

Automorphism orbits and element orders in finite groups: almost-solubility and the Monster

Alexander Bors, Michael Giudici and Cheryl E. Praeger*

October 28, 2019

Abstract

For a finite group G , we denote by $\omega(G)$ the number of $\text{Aut}(G)$ -orbits on G , and by $\text{o}(G)$ the number of distinct element orders in G . In this paper, we are primarily concerned with the two quantities $\mathfrak{d}(G) := \omega(G) - \text{o}(G)$ and $\mathfrak{q}(G) := \omega(G)/\text{o}(G)$, each of which may be viewed as a measure for how far G is from being an AT-group in the sense of Zhang (that is, a group with $\omega(G) = \text{o}(G)$). We show that the index $|G : \text{Rad}(G)|$ of the soluble radical $\text{Rad}(G)$ of G can be bounded from above both by a function in $\mathfrak{d}(G)$ and by a function in $\mathfrak{q}(G)$ and $\text{o}(\text{Rad}(G))$. We also obtain a curious quantitative characterisation of the Fischer-Griess Monster group M .

1 Introduction

The underlying theme of this paper is the study of finite groups that are “highly homogeneous”. Homogeneity conditions on structures in the general, model-theoretic sense (i.e., sets endowed with operations and relations) have been studied in various contexts for a long time. Fraïssé [23] called a structure *homogeneous* if and only if any isomorphism between finitely generated substructures extends to an automorphism of the whole structure. This notion of homogeneity has received much attention for certain classes of structures, such as graphs [28], groups [13] and linear spaces (in the design-theoretic sense) [19].

*First author’s address: Johann Radon Institute for Computational and Applied Mathematics (RICAM), Altenbergerstraße 69, 4040 Linz, Austria. E-mail: alexander.bors@ricam.oeaw.ac.at

Second and third author’s address: The University of Western Australia, Centre for the Mathematics of Symmetry and Computation, 35 Stirling Highway, Crawley 6009, WA, Australia. E-mail: michael.giudici@uwa.edu.au and cheryl.praeger@uwa.edu.au

The first author is supported by the Austrian Science Fund (FWF), project J4072-N32 “Affine maps on finite groups”. The second and third authors were supported by the Australian Research Council Discovery Project DP160102323.

2010 *Mathematics Subject Classification*: Primary: 20D60. Secondary: 20D05, 20D45.

Key words and phrases: Finite groups, Automorphism orbits, Element orders, Simple groups, Monster simple group

Of course, Fraïssé’s notion of a “homogeneous structure” is rather strong, and weaker conditions have been studied as well. For example, rather than involving all (finitely generated) substructures of a given structure X in the condition, one can restrict one’s attention to the simplest subsets of X , such as vertices (equivalently, singleton subsets) or edges when X is a graph, blocks or flags when X is a design, or elements when X is a group. The homogeneity conditions would then consist of transitivity assumptions on the natural action of the automorphism group $\text{Aut}(X)$ on these simple subsets, leading to well-studied notions such as vertex-transitive graphs [3, Definition 4.2.2, p. 85], block-transitive designs [10, 11], flag-transitive designs [35], or flag-transitive finite projective planes [56].

It should be noted that even some of these weaker (compared to Fraïssé’s approach) homogeneity conditions on structures X are so strong that only a few “standard” examples for X satisfy them. For example, the only finite 8-arc-transitive graphs are cycles [59], and the only group G such that $\text{Aut}(G)$ acts transitively on G is the trivial group. In these cases, it may be fruitful to study even weaker conditions: s -arc-transitive graphs with $2 \leq s < 8$ have received a lot of attention (see e.g. the paper [41] and references therein), and for finite groups G , the following weakenings of the condition “ $\text{Aut}(G)$ acts transitively on G .” have been studied:

- “ $\text{Aut}(G)$ admits exactly c orbits on G .” for some given, small constant c . For $c = 2$, it is not difficult to show that this is equivalent to G being nontrivial and elementary abelian (i.e., the underlying additive group of a finite vector space). For results pertaining to $c \in \{3, 4, 5, 6, 7\}$, see the papers [2, 14, 39, 54] by various authors.
- “ $\text{Aut}(G)$ admits at least one orbit of length at least $\rho|G|$ on G .” for some given constant $\rho \in (0, 1]$. For example, it is known that if $\rho > \frac{18}{19}$, then G is necessarily soluble [4, Theorem 1.1.2(1)].
- “For each element order o in G , $\text{Aut}(G)$ acts transitively on elements of order o in G .”. In other words, $\text{Aut}(G)$ is “as transitive as possible” given that automorphisms must preserve the orders of elements. Such finite groups G are called *AT-groups* and are studied extensively by Zhang in [61].

We note that there is a connection between a slightly weaker version of AT-groups, studied in [42], and so-called CI-groups (groups G such that any two isomorphic Cayley graphs over G are “naturally isomorphic” via an automorphism of G), which have been studied by various authors, see the survey [40].

The aim of this paper is to study notions of finite groups that are “close to being AT-groups”. That is, we will view AT-groups as extremal structures, lying at one end of a quantitative spectrum of homogeneity conditions. We will do so by comparing, for a given finite group G , the numbers of $\text{Aut}(G)$ -orbits on G and of distinct element orders in G respectively, observing that G is an AT-group if and only if these two numbers are equal.

One of our main results, Theorem 1.1.2, provides upper bounds on the smallest index of a soluble normal subgroup of a finite group G that is “almost an AT-group”, with the caveat that for one of the two notions of “almost-AT-groups” with which Theorem 1.1.2 is concerned, one must also assume that the maximum number of

element orders in a soluble normal subgroup of G is bounded. So, roughly speaking, Theorem 1.1.2 states that “Almost-AT-groups are almost soluble.” Before being able to prove such a result on finite groups in general, we will study the important special case of nonabelian finite simple groups, with which Theorem 1.1.3 is concerned. This involves a curious quantitative characterisation of the Fischer-Griess Monster group M , see Theorem 1.1.3(5).

1.1 Statement of our main results

Let us first introduce some notation in order to be able to state our main results in a concise way:

Definition 1.1.1. Let G be a finite group.

- (1) We denote by $\omega(G)$ the number of $\text{Aut}(G)$ -orbits on G .
- (2) We denote by $\text{Ord}(G)$ the set of element orders in G , and we set $\text{o}(G) := |\text{Ord}(G)|$, the number of element orders in G .
- (3) For $o \in \text{Ord}(G)$, we denote by $\omega_o(G)$ the number of $\text{Aut}(G)$ -orbits on the set of order o elements in G .
- (4) We introduce the following parameters:
 - (a) $\mathfrak{d}(G) := \omega(G) - \text{o}(G)$;
 - (b) $\mathfrak{q}(G) := \omega(G) / \text{o}(G)$;
 - (c) $\mathfrak{m}(G) := \max_{o \in \text{Ord}(G)} \omega_o(G)$.
- (5) Finally, we denote by $\text{Rad}(G)$ the *soluble radical of G* (the largest soluble normal subgroup of G).

We note that $\mathfrak{d}(G) \geq 0$ and $\mathfrak{m}(G) \geq \mathfrak{q}(G) \geq 1$ for all finite groups G , and that $\mathfrak{d}(G) = 0$ if and only if $\mathfrak{m}(G) = 1$ if and only if $\mathfrak{q}(G) = 1$ if and only if G is an AT-group. Throughout this paper, \exp denotes the natural exponential function (with base the Euler constant e , and not to be confused with the notation $\text{Exp}(G)$ used for the exponent of the finite group G), and \log denotes the natural logarithm (with base e). Our first main result is the following:

Theorem 1.1.2. *There are monotonically increasing (in each component) functions $f_i : [0, \infty)^i \rightarrow [1, \infty)$ for $i = 1, 2$ such that for all finite groups G , the following hold:*

- (1) $|G : \text{Rad}(G)| \leq f_1(\mathfrak{d}(G))$.
- (2) $|G : \text{Rad}(G)| \leq f_2(\mathfrak{q}(G), \text{o}(\text{Rad}(G)))$.

Moreover, denoting by M the Fischer-Griess Monster group and setting

$$c := \frac{\log \log |M|}{\log \log (413/73)} \approx 8.76843,$$

f_1 may be chosen as follows:

$$f_1(x) =$$

$$\begin{aligned} & \exp((2^x + x) \log^c(2^x + x + 3) \exp(\log^c(2^x + x + 3))) \cdot \\ & (\log^{-1} 2 \cdot (2^x + x + 3))^{(2^x + x) \exp(\log^c(2^x + x + 3))} \cdot \\ & ((2^x + x)!)^{\exp(\log^c(2^x + x + 3))}. \end{aligned}$$

As the quotient $G/\text{Rad}(G)$ is a so-called *semisimple group* (a group without nontrivial soluble normal subgroups, following [50, p. 89]), and the class of finite semisimple groups is closely connected to the class of nonabelian finite simple groups (see [50, 3.3.18, p. 89]), it is not surprising that an important stepping stone in proving Theorem 1.1.2 is the investigation of \mathfrak{q} -values of nonabelian finite simple groups S . For these, we introduce the numerical parameters

$$\epsilon_\omega(S) := \frac{\log \log \omega(S)}{\log \log |S|}$$

and

$$\epsilon_{\mathfrak{q}}(S) := \frac{\log \log (\mathfrak{q}(S) + 3)}{\log \log |S|}. \quad (1.1.1)$$

The addition of a positive quantity in the numerator of $\epsilon_{\mathfrak{q}}(S)$ is necessary because there are examples where $\mathfrak{q}(S) = 1$ (e.g., $S = \text{Alt}(5)$), and $\log \log 1$ is not defined. On the other hand, $\log \log (\mathfrak{q}(S) + 3)$ is always defined and positive, and 3 is also the largest positive constant c such that $\mathfrak{q}(S) + c \leq \omega(S)$ for all S (this is because by Burnside's $p^a q^b$ -theorem, one always has $\omega(S) \geq o(S) \geq 4$, and $\omega(\text{Alt}(5)) = o(\text{Alt}(5)) = 4$). Hence by definition, one has $0 < \epsilon_{\mathfrak{q}}(S) \leq \epsilon_\omega(S) < 1$, and

$$\exp(\log^{\epsilon_\omega(S)} |S|) = \omega(S)$$

as well as

$$\exp(\log^{\epsilon_{\mathfrak{q}}(S)} |S|) = \mathfrak{q}(S) + 3.$$

As an important stepping stone toward proving Theorem 1.1.2, we will prove the following collection of statements on nonabelian finite simple groups, which is our second main result:

Theorem 1.1.3. *Let S be a nonabelian finite simple group. Then the following hold:*

- (1) $\liminf_{|S| \rightarrow \infty} \epsilon_\omega(S) = \frac{1}{2}$.
- (2) $\epsilon_\omega(S) \geq \frac{\log \log 4}{\log \log 60} \approx 0.231720$, with equality if and only if $S \cong \text{Alt}(5)$.
- (3) $\frac{\log o(S)}{\log \omega(S)} \rightarrow 0$ as $|S| \rightarrow \infty$.
- (4) $\liminf_{|S| \rightarrow \infty} \epsilon_{\mathfrak{q}}(S) = \frac{1}{2}$. In particular, $\mathfrak{q}(S) \rightarrow \infty$ as $|S| \rightarrow \infty$.
- (5) Denoting by M the Fischer-Griess monster group, we have that $\epsilon_{\mathfrak{q}}(S) \geq \epsilon_{\mathfrak{q}}(M) = \frac{\log \log (413/73)}{\log \log |M|} \approx 0.114045$, with equality if and only if $S \cong M$.

The appearance of the monster group M in Theorem 1.1.3(5) seems to suggest itself when considering just how small $\mathfrak{q}(M)$ is compared to $\mathfrak{q}(S)$ for other nonabelian finite simple groups S of roughly the same order as M . Indeed, one has $|M| \approx 8 \cdot 10^{53}$

and $q(M) = \frac{194}{73} \approx 2.65753$, see Table 1 below, whereas, for example, $|\text{Alt}(43)| \approx 3 \cdot 10^{52}$ and $q(\text{Alt}(43)) = \frac{31659}{559} \approx 56.63506$, and $|\text{PSL}_7(13)| \approx 3 \cdot 10^{53}$ and $q(\text{PSL}_7(13)) \geq \frac{2614423}{423} \approx 6180.66903$. In the case of $S = \text{Alt}(43)$, we computed the exact values of $\omega(S)$ and $o(S)$ using GAP [26], whereas for $S = \text{PSL}_7(13)$, the specified numerator and denominator are the lower bound $[\mathbf{k}(S)/|\text{Out}(S)|]$ on $\omega(S)$ (with $\mathbf{k}(S)$ denoting the number of conjugacy classes of S , computed with GAP) and an upper bound on $o(S)$, computed by a GAP implementation of an algorithm described below in Case (5) of our proof of Theorem 1.1.3(5) in Subsection 3.3, between Tables 10 and 11. Note that the nonabelian finite simple groups S that are AT-groups (which are precisely the groups $\text{PSL}_n(q)$ with $(n, q) \in \{(2, 5), (2, 7), (2, 8), (2, 9), (3, 4)\}$, see [61, Theorem 3.1]) cannot achieve such a small ϵ_q -value because their orders are too small (the addition of 3 in the numerator of $\epsilon_q(S)$ causes the total value of the fraction to become too large).

1.2 Overview of the proofs of Theorems 1.1.2 and 1.1.3

We first discuss the proof of Theorem 1.1.3, as it will be done first (since Theorem 1.1.3 is needed in the proofs of both statements in Theorem 1.1.2). Theorem 1.1.3 is proved in Section 3, and the proof is split into the three cases “ S is sporadic”, “ S is alternating” and “ S is of Lie type”.

- The sporadic finite simple groups S , dealt with in Subsection 3.1, are irrelevant for the asymptotic statements (1), (3) and (4) of Theorem 1.1.3, so one only needs to verify the universal bounds in statements (2) and (5) for them, which is straightforward using information from the ATLAS of Finite Group Representations [1].
- For the alternating groups $\text{Alt}(m)$, which are discussed in Subsection 3.2, the two key ideas are, firstly, that $\omega(\text{Alt}(m))$ and $o(\text{Alt}(m))$ are “almost equal to” the corresponding parameters of the symmetric group $\text{Sym}(m)$, and, secondly, that both $\omega(\text{Sym}(m))$ and $o(\text{Sym}(m))$ can be expressed in terms of certain integer partition counting functions. One can therefore apply number-theoretic results, dating back to Hardy and Ramanujan’s 1918 paper [34] but also involving comparatively recent results such as Maróti’s [46, Corollary 3.1], which together yield information on the asymptotic growth rate of and explicit bounds on those partition counting functions.
- Finally, Subsection 3.3 is concerned with the finite simple groups S of Lie type. A lower bound on $\omega(S)$ can be produced, using [22, Corollary 1, p. 506], from a well-known (see e.g. [24, Theorem 1.1(1)]) lower bound on the number of conjugacy classes of S , using that $|\text{Aut}(S) : S| = |\text{Out}(S)|$ is “small” (see e.g. [38]). On the other hand, an upper bound on $o(S)$ can be obtained as follows: Firstly, one notes that $o(S)$ is “almost” (up to a small factor) the same as the number of *semisimple* element orders (i.e., element orders not divisible by the defining characteristic of S). Secondly, every semisimple element of S is contained in a maximal torus of S , so the number of semisimple element orders in S can be bounded from above nicely using classical results on the

conjugacy classes of maximal tori of S and their orders, see [12, Section 3], [32, Lemma 3.3] and [25, Theorem 1.2(b), p. 1.8] (cf. also [45, Proposition 25.1, p. 219]). The asserted asymptotic results follow swiftly from this, and for the universal bounds, one needs to determine which “small” cases are not clear by the asymptotic arguments and repeat essentially the same arguments in a more careful manner.

Next, we talk about the proof of Theorem 1.1.2(1), which is the subject of Section 4. Assume that G is a finite group; our goal is to bound $|G : \text{Rad}(G)|$ in terms of $\mathfrak{d}(G)$. We first generalise a result of Zhang [61, Lemma 1.1] to show that if N is a characteristic subgroup of a finite group G , then $\mathfrak{m}(G/N) \leq 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$, see Lemma 4.1(2). Applied with $N := \text{Rad}(G)$, we find that $\mathfrak{m}(G/\text{Rad}(G))$ is bounded in terms of $\mathfrak{d}(G)$, which allows us to restrict our attention to finite semisimple groups H , and show that $|H|$ can be bounded from above in terms of $\mathfrak{m}(H)$. But $\mathfrak{m}(\text{Soc}(H)) \leq \mathfrak{m}(H)$, see Lemma 4.2, and since H embeds into $\text{Aut}(\text{Soc}(H))$ via its conjugation action on H , it suffices to show that $|\text{Soc}(H)|$ can be bounded from above in terms of $\mathfrak{m}(\text{Soc}(H))$. Since $\text{Soc}(H)$ is a direct product of nonabelian finite simple groups, that last statement easily reduces to Theorem 1.1.3, see Lemma 4.3.

Finally, we give an overview of the proof of Theorem 1.1.2(2), with which Section 5 is concerned.

- In Subsection 5.1, a crucial starting observation is made, namely that it suffices to show that for finite semisimple groups H , the order of H can be bounded from above in terms of $\mathfrak{q}(H)$ (compare this with bounding $|H|$ in terms of $\mathfrak{m}(H)$, which is needed in the proof of Theorem 1.1.2 and is much easier). The remainder of Section 5 is concerned with proving this result for finite semisimple groups H .
- In order to bound $\mathfrak{q}(H)$ suitably from below, we partition H into certain unions of cosets of $\text{Soc}(H)$ and study the “ \mathfrak{q} -values of these subsets”; note that at the moment, $\mathfrak{q}(G)$ is only defined when G is a finite group, not a subset M thereof, but the definition will be extended accordingly in Notation 5.2.1(3), writing $\mathfrak{q}_G(M)$. Subsection 5.2 provides simple, but important abstract tools, in the form of Lemmas 5.2.2 and 5.2.3, to make this idea of working with partitions of H feasible.
- In the first instance, the “partition approach” described in the previous bullet point allows one to show that $\mathfrak{q}(H)$ is large when $\text{Soc}(H)$ contains a (non-abelian) composition factor S for which a certain other parameter, $\tilde{\mathfrak{q}}(S)$ (see Notation 5.3.2(1)), is large; in other words, it gives a partial reduction, carried out in Subsection 5.4, to nonabelian finite simple groups, and corresponding auxiliary results on nonabelian finite simple groups S are proved for later use in Subsection 5.3.
- In the brief Subsection 5.5, we change our perspective: Our goal can be equivalently restated as showing that for each constant $c \geq 1$, the class $\mathcal{H}^{(c)}$ (see Notation 5.5.1(1)), of finite semisimple groups H with $\mathfrak{q}(H) \leq c$, is finite. The remainder of the proof is concerned with giving more and more restrictions on the members of an arbitrary, but fixed class $\mathcal{H}^{(c)}$ until it becomes clear that only

finitely many finite semisimple groups can satisfy all those restrictions. A first result in this direction is Lemma 5.5.3, which shows, as an application of the theory developed so far, that $\mathcal{H}^{(c)}$ is contained in a certain other class of finite semisimple groups, $\mathcal{H}_{\hat{m},\hat{d},\hat{p}}$ (see Notation 5.5.1(2,3) for the precise definition), whose members satisfy numerical restrictions with regard to the composition factors of their socles.

- Subsection 5.6 contains a few elementary number-theoretic results, which serve as auxiliary results in the subsequent subsection.
- Subsection 5.7 consists of some technical results holding for all finite semisimple groups H belonging to a fixed class $\mathcal{H}_{\hat{m},\hat{d},\hat{p}}$ as introduced in Subsection 5.5. First, it is observed that only a very specific kind of socle coset in a finite semisimple group H , called an \hat{h} -small socle coset (see Notation 5.7.2 for the details) is “problematic” as far as the partition idea from Subsection 5.2 is concerned, see Lemma 5.7.3. Next, Lemma 5.7.4 is proved, which basically states that \hat{h} -small socle cosets (in finite semisimple groups lying in a class $\mathcal{H}_{\hat{m},\hat{d},\hat{p}}$) contain only few distinct element orders (which is useful in view of Lemma 5.2.3). Lemma 5.7.5 narrows the set of “problematic” socle cosets C further, based on the common permutation action of the members of C on the coordinates of $\text{Soc}(H)$. Finally, Lemma 5.7.9, an application of Lemmas 5.7.4 and 5.7.5 as well as the results of Subsection 5.2, exhibits a partition of a “large part of H ” in which every partition member has large \mathfrak{q}_H -value.
- The last few remaining tools for proving Theorem 1.1.2(2) are provided in Subsection 5.8. Firstly, a third kind of class of finite semisimple groups, $\mathcal{H}_{\hat{m},\hat{d},\hat{p},\hat{r},f}$ (contained in $\mathcal{H}_{\hat{m},\hat{d},\hat{p}}$), is introduced in Notation 5.8.1, and it is shown that each class $\mathcal{H}^{(c)}$ is contained in such a class, see Lemma 5.8.2. But also, each intersection $\mathcal{H}^{(c)} \cap \mathcal{H}_{\hat{m},\hat{d},\hat{p},\hat{r},f}$ is finite, see Lemma 5.8.3. Combining these two facts, one gets that indeed, $\mathcal{H}^{(c)}$ is always finite, as required.
- To round Section 5 off, Subsection 5.9 gives the actual proof of Theorem 1.1.2(2) in a concise form, referring to results from the other subsections as needed.

1.3 Some related open questions

In this subsection, we discuss three open questions related to the results and proofs of this paper. The following is natural to ask when comparing statements (1) and (2) in Theorem 1.1.2:

Question 1.3.1. *Does there exist a monotonically increasing function $f : [1, \infty) \rightarrow [1, \infty)$ such that $|G : \text{Rad}(G)| \leq f(\mathfrak{q}(G))$ for all finite groups G ?*

As will become clear later from Remark 5.1.1, Theorem 1.1.2(2) is essentially just a statement about finite semisimple groups, which is a very helpful observation, since the structure of finite semisimple groups is well understood. However, in order to answer Question 1.3.1 in the affirmative, one would need to improve on the (probably very pessimistic) bounds

$$\omega(G) \geq \omega(G/\text{Rad}(G))$$

and

$$o(G) \leq o(\text{Rad}(G)) \cdot o(G/\text{Rad}(G))$$

from the discussion in Remark 5.1.1, and it seems inevitable that in order to do so, one needs to gain a better understanding of the “interplay” between $\text{Rad}(G)$ and $G/\text{Rad}(G)$, i.e., of the theory of extensions of finite semisimple groups by finite soluble groups. In the authors’ opinion, this a probably very challenging, but also interesting research problem, and even partial results putting structural restrictions on $\text{Rad}(G)$ or $G/\text{Rad}(G)$ (for example, assuming that $\text{Rad}(G)$ is cyclic) would be of interest.

The second open question concerns the following numerical parameter associated with each finite group:

Notation 1.3.2. Let G be a nontrivial finite group. We set

$$l(G) := \frac{\log \omega(G)}{\log o(G)}.$$

Moreover, we define the l -value of the trivial group to be 1.

Note that by definition, the parameters $\mathfrak{d}(G)$, $\mathfrak{q}(G)$ and $l(G)$ satisfy the following equations for each finite group G , which could be used as implicit definitions for them (except for $l(G)$ when G is trivial):

$$\begin{aligned} \omega(G) &= o(G) + \mathfrak{d}(G), \\ \omega(G) &= o(G) \cdot \mathfrak{q}(G) \end{aligned} \tag{1.3.1}$$

and

$$\omega(G) = o(G)^{l(G)}.$$

Note also that Theorem 1.1.3(3) just says that for nonabelian finite simple groups S , $l(S) \rightarrow \infty$ as $|S| \rightarrow \infty$. However, in contrast to $\mathfrak{d}(G)$, we have the following:

Proposition 1.3.3. *There is no monotonically increasing function $f : [1, \infty) \rightarrow [1, \infty)$ such that $|G : \text{Rad}(G)| \leq f(l(G))$ for all finite groups G .*

Proof. By contradiction: Fix such a function f . Let S be a nonabelian finite simple group with $|S| > f(2)$. Set $k := |S|$, and fix k pairwise distinct primes p_1, \dots, p_k none of which divides $|S|$. Set $G := S \times (\mathbb{Z}/(p_1 \cdots p_k)\mathbb{Z})$. Then the second factor, $\mathbb{Z}/(p_1 \cdots p_k)\mathbb{Z}$, is the soluble radical of G , and the first factor, S , is the derived subgroup of G . So both factors are characteristic in G , and thus

$$\text{Aut}(G) = \text{Aut}(S) \times \text{Aut}(\mathbb{Z}/(p_1 \cdots p_k)\mathbb{Z})$$

and

$$\omega(G) = \omega(S) \cdot \omega(\mathbb{Z}/(p_1 \cdots p_k)\mathbb{Z}) = \omega(S) \cdot 2^k. \tag{1.3.2}$$

Moreover, we have a surjection

$$\text{Ord}(S) \times \text{Ord}(\mathbb{Z}/(p_1 \cdots p_k)\mathbb{Z}) \rightarrow \text{Ord}(G), (o_1, o_2) \mapsto \text{lcm}(o_1, o_2),$$

and by the choice of p_1, \dots, p_k , this surjection is a bijection. Hence

$$o(G) = o(S) \cdot o(\mathbb{Z}/(p_1 \cdots p_k)\mathbb{Z}) = o(S) \cdot 2^k. \quad (1.3.3)$$

Recall that by definition, $k = |S| \geq 60$, which entails that

$$\omega(S) \leq k \leq 2^{k/2},$$

and thus

$$\frac{\log \omega(S)}{k \log 2} \leq \frac{1}{2}. \quad (1.3.4)$$

Combining Formulas (1.3.2), (1.3.3) and (1.3.4), we conclude that

$$l(G) = \frac{\log \omega(G)}{\log o(G)} = \frac{\log \omega(S) + k \log 2}{\log o(S) + k \log 2} = \frac{\frac{\log \omega(S)}{k \log 2} + 1}{\frac{\log o(S)}{k \log 2} + 1} \leq \frac{\log \omega(S)}{k \log 2} + 1 \leq \frac{1}{2} + 1 < 2,$$

and thus

$$f(2) \geq f(l(G)) \geq |G : \text{Rad}(G)| = |S| > f(2),$$

a contradiction. \square

Observing that for the groups G used as counter-examples in the proof of Proposition 1.3.3, $o(\text{Rad}(G))$ depends on $|G : \text{Rad}(G)|$, it still seems reasonable to ask the following:

Question 1.3.4. *Is there a function $f : [1, \infty)^2 \rightarrow [1, \infty)$ that is monotonically increasing in both components and such that $|G : \text{Rad}(G)| \leq f(l(G), o(\text{Rad}(G)))$ for all nontrivial finite groups G ?*

Note that an affirmative answer to Question 1.3.4 implies Theorem 1.1.2(2). Indeed, for each nontrivial finite group G , by taking logarithms on both sides of Formula (1.3.1) and then dividing both sides by $\log o(G)$, we find that

$$l(G) = \frac{\log \omega(G)}{\log o(G)} = 1 + \frac{\log q(G)}{\log o(G)} \leq 1 + \frac{\log q(G)}{\log 2}.$$

Hence for every finite group G (the trivial group is just checked separately),

$$l(G) \leq 1 + \frac{\log q(G)}{\log 2},$$

and so if f is as in Question 1.3.4, then

$$f_2(x, y) := \begin{cases} 1, & \text{if } \min\{x, y\} < 1, \\ f(1 + \frac{\log x}{\log 2}, y), & \text{if } \min\{x, y\} \geq 1 \end{cases}$$

is a suitable choice for the function f_2 in Theorem 1.1.2(2).

In Subsection 3.2, we show that for all $n < 25000$, $o(\text{Sym}(n))$ is at most $\exp(\sqrt{n})$. This leads to the following question, an affirmative answer to which would give a simple universally valid upper bound on $o(\text{Sym}(n))$:

Question 1.3.5. *Is it true that $o(\text{Sym}(n)) \leq \exp(\sqrt{n})$ for all positive integers n ?*

We note that Erdős and Turán’s result [21, Theorem I] on the asymptotics of $o(\text{Sym}(n))$, see also Formula (3.2.2), implies that the inequality in Question 1.3.5 does hold for all large enough n . In view of this, a possible approach to answering Question 1.3.5 would be to

- (1) work through Erdős and Turán’s proof and check whether each of the asymptotic number-theoretic results which they use has a counterpart with explicit bounds, so that $o(\text{Sym}(n)) \leq \exp(\sqrt{n})$ could at least be proved for all $n \geq N_0$ for an *explicit* positive integer N_0 , and
- (2) check with a computer whether $o(\text{Sym}(n)) \leq \exp(\sqrt{n})$ for $n < N_0$.

2 Notation

In this section, we fix some basic notation that will be used throughout this paper. The symbol \mathbb{N} will always denote the set of natural numbers including 0, and \mathbb{N}^+ denotes the set of positive integers. For a finite set Ω , we denote by $\text{Sym}(\Omega)$ the symmetric group on Ω , and for $n \in \mathbb{N}^+$, $\text{Sym}(n)$ and $\text{Alt}(n)$ denote the symmetric and alternating group on $\{1, \dots, n\}$ respectively. For a prime power q , the finite field with q elements will be denoted by \mathbb{F}_q , and the algebraic closure of a field K is denoted by \overline{K} . For a finite group G , we denote by $k(G)$ the number of conjugacy classes of G and by $\text{Exp}(G)$ the exponent of G (i.e., the least common multiple of the element orders in G).

If n is a positive integer and p is a prime, we denote by $\nu_p(n)$ the *p-adic valuation of n* , i.e., the largest nonnegative integer k such that $p^k \mid n$. We will also write $\text{Div}(n)$ for the set of (positive) divisors of n , and $\tau(n)$ for the number of (positive) divisors of n (this needs to be distinguished from the variable τ used to denote so-called “ S -types” in Section 5, see Definition 5.3.1(1)). For a positive integer n and a power π of some prime ℓ , we write $\pi \parallel n$, read “ π sharply divides n ”, when π divides n , but $\pi \cdot \ell$ does not divide n .

For functions f, g mapping from some unbounded set $M \subseteq [0, \infty)$ to $[0, \infty)$, we will use the Landau notation $f = O(g)$, meaning that there is a constant $c > 0$ such that $f(x) \leq c \cdot g(x)$ for all $x \in M$.

In what follows, we set up some notation regarding the finite simple groups of Lie type. For a prime p and a Lie symbol $X_d \in \{A_d, B_d, C_d, D_d \mid d \geq 1\} \cup \{E_6, E_7, E_8, F_4, G_2\}$, we denote by $X_d(\overline{\mathbb{F}}_p)$ the associated simple Chevalley group (i.e., simple linear algebraic group of adjoint type) over $\overline{\mathbb{F}}_p$. If σ is a Lang-Steinberg endomorphism (“Frobenius map” in the terminology of [32, p. 104]) on $X_d(\overline{\mathbb{F}}_p)$, then $X_d(\overline{\mathbb{F}}_p)_\sigma$ denotes the (finite) fixed point subgroup of σ in $X_d(\overline{\mathbb{F}}_p)$. For a finite group G and a prime p , $O^{p'}(G)$ is the subgroup of G generated by the p -elements (elements of order a power of p) of G . The notation we use for finite simple groups of Lie type follows the approach taken in [32, Section 3, pp. 104f.], so that ${}^t X_d(p^{f-t})$, where the pre-superscripted t is usually omitted if it is 1, denotes $O^{p'}(X_d(\overline{\mathbb{F}}_p)_\sigma)$, where σ is a Lang-Steinberg endomorphism of $X_d(\overline{\mathbb{F}}_p)$ satisfying the following conditions involving the parameters $t = t(\sigma)$ and $f = f(\sigma)$: Let B be any σ -invariant Borel subgroup

of $X_d(\overline{\mathbb{F}_p})$, and let T be any σ -invariant maximal torus of $X_d(\overline{\mathbb{F}_p})$ contained in B . Then t is the unique smallest positive integer (independent of the choice of B and T) such that the t -th power of the map σ^* on the character group $X(T)$ induced by σ is a positive integral multiple of $\text{id}_{X(T)}$, and $f \in \mathbb{N}^+/2 = \{\frac{1}{2}, 1, \frac{3}{2}, \dots\}$ is such that $\sigma^* = p^f \sigma_0$ with $\sigma_0^t = \text{id}_{X(T)}$; f also does not depend on the choice of B and T . So $p^f = q(\sigma)$ in the notation of [32], which is also a notation we will be using, and $f \in \mathbb{N}^+$ unless ${}^t X_d(p^{f \cdot t})$ is one of the Suzuki or Ree groups, in which case f is half of an odd positive integer. For us, a *finite simple group of Lie type* is by definition any group of the form ${}^t X_d(p^{f \cdot t})$, even if it is not a simple group (such as $A_1(2)$). We say that ${}^t X_d(p^{f \cdot t})$ is of *untwisted Lie rank* r ; with a few small exceptions (such as $A_1(7) \cong A_2(2)$), each finite simple group of Lie type has precisely one untwisted Lie rank. In the context of finite simple groups of Lie type, the terms “graph automorphism”, “field automorphism” and “graph-field automorphism” (the last meaning “product of a field and a graph automorphism”) and the associated notations Φ_S and Γ_S are used as explained in [32, p. 105]. Moreover, as in [29], $\text{Inndiag}(S)$ denotes the inner diagonal automorphism group of S (so $\text{Inndiag}({}^t X_d(p^{f \cdot t})) \cong X_d(\overline{\mathbb{F}_p})_\sigma$ in the above notation), and $\text{Outdiag}(S)$, the *outer diagonal automorphism group of S* , is the image of $\text{Inndiag}(S)$ under the canonical projection $\text{Aut}(S) \rightarrow \text{Out}(S)$. As in [29, Theorem 2.5.12(b), p. 58], we also view Φ_S and Γ_S as subsets of $\text{Out}(S)$, depending on the context. When $\alpha \in \text{Aut}(S)$ (resp. $\alpha \in \text{Out}(S)$), then as stated in [32, p. 105], α admits a unique factorisation into an element of $\text{Inndiag}(S)$ (resp. $\text{Outdiag}(S)$), an element of Φ_S and an element of Γ_S , and we call these the *inner diagonal component* (resp. *outer diagonal component*), *field component* and *graph component* of α , respectively. The product of the field and graph component of α is also called the *graph-field component* of α .

3 Proof of Theorem 1.1.3

3.1 Sporadic groups

In Table 1, we give an overview of the values of $\omega(S)$ and $\text{o}(S)$ as well as of $\epsilon_\omega(S)$ and $\epsilon_q(S)$ for the sporadic nonabelian finite simple groups S , thus proving Theorem 1.1.3 for them. This was mostly just read off from the ATLAS of Finite Group Representations [1]; only for $S = \text{T}$, the Tits group, $\omega(S)$ could not be determined directly from the ATLAS, but was computed by comparing centraliser orders, in T and $\text{Aut}(\text{T})$ respectively, of conjugacy class representatives of T .

Table 1: Overview of the sporadic groups and the Tits group

S	$\text{o}(S)$	$\omega(S)$	$\epsilon_\omega(S) \approx$	$\epsilon_q(S) \approx$
M_{11}	8	10	0.380024	0.168333
M_{12}	9	12	0.373194	0.156934
M_{22}	9	11	0.340952	0.142251
M_{23}	12	17	0.374450	0.142269

M ₂₄	15	26	0.398909	0.149020
HS	13	21	0.388150	0.148125
J ₂	11	16	0.393933	0.155060
Co ₁	32	101	0.406933	0.158971
Co ₂	21	60	0.409051	0.165308
Co ₃	21	42	0.400357	0.144505
McL	15	19	0.356873	0.122978
Suz	19	37	0.390324	0.142663
He	15	26	0.381463	0.142502
HN	22	44	0.379828	0.135821
Th	25	48	0.369346	0.127106
Fi ₂₂	22	59	0.406280	0.159655
Fi ₂₃	32	98	0.405230	0.156730
Fi' ₂₄	35	97	0.378603	0.139755
B	49	184	0.379739	0.148826
M	73	194	0.344642	0.114045
J ₁	10	15	0.399899	0.163849
O'N	18	25	0.355275	0.118954
J ₃	13	17	0.362182	0.131708
Ru	18	36	0.393116	0.146573
J ₄	31	62	0.370447	0.124360
Ly	28	53	0.377735	0.126657
T	11	17	0.369863	0.147333

3.2 Alternating groups

We will prove the following five statements:

- (I) $\frac{\log o(\text{Alt}(n))}{\log \omega(\text{Alt}(n))} \rightarrow 0$ as $n \rightarrow \infty$.
- (II) For all $n \geq 5$, $\epsilon_\omega(\text{Alt}(n)) \geq \frac{\log \log 4}{\log \log 60} \approx 0.231720$, with equality if and only if $n = 5$.
- (III) $\epsilon_\omega(\text{Alt}(n)) \rightarrow \frac{1}{2}$ as $n \rightarrow \infty$.
- (IV) For all $n \geq 5$, $\epsilon_q(\text{Alt}(n)) \geq \frac{\log \log (77/16)}{\log \log 19958400} \approx 0.160121$, with equality if and only if $n = 11$.
- (V) $\epsilon_q(\text{Alt}(n)) \rightarrow \frac{1}{2}$ as $n \rightarrow \infty$.

Proof of statement (I). This can be obtained by combining the following facts (recall that $k(G)$ denotes the number of conjugacy classes of the finite group G):

- (1) For $n \geq 7$, one has $\omega(\text{Alt}(n)) \geq \frac{1}{2} k(\text{Alt}(n)) \geq \frac{1}{4} k(\text{Sym}(n)) = \frac{1}{4} p(n)$, where the last inequality uses [16, Formula (1.6), p. 90] and $p(n)$ denotes the number of (unordered) integer partitions of n .

