will be useful in proving our main result. Immediately below, we find an elementary result for 2-groups, taken from [4].

Theorem 2.2. *If G is a 2-group, then G is solvable and the quotient groups of a maximal normal series are all of order 2.*

The next theorem comes from the fact that, using the previous theorem, we can find normal subgroups of G contained in the upper central series that have a corresponding normal subgroup K containing all of them. This is also taken from [4].

Theorem 2.3. *If G is a finite 2-group and K is a normal subgroup of G not contained in Z^i, then K contains elements of $Z^{i+1} \setminus Z^i$, and its order exceeds 2^i.*

These two theorems above will come into play when proving critical statements leading to the conclusion of this chapter. Now, we will return to theorems which we will prove explicitly in this thesis. Given a finite 2-group G, it can be proved that if K^i denotes a central series of G, then the commutator of any element of K^j with any element of H^i belongs to K^{j-i}.

Before proving this claim, we introduce a shorthand by which we can discuss commutator subgroups involving other commutator subgroups. If we have subgroups

H, J, and K of G, then

$$((H,\, J),\, K) = (H,\, J,\, K).$$

This process may be iterated for many nested commutator subgroups; the shorthand used is to reduce the complexity of the statement on paper. In addition to the above notation, we take a theorem regarding such nested commutations from [4].

Theorem 2.4. *If G is any group and H, J, K are any three normal subgroups of G (not necessarily distinct), then each of the three groups $A = (H,\, J,\, K)$, $B = (J,\, K,\, L)$, and $C = (K,\, H,\, J)$ is contained in the join of the other two.*

With the statement of this theorem regarding nested commutators established, our attention returns to proving that if K^i denotes a central series of G, then the commutator of any element of K^j with any element of H^i belongs to K^{j-i}.

Theorem 2.5. *If G is a 2-group and if*

$$G = K^m \geq K^{m-1} \geq \ldots \geq K^1 \geq K^0 = E$$

is any central series of G, then

$$(K^j,\, H^i) \leq K^{j-i},\ \textit{for}$$

$$i = 1,\, 2,\, \ldots;\ j = m,\, m-1,\, \ldots$$

for H^i the terms of the lower central series.

Proof. We will prove this claim using induction. Take that $i = 1$. Then, the statement that will be proved becomes $(K^j,\, H^1) \leq K^{j-1}$. Since $H^1 = G$, by the definition of a central series K, it must hold. This provides a base case upon which we will apply induction to i.

Suppose, then, that $(K^j, H^{i-1}) \leq K^{j-i+1}$ for all $j = m, m-1, \ldots, 1$. Now, consider the group

$$\begin{aligned}(K^j, H^i) &= (H^i, K^j) \\ &= ((H^{i-1}, G), K^j) \\ &= (H^{i-1}, G, K^j).\end{aligned}$$

Take $D = (G, K^j, H^{i-1})(K^j, H^{i-1}, G)$. With the results of Theorem 2.4, it holds that $(K^j, H^i) \leq D$. In addition, $(G, K^j) \leq K^{j-1}$, and therefore $(G, K^j, H^{i-1}) \leq (K^{j-1}, H^{j-1})$.

By the hypothesis,

$$\begin{aligned}(K^{j-1}, H^{j-1}) &\leq K^{j-1-i+1} \\ &\leq K^{j-i}.\end{aligned}$$

In addition, $(K^j, H^{i-1}) \leq K^{j-i+1}$ by the hypothesis, and therefore

$$\begin{aligned}(K^j, H^{i-1}, G) &\leq (K^{j-i+1}, G) \\ &= K^{j-i}.\end{aligned}$$

Since both groups used to construct D are contained in K^{j-i}, it must be the case that their join $D \leq K^{j-i}$. This gives the desired relation $(K^j, H^i) \leq K^{j-i}$, so induction holds and the claim is proved. □

The above theorem applies to any central series K^i of G, and therefore this theorem applies in the special cases of the lower and upper central series. Below, the two corollaries will provide the necessary reformulation of Theorem 2.5.

Corollary 2.6. *For a finite 2-group G, given the upper and lower central series, $(Z^j, H^i) \leq Z^{j-i}$ for any i, j. In addition, every element of H^j commutes with every element in Z^j.*

The second statement in Corollary 2.6 comes from the fact that, by the main statement, the commutation $(Z^j, H^j) \leq Z^{j-j} = Z^0 = E$.

Corollary 2.7. *For a finite 2-group G, given the lower central series, $(H^i, H^j) \leq H^{i+j}$ for any i, j. In addition, if $cl(G) = c$ and $2i > c$, then H^i is abelian.*

The statement above will prove to ultimately be the most useful form of Theorem 2.5, but in general, Theorem 2.5 does not apply solely to finite 2-groups. As at no point was the fact that G was a finite 2-group explicitly used; in fact, it can be immediately generalized to include all p-groups.

With this in mind, we will now prove the two primary theorems of this chapter. At their conclusion, the application of the second to the first will yield the desired result that for any nonabelian finite 2-group G of derived length three, $|G/G^1| \geq 2^2$ and $|G^1/G^2| \geq 2^3$.

Theorem 2.8. *The i^{th} derived group G^i of a finite 2-group G is contained in H^{2^i}.*

Proof. Let G be a finite 2-group, where $G^0 = G$ and

$$\begin{aligned} G^i &= (G^{i-1}, G^{i-1}) \\ &= ((G^{i-2}, G^{i-2}), (G^{i-2}, G^{i-2})) \end{aligned}$$

This process will iterate until the expression for G^i is given solely by commutations of the group $G^0 = G$. Since the number of commutator groups interior to the expression doubles in each step, it is clear that when written as an expression in terms of G^0 alone,

there will be 2^i appearances in the expression. The expansion of this sequence is not included past the second round, as commutations of commutators of this complexity are difficult to write, even in shorthand notations.

Fortunately, on consideration of the lower central series, an explicit extension to the most basic components is certainly possible. By the definition of the lower central series, we have that

$$\begin{aligned} H^{2^i} &= (H^{2^i-1}, G) \\ &= ((H^{2^i-2}, G), G) \\ \ldots &= (\ldots(((G, G), G), G)\ldots, G) \end{aligned}$$

Similarly, we see that at the end of the expansion, there will be precisely 2^i appearances of G in the expression.

Using these expansions, induction will prove the claim. Clearly it holds for $i = 1$, as in that case,

$$\begin{aligned} G^1 &= (G^0, G^0) \\ &= (G, G), \end{aligned}$$

and

$$\begin{aligned} H^{2^1} &= H^2 \\ &= (H^1, G) \\ &= (G, G). \end{aligned}$$

As clearly $(G, G) \leq (G, G)$, take this to be the base case.

Now assume that the relation $G^{i-1} \leq H^{2^{i-1}}$ holds, and take both G^i and H^{2^i}. By the initial relations defined above, $G^i = (G^{i-1}, G^{i-1})$ and $H^{2^i} = (H^{2^i-1}, G)$. As $G^{i-1} \leq H^{2^{i-1}}$, and both are subgroups of G, it must be true that

$$(G^{i-1}, G^{i-1}) \leq (H^{2^{i-1}}, H^{2^{i-1}}).$$

Corollary 2.7 gives precisely that

$$\begin{aligned}(H^{2^{i-1}}, H^{2^{i-1}}) &\leq H^{2^{i-1}+2^{i-1}} \\ &\leq H^{2^i}\end{aligned}$$

Therefore, $G^i \leq H^{2^i}$, as desired. With this established, the inductive step holds, and therefore the relation holds for all nonnegative i. □

Establishing Theorem 2.8 provides important information: Given the n^{th} derived group of G, it is known precisely in which element of the lower central series it lies. In concert with the following theorem, it can be used to show that the quotient groups have bounded order, as below we will show that quotient groups using central series have bounded order.

Theorem 2.9. *Let G be a finite 2-group, and let K be a normal subgroup of G. If $K \subset H^i(G)$, then for positive a and nonnegative b, the quotient groups $K/H^a(K)$ and $K/Z^b(K)$ are all of order 2^i at least, with the terms with $H^1(K)$ and $Z^n(K)$ for each series being possible exceptions, where the class of K is n. In particular, if K is nonabelian, then $|Z(K)| \geq 2^i$ and $|K/H^2(K)| > 2^i$.*

Proof. If K is abelian, then this theorem is trivial, so we will focus on a nonabelian $K \triangleleft G$. From here, define $K_1 = K \cap Z^i$. Because $K_1 \leq K$ and $K \leq H^i$, it must be true that $K_1 \leq H^i$ as well.

