Czechoslovak Mathematical Journal

Elliot Benjamin; Chip Snyder

On some finite 2-groups in which the derived group has two generators

Czechoslovak Mathematical Journal, Vol. 73 (2023), No. 1, 71–100

Persistent URL: http://dml.cz/dmlcz/151505

Terms of use:

© Institute of Mathematics AS CR, 2023

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

Czechoslovak Mathematical Journal, 73 (148) (2023), 71–100

ON SOME FINITE 2-GROUPS IN WHICH THE DERIVED GROUP HAS TWO GENERATORS

Elliot Benjamin, Minneapolis, Chip Snyder, Orono

Received November 1, 2021. Published online June 20, 2022.

Abstract. We show that any finite 2-group, whose abelianization has either 4-rank at most 2 or 8-rank 0 and whose commutator subgroup is generated by two elements, is metabelian. We also prove that the minimal order of any 2-group with nonabelian commutator subgroup of 2-rank 2 is 2^{12}.

Keywords: 2-group; metabelian

MSC 2020: 20D15

1. Introduction

We prove the following main result and a corollary:

Main Theorem. *Let G be a finite 2-group such that* 2-rank$(G') = 2$ *and either* 4-rank$(G/G') \leqslant 2$ *or* 8-rank$(G/G') = 0$. *Then G is metabelian, i.e., G' is abelian.*

In other words, if G is any nonmetabelian finite 2-group for which 2-rank$\,G' = 2$, then G/G' must contain a subgroup isomorphic to $(8, 4, 4)$.

Corollary. *The minimal order of a finite 2-group G for which its commutator subgroup G' is nonabelian and of 2-rank 2, is 2^{12}.*

The Main Theorem is sharp in the sense that there are nonmetabelian finite 2-groups G for which G' has 2-rank 2 and such that $G/G' \simeq (8, 4, 4)$; refer to the example in Section 4 below for one of minimal order.

This theorem and its corollary may be considered as a major extension of results in Blackburn's article on p-groups (see [2]) for the prime $p = 2$. More precisely, Theorem 1 in [2] implies that any finite p-group G, whose commutator subgroup has p-rank 2, has derived length 2 or 3. In particular, by Theorem 4 of [2], if the

DOI: 10.21136/CMJ.2022.0415-21

© Institute of Mathematics, Czech Academy of Sciences 2022.

p-group G, as well as G', has p-rank 2, then the derived length of G is equal to 2. Our main goal was to obtain more general hypotheses than that of Theorem 4, which still imply that G has derived length 2. For $p = 2$ this led to our main theorem and its corollary. These results were motivated by the problem of determining the length of the 2-class field tower of certain families of algebraic number fields, and consequently they may be of use to algebraic number theorists.

The proofs of the results are elementary and combinatorial in nature. We have followed much of the presentation given in Blackburn's article, see [2].

2. Some preliminaries

In this section we review some "commutator calculus" and introduce some notation; see the exposition given, for example, in [1]. Assume for the moment that G is an arbitrary group written multiplicatively. If $x, y \in G$, then define $[x, y] = x^{-1}y^{-1}xy$, the commutator of x with y. More generally, since $[*, *]$ is not associative, we define (inductively on l) $[x_1, \ldots, x_l] = [[x_1, \ldots, x_{l-1}], x_l]$ for all $x_j \in G$ and $l > 2$. If A and B are nonempty subsets of G, then $[A, B]$ is the subgroup of G given as $[A, B] = \langle\{[a, b]\colon\ a \in A,\ b \in B\}\rangle$. In particular, the commutator subgroup G' is defined as $[G, G]$; also $G'' = (G')'$. Recall, too, that a group G is metabelian if $G'' = 1$, i.e., G' is abelian. Moreover, we denote conjugation of x by y as

$$x^y = y^{-1}xy \quad \text{for any } x, y \in G.$$

Notice then that

$$x^y = x[x, y]. \tag{1}$$

Also notice that

$$[x, y]^z = [x^z, y^z] \quad \text{for any } z \in G. \tag{2}$$

Of particular use in our analysis is the lower central series $\{G_l\}$ of G, which is defined inductively as $G_1 = G$, and $G_{l+1} = [G, G_l]$ for all $l \geqslant 1$. In particular, observe that $G_2 = G'$. The lower central series is especially useful when the group G is nilpotent, i.e., when the lower central series terminates in finitely many steps at the identity subgroup 1. As is well known, all finite p-groups are nilpotent for any prime p.

Recall that for any $x, y, z \in G$,

$$\begin{gathered}[xy, z] = [x, z][x, z, y][y, z], \quad [x, yz] = [x, z][x, y][x, y, z],\\ [x, y^{-1}]^y = [x^{-1}, y]^x = [y, x] = [x, y]^{-1},\\ [x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1 \quad \text{(Witt Identity)}\end{gathered} \tag{3}$$

(cf. [3], for example).

We also introduce here some notation: Suppose $G = \langle a_1, a_2, \ldots, a_r \rangle$; then we let

$$c_{ij} = [a_i, a_j], \quad c_{ijk} = [a_i, a_j, a_k], \quad \text{etc.}$$

Let $(2^{l_1}, 2^{l_2}, 2^{l_3})$ denote the direct sum of cyclic groups of order 2^{l_i} for $i = 1, 2, 3$ and similarly for other such cases.

As usual, we denote by $Z(G)$ the center of G and moreover $G^p = \langle x^p \colon x \in G \rangle$.

Now we recall some facts about the Frattini subgroup of a p-group and the Burnside Basis Theorem. Let G be a finite p-group (p any prime). Then recall that the Frattini subgroup of G, $\Phi(G)$, is the subgroup $G^p G'$ of G. When $p = 2$, as in our case, then $\Phi(G) = G^2$, since $G' \subseteq G^2$.

Theorem 1 ([4], Kapitel III, version of Burnside Basis Theorem)**.** *Let G be a finite p-group. Then the elements $x_1, \ldots, x_d$ generate G if and only if the cosets $x_1\Phi(G), \ldots, x_d\Phi(G)$ generate $G/\Phi(G)$.*

Recall, too, that the rank r of a finite abelian p-group is the number of nontrivial cyclic summands in its direct sum decomposition. (More generally, its p^n-rank is the number of cyclic summands of order at least p^n.) As a consequence of the Burnside Basis Theorem we see that for a finite p-group G, the order $|G/\Phi(G)| = p^r$, where r is the rank of $G^{\mathrm{ab}} = G/G'$. Again by the Burnside Basis Theorem, a minimal set of generators of G has cardinality equal to the rank of the abelianization G^{ab}. Finally, if $\{x_1 G', \ldots, x_r G'\}$ is a basis of G^{ab}, then $\{x_1, \ldots, x_r\}$ is a minimal generating set of G, and by abuse of language we will call it a basis of G, cf. [4], page 80.

3. Reduction of the proof to groups of rank 3

Proposition 1. *Let G be a finite 2-group for which its commutator subgroup G' is nonabelian and of rank 2. Then there exists a subgroup H of G for which* $\operatorname{rank} H = 3$ *and such that $H' = G'$.*

P r o o f. From Theorem 1 in [2], we have $G' = \langle a, b \rangle$ with the presentation

$$a^{2^m} = b^{2^{n+k}} = 1, \quad [a, b] = b^{2^n},$$

with integers k, m, n such that $0 < 2k \leqslant m \leqslant n$. Moreover, by Theorem 2 and the results above it in [2], we see that $G_3 \subseteq Z(G_2) = G_2^{2^k} \subseteq G_2^2$.

Next, notice that there exist x_1 and x_2 in G such that $[x_1, x_2] = a^\alpha b^\beta$ for some integers α and β with β odd. (Otherwise, G' would not contain an element of order 2^{n+k}.) If we let $b' = a^\alpha b^\beta$, then G' is generated by a and b' with the analogous

presentation as above. Relabeling b' as b gives us $[x_1, x_2] = b$. We also see that there are elements x_3, x_4 in G for which $[x_3, x_4] \equiv ab^\eta \bmod G_2^2$ for some integer η, otherwise $G' \neq \langle a, b\rangle$.

If there is an element x in G such that $[x_1, x]$ or $[x_2, x] \equiv ab^\lambda \bmod G_2^2$, then we may take $H = \langle x_1, x_2, x\rangle$ and we are done (cf. Theorem 4 of [2], which guarantees that $\operatorname{rank} H = 3$).

Now suppose that $[x_i, z] \equiv b^\delta \bmod G_2^2$ for all $z \in G$ and $i = 1, 2$. If $[x_1, x_3] \equiv b \bmod G_2^2$, then we may take $H = \langle x_1, x_3, x_4\rangle$ and then see (as the reader may verify) that $H' = G'$. On the other hand, if $[x_1, x_3] \equiv 1 \bmod G_2^2$, then let $H = \langle x_1, x_2x_3, x_4\rangle$ for $[x_1, x_2x_3] \equiv [x_1, x_2][x_1, x_3] \equiv b \bmod G_2^2$ and $[x_2x_3, x_4] \equiv [x_3, x_4][x_2, x_4] \equiv ab^\lambda \bmod G_2^2$. □

By this proposition it suffices to study 2-groups G of rank 3 such that G' is of rank 2. We now examine properties of some related groups. In what follows, when G' is nonabelian of rank 2, then we may assume that G'' has order 2; for if not, then since $(G'')^2$ is a characteristic subgroup of G and thus normal, we may consider $G/(G'')^2$ without loss of generality.

Lemma 1. *Suppose that G is a finite 2-group of rank 3, say $G^{\mathrm{ab}} \simeq (2^{l_1}, 2^{l_2}, 2^{l_3})$, and that G' is nonabelian of rank 2 such that $|G''| = 2$. Then G has a basis $\{a_1, a_2, a_3\}$ such that*

(i) $a_i^{2^{l_i}} \equiv 1 \bmod G'$ *for* $i = 1, 2, 3$;

(ii) $c_{23} \in G_2^2$ *and* $G_2 = \langle c_{12}, c_{13}\rangle$;

(iii) $c_{jik} = c_{ijk}^{-1}$ *for all* $i, j, k \in \{1, 2, 3\}$;

(iv) $G_j \subseteq G_2^{2^{j-2}} = \langle c_{12}^{2^{j-2}}, c_{13}^{2^{j-2}}\rangle$ *for all* $j \geqslant 2$;

(v) $G'' = \langle [c_{12}, c_{13}]\rangle$ *and* $[c_{12}, c_{13}] = c_{123}c_{231}c_{312}$;

(vi) *there exist integers m, n with $2 \leqslant m \leqslant n$ and $a, b \in G_2$ such that G_2 has a presentation given by*

$$G_2 = \langle a, b\colon\ a^{2^m} = b^{2^{n+1}} = 1,\ [a, b] = b^{2^n}\rangle.$$

P r o o f. In light of the discussion at the end of the previous section, we can find basis elements satisfying (i).

To prove (ii), we first see that $G_2 = \langle c_{12}, c_{13}, c_{23}, G_3\rangle = \langle c_{12}, c_{13}, c_{23}, G_2^2\rangle$, since $G_3 \subseteq G_2^2$ (for by Theorem 2 and the results immediately above it in [2], we see that $G_3 \subseteq Z(G_2) = G_2^2$, since $k = 1$). If $c_{ij} \in G_2^2$ for some $i, j \in \{1, 2, 3\}$, $i \neq j$, then we may relabel our basis so that $c_{23} \in G_2^2$. Hence, in this case, $G_2 = \langle c_{12}, c_{13}\rangle$ by the Burnside Basis Theorem, since G_2 has rank 2.

We still need to show that we can assume that some $c_{ij} \in G_2^2$. Without loss of generality, we may assume $c_{13}c_{23} \in G_2^2$ or $c_{12}c_{13}c_{23} \in G_2^2$. Now suppose $c_{13}c_{23} \in G_2^2$. Then let

$$a_1' = \begin{cases} a_2 & \text{if } l_1 \geqslant l_2, \\ a_1 & \text{if not,} \end{cases} \qquad a_2' = a_1a_2, \quad a_3' = a_3.$$

Hence, $c_{23}' \equiv c_{13}c_{23} \bmod G_2^2$ and notice that a_1', a_2', a_3' form a basis of G. Finally, suppose $c_{12}c_{13}c_{23} \in G_2^2$. Without loss of generality, assume $l_3 \leqslant l_i$ $(i = 1, 2)$ and let $a_1' = a_1a_3$, $a_2' = a_2a_3$, $a_3' = a_3$. Hence, we have $c_{12}' \equiv c_{12}c_{13}c_{23} \bmod G_2^2$ and a_1', a_2', a_3' is again a basis of G, as desired.