(2) The partition number $p(n)$ has the following asymptotics (see [34]):

$$p(n) \sim \frac{1}{4\sqrt{3n}} \exp\left(\frac{2\pi}{\sqrt{6}}\sqrt{n}\right) \quad (3.2.1)$$

(3) Clearly, $o(\text{Alt}(n)) \leq o(\text{Sym}(n))$, and by [21, Theorem I], the number of element orders in $\text{Sym}(n)$ has the following asymptotics:

$$o(\text{Sym}(n)) = \exp\left(\frac{2\pi}{\sqrt{6}}\sqrt{\frac{n}{\log n}} + O\left(\frac{\sqrt{n} \log \log n}{\log n}\right)\right). \quad (3.2.2)$$

□

Proof of statement (II). This can be checked directly for $n = 5, 6, 7, 8$. For $n \geq 9$, we use that

$$\omega(\text{Alt}(n)) \geq \frac{1}{4}p(n) > \frac{1}{56} \exp(2\sqrt{n}), \quad (3.2.3)$$

where the first inequality was already discussed in the proof of statement (I), and the second is a result of Maróti, see [46, Corollary 3.1]. Hence it suffices to check the inequality

$$\frac{\log \log (\exp(2\sqrt{n})/56)}{\log \log (n!/2)} > \frac{\log \log 4}{\log \log 60}$$

for all $n \geq 9$. For $n = 9, \dots, 54$, one just verifies this with a computer, and for $n \geq 55$, where one has

- $e\sqrt{n} \leq \frac{n}{e}$,
- $\sqrt{n} \geq \log 56$, and
- $\log(n+1) + \log \log n \leq 2 \log n$,

one proceeds as follows:

- Firstly, $\log \log (\exp(2\sqrt{n})/56) = \log(2\sqrt{n} - \log 56) \geq \log \sqrt{n} = \frac{1}{2} \log n$.
- Secondly, using the simple upper bound $n! \leq e\sqrt{n}(\frac{n}{e})^n$, which follows from Robbins' sharper bound [49], we find that

$$\log \log (n!/2) \leq \log \log n! \leq \log \log (e\sqrt{n}(\frac{n}{e})^n) \leq \log \log (\frac{n}{e})^{n+1} \leq$$

$$\log((n+1)(\log n - 1)) \leq \log((n+1) \log n) = \log(n+1) + \log \log n \leq 2 \log n.$$

Combining these inequalities, one gets that

$$\frac{\log \log (\exp(2\sqrt{n})/56)}{\log \log (n!/2)} \geq \frac{\frac{1}{2} \log n}{2 \log n} = \frac{1}{4} > \frac{\log \log 4}{\log \log 60}. \quad \square$$

Proof of statements (III) and (V). Observe that for each constant $c > 0$, using Stirling's approximation, we have that as $n \rightarrow \infty$,

$$\frac{\log \log \exp(c\sqrt{n})}{\log \log (\frac{1}{2}n!)} \rightarrow \frac{1}{2}.$$

It is thus sufficient to show that there are positive constants $c < c'$ such that for all large enough n ,

$$\exp(c\sqrt{n}) \leq \mathfrak{q}(\text{Alt}(n)) \leq \omega(\text{Alt}(n)) \leq \exp(c'\sqrt{n}). \quad (3.2.4)$$

Also, by Formula (3.2.1), for large enough n ,

$$\omega(\text{Alt}(n)) \leq \omega(\text{Sym}(n)) \leq \mathfrak{k}(\text{Sym}(n)) = p(n) \leq \exp\left(\frac{2\pi}{\sqrt{6}}\sqrt{n}\right),$$

and so $c' := \frac{2\pi}{\sqrt{6}}$ is a possible choice in Formula (3.2.4). Moreover, the bounds discussed in the proof of statement (I) yield that any choice of $c < \frac{2\pi}{\sqrt{6}}$ works in Formula (3.2.4). \square

Proof of statement (IV). For $n = 5, \dots, 37$, one verifies this directly with the aid of GAP [26]. For $n = 38, \dots, 24999$, we give an argument that relies partially on computer calculations. Indeed, one can compute $\mathfrak{o}(\text{Sym}(n))$ exactly for each such n using a certain recursion which we will now describe. Observe that

$$\mathfrak{o}(\text{Sym}(n)) = \sum_{k=0}^n r(k)$$

where $r(k)$ denotes the number of integer partitions of k into pairwise coprime prime powers each greater than 1 (note that in view of the empty partition, $r(0) = 1$). Moreover, recalling the notation \mathbb{P} for the set of primes, we have

$$r(k) = \sum_{p \leq k, p \in \mathbb{P}} r_p(k)$$

where $r_p(k)$ denotes the number of integer partitions of k into pairwise coprime prime powers greater than 1 such that the smallest prime base which occurs is p . The numbers $r_p(k)$ satisfy the recursion

$$r_p(k) = \sum_{e=1}^{\lfloor \log_p(k) \rfloor} \begin{cases} \sum_{p < \ell \leq k, \ell \in \mathbb{P}} r_\ell(k - p^e), & \text{if } k > p^e, \\ 1, & \text{if } k = p^e. \end{cases}$$

This allows one to check that $\mathfrak{o}(\text{Sym}(n)) \leq \exp(\sqrt{n})$ for all $n < 25000$. Using this and Formula (3.2.3), it follows that for all $n \in \{38, \dots, 24999\}$,

$$\mathfrak{q}(\text{Alt}(n)) = \frac{\omega(\text{Alt}(n))}{\mathfrak{o}(\text{Alt}(n))} \geq \frac{1}{4} \frac{p(n)}{\mathfrak{o}(\text{Sym}(n))} \geq \frac{1}{56} \frac{\exp(2\sqrt{n})}{\exp(\sqrt{n})} = \frac{1}{56} \exp(\sqrt{n}),$$

and thus

$$\begin{aligned} \epsilon_{\mathfrak{q}}(\text{Alt}(n)) &\geq \frac{\log \log (\exp(\sqrt{n})/56)}{\log \log (n!/2)} \geq \frac{\log (\sqrt{n} - \log 56)}{\log \log (\frac{e}{2}\sqrt{n}(\frac{n}{e})^n)} = \\ &= \frac{\log (\sqrt{n} - \log 56)}{\log (1 - \log 2 + \frac{1}{2} \log n + n(\log n - 1))}, \end{aligned}$$

and one can verify with a computer that for $n = 38, \dots, 24999$, the last expression is always at least $0.164 > \epsilon_q(\text{Alt}(11)) \approx 0.160121$.

It remains to deal with the case $n \geq 25000$. For this, we will use a different, worse upper bound on $o(\text{Sym}(n))$ than $\exp(\sqrt{n})$, obtained as follows: Note that $o(\text{Sym}(n)) \leq \sum_{k=0}^n s(k)$, where $s(k)$ denotes the number of integer partitions of k into pairwise distinct parts. By [60, Subsection 5.2], we have that $s(k) = \sum_r p(\frac{k-r(r+1)/2}{2})$, where r ranges over the nonnegative integers such that $k - \frac{r(r+1)}{2}$ is an even nonnegative integer. There are at most $\sqrt{2k}$ such r , and each corresponding summand is of the form $p(j)$ where $0 \leq j \leq \frac{k}{2}$. Using this and Erdős's explicit upper bound $p(j) \leq e^{\frac{2\pi}{\sqrt{6}}\sqrt{j}}$, see [20, pp. 437f.], it follows that $s(k) \leq \sqrt{2k} e^{\frac{\pi}{\sqrt{3}}\sqrt{k}}$, and thus $o(\text{Sym}(n)) \leq (n+1)\sqrt{2n} e^{\frac{\pi}{\sqrt{3}}\sqrt{n}}$.

Hence (and in view of Formula (3.2.3)) we get that

$$\begin{aligned} \mathfrak{q}(\text{Alt}(n)) &\geq \frac{1}{4} \frac{p(n)}{o(\text{Sym}(n))} \geq \frac{1}{56} \frac{\exp(2\sqrt{n})}{(n+1)\sqrt{2n} \cdot \exp((\pi/\sqrt{3})\sqrt{n})} = \\ &(56 \cdot (n+1)\sqrt{2n})^{-1} \cdot \exp((2 - \frac{\pi}{\sqrt{3}})\sqrt{n}). \end{aligned}$$

Note that $2 - \frac{\pi}{\sqrt{3}} > 0.1862$, and that for $n \geq 25000$, one has

$$\exp(0.1362\sqrt{n}) \geq 56(n+1)\sqrt{2n},$$

so that for all such n ,

$$\mathfrak{q}(\text{Alt}(n)) \geq \exp(\frac{1}{20}\sqrt{n}).$$

Therefore, still for $n \geq 25000$, and using again the upper bound $n! \leq e\sqrt{n}(\frac{n}{e})^n$,

$$\begin{aligned} \epsilon_q(\text{Alt}(n)) &\geq \frac{\log \log \exp(\frac{1}{20}\sqrt{n})}{\log \log (n!/2)} \geq \frac{\frac{1}{2} \log n - \log 20}{\log (1 - \log 2 + \frac{1}{2} \log n + n(\log n - 1))} \geq \\ &\frac{\frac{1}{2} \log n - \log 20}{\log (\frac{3}{2}n \log n)} = \frac{\frac{1}{2} \log n - \log 20}{\log n + \log \frac{3}{2} + \log \log n} = \frac{\frac{1}{2} - \frac{\log 20}{\log n}}{1 + \frac{\log(3/2)}{\log n} + \frac{\log \log n}{\log n}} \geq \\ &\frac{\frac{1}{2} - \frac{\log 20}{\log 25000}}{1 + \frac{\log(3/2)}{\log 25000} + \frac{\log \log 25000}{\log 25000}} > \epsilon_q(\text{Alt}(11)). \quad \square \end{aligned}$$

3.3 Groups of Lie type

We first verify the asymptotic statements (1), (3) and (4) of Theorem 1.1.3 for the finite simple groups of Lie type. Before giving the actual proofs, we make some preparatory observations. As in the previous subsection, for a finite group G , denote by $k(G)$ the number of conjugacy classes of G . As explained in Section 2, $S = {}^t X_d(p^{ft})$, and we set $q := p^f$. Then $k(\text{Inndiag}(S)) \geq q^d$ (see, for instance, [24, Theorem 1.1(1)]), and so, using [22, Corollary 1, p. 506], we have

$$k(S) \geq \frac{q^d}{|\text{Inndiag}(S) : S|} \geq \frac{q^d}{\min\{d+1, q+1\}} \tag{3.3.1}$$

Moreover, $|S| \leq q^{4d^2}$, as a simple case-by-case inspection shows. Therefore, using Kohl's bound [38],

$$|\text{Out}(S)| \leq \log_2 |S| \leq \log_2 (q^{4d^2}) = 4d^2 \log_2 q,$$

it follows that

$$\omega(S) \geq \frac{k(S)}{|\text{Out}(S)|} \geq \frac{q^d}{4d^2 \log_2 q \min\{d+1, q+1\}}. \quad (3.3.2)$$

In particular, for any $\epsilon > 0$, there is an $N_1 = N_1(\epsilon) \in \mathbb{N}^+$ such that if $\max\{d, q\} \geq N_1$, then $\omega(S) \geq q^{(1-\epsilon/2)d}$.

In what follows, we explain how to suitably bound $o(S)$ from above. Actually, our argument even provides an upper bound on $o(\text{Inndiag}(S))$. We will use the Landau notation $f = \Theta(g)$, which is defined for all functions f and g mapping from a common, unbounded set of positive real numbers to $[0, \infty)$, and it just means that $f = O(g)$ and $g = O(f)$. We will also write $\tau(n)$ for the number of divisors of a positive integer n .

- (1) We first consider unipotent element orders in $\text{Inndiag}(S)$. By [55, Corollary 0.5], the p -adic valuation of $\text{Exp}(\text{Inndiag}(S))$ is just $\lceil \log_p(H(X_d) + 1) \rceil$ where $H(X_d)$ is the height of the highest root of the root system X_d . Denote by $h(X_d)$ the *Coxeter number of X_d* , i.e., the order of any *Coxeter element* of the Weyl group $W(X_d)$ (by definition, Coxeter elements are just those elements of $W(X_d)$ that can be obtained by multiplying together, in any order, the elements of any fixed set of simple roots). Then by [36, Theorem, p. 84], $H(X_d) + 1 = h(X_d)$, so we can also write the p -adic valuation of $\text{Exp}(\text{Inndiag}(S))$ as $\lceil \log_p(h(X_d)) \rceil$ and conclude that there are exactly $1 + \lceil \log_p(h(X_d)) \rceil$ elements in $\text{Ord}(S)$ that are powers of p . The Coxeter numbers of the various indecomposable root systems can be found in tabulated form in [36, Table 2, p. 80]; for our asymptotic observations, the key property is that $h(X_d) = \Theta(d)$.
- (2) Secondly, we will consider the number of semisimple element orders in $\text{Inndiag}(S)$. We can bound this number from above by the product of
 - $k_{\text{tor}}(\text{Inndiag}(S))$, the number of conjugacy classes of maximal tori of $\text{Inndiag}(S)$, with
 - the maximum number of element orders in a maximal torus of $\text{Inndiag}(S)$.

Concerning these two quantities:

- $k_{\text{tor}}(\text{Inndiag}(S))$ is equal to the number of ϕ -conjugacy classes in the corresponding Weyl group $W = W(X_d)$ (i.e., orbits of the action of W on itself via $w^v = v^{-1}wv^\phi$), for a suitable $\phi = \phi({}^t X_d) \in \text{Aut}(W)$, see [25, Theorem 1.2(b), p. 1.8]. Since there are only finitely many Lie symbols (and thus finitely many Weyl groups) for Lie type groups of a given rank d , one has $k_{\text{tor}}(\text{Inndiag}(S)) \leq g(d)$ for some unary function g , which is of subexponential growth (see [12, Section 3] and use the asymptotics of the partition number $p(n)$ from Formula (3.2.1)).

- Recall that $\tau(n)$ denotes the number of (positive) divisors of the positive integer n . Since the order of a maximal torus in $\text{Inndiag}(S)$ is at most $(q+1)^d$ (see [32, Lemma 3.3], for instance), we find (by Lagrange's theorem) that the maximum number of element orders in a maximal torus of $\text{Inndiag}(S)$ is at most $h(d, q) := \max\{\tau(1), \tau(2), \dots, \tau((q+1)^d)\} \leq 2(q+1)^{d/2}$.

(3) Combining the above bounds, we get that

$$o(S) \leq o(\text{Inndiag}(S)) \leq (1 + \lceil \log_2 \Theta(d) \rceil) \cdot g(d) \cdot h(d, q), \quad (3.3.3)$$

and for each $\epsilon > 0$, this is at most $q^{(\frac{1}{2} + \frac{\epsilon}{2})d}$ if $\max\{d, q\} \geq N_2 = N_2(\epsilon)$.

Proof of Theorem 1.1.3(1). Note that by the results on alternating groups from the previous subsection, it suffices to show that for finite simple groups of Lie type $S = {}^tX_d(q^t)$, we have $\liminf_{|S| \rightarrow \infty} \epsilon_\omega(S) \geq \frac{1}{2}$. That is, we need to show that for each $\delta > 0$, there is an $N = N(\delta)$ such that if $\max\{d, q\} \geq N$, then $\epsilon_\omega(S) \geq \frac{1}{2} - \delta$. Assume w.l.o.g. that $\max\{d, q\} \geq N_1(1)$, with $N_1(\epsilon)$ as defined above just after Formula (3.3.2). Then

$$\epsilon_\omega(S) = \frac{\log \log \omega(S)}{\log \log |S|} \geq \frac{\log \log q^{d/2}}{\log \log q^{4d^2}} = \frac{\log d - \log 2 + \log \log q}{\log 4 + 2 \log d + \log \log q},$$

which is bounded from below by $\frac{1}{2} - \delta$ if and only if

$$\log d - \log 2 + \log \log q \geq \left(\frac{1}{2} - \delta\right) \log 4 + (1 - 2\delta) \log d + \left(\frac{1}{2} - \delta\right) \log \log q,$$

or equivalently,

$$\left(\frac{1}{2} + \delta\right) \log \log q + 2\delta \log d \geq 2(1 - \delta) \log 2,$$

and this is indeed true if $\max\{d, q\}$ is large enough (relative to δ). \square

Proof of Theorem 1.1.3(4). Note that by the definitions of $N_1(\epsilon)$ and $N_2(\epsilon)$, if

$$\max\{d, q\} \geq \max\left\{N_1\left(\frac{1}{4}\right), N_2\left(\frac{1}{4}\right)\right\},$$

then $\omega(S) \geq q^{7d/8}$ and $o(S) \leq q^{5d/8}$, whence

$$\mathfrak{q}(S) = \frac{\omega(S)}{o(S)} \geq q^{d/4}.$$

The second assertion of the statement is immediate from this, and the first also follows, using this lower bound on $\mathfrak{q}(S)$ with the same argument used for proving statement (1). \square

Proof of Theorem 1.1.3(3). Note that

$$\omega(S) \leq \omega(\text{Inndiag}(S)) \leq k(\text{Inndiag}(S)) = q^{O(1)d},$$

where the implied upper bound on $k(\text{Inndiag}(S))$ is again by [24, Theorem 1.1(1)]. But as explained after Formula (3.3.2), we also have $d = O(\log_q \omega(S))$; combining these two facts, we get

$$\omega(S) = \omega({}^tX_d(p^{ft})) = p^{\Theta(1)df} \text{ as } \max\{p, d, f\} \rightarrow \infty.$$

On the other hand, $o(S) \leq (1 + \lceil \log_2 \Theta(d) \rceil) \cdot g(d) \cdot h(d)$, and so, by the asymptotics of the number of divisors function τ (see for example [47, Théorème 1]),

$$o(S) = o({}^tX_d(p^{ft})) \leq p^{o(1)df} \text{ as } \max\{p, d, f\} \rightarrow \infty. \quad (3.3.4)$$

□

This concludes the verification of the three asymptotic statements in Theorem 1.1.3. It remains to prove the universal lower bounds on $\epsilon_\omega(S)$ and $\epsilon_q(S)$ from statements (2) and (5) respectively for finite simple groups of Lie type.

Proof of Theorem 1.1.3(2). The proof idea is simply to carefully study lower bounds on $\omega(S)$ similar to the one in Formula (3.3.2) in order to obtain a theoretical argument which proves that $\epsilon_\omega(S) > \epsilon_\omega(\text{Alt}(5))$ for all nonabelian finite simple groups S nonisomorphic to $\text{Alt}(5)$ except possibly those from an explicit finite list. These finitely many remaining exceptions are then dealt with using GAP [26]. By the results of Subsections 3.1 and 3.2, we may assume that $S = {}^tX_d(p^{ft})$ is of Lie type. Throughout, we set $q := p^f$. Moreover, we will use the following conventions: We denote by \log the function $\mathbb{R} \rightarrow \mathbb{R} \cup \{-\infty\}$ mapping

$$x \mapsto \begin{cases} \log x, & \text{if } x > 0, \\ -\infty, & \text{else.} \end{cases}$$

Furthermore, by convention,

- $-\infty < x$ for all real numbers x ,
- $-\infty + x = -\infty$ for all real numbers x , and
- $\frac{-\infty}{c} = -\infty$ for all $c > 0$.

These conventions imply the following, which will be used various times without further mentioning: If x_1, x_2, y_1, y_2 are positive real numbers with $x_1 \geq x_2$ and $y_1 \leq y_2$, then

$$\frac{\log \log x_1}{y_1} \geq \frac{\log \log x_2}{y_2}.$$

Our arguments for bounding $\epsilon_\omega(S)$, with $S = {}^tX_d(p^{ft})$, are split into the two cases “ $d \leq 2$ ” and “ $d \geq 3$ ”.

- (1) Case: $d \leq 2$. There are seven families of Lie type groups S of untwisted Lie rank d at most 2, as listed in Tables 2 and 3 below. We take the following unified approach to show that $\epsilon_\omega(S) > \epsilon_\omega(\text{Alt}(5))$ for each of them apart from $A_1(4) \cong A_1(5) \cong \text{Alt}(5)$: For each of the seven families, there is a reference in the literature for a precise formula for the number of conjugacy classes $k(S)$,

as displayed in Table 2. We note, however, that the given reference [52] for $k(B_2(q)) = k(C_2(q)) = k(\mathrm{PSp}_4(q))$ when q is odd appears to contain an error, because, according to [52, Table 2], $k(\mathrm{PSp}_4(q)) = \frac{1}{2}q^2 + \frac{13}{4}q + \frac{23}{4}$ when $q \equiv 3 \pmod{4}$, which implies that $k(\mathrm{PSp}_4(7)) = 53$, although actually (as one can check with GAP [26]) $k(\mathrm{PSp}_4(7)) = 52$. The formula for $k(\mathrm{PSp}_4(q))$ given in Table 2 is based on the fact that in each of the three cases “ q is even”, “ $q \equiv 1 \pmod{4}$ ” and “ $q \equiv 3 \pmod{4}$ ”, the conjugacy class number $k(\mathrm{PSp}_4(q))$ is a quadratic polynomial in q (the authors would like to thank Frank Lübeck for bringing this to their attention), and so in each of the three cases, the precise formula for $k(\mathrm{PSp}_4(q))$ can be obtained by computing the conjugacy class number for three different values of q from the respective congruence class, which can be done with GAP [26]. Column 2 of Table 3 contains the well-known formula for $|\mathrm{Out}(S)|$, and column 3 contains an upper bound $|S|$ on $|S|$, which is easily obtained from the well-known formula for the exact value of $|S|$. Recall from Formula (3.3.2) that

$$\omega(S) \geq k(S)/|\mathrm{Out}(S)|. \quad (3.3.5)$$

Column 4 of Table 3 lists a lower bound $\underline{\omega}(S)$ on $\omega(S)$ that can easily be derived from Formula (3.3.5) and the information in Table 2 (note that $f = \log_p q \leq \log_2 q$). In order for $\epsilon_\omega(S) > \epsilon_\omega(\mathrm{Alt}(5))$ to hold, it is sufficient to have

$$\frac{\log \log \underline{\omega}(S)}{\log \log |S|} > \epsilon_\omega(\mathrm{Alt}(5)), \quad (3.3.6)$$

and with elementary calculus, one can check that Formula (3.3.6) holds in all but finitely many cases, which are listed in column 5 of Table 3 as “fails 1”. Moreover, it is routine to check that among the finitely many groups S corresponding to column 5 of Table 3, all but those listed in column 6 as “fails 2” satisfy the inequality

$$\frac{\log \log \lceil \frac{k(S)}{|\mathrm{Out}(S)|} \rceil}{\log \log |S|} > \epsilon_\omega(\mathrm{Alt}(5)),$$

which is also sufficient for $\epsilon_\omega(S) > \epsilon_\omega(\mathrm{Alt}(5))$. Finally, for each of the remaining groups S listed in column 6, one can compute the exact value of $\omega(S)$ with a simple GAP algorithm [26] written by the authors, and use this to check that $\epsilon_\omega(S) > \epsilon_\omega(\mathrm{Alt}(5))$ in those cases as well. This algorithm proceeds by first computing the conjugacy classes of S using GAP’s built-in command `ConjugacyClasses`, and then computes the orbits of the action of $\mathrm{Out}(S)$ on the set of conjugacy classes of S using the built-in commands

- `AutomorphismGroup`,
- `InnerAutomorphismsAutomorphismGroup`,
- `RightTransversal`, and
- `IsConjugate`.

Table 2: Formulas for $k(S)$ in case $d \leq 2$.

S	formula for $k(S)$	reference for $k(S)$
$A_1(q)$	$k(S) = \begin{cases} q+1, & \text{if } 2 \mid q, \\ \frac{q+5}{2}, & \text{if } q \nmid q \end{cases}$	[44, Formula (5.2), p. 43]
$A_2(q)$	$k(S) = \begin{cases} q^2 + q, & \text{if } q \equiv 0, 2 \pmod{3}, \\ \frac{q^2+q+10}{3}, & \text{if } q \equiv 1 \pmod{3} \end{cases}$	[44, Formula (5.2), p. 43]
${}^2A_2(q^2)$	$k(S) = \begin{cases} q^2 + q + 2, & \text{if } q \equiv 0, 1 \pmod{3}, \\ \frac{q^2+q+12}{3}, & \text{if } q \equiv 2 \pmod{3} \end{cases}$	[44, Formula (6.13), p. 47]
$B_2(q) \cong C_2(q)$	$k(S) = \begin{cases} q^2 + 2q + 3, & \text{if } 2 \mid q, \\ \frac{q^2+6q+13}{2}, & \text{if } 2 \nmid q \end{cases}$	[58, Theorem 3.7.3] for q even; [52, Tables 1 and 2] for q odd, but see the paragraph before Formula (3.3.5) above
$G_2(q)$	$k(S) = \begin{cases} q^2 + 2q + 9, & \text{if } q \equiv 1, 5 \pmod{6}, \\ q^2 + 2q + 8, & \text{if } q \equiv 2, 3, 4 \pmod{6} \end{cases}$	[43]
${}^2B_2(2^{2k+1})$	$k(S) = 2^{2k+1} + 3$	[43]
${}^2G_2(3^{2k+1})$	$k(S) = 3^{2k+1} + 8$	[43]

Table 3: Remaining information for the case $d \leq 2$.

S	$ \text{Out}(S) $	$ S $	$\frac{\omega(S)}{4 \log_2 q}$	fails 1	fails 2
$A_1(q), q \geq 7$	$\gcd(2, q-1) \cdot f$	q^3	$\frac{q}{4 \log_2 q}$	$q \leq 199$	$q = 7, 8, 9, 11, 13, 16, 25, 27$
$A_2(q), q \geq 3$	$\gcd(3, q-1) \cdot 2f$	q^8	$\frac{q^2}{18 \log_2 q}$	$q \leq 25$	$q = 4, 7, 16$
${}^2A_2(q^2), q \geq 3$	$\gcd(3, q+1) \cdot 2f$	q^8	$\frac{q^2}{18 \log_2 q}$	$q \leq 25$	$q = 5, 8$
$B_2(q) \cong C_2(q), q \geq 3$	$2f$	q^{10}	$\frac{q^2}{4 \log_2 q}$	$q \leq 9$	none
$G_2(q), q \geq 3$	$\gcd(2, q-1)f$	q^{14}	$\frac{q^2}{2 \log_2 q}$	$q \leq 5$	none
${}^2B_2(2^{2k+1}), k \geq 1$	$2k+1$	2^{10k+6}	2^{k+1}	$k \leq 2$	$k = 1$
${}^2G_2(3^{2k+1}), k \geq 1$	$2k+1$	3^{14k+8}	3^{k+1}	none	none

- (2) Case: $d \geq 3$. Let $S = {}^tX_d(p^{ft}) = {}^tX_d(q^t)$. We will use the bound $|S| \leq q^{4d^2}$ from the beginning of this subsection. Note also that

$$|\text{Out}(S)| \leq \min\{d+1, q+1\} \cdot 6f,$$

as a simple case-by-case analysis shows that the number of outer diagonal components of automorphisms of S is always at most $\min\{d+1, q+1\}$, while the number of graph-field components is at most $6f$. Using Formula (3.3.1), this implies that

$$\omega(S) \geq \frac{k(S)}{|\text{Out}(S)|} \geq \frac{q^d}{\min\{d+1, q+1\} \cdot |\text{Out}(S)|} \geq \frac{q^d}{\min\{d+1, q+1\}^2 \cdot 6f}$$

$$= q^{d - \log_q(\min\{d+1, q+1\}^2 6f)}, \quad (3.3.7)$$

and so, using also that the function $x \mapsto \frac{\log x}{x}$, assumes its global maximum on $[1, \infty)$ at $x = e$,

$$\begin{aligned} \epsilon_\omega(S) &= \frac{\log \log \omega(S)}{\log \log |S|} \geq \frac{\log \log q^{d - \log_q(\min\{d+1, q+1\}^2 6f)}}{\log \log q^{4d^2}} \\ &= \frac{\log(d - \log_q(\min\{d+1, q+1\}^2 6f)) + \log \log q}{\log(4d^2) + \log \log q} \\ &\geq \frac{\log(d - \frac{2\log(d+1)}{\log q} - \frac{\log 6}{\log q} - \frac{\log f}{f \log p}) + \log f + \log \log p}{\log(4d^2) + \log f + \log \log p} \\ &\geq \frac{\log(d - \frac{2\log(d+1)}{\log q} - \frac{\log 6}{\log q} - \frac{1}{e \log p}) + \log f + \log \log p}{\log(4d^2) + \log f + \log \log p}. \end{aligned} \quad (3.3.8)$$

Note that the smallest value of q that we need to consider is 2 (we can ignore the group ${}^2F_4(2)$, and the Tits group ${}^2F_4(2)'$ is included among the sporadic groups in Subsection 3.1). Let us make a subcase distinction:

(a) Subcase: $q = 2$. Then by Formula (3.3.8),

$$\epsilon_\omega(S) \geq \frac{\log(d - \frac{2\log(d+1)}{\log 2} - \frac{\log 6}{\log 2}) + \log \log 2}{\log(4d^2) + \log \log 2},$$

which is strictly larger than $\epsilon_\omega(\text{Alt}(5))$ for $d \geq 19$.

(b) Subcase: $q > 2$. Then either $p \geq 3$, or $p = 2$ and $f \geq 3/2$, and so then

$$\log f + \log \log p \geq \min\{\log \log 3, \log(3/2) + \log \log 2\} > 0.$$

Hence in view of Formula (3.3.8), if

$$\frac{\log(d - \frac{2\log(d+1)}{\log q} - \frac{\log 6}{\log q} - \frac{1}{e \log 2})}{\log(4d^2)} > \epsilon_\omega(\text{Alt}(5)), \quad (3.3.9)$$

then we also have $\epsilon_\omega(S) > \epsilon_\omega(\text{Alt}(5))$. Conveniently, the left-hand side in Formula (3.3.9) is monotonically increasing in q . Since we are currently assuming that $q > 2$, we actually have $q \geq 2^{3/2}$, and so $\epsilon_\omega(S) > \epsilon_\omega(\text{Alt}(5))$ as long as

$$\frac{\log(d - \frac{2\log(d+1)}{1.5 \log 2} - \frac{\log 6}{1.5 \log 2} - \frac{1}{e \log 2})}{\log(4d^2)} > \epsilon_\omega(\text{Alt}(5)),$$

which holds for $d \geq 12$.

So summarising what we know so far in the case $d \geq 3$, we have $\epsilon_\omega(S) > \epsilon_\omega(\text{Alt}(5))$ for all finite simple groups $S = {}^tX_d(q^t)$ of Lie type of rank $d \geq 19$, and for $d = 11, \dots, 18$, only the case $q = 2$ is open (to include $d = 11$, substitute $q = 3$ instead of $q = \sqrt{8}$ in Formula 3.3.9 above, noting that non-integer values

of q are only relevant for $d = 4$ (and $d = 2$, which is not part of this case)). Similarly, using Formula (3.3.9), we can show for $d = 4, \dots, 10$ that if $q \geq q_0(d)$ with $q_0(d)$ as listed in Table 4 below, then $\epsilon_\omega(S) > \epsilon_\omega(\text{Alt}(5))$.

For $d = 3$, we argue as follows that one may choose $q_0(3) = 10^5$: The number of graph-field automorphisms of any rank 3 finite simple group of Lie type $S = {}^tX_3(q^t)$ is at most $2f$, not just at most $6f$ as in the general case. This allows us to improve our upper bound on $|\text{Out}(S)|$ from the beginning of the considerations for this case to $\min\{d+1, q+1\} \cdot 2f$, and repeating the chain of inequalities in Formula (3.3.8) but with this improved bound, we find that

$$\epsilon_\omega(S) \geq \frac{\log(3 - \frac{2 \log 4}{\log q} - \frac{\log 2}{\log q} - \frac{\log f}{\log q})}{\log 36}.$$

Now, assuming that $q \geq 10^5$, we have $f \geq 10$ or $p \geq \sqrt{10}$, the latter of which implies $p \geq 5$. Hence

$$\frac{\log f}{\log q} = \frac{\log f}{f \log p} \leq \max\left(\frac{\log 10}{10 \log 2}, \frac{1}{e \log 5}\right) = \frac{\log 10}{10 \log 2},$$

and so

$$\epsilon_\omega(S) \geq \frac{\log(3 - \frac{2 \log 4}{\log 10^5} - \frac{\log 2}{\log 10^5} - \frac{\log 10}{10 \log 2})}{\log 36} > \epsilon_\omega(\text{Alt}(5)).$$

This concludes the argument that $q_0(3)$ may be chosen as 10^5 .

Table 4: Lower bounds $q_0(d)$ as described above

d	$q_0(d)$
≥ 19	2
11, ..., 18	3
9, 10	4
8	5
7	7
6	13
5	32
4	373
3	10^5

For dealing with these finitely many remaining groups, the authors proceeded as follows: They wrote a GAP function which computes for each finite simple group of Lie type $S = {}^tX_d(p^{ft})$ a number $\underline{k}(S)$ which is a lower bound on $k(S)$ (in some cases, $\underline{k}(S) = k(S)$). More precisely:

- If S is classical and at least one of the following holds
 - ${}^tX \in \{A, {}^2A, B\}$;

- ${}^tX \in \{D, {}^2D\}$ and S is its own Schur cover;
- $p = 2$;

then set $\underline{k}(S) := k(S)$, to be computed according to [44, Formulas (5.2) and (6.13)] for ${}^tX \in \{A, {}^2A\}$, or [24, Theorems 3.19(1), 3.13(1), 3.16(1,2) and 3.22(1,2)] for ${}^tX \in \{B, C, D, {}^2D\}$.

- If ${}^tX = C$ and $p > 2$, set $\underline{k}(S) := \lceil \frac{k(\text{Sp}_{2d}(q))}{2} \rceil$, to be computed according to [58, Subsection 2.6, Case (B), statement (iii), p. 36].
- If ${}^tX \in \{D, {}^2D\}$, $p > 2$ and the Schur cover $\tilde{S} = \Omega_{2d}^\pm(q)$ of S has nontrivial centre, set $\underline{k}(S) := \lceil \frac{k(\tilde{S})}{2} \rceil$, to be computed according to [24, Theorem 3.18(1)].
- If S is exceptional, then Lübeck’s database [43] provides an exact formula for $k(S)$, and we set $\underline{k}(S) := k(S)$.

The authors then wrote another GAP algorithm, which simply computes

$$\frac{\log \log(\lceil \underline{k}({}^tX_d(q^t)) \rceil / |\text{Out}({}^tX_d(q^t))|)}{\log \log |{}^tX_d(q^t)|},$$

a lower bound on $\epsilon_\omega({}^tX_d(q^t))$, checks whether this numerical value is strictly larger than $\epsilon_\omega(\text{Alt}(5))$, and, if not, adds the group S to a list of exceptions which is output by the algorithm at the end. It turns out that there are only four such exceptions, namely $A_3(5)$, ${}^2A_3(3^2)$, ${}^2A_4(4^2)$ and $D_4(3)$. For each of these four groups S , the value of $\omega(S)$ can be computed exactly with GAP [26], as explained in the argument for “ $d \leq 2$ ” above, and one can thus check that $\epsilon_\omega(S) > \epsilon_\omega(\text{Alt}(5))$ for these four groups S as well, which concludes the proof. \square

Proof of Theorem 1.1.3(5). We use the same conventions with respect to \log and $-\infty$ as described at the beginning of the proof of Theorem 1.1.3(2). By the results of Subsections 3.1 and 3.2, we may assume that $S = {}^tX_d(q^t)$ is of Lie type with $q = p^f$. Let us first show that $\epsilon_q(S) > \epsilon_q(M)$ when S is *exceptional*, i.e., when ${}^tX_d \in \{{}^2B_2, G_2, {}^2G_2, F_4, {}^2F_4, {}^3D_4, E_6, {}^2E_6, E_7, E_8\}$.

Recall that $k_{\text{tor}}(\text{Inndiag}(S))$ denotes the number of conjugacy classes of maximal tori of $\text{Inndiag}(S)$. As noted at the beginning of this subsection, $k_{\text{tor}}(\text{Inndiag}(S))$ does not depend on q , but only on the symbol tX_d , and its values, which we give in the second column of Table 5 below, can be found in the two references [18] and [25], see the third column of Table 5 for more details. The Coxeter numbers $h(X_d)$ are given in the fourth column of Table 5; see [36, Table 2, p. 90] for a reference. We argue as follows:

By the observations from the beginning of this subsection,

$$\begin{aligned} o(S) &= o({}^tX_d(q^t)) \leq o(\text{Inndiag}(S)) \leq k_{\text{tor}}(\text{Inndiag}(S)) \cdot 2(q+1)^{d/2} \cdot (1 + \lceil \log_p(h(X_d)) \rceil) \\ &\leq 2k_{\text{tor}}(\text{Inndiag}(S))(1 + \lceil \log_2(h(X_d)) \rceil) \cdot (q+1)^{d/2} =: \bar{o}(S). \end{aligned}$$

On the other hand, the information in Lübeck’s database [43] allows one to derive a lower bound $\underline{k}(S)$ on the number of conjugacy classes of S , found in the fifth column

of Table 5. Together with the upper bound $\overline{\text{Out}}(S) = c(S)f$ on $|\text{Out}(S)|$ from the sixth column in Table 5, one obtains

$$\omega(S) \geq \underline{k}(S)/|\text{Out}(S)| \geq \underline{k}(S)/\overline{\text{Out}}(S).$$

Finally, the well-known formulas for $|S|$ allow one to conclude that $|S| \leq q^{e(S)}$ with $e(S)$ as in the seventh column of Table 5. One thus has

$$\epsilon_q(S) \geq \frac{\log \log (\underline{k}(S)/(\overline{\text{Out}}(S) \cdot \overline{o}(S)))}{\log \log q^{e(S)}} \geq \frac{\log \log (\underline{k}(S)/(c(S)\overline{o}(S) \cdot \log_2(q)))}{\log \log q^{e(S)}},$$

and one can check with elementary calculus that this lower bound on $\epsilon_q(S)$ is strictly larger than $\epsilon_q(M)$ unless q is from an explicit finite set specified in the eighth column of Table 5. Below Table 5, we explain how to deal with those finitely many remaining cases.

Table 5: Rough treatment of exceptional groups.

tX_d	k_{tor}	k_{tor} ref.	$h(X_d)$	$\underline{k}(S)$	$\overline{\text{Out}}$	$e(S)$	remaining q
2B_2	3	[25, Prop. 7.3]	4	$q^2 = 2^{2m+1}$	$2f = 2m + 1$	10	$2^{3/2}, \dots, 2^{21/2}$
G_2	6	[25, §5.2]	6	q^2	$2f$	14	all $q < 6947$
2G_2	4	[25, Prop. 7.4]	6	$q^2 = 3^{2m+1}$	$2f = 2m + 1$	14	$3^{3/2}, \dots, 3^{17/2}$
F_4	25	[25, §5.3]	12	q^4	$2f$	52	all $q < 157$
2F_4	11	[25, Prop. 7.5]	12	q^4	$2f = 2m + 1$	52	$2^{3/2}, \dots, 2^{13/2}$
3D_4	7	[25, Prop. 7.41]	6	q^4	$3f$	29	all $q < 79$
E_6	25	[18]	12	$q^6/3$	$6f$	78	all $q < 59$
2E_6	25	[18]	12	$q^6/3$	$6f$	78	all $q < 59$
E_7	60	[18]	18	$q^7/2$	$2f$	133	all $q < 29$
E_8	112	[18]	30	q^8	f	248	all $q < 16$

Let us now discuss how to handle the finitely many remaining exceptional Lie type groups. Table 6 gives an overview of references with information that allows one to compute the exact number $o_{\text{ss}}(\text{Inndiag}(S))$ of semisimple element orders in $\text{Inndiag}(S)$, as well as $o(S)$ (except for $o(E_8(q))$).

More precisely, the second column of Table 6 gives a reference for the complete list of cyclic structures of maximal tori of $\text{Inndiag}(S)$, from which the exponents, and thus the sets of element orders, of the maximal tori of $\text{Inndiag}(S)$ can be computed. Since every semisimple element of $\text{Inndiag}(S)$ lies in some maximal torus, this is enough to compute $o_{\text{ss}}(\text{Inndiag}(S))$.

Moreover, for all exceptional finite simple Lie type groups S except for $E_8(q)$, there is a result in the literature specifying a subset $\nu(S)$ of $\text{Ord}(S)$ such that $\text{Ord}(S)$ is the closure of $\nu(S)$ under taking divisors. These references are given in the third column of Table 6.

Now, in those cases where $o(S)$ can be computed exactly (i.e., for all exceptional S apart from the groups $E_8(q)$), go through the finitely many remaining values of q from the last column in Table 5, set $k_0(S) := k(\text{Inndiag}(S))/|\text{Outdiag}(S)|$ (the precise values of $k(\text{Inndiag}(S))$ in the various cases can be read off from Lübeck's database [43]) and $\underline{\omega}(S) := \lceil k_0(S)/|\text{Out}(S)| \rceil$, and check whether the following lower bound on $\epsilon_q(S)$ is greater than $\epsilon_q(\mathbb{M})$:

$$\frac{\log \log (\underline{\omega}(S)/o(S) + 3)}{\log \log |S|}.$$

For $S = E_8(q)$, define $\underline{\omega}(S)$ as for the other exceptional groups, but additionally, set $\bar{o}(S) := o_{\text{ss}}(\text{Inndiag}(S)) \cdot (1 + \lceil \log_p(30) \rceil)$, and check whether the following lower bound on $\epsilon_q(S)$ is greater than $\epsilon_q(\mathbb{M})$:

$$\frac{\log \log (\underline{\omega}(S)/\bar{o}(S) + 3)}{\log \log |S|}.$$

Only very few cases resist even these refined checks, and they are listed in the last column of Table 6 and will be discussed further below.