From Theorem 2.6, and the fact that $K_1 \leq Z^i$, it must be true that $K_1 \subset Z(K)$. Since K is nonabelian, it must be the case that $K_1 < K$. Then, it must be true that $K \not\subset Z^i$, and so by Theorem 2.3, the order of K exceeds 2^i. Since the center of K is of order at least 2^i it must be the case that $|K_1|$ is at least 2^i.

If $Z^a(K) < K$, then $K/Z^{a-1}(K)$ is nonabelian, and so it similarly results that

$$|Z^a(K)/Z^{a-1}(K)| \geq 2^i,$$

following precisely the same argument as above for K_1. Thus, the quotient groups of the upper central series (with the possible exceptions of the last entry) must all be of order at least 2^i.

Having proved the claim for the upper central series, our attention now turns to the lower central series. We set $K_2 = H_2(K)$ for the derived group of K. By the claim, it must be that K_2 is nontrivial. The goal here will be to establish that the order of K/K_2 is at least 2^{i+1}. To accomplish this goal, set K_3 to be a normal subgroup of G such that $|K_2/K_3| = 2$; this can be done, as G is a finite 2-group, so Theorem 2.2 gives that a such a normal subgroup exists.

By this, it must be true that K/K_3 is nonabelian, which gives that its center is of order 2^i at least, by what has previously been shown. Since the quotient is nonabelian, letting $\kappa = K/K_3$ and $Z(\kappa)$ to be the center of κ, necessarily $|\kappa/Z(\kappa)| \geq 4$. This gives that the order of K/K_3 is at least 2^{i+2}, and the order of K/K_2 is at least 2^{i+1}.

Finally, if a is the largest integer such that $H^a(K)$ is nontrivial, then let K_4 be a normal subgroup of G with $|H^a(K)/K_4| = 2$. Once again, such a subgroup exists,

by Theorem 2.2. In turn, by equation (2.7), the center of K/K_4 does not contain $H^{a-1}(K)/K_4$, as the class of K/K_4 is a. However, since K belongs to H^i by the claim, by Theorem 2.6 it must be the case that every element of $Z^i(G/Z_4)$ commutes with every element of K/K_4.

By this fact, we conclude that $Z^i(G/K_4)$ does not contain $H^{a-1}(K)/K_4$. Therefore, by Theorem 2.3,

$$|H^{a-1}(K)/K_4| \geq 2^{i+1}$$

and so we conclude that

$$|H^{a-1}(K)/H^a(K)| \geq 2^i.$$

Therefore, the quotient groups of the lower central series of K must all have order at least 2^i. □

The statement about the orders of quotient groups using the upper central series will not be used to prove the main claim of this chapter, but for completion's sake, they provide useful insight into the structure of groups of specific classes. Having established this theorem, we will proceed to the primary result.

Theorem 2.8 and Theorem 2.9 will now be utilized to give the desired bounds on the quotients of the derived series for a nonabelian finite 2-group G of derived length 3.

Theorem 2.10. *Let G be a finite 2-group. If G^{a+1} is nontrivial, then the order of G^a/G^{a+1} is greater than 2^{2^a}.*

Proof. Let G^{a+1} be a nontrivial subgroup in the derived series of G. Since G^a is nontrivial, necessarily $G^a \leq H^{2^a}$ by Theorem 2.8, as well as $G^{a+1} \leq H^{2^{a+1}}$.

We can apply Theorem 2.9 to the above result; because $G^a \leq H^{2^a}$, the quotient group $G^a/H^\alpha(G^a)$ is at least of order 2^{2^a}, for any positive integer α. In particular, if $\alpha = 2$, then

$$\begin{aligned} H^\alpha(G^a) &= H^2(G^a) \\ &= (G^a, G^a) \\ &= G^{a+1}. \end{aligned}$$

Therefore, the order of of G^a/G^{a+1} must be at least 2^{2^a}. However, by the particular case for a nonabelian group G^a and $H^2(G^a)$, $|G^a/H^2(G^a)| = |G^a/G^{a+1}| > 2^{2^a}$. Since G^{a+1} is nontrivial, and

$$G^{a+1} = (G^a, G^a),$$

it must be true that G^a is nonabelian, and so the above strict inequality holds. □

Remark 2.11. *It can be shown that if G^a is nontrivial, then G is of order $2^{2^\delta+\delta}$ at least, for δ set below. Let G, as per usual, be a finite 2-group. G^{a+1} is the derived group of G^a. If $G^\delta > E$, the order of G^δ is at least 2, and so the order of G^a/G^{a+1} is at least equal to 2^{2^a+1} for each $a = 0, 1, \ldots, \delta - 1$. Since the order of G is 2^n, it holds that:*

$$n \geq 1 + \sum_{a=0}^{\delta-1}(2^a + 1) = 2^\delta + \delta. \tag{2.8}$$

Thus G, being of order 2^n, has $|G| \geq 2^{2^\delta+\delta}$.

The remark above serves to guide further research, as it gives some notion of the order if one is searching for a 2-group of particular derived length. However, the primary result comes from Theorem 2.10, which states that if the $a + 1^{\text{th}}$ term

of a derived series is nontrivial, then $|G^a/G^{a+1}| > 2^{2^a}$. Rewriting to an equivalent statement, it becomes $|G^a/G^{a+1}| \geq 2^{2^a+1}$.

We now turn to our goal: Take G to be a nonabelian finite 2-group of derived length 3. As Theorem 2.9 states that the desired order 2^i may not hold for the last term in the series, we can now determine the orders of G/G^1 and G^1/G^2, as the final term is G^3. Taking a as appropriate,

$$\begin{aligned} |G/G^1| &\geq 2^{2^0+1} = 2^2 \\ &\geq 4, \text{ and} \\ |G^1/G^2| &\geq 2^{2^1+1} = 2^3 \\ &\geq 8, \end{aligned}$$

which were the precise bounds we set out to establish at the outset.

CHAPTER 3

Improving The Bound

In the previous chapter, it was established that, given a finite 2-group G with derived length three, the orders of G/G' and G'/G'' were bounded below by 2^2 and 2^3 respectively. It turns out that, in the case of G/G', the bound can be improved. In this chapter, it will be established that, in fact, $|G/G'|$ must be at least 2^3.

Despite the seemingly modest improvement to the bound, there is actually quite a bit of work that must be done in order to prove this. We will begin with the definition of a few mechanisms that will be instrumental in proving the claim of this section. As in the rest of this paper, the group G is assumed to be a finite 2-group.

Here, we introduce a short theorem in order to borrow notation from [3]. In characterizing the 2-groups in this paper, it is necessary to talk about abelian 2-groups and their construction.

Theorem 3.1. *A finite abelian 2-group G is the direct product of cyclic subgroups H_i, for $1 \leq i \leq n$. Moreover, the integer n and the orders $|H_i|$ are uniquely determined (up to order).*

Given this theorem, there must be a uniquely defined integer n for any such abelian 2-group G. Despite this theorem applying only to abelian 2-groups, it turns out to be useful for all finite 2-groups.

Given G as above, there is a particular subgroup that will turn out to be

handy for calculations. The subgroup of G made up of the intersection of all maximal subgroups of G is called the Frattini subgroup of G, and it is denoted by $\Phi(G)$. In the case where G has no maximal subgroups, we set $\Phi(G) = G$. The Frattini subgroup is always a characteristic subgroup. If a group has no maximal subgroups (as a maximal subgroup is a proper subgroup), then the Frattini subgroup of G is itself.

It can be proved that the Frattini subgroup of a group G is, in fact, the subgroup of all $g \in G$ such that if $X \subset G$ generates G, and $g \in X$, then $X \setminus \{g\}$ also generates G. This is described by g being a non-generator of G, for obvious reasons. If g is not a non-generator of G, then it is a generator. Put precisely, g is a generator of G if for all $M \ni g$ such that $\langle M \rangle = G$, then $\langle M \setminus \{g\} \rangle \neq G$.

