Finite groups with an automorphism inverting, squaring or cubing a non-negligible fraction of elements

Alexander Bors[*]

September 12, 2016

Abstract

Finite groups with an automorphism mapping a sufficiently large proportion of elements to their inverses resp. squares resp. cubes have been studied for a long time, and the gist of the results on them is that they are "close to being abelian". In this paper, we consider finite groups G such that, for a fixed but arbitrary $\rho \in (0,1]$, some automorphism of G maps at least $\rho|G|$ many elements of G to their inverses resp. squares resp. cubes. We will relate these conditions to some parameters that measure, intuitively speaking, how far the group G is from being solvable, nilpotent or abelian; most prominently the commuting probability of G, i.e., the probability that two independently uniformly randomly chosen elements of G commute. To this end, we will use various counting arguments, the classification of the finite simple groups and some of its consequences, as well as a classical result from character theory.

1 Introduction

1.1 Background and main results

In the literature, there are various results on "quantitative" conditions on finite groups G that imply commutativity or a weaker property, such as nilpotency or solvability. We mention the following examples (and remark that all rational constants appearing in these results are optimal):

[*] 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*: Primary: 20D25, 20D45, 20D60. Secondary: 05D05, 12E20, 20C15, 20D05.

Key words and phrases: Finite groups, Automorphisms, Powers of group elements, Solvable radical, Fitting subgroup.

1. For $e \in \mathbb{Z}$, denote by $\mathrm{L}_e(G)$ the maximum number of elements of G that are mapped to their e-th power by a single automorphism of G. Then either of the following implies that G is abelian: $\mathrm{L}_{-1}(G) > \frac{3}{4}|G|$ (this is already mentioned as "known" by Miller in 1929 (see [24, first paragraph]); we will review a short proof of this at the beginning of Subsection 2.1), $\mathrm{L}_2(G) > \frac{1}{2}|G|$ [21, Theorem 3.5], $\mathrm{L}_3(G) > \frac{3}{4}|G|$ [23, Theorem 4.1]. On the other hand, for all $e \in \mathbb{Z} \setminus \{-1, 0, 2, 3\}$, there exists a finite nonabelian group G_e such that the map $G_e \to G_e, g \mapsto g^e$, is an automorphism of G_e [25]. Furthermore, either of the following implies that G is solvable: $\mathrm{L}_{-1}(G) > \frac{4}{15}|G|$ [27, Corollary 3.2], $\mathrm{L}_2(G) > \frac{7}{60}|G|$ [10, Theorem C], $\mathrm{L}_3(G) > \frac{4}{15}|G|$ [12, Theorem 4.1]. Finally, it is known that for solvable G and fixed $\rho \in (0, 1]$, a condition of the form $\mathrm{L}_{-1}(G) \geq \rho|G|$ implies that the derived length of G is bounded from above [11, Theorems 1.1 and 2.6].
2. Denote by $\mathrm{k}(G)$ the number of conjugacy classes of G. The quotient $\mathrm{cp}(G) := \mathrm{k}(G)/|G|$ equals the *commuting probability of* G, i.e., the probability that two independently uniformly randomly chosen elements of G commute [9]. Furthermore, the following is known: If $\mathrm{cp}(G) > \frac{5}{8}$, then G is abelian [9], if $\mathrm{cp}(G) > \frac{1}{2}$, then G is nilpotent [17, Théorème 7] (see also [20, Corollary 3.2]), and if $\mathrm{cp}(G) > \frac{1}{12}$, then G is solvable [18, 19] (see also the stronger result [8, Theorem 11]). More generally, Guralnick and Robinson showed that if $\mathrm{cp}(G) \geq \rho$ for some fixed $\rho \in (0, 1]$, then both the index of the Fitting subgroup of G and the derived length of the solvable radical of G are bounded in terms of ρ [8, Theorem 10(ii) and Theorem 12 in combination with Lemma 2(iii)]; since we will need them, we will later review those bounds in more detail, see Theorem 2.3.1.
3. Denote by $\mathrm{mao}(G)$ the maximum automorphism order of G. If G is nontrivial, then $\mathrm{mao}(G) \leq |G| - 1$, and the bound is attained if and only if G is elementary abelian [13, Theorem 2]. Moreover, if $\mathrm{mao}(G) > \frac{1}{2}|G|$, then G is abelian [1, Theorem1.1.1(1)], if $\mathrm{mao}(G) > \frac{1}{10}|G|$, then G is solvable [1, Theorem 1.1.1(2)], and if $\mathrm{mao}(G) \geq \rho|G|$ for any fixed $\rho \in (0, 1]$, then the index of the solvable radical of G is bounded [1, Theorem 1.1.1(3)].

The uniting "philosophy" behind all the results above is that a finite group G for which the parameter in question (L_e, k or mao respectively) is large enough, i.e., larger than $\rho|G|$ for a fixed (large enough) $\rho \in (0, 1]$, must be abelian or at least "not too far from being abelian". Whereas, as mentioned above, results on consequences of such conditions for general, arbitrarily small $\rho \in (0, 1]$ exist for the functions k and mao, there are, to the author's knowledge, no such results for the functions L_e except for Hegarty's bound on the derived length for solvable G and $e = -1$ mentioned above.

The purpose of this paper is to study finite groups G in which $\mathrm{L}_e(G) \geq \rho|G|$ (i.e., with an automorphism mapping at least a fraction of ρ of the elements of G to their e-th power) for a fixed, but arbitrary $\rho \in (0, 1]$ and $e \in \{-1, 2, 3\}$. The aim is to generalize the known results by bounding, in terms of ρ, some parameters related to "how far" the group is from being abelian, nilpotent resp. solvable. More precisely:

- For $e = -1, 2$, we will show that the commuting probability of a finite group

G can be explicitly bounded away from 0 in terms of the quotient $\mathrm{l}_e(G) := \mathrm{L}_e(G)/|G|$. By Guralnick and Robinson's results mentioned above, this also gives explicit upper bounds on two other interesting parameters, namely the index of the Fitting subgroup and the derived length of the solvable radical, in finite groups G satisfying a condition of the form $\mathrm{l}_e(G) \geq \rho$ with $e = -1, 2$ and $\rho \in (0, 1]$ fixed. For more details, see Theorem 1.1.2(1,2) below.

- The case $e = 3$ is more difficult; this is partly due to the fact (already observed by Hegarty in [12]) that for elements x, y of a group, the assumption $x^e y^e = (xy)^e$ does *not* imply that x and y commute for $e = 3$ as opposed to $e = -1, 2$. Still, we will bound $\mathrm{cp}(G)$ in terms of $\mathrm{l}_3(G)$ if G is of odd order (Theorem 1.1.2(3a)), and without this assumption on the order, we will show that at least the index of the solvable radical of G can be explicitly bounded in terms of $\mathrm{l}_3(G)$, see Theorem 1.1.2(4).

Before giving our main result, Theorem 1.1.2, with the explicit bounds referred to above, we fix some more notation:

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

1. *The solvable radical of G is denoted by* $\mathrm{Rad}(G)$.
2. *The Fitting subgroup of G is denoted by* $\mathrm{Fit}(G)$.
3. *If G is solvable, then the derived length of G is denoted by* $\mathrm{length}(G)$.

Theorem 1.1.2. *Let $\rho \in (0, 1]$ be fixed, G a finite group. Then:*

1. *If G has an automorphism inverting at least $\rho|G|$ many elements in G, then the following hold:*
   (a) $\mathrm{cp}(G) \geq \frac{1}{12}\rho^5$,
   (b) $[G : \mathrm{Fit}(G)] \leq 144\rho^{-10}$,
   (c) $\mathrm{length}(\mathrm{Rad}(G)) \leq \max(2, \log_{3/4}(2\rho) + 3)$,
2. *If G has an automorphism squaring at least $\rho|G|$ many elements in G, then the following hold:*
   (a) $\mathrm{cp}(G) \geq \rho^2$,
   (b) $[G : \mathrm{Fit}(G)] \leq \rho^{-4}$,
   (c) $\mathrm{length}(\mathrm{Rad}(G)) \leq \max(\{4\} \cup \{l \in \mathbb{Z} \mid l \geq 0, 2^{l+1} \leq \frac{4l-7}{\rho^2}\})$,
3. *If G is of* odd order *and G has an automorphism cubing at least $\rho|G|$ many elements of G, then the following hold:*
   (a) $\mathrm{cp}(G) \geq \rho^2$,
   (b) $[G : \mathrm{Fit}(G)] \leq \rho^{-4}$,
   (c) $\mathrm{length}(\mathrm{Rad}(G)) \leq \max(\{4\} \cup \{l \in \mathbb{Z} \mid l \geq 0, 2^{l+1} \leq \frac{4l-7}{\rho^2}\})$,
4. *If G has an automorphism cubing at least $\rho|G|$ many elements of G, then* $[G : \mathrm{Rad}(G)] \leq \mathrm{g}(\rho)$, *where* $\mathrm{g} : (0, 1] \to [1, \infty)$ *is given by Notation 5.4.4.*

We postpone the definition of the function g in point (4) because it requires an auxiliary result proved later.

1.2 Overview of the paper

We will establish Theorem 1.1.2(1a,2a,3a) by means of counting arguments in finite groups which, in spite of their elementary nature, yield some surprising connections between different parameters (such as the fraction of elements squared by a finite group automorphism and its number of fixed points, see Lemma 3.1.6). The rest of Theorem 1.1.2(1,2,3) then follows from results of Hegarty as well as Guralnick and Robinson. As already remarked, the proof of Theorem 1.1.2(4) will be more involved and use the CFSG together with some heavy counting arguments in finite groups with trivial solvable radical.

Each of the next three sections of the paper will be dedicated to the proof of one of the points of Theorem 1.1.2:

1. In Section 2, we will prove Theorem 1.1.2(1). More precisely:
    - In Subsection 2.1, we show how to obtain Theorem 1.1.2(1a) by generalizing from the argument that a finite group G with $\mathrm{l}_{-1}(G) > \frac{3}{4}$ must be abelian, using an elementary observation on intersection sizes in families of "non-negligible" subsets of finite sets, Lemma 2.1.2.
    - Subsection 2.2 is dedicated to some general theory on functions f mapping finite groups to non-negative real numbers. *Inter alia*, we briefly review a simple result, Lemma 2.2.4, from another paper of the author allowing us to bound $[G : \mathrm{Rad}(G)]$ under an assumption of the form $f(G) \geq \rho > 0$ when f satisfies some assumptions.
    - Some of the observations from Subsection 2.2 together with results of Guralnick and Robinson will be applied in Subsection 2.3 to prove Theorem 1.1.2(1b,1c).
2. Section 3 is dedicated to the proof of Theorem 1.1.2(2).
    - We first prove two inequalities (given in Lemmata 3.1.2 and 3.1.6), each of them relating the number of elements squared by a finite group automorphism with the number of fixed points of that automorphism, in Subsection 3.1.
    - Theorem 1.1.2(2) will then be proved in Subsection 3.2, using the bounds from the last subsection together with some results from Subsection 2.2 and another result of Guralnick and Robinson.
3. The rather short Section 4 deals with Theorem 1.1.2(3).
    - In Subsection 4.1, we discuss briefly the proof of all subpoints of Theorem 1.1.2(3).
    - Subsection 4.2 serves as a conclusion to Sections 2 to 4 of the paper; it discusses to what extent the CFSG was used in the results proved so far.
4. The most involved part, Theorem 1.1.2(4), will be established in Section 5.
    - In Subsection 5.1, we will also relate the number of elements cubed by a finite group automorphism with its number of fixed points.

- Subsection 5.2 summarizes some known results (and easy consequences thereof) on conjugacy class numbers and outer automorphism group orders of nonabelian finite simple groups which we will need later.
- In Subsection 5.3, we establish an inequality of the form $\mathrm{L}_{-1}(\mathrm{Aut}(S)) \leq |S|^E$ for some constant $E < 1$ and all nonabelian finite simple groups S; this will serve as an auxiliary result in the proof of Theorem 1.1.2(4). In principle, we could use Theorem 1.1.2(1a) together with some bounds from Subsection 5.2 for this. However, said bounds are too crude for small S, which one would have to check separately, resulting in a rather unelegant approach. Instead, we will use a classical result from character theory about the number of square roots of finite group elements to give, modulo the results of Subsection 5.2, a rather short proof that $\mathrm{L}_{-1}(\mathrm{Aut}(S)) \leq |S|^{0.8817\ldots}$.
- In Subsection 5.4, we will show that $\mathrm{L}_3(\mathrm{Aut}(S)) \leq |S|^{0.947}$ for all large enough nonabelian finite simple groups S, another important auxiliary result. Having established this, we can also finally give the definition of the function g appearing in Theorem 1.1.2(4).
- Subsection 5.5 will elaborate on another auxiliary result, which bounds the number of elements cubed by automorphisms of certain finite groups H with trivial solvable radical coset-wise (for a certain subgroup K of H).
- In Subsection 5.6, we present a proof of Theorem 1.1.2(4) based on the auxiliary results from the previous subsections.

Finally, we will give some concluding remarks in Section 6.

1.3 Notation and terminology

We denote by $\mathbb{N}$ the set of natural numbers (including 0) and by $\mathbb{N}^+$ the set of positive integers. The image of a set M under a function f is denoted by $f[M]$, and the restriction of f to M by $f_{|M}$. The image of f, i.e., the image of the entire domain of f under f, is denoted by $\mathrm{im}(f)$. If, for $i = 1, \ldots, n$, f_i is a function $X_i \to Y_i$, we denote by $f_1 \times \cdots \times f_n$ the function $\prod_{i=1}^n X_i \to \prod_{i=1}^n Y_i$ mapping $(x_1, \ldots, x_n) \mapsto (f_1(x_1), \ldots, f_n(x_n))$.

For functions f, g mapping from an unbounded set D of non-negative real numbers into $[0, \infty)$, we use the Bachmann-Landau notation "$f(x) = \Theta(g(x))$ as $x \to \infty$", meaning that there exist positive constants C_1 and C_2 such that for all $x \in D$, $C_1 f(x) \leq g(x) \leq C_2 f(x)$.