In proving (iii), notice that by (3) and (1) and the fact that $G_3 \subseteq Z(G_2)$, $c_{jik} = [c_{ij}^{-1}, a_k] = [c_{ij}^{-1}, a_k][c_{ij}^{-1}, a_k, c_{ij}] = [c_{ij}^{-1}, a_k]^{c_{ij}} = [a_k, c_{ij}] = c_{ijk}^{-1}$.

Next, (iv) follows easily by induction on j.

Part (v) can be seen as follows: Notice that by (1), (2), (3), and the fact that $G_3 \subseteq Z(G_2)$, we have for any $x, y, z \in G$

$$\begin{aligned}[x, y^{-1}, z]^y &= [[x, y^{-1}]^y, z^y] = [[y, x], z[z, y]] = [[y, x], [z, y]][y, x, z][y, x, z, [z, y]] \\ &= [y, x, z][[y, x], [z, y]].\end{aligned}$$

Hence, using (3) again, the Witt Identity may be written as

$$1 = [y, x, z][z, y, x][x, z, y][[y, x], [z, y]][[z, y], [x, z]][[x, z], [y, x]].$$

Thus, by letting $y = a_i$, $x = a_j$, $z = a_k$ for any $i, j, k \in \{1, 2, 3\}$, we have

$$1 = c_{ijk}c_{kij}c_{jki}[c_{ij}, c_{ki}][c_{ki}, c_{jk}][c_{jk}, c_{ij}].$$

By taking $(i, j, k) = (1, 2, 3)$ and using the fact that $c_{23} \in G_2^2 = Z(G_2)$, we find that

$$1 = c_{123}c_{312}c_{231}[c_{12}, c_{31}]$$

or equivalently

$$c_{123}c_{312}c_{231} = [c_{31}, c_{12}].$$

Now since $[c_{12}, c_{31}] = [c_{12}, c_{13}^{-1}] = [c_{12}, c_{13}^{-1}]^{c_{13}}$, we have

$$[c_{12}, c_{31}] = [c_{12}, c_{13}^{-1}]^{c_{13}} = [c_{13}, c_{12}].$$

Therefore,

$$c_{123}c_{312}c_{231} = [c_{12}, c_{13}].$$

Clearly, $G'' = \langle [c_{12}, c_{13}] \rangle$, cf. Theorem 1 in [2].

Finally, (vi) follows from Theorem 1 of [2] and the assumption that G'' is of order 2.

□

By Lemma 1, we have $\langle a, b\rangle = \langle c_{12}, c_{13}\rangle$. We first consider relations between a, b and c_{12}, c_{13}.

Lemma 2. *Suppose G satisfies all the conditions of Lemma* 1.

(i) *Then there are basis elements a_j given as in Lemma* 1 *for which the order $|c_{12}| > |c_{13}|$ and whence we may let $b = c_{12}$ and $a = c_{13}c_{12}^{\delta}$ for some even integer δ.*

(ii) *If $l_2 = l_3$ and $[b, a_2] \in G_2^4$ for the basis elements a_j given in Lemma* 2 (i), *then there are basis elements, again as in Lemma* 1 *for which $b = c_{12}$ and $a = c_{13}$.*

(See the proof of Lemma 2 in [2] for a similar type of argument.)

P r o o f. With respect to (i), we may initially take

$$b = \begin{cases} c_{12} & \text{if } |c_{12}| \geqslant |c_{13}|, \\ c_{13} & \text{if not.} \end{cases}$$

If $|c_{13}| \geqslant |c_{12}|$, then switch the roles of the indices 2 and 3. Hence, we then have $|c_{12}| \geqslant |c_{13}|$ and we set $b = c_{12}$. Now suppose $|c_{12}| = |c_{13}|$. Since $G_2^{2^m}$ has rank 1, we see that $c_{13}^{2^m} = c_{12}^{2^m u}$ for some odd integer u. If $|a_2G_2| > |a_3G_2|$, then switch the roles of the indices 2 and 3 again. Now let $a_3' = a_2^{-u}a_3$. Then $c_{13}' = [a_1, a_3']$ is such that $|c_{13}'| \leqslant 2^n < 2^{n+1} = |c_{12}|$. Notice, too, that a_1, a_2, a_3' form a basis of G.

Thus, we may assume that $|c_{13}| < |c_{12}|$. Let $b = c_{12}$, and so $c_{13}^{2^m} = c_{12}^{2^m u}$, where this time u is even. Let $a = c_{13}c_{12}^{\delta}$ with $\delta = -u$. Hence, a, b satisfy the conditions above in the presentation of G_2.

Now consider (ii). Before continuing, notice that any $c \in G'$ can be taken as the element a given in the presentation of G' in Lemma 1 (vi) if and only if $|c| = 2^m$ and $\langle c\rangle \cap \langle b\rangle = 1$. We will use this characterization to come up with a basis for which $c_{13} = a$.

First notice that if $|c_{13}| = 2^m$ (the minimal possible order of c_{13}), then we may take $c_{13} = a$. For if $\langle c_{13}\rangle \cap \langle c_{12}\rangle \neq 1$, then $1 \neq c_{13}^{2^\alpha} \in \langle c_{12}\rangle$ for some integer α. But since $G_2^{2^{m-1}} = \langle c_{13}^{2^{m-1}}, c_{12}^{2^{m-1}}\rangle$ has rank 2, we see $\alpha \geqslant m$, a contradiction.

Now let $|c_{13}| = 2^t$, then we have $m \leqslant t \leqslant n$. If $t = m$, we are done, as we may take $a = c_{13}$. Thus, suppose $t > m$. Then we see that by replacing a_3 by $a_3a_2^u$ for some integer u, our new c_{13} will have order less than 2^t. Repeating the process until the order becomes 2^m completes the proof.

We will use the following results, which are left to the reader to verify:

(a) $$[G_2, G^{2^\kappa}] \subseteq G_2^{2^{\kappa+1}} \quad \text{for all integers } \kappa \geqslant 0.$$

This follows by induction on κ using (3) and the fact that $G_3 \subseteq G_2^2$.

(b) $$[c_{12}^{2^\kappa}, a_2^{2^\kappa}] \in G_2^{2^{\kappa+2}} \quad \text{for all integers } \kappa \geqslant 0.$$

This follows by induction on κ using (3), the fact that $G_3 \subseteq G_2^2$, and our assumption that $[b, a_2] \in G_2^4$. Namely, notice that for $\kappa = 0$, $[c_{12}, a_2] = [b, a_2] \in G_2^4$.

Statement (b) can then be used to establish (c):

(c) $$[a_1, a_2^{2^\kappa}] \equiv c_{12}^{2^\kappa} \bmod G_2^{2^{\kappa+1}} \quad \text{for all integers } \kappa \geqslant 0.$$

This follows again by induction on κ using (b) in the appropriate places.

Now once again assume $|c_{13}| = 2^t$, with $t > m$. Since $G_2^{2^m} = \langle c_{12}^{2^m} \rangle$, we see that $c_{13}^{2^m} = c_{12}^{-2^m u}$ for some positive integer u. Write $u = 2^v u_0$ for some positive integers v, u_0 with u_0 odd. Since $|c_{13}^{2^m}| = 2^{t-m}$, we get $v = n + 1 - t$ (for $|c_{12}^{-2^{m+v}}| = 2^{n+1-m-v} = 2^{t-m}$).

Let $a_3' = a_3 a_2^u$. By replacing $a_2^{u_0}$ by a_2 we may assume that $u_0 = 1$. Thus, $a_3' = a_3 a_2^{2^v}$. Then we claim that $c_{13}' = [a_1, a_3']$ has order $< |c_{13}|$. To see this, first notice that $c_{13}'^{2^{t-1}} = (c_{13}'^{2^m})^{2^{t-1-m}}$. Furthermore,

$$c_{13}' = [a_1, a_3 a_2^{2^v}] = c_{13}[a_1, a_2^{2^v}][c_{13}, a_2^{2^v}].$$

But $[a_1, a_2^{2^v}] \equiv c_{12}^{2^v} \bmod G_2^{2^{v+1}}$ by (c) above, and $[c_{13}, a_2^{2^v}] \equiv 1 \bmod G_2^{2^{v+1}}$ by (a). Hence, $c_{13}' = c_{13} c_{12}^{2^v} \gamma$ for some $\gamma \in G_2^{2^{v+1}}$. Now recall from above that $c_{13}^{2^m} = c_{12}^{2^{m+v}}$, since $u = 2^v$. Therefore,

$$c_{13}'^{2^m} = c_{13}^{2^m} c_{12}^{2^{m+v}} \gamma^{2^m} = \gamma^{2^m}.$$

Finally, this implies that

$$c_{13}'^{2^{t-1}} = (\gamma^{2^m})^{2^{t-1-m}} = \gamma^{2^{t-1}} \in G_2^{2^{v+t}} = G_2^{2^{n+1}} = 1,$$

as desired.

Notice that the changes in the basis elements that we made still give us a basis satisfying the conditions in Lemma 1.

This establishes the lemma. □

Now we recall a result of Blackburn:

Lemma 3. *Let G be as in Lemma 2 (i). If x is any element of G, then there are integers r, s, u, v such that*

$$[a, x] = a^{2r} b^{2s2^{n-m}}, \quad [b, x] = a^{2u} b^{2v}.$$

P r o o f. This is an immediate consequence of Equations (13) and (14) and Lemma 2 of [2], and the fact that $[b, x] \in G_3 \subseteq G_2^2 = \langle a^2, b^2 \rangle$, whence the exponent of a in $[b, x]$ must be even. □

We next obtain some congruences involving the exponents of a, b in Lemma 3.

Lemma 4. *Let G be as in Lemma 3. For $x, y \in G$, let the integers r, r^*, s, s^*, u, u^*, v, v^* be given (as in Lemma 3) by*

$$[a,x] = a^{2r}b^{2s2^{n-m}}, \quad [b,x] = a^{2u}b^{2v}, \quad [a,y] = a^{2r^*}b^{2s^*2^{n-m}}, \quad [b,y] = a^{2u^*}b^{2v^*}.$$

If $x^2 = a^\mu b^\nu$ for some integers μ, ν, then the following congruences hold:

$$\begin{aligned} &r(1+r) + us2^{n-m} \equiv 0 \bmod 2^{m-2}, \quad && s(1+r+v) \equiv 2^{m-2}\nu \bmod 2^{m-1}, \\ &u(1+r+v) \equiv 0 \bmod 2^{m-2}, && v(1+v) + us2^{n-m} \equiv 2^{n-2}\mu \bmod 2^{n-1}. \end{aligned}$$

On the other hand, if $[x,y] = a^\alpha b^\beta$ for some integers α, β, then

$$u\varrho^* - u^*\varrho \equiv 0 \bmod 2^{m-2}, \quad us^* - u^*s \equiv 2^{m-2}\alpha \bmod 2^{m-1},$$
$$s\varrho^* - s^*\varrho \equiv 2^{m-2}\beta \bmod 2^{m-1},$$

where $\varrho = v - r$ and similarly for ϱ^*.

P r o o f. (Sketch.) Using the fact that $G_3 \subseteq Z(G_2) = G_2^2$, it is straightforward to show that for any $\gamma \in G_2$ and $x \in G$, we have

$$[\gamma^l, x] = [\gamma, x]^l.$$

Now we consider calculating $[a, x^2]$ and $[b, x^2]$ in two different ways, which will give us the first set of congruences. First notice that

$$[a, x^2] = [a, a^\mu b^\nu] = [a, b]^\nu = b^{2^n\nu}.$$

On the other hand, we have by (3)

$$[a, x^2] = [a, x]^2[a, x, x].$$

Now, $[a,x] = a^{2r}b^{2s2^{n-m}}$, $[b,x] = a^{2u}b^{2v}$, and thus,

$$[a,x,x] = [a,x]^{2r}[b,x]^{2s2^{n-m}}$$

and so

$$[a, x^2] = a^{4(r(1+r)+us2^{n-m})}b^{4s2^{n-m}(1+r+v)}.$$

Therefore, using the fact that the order of a is $|a| = 2^m$ and $|b| = 2^{n+1}$ along with the observation that any element in G' is a product of a unique power of a with a unique power of b, we obtain the congruences

$$r(1+r) + us2^{n-m} \equiv 0 \bmod 2^{m-2}, \quad s(1+r+v) \equiv 2^{m-2}\nu \bmod 2^{m-1}.$$

A similar calculation on $[b, x^2]$, which is left to the reader, gives the rest of the first set of congruences in the lemma.

