J. Group Theory **23** (2020), 659–696
DOI 10.1515/jgth-2019-0152

Finite groups with only small automorphism orbits

Alexander Bors

Communicated by Robert M. Guralnick

Abstract. We study finite groups G such that the maximum length of an orbit of the natural action of the automorphism group $\mathrm{Aut}(G)$ on G is bounded from above by a constant. Our main results are the following: Firstly, a finite group G only admits $\mathrm{Aut}(G)$-orbits of length at most 3 if and only if G is cyclic of one of the orders 1, 2, 3, 4 or 6, or G is the Klein four group or the symmetric group of degree 3. Secondly, there are infinitely many finite (2-)groups G such that the maximum length of an $\mathrm{Aut}(G)$-orbit on G is 8. Thirdly, the order of a d-generated finite group G such that G only admits $\mathrm{Aut}(G)$-orbits of length at most c is explicitly bounded from above in terms of c and d. Fourthly, a finite group G such that all $\mathrm{Aut}(G)$-orbits on G are of length at most 23 is solvable.

1 Introduction

The study of *structures* X (in the model-theoretic sense, i.e., sets endowed with operations and relations) that are "highly symmetrical", expressed through transitivity assumptions on natural actions of the automorphism group $\mathrm{Aut}(X)$, has a long and rich history, during which various strong theories have been built and beautiful results have been obtained. As examples, we mention vertex-transitive graphs [2, Definition 4.2.2, p. 85], block-transitive designs [5, 6] and finite flag-transitive projective planes [23].

When X is a group G, the assumption that $\mathrm{Aut}(G)$ acts transitively on G is not interesting, as only the trivial group satisfies it. Therefore, weaker conditions have been proposed and studied, such as the following (assuming that G is *finite*):

(1) "$\mathrm{Aut}(G)$ admits exactly c orbits on G" for some given, small constant c. For $c = 2$, it is not difficult to show that this is equivalent to G being nontrivial and elementary abelian. For results concerning $c \in \{3, 4, 5, 6, 7\}$, see the papers [1, 8, 15, 22] by various authors.

The author is supported by the Austrian Science Fund (FWF), project J4072-N32 "Affine maps on finite groups".

(2) “$\mathrm{Aut}(G)$ admits at least one orbit of length at least $\rho|G|$ on G” for some given constant $\rho \in (0, 1]$. For example, it is known that if $\rho > \frac{18}{19}$, then G is necessarily solvable [3, Theorem 1.1.2 (1)].

(3) “For each element order o in G, $\mathrm{Aut}(G)$ acts transitively on elements of order o in G”. In other words, $\mathrm{Aut}(G)$ is “as transitive as possible” in view of the fact that automorphisms must preserve the orders of elements. Such finite groups G are called *AT-groups* and are studied extensively by Zhang in [26].

In this paper, we are not concerned with such “highly homogeneous” finite groups, but rather with finite groups G that are “highly inhomogeneous” in the sense that they only admit small $\mathrm{Aut}(G)$-orbits (i.e., of constantly bounded length). There is also some relevant literature in this context, most notably the 1984 paper [20] by Robinson and Wiegold, in which they characterize general (not necessarily finite) such groups structurally [20, Theorem 1] and provide, for each prime p, an example of an infinite p-group G_p of nilpotency class 2 and of exponent p^2 such that $\mathrm{Aut}(G_p)$ is uncountably infinite but only has orbits of length at most $p^2(p-1)^2$ on G_p [20, Proposition 3 and the remark after its proof]. Another noteworthy result in this regard is that there are uncountable abelian groups with only two automorphisms; see e.g. [9, Theorem II].

However, finite groups behave quite differently to infinite groups in many regards, and by a result of Ledermann and B. H. Neumann [16], as the order of a finite group G tends to ∞, so does the order of $\mathrm{Aut}(G)$. In other words: “Large finite groups have many automorphisms.” Based on this result, one might conjecture that even the following stronger assertion holds: “For finite groups G, as $|G| \to \infty$, the maximum length of an $\mathrm{Aut}(G)$-orbit on G tends to ∞ as well”. This, however, is not true; see our Theorem 1.1 (2).

Throughout the rest of this paper, we denote by $\mathrm{maol}(G)$ the maximum length of an $\mathrm{Aut}(G)$-orbit on the finite group G. Moreover, exp and log denote the natural exponential and logarithm function respectively (with base the Euler constant e). We now state our main results.

Theorem 1.1. *The following statements hold.*

(1) *For each finite group G, the following are equivalent:*

  (a) $\mathrm{maol}(G) \leqslant 3$*;*

  (b) *G is isomorphic to one of the following: $\mathbb{Z}/m\mathbb{Z}$ with $m \in \{1, 2, 3, 4, 6\}$, $(\mathbb{Z}/2\mathbb{Z})^2$,* $\mathrm{Sym}(3)$.

  In particular, there are only finitely many finite groups G with $\mathrm{maol}(G) \leqslant 3$.

(2) *There are infinitely many finite* 2*-groups* G *with* $\mathrm{maol}(G) = 8$.

(3) *For each pair* (c, d) *of positive integers and every* d*-generated finite group* G *with* $\mathrm{maol}(G) \leqslant c$*, we have that* $\log |G|$ *is at most*

$$1.01624d \cdot (A(c,d) + 1) \cdot \left(\frac{\log A(c,d)}{\log 2} + 1\right) + \frac{1}{2}\left(7 + \frac{\log c}{\log 2}\right) \log c,$$

where

$$A(c,d) := c^{d + \frac{1}{2}(7 + \frac{\log c}{\log 2})\left(\binom{d}{2} + \frac{d}{2\log 2} \cdot (7 + \frac{\log c}{\log 2}) \log c\right)}.$$

(4) *A finite group* G *with* $\mathrm{maol}(G) \leqslant 23$ *is solvable.*

Note that the constant 23 in Theorem 1.1 (4) is optimal, as $\mathrm{maol}(\mathrm{Alt}(5)) = 24$.

2 Some preparations

In this section, we list some notation that will be used throughout the paper, and we discuss a few basic facts concerning power-commutator presentations, central automorphisms and finite groups without nontrivial solvable normal subgroups.

2.1 Notation

We denote by $\mathbb{N}$ the set of natural numbers (including 0) and by $\mathbb{N}^+$ the set of positive integers. For a prime power q, the notation $\mathbb{F}_q$ stands for the finite field with q elements. The identity function on a set X is denoted by id_X. The Euler totient function will be denoted by ϕ throughout and is to be distinguished from the symbol φ reserved for group homomorphisms. The kernel of a group homomorphism φ is denoted by $\ker(\varphi)$, and the order of an element g of a group G by $\mathrm{ord}(g)$, sometimes also by $\mathrm{ord}_G(g)$ for greater clarity. When g and h are elements of a group G, then we denote by $[g,h] := g^{-1}h^{-1}gh$ the commutator of g and h, and for subsets $X, Y \subseteq G$, the notation $[X, Y]$ stands for the subgroup of G generated by the commutators $[x, y]$ with $x \in X$ and $y \in Y$. We always denote the quotient of a group G by a normal subgroup N by G/N and reserve the notation $X \setminus Y$ for the set-theoretic difference of the sets X and Y. The index of a subgroup H in a group G is written $|G : H|$. If $x_1, \dots, x_n$ are pairwise distinct variables, then $\mathrm{F}(x_1, \dots, x_n)$ stands for the free group generated by $x_1, \dots, x_n$. When A is an abelian group, then the semidirect product $A \rtimes \mathbb{Z}/2\mathbb{Z}$, where the generator of $\mathbb{Z}/2\mathbb{Z}$ acts on A by inversion, is called the *generalized dihedral group over* A and will be denoted by $\mathrm{Dih}(A)$. The symmetric group on a set X is denoted by $\mathrm{Sym}(X)$, and for $n \in \mathbb{N}^+$, the symmetric and alternating group of degree n are written $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ respectively. All group actions discussed in this paper are on the right, and when $\varphi\colon G \to \mathrm{Sym}(X)$ is an action of the group G on the set X, then for $g \in G$ and $x \in X$, we write x^g shorthand for $\varphi(g)(x)$, and we write x^G for the full orbit of x under G. The exponent (i.e., least common multiple of the element orders) of a finite group G is denoted by $\mathrm{Exp}(G)$ (to be distinguished from the notation exp reserved for the natural exponential function), and the smallest size of a generating subset of G is denoted by $d(G)$. The notation $\mathrm{Rad}(G)$ is used for the solvable radical (largest solvable normal subgroup) of a finite group G, and $\mathrm{Soc}(G)$ is used for the socle (product of all the minimal nontrivial normal subgroups) of G; see also Subsection 2.3. The center of a group G is denoted by ζG, and $G' := [G, G]$ denotes the commutator subgroup of G. The inner automorphism group of a group G is written $\mathrm{Inn}(G)$. If G and H are groups, then $\mathrm{End}(G)$ denotes the set (monoid) of endomorphisms of G, and $\mathrm{Hom}(G, H)$ denotes the set of group homomorphisms $G \to H$.

2.2 Power-commutator presentations of finite solvable groups

A group G is called *polycyclic* if and only if it admits a *polycyclic series*, that is, a subnormal series $G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n \trianglerighteq G_{n+1} = \{1_G\}$ such that all the factors G_i/G_{i+1}, with $i \in \{1, \dots, n\}$, are cyclic. A generating tuple $(g_1, \dots, g_n)$ of G is called a *polycyclic generating sequence of* G if and only if, setting

$$G_i := \langle g_i, g_{i+1}, \dots, g_n \rangle \quad \text{for } i = 1, \dots, n+1,$$

the subgroup series $G = G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n \geqslant G_{n+1} = \{1_G\}$ is a polycyclic series in G. Clearly, every polycyclic group is solvable, and all *finite* solvable groups are polycyclic. If G is a polycyclic group and $(g_1, \dots, g_n)$ is a polycyclic generating sequence of G, then with respect to the generating tuple $(g_1, \dots, g_n)$, G can be represented by a so-called *polycyclic presentation*; see e.g. [13, Theorem 8.8, p. 279]. For our purposes, it will be more convenient to work with a variant of polycyclic presentations called *power-commutator presentations*. Assume that G is a *finite* polycyclic group (the finiteness assumption is not essential, but makes the situation a bit simpler) and that $(g_1, \dots, g_n)$ is a polycyclic generating sequence of G. Then with respect to the generating tuple $(g_1, \dots, g_n)$, the group G has a power-commutator presentation of the form

$$\begin{aligned} G = \langle x_1, \dots, x_n \mid x_i^{e_i} &= x_{i+1}^{a_{i,i+1}} \cdots x_n^{a_{i,n}} \text{ for } i = 1, \dots, n; \\ [x_i, x_j] &= x_{i+1}^{b_{i,j,i+1}} \cdots x_n^{b_{i,j,n}} \text{ for } 1 \leqslant i < j \leqslant n \rangle, \end{aligned}$$

where, for $i = 1, \dots, n$, the formal generator x_i corresponds to the group element g_i, and e_i is the so-called *relative order* of g_i, i.e., the order of

$$g_i G_{i+1} = g_i \langle x_{i+1}, \dots, x_n \rangle \quad \text{in } G/G_{i+1}.$$

Moreover, the exponents $a_{i,k}$ for $i = 1, \dots, n$, $k = i + 1, \dots, n$, and the exponents $b_{i,j,k}$ for $1 \leqslant i < j \leqslant n$, $k = i + 1, \dots, n$ are integers in $\{0, 1, \dots, e_k - 1\}$. For more details on polycyclic groups, see [13, Chapter 8].

2.3 Central automorphisms

If G is a group and f is a group homomorphism $G \to \zeta G$, then it is easy to check that the function $\varphi_f: G \to G$, $g \mapsto gf(g)$, is a group endomorphism of G, and that conversely, every endomorphism of G which leaves each coset of ζG in G set-wise invariant is of this form. Such endomorphisms of G are called *central*. Moreover, a central endomorphism φ_f of a group G has trivial kernel if and only if the neutral element 1_G is the only element of ζG which is mapped to its own inverse by f. In the case of finite groups G, the central endomorphisms of G with trivial kernel are the *central automorphisms* of G, which form a subgroup of $\mathrm{Aut}(G)$ denoted by $\mathrm{Aut}_{\mathrm{cent}}(G)$.

2.4 Finite semisimple groups

Throughout this paper, the term "semisimple group" denotes a group without nontrivial solvable normal subgroups; for finite groups G, this is equivalent to the condition that the solvable radical $\mathrm{Rad}(G)$ is trivial. Note that since the class of solvable groups is closed under group extensions, for every finite group G, the quotient $G/\mathrm{Rad}(G)$ is semisimple. Moreover, for finite semisimple groups H, the structure of H is controlled by the socle $\mathrm{Soc}(H)$. More precisely, $\mathrm{Soc}(H)$ is a direct product of nonabelian finite simple groups, and H acts faithfully on $\mathrm{Soc}(H)$ via conjugation, so that, up to isomorphism, H may be viewed as a subgroup of $\mathrm{Aut}(\mathrm{Soc}(H))$ containing $\mathrm{Inn}(\mathrm{Soc}(H))$; see also [19, Result 3.3.18, p. 89].

3 Finite groups G with $\mathrm{maol}(G) \leqslant 3$

This section is concerned with the proof of Theorem 1.1 (1). We will go through the three cases $\mathrm{maol}(G) = 1, 2, 3$ separately, but first, we prove the following simple lemma, which will be used frequently.

Lemma 3.1. *The following hold.*

(1) *Let $G_1, \dots, G_n$ be finite groups. Then*

$$\mathrm{maol}\Big(\prod_{k=1}^{n} G_k\Big) \geqslant \prod_{k=1}^{n} \mathrm{maol}(G_k) \geqslant \max\{\mathrm{maol}(G_k) \mid k = 1, \dots, n\}.$$

(2) *For every finite abelian group G, we have* $\operatorname{maol}(G) \geqslant \phi(\operatorname{Exp}(G))$*, where ϕ denotes the Euler totient function.*

(3) *Let G be a finite nilpotent group. Then* $\operatorname{maol}(G) = \prod_p \operatorname{maol}(G_p)$ *where the index p ranges over the primes and G_p denotes the (unique) Sylow p-subgroup of G.*

Proof. (1) This holds since $\prod_{k=1}^{n} \operatorname{Aut}(G_k)$ embeds into $\operatorname{Aut}(\prod_{k=1}^{n} G_k)$ via "component-wise mapping".

