Finite groups with an automorphism of large order

Alexander Bors*

October 8, 2015

Abstract

Let G be a finite group, and assume that G has an automorphism of order at least $\rho|G|$, with $\rho \in (0,1)$. We prove that if $\rho > 1/2$, then G is abelian, and if $\rho > 1/10$, then G is solvable, whereas in general, the assumption implies $[G : \mathrm{Rad}(G)] \leq \rho^{-1.78}$, where $\mathrm{Rad}(G)$ denotes the solvable radical of G. We also prove analogous results for a larger class of self-transformations of finite groups, so-called bijective affine maps. Furthermore, we provide two results of independent interest: an upper bound on element orders in the holomorph of a finite group, and that every bijective affine map of a finite semisimple group has a cycle of length equal to the order of the map, extending a theorem of Horoševskiĭ.

1 Introduction

1.1 Motivation and main results

Many authors have studied finite groups satisfying "extreme" quantitative conditions of various kinds. We mention the following examples: A variety of papers deals with finite groups in which some automorphism raises some minimum fraction of elements to the e-th power for $e = -1, 2, 3$, see [20, 21, 15, 16, 17, 18, 22, 4, 27, 9]. Wall classified the finite groups G having more than $\frac{1}{2}|G|-1$ involutions [26], and this was extended to a classification of those G with more than $\frac{1}{2}|G|-1$ subgroups of prime order by Burness and Scott [2].

For a finite group G and $e \in \{-1, 2, 3\}$, let us denote by $\mathrm{l}_e(G)$ the maximum fraction of elements of G which a single automorphism of G can raise to the e-th power. The uniting "philosophy" behind the aforementioned results on l_e is that a

*University of Salzburg, Mathematics Department, Hellbrunner Straße 34, 5020 Salzburg, Austria. E-mail: alexander.bors@sbg.ac.at

The author is supported by the Austrian Science Fund (FWF): Project F5504-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

2010 *Mathematics Subject Classification*: 20B25, 20D05, 20D25, 20D45.

Key words and phrases: finite groups, automorphisms, automorphism orders, solvable radical, semisimple groups.

finite group G for which $\mathrm{l}_e(G)$ is "large enough" is abelian or at least "not too far" from being abelian. For instance, considering the case $e = -1$, it was observed by Miller in 1929 that a finite group G with $\mathrm{l}_{-1}(G) > 3/4$ is abelian [20], and in 1972, Liebeck and MacHale classified the finite groups G with $\mathrm{l}_{-1}(G) > 1/2$ [15], proving in particular that the nonabelian ones are all either nilpotent of class 2 or have an abelian subgroup of index 2. In 1988, Potter proved that $\mathrm{l}_{-1}(G) > 4/15$ implies that G is solvable [22], and in 2005, Hegarty showed that the derived length of a finite solvable group G with $\mathrm{l}_{-1}(G) \geq \rho$ for some $\rho \in (0,1)$ is bounded from above in terms of ρ [9].

The main purpose of this paper is to study finite groups that may be viewed as "extreme" with respect to their maximum automorphism order, considering conditions on finite groups G of the form "G has an automorphism of order at least $\rho|G|$" and deriving results that are similar in spirit to those mentioned in the last paragraph. Our main results are as follows:

Theorem 1.1.1. *Let G be a finite group.*

(1) If G has an automorphism of order greater than $\frac{1}{2}|G|$, then G is abelian.

(2) If G has an automorphism of order greater than $\frac{1}{10}|G|$, then G is solvable.

(3) For any $\rho \in (0,1)$, if G has an automorphism of order at least $\rho|G|$, then $[G : \mathrm{Rad}(G)] \leq \rho^{E_1}$, with $E_1 = (\log_{60}(6) - 1)^{-1} = -1.7781\ldots$.

Remark 1.1.2. (1) Theorem 1.1.1(1) is a strengthening of [1, Theorem 1.1.7], where abelianity of G was derived under the stronger assumption that G has an automorphism cycle of length larger than $\frac{1}{2}|G|$.

(2) Horoševskiĭ proved that in a nontrivial finite group G, the maximum order of an automorphism is bounded from above by $|G| - 1$ (in particular, the maximum automorphism order of a finite group G can always be written as $\rho(G) \cdot |G|$ with $0 < \rho(G) \leq 1$), and that this upper bound is attained if and only if G is *elementary* abelian [11, Theorem 2].

(3) Horoševskiĭ also extensively studied automorphisms α of finite groups having a cycle of length $\mathrm{ord}(\alpha)$ (following the terminology in [7], such cycles will be referred to as *regular*). One of the results he obtained is that every automorphism of a finite nilpotent group has a regular cycle [11, Corollary 1]. In view of this, our Theorem 1.1.1(1) and [1, Corollary 1.1.8], one obtains a classification of those pairs (G, α) where G is a finite group and α an automorphism of G of order larger than $\frac{1}{2}|G|$.

(4) The constants $\frac{1}{2}$ and $\frac{1}{10}$ in Theorem 1.1.1(1,2) are both optimal, as it is easy to check that finite dihedral groups D have automorphisms of order $\frac{1}{2}|D|$, and that the alternating group $\mathcal{A}_5$ has an automorphism of order $6 = \frac{1}{10}|\mathcal{A}_5|$.

In [1], the author introduced and studied a class of self-transformations of finite groups extending the class of endomorphisms, so-called *(left-)affine maps*; these are maps of the form $\mathrm{A}_{x,\varphi} : G \to G, x \mapsto x\varphi(g)$ for some fixed element $x \in G$ and endomorphism φ of G; note that $\mathrm{A}_{x,\varphi}$ is bijective if and only if φ is an automorphism of G. The study of such maps was motivated by the auxiliary result [1, Lemma 2.1.3], whose main morale is that for any finite group G, any automorphism α of G and any α-invariant normal subgroup N of G, every cycle length of α is the product of some cycle length of $\tilde{\alpha}$, the automorphism of G/N induced by α, and some cycle length of

a bijective affine map of N. Here, we continue our study of (bijective) affine maps by proving the following analoga to Theorem 1.1.1(2,3):

Theorem 1.1.3. *(1) Let G be a finite group such that some bijective affine map of G has order greater than $\frac{1}{4}|G|$. Then G is solvable.*

(2) Let $\rho \in (0,1)$ and let G be a finite group such that some bijective affine map of G has order at least $\rho|G|$. Then $[G : \mathrm{Rad}(G)] \leq \rho^{E_2}$, with $E_2 = (\log_{60}(30) - 1)^{-1} = -5.9068\ldots$.

Remark 1.1.4. (1) As was already observed in [1], it follows from the observations in [23, p. 37] that the bijective affine maps of a group G form a subgroup $\mathrm{Aff}(G)$ of the symmetric group on G, and denoting the holomorph of G by $\mathrm{Hol}(G)$, the map $\mathrm{Hol}(G) \to \mathrm{Aff}(G), (x, \alpha) \mapsto \mathrm{A}_{x,\alpha}$, is an isomorphism. Hence Theorem 1.1.3(1,2) may be interpreted as giving restrictions on the structure of a finite group G based on lower bounds on maximum element orders in $\mathrm{Hol}(G)$.

(2) There is no analogon to Theorem 1.1.1(1) for bijective affine maps. Indeed, it is easy to check that for the dihedral group $\mathrm{D}_{2n} = \langle r, s \mid r^n = s^2 = 1, srs^{-1} = r^{-1} \rangle$, $n \geq 3$, the bijective affine map $\mathrm{A}_{s,\alpha}$, where α maps $r \mapsto r, s \mapsto sr$, moves all elements of D_{2n} in one large cycle. In particular, D_{2n}, in spite of its nonabelianity, even has a bijective affine map of order $1 \cdot |\,\mathrm{D}_{2n}\,|$.

(3) The constant $\frac{1}{4}$ appearing in Theorem 1.1.3 is optimal, as $\mathcal{A}_5$ has a bijective affine map of order $15 = \frac{1}{4}|\mathcal{A}_5|$.

Finally, we remark that the proofs of all our main results except for Theorem 1.1.1(1) make use of the classification of finite simple groups (CFSG).

1.2 Outline

In Section 2, we prove our first and only CFSG-free main result, Theorem 1.1.1(1). The proof is elementary, but builds up on results from [11] and [1].

Section 3 is dedicated to the presentation of some more elementary tools, some already found in the literature, some new, for proving the other main results. More precisely, Subsection 3.1 consists of lemmata giving some more insight into possible orders of automorphisms and bijective affine maps of finite groups. In Subsection 3.2, we provide upper bounds on element orders in wreath products. For the readers' convenience, we also briefly recall some important facts on finite semisimple groups and on Landau's and Chebyshev's function in Subsections 3.3 and 3.4 respectively. Finally, in Subsection 3.5, we prove that every bijective affine map of a finite semisimple group has a regular cycle, extending a theorem of Horoševskiĭ which asserts this for automorphisms.

In Section 4, we will make use of the tools from Section 3 as well as results from [8] to provide some upper bounds on maximum automorphism and bijective affine map orders of finite semisimple groups. Most of the section consists of the proof of a lemma, Lemma 4.1, asserting such bounds for automorphism groups of finite nonabelian characteristically simple groups and to which the more general bounds can be reduced. How these bounds relate to our main results will become clear in Section 6 in view of results and ideas from Section 5, and readers wishing for a

motivation before studying the rather laborious proof of Lemma 4.1 (which uses the CFSG) may skip it on a first reading.

In Section 5, we first establish a general lemma bounding $[G : \mathrm{Rad}(G)]$ in finite groups G with $f(G)$ bounded away from zero for a "sufficiently well-behaved" (see the properties listed in Definition 5.1.1) function f from the class of finite groups into the interval $[0, \infty)$. This is the content of Subsection 5.1. In Subsection 5.2, we will give some nontrivial examples of "well-behaved" functions f. We will actually prove a little more than what is needed for the proof of our main results (see Remark 5.2.10), but the additional work will also result in an upper bound on the maximum element order of the holomorph of a finite group (see Theorem 5.2.5) which is of independent interest.

In Section 6, we finally prove the remaining main results, and Section 7 gives some outlook on possible future research.

1.3 Notation and terminology

We denote by $\mathbb{N}$ the set of natural numbers (von Neumann ordinals, including 0), and by $\mathbb{N}^+$ the set of positive integers. The image of a set M under a function f is denoted by $f[M]$. The identity function on a set M is denoted by id_M, and $\mathcal{S}_M$ usually denotes the symmetric group on M, except when M is a natural number n, in which case $\mathcal{S}_n$ is understood as $\mathcal{S}_{\{1,\ldots,n\}}$. Similarly, for a natural number n, $\mathcal{A}_n$ is the alternating group on $\{1, \ldots, n\}$. The set of fixed points of a permutation σ over some set is denoted by $\mathrm{fix}(\sigma)$, and the cycle length of a point x under σ by $\mathrm{cl}_\sigma(x)$.

For a prime p and $a \in \mathbb{N}^+$, we denote by $\nu_p(a)$ the p-adic valuation of a, and for a prime power q, the finite field with q elements is denoted by $\mathbb{F}_q$.

Let G be a group. For an element $r \in G$, we denote by $\tau_r : G \to G, g \mapsto rgr^{-1}$ the inner automorphism of G with respect to r. The centralizer and normalizer of a subset $X \subseteq G$ are denoted by $\mathrm{C}_G(X)$ and $\mathrm{N}_G(X)$ respectively. As in Theorem 1.1.1, $\mathrm{Rad}(G)$ denotes the solvable radical of G. We denote the derived length of a solvable group G by $\mathrm{dl}(G)$. The term "semisimple group" will always denote a group without nontrivial solvable normal subgroups. We will also frequently use the following notation from [1] and [8]:

Definition 1.3.1. *(1) Let ψ be a permutation of a finite set X. We denote by $\Lambda(\psi)$ the maximum length of one of the disjoint cycles into which ψ decomposes, and set $\lambda(\psi) := \frac{1}{|X|}\Lambda(\psi)$.*

(2) For a finite group G, we set $\Lambda(G) := \max_{\alpha \in \mathrm{Aut}(G)} \Lambda(\alpha)$ and $\lambda(G) := \frac{1}{|G|}\Lambda(G)$.

(3) For a finite group G, the group of bijective left-affine maps of G is denoted by $\mathrm{Aff}(G)$. We set $\Lambda_{\mathrm{aff}}(G) := \max_{A \in \mathrm{Aff}(G)} \Lambda(A)$ and $\lambda_{\mathrm{aff}}(G) := \frac{1}{|G|}\Lambda_{\mathrm{aff}}(G)$.

(4) For a finite group G, we denote by $\mathrm{meo}(G)$ the maximum element order of G and set $\mathrm{mao}(G) := \mathrm{meo}(\mathrm{Aut}(G))$, the maximum automorphism order of G, as well as $\mathrm{maffo}(G) := \mathrm{meo}(\mathrm{Aff}(G))$, the maximum order of a bijective affine map of G.

Finally, in this paper, exp mostly denotes the exponent of a group, although in the definition of Ψ in Subsection 3.4, it denotes the natural exponential function. log

always denotes the natural logarithm, and for $c > 1$, the logarithm with base c is denoted by $\log_c$.

2 On the proof of Theorem 1.1.1(1)

The proof of this main result will use the following simple observation:

Lemma 2.1. *Let G be a finite group, α an automorphism of G such that $\lambda(\alpha) > \frac{1}{2}$. Assume that $\eta : G \to Q$ is a surjective group homomorphism such that $\eta \circ \alpha = \eta$. Then η (and thus Q) is trivial.*

Proof. The assumption $\eta \circ \alpha = \eta$ implies that $g_1^{-1} g_2 \in \ker \eta$ whenever $g_1, g_2 \in G$ lie on the same cycle of α. Since α has a cycle of length greater than $\frac{1}{2}|G|$ by assumption, it follows that $|\ker \eta| > \frac{1}{2}|G|$, whence $\ker \eta = G$ by Lagrange's theorem, and we are done. □

Proof of Theorem 1.1.1(1). Fix an automorphism α of G such that $\mathrm{ord}(\alpha) > \frac{1}{2}|G|$. We prove that G is abelian by induction on $|G|$. For the induction step, observe that G cannot be semisimple, since otherwise, by [11, Theorem 1], α would have a regular cycle and hence G would be abelian by [1, Theorem 1.1.7], a contradiction.

Following the argument in [11, proof of Theorem 2], we fix a minimal α-invariant elementary abelian normal subgroup B of G. We may of course assume that B is proper in G. Denote by $\tilde{\alpha}$ the induced automorphism of G/B, set $m := \mathrm{ord}(\tilde{\alpha})$, $n := \mathrm{ord}(\alpha_{|B})$, and denote by C the set of fixed points of α^m in B. Horoševskiĭ proceeded to show that either $C = \{1\}$ or $C = B$ (by minimality of B) and to derive upper bounds on $\mathrm{ord}(\alpha)$ in both cases, which imply that $\mathrm{ord}(\alpha) \leq m \cdot |G/B|$ in any case and thus $m \geq \mathrm{ord}(\alpha)/|G/B| = |B| \cdot \mathrm{ord}(\alpha)/|G| > \frac{1}{2}|B|$, whence G/B is abelian by the induction hypothesis.