The second set of congruences is proved in a similar manner, in which we calculate $[a, xy]$, $[b, xy]$, and compare it to $[a, yx[x, y]]$ and $[b, yx[x, y]]$. We leave the details to the reader. Similar calculations can be found in [2]. □

We now assume that G satisfies the conditions of Lemma 2 (i) and that the 4-rank of G^{ab} is $\leqslant 2$. Hence, we have the following condition.

($\mathcal{C}$) $G/G' \simeq (2^{l_1}, 2^{l_2}, 2)$ $(l_i \geqslant 1)$ with $G = \langle a_1, a_2, a_3\rangle$ such that $a_\zeta^{2^{l_1}} \equiv a_\xi^{2^{l_2}} \equiv a_\lambda^2 \equiv 1 \bmod G'$ for $\{\zeta, \xi, \lambda\} = \{1, 2, 3\}$, $G' = \langle c_{12}, c_{13}\rangle$ is nonabelian, $c_{23} \in G_2^2$, and $|c_{13}| < |c_{12}|$; thus, $b = c_{12}$ and $a = c_{13}c_{12}^{\delta}$ with $\delta \equiv 0 \bmod 2$, where a, b are as given in Lemma 1 (vi).

In what follows, we show that these assumptions lead to a contradiction, from which we can conclude that no such nonmetabelian G exists. (It can be shown that $k = 1$ when the 4-rank of G^{ab} is not greater than 2. However, as noted above, when G' is nonabelian of rank 2, we may without loss of generaltiy assume that $|G''| = 2$, i.e., $k = 1$, cf. Theorem 1 in [2].)

From above we may assume that

$$a_\lambda^2 = a^{\mu_\lambda} b^{\nu_\lambda}, \quad c_{23} = a^{2\mu_0} b^{2\nu_0}, \quad [a, a_j] = a^{2r_j} b^{2s'_j}, \quad [b, a_j] = a^{2u_j} b^{2v_j} \quad (j = 1, 2, 3),$$

where $s'_j = s_j 2^{n-m}$ with m, n as in Lemma 1 (vi).

By Lemma 4 we have the following congruences:

(I)
$$\begin{aligned} r_\lambda(1 + r_\lambda) + u_\lambda s_\lambda\, 2^{n-m} &\equiv 0 \bmod 2^{m-2},\\ s_\lambda(1 + r_\lambda + v_\lambda) &\equiv 2^{m-2}\nu_\lambda \bmod 2^{m-1},\\ u_\lambda(1 + r_\lambda + v_\lambda) &\equiv 0 \bmod 2^{m-2},\\ v_\lambda(1 + v_\lambda) + u_\lambda s_\lambda\, 2^{n-m} &\equiv 2^{n-2}\mu_\lambda \bmod 2^{n-1}. \end{aligned}$$

More generally, if G satisfies all the conditions in Lemmas 1 and 2 (i), then

(II)
$$\begin{aligned} u_1 s_2 - u_2 s_1 &\equiv 0 \bmod 2^{m-1},\\ \varrho_1 s_2 - \varrho_2 s_1 &\equiv 2^{m-2} \bmod 2^{m-1},\\ u_1 s_3 - u_3 s_1 &\equiv 2^{m-2} \bmod 2^{m-1},\\ \varrho_1 s_3 - \varrho_3 s_1 &\equiv 0 \bmod 2^{m-1},\\ u_2 s_3 - u_3 s_2 &\equiv 0 \bmod 2^{m-1},\\ \varrho_2 s_3 - \varrho_3 s_2 &\equiv 0 \bmod 2^{m-1},\\ u_1 \varrho_2 - u_2 \varrho_1 &\equiv 0 \bmod 2^{m-2},\\ u_1 \varrho_3 - u_3 \varrho_1 &\equiv 0 \bmod 2^{m-2},\\ u_2 \varrho_3 - u_3 \varrho_2 &\equiv 0 \bmod 2^{m-2}. \end{aligned}$$

We will make use of the following proposition in our proof.

Proposition 2. *Let G be as given in Lemma* 2 (i). *Then the following congruences hold:*

$$\varrho_3 \equiv s_2 \equiv s_3 \equiv u_2 \equiv 0 \bmod 2,$$

and

$$\begin{aligned}
&\varrho_1 \equiv 0 \bmod 2 \text{ or } (s_1 \equiv 1 \bmod 2,\ \varrho_1 u_3 - \varrho_3 u_1 \equiv 2^{m-2} \bmod 2^{m-1}),\\
&\varrho_2 \equiv 0 \bmod 2 \text{ or } (s_1 \equiv 1 \bmod 2,\ \varrho_2 u_3 - \varrho_3 u_2 \equiv 2^{m-2} \bmod 2^{m-1}),\\
&u_1 \equiv 0 \bmod 2 \text{ or } (s_1 \equiv 1 \bmod 2,\ \varrho_1 u_2 - \varrho_2 u_1 \equiv 2^{m-2} \bmod 2^{m-1}),\\
&u_3 \equiv 0 \bmod 2 \text{ or } (s_1 \equiv 1 \bmod 2,\ \varrho_2 u_3 - \varrho_3 u_2 \equiv 2^{m-2} \bmod 2^{m-1}).
\end{aligned}$$

Moreover, $m = 2$ if and only if $u_3 \equiv 1 \bmod 2$ if and only if $\varrho_2 \equiv 1 \bmod 2$.

P r o o f. (Sketch.) Recall that G' has the presentation given in Lemma 1 (vi) with $2 \leqslant m \leqslant n$.

Suppose $s_3 \equiv 1 \bmod 2$; then (II_2) or (II_4) imply that

$$s_3(\varrho_1 s_2 - \varrho_2 s_1) \equiv 2^{m-2} \bmod 2^{m-1} \quad \text{or} \quad s_2(\varrho_1 s_3 - \varrho_3 s_1) \equiv 0 \bmod 2^{m-1},$$

respectively. Subtracting these two congruences and using (II_6) yields

$$2^{m-2} \equiv s_1(\varrho_2 s_3 - \varrho_3 s_2) \equiv 0 \bmod 2^{m-1},$$

a contradiction. Thus, $s_3 \equiv 0 \bmod 2$.

Similar arguments, which are left to the reader, show that $\varrho_3 \equiv s_2 \equiv u_2 \equiv 0 \bmod 2$.

Now suppose that $\varrho_1 \equiv 1 \bmod 2$ and $s_1(\varrho_1 u_3 - \varrho_3 u_1) \equiv 0 \bmod 2^{m-1}$. Then by $(\mathrm{II}_{3,4})$ we have

$$\begin{aligned}
&\varrho_1(u_1 s_3 - u_3 s_1) \equiv 2^{m-2} \bmod 2^{m-1},\\
&u_1(\varrho_1 s_3 - \varrho_3 s_1) \equiv 0 \bmod 2^{m-1}.
\end{aligned}$$

Subtracting yields

$$2^{m-2} \equiv s_1(\varrho_1 u_3 - \varrho_3 u_1) \equiv 0 \bmod 2^{m-1},$$

a contradiction.

The rest can be treated in a (more or less) similar fashion, as the reader may verify.

The last statement of the proposition follows immediately from $(\mathrm{II}_{2,3})$. □

Next, assuming Condition $(\mathcal{C})$ again, notice that for any $j=1,2,3$, $[a_\lambda^2, a_j] \in G_3 \subseteq G_2^2$. Thus, we may write

$$[a_\lambda^2, a_j] = a^{2\alpha_{\lambda j}} b^{2\beta_{\lambda j}}$$

for some integers $\alpha_{\lambda j}$, $\beta_{\lambda j}$. Notice, too, that for $j = \lambda$, we have $\alpha_{\lambda\lambda} = \beta_{\lambda\lambda} = 0$, since the commutator is trivial in this case.

Moreover, since $a_\lambda^2 = a^{\mu_\lambda} b^{\nu_\lambda}$, we get

$$\begin{aligned}[a_\lambda^2, a_j] &= [a^{\mu_\lambda} b^{\nu_\lambda}, a_j] = [a, a_j]^{\mu_\lambda} [b, a_j]^{\nu_\lambda} \\ &= (a^{2r_j} b^{2s_j'})^{\mu_\lambda} (a^{2u_j} b^{2v_j})^{\nu_\lambda} = a^{2(r_j\mu_\lambda + u_j\nu_\lambda)} b^{2s_j'\mu_\lambda + v_j\nu_\lambda)}.\end{aligned}$$

(Recall once again that $s_j' = s_j 2^{n-m}$.) Hence, from the fact that the orders of a and b are 2^m and 2^{n+1}, respectively, the above yields:

(III(j)) $$r_j\mu_\lambda + u_j\nu_\lambda \equiv \alpha_{\lambda j} \bmod 2^{m-1}, \quad s_j'\mu_\lambda + v_j\nu_\lambda \equiv \beta_{\lambda j} \bmod 2^n.$$

Since by (3) and the fact that $G_3 \subseteq Z(G_2)$, we have $[a_\lambda^2, a_j] = c_{\lambda j}^2 c_{\lambda j\lambda}$, and writing the right-hand side in terms of a product of powers of a and b we obtain the following table of values of our α's and β's:

α/β	$\lambda = 1$	$\lambda = 2$	$\lambda = 3$
$\alpha_{\lambda 1}$	0	$-u_2$	$-(1+r_3) + u_3\delta$
$\beta_{\lambda 1}$	0	$-(1+v_2)$	$-s_3' + (1+v_3)\delta$
$\alpha_{\lambda 2}$	u_1	0	$-2((1+r_3)\mu_0 + u_3\nu_0)$
$\beta_{\lambda 2}$	$1+v_1$	0	$-2(s_3'\mu_0 + (1+v_3)\nu_0)$
$\alpha_{\lambda 3}$	$1 + r_1 - u_1\delta$	$2((1+r_2)\mu_0 + u_2\nu_0)$	0
$\beta_{\lambda 3}$	$s_1' - (1+v_1)\delta$	$2(s_2'\mu_0 + (1+v_2)\nu_0)$	0

For example, let's compute α_{31} and β_{31}. We have

$$a^{2\alpha_{31}} b^{2\beta_{31}} = [a_3^2, a_1] = c_{31}^2 c_{313}.$$

But $c_{31} = c_{13}^{-1} = a^{-1}b^{\delta}$ and (by Lemma 1) $c_{313} = c_{133}^{-1} = [c_{13}, a_3]^{-1} = [ab^{-\delta}, a_3]^{-1} = [a, a_3]^{-1}[b, a_3]^{\delta} = a^{-2r_3} b^{-2s_3'} a^{2u_3\delta} b^{2v_3\delta}$, and thus we get

$$c_{31}^2 c_{313} = a^{2(-1-r_3+u_3\delta)} b^{2(\delta - s_3' + v_3\delta)}.$$

Comparing exponents gives the two relevant entries in the table. The rest are left to the reader.

One last ingredient that we need for our proof is the following pair of congruences derived from the Witt Identity (refer to the proof of Lemma 1 (v)):

$$\text{(W)} \qquad \begin{aligned} r_2 &\equiv u_3 + 2r_1\mu_0 + 2u_1\nu_0 + u_2\delta \bmod 2^{m-1}, \\ s_2' &\equiv v_3 + 2s_1'\mu_0 + 2v_1\nu_0 + v_2\delta + 2^{n-1} \bmod 2^n. \end{aligned}$$

This follows from the observations that $[c_{12}, c_{13}] = b^{2^n}$ and that $[c_{12}, c_{13}] = c_{123}c_{231}c_{312}$, and then by rewriting the last product in terms of a and b and comparing exponents. Namely, we have

$$c_{123} = [b, a_3] = a^{2u_3}b^{2v_3}, \quad c_{231} = [a^{2\mu_0}b^{2\nu_0}, a_1] = a^{4(r_1\mu_0+u_1\nu_0)}b^{4(s_1'\mu_0+v_1\nu_0)},$$
$$c_{312} = c_{132}^{-1} = [ab^{-\delta}, a_2]^{-1} = a^{2(-r_2+u_2\delta)}b^{2(-s_2'+v_2\delta)}.$$

Multiplying these together and comparing it to b^{2^n} establishes (W). Notice that (W) along with Proposition 2 implies that

$$r_3 \equiv v_3 \equiv 0 \bmod 2.$$

We are now ready to prove that Condition ($\mathcal{C}$) is vacuous by considering $\lambda = 1, 2, 3$ separately.