(2) First, note that if G is cyclic, then $\operatorname{maol}(G) = \phi(\operatorname{Exp}(G))$ as

$$\phi(\operatorname{Exp}(G)) = \phi(|G|)$$

is just the number of generators of G. If G is a general finite abelian group, then by the structure theorem for finite abelian groups, G has a cyclic direct factor of order $\operatorname{Exp}(G)$, and the asserted inequality follows by statement (1).

(3) This is clear since $\operatorname{Aut}(G)$ is isomorphic to the direct product $\prod_p \operatorname{Aut}(G_p)$ via "component-wise mapping". □

3.1 Finite groups G with $\operatorname{maol}(G) = 1$

The following proposition, whose proof is given for completeness, is easy and well known.

Proposition 3.1.1. *Let G be a finite group. The following are equivalent.*

(1) $\operatorname{maol}(G) = 1$.

(2) $\operatorname{Aut}(G)$ *is trivial.*

(3) $G \cong \mathbb{Z}/m\mathbb{Z}$ *with* $m \in \{1, 2\}$.

Proof. "(1) ⇒ (2)" Assume that $\operatorname{maol}(G) = 1$, and let $\alpha \in \operatorname{Aut}(G)$. Then for each $g \in G$, we have $g^{\alpha} \in g^{\operatorname{Aut}(G)} = \{g\}$ so that $g^{\alpha} = g$, $\alpha = \operatorname{id}_G$. Since $\alpha \in \operatorname{Aut}(G)$ was arbitrary, it follows that $\operatorname{Aut}(G) = \{\operatorname{id}_G\}$, as required.

"(2) ⇒ (3)" Assume that $\operatorname{Aut}(G)$ is trivial. Since $G/\zeta G \cong \operatorname{Inn}(G) \leqslant \operatorname{Aut}(G)$, it follows that $G = \zeta G$, i.e., G is abelian. Writing G additively, we find that the inversion on G, $-\operatorname{id}_G$, is an automorphism of G, and so $-\operatorname{id}_G = \operatorname{id}_G$, i.e., G is of exponent 2, and thus $G \cong (\mathbb{Z}/2\mathbb{Z})^d$ for some $d \in \mathbb{N}$. But if $d \geqslant 2$, then by Lemma 3.1 (1),

$$\operatorname{maol}(G) \geqslant \operatorname{maol}((\mathbb{Z}/2\mathbb{Z})^2) = 3 > 1$$

so that $\operatorname{Aut}(G)$ must be nontrivial, a contradiction. Hence $d \in \{0, 1\}$, as required.

"(3) ⇒ (1)" Assume that G is of order at most 2. Then since $\operatorname{Aut}(G)$ is contained in a point stabilizer in $\operatorname{Sym}(G)$, every element of G must be fixed by all permutations in $\operatorname{Aut}(G)$, whence $\operatorname{maol}(G) = 1$, as required. □

3.2 Finite groups G with $\mathrm{maol}(G) = 2$

These groups are less trivial to deal with than the ones with maol-value 1. Note that if G is a finite group with $\mathrm{maol}(G) = 2$, then $\alpha^2 = \mathrm{id}_G$ for every automorphism α of G. Hence $\mathrm{Aut}(G)$ is of exponent 2, i.e., $\mathrm{Aut}(G)$ is an elementary abelian 2-group. We will need a few results on finite groups with abelian automorphism group.

Definition 3.2.1. A nonabelian finite group with abelian automorphism group is called a *Miller group*.

This terminology, taken from the survey paper [14], is in honor of G. A. Miller, who gave the first example of such a group (of order 64) in 1913 [17] (see also [14, Section 3, (3.1)]). Since then, a rich theory of Miller groups with many beautiful results and examples has emerged. We will need the following.

Proposition 3.2.2. *Let G be a Miller group. Then the following hold.*

(1) *G is nilpotent of class* 2*.*

(2) *Every Sylow subgroup of G has abelian automorphism group.*

(3) *If G is a p-group for some prime p and $|G'| > 2$, then G' is not cyclic.*

Proof. (1) This holds since for every group H, being nilpotent of class at most 2 is equivalent to the commutativity of $\mathrm{Inn}(H)$; see also [14, Section 1].

(2) This is clear since $\mathrm{Aut}(G)$ is the direct product of the automorphism groups of the Sylow subgroups of G (see also the proof of Lemma 3.1 (3)).

(3) By [14, statement (4) at the end of Section 1], this holds if one additionally assumes that G is *purely nonabelian*, i.e., G has no nontrivial abelian direct factor. However, this additional assumption can be dropped, for if G is not purely nonabelian, then $G = G_0 \times A$, where G_0 is purely nonabelian and A is abelian. Since $\mathrm{Aut}(G_0)$ embeds into $\mathrm{Aut}(G)$, we have that G_0 is also a Miller p-group, and $|G'| = |G_0'| > 2$, so G_0' is not cyclic. But $G' \cong G_0'$, whence G' is not cyclic. □

We can now prove the following lemma, which will be used in our proof of the classification of finite groups G with $\mathrm{maol}(G) = 2$ (see Proposition 3.2.4 below).

Lemma 3.2.3. *Let G be a finite group with* $\mathrm{maol}(G) = 2$*. Then the following hold.*

(1) *If G is abelian, then $G \cong \mathbb{Z}/m\mathbb{Z}$ with $m \in \{3, 4, 6\}$.*

(2) *If G is nonabelian, then*

   (a) *G is a Miller* 2*-group,*

(b) *ζG is cyclic,*

(c) $|G'| = 2$,

(d) $|\zeta G| > 2$,

(e) *G/G' is an elementary abelian 2-group.*

Proof. (1) By Lemma 3.1 (3), $\mathrm{maol}(G) = \prod_p \mathrm{maol}(G_p)$, where the index p ranges over the primes and G_p denotes the Sylow p-subgroup of G. Moreover, if G_p is nontrivial, then by Lemma 3.1 (2), $\mathrm{maol}(G_p) \geqslant \phi(\mathrm{Exp}(G_p)) \geqslant p-1$. It follows that G_p is trivial unless $p \in \{2,3\}$, i.e., G is a finite abelian $\{2,3\}$-group of order at least 3. Consider the following cases.

Case (1): *G is a 2-group.* By Lemma 3.1 (2), $\mathrm{maol}(G) \geqslant \phi(\mathrm{Exp}(G))$, and thus $\mathrm{Exp}(G) \leqslant 4$. But $\mathrm{Exp}(G) = 2$ is impossible since then $G \cong (\mathbb{Z}/2\mathbb{Z})^d$ for some $d \geqslant 2$, and thus $\mathrm{maol}(G) \geqslant \mathrm{maol}((\mathbb{Z}/2\mathbb{Z})^2) = 3$ by Lemma 3.1 (1). Hence we have $\mathrm{Exp}(G) = 4$. If G has more than one direct factor $\mathbb{Z}/4\mathbb{Z}$ in its decomposition into primary cyclic groups, by Lemma 3.1 (1), $\mathrm{maol}(G) \geqslant \mathrm{maol}((\mathbb{Z}/4\mathbb{Z})^2) = 12$, a contradiction. Hence $G \cong (\mathbb{Z}/2\mathbb{Z})^d \times \mathbb{Z}/4\mathbb{Z}$ for some $d \in \mathbb{N}$. If $d \geqslant 1$, then by Lemma 3.1 (1), $\mathrm{maol}(G) \geqslant \mathrm{maol}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) = 4$, a contradiction. It follows that $G \cong \mathbb{Z}/4\mathbb{Z}$.

Case (2): *G is a 3-group.* Again, $\mathrm{maol}(G) \geqslant \phi(\mathrm{Exp}(G))$ by Lemma 3.1 (2), which implies that $\mathrm{Exp}(G) = 3$, whence $G \cong (\mathbb{Z}/3\mathbb{Z})^d$ for some $d \in \mathbb{N}^+$. If $d \geqslant 2$, then by Lemma 3.1 (1), $\mathrm{maol}(G) \geqslant \mathrm{maol}((\mathbb{Z}/3\mathbb{Z})^2) = 8$, a contradiction. Hence $G \cong \mathbb{Z}/3\mathbb{Z}$.

Case (3): *G is neither a 2- nor a 3-group.* Then $G = G_2 \times G_3$ with G_p a nontrivial abelian p-group for $p \in \{2,3\}$. By Lemma 3.1 (3), we have

$$2 = \mathrm{maol}(G) = \mathrm{maol}(G_2) \cdot \mathrm{maol}(G_3).$$

Hence $(\mathrm{maol}(G_2), \mathrm{maol}(G_3))$ is either $(2,1)$ or $(1,2)$. But the former is impossible since by Proposition 3.1.1, there are no nontrivial finite 3-groups with maol-value 1. Hence $\mathrm{maol}(G_2) = 1$ and $\mathrm{maol}(G_3) = 2$. It follows by Proposition 3.1.1 and the previous case that $G_2 \cong \mathbb{Z}/2\mathbb{Z}$ and $G_3 \cong \mathbb{Z}/3\mathbb{Z}$, whence $G \cong \mathbb{Z}/6\mathbb{Z}$.

(2) (a) As noted at the beginning of this subsection, $\mathrm{Aut}(G)$ is an elementary abelian 2-group, so G is certainly a Miller group. By Proposition 3.2.2 (1), G is nilpotent, so we can write $G = \prod_p G_p$, where the index p ranges over the primes and G_p denotes the Sylow p-subgroup of G. By Lemma 3.1 (3), we have $2 = \mathrm{maol}(G) = \prod_p \mathrm{maol}(G_p)$, and so $\mathrm{maol}(G_p) = 2$ for exactly one prime p, and $\mathrm{maol}(G_\ell) = 1$ for all primes $\ell \neq p$. We claim that G is a p-group. Indeed, otherwise, in view of Proposition 3.1.1, $|G|$ has exactly two distinct prime divisors, and more precisely, $p > 2$ and $\pi(G) = \{2, p\}$, with $G_2 \cong \mathbb{Z}/2\mathbb{Z}$. Since G is

nonabelian, it follows that G_p is nonabelian, whence G_p has an (inner) automorphism of order p, which implies that $\mathrm{maol}(G) \geqslant \mathrm{maol}(G_p) \geqslant p > 2$, a contradiction. So G is indeed a p-group for some prime p, and again, since G is nonabelian, $2 = \mathrm{maol}(G) \geqslant p$, whence $p = 2$. This concludes the proof of statement (2) (a).

(2) (b) Assume that ζG is not cyclic so that we have an embedding

$$\iota\colon (\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow \zeta G.$$

As G is of nilpotency class 2 (by Proposition 3.2.2 (1)), the central quotient $G/\zeta G$ is an abelian 2-group, whence we also have a projection $\pi\colon G/\zeta G \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$. There are four distinct homomorphisms $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^2$, and by composition, we get four distinct homomorphisms

$$f\colon G \overset{\text{can.}}{\twoheadrightarrow} G/\zeta G \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z} \overset{\varphi}{\to} (\mathbb{Z}/2\mathbb{Z})^2 \overset{\iota}{\hookrightarrow} \zeta G.$$

For each such homomorphism $f\colon G \to \zeta G$, we have that $\zeta G \leqslant \ker(f)$, and so the neutral element 1_G is the only element of ζG inverted by f. We may thus consider the associated central automorphism $\alpha_f\colon G \to G$, $g \mapsto gf(g)$. Now fix an element $g \in G$ outside the (index 2) kernel of the composition

$$G \overset{\text{can.}}{\twoheadrightarrow} G/\zeta G \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z}.$$

Then the images of g under the four mentioned central automorphisms α_f are pairwise distinct, which implies that $\mathrm{maol}(G) \geqslant 4$, a contradiction. This concludes the proof of statement (2) (b).

(2) (c) Recall that by Proposition 3.2.2 (1), G is nilpotent of class 2, whence $G' \leqslant \zeta G$, and so G' is cyclic by statement (2) (b). Proposition 3.2.2 (3) now implies that $|G'| = 2$, as required.

(2) (d) Assume, aiming for a contradiction, that $|\zeta G| = 2$. Then, since G is nilpotent of class 2 by Proposition 3.2.2 (1), we have $G' = \zeta G \cong \mathbb{Z}/2\mathbb{Z}$ so that G is an extraspecial 2-group. By [25, Theorem 1 (c)], the induced action of $\mathrm{Aut}(G)$ on $G/\zeta G \cong \mathbb{F}_2^{2n}$ corresponds to the one of an orthogonal group $O_{2n}^{\epsilon}(2)$, for some $\epsilon \in \{+,-\}$ (depending on the isomorphism type of G). In any case, this implies that $3 \mid |\mathrm{Aut}(G)|$ so that $\mathrm{Aut}(G)$ contains an element of order 3 by Cauchy's theorem, and thus $\mathrm{maol}(G) \geqslant 3$, a contradiction. This concludes the proof of statement (2) (d).

(2) (e) Assume, aiming for a contradiction, that G/G' is *not* an elementary abelian 2-group. Then we have a projection $\pi\colon G/G' \twoheadrightarrow \mathbb{Z}/4\mathbb{Z}$. There are four endomorphisms φ of $\mathbb{Z}/4\mathbb{Z}$, and by composition, we obtain four distinct homomorphisms

$$f\colon G \overset{\text{can.}}{\twoheadrightarrow} G/G' \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/4\mathbb{Z} \overset{\varphi}{\to} \mathbb{Z}/4\mathbb{Z} \hookrightarrow \zeta G.$$

By the three facts that G' is nontrivial, $G' \leqslant \zeta G$ and ζG is a cyclic 2-group, each such homomorphism $f\colon G \to \zeta G$ has the property that any nontrivial element of ζG is mapped under f to an element of smaller order; in particular, 1_G is the only element of ζG which is inverted by f. It follows that each such homomorphism f induces a central automorphism $\alpha_f\colon G \to G$, $g \mapsto gf(g)$, and any element $g \in G$ which gets mapped under the composition

$$G \overset{\text{can.}}{\twoheadrightarrow} G/G' \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/4\mathbb{Z}$$

to a generator of $\mathbb{Z}/4\mathbb{Z}$ assumes four distinct images under these central automorphisms α_f. It follows that $\mathrm{maol}(G) \geqslant 4$, a contradiction, which concludes the proof of statement (2) (e). □

We are now ready to classify the finite groups G with $\mathrm{maol}(G) = 2$.

Proposition 3.2.4. *Let G be a finite group. The following are equivalent.*

(1) $\mathrm{maol}(G) = 2$.