For $n \in \mathbb{N}$, we denote the symmetric group and alternating group on $\{1, \ldots, n\}$ by $\mathcal{S}_n$ and $\mathcal{A}_n$ respectively. For a group G and an element $g \in G$, $\tau_g : G \to G, x \mapsto gxg^{-1}$, denotes the inner automorphism of G with respect to g, and $\mathrm{ord}(g)$ denotes the order of g. The centralizer in G of an element $g \in G$ is denoted by $\mathrm{C}_G(g)$, and the center of G by ζG. We write $H \leq G$ for "H is a subgroup of G" and $N \,\mathrm{char}\, G$ for "N is a characteristic subgroup of G".

Introducing some more notation related to the problems with which we will deal in this paper, we set, for an automorphism α of a finite group G and $e \in \mathbb{Z}$, $\mathrm{P}_e(\alpha) :=$

$\{g \in G \mid \alpha(g) = g^e\}$, $\mathrm{L}_e(\alpha) := |\mathrm{P}_e(\alpha)|$ and $\mathrm{l}_e(\alpha) := \frac{1}{|G|}\mathrm{L}_e(\alpha)$. Hence $\mathrm{L}_e(G) = \max_{\alpha\in\mathrm{Aut}(G)} \mathrm{L}_e(\alpha)$ and $\mathrm{l}_e(G) = \frac{1}{|G|}\mathrm{L}_e(G) = \max_{\alpha\in\mathrm{Aut}(G)} \mathrm{l}_e(\alpha)$.

For a nonzero polynomial $P(X)$ over some field K, we denote by $\deg(P(X))$ the degree of $P(X)$ and by $\mathrm{mindeg}(P(X))$ the minimum degree of a nonzero monomial of $P(X)$.

The rest of our notation is either defined at some point in the text or standard.

1.4 Finite semisimple groups

For the readers' convenience, we now briefly recall the basic theory of finite groups with trivial solvable radical. We call such groups *semisimple*, in accordance with the terminology of [28, pp. 89ff.], where one can find most of the theory mentioned below in detail.

Let H be a finite semisimple group. Then the socle of H, $\mathrm{Soc}(H)$, is a finite centerless completely reducible group, i.e., it can be written as follows: $\mathrm{Soc}(H) = S_1^{n_1} \times \cdots \times S_r^{n_r}$, where the S_i are pairwise nonisomorphic nonabelian finite simple groups, the n_i are positive integers, and $r \in \mathbb{N}$ (with $r = 0$ if and only if H is trivial). One can show that the conjugation action of H on $\mathrm{Soc}(H)$ is faithful, yielding an embedding $H \hookrightarrow \mathrm{Aut}(\mathrm{Soc}(H))$ whose image contains $\mathrm{Inn}(\mathrm{Soc}(H)) \cong \mathrm{Soc}(H)$.

Conversely, if R is a finite centerless completely reducible group, and H is such that $\mathrm{Inn}(R) \leq H \leq \mathrm{Aut}(R)$, then H is semisimple with $\mathrm{Soc}(H) = \mathrm{Inn}(R) \cong R$. Hence the finite semisimple groups are just the groups occurring in between the inner and the full automorphism group of a finite centerless completely reducible group.

Fortunately for the study of finite semisimple groups, the structure of the automorphism groups of finite centerless completely reducible groups is known: We have $\mathrm{Aut}(S_1^{n_1} \times \cdots \times S_r^{n_r}) = \mathrm{Aut}(S_1^{n_1}) \times \cdots \times \mathrm{Aut}(S_r^{n_r})$, and for a nonabelian finite simple group S and $n \in \mathbb{N}^+$, we have $\mathrm{Aut}(S^n) = \mathrm{Aut}(S) \wr \mathcal{S}_n$ (permutational wreath product).

Furthermore, it follows from a result of Rose (see [29, Lemma 1.1]) that for any finite semisimple group H, viewing H as a subgroup of $\mathrm{Aut}(\mathrm{Soc}(H))$ via the embedding mentioned above, the automorphism group of H is naturally isomorphic with the normalizer of H in $\mathrm{Aut}(\mathrm{Soc}(H))$. In particular, the automorphism group of a finite centerless completely reducible group is always complete.

We remark that the results of the previous paragraph imply in particular that every automorphism of a finite semisimple group H extends naturally to an (inner) automorphism of $\mathrm{Aut}(\mathrm{Soc}(H))$. In particular, if S is a nonabelian finite simple group, then for all $e \in \mathbb{Z}$, $\mathrm{L}_e(S) \leq \mathrm{L}_e(\mathrm{Aut}(S))$.

2 Dealing with l_{-1}

2.1 Intersection of translates of the set of elements inverted by a finite group automorphism

Our argument builds up on a part of a proof of the following well-known fact, which we review first:

Proposition 2.1.1. *A finite group G with $\mathrm{l}_{-1}(G) > \frac{3}{4}$ is abelian.*

Proof (see [7]). Fix an automorphism α of G inverting more than $\frac{3}{4}|G|$ many elements, and set $S := \mathrm{P}_{-1}(\alpha)$. For $s \in S$, since both S and its translate sS are subsets of G size more than $\frac{3}{4}|G|$, it follows that $|sS \cap S| > \frac{1}{2}|G|$. Hence for more than $\frac{1}{2}|G|$ many $t \in S$, we have that $st \in S$ as well. It follows that $t^{-1}s^{-1} = (st)^{-1} = \alpha(st) = \alpha(s)\alpha(t) = s^{-1}t^{-1}$, or equivalently $t \in \mathrm{C}_G(s)$. Therefore, $|\mathrm{C}_G(s)| > \frac{1}{2}|G|$, and thus $\mathrm{C}_G(s) = G$, i.e., $s \in \zeta G$, by Lagrange's theorem. We just showed that $S \subseteq \zeta G$, whence $\zeta G = G$ by another application of Lagrange's theorem, and so G is abelian. □

The gist of this argument is that because $S := \mathrm{P}_{-1}(\alpha)$ is so large, the intersection of S with the translate sS by any element $s \in S$ is also large (first inference), and therefore, all $s \in S$ have large centralizers (second inference). Both inferences have analogues under the weaker assumption that $\mathrm{l}_{-1}(\alpha) \geq \rho$ for some fixed $\rho \in (0,1]$. The following elementary lemma generalizes the first inference:

Lemma 2.1.2. *Let $\rho \in (0,1]$, M a finite set, $(S_i)_{i\in I}$ a nonempty family of subsets of M such that $|S_i| \geq \rho|M|$ for all $i \in I$. Set $k(\rho) := \lceil \rho^{-1} \rceil + 1$ (so that $k(\rho)\cdot\rho \geq 1+\rho$) and $t(\rho) := \rho/\Delta_{k(\rho)-1} = \rho/\Delta_{\lceil \rho^{-1}\rceil}$, where $\Delta_n := \frac{1}{2}n(n+1)$ denotes the n-th triangle number. Then the following hold:*

1. *If $J \subseteq I$ with $|J| \geq k(\rho)$, then there exist distinct $i,j \in I$ such that $|S_i \cap S_j| \geq t(\rho)|M|$.*
2. *There exists $i \in I$ such that for at least $\frac{|I|-(k(\rho)-1)}{k(\rho)-1}$ many $j \in I \setminus \{i\}$, we have $|S_i \cap S_j| \geq t(\rho)|M|$.*
3. *If $|I| \geq 2(k(\rho)-1)$, then there exists $i \in I$ such that for at least $\frac{1}{2(k(\rho)-1)}|I|$ many $j \in I \setminus \{i\}$, we have $|S_i \cap S_j| \geq t(\rho)|M|$.*

Proof. For (1): We may of course assume w.l.o.g. that $|J| = k(\rho)$, and we will show the assertion for such J by contradiction; assume that $|S_i \cap S_j| < t(\rho)|M|$ for all distinct $i,j \in J$. Say $J = \{j_1,\ldots,j_{k(\rho)}\}$, and set, for $l = 1,\ldots,k(\rho)$, $U_l := \bigcup_{t=1}^{l} S_{j_t}$. We show by induction on l that

$$|U_l| > (l\cdot\rho - \Delta_{l-1}t(\rho))|M| \tag{1}$$

for $l = 2,\ldots,k(\rho)$. Indeed, we find that

$$|U_2| = |S_{j_1} \cup S_{j_2}| \geq |S_{j_1}| + |S_{j_2}| - |S_{j_1} \cap S_{j_2}| > \rho|M| + \rho|M| - t(\rho)|M| = (2\rho - t(\rho))|M|,$$

and if the assertion has been verified up to $l-1$, it follows that

$$\begin{aligned}|U_l| &= |U_{l-1}\cup S_{j_l}| \geq |U_{l-1}|+|S_{j_l}|-|U_{l-1}\cap S_{j_l}| \\ &\geq ((l-1)\rho-\Delta_{l-2}t(\rho))|M|+\rho|M|-|\bigcup_{i=1}^{l-1}S_{j_i}\cap S_{j_l}| \\ &> (l\rho-\Delta_{l-2}t(\rho))|M|-(l-1)t(\rho)|M| = (l\rho-\Delta_{l-1}t(\rho))|M|,\end{aligned}$$

as required. However, by setting $l:=k(\rho)$ in Equation (1), we get that

$$|U_{k(\rho)}| > (k(\rho)\rho-\Delta_{k(\rho)-1}t(\rho))|M| \geq (1+\rho-\rho)|M| = |M|,$$

a contradiction.

For (2): If $|I|\leq k(\rho)-1$, there is nothing to show, so assume that $|I|\geq k(\rho)$. Let $J\subseteq I$ be maximal such that for all distinct $i,j\in J$, we have $|S_i\cap S_j|<t(\rho)|M|$. By (1), $|J|\leq k(\rho)-1$. Set $K:=I\setminus J$; then $|K|\geq |I|-(k(\rho)-1)$. Furthermore, by maximality of J, there exists a function $\iota: K\rightarrow J$ such that for all $j\in K$, $|S_{\iota(j)}\cap S_j|\geq t(\rho)|M|$. For at least one $i\in J$, the fiber $\iota^{-1}[\{i\}]$ has size at least $\frac{|K|}{|J|}\geq\frac{|I|-(k(\rho)-1)}{k(\rho)-1}$, and any such i "does the job".

For (3): This follows from (2), since by assumption,

$$\frac{|I|-(k(\rho)-1)}{k(\rho)-1}=\frac{|I|}{k(\rho)-1}-1\geq\frac{|I|}{k(\rho)-1}-\frac{1}{2}\frac{|I|}{k(\rho)-1}=\frac{1}{2(k(\rho)-1)}|I|.$$

□

The second inference has the following generalization:

Lemma 2.1.3. *Let $\epsilon\in(0,1]$, G a finite group, α an automorphism of G, $S:=\mathrm{P}_{-1}(\alpha)$. Assume that $s,t\in S$ are such that $|sS\cap tS|\geq\epsilon|G|$. Then $|\mathrm{C}_G(st^{-1})|\geq\epsilon|G|$.*

Proof. By assumption, we have $|S\cap s^{-1}tS|=|s^{-1}(sS\cap tS)|=|sS\cap tS|\geq\epsilon|G|$. In other words, for at least $\epsilon|G|$ many $u\in S$, we have that $s^{-1}tu\in S$ as well. It follows that $u^{-1}t^{-1}s=(s^{-1}tu)^{-1}=\alpha(s^{-1}tu)=\alpha(s)^{-1}\alpha(t)\alpha(u)=st^{-1}u^{-1}$, or equivalently $\tau_{s^{-1}}(st^{-1})=t^{-1}s=\tau_u(st^{-1})$, whence for all such u, we have $su\in\mathrm{C}_G(st^{-1})$, and the assertion follows. □

We can now prove Theorem 1.1.2(1a):

Proof of Theorem 1.1.2(1a). First, assume that $|G|<2(k(\rho)-1)\rho^{-1}=2\lceil\rho^{-1}\rceil\rho^{-1}\leq 2\cdot 2\rho^{-1}\cdot\rho^{-1}=4\rho^{-2}$. Then if we had $\mathrm{cp}(G)<\frac{1}{12}\rho^5$, we would get the contradictory chain of inequalities $\frac{1}{12}\rho^5>\mathrm{cp}(G)\geq|G|^{-1}>\frac{1}{4}\rho^2$. Therefore, we may assume that $|G|\geq 2(k(\rho)-1)\rho^{-1}$. Let α be an automorphism of G with $\mathrm{l}_{-1}(\alpha)\geq\rho$, and set $S:=\mathrm{P}_{-1}(\alpha)$. Note that by assumption, $|S|\geq\rho|G|\geq 2(k(\rho)-1)$. Hence by applying Lemma 2.1.2(3) to the family $(sS)_{s\in S}$ of subsets of G, we get that there exists $s\in S$ such that for at least $\frac{|S|}{2(k(\rho)-1)}\geq\frac{\rho}{2(k(\rho)-1)}|G|$ many elements $t\in S$, $|sS\cap tS|\geq t(\rho)|G|$. By Lemma 2.1.3, this yields that for all such t, $|\mathrm{C}_G(st^{-1})|\geq t(\rho)|G|$. Hence

$$\begin{aligned}\mathrm{cp}(G) &\geq \frac{\rho}{2(k(\rho)-1)}\cdot t(\rho) = \frac{\rho}{2\lceil\rho^{-1}\rceil}\cdot\frac{\rho}{\Delta_{\lceil\rho^{-1}\rceil}} = \frac{\rho^2}{\lceil\rho^{-1}\rceil^2(\lceil\rho^{-1}\rceil+1)} \\ &\geq \frac{\rho^2}{(\rho^{-1}+1)^2(\rho^{-1}+2)} \geq \frac{\rho^2}{(2\rho^{-1})^2\cdot 3\rho^{-1}} = \frac{1}{12}\rho^5.\end{aligned}$$

□

2.2 Group-theoretic functions

Consider a function f from the class $\mathcal{G}^{\mathrm{fin}}$ of finite groups into the set of non-negative real numbers. In this subsection, we provide a simple result on when a condition of the form $f(G)\geq\rho>0$, ρ fixed, implies that $[G:\mathrm{Rad}(G)]$ is bounded. We note that Definition 2.2.1 and Lemma 2.2.4 were already included in another manuscript of the author which is currently under review for journal publication, and we refrain from giving the (very simple) proof of Lemma 2.2.4 again here; however, see the preprint version of the manuscript at hand (arXiv:1601.04311) for the proof and some more of this theory.