Proposition 3. *There exists no group G satisfying Condition ($\mathcal{C}$) above with $\lambda = 1$.*

P r o o f. Assume $\lambda = 1$. Then (III(3)) implies that $s_1' \equiv 0 \bmod 2$ and $u_3\nu_1 \equiv 1 + r_1 \bmod 2$. Moreover, (III(2)) implies $v_2\nu_1 \equiv 1 + v_1 \bmod 2$ and $r_2\mu_1 \equiv u_1 \bmod 2$. Also, by (III(1)), $v_1\nu_1 \equiv 0 \bmod 2$.

Suppose $r_1 \equiv 0 \bmod 2$. Hence, $u_3\nu_1 \equiv 1 \bmod 2$ and so $u_3 \equiv 1, \nu_1 \equiv 1 \bmod 2$. Thus, $v_1 \equiv 0 \bmod 2$ and so $v_2 \equiv 1 \bmod 2$. Now (W) implies that $r_2 \equiv 1 \bmod 2$ and hence, $\varrho_2 \equiv 0 \bmod 2$. But Proposition 2 yields a contradiction.

Thus, we must have $r_1 \equiv 1 \bmod 2$. Hence, $u_3\nu_1 \equiv 0 \bmod 2$. First suppose $u_3 \equiv 1 \bmod 2$ and so $r_2 \equiv 1 \bmod 2$. Thus, $\nu_1 \equiv 0 \bmod 2$ and so $v_1 \equiv 1 \bmod 2$. This implies that $\varrho_1 \equiv 0 \bmod 2$. Proposition 2 then implies that $s_1 \equiv 1 \bmod 2$, $m = 2$, and $\varrho_2 \equiv 1 \bmod 2$; thus, $v_2 \equiv 0 \bmod 2$. By (I_2), $s_1 \equiv \nu_1 \equiv 0 \bmod 2$, a contradiction.

Therefore, $u_3 \equiv 0 \bmod 2$ and so $r_2 \equiv 0 \bmod 2$. Since by Proposition 2, $\varrho_2 \equiv 0 \bmod 2$, we have $v_2 \equiv 0 \bmod 2$. Thus, from above we have $u_1 \equiv 0 \bmod 2$, $r_1 \equiv v_1 \equiv 1 \bmod 2$, $\nu_1 \equiv 0 \bmod 2$. Now (II_2) then implies $m > 2$. By (I) we thus have $s_1 \equiv 0 \bmod 2^{m-1}$ and $u_1 \equiv 0 \bmod 2^{m-2}$. But then ($\mathrm{II}_3$) implies that $0 \equiv 2^{m-2} \bmod 2^{m-1}$, a contradiction. This establishes the proposition. □

Proposition 4. *There exists no group G satisfying Condition $(\mathcal{C})$ above with $\lambda = 2$.*

P r o o f. In order to take advantage of the congruences (I), we first show that r_2 and v_2 are both even. We consider an argument depending on the parity of ν_2.

First suppose $\nu_2 \equiv 1 \bmod 2$. Then (III(3)) implies that $u_3 \equiv 0 \bmod 2$ and so by (W), $r_2 \equiv 0 \bmod 2$. But then (III(2)) implies that $v_2 \equiv 0 \bmod 2$.

Next suppose $\nu_2 \equiv 0 \bmod 2$. Assume for the sake of argument that $v_2 \equiv 1 \bmod 2$. Then by Proposition 2, (II_2), and (W), we see that r_2 must be odd and thus $\varrho_2 \equiv 0 \bmod 2$. But (W) then implies $u_3 \equiv 1 \bmod 2$, contradicting Proposition 2. Therefore, $v_2 \equiv 0 \bmod 2$. Now (III(1)) then implies that in particular $\mu_2 \equiv 1 \bmod 2$. Hence by (III(2)) we see that $r_2 \equiv 0 \bmod 2$.

Thus, we have shown that $r_2 \equiv v_2 \equiv 0 \bmod 2$. In particular (III(1)) gives us $(\mu_2, \nu_2) \not\equiv (0,0) \bmod 2$. Moreover, by (I) we have

$$\begin{aligned} s_2 &\equiv 2^{m-2}\nu_2 \bmod 2^{m-1}, \quad \text{or equivalently} \quad s_2' \equiv 2^{n-2}\nu_2 \bmod 2^{n-1}, \\ v_2 &\equiv 2^{n-2}\mu_2 \bmod 2^{n-1}, \quad u_2 \equiv 0 \bmod 2^{m-2}, \quad r_2 \equiv 0 \bmod 2^{m-2}. \end{aligned}$$

Next, we show that μ_2 must be even. Notice that (II_3) implies that

$$u_1 s_3' \mu_2 - u_3 s_1' \mu_2 \equiv 2^{n-2}\mu_2 \bmod 2^{n-1}.$$

We will be done if we can show the left-hand side $\equiv 0 \bmod 2^{n-1}$. By (III(3))

$$u_1 s_3' \mu_2 \equiv -u_1 v_3 \nu_2 + 2u_1\nu_0 \bmod 2^{n-1}.$$

By (W) (looking modulo 2^{n-1}), we have

$$\begin{aligned} -u_1 v_3 \nu_2 &\equiv -u_1 s_2' \nu_2 + 2s_1' u_1 \mu_0 \nu_2 + 2v_1 u_1 \nu_0 \nu_2 \bmod 2^{n-1}, \\ -u_3 s_1' \mu_2 &\equiv -r_2 s_1' \mu_2 + 2r_1 \mu_0 s_1' \mu_2 + 2u_1 \nu_0 s_1' \mu_2 \bmod 2^{n-1}. \end{aligned}$$

Thus, we have

$$\begin{aligned} u_1 s_3' \mu_2 - u_3 s_1' \mu_2 \equiv\ & - u_1 s_2' \nu_2 + 2s_1' u_1 \mu_0 \nu_2 + 2v_1 u_1 \nu_0 \nu_2 + 2u_1 \nu_0 \\ & - r_2 s_1' \mu_2 + 2r_1 \mu_0 s_1' \mu_2 + 2u_1 \nu_0 s_1' \mu_2 \bmod 2^{n-1}. \end{aligned}$$

By (III(1)) we have

$$\begin{aligned} 2s_1'\mu_0(u_1\nu_2 + r_1\mu_2) &\equiv -2s_1' u_2 \mu_0 \equiv 0 \bmod 2^{n-1}, \\ 2u_1\nu_0(v_1\nu_2 + s_1'\mu_2) &\equiv -2u_1\nu_0(1+v_2) \equiv -2u_1\nu_0 \bmod 2^{n-1}. \end{aligned}$$

Hence,

$$u_1 s_3' \mu_2 - u_3 s_1' \mu_2 \equiv -u_1 s_2' \nu_2 - r_2 s_1' \mu_2 \bmod 2^{n-1}.$$

Finally, by applying (II_1) and (III(2)) to the right-hand side, we get

$$u_1 s_3' \mu_2 - u_3 s_1' \mu_2 \equiv -s_1'(u_2\nu_2 + r_2\mu_2) \equiv 0 \bmod 2^{n-1},$$

as desired. Therefore, $\mu_2 \equiv 0 \bmod 2$.

Hence, the proof of the proposition is reduced to the case $(\mu_2, \nu_2) \equiv (0, 1) \bmod 2$. By (I) we thus have

$$s_2' \equiv 2^{n-2} \bmod 2^{n-1}, \quad v_2 \equiv 0 \bmod 2^{n-1}, \quad r_2 \equiv 0 \bmod 2^{m-2}.$$

Then (III(2)) implies that

$$u_2 \equiv 0 \bmod 2^{m-1}.$$

By (III(1)),

$$u_1 \equiv 0, \quad v_1 \equiv 1 \bmod 2.$$

(III(3)) implies that

$$u_3 \equiv 0 \bmod 2.$$

Therefore, by (II_3) we see that $m \geqslant 3$.

Next notice that (II_3) implies that

$$u_1 s_3' \nu_2 - u_3 s_1' \nu_2 \equiv 2^{n-2} \bmod 2^{n-1}.$$

We complete the proof by showing that the left-hand side is $\equiv 0 \bmod 2^{n-1}$. By (III(1)) and the fact that $s_3' \equiv 0 \bmod 2^{n-m+1}$ by Proposition 2, we have

$$u_1 \nu_2 s_3' \equiv -r_1 s_3' \mu_2 \bmod 2^{n-1}.$$

(III(3)) implies

$$-r_1 s_3' \mu_2 \equiv r_1 v_3 \nu_2 - 2 r_1 \nu_0 \bmod 2^{n-1}.$$

By (W)

$$r_1 v_3 \nu_2 \equiv r_1 s_2' \nu_2 - 2 s_1' r_1 \mu_0 \nu_2 - 2 v_1 r_1 \nu_0 \nu_2 \bmod 2^{n-1}.$$

By (III(1))

$$-2 r_1 \nu_0 v_1 \nu_2 \equiv 2 r_1 \nu_0 s_1' \mu_2 + 2 r_1 \nu_0 \bmod 2^{n-1},$$

implying that

$$u_1 s_3' \nu_2 \equiv r_1 s_2' \nu_2 - 2 s_1' r_1 \mu_0 \nu_2 + 2 r_1 \nu_0 s_1' \mu_2 \bmod 2^{n-1}.$$

By (W) we have

$$-u_3 s_1' \nu_2 \equiv -r_2 s_1' \nu_2 + 2 r_1 s_1' \mu_0 \nu_2 + 2 u_1 s_1' \nu_0 \nu_2 \bmod 2^{n-1}$$

and therefore,

$$u_1 s_3' \nu_2 - u_3 s_1' \nu_2 \equiv r_1 s_2' \nu_2 - r_2 s_1' \nu_2 + 2 s_1' \nu_0 r_1 \mu_2 + 2 s_1' \nu_0 u_1 \nu_2 \bmod 2^{n-1}.$$

But (III(1)) implies that

$$2s_1'\nu_0(r_1\mu_2 + u_1\nu_2) \equiv 0 \bmod 2^{n-1}$$

and thus,

$$u_1s_3'\nu_2 - u_3s_1'\nu_2 \equiv (r_1s_2' - r_2s_1')\nu_2 \bmod 2^{n-1}.$$

Now, by (II_2) we have

$$\varrho_2s_1' - \varrho_1s_2' \equiv 2^{n-2} \bmod 2^{n-1}.$$

But since $v_2 \equiv 0, s_2' \equiv 2^{n-2} \bmod 2^{n-1}$ as above, we see that

$$\varrho_2s_1' - \varrho_1s_2' \equiv (r_1s_2' - r_2s_1') + 2^{n-2} \bmod 2^{n-1},$$

which implies that

$$(r_1s_2' - r_2s_1')\nu_2 \equiv 0 \bmod 2^{n-1}.$$

This yields the desired contradiction and thus the proof of the proposition is established. □

We are now left with the case where $\lambda = 3$, which is a little more involved. We first start with a lemma.