In particular, we have $G' \leq B$ and $\lambda(\tilde{\alpha}) > \frac{1}{2}$ by [11, Corollary 1]. Consider the homomorphism $\varphi : G \to \mathrm{Aut}(B)$ corresponding to the conjugation action of G on B. Since B is abelian, we have $B \leq \ker(\varphi)$, and so there is a homomorphism $\overline{\varphi} : G/B \to \mathrm{Aut}(B)$ such that $\overline{\varphi} \circ \pi_B = \varphi$, where $\pi_B : G \to G/B$ is the canonical projection.

Now the kernel of $\overline{\varphi}$ consists by definition of those $\pi_B(g) \in G/B$ such that $gB \subseteq \mathrm{C}_G(B)$. Clearly, since B is α-invariant, so is $\mathrm{C}_G(B)$, and thus $\ker(\overline{\varphi})$ is $\tilde{\alpha}$-invariant. It follows that there exists an automorphism $\overline{\alpha}$ on the image $\overline{\varphi}(G/B) \leq \mathrm{Aut}(B)$ such that the following diagram commutes:

$$\begin{array}{ccc} G/B & \xrightarrow{\tilde{\alpha}} & G/B \\ \Big\downarrow{\scriptstyle \overline{\varphi}} & & \Big\downarrow{\scriptstyle \overline{\varphi}} \\ \overline{\varphi}(G/B) & \xrightarrow[\overline{\alpha}]{} & \overline{\varphi}(G/B) \end{array}$$

By this definition of $\overline{\alpha}$, it is clear that $\mathrm{ord}(\overline{\alpha}) \mid \mathrm{ord}(\tilde{\alpha}) = m$. We now give an alternative definition of $\overline{\alpha}$. The element $\overline{\varphi}(gB) \in \overline{\varphi}(G/B)$, which is by definition the

restriction of conjugation by g to B, is mapped by $\overline{\alpha}$ to $\overline{\alpha}(\overline{\varphi}(gB)) = \overline{\varphi}(\tilde{\alpha}(gB)) = \overline{\varphi}(\alpha(g)B)$, which is the restriction of conjugation by $\alpha(g)$ to B. But this implies that $\overline{\alpha}$ is the restriction of conjugation by $\alpha_{|B}$ in $\mathrm{Aut}(B)$ to its subgroup $\overline{\varphi}(G/B)$. In particular, $\mathrm{ord}(\overline{\alpha}) \mid \mathrm{ord}(\alpha_{|B}) = n$.

We now distinguish two cases. First, assume that B is cyclic. Then $\mathrm{Aut}(B)$ is abelian, and so by the second definition of $\overline{\alpha}$, it is clear that $\overline{\alpha} = \mathrm{id}_{\overline{\varphi}(G/B)}$. By Lemma 2.1, this implies that $\overline{\varphi}$ is the trivial homorphism $G/B \to \mathrm{Aut}(B)$, and by definition of $\overline{\varphi}$, this just means that $B \leq \zeta G$. In particular, we have $G' \leq \zeta G$, whence G is nilpotent of class 2. By [11, Corollary 1], this implies that $\lambda(\alpha) = \mathrm{ord}(\alpha) > \frac{1}{2}|G|$, and so G is abelian by [1, Theorem 1.1.7].

Now assume that $B \cong (\mathbb{Z}/p\mathbb{Z})^n$ for some prime p and $n \geq 2$. By the argument in [11, proof of Theorem 2], if $C = B$, we have $\mathrm{ord}(\alpha) \leq m \cdot p \leq |G/B| \cdot \frac{1}{p}|B| = \frac{1}{p}|G|$, a contradiction. Hence $C = \{1\}$, whence by [11, Lemma 3a], we have $\mathrm{ord}(\alpha) = \mathrm{lcm}(m, n)$. If $\gcd(m, n) > 1$, it follows that $\mathrm{ord}(\alpha) \leq \frac{1}{2} \cdot m \cdot n \leq \frac{1}{2} \cdot |G/B| \cdot |B| = \frac{1}{2}|G|$, a contradiction. Therefore, $\gcd(m, n) = 1$, which implies that $\overline{\alpha} = \mathrm{id}_{\overline{\varphi}(G/B)}$. Now repeat the argument from the first case to conclude the proof. □

3 Some tools

3.1 Lemmata concerning orders of automorphisms and bijective affine maps

We begin with a very simple observation. For a family $(f_i)_{i \in I}$, where $f_i : X_i \to Y_i$, we call the map $\prod_{i \in I} f_i : \prod_{i \in I} X_i \to \prod_{i \in I} Y_i, (x_i)_{i \in I} \mapsto (f_i(x_i))_{i \in I}$, the *product of the maps* f_i, $i \in I$. Let us say that a family $(G_i)_{i \in I}$ of groups has the *splitting property* if and only if every automorphism α of $\prod_{i \in I} G_i$ can be written as a product of automorphisms of the single G_i. Then the following is easy to prove:

Lemma 3.1.1. *Let $(G_1, \ldots, G_r)$ be a tuple of finite groups with the splitting property. Then:*

(1) $\mathrm{mao}(G_1 \times \cdots \times G_r) \leq \mathrm{mao}(G_1) \cdots \mathrm{mao}(G_r)$.

(2) Each bijective affine map of $G_1 \times \cdots \times G_r$ is a product of bijective affine maps of the single G_i. In particular, we have $\mathrm{maffo}(G_1 \times \cdots \times G_r) \leq \mathrm{maffo}(G_1) \cdots \mathrm{maffo}(G_r)$. □

We now provide some lemmata that are useful for the study of orders of bijective affine maps in finite groups. It turns out that the following elements play an important role (see the remarks after Lemma 3.1.3 below):

Definition 3.1.2. *Let G be a finite group, $x \in G$, α an automorphism of G, $n \in \mathbb{N}^+$.*

(1) The element $\mathrm{sh}_\alpha^{(n)}(x) := x\alpha(x) \cdots \alpha^{n-1}(x) \in G$ *is called the* ***n-th shift of x under α****.*

(2) The element $\mathrm{sh}_\alpha(x) := \mathrm{sh}_\alpha^{(\mathrm{ord}(\alpha))} \in G$ *is called the* ***shift of x under α****.*

The following calculation rules for shifts are easy to show:

Lemma 3.1.3. *Let G be a finite group, $x \in G$, α an automorphism of G.*
(1) $\alpha(\mathrm{sh}_\alpha(x)) = x\,\mathrm{sh}_\alpha(x)x^{-1}$.
(2) If $d \in \mathbb{N}^+$ *is such that* $\mathrm{cl}_\alpha(x) \mid d \mid \mathrm{ord}(\alpha)$, *then* $\mathrm{sh}_\alpha(x) = \mathrm{sh}_\alpha^{(d)}(x)^{\frac{\mathrm{ord}\,\alpha}{d}}$. □

Definition 3.1.2 is motivated by the following: Note that by the isomorphism $\mathrm{Hol}(G) \to \mathrm{Aff}(G)$ mentioned in Remark 1.1.4(1), it is clear that for all finite groups G, all $x \in G$ and all $\alpha \in \mathrm{Aut}(G)$, we have $\mathrm{ord}(\alpha) \mid \mathrm{ord}(\mathrm{A}_{x,\alpha})$. Now computing, in $\mathrm{Hol}(G)$, the power $(x,\alpha)^{\mathrm{ord}(\alpha)}$ (which is of course an element of G), one sees that this is just the element which we called $\mathrm{sh}_\alpha(x)$ above. Consequently, we get the following formula for computing orders of bijective affine maps of finite groups:

$$\mathrm{ord}(\mathrm{A}_{x,\alpha}) = \mathrm{ord}(\alpha) \cdot \mathrm{ord}(\mathrm{sh}_\alpha(x)).$$

We will also make use of this isomorphism, providing us with a natural faithful permutation representation of $\mathrm{Hol}(G)$ on G, in the proof of the next lemma. When ψ is a permutation of a finite set X and $n \in \mathbb{N}^+$, we say that an orbit O of the action of ψ on X *induces* an orbit $\tilde{O}$ of ψ^n (or that $\tilde{O}$ *stems from* O) if and only if $\tilde{O} \subseteq O$, in which case $|\tilde{O}| = \frac{1}{\gcd(n,|O|)}|O|$. Every orbit of ψ induces an orbit of ψ^n, and every orbit of ψ^n stems from precisely one orbit of ψ.

Lemma 3.1.4. *Let G be a finite group, $x \in G$, α an automorphism of G. Then every cycle length of $\mathrm{A}_{x,\alpha}$ is divisible by $\mathrm{L}_G(x,\alpha) := \mathrm{ord}(\mathrm{sh}_\alpha(x)) \cdot \prod_p p^{\nu_p(\mathrm{ord}(\alpha))}$, where p runs through the common prime divisors of $\mathrm{ord}(\mathrm{sh}_\alpha(x))$ and $\mathrm{ord}(\alpha)$. In particular, $\mathrm{L}_G(x,\alpha) \mid |G|$.*

Proof. Every orbit of $\mathrm{A}_{x,\alpha}^{\mathrm{ord}(\alpha)}$, the left multiplication by $\mathrm{sh}_\alpha(x)$ in G, has cardinality $\mathrm{ord}(\mathrm{sh}_\alpha(x))$, so certainly every cycle length of $\mathrm{A}_{x,\alpha}$ is divisible by $\mathrm{ord}(\mathrm{sh}_\alpha(x))$. In particular, if p is a common prime divisor of $\mathrm{ord}(\mathrm{sh}_\alpha(x))$ and $\mathrm{ord}(\alpha)$, and O is any orbit of $\mathrm{A}_{x,\alpha}$, then $p \mid |O|$, but $p^{\nu_p(\mathrm{ord}(\mathrm{sh}_\alpha(x)))}$ still divides $|\tilde{O}|$, where $\tilde{O}$ is any orbit of $\mathrm{A}_{x,\alpha}^{\mathrm{ord}(\alpha)}$ induced by O. This is only possible if $|O|$ actually is divisible by $p^{\nu_p(\mathrm{ord}(\mathrm{sh}_\alpha(x)))+\nu_p(\mathrm{ord}(\alpha))}$, and the assertion follows. □

Lemma 3.1.5. *Let G be a finite group, $x, r \in G$. Then $x^{-1}r \in \mathrm{C}_G(\mathrm{sh}_{\tau_r}(x))$. In particular, if, for some subgroup $H \leq G$, $\mathrm{C}_G(\mathrm{sh}_{\tau_r}(x)) \subseteq H$, then $x \in H$ if and only if $r \in H$.*

Proof. This follows immediately from the equation $r\,\mathrm{sh}_{\tau_r}(x)r^{-1} = \tau_r(\mathrm{sh}_{\tau_r}(x)) = x\,\mathrm{sh}_{\tau_r}(x)x^{-1}$, where the first equality is by the definition of τ_r and the second by Lemma 3.1.3(1). □

Lemma 3.1.6. *(1) Let G be a finite centerless group, $r, s \in G$. Set $x := sr^{-1}$. Then $\mathrm{sh}_{\tau_r}(x) = s^{\mathrm{ord}(r)}$. In particular, $\mathrm{ord}(\mathrm{A}_{x,\tau_r}) = \mathrm{lcm}(\mathrm{ord}(s), \mathrm{ord}(r))$.*
(2) Let G be any finite group, $r, s \in G$, x as in point (1). Then $\mathrm{sh}_{\tau_r}(x) = s^{\mathrm{ord}(\tau_r)} \cdot r^{-\mathrm{ord}(\tau_r)}$. In particular, if $\gcd(\mathrm{ord}(r), \mathrm{ord}(s)) = 1$, then $\mathrm{ord}(\mathrm{A}_{x,\tau_r}) = \mathrm{ord}(s) \cdot \mathrm{ord}(r)$.

Proof. An easy induction on $n \in \mathbb{N}^+$ proves that in both cases, we have $\mathrm{sh}_{\tau_r}^{(n)}(x) = s^n r^{-n}$. Therefore, we have $\mathrm{sh}_{\tau_r}(x) = s^{\mathrm{ord}(r)}$ under the assumptions of point (1). This

implies that

$$\begin{aligned}\operatorname{ord}(\mathrm{A}_{x,\tau_r}) &= \operatorname{ord}(\tau_r)\cdot\operatorname{ord}(\operatorname{sh}_{\tau_r}(x)) = \operatorname{ord}(r)\cdot\frac{\operatorname{ord}(s)}{\gcd(\operatorname{ord}(s),\operatorname{ord}(r))}\\ &= \operatorname{lcm}(\operatorname{ord}(s),\operatorname{ord}(r)),\end{aligned}$$

proving the statement of point (1). The proof of point (2) is similar, using that $r^{-\operatorname{ord}(\tau_r)} \in \zeta G$ and that the order of a product of two commuting elements with coprime orders is the product of their orders. □

Remark 3.1.7. Using the notation of Lemma 3.1.6, view r as fixed. Then, as s runs through G, $x = sr^{-1}$ assumes every value in G. Hence Lemma 3.1.6 provides a simple formula for shifts of group elements under any bijective affine map $\mathrm{A}_{x,\alpha}$, where α is an *inner automorphism*.

3.2 Upper bounds on element orders in wreath products

We will need upper bounds on $\operatorname{meo}(G)$ and $\operatorname{mao}(G)$ for finite semisimple groups G. To this end, some bounds on orders of elements in wreath products in general come in handy. Before formulating and proving Lemma 3.2.2 below, we introduce the following notation and terminology:

Definition 3.2.1. *Let G be a finite group, $n \in \mathbb{N}^+$, and $\psi \in \mathcal{S}_n$.*

(1) Let $g = (g_1,\dots,g_n) \in G^n$. For $i = 1,\dots,n$, we define

$$\operatorname{el}_i^{(\psi)}(g) := g_i g_{\psi^{-1}(i)} \cdots g_{\psi^{-\operatorname{cl}_\psi(i)+1}(i)} \in G.$$

Alternatively, one can describe $\operatorname{el}_i^{(\psi)}(g)$ as the image of $\operatorname{sh}_{\tau_\psi}^{(\operatorname{cl}_\psi(i))}(g) \in G^n \leq G \wr \mathcal{S}_n$ under the projection $\pi_i : G^n \to G$ onto the i-th component.

(2) We denote the set of orbits of the action of ψ on $\{1,\dots,n\}$ by $\operatorname{Orb}(\psi)$.

*(3) An **assignment to ψ in G** is a function $\beta : \operatorname{Orb}(\psi) \to G$. For such an assignment β, we define its **order** to be the least common multiple of the numbers $\operatorname{ord}(\beta(O)^{\frac{\operatorname{ord}(\psi)}{|O|}})$, where O runs through $\operatorname{Orb}(\psi)$.*

Lemma 3.2.2. *Let G be a finite group, $n \in \mathbb{N}^+$, denote by $\pi : G \wr \mathcal{S}_n \to \mathcal{S}_n$ the canonical projection, and let $\psi \in \mathcal{S}_n$.*

(1) Let $g = (g_1,\dots,g_n) \in G^n$ and consider the element $x := (g,\psi) \in G^n \rtimes \mathcal{S}_n = G \wr \mathcal{S}_n$. Then for $i = 1,\dots,n$, the i-th component of $x^{\operatorname{ord}(\psi)} \in G^n$ equals $\operatorname{el}_i^{(\psi)}(g)^{\frac{\operatorname{ord}(\psi)}{\operatorname{cl}_\psi(i)}}$.