We will require that f satisfy certain inequalities relating $f(G)$ to values of f on subgroups and quotients of G. More precisely, we will work with the following concepts:

Definition 2.2.1. *A function $f:\mathcal{G}^{\mathrm{fin}}\to[0,\infty)$ is called* group-theoretic *if and only if $f(G_1)=f(G_2)$ whenever G_1 and G_2 are isomorphic finite groups. Henceforth, assume that f is a group-theoretic function.*

1. *f is called* relative *if and only if* $\mathrm{im}(f)\subseteq[0,1]$.
2. *We define f_{rel}, the* relativization of *f, to be the function $\mathcal{G}^{\mathrm{fin}}\to[0,\infty), G\mapsto f(G)/|G|$.*
3. *f is called* increasing on characteristic quotients *(*CQ-increasing*) if and only if for all finite groups G and all $N\,\mathrm{char}\,G$, we have $f(G)\leq f(G/N)$.*
4. *f is called* increasing on characteristic subgroups *(*CS-increasing*) if and only if for all finite groups G and all $N\,\mathrm{char}\,G$, we have $f(G)\leq f(N)$.*
5. *f is called* characteristically submultiplicative *(*C-submultiplicative*) if and only if for all finite groups G and all $N\,\mathrm{char}\,G$, we have $f(G)\leq f(N)\cdot f(G/N)$.*

As for Definition 2.2.1(2), observe that f_{rel} is of course *not* relative in general, but many "natural" group-theoretic functions f (such as the ones from the introductory examples in Subsection 1.1) satisfy $f(G)\leq|G|$ for all $G\in\mathcal{G}^{\mathrm{fin}}$, and for such f, f_{rel} *is* relative.

Remark 2.2.2. We note the following facts following immediately from the definitions of the concepts involved:

1. A relative and C-submultiplicative group-theoretic function is CS-increasing and CQ-increasing.

2. For a group-theoretic function F, F_{rel} is CQ-increasing if and only if for all finite groups G and all $N \operatorname{char} G$, we have $F(G) \leq |N| \cdot F(G/N)$.
3. A group-theoretic function F is C-submultiplicative if and only if F_{rel} is C-submultiplicative.

We now illustrate the concepts introduced in Definition 2.2.1 by means of several examples, some of which will also be of relevance later.

Example 2.2.3. Consider the following examples of group-theoretic functions and their properties:

1. All the functions l_e, $e \in \mathbb{Z}$, are CQ-increasing, by the following coset-wise counting argument (which may be seen as a generalization of the argument in [27, proof of Lemma 2.2] with $t := 1$): Fix an automorphism α of G such that $\mathrm{L}_e(\alpha) = \mathrm{L}_e(G)$. Denoting by $\tilde{\alpha}$ the automorphism of G/N induced by α and by π the canonical projection $G \to G/N$, we find that $g \in \mathrm{P}_e(\alpha)$ implies that $\pi(g) \in \mathrm{P}_e(\tilde{\alpha})$. Hence $\mathrm{P}_e(\alpha)$ is contained in the union of the $\mathrm{L}_e(\tilde{\alpha}) \leq \mathrm{L}_e(G/N)$ many cosets of N in G that correspond to elements from $\mathrm{P}_e(\tilde{\alpha}) \subseteq G/N$. This shows that $\mathrm{L}_e(G) = \mathrm{L}_e(\alpha) \leq |N| \cdot \mathrm{L}_e(G/N)$, as required.
2. The function L_{-1} (and thus l_{-1} too) is C-submultiplicative, see [11, Lemma 1.2].
3. The function L_2 is *not* C-submultiplicative, since l_2 is not even CS-increasing: $\mathrm{l}_2((\mathbb{Z}/2\mathbb{Z})^2) = 1/4 < 5/12 = \mathrm{l}_2(\mathcal{A}_4)$, although $\mathcal{A}_4$ contains a characteristic subgroup isomorphic with $(\mathbb{Z}/2\mathbb{Z})^2$.
4. The function k (and thus $\mathrm{k}_{\mathrm{rel}} = \mathrm{cp}$ too) is C-submultiplicative; actually, it even satisfies the stronger property that $\mathrm{k}(G) \leq \mathrm{k}(N) \cdot \mathrm{k}(G/N)$ for all finite groups G and all *normal* subgroups N of G, see [5].
5. It is readily verified that for all finite groups G and all normal subgroups N of G, we have $\exp(G) \mid \exp(N) \cdot \exp(G/N)$, where exp denotes the group exponent. In particular, exp is C-submultiplicative.
6. The function $\mathrm{mao}_{\mathrm{rel}}$ is relative and CQ-increasing, see [13, Theorem 2] and [1, Corollary 5.2.9(2)].

The following lemma will be used in the proof of Theorem 1.1.2(4) in Section 5; it allows us to restrict our attention to semisimple groups when trying to bound the index of $\mathrm{Rad}(G)$ under a condition of the form $f(G) \geq \rho$ for CQ-increasing f:

Lemma 2.2.4. *Let f be a CQ-increasing group-theoretic function. Assume that, for finite semisimple groups H, we have $f(H) \to 0$ as $|H| \to \infty$. More explicitly, fix a function $g : (0,\infty) \to (0,\infty)$ such that for all $\rho \in (0,\infty)$ and all finite semisimple groups H such that $f(H) \geq \rho$, we have $|H| \leq g(\rho)$.*

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

2.3 Proof of Theorem 1.1.2(1b,1c)

Let us first note the following two bounds by Guralnick and Robinson, see [8, Theorems 10(ii) and 12(i)]:

Theorem 2.3.1. *Let G be a finite group. Then:*

1. $\mathrm{cp}(G) \leq \mathrm{cp}(\mathrm{Fit}(G))^{1/2}[G:\mathrm{Fit}(G)]^{-1/2}$.
2. *If G is solvable and* $\mathrm{length}(G) \geq 4$*, then* $\mathrm{cp}(G) \leq (4\,\mathrm{length}(G)-7)/2^{\mathrm{length}(G)+1}$. □

Proof of Theorem 1.1.2(1b,1c). For (1b): We already know by Theorem 1.1.2(1a) that $\mathrm{cp}(G) \geq \frac{1}{12}\rho^5$. Therefore, using Theorem 2.3.1(1), we conclude that $[G:\mathrm{Fit}(G)] \leq \mathrm{cp}(G)^{-2} \leq (\frac{1}{12}\rho^5)^{-2} = 144\rho^{-10}$, as required.

For (1c): It is easy to see that [11, Theorem 2.6] is equivalent to the following: “For a finite *solvable* group G with $\mathrm{l}_{-1}(G) \geq \rho$, we have that $\mathrm{length}(G) \leq \max(2, \log_{3/4}(2\rho)+3)$.”. This implies that, more generally, we have $\mathrm{length}(\mathrm{Rad}(G)) \leq \max(2, \log_{3/4}(2\rho)+3)$ for a finite group G with $\mathrm{l}_{-1}(G) \geq \rho$, since $\mathrm{l}_{-1}(\mathrm{Rad}(G)) \geq \mathrm{l}_{-1}(G)$ as l_{-1} is CS-increasing (see Example 2.2.3(2) and Remark 2.2.2(1)). □

3 Dealing with l_2

3.1 Fixed points and elements squared by a finite group automorphism

In this subsection, we establish bounds on L_2-values of finite group automorphisms that involve the number of fixed points of the automorphism. This is basically due to the appearance of functions of the following type in our arguments:

Notation 3.1.1. *Let G be a group, α an automorphism of G. We denote by $\mathcal{T}_\alpha$ the function $G \to G$ mapping $g \mapsto g^{-1}\alpha(g)$.*

It is well-known that the fibers of $\mathcal{T}_\alpha$ are just the right cosets of $\mathrm{fix}(\alpha)$, the subgroup of G consisting of the fixed points of α.

We begin with the following general bound for $\mathrm{L}_e(\alpha)$, which is obtained by counting conjugacy-class-wise and is a generalization of [21, Lemma 3.3]:

Lemma 3.1.2. *Let G be a finite group, α an automorphism of G and $e \in \mathbb{Z}$. Then* $\mathrm{L}_e(\alpha) \leq \mathrm{k}(G) \cdot |\,\mathrm{fix}(\alpha)|$

Proof. It is sufficient to show that $\mathrm{P}_e(\alpha)$ contains at most $|\,\mathrm{fix}(\alpha)|$ many elements from each conjugacy class in G. Hence we fix $g \in \mathrm{P}_e(\alpha)$ and show that the number of conjugates tgt^{-1}, $t \in G$, that are also in $\mathrm{P}_e(\alpha)$ is at most $|\,\mathrm{fix}(\alpha)|$. This is equivalent to showing that the number of $t \in G$ such that $tgt^{-1} \in \mathrm{P}_e(\alpha)$ is at most $|\,\mathrm{fix}(\alpha)| \cdot |\,\mathrm{C}_G(g)|$. Now if $tgt^{-1} \in \mathrm{P}_e(\alpha)$, it follows that $tg^et^{-1} = \alpha(tgt^{-1}) = \alpha(t)g^e\alpha(t)^{-1}$, or equivalently $t^{-1}\alpha(t) \in \mathrm{C}_G(g^e)$. Note that since $\alpha(g) = g^e$, e and $\mathrm{ord}(g)$ must be coprime, and so $\mathrm{C}_G(g^e) = \mathrm{C}_G(g)$. Hence a necessary (and sufficient) condition for $tgt^{-1} \in \mathrm{P}_e(\alpha)$ to hold is that t is in the preimage of $\mathrm{C}_G(g)$ under the function $\mathcal{T}_\alpha$.

Since this preimage has size at most $|\operatorname{C}_G(g)|\cdot|\operatorname{fix}(\alpha)|$ by the fiber structure of $\mathcal{T}_\alpha$, we are done. □

Note that the upper bound on $\operatorname{L}_e(\alpha)$ from Lemma 3.1.2 is good by trend if the number of fixed points of α is small. In the rest of this subsection, we derive another upper bound on L_2-values of finite group automorphisms, which has a tendency to be good if the number of fixed points is large. This bound is obtained by counting N-coset-wise for a characteristic subgroup N; the following result is the basis for our argument:

Proposition 3.1.3. *Let G be a group, $e\in\mathbb{N}^+$, $N\operatorname{char}G$, and $\alpha,\beta_1,\ldots,\beta_e$ automorphisms of G. Set $\operatorname{P}_e(\alpha\mid\beta_1,\ldots,\beta_e):=\{g\in G\mid\alpha(g)=\beta_1(g)\cdots\beta_e(g)\}$. Fix $g\in\operatorname{P}_e(\alpha\mid\beta_1,\ldots,\beta_e)$. Then for $n\in N$, we have $ng\in\operatorname{P}_e(\alpha\mid\beta_1,\ldots,\beta_e)$ if and only if*

$$n\in\operatorname{P}_e(\alpha_{|N}\mid(\beta_1)_{|N},(\tau_{\beta_1(g)}\circ\beta_2)_{|N},(\tau_{\beta_1(g)}\circ\tau_{\beta_2(g)}\circ\beta_3)_{|N},\ldots,(\tau_{\beta_1(g)}\circ\cdots\circ\tau_{\beta_{e-1}(g)}\circ\beta_e)_{|N}).$$

Proof. Under the assumptions, we have that $ng\in\operatorname{P}_e(\alpha\mid\beta_1,\ldots,\beta_e)$ if and only if (expressing $\alpha(ng)$ in two different ways)

$$\beta_1(n)\beta_1(g)\beta_2(n)\beta_2(g)\cdots\beta_e(n)\beta_e(g)=\alpha(n)\beta_1(g)\beta_2(g)\cdots\beta_e(g),$$

which is equivalent to

$$\begin{aligned}\alpha(n)&=\beta_1(n)\beta_1(g)\beta_2(n)\beta_2(g)\cdots\beta_{e-1}(n)\beta_{e-1}(g)\beta_e(n)\beta_{e-1}(g)^{-1}\cdots\beta_1(g)^{-1}\\&=\beta_1(n)\cdot(\tau_{\beta_1(g)}\circ\beta_2)(n)\cdots(\tau_{\beta_1(g)}\circ\cdots\circ\tau_{\beta_{e-1}(g)}\circ\beta_e)(n).\end{aligned}$$

□

We will need Proposition 3.1.3 several times in this paper. At the moment, we only require a special case of it, which can be formulated more concisely using the following notation from [1, Definition 3.1.2]:

Notation 3.1.4. *For a group G, an automorphism α of G and $e\in\mathbb{N}$, we define a function $\operatorname{sh}_\alpha^{(e)}:G\to G$ via $\operatorname{sh}_\alpha^{(e)}(g):=g\alpha(g)\alpha^2(g)\cdots\alpha^{e-1}(g)$ (called the **e-th shift of** g **under** α).*

Corollary 3.1.5. *Let G be a group, $e\in\mathbb{N}^+$, $N\operatorname{char}G$ and α an automorphism of G. Fix $g\in\operatorname{P}_e(\alpha)$. Then for $n\in N$, we have $ng\in\operatorname{P}_e(\alpha)$ if and only if $\alpha(n)=\operatorname{sh}_{\tau_g}^{(e)}(n)$.*

Proof. Set $\beta_i:=\operatorname{id}$ for $i=1,\ldots,e$ in Proposition 3.1.3. □

We can use Corollary 3.1.5 to prove the following upper bound on L_2-values of finite group automorphisms:

Lemma 3.1.6. *Let G be a finite group, $N\operatorname{char}G$, let α be an automorphism of G, and denote by $\tilde{\alpha}$ the induced automorphism of G/N. Then $\operatorname{L}_2(\alpha)\leq[N:\operatorname{fix}(\alpha_{|N})]\cdot\operatorname{L}_2(\tilde{\alpha})$, or equivalently, $\operatorname{l}_2(\alpha)\leq|\operatorname{fix}(\alpha_{|N})|^{-1}\cdot\operatorname{l}_2(\tilde{\alpha})$.*

Observe that with $N := G$, this implies that an automorphism of a finite group G with at least m fixed points can only square at most $\frac{1}{m}|G|$ elements of G.