Lemma 5. *Let G satisfy Condition $(\mathcal{C})$ above with $\lambda = 3$. Then the following congruences hold:*

$$(\varrho_1s_2' - \varrho_2s_1')\nu_3 \equiv (u_3s_1' - v_3r_1)\nu_3 \bmod 2^{n-1},$$
$$(u_1s_2' - u_2s_1')\nu_3 \equiv u_1v_3\nu_3 + u_3s_1'\mu_3 \bmod 2^{n-1}.$$

P r o o f. By Proposition 2 and (W), we have $r_3 \equiv v_3 \equiv 0 \bmod 2$ and thus, (I) yields

$$s_3' \equiv 2^{n-2}\nu_3 \bmod 2^{n-1}, \quad v_3 \equiv 2^{n-2}\mu_3 \bmod 2^{n-1}, \quad u_3 \equiv r_3 \equiv 0 \bmod 2^{m-2}.$$

We first consider $(\varrho_1s_2' - \varrho_2s_1')\nu_3$. Since $\varrho_2 = v_2 - r_2$, we have

$$-\varrho_2s_1'\nu_3 = -v_2\nu_3s_1' + r_2\nu_3s_1'.$$

(III(2)) implies that

$$-v_2\nu_3 \equiv s_2'\mu_3 + 2\nu_0 \bmod 2^{n-1}.$$

Now by (W)

$$-v_2\nu_3 \equiv v_3\mu_3 + 2s_1'\mu_0\mu_3 + 2v_1\nu_0\mu_3 + v_2\mu_3\delta + 2\nu_0 \bmod 2^{n-1},$$
$$r_2\nu_3 \equiv u_3\nu_3 + 2r_1\mu_0\nu_3 + 2u_1\nu_0\nu_3 + u_2\nu_3\delta \bmod 2^{m-1}.$$

(III(1)) implies that

$$2\mu_0 s_1'\mu_3 \equiv -2\mu_0 v_1\nu_3 + 2\mu_0\delta \bmod 2^{n-1}, \quad 2\nu_0 u_1\nu_3 \equiv -2\nu_0 r_1\mu_3 - 2\nu_0 \bmod 2^{m-1}.$$

Hence,

$$\begin{aligned}-\varrho_2 s_1'\nu_3 \equiv{}& v_3\mu_3 s_1' + u_3\nu_3 s_1' - 2\mu_0 v_1\nu_3 s_1' + 2v_1\nu_0\mu_3 s_1' + 2\mu_0 r_1\nu_3 s_1' - 2\nu_0 r_1\mu_3 s_1' \\ &+ (v_2\mu_3 s_1' + u_2\nu_3 s_1' + 2\mu_0 s_1')\delta \bmod 2^{n-1}.\end{aligned}$$

On the other hand, by (W) we have

$$\varrho_1 s_2'\nu_3 \equiv v_3\varrho_1\nu_3 + 2s_1'\mu_0\varrho_1\nu_3 + 2v_1\nu_0\varrho_1\nu_3 + v_2\varrho_1\nu_3\delta \bmod 2^{n-1}.$$

Therefore, we get

$$\begin{aligned}(\varrho_1 s_2' - \varrho_2 s_1')\nu_3 \equiv{}& v_3\mu_3 s_1' + u_3\nu_3 s_1' + v_3\varrho_1\nu_3 + 2v_1\nu_0\mu_3 s_1' - 2\nu_0 r_1\mu_3 s_1' + 2v_1\nu_0\varrho_1\nu_3 \\ &+ (v_2\mu_3 s_1' + u_2\nu_3 s_1' + 2\mu_0 s_1' + v_2\varrho_1\nu_3)\delta \bmod 2^{n-1}.\end{aligned}$$

Now, by (III(1)) we have

$$\begin{aligned}2v_1\nu_0 s_1'\mu_3 &\equiv -2v_1\nu_0 v_1\nu_3 + 2v_1\nu_0\delta \bmod 2^{n-1}, \\ -2r_1\nu_0(s_1'\mu_3 + v_1\nu_3) &\equiv -2r_1\nu_0\delta \bmod 2^{n-1}, \\ v_2 s_1'\mu_3 + v_2 v_1\nu_3 &\equiv -s_3' v_2 + v_2\delta \bmod 2^{n-1},\end{aligned}$$

and (III(2)) implies

$$-r_1 v_2\nu_3 \equiv r_1 s_2'\mu_3 + 2r_1\nu_0 \bmod 2^{n-1}.$$

These along with (II_1) yield

$$\begin{aligned}(\varrho_1 s_2' - \varrho_2 s_1')\nu_3 \equiv{}& v_3\mu_3 s_1' + u_3\nu_3 s_1' + v_3\varrho_1\nu_3 \\ &+ (2v_1\nu_0 + 2\mu_0 s_1' - s_3' v_2 + v_2\delta + u_1 s_2'\nu_3 + r_1\mu_3 s_2')\delta \bmod 2^{n-1}.\end{aligned}$$

By (III(1))

$$u_1 s_2'\nu_3 + r_1\mu_3 s_2' \equiv -s_2' \bmod 2^{n-1}$$

and then by (W) we obtain

$$(\varrho_1 s_2' - \varrho_2 s_1')\nu_3 \equiv v_3\mu_3 s_1' + u_3\nu_3 s_1' + v_3 v_1\nu_3 - v_3 r_1\nu_3 - (v_3 + s_3' v_2)\delta \bmod 2^{n-1}.$$

Since δ is even and by the congruence relations on v_3 and s_3' above, we see that $(v_3 + s_3' v_2)\delta \equiv 0 \bmod 2^{n-1}$, and thus by (III(1)) (since $v_3(s_1'\mu_3 + v_1\nu_3) \equiv 0 \bmod 2^{n-1}$) we have

$$(\varrho_1 s_2' - \varrho_2 s_1')\nu_3 \equiv (u_3 s_1' - v_3 r_1)\nu_3 \bmod 2^{n-1},$$

as desired.

For the second congruence, first notice by (W) that

$$u_1 s_2' \nu_3 \equiv u_1 v_3 \nu_3 + 2u_1 s_1' \mu_0 \nu_3 + 2u_1 v_1 \nu_0 \nu_3 + u_1 v_2 \nu_3 \delta \bmod 2^{n-1}.$$

By (III(2)) and the congruences above,

$$-u_2 \nu_3 s_1' \equiv r_2 \mu_3 s_1' + 2\mu_0 s_1' \bmod 2^{n-1},$$

and by (W)

$$r_2 \mu_3 s_1' \equiv u_3 \mu_3 s_1' + 2r_1 \mu_3 \mu_0 s_1' + 2u_1 \nu_0 \mu_3 s_1' + u_2 \mu_3 s_1' \delta \bmod 2^{n-1},$$

which imply that

$$\begin{aligned} u_1 s_2' \nu_3 - u_2 s_1' \nu_3 \equiv u_1 v_3 \nu_3 + u_3 \mu_3 s_1' + 2u_1 s_1' \mu_0 \nu_3 + 2u_1 v_1 \nu_0 \nu_3 + 2r_1 \mu_0 \mu_3 s_1' \\ + 2u_1 \nu_0 \mu_3 s_1' + 2\mu_0 s_1' + (u_1 v_2 \nu_3 + u_2 \mu_3 s_1')\delta \bmod 2^{n-1}. \end{aligned}$$

(III(1)) (along with the congruences above) then implies that

$$2s_1' \mu_0 (u_1 \nu_3 + r_1 \mu_3) \equiv -2s_1' \mu_0 \bmod 2^{n-1}, \quad 2u_1 \nu_0 (v_1 \nu_3 + s_1' \mu_3) \equiv 2u_1 \nu_0 \delta \bmod 2^{n-1},$$

and thus,

$$u_1 s_2' \nu_3 - u_2 s_1' \nu_3 \equiv u_1 v_3 \nu_3 + u_3 s_1' \mu_3 + (2u_1 \nu_0 + u_1 v_2 \nu_3 + u_2 s_1' \mu_3)\delta \bmod 2^{n-1}.$$

By (II_1)

$$u_2 s_1' \mu_3 \equiv u_1 s_2' \mu_3 \bmod 2^{n-1},$$

and so

$$u_1 s_2' \nu_3 - u_2 s_1' \nu_3 \equiv u_1 v_3 \nu_3 + u_3 s_1' \mu_3 + u_1 (2\nu_0 + v_2 \nu_3 + s_2' \mu_3)\delta \bmod 2^{n-1}.$$

But by (III(2)) we have $2\nu_0 + v_2 \nu_3 + s_2' \mu_3 \equiv 0 \bmod 2^{n-1}$, and therefore,

$$(u_1 s_2' - u_2 s_1')\nu_3 \equiv u_1 v_3 \nu_3 + u_3 s_1' \mu_3 \bmod 2^{n-1},$$

as desired. □

With this result, we can finally prove the following proposition.

Proposition 5. *There exists no group G satisfying Condition $(\mathcal{C})$ above with $\lambda = 3$.*

P r o o f. By looking at (III(1)) modulo 2, we have $(\mu_3, \nu_3) \not\equiv (0,0) \bmod 2$. First suppose $(\mu_3, \nu_3) \equiv (0,1) \bmod 2$. By (II_2) we have

$$(\varrho_1 s_2' - \varrho_2 s_1')\nu_3 \equiv 2^{n-2} \bmod 2^{n-1}.$$

Now Lemma 5 implies that

$$(\varrho_1 s_2' - \varrho_2 s_1')\nu_3 \equiv (u_3 s_1' - v_3 r_1)\nu_3 \bmod 2^{n-1}.$$

By (I) we see that $v_3 \equiv 0 \bmod 2^{n-1}$ and $s_3 \equiv 2^{m-2} \bmod 2^{m-1}$. (III(1)) implies that $u_1 \equiv 1 \bmod 2$ and hence, Proposition 2 yields $s_1 \equiv 1 \bmod 2$. Thus, by (II_3), $u_3 \equiv 0 \bmod 2^{m-1}$. Therefore,

$$(u_3 s_1' - v_3 r_1)\nu_3 \equiv 0 \bmod 2^{n-1}.$$

This is the desired contradiction in this case.

By (II_1) and Lemma 5 we have

$$0 \equiv (u_1 s_2' - u_2 s_1')\nu_3 \equiv u_1 v_3 \nu_3 + u_3 s_1' \mu_3 \bmod 2^{n-1}.$$

For $\mu_3 \equiv 1 \bmod 2$, we show that the right-hand side $\equiv 2^{n-2} \bmod 2^{n-1}$, giving us the desired contradiction.

Assume that $(\mu_3, \nu_3) \equiv (1,0) \bmod 2$. Hence, by (I), $v_3\nu_3 \equiv 0 \bmod 2^{n-1}$. Also by (I), $s_3 \equiv 0 \bmod 2^{m-1}$, and thus by (II_3) we have $u_3 s_1 \equiv 2^{m-2} \bmod 2^{m-1}$. Therefore, again by (I), $s_1 \equiv 1 \bmod 2$ and $u_3 \equiv 2^{m-2} \bmod 2^{m-1}$. Hence,

$$u_1 v_3 \nu_3 + u_3 s_1' \mu_3 \equiv 2^{n-2} \bmod 2^{n-1},$$

as we wanted.

Finally, assume $(\mu_3, \nu_3) \equiv (1,1) \bmod 2$. First suppose $u_3 \equiv 0 \bmod 2^{m-1}$. Then (II_3) implies that $u_1 \equiv 1 \bmod 2$ and since by (I) $v_3 \equiv 2^{n-2} \bmod 2^{n-1}$, we have

$$u_1 v_3 \nu_3 + u_3 s_1' \mu_3 \equiv 2^{n-2} \bmod 2^{n-1},$$

giving the desired contradiction. Now suppose $u_3 \equiv 2^{m-2} \bmod 2^{m-1}$. Hence, (II_3) implies $u_1 \not\equiv s_1 \bmod 2$. But then Proposition 2 implies that $u_1 \equiv 0 \bmod 2$ and so $s_1 \equiv 1 \bmod 2$. Thus, $u_1 v_3 \equiv 0 \bmod 2^{n-1}$. Once again we have

$$u_1 v_3 \nu_3 + u_3 s_1' \mu_3 \equiv 2^{n-2} \bmod 2^{n-1},$$

which completes the proof of the proposition. □

Summarizing, we have proved the first part of the Main Theorem:

Theorem 2. *Let G be a finite 2-group such that* 4-rank$(G/G') \leqslant 2$ *and* rank$(G') = 2$. *Then G is metabelian.*

4. The minimal order of a nonmetabelian 2-group with a commutator subgroup of rank 2

In this section we exhibit a nonmetabelian 2-group G of order 2^{12} with a commutator subgroup G' generated by two elements. We then show, by proving the second part of our Main Theorem, that this is the minimal order of any 2-group with nonabelian commutator subgroup of rank 2.

Example 1. Let $G = \langle a_1, a_2, a_3 \rangle$ such that

$$a_1^8 = 1, \quad a_2^4 = c_{12}^2, \quad a_3^4 = 1, \quad c_{12}^8 = c_{13}^4 = c_{23} = 1,$$
$$c_{121} = c_{12}^2, \quad c_{122} = 1, \quad c_{123} = c_{12}^4 c_{13}^2, \quad c_{131} = c_{12}^2, \quad c_{132} = c_{13}^2, \quad c_{133} = 1.$$

Then, as verified by Magma, $G/G' \simeq (8,4,4)$, $G'/G'' \simeq (4,4)$, and $G'' \simeq (2)$; therefore, the derived length of G is 3 and $|G| = 2^{12}$.