Lemma 3.2. *The Frattini subgroup $\Phi(G)$ of a finite group G is the set of all non-generating elements of G.*

Proof. We begin this proof by showing that if g is not an element of the Frattini subgroup, then g must be a generating element of the group G. If $g \notin \Phi(G)$, then there exists a maximal subgroup M of G such that $g \notin M$. The subgroup M is maximal, so if there exists a subgroup K such that

$$M \leq K \leq G,$$

then either $K = M$ or $K = G$. Take the subgroup generated by $\{g\} \cup M$. Then:

$$M \leq \langle M, g \rangle \leq G. \tag{3.1}$$

Since M was maximal, it must be true that $\langle M, g \rangle = G$. Since $M \neq G$, g is a generating element of G. Thus, any element not in $\Phi(G)$ is a generating element of G.

Next, we will show that any generator g of G is not in the Frattini subgroup. This will be done by showing that if g is a generator, there is a maximal subgroup of G that does not contain g. If g is a generator, then there exists a subset X of G such that $G = \langle X, g \rangle$, and $\langle X \rangle \neq G$. Necessarily, then, $g \notin X$, as otherwise $\langle X \rangle = G$.

Since $\langle X \rangle \neq G$, $\langle X \rangle$ is contained in a maximal subgroup H. Since H is maximal, for all K such that

$$H \leq K \leq G,$$

either $K = H$ or $K = G$. It must be true that g is not in H, as otherwise

$$G = \langle \{g\} \cup X \rangle$$

$$\subset H.$$

This cannot be true, as H is a maximal subgroup, and so $g \notin H$. Thus, there exists a maximal subgroup of G that does not contain g, so $g \notin \Phi(G)$, precisely as desired.

Therefore, $g \notin \Phi(G)$ if and only if g is a generating element of G, which is equivalent to the claim. □

With the above lemma proved, it will be convenient to refer to the Frattini subgroup of any G in this thesis as the set of non-generating elements of G.

It can also be shown that if $G/\Phi(G)$ is cyclic, then G must be cyclic. This comes from the fact that $\Phi(G)$ contains no generators of G. If there is an x in G such that $\Phi(G)x$ generates $G/\Phi(G)$, then

$$G = \langle x, \Phi(G) \rangle.$$

As every element of $\Phi(G)$ may be removed from a generating set, then $\langle x, \Phi(G)\rangle = \langle x\rangle$, and so the above equality gives that

$$G = \langle x\rangle.$$

Thus, G must be cyclic.

As once again the class of a group G shows up in this chapter, so a reminder of the definition will be useful. Given a group G, the length of the lower central series defines the class; that is, for $H^1 = G$, and $H^i = (H^{i-1}, G)$, $\mathrm{cl}(G) = n$ when H^{n+1} is trivial and H^n is nontrivial. Any nontrivial abelian group will have class 1, as $H^2 = E$.

Moving on, it will be handy to define a few of the commonly seen 2-groups; in fact, these 2-groups will form the basis for the improvement of the bounds set out above. In each of the following constructions, m is assumed to be at least 3. First, there is the dihedral group D_m, which is defined handily by the relation

$$D_m = \langle r, s \mid r^{2^{m-1}} = e, s^2 = e, sr = r^{-1}s = r^{2^{m-1}-1}s\rangle. \tag{3.2}$$

This dihedral group has order 2^m. In other texts, usually D_m is defined as the dihedral group of order m, but that is not the case here, as we are only interested in 2-groups.

In addition to the dihedral group, there are S_m, Q_m, and $M_m(2)$. The first is known as the semidihedral group, and the second as the generalized quaternion group. The last, as defined by [3], is not known by any particular name. The semidihedral group has a construction similar to that of D_m, and is in fact given by

$$S_m = \langle r, s \mid r^{2^{m-1}} = e, s^2 = e, sr = r^{2^{m-2}-1}s\rangle. \tag{3.3}$$

Note that the order-reversal action on sr now takes r to $r^{2^{m-2}}r^{-1}$, rather than simply r^{-1}. In addition, this group necessarily has $m \geq 4$; if $m = 3$, then the relation becomes

$$\begin{aligned} sr &= r^{2-1}s \\ &= rs, \end{aligned}$$

so the group would be abelian. The construction of $M_m(2)$ is very similar to that of the semidihedral group, and is constructed by

$$M_m(2) = \langle r,\, s \mid r^{2^{m-1}} = e,\, s^2 = e,\, sr = r^{2^{m-2}+1}s \rangle. \tag{3.4}$$

This group is denoted by $M_m(2)$ because this construction can be performed with any prime p replacing 2. In this thesis, we will deal exclusively with $M_m(2)$, so for brevity's sake, from now on it will be referred to as simply M_m.

The final general 2-group construction needed for this chapter is the generalized quaternion group, Q_m. The smallest quaternion group is of order 8, which is in agreement with the assumption that, for all these 2-groups, $m \geq 3$. The generalized quaternion group is defined as

$$Q_m = \langle r,\, s \mid r^{2^{m-1}} = e,\, s^4 = e,\, r^{2^{m-2}} = s^2,\, sr = r^{-1}s \rangle. \tag{3.5}$$

Under this construction, Q_m has order 2^m, and so $Q_3 = Q$, the familiar order 8 quaternion group. These four families of 2-groups, D_m, S_m, M_m and Q_m, will eventually be used to show that any 2-group that fails to have $|G/G'| \geq 2^3$ will also be a 2-group of derived length less than 3.

Each of the groups D_m, S_m, Q_m, and M_m has order 2^m. In fact, by using the defining relations, any element of any of those groups can be expressed uniquely in the form $r^a s^b$ with $0 \leq a < 2^{m-1}$ and $0 \leq b \leq 1$.

With the construction of these specific groups behind us, we now turn to specific subgroups of an arbitrary finite 2-group G. First, there is $\Omega_i(G)$, which is the subgroup of G generated by its elements of order dividing 2^i; that is, if $x \in G$ has order 2^j for $j \leq i$, then x is a generating element of $\Omega_i(G)$. Similarly, $\mho^i(G)$ is the subgroup generated by the elements of the form x^{2^i}, where x is an element of G. Because group automorphisms maintain the order of elements, both $\Omega_i(G)$ and $\mho^i(G)$ must be characteristic subgroups of G as they remain fixed under any automorphism.

As a final note of convenience, when discussing these groups, let $H = \langle r \rangle$; namely, H is the maximal cyclic subgroup for any of these groups defined above.

Having established these definitions, we may now move on to some basic lemmas regarding groups. Let G be a finite 2-group, and let $Z(G)$ be the center of G, as usual.

Lemma 3.3. *If $G/Z(G)$ is cyclic, then $G = Z(G)$ and G is abelian.*

Proof. If y is an element of G whose image generates $G/Z(G)$, then every element of G is of the form xy^i for some x in $Z(G)$ and some integer i. But then it is immediate that any two elements of G commute, and so $G = Z(G)$ is abelian. □

In addition to the lemma above, it will be useful to show that any group that has no element of order greater than two is an abelian group.

Lemma 3.4. *Let G be a group wherein all non-identity elements are of order 2. Then G is abelian.*

Proof. If x, $y \in G$, then $(xy)^2 = x^2 = y^2 = 1$, and so necessarily

$$xyxy = x^2y^2$$

$$= xxyy.$$

Therefore, $xy = yx$ and so then G must be abelian. □

With all these things out of the way, we can now proceed to the theorems that will show that any finite 2-group of derived length 3 cannot have $|G/G'| = 2^2$. To start, we will focus on proving some statements about these 2-groups; primarily, it will be shown that none of the groups defined above are isomorphic. This will not be used to directly show the main claim of this chapter, but it will provide a better classification for finite nonabelian 2-groups that are not of derived length 3. As there are many properties to cover, the claims will be made distinct.

Theorem 3.5. *If $G = M_m$, then the following hold:*

(a) $cl(G) = 2$ and $|G'| = 2$.

(b) $\Phi(G) = Z(G)$ is cyclic of order 2^{m-2}.

(b) $\Omega_i(G)$ is abelian and isomorphic to $\mathbb{Z}_{2^i} \times \mathbb{Z}_2$, for $1 \leq i \leq m-2$.