(2) $G \cong \mathbb{Z}/m\mathbb{Z}$ *for some* $m \in \{3, 4, 6\}$.

Proof. The implication "(2) ⇒ (1)" is easy, so we focus on proving "(1) ⇒ (2)". By Lemma 3.2.3 (1), it suffices to show that G is abelian. So, working toward a contradiction, let us assume that G is nonabelian. Then we can use all the structural information on G displayed in Lemma 3.2.3 (2).

Write $G/G' \cong (\mathbb{Z}/2\mathbb{Z})^d$ with $d \in \mathbb{N}^+$. Note that $d \geqslant 3$, as otherwise,

$$|G| = |G'| \cdot |G/G'| \leqslant 2 \cdot 4 = 8,$$

which implies $|\zeta G| = 2$, contradicting Lemma 3.2.3 (2) (d). Let us call a d-tuple $(g_1, \ldots, g_d) \in G^d$ a *standard tuple in* G if and only if it projects to an $\mathbb{F}_2$-basis of G/G' under the canonical projection $G \twoheadrightarrow G/G'$ (we remark that this notion of a "standard tuple" will also appear in the next subsection, Subsection 3.3, and it will be introduced and studied in greater generality in Section 5).

Since $|G'| = 2$, the number of standard tuples in G is exactly

$$2^d \cdot \prod_{i=0}^{d-1} (2^d - 2^i).$$

For each standard tuple $(g_1, \ldots, g_d)$ in G, the associated *power-commutator tuple* is defined to be the following $(d + \binom{d}{2})$-tuple with entries in G':

$$(g_1^2, g_2^2, \ldots, g_d^2, [g_1, g_2], [g_1, g_3], \ldots, [g_1, g_d], \\ [g_2, g_3], [g_2, g_4], \ldots, [g_2, g_d], \ldots, [g_{d-1}, g_d]).$$

We say that two standard tuples in G are *equivalent* if and only if they have the same power-commutator tuple. Now, if c denotes the unique nontrivial element of G', then for every standard tuple $(g_1, \dots, g_d)$ in G, the $(d+1)$-tuple $(g_1, \dots, g_d, c)$ is a polycyclic generating sequence of G. Further, if $(h_1, \dots, h_d)$ is a standard tuple in G which is equivalent to $(g_1, \dots, g_d)$, then the two polycyclic generating sequences $(g_1, \dots, g_d, c)$ and $(h_1, \dots, h_d, c)$ of G induce the same power-commutator presentation of G (this is because since c is central in G, one has $[g_i, c] = [h_i, c] = 1$ for all $i = 1, \dots, d$) so that there exists an automorphism α of G with $g_i^\alpha = h_i$ for $i = 1, \dots, d$. This shows that equivalent standard tuples lie in the same orbit of the component-wise action of $\mathrm{Aut}(G)$ on G^d.

Note that since $|G'| = 2$, the number of distinct power-commutator tuples of standard tuples in G, and thus the number of equivalence classes of standard tuples in G, is at most $2^{d+\binom{d}{2}}$. It follows that there is an equivalence class of standard tuples in G which is of size at least

$$\begin{aligned}\frac{2^d \cdot \prod_{i=0}^{d-1} (2^d - 2^i)}{2^{d+\binom{d}{2}}} &= \frac{\prod_{i=0}^{d-1} (2^d - 2^i)}{2^{\binom{d}{2}}} \\ &= \frac{2^{0+1+2+\cdots+d-1} \cdot \prod_{i=0}^{d-1} (2^{d-i} - 1)}{2^{\binom{d}{2}}} \\ &= \prod_{i=0}^{d-1} (2^{d-i} - 1) = \prod_{j=1}^{d} (2^j - 1).\end{aligned}$$

In particular, the component-wise action of $\mathrm{Aut}(G)$ on G^d has an orbit of length at least $\prod_{j=1}^{d} (2^j - 1)$. However, since $\mathrm{maol}(G) = 2$, no orbit of the action of $\mathrm{Aut}(G)$ on G^d can be of length larger than 2^d. It follows that

$$2^d \geqslant \prod_{j=1}^{d} (2^j - 1),$$

which does not hold for any $d \geqslant 3$, a contradiction. □

3.3 Finite groups G with $\mathrm{maol}(G) = 3$

We begin by proving some properties of finite groups G with $\mathrm{maol}(G) = 3$ which will be crucial for the subsequent discussion.

Lemma 3.3.1. *Let G be a finite group with* $\mathrm{maol}(G) = 3$. *Then the following hold.*

(1) *If G is abelian, then $G \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

(2) *If G is nonabelian, then the following hold:*

(a) *the set of element orders of* $\mathrm{Aut}(G)$ *is contained in* $\{1, 2, 3\}$ *(in particular,* $\mathrm{Aut}(G)$ *is solvable);*

(b) *G is a $\{2, 3\}$-group (in particular, G is solvable).*

Proof. (1) Write $G = \prod_p G_p$, where p ranges over the primes and G_p denotes the Sylow p-subgroup of G. If G_p is nontrivial for some prime $p \geqslant 5$, then by Lemma 3.1 (1) (2),

$$\mathrm{maol}(G) \geqslant \mathrm{maol}(G_p) \geqslant \phi(p) = p - 1 \geqslant 4 > 3,$$

a contradiction. Hence $G = G_2 \times G_3$, and by Lemma 3.1 (3), we have

$$3 = \mathrm{maol}(G) = \mathrm{maol}(G_2) \cdot \mathrm{maol}(G_3).$$

We distinguish two cases.

Case (1): $\mathrm{maol}(G_2) = 3$ *and* $\mathrm{maol}(G_3) = 1$. Then by Proposition 3.1.1, G_3 is trivial, and so G is an abelian 2-group. By Lemma 3.1 (2), we have

$$3 = \mathrm{maol}(G) \geqslant \phi(\mathrm{Exp}(G)),$$

which implies that $\mathrm{Exp}(G) \in \{2, 4\}$. Distinguish two subcases.

Subcase (a): $\mathrm{Exp}(G) = 2$. Then $G \cong (\mathbb{Z}/2\mathbb{Z})^d$ for some positive integer d, and we have $3 = \mathrm{maol}(G) = 2^d - 1$. It follows that $d = 2$, i.e., $G \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Subcase (b): $\mathrm{Exp}(G) = 4$. Then $G \cong (\mathbb{Z}/2\mathbb{Z})^{d_1} \times (\mathbb{Z}/4\mathbb{Z})^{d_2}$ for some $d_1 \in \mathbb{N}$ and some $d_2 \in \mathbb{N}^+$. If $d_2 \geqslant 2$, then by Lemma 3.1 (1),

$$\mathrm{maol}(G) \geqslant \mathrm{maol}((\mathbb{Z}/4\mathbb{Z})^2) = 12 > 3,$$

a contradiction. Hence $d_2 = 1$. If $d_1 = 0$, then

$$\mathrm{maol}(G) = \mathrm{maol}(\mathbb{Z}/4\mathbb{Z}) = 2 < 3,$$

a contradiction. Hence $d_1 \geqslant 1$, which implies by Lemma 3.1 (1) that

$$\mathrm{maol}(G) \geqslant \mathrm{maol}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) = 4 > 3,$$

another contradiction.

Case (2): $\mathrm{maol}(G_2) = 1$ *and* $\mathrm{maol}(G_3) = 3$. By Lemma 3.1 (2),

$$3 = \mathrm{maol}(G_3) \geqslant \phi(\mathrm{Exp}(G_3)),$$

whence $\mathrm{Exp}(G_3) = 3$. It follows that $G_3 \cong (\mathbb{Z}/3\mathbb{Z})^d$ for some positive integer d, and therefore $\mathrm{maol}(G_3) = 3^d - 1$, which is never equal to 3, a contradiction.

(2) (a) The "in particular" follows from Burnside's $p^a q^b$-theorem, so we focus on proving the main assertion. Let α be an automorphism of G. For each positive integer k, consider the subgroup

$$\mathrm{C}_G(\alpha^k) = \{g \in G \mid g^{\alpha^k} = g\} \leqslant G.$$

Since $\mathrm{maol}(G) = 3$, all cycles of α on G are of one of the lengths 1, 2 or 3. Equivalently, $G = \mathrm{C}_G(\alpha^2) \cup \mathrm{C}_G(\alpha^3)$. But no finite group is a union of two proper subgroups (see e.g. [19, Exercise 1.3.9, p. 17]). It follows that either $\mathrm{C}_G(\alpha^2) = G$ or $\mathrm{C}_G(\alpha^3) = G$, and accordingly, that the order of α divides 2 or 3, which concludes the proof of statement (2) (a).

(2) (b) By statement (2) (a), $\mathrm{Aut}(G)$ is solvable. It follows that G, being an extension of the solvable group $\mathrm{Inn}(G)$ by the abelian group ζG, is also solvable. By assumption, all conjugacy classes in G are of one of the lengths 1, 2 or 3, and thus all element centralizers in G are of one of the indices 1, 2 or 3. It follows that the central quotient $G/\zeta G$ is a $\{2,3\}$-group. Since G is solvable, G has a Hall $\{2,3\}'$-subgroup $G_{\{2,3\}'}$, which must be central and thus normal (or, equivalently, unique). Moreover, G has a Hall $\{2,3\}$-subgroup $G_{\{2,3\}}$, which, being centralized by $G_{\{2,3\}'}$, is also normal, and so we have $G = G_{\{2,3\}} \times G_{\{2,3\}'}$. If $G_{\{2,3\}'}$ was nontrivial, it would follow by Lemma 3.1 (2) that

$$3 = \mathrm{maol}(G) \geqslant \mathrm{maol}(G_{\{2,3\}'}) \geqslant \phi(\mathrm{Exp}(G_{\{2,3\}'})) \geqslant 4,$$

a contradiction. Hence $G = G_{\{2,3\}}$, concluding our proof of statement (2) (b). □

Note that according to Theorem 1.1 (1), the only nonabelian finite group G with $\mathrm{maol}(G) = 3$ is $G = \mathrm{Sym}(3)$, for which the set of orders of inner automorphisms is $\{1,2,3\}$. It is precisely this property which we will show next for all nonabelian finite groups G with $\mathrm{maol}(G) = 3$.

Lemma 3.3.2. *Let G be a nonabelian finite group with* $\mathrm{maol}(G) = 3$. *Then the set of orders of inner automorphisms of G is* $\{1,2,3\}$ *(and hence the set of orders of all automorphisms of G is also* $\{1,2,3\}$*).*

Proof. The "and hence" follows from Lemma 3.3.1 (2) (a), so we focus on proving the main assertion. Note that by Lemma 3.3.1 (2) (a), the set of orders of inner automorphisms of G is contained in $\{1,2,3\}$, whence it suffices to show that $\mathrm{Exp}(\mathrm{Inn}(G))$ can neither be 2 nor 3. Assume otherwise. Then $\mathrm{Inn}(G) = G/\zeta G$ is of prime-power order, and thus G is nilpotent. Hence, by Lemma 3.3.1 (2) (b), we have $G = G_2 \times G_3$, where G_p denotes the Sylow p-subgroup of G for $p \in \{2,3\}$. By Lemma 3.1 (3), it follows that $3 = \mathrm{maol}(G) = \mathrm{maol}(G_2) \cdot \mathrm{maol}(G_3)$. Distinguish two cases.

Case (1): $\mathrm{maol}(G_2) = 3$ *and* $\mathrm{maol}(G_3) = 1$. Then by Proposition 3.1.1, G_3 is trivial, so G is a nonabelian 2-group with $\mathrm{maol}(G) = 3$. All non-central conjugacy classes in G are of length 2 and are $\mathrm{Aut}(G)$-orbits (otherwise, there would be an $\mathrm{Aut}(G)$-orbit of length at least $2 \cdot 2 = 4 > 3$). It follows that for any $\alpha \in \mathrm{Aut}(G)$, the subgroup

$$\mathrm{C}_G(\alpha^2) = \{g \in G \mid g^{\alpha^2} = g\}$$

contains the generating set $G \setminus \zeta G$, and thus $\mathrm{C}_G(\alpha^2) = G$. Therefore, $\alpha^2 = \mathrm{id}_G$, whence $\mathrm{Exp}(\mathrm{Aut}(G)) = 2$. However, we are assuming that $\mathrm{maol}(G) = 3$, and so by the orbit-stabilizer theorem, $3 \mid |\mathrm{Aut}(G)|$ so that $\mathrm{Aut}(G)$ contains an order 3 element by Cauchy's theorem, a contradiction.

Case (2): $\mathrm{maol}(G_2) = 1$ *and* $\mathrm{maol}(G_3) = 3$. Then by Proposition 3.1.1, G_2 is abelian, whence G_3 is a nonabelian 3-group with $\mathrm{maol}(G_3) = 3$. Observe that all non-central conjugacy classes in G_3 are of length 3 and are $\mathrm{Aut}(G_3)$-orbits. Since the Sylow 3-subgroup of $\mathrm{Sym}(3)$ is abelian, it follows that any two inner automorphisms of G_3 commute on $G_3 \setminus \zeta G_3$, and thus on G_3, so that $\mathrm{Inn}(G_3)$ is abelian, i.e., G_3 is nilpotent of class 2. We now list some more structural properties of G_3, in the spirit of Lemma 3.2.3 (2).

- ζG_3 is cyclic. Indeed, otherwise, a suitable non-central element of G_3 would have at least $|\mathrm{Hom}(\mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/3\mathbb{Z})^2)| = 9$ distinct images under central automorphisms of G_3, a contradiction.

- $|\zeta G_3| > 3$. Indeed, otherwise, G_3 would be an extraspecial 3-group. If we have $|G_3| = 3^{1+2}$, then either
  - $G = \langle a, b, c \mid a^3 = b^3 = c^3 = [a, b] = [a, c] = 1, b^c = ab\rangle$, and it is easy to check that each of the assignments $a \mapsto a$, $b \mapsto b$, $c \mapsto a^{k_1} b^{k_2} c$ with $k_1, k_2 \in \{0, 1, 2\}$ extends to an automorphism of G so that $\mathrm{maol}(G) \geqslant 9 > 3$, a contradiction, or
  - $G = \langle a, b \mid a^9 = b^3 = 1, a^b = a^4\rangle$, and it is easy to check that each of the assignments $a \mapsto a^k$, $b \mapsto b$ with $k \in \{1, \ldots, 9\}$ and $3 \nmid k$ extends to an automorphism of G so that $\mathrm{maol}(G) \geqslant \phi(9) = 6 > 3$, a contradiction.