Now we wish to show that any 2-group of order $\leqslant 2^{11}$ with commutator subgroup of rank 2 is metabelian. Toward this end, let G be a finite 2-group with nonabelian commutator subgroup of rank 2. By Theorem 2 (and Theorems 1 and 4 in [2]), $|G| \geqslant 2^{11}$ and moreover the only possibility of such a group G of order 2^{11} is one satisfying the following properties:

$$G/G' \simeq (4,4,4), \quad G'/G'' \simeq (4,4), \quad G'' \simeq (2).$$

We show that any group satisfying these properties does not exist by proving the second part of the Main Theorem (where we assume that 8-rank$(G/G') = 0$). We now proceed to prove this result.

First, by Proposition 1 we may assume that G has rank 3.

For convenience we gather some of our assumptions in one place in the following hypothesis:

($\mathcal{H}$) Assume that G is a finite 2-group, m, n are integers such that $2 \leqslant m \leqslant n$, and that $G' = \langle a, b \rangle$ is presented as

$$a^{2^m} = b^{2^{n+1}} = 1, \quad [a,b] = b^{2^n}.$$

Before stating the next results, we introduce some notation. If x, y are elements of a multiplicative group and α, β are integers, then define the inner product exponentially as

$$(x,y) * (\alpha,\beta)^t = x^\alpha y^\beta,$$

where t indicates the transpose. Moreover, if M is any 2×2 matrix with integer entries, then $(x,y) * M$ is defined using the above exponential inner product:

$$(x,y) * \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (x^\alpha y^\gamma, x^\beta y^\delta).$$

In terms of our 2-group G above, the following properties are satisfied by the operation $*$.

Lemma 6. *Let G satisfy Hypothesis ($\mathcal{H}$) above. Suppose $w = (x, y) \in G' \times G'$, where the group operation is defined componentwise.*

(i) *Let A and B be either both 2×2 or both 2×1 matrices with integral entries. If at least one of A and B has all entries even, then*

$$w * (A + B) = (w * A)(w * B).$$

(ii) *Let A be a 2×2 matrix with even integer entries and let B be either a 2×2 or a 2×1 matrix with arbitrary integer entries. Then*

$$w * AB = (w * A) * B.$$

P r o o f. (Sketch.) Let $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{smallmatrix}\right)$ with arbitrary integer entries. Then we have

$$w * (A + B) = (x^{\alpha+\alpha'} y^{\gamma+\gamma'}, x^{\beta+\beta'} y^{\delta+\delta'})$$

and on the other hand

$$(w * A)(w * B) = (x^{\alpha} y^{\gamma} x^{\alpha'} y^{\gamma'}, x^{\beta} y^{\delta} x^{\beta'} y^{\delta'}).$$

If all the entries in at least one of A or B are even, then these two expressions are equal since Hypothesis ($\mathcal{H}$) implies that $G_2^2 = Z(G_2)$. A similar argument works if A and B are 2×1 matrices. This establishes (i).

With respect to (ii), let A and B be as above. Then

$$w * (AB) = (x^{\alpha\alpha'+\beta\gamma'} y^{\gamma\alpha'+\delta\gamma'}, x^{\alpha\beta'+\beta\delta'} y^{\gamma\beta'+\delta\delta'})$$

and on the other hand

$$(w * A) * B = ((x^{\alpha} y^{\gamma})^{\alpha'} (x^{\beta} y^{\delta})^{\gamma'}, (x^{\alpha} y^{\gamma})^{\beta'} (x^{\beta} y^{\delta})^{\delta'}).$$

If all the entries in A are even, then the two expressions are equal, since again $G_2^2 = Z(G_2)$. The argument is similar when B is a 2×1 matrix. Hence (ii) is established. □

Proposition 6. *Let G satisfy Hypothesis ($\mathcal{H}$) above. By Lemma 3 for $x \in G$ there is a 2×2 matrix $A = \left(\begin{smallmatrix} 2r & 2u \\ 2s' & 2v \end{smallmatrix}\right)$ with integers r, s, u, v, and $s' = 2^{n-m}s$ such that $([a, x], [b, x]) = (a, b) * A$. Then the following are valid:*

(i) *If* $(c,d) = (a,b) * B$, *where* B *is a* 2×2 *matrix with integer entries, then*

$$([c,x],[d,x]) = (a,b) * (AB).$$

(ii) *For any integer* $\kappa \geqslant 0$,

$$([a,x^\kappa],[b,x^\kappa]) = (a,b) * \big((I+A)^\kappa - I\big),$$

where I *is the* 2×2 *identity matrix.*

P r o o f. To prove (i), let $(c,d) = (a,b) * B$, where $B = \left(\begin{smallmatrix} h & i \\ j & k \end{smallmatrix}\right)$. Hence, $(c,d) = (a^h b^j, a^i b^k)$. But then

$$\begin{aligned}([c,x],[d,x]) &= ([a,x]^h[b,x]^j,[a,x]^i[b,x]^k) = ([a,x],[b,x]) * B \\ &= ((a,b) * A) * B = (a,b) * (AB)\end{aligned}$$

by Lemma 6.

With respect to (ii), we use induction on κ. The result is certainly true for $\kappa = 0$ and 1. So now suppose that for some $\kappa \geqslant 1$, we have

$$([a,x^\kappa],[b,x^\kappa]) = (a,b) * ((I+A)^\kappa - I).$$

We then show that

$$([a,x^{\kappa+1}],[b,x^{\kappa+1}]) = (a,b) * ((I+A)^{\kappa+1} - I).$$

First notice that

$$(I+A)^{\kappa+1} - I = (I+A)^\kappa - I + A\big((I+A)^\kappa - I\big) + A.$$

Hence,

$$\begin{aligned}(a,b) * \big((I+A)^{\kappa+1} - I\big) &= (a,b) * ((I+A)^\kappa - I + A((I+A)^\kappa - I) + A) \\ &= (a,b) * ((I+A)^\kappa - I)(a,b) * A((I+A)^\kappa - I)(a,b) * A\end{aligned}$$

by Lemma 6. Now by the induction hypothesis

$$([a,x^\kappa],[b,x^\kappa]) = (a,b) * \big((I+A)^\kappa - I\big)$$

and

$$(a,b) * A((I+A)^\kappa - I) = ([a,x^\kappa,x],[b,x^\kappa,x])$$

by (i) above. Hence,

$$\begin{aligned}(a,b) * ((I+A)^{\kappa+1} - I) &= ([a,x^\kappa][a,x^\kappa,x][a,x],[b,x^\kappa][b,x^\kappa,x][b,x]) \\ &= ([a,x^{\kappa+1}],[b,x^{\kappa+1}])\end{aligned}$$

by (3). □

Corollary 1. *Let G satisfy Hypothesis $(\mathcal{H})$ above and suppose $x \in G$ such that $x^4 \in G'$, say $x^4 = a^\mu b^\nu$. Let $([a,x],[b,x]) = (a,b) * A$ with $A = \left(\begin{smallmatrix} 2r & 2u \\ 2s' & 2v \end{smallmatrix}\right)$, as described in Proposition 6. Then*

$$([a,x^4],[b,x^4]) = (a,b) * ((I+A)^4 - I) = (b^{2^n\nu}, b^{2^n\mu}).$$

Equivalently, let

$$((I+A)^4 - I) = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix},$$

then

$$\begin{aligned} \alpha_{11} &\equiv 0 \bmod 2^m, & \alpha_{12} &\equiv 0 \bmod 2^m, \\ \alpha_{21} &\equiv 2^n\nu \bmod 2^{n+1}, & \alpha_{22} &\equiv 2^n\mu \bmod 2^{n+1}. \end{aligned}$$

Moreover,

$$\begin{aligned} \alpha_{11} &= 8(r(r+1)(1+2r(r+1)) + s'u(1+2(v+1)^2 + 2r(3r+4) + 4rv) + 2s'^2u^2), \\ \alpha_{22} &= 8(v(v+1)(1+2v(v+1)) + s'u(1+2(r+1)^2 + 2v(3v+4) + 4rv) + 2s'^2u^2) \end{aligned}$$

and

$$\alpha_{12} = \eta u, \quad \alpha_{21} = \eta s',$$

where

$$\eta = 8(1 + 3(r+v) + 4(r^2+v^2) + 2(r^3+v^3) + 2rv(2+r+v) + 4s'u(1+r+v)).$$

We leave the details to the reader, except to observe that, for example, the commutator $[a,x^4] = [a,a^\mu b^\nu] = [a,b]^\nu = b^{2^n\nu}$ etc. Also, the expressions for α_{ij} are found by direct computation.

Proposition 7. *Let G satisfy Hypothesis $(\mathcal{H})$ and suppose $x, y \in G$ and $[x,y] = a^\alpha b^\beta$ with integers α, β such that $\alpha\beta \equiv 0 \bmod 2$. Let A be as in Proposition 6 so that $([a,x],[b,x]) = (a,b) * A$. Then for all integers $\kappa \geqslant 0$,*

$$[x^{2^\kappa}, y] = (a,b) * C(\kappa) \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

where (formally)

$$C(\kappa) = ((I+A)^{2^\kappa} - I)A^{-1}.$$

P r o o f. The result is trivial for $\kappa = 0$. For $\kappa \geqslant 1$, the proposition will be established by proving the following statement by induction on κ: for any $\kappa \geqslant 1$ for all $x, y \in G$ and all integers α, β with $\alpha\beta \equiv 0 \bmod 2$,

$$[x^{2^\kappa}, y] = (a,b) * C(\kappa) \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

We first show the statement is true for $\kappa = 1$. By (3) and the fact that $G_3 \subseteq Z(G_2)$,

$$\begin{aligned}[x^2, y] &= [x, y]^2 [x, y, x] = (a^\alpha b^\beta)^2 [a^\alpha b^\beta, x] = a^{2\alpha} b^{2\beta} [b, a]^{\alpha\beta} [a, x]^\alpha [b, x]^\beta \\ &= (a, b) * (2I + A) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} [a, b]^{-\alpha\beta} = (a, b) * C(1) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} [a, b]^{-\alpha\beta} \\ &= (a, b) * C(1) \begin{pmatrix} \alpha \\ \beta \end{pmatrix},\end{aligned}$$

since $\alpha\beta$ is even and $[a, b]$ has order 2. Thus, the proposition holds for $\kappa = 1$.

Suppose the statement is true for some $\kappa \geqslant 1$. We then show

$$[x^{2^{\kappa+1}}, y] = (a, b) * C(\kappa + 1) \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

On one hand,

$$[x^{2^{\kappa+1}}, y] = [(x^{2^\kappa})^2, y] = [x^{2^\kappa}, y]^2 [x^{2^\kappa}, y, x^{2^\kappa}].$$

By the induction hypothesis and Lemma 6,

$$[x^{2^\kappa}, y]^2 = (a, b) * 2C(\kappa) \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Also by Proposition 6 we have

$$[x^{2^\kappa}, y, x] = (a, b) * AC(\kappa) \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

or equivalently

$$[x, [x^{2^\kappa}, y]] = (a, b) * \left(-AC(\kappa) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right).$$

Hence, by the induction hypothesis

$$[x^{2^\kappa}, [x^{2^\kappa}, y]] = (a, b) * \left(-AC(\kappa)^2 \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right)$$

or equivalently

$$[x^{2^\kappa}, y, x^{2^\kappa}] = (a, b) * AC(\kappa)^2 \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Hence,

$$[x^{2^{\kappa+1}}, y] = (a, b) * (2C(\kappa) + AC(\kappa)^2) \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

On the other hand, a straightforward argument shows that

$$C(\kappa + 1) = 2C(\kappa) + AC(\kappa)^2.$$

All this establishes the proposition. □

We will only need the following special case.

Corollary 2. *Assume all the conditions in Proposition 7. In addition suppose* $x^4 = a^\mu b^\nu$. *Let* A^* *be the matrix with even integral entries such that* $([a,y],[b,y]) = (a,b) * A^*$. *Then*

$$(a,b) * C(2) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = (a,b) * A^* \begin{pmatrix} \mu \\ \nu \end{pmatrix},$$

where $C(2) = \big((I+A)^4 - I\big)A^{-1} = 4I + 6A + 4A^2 + A^3$.