Table 6: Refined treatment of exceptional groups.

${}^t X_d$	ref. for cyclic structure	ref. for $\nu(S)$	remaining q
${}^2 B_2$	[25, Prop. 7.3]	[53, Theorem 2]	$2^{3/2}$
G_2	[25, §5.2, Table 5.1]	[57, Lemma 1.4]	none
${}^2 G_2$	[25, Prop. 7.4]	[5, Lemma 4]	$3^{3/2}$
F_4	[25, §5.3, Table 5.2]	[30, Theorem 3.1]	none
${}^2 F_4$	[25, §7.4, Table 7.3]	[17, Lemma 3]	$2^{3/2}$
${}^3 D_4$	[25, §7.5, Table 7.5]	[30, Theorem 3.2]	2
E_6	[18]	[7, Theorem 1]	none
${}^2 E_6$	[18]	[7, Theorem 1]	2
E_7	[18]	[8, Theorem 2]	none
E_8	[18]	no ref.	none

We now discuss the remaining five exceptional Lie type groups S specified by the last column in Table 6.

- Note that by the definition of ϵ_q , for every nonabelian finite simple group S , $\epsilon_q(S) \geq \frac{\log \log 4}{\log \log |S|}$. For $S = {}^2 B_2(8)$, this trivial lower bound is actually larger than $\epsilon_q(\mathbb{M})$.
- For $S = {}^2 G_2(27)$: By [5, Lemma 4], we have $o(S) = 11$, and in order to conclude that $\epsilon_q(S) > \epsilon_q(\mathbb{M})$, it is enough to know that $\omega(S) \geq 13$, which we will show now. Let \mathcal{C} be the set of conjugacy classes of S , and let \mathcal{M} be the multiset of positive integers obtained by replacing each class $C \in \mathcal{C}$ by the common order

(in S) of the elements of C . Then the elements of \mathcal{M} are just the element orders in S , and the multiplicity in \mathcal{M} of each element order o in S is just $k_o(S)$, the number of S -conjugacy classes of order o elements in S . From the page on ${}^2G_2(27)$ in the ATLAS of Finite Group Representations [1], one can read off that \mathcal{M} is the following multiset (where the notation x_n is shorthand for n copies of x):

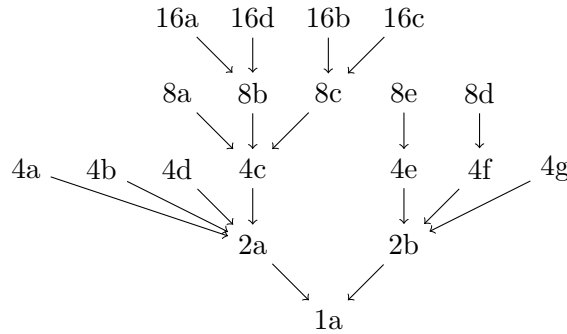
$$\mathcal{M} = \{1_1, 2_1, 3_3, 6_2, 7_1, 9_3, 13_6, 14_3, 19_3, 26_6, 37_6\}.$$

Since $|\text{Out}(S)| = 3$, each orbit of the natural action of $\text{Aut}(S)$ on \mathcal{C} is of length 1 or 3, and so, writing $k_o(S) = 3 \cdot q_o + r_o$ with $r_o \in \{0, 1, 2\}$, we find that $\omega_o(S) \geq q_o + r_o$ and

$$\omega(S) = \sum_{o \in \text{Ord}(S)} \omega_o(S) \geq \sum_{o \in \text{Ord}(S)} (q_o + r_o) = 15 > 13,$$

as required.

- For $S = {}^2F_4(8)$: By [17, Lemma 3], we have $o(S) = 28$. In order to conclude that $\epsilon_q(S) > \epsilon_q(\mathcal{M})$, it is sufficient to show that $\omega(S) \geq 52$, which we will do now, based on the extended character table of S available in GAP [26]. There are 19 unipotent conjugacy classes in S . The following is a drawing of the finite digraph whose vertices are these 19 unipotent conjugacy classes and which has an edge $c_1 \rightarrow c_2$ if and only if the elements in c_1 square to elements in c_2 :



Noting that $|\text{Out}(S)| = 3$, one can use this graph to argue that distinct conjugacy classes of elements of S whose order lies in $\{1, 2, 8, 16\}$ span distinct $\text{Aut}(S)$ -orbits, and that no two of the conjugacy classes $4a, 4c, 4e, 4f, 4g$ span the same $\text{Aut}(S)$ -orbit. It follows that the number of $\text{Aut}(S)$ -orbits consisting of unipotent elements is at least 17. Now, for each non-unipotent element order $o \in \text{Ord}(S)$, write the number of conjugacy classes of order o elements in S as $3 \cdot q_o + r_o$ with $q_o \in \mathbb{N}$ and $r_o \in \{0, 1, 2\}$. Then, as for $S = {}^2G_2(27)$ above, since $|\text{Out}(S)| = 3$, $\omega_o(S) \geq q_o + r_o$. Denoting by $\text{Ord}'(S)$ the set of non-unipotent element orders in S , it follows that

$$\omega(S) \geq 17 + \sum_{o \in \text{Ord}'(S)} (q_o + r_o) = 53 > 52,$$

as asserted.

- For $S = {}^3D_4(8)$: By [30, Theorem 3.2], $o(S) = 14$, and in order to deduce that $\epsilon_q(S) > \epsilon_q(M)$, it is enough to know that $\omega(S) \geq 15$, i.e., that S is not an AT-group. But this is clear by Zhang's characterisation of AT-groups [61, Theorem 3.1]. Alternatively, one can use the extended character table of S available in GAP [26] together with the fact that $|\text{Out}(S)| = 3$ to conclude (as for ${}^2G_2(27)$) that

$$\omega(S) \geq \sum_{o \in \text{Ord}(S)} (q_o + r_o) = 19 > 15.$$

- For $S = {}^2E_6(2^2)$: By [7, Theorem 1], $o(S) = 27$, and in order to get that $\epsilon_q(S) > \epsilon_q(M)$, it is enough to know that $\omega(S) \geq 48$. Using the extended character table of S available in GAP [26] together with the fact that $|\text{Out}(S)| = 3$, we conclude (as for ${}^2G_2(27)$) that

$$\omega(S) \geq \sum_{o \in \text{Ord}(S)} (q_o + r_o) = 66 > 48.$$

This concludes our discussion of exceptional S , and we may assume from now on that $S = {}^tX_d(q^t)$ is a classical finite simple group of Lie type. Note that by [36, Table 2, p. 90], the Coxeter number $h(X_d)$ is at most $2d$. Moreover, recall the notation $k_{\text{tor}}(\text{Inndiag}(S))$ for the number of conjugacy classes of maximal tori in the inner diagonal automorphism group of S . We proceed in several steps, showing successively stronger statements:

- (1) $\epsilon_q(S) > \epsilon_q(M)$ if $d \geq 1012$, or $q \geq 3$ and $d \geq 180$. By [12, Section 3], [20, pp. 437f.] and the fact that the function $x \mapsto \sqrt{x} + \sqrt{d-x}$, has maximum value $\sqrt{2d}$ on the domain $[0, d]$, we have the following, where $p(k)$ denotes the number of ordered integer partitions of $k \in \mathbb{N}$:

- If ${}^tX \in \{A, {}^2A\}$, then $k_{\text{tor}}(\text{Inndiag}(S)) = p(d+1) \leq \exp(\frac{2\pi}{\sqrt{6}}\sqrt{d+1})$.
- If ${}^tX \in \{B, C, D, {}^2D\}$, then

$$\begin{aligned} k_{\text{tor}}(\text{Inndiag}(S)) &= \sum_{i=0}^d p(i)p(d-i) \leq \sum_{i=0}^d \exp(\frac{2\pi}{\sqrt{6}}(\sqrt{i} + \sqrt{d-i})) \\ &\leq (d+1) \exp(\frac{2\pi}{\sqrt{3}}\sqrt{d}). \end{aligned}$$

Set

$$g_1(d) := (d+1) \exp(\frac{2\pi}{\sqrt{3}}\sqrt{d})$$

and $h_1(d, q) := 2(q+1)^{d/2}$. Then by the observations from the beginning of this subsection (see Formula (3.3.3)) and letting T range over the maximal tori in $\text{Inndiag}(S)$,

$$\begin{aligned} o(S) &\leq k_{\text{tor}}(\text{Inndiag}(S)) \cdot \max_T o(T) \cdot (1 + \lceil \log_p(h(X_d)) \rceil) \\ &\leq g_1(d) \cdot h_1(d, q) \cdot (1 + \lceil \log_p(2d) \rceil). \end{aligned}$$

On the other hand, analogously to Formula (3.3.7) from the proof of Theorem 1.1.3(2), we have

$$\omega(S) \geq q^{d - \log_q(\min\{d+1, q+1\}^2 \cdot 2f)},$$

since we can use $2f$ instead of $6f$ in the exponent because the number of graph-field automorphisms of S is at most $2f$ (as $6f$ only occurs when $d = 4$). Combining these bounds on $o(S)$ and $\omega(S)$, we get that

$$\begin{aligned} \mathfrak{q}(S) &\geq q^{d - \log_q(\min\{d+1, q+1\}^2 \cdot 2f \cdot (1 + \lceil \log_p(2d) \rceil) \cdot (d+1) \exp(2\pi\sqrt{d/3}) \cdot 2(q+1)^{d/2})} \\ &\geq q^{(1 - \frac{\log(q+1)}{2\log q})d - \frac{\frac{2\pi}{\sqrt{3}}\sqrt{d} + 3\log(d+1) + \log(2 + \frac{\log(2d)}{\log 2}) + \log 4}{\log q} - \frac{\log f}{\log q}}. \end{aligned} \quad (3.3.10)$$

In view of $|S| \leq q^{4d^2}$, this implies that

$$\epsilon_q(S) \geq \frac{\log\left(\left(1 - \frac{\log(q+1)}{2\log q}\right)d - \frac{\frac{2\pi}{\sqrt{3}}\sqrt{d} + 3\log(d+1) + \log(2 + \frac{\log(2d)}{\log 2}) + \log 4}{\log q} - \frac{\log f}{\log q}\right) + \log \log q}{\log(4d^2) + \log \log q}. \quad (3.3.11)$$

For $q = 2$, the lower bound in Formula (3.3.11) becomes

$$\frac{\log\left(\left(1 - \frac{\log 3}{\log 4}\right)d - \frac{\frac{2\pi}{\sqrt{3}}\sqrt{d} + 3\log(d+1) + \log(2 + \frac{\log 2d}{\log 2}) + \log 4}{\log 2}\right) + \log \log 2}{\log(4d^2) + \log \log 2},$$

which is indeed larger than $\epsilon_q(M)$ if $d \geq 1012$. So we may henceforth assume that $q \geq 3$; in particular, $\log \log q > 0$. Moreover,

$$\frac{\log f}{\log q} = \frac{\log f}{f \log p} \leq \frac{1}{e \log 2}$$

since the function $x \mapsto \frac{\log x}{x}$, assumes its maximum on $(0, \infty)$ at $x = e$. Combining this with Formula (3.3.11), we conclude that

$$\begin{aligned} \epsilon_q(S) &\geq \frac{\log\left(\left(1 - \frac{\log(q+1)}{2\log q}\right)d - \frac{\frac{2\pi}{\sqrt{3}}\sqrt{d} + 3\log(d+1) + \log(2 + \frac{\log(2d)}{\log 2}) + \log 4}{\log q} - \frac{\log f}{\log q}\right)}{\log(4d^2)} \\ &\geq \frac{\log\left(\left(1 - \frac{\log 4}{\log 9}\right)d - \frac{\frac{2\pi}{\sqrt{3}}\sqrt{d} + 3\log(d+1) + \log(2 + \frac{\log(2d)}{\log 2}) + \log 4}{\log 3} - \frac{1}{e \log 2}\right)}{\log(4d^2)}, \end{aligned}$$

which is larger than $\epsilon_q(M)$ if $d \geq 180$, as required.

- (2) $\epsilon_q(S) > \epsilon_q(M)$ if $d \geq 91$, or $q \geq 3$ and $d \geq 54$. We will use the main results of [9], which provide information on the cyclic structure of maximal tori of S (not just $\text{Inndiag}(S)$). We need two new terminologies:

- Call a set $M \subseteq \{1, \dots, (q+1)^d\}$ *sufficient* if and only if for every maximal torus T of $\text{Inndiag}(S)$, there is an $o \in M$ such that the group exponent $\text{Exp}(T \cap S)$ divides o . For every sufficient set M of positive integers, the set of semisimple element orders in S is just the union of the sets of divisors of the $o \in M$.

- If λ is an ordered integer partition, say $\lambda \vdash n$, then we denote by $\bar{\lambda}$ the unique ordered integer partition such that
 - (a) $\bar{\lambda} \vdash n$;
 - (b) for each positive integer $k > 1$, we have that k is a part of $\bar{\lambda}$ if and only if it is a part of λ ; and
 - (c) each positive integer $k > 1$ occurs with multiplicity at most 1 in $\bar{\lambda}$.
 For example, $\overline{(4, 3, 3, 2, 2, 2, 1)} = (4, 3, 2, 1, 1, 1, 1, 1, 1, 1)$. An ordered integer partition λ will be called *reduced* if and only if $\lambda = \bar{\lambda}$.

We noted earlier that the number of semisimple element orders of S can be bounded from above by the product of

- the number $k_{\text{tor}}(\text{Inndiag}(S))$ of conjugacy classes of maximal tori of $\text{Inndiag}(S)$ with
- the maximum number of divisors of a given positive integer between 1 and $(q+1)^d$.

However, in such a count, many conjugacy classes C of maximal tori are usually redundant in the sense that there are lots of other conjugacy classes C' such that the exponent of an element of C' is a multiple of the exponent of an element of C . It is therefore more efficient to replace $k_{\text{tor}}(\text{Inndiag}(S))$ by a sufficiently good upper bound on the size of a sufficient set of positive integers for S . Hence our goal is to find a “small” sufficient set $M(S)$ of positive integers (and an upper bound on $|M(S)|$). The notion of a reduced partition as well as the results of [9] will help us achieve this goal. More precisely:

- Assume first that $S = {}^tA_d(q^t)$ for some $t \in \{1, 2\}$. In the notation of [9], $S = \text{PSL}_{d+1}^\epsilon(q)$ for some $\epsilon \in \{+, -\}$. Then the conjugacy classes of maximal tori of S are in bijection with ordered integer partitions $\lambda \vdash d+1$. Denote by T_λ any fixed maximal torus of $\text{Inndiag}(S)$ whose conjugacy class corresponds to λ . As we will now explain, the results [9, Theorems 2.1 and 2.2] allow us to determine $\text{Exp}(T_\lambda \cap S)$ in terms of $\lambda = (n_1, \dots, n_t)$ (where $n_1 \geq n_2 \geq \dots \geq n_t$). One can check that the cyclic decompositions $a_1 \times \dots \times a_t$ of $T_\lambda \cap S$ given in [9, Theorems 2.1 and 2.2] are canonical in the sense that $a_t \mid a_{t-1} \mid \dots \mid a_2 \mid a_1$ (note, however, that some of the later a_i may be 1). It follows that the exponent of $T_\lambda \cap S$ is always the order of the first (i.e., left-most) cyclic direct factor in the decomposition from [9, Theorems 2.1 and 2.2]. Hence, setting

$$d_1(\lambda) := d_1^\epsilon(\lambda, q) := \text{lcm}(q^{n_1} - (\epsilon 1)^{n_1}, \dots, q^{n_t} - (\epsilon 1)^{n_t}),$$

we have the following:

- If $t > 2$, then $\text{Exp}(T_\lambda \cap S) = d_1(\lambda)$.
- If $t = 2$, then $\text{Exp}(T_\lambda \cap S) = \frac{d_1(\lambda)}{\text{gcd}((d+1)/\text{gcd}(n_1, n_2), q-\epsilon 1)}$.
- If $t = 1$, then $\text{Exp}(T_\lambda \cap S) = \frac{d_1(\lambda)}{\text{gcd}(d+1, q-\epsilon 1)(q-\epsilon 1)} = \frac{q^{d+1} - (\epsilon 1)^{d+1}}{\text{gcd}(d+1, q-\epsilon 1)(q-\epsilon 1)}$.

From this, it is immediate that $\text{Exp}(T_\lambda \cap S)$ divides $\text{Exp}(T_{\bar{\lambda}} \cap S)$. Therefore, the set of all positive integers of the form $d_1^\epsilon(\lambda, q)$ where λ is a *reduced*

partition of $d+1$ is a sufficient set of positive integers for $S = \text{PSL}_{d+1}^\epsilon(q)$; we define $M(S)$ to be this set. The number of reduced partitions of $d+1$, and thus the cardinality of $M(S)$, is at most $\sum_{i=0}^{d+1} s(i)$ where, as in Subsection 3.2, $s(i)$ denotes the number of partitions of i into pairwise distinct parts.

- Now assume that S is orthogonal or symplectic. Then the conjugacy classes of maximal tori of $\text{Inndiag}(S)$ are in bijection with (certain, depending on the case) conjugacy classes of signed permutations of $\{\pm 1, \dots, \pm d\}$, and hence they are in bijection with (certain) ordered pairs $\lambda = (\lambda_+, \lambda_-)$ of ordered integer partitions (corresponding to the multisets of lengths of positive, respectively negative, cycles) such that if $\lambda_+ \vdash d_+$ and $\lambda_- \vdash d_-$, then $d_+ + d_- = d$. For each such pair $\lambda = (\lambda_+, \lambda_-)$, write $\lambda_\epsilon = (n_{1^\epsilon}, \dots, n_{t_\epsilon}^\epsilon)$ for $\epsilon \in \{+, -\}$, and set

$$d_1(\lambda) := \begin{cases} \text{lcm}(\{q^{n_{i_+}^+} - 1, q^{n_{i_-}^-} + 1 \mid i_\epsilon = 1, \dots, t_\epsilon\}), & \text{if } t_+ + t_- > 1 \text{ or } p = 2, \\ \frac{1}{2} \text{lcm}(\{q^{n_{i_+}^+} - 1, q^{n_{i_-}^-} + 1 \mid i_\epsilon = 1, \dots, t_\epsilon\}), & \text{if } t_+ + t_- = 1 \text{ and } p > 2. \end{cases}$$

Moreover, set $\bar{\lambda} := (\bar{\lambda}_+, \bar{\lambda}_-)$. Then $d_1(\lambda) \mid d_1(\bar{\lambda})$. Moreover, every pair λ corresponds to a conjugacy class C_λ of maximal tori of $\text{Inndiag}(C_d(q))$, and by [9, Theorem 3], $d_1(\lambda)$ is the exponent of any torus in C_λ , whence $d_1(\lambda) \leq (q+1)^d$. Finally, by [9, Theorems 3–7], for each $S = {}^tX_d(q^t)$ with $X \in \{B, C, D\}$, if λ corresponds to a conjugacy class C_λ of maximal tori of $\text{Inndiag}(S)$, then the exponent of any representative of C_λ divides $d_1(\lambda)$. Combining these facts, it follows that for any symplectic or orthogonal group $S = {}^tX_d(q^t)$, the set $M(S)$ of all numbers of the form $d_1(\lambda)$ such that both entries of λ are reduced partitions is sufficient, and

$$|M(S)| \leq \sum_{d_+ + d_- = d} \left(\sum_{i_+ = 0}^{d_+} \sum_{i_- = 0}^{d_-} s(i_+)s(i_-) \right),$$

where, again, $s(i)$ denotes the number of ordered integer partitions of i with pairwise distinct parts.

It is not difficult to check that for each $d \geq 1$,

$$\sum_{i=0}^{d+1} s(i) \leq \sum_{d_+ + d_- = d} \left(\sum_{i_+ = 0}^{d_+} \sum_{i_- = 0}^{d_-} s(i_+)s(i_-) \right) =: g_2(d),$$

and hence every classical finite simple group of Lie type S of untwisted rank d admits a sufficient set $M(S)$ of positive integers of size at most $g_2(d)$.

It will also be necessary to use sharper upper bounds on

$$\max\{\tau(1), \dots, \tau((q+1)^d)\},$$

where $\tau(n)$ denotes the number of (positive) divisors of n , exploiting that by assumption, $(q+1)^d$ is “large”. Assume first that $d \geq 91$ (and $q = 2$). Then

$$(q+1)^{0.311 \cdot d} = 3^{0.311 \cdot d} \geq 3^{0.311 \cdot 91} \geq \exp(\exp(0.311^{-1} \cdot 1.538 \cdot \log 2)),$$

which (by taking logarithms twice) is equivalent to

$$\frac{1.538 \log 2}{\log \log (q+1)^{0.311 \cdot d}} \leq 0.311.$$

Hence by [47, Théorème 1], for every positive integer $k \geq (q+1)^{0.311 \cdot d}$, we have $\tau(k) \leq k^{0.311}$. We claim that this implies that

$$\max\{\tau(1), \dots, \tau((q+1)^d)\} \leq (q+1)^{0.311d}.$$

Indeed, let k be a positive integer with $1 \leq k \leq (q+1)^d$. If $k \geq (q+1)^{0.311 \cdot d}$, then by the above, $\tau(k) \leq k^{0.311} \leq (q+1)^{0.311 \cdot d}$. And if $k < (q+1)^{0.311 \cdot d}$, then $\tau(k) \leq k < (q+1)^{0.311 \cdot d}$.

Now, following the argument from the case (1) and replacing $\min\{d+1, q+1\}$ in Formula (3.3.10) by $q+1 = 3$ instead of $d+1$, we obtain that

$$\epsilon_q(S) \geq \frac{\log\left(\left(1 - 0.311 \cdot \frac{\log 3}{\log 2}\right)d - \frac{\log g_2(d) + 2 \log 3 + \log\left(2 + \frac{\log(2d)}{\log 2}\right) + \log 2}{\log 2}\right) + \log \log 2}{\log(4d^2) + \log \log 2},$$

and one can check this lower bound to be greater than $\epsilon_q(M)$ for $d = 91, \dots, 1011$ (we use the table of values of $s(k)$ from [48] to compute $g_2(d)$). This concludes the discussion of this case for $q = 2$, so we may henceforth assume that $q \geq 3$ and $d \in \{54, \dots, 179\}$. Then we repeat the argument for $q = 2$ with $\frac{1}{3}$ instead of 0.311, obtaining that

$$\epsilon_q(S) \geq \frac{\log\left(\left(1 - \frac{\log 4}{\log 27}\right)d - \frac{\log g_2(d) + 2 \log(d+1) + \log\left(2 + \frac{\log(2d)}{\log 2}\right) + \log 2}{\log 3} - \frac{1}{e \log 2}\right)}{\log(4d^2)},$$

which can also be checked to be larger than $\epsilon_q(M)$ for each $d \in \{54, \dots, 179\}$.

- (3) $\epsilon_q(S) > \epsilon_q(M)$ if $d \geq 54$. Compared to the previous case, the only groups S additionally included here are those where $q = 2$ and $d \in \{54, \dots, 90\}$. Observe that the Schur cover of ${}^tX_d(2^t)$ embeds into ${}^tX_{d+1}(2^t)$; for example, $\text{SL}_{d+1}(2)$ embeds into $\text{PSL}_{d+2}(2)$ via

$$M \mapsto \overline{\begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}},$$

and similar arguments work for the other types of classical groups. In particular,

$$o_{\text{ss}}({}^tX_d(2^t)) \leq o_{\text{ss}}({}^tX_{d+1}(2^t)). \tag{3.3.12}$$

Now let $S = {}^tX_d(2^t)$ with $d \in \{54, \dots, 90\}$. Then by Formula (3.3.12),

$$o(S) \leq o_{\text{ss}}(S) \cdot (1 + \lceil \log_2(h(X_d)) \rceil) \leq o_{\text{ss}}({}^tX_{90}(2^t)) \cdot (1 + \lceil \log_2(h(X_d)) \rceil). \tag{3.3.13}$$

Define $o_0(S)$ to be the upper bound on $o(S)$ from Formula (3.3.13). In order to make use of it, one needs upper bounds on $o_{\text{ss}}({}^tX_{90}(2^t))$ for each of the six Lie classes of finite simple classical groups. The authors computed such bounds using GAP [26]; let us briefly explain how this was done.

Consider the following case-dependent notion of an admissible partition or partition pair:

- For ${}^tX \in \{A, {}^2A\}$, a partition λ is called tX -admissible if and only if λ is reduced.
- For ${}^tX \in \{B, C\}$, a partition pair $\boldsymbol{\lambda} = (\lambda_+, \lambda_-)$ is called tX -admissible if and only if both entries of $\boldsymbol{\lambda}$ are reduced.
- For $t \in \{1, 2\}$, a partition pair $\boldsymbol{\lambda} = (\lambda_+, \lambda_-)$ is called tD -admissible if and only if λ_+ is reduced, the number of parts of λ_- is congruent to $t + 1$ modulo 2, and λ_- is “almost reduced” in the sense that if some positive integer $k > 1$ occurs $m > 1$ times as a part of λ_- , then $(k, m) = (2, 2)$.

Then every admissible partition or partition pair with the “right” sum of parts corresponds to a conjugacy class of maximal tori of $\text{Inndiag}(S)$, and for every maximal torus T_1 of $\text{Inndiag}(S)$, there is an admissible partition or partition pair with corresponding maximal torus T_2 such that $\text{Exp}(T_1 \cap S)$ divides $\text{Exp}(T_2 \cap S)$. Therefore, $\text{o}_{\text{ss}}(S)$ is bounded from above by the sum of the numbers of divisors of the exponents of the groups $T \cap S$ where T ranges over a set of representatives for the conjugacy classes of maximal tori of $\text{Inndiag}(S)$ corresponding to admissible partitions or partition pairs. It is this sum which we computed for each of the five (taking $B_{90}(2) \cong C_{90}(2)$ into account) rank 90 classical groups using GAP, and we list the computed values in the following table:

Table 7: Upper bounds for rank 90 groups.

tX	upper bound on $\text{o}_{\text{ss}}({}^tX_{90}(2^t))$
A	4235078858
2A	3178257722
B, C	22293229392
D	15931588348
2D	12297818620

Observe that by [24, Theorem 1.1(1)], we have

$$k(S) \geq \frac{k(\text{Inndiag}(S))}{|\text{Inndiag}(S) : S|} \geq \frac{2^d}{|\text{Inndiag}(S) : S|} = \begin{cases} 2^d, & \text{if } {}^tX \neq {}^2A, \\ \frac{2^d}{\gcd(3, d+1)}, & \text{if } {}^tX = {}^2A. \end{cases} \quad (3.3.14)$$

Set $\omega_0(S) := \lceil k_0(S) / |\text{Out}(S)| \rceil$ where $k_0(S)$ is the lower bound on $k(S)$ from Formula (3.3.14). Then one can check that

$$\epsilon_q(S) \geq \frac{\log \log (\omega_0(S) / \text{o}_0(S) + 3)}{\log \log |S|} > \epsilon_q(\mathbb{M}),$$

as required.

- (4) $\epsilon_q(S) > \epsilon_q(\mathbb{M})$ for all classical finite simple groups of Lie type S except possibly those from an explicit, finite list (given below). Note that by case (3), we only need to consider classical groups S of untwisted Lie rank at most 53. The goal

is to explicitly determine, for each $d = 1, \dots, 53$, a prime power $q_0(d)$ such that for all prime powers $q \geq q_0(d)$, we have $\epsilon_q({}^t X_d(q^t)) > \epsilon_q(M)$, and then use a computer to sort out most of the remaining finitely many groups in order to arrive at a short, explicit list of potential exceptions that will need to be checked with more careful methods.

Let us start with $d = 1$, which is discussed separately because the method used for $d \geq 2$ would produce too large a value for $q_0(1)$. So we need to consider $S = A_1(q) = \text{PSL}_2(q)$. By [44, Table 4, p. 43],

$$k(\text{PSL}_2(q)) = \begin{cases} q+1, & \text{if } 2 \mid q, \\ \frac{q+5}{2}, & \text{if } 2 \nmid q, \end{cases}$$

and so in any case, $k(\text{PSL}_2(q)) \geq \frac{q+1}{2}$. Moreover,

$$|\text{Out}(\text{PSL}_2(q))| = \gcd(2, q-1) \cdot f,$$

so that

$$\omega(\text{PSL}_2(q)) \geq \frac{q+1}{4f} \geq \frac{q+1}{4 \log_2(q)}.$$

Finally, by [9, Theorem 2.1], the maximal tori of $\text{PSL}_2(q)$ are cyclic of orders $\frac{q \pm 1}{\gcd(2, q-1)}$, and since

$$\left\{ \overline{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}} \mid a \in \mathbb{F}_q \right\}$$

is a Sylow p -subgroup of $\text{PSL}_2(q)$ which is of exponent p and equal to the centraliser in $\text{PSL}_2(q)$ of any of its nontrivial elements, the only non-semisimple element order in $\text{PSL}_2(q)$ is p . It follows that $\text{Ord}(\text{PSL}_2(q))$ is just the set of positive integers dividing at least one of the numbers $\frac{q+1}{2}$, $\frac{q-1}{2}$ or p , so that

$$o(\text{PSL}_2(q)) \leq 2 + 2\sqrt{\frac{q+1}{2}} - 1 + 2\sqrt{\frac{q-1}{2}} - 1 = 2\left(\sqrt{\frac{q+1}{2}} + \sqrt{\frac{q-1}{2}}\right).$$

It follows that

$$\epsilon_q(\text{PSL}_2(q)) \geq \frac{\log \log \left(\frac{q+1}{8 \log_2(q) \cdot (\sqrt{(q+1)/2} + \sqrt{(q-1)/2})} \right)}{\log \log (q(q^2 - 1))},$$

which can be checked to be larger than $\epsilon_q(M)$ for $q \geq 1100543 =: q_0(1)$, as recorded in Table 8.

Let us now discuss how to handle $d = 2, \dots, 53$. Set

$$c := c(d) := \begin{cases} 2, & \text{if } d \neq 4, \\ 6, & \text{if } d = 4. \end{cases}$$

Then

$$\omega(S) \geq \frac{q^d}{\min\{d+1, q+1\}^2 \cdot cf} \geq \frac{q^d}{c \log_2(q) \cdot \min\{d+1, q+1\}^2}$$

and

$$o(S) \leq g_2(d) \cdot 2(q+1)^{d/2} \cdot (1 + \lceil \log_2(2d) \rceil).$$

It follows that

$$\epsilon_q(S) \geq \frac{\log \log \frac{q^d}{2c \cdot \log_2(q) \cdot \min\{d+1, q+1\}^2 \cdot g_2(d) (1 + \lceil \log_2(2d) \rceil) \cdot (q+1)^{d/2}}}{\log \log q^{4d^2}},$$

which can be checked to be greater than $\epsilon_q(M)$ for all $q \geq q_0(d)$ with $q_0(d)$ as in the following table:

Table 8: Values of $q_0(d)$.

d	$q_0(d)$	d	$q_0(d)$
1	1100543	13	25
2	62753	14	23
3	4903	15	19
4	1801	16, 17	16
5	401	18	13
6	197	19, 20, 21	11
7	121	22	9
8	79	23, 24, 25	8
9	59	26, ..., 34	7
10	43	35, ..., 45	5
11	37	46, ..., 53	4
12	29		

So, at this point, we are down to an explicit, finite list of potential exceptions S to $\epsilon_q(S) > \epsilon_q(M)$. We can still reduce this list further by checking, for each $S = {}^t X_d(q^t)$ with $d \in \{1, \dots, 53\}$ and $q < q_0(d)$, whether certain sharper lower bounds on $\epsilon_q(S)$ are larger than $\epsilon_q(M)$. More precisely,

- with T ranging over a complete set of representatives of the conjugacy classes of maximal tori of $\text{Inndiag}(S)$ corresponding to an admissible partition or partition pair as defined in the argument for the previous case, (3),
 - observe that $o_{\text{ss}}(S)$ is just the cardinality of the set of positive integers dividing one of the numbers $\text{Exp}(T \cap S)$, and
 - let $\overline{o}_{\text{ss}}(S)$ denote the sum of the numbers $\tau(\text{Exp}(T \cap S))$, where $\tau(k)$ denotes the number of divisors of k .

Then $o_{\text{ss}}(S) \leq \overline{o}_{\text{ss}}(S)$. Moreover, set

$$\overline{o}(S) := o_{\text{ss}}(S) \cdot (1 + \lceil \log_p(h(X_d)) \rceil)$$

and

$$\bar{o}(S) := \overline{o_{\text{ss}}}(S) \cdot (1 + \lceil \log_p(h(X_d)) \rceil).$$

We have $o(S) \leq \bar{o}(S) \leq \overline{o}(S)$.

- consider the following lower bounds $\underline{k}(S)$ and $\underline{\underline{k}}(S)$ on $k(S)$, which satisfy $k(S) \geq \max\{\underline{k}(S), \underline{\underline{k}}(S)\}$:

– Assume that at least one of the following holds:

- * ${}^tX \in \{A, {}^2A, B\}$;
- * ${}^tX \in \{D, {}^2D\}$ and S is its own Schur cover;
- * $p = 2$.

Then set $\underline{k}(S) := k(S)$, to be computed according to [44, Formulas (5.2) and (6.13)] for ${}^tX \in \{A, {}^2A\}$, or [24, Theorems 3.19(1), 3.13(1), 3.16(1,2) and 3.22(1,2)] for ${}^tX \in \{B, C, D, {}^2D\}$.

– If ${}^tX = C$ and $p > 2$, set $\underline{k}(S) := \lceil \frac{k(\text{Sp}_{2d}(q))}{2} \rceil$, to be computed according to [58, Subsection 2.6, Case (B), statement (iii), p. 36].

– If ${}^tX \in \{D, {}^2D\}$, $p > 2$ and the Schur cover $\tilde{S} = \Omega_{2d}^{\pm}(q)$ of S has nontrivial centre, set $\underline{k}(S) := \lceil \frac{k(\tilde{S})}{2} \rceil$, to be computed according to [24, Theorem 3.18(1)].

– Set

$$\underline{\underline{k}}(S) := \begin{cases} \underline{k}(S) = k(S), & \text{if } {}^tX \in \{A, {}^2A\}, \\ \lceil \frac{q^d}{\gcd(2, q-1)} \rceil, & \text{if } {}^tX \in \{B, C\}, \\ \lceil \frac{q^d}{\gcd(2, q-1)^2} \rceil, & \text{if } {}^tX \in \{D, {}^2D\}. \end{cases}$$

The fact that $k(S) \geq \max\{\underline{k}(S), \underline{\underline{k}}(S)\}$ follows from the above definitions and the bound $k(\text{Inndiag}(S)) \geq q^d$, see [24, Theorem 1.1(1)]. Using these lower bounds on $k(S)$, set

$$\underline{\omega}(S) := \lceil \underline{k}(S) / |\text{Out}(S)| \rceil$$

and

$$\underline{\underline{\omega}}(S) := \lceil \underline{\underline{k}}(S) / |\text{Out}(S)| \rceil,$$

so that $\omega(S) \geq \max\{\underline{\omega}(S), \underline{\underline{\omega}}(S)\}$.

Note that, while $\bar{o}(S)$ is a better upper bound on $o(S)$ than $\overline{o}(S)$, it takes longer to compute, and similarly, $\underline{\omega}(S)$ (which seems to be larger than $\underline{\underline{\omega}}(S)$ by empirical evidence) takes longer to compute than $\underline{\underline{\omega}}(S)$. In order to minimise the computation time for our checks, we proceed as follows:

For each pair (d, q) with $d \in \{1, \dots, 53\}$ and q being a prime power less than $q_0(d)$, we go through the finite simple classical Lie type groups $S = {}^tX_d(q^t)$, and, for each of them, we check first whether

$$\frac{\log \log (\underline{\underline{\omega}}(S) / \bar{o}(S) + 3)}{\log \log |S|} > \epsilon_q(M).$$

If this fails, we check if

$$\frac{\log \log (\underline{\omega}(S)/\overline{\omega}(S) + 3)}{\log \log |S|} > \epsilon_q(M),$$

and if this also fails, we check whether

$$\frac{\log \log (\underline{\omega}(S)/\overline{\omega}(S) + 3)}{\log \log |S|} > \epsilon_q(M).$$

If this third check also fails and $d > 1$, we take note of S , progressively building a (hopefully short) list of exceptions that require further inspection. When $d = 1$ (and so $S = A_1(q) = \text{PSL}_2(q)$), we know that $o(S) = o_{\text{ss}}(S) + 1$ and perform one more check, namely whether

$$\frac{\log \log (\underline{\omega}(S)/(o_{\text{ss}}(S) + 1) + 3)}{\log \log |S|} > \epsilon_q(M),$$

and only if S fails this check as well do we add it to the list. We note that the GAP algorithm written by the authors to perform these checks prints a warning several times, stating that the calculations are carried out under the assumption that 37644053098601 is a prime. This, however is not a problem, as one can actually check with GAP's built-in primality testing algorithm that this number is indeed a prime (GAP's primality testing algorithm is deterministic for inputs less than 10^{18} , see [27, Subsection 14.4-2: `IsPrimeInt`]).

It turns out that only the following 68 groups fail each of these refined checks:

- $A_d(q)$ with (d, q) from the set

$$\{(2, 2), (2, 4), (2, 7), (2, 8), (2, 9), (2, 13), (2, 16), (2, 19), (2, 25), (2, 49), (2, 64), (3, 2), (3, 3), (3, 4), (3, 5), (3, 7), (3, 9), (3, 13), (4, 2), (4, 3), (4, 4), (4, 16), (5, 2), (5, 3), (5, 4), (6, 2)\}.$$
- ${}^2A_d(q^2)$ with (d, q) from the set

$$\{(2, 2), (2, 4), (2, 5), (2, 8), (2, 11), (2, 17), (2, 23), (2, 29), (2, 32), (3, 3), (3, 4), (3, 5), (3, 7), (3, 9), (3, 11), (4, 4), (4, 9), (5, 2), (5, 3), (5, 5), (7, 3), (8, 2)\}.$$
- $B_d(q)$ with (d, q) from the set

$$\{(2, 4), (2, 8), (2, 9), (3, 3), (3, 4), (3, 5)\}$$
- None of the groups $C_d(q)$ with $d \geq 3$ except for $C_3(4) \cong B_3(4)$.
- $D_d(q)$ with (d, q) from the set

$$\{(4, 2), (4, 3), (4, 4), (4, 5), (4, 7), (4, 9), (5, 2), (5, 3), (5, 5), (6, 3), (7, 3)\}$$
- ${}^2D_d(q^2)$ with (d, q) from the set

$$\{(4, 2), (4, 3), (5, 3)\}.$$

- (5) $\epsilon_q(S) > \epsilon_q(M)$ for all finite simple classical groups of Lie type S . We need to deal with the 67 remaining groups listed above. The authors implemented simple algorithms in GAP [26] for computing $o(S)$ and $\omega(S)$ (and thus $\epsilon_q(S)$) exactly. These algorithms require one to first compute the set of conjugacy classes of S , for which GAP has the built-in command `ConjugacyClasses`. This allows one to deal with 46 out of the 68 groups, as listed in the following table:

Table 9: Exact computation of $\epsilon_q(S)$.