  If $|G_3| = 3^{1+2n}$ with $n \geqslant 2$, then by [25, Theorem 1] (and the fact that the symplectic group $\mathrm{Sp}_{2n}(q) \leqslant \mathrm{GL}_{2n}(q)$ acts transitively on $\mathbb{F}_q^{2n} \setminus \{0\}$, which can be derived from Witt's theorem), $\mathrm{Aut}(G)$ has an orbit of length at least

  $$3^{2n-2} - 1 \geqslant 8 > 3$$

  on G, a contradiction.

- $G_3/\zeta G_3$ is an elementary abelian 3-group. Indeed, otherwise, a suitable noncentral element of G_3 would have at least $|\mathrm{End}(\mathbb{Z}/9\mathbb{Z})| = 9$ distinct images under central automorphisms of G_3, a contradiction.
- $G_3' \cong \mathbb{Z}/3\mathbb{Z}$. Since G_3 is nilpotent of class 2, $G_3' \leqslant \zeta G_3$, whence G_3' is cyclic. Moreover, since G_3 is nilpotent of class 2 (which implies $[x^e, y^f] = [x, y]^{ef}$ for all $x, y \in G_3$ and all $e, f \in \mathbb{Z}$) and $\mathrm{Exp}(G_3/\zeta G_3) = 3$, the exponent of G_3' must be 3 as well.
- G_3/G_3' is an elementary abelian 3-group. Indeed, otherwise, a suitable element of G_3 outside G_3' would have at least $|\mathrm{End}(\mathbb{Z}/9\mathbb{Z})| = 9$ distinct images under central automorphisms of G_3 (note that any homomorphism $f: G_3 \to \zeta G_3$ has the property that 1_{G_3} is the only element of ζG_3 mapped to its inverse by f since $\ker(f)$ contains G_3', which is a nontrivial subgroup of the cyclic 3-group ζG_3), a contradiction.

We can now repeat the "standard tuples" argument from the proof of Proposition 3.2.4 almost verbatim (only needing to replace the prime 2 by 3) and find that with $G_3/G_3' \cong (\mathbb{Z}/3\mathbb{Z})^d$, we necessarily have

$$3^d \geqslant \prod_{j=1}^{d} (3^j - 1),$$

which implies that $d = 1$ and thus $|G_3| = 3^2$, contradicting that G_3 is nonabelian. □

We are now ready to prove the main result of this subsection.

Proposition 3.3.3. *Let G be a finite group. The following are equivalent.*

(1) $\mathrm{maol}(G) = 3$.

(2) *G is isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^2$ *or to* $\mathrm{Sym}(3)$.

Proof. The implication "(2) ⇒ (1)" is easy, so we focus on proving "(1) ⇒ (2)". So, assume that G is a finite group with $\mathrm{maol}(G) = 3$. If G is abelian, then $G \cong (\mathbb{Z}/2\mathbb{Z})^2$ by Lemma 3.3.1 (1). We may thus assume that G is nonabelian and need to show that $G \cong \mathrm{Sym}(3)$.

By Lemma 3.3.2, the set of element orders of $\mathrm{Inn}(G)$ is $\{1, 2, 3\}$, and hence by [4, Theorem], $\mathrm{Inn}(G) \cong G/\zeta G$ is one of the following:

- the Frobenius group $(\mathbb{Z}/3\mathbb{Z})^d \rtimes \mathbb{Z}/2\mathbb{Z} = \mathrm{Dih}((\mathbb{Z}/3\mathbb{Z})^d)$ for some $d \in \mathbb{N}^+$,
- the Frobenius group $(\mathbb{Z}/2\mathbb{Z})^{2d} \rtimes \mathbb{Z}/3\mathbb{Z}$ for some $d \in \mathbb{N}^+$.

Note that the maximum conjugacy class length in $\mathrm{Inn}(G)$ cannot exceed the maximum conjugacy class length in G, which is at most 3. But in the Frobenius group $(\mathbb{Z}/2\mathbb{Z})^{2d} \rtimes \mathbb{Z}/3\mathbb{Z}$, the length of the conjugacy class of any generator of the Frobenius complement $\mathbb{Z}/3\mathbb{Z}$ is $2^{2d} \geqslant 4 > 3$. Hence $\mathrm{Inn}(G) \cong \mathrm{Dih}((\mathbb{Z}/3\mathbb{Z})^d)$, which has a conjugacy class of length 3^d, so that $d = 1$ and thus

$$G/\zeta G \cong \mathrm{Inn}(G) \cong \mathrm{Dih}(\mathbb{Z}/3\mathbb{Z}) \cong \mathrm{Sym}(3).$$

Next, we claim that ζG is a 3-group. Indeed, otherwise, by Lemma 3.3.1 (2) (b), there is an embedding $\mathbb{Z}/2\mathbb{Z} \overset{\iota}{\hookrightarrow} \zeta G$. Moreover, we have a finite sequence of group homomorphisms

$$G \overset{\text{can.}}{\twoheadrightarrow} G/\zeta G \overset{\sim}{\to} \mathrm{Sym}(3) \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z},$$

and through composition, we obtain a nontrivial homomorphism $G \overset{f}{\to} \zeta G$ with nontrivial associated central automorphism α_f. Now, let

$$g \in G \setminus \ker\bigl(G \overset{\text{can.}}{\twoheadrightarrow} G/\zeta G \overset{\sim}{\to} \mathrm{Sym}(3) \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z}\bigr).$$

Then the conjugacy class length of the image of g in $G/\zeta G \cong \mathrm{Sym}(3)$ is 3, whence g^G meets three distinct cosets of ζG in G. Moreover, g^{α_f} is an element in the same central coset as g, but distinct from g itself. It follows that $|g^G| \geqslant 2 \cdot 3 = 6 > 3$, a contradiction. This concludes our argument that ζG is a 3-group.

It now follows that G has a normal, abelian Sylow 3-subgroup G_3, and we have $G = G_3 \rtimes \mathbb{Z}/2\mathbb{Z}$, where the generator h of $\mathbb{Z}/2\mathbb{Z}$ centralizes the index 3 subgroup ζG of G_3. Let $g \in G_3 \setminus \zeta G$. Then, writing G_3 additively, we have $g^h = -g + z$ for some $z \in \zeta G$. It follows that

$$3g = (3g)^h = 3g^h = 3(-g + z) = -3g + 3z,$$

and thus $3(2g - z) = 0$. Through replacing g by $2g - z$, we may assume without loss of generality that $\mathrm{ord}(g) = 3$. Recall that $g^h = -g + z$ for some $z \in \zeta G$, and note that $\mathrm{ord}(z) \mid 3$ (otherwise, g^h would have order larger than $3 = \mathrm{ord}(g)$, a contradiction). Set $g' := g + z$. Then

$$(g')^h = g^h + z^h = -g + z + z = -g - z = -g'.$$

Hence, through replacing g by g', we may assume without loss of generality that $g^h = g^{-1}$. This entails that

$$G = G_3 \rtimes \mathbb{Z}/2\mathbb{Z} = (\zeta G \times \langle g\rangle) \rtimes \mathbb{Z}/2\mathbb{Z} = \zeta G \times (\langle g\rangle \rtimes \mathbb{Z}/2\mathbb{Z}) \cong \zeta G \times \mathrm{Sym}(3).$$

Therefore, if ζG is nontrivial, then by Lemma 3.1 (2),

$$\mathrm{maol}(\zeta G) \geqslant \phi(\mathrm{Exp}(\zeta G)) \geqslant \phi(3) = 2,$$

and thus, by Lemma 3.1 (1),

$$3 = \mathrm{maol}(G) \geqslant \mathrm{maol}(\zeta G) \cdot \mathrm{maol}(\mathrm{Sym}(3)) \geqslant 2 \cdot 3 = 6,$$

a contradiction. Hence ζG is trivial, so $G \cong \mathrm{Sym}(3)$, as we needed to show. □

3.4 Proof of Theorem 1.1 (1)

This is immediate from Propositions 3.1.1, 3.2.4 and 3.3.3.

4 Finite groups G with $\mathrm{maol}(G) = 8$

This section is concerned with the proof of Theorem 1.1 (2). We begin by introducing a certain infinite sequence of finite 2-groups.

Definition 4.1. For $n \in \mathbb{N}^+$, let G_n be the finite 2-group given by the power-commutator presentation

$$\begin{aligned}\langle x_1, \ldots, x_{2^n+1}, a, b \mid\ & [a,b] = [x_i, a] = [x_i, b] = 1, \\ & [x_{2i-1}, x_{2i}] = a,\ [x_{2i}, x_{2i+1}] = b, \\ & [x_i, x_j] = 1 \text{ if } |i-j| > 1,\ x_1^2 = x_{2^n+1}^2 = b, \\ & a^2 = b^2 = x_i^2 = 1 \text{ if } 1 < i < 2^n + 1\rangle.\end{aligned}$$

Remark 4.2. We note the following concerning Definition 4.1.

(1) As is easy to check, G_n is a finite 2-group of order 2^{2^n+3}, of nilpotency class 2 and of exponent 4. Moreover, $C_n := \zeta G_n = \langle a, b\rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$ and $Q_n := G_n / C_n \cong (\mathbb{Z}/2\mathbb{Z})^{2^n+1}$.

(2) The specified power-commutator presentation of G_n is inspired by the presentation of the infinite 2-group

$$\begin{aligned}\langle a, b, x_1, x_2, \ldots \mid\ & [a,b] = [x_i, a] = [x_i, b] = 1, \\ & [x_{2i-1}, x_{2i}] = a,\ [x_{2i}, x_{2i+1}] = b, \\ & [x_i, x_j] = 1 \text{ if } |i-j| > 1,\ x_1^2 = b, \\ & a^2 = b^2 = x_i^2 = 1 \text{ if } i > 1\rangle,\end{aligned}$$

which was given by Robinson and Wiegold as an example of a group with infinite automorphism group but largest automorphism orbit length 4, see [20, Section 4, construction before Proposition 3, Proposition 3 itself and the remark after the proof of Proposition 3].

(3) The assignment $a \mapsto a$, $b \mapsto b$, $x_i \mapsto x_i$ for $i \neq 2^n$ and $x_{2^n} \mapsto x_{2^n} x_{2^n+1}$ extends to a non-central automorphism α_n of G_n.

We prove Theorem 1.1 (2) by proving the following proposition.

Proposition 4.3. *For all $n \in \mathbb{N}^+$, we have $|\mathrm{Aut}(G_n) : \mathrm{Aut}_{\mathrm{cent}}(G_n)| = 2$. In particular,* $\mathrm{maol}(G_n) = 8$.

Proof. The "in particular" follows from the observations that $\mathrm{Aut}_{\mathrm{cent}}(G_n)$ acts transitively on each nontrivial coset of C_n and that $|C_n| = 4$ (see Remark 4.2 (1)). As for the main assertion, we will show that every automorphism of G_n lies in the coset union $\mathrm{Aut}_{\mathrm{cent}}(G_n) \cup \mathrm{Aut}_{\mathrm{cent}}(G_n)\alpha_n$, with α_n as in Remark 4.2 (3). We do so in several steps, in each of which we first make a claim, which is subsequently proved.

Claim 1. *Let $g \in G_n$, and assume that* $\mathrm{ord}(g) = 4$ *and* $|G_n : \mathrm{C}_{G_n}(g)| = 2$.

(1) *If there is no $h \in G_n$ with $g^2 = [g, h]$, then $g \in x_1 C_n$.*

(2) *If there is an $h \in G_n$ with $g^2 = [g, h]$, then $g \in x_{2^n+1} C_n$.*

In particular, the two subgroups $\langle x_1, C_n \rangle$ and $\langle x_{2^n+1}, C_n \rangle$ are characteristic in G_n.

Write $g \equiv x_1^{u_1} \cdots x_k^{u_k} \pmod{C_n}$, where $u_i \in \mathbb{Z}/2\mathbb{Z}$ and $u_k \neq 0$. If $k = 1$, then both asserted implications are true; the former because its necessary condition is true, and the latter because its sufficient condition is false ($g^2 = x_1^2 = b$, but $[g, G_n] = [x_1, G_n] = \{1, a\}$). So assume henceforth that $k > 1$. We make a case distinction.

Case (1): $k < 2^n + 1$. This case plays out analogously to the proof of statement (i) in [20, proof of Proposition 3], but we will give the argument here for completeness and the reader's convenience. If $h \in \mathrm{C}_{G_n}(g)$, then modulo elements known to commute with g, we can write $h = x_1^{v_1} \cdots x_{k+1}^{v_{k+1}}$ with $v_i \in \mathbb{Z}/2\mathbb{Z}$. Then the assumption that $1 = [g, h]$ yields

$$1 = [x_1, x_2]^{u_1 v_2 + u_2 v_1} [x_2, x_3]^{u_2 v_3 + u_3 v_2} \cdots \\ [x_{k-1}, x_k]^{u_{k-1} v_k + u_k v_{k-1}} [x_k, x_{k+1}]^{u_k v_{k+1}}. \tag{4.1}$$

Now use the commutator relations to equivalently rewrite formula (4.1) into a pair of linear equations over $\mathbb{F}_2$ in the variables $v_1, \ldots, v_{k+1}$. The final terms of these equations look as follows:

$$\cdots + u_k v_{k-1} + u_{k-1} v_k = 0,$$
$$\cdots + u_k v_{k+1} = 0.$$

Since $u_k \neq 0$ by assumption and v_{k+1} does not occur in the first equation, the two equations are $\mathbb{F}_2$-linearly independent, which implies $|G_n : \mathrm{C}_{G_n}(g)| = 2^2 = 4 > 2$, a contradiction.

Case (2): $k = 2^n + 1$. If $h \in \mathrm{C}_{G_n}(g)$, then modulo elements known to commute with g (namely a and b), we can write $h = x_1^{v_1} \cdots x_{2^n+1}^{v_{2^n+1}}$ with $v_i \in \mathbb{Z}/2\mathbb{Z}$. The assumption that $1 = [g, h]$ yields

$$1 = [x_1, x_2]^{u_1 v_2 + u_2 v_1} [x_2, x_3]^{u_2 v_3 + u_3 v_2} \cdots [x_{2^n}, x_{2^n+1}]^{u_{2^n} v_{2^n+1} + u_{2^n+1} v_{2^n}}. \tag{4.2}$$

Using the commutator relations, we can equivalently rewrite formula (4.2) into the following pair of linear equations over $\mathbb{F}_2$ in the variables $v_1, \ldots, v_{2^n+1}$:

$$u_2 v_1 + u_1 v_2 + u_4 v_3 + u_3 v_4 + \cdots + u_{2^n} v_{2^n-1} + u_{2^n-1} v_{2^n} = 0,$$
$$u_3 v_2 + u_2 v_3 + u_5 v_4 + u_4 v_5 + \cdots + u_{2^n-2} v_{2^n-1} + u_{2^n+1} v_{2^n} + u_{2^n} v_{2^n+1} = 0.$$

We make a subcase distinction.