Proof of Lemma 3.1.6. By the argument in Example 2.2.3(1), $\mathrm{P}_2(\alpha)$ can only contain elements from $\mathrm{L}_2(\tilde{\alpha})$ many cosets of N in G. Hence it suffices to show that the intersection of any coset of N in G with $\mathrm{P}_2(\alpha)$ has size at most $[N : \mathrm{fix}(\alpha_{|N})]$. To this end, assume that the intersection is nonempty, say containing g. Then upon setting $e := 2$ in Corollary 3.1.5, we find that the elements of $C = Ng$ squared by α are in bijective correspondence with the $n \in N$ such that $\alpha(n) = \mathrm{sh}_{\tau_g}^{(2)}(n) = n\tau_g(n)$, or equivalently $\mathcal{T}_\alpha(n) = \tau_g(n)$. Since τ_g is bijective, by the fiber structure of $\mathcal{T}_\alpha$, this equality can only hold for at most one n from each right coset of $\mathrm{fix}(\alpha_{|N})$. Hence the total number of such n is bounded from above by the number of such cosets, i.e., by $[N : \mathrm{fix}(\alpha_{|N})]$, which proves the assertion. □

3.2 Proof of Theorem 1.1.2(2)

For (2a): Let G be a finite group with $\mathrm{l}_2(G) \geq \rho$. Fix an automorphism α of G squaring at least $\rho|G|$ many elements of G. In view of Lemma 3.1.6, this implies that $|\,\mathrm{fix}(\alpha)| \leq \rho^{-1}$. Now an application of Lemma 3.1.2 yields $\rho \leq \mathrm{l}_2(G) = \mathrm{l}_2(\alpha) \leq \mathrm{cp}(G) \cdot \rho^{-1}$, and the asserted inequality, $\mathrm{cp}(G) \geq \rho^2$, follows.

For (2b): This follows from subpoint (2a) using Theorem 2.3.1(1).

For (2c): We know already that $\mathrm{l}_2(G) \geq \rho$ implies $\mathrm{cp}(G) \geq \rho^2$. By [8, Lemma 2(iii)], this, in turn, implies $\mathrm{cp}(\mathrm{Rad}(G)) \geq \rho^2$, and we can conclude with an application of Theorem 2.3.1(2).

4 Dealing with l_3 under odd group order

4.1 Proof of Theorem 1.1.2(3)

We start with subpoint (3a). Set $\rho := \mathrm{l}_3(G)$, and fix an automorphism α of G cubing $\rho|G|$ many elements of G. Then we have

$$\rho|G| = |\,\mathrm{P}_3(\alpha)| = |\{g \in G \mid \alpha(g) = g^3\}| = |\{g \in G \mid g^{-1}\alpha(g) = g^2\}| \leq [G : \mathrm{fix}(\alpha)],$$

where the last inequality holds since the map $\mathcal{T}_\alpha : g \mapsto g^{-1}\alpha(g)$ is constant on right cosets of $\mathrm{fix}(\alpha)$, whereas the map $g \mapsto g^2$ is injective on G. This implies that $|\,\mathrm{fix}(\alpha)| \leq \rho^{-1}$, and so we can conclude as in the proof of Theorem 1.1.2(2a). This completes the proof of Theorem 1.1.2(3a).

The other two subpoints now follow easily. (3b) is again by Theorem 2.3.1(1), and (3c) follows, just like (2c) did, from Theorem 2.3.1(2). □

4.2 On the use of the CFSG for our results

Let us take a moment to look back. By showing that $\mathrm{cp}(G)$ can be bounded from below in terms of both $\mathrm{l}_{-1}(G)$ and $\mathrm{l}_2(G)$ (and $\mathrm{l}_3(G)$ when $|G|$ is odd), we could also bound $[G : \mathrm{Fit}(G)]$ due to a result of Guralnick and Robinson, [8, Theorem 10(ii)], which we gave in this paper as Theorem 2.3.1(1). Our arguments leading to the lower bounds of the form $\mathrm{cp}(G) \geq f_1(\mathrm{l}_{-1}(G))$ and $\mathrm{cp}(G) \geq f_2(\mathrm{l}_2(G))$ (and $\mathrm{cp}(G) \geq f_3(\mathrm{l}_3(G))$ when $2 \nmid |G|$) are elementary and do not require the CFSG; neither do the proofs of Theorem 1.1.2(1c,2c,3c)).

However, we note that Theorem 2.3.1(1) does require the CFSG. More precisely, it depends on two other results from the same paper:

- [8, Theorem 4(ii)], stating that in a finite *solvable* group G, we have $\mathrm{cp}(G) \leq \mathrm{cp}(\mathrm{Fit}(G))^{1/2}[G : \mathrm{Fit}(G)]^{-1/2}$, and
- [8, Theorem 9], which says that $\mathrm{cp}(G) \leq [G : \mathrm{Rad}(G)]^{-1/2}$ in *all* finite groups.

The proof of [8, Theorem 4(ii)] does not require the CFSG (though it does require quite a bit of character theory, more precisely one of the main results of [15]), but the CFSG is used for [8, Theorem 9]. However, just to show CFSG-freely that $\mathrm{cp}(G) \geq \rho$ implies that $[G : \mathrm{Fit}(G)]$ is bounded *per se* (without the explicit bound established with the CFSG), it would suffice to show CFSG-freely that $\mathrm{cp}(G) \geq \rho$ implies that $[G : \mathrm{Rad}(G)]$ is bounded in terms of ρ (and combine this with the CFSG-free [8, Theorem 4(ii)] just as Guralnick and Robinson did). And this is indeed possible:

Proposition 4.2.1. *(CFSG-free) For finite groups G, $\mathrm{cp}(G) \to 0$ as $[G : \mathrm{Rad}(G)] \to \infty$.*

Proof. Fix $\rho \in (0, 1]$, and assume that G is a finite group with $\mathrm{cp}(G) \geq \rho$. We will show that $[G : \mathrm{Rad}(G)]$ is bounded. By [8, Lemma 2(iv)] and the fact that $\mathrm{cp}(G) \leq \frac{5}{8}$ when G is nonabelian [9], we get that the number of non-abelian composition factors of G, counting with multiplicities, is bounded. Furthermore, the order of each such composition factor S is also bounded, in view of $\mathrm{cp}(S) \geq \rho$ (which follows from [8, Lemma 2(iii)]). This is because by simplicity of S, the minimum index of a proper subgroup of S is bounded from below by the smallest positive integer $r(S)$ such that $r(S)! \geq |S|$, and $r(S) \to \infty$ as $|S| \to \infty$. Hence $\mathrm{cp}(S) \leq \frac{1-1/|S|}{r(S)} + \frac{1}{|S|} \to 0$ as $|S| \to \infty$, because centralizers of nontrivial elements of S are proper subgroups.

However, writing $\mathrm{Soc}(G/\mathrm{Rad}(G)) = S_1^{n_1} \times \cdots \times S_r^{n_r}$, where the S_i are pairwise nonisomorphic nonabelian finite simple groups, it is clear that each S_i, $i = 1, \ldots, r$, is a composition factor of G with multiplicity at least n_i. Hence in view of the last paragraph, $|\mathrm{Soc}(G/\mathrm{Rad}(G))|$ is bounded in terms of ρ, and thus $[G : \mathrm{Rad}(G)] = |G/\mathrm{Rad}(G)|$ is also bounded, since $G/\mathrm{Rad}(G)$ embeds into $\mathrm{Aut}(\mathrm{Soc}(G/\mathrm{Rad}(G)))$. □

5 Dealing with l_3 in general

5.1 Fixed points once again

The aim of this subsection is to establish an upper bound on the number of elements cubed by a finite group automorphism analogous to the one in Lemma 3.1.6. We first need the following auxiliary result concerning the fiber structure of a certain class of functions on groups:

Proposition 5.1.1. *Let G be a group, α an automorphism of G, and fix $c \in G$. Consider the map $\mathrm{f}_{c,\alpha}: G \to G, g \mapsto gc\alpha(g)$. Then for $g_1, g_2 \in G$, we have $\mathrm{f}_{c,\alpha}(g_1) = \mathrm{f}_{c,\alpha}(g_2)$ if and only if $g_2 \in \mathrm{P}_{-1}(\tau_{g_1} \circ \tau_c \circ \alpha)g_1$. In other words, the fibers of $\mathrm{f}_{c,\alpha}$ are just the subsets of G of the form $\mathrm{P}_{-1}(\tau_g \circ \tau_c \circ \alpha)g$, $g \in G$.*

Proof. Write $g_2 = g_1 x = y g_1$ with $x, y \in G$ (so that $x = \tau_{g_1^{-1}}(y)$). Then

$$\begin{aligned}\mathrm{f}_{c,\alpha}(g_1) = \mathrm{f}_{c,\alpha}(g_2) &\Leftrightarrow g_1 c\alpha(g_1) = g_2 c\alpha(g_2) = g_1 x c \alpha(y)\alpha(g_1) \\ &\Leftrightarrow \alpha(y) = c^{-1}x^{-1}c = (\tau_{c^{-1}} \circ \tau_{g_1^{-1}})(y^{-1}) \\ &\Leftrightarrow (\tau_{g_1} \circ \tau_c \circ \alpha)(y) = y^{-1} \Leftrightarrow y \in \mathrm{P}_{-1}(\tau_{g_1} \circ \tau_c \circ \alpha).\end{aligned}$$

□

Before formulating and proving the aforementioned analogue to Lemma 3.1.6, we note the following consequence of Proposition 5.1.1, which will also be needed later:

Lemma 5.1.2. *Let G be a finite centerless nonsolvable group. Let α, β, γ be automorphisms of G. Then there exists $g \in G$ such that $\alpha(g) \neq g\beta(g)\gamma(g)$ (i.e., $g \notin \mathrm{P}_3(\alpha \mid \mathrm{id}, \beta, \gamma)$ in the notation of Proposition 3.1.3).*

Proof. Assume otherwise. Then $\mathcal{T}_\alpha = \beta \circ \mathrm{sh}^{(2)}_{\beta^{-1}\circ\gamma}$, or equivalently, $\beta^{-1} \circ \mathcal{T}_\alpha = \mathrm{sh}^{(2)}_{\beta^{-1}\circ\gamma} =: f$. Now let $g \in G$ be arbitrary, but fixed. Since the function $\beta^{-1} \circ \mathcal{T}_\alpha$ assumes the value $f(g)$ precisely on the set $\mathrm{fix}(\alpha)g$, and the function $\mathrm{sh}^{(2)}_{\beta^{-1}\circ\gamma}$ by Proposition 5.1.1 assumes this value precisely on the set $\mathrm{P}_{-1}(\tau_g \circ \beta^{-1} \circ \gamma)g$, we conclude that for all $g \in G$, $\mathrm{fix}(\alpha) = \mathrm{P}_{-1}(\tau_g \circ \beta^{-1} \circ \gamma)$. In particular, setting $g := 1$, we find that $\beta^{-1} \circ \gamma$ inverts all fixed points of α. Since G is nonsolvable, we can fix, by [30, Theorem], a nontrivial fixed point x of α, and since G is centerless, there is an element $g \in G$ such that $\tau_g(x^{-1}) \neq x^{-1}$. Hence we have $x^{-1} = (\tau_g \circ \beta^{-1} \circ \gamma)(x) = \tau_g(x^{-1}) \neq x^{-1}$, a contradiction. □

We note that the statement of Lemma 5.1.2 applies in particular to all nonabelian finite simple groups G. Coming back to our goal of bounding $\mathrm{L}_3(\alpha)$ in terms of $|\mathrm{fix}(\alpha)|$, we will now prove the following:

Lemma 5.1.3. *Let G be a finite group, $N \operatorname{char} G$, let α be an automorphism of G and denote by $\tilde{\alpha}$ the induced automorphism of G/N. Then $\mathrm{L}_3(\alpha) \leq [N : \mathrm{fix}(\alpha_{|N})] \cdot \mathrm{L}_{-1}(N) \cdot \mathrm{L}_3(\tilde{\alpha})$, or equivalently $\mathrm{l}_3(\alpha) \leq \frac{\mathrm{L}_{-1}(N)}{\mathrm{fix}(\alpha_{|N})} \cdot \mathrm{l}_3(\tilde{\alpha})$.*

Proof. Counting coset-wise just as in the proof of Lemma 3.1.6, we see that it suffices to show that for all cosets C of N in G, we have $|C \cap \mathrm{P}_3(\alpha)| \leq [N : \mathrm{fix}(\alpha_{|N})] \cdot \mathrm{L}_{-1}(N)$. To this end, assume that $C = Ng$ with $g \in \mathrm{P}_3(\alpha)$. Setting $e := 3$ in Corollary 3.1.5, we find that the elements of C that are also in $\mathrm{P}_3(\alpha)$ are in bijective correspondence with the $n \in N$ such that $\alpha(n) = \mathrm{sh}^{(3)}_{\tau_g}(n) = n\tau_g(n)\tau_g^2(n)$, or equivalently (using the notation from Proposition 5.1.1):

$$(\tau_{g^{-1}} \circ \mathcal{T}_\alpha)(n) = \mathrm{sh}^{(2)}_{\tau_g}(n) = \mathrm{f}_{1,\tau_g}(n). \tag{2}$$

Denote by K the set of $n \in N$ such that (2) holds, and note that at least one of the $[N : \mathrm{fix}(\alpha_{|N})]$ many right cosets of $\mathrm{fix}(\alpha_{|N})$ in N must contain at least $\frac{|K|}{[N:\mathrm{fix}(\alpha_{|N})]}$ many elements of K. Let D be such a coset, and fix $n \in D \cap K$. Then for all $m \in D \cap K$, we have $\mathcal{T}_\alpha(n) = \mathcal{T}_\alpha(m)$, and hence by (2), $\mathrm{f}_{1,\tau_g}(n) = \mathrm{f}_{1,\tau_g}(m)$. It now follows by Proposition 5.1.1 that $\mathrm{L}_{-1}(N) \geq \mathrm{L}_{-1}((\tau_n \circ \tau_g)_{|N}) \geq \frac{|K|}{[N:\mathrm{fix}(\alpha_{|N})]}$, which concludes the proof. □

Note that compared to the upper bound from Lemma 3.1.6, unfortunately, we have an additional factor $\mathrm{L}_{-1}(N)$ here, which prevents us from treating l_3 just like l_2 in Section 3.