Proof. Set G to be M_m. Let $G = \langle r, s \rangle$ satisfying the relations defined previously in equation (3.4). Clearly, in G, any r^i commutes with any other r^j. If it can be shown, then, that for some i, r^i commutes with s, then that $r^i \in Z(G)$. To find such an i,

take sr^i and set it equal to its commutation, $r^i s$:

$$\begin{aligned} sr^i &= (r^{1+2^{m-2}})^i s \\ &= r^{i+2^{m-2}i} s \\ &= r^i s. \end{aligned}$$

Therefore, $r^i \in Z(G)$ when $i \equiv i + 2^{m-2}i \pmod{2^{m-1}}$. Since $2^{m-2}i \equiv 0 \pmod{2^{m-1}}$ for any even i, it is easy to see that then $r^i \in Z(G)$ for any even $i \leq 2^{m-1}$.

In addition, it can be shown that for any odd positive integer $a < 2^{m-1}$, $r^a s \notin Z(G)$:

$$\begin{aligned} (r^a s)^{-1} s (r^a s) &= s r^{-a} s r^a s \\ &= r^{-a(2^{m-2}+1)} s s r^a s \\ &= r^{-a2^{m-2}-a+a} s \\ &= r^{-a2^{m-2}} s. \end{aligned}$$

This gives that if a is odd, then $r^a s$ is not central. On the other hand, $srs = r^{1+2^{m-2}}$, so $s \notin Z(G)$. Now, assume that for an even positive $a < 2^{m-1}$, $r^a s \in Z(G)$. The above statements show that $r^a \in Z(G)$, and so since $Z(G)$ is closed under the group operation, $r^{-a} \in Z(G)$. Thus $s \in Z(G)$, which is a contradiction. Therefore $Z(G) = \langle r^2 \rangle$. This is a cyclic group of order 2^{m-2}, as that is the order of r^2.

We will now show that $Z(G) = \Phi(G)$. As $\Phi(G)$ may not contain any generators of G, necessarily neither r nor s are in $\Phi(G)$. In addition, $Z(G) \subset \Phi(G)$, as $\langle r^2 \rangle$ contains no generators of G. To show that $Z(G) = \Phi(G)$, assume that for some i, $r^i s \in \Phi(G)$. If i is even, then $r^{-i} \in \Phi(G)$, so by closure, $s \in \Phi(G)$, a contradiction.

If i is odd, since $r^2 \in \Phi(G)$, by closure $r^{2j+i}s \in \Phi(G)$ for any $j < 2^{m-2}$; in other words, $r^k s \in \Phi(G)$ for all odd k and $r^k \in G$. Therefore, $|\Phi(G)| = 2^{m-1}$. Now, take $G/\Phi(G)$. There are precisely two left cosets, so $|G/\Phi(G)| = 2$ in this case. Therefore, $G/\Phi(G)$ is cyclic, which implies that G is cyclic, which is a contradiction, as M_m is nonabelian. Therefore $Z(G) = \Phi(G)$.

From here, assign $r^{2^{m-2}} = z$; this shorthand will be more convenient when discussing commutators of the group G, as the relations reduce to significantly less complex exponents. In equation (3.4), then, the order-reversal for M_m would then be given by $sr = zrs$. Clearly,

$$\begin{aligned} z^2 &= r^{2\cdot 2^{m-2}} \\ &= e. \end{aligned}$$

Then, for any positive integer k such that $k < m - 1$:

$$\begin{aligned} [r^k,\, s] &= r^{-k}sr^k s \\ &= r^{-k}(r^k)^{2^{m-2}+1}ss \\ &= r^{k2^{m-2}+k-k} \\ &= z^k, \end{aligned}$$

and

$$\begin{aligned} (sr^k)^2 &= sr^k sr^k \\ &= (r^k)^{2^{m-2}+1}ssr^k \\ &= r^{2k+2^{m-2}k} \\ &= r^{2k}z^k. \end{aligned}$$

First, using the above calculations, it is clear that

$$\langle z \rangle \subset (G, G) = G'.$$

For the opposite inclusion, as $\langle z \rangle$ is normal, take $G/\langle z \rangle$. This quotient group is abelian, so then $G' \subset \langle z \rangle$. Thus, $\langle z \rangle = G'$ and so G' is of order 2. Since G' is then abelian, G'' is trivial. By the definition of the lower central series found in the previous chapter, $H^2 = (G, G)$ and

$$\begin{aligned} H^3 &= (H^2, G) \\ &= (\langle z \rangle, G) \\ &= E, \end{aligned}$$

so $\mathrm{cl}(G) = 2$ as H^3 is trivial.

Next, we turn our attention to $\Omega_i(G)$, which is generated by elements whose orders divide 2^i. For any positive integer $i < m - 1$, it must be true that $s \in \Omega_i(G)$, and similarly $z \in \Omega_i(G)$, as both are of order 2. Since $m > 3$ both by the assumptions for G and the definition of M_m, sr^k has order dividing 2^i whenever $(sr^k)^{2^i} = e$. Then:

$$\begin{aligned} (sr^k)^{2^i} &= (sr^k sr^k)^{2^{i-1}} \\ &= (r^{2k} z^k)^{2^{i-1}} \\ &= r^{2k \cdot 2^{i-1}} z^{k \cdot 2^{i-1}} \\ &= r^{k 2^i} = e. \end{aligned}$$

Since the order of r is 2^{m-1}, for the above equality to hold, then

$$\begin{aligned} r^{k2^i} &= r^{(n2^{m-1-i})2^i} \\ &= (r^{2^{m-1-i+i}})^n \\ &= e^n = e. \end{aligned}$$

Therefore k must be divisible by $2^{(m-1)-i}$.

We will now show that that $\Omega_i(G) \cong \mathbb{Z}_{2^i} \times \mathbb{Z}_2$. First, it was already determined that $Z(G) = \langle r^2 \rangle$; that is, any even power of r will commute with any other element of G. In particular, any r^k where $k|2^i$ and $k \neq 1$ will commute with all elements of G.

In addition, if $k|2^i$ and $k \neq 1$, then $|r^k s| = |r^k|$, as for even k,

$$\begin{aligned} r^k s r^k s &= r^k z^k r^k s s \\ &= r^{2k}. \end{aligned}$$

This gives us that if $r^k \in \Omega_i(G)$, then necessarily $r^k s \in \Omega_i(G)$ as well. In addition, any element of this form will commute with others. Let a and b be divisible by $2^{(m-1)-i}$. Then:

$$\begin{aligned} (r^a s)(r^b s) &= r^a s r^b s \\ &= r^a z^b r^b s s \\ &= r^{a+b}, \end{aligned}$$

and

$$\begin{aligned}(r^b s)(r^a s) &= r^b s r^a s \\ &= r^b z^a r^a s s \\ &= r^{a+b}.\end{aligned}$$

Since any element of order dividing 2^i commutes with any other, $\Omega_i(G)$ must be an abelian 2-group. In addition, $\Omega_i(G) = \langle r^{2^{m-i-1}}, s\rangle$, so it must be isomorphic to an abelian 2-group with two generators, and the group must be of order $2^i \cdot 2 = 2^{i+1}$.

From these derived facts, we shall see if an isomorphism ϕ may be constructed between $\Omega_i(G)$ and $\mathbb{Z}_{2^i} \times \mathbb{Z}_2$. The group $\mathbb{Z}_{2^i} \times \mathbb{Z}_2$ has precisely two elements of order 2, as does $\Omega_i(G)$, so we will begin there. Set $\phi(s) = (0,1)$ and $\phi(z) = (2^{i-1}, 0)$. Since $\Omega_i(G)$ is generated by $\{r^{2^{m-i-1}}, s\}$, we know that $\phi(r^{2^{m-i-1}}) = (1,0)$. Once the homomorphism property for this function is verified, it will be shown that this assignment for the generators gives the correct assignment for z. Since $|r^k| = |r^k s|$ by the above considerations, it makes intuitive sense to set $\phi(r^{2^{m-i-1}} s) = (1,1)$. In general, this mapping will be defined by the following:

$$\phi(r^{a2^{m-i-1}} s^b) = (a, b) \tag{3.6}$$

where $1 \leq a < 2^i$ and $b \in \{0,1\}$.