(2) In particular, the maximum order of an element $x \in G \wr \mathcal{S}_n$ such that $\pi(x) = \psi$ equals the product of $\operatorname{ord}(\psi)$ with the maximum order of an assignment to ψ in G and is bounded from above by $\operatorname{ord}(\psi)\cdot\operatorname{meo}(G^{|\operatorname{Orb}(\psi)|})$.

Proof. For (1): We may assume that G is nontrivial. Fix i, and denote by $\pi_i : G^n \to G$ the projection onto the i-th component. It is clear that $x^{\operatorname{ord}(\psi)} = \operatorname{sh}_{\tau_\psi}(g)$ (where the shift is formed inside $G \wr \mathcal{S}_n$ and τ_ψ is the inner automorphism of $G \wr \mathcal{S}_n$ with respect to ψ), whence $\pi_i(x^{\operatorname{ord}(\psi)}) = \pi_i(\operatorname{sh}_{\tau_\psi}(g))$. But the i-th component of $\operatorname{sh}_{\tau_\psi}(g)$ only depends on the components of g whose indices are from the orbit O_i of

i under ψ, so if we denote by $\tilde{g}$ the element of G^n which has the same entries as g in the components whose indices are in O_i but all other entries equal to 1_G, we have $\pi_i(x^{\mathrm{ord}(\psi)}) = \pi_i(\mathrm{sh}_{\tau_\psi}(\tilde{g}))$. Now note that $\mathrm{cl}_\psi(i)$ is a multiple of $\mathrm{cl}_{\tau_\psi}(\tilde{g})$ and a divisor of $\mathrm{ord}(\psi) = \mathrm{ord}(\tau_\psi)$, which gives us, by an application of Lemma 3.1.3(2),

$$\begin{aligned}\pi_i(x^{\mathrm{ord}(\psi)}) = \pi_i(\mathrm{sh}_{\tau_\psi}(\tilde{g})) = \pi_i(\mathrm{sh}_{\tau_\psi}^{(\mathrm{cl}_\psi(i))}(\tilde{g})^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}}) = \pi_i(\mathrm{sh}_{\tau_\psi}^{(\mathrm{cl}_\psi(i))}(\tilde{g}))^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}} \\ = \pi_i(\mathrm{sh}_{\tau_\psi}^{(\mathrm{cl}_\psi(i))}(g))^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}} = \mathrm{el}_i^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}}.\end{aligned}$$

For (2): For any element $x \in G \wr \mathcal{S}_n$ of the form (g, ψ), we have $\mathrm{ord}(x) = \mathrm{ord}(\psi) \cdot \mathrm{ord}(x^{\mathrm{ord}(\psi)})$, where, by (1), the second factor is the least common multiple of the numbers $\mathrm{ord}(\mathrm{el}_i^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}})$ for $i = 1, \ldots, n$. Fix a set $\mathcal{R}$ of representatives of the orbits of ψ, which is in canonical bijection with $\mathrm{Orb}(\psi)$. It is not difficult to see that if $i, j \in \{1, \ldots, n\}$ are from the same orbit under ψ, then $\mathrm{el}_i^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}}$ and $\mathrm{el}_j^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(j)}}$ are conjugate in G and thus have the same order, so $\mathrm{ord}(x^{\mathrm{ord}(\psi)})$ is equal to just the least common multiple of the numbers $\mathrm{ord}(\mathrm{el}_i^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}})$ for $i \in \mathcal{R}$. Therefore, composing the canonical bijection $\mathrm{Orb}(\psi) \to \mathcal{R}$ with the function $\mathcal{R} \to G, i \mapsto \mathrm{el}_i^{(\psi)}(g)$ gives an assignment to ψ in G whose order coincides with $\mathrm{ord}(x^{\mathrm{ord}(\psi)})$. Conversely, if any assignment β to ψ in G is given, by choosing the components $g_1, \ldots, g_n$ of g such that for all $O \in \mathrm{Orb}(\psi)$ there exists $i \in O$ such that $g_i g_{\psi^{-1}(i)} \cdots g_{\psi^{-\mathrm{cl}_\psi(i)+1}(i)} = \beta(O)$, we can assure that $\mathrm{ord}((g, \psi)^{\mathrm{ord}(\psi)}) = \mathrm{ord}(\beta)$. This proves the claim. □

3.3 Finite semisimple groups

In this subsection, for the readers' convenience, we briefly recall some basic facts on finite semisimple groups which we will need later, following mostly the exposition in [23, pp. 89ff.].

Any group G has a unique largest normal centerless completely reducible subgroup, the centerless CR-radical of G, which we denote by $\mathrm{CRRad}(G)$. From now on, assume that G is finite and semisimple. Then $\mathrm{CRRad}(G)$ coincides with $\mathrm{Soc}(G)$, the socle of G. G canonically embeds into $\mathrm{Aut}(\mathrm{Soc}(G))$ by its conjugation action (which shows that for any finite centerless CR-group R, there are only finitely many isomorphism types of finite semisimple groups G such that $\mathrm{Soc}(G) \cong R$), and the image G^* of this embedding clearly contains $\mathrm{Inn}(\mathrm{Soc}(G))$. Conversely, for every finite centerless completely reducible (CR-)group R, any group G such that $\mathrm{Inn}(R) \leq G \leq \mathrm{Aut}(R)$ is semisimple with socle $\mathrm{Inn}(R) \cong R$.

If $S_1, \ldots, S_r$ are pairwise nonisomorphic nonabelian finite simple groups, and $n_1, \ldots, n_r \in \mathbb{N}^+$, then the tuple $(S_1^{n_1}, \ldots, S_r^{n_r})$ has the splitting property, i.e., we have $\mathrm{Aut}(S_1^{n_1} \times \cdots \times S_r^{n_r}) = \mathrm{Aut}(S_1^{n_1}) \times \cdots \times \mathrm{Aut}(S_r^{n_r})$. The structure of the automorphism groups of finite nonabelian characteristically simple groups can be described by permutational wreath products. More precisely, $\mathrm{Aut}(S^n) = \mathrm{Aut}(S) \wr \mathcal{S}_n$ for any finite nonabelian simple group S and any $n \in \mathbb{N}^+$.

Rose [24, Lemma 1.1] observed that, in generalization of the embedding of G into $\mathrm{Aut}(\mathrm{Soc}(G))$ for finite semisimple groups G, if G is any group, and H a characteristic subgroup of G such that $\mathrm{C}_G(H) = \{1_G\}$, then G embeds into $\mathrm{Aut}(H)$ by its conjugation action on H, and, viewing G as a subgroup of $\mathrm{Aut}(H)$, $\mathrm{Aut}(G)$ is canonically isomorphic to $\mathrm{N}_{\mathrm{Aut}(H)}(G)$. This implies, among other things, that automorphism groups of finite centerless CR-groups are complete and that for each finite semisimple group H, $\mathrm{Hol}(H)$ canonically embeds into $\mathrm{Hol}(\mathrm{Aut}(\mathrm{Soc}(H)))$.

3.4 Landau's and Chebyshev's function

Both Landau's function $g : \mathbb{N}^+ \to \mathbb{N}^+, n \mapsto \mathrm{meo}(\mathcal{S}_n)$, and Chebyshev's function $\psi : \mathbb{N}^+ \to \mathbb{N}^+, n \mapsto \log(\exp(\mathcal{S}_n))$, are well-studied in analytic number theory. Apart from information on their asymptotic growth behavior, explicit upper bounds are also available. More precisely, Massias [19, Théorème, p. 271] proved that $\log(g(n)) \leq 1.05314 \cdot \sqrt{n \log(n)}$ for all $n \in \mathbb{N}^+$, and Rosser and Schoenfeld [25, Theorem 12] that $\psi(n) < 1.03883 \cdot n$ for all $n \in \mathbb{N}^+$.

The latter result translates into an exponential upper bound on $\Psi := \exp \circ \psi$. For $n \leq 27$, the following best possible exponential bound on $g(n)$ is sharper than the subexponential bound by Massias, and its use will make some of our arguments easier:

Proposition 3.4.1. *For all $n \in \mathbb{N}^+$, we have $g(n) \leq 3^{\frac{n}{3}}$, with equality if and only if $n = 3$.* □

We conclude with the following consequence of Lemma 3.2.2:

Lemma 3.4.2. *(1) Let G be a finite group, $n \in \mathbb{N}^+$. Then $\mathrm{meo}(G \wr \mathcal{S}_n) \leq g(n) \cdot \mathrm{meo}(G^n)$.*

(2) Let S be a nonabelian finite simple group, $n \in \mathbb{N}^+$. Then the inequality $g(n) \cdot \mathrm{meo}(\mathrm{Aut}(S)^n) < |S|^{n/3}$ implies that $\mathrm{mao}(\mathrm{Aut}(S^n)) < |S^n|^{1/3}$ and $\mathrm{maffo}(\mathrm{Aut}(S^n)) < |S^n|^{2/3}$.

Proof. For (1): This follows immediately from Lemma 3.2.2(2).

For (2): By completeness of $\mathrm{Aut}(S^n)$ and (1), we have

$$\begin{aligned}\mathrm{mao}(\mathrm{Aut}(S^n)) &= \mathrm{meo}(\mathrm{Aut}(S^n)) = \mathrm{meo}(\mathrm{Aut}(S) \wr \mathcal{S}_n) \leq g(n) \cdot \mathrm{meo}(\mathrm{Aut}(S)^n) \\ &< |S|^{n/3} = |S^n|^{1/3},\end{aligned}$$

and that

$$\begin{aligned}\mathrm{maffo}(\mathrm{Aut}(S^n)) &= \mathrm{meo}(\mathrm{Hol}(\mathrm{Aut}(S^n))) = \mathrm{meo}(\mathrm{Aut}(S^n) \rtimes \mathrm{Aut}(\mathrm{Aut}(S^n))) \\ &\leq \mathrm{meo}(\mathrm{Aut}(S^n)) \cdot \mathrm{meo}(\mathrm{Aut}(\mathrm{Aut}(S^n))) = \mathrm{meo}(\mathrm{Aut}(S^n))^2 \\ &< |S^n|^{2/3}.\end{aligned}$$

□

3.5 On regular cycles in finite semisimple groups

We already mentioned in Remark 1.1.2(3) that Horoševskiĭ proved that every automorphism of a finite nilpotent group has a regular cycle. He also established this for finite semisimple groups [11, Theorem 1]. In this subsection, we will extend Horoševskiĭ's Theorem 1 to bijective affine maps:

Theorem 3.1. *Let G be a finite semisimple group. Then every bijective affine map of G has a regular cycle.*

Our proof of Theorem 3.1 is mostly an adaptation of Horoševskiĭ's proof, with the arguments getting slightly more complicated because of the more general situation. However, at one point, our proof differs from the one of Horoševskiĭ, using the recent result [7, Theorem 3.2] to settle one particular case. Just like Horoševskiĭ, we use the following:

Lemma 3.5.1. *Let X be a finite set, $\psi \in \mathcal{S}_X$, p a prime such that $p^2 \mid \mathrm{ord}(\psi)$. The following are equivalent:*
(1) ψ has a regular cycle.
(2) ψ^p has a regular cycle.

Proof. See [11, Lemma 1]. The assumption there that ψ (called ϕ there) is an automorphism of a finite group is not needed. □

Lemma 3.5.2. *Let G be a group, $B \trianglelefteq G$, A a bijective affine map of G such that $A_{|B} = \mathrm{id}_B$. Then $\mathrm{C}_G(B) \trianglelefteq G$, and A induces the identity map in $G/\mathrm{C}_G(B)$.*

Proof. In general, for all $x \in G$ and $\alpha \in \mathrm{Aut}(G)$, it follows immediately from the definition of $\mathrm{A}_{x,\alpha}$ that $\mathrm{A}_{x,\alpha}(1_G) = x$. Since $A(1_G) = 1_G$ by assumption, A thus actually is an automorphism of G, so the claim follows from [11, Lemma 2]. □

The following lemma (in which we use the "product of maps" notion from the beginning of Subsection 3.1) is easy to prove:

Lemma 3.5.3. *Let $X_1, \ldots, X_n$ be finite sets, ψ_i, $i = 1, \ldots, n$, a permutation of X_i with a regular cycle. Then $\psi_1 \times \cdots \times \psi_n$ has a regular cycle.* □

One additional simple observation which we will need is the following:

Lemma 3.5.4. *Let G be a group, $A = \mathrm{A}_{x,\alpha}$ a bijective left-affine map of G such that $\mathrm{fix}(A) \neq \emptyset$. Then $\mathrm{fix}(A)$ is a left coset of the subgroup $\mathrm{fix}(\alpha) \leq G$.*

Proof. For all $g \in G$, we have that $g \in \mathrm{fix}(A)$ if and only if $x\alpha(g) = g$, or $x = g\alpha(g)^{-1}$. Therefore, if we fix $f \in \mathrm{fix}(A)$, then $\mathrm{fix}(A)$ can be desribed as $\{g \in G \mid g\alpha(g)^{-1} = f\alpha(f)^{-1}\} = \{g \in G \mid g^{-1}f \in \mathrm{fix}(\alpha)\} = f\,\mathrm{fix}(\alpha)$. □

Proof of Theorem 3.1. The proof is by induction on $|G|$ with an inner induction on $\mathrm{ord}(A)$. For the induction step, assume that $A = \mathrm{A}_{x,\alpha}$ is a bijective affine map of the finite semisimple group G. To show that A has a regular cycle, we make a case distinction:

1. Case: G is simple. This case is by contradiction, so assume that A does not have a regular cycle. Note that by Lemma 3.5.1 and the induction hypothesis, $\mathrm{ord}(A)$ then must be squarefree, say $\mathrm{ord}(A) = p_1 \cdots p_r$, with the p_i pairwise distinct primes. Since by the induction hypothesis, A^{p_i}, $i = 1, \ldots, r$, has a cycle of length $\mathrm{ord}(A^{p_i}) = \prod_{j \neq i} p_j$, but A has no regular cycle, A must also have a cycle of length $\prod_{j \neq i} p_j$. In particular, we have $p_2 \cdots p_r < |G|$. Now note that by the assumption that A does not have a regular cycle, we have $G \subseteq \bigcup_{i=1}^{r} \mathrm{fix}(A^{\prod_{j \neq i} p_j})$. By Lemma 3.5.4, we have $|\mathrm{fix}(A^{\prod_{j \neq i} p_j})| = |\mathrm{fix}(\alpha^{\prod_{j \neq i} p_j})|$, and so there must exist $i \in \{1, \ldots, r\}$ such that $[G : \mathrm{fix}(\alpha^{\prod_{j \neq i} p_j})] \leq r$ (otherwise, G could not be covered by the r fixed point sets above). But since G is simple, this implies that $|G| \leq r! \leq p_2 \cdots p_r < |G|$, a contradiction.
2. Case: G is characteristically simple, but not simple. Let S be a nonabelian finite simple group and $n \geq 2$ such that $G \cong S^n$. α is an element of the permutational wreath product $\mathrm{Aut}(S) \wr \mathcal{S}_n$, i.e., α is a composition $(\alpha_1 \times \cdots \times \alpha_n) \circ \psi$, where each α_i is an automorphism of S and ψ is a permutation of coordinates on S^n. Writing $x = (x_1, \ldots, x_n)$, and denoting by μ_x the left multiplication by x in S^n, it follows that $A = \mu_x \circ ((\alpha_1 \times \cdots \times \alpha_n) \circ \psi) = ((\mu_{x_1} \times \cdots \times \mu_{x_n}) \circ (\alpha_1 \times \cdots \times \alpha_n)) \circ \psi = (\mathrm{A}_{x_1,\alpha_1} \times \cdots \times \mathrm{A}_{x_n,\alpha_n}) \circ \psi$. This proves that $A \in \mathrm{Aff}(S) \wr \mathcal{S}_n$ (actually, we just proved that $\mathrm{Aff}(S^n) = \mathrm{Aff}(S) \wr \mathcal{S}_n$). By induction hypothesis, every permutation from $\mathrm{Aff}(S)$ has a regular cycle, and so by [7, Theorem 3.2], A has a regular cycle.
3. Case: G is completely reducible, but not characteristically simple. Then there exist $r \geq 2$, pairwise nonisomorphic nonabelian finite simple groups $S_1, \ldots, S_r$ and $n_1, \ldots, n_r \in \mathbb{N}^+$ such that $G \cong S_1^{n_1} \times \cdots \times S_r^{n_r}$. Since $(S_1^{n_1}, \ldots, S_r^{n_r})$ has the splitting property, by Lemma 3.1.1(2), A can be written as a product of bijective affine maps over the single $S_i^{n_i}$, each of which has a regular cycle by the induction hypothesis, and so A has a regular cycle by Lemma 3.5.3.
4. Case: G is not completely reducible. Set $B := \mathrm{Soc}(G)$, and note that B is proper in G and $\mathrm{C}_G(B) = \{1_G\}$. Denote by $\tilde{A}$ the bijective affine map of G/B induced by A, and let k denote the cycle length of the identity element of G/B under $\tilde{A}$. Set $A_0 := A^k$. Then A_0 restricts to a bijective affine map of B, so by the induction hypothesis, $A_{0|B}$ has a cycle of length $n := \mathrm{ord}(A_{0|B})$; fix an element $x \in B$ such that $\mathrm{cl}_{A_0}(x) = n$. Now A_0^n acts identically in B, and thus by Lemma 3.5.2 also in $G \cong G/\mathrm{C}_G(B)$. This means that $n = \mathrm{ord}(A_0)$, and so $\mathrm{ord}(A) \leq k \cdot n$. But clearly, $\mathrm{cl}_A(x) = k \cdot n$, since k divides the cycle length under A of any element from B. Therefore, $\mathrm{ord}(A) = k \cdot n$ and A has a regular cycle. □

4 Upper bounds on $\mathrm{mao}(G)$ and $\mathrm{maffo}(G)$ for finite semisimple groups G

The main challenge of this section will be to establish the following lemma:

Lemma 4.1. *Let G be a finite nonabelian characteristically simple group. Then:*
(1) $\mathrm{mao}(G) < |G|^{\frac{1}{3}}$*, with the following exceptions:*

- $G \cong \mathrm{PSL}_2(q)$ *for some prime power* $q \geq 5$*. In this case,* $\mathrm{mao}(G) = q+1$*, we have* $\frac{1}{3} < \log_{|G|}(q+1) \leq \frac{\log(q+1)}{\log(\frac{1}{2}q(q^2-1))}$*, and as* $q \to \infty$*, this upper bound converges to* $\frac{1}{3}$ *strictly monotonously from above.*
- $G \cong \mathrm{PSL}_2(p)^2$ *for some prime* $p \geq 5$*. In this case,* $\mathrm{mao}(G) = p(p+1)$*, we have* $\frac{1}{3} < \log_{|G|}(p(p+1)) = \frac{\log(p(p+1))}{2\cdot\log(\frac{1}{2}p(p^2-1))}$*, and as* $p \to \infty$*, this upper bound converges to* $\frac{1}{3}$ *strictly monotonously from above.*
- $G \cong \mathrm{PSL}_2(p)^3$ *for some prime* $p \geq 5$*. In this case,* $\mathrm{mao}(G) = \frac{1}{2}p(p^2-1) = |G|^{\frac{1}{3}}$*.*

(2) $\mathrm{maffo}(\mathrm{Aut}(G)) \leq |G|^{\frac{2}{3}}$*, with the following exceptions:* $G \cong \mathrm{PSL}_2(p)$ *for some prime* $p \geq 5$*. In this case,* $\mathrm{maffo}(\mathrm{Aut}(G)) = p(p+1)$*, we have* $\frac{2}{3} < \log_{|G|}(p(p+1)) = \frac{\log(p(p+1))}{\log(\frac{1}{2}p(p^2-1))}$*, and as* $p \to \infty$*, this upper bound converges to* $\frac{2}{3}$ *strictly monotonously from above.*

Note that by completeness of of $\mathrm{Aut}(G)$, we have $\mathrm{mao}(G) = \mathrm{meo}(\mathrm{Aut}(G)) = \mathrm{mao}(\mathrm{Aut}(G))$, so the lemma provides upper bounds on both automorphism and bijective affine map orders of automorphism groups of finite nonabelian characteristically simple groups. Before tackling its proof, we note some important consequences.

Lemma 4.2. *(1) For all finite nonabelian characteristically simple groups G, we have that* $\mathrm{mao}(G) \leq |G|^{\log_{60}(6)}$*, with equality if and only if* $G \cong \mathrm{PSL}_2(5) \cong \mathcal{A}_5$*.*

(2) For every $\epsilon > 0$*, we have* $\mathrm{mao}(G) \leq |G|^{\frac{1}{3}+\epsilon}$ *for almost all finite nonabelian characteristically simple groups G.*

(3) For all finite nonabelian characteristically simple groups G, we have that $\mathrm{maffo}(\mathrm{Aut}(G)) \leq |G|^{\log_{60}(30)}$*, with equality if and only if* $G \cong \mathrm{PSL}_2(5) \cong \mathcal{A}_5$*.*

(4) For every $\epsilon > 0$*, we have* $\mathrm{maffo}(\mathrm{Aut}(G)) \leq |G|^{\frac{2}{3}+\epsilon}$ *for almost all finite nonabelian characteristically simple groups G.*

Proof. The statements in (2) and (4) follow immediately from Lemma 4.1. For (1), note that by Lemma 4.1(1), we have $\mathrm{mao}(\mathrm{Aut}(\mathrm{PSL}_2(5))) = 6 = |\mathrm{PSL}_2(5)|^{\log_{60}(6)}$, and using the strict monotonicity of the upper bounds in Lemma 4.1(1), it is not difficult to see that this is the only case where equality holds. The proof of (3) is analogous. □

Remark 4.3. The exceptions in Lemma 4.1 show that the statements of Lemma 4.2(2,4) become false if $\frac{1}{3}$ and $\frac{2}{3}$ respectively are replaced by smaller constants.

The result which we will actually use in the proof of our main results is the following:

Theorem 4.4. *Let H be a finite semisimple group. Then:*
(1) $\mathrm{mao}(H) \leq |\mathrm{Soc}(H)|^{\log_{60}(6)}$*.*
(2) $\mathrm{maffo}(H) \leq |\mathrm{Soc}(H)|^{\log_{60}(30)}$*.*

Proof. Let $S_1, \dots, S_r$ be pairwise nonisomorphic nonabelian finite simple groups, $n_1, \dots, n_r \in \mathbb{N}^+$ such that $\mathrm{Soc}(H) \cong S_1^{n_1} \times \dots \times S_r^{n_r}$. Using the facts that $\mathrm{Aut}(H)$ embeds into $\mathrm{Aut}(\mathrm{Soc}(H))$ and that $(S_1^{n_1}, \dots, S_r^{n_r})$ has the splitting property, we conclude that

$$\begin{aligned}\mathrm{mao}(H) &= \mathrm{meo}(\mathrm{Aut}(H)) \leq \mathrm{meo}(\mathrm{Aut}(\mathrm{Soc}(H))) = \mathrm{mao}(\mathrm{Soc}(H))\\ &= \mathrm{mao}(S_1^{n_1} \times \dots \times S_r^{n_r}) \leq \mathrm{mao}(S_1^{n_1}) \cdots \mathrm{mao}(S_r^{n_r})\\ &\leq |S_1|^{n_1 \log_{60}(6)} \cdots |S_r|^{n_r \log_{60}(6)} = |\operatorname{Soc}(H)|^{\log_{60}(6)},\end{aligned}$$

where the last inequality follows from Lemma 4.2(1). This proves the inequality in (1). For (2), we use the facts that $\mathrm{Hol}(H)$ embeds into $\mathrm{Hol}(\mathrm{Aut}(\mathrm{Soc}(H)))$ and that, by completeness of $\mathrm{Aut}(S_1^{n_1} \times \dots \times S_r^{n_r}) = \mathrm{Aut}(S_1^{n_1}) \times \dots \times \mathrm{Aut}(S_r^{n_r})$, the tuple $(\mathrm{Aut}(S_1^{n_1}), \dots, \mathrm{Aut}(S_r^{n_r}))$ has the splitting property, to conclude, with one application of Lemma 4.2(3) at the end, that

$$\begin{aligned}\mathrm{maffo}(H) &= \mathrm{meo}(\mathrm{Hol}(H)) \leq \mathrm{meo}(\mathrm{Hol}(\mathrm{Aut}(\mathrm{Soc}(H)))) = \mathrm{maffo}(\mathrm{Aut}(\mathrm{Soc}(H)))\\ &= \mathrm{maffo}(\mathrm{Aut}(S_1^{n_1}) \times \dots \times \mathrm{Aut}(S_r^{n_r}))\\ &\leq \mathrm{maffo}(\mathrm{Aut}(S_1^{n_1})) \cdots \mathrm{maffo}(\mathrm{Aut}(S_r^{n_r}))\\ &\leq |S_1|^{n_1 \log_{60}(30)} \cdots |S_r|^{n_r \log_{60}(30)} = |\operatorname{Soc}(H)|^{\log_{60}(30)}.\end{aligned}$$

□

The rest of this section is dedicated to the proof of Lemma 4.1. Essentially, the proof will be an application of the CFSG, the rather recent results on upper bounds on automorphism orders of finite simple groups from [8] and the tools developed in Section 3.

Let $G = S^n$, with S a nonabelian finite simple group. We prove the statement of Lemma 4.1 in a case distinction in accordance with the CFSG.

4.1 Case: S is sporadic

Note that $g(n) \cdot \mathrm{meo}(\mathrm{Aut}(S)^n) < 3^{n/3} \cdot \mathrm{meo}(\mathrm{Aut}(S))^n \leq (3^{1/3} \cdot |\operatorname{Out}(S)| \cdot \mathrm{meo}(S))^n$, and so in view of Lemma 3.4.2(2), it is sufficient to have $3^{1/3} \cdot |\operatorname{Out}(S)| \cdot \mathrm{meo}(S) \leq |S|^{1/3}$, which can be checked for all sporadic S using information from the ATLAS [3].

4.2 Case: $S = \mathcal{A}_m, m \geq 7$

We remark that $\mathcal{A}_5 \cong \mathrm{PSL}_2(5)$ and $\mathcal{A}_6 \cong \mathrm{PSL}_2(9)$ will be treated in the next case. In view of Lemma 3.4.2(2), it is sufficient to show $g(n) \cdot \mathrm{meo}(\mathcal{S}_m^n) < (\frac{1}{2}m!)^{n/3}$ for all $n \in \mathbb{N}^+$ and all $m \geq 7$. For $n = 1, 2, 3$, one checks the inequality for $m = 7$ directly, and for $m \geq 8$, replacing $\mathrm{meo}(\mathcal{S}_m^n)$ by $3^{nm/3}$ yields a stronger inequality which can be easily verified. For $n \geq 4$, using the results of Subsection 3.4, one can replace $g(n)$ by $3^{n/3}$ and $\mathrm{meo}(\mathcal{S}_m^n)$ by $\mathrm{e}^{1.03883 \cdot m}$ for a stronger inequality which is easy to verify.

4.3 Case: $S = \mathrm{PSL}_2(q), q \geq 5$

This is the most complicated case, requiring to investigate the five subcases $n = 1, 2, 3, 4$ and $n \geq 5$. Recall that $\mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, and in particular, there is a natural embedding $\mathrm{PSL}_2(q) \hookrightarrow \mathrm{PGL}_2(q)$.

4.3.1 Subcase: $n = 1$

Our goal is to show the following:

Theorem 4.3.1. *Let $q \geq 5$ be a prime power. Then:*
(1) $\mathrm{mao}(\mathrm{PSL}_2(q)) = q + 1$.
(2) $\mathrm{maffo}(\mathrm{Aut}(\mathrm{PSL}_2(q))) = \begin{cases} q(q+1), & \text{if } q \text{ is prime,} \\ q^2 - 1, & \text{if } q \text{ is even,} \\ \frac{1}{2}(q^2-1), & \text{if } q \text{ is odd and not prime.} \end{cases}$.

Now $\mathrm{mao}(\mathrm{PSL}_2(q)) = q + 1$ was already proved by Guest, Morris, Praeger and Spiga in [8], see Table 3 there. The following lemma is an extract from the proof of [8, Theorem 2.16]:

Lemma 4.3.2. *Let $q \geq 5$ be a power of the prime p.*
(1) Denote by $\pi : \mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \to \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ the canonical projection. Let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ such that $\mathrm{ord}(\pi(\alpha)) = e$. Then $\mathrm{ord}(\alpha) \leq e \cdot (q^{1/e} + 1)$.
(2) $\mathrm{mao}(\mathrm{PSL}_2(q)) = q + 1$. □

Point (2) can be verified using point (1). Since point (1) of Theorem 4.3.1 is now clear, let us outline the strategy for proving its point (2): Consider a bijective affine map $\mathrm{A}_{x,\alpha}$ of $\mathrm{Aut}(\mathrm{PSL}_2(q))$, having order $\mathrm{ord}(\alpha) \cdot \mathrm{ord}(\mathrm{sh}_\alpha(x))$. By completeness of $\mathrm{Aut}(\mathrm{PSL}_2(q))$, we know that $\mathrm{ord}(\alpha)$ is an element order in $\mathrm{Aut}(\mathrm{PSL}_2(q))$, so the order of any bijective affine map of $\mathrm{Aut}(\mathrm{PSL}_2(q))$ is the product of two automorphism orders of $\mathrm{PSL}_2(q)$. If we know a list of the first few largest automorphism orders of $\mathrm{PSL}_2(q)$ which is long enough to ensure that for any bijective affine map whose order exceeds the asserted maffo-value, the two factor orders must be in the list, we can systematically go through the possible combinations, deriving a contradiction in each case using Lemmata 3.1.4 and 3.1.5. It will then remain to show that the asserted maffo-value is indeed the order of some bijective affine map of $\mathrm{Aut}(\mathrm{PSL}_2(q))$, which can be done by Lemma 3.1.6.