5.2 Some facts on nonabelian finite simple groups

We now cite three results on nonabelian finite simple groups from the literature and derive some easy consequences. The first result is a consequence of bounds on conjugacy class numbers due to Fulman and Guralnick [4] and is mentioned and used in [8, proof of Theorem 9]:

Theorem 5.2.1. *Let T be a finite almost simple group. Then $\mathrm{k}(T) \leq |T|^{0.41}$.* □

The second result involves nice uniform bounds for conjugacy class numbers in subgroups of finite symmetric groups and in finite simple groups of Lie type, both due to Liebeck and Pyber, see [22, Theorems 1 and 2].

Theorem 5.2.2. *The following hold:*

1. *Let $n \in \mathbb{N}^+$ and $H \leq \mathcal{S}_n$. Then $\mathrm{k}(H) \leq 2^{n-1}$.*
2. *Let S be a finite simple group of Lie type. Denote by l the untwisted Lie rank and by q the field parameter of S. Then $\mathrm{k}(S) \leq (6q)^l$.* □

Whereas the bound from Theorem 5.2.1 yields in particular an upper bound $\mathrm{k}(S) \leq |S|^{0.41}$ holding for all nonabelian finite simple groups S, we can use those from Theorem 5.2.2 to deduce the following asymptotic result:

Corollary 5.2.3. *Let the variable S range over all nonabelian finite simple groups not isomorphic with any $\mathrm{A}_1(q)$ for q a prime power. Then $\limsup_{|S|\to\infty} \log_{|S|}\mathrm{k}(S) = 1/4$.*

Proof. To see that said limit superior is at least 1/4, it suffices to observe that by [4, Theorem 1.1(1)], $\mathrm{k}(\mathrm{A}_2(q)) = \Theta(q^2)$ as $q \to \infty$, whereas $|\mathrm{A}_2(q)| = \Theta(q^8)$ as $q \to \infty$.

The reverse inequality follows easily from Theorem 5.2.2 and the CFSG. □

The third result was proved by Kohl in [16]:

Theorem 5.2.4. *For all nonabelian finite simple groups S, we have $|\mathrm{Out}(S)| < \log_2(|S|)$.* □

This implies the following, which we will use in the next subsection:

Corollary 5.2.5. *The following hold:*

1. *For nonabelian finite simple groups S, $\log_{|S|}|\mathrm{Out}(S)| \to 0$ as $|S| \to \infty$.*
2. *For all nonabelian finite simple groups S, $\log_{|S|}|\mathrm{Out}(S)| \leq \log_{20160}(12)$, with equality if and only if $S = \mathrm{A}_2(4) = \mathrm{PSL}_3(4)$.*

Proof. Point (1) follows immediately from Theorem 5.2.4. Theorem 5.2.4 also implies that the inequality asserted in point (2) holds for all S but possibly those of order up to an explicit constant. For such "small" S, one can check the validity of the assertion directly, using the CFSG and the known formulas for outer automorphism group orders of nonabelian finite simple groups of the various types (alternating, sporadic, and the various classes of Lie type groups). □

5.3 On L_{-1}-values of (almost) simple groups

In this subsection, we will prove the following:

Theorem 5.3.1. *Set $E := 0.705(1+\log_{20160}(12)) = 0.8817\ldots$. For all nonabelian finite simple groups S, we have $\mathrm{L}_{-1}(\mathrm{Aut}(S)) \leq |S|^E$.*

Let us first reinterpret the maximum number of elements which an *inner* automorphism of a finite group G can invert as the maximum number of square roots that an element of G has in G (see Proposition 5.3.3(2) below); of course, for *complete* G (such as automorphism groups of nonabelian finite simple groups), this number coincides with $\mathrm{L}_{-1}(G)$.

Notation 5.3.2. *We introduce the following notation:*

1. *For a group G and an element $g \in G$, set $\sqrt{g} := \{f \in G \mid f^2 = g\} \subseteq G$.*
2. *For a finite group G, set $\mathrm{maxsqrt}(G) := \max_{g\in G}|\sqrt{g}|$, the maximum number of square roots in G of an element of G.*

Proposition 5.3.3. *Let G be a finite group.*

1. *For any $g \in G$, we have $\mathrm{P}_{-1}(\tau_g) = \sqrt{g^{-2}} \cdot g = \{rg \mid r \in G, r^2 = g^{-2}\}$.*
2. *The maximum number of elements of G inverted by an* ***inner*** *automorphism of G is equal to $\mathrm{maxsqrt}(G)$.*
3. *If G is complete, then $\mathrm{L}_{-1}(G) = \mathrm{maxsqrt}(G)$.*

Proof. Clearly, (2) follows from (1), and (3) follows from (2). Hence it suffices to prove (1), which follows from [26, Proposition 2.22, equivalence of (i) and (iii)]. □

Proposition 5.3.3(3) allows us to establish a connection to character theory, due to the following classical result:

Theorem 5.3.4. *For a finite group G and an irreducible $\mathbb{C}$-character χ of G, denote the Frobenius-Schur indicator of χ by $\nu_2(\chi)$. Then for an element $g \in G$, we have $|\sqrt{g}| = \sum_{\chi}\nu_2(\chi)\chi(g)$, where χ runs through the irreducible $\mathbb{C}$-characters of G.*

Proof. See, for example, [14, pp. 49ff.]. □

Notation 5.3.5. *Let G be a finite group.*

1. *Denote by* $\mathrm{Irr}(G)$ *the set of irreducible* $\mathbb{C}$*-characters of* G.
2. *Set* $\mathrm{degsum}(G) := \sum_{\chi\in\mathrm{Irr}(G)}\chi(1)$.

Corollary 5.3.6. *Let G be a finite complete group. Then* $\mathrm{L}_{-1}(G) \leq \mathrm{degsum}(G) \leq \sqrt{\mathrm{k}(G)\cdot|G|}$.

Proof. Fix $g \in G$ such that $|\sqrt{g}| = \mathrm{maxsqrt}(G)$, and note that by Proposition 5.3.3 and Theorem 5.3.4, we have

$$\begin{aligned}\mathrm{L}_{-1}(G) = \mathrm{maxsqrt}(G) = |\sqrt{g}| = ||\sqrt{g}|| = |\sum_{\chi\in\mathrm{Irr}(G)}\nu_2(\chi)\chi(g)| \\ \leq \sum_{\chi\in\mathrm{Irr}(G)}|\nu_2(\chi)|\cdot|\chi(g)| \leq \sum_{\chi\in\mathrm{Irr}(G)} 1\cdot\chi(1) = \mathrm{degsum}(G).\end{aligned}$$

The inequality $\mathrm{degsum}(G) \leq \sqrt{\mathrm{k}(G)\cdot|G|}$ is a well-known application of the Cauchy-Schwarz inequality (using that $\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)^2 = |G|$). □

We are now ready to prove Theorem 5.3.1.

Proof of Theorem 5.3.1. Since $\mathrm{Aut}(S)$ is complete, we have, by Corollary 5.3.6 and Theorem 5.2.1,

$$\mathrm{L}_{-1}(\mathrm{Aut}(S)) \leq \sqrt{\mathrm{k}(\mathrm{Aut}(S))\cdot|\mathrm{Aut}(S)|} \leq \sqrt{|\mathrm{Aut}(S)|^{0.41}\cdot|\mathrm{Aut}(S)|} = |\mathrm{Aut}(S)|^{0.705},$$

which in view of Corollary 5.2.5 implies the assertion. □

5.4 On L_3-values of (almost) simple groups

This subsection is dedicated to the proof of the following theorem:

Theorem 5.4.1. *For all large enough nonabelian finite simple groups S, we have* $\mathrm{L}_3(\mathrm{Aut}(S))/|S| \leq |S|^{-0.053}$. *In particular,* $\mathrm{L}_3(\mathrm{Aut}(S))/|S| \to 0$ *as* $|S| \to \infty$.

This implies that $\mathrm{l}_3(T) \to 0$ as $|T| \to \infty$ for finite almost simple groups T, which in view of Lemma 2.2.4 is a weaker form of Theorem 1.1.2(4). We will see that using what we know so far, the inequality $\mathrm{L}_3(\mathrm{Aut}(S))/|S| \leq |S|^{-0.053}$ can be verified with a rather short argument for all large enough S except for those from the infinite family $\mathrm{A}_1(q)$, q a prime power, which are settled in the following theorem:

Theorem 5.4.2. *Fix $\epsilon \in (0, 1/4)$. Then for all large enough prime powers q, we have* $\mathrm{L}_3(\mathrm{Aut}(\mathrm{A}_1(q))) \leq q^{11/4+\epsilon}$.

For proving Theorem 5.4.2, we require the following technical lemma, which gives, for polynomials $P(X) \in \mathbb{F}_q[X]$ satisfying a lacunarity condition of a special kind, an upper bound on the number of roots of $P(X)$ in $\mathbb{F}_q$ which is better than the trivial bound, $\deg(P(X))$.

Lemma 5.4.3. *Let $q = p^K$ be a prime power, $L \in \mathbb{Z}$ with $\frac{3}{4}K \leq L < K$, and $0 < \epsilon < \frac{1}{4}$. Furthermore, let $P(X) \in \mathbb{F}_q[X]$, and assume that $P(X) = P_1(X) + P_2(X)$, where $\deg(P_1(X)) \leq q^{1/2+\epsilon}$, and $\deg(P_2(X)) \leq q^{L/K} + q^{1/2+\epsilon} - 1 < q$, but $\operatorname{mindeg}(P_2(X)) \geq p^L = q^{L/K}$. Then there exists a nonzero polynomial $Q(X) \in \mathbb{F}_q[X]$ of degree at most $q^{3/4+\epsilon}$ such that for all $x \in \mathbb{F}_q$, x is a root of $P(X)$ if and only if it is a root of $Q(X)$. In particular, $P(X)$ has at most $q^{3/4+\epsilon}$ roots in $\mathbb{F}_q$.*

Proof. Denote by Frob the Frobenius endomorphism of the ring $\mathbb{F}_q[X]$. Set $\tilde{P}_i(X) := \operatorname{Frob}^{K-L}(P_i(X))$ for $i = 1, 2$, and let $\tilde{P}(X) := \tilde{P}_1(X) + \tilde{P}_2(X) = \operatorname{Frob}^{K-L}(P(X))$. Observe that for all $x \in \mathbb{F}_q$, $P(x) = 0$ if and only if $\tilde{P}(x) = 0$. Furthermore, we have $\deg(\tilde{P}_1(X)) \leq q^{1/2+\epsilon} \cdot q^{(K-L)/K} \leq q^{3/4+\epsilon}$, and since the degrees of the nonzero monomials of $P_2(X)$ are of the form $q^{L/K} + e$ with $e \in \left[0, q^{1/2+\epsilon} - 1\right]$, we find that the degrees of the nonzero monomials of $\tilde{P}_2(X)$ are of the form $q + \tilde{e}$ with $\tilde{e} \in \left[0, q^{3/4+\epsilon} - q^{(K-L)/K}\right]$. Let $T(X) \in \mathbb{F}_q[X]$ be the polynomial obtained from $\tilde{P}_2(X)$ by reducing the exponent of X in each monomial modulo $q - 1$ (i.e., by subtracting $q - 1$). Then $\deg(T(X)) \leq 1 + (q^{3/4+\epsilon} - q^{(K-L)/K}) < q^{3/4+\epsilon}$, and since the identity $x^q = x$ holds in $\mathbb{F}_q$, we have $T(x) = \tilde{P}_2(X)$ for all $x \in \mathbb{F}_q$. Hence, setting $Q(X) := \tilde{P}_1(X) + T(X)$, we find that $Q(X)$ has the required properties; note that $Q(X)$ is nonzero since it has only $\deg(P(X)) < q$ many roots in $\mathbb{F}_q$. □

Proof of Theorem 5.4.2. Write $q = p^K$, where p is a prime and $K \in \mathbb{N}^+$. Denote by Frob the Frobenius automorphism of the field $\mathbb{F}_q$. We know that $\operatorname{Aut}(\mathrm{A}_1(q)) = \operatorname{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q) \rtimes \operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, and that it is a complete group. We think of the elements of $\mathrm{PGL}_2(q)$ as represented by (2×2)-matrices over $\mathbb{F}_q$ such that either the bottom right entry is 1 or the bottom right entry is 0 and the top right entry is 1 ("normalized form"). For $U \in \mathrm{GL}_2(q)$ (not necessarily normalized), we denote by $\overline{U}$ the image of U under the canonical projection $\mathrm{GL}_2(q) \to \mathrm{PGL}_2(q)$.