Equivalently, let

$$A = 2\begin{pmatrix} r & u \\ s' & v \end{pmatrix}, \quad A^* = 2\begin{pmatrix} r^* & u^* \\ s^{*\prime} & v^* \end{pmatrix}, \quad C(2) = \begin{pmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{pmatrix},$$

where the entries of A^* *are defined analogously to those of* A. *Then*

$$2(r^*\mu + u^*\nu) \equiv \gamma_{11}\alpha + \gamma_{12}\beta \bmod 2^m, \quad 2(s^{*\prime}\mu + v^*\nu) \equiv \gamma_{21}\alpha + \gamma_{22}\beta \bmod 2^{n+1},$$

and

$$\gamma_{11} = 4((1+r)(1+2r(1+r)) + 2s'u(2+v+2r)),$$
$$\gamma_{22} = 4((1+v)(1+2v(1+v)) + 2s'u(2+r+2v)),$$
$$\gamma_{12} = \tau u, \quad \gamma_{21} = \tau s',$$

where

$$\tau = 4\big(3 + 4(r+v) + 2(r^2+v^2) + 2rv + 2s'u\big).$$

Now we are ready to prove the second part of our Main Theorem.

Theorem 3. *There are no finite* 2*-groups* G *with* $8\text{-rank}(G/G') = 0$ *such that* G' *is nonabelian of rank* 2.

This theorem will follow from the results below.

First notice that by Theorem 2, Proposition 1, and Lemmas 1 and 2 (i), we need only show the nonexistence of groups G satisfying the following assumptions:

($\mathcal{A}1$) $G/G' \simeq (4,4,4)$;

($\mathcal{A}2$) $G = \langle a_1, a_2, a_3\rangle$ with $a_i^4 = a^{\mu_i} b^{\nu_i}$ for some $\mu_i, \nu_i \in \mathbb{Z}$, $i = 1,2,3$;

($\mathcal{A}3$) $G' = \langle a, b\rangle$ with presentation $a^{2^m} = b^{2^{n+1}} = 1$, $b^{2^n} = [a,b]$, where $2 \leqslant m \leqslant n$;

($\mathcal{A}4$) $c_{12} = b$, $c_{13} = ab^{-\delta}$, $c_{23} = a^{2\mu_0} b^{2\nu_0}$ for some integers δ, μ_0, ν_0 with δ even.

Now let G satisfy Assumptions ($\mathcal{A}1$)–($\mathcal{A}4$) and define the matrices A_i by

$$([a,a_i],[b,a_i]) = (a,b) * A_i, \quad \text{where } A_i = 2\begin{pmatrix} r_i & u_i \\ s_i' & v_i \end{pmatrix},$$

and where $s_i' = 2^{n-m} s_i$.

Then Corollary 1 takes the following form ($i = 1, 2, 3$):

$$\begin{aligned}(\mathrm{C}(i)) \qquad & \alpha_{11}(i) \equiv 0 \bmod 2^m, \qquad \alpha_{12}(i) \equiv 0 \bmod 2^m, \\ & \alpha_{21}(i) \equiv 2^n \nu_i \bmod 2^{n+1}, \quad \alpha_{22}(i) \equiv 2^n \mu_i \bmod 2^{n+1},\end{aligned}$$

where

$$\alpha_{11}(i) = f_i(r_i, v_i), \quad \alpha_{12}(i) = \eta(i) u_i, \quad \alpha_{21}(i) = \eta(i) s_i', \quad \alpha_{22}(i) = f_i(v_i, r_i),$$

such that

$$f_i(x,y) = 8(x(1+x)(1+2x(1+x)) + s_i' u_i (1 + 2(1+y)^2 + 2x(3x+4) + 4xy) + 2 s_i'^2 u_i^2)$$

and

$$\eta(i) = 8(1 + 3(r_i + v_i) + 4(r_i^2 + v_i^2) + 2(r_i^3 + v_i^3) + 2 r_i v_i (2 + r_i + v_i) + 4 s_i' u_i (1 + r_i + v_i)).$$

Corollary 2 becomes (for $i, j = 1, 2, 3$):

$$\begin{aligned}(\mathrm{C}(i,j)) \qquad & 2(r_j \mu_i + u_j \nu_i) \equiv \gamma_{11}(i)\alpha(i,j) + \gamma_{12}(i)\beta(i,j) \bmod 2^m, \\ & 2(s_j' \mu_i + v_j \nu_i) \equiv \gamma_{21}(i)\alpha(i,j) + \gamma_{22}(i)\beta(i,j) \bmod 2^{n+1},\end{aligned}$$

and

$$\begin{aligned}\gamma_{11}(i) &= 4((1+r_i)(1+2r_i(1+r_i)) + 2 s_i' u_i (2 + v_i + 2r_i)), \\ \gamma_{22}(i) &= 4((1+v_i)(1+2v_i(1+v_i)) + 2 s_i' u_i (2 + r_i + 2v_i)), \\ \gamma_{12}(i) &= \tau(i) u_i, \quad \gamma_{21}(i) = \tau(i) s_i',\end{aligned}$$

where

$$\tau(i) = 4(3 + 4(r_i + v_i) + 2(r_i^2 + v_i^2) + 2 r_i v_i + 2 s_i' u_i)$$

and $c_{ij} = a^{\alpha(i,j)} b^{\beta(i,j)}$.

Since $c_{ij} = a^{\alpha(i,j)} b^{\beta(i,j)}$, we have the following table of values for α and β:

α/β	$i=1$	$i=2$	$i=3$
$\alpha(i,1)$	0	0	-1
$\beta(i,1)$	0	-1	δ
$\alpha(i,2)$	0	0	$-2\mu_0$
$\beta(i,2)$	1	0	$-2\nu_0$
$\alpha(i,3)$	1	$2\mu_0$	0
$\beta(i,3)$	$-\delta$	$2\nu_0$	0

Now, in order to prove the theorem, we consider the cases $m = 2$ and $m \geqslant 3$ separately.

Proposition 8. *There exists no group G satisfying Assumptions $(\mathcal{A}1)$–$(\mathcal{A}4)$ for which $m = 2$.*

P r o o f. Since $m = 2$, Proposition 2 and (W) imply that

$$\begin{pmatrix} u_1 & v_1 & r_1 & s_1 \\ u_2 & v_2 & r_2 & s_2 \\ u_3 & v_3 & r_3 & s_3 \end{pmatrix} \equiv \begin{pmatrix} u_1 & v_1 & r_1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \bmod 2.$$

By (C(i)) notice that $\alpha_{21}(i) = \eta(i)2^{n-2}s_i \equiv 0 \bmod 2^{n+1}$, since $\eta(i) \equiv 0 \bmod 8$ and thus, $2^n\nu_i \equiv 0 \bmod 2^{n+1}$. Therefore, we have

$$\nu_1 \equiv \nu_2 \equiv \nu_3 \equiv 0 \bmod 2.$$

Also by (C(i)) again, $\alpha_{22}(i) \equiv 8v_i(1 + v_i) \bmod 2^{n+1}$ ($\alpha_{22}(i) \equiv 0 \bmod 2^n$). Thus,

$$2^n\mu_i \equiv 8v_i(1 + v_i) \bmod 2^{n+1}.$$

Next, consider (C(i, j)). In particular notice that $r_j\mu_i + u_j\nu_i \equiv 0 \bmod 2$, since $\gamma_{11}(i) \equiv \gamma_{12}(i) \equiv 0 \bmod 4$. But since $r_2 \equiv 1 \bmod 2$ and $\nu_i \equiv 0 \bmod 2$, we have

$$\mu_1 \equiv \mu_2 \equiv \mu_3 \equiv 0 \bmod 2.$$

Hence, from the above we have

$$v_i(1 + v_i) \equiv 0 \bmod 2^{n-2}.$$

Also notice that $\gamma_{21}(i) \equiv 2^n s_i \bmod 2^{n+1}$ (since $\tau(i) \equiv 4 \bmod 8$) and $\gamma_{22}(i) \equiv 4(1 + v_i) \bmod 2^{n+1}$. Hence, (C($i, j$)) implies

$$\text{(E}(i,j)\text{)} \qquad 2^{n-2}s_j\mu_i + v_j\nu_i \equiv 2^{n-1}s_i\alpha(i,j) + 2(1 + v_i)\beta(i,j) \bmod 2^n.$$

Now we consider the cases $n = 2$ and $n \geqslant 3$ individually.

Let $n = 2$. Then we have (refer to the table of values for α and β above)

$$\text{(E(1,3))} \qquad s_3\mu_1 + v_3\nu_1 \equiv 2s_1 - 2(1 + v_1)\delta \bmod 4,$$

or equivalently,

$$s_1 \equiv 0 \bmod 2,$$

a contradiction, since $s_1 \equiv 1 \bmod 2$.

Now suppose $n \geqslant 3$. Recall from above that $v_i(1 + v_i) \equiv 0 \bmod 2^{n-2}$. Then

$$\text{(E(1,2))} \qquad 2^{n-2}s_2\mu_1 + v_2\nu_1 \equiv 2(1 + v_1) \bmod 2^n.$$

Consequently, $v_1 \equiv 1 \bmod 2$, and so

$$1 + v_1 \equiv 0 \bmod 2^{n-2}.$$

We have

(E(1,1)) $$2^{n-2}s_1\mu_1 + v_1\nu_1 \equiv 0 \bmod 2^n,$$

and thus,

$$\nu_1 \equiv 0 \bmod 4.$$

Finally,

(E(1,3)) $$2^{n-2}s_3\mu_1 + v_3\nu_1 \equiv 2^{n-1}s_1 - 2(1+v_1)\delta \bmod 2^n,$$

and so

$$v_3\nu_1 \equiv 2^{n-1} \bmod 2^n.$$

But notice that $v_3 \equiv 0 \bmod 2^{n-2}$ and $\nu_1 \equiv 0 \bmod 4$. Therefore, $0 \equiv 2^{n-1} \bmod 2^n$, a contradiction.

Thus, we have established the proposition. □

Now we consider the case when $m \geqslant 3$.

Proposition 9. *There exists no group G satisfying Assumptions $(\mathcal{A}1)$–$(\mathcal{A}4)$ for which $m \geqslant 3$.*

P r o o f. Since $m \geqslant 3$, Proposition 2 and (W) imply that

$$\begin{pmatrix} u_1 & v_1 & r_1 & s_1 \\ u_2 & v_2 & r_2 & s_2 \\ u_3 & v_3 & r_3 & s_3 \end{pmatrix} \equiv \begin{pmatrix} u_1 & v_1 & r_1 & s_1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \bmod 2.$$

Thus, by Lemma 2 (ii), we choose the basis elements a_i of G so that $\delta = 0$, i.e., so that $c_{12} = b$ and $c_{13} = a$.