We can indeed extend the list of largest automorphism orders of $\mathrm{PSL}_2(q)$ to our needs in a way similar to how Guest, Morris, Praeger and Spiga derived point (2) of Lemma 4.3.2 from point (1):

Lemma 4.3.3. *(1) Let $q = 2^f$ with $f \geq 3$. The two largest automorphism orders of $\mathrm{PSL}_2(q)$ are $q + 1$ and $q - 1$.*
(2) Let $q = p^f \geq 5$ with p an odd prime and $f \geq 1$.

- *If $f = 1$, then the five largest automorphism orders of $\mathrm{PSL}_2(q)$ are $q + 1, q, q - 1, \frac{q+1}{2}, \frac{q-1}{2}$.*
- *If $f \geq 2$ and $(p, f) \neq (3, 2)$, then the four largest automorphism orders of $\mathrm{PSL}_2(q)$ are $q + 1, q - 1, \frac{q+1}{2}, \frac{q-1}{2}$. Furthermore, $\mathrm{ord}(\alpha) \leq \frac{q-1}{2}$ for any $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q)) \setminus \mathrm{PGL}_2(q)$, where the inequality is strict for $q \neq 25$.*
- *The four largest automorphism orders of $\mathrm{PSL}_2(9) \cong \mathcal{A}_6$ are $10, 8, 6, 5$.*

For those parts of the argument where we will use Lemma 3.1.5, we will need some statements about centralizers in $\mathrm{Aut}(\mathrm{PSL}_2(q))$ for odd q:

Lemma 4.3.4. *(1) Let $p \geq 5$ be prime, and let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(p)) = \mathrm{PGL}_2(p)$ be of order p. Then $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(p))}(\alpha) = \langle \alpha \rangle \subseteq \mathrm{PSL}_2(p)$.*

(2) Let $q \geq 5$ be an odd prime power, $q \notin \{9, 25\}$, and let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ be of order $\frac{q-1}{2}$. Then $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\alpha) \subseteq \mathrm{PGL}_2(q)$.

(3) Let $q \geq 5$ be an odd prime power, $q \neq 9$, and let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ be of order $q-1$. Then $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\alpha) \subseteq \mathrm{PGL}_2(q)$.

(4) Let $q \geq 5$ be an odd prime power, and let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ be of order $\frac{q+1}{2}$. Then $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\alpha) \subseteq \mathrm{PGL}_2(q)$.

(5) Let $q \geq 5$ be an odd prime power, and let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ be of order $q+1$. Then $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\alpha) \subseteq \mathrm{PGL}_2(q)$.

Proof of Lemma 4.3.3. Denote by $\pi : \mathrm{Aut}(\mathrm{PSL}_2(q)) \to \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ the canonical projection.

For (1): That $q+1$ is the largest automorphism order is just a special case of Lemma 4.3.2(2), and $q-1$ is an automorphism order by the well-known element structure of $\mathrm{PGL}_2(q)$. It remains to show that $q = 2^f$ is not an automorphism order, which goes as follows: If $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ had order 2^f, then $2^f = \mathrm{ord}(\alpha) = \mathrm{ord}(\pi(\alpha)) \cdot \mathrm{ord}(\alpha^{\mathrm{ord}(\pi(\alpha))})$. Now by its element structure, the only element orders in $\mathrm{PGL}_2(q)$ which are powers of 2 are 1 and 2, and so $\mathrm{ord}(\alpha^{\mathrm{ord}(\pi(\alpha))}) \leq 2$, and thus $\mathrm{ord}(\pi(\alpha)) \geq 2^{f-1}$. But $\mathrm{ord}(\pi(\alpha)) \mid |\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_2)| = f$, a contradiction.

For (2,i): Since $\mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q)$ if q is prime, the statement follows from the element structure of $\mathrm{PGL}_2(q)$.

For (2,ii): Again, by the element structure of $\mathrm{PGL}_2(q)$, the four listed numbers are certainly the four largest element orders in $\mathrm{PGL}_2(q)$, so it suffices to prove the second part of the claim. Let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q)) \setminus \mathrm{PGL}_2(q)$, so that $e := \mathrm{ord}(\pi(\alpha)) > 1$. We need to show that $\mathrm{ord}(\alpha) \leq \frac{q-1}{2}$, and actually $\mathrm{ord}(\alpha) < \frac{q-1}{2}$ unless $q = 25$. By Lemma 4.3.2(1), it is sufficient to show that $e(q^{1/e}+1) < \frac{q-1}{2}$ for $q \neq 25$ (and to check that for $q = 25$, where $e = 2$, the left-hand side is equal to the right-hand side). For $q \neq 25$ (i.e., $q \geq 27$), note that it suffices to show

$$\frac{4}{3} e q^{1/e} < \frac{13}{27} q, \tag{1}$$

since

$$e(q^{1/e}+1) = e q^{1/e}(1 + \frac{1}{q^{1/e}}) \leq \frac{4}{3} e q^{1/e},$$

and

$$\frac{q-1}{2} = q(\frac{1}{2} - \frac{1}{2q}) \geq q(\frac{1}{2} - \frac{1}{54}) = \frac{13}{27} q.$$

Equation (1) is equivalent to

$$q \geq (\frac{36}{13} e)^{1 + \frac{1}{e-1}},$$

which is easy to verify in the case distinction $e = 2$ (where $q \geq 49$) versus $e \geq 3$ (using that $q \geq 3^e$).

For (2,iii): This is readily checked with GAP [6]. □

Proof of Lemma 4.3.4. For (1): By the element structure of $\mathrm{PGL}_2(p)$, we have $\alpha \in \mathrm{PSL}_2(p)$, and α is conjugate in $\mathrm{PGL}_2(p)$ to $\pi_0(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix})$ for some $x \in \mathbb{F}_p^*$, so it suffices to prove the assertion for all such elements. However, since they are powers of one another, it actually suffices to show the assertion for $\alpha = \pi_0(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix})$. So let $\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{GL}_2(p)$ such that

$$\pi_0(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}a & b\\ c & d\end{pmatrix} \cdot \begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}) = \pi_0(\begin{pmatrix}a & b\\ c & d\end{pmatrix}). \tag{2}$$

Equation (2) is equivalent to the existence of some $\mu \in \mathbb{F}_p^*$ such that

$$\begin{pmatrix}a+c & b+d-a-c\\ c & d-c\end{pmatrix} = \mu \cdot \begin{pmatrix}a & b\\ c & d\end{pmatrix}. \tag{3}$$

If $\mu \neq 1$, then a comparison of the bottom left entries in equation (3) implies $c = 0$ and thus also $a = 0$, a contradiction. So $\mu = 1$, turning equation (3) into a system of linear equations over $\mathbb{F}_p$ which one checks to be equivalent to $c = 0, a = d$. It follows that

$$\pi_0(\begin{pmatrix}a & b\\ c & d\end{pmatrix}) = \pi_0(\begin{pmatrix}a & b\\ 0 & a\end{pmatrix}) = \pi_0(\begin{pmatrix}1 & b/a\\ 0 & 1\end{pmatrix}) \in \langle\alpha\rangle.$$

For (2): Note that by Lemma 4.3.3(2,ii), α is an element of $\mathrm{PGL}_2(q)$, and so by the element structure of $\mathrm{PGL}_2(q)$, α is conjugate in $\mathrm{PGL}_2(q)$ to an element of the form $\pi_0(\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix})$ with $x \in \mathbb{F}_q^*$ of order $\frac{q-1}{2}$ (i.e., x generates the subgroup of squares in $\mathbb{F}_q^*$); it suffices to show that the centralizers in $\mathrm{Aut}(\mathrm{PSL}_2(q))$ of such elements are contained in $\mathrm{PGL}_2(q)$. We do so by contradiction: Assume that for some nontrivial field automorphism $\sigma = \mathrm{Frob}^e$ of $\mathbb{F}_q$, where Frob denotes the Frobenius automorphism of $\mathbb{F}_q$ and $1 \leq e < f$, and for some $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{GL}_2(q)$, we have

$$\pi_0(A\sigma \cdot \begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix} \cdot \sigma^{-1}A^{-1}) = \pi_0(\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix}). \tag{4}$$

Easy computations reveal that equation (4) is equivalent to the existence of some $\mu \in \mathbb{F}_q^*$ such that

$$\frac{1}{ad-bc} \cdot \begin{pmatrix}ad-\sigma(x)bc & ab(\sigma(x)-1)\\ cd(1-\sigma(x)) & \sigma(x)ad-bc\end{pmatrix} = \mu \cdot \begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix}. \tag{5}$$

Comparing the coefficients in the bottom left and top right corners in equation (5), we find that $ab = 0$ and $cd = 0$, so either $a = d = 0$ or $b = c = 0$. In the first case, comparing the coefficients in the top left corners of equation (5) gives $\mu = \sigma(x)$, and thus by comparing the coefficients in the bottom right corners of equation (5), $\sigma(x) = x^{-1}$, which implies $\frac{p^f-1}{2} \mid p^e+1$, or $p^f-1 \mid 2(p^e+1)$, although it is easy to check

that $2(p^e+1) \leq 2(p^{f-1}+1) < p^f - 1$, a contradiction. In the latter case, comparing the coefficients in the top left corners of equation (5) yields $\mu = 1$, and thus comparing the bottom right coefficients in equation (5), we get that $\sigma(x) = x$, which implies $\frac{p^f-1}{2} \mid p^e-1$, or $p^f-1 \mid 2(p^e-1)$, although $p^f-1 > p^f-p = p\cdot(p^{f-1}-1) > 2\cdot(p^e-1)$, a contradiction.

For (3): This follows with an argument analogous to the one for (2) (alternatively, one can observe that, except for the case $q = 25$, which can be checked with GAP, the statement follows from (2)).

For (4): Consider the natural embedding

$$\begin{aligned}\mathrm{Aut}(\mathrm{PSL}_2(q)) &= \mathrm{PGL}_2(q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)\\ &\hookrightarrow \mathrm{PGL}_2(q^2) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p) = \mathrm{Aut}(\mathrm{PSL}_2(q^2))\end{aligned}$$

extending the natural embedding $\mathrm{PGL}_2(q) \hookrightarrow \mathrm{PGL}_2(q^2)$, by means of which we view $\mathrm{Aut}(\mathrm{PSL}_2(q))$ as a subgroup of $\mathrm{Aut}(\mathrm{PSL}_2(q^2))$. By Lemma 4.3.3(2,ii), $\alpha \in \mathrm{PGL}_2(q)$, and by the element structure of $\mathrm{PGL}_2(q)$, α is conjugate in $\mathrm{PGL}_2(q^2)$ to an element of the form $\pi_1(\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix})$, where the order of $x \in \mathbb{F}_{q^2}^*$ is $\frac{q+1}{2}$. Denote by Frob the Frobenius automorphism of $\mathbb{F}_{q^2}$. It is sufficient to show that $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q^2))}(\pi_1(\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix})) \subseteq \mathrm{PGL}_2(q^2) \rtimes \langle \mathrm{Frob}^f \rangle$, since this implies that $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q^2))}(\alpha) \subseteq \mathrm{PGL}_2(q^2) \rtimes \langle \mathrm{Frob}^f \rangle$, and so

$$\begin{aligned}\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\alpha) &= \mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q^2))}(\alpha) \cap \mathrm{Aut}(\mathrm{PSL}_2(q))\\ &\subseteq (\mathrm{PGL}_2(q^2) \rtimes \langle \mathrm{Frob}^f \rangle) \cap \mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q).\end{aligned}$$

To see that among the elements of $\mathrm{Aut}(\mathrm{PSL}_2(q^2))$, $\pi_1(\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix})$ only commutes with elements from $\mathrm{PGL}_2(q^2) \rtimes \langle \mathrm{Frob}^f \rangle$, we proceed by contradiction, with the same ansatz as in point (2). This time, the divisibility relations at which one arrives in the two cases are $p^f + 1 \mid 2(p^e - 1)$ and $p^f + 1 \mid 2(p^e + 1)$ respectively. Note that now, $1 \leq e < 2f$, so we cannot argue as in point (2) that the supposed multiple is always smaller than the supposed divisor. However, this idea at least excludes the case $e < f$, so we may write $e = f + k$ with $0 \leq k < f$. Then it is easy to check that $2p^k - 1 < \frac{2(p^e-1)}{p^f+1} < 2p^k$, making the first case contradictory. Similarly, one can exclude $k > 0$ for the second case, leaving only $k = 0$, i.e., $e = f$.

For (5): This follows immediately from (4). □

Proof of Theorem 4.3.1. As pointed out before, point (1) of the theorem follows from Lemma 4.3.2(2), so we focus on the proof of point (2). Let $A = \mathrm{A}_{x,\alpha} \in \mathrm{Aff}(\mathrm{Aut}(\mathrm{PSL}_2(q)))$ be such that $\mathrm{ord}(A) = \mathrm{maffo}(\mathrm{Aut}(\mathrm{PSL}_2(q)))$. Set $o_1 := \mathrm{ord}(\alpha)$ and $o_2 := \mathrm{ord}(\mathrm{sh}_\alpha(x))$, so that $\mathrm{ord}(A) = o_1 \cdot o_2$, and note that $o_1, o_2 \leq q+1$.

If q is prime, then on the one hand, we cannot have $o_1 = o_2 = q+1$, since that would imply by Lemma 3.1.4 that $(q+1)^2 \mid |\mathrm{Aut}(\mathrm{PSL}_2(q))| = |\mathrm{PGL}_2(q)| = q(q^2-1)$, a contradiction. The next smaller potential order of A is $q(q+1)$, which is indeed

attained by Lemma 3.1.6 and the fact that $\mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q)$ contains both an element of order q and of order $q+1$.

If $q = 2^f$ with $f \geq 3$, then Lemma 3.1.4 again excludes the case $o_1 = o_2 = q+1 = 2^f+1$. By Lemma 4.3.3(1), the next smaller potential order of A is $(q+1)\cdot(q-1) = q^2-1$, which can be attained in view of Lemma 3.1.6.

Finally, consider the case $q = p^f$ with p an odd prime and $f \geq 2$. First, one verifies with GAP [6] that $\mathrm{maffo}(\mathrm{Aut}(\mathrm{PSL}_2(9))) = 40 = \frac{1}{2}(9^2-1)$ and that $\mathrm{maffo}(\mathrm{Aut}(\mathrm{PSL}_2(25))) = 312 = \frac{1}{2}(25^2-1)$, so we may henceforth assume that $(p,f) \notin \{(3,2),(5,2)\}$. By the element structure of $\mathrm{PGL}_2(q)$ and Lemma 3.1.6, it is clear that $\frac{1}{2}(q^2-1)$ can be attained as the order of some bijective affine map of $\mathrm{Aut}(\mathrm{PSL}_2(q))$, so it remains to show that $o_1 \cdot o_2 \leq \frac{1}{2}(q^2-1)$. We do this in a case distinction.