This function ϕ then maps generators to generators, as $\mathbb{Z}_{2^i} \times \mathbb{Z}_2 = \langle (1,0),\ (0,1)\rangle$. It can also be shown to satisfy the homomorphism property. Using the definition pro-

vided above:

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

The commutation follows in the final step, as $r^{n2^{m-i-1}}$ is of even exponent and is therefore in the center of G. This verifies that, indeed, this mapping is a homomorphism. With this in mind, it is easy to see that $\phi(z) = (2^{i-1}, 0)$, as $(2^{i-1}, 0) = \phi([r^{2^{m-i-1}}])^{2^{i-1}} = \phi(r^{2^{m-i-1} \cdot 2^{i-1}}) = \phi(r^{2^{m-2}}) = \phi(z)$, so the initial intuition was correct.

By the construction of ϕ, it is easy to see that it must be surjective, and since $|\Omega_i(G)| = |\mathbb{Z}_{2^i} \times \mathbb{Z}_2|$, then it must be injective as well. Therefore a bijective homomorphism exists between them, and so they are isomorphic as claimed. □

With these facts proved about M_m, our attention now turns to the other three 2-groups defined previously.

Theorem 3.6. *Set $G = D_m$, with $m \geq 3$, Q_m, or S_m. Then the following hold:*

(a) $cl(G) = m - 1$.

(b) $\Phi(G) = G'$ is cyclic, and of order 2^{m-2}.

(c) $|Z(G)| = 2$ and $G/Z(G)$ is isomorphic to D_{m-1}.

Proof. Take G to be a 2-group as above, with $m \geq 3$. By the definitions provided

earlier in this chapter, for both D_m and Q_m, $sr = r^{-1}s$; for S_m, on the other hand, $sr = r^{2^{m-2}-1}s = zr^{-1}s$ (continuing the usage of z as defined in the previous proof).

Now, consider $[r, s]$. If G is either D_m or Q_m, then $[r, s] = r^{-1}srs = r^{-2}$, which would then give that $r^{-2} \in G'$. Since G' is a subgroup and therefore closed under taking inverses, $r^2 \in G'$. If G is S_m, then

$$\begin{aligned}[r^{2^{m-3}+1}, s] &= r^{-2^{m-3}-1}sr^{2^{m-3}+1}s \\ &= r^{-2^{m-3}-1}(r^{2^{m-3}+1})^{2^{m-2}-1} \\ &= r^{-2^{m-3}}r^{-1}r^{2^{2m-5}}r^{2^{m-2}}r^{-2^{m-3}}r^{-1}.\end{aligned}$$

Since here $m > 3$,

$$\begin{aligned}r^{2^{2m-5}} &= (r^{2^{m-1}})^{2^{m-4}} \\ &= e.\end{aligned}$$

Then $[r^{2^{m-3}+1}, s] = zzr^{-2}$, so $r^{-2} \in G'$ and so it follows that, once again, $r^2 \in G'$.

With these facts established, for any of these three cases $|G'| \geq 2^{m-2}$, and therefore $|G/G'| \leq 2^m/2^{m-2} = 4$. Now, $r \notin G'$; if it can be shown that $s \notin G'$, then necessarily $G' \subset \Phi(G)$. Assume that s is an element of the commutator subgroup. Then, s can be written as the product of commutators of elements of G; namely, there exist $a_1, \ldots, a_n, b_1, \ldots, b_n \in G$ such that

$$a_1^{-1}b_1^{-1}a_1b_1 \cdots a_n^{-1}b_n^{-1}a_nb_n = s.$$

Since no element of the form r^k has an inverse of the form r^ks, it is clear that the left hand side of the equation contains an even number of occurrences of s. If G

is D_m or S_m, the order of s is 2, and as such an equality is impossible, as the left side will always end with s^j, for a positive even integer j. If G is Q_m, then the order of s is 4, and $z = s^2$; once again, this equality is impossible, as the left side will always end with s^j, similarly to the above case. Therefore, in all three cases, G' is generator-free, and as such, $G' \subset \Phi(G)$.

If $\Phi(G)$ strictly contained G', then as $|G/G'| = 4$, and $\Phi(G) \neq G$ because G is finite and nontrivial, it must be true that $|G/\Phi(G)| \leq 2$. However, if $|G/\Phi(G)| = 2$, then $G/\Phi(G)$ is cyclic, and so G would be cyclic as well, which is a contradiction. The remaining possibility is that $|G/\Phi(G)| = 1$, but G is finite and nontrivial, so this is not possible either. Then, here, $G' = \Phi(G)$ and $|G/\Phi(G)| = 4$.

Next, we examine the center of G, so take $[r^k, s]$. This is either $[r^k, s] = r^{-2k}$ or $r^{-2k+k2^{m-2}} = r^{-2k}z^k$, so s commutes with r if and only if $2^{m-2}|k$. Therefore, $z \in Z(G)$ and no other power of r is in $Z(G)$. In addition, no element of the form $r^j s$ centralizes r for any j, so then the center is simply $\langle z \rangle = \{e, z\}$, and so $|Z(G)| = 2$ as claimed.

Now, set $\bar{G} = G/Z(G) = \langle \bar{r}, \bar{s} \rangle$. Since G is finite,

$$\begin{aligned} |G/Z(G)| &= \frac{|G|}{|Z(G)|} \\ &= \frac{2^m}{2} = 2^{m-1}. \end{aligned}$$

In addition, for $0 \leq k < 2^{m-2}$, $r^k Z(G) = zr^k Z(G)$, so $|\bar{r}| = 2^{m-2}$. Next, if $G = Q_m$, then $s^2 = r^{2^{m-2}}$, and so $\bar{s}^2 = e$. If G is either S_m or D_m, then $s^2 = e$ to begin with, and so $\bar{s}^2 = e$ as well. Thus, in any case, $|\bar{s}| = 2$.

To demonstrate that $\bar{G} \cong D_{m-1}$, take $\bar{s}\bar{r}\bar{s}$. If G is either Q_m or D_m, then

$srs = r^{-1}$ by the construction of the group, so $\bar{s}\bar{r}\bar{s} = \bar{r}^{-1}$. If G is S_m, then

$$\begin{aligned} srsZ(G) &= \{srs,\, srsz\} \\ &= \{zr^{-1},\, r^{-1}\} \\ &= r^{-1}Z(G), \end{aligned}$$

so here as well $\bar{s}\bar{r}\bar{s} = \bar{r}^{-1}$. Therefore,

$$\bar{G} = \langle \bar{r}, \bar{s} \mid \bar{r}^{2^{m-2}} = \bar{s}^2 = e,\, \bar{s}\bar{r} = \bar{r}^{-1}\bar{s} \rangle \cong D_{m-1} \rangle.$$

If $m = 3$, then $m - 1 = 2$, and $\bar{G} \cong D_2$ is an abelian group, so necessarily $\mathrm{cl}(\bar{G}) = 1 = m - 2$. If $m \geq 4$, then $m - 1 \geq 3$ and D_{m-1} is nonabelian. For this group, $[r,\, s] = r^2$, and so $(D_{m-1},\, D_{m-1}) = \langle r^2 \rangle = H^2$, for H^i defining the lower central series. If $m = 4$, then $H^3 = (H^2,\, D_3) = \{e\}$, as $[r^2,\, x] = e$ for any $x \in D_3$, and so $\mathrm{cl}(\bar{G}) = 2 = m - 2$. Consider this to be the base case.

Consider, then, that $\mathrm{cl}(D_{m-1}) = m-2$. Now, take D_m and evaluate $(D_m,\, D_m)$. $H^2 = (D_m,\, D_m) = \langle r^2 \rangle$, and so $|\langle r^2 \rangle| = 2^{m-1}$. Then $H^3 = (H^2,\, D_m) = \langle r^4 \rangle$, as $[r^2,\, s] = r^{-2}sr^2s = r^{-4}$, so $H^3 = \langle r^4 \rangle$ and $|H^3| = 2^{m-2}$. Then, $H^3 \cong (D_{m-1},\, D_{m-1})$, and since the lower central series contains exactly one more group, $\mathrm{cl}(D_m) = m - 2 + 1 = m - 1$. By this inductive step, for any $m \geq 3$, $\mathrm{cl}(\bar{G}) = m - 2$. Therefore, we have that $\mathrm{cl}(G) = m - 1$. □

Now, facts have been established about all of D_m, S_m, Q_m, and M_m, for $m \geq 3$. It remains to be shown, then, that none of these four groups are isomorphic when of the same order.