S	$\omega(S)$	$o(S)$	$\epsilon_q(S) \approx$	S	$\omega(S)$	$o(S)$	$\epsilon_q(S) \approx$
$A_2(2)$	5	5	0.199907	${}^2A_2(2^2)$	4	4	0.224773
$A_2(4)$	6	6	0.142406	${}^2A_2(4^2)$	9	8	0.145146
$A_2(7)$	15	10	0.152856	${}^2A_2(5^2)$	10	9	0.140543
$A_2(8)$	17	10	0.155376	${}^2A_2(8^2)$	10	9	0.126245
$A_2(9)$	32	17	0.160853	${}^2A_2(11^2)$	30	15	0.164402
$A_2(13)$	39	15	0.183387	${}^2A_2(17^2)$	62	21	0.188453
$A_2(16)$	20	12	0.141745	${}^2A_3(3^2)$	14	10	0.145173
$A_2(19)$	75	23	0.19498	${}^2A_3(4^2)$	35	14	0.175921
$A_2(25)$	72	21	0.193765	${}^2A_3(5^2)$	64	21	0.186343
$A_2(49)$	237	31	0.253006	${}^2A_3(7^2)$	76	23	0.18362
$A_3(2)$	12	8	0.177958	${}^2A_4(4^2)$	34	19	0.129955
$A_3(3)$	21	12	0.161363	${}^2A_5(2^2)$	44	18	0.167802
$A_3(4)$	36	16	0.16688	$B_2(2)$	12	9	0.145857
$A_3(5)$	34	16	0.157277	$B_2(8)$	21	14	0.134539
$A_3(7)$	137	30	0.210503	$B_2(9)$	41	16	0.176644
$A_3(9)$	85	26	0.175965	$B_3(3)$	52	16	0.195259
$A_3(13)$	358	36	0.260237	$B_3(4)$	75	22	0.183849
$A_4(2)$	20	13	0.14886	$B_3(5)$	136	27	0.209901
$A_4(3)$	72	24	0.178591	$D_4(2)$	27	12	0.181326
$A_4(4)$	110	32	0.177528	$D_4(3)$	38	16	0.161802
$A_5(2)$	44	18	0.166564	$D_5(2)$	84	24	0.189461
$A_5(4)$	169	40	0.176772	${}^2D_4(2^2)$	39	15	0.1844
$A_6(2)$	77	27	0.163159	${}^2D_4(3^2)$	100	25	0.195833

For $S = D_4(4)$, one can compute the set of conjugacy classes of S with GAP and use this to determine $o(S)$ exactly as well as to provide a certain lower bound on $\omega(S)$. This lower bound, the derivation of which is explained in detail after Table 10, is larger than $\underline{\omega}(S)$ and (unlike $\underline{\omega}(S)$) is sufficient to conclude that $\epsilon_q(S) > \epsilon_q(M)$:

Table 10: A conjugacy class argument.

S	$\omega(S) \geq$	$o(S)$	$\epsilon_q(S) \geq$
$D_4(4)$	51	23	0.143317

Indeed, consider the set \mathcal{C} of conjugacy classes of S . View \mathcal{C} as a multiset, and consider the multiset obtained from it by replacing each element $C \in \mathcal{C}$ by the order of a representative of C . The following is the said multiset (we write x_n shorthand for n copies of x):

$$\{1_1, 2_5, 3_5, 4_6, 5_{19}, 6_{14}, 7_1, 8_2, 9_3, 10_{43}, 12_7, 13_2, 15_{43}, 17_{24}, 20_{18}, 21_8, 30_{42}, 34_{12}, 51_{12}, 63_{18}, 65_{48}, 85_{24}, 255_{48}\}.$$

In particular, $o(S) = 23$, and since $|\text{Out}(S)| = 12$, for each element order o in S , $\omega_o(S)$ is bounded from below by the shortest length of an integer partition of o into divisors of 12. Hence

- $\omega_o(S) \geq 2$ for $o \in \{2, 3, 6, 12, 17, 20, 21, 63, 85\}$,
- $\omega_5(S) \geq 3$,
- $\omega_o(S) \geq 4$ for $o \in \{30, 65, 255\}$, and
- $\omega_o(S) \geq 5$ for $o \in \{10, 15\}$.

It follows that $\omega(S) \geq o(S) + 28 = 51$, as asserted.

In order to deal with the remaining 20 possibilities for S , which are all of Lie type A , 2A , D or 2D (and those of types D or 2D all have odd defining characteristic), it will be useful to have an algorithm for computing an upper bound on $o(S)$, and it is our next goal to describe such an algorithm.

Let $S = {}^tX_d(p^{ft})$. Recall from the beginning of this subsection that by [55, Corollary 0.5], the largest power of p dividing $\text{Exp}(S)$ is $p^{\lceil \log_p(h(X_d)) \rceil}$ where $h(X_d)$ is the Coxeter number of the root system X_d . Recall also from earlier in this proof that we already described and used an algorithm for computing $o_{\text{ss}}(S)$, the number of semisimple element orders in S . This latter algorithm essentially consists of looping over certain conjugacy classes of maximal tori T of $\text{Inndiag}(S)$ and joining the divisor sets $\text{Div}(\text{Exp}(T \cap S))$, based on the formulas in [9]. Now, for $e = 0, \dots, \lceil \log_p(h(X_d)) \rceil$, denote by $o_{p,e}(S)$ the number of element orders o in S such that the largest power of p dividing o is p^e . Hence, $o_{p,0}(S)$ is just $o_{\text{ss}}(S)$, $o_{p,1}(S)$ is the number of element orders in S that are sharply divisible by p , and so on. Our algorithm for computing an upper bound on $o(S)$ proceeds by computing a certain upper bound $\overline{o_{p,e}}(S)$ on $o_{p,e}(S)$ for each $e = 0, \dots, \lceil \log_p(h(X_d)) \rceil$ and then adding those upper bounds.

We set $\overline{o_{p,0}}(S) := o_{\text{ss}}(S)$, to be computed as described above. Hence we assume that $e \geq 1$. The following theoretical results are the basis of our argument:

- (a) Let $S = A_d(q) = \text{PSL}_{d+1}(q)$, and let $o \in \text{Ord}(S)$ with $p^e \parallel o$, for some given $e \in \mathbb{N}^+$ (in particular, $p^{e-1} + 1 \leq h(A_d) = d + 1$). Then:
 - i. There is an element $g \in \text{GL}_{d+1}(q)$ such that $o \mid \text{ord}(g)$ and the following hold:

- the rational canonical form of g has exactly one non-semisimple block, which is of the form $\text{Comp}((X - a)^{p^{e-1}+1})$ for some $a \in \mathbb{F}_q^*$; and
 - the semisimple blocks of the rational canonical form of g form the rational canonical form of a (semisimple) element of $\text{GL}_{d-p^{e-1}}(q)$.
- In particular, $\frac{o}{p^e}$ divides a number of the form $\text{lcm}(q - 1, o')$ for some $o' \in \text{Ord}_{\text{ss}}(\text{GL}_{d-p^{e-1}}(q))$.
- ii. If $p^{e-1} + 1 = d + 1 = h(A_d)$, then $o = p^e$.
 - iii. If $p^{e-1} + 1 = d = h(A_d) - 1$, then $\frac{o}{p^e}$ divides $\frac{q-1}{\text{gcd}(d+1, q-1)}$.
- (b) Let $S = {}^2A_d(q^2) = \text{PSU}_{d+1}(q)$, and let $o \in \text{Ord}(S)$ with $p^e \parallel o$, for some given $e \in \mathbb{N}^+$ (in particular, $p^{e-1} + 1 \leq h(A_d) = d + 1$). Then:
- i. There is an element $g \in \text{GU}_{d+1}(q) \leq \text{GL}_{d+1}(q^2)$ such that $o \mid \text{ord}(g)$ and the following hold:
 - the rational canonical form of g has exactly one non-semisimple block, which is of the form $\text{Comp}((X - a)^{p^{e-1}+1})$ for some $a \in \mathbb{F}_{q^2}^*$ with $\text{ord}(a) \mid q + 1$; and
 - the semisimple blocks of the rational canonical form of g form the rational canonical form of a (semisimple) element of $\text{GU}_{d-p^{e-1}}(q)$.

In particular, $\frac{o}{p^e}$ divides a number of the form $\text{lcm}(q + 1, o')$ for some $o' \in \text{Ord}_{\text{ss}}(\text{GU}_{d-p^{e-1}}(q))$.

 - ii. If $p^{e-1} + 1 = d + 1 = h(A_d)$, then $o = p^e$.
 - iii. If $p^{e-1} + 1 = d = h(A_d) - 1$, then $\frac{o}{p^e}$ divides $\frac{q+1}{\text{gcd}(d+1, q+1)}$.
- (c) Let $S = \text{P}\Omega_{2d}^\epsilon(q)$ with $\epsilon \in \{+, -\}$ and q odd, and let $o \in \text{Ord}(S)$ with $p^e \parallel o$, for some given $e \in \mathbb{N}^+$ (in particular, $p^{e-1} + 1 \leq h(D_d) = 2d - 2$). Then:
- i. There is an element $g \in \text{GO}_{2d}^\epsilon(q)$ such that $o \mid \text{ord}(g)$ and the following hold:
 - the rational canonical form of g has exactly one non-semisimple block, which is of one of the two forms $\text{Comp}((X + 1)^{p^{e-1}+2})$ or $\text{Comp}(P(X)^{p^{e-1}+1})$ for some monic quadratic irreducible polynomial $P(X) \in \mathbb{F}_q[X]$ such that $\text{ord}(P(X)) \mid q + 1$;
 - if the unique non-semisimple block of g is of the form $\text{Comp}((X + 1)^{p^{e-1}+2})$, then the semisimple blocks of the rational canonical form of g form the rational canonical form of a (semisimple) element of $\text{GO}_{2d-p^{e-1}-2}(q)$; and
 - if the unique non-semisimple block of g is of the form $\text{Comp}(P(X)^{p^{e-1}+1})$, then the semisimple blocks of the rational canonical form of g form the rational canonical form of a (semisimple) element of $\text{GO}_{2d-2(p^{e-1}+1)}^\epsilon(q)$.

In particular, $\frac{o}{p^e}$ divides a number of one of the two forms $\text{lcm}(2, o')$ for some $o' \in \text{Ord}_{\text{ss}}(\text{GO}_{2d-p^{e-1}-2}(q))$, or $\text{lcm}(q + 1, o'')$ for some $o'' \in \text{Ord}_{\text{ss}}(\text{GO}_{2d-2(p^{e-1}+1)}^\epsilon(q))$.
- (d) If $p^{e-1} + 1 = 2d - 2 = h(D_d)$, then $o = p^e$.

These results can be deduced from the classification of rational canonical forms of a given finite classical isometry group due to Wall [58, Case (A), p. 34; Case (C), pp. 38f.]. We only exemplarily prove the result for $S = {}^2A_d(q^2) = \text{PSU}_{d+1}(q)$ and leave the remaining two cases as exercises to the inclined reader. Fix an element $s \in S$ with $\text{ord}(s) = o$, and let $\tilde{s} \in \text{SU}_{d+1}(q)$ be a lift of s . By [58, Case (A), p. 34], the rational canonical form of \tilde{s} has the property that its multiset of (Frobenius) blocks is closed under the involutory operation $\text{Comp}(P(X)^k) \mapsto \text{Comp}(\tilde{P}(X)^k)$, where $\tilde{P}(X)$ is the minimal polynomial over \mathbb{F}_{q^2} of ξ^{-q} , for any root $\xi \in \overline{\mathbb{F}_{q^2}}$ of $P(X)$. Since p does not divide the centre order $|\zeta \text{SU}_{d+1}(q)|$, we also have $p^e \parallel \text{ord}(\tilde{s})$, and so all Frobenius blocks $\text{Comp}(P(X)^k)$ of \tilde{s} have the property that $k \leq p^e$, and there is at least one block with $k \geq p^{e-1} + 1$. Choose one copy of a Frobenius block $\text{Comp}(P(X)^k)$ of \tilde{s} for some $P(X)$ with $k \geq p^{e-1} + 1$, mark it, and if $P(X) \neq \tilde{P}(X)$, additionally mark one copy of $\text{Comp}(\tilde{P}(X)^k)$. Now apply the following transformations, in the given order, to the rational canonical form of \tilde{s} :

- Replace each unmarked block $\text{Comp}(Q(X)^\ell)$ by one copy of $\text{Comp}(Q(X))$ and $\deg(Q(X)) \cdot (\ell - 1)$ copies of the trivial block I_1 .
- Replace each of the (at most two) marked blocks $\text{Comp}(R(X)^k)$ by one marked copy of $\text{Comp}(R(X)^{p^{e-1}+1})$ and $\deg R(X) \cdot (k - p^{e-1} - 1)$ unmarked copies of the trivial block I_1 .
- If there are now two distinct marked blocks $\text{Comp}(P(X)^{p^{e-1}+1})$ and $\text{Comp}(\tilde{P}(X)^{p^{e-1}+1})$, then replace them by one unmarked copy of each of $\text{Comp}(P(X))$ and $\text{Comp}(\tilde{P}(X))$, as well as one unmarked copy of $\text{Comp}((X-1)^{p^{e-1}+1})$ and $2 \deg(P(X)) \cdot (p^{e-1} + 1) - 2 \deg(P(X)) - (p^{e-1} + 1)$ unmarked copies of the trivial block I_1 . If, on the other hand, there is exactly one marked block, namely $\text{Comp}(P(X)^{p^{e-1}+1})$, then proceed as follows: If $P(X)$ is linear, just remove the mark and leave the block itself unchanged. If $P(X)$ is not linear, replace the block by one unmarked copy of $\text{Comp}(P(X))$, one unmarked copy of $\text{Comp}((X-1)^{p^{e-1}+1})$ and $\deg(P(X)) \cdot (p^{e-1} + 1) - \deg(P(X)) - (p^{e-1} + 1)$ unmarked copies of the trivial block I_1 .

These transformations result in a rational canonical form in $\text{GL}_{d+1}(q^2)$ whose multiset of Frobenius blocks is still closed under the operation $\text{Comp}(Q(X)^\ell) \mapsto \text{Comp}(\tilde{Q}(X)^\ell)$, whence by [58, Case (A), p. 34], the constructed rational canonical form is attained by some element $g \in \text{GU}_{d+1}(q)$. Moreover, it is clear by construction that the rational canonical form of g has exactly one non-semisimple block, which is of the form $\text{Comp}(L(X)^{p^{e-1}+1})$ for some linear polynomial $L(X) \in \mathbb{F}_{q^2}[X]$ with $L(X) = \tilde{L}(X)$, which forces $L(X)$ to be of the form $X - a$ with $\text{ord}(a)$ divides $q + 1$. The multiset of semisimple blocks of the rational canonical form of g is closed under $\text{Comp}(Q(X)^\ell) \mapsto \text{Comp}(\tilde{Q}(X)^\ell)$ and thus by [58, Case (A), p. 34] forms the rational canonical form of an element of $\text{GU}_{(d+1)-(p^{e-1}+1)}(q) = \text{GU}_{d-p^{e-1}}(q)$. Finally, none of the three transformations described above which lead from the rational canonical form of \tilde{s} to the one of g change the order of the form, whence $o = \text{ord}(s)$ divides $\text{ord}(\tilde{s}) = \text{ord}(g)$, as required. This concludes the proof of statement (i) for $S = {}^2A_d(q^2)$.

As for statement (ii), note that any lift $\tilde{s} \in \mathrm{SU}_{d+1}(q)$ of s must have a Frobenius block of the form $\mathrm{Comp}(P(X)^k)$ with $k \geq p^{e-1} + 1 = d + 1$. It follows that the rational canonical form of \tilde{s} consists of exactly one Frobenius block, of the form $\mathrm{Comp}((X - a)^{d+1})$ with $a \in \mathbb{F}_{q^2}^*$ of order dividing $q + 1$. Hence $(\tilde{s} - aI_{d+1})^{d+1} = 0$, and consequently (raising both sides to the power p^e) $(\tilde{s}^{p^e} - a^{p^e}I_{d+1})^{d+1} = 0$. However, \tilde{s}^{p^e} is semisimple, and so the minimal polynomial of \tilde{s}^{p^e} divides $(X - a^{p^e})^{d+1}$. It follows that the minimal polynomial of \tilde{s}^{p^e} is $X - a^{p^e}$, whence \tilde{s}^{p^e} is the scalar matrix $a^{p^e}I_{d+1}$. Denoting by π the canonical projection $\mathrm{SU}_{d+1}(q) \rightarrow \mathrm{PSU}_{d+1}(q) = S$, it follows that

$$s^{p^e} = \pi(\tilde{s})^{p^e} = \pi(\tilde{s}^{p^e}) = \pi(a^{p^e}I_{d+1}) = 1_S,$$

whence $o = p^e$, as asserted.

Finally, as for statement (iii), let, again, $\tilde{s} \in \mathrm{SU}_{d+1}(q)$ be a lift of s . Then \tilde{s} has a Frobenius block of the form $\mathrm{Comp}(P(X)^k)$ with $k \geq p^{e-1} + 1 = d$, so either \tilde{s} is as in the argument for statement (ii), which implies that $\mathrm{ord}(s) = p^e$, or \tilde{s} has two Frobenius blocks, one of the form $\mathrm{Comp}((X - a)^{p^{e-1}+1}) = \mathrm{Comp}((X - a)^d)$ for some $a \in \mathbb{F}_{q^2}^*$ with $\mathrm{ord}(a)$ divides $q + 1$, and the other block is $\mathrm{Comp}(X - a^{-d})$ (taking into account that $\det(\tilde{s}) = 1$). Similarly to the argument for statement (ii), we find that \tilde{s}^{p^e} is similar to the diagonal matrix which has the eigenvalues a^{p^e} , with multiplicity d , and a^{-dp^e} , with multiplicity 1. Modulo the scalars $\zeta \in \mathrm{GU}_{d+1}(q)$, the said diagonal matrix is congruent to the one which has eigenvalues 1, with multiplicity d , and $a^{-(d+1)p^e}$. It follows that

$$\frac{o}{p^e} = \mathrm{ord}(s^{p^e}) \text{ divides } \mathrm{ord}(a^{-(d+1)p^e}) \text{ divides } \frac{q+1}{\mathrm{gcd}(q+1, d+1)},$$

as required. This concludes our proof of result (b), exemplary for the entire proof of results (a)–(c).

Now let $e \in \{1, \dots, \lceil \log_p(h(X_d)) \rceil\}$. By the above results (a)–(c), each of the following numbers $\overline{o}_{p,e}(S)$ is an upper bound on $o_{p,e}(S)$:

(a) If $S = A_d(q)$, set

$$\overline{o}_{p,e}(S) := \begin{cases} 1, & \text{if } p^{e-1} + 1 = d + 1, \\ \tau\left(\frac{q-1}{\mathrm{gcd}(d+1, q-1)}\right), & \text{if } p^{e-1} + 1 = d, \\ \left| \bigcup_{o \in \mathrm{Ord}_{\mathrm{ss}}(\mathrm{GL}_{d-p^{e-1}}(q))} \mathrm{Div}(\mathrm{lcm}(q-1, o)) \right|, & \text{otherwise.} \end{cases}$$

(b) If $S = {}^2A_d(q^2)$, set

$$\overline{o}_{p,e}(S) := \begin{cases} 1, & \text{if } p^{e-1} + 1 = d + 1, \\ \tau\left(\frac{q+1}{\mathrm{gcd}(d+1, q+1)}\right), & \text{if } p^{e-1} + 1 = d, \\ \left| \bigcup_{o \in \mathrm{Ord}_{\mathrm{ss}}(\mathrm{GU}_{d-p^{e-1}}(q))} \mathrm{Div}(\mathrm{lcm}(q+1, o)) \right|, & \text{otherwise.} \end{cases}$$

(c) If $S = \mathrm{P}\Omega_{2d}^\epsilon(q)$, set

$$U_1 := \bigcup_{o \in \mathrm{Ord}_{\mathrm{ss}}(\mathrm{GO}_{2d-p^{e-1}-2}(q))} \mathrm{Div}(\mathrm{lcm}(2, o))$$

and

$$U_2 := \bigcup_{o \in \text{Ord}_{\text{ss}}(\text{GO}_{2d-2(p^{e-1}+1)}^\epsilon(q))} \text{Div}(\text{lcm}(q+1, o)).$$

Then set

$$\overline{o_{p,e}}(S) := \begin{cases} 1, & \text{if } p^{e-1} + 1 = 2d - 2, \\ |U_1 \cup U_2|, & \text{otherwise.} \end{cases}$$

In order to compute these upper bounds $\overline{o_{p,e}}(S)$, we need to be able to compute the set of semisimple element orders in the groups $\text{GL}_n(q)$, $\text{GU}_n(q)$, $\text{GO}_n(q)$ for n odd, and $\text{GO}_n^\epsilon(q)$ for n even. This is similar to (and actually easier than) the computation of $\text{o}_{\text{ss}}(S)$ following [9], and it uses the following well-known facts:

- (a) The conjugacy classes of maximal tori of $\text{GL}_n(q)$ are in a natural bijection with the ordered integer partitions λ of n . Moreover, for any maximal torus $T \leq \text{GL}_n(q)$ in the class corresponding to $\lambda = (\lambda_1, \dots, \lambda_s)$, we have $\text{Exp}(T) = \text{lcm}(q^{\lambda_1} - 1, \dots, q^{\lambda_s} - 1)$.
- (b) The conjugacy classes of maximal tori of $\text{GU}_n(q)$ are in a natural bijection with the ordered integer partitions λ of n . Moreover, for any maximal torus $T \geq \text{GU}_n(q)$ in the class corresponding to $\lambda = (\lambda_1, \dots, \lambda_s)$, we have $\text{Exp}(T) = \text{lcm}(q^{\lambda_1} - (-1)^{\lambda_1}, \dots, q^{\lambda_s} - (-1)^{\lambda_s})$.
- (c) Let $n \in \mathbb{N}^+$ be odd. The conjugacy classes of maximal tori of $\text{GO}_n(q)$ are in a natural bijection with the ordered pairs (λ_+, λ_-) of ordered integer partitions such that the total sum of the parts of λ_+ and λ_- is $\frac{n-1}{2}$. Moreover, for any maximal torus $T \leq \text{GO}_n(q)$ in the class corresponding to (λ_+, λ_-) with $\lambda_+ = (\lambda_+^{(1)}, \dots, \lambda_+^{(s_+)})$ and $\lambda_- = (\lambda_-^{(1)}, \dots, \lambda_-^{(s_-)})$, we have $\text{Exp}(T) = \text{lcm}(q^{\lambda_+^{(1)}} - 1, \dots, q^{\lambda_+^{(s_+)}} - 1, q^{\lambda_-^{(1)}} + 1, \dots, q^{\lambda_-^{(s_-)}} + 1)$.
- (d) Let $n \in \mathbb{N}^+$ be even. The conjugacy classes of maximal tori of $\text{GO}_n^\epsilon(q)$, with $\epsilon \in \{+, -\}$, are in a natural bijection with the ordered pairs (λ_+, λ_-) of ordered integer partitions such that the total sum of the parts of λ_+ and λ_- is $\frac{n}{2}$ and the number of parts of λ_- is even when $\epsilon = +$ and odd when $\epsilon = -$. Moreover, for any maximal torus $T \leq \text{GO}_n^\epsilon(q)$ in the class corresponding to (λ_+, λ_-) with $\lambda_+ = (\lambda_+^{(1)}, \dots, \lambda_+^{(s_+)})$ and $\lambda_- = (\lambda_-^{(1)}, \dots, \lambda_-^{(s_-)})$, we have $\text{Exp}(T) = \text{lcm}(q^{\lambda_+^{(1)}} - 1, \dots, q^{\lambda_+^{(s_+)}} - 1, q^{\lambda_-^{(1)}} + 1, \dots, q^{\lambda_-^{(s_-)}} + 1)$.

Recall the notion of a tX -admissible partition (pair) from case (3) earlier in this proof. The above results on exponents of maximal tori of $\text{GL}_n(q)$ and $\text{GU}_n(q)$ respectively imply that for $G \in \{\text{GL}_n(q), \text{GU}_n(q)\}$ and for each partition λ of n , there is a reduced (i.e., admissible) partition μ of n (namely $\mu = \bar{\lambda}$) such that the exponent of any maximal torus of G in the class corresponding to λ is equal to the exponent of any maximal torus of G in the class corresponding to μ . Hence $\text{Ord}_{\text{ss}}(G)$ can be computed by looping only over conjugacy classes of maximal tori corresponding to admissible (i.e., reduced) partitions of n and joining the sets of divisors of the exponents of such maximal tori. Similarly, $\text{Ord}_{\text{ss}}(G)$ for G an orthogonal group, can be computed by looping only over conjugacy classes of maximal tori corresponding to admissible partition pairs

and joining the sets of divisors of the exponents of such maximal tori. This concludes our description of the algorithm for computing $\text{Ord}_{\text{ss}}(G)$.

We now start to apply this algorithm, which the authors have implemented in GAP [26]. For the 10 groups listed in Table 11, the direct computation of $\omega(S)$ (and for some also of $\text{o}(S)$) via a computation of the conjugacy classes of S was either not possible at all or just too costly. However, combining either

- the exact value of $\text{o}(S)$ (where it can be computed) or
- the upper bound $\overline{\text{o}}(S)$ on it as computed by the above described algorithm

with the lower bound $\underline{\omega}(S)$ on $\omega(S)$ from the end of case (4) above is enough for those 9 groups S to show that $\epsilon_q(S) > \epsilon_q(M)$.

Table 11: Computation of $\underline{\omega}(S)$ and of $\text{o}(S)$ or $\overline{\text{o}}(S)$ is sufficient.

S	$\underline{\omega}(S)$	$\text{o}(S)$	$\epsilon_q(S) \geq$
$A_2(64)$	39	= 26	0.11759
$A_4(16)$	350	\leq 86	0.1607
$A_5(3)$	51	= 33	0.114388
${}^2A_2(23^2)$	32	\leq 20	0.13303
${}^2A_2(29^2)$	49	\leq 25	0.14480
${}^2A_3(9^2)$	56	\leq 27	0.13961
${}^2A_4(9^2)$	76	\leq 41	0.11623
${}^2A_5(3^2)$	66	\leq 35	0.12715
$D_5(5)$	166	\leq 81	0.11635
$D_7(3)$	557	\leq 113	0.16116

The group $S = {}^2A_2(32^2) = \text{PSU}_3(32)$ can be dealt with similarly; the lower bound $\underline{\omega}(S) = 12$ fails us by 1, but this can be easily fixed:

Table 12: A group with similar treatment.

S	$\omega(S) \geq$	$\text{o}(S)$	$\epsilon_q(S) \geq$
${}^2A_2(32^2)$	13	\leq 10	0.11502

Indeed, in order to get $\omega(S) \geq 13$, we note that $k(S) = 356$. This leads to the lower bound

$$\underline{\omega}(S) = \left\lceil \frac{356}{|\text{Out}(S)|} \right\rceil = \left\lceil \frac{356}{30} \right\rceil = 12,$$

and we can improve this by 1 by noting that the trivial conjugacy class of S is

certainly fixed under the action of $\text{Out}(S)$, so that

$$\omega(S) \geq 1 + \lceil \frac{355}{30} \rceil = 1 + 12 = 13,$$

as asserted.

Only the 10 groups S listed in Table 13 below remain to be dealt with. For each of them, we proceed as follows: First, we compute the upper bound $\bar{o}(S)$ on $o(S)$ listed in Table 13 with our algorithm. Once this is done, we consider certain element orders $o \in \text{Ord}(S)$, for which we provide nontrivial (i.e., greater than 1) lower bounds on $\omega_o(S)$; essentially, we do so by specifying various distinct rational canonical forms of elements in the Schur cover of S which project to order o elements in S , but in light of graph-field automorphisms, the correspondence between rational canonical forms and $\text{Aut}(S)$ -orbits of order o elements is not always injective, so in general, we need to divide the number of normal forms by a certain number to get a lower bound on $\omega_o(S)$. This is particularly cumbersome when $S = D_4(q)$, due to the large number of graph-field automorphisms, though we will be able to use [6, Proposition 3.55(i)] to at least get better bounds when $o = p$. In any case, this approach allows us to show that $\omega(S) \geq o(S) + W(S)$ for a certain number $W(S)$, also listed in Table 13. We then conclude that $\mathfrak{q}(S) = \frac{\omega(S)}{o(S)} \geq \frac{\bar{o}(S) + W(S)}{\bar{o}(S)}$, and this will be sufficient to get that $\epsilon_{\mathfrak{q}}(S) > \epsilon_{\mathfrak{q}}(\mathbb{M})$.

Table 13: The remaining groups.

S	$W(S)$	$\bar{o}(S)$	$\epsilon_{\mathfrak{q}}(S) \geq$
${}^2A_3(11^2)$	29	38	0.12567
${}^2A_5(5^2)$	65	70	0.11677
${}^2A_7(3^2)$	84	76	0.11593
${}^2A_8(2^2)$	48	48	0.11922
$D_4(5)$	17	31	0.11483
$D_4(7)$	35	47	0.11611
$D_4(9)$	38	47	0.11459
$D_5(3)$	30	44	0.1153
$D_6(3)$	69	61	0.11808
${}^2D_5(3^2)$	23	29	0.1161

As for the details of computing $W(S)$, we start by discussing the four remaining groups S of type 2A . Let $S = {}^2A_d(q^2) = \text{PSU}_{d+1}(q)$. The Schur cover of S is $\text{SU}_{d+1}(q)$, sitting inside $\text{GU}_{d+1}(q) \leq \text{GL}_{d+1}(q^2)$. The rational canonical forms in $\text{GL}_{d+1}(q^2)$ that are attained by elements of $\text{GU}_{d+1}(q)$ are characterised by Wall in [58, Subsection 2.6, Case (a), p. 34] to be those where the multiset of (Frobenius) blocks is closed under the involutory operation $\text{Comp}(P(X)^k) \mapsto \text{Comp}(\tilde{P}(X)^k)$, where $\tilde{P}(X)$ is the minimal polynomial over \mathbb{F}_{q^2} of ξ^{-q} , for any

root $\xi \in \overline{\mathbb{F}_{q^2}}$ of $P(X)$. Henceforth, we will refer to rational canonical forms in $\mathrm{GL}_{d+1}(q^2)$ satisfying Wall's criterion as *admissible*.

It is easy to see that a monic irreducible polynomial $P(X) \in \mathbb{F}_{q^2}[X]$ satisfies $P(X) = \tilde{P}(X)$ if and only if $\deg P(X)$ is odd and $\mathrm{ord}(P(X))$ divides $q^{\deg P(X)} + 1$, in which case we call either of

- the positive p' -integer $\mathrm{ord}(P(X))$,
- the polynomial $P(X)$, or
- the Frobenius block $\mathrm{Comp}(P(X)^k)$

U-economic, or just *economic* for short (the U stresses the fact that this notion of “economy” is specific for the treatment of the unitary case; for orthogonal groups, we will use a different notion of economic objects, see below). Positive p' -integers, monic irreducible polynomials in $\mathbb{F}_{q^2}[X]$ or Frobenius blocks over \mathbb{F}_{q^2} which are not economic will be called *uneconomic*. Note that these notions of (un)economic objects depend on q , which we view as fixed.

It is not difficult to show that a positive p' -integer o is economic if and only if it satisfies either of the following, equivalent conditions:

- o divides some number of the form $q^{2k+1} + 1$ with $k \in \mathbb{N}$.
- The q^2 -degree of o , denoted by $\deg_{q^2}(o)$, which is defined as the smallest positive integer t such that $o \mid q^{2t} - 1$, is odd, and $o \mid q^{\deg_{q^2}(o)} + 1$.

Now, given an element order o in $S = \mathrm{PSU}_{d+1}(q)$, our goal is to specify a set \mathcal{F}_o of order o admissible rational canonical forms in $\mathrm{GL}_{d+1}(q^2)$ such that

- (a) all forms in \mathcal{F}_o have determinant 1 (so that they actually represent elements in $\mathrm{SU}_{d+1}(q)$, not just $\mathrm{GU}_{d+1}(q)$);
- (b) all forms in \mathcal{F}_o have order o “modulo the scalars $\zeta \mathrm{GU}_{d+1}(q)$ ” (i.e., for each form in \mathcal{F}_o , o is the smallest positive integer m such that the m -th power of the form is in $\zeta \mathrm{GU}_{d+1}(q)$); and
- (c) no two matrix similarity classes represented by distinct forms in \mathcal{F}_o are fused under multiplication by scalars in $\zeta \mathrm{GU}_{d+1}(q)$.

It is easy to check that each of these three properties, say (x), is implied by a certain other property, (x'), which we will now formulate:

- (a') o is coprime to $\mathrm{gcd}(d+1, q+1) = |\zeta \mathrm{GU}_{d+1}(q)|$ (equivalently, every Frobenius block of every form in \mathcal{F}_o has order coprime to $\mathrm{gcd}(d+1, q+1)$).
- (b') Either o is coprime to $\mathrm{gcd}(d+1, q+1)$, or $p \mid o$ and each form in \mathcal{F}_o has at least one unipotent block $\mathrm{Comp}((X-1)^k)$.
- (c') There is a divisor o' of o which is coprime to $\mathrm{gcd}(d+1, q+1)$ and such that each form in \mathcal{F}_o has at least one block of order o' , but no form in \mathcal{F}_o has a block of order a proper multiple of o' .

Assume now that we have specified such a set \mathcal{F}_o of rational canonical forms. Then different elements in \mathcal{F}_o correspond to different conjugacy classes in S , and by property (c) above, the only fusion under the action of $\mathrm{Aut}(S) = \mathrm{PGU}_{d+1}(q) \rtimes \Phi_S$ of conjugacy classes in S corresponding to different forms

in \mathcal{F}_o that can occur is under Φ_S , the group of field automorphisms of S . In each of the four examples S that we need to consider, $q = p$ is a prime, and thus $|\Phi_S| = 2$. It follows that $\omega_o(S) \geq \lceil \frac{|\mathcal{F}_o|}{2} \rceil$, and we even get $\omega_o(S) \geq |\mathcal{F}_o|$ if we can argue that no fusion under field automorphisms can occur either (which is possible in some cases).

Each of the element orders o in S which we consider for the definition of \mathcal{F}_o falls into exactly one of the following three categories:

- Category I: o is semisimple and coprime to $\gcd(d+1, q+1)$. Then
 - if o is economic, we define \mathcal{F}_o to consist of those (admissible) rational canonical forms with exactly one nontrivial block, which is of the form $\text{Comp}(P(X))$ for some monic irreducible polynomial $P(X) \in \mathbb{F}_{q^2}[X]$ of order o . Then $|\mathcal{F}_o| \geq \frac{\phi(o)}{\deg_{q^2}(o)}$, and $\omega_o(S) \geq \lceil \frac{|\mathcal{F}_o|}{2} \rceil$;
 - if o is uneconomic, we define \mathcal{F}_o to consist of those (admissible) rational canonical forms with exactly two nontrivial blocks, of the forms $\text{Comp}(P(X))$ and $\text{Comp}(\tilde{P}(X))$ for some monic irreducible polynomial $P(X) \in \mathbb{F}_{q^2}[X]$ of order o . Then $|\mathcal{F}_o| \geq \lceil \frac{\phi(o)}{2 \deg_{q^2}(o)} \rceil$ and $\omega_o(S) \geq \lceil \frac{|\mathcal{F}_o|}{2} \rceil$.
- Category II: $o = p^e$ is unipotent. Then we let \mathcal{F}_o consist of all unipotent rational canonical forms in $\text{GL}_{d+1}(q^2)$ whose order is p^e (note that unipotent rational canonical forms are always admissible). Then $|\mathcal{F}_o|$ is just $\pi(d+1, p, e)$, which is defined as the number of ordered integer partitions of $d+1$ all of whose parts are at most p^e and which have at least one part strictly larger than p^{e-1} . Moreover, since all unipotent forms have coefficients in the prime field \mathbb{F}_p , no fusion can occur under Φ_S , whence $\omega_o(S) \geq |\mathcal{F}_o|$.
- Category III: o is neither semisimple nor unipotent. This only occurs in the following two cases:
 - $S = {}^2A_7(2^2) = \text{PSU}_8(2)$ and $o = 6 = 2^e \cdot 3$ with $e = 1$;
 - $S = {}^2A_8(2^2) = \text{PSU}_9(2)$ and $o = 2^e \cdot 3$ with $e \in \{1, 2\}$.

In both cases, let $\xi \in \mathbb{F}_{2^2}$ be a generator of $\mathbb{F}_{2^2}^*$. We let \mathcal{F}_o consist of those rational canonical forms in $\text{GL}_{d+1}(2^2)$ whose nontrivial semisimple blocks are $\text{Comp}(X - \xi)$ and $\text{Comp}(X - \xi^{-1})$, occurring with the same multiplicity $m \in \{1, 2, 3\}$ (this is to ensure that the determinant is 1) and whose other nontrivial blocks are all unipotent of maximal order 2^e . It is not difficult to see that $|\mathcal{F}_o| = \sum_{m=1}^3 \pi(d+1 - 2m, 2, e)$ and $\omega_o(S) \geq |\mathcal{F}_o|$.

We are now ready to give the arguments for the lower bounds $W(S)$ on $\mathfrak{d}(S) = \omega(S) - o(S)$ when S is one of the four 2A examples in compact, tabular form. Each table corresponds to one group S , and each row to an element order o in S . One can then check that the value of $W(S)$ given in Table 13 coincides with $\sum_o (\underline{\omega}_o(S) - 1)$, where o ranges over the element orders in S listed in the respective table and $\underline{\omega}_o(S)$ is the lower bound on $\omega_o(S)$ given in the last column of the table.