First assume that $o_1 = q+1$, so that by Lemma 4.3.3(2,ii), $\alpha \in \mathrm{PGL}_2(q)$. Then the inequality is equivalent to $o_2 \leq \frac{q-1}{2}$. If $o_2 > \frac{q-1}{2}$, by Lemma 4.3.3(2,ii) again, it follows that $o_2 \in \{q+1, q-1, \frac{q+1}{2}\}$. In each of these three cases, using Lemma 3.1.5 and Lemma 4.3.4(5,3,4) respectively, we conclude that $x \in \mathrm{PGL}_2(q)$. This gives a contradiction when $o_2 = q+1$ or $o_2 = q-1$, since by the fact that $[\mathrm{PGL}_2(q) : \mathrm{PSL}_(q)] = 2$ and o_1 is even, we get that $\mathrm{sh}_\alpha(x) \in \mathrm{PSL}_2(q)$, but $\mathrm{PSL}_2(q)$ does not have any elements of order $q+1$ or $q-1$. The case $o_2 = \frac{q+1}{2}$ can be refuted by Lemma 3.1.4 (applied to $G := \mathrm{PGL}_2(q)$) again.

Next assume that $o_1 = q-1$, in which case $\alpha \in \mathrm{PGL}_2(q)$ as well. The inequality is equivalent to $o_2 \leq \frac{q+1}{2}$, so it remains to exclude the two cases $o_2 = q+1$ and $o_2 = q-1$, which can be done as in the previous case, deriving the contradictory $\mathrm{sh}_\alpha(x) \in \mathrm{PSL}_2(q)$.

If $o_1 = \frac{q+1}{2}$, we only need to exclude the case $o_2 = q+1$, which can be done as in the case $o_1 = q+1$ using Lemma 3.1.4. Finally, if $o_1 \leq \frac{q-1}{2}$, then the inequality holds for sure. □

It now follows by some easy computations that $\mathrm{mao}(\mathrm{PSL}_2(q)) > |\mathrm{PSL}_2(q)|^{\frac{1}{3}}$ for all prime powers $q \geq 5$, and $\mathrm{maffo}(\mathrm{Aut}(\mathrm{PSL}_2(q))) \geq |\mathrm{PSL}_2(q)|^{\frac{2}{3}}$ if and only if q is a prime, in which case $\mathrm{maffo}(\mathrm{Aut}(\mathrm{PSL}_2(q))) = q(q+1)$, and verification of the statements about strict monotonous convergence of the upper bounds is also easy. This settles our discussion of the subcase $n = 1$.

4.3.2 Useful observations for the other subcases

The following lemma is immediate from the element structure of $\mathrm{PGL}_2(p)$:

Lemma 4.3.5. *Let $p \geq 5$ be a prime, and let $A \in \mathrm{Aff}(\mathrm{PGL}_2(p))$. Then $\mathrm{ord}(A)$ is a divisor of one of the following: $p(p+1), p(p-1), p^2-1$.* □

Another useful observation (similar in spirit to Lemma 3.4.2(2)) is the following: Since $\mathrm{maffo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^n)) \leq \mathrm{mao}(\mathrm{PSL}_2(q)^n)^2$, whenever $\mathrm{mao}(\mathrm{PSL}_2(q)^n) \leq |\mathrm{PSL}_2(q)|^{\frac{n}{3}}$, we can conclude that $\mathrm{maffo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^n)) \leq |\mathrm{PSL}_2(q)|^{\frac{2n}{3}}$.

4.3.3 Subcase: $n = 2$

Clearly, for primes $p \geq 5$, $\mathrm{mao}(\mathrm{PSL}_2(p)^2) = \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(p)) \wr \mathcal{S}_2)$ is bounded from below by $p(p+1) = \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(p))^2)$, and by Lemma 3.2.2, elements from $\mathrm{Aut}(\mathrm{PSL}_2(p)^2) \setminus \mathrm{Aut}(\mathrm{PSL}_2(p))^2$ have order bounded from above by $2 \cdot (p+1) < p(p+1)$, so indeed, we have $\mathrm{mao}(\mathrm{PSL}_2(p)^2) = p(p+1) > (\frac{1}{2}p(p^2-1))^{\frac{2}{3}}$. As for $q \geq 5$ that are not prime, we first verify directly with GAP [6] that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(9)^2)) = 40 < 360^{2/3}$. For all other odd q, we can use Lemma 4.3.3(2,ii) to conclude that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^2)) = \frac{1}{2}(q^2-1) < (\frac{1}{2}q(q^2-1))^{\frac{2}{3}}$, and Lemma 3.2.2 to treat automorphisms outside $\mathrm{Aut}(\mathrm{PSL}_2(q)^2)$ as before. Finally, for $q = 2^f$ with $f \geq 3$, by Lemma 4.3.3(1), we have $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^2)) = q^2 - 1 < (q(q^2-1))^{\frac{2}{3}}$, and we can treat all other automorphisms by Lemma 3.2.2 again.

As for maffo-values in the subcase $n = 2$, by the "useful observation" after Lemma 4.3.5, it remains to show that $\mathrm{maffo}(\mathrm{Aut}(\mathrm{PSL}_2(p)^2)) \leq |\mathrm{PSL}_2(p)|^{\frac{4}{3}}$ for primes $p \geq 5$. It is easily checked with GAP [6] that $\mathrm{maffo}(\mathrm{Aut}(\mathrm{PSL}_2(5)^2)) = 120 < 60^{\frac{4}{3}}$, so we may assume $p \geq 7$ from now on. Let $A = \mathrm{A}_{x,\alpha}$ be a bijective affine map of $\mathrm{Aut}(\mathrm{PSL}_2(p)^2)$. We know that we can identify α with an element in $\mathrm{Aut}(\mathrm{PSL}_2(p)^2)$, that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(p))^2) = p(p+1)$ and that the maximum element order in the complement $\mathrm{Aut}(\mathrm{PSL}_2(p)^2) \setminus \mathrm{Aut}(\mathrm{PSL}_2(p))^2$ is bounded from above by $2 \cdot (p+1)$. Therefore, if not both $\alpha, \mathrm{sh}_\alpha(x) \in \mathrm{Aut}(\mathrm{PSL}_2(p))^2$, then the order of A is at most $2(p+1) \cdot p(p+1) < (\frac{1}{2}p(p^2-1))^{\frac{4}{3}}$. So we may assume $\alpha, \mathrm{sh}_\alpha(x) \in \mathrm{Aut}(\mathrm{PSL}_2(p))^2$ from now on, and also $\mathrm{ord}(A) > 2(p+1) \cdot p(p+1)$. The latter implies that the two components of $\mathrm{sh}_\alpha(x)$ must be of different order. But conjugation of $\mathrm{sh}_\alpha(x)$ by any element from $\mathrm{Aut}(\mathrm{PSL}_2(p)^2) \setminus \mathrm{Aut}(\mathrm{PSL}_2(p)^2)$ swaps the orders of the components, and so $\mathrm{sh}_\alpha(x)$ cannot commute with any such element. In other words, $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(p)^2)}(\mathrm{sh}_\alpha(x)) \subseteq \mathrm{Aut}(\mathrm{PSL}_2(p))^2$, and so, by an application of Lemma 3.1.5, we conclude that $x \in \mathrm{Aut}(\mathrm{PSL}_2(p))^2$. Together with $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(p))^2$, this implies that A decomposes as a product $A_1 \times A_2$, with $A_1, A_2 \in \mathrm{Aff}(\mathrm{Aut}(\mathrm{PSL}_2(p)))$. Therefore, by Lemma 4.3.5, $\mathrm{ord}(A) = \mathrm{lcm}(\mathrm{ord}(A_1), \mathrm{ord}(A_2)) \leq p(p^2-1) < (\frac{1}{2}p(p^2-1))^{\frac{4}{3}}$.

4.3.4 Subcase: $n = 3$

Denote by $\pi_3 : \mathrm{Aut}(\mathrm{PSL}_2(q)^3) = \mathrm{Aut}(\mathrm{PSL}_2(q)) \wr \mathcal{S}_3 \to \mathcal{S}_3$ the canonical projection. By a simple case distinction according to the cycle type of $\pi_3(\alpha)$, Lemma 3.2.2 can be used to show that automorphisms α outside $\mathrm{Aut}(\mathrm{PSL}_2(q))^3$ have order bounded from above by $2q(q+1) < |\mathrm{PSL}_2(q)|$ in all cases. If q is a prime, then since the element orders in $\mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q)$ are just the divisors of $q+1, q$ and $q-1$, we have $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q))^3) = \mathrm{lcm}(q+1, q, q-1) = \frac{1}{2}q(q^2-1) = |\mathrm{PSL}_2(q)|^{\frac{3}{3}}$. If $q = 2^f$ with $f \geq 3$, by Lemma 4.3.3(1), we have $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^3)) < (q+1)(q-1)^2 < |\mathrm{PSL}_2(q)|$. For $q = 9$, one checks with GAP [6] that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(9)^3)) = 120 < 360$, and for odd $q \geq 25$, using Lemma 4.3.3(2,ii), we have $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q))^3) < \frac{1}{2}(q+1)(q-1)^2 < |\mathrm{PSL}_2(q)|$.

4.3.5 Subcase: $n = 4$

We will show $\mathrm{mao}(\mathrm{PSL}_2(q)^4) < |\mathrm{PSL}_2(q)|^{\frac{4}{3}}$ for all prime powers $q \geq 5$. For $q = 5$, one can check directly that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(5))^4) = 60 < 60^{\frac{4}{3}}$, and automorphisms α from outside $\mathrm{Aut}(\mathrm{PSL}_2(5))^4$ are treated with Lemma 3.2.2 like before. Assuming $q \geq 7$, and using that $[\mathrm{Aut}(\mathrm{PSL}_2(q)) : \mathrm{PGL}_2(q)] = \log_p(q)$, we have $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^4)) \leq g(4) \cdot \exp(\mathrm{Aut}(\mathrm{PSL}_2(q))) \leq 4 \cdot \log_p(q) \cdot p \cdot \frac{q^2-1}{\gcd(2,q-1)} \leq 4 \cdot |\mathrm{PSL}_2(q)| < |\mathrm{PSL}_2(q)|^{\frac{4}{3}}$.

4.3.6 Subcase: $n \geq 5$

Here we can use crude upper bounds and "get away with it"; it is sufficient and easy to verify that

$$\mathrm{mao}(\mathrm{PSL}_2(q)^n) \leq g(n) \cdot \exp(\mathrm{Aut}(\mathrm{PSL}_2(q))) < 3^{\frac{n}{3}} \cdot |\mathrm{PSL}_2(q)| \leq |\mathrm{PSL}_2(q)|^{n/3}.$$

4.4 Case: $S = \mathrm{PSL}_d(q), d \geq 3, q \geq 2$

From now on, we will always work with Lemma 3.4.2(2). Furthermore, we will use the information on maximum automorphism orders of finite simple groups from [8, Table 3]. Note that since $\mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$, we may assume that $(d, q) \neq (3, 2)$, and so $\mathrm{mao}(\mathrm{PSL}_d(q)) = \frac{q^d-1}{q-1}$. In view of $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_d(q))^n) \leq \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_d(q)))^n$, our goal is to show that

$$g(n) \cdot \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_d(q)))^n < |\mathrm{PSL}_d(q)|^{\frac{n}{3}} = \left(\frac{q^{d(d-1)/2}}{\gcd(d, q-1)} \cdot \prod_{i=2}^{d} (q^i - 1)\right)^{\frac{n}{3}}. \quad (6)$$

4.4.1 Subcase: $d = 3, 4, 5$

For $d = 3$, we treat the subsubcases $q = 3$ and $q = 4$ separately. Using GAP [6], one finds that the element orders in $\mathrm{Aut}(\mathrm{PSL}_3(3))$ are $1, 2, 3, 4, 6, 8, 12, 13$. By this, one can check directly that $g(n) \cdot \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_3(3))^n) < |\mathrm{PSL}_3(3)|^{\frac{n}{3}} = 5616^{\frac{n}{3}}$ for $n = 1, 2$, and it implies that $g(n) \cdot \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_3(3)^n)) = g(n) \cdot 312 < 5616^{n/3}$ for $n \geq 3$. The subsubcase $q = 4$ is treated analogously. For $q \geq 5$, the stronger inequality obtained by replacing $g(n)$ by $3^{n/3}$ in equation (6) is easy to verify.

For $d = 4$ and $d = 5$, again, the stronger inequality obtained by substituting $3^{n/3}$ for $g(n)$ in equation (6) is easy to verify.

4.4.2 Subcase: $d \geq 6$

One can check that $2d \leq \frac{d(d-1)}{2} - 2$ for $d \geq 6$. The left-hand side of equation (6) is therefore bounded from above by

$$\begin{aligned}(q^2)^{\frac{n}{3}} \cdot (q^d - 1)^n &< (q^2)^{\frac{n}{3}} \cdot (q^d - 1)^{\frac{n}{3}} \cdot (q^{2d})^{\frac{n}{3}} \\ &\leq (q^2)^{\frac{n}{3}} \cdot (q^d - 1)^{\frac{n}{3}} \cdot (q^{\frac{d(d-1)}{2}-2})^{\frac{n}{3}} = (q^{d(d-1)/2} \cdot (q^d - 1))^{\frac{n}{3}},\end{aligned}$$

which is obviously smaller than the right-hand side of equation (6).

4.5 Case S is a classical group of Lie type not isomorphic to any $\mathrm{PSL}_d(q)$

These can all be treated with arguments analogous to the ones used for the $\mathrm{PSL}_d(q)$ with $d \geq 3$ in the previous subcase (Subsection 4.4), mostly by verifying an inequality of the form $g(n) \cdot o(S)^n < |S|^{\frac{n}{3}}$, where $o(S)$ is an upper bound on $\mathrm{mao}(S)$ read off from [8, Table 3]. There is just one particular case where that inequality does not hold, namely $S = \mathrm{PSU}_3(5)$; this group can be treated like $\mathrm{PSL}_3(3)$.

4.6 Case: S is an exceptional group of Lie type

Guest, Morris, Praeger and Spiga [8, Proof of Theorem 1.2] derived upper bounds on $\mathrm{mao}(S)$ for such S, based on the information on largest element orders of exceptional Lie type groups of odd characteristic from [12, Table A.7], the upper bounds on largest element orders for those of even characteristic from [8, Table 5], and information on outer automorphism group orders of such groups from [3, Table 5, p. xvi]. Denoting their upper bound by $o(S)$, one can, in almost all cases, prove the sufficient inequality

$$g(n) \cdot o(S)^n < |S|^{\frac{n}{3}} \tag{7}$$

with arguments similar to those used in the nonexceptional cases. There are three groups where a different approach is necessary, namely $S = {}^2\mathrm{B}_2(2), {}^3\mathrm{D}_4(2), {}^2\mathrm{F}_4(2)'$. ${}^2\mathrm{B}_2(2)$ can be treated like $\mathrm{PSL}_3(3)$ in Subsection 4.4. For the last two S, one reads off the precise value of $\mathrm{meo}(S)$ and of $|\operatorname{Out}(S)|$ from [3], sets $o(S) := \mathrm{meo}(S) \cdot |\operatorname{Out}(S)|$ and easily verifies equation (7) for that value of $o(S)$.