Fix an (inner) automorphism α of $\operatorname{Aut}(\mathrm{A}_1(q))$, say the conjugation by the element $\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}\sigma$, where $\sigma = \operatorname{Frob}^L$ with $L \in \{0, 1, \ldots, K-1\}$ and the coefficients a, b, c, d are such that the matrix is normalized. We want to show that for large enough q, the number of elements $\beta = \beta(e, f, g, h, \psi) = \overline{\begin{pmatrix} e & f \\ g & h \end{pmatrix}}\psi \in \operatorname{Aut}(\mathrm{A}_1(q))$, say with $\psi = \operatorname{Frob}^M$ and e, f, g, h such that the matrix is normalized, that are cubed by α (call such elements "good") is bounded from above by $q^{11/4+\epsilon}$.

Observe first that by considering the equation $\alpha(\beta(e, f, g, h, \psi)) = \beta(e, f, g, h, \psi)^3$ in $\operatorname{Aut}(\mathrm{A}_1(q))$ modulo the characteristic subgroup $\mathrm{PGL}_2(q)$, we find that a necessary condition for goodness of β is that $\psi^3 = \psi$, or equivalently $\psi^2 = \mathrm{id}$. This leaves at most two possibilities for ψ: The identity automorphism of $\mathbb{F}_q$, and if $2 \mid K$ (i.e., if q is a square) the unique element of order 2 in $\operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, $\operatorname{Frob}^{K/2}$. Henceforth, we will always assume that $\psi^2 = \mathrm{id}$.

Easy computations reveal that

$$\beta^3 = \overline{\left(\begin{matrix} e^2\psi(e)+ef\psi(g)+eg\psi(f)+fg\psi(h) \\ eg\psi(e)+eh\psi(g)+g^2\psi(f)+gh\psi(h) \end{matrix}\right.}$$
$$\overline{\left.\begin{matrix} ef\psi(e)+f^2\psi(g)+eh\psi(f)+fh\psi(h) \\ fg\psi(e)+fh\psi(g)+gh\psi(f)+h^2\psi(h) \end{matrix}\right)}\psi \tag{3}$$

(note that the matrix is broken over two lines, with the first column in the first line and the second column in the second line) and

$$\alpha(\beta) = \overline{\left(\begin{matrix} a\sigma(e)\psi(d)+b\sigma(g)\psi(d)-a\sigma(f)\psi(c)-b\sigma(h)\psi(c) \\ c\sigma(e)\psi(d)+d\sigma(g)\psi(d)-c\sigma(f)\psi(c)-d\sigma(h)\psi(c) \end{matrix}\right.}$$
$$\overline{\left.\begin{matrix} -a\sigma(a)\psi(b)-b\sigma(g)\psi(b)+a\sigma(f)\psi(a)+b\sigma(h)\psi(a) \\ -c\sigma(e)\psi(b)-d\sigma(g)\psi(b)+c\sigma(f)\psi(a)+d\sigma(h)\psi(a) \end{matrix}\right)}\psi. \tag{4}$$

Note that the matrices appearing under the overlines on the right-hand sides of Equations (3) and (4) are in general not normalized. In order to bound the number of good elements, we partition the elements $\beta(e,f,g,h,\psi)$ of $\mathrm{Aut}(\mathrm{A}_1(q))$ such that $\psi^2=\mathrm{id}$ into several types (the idea being to exclude some non-generic cases from the main argument):

1. Type: $f=0$ or $g=0$. By our concept of normalized form, the assumption implies that $h=1$, so there are at most $4q^2$ such elements in total (at most $2q^2$ for each of the two cases $f=0$ resp. $g=0$, where the factor 2 comes from the two choices for ψ, and the factor q^2 is an upper bound for the number of choices for (e,g) resp. (e,f)). In particular, there are at most $4q^2$ good elements of that type.
2. Type: $f,g\neq 0$ and $fg\psi(e)+fh\psi(g)+gh\psi(f)+h^2\psi(h)=0$. Thinking of f,g,h,ψ as fixed, the last assumption becomes a nonzero polynomial equation in e of degree $p^M\leq q^{1/2}$, so for at most $q^{1/2}$ values of e, the resulting element β is of this type. Hence there are at most $2(q^2+q)q^{1/2}$ elements of that type in total, in particular at most that many good elements of that type.
3. Type: $f,g\neq 0$ and $fg\psi(e)+fh\psi(g)+gh\psi(f)+h^2\psi(h)\neq 0$. Note that if β is to be a good element of that type, it follows that $-c\sigma(e)\psi(b)-d\sigma(g)\psi(b)+c\sigma(f)\psi(a)+d\sigma(h)\psi(a)\neq 0$ as well. This allows us to normalize the matrices occurring on the right-hand sides of Equations (3) and (4) by dividing through the bottom right entry. We may then compare the top left entries of the normalized matrices to obtain the following necessary condition for goodness of β:

$$\begin{aligned}
&(e^2\psi(e)+ef\psi(g)+eg\psi(f)+fg\psi(h)) \\
&\cdot(-c\sigma(e)\psi(b)-d\sigma(g)\psi(b)+c\sigma(f)\psi(a)+d\sigma(h)\psi(a)) \\
&=(fg\psi(e)+fh\psi(g)+gh\psi(f)+h^2\psi(h)) \\
&\cdot(a\sigma(e)\psi(d)+b\sigma(g)\psi(d)-a\sigma(f)\psi(c)-b\sigma(h)\psi(c)).
\end{aligned} \tag{5}$$

We will now bound the number of elements β such that Equation (5) holds. To this end, we make a case distinction:

(a) Case: $b, c \neq 0$. View f, g, h, ψ as fixed. We want to bound the number of $e \in \mathbb{F}_q$ such that Equation (5) holds. It is easy to check by the assumptions that Equation (5) is a polynomial equation in e of degree precisely $p^L + p^M + 2$. We distinguish two subcases:

- Subcase: $L \leq \frac{3}{4}K$. Then Equation (5) is a nonzero polynomial equation in e of degree at most $q^{3/4} + q^{1/2} + 2 \leq q^{3/4+\epsilon/3}$ for q large enough. Hence the number of good elements of Type 3 is bounded from above by $2(q^2+q)q^{3/4+\epsilon/3} \leq q^{11/4+\epsilon/2}$ for q large enough, and so the total number of good elements is, still for large enough q, bounded from above by $4q^2 + 2(q^2+q)q^{1/2} + q^{11/4+\epsilon/2} \leq q^{11/4+\epsilon}$, as required.
- Subcase: $L > \frac{3}{4}K$. Note that the nonzero e-monomials occurring in the polynomial Equation (5) have degrees among the following numbers: $p^L + p^M + 2$, $p^L + p^M$, $p^L + 1$, p^L, $p^M + 2$, p^M, 1 and 0. Hence for large enough q, we find that Equation (5) is equivalent to a condition of the form $P(e) = 0$, where $P(X) \in \mathbb{F}_q[X]$ depends on f, g, h, ψ and satisfies the lacunarity assumptions of Lemma 5.4.3 with ϵ replaced by $\epsilon/3$. Hence by an application of Lemma 5.4.3, we can conclude just as in the first subcase.

(b) Case: $b = 0$ or $c = 0$. We note that by our concept of normalization, the case assumption implies that $a \neq 0$ and $d = 1$. Observe also that it implies that the first summand $-c\sigma(e)\psi(b)$ of the second factor on the left-hand side of Equation (5) vanishes, turning the factor into a constant e-polynomial distinct from 0, so that the e-polynomial on the left-hand side of Equation (5) now only has degree $p^M + 2$, whereas the polynomial on the right-hand side has degree $p^M + p^L$. Hence if $L > 1$, and thus $p^M + p^L > p^M + 2$, then Equation (5) is equivalent to a condition of the form $P(e) = 0$, where $P(X) \in \mathbb{F}_q[X]$ is of degree $p^M + p^L$, and we can conclude as in Case (a) (distinguishing between the subcases $L \leq \frac{3}{4}K$ and $L > \frac{3}{4}K$).

It remains to discuss the two cases $L = 0$ and $L = 1$. Note that we are done once we have shown that for each choice of f, g, h, ψ, there are, for large enough q, at most $q^{3/4+\epsilon/3}$ many choices of e such that Equation (5) holds. For $L = 0$, Equation (5) is a polynomial equation in e of degree $p^M + 2 \leq q^{1/2+\epsilon/2}$ for q large enough, whence we are done. For $L = 1$, which implies that $K \geq 2$, and assuming $p > 2$, Equation (5) is polynomial in e of degree $p^M + p \leq 2q^{1/2} \leq q^{1/2+\epsilon/3}$ for q large enough, whence we are also done.

Let us now discuss the final case, $L = 1$ and $p = 2$. Then both sides of Equation (5) are polynomials in e of degree $2^M + 2 \leq q^{1/2+\epsilon/3}$ for $q = 2^K$ large enough, so all that we need to show is that for each choice of f, g, h, ψ, there always is at least one e-monomial that does not cancel when subtracting the monomials of one side of Equation (5) from the other. This is certainly true when the leading coefficients are distinct, so we assume that they are equal. Furthermore, note that if $fh\psi(g)+gh\psi(f)+h^2\psi(h)\neq 0$, then the RHS of Equation (5) has an e-monomial of degree 2, which the LHS does not have, and we are done. Hence assume $fh\psi(g)+gh\psi(f)+h^2\psi(h)=0$. Then if $h\neq 0$, the LHS has a constant e-monomial, but the RHS does not have such a monomial, whence we may even assume that $h=0$. Henceforth, we assume additionally that $b=0$; the case $c=0$ works analogously. Note that under this additional assumption, by comparing the leading coefficients of the two sides of Equation (5), we obtain $cf^2a^{2^M}=fga$, which implies that $c\neq 0$. Moreover, we know that $M\in\{0,\frac{K}{2}\}$, but if $M=\frac{K}{2}$, then the LHS of Equation (5), in contrast to the RHS, does not have an e-monomial of degree 2^M. Therefore, we may assume $M=0$ from now on. Then the coefficient of the e-monomial of degree 1 on the LHS of Equation (5) equals $(fg+gf)\cdot c\sigma(f)\psi(a)=0$, and so the e-monomial of degree 1 on the RHS does not cancel, which concludes the proof.

□

Proof of Theorem 5.4.1. By Theorem 5.4.2 and observing that $|\mathrm{A}_1(q)|=\Theta(q^3)$ as $q\to\infty$, we may assume that S is not isomorphic with any $\mathrm{A}_1(q)$, q a prime power. Then by Corollary 5.2.5 and Corollary 5.2.3, we have $|\mathrm{Out}(S)|\leq|S|^{0.001}$ and $\mathrm{k}(S)\leq|S|^{0.26}$, provided that S is large enough. Fix an automorphism α of $\mathrm{Aut}(S)$ such that $\mathrm{L}_3(\alpha)=\mathrm{L}_3(\mathrm{Aut}(S))$. Distinguish two cases:

1. Case: $|\mathrm{fix}(\alpha_{|S})|\geq|S|^{0.685}$. Then we have

$$\begin{aligned}\frac{\mathrm{L}_3(\mathrm{Aut}(S))}{|S|}&=\frac{\mathrm{L}_3(\alpha)}{|S|}\leq\frac{\mathrm{L}_3(\mathrm{Out}(S))\cdot\mathrm{L}_{-1}(S)}{|\mathrm{fix}(\alpha_{|S})|}\leq\frac{|\mathrm{Out}(S)|}{|\mathrm{fix}(\alpha_{|S})|}\cdot\mathrm{L}_{-1}(\mathrm{Aut}(S))\\&\leq\frac{|\mathrm{Out}(S)|}{|\mathrm{fix}(\alpha_{|S})|}\cdot\sqrt{\mathrm{k}(\mathrm{Aut}(S))\cdot|\mathrm{Aut}(S)|}\\&\leq\frac{|\mathrm{Out}(S)|}{|\mathrm{fix}(\alpha_{|S})|}\cdot\sqrt{\mathrm{k}(S)}\cdot|\mathrm{Out}(S)|\cdot\sqrt{|S|}\\&\leq|S|^{0.001+0.13+0.001+0.5-0.685}=|S|^{-0.053}.\end{aligned}$$

2. Case: $|\mathrm{fix}(\alpha_{|S})|<|S|^{0.685}$. Then $|\mathrm{fix}(\alpha)|\leq|\mathrm{fix}(\alpha_{|S})|\cdot|\mathrm{Out}(S)|<|S|^{0.686}$. It follows that

$$\begin{aligned}\mathrm{L}_3(\mathrm{Aut}(S))&\leq\mathrm{k}(\mathrm{Aut}(S))\cdot|\mathrm{fix}(\alpha)|\leq\mathrm{k}(S)\cdot|\mathrm{Out}(S)|\cdot|\mathrm{fix}(\alpha)|\\&<|S|^{0.26+0.001+0.686}=|S|^{0.947},\end{aligned}$$

and so $\mathrm{L}_3(\mathrm{Aut}(S))/|S|<|S|^{-0.053}$.

□

As mentioned in the Overview (Subsection 1.2), we can now define the function g and thus fill Theorem 1.1.2(4) with meaning:

Notation 5.4.4. *We define a function* $\mathrm{g}:(0,1]\rightarrow[1,\infty)$ *as follows:*

Let C *be the minimal positive constant such that for all nonabelian finite simple groups* S *with* $|S|>\mathrm{C}$*, the inequality* $\mathrm{L}_3(\mathrm{Aut}(S))/|S|\leq|S|^{-0.053}$ *holds. Then for* $\rho\in(0,1]$*, let* $\mathrm{O}(\rho)$ *denote the maximum outer automorphism group order of a nonabelian finite simple group of order at most* $\max(\mathrm{C},\rho^{-1/0.053})$*, and set* $\mathrm{n}(\rho):=\lfloor 16\cdot\frac{\log_{60}(\rho)}{-0.053}+\log_{(1-\frac{1}{\max(\mathrm{C},\rho^{-1/0.053})})}(\frac{\rho}{\mathrm{O}(\rho)^{16\cdot\frac{\log_{60}(\rho)}{-0.053}}})\rfloor$.