Subcase (a): *at least one of* $u_1, u_2, \ldots, u_{2^n}$ *is nonzero.* Then since $u_{2^n+1} \neq 0$ by assumption, both equations are nonzero, and since $|G_n : \mathrm{C}_{G_n}(g)| = 2$, they must be $\mathbb{F}_2$-linearly dependent, which implies that $u_2 = u_4 = \cdots = u_{2^n} = 0$ and $u_1 = u_3 = \cdots = u_{2^n+1} = 1$. We conclude that

$$g \equiv x_1 x_3 \cdots x_{2^n+1} \pmod{C_n},$$

whence $g^2 = x_1^2 x_3^2 \cdots x_{2^n+1}^2 = b \cdot 1 \cdots 1 \cdot b = b^2 = 1$, contradicting our assumption that $\mathrm{ord}(g) = 4$.

Subcase (b): $u_1 = u_2 = \cdots = u_{2^n} = 0$. Then $g \equiv x_{2^n+1} \pmod{C_n}$. Similarly to the argument for $k = 1$ above, we find that both asserted implications are true; the former because its sufficient condition is false,

$$g^2 = x_{2^n+1}^2 = b = [x_{2^n}, x_{2^n+1}] = [x_{2^n}, g],$$

and the latter because its necessary condition is true.

Claim 2. *Each of the three central order* 2 *subgroups* $\langle a \rangle$, $\langle b \rangle$ *and* $\langle ab \rangle$ *is characteristic in* G_n.

Indeed, we have that

- $\langle a \rangle = [\langle x_1, C_n \rangle, G_n]$,
- $\langle b \rangle = \mho^1(\langle x_1, C_n \rangle) = \langle \{ g^2 \mid g \in \langle x_1, C_n \rangle \} \rangle$,
- $\langle ab \rangle = \langle C_n \setminus (\langle a \rangle \cup \langle b \rangle) \rangle$.

Claim 3. *For each* $m \in \{0, \dots, 2^{n-1}\}$*, the subgroup* $\langle C_n, x_1, x_3, \dots, x_{2m+1} \rangle$ *is characteristic in* G_n.

We proceed by induction on m. The induction base, $m = 0$, is clear by Claim 1. So assume that $m \geqslant 1$, and that $\langle C_n, x_1, x_3, \dots, x_{2m-1} \rangle$ is characteristic in G_n. Note that if $m = 2^{n-1}$, then we are done by Claim 1 as

$$\begin{aligned}\langle C_n, x_1, x_3, \dots, x_{2m+1} \rangle &= \langle \langle C_n, x_1, x_3, \dots, x_{2m-1} \rangle, \langle C_n, x_{2m+1} \rangle \rangle \\ &= \langle \langle C_n, x_1, x_3, \dots, x_{2m-1} \rangle, \langle C_n, x_{2^n+1} \rangle \rangle.\end{aligned}$$

We may thus also assume that $m < 2^{n-1}$. Set

$$\begin{aligned}H_m &:= \mathrm{C}_{G_n}(\langle C_n, x_1, x_3, \dots, x_{2m-1} \rangle) \\ &= \langle C_n, x_1, x_3, \dots, x_{2m-1}, x_{2m+1}, x_{2m+2}, \dots, x_{2^n+1} \rangle.\end{aligned}$$

Note that by the induction hypothesis, H_m is characteristic in G_n and

$$\zeta H_m = \langle C_n, x_1, x_3, \dots, x_{2m-1} \rangle.$$

We will show the following claim: "if $g \in H_m$, $[g, H_m] = \langle a \rangle$, $|H_m : \mathrm{C}_{H_m}(g)| = 2$, then $g \in x_{2m+1} \zeta H_m$."

Note that since

$$\langle C_n, x_1, x_3, \dots, x_{2m+1} \rangle = \langle \zeta H_m, x_{2m+1} \zeta H_m \rangle,$$

once this claim is proved, our inductive proof of Claim 3 is complete.

The proof of the claim is similar to the argument for Claim 1. Write

$$g \equiv x_{2m+1}^{u_{2m+1}} \cdots x_k^{u_k} \pmod{\zeta H_m}$$

with $u_i \in \mathbb{Z}/2\mathbb{Z}$ and $u_k \neq 0$. Note that if $k = 2m + 1$, then the asserted implication is true because its necessary condition is true. So we may assume that $k > 2m + 1$. We make a case distinction.

Case (1): $k < 2^n + 1$. If $h \in \mathrm{C}_{H_m}(g)$, then modulo elements known to commute with g, we can write $h = x_{2m+1}^{v_{2m+1}} \cdots x_{k+1}^{v_{k+1}}$ with $v_i \in \mathbb{Z}/2\mathbb{Z}$. Our assumption that $1 = [g, h]$ yields

$$\begin{aligned}1 = [x_{2m+1}, x_{2m+2}]^{u_{2m+1}v_{2m+2}+u_{2m+2}v_{2m+1}} \dots \\ [x_{k-1}, x_k]^{u_{k-1}v_k+u_k v_{k-1}} [x_k, x_{k+1}]^{u_k v_{k+1}}.\end{aligned} \tag{4.3}$$

Using the commutator relations, we can equivalently rewrite formula (4.3) into a pair of linear equations over $\mathbb{F}_2$, which look like this:

$$\begin{aligned}\dots + u_k v_{k-1} + u_{k-1} v_k &= 0, \\ \dots + u_k v_{k+1} &= 0.\end{aligned}$$

Since $u_k \neq 0$, these two equations are $\mathbb{F}_2$-linearly independent, which implies that $|H_m : \mathrm{C}_{H_m}(g)| = 2^2 = 4 > 2$, a contradiction.

Case (2): $k = 2^n + 1$. If $h \in \mathrm{C}_{H_m}(g)$, then modulo elements known to commute with g, we can write $h = x_{2m+1}^{v_{2m+1}} \cdots x_{2^n+1}^{v_{2^n+1}}$ with $v_i \in \mathbb{Z}/2\mathbb{Z}$. Our assumption that $1 = [g, h]$ yields

$$\begin{aligned} 1 = [x_{2m+1}, x_{2m+2}]^{u_{2m+1}v_{2m+2}+u_{2m+2}v_{2m+1}} \cdots \\ [x_{2^n}, x_{2^n+1}]^{u_{2^n}v_{2^n+1}+u_{2^n+1}v_{2^n}}. \end{aligned} \tag{4.4}$$

Using the commutator relations, we can equivalently rewrite formula (4.4) into the following pair of linear equations over $\mathbb{F}_2$:

$$\begin{aligned} &u_{2m+2}v_{2m+1} + u_{2m+1}v_{2m+2} + u_{2m+4}v_{2m+3} + \cdots \\ &\qquad + u_{2^n}v_{2^n-1} + u_{2^n-1}v_{2^n} = 0, \\ &u_{2m+3}v_{2m+2} + u_{2m+2}v_{2m+3} + \cdots \\ &\qquad + u_{2^n-2}v_{2^n-1} + u_{2^n+1}v_{2^n} + u_{2^n}v_{2^n+1} = 0. \end{aligned}$$

We make a subcase distinction.

Subcase (a): *at least one of* $u_{2m+1}, \ldots, u_{2^n}$ *is nonzero.* Then since $u_{2^n+1} \neq 0$ by assumption, both equations are nonzero, and since $|H_m : \mathrm{C}_{H_m}(g)| = 2$, the equations must be $\mathbb{F}_2$-linearly dependent. It follows that

$$\begin{aligned} u_{2m+2} = u_{2m+4} = \cdots = u_{2^n} = 0, \\ u_{2m+1} = u_{2m+3} = \cdots = u_{2^n+1} = 1. \end{aligned}$$

Hence

$$g \equiv x_{2m+1}x_{2m+3}\cdots x_{2^n+1} \pmod{\zeta H_m},$$

and therefore

$$[g, x_{2m+2}] = [x_{2m+1}, x_{2m+2}] \cdot [x_{2m+2}, x_{2m+3}] = a \cdot b \neq a,$$

contradicting our assumption that $[g, H_m] = \langle a \rangle$.

Subcase (b): $u_{2m+1} = u_{2m+2} = \cdots = u_{2^n} = 0$. Then $g \equiv x_{2^n+1} \pmod{\zeta H_m}$, and thus

$$[g, H_m] = \langle [x_{2^n}, x_{2^n+1}] \rangle = \langle b \rangle,$$

contradicting our assumption that $[g, H_m] = \langle a \rangle$.

In what follows, α is an arbitrary automorphism of G_n. We can write

$$x_i^{\alpha} = x_1^{\alpha_{i,1}} x_2^{\alpha_{i,2}} \cdots x_{2^n+1}^{\alpha_{i,2^n+1}} \pmod{C_n} \quad \text{for } i \in \{1, 2, \ldots, 2^n + 1\},$$

with $\alpha_{i,j} \in \mathbb{Z}/2\mathbb{Z}$.

Claim 4. *The following hold.*

(1) $\alpha_{1,1} = 1$, *and* $\alpha_{1,j} = 0$ *for* $j > 1$.

(2) $\alpha_{2^n+1,2^n+1} = 1$, *and* $\alpha_{2^n+1,j} = 0$ *for* $j < 2^n + 1$.

(3) *For* $i \in \{1, \ldots, 2^{n-1} - 1\}$ *and* $j \in \{1, \ldots, 2^{n-1}\}$*:*

  (a) $\alpha_{2i+1,2j} = 0$*;*

  (b) *if* $j > i$, *then* $\alpha_{2i+1,2j+1} = 0$*;*

  (c) $\alpha_{2i+1,1} = 0$, *and* $\alpha_{2i+1,2i+1} = 1$.

Indeed, statements (1) and (2) are clear by Claim 1. Moreover, statements (3) (a) and (b) are clear by Claim 3. As for statement (3) (c), note that if $\alpha_{2i+1,1} = 1$, then $\mathrm{ord}(x_{2i+1}^{\alpha}) = 4$, a contradiction. Finally, $\alpha_{2i+1,2i+1} = 1$ since otherwise, by Claim 3,

$$x_{2i+1}^{\alpha} \in \langle C_n, x_1, x_3, \ldots, x_{2i-1} \rangle,$$

which contradicts the fact that $\langle C_n, x_1, x_3, \ldots, x_{2i-1} \rangle$ is characteristic in G_n.

Claim 5. *For each* $i \in \{1, \ldots, 2^{n-1} + 1\}$, *we have the following.*

(1) *The subgroup* $\langle x_{2i-1}, C_n \rangle$ *is characteristic in* G_n.

(2) *For* $j = 1, 2, \ldots, i - 1$, *we have*

  (a) $\alpha_{2j,2j} = 1$,

  (b) $x_{2j}^{\alpha} x_{2j}^{-1} \equiv x_1^{\alpha_{2j,1}} x_3^{\alpha_{2j,3}} \cdots x_{2i-1}^{\alpha_{2j,2i-1}} x_{2i}^{\alpha_{2j,2i}} \cdots x_{2^n+1}^{\alpha_{2j,2^n+1}} \pmod{C_n}$.

This is analogous to the proof of statement (iv) in [20, proof of Proposition 3], but we will give the argument in detail here, for the reader's convenience and to make sure it is not a problem that (in contrast to the situation in [20, proof of Proposition 3]) we do not know at this point whether $x_{2j,1} = 0$.

We proceed by induction on i. The case "$i = 1$" is clear by Claim 1, and the case "$i = 2$" is clear by Claim 4 (3) and the observation that if $\alpha_{2,2} = 0$, then $x_2^{\alpha} \in \mathrm{C}_{G_n}(\langle x_1, C_n \rangle)$, which contradicts the fact that $\mathrm{C}_{G_n}(\langle x_1, C_n \rangle)$ is characteristic in G_n.

We may thus assume that $i \geqslant 2$, and that the assertion has been proved for i. Let $j \in \{1, 2, \dots, i-1\}$. Then by the induction hypothesis,

$$x_{2j}^{\alpha} \equiv x_{2j} \cdot x_1^{\alpha_{2j,1}} x_3^{\alpha_{2j,3}} \cdots x_{2i-1}^{\alpha_{2j,2i-1}} x_{2i}^{\alpha_{2j,2i}} \cdots x_{2^n+1}^{\alpha_{2j,2^n+1}} \pmod{C_n},$$
$$x_{2i-1}^{\alpha} \equiv x_{2i-1} \pmod{C_n}.$$

Hence if $j < i-1$, it follows from $1 = [x_{2j}, x_{2i-1}]$ that

$$1 = [x_{2i-1}, x_{2i}]^{\alpha_{2j,2i}} = a^{\alpha_{2j,2i}},$$

and thus $\alpha_{2j,2i} = 0$. And if $j = i-1$, it follows from

$$b = [x_{2i-2}, x_{2i-1}] = [x_{2j}, x_{2i-1}]$$

that

$$b = [x_{2i-2}, x_{2i-1}] \cdot [x_{2i-1}, x_{2i}]^{\alpha_{2j,2i}} = b \cdot a^{\alpha_{2j,2i}},$$

whence, again, $\alpha_{2j,2i} = 0$. We just showed that

$$\alpha_{2j,2i} = 0 \quad \text{for } j = 1, 2, \dots, i-1. \tag{4.5}$$

Now, by the induction hypothesis and formula (4.5), we have

$$x_{2j}^{\alpha} \equiv x_{2j} \cdot x_1^{\alpha_{2j,1}} x_3^{\alpha_{2j,3}} \cdots x_{2i+1}^{\alpha_{2j,2i+1}} x_{2i+2}^{\alpha_{2j,2i+2}} \cdots x_{2^n+1}^{\alpha_{2j,2^n+1}} \pmod{C_n},$$
$$x_{2i+1}^{\alpha} \equiv x_3^{\alpha_{2i+1,3}} x_5^{\alpha_{2i+1,5}} \cdots x_{2i+1}^{\alpha_{2i+1,2i+1}} \pmod{C_n}.$$