Table 14: $S = {}^2A_3(11^2) = \text{PSU}_4(11)$, $\gcd(d+1, q+1) = 4$.

o	Category of o	Relevant info	$ \mathcal{F}_o $	$\omega_o(S) \geq$
$305 = 5 \cdot 61$	I	o is uneco., $\deg_{11^2}(o) = 2$	$\geq \lceil \frac{\phi(305)}{4} \rceil = 60$	$\lceil \frac{60}{2} \rceil = 30$

Table 15: $S = {}^2A_5(5^2) = \text{PSU}_6(5)$, $\gcd(d+1, q+1) = 6$.

o	Category of o	Relevant info	$ \mathcal{F}_o $	$\omega_o(S) \geq$
$217 = 7 \cdot 31$	I	o is uneco., $\deg_{5^2}(o) = 3$	$\geq \lceil \frac{\phi(217)}{2 \cdot 3} \rceil = 30$	$\lceil \frac{30}{2} \rceil = 15$
521	I	o is eco., $\deg_{5^2}(o) = 5$	$= \frac{\phi(521)}{5} = 104$	$\lceil \frac{104}{2} \rceil = 52$

Table 16: $S = {}^2A_7(3^2) = \text{PSU}_8(3)$, $\gcd(d+1, q+1) = 4$.

o	Category of o	Relevant info	$ \mathcal{F}_o $	$\omega_o(S) \geq$
3	II	$ \mathcal{F}_o = \pi(8, 3, 1)$	$= 9$	9
$6 = 2 \cdot 3$	III	$ \mathcal{F}_o = \sum_{m=1}^3 \pi(8-2m, 3, 1)$	$= 9$	9
$9 = 3^2$	II	$ \mathcal{F}_o = \pi(8, 3, 2)$	$= 12$	12
61	I	o is eco., $\deg_{3^2}(o) = 5$	$= \frac{\phi(61)}{5} = 12$	$\lceil \frac{12}{2} \rceil = 6$
$91 = 7 \cdot 13$	I	o is uneco., $\deg_{3^2}(o) = 3$	$\geq \lceil \frac{\phi(91)}{2 \cdot 3} \rceil = 12$	$\lceil \frac{12}{2} \rceil = 6$
$205 = 5 \cdot 41$	I	o is uneco., $\deg_{3^2}(o) = 4$	$\geq \lceil \frac{\phi(205)}{4} \rceil = 20$	$\lceil \frac{20}{2} \rceil = 10$
547	I	o is eco., $\deg_{3^2}(o) = 7$	$= \frac{\phi(547)}{7} = 78$	$\lceil \frac{78}{2} \rceil = 39$

Table 17: $S = {}^2A_8(2^2) = \text{PSU}_9(2)$, $\gcd(d+1, q+1) = 3$.

o	Category of o	Relevant info	$ \mathcal{F}_o $	$\omega_o(S) \geq$
2	II	$ \mathcal{F}_o = \pi(9, 2, 1)$	$= 4$	4
$4 = 2^2$	II	$ \mathcal{F}_o = \pi(9, 2, 2)$	$= 13$	13
$6 = 2 \cdot 3$	III	$ \mathcal{F}_o = \sum_{m=1}^3 \pi(9-2m, 2, 1)$	$= 6$	6
$8 = 2^3$	II	$ \mathcal{F}_o = \pi(9, 2, 3)$	$= 11$	11
$12 = 2^2 \cdot 3$	III	$ \mathcal{F}_o = \sum_{m=1}^3 \pi(9-2m, 2, 2)$	$= 14$	14
43	I	o is eco., $\deg_{2^2}(o) = 7$	$= \frac{\phi(43)}{7} = 6$	$\lceil \frac{6}{2} \rceil = 3$
$85 = 5 \cdot 17$	I	o is uneco., $\deg_{2^2}(o) = 4$	$\geq \lceil \frac{\phi(85)}{8} \rceil = 8$	$\lceil \frac{8}{2} \rceil = 4$

We now turn to the remaining six groups S , all of which are of type D or 2D , i.e.,

of the form $P\Omega_{2d}^\epsilon(q)$ with $\epsilon \in \{+, -\}$, and they have odd defining characteristic. The Schur cover of S is $\Omega_{2d}^\epsilon(q)$, a subgroup of $\text{GO}_{2d}^\epsilon(q) \leq \text{GL}_{2d}(q)$. In [58, Subsection 2.6, Case (C), pp. 38f.], Wall characterised those rational canonical forms in $\text{GL}_{2d}(q)$ which are attained by an element of $\text{GO}_{2d}^\epsilon(q)$. More precisely, these are just those rational canonical forms where

- the multiset of Frobenius blocks is closed under the involutory operation $\text{Comp}(P(X)^k) \mapsto \text{Comp}(P^*(X)^k)$ where $P^*(X)$ is the minimal polynomial over \mathbb{F}_q of ξ^{-1} for any root $\xi \in \overline{\mathbb{F}_q}$ of $P(X)$;
- the multiplicity of each block of the form $\text{Comp}((X \pm 1)^{2k})$ is even; and
- denoting by $\mu(P(X)^k)$ the multiplicity of the block $\text{Comp}(P(X)^k)$ in the form: if there are no blocks of the form $\text{Comp}((X \pm 1)^{2k+1})$, then

$$\sum_{P(X), k} k\mu(P(X)^k) \equiv \begin{cases} 0 \pmod{2}, & \text{if } \epsilon = +, \\ 1 \pmod{2}, & \text{if } \epsilon = -, \end{cases}$$

where $P(X)$ ranges over all monic irreducible polynomials in $\mathbb{F}_q[X]$ and k ranges over all positive integers.

It is easy to see that a monic irreducible polynomial $P(X) \in \mathbb{F}_q[X]$ satisfies $P(X) = P^*(X)$ if and only if $\deg P(X)$ is even and $\text{ord}(P(X)) \mid q^{\deg(P(X))/2} + 1$, in which case we call either of

- the positive p' -integer $\text{ord}(P(X))$,
- the polynomial $P(X) \in \mathbb{F}_q[X]$, or
- the Frobenius block $\text{Comp}(P(X)^k)$

O -*economic* or just *economic* for short (note that this is distinct from the notion of U -*economic* objects used in the unitary case above). Positive p' -integers, monic irreducible polynomials in $\mathbb{F}_q[X]$, and Frobenius blocks over \mathbb{F}_q which are not economic will be called *uneconomic*. Note that, as in the unitary case, these notions of (un)economic objects depend on q , which we view as fixed. Also, observe that a positive p' -integer o is economic if and only if it satisfies either of the following, equivalent conditions:

- o divides some number of the form $q^k + 1$ with $k \in \mathbb{N}^+$.
- Either $o \leq 2$, or the q -degree of o , denoted by $\deg_q(o)$ and defined as the smallest positive integer t such that o divides $q^t - 1$, is even, and $o \mid q^{\deg_q(o)/2} + 1$.

Our basic strategy is to specify, for a given element order o in $S = P\Omega_{2d}^\epsilon(q)$, a (preferably large) set \mathcal{F}_o of order o rational canonical forms in $\text{GL}_{2d}(q)$ such that the following hold:

- (a) all forms in \mathcal{F}_o are attained by an element of $P\Omega_{2d}^\epsilon(q)$ (not just $\text{GO}_{2d}^\epsilon(q)$);
- (b) all forms in \mathcal{F}_o have order o “modulo the scalars $\zeta\Omega_{2d}^\epsilon$ ” (i.e., for each form in \mathcal{F}_o , o is the smallest positive integer m such that the m -th power of the form is a scalar matrix in $\zeta\Omega_{2d}^\epsilon$);

- (c) no two matrix similarity classes represented by distinct forms in \mathcal{F}_o are fused under multiplication by scalars in $\zeta\Omega_{2d}^\epsilon(q)$.

Each of these properties, say (x), is implied by a certain other property, (x'), which we will now list:

- (a') all forms in \mathcal{F}_o are similar to the square of the rational canonical form of some element in $\text{GO}_{2d}^\epsilon(q)$, as characterised by Wall;
 (b') all forms in \mathcal{F}_o have at least one Frobenius block of odd order;
 (c') there is an odd divisor o' of o such that every form in \mathcal{F}_o has at least one block of order o' , but no form in \mathcal{F}_o has a block of order $2o'$.

To see that (a') implies (a), use that $\text{GO}_{2d}^\epsilon(q)/\Omega_{2d}^\epsilon(q)$ is of exponent 2, and to see that (b') implies (b) and (c') implies (c), use that $|\zeta\Omega_{2d}^\epsilon(q)| \leq 2$. Since $D_5(3) = \Omega_{10}^+(3)$ is centreless, we do not need to worry about properties (b) and (c) at all when $S = D_5(3)$. Throughout the concrete discussion of the six remaining examples S below, properties (a') and (b') (and thus (a) and (b)) will be satisfied for each of the element orders o of S that we will consider. Property (c) will also always be satisfied, but sometimes, property (c') is not (for example, when $S = D_4(7)$ and $o = 4$); in those cases, one needs to verify directly that no two of the given forms are fused under scalar multiplication (by $-I_{2d}$).

After specifying \mathcal{F}_o and computing its cardinality, we need to consider potential fusion of forms in \mathcal{F}_o under $\text{Aut}(S)$. Note that $\text{Aut}(S)$ contains the subgroup $\text{PCO}_{2d}^\epsilon(q)$, which does not fuse distinct matrix similarity classes. If $S = {}^2D_5(3^2)$, which is the only group of type 2D that we need to consider, then $\text{Aut}(S) = \text{PCO}_{2d}^-(3)$, and we may use $|\mathcal{F}_o|$ itself as a lower bound on $\omega_o(S)$. So assume for the rest of this paragraph that $S = D_d(q) = \text{P}\Omega_{2d}^+(q)$. Then the fusion of forms in \mathcal{F}_o under $\text{Aut}(S)$ is controlled by the index $|\text{Aut}(S) : \text{PCO}_{2d}^+(q)|$. If $d > 4$, then $\text{Aut}(S) = \text{P}\Gamma\text{O}_{2d}^+(q) = \text{PCO}_{2d}^+(q)\Phi_S$, and so we only need to worry about fusion under field automorphisms of S , of which there are $|\Phi_S| = f$, and we conclude that $\omega_o(S) \geq \frac{|\mathcal{F}_o|}{f}$. If, on the other hand, $d = 4$, then $\text{P}\Gamma\text{O}_{2d}^+(q)$ is an index 3 subgroup of $\text{Aut}(S)$, and $\text{Aut}(S) = \text{P}\Gamma\text{O}_{2d}^+(q)\langle\gamma\rangle$ where γ is an order 3 graph automorphism of S ; it follows that $\omega_o(S) \geq \frac{|\mathcal{F}_o|}{3f}$. The only case where we obtain better lower bounds on $\omega_o(S)$ is when $d = 4$ and $o = p$ (the defining characteristic), using [6, Proposition 3.55(i)].

We now provide some more information relevant for reading Tables 18 to 22 below. Each table corresponds to one group S , and the rows correspond to the element orders o in S for which we specify a set \mathcal{F}_o of rational canonical forms as explained above and subsequently compute a lower bound on $\omega_o(S)$.

When o' is a semisimple element order in S , then the number of distinct monic irreducible polynomials in $\mathbb{F}_q[X]$ of order o' (all of which have degree $\deg_q(o')$) is exactly $\frac{\phi(o')}{\deg_q(o')}$. If o' is uneconomic, then these polynomials come in at least $\lceil \frac{\phi(o')}{2\deg_q(o')} \rceil$ pairs $\{P(X), P^*(X)\}$. We use the notation $P_{o'} = P_{o'}(X)$ to denote an arbitrary monic irreducible polynomial in $\mathbb{F}_q[X]$ of order o' .

For describing the forms in \mathcal{F}_o , we specify the multiplicities of their Frobenius blocks $\text{Comp}(P(X)^k)$, with the convention that blocks which are not mentioned occur with multiplicity 0. When doing so, we identify $P^k = P(X)^k$ with $\text{Comp}(P(X)^k)$ for brevity, and we use I_k to denote the $(k \times k)$ -identity matrix over \mathbb{F}_q ; in particular, I_1 is a copy of the trivial Frobenius block over \mathbb{F}_q . We write (B, a) shorthand for “the Frobenius block B occurs with multiplicity a ”, and we separate these multiplicity specifications for one type of form by commas, with a semicolon separating descriptions of forms of different shape in the same set \mathcal{F}_o (such as for $S = D_4(5)$ and $o = 13$). When the form may involve several companion blocks of polynomials of the same order o' which may or may not be equal, we denote those polynomials by $P_{o'}^{(1)}, P_{o'}^{(2)}$, and so on.

In order to see that in those cases where o is even, the specified forms in \mathcal{F}_o are indeed similar to squares of forms of elements in $\text{GO}_{2d}^\epsilon(q)$, we make the following observations:

- When $q = 3$ (relevant for $S = D_5(3), {}^2D_5(3^2), D_6(3)$): $-I_2 = \text{Comp}(P_4(X))^2$ for the unique order 4 (quadratic) monic irreducible polynomial $P_4(X) \in \mathbb{F}_3[X]$, which is economic.
- When $q = 5$ (relevant for $S = D_4(5)$): $-I_2$ is the square of the rational canonical form whose nontrivial blocks (both occurring with multiplicity 1) are the companion matrices of the two order 4 (linear) monic irreducible polynomials $P_4(X)$ and $P_4^*(X)$ in $\mathbb{F}_5[X]$.
- When $q = 7$ (relevant for $S = D_4(7)$):
 - $-I_2 = \text{Comp}(P_4(X))^2$ for the unique order 4 (quadratic) monic irreducible polynomial $P_4(X) \in \mathbb{F}_7[X]$, which is economic;
 - $\text{Comp}(P_4(X))$ is similar to $\text{Comp}(P_8(X))^2$ for any of the two order 8 (quadratic) monic irreducible polynomials $P_8(X) \in \mathbb{F}_7[X]$, which are economic.

Finally, for the counting of forms of unipotent elements in S , we denote by $\Pi'(2d, p, e)$ (resp. $\pi'(2d, p, e)$) the set (resp. number) of ordered integer partitions of $2d$ such that all parts are at most p^e , at least one part is larger than p^{e-1} , and all multiplicities of even parts are even. We identify elements of $\Pi'(2d, p, e)$ with unipotent rational canonical forms in S by assigning to a partition $\lambda = (\lambda_1, \dots, \lambda_s) \in \Pi'(2d, p, e)$ the form with blocks $\text{Comp}((X - 1)^{\lambda_1}), \dots, \text{Comp}((X - 1)^{\lambda_s})$, listed with multiplicities.

Table 18: $S = D_4(5) = \text{P}\Omega_8^+(5)$.

o	relevant info	forms in \mathcal{F}_o	$ \mathcal{F}_o $	$\omega_o(S) \geq$
3	3 is eco., $\deg_5(3) = 2$, $\#P_3 = \frac{\phi(3)}{2} = 1$	$(P_3, a), (I_1, 8 - 2a)$ for $a \in \{1, 2, 3, 4\}$	4	$\lceil \frac{4}{3} \rceil = 2$
5	Use [6, Proposition 3.55(i)]	$\Pi'(8, 5, 1) \setminus \{(2, 2, 2, 2), (4, 4)\}$	$\pi'(8, 5, 1) - 2 = 5$	5
6	3 is eco., $\deg_5(3) = 2$, $\#P_3 = \frac{\phi(3)}{2} = 1$	$(P_3, a), (-I_1, 2b), (I_1, 8 - 2(a + b))$ for $a, b \geq 1, a + b \leq 4$	6	$\lceil \frac{6}{3} \rceil = 2$

10	none	$(-I_1, 2a), \Pi'(8 - 2a, 5, 1)$ for $a \in \{1, 2\}$	6	$\lceil \frac{6}{3} \rceil = 2$
13	13 is eco., $\deg_5(13) = 4$, $\#P_{13} = \frac{\phi(13)}{4} = 3$	$(P_{13}, 1), (I_1, 4);$ $(P_{13}^{(1)}, 1), (P_{13}^{(2)}, 1)$	$3 + 3 + \binom{3}{2} = 9$	$\lceil \frac{9}{3} \rceil = 3$
21	21 is eco., $\deg_5(21) = 6$, $\#P_{21} = \frac{\phi(21)}{6} = 2$; 3 is eco., $\deg_5(3) = 2$, $\#P_3 = \frac{\phi(3)}{2} = 1$	$(P_{21}, 1), (I_1, 2);$ $(P_{21}, 1), (P_3, 1)$	$2 + 2 = 4$	$\lceil \frac{4}{3} \rceil = 2$
26	13 is eco., $\deg_5(13) = 4$ $\#P_{13} = \frac{\phi(13)}{4} = 3$	$(P_{13}, 1), (-I_1, 2a), (I_1, 4 - 2a)$ for $a \in \{1, 2\}$	$2 \cdot 3 = 6$	$\lceil \frac{6}{3} \rceil = 2$
31	31 is uneco., $\deg_5(31) = 3$, $\#\{P_{31}, P_{31}^*\} = \frac{\phi(31)}{2 \cdot 3} = 5$	$(P_{31}, 1), (P_{31}^*, 1), (I_1, 2)$	5	$\lceil \frac{5}{3} \rceil = 2$
62	31 is uneco., $\deg_5(31) = 3$, $\#\{P_{31}, P_{31}^*\} = \frac{\phi(31)}{2 \cdot 3} = 5$	$(P_{31}, 1), (P_{31}^*, 1), (-I_1, 2)$	5	$\lceil \frac{5}{3} \rceil = 2$
63	63 is eco., $\deg_5(63) = 6$, $\#P_{63} = \frac{\phi(63)}{6} = 6$; 3 is eco., $\deg_5(3) = 2$, $\#P_3 = \frac{\phi(3)}{2} = 1$	$(P_{63}, 1), (I_1, 2);$ $(P_{63}, 1), (P_3, 1)$	$6 + 6 = 12$	$\lceil \frac{12}{3} \rceil = 4$
126	63 is eco., $\deg_5(63) = 6$, $\#P_{63} = \frac{\phi(63)}{6} = 6$; 3 is eco., $\deg_5(3) = 2$, $\#P_3 = \frac{\phi(3)}{2} = 1$	$(P_{63}, 1), (-I_1, 2)$	6	$\lceil \frac{6}{3} \rceil = 2$

Table 19: $S = D_4(7) = \text{P}\Omega_8^+(7)$.

o	relevant info	forms in \mathcal{F}_o	$ \mathcal{F}_o $	$\omega_o(S) \geq$
3	3 is uneco., $\deg_7(3) = 1$, $\#\{P_3, P_3^*\} = \frac{\phi(3)}{2 \cdot 1} = 1$	$(P_3, a), (P_3^*, a), (I_1, 8 - 2a)$ for $a \in \{1, 2, 3, 4\}$	4	$\lceil \frac{4}{3} \rceil = 2$
4	4 is eco., $\deg_7(4) = 2$, $\#P_4 = \frac{\phi(4)}{2} = 1$	$(P_4, a), (-I_1, 2b), (I_1, 8 - 2(a + b))$ for $1 \leq a \leq 3, b \geq 0, a + 2b \leq 4$	5	$\lceil \frac{5}{3} \rceil = 2$
6	3 is uneco., $\deg_7(3) = 1$, $\#\{P_3, P_3^*\} = \frac{\phi(3)}{2 \cdot 1} = 1$	$(P_3, a), (P_3^*, a), (-I_1, 2b), (I_1, 8 - 2(a + b))$ for $a, b \geq 1, a + b \leq 4$	6	$\lceil \frac{6}{3} \rceil = 2$
7	Use [6, Proposition 3.55(i)]	$\Pi'(8, 7, 1) \setminus \{(2, 2, 2, 2), (4, 4)\}$	6	6
12	3 is uneco., $\deg_7(3) = 1$, $\#\{P_3, P_3^*\} = \frac{\phi(3)}{2 \cdot 1} = 1$; 4 is eco., $\deg_7(4) = 2$, $\#P_4 = \frac{\phi(4)}{2} = 1$	$(P_3, a), (P_3^*, a), (P_4, b), (-I_1, 2c), (I_1, 8 - 2(a + b + c))$ for $a, b \geq 1, c \geq 0, a + b + 2c \leq 4$, and if $c = 0$ and $a + b = 4$, then $2 \mid b$	8	$\lceil \frac{8}{3} \rceil = 3$

25	25 is eco., $\deg_7(25) = 4$, $\#P_{25} = \frac{\phi(25)}{4} = 5$; 5 is eco., $\deg_7(5) = 4$, $\#P_5 = \frac{\phi(5)}{4} = 1$	$(P_{25}, 1), (I_1, 4)$; $(P_{25}, 1), (P_5, 1)$; $(P_{25}^{(1)}, 1), (P_{25}^{(2)}, 1)$	25	$\lceil \frac{25}{3} \rceil = 9$
43	43 is eco., $\deg_7(43) = 6$, $\#P_{43} = \frac{\phi(43)}{6} = 7$	$(P_{43}, 1), (I_1, 2)$	7	$\lceil \frac{7}{3} \rceil = 3$
50	25 is eco., $\deg_7(25) = 4$, $\#P_{25} = \frac{\phi(25)}{4} = 5$; 4 is eco., $\deg_7(4) = 2$, $\#P_4 = \frac{\phi(4)}{2} = 1$	$(P_{25}, 1), (P_4, 1), (I_1, 2)$	10	$\lceil \frac{10}{3} \rceil = 4$
57	57 is uneco., $\deg_7(57) = 3$, $\#\{P_{57}, P_{57}^*\} = \frac{\phi(57)}{2 \cdot 3} = 6$	$(P_{57}, 1), (I_1, 2)$	6	$\lceil \frac{6}{3} \rceil = 2$
75	25 is eco., $\deg_7(25) = 4$, $\#P_{25} = \frac{\phi(25)}{4} = 5$; 3 is uneco., $\deg_7(3) = 1$, $\#\{P_3, P_3^*\} = \frac{\phi(3)}{2 \cdot 1} = 1$	$(P_{25}, 1), (P_3, 1), (P_3^*, 1), (I_1, 2)$	5	$\lceil \frac{5}{3} \rceil = 2$
86	43 is eco., $\deg_7(43) = 6$, $\#P_{43} = \frac{\phi(43)}{6} = 7$	$(P_{43}, 1), (-I_1, 2)$	7	$\lceil \frac{7}{3} \rceil = 3$
100	25 is eco., $\deg_7(25) = 4$, $\#P_{25} = \frac{\phi(25)}{4} = 5$; 4 is eco., $\deg_7(4) = 2$, $\#P_4 = \frac{\phi(4)}{2} = 1$	$(P_{25}, 1), (P_4, 1), (I_1, 2)$	5	$\lceil \frac{5}{3} \rceil = 2$
171	171 is uneco., $\deg_7(171) = 3$, $\#\{P_{171}, P_{171}^*\} = \frac{\phi(171)}{2 \cdot 3} = 18$	$(P_{171}, 1), (P_{171}^*, 1), (I_1, 2)$	18	$\lceil \frac{18}{3} \rceil = 6$
172	43 is eco., $\deg_7(43) = 6$, $\#P_{43} = \frac{\phi(43)}{6} = 7$; 4 is eco., $\deg_7(4) = 2$, $\#P_4 = \frac{\phi(4)}{2} = 1$	$(P_{43}, 1), (P_4, 1)$	7	$\lceil \frac{7}{3} \rceil = 3$

Table 20: $S = D_4(9) = P\Omega_8^+(9)$.

o	relevant info	forms in \mathcal{F}_o	$ \mathcal{F}_o $	$\omega_o(S) \geq$
3	Use [6, Proposition 3.55(i)]	$\Pi'(8, 3, 1) \setminus \{(2, 2, 2, 2), (4, 4)\}$	4	4
5	5 is eco., $\deg_9(5) = 2$, $\#P_5 = \frac{\phi(5)}{2} = 2$	$(P_5^{(1)}, a), (P_5^{(2)}, b), (I_1, 8 - 2(a + b))$ for $P_5^{(1)} \neq P_5^{(2)}$, $a, b \geq 0$, $1 \leq a + b \leq 4$	14	$\lceil \frac{14}{6} \rceil = 3$
41	41 is eco., $\deg_9(41) = 4$, $\#P_{41} = \frac{\phi(41)}{4} = 10$	$(P_{41}, 1), (I_1, 4)$; $(P_{41}^{(1)}, 1), (P_{41}^{(2)}, 1)$	65	$\lceil \frac{65}{6} \rceil = 11$

365	365 is eco., $\deg_9(365) = 6$, $\#P_{365} = \frac{\phi(365)}{6} = 48$; 5 is eco., $\deg_9(5) = 2$, $\#P_5 = \frac{\phi(5)}{2} = 2$	$(P_{365}, 1), (I_1, 2); (P_{365}, 1), (P_5, 1)$	144	$\lceil \frac{144}{6} \rceil = 24$
-----	---	--	-----	------------------------------------

Table 21: $S = D_5(3) = P\Omega_{10}^+(3) = \Omega_{10}^+(3)$.

o	relevant info	forms in \mathcal{F}_o	$ \mathcal{F}_o $	$\omega_o(S) \geq$
2	none	$(-I_1, 2a), (I_1, 10 - 2a)$ for $a \in \{1, \dots, 5\}$	5	5
3	none	$\Pi'(10, 3, 1)$	7	7
5	5 is eco. $\deg_3(5) = 4$, $\#P_5 = \frac{\phi(4)}{4} = 1$	$(P_4, a), (I_1, 10 - 4a)$ for $a \in \{1, 2\}$	2	2
6	none	$(-I_1, 2a), \Pi'(10 - 2a, 3, 1)$ for $a \in \{1, 2, 3\}$	10	10
9	none	$\Pi'(10, 3, 2)$	8	8
10	5 is eco. $\deg_3(5) = 4$, $\#P_5 = \frac{\phi(4)}{4} = 1$	$(P_5, 1), (-I_1, 2a), (I_1, 6 - 2a)$ for $a \in \{1, 2, 3\}$	4	4

Table 22: $S = {}^2D_5(3^2) = P\Omega_{10}^-(3)$.

o	relevant info	forms in \mathcal{F}_o	$ \mathcal{F}_o $	$\omega_o(S) \geq$
2	none	$(-I_1, 2a), (I_1, 10 - 2a)$ for $a \in \{1, 2\}$	2	2
3	none	$\Pi'(10, 3, 1)$	7	7
5	5 is eco. $\deg_3(5) = 4$, $\#P_5 = \frac{\phi(4)}{4} = 1$	$(P_4, a), (I_1, 10 - 4a)$ for $a \in \{1, 2\}$	2	2
6	none	$(-I_1, 2a), \Pi'(10 - 2a, 3, 1)$ for $a \in \{1, 2, 3\}$	10	10
10	5 is eco. $\deg_3(5) = 4$, $\#P_5 = \frac{\phi(4)}{4} = 1$	$(P_5, 1), (-I_1, 2a), (I_1, 6 - 2a)$ for $a \in \{1, 2, 3\}$	4	4

Table 23: $S = D_6(3) = P\Omega_{12}^+(3)$.

o	relevant info	forms in \mathcal{F}_o	$ \mathcal{F}_o $	$\omega_o(S) \geq$
2	none	$(-I_1, 2a), (I_1, 12 - 2a)$ for $a \in \{1, 2, 3\}$	3	3
3	none	$\Pi'(12, 3, 1)$	10	10
6	none	$(-I_1, 2a), \Pi'(12 - 2a, 3, 1)$ for $a \in \{1, 2, 3, 4\}$	17	17
9	none	$\Pi'(12, 3, 2)$	15	15
41	41 is eco., $\deg_3(41) = 8,$ $\#P_{41} = \frac{\phi(41)}{8} = 5$	$(P_{41}, 1), (I_1, 4)$	5	5
61	61 is eco., $\deg_3(61) = 10,$ $\#P_{61} = \frac{\phi(61)}{10} = 6$	$(P_{61}, 1), (I_1, 2)$	6	6
82	41 is eco., $\deg_3(41) = 8,$ $\#P_{41} = \frac{\phi(41)}{8} = 5$	$(P_{41}, 1), (-I_1, 2a), (I_1, 4 - 2a)$ for $a \in \{1, 2\}$	10	10
91	91 is uneco., $\deg_3(91) = 6,$ $\#\{P_{91}, P_{91}^*\} = \frac{\phi(91)}{2 \cdot 6} = 6$	$(P_{91}, 1), (P_{91}^*, 1)$	6	6
122	61 is eco., $\deg_3(61) = 10,$ $\#P_{61} = \frac{\phi(61)}{10} = 6$	$(P_{122}, 1), (-I_1, 2)$	6	6

□

4 Proof of Theorem 1.1.2(1)

We start with the following lemma, which provides upper bounds for $\mathfrak{d}(N)$ and $\mathfrak{m}(G/N)$ in terms of $\mathfrak{d}(G)$ (see Definition 1.1.1(4,a)), where N is a characteristic subgroup of G :

Lemma 4.1. *Let G be a finite group, and let N be a characteristic subgroup of G . Then*

- (1) $\mathfrak{d}(N) \leq \mathfrak{d}(G)$.
- (2) $\mathfrak{m}(G/N) \leq 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$.

We note that the special case $\mathfrak{d}(G) = 0$ (i.e., when G is an AT-group) in Lemma 4.1 is just [61, Lemma 1.1], and the proof of Lemma 4.1 is also a generalisation of the proof of [61, Lemma 1.1].

Proof of Lemma 4.1. For statement (1): If two elements of N are $\text{Aut}(G)$ -conjugate, then they are also $\text{Aut}(N)$ -conjugate (or, equivalently, $\text{Aut}(N)$ -orbits on N are unions of $\text{Aut}(G)$ -orbits on N). In particular, $\omega_o(G) \geq \omega_o(N)$ for each $o \in \text{Ord}(N) \subseteq \text{Ord}(G)$. It follows that

$$\mathfrak{d}(G) = \sum_{o \in \text{Ord}(G)} (\omega_o(G) - 1) \geq \sum_{o \in \text{Ord}(N)} (\omega_o(G) - 1) \geq \sum_{o \in \text{Ord}(N)} (\omega_o(N) - 1) = \mathfrak{d}(N),$$

as required.

For statement (2): For a group H and a positive integer o , we denote the set of order o elements in H by H_o . By definition, $\mathfrak{m}(G/N)$ is the maximum value of $\omega_{\bar{o}}(G/N)$ where \bar{o} ranges over the element orders of G/N . So the goal will be to show that $\omega_{\bar{o}}(G/N) \leq 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$ for all $\bar{o} \in \text{Ord}(G/N)$. Consider the following two conditions on such an \bar{o} :

- (1) There is a set $M_{\bar{o}}$ of $\text{Aut}(G)$ -orbits on G with $|M_{\bar{o}}| \leq 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$ such that for each $\bar{x} \in (G/N)_{\bar{o}}$, there is a lift x of \bar{x} in G such that x lies in one of the orbits from $M_{\bar{o}}$.
- (2) There is a set $N_{\bar{o}}$ of positive integers with $|N_{\bar{o}}| \leq 2^{\mathfrak{d}(G)}$ such that each $\bar{x} \in (G/N)_{\bar{o}}$ admits a lift x in G such that $\text{ord}(x) \in N_{\bar{o}}$.

Since N is characteristic in G , if two elements of G/N have lifts in the same $\text{Aut}(G)$ -orbit on G , then they are $\text{Aut}(G/N)$ -conjugate, and so the first condition implies that $\omega_{\bar{o}}(G/N) \leq 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$ (which is what we want to show). Moreover, the second condition implies the first, by letting $M_{\bar{o}}$ be the set of all $\text{Aut}(G)$ -orbits on G consisting of elements whose order lies in $N_{\bar{o}}$ – then by definition of $\mathfrak{d}(G)$, $|M_{\bar{o}}| \leq |N_{\bar{o}}| + \mathfrak{d}(G) \leq 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$.

Hence we will aim at verifying that the second condition holds for all $\bar{o} \in \text{Ord}(G/N)$. So, fix such an \bar{o} , say with prime power factorisation $\bar{o} = p_1^{f_1} \cdots p_s^{f_s}$. Denote by π the canonical projection $G \rightarrow G/N$, and consider the following function $\lambda_{\bar{o}}$, which maps the set $\pi^{-1}[(G/N)_{\bar{o}}]$, of all lifts in G of order \bar{o} elements of G/N , into itself: For $x \in \pi^{-1}[(G/N)_{\bar{o}}]$, let $x = x_1 \cdots x_r$ be the unique (up to reordering the factors) factorisation of x into pairwise commuting elements of pairwise coprime prime-power orders. Since $\pi(x)$ has order \bar{o} , we have that $p_i \mid \text{ord}(x)$ for $i = 1, \dots, s$, so $r \geq s$, and we may assume w.l.o.g. that $\text{ord}(x_i) = p_i^{k_i}$ for some $k_i \in \mathbb{N}^+$ for $i = 1, \dots, s$. Set $\lambda_{\bar{o}}(x) := x_1 \cdots x_s$. Note that $x_{s+1}, \dots, x_r \in N$, and we have

$$\pi(\lambda_{\bar{o}}(x)) = \pi(x), \quad (4.1)$$

which shows in particular that $\lambda_{\bar{o}}(x) \in \pi^{-1}[(G/N)_{\bar{o}}]$, as asserted. We let $X_{\bar{o}}$ denote the set of orders of elements in the image of $\lambda_{\bar{o}}$. By Formula (4.1), each $\bar{x} \in (G/N)_{\bar{o}}$ has a lift in $\text{im}(\lambda_{\bar{o}})$, and thus a lift with order in $X_{\bar{o}}$. It remains to show that $|X_{\bar{o}}| \leq 2^{\mathfrak{d}(G)}$.

For $i \in \{1, \dots, s\}$, let $t_i \in \mathbb{N}^+$ be maximal subject to $p_i^{t_i} \in \text{Ord}(N)$, and let u_i be the number of distinct p_i -adic valuations of $\text{ord}(x^{p_i^{f_i}})$ where x ranges over $\text{im}(\lambda_{\bar{o}})$; hence by definition, $|X_{\bar{o}}| \leq \prod_{i=1}^s u_i$. Note that $u_i \leq t_i + 1$, since the p_i -part of $x^{p_i^{f_i}}$ is (by definition of f_i) always an element of N . Observe also that for a fixed i , as long as each of the subsets $G_1, G_{p_i}, G_{p_i^2}, \dots, G_{p_i^{t_i}} \subseteq G$ is a single $\text{Aut}(G)$ -orbit (which must hold for all but at most $\mathfrak{d}(G)$ of the indices $i \in \{1, \dots, s\}$), then the argument in [61, proof of Lemma 1.1] gives that the p_i -adic valuation of $\text{ord}(x)$ is $f_i + t_i$ for all $x \in \text{im}(\lambda_{\bar{o}})$, and so $u_i = 1$. Let the number of indices $i \in \{1, \dots, s\}$ for which this is not the case be e , and let these e “exceptional” indices be w.l.o.g. just $1, \dots, e$. Note

that if $e = 0$, then $u_i = 1$ for all $i \in \{1, \dots, s\}$, so that

$$\prod_{i=1}^s u_i = 1 \leq 2^{\mathfrak{d}(G)},$$

as required. We may thus assume that $e \geq 1$. Moreover, we claim that

$$\sum_{i=1}^s (u_i - 1) = \sum_{i=1}^e (u_i - 1) \leq \mathfrak{d}(G). \quad (4.2)$$

Indeed, the equality in Formula (4.2) is clear by the above remark that $i \in \{1, \dots, s\}$ not being among the e exceptional indices $1, \dots, e$ implies that $u_i = 1$. As for the inequality in Formula (4.2), we will argue as follows: Consider the set \mathcal{M} , of all pairs (i, m) such that

- $i \in \{1, \dots, e\}$,
- $m \in \{0, \dots, t_i - 1\}$, and
- there exists $x \in \text{im}(\lambda_{\bar{\sigma}})$ such that $\nu_{p_i}(\text{ord}(x^{p_i^{f_i}})) = m$.

Note that if the second condition in the definition of \mathcal{M} was replaced by “ $m \in \{0, \dots, t_i\}$ ”, then by definition of t_i and u_i , the cardinality of \mathcal{M} would be $\sum_{i=1}^e u_i$; excluding the possibility $m = t_i$ removes at most one pair (i, m) for each i , and so the actual cardinality of \mathcal{M} is bounded from below by $\sum_{i=1}^e (u_i - 1)$. Consider the injective function $f : \mathcal{M} \rightarrow \mathbb{N}^+$, $(i, m) \mapsto p_i^{m+1}$. Observe that the image of f consists of element orders $o \in \text{Ord}(G)$ such that G contains elements of order o both inside and outside of N (the former since $m + 1 \leq t_i$, and the latter by considering the p_i -part of $x^{p_i^{f_i-1}}$ where x is as in the third bullet point of the definition of \mathcal{M} above). In particular, $\omega_o(G) \geq 2$ for each such o , and thus

$$\mathfrak{d}(G) = \sum_{o \in \text{Ord}(G)} (\omega_o(G) - 1) \geq |\text{im}(f)| \geq |\mathcal{M}| \geq \sum_{i=1}^e (u_i - 1),$$

as asserted. Using the now established Formula (4.2) and the inequality of arithmetic and geometric means, we deduce that

$$|X_{\bar{\sigma}}| \leq \prod_{i=1}^s u_i = \prod_{i=1}^e u_i \leq \left(\frac{\sum_{i=1}^e u_i}{e} \right)^e \leq \left(\frac{\mathfrak{d}(G) + e}{e} \right)^e = \left(\frac{\mathfrak{d}(G)}{e} + 1 \right)^e. \quad (4.3)$$

Now for each real number $y \geq 1$, we have $2^y \geq y + 1$. Applied with $y := \mathfrak{d}(G)/e$ (using that $e \leq \mathfrak{d}(G)$ by definition of e), we get that

$$\frac{\mathfrak{d}(G)}{e} + 1 \leq 2^{\mathfrak{d}(G)/e},$$

or equivalently,

$$\left(\frac{\mathfrak{d}(G)}{e} + 1 \right)^e \leq 2^{\mathfrak{d}(G)},$$

which together with Formula (4.3) implies that $|X_{\bar{\sigma}}| \leq 2^{\mathfrak{d}(G)}$ and thus concludes the proof. \square

Note that by applying Lemma 4.1(2) with $N := \text{Rad}(G)$, the soluble radical of G , we get in particular that $\mathfrak{m}(G/\text{Rad}(G)) \leq 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$. Since we want to bound the index $|G : \text{Rad}(G)|$, i.e., the order of the group $G/\text{Rad}(G)$, in terms of $\mathfrak{d}(G)$, and since $G/\text{Rad}(G)$ is always semisimple, our next goal will be to bound the order of a finite semisimple group H in terms of $\mathfrak{m}(H)$. Consider the following simple bound:

Lemma 4.2. *Let G be a finite group, and let N be a characteristic subgroup of G . Then $\mathfrak{m}(N) \leq \mathfrak{m}(G)$.*

Proof. For each $o \in \text{Ord}(N)$ we have $\omega_o(N) \leq \omega_o(G)$ (as was already observed in the proof of Lemma 4.1(1)), and so

$$\begin{aligned} \mathfrak{m}(G) &= \max\{\omega_o(G) \mid o \in \text{Ord}(G)\} \geq \max\{\omega_o(G) \mid o \in \text{Ord}(N)\} \\ &\geq \max\{\omega_o(N) \mid o \in \text{Ord}(N)\} = \mathfrak{m}(N), \end{aligned}$$

as required. □

By Lemma 4.2, $\mathfrak{m}(\text{Soc}(H)) \leq \mathfrak{m}(H)$. Hence if we can bound $|\text{Soc}(H)|$ by a monotonically increasing function in $\mathfrak{m}(\text{Soc}(H))$, then $|\text{Soc}(H)|$ is also bounded in terms of $\mathfrak{m}(H)$, and this implies that $|H|$ is bounded in terms of $\mathfrak{m}(H)$, because H embeds into $\text{Aut}(\text{Soc}(H))$ (see e.g. [51, Lemma 1.1]). Since we know by [50, 3.3.18, p. 89] that $\text{Soc}(H)$ is isomorphic to a direct product of nonabelian finite simple groups, the following will be useful:

Lemma 4.3. *Let S_1, \dots, S_r be pairwise nonisomorphic nonabelian finite simple groups, and let $n_1, \dots, n_r \in \mathbb{N}^+$. Then $\mathfrak{m}(S_1^{n_1} \times \dots \times S_r^{n_r}) \geq \prod_{i=1}^r (n_i \cdot \mathfrak{m}(S_i))$.*

Proof. First note that if two elements in $S_i^{n_i}$ have a different number of nontrivial entries, then they lie in different orbits of $\text{Aut}(S_i^{n_i}) = \text{Aut}(S_i) \wr \text{Sym}(n_i)$. Thus for each element order o_i of S_i , there are at least $n_i \cdot \omega_{o_i}(S_i)$ many $\text{Aut}(S_i^{n_i})$ -orbits on the set of elements of $S_i^{n_i}$ of order o_i . Now for each $i \in \{1, \dots, r\}$, let o_i be an element order of S_i such that $\omega_{o_i}(S_i)$ is as large as possible, that is, $\omega_{o_i}(S_i) = \mathfrak{m}(S_i)$. Observe that

$$\text{Aut}(S_1^{n_1} \times \dots \times S_r^{n_r}) = \text{Aut}(S_1^{n_1}) \times \dots \times \text{Aut}(S_r^{n_r}),$$

and so if there is an $i \in \{1, \dots, r\}$ such that the projections of two elements $g, h \in S_1^{n_1} \times \dots \times S_r^{n_r}$ to the i -th component $S_i^{n_i}$ lie in different $\text{Aut}(S_i^{n_i})$ -orbits, then g, h lie in different $\text{Aut}(S_1^{n_1} \times \dots \times S_r^{n_r})$ -orbits. Thus letting $o := \text{lcm}(o_1, \dots, o_r)$, we see that $o \in \text{Ord}(S_1^{n_1} \times \dots \times S_r^{n_r})$ and

$$\omega_o(S_1^{n_1} \times \dots \times S_r^{n_r}) \geq \prod_{i=1}^r (n_i \mathfrak{m}(S_i)).$$

Hence the lower bound in the statement holds. □

We are now ready for the

Proof of Theorem 1.1.2(1). Let G be an arbitrary finite group. By Lemma 4.1(2), applied with $N := \text{Rad}(G)$, we find that $\mathfrak{m}(G/\text{Rad}(G)) \leq 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$. Set $H := G/\text{Rad}(G)$. Write $\text{Soc}(H) = S_1^{n_1} \times \cdots \times S_r^{n_r}$ where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$. Then by combining the above and Lemmas 4.2 and 4.3, we get

$$2^{\mathfrak{d}(G)} + \mathfrak{d}(G) \geq \mathfrak{m}(H) \geq \mathfrak{m}(\text{Soc}(H)) \geq \prod_{i=1}^r (n_i \cdot \mathfrak{m}(S_i)) \geq \max\{n_i, \mathfrak{m}(S_i) \mid i = 1, \dots, r\}. \quad (4.4)$$

Hence for each $i \in \{1, \dots, r\}$, we have

$$n_i \leq 2^{\mathfrak{d}(G)} + \mathfrak{d}(G), \quad (4.5)$$

and, setting $c' := \frac{\log \log(413/73)}{\log \log |M|} \approx 0.11404$ as in Theorem 1.1.3(5), where M is the Fischer-Griess Monster group, we have

$$\exp(\log^{c'} |S_i|) - 3 \leq \mathfrak{q}(S_i) \leq \mathfrak{m}(S_i) \leq \mathfrak{m}(\text{Soc}(H)) \leq 2^{\mathfrak{d}(G)} + \mathfrak{d}(G). \quad (4.6)$$

Indeed, for the first inequality in Formula (4.6), note that by Theorem 1.1.3(5),

$$\epsilon_{\mathfrak{q}}(S_i) \geq \epsilon_{\mathfrak{q}}(M) = c',$$

where $\epsilon_{\mathfrak{q}}(S)$ is as defined in Formula (1.1.1). Hence, using the said definition of $\epsilon_{\mathfrak{q}}$,

$$\frac{\log \log (\mathfrak{q}(S_i) + 3)}{\log \log |S_i|} \geq c',$$

or equivalently,

$$\log \log (\mathfrak{q}(S_i) + 3) \geq c' \log \log |S_i|,$$

and by applying \exp to both sides twice, one obtains the first inequality in Formula (4.6). The second inequality in Formula (4.6) follows from the definitions of \mathfrak{q} and \mathfrak{m} , see Definition 1.1.1(4) and also the first sentence after Definition 1.1.1(4). The third inequality in Formula (4.6) is by Lemma 4.3, and the last inequality in Formula (4.6) follows from the first two inequalities in Formula (4.4).