Now consider the consequences of (C(i)) for $i = 2, 3$. Since $r_i \equiv v_i \equiv 0 \bmod 2$ for $i = 2, 3$, we have $\eta(i) \equiv 8 \bmod 16$. Hence, $0 \equiv \alpha_{12}(i) = \eta(i)u_i \bmod 2^m$ and thus, $u_i \equiv 0 \bmod 2^{m-3}$. Similarly, $2^n\nu_i \equiv \alpha_{21}(i) = \eta(i)s_i' \bmod 2^{n+1}$, whence $s_i' \equiv 2^{n-3}\nu_i \bmod 2^{n-2}$. From this, we see that $0 \equiv \alpha_{11}(i) \equiv 8r_i(1+r_i) \bmod 2^m$ and thus, $r_i \equiv 0 \bmod 2^{m-3}$. Finally, since $2^n\mu_i \equiv \alpha_{22}(i) \equiv 8v_i(1+v_i) \bmod 2^{n+1}$, we get $v_i \equiv 2^{n-3}\mu_i \bmod 2^{n-2}$. Summarizing we have:

For $i = 2, 3$,

(E(i)) $$r_i \equiv u_i \equiv 0 \bmod 2^{m-3}, \quad s_i' \equiv 2^{n-3}\nu_i \bmod 2^{n-2}, \quad v_i \equiv 2^{n-3}\mu_i \bmod 2^{n-2}.$$

With respect to (C(i, j)), by applying (E(i)) (again with $i = 2, 3$) we obtain

$$\gamma_{11}(i) \equiv 4(1+r_i) \bmod 2^m, \quad \gamma_{12}(i) \equiv -4u_i \bmod 2^m,$$
$$\gamma_{21}(i) \equiv 2^{n-1}\nu_i \bmod 2^n, \quad \gamma_{22}(i) \equiv 4(1+v_i) + 2^n\mu_i \bmod 2^{n+1}.$$

(Notice that to obtain the congruence for γ_{21} using (E(i)) we needed to consider the congruence modulo 2^n rather than 2^{n+1}.) We thus obtain the following congruences from (C(i,j)) (and the table below it):

(E(3,1)) $\quad r_1\mu_3 + u_1\nu_3 \equiv -2(1+r_3) \bmod 2^{m-1},\ s_1'\mu_3 + v_1\nu_3 \equiv 2^{n-2}\nu_3 \bmod 2^{n-1},$

(E(2,1)) $\quad r_1\mu_2 + u_1\nu_2 \equiv 2u_2 \bmod 2^{m-1},\ s_1'\mu_2 + v_1\nu_2 \equiv -2(1+v_2) + 2^{n-1}\mu_2 \bmod 2^n.$

Now let R and Ω be the matrices given by

$$R = \begin{pmatrix} r_1 & u_1 \\ s_1' & v_1 \end{pmatrix}, \quad \Omega = \begin{pmatrix} \mu_3 & \mu_2 \\ \nu_3 & \nu_2 \end{pmatrix}.$$

Hence, we see that

$$R\Omega \equiv 2I \bmod 4,$$

where I is the identity matrix. (This is obvious for $n \geqslant 4$ and also holds for $n = 3$ since (E(i)) then implies that $\nu_3 \equiv 0 \bmod 2$ for recall that s_3 is even.) Therefore, $\det R \det \Omega = \det(R\Omega) \equiv 4 \bmod 8$ and thus, we have 3 possibilities

(a) $\det R \equiv 1 \bmod 2$ and $\det \Omega \equiv 4 \bmod 8$,

(b) $\det R \equiv 2 \bmod 4$ and $\det \Omega \equiv 2 \bmod 4$,

(c) $\det R \equiv 4 \bmod 8$ and $\det \Omega \equiv 1 \bmod 2$.

Again using (C(1,1)), we see that

$$r_1\mu_1 + u_1\nu_1 \equiv 0 \bmod 2^{m-1}, \quad s_1'\mu_1 + v_1\nu_1 \equiv 0 \bmod 2^n,$$

and hence,

$$R\begin{pmatrix} \mu_1 \\ \nu_1 \end{pmatrix} = \begin{pmatrix} 2^{m-1}x \\ 2^n y \end{pmatrix}$$

for some integers x, y. By multiplying by $\operatorname{adj} R = (\det R)R^{-1}$, the adjoint of R, we obtain

$$\det R \begin{pmatrix} \mu_1 \\ \nu_1 \end{pmatrix} = \begin{pmatrix} v_1 & -u_1 \\ -s_1' & r_1 \end{pmatrix} \begin{pmatrix} 2^{m-1}x \\ 2^n y \end{pmatrix}.$$

Therefore,

$$\det R \begin{pmatrix} \mu_1 \\ \nu_1 \end{pmatrix} \equiv \begin{pmatrix} 2^{m-1}v_1 x \\ 2^{m-1}s_1' x \end{pmatrix} \bmod 2^n. \tag{4}$$

Now by (C(1,2)) and (C(1,3)) we get in particular

(E(1,2)) $$r_2\mu_1 + u_2\nu_1 \equiv \frac{1}{2}\gamma_{12}(1) \bmod 2^{m-1},$$

(E(1,3)) $$s_3'\mu_1 + v_3\nu_1 \equiv \frac{1}{2}\gamma_{21}(1) \bmod 2^n,$$

where $\gamma_{12}(1) = \tau(1)u_1$, $\gamma_{21}(1) = \tau(1)s_1'$, and $\tau(1) \equiv 4 \bmod 8$.

From all of this, we want to arrive at a contradiction of some sort. The way we do it is with the congruence (essentially) (II_3):

$$u_1 s_3' - u_3 s_1' \equiv 2^{n-2} \bmod 2^{n-1}.$$

If we can get $u_1 s_3' \equiv u_3 s_1' \equiv 0 \bmod 2^{n-1}$, then we would have $0 \equiv 2^{n-2} \bmod 2^{n-1}$, the desired contradiction.

Notice that if $u_1 \equiv 0 \bmod 2^{m-2}$, then since $s_3' \equiv 0 \bmod 2^{n-3}$, we would have $u_1 s_3' \equiv 0 \bmod 2^{n+m-5}$. Hence, if $m \geqslant 4$, then we would have $u_1 s_3' \equiv 0 \bmod 2^{n-1}$. So given $m \geqslant 4$, we see from (E(1,2)) above that $u_1 \equiv 0 \bmod 2^{m-2}$ if $r_2\mu_1 + u_2\nu_1 \equiv 0 \bmod 2^{m-1}$. Since $r_2 \equiv u_2 \equiv 0 \bmod 2^{m-3}$, we see that it suffices that $\mu_1 \equiv \nu_1 \equiv 0 \bmod 4$. Since $m \geqslant 4$ and by (4) above, we have $\mu_1 \equiv \nu_1 \equiv 0 \bmod 4$, if $\det R \equiv 1 \bmod 2$ or $\equiv 2 \bmod 4$.

Thus, in summary, if $m \geqslant 4$ and $\det R \equiv 1 \bmod 2$ or $\equiv 2 \bmod 4$, then $u_1 s_3' \equiv 0 \bmod 2^{n-1}$. But given these conditions, since $s_3' \equiv v_3 \equiv 0 \bmod 2^{n-3}$ and $\mu_1 \equiv \nu_1 \equiv 0 \bmod 4$, we see that $s_3'\mu_1 + v_3\nu_1 \equiv 0 \bmod 2^{n-1}$. But then by (E(1,3)) above, we have $s_1' \equiv 0 \bmod 2^{n-2}$. Thus since $u_3 \equiv 0 \bmod 2$, we obtain $u_3 s_1' \equiv 0 \bmod 2^{n-1}$.

Therefore, if $m \geqslant 4$ and $\det R \equiv 1 \bmod 2$ or $\equiv 2 \bmod 4$, then we have a contradiction.

Hence, we are left to consider the cases:

(i) $m \geqslant 4$ with $\det R \equiv 4 \bmod 8$,

(ii) $m = 3$.

Suppose $m \geqslant 4$ with $\det R \equiv 4 \bmod 8$. Then $\det \Omega \equiv 1 \bmod 2$, and thus multiplying $R\,\Omega \equiv 2I \bmod 4$ by $\operatorname{adj}\Omega$, we obtain $R \equiv 2 \operatorname{adj}\Omega \bmod 4$. Therefore, in particular $v_1 \equiv s_1' \equiv 0 \bmod 2$. Hence, by (4), we have $\mu_1 \equiv \nu_1 \equiv 0 \bmod 4$. Now the proof follows exactly as in the previous case above.

Finally, suppose $m = 3$. For $i = 2, 3$, (E(i)) implies that $s_i \equiv 2^{m-3}\nu_i \bmod 2^{m-2}$, and since $m = 3$ and $s_i \equiv 0 \bmod 2$, we have $\nu_2 \equiv \nu_3 \equiv 0 \bmod 2$. This implies that $\det \Omega \equiv 0 \bmod 2$. Whence we need only consider $\det R \equiv 1 \bmod 2$ or $\equiv 2 \bmod 4$.

Now by (C(1)), $2^n\nu_1 \equiv \alpha_{21}(1) = \eta(1)2^{n-3}s_1 \equiv 2^n(1 + \varrho_1)s_1 \bmod 2^{n+1}$, since $\eta(1) \equiv 8(1 + \varrho_1) \bmod 16$. Therefore,

$$\nu_1 \equiv (1 + \varrho_1)s_1 \bmod 2. \tag{5}$$

Our goal is to come up with a contradiction to (II_3), which for $m = 3$ is given by

$$u_1 s_3 - u_3 s_1 \equiv 2 \bmod 4.$$

Suppose $\det R \equiv 1 \bmod 2$. Since $\det R$ is odd and $R\Omega \equiv 2I \bmod 4$, we have $\Omega \equiv 2 \operatorname{adj} R \bmod 4$, i.e.,

$$\begin{pmatrix} \mu_3 & \mu_2 \\ \nu_3 & \nu_2 \end{pmatrix} \equiv \begin{pmatrix} 2v_1 & -2u_1 \\ -2s_1' & 2r_1 \end{pmatrix} \bmod 4.$$

Again since $\det R \equiv 1 \bmod 2$, we see by (4) that $\mu_1 \equiv \nu_1 \equiv 0 \bmod 4$. By (E(1,2)) above we have $2u_1 \equiv r_2\mu_1 + u_2\nu_1 \bmod 4$ and thus, $2u_1 \equiv 0 \bmod 4$, i.e., $u_1 \equiv 0 \bmod 2$. But $1 \equiv \det R = r_1v_1 - u_1s_1' \bmod 2$. Hence, $r_1 \equiv v_1 \equiv 1 \bmod 2$. Thus, $\varrho_1 \equiv 0 \bmod 2$. Therefore, by (5) we must have $s_1 \equiv 0 \bmod 2$. But then $u_1s_3 - u_3s_1 \equiv 0 \bmod 4$. This contradicts ($\mathrm{II}_3$).

Now suppose $\det R \equiv 2 \bmod 4$. By (4) we have $\mu_1 \equiv \nu_1 \equiv 0 \bmod 2$ and thus, (E(1,2)) again implies that $u_1 \equiv 0 \bmod 2$. By (E(1,3)), we see that $2^{n-2}s_1 \equiv 2^{n-3}s_3\mu_1 + v_3\nu_1 \bmod 2^n$. Hence, $2^{n-2}s_1 \equiv v_3\nu_1 \bmod 2^{n-1}$ (recall that s_3 is even). If $n = 3$, then we have $2s_1 \equiv 0 \bmod 4$, and thus $s_1 \equiv 0 \bmod 2$. On the other hand, if $n > 3$, then (4) implies that $\nu_1 \equiv 0 \bmod 4$, since $s_1' \equiv 0 \bmod 2$. Thus, again $s_1 \equiv 0 \bmod 2$. Therefore, since $u_1 \equiv u_3 \equiv s_1 \equiv s_3 \equiv 0 \bmod 2$, we see that $u_1s_3 - u_3s_1 \equiv 0 \bmod 4$, contradicting ($\mathrm{II}_3$) above. This establishes the proposition. □

With this result, we have proved Theorem 3 and therefore the Main Theorem is now established. In light of the example above, we immediately get our Corollary to the Main Theorem:

Corollary. *The minimal order of a finite 2-group G, for which its commutator subgroup G' has rank 2 and is nonabelian, is 2^{12}.*

Acknowledgements. We would like to thank Ben Weiss, a friend and former colleague of the second author, for his help (and patience) using Magma to debunk some of our initial attempts at finding counterexamples to the Main Theorem.

We also very much thank Dr. Daniel C. Mayer for all his help, first in detecting (with Magma) a major error in our original formulation of the Main Theorem, and then for checking all our examples of groups as we tried to find one of derived length 3. All his contributions are truly appreciated!

References

[1] *E. Benjamin, C. Snyder*: Some real quadratic number fields whose Hilbert 2-class fields have class number congruent to 2 modulo 4. Acta Arith. *177* (2017), 375–392. zbl MR doi

[2] *N. Blackburn*: On prime-power groups in which the derived group has two generators. Proc. Camb. Philos. Soc. *53* (1957), 19–27. zbl MR doi

[3] *N. Blackburn*: On prime-power groups with two generators. Proc. Camb. Philos. Soc. *54* (1958), 327–337. zbl MR doi

[4] *B. Huppert*: Endliche Gruppen. I. Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen 134. Springer, Berlin, 1967. (In German.) zbl MR doi

Authors' addresses: Elliot Benjamin (corresponding author), School of Social and Behavioral Sciences, Capella University, 225 South 6th Street, Minneapolis, MN 55402, USA, e-mail: `ben496@prexar.com`; Chip Snyder, Department of Mathematics and Statistics, University of Maine, 333 Neville Hall, Orono, ME 04469-5752, USA, e-mail: `wsnyder@maine.edu`.