Theorem 3.7. *No two of the groups M_m, D_m, Q_m, or S_m are isomorphic.*

Proof. In order to show that none of these four groups are isomorphic, it is sufficient to show that a property preserved under isomorphism differs between the four of them. For this proof, we will focus on $\Omega_1(G)$, for G one of the four finite 2-groups above; as usual, take $m \geq 3$ as appropriate. As a refresher, recall that $\Omega_i(G)$ is the subgroup of G generated by elements of order dividing 2^i. This subgroup is an invariant, so if the order differs for M_m, D_m, Q_m, or S_m, then they cannot be isomorphic.

In Theorem 3.5, it was established that $\Omega_i(M_m)$ is isomorphic to $\mathbb{Z}_{2^i} \times \mathbb{Z}_2$. Therefore, if $G = M_m$, then $\Omega_1(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. This subgroup is therefore of order 4, and is noncyclic abelian.

We begin the examination of the other three groups with $G = D_m$. In G,

$$\begin{aligned}(rs)^2 &= r(srs) \\ &= r(r^{-1}ss) = rr^{-1} \\ &= e,\end{aligned}$$

so $|rs| = |s| = 2$. Then, $\Omega_1(G) \supset \langle rs,\, s\rangle = \langle r,\, s\rangle = G$, so $G = \Omega_1(G)$. Therefore $\Omega_1(D_m)$ is of order 2^m and is noncyclic nonabelian.

Next, take $G = Q_m$. For any positive integer $k < 2^{m-1}$,

$$\begin{aligned}(r^k s)^2 &= r^k(sr^k s) \\ &= r^k(r^{-k}ss) = r^k r^{-k}s^2 \\ &= r^{2^{m-2}}.\end{aligned}$$

Therefore, no element of the form $r^k s$ has order 2 in G. Since $s^2 = r^{2^{m-2}} = z$ is of order 2, therefore $\Omega_1(G) = \langle z\rangle = Z(G)$. Then $\Omega_1(Q_m)$ is cyclic of order 2.

Finally, take $G = S_m$. In G, $|s| = 2$, so $s \in \Omega_1(G)$. Now, once again take any positive integer $k < 2^{m-1}$, and evaluate

$$\begin{aligned}(r^k s)^2 &= r^k(sr^k s) \\ &= r^k(r^{k2^{m-2}-k}ss) = r^k r^{k2^{m-2}-k} \\ &= r^{k2^{m-2}-k+k} = r^{k2^{m-2}} = z^k.\end{aligned}$$

Then, $|r^k s| = 2$ if and only if k is even. Then, $\Omega_1(G) = \langle r^2 s,\, s\rangle = \langle r^2,\, s\rangle$. Let $r^2 = a$. Then, $|a| = 2^{m-2}$, and

$$\begin{aligned}sa &= a^{2^{m-2}-1}s \\ &= r^{2^{m-1}-2}s \\ &= r^{-2}s = a^{-1}s.\end{aligned}$$

Therefore, $\Omega_1(G) = \langle a,\, s \mid a^{2^{m-2}} = s^2 = e,\, sa = a^{-1}s\rangle$, which is isomorphic to D_{m-1}, a noncyclic (and nonabelian for $m > 3$) group of order 2^{m-1}.

Clearly, none of $\Omega_1(M_m)$, $\Omega_1(D_m)$, $\Omega_1(Q_m)$, or $\Omega_1(S_m)$ are isomorphic, and since this subgroup is invariant, necessarily none of the four groups themselves are isomorphic, either. Thus, the claim is proved. □

With these facts established, distinguishing the above four finite 2-groups, the attention of this chapter now turns to a finite nonabelian 2-group G and discussing its structure. Before we begin the next theorem, a small piece of notation will be useful to introduce.

If G is a group and A is a subgroup of the set of automorphisms on G, then $C_G(A)$ is the set of all elements of G that are fixed by elements of A. Clearly, if

A is the trivial subgroup, then $C_G(A) = G$, as all elements are fixed by the identity automorphism. As a constructive example, we will examine $C_{\mathbb{Z}}(A)$. The integers have precisely two automorphisms: The trivial automorphism, and negation. If A contains the negation automorphism, then $C_{\mathbb{Z}}(A) = \{0\}$, as only the identity is left fixed.

For a case where this subgroup is nontrivial, consider $\mathbb{Z}_4$, again with A being the trivial and negation automorphisms. Here, $C_{\mathbb{Z}_4}(A) = \{0, 2\} \cong \mathbb{Z}_2$, as $-2 \equiv 2 \pmod 4$.

As a final issue of notation, sometimes this subgroup will be generated using a subgroup $H \subset G$. The subgroup $C_G(H)$ is the set of elements of G fixed by all inner automorphisms by elements of H. That is, $C_G(H) = \{g \mid h^{-1}gh = g \text{ for all } h \in H\}$. Note that if G is abelian, then any inner automorphism will be trivial and so $C_G(H) = G$; take any $g \in G$ and for any $h \in H$, with H a subgroup of G, $h^{-1}gh = h^{-1}hg = g$.

We now prove the key lemma en route to the main theorem of this chapter. It is a classification theorem for certain finite 2-groups. It turns out that if G is a finite nonabelian 2-group with a cyclic subgroup of half its order, then it will be isomorphic to one of the four M_m, D_m, Q_m, and S_m.

Theorem 3.8. *Let G be a nonabelian 2-group of order 2^m, which contains a cyclic subgroup H of order 2^{m-1}. Then:*

(i) If $m = 3$, then G is isomorphic to D_3 or Q_3.

(ii) If $m > 3$, then G is isomorphic to M_m, D_m, Q_m, or S_m.

Proof. Necessarily, as G is a finite nonabelian 2-group, $m \geq 3$ (as given $m < 3$, G could not be a nonabelian 2-group). In addition, H is a cyclic subgroup of order

2^{m-1} in G. This subgroup is normal, and since $|H| = 2^{m-1}$, G/H is of order 2 and therefore cyclic.

Now, as G/H is cyclic, it must be true that $H \not\subset Z(G)$. By Lemma 3.3, if $G/Z(G)$ is cyclic, then G is abelian, which contradicts the assumption of this theorem. In addition, since G is a finite group, any subgroup of G must have order dividing 2^m. Using this, it can be shown that $C_G(H) = H$. First, necessarily $H \subset C_G(H)$; as H is cyclic, for any h_1, $h_2 \in H$, $h_1^{-1}h_2h_1 = h_2$. Thus, any inner automorphism generated by an element of H will fix elements of H.

If $C_G(H)$ is not a subset of H, then $C_G(H) = G$. Therefore, $|C_G(H)| = 2^m$. This gives that H is in $Z(C_G(H))$, and because $|C_G(H)/Z(C_G(H))| = 1$ or 2, then $C_G(H)$ must be abelian, which is a contradiction. Therefore $C_G(H) \subset H$ and it can be concluded that $H = C_G(H)$. Therefore, G/H is isomorphic to a subgroup of Aut H of order 2. With this established, set $H = \langle h \rangle$, with $|h| = 2^{m-1}$.

Beginning with the first part of this theorem, assume $m = 3$. Since H is a cyclic group of order 4, it has a unique nontrivial automorphism (namely, negation). Therefore, for any $g \in G \setminus H$, it must be true that $g^{-1}hg = h^{-1}$. In addition, $G = \langle h, g \rangle$, also for $g \in G \setminus H$. Since G is nonabelian and $m = 3$, then for some positive integer a, $g^2 = h^{2a}$. If a is even, then $h^{2a} = g^2 = e$, and so $G \cong D_3$. If a is odd, then $h^{2a} = h^2 = g^2$ and so $G \cong Q_3$. Therefore, part (i) of the above claim holds.

If $m = 3$, then S_3 is abelian, and therefore it cannot be isomorphic to G. In addition, if $m = 3$, then $M_3 = \langle r, s \mid r^4 = s^2 = e, sr = r^3s = r^{-1}s \rangle$, so $M_3 = D_3$. Beginning with $m = 4$, these four groups are all nonabelian and non-isomorphic, so now we turn to part (ii) of the claim.

Suppose now that $m > 3$. Take two elements of G outside of H, namely $u, g \in G \setminus H$. Since H is of index 2 in G, $u^2 \in H$. Then $u^2 = h^{2a}$ for some nonnegative integer $a < 2^{m-1}$; if the exponent was not even, then it would generate the whole group, which is not possible as it is noncyclic.