Using Formula (4.6), and noting that the value of c from the statement of Theorem 1.1.2 is just $1/c'$, we conclude that

$$|S_i| \leq \exp(\log^c (2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3)). \quad (4.7)$$

In view of Formula (4.7) and Kohl's bound $|\text{Out}(S_i)| \leq \log_2 |S_i|$ from [38] already used at the beginning of Subsection 3.3, we deduce that

$$|\text{Aut}(S_i)| \leq |S_i| \cdot \log_2 |S_i| \leq \exp(\log^c (2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3)) \cdot \frac{\log^c (2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3)}{\log 2} \quad (4.8)$$

Combining Formulas (4.5) and (4.8), we obtain, still for all $i = 1, \dots, r$,

$$|\text{Aut}(S_i)^{n_i}| \leq$$

$$\exp((2^{\mathfrak{d}(G)} + \mathfrak{d}(G)) \log^c(2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3)) \cdot (\log^{-1} 2 \cdot (2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3))^{2^{\mathfrak{d}(G)} + \mathfrak{d}(G)}. \quad (4.9)$$

Recall from above that S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups. For each $m \in \mathbb{N}^+$, there are at most m isomorphism types of nonabelian finite simple groups of order at most m , because all nonabelian finite simple groups are of even order, and for each given $k \in \mathbb{N}^+$, there are at most two nonisomorphic nonabelian finite simple groups of order k . In particular, in view of Formula (4.7), we have

$$r \leq \exp(\log^c(2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3)). \quad (4.10)$$

Formulas (4.9) and (4.10) yield

$$\begin{aligned} |H \cap (\text{Aut}(S_1)^{n_1} \times \cdots \times \text{Aut}(S_r)^{n_r})| &\leq |\text{Aut}(S_1)^{n_1} \times \cdots \times \text{Aut}(S_r)^{n_r}| \leq \\ &\exp((2^{\mathfrak{d}(G)} + \mathfrak{d}(G)) \log^c(2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3) \exp(\log^c(2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3))) \cdot \\ &(\log^{-1} 2 \cdot (2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3))^{(2^{\mathfrak{d}(G)} + \mathfrak{d}(G)) \exp(\log^c(2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3))}. \end{aligned} \quad (4.11)$$

Moreover, since $H/(H \cap (\text{Aut}(S_1)^{n_1} \times \cdots \times \text{Aut}(S_r)^{n_r}))$ embeds into $\text{Sym}(n_1) \times \cdots \times \text{Sym}(n_r)$, Formulas (4.5) and (4.10) imply that

$$|H : (H \cap (\text{Aut}(S_1)^{n_1} \times \cdots \times \text{Aut}(S_r)^{n_r}))| \leq ((2^{\mathfrak{d}(G)} + \mathfrak{d}(G))!)^{\exp(\log^c(2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3))}. \quad (4.12)$$

Together, Formulas (4.11) and (4.12) yield that

$$\begin{aligned} |G : \text{Rad}(G)| &= |H| \leq \\ &\exp((2^{\mathfrak{d}(G)} + \mathfrak{d}(G)) \log^c(2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3) \exp(\log^c(2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3))) \cdot \\ &(\log^{-1} 2 \cdot (2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3))^{(2^{\mathfrak{d}(G)} + \mathfrak{d}(G)) \exp(\log^c(2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3))} \cdot \\ &((2^{\mathfrak{d}(G)} + \mathfrak{d}(G))!)^{\exp(\log^c(2^{\mathfrak{d}(G)} + \mathfrak{d}(G) + 3))}, \end{aligned}$$

which is what we needed to show. \square

5 Proof of Theorem 1.1.2(2)

5.1 Reduction to semisimple groups

We first make the following observation, which allows us to restrict our attention to finite *semisimple* groups (recall that these are by definition groups without nontrivial soluble normal subgroups, or, equivalently, with trivial soluble radical):

Remark 5.1.1. We claim that the following are equivalent:

- (1) The existence of a function $f_2 : [0, \infty)^2 \rightarrow [1, \infty)$ that is monotonically increasing in both variables and such that $|G : \text{Rad}(G)| \leq f_2(\mathfrak{q}(G), \mathfrak{o}(\text{Rad}(G)))$ for all finite groups G , as asserted by Theorem 1.1.2(2).
- (2) The existence of a monotonically increasing function $\mathfrak{g} : [1, \infty) \rightarrow [1, \infty)$ such that $|H| \leq \mathfrak{g}(\mathfrak{q}(H))$ for all finite semisimple groups H .

Indeed, assuming the first statement and aiming at deriving the second, just observe that for each finite semisimple group H , since $\text{Rad}(H) = \{1_H\}$,

$$|H| = |H : \text{Rad}(H)| \leq f_2(\mathfrak{q}(H), \mathfrak{o}(\text{Rad}(H))) = f_2(\mathfrak{q}(H), 1),$$

so one may choose $\mathfrak{g}(x) := f_2(x, 1)$ in the second statement.

On the other hand, assuming the second statement, we can infer the first as follows: Let G be an arbitrary finite group. Observe that

$$\mathfrak{o}(G) \leq \mathfrak{o}(\text{Rad}(G)) \cdot \mathfrak{o}(G/\text{Rad}(G)),$$

and

$$\omega(G) \geq \omega(G/\text{Rad}(G)).$$

It follows that

$$\mathfrak{q}(G) = \frac{\omega(G)}{\mathfrak{o}(G)} \geq \frac{\omega(G/\text{Rad}(G))}{\mathfrak{o}(\text{Rad}(G)) \mathfrak{o}(G/\text{Rad}(G))} = \frac{\mathfrak{q}(G/\text{Rad}(G))}{\mathfrak{o}(\text{Rad}(G))},$$

or equivalently,

$$\mathfrak{q}(G/\text{Rad}(G)) \leq \mathfrak{q}(G) \cdot \mathfrak{o}(\text{Rad}(G)).$$

Applying the assumed second statement with $H := G/\text{Rad}(G)$, we get that

$$|G : \text{Rad}(G)| = |G/\text{Rad}(G)| \leq \mathfrak{g}(\mathfrak{q}(G/\text{Rad}(G))) \leq \mathfrak{g}(\mathfrak{q}(G) \cdot \mathfrak{o}(\text{Rad}(G))).$$

Hence (and since $\min\{\mathfrak{q}(G), \mathfrak{o}(\text{Rad}(G))\} \geq 1$ for all finite groups G),

$$f_2(x, y) := \begin{cases} 1, & \text{if } \min\{x, y\} < 1, \\ \mathfrak{g}(x \cdot y), & \text{if } \min\{x, y\} \geq 1 \end{cases}$$

is a suitable choice for the function in the first statement. This proves the claim.

In the rest of this section, we will be concerned with proving the second statement in Remark 5.1.1, so we will primarily be concerned with finite *semisimple* groups only.

5.2 Two lemmas for working with partitions

Given a finite group G , rather than determining $\omega(G)$ and bounding $\mathfrak{o}(G)$ directly, it may be easier to determine corresponding parameters for each subset $M \subseteq G$ belonging to a suitable, fixed partition \mathfrak{P} of G (i.e., to a family of *nonempty*, pairwise disjoint subsets of G that cover G). In this subsection, we present two simple, but important lemmas for deriving information on $\mathfrak{q}(G)$ using such an approach. First, we extend the notations $\omega(G)$ and $\mathfrak{o}(G)$ to subsets of G :

Notation 5.2.1. Let G be a finite group and $M \subseteq G$.

- (1) We denote by $\omega_G(M)$ the number of $\text{Aut}(G)$ -orbits on G whose intersection with M is nonempty.

- (2) We denote by $\text{Ord}_G(M)$ (or simply $\text{Ord}(M)$, see below) the set of distinct orders of elements of M and we define $\text{o}_G(M)$ (also usually simplified to $\text{o}(M)$, see below) as $|\text{Ord}_G(M)|$.
- (3) We set $\mathfrak{q}_G(M) := \frac{\omega_G(M)}{\text{o}_G(M)}$.

We note that while the concept $\text{Ord}_G(M)$ (and, likewise, $\text{o}_G(M)$) does depend on G to the extent that G provides the algebraic structure (which M itself, being only a set, is lacking) to make talking about the “order of an element of M ” meaningful, it does have the property that if $M \subseteq G_1 \leq G_2$ for a finite group G_2 , then $\text{Ord}_{G_1}(M) = \text{Ord}_{G_2}(M)$. So as long as the context of discussion provides a “natural” smallest finite group into which the given finite set M embeds (which will always be the case in our paper), we can and will omit the subscript G in $\text{Ord}_G(M)$ and $\text{o}_G(M)$. On the other hand, the subscript G will *always* be included in the notations $\omega_G(M)$ and $\mathfrak{q}_G(M)$ for the sake of necessity.

Lemma 5.2.2. *Let G be a finite group, let $M \subseteq G$, and let \mathfrak{P} be a partition of M into $\text{Aut}(G)$ -invariant subsets. Then $\mathfrak{q}_G(M) \geq \min\{\mathfrak{q}_G(N) \mid N \in \mathfrak{P}\}$.*

Proof. As each $N \in \mathfrak{P}$ is $\text{Aut}(G)$ -invariant, we have $\omega_G(M) = \sum_{N \in \mathfrak{P}} \omega_G(N)$. Moreover, $\text{o}(M) \leq \sum_{N \in \mathfrak{P}} \text{o}(N)$, since the $N \in \mathfrak{P}$ cover M . Setting $c := \min\{\mathfrak{q}_G(N) \mid N \in \mathfrak{P}\}$, it follows that

$$\mathfrak{q}_G(M) = \frac{\omega_G(M)}{\text{o}(M)} \geq \frac{\sum_{N \in \mathfrak{P}} \omega_G(N)}{\sum_{N \in \mathfrak{P}} \text{o}(N)} \geq \frac{\sum_{N \in \mathfrak{P}} c \text{o}(N)}{\sum_{N \in \mathfrak{P}} \text{o}(N)} = c,$$

as required. □

We will be applying Lemma 5.2.2 in the special case where G is a finite semisimple group. With $M := G$, Lemma 5.2.2 says in particular that if we can find a partition of G into $\text{Aut}(G)$ -invariant subsets each of which has “large” \mathfrak{q}_G -value, then $\mathfrak{q}_G(G) = \mathfrak{q}(G)$ will be large. However, sometimes it is easier to consider partitions where not every partition member has large \mathfrak{q}_G -value, forcing us to distinguish between “good” and “bad” partition members. The following lemma basically says that as long as the total number of element orders in the “bad” partition members is suitably bounded from above, one may still produce a useful lower bound on $\mathfrak{q}(G)$ from such a “mixed” partition:

Lemma 5.2.3. *Let G be a finite group, let $M \subseteq G$, and let $\mathfrak{P} = \{M_{\text{good}}, M_{\text{bad}}\}$ be a partition of M into two distinct (nonempty) $\text{Aut}(G)$ -invariant subsets. Then*

$$\mathfrak{q}_G(M) \geq \frac{\mathfrak{q}_G(M_{\text{good}})}{1 + \text{o}(M_{\text{bad}})}.$$

Proof. Since $M_{\text{good}} \neq \emptyset$, we have $\text{o}(M_{\text{good}}) \geq 1$, and therefore

$$\text{o}(M) \leq \text{o}(M_{\text{good}}) + \text{o}(M_{\text{bad}}) \leq (1 + \text{o}(M_{\text{bad}})) \text{o}(M_{\text{good}}).$$

Furthermore,

$$\omega_G(M) = \omega_G(M_{\text{good}}) + \omega_G(M_{\text{bad}}) \geq \omega_G(M_{\text{good}}),$$

and so

$$\mathfrak{q}_G(M) = \frac{\omega_G(M)}{\mathfrak{o}(M)} \geq \frac{\omega_G(M_{\text{good}})}{(1 + \mathfrak{o}(M_{\text{bad}})) \mathfrak{o}(M_{\text{good}})} = \frac{\mathfrak{q}_G(M_{\text{good}})}{1 + \mathfrak{o}(M_{\text{bad}})}. \quad \square$$

When using Lemma 5.2.2 to study $\mathfrak{q}(H)$ for finite semisimple groups H , an important partition of H to consider is \mathfrak{P}_H , defined as follows: Say $\text{Soc}(H) = S_1^{n_1} \times \cdots \times S_r^{n_r}$ where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$ (see e.g. [50, 3.3.18, p. 89]). Note that H may be viewed (via its conjugation action on $\text{Soc}(H)$) as a subgroup of

$$\text{Aut}(\text{Soc}(H)) = (\text{Aut}(S_1) \wr \text{Sym}(n_1)) \times \cdots \times (\text{Aut}(S_r) \wr \text{Sym}(n_r)),$$

so that each coset of $\text{Soc}(H)$ in H can be written as $\text{Soc}(H)\vec{\alpha}\vec{\psi}$ where $\vec{\alpha} \in \text{Aut}(S_1)^{n_1} \times \cdots \times \text{Aut}(S_r)^{n_r}$ and $\vec{\psi} \in \text{Sym}(n_1) \times \cdots \times \text{Sym}(n_r)$. Using these notational conventions, we set

$$\begin{aligned} \mathfrak{P}_H := \{ & (\text{Soc}(H)\vec{\alpha}\vec{\psi})^{\text{Aut}(H)} \mid \vec{\alpha} \in \text{Aut}(S_1)^{n_1} \times \cdots \times \text{Aut}(S_r)^{n_r}, \\ & \vec{\psi} \in \text{Sym}(n_1) \times \cdots \times \text{Sym}(n_r), \\ & \vec{\alpha}\vec{\psi} \in H \}. \end{aligned}$$

Equivalently, \mathfrak{P}_H is the unique finest partition of H into subsets that are both $\text{Aut}(H)$ -invariant and unions of cosets of $\text{Soc}(H)$. By applying Lemma 5.2.2 with $G := H$ and $\mathfrak{P} := \mathfrak{P}_H$, we will be able to show that $\mathfrak{q}(H)$ is large if $\max\{\tilde{\mathfrak{q}}(S_i) \mid i = 1, \dots, r\}$ is large (see Lemma 5.4.5(5)), where $\tilde{\mathfrak{q}}(S)$ is a certain parameter associated with each nonabelian finite simple group S , which will be introduced and studied in the next subsection.

5.3 Some auxiliary results on finite simple groups

We begin with the following definition, most of which is taken from [4, Definition 2.2.1]:

Definition 5.3.1. Let S be a nonabelian finite simple group, and let $\pi : \text{Aut}(S) \rightarrow \text{Out}(S)$ be the canonical projection.

- (1) The term *S-type* is a synonym for “ $\text{Out}(S)$ -conjugacy class”.
- (2) For each $\text{Aut}(S)$ -conjugacy class c , we call the element-wise image of c under π the *S-type of c* .
- (3) For each $\alpha \in \text{Aut}(S)$, the *S-type of α* is defined as the *S-type of $\alpha^{\text{Aut}(S)}$* .

S-types played an important role in the first author’s result [4, Lemma 2.2.5(2)], which gave an upper bound on the size of a conjugacy class in a finite semisimple group and which is based on James and Kerber’s characterisation of conjugacy in wreath products of the form $G \wr \text{Sym}(n)$ [37, Theorem 4.2.8, p. 141]. Likewise, we will use James and Kerber’s result to give, for each finite semisimple group H and each coset C of $\text{Soc}(H)$ in H , bounds on $\omega_H(C)$, $\mathfrak{o}(C)$ and $\mathfrak{q}_H(C)$, see Lemma 5.4.5(2,4,5). These bounds will also involve *S*-types, and one of the (lower) bounds on $\mathfrak{q}_H(C)$ from Lemma 5.4.5(5) will also involve the parameters $\tilde{\mathfrak{q}}(S)$ for nonabelian finite simple groups S , defined as follows:

Notation 5.3.2. Let S be a nonabelian finite simple group.

- (1) We set $\tilde{\omega}(S) := \min\{\omega_{\text{Aut}(S)}(S\alpha) \mid \alpha \in \text{Aut}(S)\}$ and $\tilde{q}(S) := \min\{q_{\text{Aut}(S)}(S\alpha) \mid \alpha \in \text{Aut}(S)\}$.
- (2) For each S -type τ , denote by $\alpha(\tau)$ some fixed automorphism of S such that $\alpha(\tau)^{\text{Aut}(S)}$ has S -type τ , and set $\omega(\tau) := \omega_{\text{Aut}(S)}(S\alpha(\tau))$ and $o(\tau) := o(S\alpha(\tau))$ (note that $\omega(\tau)$ and $o(\tau)$ do not depend on the choice of $\alpha(\tau)$).

For later reference, we note the following:

Lemma 5.3.3. *For every nonabelian finite simple group S , $\tilde{\omega}(S) \geq 2$.*

Proof. By [4, Lemma 2.4.2(1)], for each $\alpha \in \text{Aut}(S)$, the size of the intersection of $S\alpha$ with any $\text{Aut}(S)$ -conjugacy class is at most $\frac{18}{19}|S|$; in particular, $S\alpha$ is never fully contained in a single $\text{Aut}(S)$ -conjugacy class. Hence $\omega_{\text{Aut}(S)}(S\alpha) \geq 2$ for all $\alpha \in \text{Aut}(S)$, which by definition of $\tilde{\omega}(S)$ entails that $\tilde{\omega}(S) \geq 2$. \square

We note that the bound in Lemma 5.3.3 is optimal, as

$$\tilde{\omega}(\text{Alt}(6)) = \omega_{\text{Aut}(\text{Alt}(6))}(\text{M}_{10} \setminus \text{Alt}(6)) = 2.$$

As noted above, the parameter $\tilde{q}(S)$ from Notation 5.3.2 will appear in a lower bound in Lemma 5.4.5(5), and thus we will be interested in knowing for which nonabelian finite simple groups S this parameter is large. To state a corresponding asymptotic result (see Lemma 5.3.7 below), we need some more preparation, including the following notation, which is motivated by [32, Propositions 4.1 and 4.2] and part of which already appeared in [32]:

Notation 5.3.4. Let S be a nonabelian finite simple group, and let $\alpha \in \text{Aut}(S)$. We introduce the following numerical parameters $f(S)$ and $g(\alpha)$:

- (1) If S is isomorphic to some alternating or sporadic finite simple group, we set $f(S) := 1$ and $g(\alpha) := 1$.
- (2) If S is not isomorphic to any alternating or sporadic finite simple group, then S is in particular of Lie type, so as in Section 2, we can write $S = \text{O}^{p'}(\overline{S}_\sigma)$ where $\overline{S} = X_d(\overline{\mathbb{F}}_p)$ is a simple linear algebraic group of adjoint type and σ is a Lang-Steinberg endomorphism of \overline{S} . We then set $f(S) := 6f(\sigma)$, where $f(\sigma)$ is as in the paragraph on simple Lie type groups in Section 2 (i.e., $f(\sigma)$ is the f in the notation $S = {}^tX_d(p^{ft})$). As for $g(\alpha)$:
 - (a) Assume that $X_d \notin \{B_2, F_4, G_2\}$. Then, as explained at the end of Section 2, we can write $\alpha = s\phi\delta$ where s is the inner diagonal, ϕ is the field and δ is the graph component of α , and we set $g(\alpha) := \text{ord}(\phi)$.
 - (b) Assume that $X_d \in \{B_2, F_4, G_2\}$. Then we can write $\alpha = s\phi$ where s is the inner diagonal and ϕ is the graph-field component of α , and we set $g(\alpha) := \text{ord}(\phi)$.

Moreover, for each S -type τ , we set $g(\tau) := g(\alpha(\tau))$ (which is independent of the choice of $\alpha(\tau)$ as in Notation 5.3.2(2)).

Note that by definition, $f(S)$ and $g(\alpha)$ are always positive integers, and one has that $g(\alpha) \mid f(S)$. The following lemma provides some restrictions, in terms of $g(\alpha)$, on the possible orders of elements of a coset $S\alpha$ where S is a finite simple group of Lie type and $\alpha \in \text{Aut}(S)$ (this will be useful for studying $\tilde{q}(S)$):

Lemma 5.3.5. *Let $S = {}^tX_d(p^{ft})$ be a finite simple group of Lie type, and let $\alpha \in \text{Aut}(S)$. The following hold:*

(1) *If $X_d \in \{B_2, F_4, G_2\}$, then*

$$\text{Ord}(\text{Inndiag}(S)\alpha) \subseteq g(\alpha) \cdot \text{Ord}(\text{Inndiag}({}^tX_d(p^{f/g(\alpha)t}))).$$

(2) *If $X_d \notin \{B_2, F_4, G_2\}$, then*

$$\text{Ord}(\text{Inndiag}(S)\alpha) \subseteq g(\alpha) \cdot \text{Ord}(\text{Inndiag}({}^uX_d(p^{(f/g(\alpha))\cdot v}))),$$

where, denoting by t' the order of the graph component of α ,

$$(u, v) = \begin{cases} (1, 1), & \text{if } t = t' = 1, \\ (1, 1), & \text{if } t = 1, t' > 1, t' \nmid g(\alpha), \\ (t', t'), & \text{if } t = 1, t' > 1, t' \mid g(\alpha), \\ (t, t), & \text{if } t > 1, t \nmid g(\alpha), \\ (1, t), & \text{if } t > 1, t \mid g(\alpha). \end{cases}$$

Proof. Statement (1) as well as the first four cases in statement (2) follow from [4, Proposition 2.4.3] (more precisely, the properties of the Lang-Steinberg endomorphism μ mentioned there and which fixes $\alpha^g = \alpha^{g(\alpha)}$), which is really just a more detailed version of [32, Propositions 4.1 and 4.2].

In the last case in statement (2), i.e., when $t > 1$ and $t \mid g(\alpha)$, neither [4, Proposition 2.4.3] nor [32, Propositions 4.1 and 4.2] explicitly mention a Lang-Steinberg endomorphism fixing $\alpha^{g(\alpha)}$ (or a suitable other power of α), so we resort to an argument from [31, proof of Theorem 2.16, pp. 7678f.] to deal with this case.

More precisely, since S is twisted, it has no (nontrivial) graph automorphisms. In particular, α does not involve any (nontrivial) graph automorphisms, and so we can write an arbitrary element of $\text{Inndiag}(S)\alpha$ as $\delta\phi^{-1}$ where $\delta \in \text{Inndiag}(S)$ and ϕ is a field automorphism of S of order $g(\alpha)$. By [32, proof of Proposition 4.1, Case 4], ϕ is the restriction to S of some untwisted Lang-Steinberg endomorphism of $X_d(\overline{\mathbb{F}_p})$, which we, by abuse of notation, also denote by ϕ , and which satisfies $q(\phi) = p^{ft/g(\alpha)}$ (see the paragraph on Lie type groups in Section 2 for the notation $q(\mu)$ where μ is a Lang-Steinberg endomorphism of a simple linear algebraic group).

By Lang's theorem, there is an $\epsilon \in X_d(\overline{\mathbb{F}_p})$ such that $\epsilon\epsilon^{-\phi} = \delta$. Set $\eta := \epsilon^{-1}(\delta\phi^{-1})^{g(\alpha)}\epsilon$, and note that

$$(\delta\phi^{-1})^{g(\alpha)} = \delta\delta^\phi \dots \delta^{\phi^{g(\alpha)-2}}\delta^{\phi^{g(\alpha)-1}},$$

which implies that

$$\eta^\phi = \epsilon^{-\phi}(\delta^\phi\delta^{\phi^2} \dots \delta^{\phi^{g(\alpha)-1}}\delta^{\phi^{g(\alpha)}})\epsilon^\phi$$

$$\begin{aligned}
 &= \epsilon^{-\phi}(\delta^\phi \delta^{\phi^2} \dots \delta^{\phi^{g(\alpha)-1}} \delta) \epsilon^\phi \\
 &= (\epsilon^{-\phi} \delta^{-1})(\delta \delta^\phi \dots \delta^{\phi^{g(\alpha)-1}})(\delta \epsilon^\phi) \\
 &= \epsilon^{-1}(\delta \phi^{-1})^{g(\alpha)} \epsilon = \eta.
 \end{aligned}$$

This shows that η , which is conjugate in $X_d(\overline{\mathbb{F}_p})$ to $(\delta \phi^{-1})^{g(\alpha)}$ and thus has order $\frac{1}{g(\alpha)} \text{ord}(\delta \phi^{-1})$, lies in $(X_d(\overline{\mathbb{F}_p}))_\phi$, which, since ϕ is untwisted and has q -value $p^{ft/g(\alpha)}$, is isomorphic to $\text{Inndiag}(X_d(p^{ft/g(\alpha)}))$. Since $\delta \phi^{-1}$ was an arbitrary element of $\text{Inndiag}(S)\alpha$, we are done. \square

We will not need the full level of detail of Lemma 5.3.5; in fact, the following weaker version of it will suffice for our purposes:

Lemma 5.3.6. *Let $S = {}^t X_d(p^{ft})$ be a finite simple group of Lie type, and let $\alpha \in \text{Aut}(S)$. Then there exists $t' \in \{1, 2, 3\}$ such that*

$$\begin{aligned}
 &\text{Ord}(\text{Inndiag}(S)\alpha) \subseteq \\
 &g(\alpha) \cdot \begin{cases} \text{Ord}(\text{Inndiag}({}^t X_d(p^{(f/g(\alpha))t'}))), & \text{if } t = 1 \text{ or } X_d \in \{B_2, F_4, G_2\} \text{ or } t \nmid g(\alpha), \\ \text{Ord}(\text{Inndiag}({}^t X_d(p^{(tf/g(\alpha))t'}))), & \text{else.} \end{cases}
 \end{aligned}$$

\square

At last, we are now able to state and prove the following asymptotic result on the parameter $\tilde{q}(S)$ defined in Notation 5.3.2(1):

Lemma 5.3.7. *The following hold:*

- (1) As $m \rightarrow \infty$,
 - (a) $\tilde{q}(\text{Alt}(m)) \rightarrow \infty$, and
 - (b) $\min_{\alpha \in \text{Aut}(\text{Alt}(m))} \frac{\log \omega_{\text{Aut}(\text{Alt}(m))}(S\alpha)}{\log o(S\alpha)} \rightarrow \infty$.
- (2) Let $S = \text{O}^{p'}(X_d(\overline{\mathbb{F}_p})_\sigma) = {}^{t(\sigma)} X_d(p^{f(\sigma)t(\sigma)})$ be a finite simple group of Lie type, where σ is a Lang-Steinberg endomorphism of $X_d(\overline{\mathbb{F}_p})$, and let $\alpha \in \text{Aut}(S)$. Then as $\max\{p, d, f(\sigma)/g(\alpha)\} \rightarrow \infty$,
 - (a) $\mathfrak{q}_{\text{Aut}(S)}(S\alpha) \rightarrow \infty$, and
 - (b) $\frac{\log \omega_{\text{Aut}(S)}(S\alpha)}{\log(o(S\alpha)+1)} \rightarrow \infty$.

In particular, $\tilde{q}(S) \rightarrow \infty$ as $\max\{p, d\} \rightarrow \infty$.

Proof. For statement (1): We may assume throughout that $m \geq 7$, so that $\text{Aut}(\text{Alt}(m)) = \text{Sym}(m)$ and there are exactly two cosets of $\text{Alt}(m)$ in $\text{Aut}(\text{Alt}(m))$. Note that as $m \rightarrow \infty$,

$$\min_{\alpha \in \text{Sym}(m)} o(\text{Alt}(m)\alpha) \rightarrow \infty,$$

and so statement (1,a) follows from statement (1,b), because statement (1,b) implies that for sufficiently large m and all $\alpha \in \text{Sym}(m)$,

$$\omega_{\text{Sym}(m)}(\text{Alt}(m)\alpha) \geq o(\text{Alt}(m)\alpha)^2,$$

or equivalently,

$$\mathfrak{q}_{\text{Sym}(m)}(\text{Alt}(m)\alpha) \geq \mathfrak{o}(\text{Alt}(m)\alpha).$$

We will thus restrict our attention to showing statement (1,b). It is clear by Theorem 1.1.3(3) that

$$\frac{\log \omega(\text{Alt}(m))}{\log \mathfrak{o}(\text{Alt}(m))} \rightarrow \infty$$

as $m \rightarrow \infty$, which deals with the case $\alpha \in S = \text{Alt}(m)$, so consider the nontrivial coset $\text{Sym}(m) \setminus \text{Alt}(m)$. Recall from Section 3 that for a finite group G , $k(G)$ denotes the number of conjugacy classes of G . By [16, Formula (1.5), p. 90],

$$k(\text{Alt}(m)) \sim \frac{1}{2} k(\text{Sym}(m)),$$

so for sufficiently large m ,

$$\omega(\text{Alt}(m)) \leq k(\text{Alt}(m)) \leq \frac{2}{3} k(\text{Sym}(m)) = \frac{2}{3} \omega(\text{Sym}(m)).$$

Hence, using Formula (3.2.1) and recalling that $p(m)$ denotes the number of ordered integer partitions of m ,

$$\omega_{\text{Sym}(m)}(\text{Sym}(m) \setminus \text{Alt}(m)) \geq \frac{1}{3} \omega(\text{Sym}(m)) = \frac{1}{3} p(m) \sim \frac{1}{12\sqrt{3m}} \exp\left(\frac{2\pi}{\sqrt{6}}\sqrt{m}\right).$$

On the other hand, recalling Formula (3.2.2),

$$\mathfrak{o}(\text{Sym}(m) \setminus \text{Alt}(m)) \leq \mathfrak{o}(\text{Sym}(m)) = \exp\left(\frac{2\pi}{\sqrt{6}}\sqrt{\frac{m}{\log m}} + O\left(\frac{\sqrt{m} \log \log m}{\log m}\right)\right),$$

so clearly, $\omega_{\text{Sym}(m)}(\text{Sym}(m) \setminus \text{Alt}(m))$ grows faster than any power of $\mathfrak{o}(\text{Sym}(m) \setminus \text{Alt}(m))$, which is just what we wanted to show.

For statement (2): For a finite group G , denote by

$$\text{MCS}(G) := \min\{|\mathcal{C}_G(g)| \mid g \in G\}$$

the minimum size of an element centraliser in G . The bounds in [4, Proposition 2.4.4] (which are based on earlier work of Hartley and Kuzucuoğlu from [33, proof of Theorem A1, pp. 319f.]) together with Fulman and Guralnick's bounds from [24, Section 6] are strong enough to show that $\text{MCS}(X_d(\overline{\mathbb{F}}_p)_\mu) \geq q(\mu)^{d/8}$ for any Lang-Steinberg endomorphism μ of $X_d(\overline{\mathbb{F}}_p)$. But by [32, Propositions 4.1 and 4.2], there is a Lang-Steinberg endomorphism μ on $X_d(\overline{\mathbb{F}}_p)$ such that $q(\mu) \geq q(\sigma)^{1/g(\alpha)}$ and for all $s \in S$,

$$|\mathcal{C}_{\text{Aut}(S)}(s\alpha)| \geq g(\alpha) \text{MCS}(X_d(\overline{\mathbb{F}}_p)_\mu) \geq g(\alpha) q(\mu)^{d/8} \geq g(\alpha) q(\sigma)^{d/(8g(\alpha))} = g(\alpha) p^{\frac{d}{8} \cdot \frac{f(\sigma)}{g(\alpha)}},$$

and so

$$|(s\alpha)^{\text{Aut}(S)}| \leq \frac{|\text{Aut}(S)|}{g(\alpha) \cdot p^{\frac{d}{8} \cdot \frac{f(\sigma)}{g(\alpha)}}} \leq \frac{6df(\sigma)|S|}{g(\alpha) \cdot p^{\frac{d}{8} \cdot \frac{f(\sigma)}{g(\alpha)}}} = 6 \frac{df(\sigma)}{g(\alpha)} p^{-\frac{d}{8} \cdot \frac{f(\sigma)}{g(\alpha)}} |S|.$$

Using that $\text{Aut}(S)$ is a complete group, it follows that

$$\omega_{\text{Aut}(S)}(S\alpha) \geq \left(6 \frac{df(\sigma)}{g(\alpha)} p^{-\frac{d}{8} \frac{f(\sigma)}{g(\alpha)}}\right)^{-1} = \frac{p^{\frac{d}{8} \frac{f(\sigma)}{g(\alpha)}}}{6 \frac{df(\sigma)}{g(\alpha)}}.$$

In particular, if $\max\{p, d, f(\sigma)/g(\alpha)\}$ is large enough, then

$$\omega_{\text{Aut}(S)}(S\alpha) \geq p^{\frac{d}{16} \frac{f(\sigma)}{g(\alpha)}},$$

in particular $\omega_{\text{Aut}(S)}(S\alpha) \rightarrow \infty$ as $\max\{p, d, f(\sigma)/g(\alpha)\} \rightarrow \infty$.

What about $o(S\alpha)$? In view of Lemma 5.3.6 and Formula (3.3.4) from Subsection 3.3, as $\max\{p, d, f(\sigma)/g(\alpha)\} \rightarrow \infty$,

$$o(S\alpha) \leq p^{o(1)df(\sigma)/g(\alpha)},$$

so $o(S\alpha)$ does indeed grow more slowly than any power of $\omega_{\text{Aut}(S)}(S\alpha)$ as

$$\max\{p, d, f(\sigma)/g(\alpha)\} \rightarrow \infty,$$

which is just statement (2,b). Statement (2,a) follows from this since therefore, if $\max\{p, d, f(\sigma)/g(\alpha)\}$ is large enough,

$$q_{\text{Aut}(S)}(S\alpha) \geq \sqrt{\omega_{\text{Aut}(S)}(S\alpha)},$$

which also converges to ∞ as $\max\{p, d, f(\sigma)/g(\alpha)\} \rightarrow \infty$. \square

We conclude this subsection with the following lemma concerning q -values of direct products of nonabelian finite simple groups, which will be used in the proof of Lemma 5.8.2:

Lemma 5.3.8. *Let S, S_1, \dots, S_r be nonabelian finite simple groups, $S_i \not\cong S_j$ for $1 \leq i < j \leq r$, and let $n, n_1, \dots, n_r \in \mathbb{N}^+$. Set $T := S_1^{n_1} \times \dots \times S_r^{n_r}$. Then:*

- (1) $q(T) \geq \prod_{i=1}^r q(S_i^{n_i}) \geq \max\{q(S_i^{n_i}) \mid i = 1, \dots, r\}$.
- (2) $q(S^n) \geq q(S)$.
- (3) $q(T) \rightarrow \infty$ as $|T| \rightarrow \infty$.

Proof. For statement (1): Since $\text{Aut}(T) = \text{Aut}(S_1^{n_1}) \times \dots \times \text{Aut}(S_r^{n_r})$, it is clear that $\omega(T) = \prod_{i=1}^r \omega(S_i^{n_i})$, and since every element order in T is a least common multiple over an r -tuple of one element order choice from each $S_i^{n_i}$, it is also clear that $o(T) \leq \prod_{i=1}^r o(S_i^{n_i})$. From this, the first inequality follows, and the second inequality holds because every q -value is at least 1.

For statement (2): It is clear from the fact that $\text{Aut}(S^n) = \text{Aut}(S) \wr \text{Sym}(n)$ that the set of $\text{Aut}(S^n)$ -orbits on S^n is in bijection with the set of cardinality n multisets formed from $\text{Aut}(S)$ -orbits on S , whose total number is by definition $\omega(S)$. Hence

$$\omega(S^n) = \binom{n + \omega(S) - 1}{\omega(S) - 1}. \quad (5.3.1)$$

On the other hand, each element order in S^n can be written as a least common multiple over an n -tuple of element orders in S . In particular, $o(S^n)$ is bounded from above by the number of cardinality n multisets formed from element orders in S , whose total number is by definition $o(S)$. It follows that

$$o(S^n) \leq \binom{n + o(S) - 1}{o(S) - 1}. \quad (5.3.2)$$

Combining Formulas (5.3.1) and (5.3.2), we get

$$\begin{aligned} q(S^n) &= \frac{\omega(S^n)}{o(S^n)} \geq \frac{\binom{n + \omega(S) - 1}{\omega(S) - 1}}{\binom{n + o(S) - 1}{o(S) - 1}} = \frac{\frac{(n + \omega(S) - 1)!}{(\omega(S) - 1)!n!}}{\frac{(n + o(S) - 1)!}{(o(S) - 1)!n!}} = \frac{(n + \omega(S) - 1)!(o(S) - 1)!}{(n + o(S) - 1)!(\omega(S) - 1)!} \\ &= \frac{\omega(S) + n - 1}{o(S) + n - 1} \cdot \frac{\omega(S) + n - 2}{o(S) + n - 2} \cdots \frac{\omega(S) + 1}{o(S) + 1} \cdot \frac{\omega(S)!(o(S) - 1)!}{o(S)!(\omega(S) - 1)!} \\ &\geq 1 \cdot 1 \cdots 1 \cdot \frac{\omega(S)}{o(S)} = q(S), \end{aligned}$$

as required.