It follows from $1 = [x_{2j}, x_{2i+1}]$ that

$$\begin{aligned} 1 &= [x_{2j-1}, x_{2j}]^{\alpha_{2i+1,2j-1}} [x_{2j}, x_{2j+1}]^{\alpha_{2i+1,2j+1}} \\ &\quad [x_{2i+1}, x_{2i+2}]^{\alpha_{2j,2i+2}\alpha_{2i+1,2i+1}} \\ &= a^{\alpha_{2i+1,2j-1}+\alpha_{2j,2i+2}\alpha_{2i+1,2i+1}} b^{\alpha_{2i+1,2j+1}}, \end{aligned}$$

which implies that $\alpha_{2i+1,2j+1} = 0$. We just showed that

$$\alpha_{2i+1,2j+1} = 0 \quad \text{for } j = 1, 2, \dots, i-1. \tag{4.6}$$

Together with Claim 4 (3), formula (4.6) implies that $\langle x_{2i+1}, C_n \rangle$ is characteristic in G_n. Finally, by definition,

$$x_{2i}^{\alpha} \equiv x_1^{\alpha_{2i,1}} x_2^{\alpha_{2i,2}} \cdots x_{2^n+1}^{\alpha_{2i,2^n+1}} \pmod{C_n},$$

and by the induction hypothesis,

$$x_{2j+1}^{\alpha} \equiv x_{2j+1} \pmod{C_n}.$$

If $j < i-1$, then it follows from $1 = [x_{2i}, x_{2j+1}]$ that

$$1 = [x_{2j}, x_{2j+1}]^{\alpha_{2i,2j}} [x_{2j+1}, x_{2j+2}]^{\alpha_{2i,2j+2}} = b^{\alpha_{2i,2j}} a^{\alpha_{2i,2j+2}},$$

whence $\alpha_{2i,2j} = \alpha_{2i,2j+2} = 0$. This shows that

$$\alpha_{2i,2j} = 0 \quad \text{for } j = 1, \dots, i-1. \tag{4.7}$$

To complete the inductive proof of Claim 5, it remains to show that $\alpha_{2i,2i} = 1$. Assume otherwise. Then by formula (4.7), $x_{2i}^{\alpha} \in \mathrm{C}_{G_n}(\langle C_n, x_1, x_3, \dots, x_{2i-1}\rangle)$, which contradicts that $\mathrm{C}_{G_n}(\langle C_n, x_1, x_3, \dots, x_{2i-1}\rangle)$ is characteristic in G_n.

Claim 6. *For all $i, j \in \{1, 2, \dots, 2^{n-1}\}$, we have*

$$\alpha_{2i,2j} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise}. \end{cases}$$

In other words,

$$x_{2i}^{\alpha} \equiv x_{2i} \cdot x_1^{\alpha_{2i,1}} x_3^{\alpha_{2i,3}} \cdots x_{2^n+1}^{\alpha_{2i,2^n+1}} \pmod{C_n}.$$

This is immediate from Claim 5 with $i = 2^{n-1}+1$. Note that by Claims 5 and 6, we now know that modulo C_n, α fixes each of $x_1, x_3, \dots, x_{2^n+1}$, and maps each of $x_2, x_4, \dots, x_{2^n}$ to itself times some product of $x_1, x_3, \dots, x_{2^n+1}$. The next claim gives some restrictions on these odd-index factors.

Claim 7. *Let $i, j \in \{1, 2, \dots, 2^{n-1}\}$. Then the following hold.*

(1) $\alpha_{2i,2i-1} = 0$.

(2) $\alpha_{2j,2i-1} = \alpha_{2i,2j-1}$ *and* $\alpha_{2j,2i+1} = \alpha_{2i,2j+1}$.

Indeed, for statement (1), observe that if $\alpha_{2i,2i-1} = 1$, then

$$x_{2i}^{\alpha} \equiv x_{2i} \cdot x_1^{\alpha_{2i,1}} x_3^{\alpha_{2i,3}} \cdots x_{2i-3}^{\alpha_{2i,2i-3}} x_{2i-1} x_{2i+1}^{\alpha_{2i,2i+1}} \cdots x_{2^n+1}^{\alpha_{2i,2^n+1}} \pmod{C_n}$$

and thus

$$\begin{aligned}(x_{2i}^{\alpha})^2 &= [x_{2i-1}, x_{2i}] \cdot [x_{2i}, x_{2i+1}]^{\alpha_{2i,2i+1}} \cdot x_{2i}^2 \cdot \prod_{k=1}^{2^{n-1}} x_{2k+1}^{2\alpha_{2i,2k+1}} \\ &= a \cdot b^{\alpha_{2i,2i+1}} \cdot b^{\alpha_{2i,1}+\alpha_{2i,2^n+1}} \neq 1,\end{aligned}$$

which contradicts the fact that $\mathrm{ord}(x_{2i}) = 2$.

For statement (2), note that

$$x_{2i}^{\alpha} \equiv x_{2i} \cdot x_1^{\alpha_{2i,1}} x_3^{\alpha_{2i,3}} \cdots x_{2i-3}^{\alpha_{2i,2i-3}} x_{2i+1}^{\alpha_{2i,2i+1}} x_{2i+3}^{\alpha_{2i,2i+3}} \cdots x_{2^n+1}^{\alpha_{2i,2^n+1}} \pmod{C_n},$$
$$x_{2j}^{\alpha} \equiv x_{2j} \cdot x_1^{\alpha_{2j,1}} x_3^{\alpha_{2j,3}} \cdots x_{2j-3}^{\alpha_{2j,2j-3}} x_{2j+1}^{\alpha_{2j,2j+1}} x_{2j+3}^{\alpha_{2j,2j+3}} \cdots x_{2^n+1}^{\alpha_{2j,2^n+1}} \pmod{C_n}.$$

It follows from $1 = [x_{2i}, x_{2j}]$ that

$$\begin{aligned} 1 &= [x_{2i-1}, x_{2i}]^{\alpha_{2j,2i-1}} [x_{2i}, x_{2i+1}]^{\alpha_{2j,2i+1}} \\ &\qquad [x_{2j-1}, x_{2j}]^{\alpha_{2i,2j-1}} [x_{2j}, x_{2j+1}]^{\alpha_{2i,2j+1}} \\ &= a^{\alpha_{2j,2i-1}+\alpha_{2i,2j-1}} \cdot b^{\alpha_{2j,2i+1}+\alpha_{2i,2j+1}}, \end{aligned}$$

whence indeed, $\alpha_{2j,2i-1} = \alpha_{2i,2j-1}$ and $\alpha_{2j,2i+1} = \alpha_{2i,2j+1}$, as required.

Claim 8. *The following hold.*

(1) *For each $i \in \{1, 2, \ldots, 2^{n-1} - 1\}$, the subgroup $\langle x_{2i}, C_n \rangle$ is characteristic in G_n.*

(2) *The coset union $x_{2^n} C_n \cup x_{2^n} x_{2^n+1} C_n$ is a characteristic subset of G_n.*

Note that by Claim 7 (2), if $\alpha_{2k,2l-1} = 0$ for some $k \in \{1, 2, \ldots, 2^{n-1}\}$ and some $l \in \{1, 2, \ldots, 2^{n-1} + 1\}$, then we can actually conclude that $\alpha_{e,o} = 0$ for all pairs $(e, o) \in \{1, 2, \ldots, 2^n + 1\}^2$ where e is even, o is odd, $e + o = 2k + 2l - 1$. This is because

$$\begin{aligned} \alpha_{2k,2l-1} &= \alpha_{2l,2k-1} = \alpha_{2k-2,2l+1} \\ &\qquad \text{if } 2k-2, 2l+1 \in \{1, \ldots, 2^n + 1\}, \\ \alpha_{2k,2l-1} &= \alpha_{2l-2,2k+1} = \alpha_{2k+2,2l-3} \\ &\qquad \text{if } 2l-3, 2k+2 \in \{1, 2, \ldots, 2^n + 1\}. \end{aligned}$$

Therefore, by Claim 7 (1), we conclude that $\alpha_{e,o} = 0$ whenever $e + o \equiv 3 \pmod 4$. We claim that more generally, for each $k = 2, 3, \ldots, n+1$, $\alpha_{e,o} = 0$ whenever $e + o \equiv 1 + 2^{k-1} \pmod{2^k}$. We will show this by induction on k, with the induction base, $k = 2$, done just above. So assume now that $k \leqslant n$, and that we know that $\alpha_{e,o} = 0$ whenever $e + o \equiv 1 + 2^{k-1} \pmod{2^k}$. Then, in particular, $\alpha_{\epsilon,1} = \alpha_{\epsilon,2^n+1} = 0$ whenever $\epsilon \in \{1, 2 \ldots, 2^n + 1\}$ and $\epsilon \equiv 2^{k-1} \pmod{2^k}$. If $\alpha_{\epsilon,\epsilon+1} = 1$, it follows (in view of Claims 6 and 7 (1)) that

$$(x_\epsilon^\alpha)^2 = [x_\epsilon, x_{\epsilon+1}] = b \neq 1,$$

a contradiction. Hence $\alpha_{\epsilon,\epsilon+1} = 0$ for all

$$\epsilon \in \{1, 2, \ldots, 2^n + 1\} \quad \text{with } \epsilon \equiv 2^{k-1} \pmod{2^k},$$

and thus $\alpha_{e,o} = 0$ for all pairs $(e, o) \in \{1, 2, \ldots, 2^n + 1\}^2$, where e is even, o is odd and $e + o \equiv 1 + 2^k \pmod{2^{k+1}}$, as we wanted to show.

An equivalent reformulation of what we just proved by induction on k is that $\alpha_{e,o} = 0$ for all pairs $(e, o) \in \{1, 2, \ldots, 2^n + 1\}^2$, where e is even and o is odd *unless* $e + o \equiv 1 \pmod{2^{n+1}}$, i.e., unless $(e, o) = (2^n, 2^n + 1)$. Together with Claim 6, this proves Claim 8.

We can now conclude the proof of Proposition 4.3 as follows: By Claims 5 and 8, we have that modulo $\mathrm{Aut}_{\mathrm{cent}}(G_n)$, every automorphism of G_n either fixes all generators of G_n, or it maps $x_{2^n} \mapsto x_{2^n} x_{2^n+1}$ while fixing all the other generators of G_n. In other words, modulo $\mathrm{Aut}_{\mathrm{cent}}(G_n)$, every automorphism of G_n is equal to id_{G_n} or α_n as defined in Remark 4.2 (3), which is just what we wanted to show (see the beginning of this proof). □

5 Finite groups G with both maol(G) and $d(G)$ bounded

This section is concerned with the proof of Theorem 1.1 (3). Recall from Subsection 2.1 that $d(G)$ denotes the minimum size of a generating subset of the finite group G. We note that if G is any finite group with $\mathrm{maol}(G) \leqslant c$, then in particular, all conjugacy classes of G are of length at most c, and so if $d(G) \leqslant d$, then the center ζG, being the intersection of the centralizers of the elements of any fixed generating subset of G, has index at most c^d in G. Hence an upper bound on $|G|$ could be derived from an explicit version of Robinson and Wiegold's theorem [20, Theorem 1], more precisely from an explicit upper bound on $|\zeta G|$ for all finite groups G with $\mathrm{maol}(G) \leqslant c$. As noted in [20, Remark (i) at the end of Section 1], the proof of [20, Theorem 1] actually provides such an explicit upper bound, but it is complicated and was not worked out explicitly by Robinson and Wiegold.

Rather than proving our Theorem 1.1 (3) by making Robinson and Wiegold's result explicit, we will exploit the fact that a related, celebrated result of B. H. Neumann (which motivated Robinson and Wiegold's paper) has known explicit versions. This also means that modulo known, explicitly spelled out results, our proof will be elementary (the Robinson–Wiegold proof uses cohomological methods).

A *BFC-group* is a group G such that the maximum conjugacy class length in G is bounded from above by some constant. The above mentioned theorem of B. H. Neumann states that a group G is a BFC-group if and only if the commutator subgroup G' is finite (see [18, Theorem 3.1]). Later, an explicit version of Neumann's theorem was proved by Wiegold [24, Theorem 4.7], stating that if G is a group in which all conjugacy classes are of length at most ℓ, then the order of G' is at most $f(\ell)$ for some explicit function f. The currently best known choice for f is the one from the following theorem.

Theorem 5.1 (Guralnick–Maróti, [11, Theorem 1.9]). *Let ℓ be a positive integer, and let G be a group such that all conjugacy classes of G are of length at most ℓ. Then*

$$|G'| \leqslant \ell^{\frac{1}{2}(7+\frac{\log \ell}{\log 2})}.$$

In our proof of Theorem 1.1 (3), we will also need some simple lower bounds on the number of automorphisms of a finite abelian p-group P, which can be derived from the following exact formula for $|\mathrm{Aut}(P)|$.

Theorem 5.2 (Hillar–Rhea, [12, Theorem 4.1]). *Let p be a prime, and let P be a finite abelian p-group. Write*

$$P \cong \mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_n}\mathbb{Z} \quad \textit{with } 1 \leqslant e_1 \leqslant \cdots \leqslant e_n.$$

For $k = 1, \dots, n$, set

$$d_k := \max\{l \in \{1, \dots, n\} \mid e_l = e_k\},$$
$$c_k := \min\{l \in \{1, \dots, n\} \mid e_l = e_k\}.$$

Then

$$|\mathrm{Aut}(P)| = \prod_{k=1}^{n} (p^{d_k} - p^{k-1}) \cdot \prod_{j=1}^{n} p^{e_j(n-d_j)} \prod_{i=1}^{n} p^{(e_i-1)(n-c_i+1)}.$$

Corollary 5.3. *With notation as in Theorem* 5.2*, and assuming that P is nontrivial, we have* $|\mathrm{Aut}(P)| \geqslant \max\{p-1, p^{e_n-1}\}$.

Proof. Note that by definition, $d_1 \geqslant 1$ and $c_n \leqslant n$. It follows that

$$\begin{aligned}
|\mathrm{Aut}(P)| &= (p^{d_1} - 1) \cdot \prod_{k=2}^{n} (p^{d_k} - p^{k-1}) \\
&\quad \cdot \prod_{j=1}^{n} p^{e_j(n-d_j)} \prod_{i=1}^{n} p^{(e_i-1)(n-c_i+1)} \\
&\geqslant p - 1, \\
|\mathrm{Aut}(P)| &= \prod_{k=1}^{n} (p^{d_k} - p^{k-1}) \\
&\quad \cdot \prod_{j=1}^{n} p^{e_j(n-d_j)} \prod_{i=1}^{n-1} p^{(e_i-1)(n-c_i+1)} \cdot p^{(e_n-1)(n-c_n+1)} \\
&\geqslant 1 \cdot p^{(e_n-1)(n-c_n+1)} \geqslant p^{(e_n-1)(n-n+1)} = p^{e_n-1},
\end{aligned}$$

as required. □

Furthermore, we will make use of the following upper bound on the first Chebyshev function.