Now, we choose an integer c such that

$$a + c(1 + 2^{m-3}) \equiv 0 \pmod{2^{m-2}}. \tag{3.7}$$

This is possible, as $m > 3$, so the exponents in the expression will never be zero. Now, take the h from above and set $g = uh^c$. Given this equality:

$$\begin{aligned} g^2 = (uh^c)^2 &= uh^c uh^c \\ &= u(uu^{-1})h^c(uu^{-1})uh^c \\ &= u^2(u^{-1}h^c u)h^c = h^2 a h^{c(1+2^{m-2})}h^c \\ &= h^{2a+2c(1+2^{m-3})} = (h^{a+c(1+2^{m-3})})^2. \end{aligned}$$

By the expression in equation (3.7), it must be that $h^{a+c(1+2^{m-3})} = e$ as h has order 2^{m-1}, so then $g^2 = e$.

With the formulation of $g \in G \setminus H$ established, we can now examine the action of g on $h \in H$. Given that $|g| = 2$, one of the following three relations must hold:

$$g^{-1}hg = h^{1+2^{m-2}}, \tag{3.8}$$

$$g^{-1}hg = h^{-1}, \tag{3.9}$$

or

$$g^{-1}hg = h^{-1+2^{m-2}}. \tag{3.10}$$

Having established these three possibilities, let us first take equation (3.8) to be the case. Since $|g| = 2$, $|h| = 2^{m-1}$, taking g on both sides of the expression yields that

$$g^{-1}hg = h^{1+2^{m-2}}$$

$$gg^{-1}hg = gh^{1+2^{m-2}} = hg,$$

so it follows from the definition of M_m that $G \cong M_m$.

Now our attention turns to the actions given by equations 3.9 and 3.10. In the case of the former, set

$$g^{-1}h^k g = h^k$$

$$= h^{-k} = h^k.$$

Since $-k \cong k \pmod{2^{m-1}}$ when $k = 2^{m-2}$, and again setting $h^{2^{m-2}} = z$, we have $\langle z \rangle \subset Z(G)$. In the case of the latter, once again set

$$g^{-1}h^k g = h^k$$

$$= h^{k(-1+2^{m-2})} = h^k.$$

Once again, we examine $-k + k2^{m-2} \cong k \pmod{2^{m-1}}$. From this, k must be even, as otherwise $k2^{m-2} \cong 2^{m-2} \pmod{2^{m-1}}$, the expression reduces to $-k \cong k \pmod{2^{m-1}}$. This gives that $k = 2^{m-2}$, so as above, $\langle z \rangle \subset Z(G)$.

In both cases, with some calculation, it turns out that $\langle z \rangle = Z(G)$. On the other hand, as $g^2 \in H$, for any $h \in H$, it must be true that $g^{-2}hg^2 = h$. In addition, $g^{-2}gg^2 = g$, so then $g^2 \in Z(G)$. Since $Z(G) = \langle z \rangle$, for some b, we have that $g^2 = z^b = h^{b2^{m-2}}$.

If b is even, then $g^2 = e$. Since g was an arbitrary element of $G \setminus H$, it can be concluded that any element in $G \setminus H$ is of order 2. Thus, if equation (3.9) is the action of g on h, then G is isomorphic to D_m. If equation (3.10) is the action, then G is isomorphic to S_m.

If b is odd, then $g^2 = z$, and if the action of g on h is given by equation (3.9), then G is isomorphic to Q_m. There remains a final case to consider, where b is odd and the action is $g^{-1}hg = h^{-1+2^{m-2}}$.

In this case, set $g = uh$. Since b was odd, it must hold that $u^2 = z$, and so

$$\begin{aligned} g^2 &= (uh)^2 \\ &= uhuh \\ &= u^2(u^{-1}hu)h \\ &= zh^{-1+2^{m-2}}h \\ &= zh^{-1+2^{m-2}+1} \\ &= z^2 = e. \end{aligned}$$

Therefore, by the defined action of g on h, in this case G is isomorphic to S_m. Thus, for any $m > 3$, G is isomorphic to one of M_m, D_m, Q_m, or S_m. □

The groups D_m, Q_m, and S_m each have class $m-1$. They also have commutator factor groups of order 4. The theorem below will show that, if $|G/G'| = 4 = 2^2$, then G is one of D_m, Q_m, or S_m and as such, G'' is trivial and therefore G does not have derived length three.

Theorem 3.9. *Let G be a finite nonabelian 2-group of order 2^m, with $cl(G) = m-1$. Then, $|G/G'| = 4$.*

Proof. Suppose $\mathrm{cl}(G) = m - 1$. G is nonabelian, and so it must be noncyclic. It was proved earlier that if $G/\Phi(G)$ is cyclic, then G is cyclic. The contrapositive of this statement gives that, necessarily, $G/\Phi(G)$ is noncyclic, so $|G/\Phi(G)| \geq 4$. Given this, it comes from [3] that $|G/G'| \geq 4$ as well.

Assume, then, that $|G/G'| > 4$. If that is the case, then the next term in the lower central series (as $H^2 = G'$), will be $H^3 = (G', G)$. Since $|G/G'| \geq 8 = 2^3$, the the case for the largest possible class of G begins with $|G/G'| = 8$, or $|H^2| = 2^{m-3}$. To maximize the length of the lower central series, for every $i \geq 3$,

$$\begin{aligned} |H^i| &= \frac{|H^{i-1}|}{2} \\ &= 2^{m-i-1} = 2^{m-(i+1)}. \end{aligned}$$

This iteration ends when $i = m - 1$, as

$$\begin{aligned} |H^{m-1}| &= 2^{m-(m-1+1)} \\ &= 2^0 = 1, \end{aligned}$$

so H^{m-1} is trivial. However, by the definition of the class of G, this would mean $\mathrm{cl}(G)$ is maximally $m - 2$, which is a contradiction with the assumption. Therefore, $|G/G'| = 4$. □

For the purposes of our main theorem, this theorem, while noncritical, provides a useful insight into groups of derived length three. As we shall see in the following theorem, if a finite 2-group G has $|G/G'| = 4$, it cannot be of derived length three. Therefore, any finite 2-group of derived length three or larger must not have class $m - 1$. In fact, it is said that any group of order 2^m with class $m - 1$ is of maximal class, and so this theorem is a classification of all groups of maximal class for $p = 2$.

Before we improve the bound, there is a lemma regarding the family of groups D_m, Q_m, and S_m that will be handy.

Lemma 3.10. *If $m > 3$, then D_m, Q_m, and S_m contain no noncyclic abelian subgroup of order 8.*

Proof. Since $m > 3$, if G is one of the groups in the claim, then $|G| \geq 16$. The goal will be to show that if G has an abelian subgroup of order 8, it must be cyclic. Unfortunately, there seems to be no way to prove the claim without explicit calculation for each group, so we will be brief and demonstrate the process for D_m.

Take G as above, and assume that there is a subgroup $H < G$ such that $|H| = 8$, and H is abelian and noncyclic. By the fundamental theorem of finite abelian groups, there are precisely two choices for H:

$$H \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \text{ or}$$

$$H \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$

In the first case, H must be generated by three distinct, commutating elements of G, each of order 2; in the second, H must be generated by two distinct, commutating elements of G, one of order 4 and the other of order 2.

If $G = D_m$, then take x, y, $z \in G$ such that $H = \langle x, y, z \rangle$ for the first case. The elements of order 2 in G are $r^{2^{m-2}}$ and $r^a s$ for $a = 1, \ldots, 2^{m-1}$, so at least two elements must be of the form $r^a s$, as each are distinct. Moreover, for at least one of them, a must not equal 2^{m-2}, in order for x, y, z to generate a group of order 8. But then, an element of that form cannot commute with another element of the form form $r^b s$ for b even. Therefore, the subgroup cannot be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Thus, H can only be isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$. Once again, all elements of order 2 are $r^{2^{m-2}}$ and $r^a s$ for $a = 1, \ldots, 2^{m-1}$, and the elements of order 4 are $r^{2^{m-3}}$ and its inverse. The order 2 element cannot be $r^{2^{m-2}}$, as otherwise the group is not of order 8, but no element of the form $r^a s$ commutes with $r^{2^{m-3}}$, so this is not possible either. Thus, $G \cong D_m$ does not have a noncyclic abelian subgroup of order 8.