5 On relative functions on finite groups

5.1 Some general theory

Assume we have given a function f assigning to each finite group a number from the real interval $[0, 1]$ (for example, f could be the function assigning to G the quotient $\mathrm{mao}(G)/|G|$). For proving that a condition of the form $f(G) \geq \rho$ for fixed $\rho \in (0, 1)$ results in a restriction on the structure of G, it is useful if we know that f "respects" the structure of finite groups in some sense. Examples of such useful properties of f are given in the following definition:

Definition 5.1.1. *A function f from the class of finite groups to the real interval $[0, \infty)$ such that $f(G_1) = f(G_2)$ whenever G_1 and G_2 are isomorphic is called a **group-theoretic function**, and a group-theoretic function f is called a **relative function** if and only if $f(G) \leq 1$ for all finite groups G. Assume that f is a group-theoretic function. Then:*

*(1) f is called **characteristically submultiplicative (C-submultiplicative)** if and only if for all finite groups G and all $N \operatorname{char} G$, we have $f(G) \leq f(N) \cdot f(G/N)$.*

*(2) f is called **increasing on characteristic quotients (CQ-increasing)** if and only if for all finite groups G and all $N \operatorname{char} G$, we have $f(G) \geq f(G/N)$.*

(3) f is called ***increasing on characteristic subgroups (CS-increasing)*** *if and only if for all finite groups G and all $N \operatorname{char} G$, we have $f(G) \geq f(N)$.*

Clearly, relative C-submultiplicative functions are both CQ-increasing and CS-increasing.

Example 5.1.2. (1) The relative function l_{-1} is C-submultiplicative, see [9, Lemma 1.2]. Actually, this property was one of the key ingredients in Hegarty's proof that the derived length of a finite solvable group G with $\mathrm{l}_{-1}(G) \geq \rho$ is bounded from above in terms of ρ, see also Section 7.

(2) All the relative functions l_e are CQ-increasing, since the fraction of elements of G raised to the e-th power by some automorphism α is at most as large as the fraction of elements of G/N, $N \operatorname{char} G$, raised to the e-th power by the automorphism of G/N induced by α. However, l_2 is *not* CS-increasing (and thus not C-submultiplicative), as follows from studying the example $(\mathbb{Z}/2\mathbb{Z})^2 \cong \langle (1,2)(3,4), (1,3)(2,4) \rangle \operatorname{char} \mathcal{A}_4$.

(3) By [1, Lemma 2.1.3], the relative function λ_{aff} is C-submultiplicative, and the relative function λ is CQ-increasing. However, λ is not CS-increasing, as $\lambda(\mathbb{Z}/6\mathbb{Z}) = 1/3 < 1/2 = \lambda(\mathrm{D}_{12})$, although D_{12} contains a characteristic subgroup isomorphic with $\mathbb{Z}/6\mathbb{Z}$.

The following simple lemma outlines our basic strategy for proving the upper bounds on the index of $\mathrm{Rad}(G)$ in Theorems 1.1.1(3) and 1.1.3(2):

Lemma 5.1.3. *Let f be a CQ-increasing group-theoretic function, and assume that for finite semisimple groups H, $f(H) \to 0$ as $|H| \to \infty$; more explicitly, fix a function $g : (0,\infty) \to (0,\infty)$ such that for any $\rho \in (0,\infty)$, $f(H) < \rho$ whenever H is a finite semisimple group with $|H| > g(\rho)$.*

Then for any $\rho \in (0,\infty)$, if G is a finite group such that $f(G) \geq \rho$, then $[G : \mathrm{Rad}(G)] \leq g(\rho)$.

Proof. By assumption, we have $f(G/\operatorname{Rad}(G)) \geq f(G) \geq \rho$. Since $G/\operatorname{Rad}(G)$ is semisimple, this implies $[G : \mathrm{Rad}(G)] = |G/\operatorname{Rad}(G)| \leq g(\rho)$ by choice of g. □

Remark 5.1.4. Note that we did not use the full power of the assumption that f be CQ-increasing in the proof of Lemma 5.1.3; for the proof to work, it would be enough to know that $f(G/\operatorname{Rad}(G)) \geq f(G)$ for all finite groups G; let us call such group-theoretic functions f *RadQ-increasing* (see also Remark 5.2.10).

5.2 Some nontrivial examples of "well-behaved" functions

Of course, for proving our main results, we would like to apply Lemma 5.1.3 to the following two group-theoretic functions:

Definition 5.2.1. *For a finite group G, we define* $\mathrm{mao}_{\mathrm{rel}}(G) := \mathrm{mao}(G)/|G|$ *and* $\mathrm{maffo}_{\mathrm{rel}}(G) := \mathrm{maffo}(G)/|G|$.

To this end, we would like to prove that they are both CQ-increasing and tend to 0 on finite semisimple groups whose orders tend to ∞. The latter follows immediately

from Theorem 4.4, and for the rest of this subsection, we will be concerned with proving that the two functions are CQ-increasing.

Now trying to establish a "transfer lemma" for $\mathrm{maffo}_{\mathrm{rel}}$ similar to [1, Lemma 2.1.3] yields the following result:

Lemma 5.2.2. *Let G be a finite group, $A = \mathrm{A}_{x,\alpha}$ a bijective affine map of G and $N \operatorname{char} G$. Denote by $\pi : G \to G/N$ the canonical projection and by $\tilde{\alpha}$ the automorphism of G/N induced by α. Let $\tilde{A} = \mathrm{A}_{\pi(x),\tilde{\alpha}}$ denote the bijective affine map of G/N induced by A, and set $o := \operatorname{ord}(\tilde{A})$. Then $\operatorname{ord}(A)$ is a divisor of $o \cdot \operatorname{lcm}_{n\in N} \operatorname{ord}(\mathrm{A}_{n,(\alpha_{|N})^o})$.*

Proof. Clearly, o divides $\operatorname{ord}(A)$, so we only need to show that $\operatorname{ord}(A^o)$ divides $\operatorname{lcm}_{n\in N} \operatorname{ord}(\mathrm{A}_{n,(\alpha_{|N})^o})$. Now by definition of o, A^o restricts to a permutation on each coset of N in G, and the order of A^o is the least common multiple of the orders of the restrictions of A^o to the various cosets. But by [1, Lemma 2.1.3] each action of A^o on a coset of N is isomorphic (in the sense of an isomorphism of finite dynamical systems, see [1, remarks after Definition 1.1.5]) with the action on N of some bijective affine map of N of the form $\mathrm{A}_{n,(\alpha_{|N})^o}$. The result follows. □

Unfortunately, this result is not strong enough to imply that either of $\mathrm{mao}_{\mathrm{rel}}$ and $\mathrm{maffo}_{\mathrm{rel}}$ is CQ-increasing. However, it led the author to study the following curious function on finite groups, which eventually resulted in a proof of this property for the two functions:

Definition 5.2.3. *For a finite group G, we define*

$$\mathfrak{f}(G) := \frac{1}{|G|} \cdot \max_{\alpha\in\mathrm{Aut}(G)} (\operatorname{lcm}_{x\in G} \operatorname{ord}(\mathrm{A}_{x,\alpha})).$$

Note that in view of the natural isomorphism $\mathrm{Hol}(G) \to \mathrm{Aff}(G)$, $\mathfrak{f}(G)$ can also be defined as follows: The cosets of the canonical copy of G inside $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$ are in bijective correspondence with automorphisms α of G. For each such coset, consider the least common multiple of the orders of all its elements, and denote the maximum of all such least common multiples by $\mathfrak{F}(G)$. Then $\mathfrak{f}(G) = \mathfrak{F}(G)/|G|$.

It is clear that $\mathfrak{f}(G_1) = \mathfrak{f}(G_2)$ whenever $G_1 \cong G_2$ and that $\mathfrak{f} > 0$. One can also show with a rather simple argument that $\mathfrak{f}$ is C-submultiplicative:

Lemma 5.2.4. *The group-theoretic function $\mathfrak{f}$ is C-submultiplicative, i.e., for all finite groups G and $N \operatorname{char} G$, we have $\mathfrak{f}(G) \leq \mathfrak{f}(N) \cdot \mathfrak{f}(G/N)$.*

Proof. Let us prove the equivalent $\mathfrak{F}(G) \leq \mathfrak{F}(N) \cdot \mathfrak{F}(G/N)$. Fix an automorphism α of G such that $\mathfrak{F}(G) = \operatorname{lcm}_{x\in G} \operatorname{ord}(\mathrm{A}_{x,\alpha}) =: L$. Denote by $\tilde{\alpha}$ the automorphism of G/N induced by α, by $\pi : G \to G/N$ the canonical projection, and set $L_1 := \operatorname{lcm}_{y\in G/N} \operatorname{ord}(\mathrm{A}_{y,\tilde{\alpha}})$. Clearly, $L_1 \leq \mathfrak{F}(G/N)$. On the other hand, setting $L_2 := \operatorname{lcm}_{x\in G} \operatorname{ord}(\mathrm{A}_{x,\alpha}^{L_1})$, since each $\operatorname{ord}(\mathrm{A}_{x,\alpha})$ divides $L_1 \cdot L_2$, L divides and thus is bounded from above by $L_1 \cdot L_2$, so it suffices to show that $L_2 \leq \mathfrak{F}(N)$. Now as in the proof of Lemma 5.2.2, each $\operatorname{ord}(\mathrm{A}_{x,\alpha}^{L_1})$ is a least common multiple of orders of bijective affine maps of N of the form $\mathrm{A}_{n,(\alpha_{|N})^{L_1}}$ for various $n \in N$. But therefore, L_2 itself is also a least common multiple of such orders, and thus bounded from above by $\mathfrak{F}(N)$, as we wanted to show. □

However, for establishing that $\mathrm{mao}_{\mathrm{rel}}$ and $\mathrm{maffo}_{\mathrm{rel}}$ are CQ-increasing, we would rather be interested in proving that $\mathfrak{f}$ is relative. Our proof of this will make use of the CFSG.

Theorem 5.2.5. *For all finite groups G, $\mathfrak{f}(G) \leq 1$. In particular, for all finite groups G, we have* $\mathrm{meo}(\mathrm{Hol}(G)) \leq |G|$.

Before proving Theorem 5.2.5, we need three auxiliary results. The first provides some sufficient conditions for a least common multiple as in the definition of $\mathfrak{f}$ to be bounded by the group order:

Lemma 5.2.6. *Let G be a finite group, $\alpha \in \mathrm{Aut}(G)$.*
(1) If $\mathrm{ord}(\alpha) \mid |G|$, then $\mathrm{lcm}_{x \in G} \mathrm{ord}(\mathrm{A}_{x,\alpha}) \mid |G|$.
(2) For every prime $p \mid |G|$, we have

$$\mathrm{lcm}_{x \in G} \mathrm{ord}(\mathrm{A}_{x,\alpha}) \mid \prod_{q \mid\mid G|, q \neq p} q^{\nu_q(|G|)} \cdot p^{2\nu_p(\exp(G))} \cdot \exp(\mathrm{Out}(G)).$$

In particular, if, for some prime $p \mid |G|$, we have

$$p^{2\nu_p(\exp(G))} \cdot \exp(\mathrm{Out}(G)) \leq p^{\nu_p(|G|)},$$

then $\mathrm{lcm}_{x \in G} \mathrm{ord}(A_{x,\alpha}) \leq |G|$.

Proof. For (1): Fix $x \in G$. We will show that $\mathrm{ord}(\mathrm{A}_{x,\alpha})$. which equals $\mathrm{ord}(\alpha) \cdot \mathrm{ord}(\mathrm{sh}_\alpha(x))$, divides $|G|$. This is tantamount to proving that for any prime p, we have $\nu_p(\mathrm{ord}(\alpha)) + \nu_p(\mathrm{ord}(\mathrm{sh}_\alpha(x))) \leq \nu_p(|G|)$. This is clear (*inter alia* by assumption) if p divides at most one of the two numbers $\mathrm{ord}(\alpha)$ and $\mathrm{ord}(\mathrm{sh}_\alpha(x))$, and if p divides both these numbers, the inequality holds by Lemma 3.1.4.

For (2): Again, we fix $x \in G$. We shall prove that

$$\mathrm{ord}(\alpha) \cdot \mathrm{ord}(\mathrm{sh}_\alpha(x)) \mid \prod_{q \mid\mid G|, q \neq p} q^{\nu_q(|G|)} \cdot p^{2\nu_p(\exp(G))} \cdot \exp(\mathrm{Out}(G)).$$

Denoting by $\pi : \mathrm{Aut}(G) \to \mathrm{Out}(G)$ the canonical projection and noting that $\mathrm{ord}(\alpha) = \mathrm{ord}(\pi(\alpha)) \cdot \mathrm{ord}(\alpha^{\mathrm{ord}(\pi(\alpha))})$ with $\mathrm{ord}(\pi(\alpha)) \mid \exp(\mathrm{Out}(G))$, we find that it is sufficient to prove that $\mathrm{ord}(\alpha^{\mathrm{ord}(\pi(\alpha))}) \cdot \mathrm{ord}(\mathrm{sh}_\alpha(x)) \mid \prod_{q \mid\mid G|, q \neq p} q^{\nu_q(|G|)} \cdot p^{2\nu_p(\exp(G))}$. Fix a prime l. If l divides at most one of the numbers $\mathrm{ord}(\alpha^{\mathrm{ord}(\pi(\alpha))})$ and $\mathrm{ord}(\mathrm{sh}_\alpha(x))$, it is clear that the corresponding inequality of l-adic valuations holds. Hence assume that l divides both these numbers. If $l \neq p$, we are done by an application of Lemma 3.1.4, and if $l = p$, we are done since both orders divide $p^{\nu_p(\exp(G))}$. □

We will also need the following well-known result:

Lemma 5.2.7. *Let p be a prime, K a field of characteristic p, $d \in \mathbb{N}^+$. Let $A \in \mathrm{GL}_d(K)$ be of finite order. Then $\nu_p(\mathrm{ord}(A)) \leq \lceil \log_p(d) \rceil$.* □

The final lemma concerns orders of non-fixed-point-free automorphisms of finite vector spaces over prime fields:

Lemma 5.2.8. *Let V be a finite vector space over $\mathbb{F}_p$ and α a non-fixed-point-free automorphism of V (i.e., $\alpha(v) = v$ for some $v \in V \setminus \{0\}$). Then* $\mathrm{ord}(\alpha) \leq |V|/p$.