We define $\mathrm{g}(\rho):=|\,\mathrm{Aut}(\prod_S S^{\mathrm{n}(\rho)})|$*, where* S *runs through all nonabelian finite simple groups of order at most* $\max(\mathrm{C},\rho^{-1/0.053})$.

5.5 Coset-wise counting of elements cubed by an automorphism in finite semisimple groups with characteristically simple socle

We begin by fixing the meaning of some variables. Let H be a finite semisimple group with characteristically simple socle, say $\mathrm{Soc}(H)=S^n$ for a nonabelian finite simple group S. Viewing H as a subgroup of $\mathrm{Aut}(\mathrm{Soc}(H))=\mathrm{Aut}(S)^n\rtimes\mathcal{S}_n$, we set $K:=H\cap\mathrm{Aut}(S)^n$. Note that $\mathrm{Soc}(H)\leq K$, and that elements of H lie in the same coset of K if and only if their images under the canonical projection $\pi:\mathrm{Aut}(\mathrm{Soc}(H))\rightarrow\mathcal{S}_n$ are equal. Fix an automorphism α of H, which is already determined by its restriction to $\mathrm{Soc}(H)=S^n$, so that we can write (identifying α with that restriction) $\alpha=(\alpha_1\times\cdots\times\alpha_n)\circ\sigma_\alpha$, where α_i is an automorphism of S for $i=1,\ldots,n$, and σ_α is a coordinate permutation on S^n identified with an element of $\mathcal{S}_n$.

Now assume that $\beta\in H$ is cubed by α. Just like α, write $\beta=(\beta_1\times\cdots\times\beta_n)\circ\sigma_\beta$. Our goal in this subsection is to establish an upper bound on the number of elements in the coset $K\beta$ that are cubed by α based on the cycle structures of σ_α and σ_β. This will be used in the proof of Theorem 1.1.2(4) in a K-coset-wise counting argument.

To this end, set $K_\beta:=\{k\in K\mid\alpha(k\beta)=(k\beta)^3\}$. An application of Corollary 3.1.5 with $e:=3$ yields:

Proposition 5.5.1. *Let* $k=(k_1,\ldots,k_n)\in K\subseteq\mathrm{Aut}(S)^n$*. Then* $k\in K_\beta$ *if and only if* $\alpha(k)=k\beta(k)\beta^2(k)$*, i.e., if and only if for all* $i=1,\ldots,n$*, we have*

$$\alpha_i(k_{\sigma_\alpha^{-1}(i)})=k_i\cdot\beta_i(k_{\sigma_\beta^{-1}(i)})\cdot(\beta_i\circ\beta_{\sigma_{\beta^{-1}(i)}})(k_{\sigma_\beta^{-2}(i)}).\tag{6}$$

□

The idea now is to derive dependencies between certain coordinates of elements $k=(k_1,\ldots,k_n)\in K_\beta$ based on Equation (6). More precisely, we will work with the following concept (defining, or $i=1,\ldots,n$, π_i as the i-th coordinate projection $\mathrm{Aut}(S)^n\rightarrow\mathrm{Aut}(S)$):

Definition 5.5.2. *Let* $I\subseteq\{1,\ldots,n\}$*, say* $I=\{i_1,\ldots,i_j\}$ *with* $i_1<i_2<\cdots<i_j$*, and let* $F\subseteq K$ *and* $C>0$*. We say that* F *is* C***-determined by*** I *if and only if for* *all $k_{i_1},\ldots,k_{i_j} \in \mathrm{Aut}(S)$, there are at most C elements $f \in F$ such that $\pi_{i_l}(f) = k_{i_l}$ for all $l = 1,\ldots,j$.*

Proposition 5.5.3. *Let $I \subseteq \{1,\ldots,n\}$, $C > 0$, and assume that $F \subseteq K$ is C-determined by I. Then $|F| \leq \frac{C}{|S|^{n-|I|}} \cdot |K|$.*

Proof. Say $I = \{i_1,\ldots,i_j\}$, $i_1 < i_2 < \cdots < i_j$. For proving the assertion, it is sufficient to give exact covers $(F_{\vec{k}})_{\vec{k}\in\mathrm{Aut}(S)^j}$ and $(K_{\vec{k}})_{\vec{k}\in\mathrm{Aut}(S)^j}$ of F and K respectively such that for all $\vec{k} \in \mathrm{Aut}(S)^j$, $|F_{\vec{k}}| \leq \frac{C}{|S|^{n-|I|}}|K_{\vec{k}}|$. To this end, define, for $X \in \{F, K\}$ and $\vec{k} = (k_{i_1},\ldots,k_{i_j}) \in \mathrm{Aut}(S)^j$, $X_{\vec{k}}$ as the set of those $x \in X$ such that $\pi_{i_l}(x) = k_{i_l}$ for $l = 1,\ldots,j$.

Clearly, $(X_{\vec{k}})_{\vec{k}\in\mathrm{Aut}(S)^j}$ is an exact cover of X for $X = F, K$, and $F_{\vec{k}} \subseteq K_{\vec{k}}$ for all $\vec{k} \in \mathrm{Aut}(S)^j$. Hence the asserted inequality concerning the cardinalities of $F_{\vec{k}}$ and $K_{\vec{k}}$ is trivial if $K_{\vec{k}} = \emptyset$. On the other hand, if $K_{\vec{k}} \neq \emptyset$, the inequality follows by observing that $|F_{\vec{k}}| \leq C$ by assumption, whereas $|K_{\vec{k}}| \geq |S|^{n-j}$, since if $k \in K_{\vec{k}}$, we also have $kt \in K_{\vec{k}}$ for all $t \in S^n$ with $\pi_{i_l}(t) = 1$ for $l = 1,\ldots,j$. □

In order to apply Proposition 5.5.3 for our problem of bounding $|K_\beta|$, we introduce the following notions:

Definition 5.5.4. *(1) We call an index $i \in \{1,\ldots,n\}$* ***opportune*** *if and only if i is not a common fixed point of σ_α and σ_β.*

(2) For an opportune index $i \in \{1,\ldots,n\}$, we call the set $\mathrm{O}_i := \{i, \sigma_\alpha^{-1}(i), \sigma_\beta^{-1}(i), \sigma_\beta^{-2}(i)\}$ an ***opportune index set****.*

The next lemma provides the aforementioned bound on $|K_\beta|$ based on the cycle structures of σ_α and σ_β:

Lemma 5.5.5. *(1) Let $M \in \mathbb{N}$. If there are at least M opportune $i \in \{1,\ldots,n\}$, then there exists a family of $\lceil \frac{M}{16} \rceil$ pairwise disjoint opportune index sets.*

(2) If $O_1,\ldots,O_t$ are t pairwise disjoint opportune index sets, then there exist $o_i \in O_i$, $i = 1,\ldots,t$, such that K_β is $|S|^{0.882t}$-determined by $\{1,\ldots,n\} \setminus \{o_1,\ldots,o_t\}$.

(3) Let $M \in \mathbb{N}$, $M \geq 1$. If there are at least M opportune $i \in \{1,\ldots,n\}$, then $\frac{|K_\beta|}{|K|} \leq |S|^{-0.118\lceil M/16\rceil} \leq \min(|S|^{-0.118}, 60^{-0.118\lceil M/16\rceil})$.

Proof. (3) follows from (1) and (2) via Proposition 5.5.3.

For (1): This is clear if $M \leq 16$, so assume that $M > 16$. Define $\mathcal{O}_0$ as the set of opportune indices $i \in \{1,\ldots,n\}$. Note that $|\mathcal{O}_0| \geq M$ by assumption, fix any $i_0 \in \mathcal{O}_0$, and set $\Omega_0 := \mathrm{O}_{i_0}$. Assume now that, for some $k \in \{0,\ldots,\lceil M/16\rceil - 2\}$, we have already defined a decreasing chain of $k+1$ sets of opportune indices $\mathcal{O}_0 \supseteq \mathcal{O}_1 \supseteq \cdots \supseteq \mathcal{O}_k$ such that $|\mathcal{O}_k| \geq M - 16k$. Assume further that we have defined $k+1$ pairwise disjoint opportune index sets $\Omega_0,\ldots,\Omega_k$ such that for $l = 0,\ldots,k-1$, $(\Omega_l \cup \sigma_\alpha[\Omega_l] \cup \sigma_\beta[\Omega_l] \cup \sigma_\beta^2[\Omega_l]) \cap \mathcal{O}_{l+1} = \emptyset$. Then set $\mathcal{O}_{k+1} := \mathcal{O}_k \setminus (\Omega_k \cup \sigma_\alpha[\Omega_k] \cup \sigma_\beta[\Omega_k] \cup \sigma_\beta^2[\Omega_k])$. Noting that $|\mathcal{O}_{k+1}| \geq |\mathcal{O}_k| - 16 \geq M - 16(k+1) > 0$, fix any $i_{k+1} \in \mathcal{O}_{k+1}$ and set $\Omega_{k+1} := \mathcal{O}_{i_{k+1}}$. It is easy to check that with these definitions, the recursive construction is continued, and we can use this to construct $\lceil M/16\rceil$ pairwise disjoint opportune index sets $\Omega_0, \Omega_1, \ldots, \Omega_{\lceil M/16\rceil - 1}$, as required.

For (2): By Theorem 5.3.1, it suffices to show that for any opportune index i, there exists $r \in \mathrm{O}_i = \{i, \sigma_\alpha^{-1}(i), \sigma_\beta^{-1}(i), \sigma_\beta^{-2}(i)\}$ such that upon fixing, for each $t \in \mathrm{O}_i \setminus \{r\}$, an element $k_t \in \mathrm{Aut}(S)$, there exists a subset $R \subseteq \mathrm{Aut}(S)$ of size at most $\mathrm{L}_{-1}(\mathrm{Aut}(S))$ such that for all $k \in K_\beta$ with $\pi_t(k) = k_t$ for all $t \in \mathrm{O}_i \setminus \{r\}$, we have $\pi_r(k) \in R$. We prove the existence of such an R in a case distinction. Write $k = (k_1, \ldots, k_n)$.

1. Case: $\sigma_\alpha^{-1}(i) \notin \{i, \sigma_\beta^{-1}(i), \sigma_\beta^{-2}(i)\}$. Then by Equation (6), we see that the $\sigma_\alpha^{-1}(i)$-th coordinate of k is fully determined by the i-th, $\sigma_\beta^{-1}(i)$-th and $\sigma_\beta^{-2}(i)$-th coordinates of k. In particular, we can choose R of cardinality $1 \leq \mathrm{L}_{-1}(\mathrm{Aut}(S))$ in this case.
2. Case: $\sigma_\alpha^{-1}(i) \in \{i, \sigma_\beta^{-1}(i), \sigma_\beta^{-2}(i)\}$. We distinguish further according to the length l of the cycle of i under σ_β.
   - Subcase: $l \geq 3$. Then it is not difficult to see that one can always isolate one of the three distinct coordinates of k appearing in Equation (6), so that one can again choose R of cardinality 1. For example, if $\sigma_\alpha^{-1}(i) = i$, Equation (6) is equivalent to

     $$k_{\sigma_\beta^{-2}(i)} = (\beta_{\sigma_\beta^{-1}(i)}^{-1} \circ \beta_i^{-1})(\beta_i(k_{\sigma_\beta^{-1}(i)})^{-1} k_i^{-1} \alpha_i(k_i)).$$

   - Subcase: $l = 2$. Then $\sigma_\beta^{-2}(i) = i$, so there are only two distinct coordinates in Equation (6) now, k_i and $k_{\sigma_\beta^{-1}(i)}$. If $\sigma_\alpha^{-1}(i) = i$, one can isolate $k_{\sigma_\beta^{-1}(i)}$, and if $\sigma_\alpha^{-1}(i) = \sigma_\beta^{-1}(i) =: j$, Equation (6) turns into

     $$\alpha_i(k_j) = k_i \cdot \beta_i(k_j) \cdot (\beta_i \circ \beta_j)(k_i).$$

     Hence upon fixing the value of the coordinate k_j, the terms $\alpha_i(k_j) =: C_1$ and $\beta_i(k_j) =: C_2$ become constants, and we see that a possible choice for R is the fiber of C_1 under the function $\mathrm{f}_{C_2, \beta_i \circ \beta_j} : \mathrm{Aut}(S) \to \mathrm{Aut}(S)$ (notation as in Proposition 5.1.1). By Proposition 5.1.1, this fiber has cardinality bounded from above by $\mathrm{L}_{-1}(\mathrm{Aut}(S))$, as required.
   - Subcase: $l = 1$. This subcase cannot occur, since i is opportune.

□

5.6 Proof of Theorem 1.1.2(4)

Fix $\rho \in (0, 1]$. We would like to show that the orders of finite semisimple groups H such that $\mathrm{l}_3(H) \geq \rho$ are bounded by $\mathrm{g}(\rho)$. In this proof, we will concentrate on just showing that $|H|$ is bounded (without paying attention to proving the given explicit bound), but the reader can check without difficulty that the bound on $|H|$ that our argument gives is just $\mathrm{g}(\rho)$.

Note that it suffices to bound $|\mathrm{Soc}(H)|$, since H embeds into $\mathrm{Aut}(\mathrm{Soc}(H))$. Write $\mathrm{Soc}(H) = S_1^{n_1} \times \cdots \times S_r^{n_r}$, where the S_i are pairwise nonisomorphic nonabelian finite simple groups and $n_i \in \mathbb{N}^+$ for $i = 1, \ldots, r$. The task of bounding $|\mathrm{Soc}(H)|$ can be split up into the following two subtasks:

1. Prove that $\max(|S_1|,\ldots,|S_r|)$ is bounded ("order bound").
2. Prove that $\max(n_1,\ldots,n_r)$ is bounded ("exponent bound").