Similar techniques apply almost identically to show the same for Q_m and S_m, so the claim is then proved, and no group in the family D_m, Q_m, and S_m for $m > 3$ have a noncyclic abelian subgroup of order 8. □

With this brief lemma completed, attention now turns to the final claim, which will show that any finite 2-group G of derived length three must have $|G/G'| > 4$.

Theorem 3.11. *Let G be a finite nonabelian 2-group, of order 2^m with $m \geq 3$, in which $|G/G'| = 4$. Then G is isomorphic to one of D_m, Q_m, or S_m, none of which are of derived length 3.*

Proof. First, let G be a finite nonabelian 2-group, of order 2^m with $m = 3$. We know that G is nonabelian, so by Lemma 3.4, there must be at least one element of order greater than 2. That element cannot be of order 8, as then G would be cyclic, so G must contain an element of order 4. Then, G must contain a cyclic subgroup of order 4. By Theorem 3.8 (i), G must then either be D_3 or Q_3.

Now, let $m \geq 3$. We know that G' is a normal subgroup of G and G' is nontrivial as G is nonabelian, so there is a nontrivial subgroup of order 2 in the intersection of $Z(G)$ and G'. Set Z to be precisely that subgroup, and now set $\bar{G} = G/Z$.

Next, set $\bar{G}'$ as the image of G' under the natural surjective homomorphism

$G \to G/Z$, and so $|\bar{G}/\bar{G}'| = 4$ as well. Since $m > 3$, it is guaranteed that $\bar{G}$ is nonabelian, because

$$|\bar{G}| = |G|/2 = 2^{m-1},$$

and $m - 1 \geq 3$. Using the $m = 3$ case as the base case for induction, it holds then that $\bar{G}$ is isomorphic to one of D_{m-1}, Q_{m-1}, or S_{m-1}. Since $\bar{G}$ is one of those three groups, define $\bar{H}$ to be the maximal cyclic subgroup of $\bar{G}$. Correspondingly, let H in G be the inverse image of $\bar{H}$.

If H is cyclic, then by Theorem 3.8(i), G must be isomorphic to one of M_m, D_m, Q_m, or S_m. However, by Theorem 3.5, for any $m > 3$, if $G \cong M_m$:

$$\begin{aligned} |G/G'| &= 2^{m-1} \\ &> 2^{3-1} = 4, \end{aligned}$$

which contradicts the assumption of this theorem. Thus G is isomorphic to one of the three desired groups.

Now, we consider the case in which H is not cyclic. Take the center of H, that is, $Z(H)$. Since $H \leq G$, it must be the case that $Z(H)$ contains $Z(G)$, as any element of $Z(G)$ commutes with all elements of H. Therefore, the above Z is in $Z(H)$. In addition, as H/Z is cyclic by above, Lemma 3.3 gives that H must be abelian, but it

is not cyclic. The above statements show that $|Z| = 2$, and

$$\begin{aligned} |\bar{H}| &= 2^{m-2} \\ &= |H/Z| \\ &= \frac{|H|}{|Z|} \end{aligned}$$

which in turn gives that

$$\begin{aligned} |H| &= 2^{m-2} \cdot |Z| \\ &= 2^{m-2} \cdot 2 \\ &= 2^{m-1}. \end{aligned}$$

By the fundamental theorem of finite abelian groups, H must be the product of cyclic groups, and since H/Z is cyclic of order 2^{m-2}, H has a cyclic factor of at least that order. Since H is not cyclic and of order 2^{m-1} by the above considerations, it must be true that

$$H = \langle x,\, y \mid x^{2^{m-2}} = y^2 = e \rangle.$$

Once again, out of convenience, we set $x^{2^{m-3}} = z$. Now, consider both the subgroups $\mho^1(H)$ and $\Omega_1(H)$; recall that the former is the subgroup of H generated by elements of exponent 2, and the latter is generated by elements whose order divides 2. Since $m > 3$, these two subgroups are given by

$$\begin{aligned} \Omega_1(H) &= \langle x^2 \rangle \\ \mho^1(H) &= \{e,\, z,\, y,\, zy\}. \end{aligned}$$

Now, set X to be the intersection of $\Omega_1(H)$ and $\mho^1(H)$. Clearly, since $y \notin \Omega_1(H)$, $X = \langle z \rangle$, and X is a characteristic subgroup of H that is normal in G. Therefore, $X \subset Z(G)$, and so $\bar{X} \subset Z(\bar{G})$, where $\bar{X}$ is understood to be the image of X under the natural surjective homomorphism.

$\bar{X}$ is nontrivial in $\bar{G}$, so by Theorem 3.8(ii), $\bar{X} = Z(\bar{G})$. In addition, $Z(\bar{G}) \subset \bar{G}'$, so therefore $X \subset G'$. With this, set $\hat{G} = G/X$. Since $|X| = 2$, once again applying the induction of earlier, we get that $\hat{G}$ is isomorphic to D_{m-1}, Q_{m-1}, or S_{m-1}.

By Lemma 3.10, it was shown that no group in the family D_m, Q_m, or S_m has a noncyclic abelian subgroup of order 8 for $m > 3$. Since x, y form a basis of H, the image $\hat{H}$ of H in $\hat{G}$ must be abelian and isomorphic to $\mathbb{Z}_{2^{m-3}} \times \mathbb{Z}_2$. By the above considerations, since $\hat{G}$ cannot contain a noncyclic abelian subgroup of order 8, the only possibility is that $m = 4$.

Assume that is the case. Then, $XZ \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so $|XZ| = 4$, and so

$$\begin{aligned} |G/XZ| &= \frac{|G|}{|XZ|} \\ &= \frac{16}{4} = 4. \end{aligned}$$

In addition, $XZ \subset G' \cap Z(G)$. If XZ were a proper subset of $G' \cap Z(G)$, then $|G/Z(G)| \leq 2$, which would imply that G is cyclic. This is a contradiction, as G was assumed to be nonabelian, so necessarily $XZ = Z(G)$, and so $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Therefore, for suitable $\alpha, \beta \in G$, $G = \langle Z(G), \alpha, \beta \rangle$. This can be done because $G/Z(G)$ must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, and so α and β may be taken to be the preimages of (1, 0) and (0, 1).

From this, it follows that the commutation $[\alpha, \beta]$ must generate G', so G' is

cyclic. This is a contradiction, as $XZ \subset G'$ by the above considerations, and XZ is noncyclic. Therefore, it must be concluded that H cannot be noncyclic. Consequently H, as taken initially, must be cyclic in G. Thus, as was proved above in that case, G must be isomorphic to one of D_m, Q_m, or S_m. □

With this proof completed, the results can now be combined with the main result of the previous chapter to give the main result of this thesis. If G is a finite nonabelian 2-group that has $|G/G'| = 4$, then it must be one of the family D_m, Q_m, or S_m. However, if G is any one of these, then G'' is abelian. Therefore, $|G'/G''| = 2^{m-2}$, and G''' is trivial.

Since $G''' = G^3$ is trivial, it must be that G has derived length 2. It can then be concluded that if G is a finite nonabelian 2-group with $|G/G'| = 4$, then G does not have derived length 3. In the conclusion of Chapter 2, the proved statement was that if G is of derived length 3, then $|G/G'| \geq 4$ and $|G'/G''| \geq 8$. Since any group that has $|G/G'| = 4$ is not of derived length 3, we reformulate the statement to the one that appears below.

Corollary 3.12. *If G is a finite nonabelian 2-group of derived length 3, then $|G/G^1| \geq 2^3$ and $|G^1/G^2| \geq 2^3$.*

With this established, we have improved the lower bounds on the quotients of the derived series, and the main goal of this paper is accomplished.

REFERENCES

[1] A. Al–Fares, *Semidirect Products Of The Integers Modulo 2,* Master's Thesis, California State University, Los Angeles, 2014.

[2] D. S. Dummit and R. M. Foote, *Abstract Algebra,* Graduate Texts in Mathematics, John Wiley & Sons, Inc., Hoboken, 2004.

[3] D. Gorenstein, *Finite Groups, Second Edition,* A Book in Mathematics, Chelsea Publishing Co., New York, 1980.

[4] P. Hall, *A Contribution to the Theory of Groups of Prime-Power Order,* Proceedings of the London Mathematical Society: **S2-36**, No 1, 29–07.

[5] M. Krebs and A. Shaheen, *Expander Families And Cayley Graphs,* Oxford University Press, New York, 2011.