Theorem 5.4 (Rosser–Schoenfeld, [21, Theorem 9]). *Let*

$$\vartheta\colon [0,\infty) \to [0,\infty),\ x \mapsto \sum_{p \leqslant x} \log p,$$

where the summation index p ranges over primes, be the first Chebyshev function. Then for all $x > 0$, we have $\vartheta(x) < 1.01624x$.

The following elementary upper bound on the number of automorphisms of a finite group will also be used.

Lemma 5.5. *Let G be a finite group. Then $|\mathrm{Aut}(G)| \leqslant |G|^{\log(|G|)/\log 2}$.*

Proof. Let $S = \{x_1, \dots, x_{d(G)}\}$ be a (necessarily minimal) generating subset of G of size $d(G)$. Then, setting $G_i := \langle x_i, \dots, x_{d(G)} \rangle$ for $i = 1, \dots, d(G)$, we obtain a subgroup series $G = G_1 > G_2 > \cdots > G_{d(G)} > G_{d(G)+1} := \{1_G\}$. By Lagrange's theorem, $|G_{i+1}| \geqslant 2|G_i|$ for each $i \in \{1, \dots, d(G)\}$, so $|G| \geqslant 2^{d(G)}$, whence

$$|S| = d(G) \leqslant \frac{\log |G|}{\log 2}.$$

The function which assigns to each automorphism of G its restriction to S is an injection, and so $|\mathrm{Aut}(G)|$ is at most the number of functions $S \to G$, which is exactly $|G|^{|S|} \leqslant |G|^{\log(|G|)/\log 2}$. □

Finally, we will need generalizations of the concepts of a "standard tuple" and of the "power-commutator tuple" associated to a standard tuple as defined in the proof of Proposition 3.2.4.

Definition 5.6. Consider the following concepts.

(1) Let p be a prime, and let P be a finite abelian p-group. Write

$$P \cong \mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_m}\mathbb{Z} \quad \text{with } 1 \leqslant e_1 \leqslant \cdots \leqslant e_m.$$

For $n \in \mathbb{N}^+$ with $n \geqslant m$, a *length n standard generating tuple of P* is an n-tuple $(x_1, \dots, x_n) \in P^n$ such that $P = \langle x_1, \dots, x_n \rangle$ and for $i \in \{1, \dots, n\}$,

$$\mathrm{ord}(x_i) = \begin{cases} p^{e_i} & \text{if } i \leqslant m, \\ 1 & \text{if } i > m. \end{cases}$$

(2) Let H be a finite abelian group, say with $d(H) = n$. For $k \in \mathbb{N}^+$, denote by p_k the k-th prime, and by P_k the Sylow p_k-subgroup of H. Hence up to isomorphism, we can write $H = \prod_{k \geqslant 1} P_k$. A *standard generating tuple of H* is an n-tuple $(h_1, \ldots, h_n) \in H^n$ such that $H = \langle h_1, \ldots, h_n \rangle$ and for each $k \geqslant 1$, the entry-wise projection of $(h_1, \ldots, h_n)$ to P_k is a length n standard generating tuple of P_k.

(3) Let G be a finite group, and let $n := d(G/G')$. A *standard tuple in G* is an n-tuple $(g_1, \ldots, g_n) \in G^n$ whose entry-wise image under the canonical projection $G \to G/G'$ is a standard generating tuple of G/G'.

Remark 5.7. Let H be a finite abelian group, and let G be an arbitrary finite group.

(1) All standard generating tuples of H are polycyclic generating sequences of H, and they all induce the same power-commutator presentation of H. Moreover, any polycyclic generating sequence of H inducing this said power-commutator presentation is a standard generating tuple. Hence $\mathrm{Aut}(H)$ acts 1-transitively on the set of standard generating tuples of H, and so the number of standard generating tuples of H is exactly $|\mathrm{Aut}(H)|$.

(2) The number of standard tuples in G is exactly $|\mathrm{Aut}(G/G')| \cdot |G'|^{d(G/G')}$.

(3) For each standard tuple $(g_1, \ldots, g_n)$ in G, we have $G = \langle g_1, \ldots, g_n, G' \rangle$.

Definition 5.8. Let G be a finite group, let $n := d(G/G')$, and let $(g_1, \ldots, g_n)$ be a standard tuple in G.

(1) The *power-automorphism-commutator tuple associated with* $(g_1, \ldots, g_n)$ is the $(2n + \binom{n}{2})$-tuple

$$(\pi_1, \ldots, \pi_n, \alpha_1, \ldots, \alpha_n,\\ \gamma_{1,1}, \gamma_{1,2}, \ldots, \gamma_{1,n}, \gamma_{2,3}, \gamma_{2,4}, \ldots, \gamma_{2,n}, \ldots, \gamma_{n-1,n})$$

with entries in $G' \cup \mathrm{Aut}(G')$ such that

- $\pi_i = g_i^{\mathrm{ord}_{G/G'}(g_i G')} \in G'$ for $i = 1, \ldots, n$,
- $\alpha_i \in \mathrm{Aut}(G')$ is the automorphism induced through conjugation by g_i for $i = 1, \ldots, n$,
- $\gamma_{i,j} = [g_i, g_j] \in G'$ for $1 \leqslant i < j \leqslant n$.

(2) Two standard tuples in G are called *equivalent* if and only if they have the same associated power-automorphism-commutator tuple.

Remark 5.9. Let G be a finite group, let $H := G/G'$, and let $n := d(G/G')$. Every standard generating tuple $(h_1, \dots, h_n)$ of H is a polycyclic generating sequence of H, with respect to which H has the power-commutator presentation

$$H = \langle x_1, \dots, x_n \mid x_i^{\mathrm{ord}(h_i)} = 1 \text{ for } i = 1, \dots, n;\ [x_i, x_j] = 1 \text{ for } 1 \leqslant i < j \leqslant n \rangle.$$

Now, let $(c_1, \dots, c_m)$ be a fixed generating tuple of G', with respect to which G' has the presentation

$$G' = \langle y_1, \dots, y_m \mid \rho_j = 1 \text{ for } j = 1, \dots, k \rangle$$

with ρ_j an element of the free group $\mathrm{F}(y_1, \dots, y_m)$ for $j = 1, \dots, k$. Then with respect to any (generating) $(m+n)$-tuple of the form

$$(g_1, \dots, g_n, c_1, \dots, c_m) \in G^{m+n},$$

where $(g_1, \dots, g_n)$ is a standard tuple in G, the group G has a presentation of the form

$$\begin{aligned} G = \langle x_1, \dots, x_n, y_1, \dots, y_m \mid \rho_j &= 1 \text{ for } j = 1, \dots, m; \\ x_i^{o_i} &= w_i \text{ for } i = 1, \dots, n; \\ [x_i, x_j] &= w_{i,j} \text{ for } 1 \leqslant i < j \leqslant n; \\ y_k^{x_i} &= v_{i,k} \text{ for } i = 1, \dots, n \text{ and } k = 1, \dots, m \rangle, \end{aligned}$$

where o_i denotes the common order of the i-th entry of any standard generating tuple of $H = G/G'$, and $w_i, w_{i,j}, v_{i,k} \in \mathrm{F}(y_1, \dots, y_m)$.

From this, it is clear that any two equivalent standard tuples in G lie in the same orbit of the component-wise action of $\mathrm{Aut}(G)$; in fact, they are conjugate under an automorphism of G which fixes G' element-wise.

Proof of Theorem 1.1 (3). Let G be a finite group with $\mathrm{maol}(G) \leqslant c$, $d(G) \leqslant d$. Then in particular, all conjugacy classes of G are of length at most c. It follows from Theorem 5.1 that

$$|G'| \leqslant c^{\frac{1}{2}(7+\log c)}.$$

Our goal will thus be to bound $|G : G'|$ explicitly from above in terms of c and d. First, we show the following.

Claim. *If p is a prime divisor of $|G : G'|$, then noting the definition of $A(c,d)$ from Theorem* 1.1 (3),

$$p \leqslant A(c,d) + 1 = c^{d + \frac{1}{2}(7+\frac{\log c}{\log 2})\left(\binom{d}{2} + \frac{d}{2\log 2}\cdot(7+\frac{\log c}{\log 2})\log c\right)} + 1.$$

In order to prove the claim, observe that by Corollary 5.3 and Remark 5.7 (2), the number of standard tuples in G is at least

$$(p-1)\cdot|G'|^{d(G/G')}.$$

On the other hand, in view of Lemma 5.5, the number of equivalence classes of standard tuples in G is at most

$$|G'|^{d(G/G')+d(G/G')\frac{\log|G'|}{\log 2}+\binom{d(G/G')}{2}}.$$

It follows that there is an equivalence class of standard tuples in G which is of size at least

$$\frac{(p-1)|G'|^{d(G/G')}}{|G'|^{d(G/G')+d(G/G')\frac{\log|G'|}{\log 2}+\binom{d(G/G')}{2}}}=\frac{p-1}{|G'|^{d(G/G')\frac{\log|G'|}{\log 2}+\binom{d(G/G')}{2}}}.$$

On the other hand, as $c\geqslant \mathrm{maol}(G)$, all $\mathrm{Aut}(G)$-orbits on $d(G/G')$-tuples over G are of length at most $c^{d(G/G')}$. In view of Remark 5.9, it follows that

$$c^{d(G/G')}\geqslant\frac{p-1}{|G'|^{d(G/G')\frac{\log|G'|}{\log 2}+\binom{d(G/G')}{2}}},$$

and hence

$$\begin{aligned}p&\leqslant c^{d(G/G')}\cdot|G'|^{d(G/G')\frac{\log|G'|}{\log 2}+\binom{d(G/G')}{2}}+1\\&\leqslant c^{d}\cdot c^{\frac{1}{2}(7+\frac{\log c}{\log 2})\left(d\frac{\frac{1}{2}(7+\frac{\log c}{\log 2})\log c}{\log 2}+\binom{d}{2}\right)}+1,\end{aligned}$$

as asserted by the claim.

Now that the claim has been proved, let f denote the largest exponent e occurring in the (essentially unique) direct factor decomposition of G/G' into primary cyclic groups $\mathbb{Z}/p^e\mathbb{Z}$. Then by the above claim and the fact that G/G' is d-generated, we have (letting the variable p range over primes)

$$\frac{|G|}{c^{\frac{1}{2}(7+\frac{\log c}{\log 2})}}\leqslant|G:G'|\leqslant\prod_{p\leqslant A(c,d)+1}p^{df}=\exp(\vartheta(A(c,d)+1)\cdot df),$$

and thus, in view of Theorem 5.4,

$$\begin{aligned}f&\geqslant\frac{\log|G|-\frac{1}{2}(7+\frac{\log c}{\log 2})\log c}{d\cdot\vartheta(A(c,d)+1)}\\&\geqslant\frac{\log|G|-\frac{1}{2}(7+\frac{\log c}{\log 2})\log c}{1.01624d\cdot(A(c,d)+1)}=:g(|G|,c,d).\end{aligned}\tag{5.1}$$

By Corollary 5.3 and Remark 5.7 (2), the number of standard tuples in G is at least

$$2^{f-1} \cdot |G'|^{d(G/G')} \geqslant 2^{g(|G|,c,d)-1} \cdot |G'|^{d(G/G')}.$$

On the other hand, the number of equivalence classes of standard tuples in G is at most

$$|G'|^{d(G/G')+d(G/G')\frac{\log|G'|}{\log 2}+\binom{d(G/G')}{2}}.$$

It follows that there is an equivalence class of standard tuples in G which is of size at least

$$\frac{2^{g(|G|,c,d)-1} \cdot |G'|^{d(G/G')}}{|G'|^{d(G/G')+d(G/G')\frac{\log|G'|}{\log 2}+\binom{d(G/G')}{2}}} = \frac{2^{g(|G|,c,d)-1}}{|G'|^{d(G/G')\frac{\log|G'|}{\log 2}+\binom{d(G/G')}{2}}}.$$

But again, since $\mathrm{maol}(G) \leqslant c$, the length of an $\mathrm{Aut}(G)$-orbit on $d(G/G')$-tuples over G cannot exceed $c^{d(G/G')}$, and so, in view of Remark 5.9,

$$c^{d(G/G')} \geqslant \frac{2^{g(|G|,c,d)-1}}{|G'|^{d(G/G')\frac{\log|G'|}{\log 2}+\binom{d(G/G')}{2}}},$$

which implies that

$$\begin{aligned} 2^{g(|G|,c,d)-1} &\leqslant c^{d(G/G')} \cdot |G'|^{d(G/G')\frac{\log|G'|}{\log 2}+\binom{d(G/G')}{2}} \\ &\leqslant c^{d} \cdot c^{\frac{1}{2}(7+\frac{\log c}{\log 2})\left(d\,\frac{\frac{1}{2}(7+\frac{\log c}{\log 2})\log c}{\log 2}+\binom{d}{2}\right)} \\ &= A(c,d). \end{aligned}$$

It follows that

$$g(|G|,c,d) \leqslant \frac{\log A(c,d)}{\log 2}+1,$$

or, equivalently (in view of the definition of $g(|G|,c,d)$ in formula (5.1) above),

$$\log|G| \leqslant 1.01624d \cdot (A(c,d)+1) \cdot \left(\frac{\log A(c,d)}{\log 2}+1\right)+\frac{1}{2}\left(7+\frac{\log c}{\log 2}\right)\log c,$$

which is just what we needed to show. □

6 Finite groups G with $\mathrm{maol}(G) \leqslant 23$

This section is concerned with the proof of Theorem 1.1 (4). Let us first introduce a shorthand notation for a concept that was already implicit in the previous section.

Notation 6.1. Let G be a finite group. We denote by

$$\mathrm{mccl}(G) := \max_{g \in G} |g^G|$$

the maximum conjugacy class length of G.

The following lemma will prove useful in our proof of Theorem 1.1 (4).

Lemma 6.2. *Let T be a finite group that can be written as a nonempty direct product of nonabelian finite simple groups. Assume that* $\mathrm{mccl}(T) \leqslant 23$. *Then we have* $T \cong \mathrm{Alt}(5)$.

Proof. We first show the following, weaker claim.