We will tackle these two tasks one after the other, but first, we make the following observation to ease notation: View H as a subgroup of $\mathrm{Aut}(\mathrm{Soc}(H))=\mathrm{Aut}(S_1^{n_1})\times\cdots\times\mathrm{Aut}(S_r^{n_r})$. For $i=1,\ldots,r$, denote by $P_i\leq\mathrm{Aut}(\mathrm{Soc}(H))$ the product of the direct factors $\mathrm{Aut}(S_j^{n_j})$ of $\mathrm{Aut}(\mathrm{Soc}(H))$ for $j\neq i$. Set $C_i:=H\cap P_i$. Then C_i is characteristic in H; set $H_i:=H/C_i$. By one of the isomorphism theorems, H_i can be identified with a subgroup of $\mathrm{Aut}(\mathrm{Soc}(H))/P_i=\mathrm{Aut}(S_i^{n_i})$ containing $S_i^{n_i}$. Since l_3 is CQ-increasing, we conclude that $\mathrm{l}_3(H_i)\geq\mathrm{l}_3(H)\geq\rho$, and so in carrying out the two subtasks above, we may assume w.l.o.g. that $r=1$.

Assume thus henceforth that H is a finite semisimple group with characteristically simple socle, say $\mathrm{Soc}(H)=S^n$ for a nonabelian finite simple group S and $n\in\mathbb{N}^+$, and assume that $\mathrm{l}_3(H)\geq\rho$. Just as in Notation 5.4.4, denote by C the smallest positive constant such that for all nonabelian finite simple groups S with $|S|\geq C$, we have $\frac{\mathrm{L}_3(\mathrm{Aut}(S))}{|S|}\leq|S|^{-0.053}$ (C exists by Theorem 5.4.1), and, just as in Notation 5.4.4, denote by $\mathrm{O}(\rho)$ the maximum outer automorphism group order of a nonabelian finite simple group of order at most $\max(\mathrm{C},\rho^{-1/0.053})$. We will show that

$$|S|\leq\max(\mathrm{C},\rho^{-1/0.053}) \tag{7}$$

and that

$$n\leq 16\cdot\frac{\log_{60}(\rho)}{-0.053}+\log_{(1-\frac{1}{\max(\mathrm{C},\rho^{-1/0.053})})}\left(\frac{\rho}{\mathrm{O}(\rho)^{16\cdot\frac{\log_{60}(\rho)}{-0.053}}}\right). \tag{8}$$

Using henceforth the notation of Subsection 5.5 throughout, fix an automorphism α of H.

For establishing Equation (7), assume that $|S|>\max(\mathrm{C},\rho^{-1/0.053})$. Then $|S|>\rho^{-1/0.118}$, and so by Lemma 5.5.5(3), cosets $K\beta$ of K in H (where, if $K\beta$ contains any elements cubed by α, β is chosen to be such an element) that are distinct from K contain less than $\rho|K|$ many elements cubed by α (this is because for such cosets, $\sigma_\beta\neq\mathrm{id}$, whence there exists at least one opportune $i\in\{1,\ldots,n\}$). Hence if we can also show that the number of elements of K that are cubed by α is less than $\rho|K|$, we have a contradiction. Note that if $\sigma_\alpha\neq\mathrm{id}$, then even under $\sigma_\beta=\mathrm{id}$, there still exist opportune indices i, and we are done. On the other hand, if $\sigma_\alpha=\mathrm{id}$, and thus $\alpha=\alpha_1\times\cdots\times\alpha_n$, then since $|S|>\mathrm{C}$, the unique extension of $\alpha_{|K}$ to an automorphism of $\mathrm{Aut}(S)^n$ only cubes at most $|S|^{(1-0.053)\cdot n}$ elements in all of $\mathrm{Aut}(S)^n$, and so α only cubes at most a fraction of $|S|^{-0.053\cdot n}\leq|S|^{-0.053}<\rho$ of the elements of K, as we wanted to show.

We will also establish Equation (8) by contradiction, so assume that n is larger than the right-hand side of Equation (8). Again, we will reach a contradiction by showing that for each coset $K\beta$ of K in H, the number of elements of $K\beta$ that are cubed by α (i.e., the cardinality of the set K_β) is less than $\rho|K|$. We do so in a case distinction according to the value of the number M of opportune indices $i\in\{1,\ldots,n\}$:

1. Case: $M > 16 \cdot \frac{\log_{60}(\rho)}{-0.053}$. Then $\lceil \frac{M}{16} \rceil > \frac{\log_{60}(\rho)}{-0.118}$, or equivalently, $60^{-0.118\lceil M/16 \rceil} < \rho$, so in view of Lemma 5.5.5(3), we are done.
2. Case: $M \leq 16 \cdot \frac{\log_{60}(\rho)}{-0.053}$. Note that by assumption, we then have

$$(1 - \frac{1}{\max(\mathrm{C}, \rho^{-1/0.053})})^{n-M} \cdot \mathrm{O}(\rho)^M < \rho. \tag{9}$$

Assume w.l.o.g. that the set of common fixed points of σ_α and σ_β is $\{1, \ldots, n-M\}$. Let $\pi : \mathrm{Aut}(S)^n \to \mathrm{Aut}(S)^{n-M}$ be the projection onto the first $n-M$ coordinates. Since we may of course assume that $K\beta$ contains at least one element cubed by α, we have $\alpha(\beta) = \beta^3$ by the above convention on the choice of β. Hence by Equation (6), we have, for each $k = (k_1, \ldots, k_n) \in K_\beta$, that

$$\alpha_i(k_i) = k_i \beta_i(k_i) \beta_i^2(k_i) \tag{10}$$

for all $i = 1, \ldots, n-M$. We use this to prove that

$$|\pi[K_\beta]| \leq (1 - \frac{1}{\max(\mathrm{C}, \rho^{-1/0.053})})^{n-M} \cdot |\pi[K]|. \tag{11}$$

To see that Equation (11) holds, we count $\pi[S^n]$-coset-wise in $\pi[K]$. Fix such a coset $\pi[S^n]\kappa$ with $\kappa = (\kappa_1, \ldots, \kappa_{n-M})$, assuming w.l.o.g. that $\kappa \in \pi[K_\beta]$ and thus by Equation (10), $\alpha_i(\kappa_i) = \kappa_i \beta_i(\kappa_i) \beta_i^2(\kappa_i)$, i.e., $\kappa_i \in \mathrm{P}_3(\alpha_i \mid \mathrm{id}, \beta_i, \beta_i^2)$ (notation from Proposition 3.1.3), for $i = 1, \ldots, n-M$. Analogously, for $s = (s_1, \ldots, s_{n-M}) \in S^{n-M} = \pi[S^n]$, we have $s\kappa \in \pi[K_\beta]$ only if $s_i\kappa_i \in \mathrm{P}_3(\alpha_i \mid \mathrm{id}, \beta_i, \beta_i^2)$ for all $i = 1, \ldots, n-M$. Hence by Proposition 3.1.3, a necessary condition on $s \in S^{n-M}$ for $s\kappa \in \pi[K_\beta]$ to hold is that for $i = 1, \ldots, n-M$,

$$\alpha_i(s_i) = s_i \cdot (\tau_{\kappa_i} \circ \beta_i)(s_i) \cdot (\tau_{\kappa_i \beta_i(\kappa_i)} \circ \beta_i^2)(s_i). \tag{12}$$

By Lemma 5.1.2, for each $i = 1, \ldots, n-M$, Equation (12) holds for at most $|S|-1$ many values of $s_i \in S$, and so $\pi[S^n]$-coset-wise (and thus as a whole), the fraction of elements of $\pi[K]$ that lie in $\pi[K_\beta]$ is bounded from above by $(\frac{|S|-1}{|S|})^{n-M} = (1 - \frac{1}{|S|})^{n-M}$. Using that $|S| \leq \max(C, \rho^{-1/0.053})$, Equation (11) follows.

Observing that $|S|^M \leq |\ker \pi| \leq |\mathrm{Aut}(S)|^M$ and using Equations (9) and (11), we conclude that

$$\begin{aligned} \frac{|K_\beta|}{|K|} &\leq \frac{(1 - \frac{1}{\max(\mathrm{C}, \rho^{-1/0.053})})^{n-M} \cdot |\pi[K]| \cdot |\mathrm{Aut}(S)|^M}{|\pi[K]| \cdot |S|^M} \\ &\leq (1 - \frac{1}{\max(\mathrm{C}, \rho^{-1/0.053})})^{n-M} \cdot \mathrm{O}(\rho)^M < \rho, \end{aligned}$$

as we wanted to show.

□

6 Concluding remarks

In retrospect, we proved several results that can be used for a general investigation of the functions L_e with $e \in \mathbb{Z}$ (such as Lemma 3.1.2, Proposition 3.1.3 and Lemma 2.2.4). Still, the techniques used in the proofs of some of our results (such as Lemma 3.1.6 as well as Lemma 5.1.3 and Theorem 5.4.1, whose proof by Lemma 5.1.3 was basically reduced to the case $S = \mathrm{A}_1(q)$) were tailored for a particular exponent $e \in \{-1, 2, 3\}$, and we do not expect those results to have a straightforward generalization to other exponents.

C-submultiplicative group-theoretic functions, such as L_{-1}, allow for a particularly nice treatment. However, we note that a group-theoretic function f need not be C-submultiplicative itself in order to make use of the respective results of Subsection 2.2 for the investigation of f; it suffices to find a C-submultiplicative group-theoretic function f_0 that "majorizes" f (i.e., such that $f(G) \leq f_0(G)$ for all finite groups G) and to be able to apply the techniques for C-submultiplicative functions to f_0. In view of this, it might be interesting to note that, as is easy to see with a coset-wise counting argument and using Proposition 3.1.3, for each $e \in \mathbb{N}^+$, the group-theoretic function $\mathcal{L}_e$, defined by $G \mapsto \max_{\alpha,\beta_1,\ldots,\beta_e \in \mathrm{Aut}(G)}(|\mathrm{P}_e(\alpha \mid \beta_1, \ldots, \beta_e)|)$ (for the notation, see Proposition 3.1.3), majorizes L_e and is C-submultiplicative. In particular, in order to show, for instance, that under a condition of the form $\mathrm{l}_3(G) \geq \rho$ for some $\rho \in (0, 1]$, length(Rad(G)) is bounded, it would suffice to prove that for large enough numbers $\rho_0 \in (0, 1)$ and $k \in \mathbb{N}^+$, all finite solvable groups H with length(H) $\geq k$ satisfy $\mathcal{L}_3(H) \leq \rho_0|H|$.

While hoping that these ideas will lead to extensions of our main results to other exponents $e \in \mathbb{Z}$, we do note that analoga of our main results do not exist for *all* $e \in \mathbb{Z}$. For example, if there exists a nonabelian finite simple group S such that $e \equiv 1 \pmod{\exp(S)}$ (the smallest such $e > 1$ being 31), then for all $n \in \mathbb{N}$, $\mathrm{l}_e(S^n) = \mathrm{l}_1(S^n) = 1$, and so then not even demanding that $\mathrm{l}_e(G) = 1$ is enough to ensure that $[G : \mathrm{Rad}(G)]$ is bounded.

References

[1] A. Bors, Finite groups with an automorphism of large order, submitted (2015), preprint available on `http://www.finanz.jku.at/fileadmin/SFB_documents/LargeAutOrd_Bors.pdf`.

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

[3] J. D. Dixon, The Fitting subgroup of a linear solvable group, *J. Austral. Math. Soc.* **7** (1967) 417–424.

[4] J. Fulman and R. Guralnick, Bounds on the numbers and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Trans. Amer. Math. Soc.* **364**(6) (2012) 3023–3070.

[5] P. X. Gallagher, The number of conjugacy classes in a finite group, *Math. Z.* **118**(3) (1970) 175–179.

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

[7] V. Naik, *Groupprops, The Group Properties Wiki (beta). Automorphism sends more than three-fourths of elements to inverses implies abelian*, `http://groupprops.subwiki.org/wiki/Automorphism_sends_more_than_three-fourths_of_elements_to_inverses_implies_abelian` (2011).

[8] R. M. Guralnick and G. R. Robinson, On the commuting probability in finite groups, *J. Algebra* **300** (2006) 509–528.

[9] W. H. Gustafson, What is the probability that two group elements commute?, *Amer. Math. Monthly* **80** (1973) 1031–1034.

[10] P. V. Hegarty, On a conjecture of Zimmerman about group automorphisms, *Arch. Math. (Basel)* **80** (2003) 1–11.

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

[12] P. V. Hegarty, Finite groups with an automorphism cubing a large fraction of elements, *Math. Proc. R. Ir. Acad.* **109A**(1) (2005) 79–99.

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

[14] I. M. Isaacs, *Character theory of finite groups* (Academic Press, 1976).

[15] R. Knörr, On the number of characters in a p-block of a p-solvable group, *Illinois J. Math.* **28** (1984) 181–210.

[16] S. Kohl, A bound on the order of the outer automorphism group of a finite simple group of given order, preprint avalailable on `http://www.gap-system.org/DevelopersPages/StefanKohl/preprints/outbound.pdf` (2003).

[17] P. Lescot, Sur certains groupes finis, *Rev. Math. Spéciales* **8** (1987) 276–277.

[18] P. Lescot, Degré de commutativité et structure d'un groupe fini (1), *Rev. Math. Spéciales* **8** (1988) 276–279.

[19] P. Lescot, Degré de commutativité et structure d'un groupe fini (2), *Rev. Math. Spéciales* **4** (1989) 200–202.

[20] P. Lescot, Isoclinism classes and commutativity degrees of finite groups, *J. Algebra* **177** (1995) 847–869.

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

[22] M. W. Liebeck and L. Pyber, Upper bounds for the number of conjugacy classes of a finite group, *J. Algebra* **198**(2) (1997) 538–562.

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

[24] 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.

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

[26] A. G. O'Farrell and I. Short, *Reversibility in Dynamics and Group Theory* (Cambridge Univ. Press, 2015).

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

[28] D. J. S. Robinson, *A Course in the Theory of Groups* (Springer, 1996).

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

[30] P. Rowley, Finite groups admitting a fixed-point-free automorphism group, *J. Algebra* **174** (1995) 724–727.