For statement (3): By statements (1) and (2) and Theorem 1.1.3(5), it is clear that $q(T)$ is large if T has a large (nonabelian) composition factor, so assume that the orders of the composition factors of T are bounded. Then T contains some small nonabelian finite simple group, say S , with large multiplicity, say n . As already noted in the proof of statement (2), every element order in S^n is a least common multiple over an n -tuple of element orders in S , whose total number is $o(S)$, and so $o(S^n) \leq 2^{o(S)}$, an upper bound which does not depend on n . On the other hand, using Formula (5.3.1) and that $\omega(S) \geq o(S) \geq 4$ by Burnside's $p^a q^b$ -theorem,

$$\omega(S^n) = \binom{n + \omega(S) - 1}{\omega(S) - 1} \geq \binom{n + 3}{3},$$

so that $q(S^n) \rightarrow \infty$ as $n \rightarrow \infty$, and thus $q(T) \rightarrow \infty$ by statement (1). \square

5.4 Gaining some control over socle cosets in finite semisimple groups

Recall Notation 5.2.1. The main purpose of this subsection is to obtain some bounds on the parameters $\omega_H(C)$, $o(C)$ and $q_H(C)$, where H is a finite semisimple group and C is a coset of $\text{Soc}(H)$ in H . This is achieved via Lemma 5.4.5 below, which was already announced in Subsection 5.3 and which will involve the concept of an S -type, see Definition 5.3.1(1). Before being able to formulate Lemma 5.4.5, we will need to introduce quite a few more notations, see Notations 5.4.1, 5.4.2, 5.4.4 and 5.4.3 below:

Notation 5.4.1. Let I be a finite set, and let $\mathcal{F} = (M_i)_{i \in I}$ be a family of finite subsets of \mathbb{N}^+ indexed by the elements of I .

- (1) We denote by $\Lambda(\mathcal{F})$ the set of all numbers of the form $\text{lcm}_{i \in I} a_i$ where $a_i \in M_i$ for $i \in I$.

(2) We set $\lambda(\mathcal{F}) := |\Lambda(\mathcal{F})|$.

For example,

$$\Lambda(\{\{2, 3\}, \{3, 4\}\}) = \{\text{lcm}(2, 3), \text{lcm}(2, 4), \text{lcm}(3, 3), \text{lcm}(3, 4)\} = \{3, 4, 6, 12\},$$

and so $\lambda(\{2, 3\}, \{3, 4\}) = 4$. Note that

$$\lambda((M_i)_{i \in I}) \leq \prod_{i \in I} |M_i|,$$

and that $\Lambda((M_i)_{i \in I}) = \emptyset$ if and only if at least one of the sets M_i is empty; as a small technicality, we note that if $I = \emptyset$, and thus $(M_i)_{i \in I} = \emptyset$, then by definition,

$$\Lambda((M_i)_{i \in I}) = \Lambda(\emptyset) = \{\text{lcm}(\emptyset)\} = \{1\},$$

which is also the only way to define $\Lambda(\emptyset)$ so that Lemma 5.4.5(3) also applies when the semisimple group H in its formulation is trivial.

Notation 5.4.2. Let $n \in \mathbb{N}^+$ and $\psi \in \text{Sym}(n)$. We denote by $\Gamma(\psi)$ the number of distinct cycles of ψ on $\{1, \dots, n\}$ including fixed points.

This notation will mainly be applied to an element $\vec{\psi} = (\psi_1, \dots, \psi_r)$ of the direct product $\prod_{i=1}^r \text{Sym}(n_i)$, and in order to make sense of this, we identify the abstract direct product $\prod_{i=1}^r \text{Sym}(n_i)$ with the subgroup of the symmetric group over the size $\sum_{i=1}^r n_i$ set

$$\bigcup_{i=1}^r (\{i\} \times \{1, \dots, n_i\})$$

which consists of all permutations of the form $(i, j) \mapsto (i, \sigma_i(j))$ for some given element $(\sigma_1, \dots, \sigma_r)$ of the abstract direct product $\prod_{i=1}^r \text{Sym}(n_i)$. Under this identification, $\vec{\psi}$ corresponds to the permutation $(i, j) \mapsto (i, \psi_i(j))$, so that $\Gamma(\vec{\psi}) = \sum_{i=1}^r \Gamma(\psi_i)$ and $\text{ord}(\vec{\psi}) = \text{lcm}(\text{ord}(\psi_1), \dots, \text{ord}(\psi_r))$. Finally, if $C = \text{Soc}(H)\vec{\alpha}\vec{\psi}$ is a socle coset in some finite semisimple group H (with notation as introduced in the paragraph after the proof of Lemma 5.2.3 above), we set $\Gamma(C) := \Gamma(\vec{\psi})$.

Notation 5.4.3. Let Ω be a finite set, let $\psi \in \text{Sym}(\Omega)$, and let $\zeta = (\gamma_1, \dots, \gamma_\ell)$ be an ℓ -cycle of ψ (possibly with $\ell = 1$).

(1) We set $\text{supp}(\zeta) := \{\gamma_1, \dots, \gamma_\ell\}$.

(2) Assume now additionally that S is a nonabelian finite simple group and $\vec{\alpha} = (\alpha_\gamma)_{\gamma \in \Omega} \in \text{Aut}(S)^\Omega$ is a family of automorphisms of S labelled by the elements of Ω . For each $\gamma \in \text{supp}(\zeta)$, we set

$$\text{bcp}_\gamma(\psi, \vec{\alpha}) := \alpha_\gamma \alpha_{\psi^{-1}(\gamma)} \alpha_{\psi^{-2}(\gamma)} \cdots \alpha_{\psi^{-\ell+1}(\gamma)} \in \text{Aut}(S),$$

the *index γ backward cycle product associated with ψ and $\vec{\alpha}$* . Moreover, we set

$$\text{bcpc}_\zeta(\vec{\alpha}) := \text{bcp}_\gamma(\psi, \vec{\alpha})^{\text{Aut}(S)}$$

for any $\gamma \in \text{supp}(\zeta)$, the *backward cycle product class associated with ζ and $\vec{\alpha}$* .

Note that the definition of $\text{bcpc}_\zeta(\vec{\alpha})$ does not depend on the choice of $\gamma \in \text{supp}(\zeta)$, because if $\gamma, \gamma' \in \text{supp}(\zeta)$, then $\text{bcp}_\gamma(\psi, \vec{\alpha})$ and $\text{bcp}_{\gamma'}(\psi, \vec{\alpha})$ are cyclic shifts of each other; in particular, they are conjugate in $\text{Aut}(S)$.

The parameters introduced in the following notation all play a role in Lemma 5.4.5:

Notation 5.4.4. Let $r \in \mathbb{N}^+$, S_1, \dots, S_r be pairwise nonisomorphic nonabelian finite simple groups, let $n_1, \dots, n_r \in \mathbb{N}^+$, and let $\vec{\psi} = (\psi_1, \dots, \psi_r) \in \text{Sym}(n_1) \times \dots \times \text{Sym}(n_r)$ and $\vec{\alpha} = (\vec{\alpha}_1, \dots, \vec{\alpha}_r) \in \text{Aut}(S_1)^{n_1} \times \dots \times \text{Aut}(S_r)^{n_r}$. We view $\vec{\alpha}$ as an array of automorphisms of nonabelian finite simple groups whose entries are labelled by pairs (i, j) with $i \in \{1, \dots, r\}$ and $j \in \{1, \dots, n_i\}$.

- (1) For $i = 1, \dots, r$, we denote by $\vec{\psi}_i$ the permutation of $\{i\} \times \{1, \dots, n_i\}$ mapping $(i, j) \mapsto (i, \psi_i(j))$.
- (2) We say that a triple (i, ℓ, τ) where $i \in \{1, \dots, r\}$, $\ell \in \{1, \dots, n_i\}$ and τ is an S_i -type is $(\vec{\psi}, \vec{\alpha})$ -admissible if and only if for some ℓ -cycle ζ of $\vec{\psi}_i$, $\text{bcpc}_\zeta(\vec{\alpha})$ has S_i -type τ , and each such cycle ζ is called an (i, ℓ, τ) -cycle of $(\vec{\psi}, \vec{\alpha})$.
- (3) We denote by $\text{Adm}(\vec{\psi}, \vec{\alpha})$ the set of all $(\vec{\psi}, \vec{\alpha})$ -admissible triples.
- (4) Assume that $(i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})$.
 - (a) We denote by $\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})$ the number of (i, ℓ, τ) -cycles of $(\vec{\psi}, \vec{\alpha})$.
 - (b) We denote by $\Omega_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})$ the number of multisets with elements from $\{1, \dots, \omega(\tau)\}$ and with cardinality $\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})$, where $\omega(\tau)$ is as in Notation 5.3.2(2).
 - (c) We denote by $\mathcal{O}_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})$ the number of subsets of $\{1, \dots, \omega(\tau)\}$ of cardinality at most $\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})$, where $\omega(\tau)$ is as in Notation 5.3.2(2).
 - (d) We denote by $\mathcal{F}_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})$ the tuple of length $\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})$ whose entries are all equal to the set $\text{Ord}_{\text{Aut}(S_i)}((S_i \alpha(\tau))^{\text{ord}(\vec{\psi})/\ell})$ of orders of $(\text{ord}(\vec{\psi})/\ell)$ -th powers of elements of the coset $S_i \alpha(\tau)$.
 - (e) We set $M_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) := \Lambda(\mathcal{F}_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}))$, where Λ is as in Notation 5.4.1.
 - (f) We set $\mathcal{G}(\vec{\psi}, \vec{\alpha}) := \Lambda((M_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}))_{(i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})})$.

Observe that by definition,

$$\Omega_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) = \binom{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \omega(\tau) - 1}{\omega(\tau) - 1}, \quad (5.4.1)$$

and that $\mathcal{O}_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})$ is bounded from above by the number of multisets with elements from $\{1, \dots, \omega(\tau)\}$ and with cardinality $\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})$, which is

$$\binom{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \omega(\tau) - 1}{\omega(\tau) - 1}.$$

At last, we are able to formulate and prove Lemma 5.4.5, providing bounds on ω_H -, \mathfrak{o} - and \mathfrak{q}_H -values (see Notation 5.2.1) of socle cosets in finite semisimple groups:

Lemma 5.4.5. *Let $r \in \mathbb{N}^+$, S_1, \dots, S_r be pairwise nonisomorphic nonabelian finite simple groups, let $n_1, \dots, n_r \in \mathbb{N}^+$, let H be a finite semisimple group with $\text{Soc}(H) = S_1^{n_1} \times \dots \times S_r^{n_r}$, and let $\vec{\psi} = (\psi_1, \dots, \psi_r) \in \text{Sym}(n_1) \times \dots \times \text{Sym}(n_r)$ and $\vec{\alpha} = (\vec{\alpha}_1, \dots, \vec{\alpha}_r) \in \text{Aut}(S_1)^{n_1} \times \dots \times \text{Aut}(S_r)^{n_r}$ be such that $\vec{\alpha}\vec{\psi} \in H$. Let $C := \text{Soc}(H)\vec{\alpha}\vec{\psi}$ be the associated socle coset in H . Then:*

- (1) $\omega_H(C) = \omega_H(C^{\text{Aut}(H)})$ and $\text{o}(C) = \text{o}(C^{\text{Aut}(H)})$.
- (2) $\omega_H(C) \geq \omega_{\text{Aut}(\text{Soc}(H))}(C) = \prod_{(i,\ell,\tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})} \Omega_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$.
- (3) $\text{Ord}(C) = \text{ord}(\vec{\psi}) \cdot \mathcal{G}(\vec{\psi}, \vec{\alpha})$.
- (4) $\text{o}(C) = |\mathcal{G}(\vec{\psi}, \vec{\alpha})| \leq \prod_{(i,\ell,\tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})} \text{O}_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$.
- (5)

$$\begin{aligned} \mathfrak{q}_H(C) &\geq \mathfrak{q}_{\text{Aut}(\text{Soc}(H))}(C) \geq \prod_{(i,\ell,\tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})} \frac{\Omega_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})}{\text{O}_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})} \\ &\geq \prod_{(i,\ell,\tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})} \mathfrak{q}_{\text{Aut}(S_i)}(S_i\alpha(\tau)) \geq \max\{\tilde{\mathfrak{q}}(S_i) \mid i = 1, \dots, r\}, \end{aligned}$$

where $\alpha(\tau)$ and $\tilde{\mathfrak{q}}(S_i)$ are as in Notation 5.3.2.

Proof. For statement (1): The second equality (of the o-values) is clear since group automorphisms preserve the orders of elements. The first equality holds because each coset of $\text{Soc}(H)$ that is contained in the union of socle cosets $(\text{Soc}(H)\vec{\alpha}\vec{\psi})^{\text{Aut}(H)}$ intersects the same $\text{Aut}(H)$ -orbits, namely those that are contained in $(\text{Soc}(H)\vec{\alpha}\vec{\psi})^{\text{Aut}(H)}$.

For statement (2): The inequality $\omega_H(\text{Soc}(H)\vec{\alpha}\vec{\psi}) \geq \omega_{\text{Aut}(\text{Soc}(H))}(\text{Soc}(H)\vec{\alpha}\vec{\psi})$ holds because $\text{Aut}(H)$ embeds naturally into $\text{Aut}(\text{Soc}(H))$ (see e.g. [51, Lemma 1.1]), which is complete.

The asserted formula for $\omega_{\text{Aut}(\text{Soc}(H))}(\text{Soc}(H)\vec{\alpha}\vec{\psi})$ is an immediate consequence of [4, Lemma 2.2.5(1)], which is an equivalent reformulation of James and Kerber's characterisation of conjugacy in wreath products $G \wr \text{Sym}(n)$ [37, Theorem 4.2.8, p. 141].

For statement (3): For the proof of this statement, view $\vec{\psi}$ as a permutation on

$$\bigcup_{i=1}^r (\{i\} \times \{1, \dots, n_i\})$$

as explained after Notation 5.4.2. Observe that each element

$$h\vec{\alpha}\vec{\psi} \in \text{Soc}(H)\vec{\alpha}\vec{\psi}$$

has order divisible by $\text{ord}(\vec{\psi})$ and that it thus suffices to show that the set of orders of the powers

$$(h\vec{\alpha}\vec{\psi})^{\text{ord}(\vec{\psi})} \in \prod_{i=1}^r \text{Aut}(S_i)^{n_i},$$

where h ranges over $\text{Soc}(H)$, is just $\mathcal{G}(\vec{\psi}, \vec{\alpha})$.

Now, for each $(\vec{\psi}, \vec{\alpha})$ -admissible triple (i, ℓ, τ) , for each (i, ℓ, τ) -cycle ζ of $(\vec{\psi}, \vec{\alpha})$ and each $(i, j) \in \text{supp}(\zeta)$, the (i, j) entry of

$$(h\vec{\alpha}\vec{\psi})^{\text{ord}(\vec{\psi})}$$

is the $(\text{ord}(\vec{\psi})/\ell)$ -th power of

$$\text{bcp}_{(i,j)}(\vec{\psi}, \vec{\alpha}).$$

In particular, with h ranging over $\text{Soc}(H)$, we have the following:

- for each given $(i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})$, the possible orders of each entry of

$$(h\vec{\alpha}\vec{\psi})^{\text{ord}(\vec{\psi})}$$

whose index lies on an (i, ℓ, τ) -cycle of $(\vec{\psi}, \vec{\alpha})$ are just the elements of

$$\text{Ord}((S_i\alpha(\tau))^{\text{ord}(\psi)/\ell});$$

- entries of

$$(h\vec{\alpha}\vec{\psi})^{\text{ord}(\vec{\psi})}$$

whose indices lie on the same cycle of $\vec{\psi}$ are conjugate (in particular, of the same order); and

- the orders of entries of

$$(h\vec{\alpha}\vec{\psi})^{\text{ord}(\vec{\psi})}$$

whose indices (i_k, j_k) lie on pairwise distinct cycles, of lengths ℓ_k and with backward cycle product type τ_k , of $\vec{\psi}$ can be chosen independently of each other from the respective set

$$\text{Ord}((S_{i_k}\alpha(\tau_k))^{\text{ord}(\vec{\psi})/\ell_k}).$$

Hence for each given $(i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})$, the possible orders (in a suitable power of $\text{Aut}(S_i)$) of the projection of

$$(h\vec{\alpha}\vec{\psi})^{\text{ord}(\vec{\psi})}$$

to the coordinates lying on one of the (i, ℓ, τ) -cycles of $(\vec{\psi}, \vec{\alpha})$ are just the least common multiples formed from $\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$ -tuples with entries from

$$\text{Ord}((S_i\alpha(\tau))^{\text{ord}(\vec{\psi})/\ell},$$

i.e., the elements of $M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$ by definition. Moreover, the possible orders of the entire power

$$(h\vec{\alpha}\vec{\psi})^{\text{ord}(\vec{\psi})}$$

are just the least common multiples formed from a tuple consisting of one element choice from each set $M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$ with (i, ℓ, τ) ranging over $\text{Adm}(\vec{\psi}, \vec{\alpha})$, i.e., the elements of $\mathcal{G}(\vec{\psi}, \vec{\alpha})$ by definition, as required.

For statement (4): By statement (3),

$$o(C) = |\mathcal{G}(\vec{\psi}, \vec{\alpha})| \leq \prod_{(i,\ell,\tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})} \lambda(\mathcal{F}_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})).$$

By the definitions of the notations λ and $O_{i,\ell,\tau}$, the result now follows.

For statement (5): The first two inequalities are consequences of statements (2) and (4), and the last inequality is clear from the definition of $\tilde{q}(S)$ (which entails that $\mathfrak{q}_{\text{Aut}(S)}(S\alpha) \geq \tilde{q}(S) \geq 1$ for all nonabelian finite simple groups S and all $\alpha \in \text{Aut}(S)$). Hence we may restrict our attention to the third inequality. We are done if we can show that for each $(i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})$,

$$\frac{\Omega_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})}{O_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})} \geq \mathfrak{q}_{\text{Aut}(S_i)}(S_i\alpha(\tau)).$$

And indeed, by the remarks after Notation 5.4.4 and the fact that $o(\tau) \leq \omega(\tau)$, we conclude that

$$\begin{aligned} \frac{\Omega_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})}{O_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})} &\geq \frac{\binom{\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + \omega(\tau) - 1}{\omega(\tau) - 1}}{\binom{\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + o(\tau) - 1}{o(\tau) - 1}} = \frac{(\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + \omega(\tau) - 1)!(o(\tau) - 1)!}{(\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + o(\tau) - 1)!(\omega(\tau) - 1)!} \\ &= \frac{\omega(\tau) + \Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) - 1}{o(\tau) + \Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) - 1} \cdot \frac{\omega(\tau) + \Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) - 2}{o(\tau) + \Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) - 2} \cdots \frac{\omega(\tau) + 1}{o(\tau) + 1} \cdot \frac{\omega(\tau)!(o(\tau) - 1)!}{o(\tau)!(\omega(\tau) - 1)!} \\ &\geq 1 \cdot 1 \cdots 1 \cdot \frac{\omega(\tau)!(o(\tau) - 1)!}{o(\tau)!(\omega(\tau) - 1)!} = \frac{\omega(\tau)}{o(\tau)} = \mathfrak{q}_{\text{Aut}(S_i)}(S_i\alpha(\tau)), \end{aligned}$$

as required. □

5.5 Another equivalent reformulation of Theorem 1.1.2(2)

Consider the following notation:

Notation 5.5.1. Let $\hat{m}, \hat{d}, \hat{p}, c \geq 1$.

- (1) We denote by $\mathcal{H}^{(c)}$ the class of finite semisimple groups H with $\mathfrak{q}(H) \leq c$.
- (2) We denote by $\mathcal{S}_{\hat{m}, \hat{d}, \hat{p}}$ the class of nonabelian finite simple groups S which are one of the following:
 - a sporadic nonabelian finite simple group,
 - an alternating group $\text{Alt}(m)$ where $m \leq \hat{m}$, or
 - a finite simple group of Lie type ${}^tX_d(p^{ft})$ where $d \leq \hat{d}$ and $p \leq \hat{p}$.
- (3) We denote by $\mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$ the class of finite semisimple groups H such that $\text{Soc}(H)$ only has composition factors from $\mathcal{S}_{\hat{m}, \hat{d}, \hat{p}}$.

As an extension of Remark 5.1.1, we note the following:

Remark 5.5.2. The following are equivalent:

- (1) The existence of a function $f_2 : [0, \infty)^2 \rightarrow [1, \infty)$ that is monotonically increasing in each variable and such that $|G : \text{Rad}(G)| \leq f_2(\mathfrak{q}(G), \mathfrak{o}(\text{Rad}(G)))$ for all finite groups G , as asserted by Theorem 1.1.2(2).
- (2) The existence of a monotonically increasing function $\mathfrak{g} : [1, \infty) \rightarrow [1, \infty)$ such that $|H| \leq \mathfrak{g}(\mathfrak{q}(H))$ for all finite semisimple groups H .
- (3) The finiteness (up to isomorphism of the elements) of the classes $\mathcal{H}^{(c)}$ for all $c \geq 1$.

Indeed, the equivalence of (1) and (2) was already shown in Remark 5.1.1, and the equivalence of (2) and (3) is obvious.

We will prove Theorem 1.1.2(2) by ultimately showing that the classes $\mathcal{H}^{(c)}$ are all finite. As an intermediate step toward proving this, we will now show the following, as an application of the theory developed so far:

Lemma 5.5.3. *For each constant $c \geq 1$, there are constants $\hat{m} = \hat{m}(c)$, $\hat{d} = \hat{d}(c)$ and $\hat{p} = \hat{p}(c)$, all in $[1, \infty)$, such that $\mathcal{H}^{(c)} \subseteq \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$.*

Proof. Let $H \in \mathcal{H}^{(c)}$, i.e., H is a finite semisimple group with $\mathfrak{q}(H) \leq c$. Write $\text{Soc}(H) = S_1^{n_1} \times \cdots \times S_r^{n_r}$, where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$. Recall the partition \mathfrak{P}_H of H introduced after the proof of Lemma 5.2.3. By Lemma 5.2.2, applied with $G := H$, $M := H$ and $\mathfrak{P} := \mathfrak{P}_H$, as well as Lemma 5.4.5(1,5), we find that (recalling $\tilde{\mathfrak{q}}$ from Notation 5.3.2(1))

$$\begin{aligned} \max\{\tilde{\mathfrak{q}}(S_i) \mid i = 1, \dots, r\} &\leq \min\{\mathfrak{q}_H(C) \mid C \text{ is a socle coset in } H\} \\ &= \min\{\mathfrak{q}_H(N) \mid N \in \mathfrak{P}_H\} \leq \mathfrak{q}(H) \leq c. \end{aligned} \quad (5.5.1)$$

By Lemma 5.3.7, there are constants $\hat{m} = \hat{m}(c)$, $\hat{d} = \hat{d}(c)$ and $\hat{p} = \hat{p}(c)$ in $[1, \infty)$ such that

- For all $m \geq 5$, if $\tilde{\mathfrak{q}}(\text{Alt}(m)) \leq c$, then $m \leq \hat{m}$.
- For all $d \geq 1$ and all primes p , if S is a finite simple group of Lie type of rank d and defining characteristic p such that $\tilde{\mathfrak{q}}(S) \leq c$, then $d \leq \hat{d}$ and $p \leq \hat{p}$.

Combining this with Formula (5.5.1) shows that each composition factor S_i of $\text{Soc}(H)$ must lie in the class $\mathcal{S}_{\hat{m}, \hat{d}, \hat{p}}$, defined in Notation 5.5.1(2) above, and this just means by definition that $H \in \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$, as required. \square

In order to derive further restrictions on the classes $\mathcal{H}^{(c)}$, it is, in view of Lemma 5.5.3, natural to study the classes $\mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$. This will be done in Subsection 5.7, but before that, we will need some elementary number-theoretic preparations, which will be carried out in Subsection 5.6.

5.6 A bit of elementary number theory

We start with the following notation:

Notation 5.6.1. Let $k \in \mathbb{N}^+$.

- (1) For a positive integer m , set $m//k := \frac{m}{\gcd(m,k)}$.
- (2) For a set (or multiset) M of positive integers, set $M//k := \{m//k \mid m \in M\}$.

This occurs naturally in the following basic group-theoretic lemma:

Lemma 5.6.2. *Let G be a finite group, $g \in G$, $M \subseteq G$, and $k \in \mathbb{N}^+$. Denote by M^k the set of k -th powers of elements of M . Then*

- (1) $\text{ord}(g^k) = \text{ord}(g)//k$.
- (2) $\text{Ord}(M^k) = \text{Ord}(M)//k$.

□

We also have a number-theoretic lemma associated with Notation 5.6.1, and with Notation 5.4.1:

Lemma 5.6.3. *Let $(M_i)_{i \in I}$ be a finite family of finite subsets of \mathbb{N}^+ , and let $k \in \mathbb{N}^+$. Then*

$$\Lambda((M_i//k)_{i \in I}) = \Lambda((M_i)_{i \in I})//k.$$

Proof. Assume w.l.o.g. that $I = \{1, \dots, r\}$. Note that a general element of $\Lambda((M_i//k)_{i \in I})$ is of the form

$$\text{lcm}\left(\frac{m_1}{\gcd(m_1, k)}, \dots, \frac{m_r}{\gcd(m_r, k)}\right) \quad (5.6.1)$$

for $m_i \in M_i$ for $i = 1, \dots, r$, whereas a general element of $\Lambda((M_i)_{i \in I})//k$ is of the form

$$\frac{\text{lcm}(m_1, \dots, m_r)}{\gcd(\text{lcm}(m_1, \dots, m_r), k)} \quad (5.6.2)$$

for $m_i \in M_i$ for $i = 1, \dots, r$. We are done if we can show that for each $(m_1, \dots, m_r) \in \prod_{i=1}^r M_i$, the numbers in Formulas (5.6.1) and (5.6.2) are equal. Now, for each prime p , write $\nu_p(m)$ for the p -adic valuation of m , i.e., the largest nonnegative integer a such that p^a divides m . Then

$$\begin{aligned} & \nu_p\left(\text{lcm}\left(\frac{m_1}{\gcd(m_1, k)}, \dots, \frac{m_r}{\gcd(m_r, k)}\right)\right) \\ &= \max\{\nu_p(m_i) - \min\{\nu_p(m_i), \nu_p(k)\} \mid i = 1, \dots, r\} \\ &= \max\{\nu_p(m_i) \mid i = 1, \dots, r\} - \min\{\max\{\nu_p(m_i) \mid i = 1, \dots, r\}, \nu_p(k)\} \\ &= \nu_p\left(\frac{\text{lcm}(m_1, \dots, m_r)}{\gcd(\text{lcm}(m_1, \dots, m_r), k)}\right), \end{aligned}$$

where the second equality uses the monotonicity of max and min, which implies that the maximum value in the second expression is assumed for those $i \in \{1, \dots, r\}$ where $\nu_p(m_i)$ is maximal. Hence the third expression (obtained from the second by substituting $\max\{\nu_p(m_i) \mid i = 1, \dots, r\}$ into $\nu_p(m_i)$) is the said maximum value, as asserted. □

Note that a subset $M \subseteq \mathbb{N}^+$ is equal to the set $\text{Div}(n)$ of positive divisors of some fixed positive integer n if and only if M is a finite subset of \mathbb{N}^+ that is closed under the binary operations gcd and lcm (i.e., M is a sublattice of $(\mathbb{N}^+, |)$) as well as closed under taking divisors of its elements; we will henceforth call such sets M *divisors sets*. For example, $\text{Div}(12) = \{1, 2, 3, 4, 6, 12\}$ is a divisors set.

Lemma 5.6.4. *Let $M \subseteq \mathbb{N}^+$ be a divisors set, and let $a_1, \dots, a_k \in \mathbb{N}^+$ and $m_1, \dots, m_k \in M$. Then $\text{lcm}(a_1 m_1, \dots, a_k m_k) \in \text{lcm}(a_1, \dots, a_k)M$.*

Proof. For each prime p , we have that

$$\begin{aligned} \nu_p(\text{lcm}(a_1 m_1, \dots, a_k m_k)) &= \max\{\nu_p(a_i) + \nu_p(m_i) \mid i = 1, \dots, k\} \leq \\ &\max\{\nu_p(a_i) \mid i = 1, \dots, k\} + \max\{\nu_p(m_i) \mid i = 1, \dots, k\}, \end{aligned}$$

and thus

$$\nu_p\left(\frac{\text{lcm}(a_1 m_1, \dots, a_k m_k)}{\text{lcm}(a_1, \dots, a_k)}\right) \leq \max\{\nu_p(m_i) \mid i = 1, \dots, k\} \leq \max\{\nu_p(m) \mid m \in M\}.$$

As M is closed under divisibility, the quotient $\text{lcm}(a_1 m_1, \dots, a_k m_k) / \text{lcm}(a_1, \dots, a_k)$ is thus a product of pairwise coprime prime powers that are in M , and since M is closed under taking finitary least common multiples, it follows that said quotient is an element of M , as required. \square

Lemma 5.6.5. *Let $M \subseteq \mathbb{N}^+$ be a divisors set, let $t, a \in \mathbb{N}^+$ and $m \in M$. Then, using Notation 5.6.1, $((mt)//a) \in (t//a)M$.*

Proof. The quotient

$$\frac{(mt)//a}{t//a} = \frac{\frac{mt}{\text{gcd}(mt, a)}}{\frac{t}{\text{gcd}(t, a)}} = \frac{m \cdot \text{gcd}(t, a)}{\text{gcd}(mt, a)}$$

is a positive integer and divides m , and thus it lies in M . \square

Notation 5.6.6. Let $f \in \mathbb{N}^+$ and $h \geq 1$. We denote by $\text{coBD}_h(f)$ the set of divisors g of f such that $\frac{f}{g} \leq h$.

Lemma 5.6.7. *The following hold:*

- (1) *Let $f, a \in \mathbb{N}^+$, $h \geq 1$ and $g \in \text{coBD}_h(f)$. Then $(g//a) \in \text{coBD}_h(f//a)$.*
- (2) *Let $f_1, \dots, f_k \in \mathbb{N}^+$, $h \geq 1$ and $g_i \in \text{coBD}_h(f_i)$ for $i = 1, \dots, k$. Then $\text{lcm}(g_1, \dots, g_k) \in \text{coBD}_{\text{lcm}(1, \dots, [h])}(\text{lcm}(f_1, \dots, f_k))$.*

Proof. For statement (1): Firstly, we note that

$$\frac{f//a}{g//a} = \frac{\frac{f}{\text{gcd}(f, a)}}{\frac{g}{\text{gcd}(g, a)}} = \frac{f}{g} \cdot \frac{\text{gcd}(g, a)}{\text{gcd}(f, a)} \leq \frac{f}{g} \cdot 1 \leq h.$$

Secondly, we show that $g//a$ divides $f//a$. Indeed, for each prime p , we can write $\nu_p(f) = \nu_p(g) + v_p$ where $v_p \in \mathbb{N}$. Then

$$\nu_p(g//a) = \nu_p\left(\frac{g}{\gcd(g, a)}\right) = \nu_p(g) - \min\{\nu_p(g), \nu_p(a)\}$$

and

$$\nu_p(f//a) = \nu_p\left(\frac{f}{\gcd(f, a)}\right) = \nu_p(f) - \min\{\nu_p(f), \nu_p(a)\} = \nu_p(g) + v_p - \min\{\nu_p(g) + v_p, \nu_p(a)\}.$$

Hence the inequality $\nu_p(g//a) \leq \nu_p(f//a)$ is equivalent to

$$\min\{\nu_p(g) + v_p, \nu_p(a)\} \leq v_p + \min\{\nu_p(g), \nu_p(a)\},$$

which holds in view of the formula $\min\{\alpha, \beta\} + \gamma = \min\{\alpha + \gamma, \beta + \gamma\}$ and the monotonicity of \min in each component. Thus $(g//a) \in \text{coBD}_h(f//a)$.

For statement (2): It is clear that $\text{lcm}(g_1, \dots, g_k)$ divides $\text{lcm}(f_1, \dots, f_k)$, so we only need to show that their quotient is bounded from above by $\text{lcm}(1, \dots, \lfloor h \rfloor)$. For $i = 1, \dots, k$, let us write $f_i = g_i \cdot g'_i$, where $g'_i \leq h$. We claim and will prove that the quotient $\text{lcm}(f_1, \dots, f_k) / \text{lcm}(g_1, \dots, g_k)$ divides $\text{lcm}(g_1, \dots, g_k) = \text{lcm}\left(\frac{f_1}{g'_1}, \dots, \frac{f_k}{g'_k}\right)$.

Indeed, for each prime p ,

$$\nu_p\left(\frac{\text{lcm}(f_1, \dots, f_k)}{\text{lcm}(g_1, \dots, g_k)}\right) = \max\{\nu_p(f_i) \mid i = 1, \dots, k\} - \max\{\nu_p(g'_i) \mid i = 1, \dots, k\},$$

and

$$\nu_p(\text{lcm}(g_1, \dots, g_k)) = \max\{\nu_p(f_i) - \nu_p(g'_i) \mid i = 1, \dots, k\}.$$

Hence our claim is equivalent to

$$\begin{aligned} & \max\{\nu_p(f_i) \mid i = 1, \dots, k\} \\ & \leq \max\{\nu_p(f_i) - \nu_p(g'_i) \mid i = 1, \dots, k\} + \max\{\nu_p(g'_j) \mid j = 1, \dots, k\} = \\ & \max\{\nu_p(f_i) - \nu_p(g'_i) + \max\{\nu_p(g'_j) \mid j = 1, \dots, k\} \mid i = 1, \dots, k\}, \end{aligned}$$

which is clearly true, thus concluding the proof of the claim. Now the claim yields in particular that

$$\frac{\text{lcm}(f_1, \dots, f_k)}{\text{lcm}(1, \dots, \lfloor h \rfloor)} \leq \frac{\text{lcm}(f_1, \dots, f_k)}{\text{lcm}(g'_1, \dots, g'_k)} \leq \text{lcm}(g_1, \dots, g_k),$$

as required. □

5.7 Some results concerning the classes $\mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$

Recall from the end of Subsection 5.5 that our next goal is to study the classes $\mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$ introduced in Notation 5.5.1(2,3). We will do so in the form of Lemmas 5.7.4, 5.7.5 and 5.7.9 below. Before formulating and proving each of them, we introduce some more notation and give some motivation:

Notation 5.7.1. We introduce the following notation:

- (1) Let $n \in \mathbb{N}^+$, and let $\psi \in \text{Sym}(n)$. We denote by $\text{cl}(\psi)$ the set of distinct cycle lengths of ψ (where fixed points count as 1-cycles).
- (2) Let $r \in \mathbb{N}^+$, let $n_1, \dots, n_r \in \mathbb{N}^+$, and let $\vec{\psi} = (\psi_1, \dots, \psi_r) \in \text{Sym}(n_1) \times \dots \times \text{Sym}(n_r)$. We set $\text{cl}(\vec{\psi}) := (\text{cl}(\psi_1), \dots, \text{cl}(\psi_r))$.
- (3) For each finite semisimple group H with $\text{Soc}(H) = S_1^{n_1} \times \dots \times S_r^{n_r}$ where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$, and for each socle coset C of H , writing $C = \text{Soc}(H)\vec{\alpha}\vec{\psi}$, we set $\text{cl}(C) := \text{cl}(\vec{\psi})$ (note that this is independent of the choice of coset representative $\vec{\alpha}\vec{\psi}$).

For the subsequent Notation 5.7.2, recall Definition 5.3.1(1) as well as Notations 5.3.4 and 5.4.4(3).

Notation 5.7.2. Let S be a nonabelian finite simple group, let $\alpha \in \text{Aut}(S)$, and let τ be an S -type.

- (1) We set $h(\alpha) := \frac{f(S)}{g(\alpha)}$, where $f(S)$ and $g(\alpha)$ are as in Notation 5.3.4.
- (2) We set $h(\tau) := \frac{f(S)}{g(\tau)}$, where $f(S)$ and $g(\tau)$ are as in Notation 5.3.4.

Moreover, for a socle coset $C = \text{Soc}(H)\vec{\alpha}\vec{\psi}$ in a finite semisimple group H with $\text{Soc}(H) \cong S_1^{n_1} \times \dots \times S_r^{n_r}$, we set

$$h(C) := \max\{h(\tau) \mid (i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})\},$$

which is independent of the choice of coset representative $\vec{\alpha}\vec{\psi}$. For a constant $\hat{h} \geq 1$, we say that C is \hat{h} -large if and only if $h(C) > \hat{h}$, and \hat{h} -small otherwise.

Note that by definition, if

- $\hat{h} \geq 1$ is a constant,
- H is a finite semisimple group with $\text{Soc}(H) = S_1^{n_1} \times \dots \times S_r^{n_r}$ where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$,
- $C = \text{Soc}(H)\vec{\alpha}\vec{\psi}$ is a socle coset in H , and
- (i, ℓ, τ) is a $(\vec{\psi}, \vec{\alpha})$ -admissible triple as defined in Notation 5.4.4(2),

then $h(\tau) = 1 \leq \hat{h}$ for all admissible triples (i, ℓ, τ) such that S_i is alternating or sporadic (see Notation 5.3.4(1)). Thus the assumption that C be \hat{h} -small gives no additional restrictions. On the other hand, if S_i is neither alternating nor sporadic, then $h(\tau) \leq \hat{h}$ is by definition (see Notation 5.3.4(2)) equivalent to $g(\tau) \geq \frac{f(S_i)}{\hat{h}}$. This, in turn, is equivalent to the assumption that the common field or graph-field automorphism part order (note the case distinction in Notation 5.3.4(2)) of automorphisms of S_i with S_i -type τ is at least $\frac{f(S_i)}{\hat{h}}$, thus “close to being maximal”.

The point behind introducing the concepts of \hat{h} -small and \hat{h} -large socle cosets is the following:

Lemma 5.7.3. *For each constant $c \geq 1$, there is a constant $\hat{h} = \hat{h}(c)$ such that $\mathfrak{q}_H(C) > c$ for every finite semisimple group H and all \hat{h} -large socle cosets C in H .*

Proof. Write $\text{Soc}(H) = S_1^{n_1} \times \cdots \times S_r^{n_r}$ where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$. If C is \hat{h} -large (i.e., $h(C) > \hat{h}$) for some constant $\hat{h} \geq 1$, then

$$h(C) = \max\{h(\tau) \mid (i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})\}$$

is attained at some $(\vec{\psi}, \vec{\alpha})$ -admissible triple (i_0, ℓ_0, τ_0) such that S_{i_0} is neither alternating nor sporadic (otherwise, $h(\tau_0) = 1$ by definition). In particular, $S_{i_0} = {}^tX_d(p^{ft})$ is of Lie type, and

$$\hat{h} < h(\tau_0) = \frac{f(S_{i_0})}{g(\tau_0)} = \frac{6f}{g(\tau_0)},$$

or equivalently,

$$\frac{f}{g(\tau_0)} > \frac{\hat{h}}{6}. \quad (5.7.1)$$

By Lemma 5.3.7(2), there is a constant $h' = h'(c) \geq 1$ such that if

$$\frac{f}{g(\tau_0)} > h'(c), \quad (5.7.2)$$

then $\mathfrak{q}_{\text{Aut}(S_{i_0})}(S_{i_0}\alpha(\tau_0)) > c$ (see also Notation 5.3.2(1)). But in view of Formula (5.7.1), Formula (5.7.2) can be forced to be true by setting $\hat{h}(c) := 6h'(c)$, and then, applying Lemma 5.4.5(5) (see also Notation 5.4.4),

$$\mathfrak{q}_H(C) \geq \max\{\mathfrak{q}_{\text{Aut}(S_i)}(S_i\alpha(\tau)) \mid (i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})\} \geq \mathfrak{q}_{\text{Aut}(S_{i_0})}(S_{i_0}\alpha(\tau_0)) > c,$$

as required. \square

So, whenever we are in a situation where we need to show that $\mathfrak{q}(H) > c$, Lemmas 5.2.2, 5.2.3 and 5.7.3 imply that it is only the $\hat{h}(c)$ -small socle cosets that we need to worry about. Also, the following Lemma 5.7.4 gives us some control over the number of element orders in \hat{h} -small socle cosets, which is useful with regard to the nature of the bound in Lemma 5.2.3:

Lemma 5.7.4. *Let $\hat{m}, \hat{d}, \hat{p}, \hat{h} \geq 1$. There is a constant $D = D(\hat{m}, \hat{d}, \hat{p}, \hat{h}) > 0$ such that for all $H \in \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$, each union U of all \hat{h} -small socle cosets C in H with a fixed cl-value satisfies $\text{o}(U) \leq D$.*

Proof. Let $H \in \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$, say with $\text{Soc}(H) = S_1^{n_1} \times \cdots \times S_r^{n_r}$ where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$. Denote by $N = N(\hat{m}, \hat{d}, \hat{p}, \hat{h}) \subseteq \mathbb{N}^+$ the closure under the binary operation lcm of the union of the sets $\text{Ord}(G)$, where G ranges over the following (finitely many) finite groups:

- the automorphism groups of the sporadic nonabelian finite simple groups,
- the groups $\text{Aut}(\text{Alt}(m))$ where $5 \leq m \leq \hat{m}$, and
- the inner-diagonal automorphism groups of the finite simple groups of Lie type ${}^tX_d(p^{ft})$ where $d \leq \hat{d}$, $p \leq \hat{p}$ and $f \leq \hat{h}$.