Claim. *Let S be a nonabelian finite simple group with* $\mathrm{mccl}(S) \leqslant 23$. *Then we have* $S \cong \mathrm{Alt}(5)$.

Using the ATLAS of Finite Groups [7], one can check that $\mathrm{mccl}(S) > 23$ for all sporadic finite simple groups S. Moreover, if $S = \mathrm{Alt}(m)$ with $m \geqslant 6$, then the length of the S-conjugacy class of any 3-cycle in S is

$$2 \cdot \binom{m}{3} = \frac{m(m-1)(m-2)}{3} \geqslant \frac{6 \cdot 5 \cdot 4}{3} = 40 > 23.$$

It remains to show that if S is a nonabelian finite simple group of Lie type with $\mathrm{mccl}(S) \leqslant 23$, then

$$S \cong A_1(4) \cong A_1(5) \cong \mathrm{Alt}(5).$$

To that end, note that if $\mathrm{mccl}(S) \leqslant 23$, then S has a proper subgroup (namely an element centralizer) of index at most 23, and so $m(S) \leqslant 23$, where $m(S)$ denotes the minimum faithful permutation representation degree of S (or, equivalently, the smallest index of a maximal subgroup of S). The values of $m(S)$ when S is a finite simple group of Lie type can be found in [10, Table 4, p. 7682] (see also the references mentioned in [10, paragraph preceding Table 4]), and using this information, it is easy to check that $m(S) \leqslant 23$ unless $S \cong A_d(q) \cong \mathrm{PSL}_{d+1}(q)$ with (d, q) from the set

$$\{(1,5), (1,7), (1,8), (1,9), (1,11), (1,13), (1,16), (1,17), (1,19), \\ (2,3), (2,4), (3,2)\}.$$

By going through the extended character tables of these finitely many groups S, which can be found in the ATLAS of Finite Groups [7], one finds that indeed,

$$S = A_1(5) \cong \mathrm{Alt}(5)$$

is the only nonabelian finite simple group with $\mathrm{mccl}(S) \leqslant 23$.

Now that the claim is proved, we can conclude as follows: Write

$$T = S_1^{n_1} \times \cdots \times S_r^{n_r},$$

where $S_1, \ldots, S_r$ are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \ldots, n_r \in \mathbb{N}^+$. Then, since the conjugacy classes of a direct product $G_1 \times G_2$ are just the Cartesian products of the conjugacy classes of G_1 with the conjugacy classes of G_2, we find that

$$23 \geqslant \mathrm{mccl}(T) = \prod_{i=1}^{r} \mathrm{mccl}(S_i)^{n_i}.$$

Hence, by the above claim, we have $r = 1$ and $S_1 = \mathrm{Alt}(5)$, so $T \cong \mathrm{Alt}(5)^{n_1}$. But if $n_1 \geqslant 2$, then

$$23 \geqslant \mathrm{mccl}(T) = \mathrm{mccl}(\mathrm{Alt}(5))^{n_1} = 20^{n_1} \geqslant 20^2 = 400 > 23,$$

a contradiction. Therefore, $T \cong \mathrm{Alt}(5)$, as we needed to show. □

Proof of Theorem 1.1 (4). We proceed by contradiction. Assume that G is a finite nonsolvable group with $\mathrm{maol}(G) \leqslant 23$. Recall the facts on finite semisimple groups listed in Subsection 2.4. We have that $G/\mathrm{Rad}(G)$ is a nontrivial finite semisimple group, and

$$23 \geqslant \mathrm{maol}(G) \geqslant \mathrm{mccl}(G) \geqslant \mathrm{mccl}(G/\mathrm{Rad}(G)) \geqslant \mathrm{mccl}(\mathrm{Soc}(G/\mathrm{Rad}(G))).$$

Since $\mathrm{Soc}(G/\mathrm{Rad}(G))$ is a nonempty direct product of nonabelian finite simple groups, Lemma 6.2 yields that $\mathrm{Soc}(G/\mathrm{Rad}(G)) \cong \mathrm{Alt}(5)$, and thus $G/\mathrm{Rad}(G)$ is isomorphic to either Alt(5) or Sym(5). However,

$$\mathrm{mccl}(\mathrm{Sym}(5)) = 24 > 23,$$

so we conclude that $G/\mathrm{Rad}(G) \cong \mathrm{Alt}(5)$. We now show the following.

Claim 1. *Let $x \in G/\mathrm{Rad}(G)$, and let $\tilde{x}$ be a lift of x in G. Then the conjugacy class $\tilde{x}^G$ consists of exactly one element from each of the cosets of* Rad(G) *which correspond to the elements of the conjugacy class $x^{G/\mathrm{Rad}(G)}$. In particular, we have* $\mathrm{Rad}(G) = \zeta G$.

For the proof of Claim 1, assume first x is a *nontrivial* element of $G/\mathrm{Rad}(G)$. Then since $G/\mathrm{Rad}(G) \cong \mathrm{Alt}(5)$, we have

$$|x^{G/\mathrm{Rad}(G)}| \geqslant 12 > \frac{23}{2}.$$

Hence the conjugacy class length $|\tilde{x}^G|$, being a multiple of $|x^{G/\mathrm{Rad}(G)}|$, must be equal to $|x^{G/\mathrm{Rad}(G)}|$, and the assertion follows for x. As for $x = 1_{G/\mathrm{Rad}(G)}$, the assertion is equivalent to $\mathrm{Rad}(G) \leqslant \zeta G$, which we can prove as follows. Fix a nontrivial element $y \in G/\mathrm{Rad}(G)$, let $\tilde{y}$ be a lift of y in G, and let $r \in \mathrm{Rad}(G)$ be arbitrary. Then

$$(\tilde{y}r)^{\tilde{y}} = \tilde{y}r^{\tilde{y}} \in \tilde{y}\mathrm{Rad}(G) \cap (\tilde{y}r)^G = (\tilde{y}r)\mathrm{Rad}(G) \cap (\tilde{y}r)^G = \{\tilde{y}r\},$$

whence $r^{\tilde{y}} = r$. This shows that $\mathrm{C}_G(r)$ contains all of $G \setminus \mathrm{Rad}(G)$, and thus $\mathrm{C}_G(r) = G$, i.e., $r \in \zeta G$. This concludes the proof of the main assertion, which involved showing that $\mathrm{Rad}(G) \leqslant \zeta G$. As for the "in particular", i.e., $\mathrm{Rad}(G) = \zeta G$, just use that $G/\mathrm{Rad}(G) \cong \mathrm{Alt}(5)$ is centerless.

Claim 1 implies the following.

Claim 2. *Let $g_1, g_2 \in G$. Then g_1 and g_2 commute if and only if their images in $G/\mathrm{Rad}(G)$ commute.*

Note that the implication "$\Rightarrow$" in Claim 2 is trivial, so we focus on proving the implication "$\Leftarrow$". Let x_1 and x_2 be commuting elements of $G/\mathrm{Rad}(G)$, and let $\widetilde{x_1}$ and $\widetilde{x_2}$ be lifts in G of x_1 and x_2 respectively. We need to show that $\widetilde{x_1}$ and $\widetilde{x_2}$ commute. Since x_1 and x_2 commute in $G/\mathrm{Rad}(G)$, we conclude that

$$\widetilde{x_1}^{\widetilde{x_2}} \in \widetilde{x_1}\mathrm{Rad}(G) \cap \widetilde{x_1}^G = \{\widetilde{x_1}\},$$

where the equality is by Claim 1. Hence $\widetilde{x_1}^{\widetilde{x_2}} = \widetilde{x_1}$, which just means that $\widetilde{x_1}$ and $\widetilde{x_2}$ commute, as we wanted to show.

By Claim 2 and the facts that $\mathrm{Rad}(G) = \zeta G$ (see Claim 1) and that the Sylow subgroups of $G/\mathrm{Rad}(G) \cong \mathrm{Alt}(5)$ are abelian, it follows that the Sylow subgroups of G are abelian. Hence, by [19, Result 10.1.7, p. 289], we have

$$G' \cap \mathrm{Rad}(G) = G' \cap \zeta G = \{1_G\}.$$

But since $G/\mathrm{Rad}(G) \cong \mathrm{Alt}(5)$ is perfect, $G = \langle \mathrm{Rad}(G), G' \rangle$, whence

$$G = \mathrm{Rad}(G) \times G'.$$

It follows that

$$G' \cong G/\mathrm{Rad}(G) \cong \mathrm{Alt}(5),$$

and by Lemma 3.1 (1), we find that

$$23 \geqslant \mathrm{maol}(G) \geqslant \mathrm{maol}(G') = \mathrm{maol}(\mathrm{Alt}(5)) = 24,$$

a contradiction. □

7 Concluding remarks

We conclude this paper with some related open problems for further research. Arguably the most glaring open problem, arising when comparing statements (1) and (2) of Theorem 1.1 (1), is the following.

Problem 7.1. *Determine the largest positive integer c_0 such that there are only finitely many finite groups G with $\mathrm{maol}(G) \leqslant c_0$ (and, if possible, list those finitely many G).*

Observe that by Theorem 1.1 (1) and (2), we have $c_0 \in \{3, 4, 5, 6, 7\}$. The next problem is motivated by the fact that the 2-groups discussed in Section 4 "just" fail to have the property that all their automorphisms are central.

Question 7.2. *Do there exist infinitely many finite groups G with $|\zeta G| = 4$ such that all automorphisms of G are central?*

If the answer to Question 7.2 is "yes", then by Theorem 1.1 (1), the constant c_0 from Problem 7.1 is 3, and Problem 7.1 is solved completely by Theorem 1.1 (1).

Finally, we would like to pose the following related problem on permutation groups.

Problem 7.3. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group of finite degree, and set*

$$\mathrm{maol}_{\mathrm{perm}}(G) := \max_{g \in G} |g^{\mathrm{N}_{\mathrm{Sym}(\Omega)}(G)}|.$$

Determine the largest non-negative integer c_1 such that all finite-degree permutation groups G with $\mathrm{maol}_{\mathrm{perm}}(G) \leqslant c_1$ have constantly bounded order, and, if possible, classify those G. Is $c_1 = c_0$, with c_0 as in Problem 7.1?

Bibliography

[1] R. Bastos and A. C. Dantas, On finite groups with few automorphism orbits, *Comm. Algebra* **44** (2016), no. 7, 2953–2958.

[2] N. L. Biggs and A. T. White, *Permutation Groups and Combinatorial Structures*, London Math. Soc. Lecture Note Ser. 33, Cambridge University, Cambridge, 1979.

[3] A. Bors, Finite groups with a large automorphism orbit, *J. Algebra* **521** (2019), 331–364.

[4] R. Brandl and W. J. Shi, Finite groups whose element orders are consecutive integers, *J. Algebra* **143** (1991), no. 2, 388–400.

[5] P. J. Cameron and C. E. Praeger, Block-transitive t-designs. I. Point-imprimitive designs, *Discrete Math.* **118** (1993), no. 1–3, 33–43.

[6] P. J. Cameron and C. E. Praeger, Block-transitive t-designs. II. Large t, in: *Finite Geometry and Combinatorics* (Deinze 1992), London Math. Soc. Lecture Note Ser. 191, Cambridge University, Cambridge (1993), 103–119.

[7] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Oxford University, Eynsham, 1985.

[8] A. C. Dantas, M. Garonzi and R. Bastos, Finite groups with six or seven automorphism orbits, *J. Group Theory* **20** (2017), no. 5, 945–954.

[9] J. de Groot, Indecomposable abelian groups, *Nederl. Akad. Wetensch. Proc. Ser. A.* **19** (1957), 137–145.

[10] S. Guest, J. Morris, C. E. Praeger and P. Spiga, On the maximum orders of elements of finite almost simple groups and primitive permutation groups, *Trans. Amer. Math. Soc.* **367** (2015), no. 11, 7665–7694.

[11] R. M. Guralnick and A. Maróti, Average dimension of fixed point spaces with applications, *Adv. Math.* **226** (2011), no. 1, 298–308.

[12] C. J. Hillar and D. L. Rhea, Automorphisms of finite abelian groups, *Amer. Math. Monthly* **114** (2007), no. 10, 917–923.

[13] D. F. Holt, B. Eick and E. A. O'Brien, *Handbook of Computational Group Theory*, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, 2005.

[14] R. D. Kitture and M. K. Yadav, Finite groups with abelian automorphism groups: a survey, in: *Group Theory and Computation*, Indian Stat. Inst. Ser., Springer, Singapore (2018), 119–140.

[15] T. J. Laffey and D. MacHale, Automorphism orbits of finite groups, *J. Aust. Math. Soc. Ser. A* **40** (1986), no. 2, 253–260.

[16] W. Ledermann and B. H. Neumann, On the order of the automorphism group of a finite group. I, *Proc. Roy. Soc. London Ser. A* **233** (1956), 494–506.

[17] G. A. Miller, The group of isomorphisms of an abelian group and some of its abelian subgroups, *Amer. J. Math.* **36** (1914), no. 1, 47–52.

[18] B. H. Neumann, Groups covered by permutable subsets, *J. London Math. Soc.* **29** (1954), 236–248.

[19] D. J. S. Robinson, *A Course in the Theory of Groups*, 2nd ed., Grad. Texts in Math. 80, Springer, New York, 1996.

[20] D. J. S. Robinson and J. Wiegold, Groups with boundedly finite automorphism classes, *Rend. Semin. Mat. Univ. Padova* **71** (1984), 273–286.

[21] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.

[22] M. Stroppel, Locally compact groups with few orbits under automorphisms, *Topol. Proc.* **26** (2002), no. 2, 819–842.

[23] K. Thas, Finite flag-transitive projective planes: A survey and some remarks, *Discrete Math.* **266** (2003), no. 1–3, 417–429.

[24] J. Wiegold, Groups with boundedly finite classes of conjugate elements, *Proc. Roy. Soc. London Ser. A* **238** (1957), 389–401.

[25] D. L. Winter, The automorphism group of an extraspecial p-group, *Rocky Mountain J. Math.* **2** (1972), no. 2, 159–168.

[26] J. P. Zhang, On finite groups all of whose elements of the same order are conjugate in their automorphism groups, *J. Algebra* **153** (1992), no. 1, 22–36.

Received October 24, 2019; revised February 14, 2020.

Author information

Alexander Bors, Johann Radon Institute for Computational and Applied Mathematics (RICAM), Altenbergerstraße 69, 4040 Linz, Austria.
E-mail: `alexander.bors@ricam.oeaw.ac.at`