Proof. Considering the primary rational canonical form of α (corresponding to a decomposition of V into a maximal number of subspaces that are cyclic for α), we may assume by induction that α can be represented by the companion matrix of $P(X)^k$ for some irreducible $P(X) \in \mathbb{F}_p[X]$. That α is not fixed-point-free translates into the existence of a nonzero $Q(X) \in \mathbb{F}_p[X]$ of degree less than $\deg(P(X)^k)$ such that $X \cdot Q(X) \equiv Q(X) \pmod{P(X)^k}$, or equivalently $P(X)^k \mid Q(X) \cdot (X-1)$. Since $P(X)^k \nmid Q(X)$, it follows that $P(X) \mid X-1$, and thus $P(X) = X-1$ by irreducibility. In view of the formula for the order of the companion matrix of $P(X)^k$ (first proved by Elspas [5, Appendix II, 9], see also [14, Theorem 3.11] and [10, Theorem 5 and remarks afterward]), it follows that $\mathrm{ord}(\beta) = p^{\lceil \log_p(k) \rceil} \leq p^{k-1} = \frac{1}{p}|V|$. □

Proof of Theorem 5.2.5. The proof is by induction on $|G|$. For the induction step, note that if G is not characteristically simple, then fixing any proper nontrivial characteristic subgroup N of G, we have, by Lemma 5.2.4 and the induction hypothesis, $\mathfrak{f}(G) \leq \mathfrak{f}(N) \cdot \mathfrak{f}(G/N) \leq 1 \cdot 1 = 1$. Hence we may assume that G is characteristically simple, i.e., $G = S^n$ for some finite (not necessarily nonabelian) simple group S and $n \in \mathbb{N}^+$.

Let us first assume that S is abelian, i.e., $S = \mathbb{Z}/p\mathbb{Z}$ for some prime p. Fix an automorphism α of G such that $\mathrm{lcm}_{x \in G} \mathrm{ord}(\mathrm{A}_{x,\alpha}) = \mathfrak{F}(G)$. In view of the formula $\mathrm{ord}(\mathrm{A}_{x,\alpha}) = \mathrm{ord}(\alpha) \cdot \mathrm{ord}(\mathrm{sh}_\alpha(x))$ and the fact that all elements of G have order 1 or p, we get that $\mathfrak{F}(G)$ is equal to either $\mathrm{ord}(\alpha) \cdot p$ or $\mathrm{ord}(\alpha)$, according to whether or not one of the shifts $\mathrm{sh}_\alpha(x)$ for the various $x \in G$ is nontrivial or not. But in the latter case, $\mathfrak{F}(G) < |G|$ by [11, Theorem 2], so assume that the first case applies. Note that all $\mathrm{sh}_\alpha(x)$ are fixed points of α (this is easy to check directly, and it is also a special case of Lemma 3.1.5, applied to $\mathrm{Hol}(G)$ and using that G is abelian). Hence α is not fixed-point-free, and so by Lemma 5.2.8, we get that $\mathfrak{F}(G) = p \cdot \mathrm{ord}(\alpha) \leq |G|$, q.e.d.

So we may henceforth assume that S is nonabelian. Let us first treat the case $n \geq 2$. Note that by Lemma 4.2(1), we have $\mathrm{mao}(S^n) < |S^n|^{0.438}$. Furthermore, $\exp(S^n) = \exp(S) \leq |S| \leq |S^n|^{0.5}$. It follows that $\mathrm{lcm}_{x \in S^n} \mathrm{ord}(\mathrm{A}_{x,\alpha}) = \mathrm{ord}(\alpha) \cdot \mathrm{lcm}_{x \in S^n} \mathrm{ord}(\mathrm{sh}_\alpha(x)) \leq |S^n|^{0.438} \cdot |S^n|^{0.5} < |S^n|$.

We may thus henceforth assume that $G = S$ is a nonabelian finite simple group. It is well-known that the Sylow 2-subgroups of S are not cyclic, whence we are done by Lemma 5.2.6(1) if $\exp(\mathrm{Out}(S)) \leq 2$. This settles all alternating and all sporadic S.

Now assume that S is of Lie type. We will treat this case mostly by applications of Lemma 5.2.6(2), with p always equal to the defining characteristic of S. Hence our goal is to show the inequality $p^{2\nu_p(\exp(S))} \cdot \exp(\mathrm{Out}(S)) \leq p^{\nu_p(|S|)}$. To this end, we use information on $|S|$ and $|\mathrm{Out}(S)|$ from [3, p. xvi, Tables 5 and 6]; moreover, note that by Lemma 5.2.7, if $d_p(S)$ denotes the minimum faithful projective representation degree of S in characteristic p, then $\nu_p(\exp(S)) \leq \lceil \log_p(d_p(S)) \rceil$. The values of $d_p(S)$ for the various finite simple groups of Lie type can be found in [13, p. 200, Table 5.4.C].

Verification of $p^{2\lceil \log_p(d_p(S))\rceil} \cdot |\operatorname{Out}(S)| \leq p^{\nu_p(|S|)}$, which is sufficient, is straightforward for $S = \mathrm{PSL}_2(p^f)$ with $f \geq 3$, with the exception of the cases $(p,f) = (2,3),(3,3),(5,3)$, for $S = \mathrm{PSL}_d(q)$ with $d \geq 3$, with the exception of $(d,q) = (3,2),(3,4)$, and for all S of Lie type which are not isomorphic with any $\mathrm{PSL}_d(q)$.

For $S = \mathrm{PSL}_2(p)$ with $p \geq 5$ or $S = \mathrm{PSL}_2(p^2)$ with $p \geq 3$, we note that $\exp(\operatorname{Out}(S)) = 2$, whence we are done as in the alternating and sporadic case. The same applies to $S = \mathrm{PSL}_3(2)$. Finally, one can check with GAP [6] that for $S = \mathrm{PSL}_2(8), \mathrm{PSL}_2(27), \mathrm{PSL}_2(125), \mathrm{PSL}_3(4)$, all automorphism orders of S divide $|S|$, whence Lemma 5.2.6(1) can be applied to conclude the proof. □

Theorem 5.2.5 has the following consequences:

Corollary 5.2.9. *(1) The group-theoretic function* $\mathrm{maffo}_{\mathrm{rel}}$ *is relative.*
(2) The group-theoretic functions $\mathrm{mao}_{\mathrm{rel}}$ *and* $\mathrm{maffo}_{\mathrm{rel}}$ *are both CQ-increasing.*

Proof. (1) is just a reformulation of the "In particular" in Theorem 5.2.5. As for (2), fix a finite group G and N char G, and let A be an automorphism (resp. bijective affine map) of G of maximal order. Combining the results of Lemma 5.2.2 and Theorem 5.2.5, we obtain that the order of A, which equals $\mathrm{mao}(G)$ (resp. $\mathrm{maffo}(G)$), is bounded from above by $|N| \cdot \mathrm{mao}(G/N)$ (resp. by $|N| \cdot \mathrm{maffo}(G/N)$). Dividing both sides of the respective inequality by $|G|$ yields the desired conclusion. □

Remark 5.2.10. In view of Remark 5.1.4, just for proving our main results, it would be enough to know that $\mathrm{mao}_{\mathrm{rel}}$ and $\mathrm{maffo}_{\mathrm{rel}}$ are RadQ-increasing. We note that this weaker property can be established without referring to the CFSG. More precisely, it can be proved by induction on $|\operatorname{Rad}(G)|$, fixing in the induction step a nontrivial elementary abelian characteristic subgroup B of G and using Lemma 5.2.2 and the argument that $\mathfrak{F}(A) \leq |A|$ for elementary abelian A from the proof of Theorem 5.2.5. This would have spared us of having to bound the values of $\mathfrak{F}$ on nonabelian characteristically simple groups, but we would only have established the upper bound on $\mathrm{meo}(\mathrm{Hol}(G))$ for finite *solvable* G (by induction on the length of a characteristic series of G where all factors are elementary abelian).

6 Proof of the remaining main results

Proof of Theorem 1.1.1(2,3). We first prove (3). By Corollary 5.2.9(2) and Theorem 4.4(1), we have

$$\rho \leq \mathrm{mao}_{\mathrm{rel}}(G) \leq \mathrm{mao}_{\mathrm{rel}}(G/\operatorname{Rad}(G)) \leq |G/\operatorname{Rad}(G)|^{\log_{60}(6)-1},$$

yielding the desired upper bound on $[G : \operatorname{Rad}(G)]$ by Lemma 5.1.3. For (2), note that by (3) and strict monotonicity of power functions, $\mathrm{mao}_{\mathrm{rel}}(G) > \frac{1}{10}$ implies that $[G : \operatorname{Rad}(G)] < (1/10)^{(\log_{60}(6)-1)^{-1}} = 60$. Since the smallest order of a nonabelian finite simple group is 60, $G/\operatorname{Rad}(G)$ must thus be trivial, i.e., G is solvable. □

Proof of Theorem 1.1.3(1,2). (2) can be proved analogously to Theorem 1.1.1(3). Deriving (1) from (2) is also similar to the proof of Theorem 1.1.1(2), but a little more

involved. By (2), $\mathrm{maffo}_{\mathrm{rel}}(G) > \frac{1}{4}$ implies that $[G : \mathrm{Rad}(G)] < (1/4)^{(\log_{60}(30)-1)^{-1}} = 3600$. Hence if any nonsolvable finite group G such that $\mathrm{maffo}_{\mathrm{rel}}(G) > \frac{1}{4}$ existed, then $G/\mathrm{Rad}(G)$ would have socle a nonabelian finite simple group S of order less than 3600. Now using Theorem 3.1 and that the function λ_{aff} is CS-increasing, we derive that $\mathrm{maffo}_{\mathrm{rel}}(S) = \lambda_{\mathrm{aff}}(S) \geq \lambda_{\mathrm{aff}}(G) = \mathrm{maffo}_{\mathrm{rel}}(G) > 1/4$. Hence all that remains to derive a contradiction is to check that all nonabelian finite simple groups S of order less than 3600 have maffo-value at most $1/4|S|$, which is readily done with the help of GAP [6]. □

7 Outlook

We hope that our rather general approach of studying "sufficiently well-behaved" group-theoretic functions f in Section 5 will allow for extensions to other "interesting" f, and also to a more general view on methods already found in the literature. As an example for the latter, let us remark that a closer investigation of Hegarty's proof that the derived length of a finite solvable group G is bounded in terms of the value of G under the C-submultiplicative relative function l_{-1} [9, Theorem 1.1] leads to the following lemma:

Lemma 7.1. *Let f be a C-submultiplicative relative function, and assume that there exist $k \in \mathbb{N}^+$ and $\rho_0 \in (0,1)$ such that for any finite solvable group G of derived length at least k, we have $f(G) \leq \rho_0$. Then:*

(1) For any finite solvable group G, we have $f(G) \leq \rho_0^{\lfloor \mathrm{dl}(G)/k \rfloor}$.

(2) For any $\rho \in (0,1)$ and any finite group G with $f(G) \geq \rho$, we have that $\mathrm{dl}(\mathrm{Rad}(G)) \leq k \cdot \log(\rho)/\log(\rho_0) + k - 1$.

Proof. For (1): If G is a finite solvable group, then G has a characteristic series of length $\lfloor \mathrm{dl}(G)/k \rfloor$ in which each factor has derived length at least k. The assertion follows by C-submultiplicativity of f and induction on the length of the series.

For (2): Since f is CS-increasing, we derive that $f(\mathrm{Rad}(G)) \geq f(G) \geq \rho$, whence $\rho \leq \rho_0^{\lfloor \mathrm{dl}(\mathrm{Rad}(G))/k \rfloor}$ by (1), and the upper bound on $\mathrm{dl}(\mathrm{Rad}(G))$ follows in view of $k \cdot \lfloor \mathrm{dl}(\mathrm{Rad}(G))/k \rfloor \geq \mathrm{dl}(\mathrm{Rad}(G)) - (k-1)$. □

We plan to study extensions of our main results and of Hegarty's result to some more group-theoretic functions f of interest in a subsequent paper.

References

[1] A. Bors, *Classification of finite group automorphisms with a large cycle*, to appear in *Comm. Algebra*, `http://arxiv.org/abs/1410.2284`.

[2] T. C. Burness and S. D. Scott, On the number of prime order subgroups of finite groups, *J. Austral. Math. Soc.* **87** (2009), 329–357.

[3] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985 (reprinted 2013).

[4] M. Deaconescu and D. MacHale, Odd order groups with an automorphism cubing many elements, *J. Austral. Math. Soc. Ser. A* **46**(2) (1989), 281–288.

[5] B. Elspas, The theory of autonomous linear sequential networks, *IRE Trans. Circuit Theory* **CT-6** (1959), 45–60.

[6] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.5* (2014), `http://www.gap-system.org`.

[7] M. Giudici, C. E. Praeger and P. Spiga, Finite primitive permutation groups and regular cycles of their elements, *J. Algebra* **421** (2015), 27–55.

[8] 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**(11) (2015), 7665–7694.

[9] P. V. Hegarty, Soluble groups with an automorphism inverting many elements, *Math. Proc. R. Ir. Acad.* **105A**(1) (2005), 59–73.

[10] R. A. Hernández-Toledo, Linear finite dynamical systems, *Comm. Algebra* **33**(9) (2005), 2977–2989.

[11] M. V. Horoševskiĭ, On automorphisms of finite groups, *Math. USSR-Sb.* **22**(4) (1974), 584–594.

[12] W. M. Kantor and Á. Seress, Large element orders and the characteristic of Lie-type simple groups, *J. Algebra* **322**(3) (2009), 802–832.

[13] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series 129, Cambridge University Press, Cambridge, 1990.

[14] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, Cambridge, 1997.

[15] H. Liebeck and D. MacHale, Groups with automorphisms inverting most elements, *Math. Z.* **124** (1972), 51–63.

[16] H. Liebeck, Groups with an automorphism squaring many elements, *J. Austral. Math. Soc.* **16** (1973), 33–42.

[17] H. Liebeck and D. MacHale, Groups of odd order with automorphisms inverting many elements, *J. London Math. Soc. (2)* **6** (1973), 215–223.

[18] D. MacHale, Groups with an automorphism cubing many elements, *J. Austral. Math. Soc.* **20**(2) (1975), 253–256.

[19] J.-P. Massias, Majoration explicite de l'ordre maximum d'un élément du groupe symétrique, *Ann. Fac. Sci. Toulouse Math. (5)* **6**(3–4) (1985), 269–281.

[20] G. A. Miller, Groups which admit automorphisms in which exactly three-fourths of the operators correspond to their inverses, *Bull. Amer. Math. Soc.* **35**(4) (1929), 559–565.

[21] G. A. Miller, Possible α-automorphisms of non-abelian groups, *Proc. Nat. Acad. Sci. U.S.A.* **15**(2) (1929), 89–91.

[22] W. M. Potter, Nonsolvable groups with an automorphism inverting many elements, *Arch. Math. (Basel)* **50**(4) (1988), 292–299.

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

[24] J. S. Rose, Automorphism groups of groups with trivial centre, *Proc. London Math. Soc. (3)* **31**(2) (1975), 167–193.

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

[26] C. T. C. Wall, On groups consisting mostly of involutions, *Proc. Cambridge Philos. Soc.* **67** (1970), 251–262.

[27] J. Zimmerman, Groups with automorphisms squaring most elements, *Arch. Math. (Basel)* **54**(3) (1990), 241–246.