Note that N is a divisors set. Consider any fixed \hat{h} -small socle coset $C = \text{Soc}(H)\vec{\alpha}\vec{\psi}$. Finally, fix also a $(\vec{\psi}, \vec{\alpha})$ -admissible triple (i, ℓ, τ) as defined in Notation 5.4.4(2). The proof idea is to exhibit a superset for $\text{Ord}(C)$ which only depends on $\text{cl}(C)$ (see Notation 5.7.1(1,3)), and for this, we will use Lemma 5.4.5(3), which gives us an explicit description of $\text{Ord}(C)$ in general, and we will work “bottom-up”, exhibiting suitable supersets for sets of gradually increasing complexity which occur in the construction of $\text{Ord}(C)$.

We start by claiming that

$$\text{Ord}(S_i\alpha(\tau)) \subseteq \text{coBD}_{\hat{h}}(f(S_i)) \cdot N, \quad (5.7.3)$$

where $f(S_i)$ is as in Notation 5.3.4 and $\text{coBD}_{\hat{h}}(f(S_i))$ is the set of divisors g of $f(S_i)$ such that $f(S_i)/g \leq \hat{h}$, as defined in Notation 5.6.6. Let us argue why Formula (5.7.3) holds. On the one hand, if S_i is sporadic or alternating, then by definition (see Notation 5.3.4(1)), $f(S_i) = 1$, and thus

$$\text{coBD}_{\hat{h}}(f(S_i)) = \text{coBD}_{\hat{h}}(1) = \{1\},$$

while also

$$\text{Ord}(S_i\alpha(\tau)) \subseteq \text{Ord}(\text{Aut}(S_i)) \subseteq N = \{1\} \cdot N = \text{coBD}_{\hat{h}}(f(S_i)) \cdot N$$

by the definition of N . On the other hand, if S_i is neither alternating nor sporadic, then $S_i = {}^tX_d(p^{ft})$ is of Lie type with $d \leq \hat{d}$ and $p \leq \hat{p}$. By Lemma 5.3.6, the order of each element of $S_i\alpha(\tau)$ is of the form $g(\tau) \cdot o$, where o is an element order in a group of the form $\text{Inndiag}({}^tX_d(p^{(uf/g(\tau))t'})$ for some $t' \in \{1, 2, 3\}$ and some $u \in \{1, t\}$. Now by assumption,

$$\hat{h} \geq \frac{f(S_i)}{g(\tau)},$$

and thus both $o \in N$ by definition of N and $g(\tau) \in \text{coBD}_{\hat{h}}(f(S_i))$, which concludes the proof of Formula (5.7.3).

Formula (5.7.3) provides us with a superset for $\text{Ord}(S_i\alpha(\tau))$. Consider next the set $\text{Ord}((S_i\alpha(\tau))^{\text{ord}(\vec{\psi})/\ell})$, of all orders of $(\text{ord}(\vec{\psi})/\ell)$ -th powers of elements of the coset $S_i\alpha(\tau)$ (recall that we are carrying out our arguments for a fixed $(\vec{\psi}, \vec{\alpha})$ -admissible triple (i, ℓ, τ)). Using Lemma 5.6.2(2) and Formula (5.7.3), we have

$$\begin{aligned} \text{Ord}((S_i\alpha(\tau))^{\text{ord}(\vec{\psi})/\ell}) &= \text{Ord}((S_i\alpha(\tau))//(\text{ord}(\vec{\psi})/\ell)) \\ &\subseteq (\text{coBD}_{\hat{h}}(f(S_i)) \cdot N)//(\text{ord}(\vec{\psi})/\ell). \end{aligned}$$

Fix an $o \in \text{coBD}_{\hat{h}}(f(S_i)) \cdot N$, and write $o = nf'$ with $n \in N$ and $f' \in \text{coBD}_{\hat{h}}(f(S_i))$. In view of Lemma 5.6.5 (and using that N is a divisors set), we have

$$o//(\text{ord}(\vec{\psi})/\ell) = (nf')//(\text{ord}(\vec{\psi})/\ell) \in (f'//(\text{ord}(\vec{\psi})/\ell))N,$$

and by an application of Lemma 5.6.7(1),

$$f'//(\text{ord}(\vec{\psi})/\ell) \in \text{coBD}_{\hat{h}}(f(S_i))//(\text{ord}(\vec{\psi})/\ell).$$

Thus we just proved that

$$\text{Ord}((S_i\alpha(\tau))^{\text{ord}(\vec{\psi})/\ell}) \subseteq \text{coBD}_{\hat{h}}(f(S_i)//(\text{ord}(\vec{\psi})/\ell)) \cdot N. \quad (5.7.4)$$

Recall, again, that we are working with a fixed $(\vec{\alpha}, \vec{\psi})$ -admissible triple (i, ℓ, τ) , and also recall the notation $M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$ from Notation 5.4.4(4(e)), which is by definition just the set of all positive integers that can be written as a least common multiple over tuples of elements of $\text{Ord}((S_i\alpha(\tau))^{\text{ord}(\vec{\psi})/\ell})$ of length $\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$. By Formula (5.7.4) and Lemma 5.6.4, each element of $M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$ can be written as the product of

- an element of N , with
- a least common multiple over some tuple of elements from the set

$$\text{coBD}_{\hat{h}}(f(S_i)//(\text{ord}(\vec{\psi})/\ell)),$$

and by Lemma 5.6.7(2), the said least common multiple always lies in the set

$$\text{coBD}_{\Psi(\lfloor \hat{h} \rfloor)}(f(S_i)//(\text{ord}(\vec{\psi})/\ell)),$$

where $\Psi(k) := \text{lcm}(1, \dots, k)$ (so that $\log \Psi(k)$ is the second Chebyshev function). So we have the following:

$$M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) \subseteq \text{coBD}_{\Psi(\lfloor \hat{h} \rfloor)}(f(S_i)//(\text{ord}(\vec{\psi})/\ell)) \cdot N. \quad (5.7.5)$$

At last, we are ready to exhibit a suitable overset for the set $\text{Ord}(C)$ of element orders in our socle coset $C = \text{Soc}(H)\vec{\alpha}\vec{\psi}$. By Lemma 5.4.5(3), each element of $\text{Ord}(C)$ can be written as the product of

- the number $\text{ord}(\vec{\psi})$, with
- a least common multiple over a family of numbers indexed by the $(\vec{\psi}, \vec{\alpha})$ -admissible triples (i, ℓ, τ) , and whose entry corresponding to (i, ℓ, τ) is some choice of element from $M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$.

Using this information as well as Formula (5.7.5) and Lemmas 5.6.4 and 5.6.7(2), one can conclude (analogously to how Formula (5.7.5) was derived from Formula (5.7.4)) that

$$\text{Ord}(C) \subseteq \text{ord}(\vec{\psi}) \cdot \text{coBD}_{\Psi(\lfloor \hat{h} \rfloor)}(\text{lcm}\{f(S_i)//(\text{ord}(\vec{\psi})/\ell) \mid (i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})\}) \cdot N. \quad (5.7.6)$$

Note that the superset in Formula (5.7.6) depends on \hat{m} , \hat{d} , \hat{p} , \hat{h} and $\text{cl}(C)$ (see Notation 5.7.1(1,3)), but not on the exact choice of C . It follows that

$$D(\hat{m}, \hat{d}, \hat{p}, \hat{h}) := \Psi(\Psi(\lfloor \hat{h} \rfloor)) \cdot |N(\hat{m}, \hat{d}, \hat{p}, \hat{h})|$$

is a suitable choice for the constant in Lemma 5.7.4. \square

Recall the notation $\Gamma(C)$, where C is a socle coset in the finite semisimple group H , from the paragraph after Notation 5.4.2, which just denotes the total number of cycles involved in the permutation tuple $\vec{\psi}$ in any coset representative $\vec{\alpha}\vec{\psi}$ for C in H . Apart from information on element orders in \hat{h} -small socle cosets as furnished by Lemma 5.7.4, we will also need one more tool to show that a given socle coset has large \mathfrak{q}_H -value, namely the following:

Lemma 5.7.5. *Let $\hat{m}, \hat{d}, \hat{p} \geq 1$. There is a constant $D' = D'(\hat{m}, \hat{d}, \hat{p}) > 0$ such that for all $H \in \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$ and all socle cosets C of H , one has $\mathfrak{q}_H(C) \geq \frac{1}{D'(\hat{m}, \hat{d}, \hat{p})} \Gamma(C)$.*

Proof. Again, let $H \in \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$, say with $\text{Soc}(H) = S_1^{n_1} \times \cdots \times S_r^{n_r}$ where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$. Write $C = \text{Soc}(H)\vec{\alpha}\vec{\psi}$. Assume that for a given $\hat{h} \geq 1$, we partition the set $\text{Adm}(\vec{\psi}, \vec{\alpha})$ of $(\vec{\psi}, \vec{\alpha})$ -admissible triples (i, ℓ, τ) (see Notation 5.4.4(2,3)) into two subsets (recall Notation 5.3.4):

- $\text{Adm}_-(\vec{\psi}, \vec{\alpha}) := \{(i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha}) \mid \frac{f(S_i)}{g(\tau)} \leq \hat{h}\}$ and
- $\text{Adm}_+(\vec{\psi}, \vec{\alpha}) := \{(i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha}) \mid \frac{f(S_i)}{g(\tau)} > \hat{h}\}$.

For $\epsilon \in \{+, -\}$, set (see Notations 5.4.1 and 5.4.4(4(d)))

$$M_\epsilon := \Lambda((M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}))_{(i,\ell,\tau) \in \text{Adm}_\epsilon(\vec{\psi}, \vec{\alpha})}).$$

Let $D(\hat{m}, \hat{d}, \hat{p}, \hat{h})$ be as in Lemma 5.7.4. We first show that

$$|M_-| \leq D(\hat{m}, \hat{d}, \hat{p}, \hat{h}), \tag{5.7.7}$$

as follows: By omitting all coordinates belonging to an (i, ℓ, τ) -cycle of $(\vec{\psi}, \vec{\alpha})$ where $(i, \ell, \tau) \in \text{Adm}_+(\vec{\psi}, \vec{\alpha})$, we get a (size-wise) smaller socle coset $\tilde{C} = \text{Soc}(\tilde{H})\tilde{\alpha}\tilde{\psi}$ in a smaller finite semisimple group $\tilde{H} \in \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$, and \tilde{C} is \hat{h} -small. We assume that the isomorphism types of nonabelian finite simple factors in $\text{Soc}(\tilde{H})$ are labelled by the same indices $i \in \{1, \dots, r\}$ as in $\text{Soc}(H)$ above (in particular, the set of all such indices is not necessarily an initial segment of \mathbb{N}^+). This notational convention has the advantage that we can write

$$\text{Adm}(\tilde{\psi}, \tilde{\alpha}) = \text{Adm}_-(\vec{\psi}, \vec{\alpha}).$$

Note that for each fixed $(i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})$, we are either omitting or keeping all (i, ℓ, τ) -cycles of $(\vec{\psi}, \vec{\alpha})$ in the above construction of \tilde{C} , and so for all $(i, \ell, \tau) \in \text{Adm}_-(\vec{\psi}, \vec{\alpha})$,

$$\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) = \Gamma_{i,\ell,\tau}(\tilde{\psi}, \tilde{\alpha}).$$

Now by definition, $\mathcal{F}_{i,\ell,\tau}(\tilde{\psi}, \tilde{\alpha})$ is a constant tuple of length $\Gamma_{i,\ell,\tau}(\tilde{\psi}, \tilde{\alpha})$ whose entries are equal to $\text{Ord}((S_i\alpha(\tau))^{\text{ord}(\tilde{\psi})/\ell})$. On the other hand, using Lemma 5.6.2 (see also Notation 5.6.1), $\mathcal{F}_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$ is a constant tuple of length $\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$ whose entries are equal to

$$\text{Ord}((S_i\alpha(\tau))^{\text{ord}(\vec{\psi})/\ell})$$

$$\begin{aligned}
&= \text{Ord}(((S_i\alpha(\tau))^{\text{ord}(\vec{\psi})/\ell})^{\text{ord}(\vec{\psi})/\text{ord}(\vec{\psi})}) \\
&= \text{Ord}((S_i\alpha(\tau))^{\text{ord}(\vec{\psi})/\ell})/(\text{ord}(\vec{\psi})/\text{ord}(\vec{\psi})).
\end{aligned}$$

By the definitions of $M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$ and $M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})$ as well as Lemma 5.6.3, it now follows that

$$M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) = M_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})/(\text{ord}(\vec{\psi})/\text{ord}(\vec{\psi})).$$

Hence, taking the least common multiple over all $(i, \ell, \tau) \in \text{Adm}_-(\vec{\psi}, \vec{\alpha})$ and applying Lemma 5.6.3 again,

$$M_- = \mathcal{G}(\vec{\psi}, \vec{\alpha})/(\text{ord}(\vec{\psi})/\text{ord}(\vec{\psi})),$$

whence, by Lemmas 5.4.5(3) and 5.7.4, applied to the \hat{h} -small socle coset \tilde{C} in \tilde{H} ,

$$|M_-| \leq |\mathcal{G}(\vec{\psi}, \vec{\alpha})| = o(\tilde{C}) \leq D(\hat{m}, \hat{d}, \hat{p}, \hat{h}),$$

as asserted above.

Now that we have shown Formula (5.7.7), we note that by Lemma 5.4.5(3), applied to C in H ,

$$o(C) = |\mathcal{G}(\vec{\psi}, \vec{\alpha})| = \lambda((M_+, M_-)) \leq |M_+| \cdot |M_-| \leq D(\hat{m}, \hat{d}, \hat{p}, \hat{h}) \cdot \prod_{(i,\ell,\tau) \in \text{Adm}_+(\vec{\psi}, \vec{\alpha})} \text{O}_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}),$$

and therefore (see Notation 5.4.4(4(b,c))), using Lemma 5.4.5(2),

$$\mathfrak{q}_H(C) \geq D(\hat{m}, \hat{d}, \hat{p}, \hat{h})^{-1} \cdot \prod_{(i,\ell,\tau) \in \text{Adm}_-(\vec{\psi}, \vec{\alpha})} \Omega_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) \cdot \prod_{(i,\ell,\tau) \in \text{Adm}_+(\vec{\psi}, \vec{\alpha})} \frac{\Omega_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})}{\text{O}_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})}.$$

Now note that for each $(i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})$ and using Lemma 5.3.3 as well as Formula (5.4.1), we have that

$$\Omega_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) = \binom{\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + \omega(\tau) - 1}{\omega(\tau) - 1} \geq \binom{\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + 2 - 1}{2 - 1} = \Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + 1.$$

Our goal will be to show that if \hat{h} is chosen large enough (relative to \hat{m} , \hat{d} and \hat{p}), then

$$\frac{\Omega_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})}{\text{O}_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})} \geq \Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + 1, \quad (5.7.8)$$

for all $(i, \ell, \tau) \in \text{Adm}_+(\vec{\psi}, \vec{\alpha})$, so that then

$$\begin{aligned}
\mathfrak{q}_H(C) &\geq D(\hat{m}, \hat{d}, \hat{p}, \hat{h})^{-1} \cdot \prod_{(i,\ell,\tau) \in \text{Adm}_-(\vec{\psi}, \vec{\alpha})} \Omega_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) \cdot \prod_{(i,\ell,\tau) \in \text{Adm}_+(\vec{\psi}, \vec{\alpha})} \frac{\Omega_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})}{\text{O}_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})} \\
&\geq D(\hat{m}, \hat{d}, \hat{p}, \hat{h})^{-1} \cdot \prod_{(i,\ell,\tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})} (\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + 1)
\end{aligned}$$

$$\begin{aligned} &\geq D(\hat{m}, \hat{d}, \hat{p}, \hat{h})^{-1} \cdot \sum_{(i, \ell, \tau) \in \text{Adm}(\vec{\psi}, \vec{\alpha})} (\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + 1) \\ &\geq D(\hat{m}, \hat{d}, \hat{p}, \hat{h})^{-1} \cdot \Gamma(\vec{\psi}) = D(\hat{m}, \hat{d}, \hat{p}, \hat{h})^{-1} \cdot \Gamma(C), \end{aligned}$$

as asserted. It remains to prove our claim that Formula (5.7.8) can be made true for sufficiently large \hat{h} . Assume that \hat{h} has been chosen so large that for all $S \in \mathcal{S}_{\hat{m}, \hat{d}, \hat{p}}$ and all S -types τ with $\frac{f(S)}{g(\tau)} > \hat{h}$, one has $\omega(\tau) \geq \max\{\text{o}(\tau)^4, 4\}$ (which is possible by Lemma 5.3.7). Then let $(i, \ell, \tau) \in \text{Adm}_+(\vec{\psi}, \vec{\alpha})$. We make a case distinction.

(1) Case: $\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) \leq \omega(\tau) - 1$. Then

$$\begin{aligned} \frac{\Omega_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})}{O_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})} &\geq \frac{\binom{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \omega(\tau) - 1}{\omega(\tau) - 1}}{\binom{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \text{o}(\tau) - 1}{\text{o}(\tau) - 1}} = \frac{\frac{(\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \omega(\tau) - 1)!}{(\omega(\tau) - 1)! \Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})!}}{\frac{(\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \text{o}(\tau) - 1)!}{(\text{o}(\tau) - 1)! \Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})!}} = \\ &\frac{(\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \omega(\tau) - 1)! \cdot (\text{o}(\tau) - 1)!}{(\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \text{o}(\tau) - 1)! \cdot (\omega(\tau) - 1)!} = \frac{\omega(\tau)}{\text{o}(\tau)} \cdot \frac{\omega(\tau) + 1}{\text{o}(\tau) + 1} \cdots \frac{\omega(\tau) + \Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) - 1}{\text{o}(\tau) + \Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) - 1}. \end{aligned}$$

If $\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) \leq 3$, then that last product of fractions is bounded from below by

$$\left(\frac{\omega(\tau) + 2}{\text{o}(\tau) + 2}\right)^{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})} \geq 2^{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})} \geq \Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + 1,$$

where the first inequality follows from the fact that $\omega(\tau) \geq 2\text{o}(\tau) + 2$, which can be deduced from our assumption $\omega(\tau) \geq \max\{\text{o}(\tau)^4, 4\}$. And if $4 \leq \Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) \leq \omega(\tau) - 1$, then the product of fractions is bounded from below by

$$\left(\frac{2\omega(\tau) - 2}{\text{o}(\tau) + \omega(\tau) - 2}\right)^{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})} \geq 1.5^{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})} \geq \Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + 1,$$

where the first inequality follows from $\omega(\tau) \geq 3\text{o}(\tau) - 2$, which is another consequence of our assumption $\omega(\tau) \geq \max\{\text{o}(\tau)^4, 4\}$. This concludes the proof of Formula (5.7.8) in case $\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) \leq \omega(\tau) - 1$.

(2) Case: $\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) \geq \omega(\tau)$. In this case, we use the trivial (by definition) upper bound $O_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) \leq 2^{\text{o}(\tau)}$. If $\text{o}(\tau) \leq 2$, then this yields

$$\begin{aligned} \frac{\Omega_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})}{O_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})} &\geq \frac{\binom{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \omega(\tau) - 1}{\omega(\tau) - 1}}{4} \geq \frac{\binom{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + 2}{2}}{4} = \\ &\frac{1}{8} (\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + 2) (\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + 1) \geq \Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + 1, \end{aligned}$$

where the second inequality uses that $\omega(\tau) \geq 4 > 3$. If $\text{o}(\tau) \geq 3$, then we have the following:

$$\frac{\Omega_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})}{O_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha})} \geq \frac{\binom{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \omega(\tau) - 1}{\omega(\tau) - 1}}{2^{\text{o}(\tau)}} \geq \frac{\binom{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \text{o}(\tau)}{\text{o}(\tau)}}{2^{\text{o}(\tau)}} \geq \frac{\left(\frac{\Gamma_{i, \ell, \tau}(\vec{\psi}, \vec{\alpha}) + \text{o}(\tau)}{\text{o}(\tau)}\right)^{\text{o}(\tau)}}{2^{\text{o}(\tau)}} =$$

$$\left(\frac{\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + o(\tau)}{2o(\tau)}\right)^{o(\tau)} \geq \left(\frac{\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})}{o(\tau)^2}\right)^{o(\tau)} \geq \Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})^{o(\tau)/2} \geq \Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) + 1.$$

Here, the last inequality in the first line is by the binomial coefficient bound $\binom{n}{k} \geq \left(\frac{n}{k}\right)^k$, see e.g. [15, Formula (2), p. 2]. Moreover, the second inequality in the second line follows from the observation that $\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) \geq \omega(\tau) \geq o(\tau)^4$, and thus $o(\tau)^2 \leq \Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha})^{1/2}$. Finally, the last inequality in the second line uses that $o(\tau) \geq 3$ and $\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) \geq \omega(\tau) \geq 4$. This concludes the proof of Formula (5.7.8) in case $\Gamma_{i,\ell,\tau}(\vec{\psi}, \vec{\alpha}) \geq \omega(\tau)$. \square

Lemmas 5.7.4 and 5.7.5 allow us to prove a certain technical result, Lemma 5.7.9 below, which provides lower bounds on \mathfrak{q}_H -values of certain unions of cosets of $\text{Soc}(H)$. This will be used in the proof of Lemma 5.8.3 below. Before we can formulate Lemma 5.7.9, we need some more notation and concepts.

Notation 5.7.6. For a permutation σ on a finite set, the *cycle type* of σ , denoted by $\text{ct}(\sigma)$, is defined as the multiset of cycle lengths of σ (including 1). Moreover, we introduce the following notation:

- (1) Let δ be a multiset of positive integers.
 - (a) We denote by $\Gamma(\delta)$ the (multiset) cardinality of δ . Equivalently, $\Gamma(\delta)$ is the number of cycles of any permutation on a finite set with cycle type δ .
 - (b) We denote by $\text{ord}(\delta)$ the least common multiple of the elements of δ . Equivalently, $\text{ord}(\delta)$ is the order of any permutation on a finite set with cycle type δ .
 - (c) For $e \in \mathbb{N}^+$, we denote by δ^e the multiset which for each occurrence of an element $\ell \in \delta$ contains $\gcd(\ell, e)$ occurrences of $\ell/e = \frac{\ell}{\gcd(\ell, e)}$ (see Notation 5.6.1(1)) but nothing else. Equivalently, δ^e is the cycle type of the e -th power of any permutation on a finite set with cycle type δ .
- (2) Let $\vec{\delta} = (\delta_1, \dots, \delta_r)$ be a tuple of multisets of positive integers.
 - (a) We set $\Gamma(\vec{\delta}) := \sum_{i=1}^r \Gamma(\delta_i)$.
 - (b) We set $\text{ord}(\vec{\delta}) := \text{lcm}\{\text{ord}(\delta_i) \mid i = 1, \dots, r\}$.
 - (c) We set $\vec{\delta}^e := (\delta_1^e, \dots, \delta_r^e)$.
- (3) Let H be a finite semisimple group, say with $\text{Soc}(H) = S_1^{n_1} \times \dots \times S_r^{n_r}$ where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$. Moreover, let $C = \text{Soc}(H)\vec{\alpha}\vec{\psi}$ be a socle coset in H , where $\vec{\psi} = (\psi_1, \dots, \psi_r)$. Then we set $\text{ct}(C) := (\text{ct}(\psi_1), \dots, \text{ct}(\psi_r))$, called the *cycle type of C* , which is independent of the choice of coset representative of C .

To avoid confusion among readers, let us briefly recall the different usages of the notation $\Gamma(x)$ in this paper, to which Notation 5.7.6 has added two:

- When ψ is a permutation on a finite set, then $\Gamma(\psi)$ denotes the number of distinct cycles of ψ including fixed points, see Notation 5.4.2. This is the most basic use of this notation, from which the others are derived.

- When $\vec{\psi} = (\psi_1, \dots, \psi_r)$ is a tuple of permutations on finite sets, then $\Gamma(\vec{\psi}) := \sum_{i=1}^r \Gamma(\vec{\psi})$, as explained in the paragraph after Notation 5.4.2.
- When C is a coset of the socle $\text{Soc}(H) \cong S_1^{n_1} \times \dots \times S_r^{n_r}$ of a finite semisimple group H , then $C = \text{Soc}(H)\vec{\alpha}\vec{\psi}$ for some tuple $\vec{\alpha} = (\vec{\alpha}_1, \dots, \vec{\alpha}_r)$ with $\vec{\alpha}_i \in \text{Aut}(S_i)^{n_i}$ for $i = 1, \dots, r$ and for a *unique* permutation tuple $\vec{\psi} = (\psi_1, \dots, \psi_r) \in \prod_{i=1}^r \text{Sym}(n_i)$, so that it makes sense to set $\Gamma(C) := \Gamma(\vec{\psi})$ in the sense of the paragraph after Notation 5.4.2, see also that same paragraph.
- When δ is a multiset of positive integers, then $\Gamma(\delta)$ is just $\Gamma(\psi)$ (in the sense of Notation 5.4.2) for any permutation ψ of cycle type δ , see Notation 5.7.6(1,a).
- When $\vec{\delta} = (\delta_1, \dots, \delta_r)$ is a tuple of multisets of positive integers, then $\Gamma(\vec{\delta}) := \sum_{i=1}^r \Gamma(\delta_i)$ (in the sense of Notation 5.7.6(1,a)), see Notation 5.7.6(2,a).

Definition 5.7.7. Let H be a finite semisimple group, $A > 2$ a constant.

- (1) Denote by $\text{CT}(H)$ the set of cycle types of socle cosets of H .
- (2) Say that $\vec{\delta} \in \text{CT}(H)$ is *A-good* if and only if $\Gamma(\vec{\delta}) > A$, and otherwise, say that $\vec{\delta}$ is *A-bad*.
- (3) We denote the set of *A-good* $\vec{\delta} \in \text{CT}(H)$ by $\text{CT}_{\text{good}}^{(A)}(H)$, and the set of *A-bad* $\vec{\delta} \in \text{CT}(H)$ by $\text{CT}_{\text{bad}}^{(A)}(H)$.
- (4) We distinguish further between two kinds of $\vec{\delta} \in \text{CT}_{\text{bad}}^{(A)}(H)$:
 - (a) $\vec{\delta}$ is called *A-bad of the first kind* if and only if $\text{ord}(\vec{\delta})$ is divisible by some prime strictly larger than A , and we denote the set of such $\vec{\delta}$ by $\text{CT}_{\text{bad},1}^{(A)}(H)$.
 - (b) $\vec{\delta}$ is called *A-bad of the second kind* if and only if all prime divisors of $\text{ord}(\vec{\delta})$ are at most A , and we denote the set of such $\vec{\delta}$ by $\text{CT}_{\text{bad},2}^{(A)}(H)$.
- (5) We denote by $\beta_H^{(A)}$ the function $\text{CT}_{\text{bad},1}^{(A)}(H) \rightarrow \text{CT}_{\text{good}}^{(A)}(H)$ mapping $\vec{\delta} \mapsto \vec{\delta}^{\max\{p \in \mathbb{P} \mid p \text{ divides } \text{ord}(\vec{\delta})\}}$.

Concerning the function $\beta_H^{(A)}$ from Definition 5.7.7(5), note the following two observations:

- (1) The set $\text{CT}(H)$ is closed under taking powers in the sense of Notation 5.7.6(2(c)). This is because for each $e \in \mathbb{N}^+$,

$$\text{ct}((\text{Soc}(H)\vec{\alpha}\vec{\psi})^e) = \text{ct}(\text{Soc}(H)\vec{\alpha}\vec{\psi})^e.$$

- (2) If $\vec{\delta} = (\delta_1, \dots, \delta_r) \in \text{CT}(H)$ is *A-bad of the first kind* and $p_0 := \max\{p \in \mathbb{P} \mid p \text{ divides } \text{ord}(\vec{\delta})\}$, then $p_0 > A$ by definition of “*A-bad of the first kind*”. Moreover, there is an $i \in \{1, \dots, r\}$ and an $\ell \in \delta_i$ with $p_0 \mid \ell$, and so by Notation 5.7.6(1(c)), $\delta_i^{p_0}$ contains at least p_0 occurrences of the number ℓ/p_0 , whence

$$\Gamma(\vec{\delta}^{p_0}) \geq \Gamma(\delta_i^{p_0}) \geq p_0 > A. \quad (5.7.9)$$

This shows that $\vec{\delta}^{p_0} = \beta_H^{(A)}(\vec{\delta})$ is not only an element of $\text{CT}(H)$ (as follows from the first observation), but it is also *A-good*. Hence $\beta_H^{(A)}$ indeed maps into $\text{CT}_{\text{good}}^{(A)}(H)$, as asserted in Definition 5.7.7(5).

Notation 5.7.8. Let H be a finite semisimple group, let $\hat{h} \geq 1$, and let $\vec{\delta} \in \text{CT}(H)$.

- (1) We denote by $V_{\vec{\delta}}(H)$ the union of all socle cosets in H of cycle type $\vec{\delta}$.
- (2) We denote by $W_{\vec{\delta}}^{(\hat{h})}(H)$ the union of all \hat{h} -small (see Notation 5.7.2) socle cosets in H of cycle type $\vec{\delta}$.

We are now ready for formulating and proving Lemma 5.7.9:

Lemma 5.7.9. *Let $\hat{m}, \hat{d}, \hat{p}, \hat{h} \geq 1$ be constants. There is a function $g_{\hat{m}, \hat{d}, \hat{p}, \hat{h}} : [1, \infty) \rightarrow [1, \infty)$ with $g_{\hat{m}, \hat{d}, \hat{p}, \hat{h}}(x) \rightarrow \infty$ as $x \rightarrow \infty$ such that*

$$\mathfrak{q}_H \left(V_{\vec{\delta}}(H) \cup \bigcup \{ W_{\vec{e}}^{(\hat{h})}(H) \mid \vec{e} \in (\beta_H^{(A)})^{-1}[\{\vec{\delta}\}] \} \right) \geq g_{\hat{m}, \hat{d}, \hat{p}, \hat{h}}(A)$$

for every constant $A > 2$, for all $H \in \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$ and every $\vec{\delta} \in \text{CT}_{\text{good}}^{(A)}(H)$.

Proof. For $\vec{\delta} \in \text{CT}_{\text{good}}^{(A)}(H)$, set

$$\varphi(\vec{\delta}) = \varphi_H^{(A)}(\vec{\delta}) := |(\beta_H^{(A)})^{-1}[\{\vec{\delta}\}]|.$$

We make the following two observations:

- (1) As in Formula (5.7.9) above, for each $\vec{\delta} \in \text{CT}_{\text{good}}^{(A)}(H)$ and each $\vec{e} \in (\beta_H^{(A)})^{-1}[\{\vec{\delta}\}]$, we have $\Gamma(\vec{\delta}) \geq \max\{p \in \mathbb{P} \mid p \text{ divides } \text{ord}(\vec{\delta})\}$.
- (2) For fixed $\vec{\delta}$, the function that assigns to each element \vec{e} of the $\beta_H^{(A)}$ -fibre of $\vec{\delta}$ the largest prime divisor of $\text{ord}(\vec{e})$ is injective. This is because of the following: For any prime $p > A$, if there is any A -bad cycle type \vec{e} whose p -th power is $\vec{\delta}$, then it is the one which for each $\ell \in \{1, \dots, n\}$ has exactly

$$\gamma_\ell - p \cdot \lfloor \frac{\gamma_\ell}{p} \rfloor + \lfloor \frac{\gamma_\ell/p}{p} \rfloor$$

cycles of length ℓ , where γ_x denotes the number of x -cycles of $\vec{\delta}$ if x is a positive integer, and $\gamma_x = 0$ otherwise. Indeed, all other cycle types that are p -th roots of $\vec{\delta}$ have at least p (and thus more than A) cycles of some given length $\ell \in \{1, \dots, n\}$.

Combining these two observations, we conclude that $\Gamma(\vec{\delta}) \geq p$ for at least $\varphi(\vec{\delta})$ many primes $p > A$, and so, denoting by p_k for $k \in \mathbb{N}^+$ the k -th prime,

$$\Gamma(\vec{\delta}) \geq p_{k(A) + \varphi(\vec{\delta})},$$

where $k(A) \in \mathbb{N}^+$ is such that $p_{k(A)}$ is the largest prime that is at most A ; note that $k(A) \rightarrow \infty$ as $A \rightarrow \infty$. By the Prime Number Theorem, $p_x \sim x \log x$ as $x \rightarrow \infty$, and so there is an absolute constant $c' > 0$ such that

$$p_{k(A) + \varphi(\vec{\delta})} \geq c'(k(A) + \varphi(\vec{\delta})) \log(k(A) + \varphi(\vec{\delta})).$$

Therefore and by Lemma 5.7.5,

$$\mathfrak{q}_H(V_{\vec{\delta}}) \geq D'(\hat{m}, \hat{d}, \hat{p})^{-1} \cdot c'(k(A) + \varphi(\vec{\delta})) \log(k(A) + \varphi(\vec{\delta})). \quad (5.7.10)$$

On the other hand, by Lemma 5.7.4,

$$o\left(\bigcup\{W_{\vec{\epsilon}}^{(\hat{h})}(H) \mid \vec{\epsilon} \in (\beta_H^{(A)})^{-1}[\{\vec{\epsilon}\}]\}\right) \leq \varphi(\vec{\delta}) \cdot D(\hat{m}, \hat{d}, \hat{p}, \hat{h}). \quad (5.7.11)$$

We now claim (and will show) that

$$g_{\hat{m}, \hat{d}, \hat{p}, \hat{h}} := \frac{c'}{(D(\hat{m}, \hat{d}, \hat{p}, \hat{h}) + 1) \cdot D'(\hat{m}, \hat{d}, \hat{p})} \cdot \log k(A) \quad (5.7.12)$$

is a suitable choice for the function in the statement of Lemma 5.7.9. To verify this, assume first that the fibre $(\beta_H^{(A)})^{-1}[\{\vec{\delta}\}]$ is empty, i.e., that $\varphi(\vec{\delta}) = 0$. Then by Formula (5.7.10)

$$\mathfrak{q}_H\left(V_{\vec{\delta}}(H) \cup \bigcup\{W_{\vec{\epsilon}}^{(\hat{h})}(H) \mid \vec{\epsilon} \in (\beta_H^{(A)})^{-1}[\{\vec{\delta}\}]\}\right) = \mathfrak{q}_H(V_{\vec{\delta}}) \geq \frac{c'}{D'(\hat{m}, \hat{d}, \hat{p})} \cdot k(A) \log k(A),$$

which is indeed bounded from below by $g_{\hat{m}, \hat{d}, \hat{p}, \hat{h}}(A)$ as in Formula (5.7.12). Now assume that the fibre $(\beta_H^{(A)})^{-1}[\{\vec{\delta}\}]$ is nonempty. Using Formulas (5.7.10) and (5.7.11), an application of Lemma 5.2.3 with

- $G := H$,
- $M := V_{\vec{\delta}} \cup \bigcup\{W_{\vec{\epsilon}}^{(\hat{h})}(H) \mid \vec{\epsilon} \in (\beta_H^{(A)})^{-1}[\{\vec{\epsilon}\}]\}$,
- $M_{\text{good}} := V_{\vec{\delta}}$ and
- $M_{\text{bad}} := \bigcup\{W_{\vec{\epsilon}}^{(\hat{h})}(H) \mid \vec{\epsilon} \in (\beta_H^{(A)})^{-1}[\{\vec{\epsilon}\}]\}$ (which is disjoint from M_{good} because M_{bad} is by definition a union of socle cosets with cycle type in $(\beta_H^{(A)})^{-1}[\{\vec{\epsilon}\}] \subseteq \text{CT}_{\text{bad}}^{(A)}(H)$, whereas M_{good} is a union of socle cosets with cycle type in $\text{CT}_{\text{good}}^{(A)}(H)$, and by definition, $\text{CT}_{\text{good}}^{(A)}(H) \cap \text{CT}_{\text{bad}}^{(A)}(H) = \emptyset$)

yields that

$$\begin{aligned} & \mathfrak{q}_H(V_{\vec{\delta}} \cup \bigcup\{W_{\vec{\epsilon}}^{(\hat{h})}(H) \mid \vec{\epsilon} \in (\beta_H^{(A)})^{-1}[\{\vec{\epsilon}\}]\}) \geq \\ & \frac{1}{1 + \varphi(\vec{\delta})D(\hat{m}, \hat{d}, \hat{p}, \hat{h})} \cdot \frac{1}{D'(\hat{m}, \hat{d}, \hat{p})} \cdot c'(k(A) + \varphi(\vec{\delta})) \log(k(A) + \varphi(\vec{\delta})) \geq \\ & \frac{c'}{(D(\hat{m}, \hat{d}, \hat{p}, \hat{h}) + 1) \cdot D'(\hat{m}, \hat{d}, \hat{p})} \cdot \frac{k(A) + \varphi(\vec{\delta})}{\varphi(\vec{\delta})} \cdot \log(k(A) + \varphi(\vec{\delta})) \geq \\ & \frac{c'}{(D(\hat{m}, \hat{d}, \hat{p}, \hat{h}) + 1) \cdot D'(\hat{m}, \hat{d}, \hat{p})} \cdot \log k(A) = g_{\hat{m}, \hat{d}, \hat{p}, \hat{h}}(A), \end{aligned}$$

as required. \square

5.8 More restrictions on finite semisimple groups with bounded \mathfrak{q} -value

This subsection provides the last few remaining jigsaw pieces for completing the proof of Theorem 1.1.2(2) (or, rather, of the finiteness of the classes $\mathcal{H}^{(c)}$ from Notation 5.5.1(1), see Remark 5.5.2). Recall Lemma 5.5.3, which states that for each constant $c > 0$, the class $\mathcal{H}^{(c)}$, of all finite semisimple groups H with $\mathfrak{q}(H) \leq c$, is contained in the class $\mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$ of finite semisimple groups (with restrictions on the simple factors in the socle, see Notation 5.5.1(2,3) for details), where $\hat{m} = \hat{m}(c)$, $\hat{d} = \hat{d}(c)$ and $\hat{p} = \hat{p}(c)$. So this already provides some restrictions on finite semisimple groups with bounded \mathfrak{q} -value, and using Lemmas 5.7.4 and 5.7.5, we will be able to add even more restrictions to this list, see Lemma 5.8.2 below.

Notation 5.8.1. Let $\hat{m}, \hat{d}, \hat{p}, \hat{r} \geq 1$, and let $f : [1, \infty) \rightarrow [1, \infty)$. We denote by $\mathcal{H}_{\hat{m}, \hat{d}, \hat{p}, \hat{r}, f}$ the class of finite semisimple groups H such that

- (1) $H \in \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$,
- (2) the number of nonisomorphic nonabelian simple factors in $\text{Soc}(H)$ is at most \hat{r} , and
- (3) the composition length of $\text{Soc}(H)$ is at least $f(|H|)$.

Lemma 5.8.2. *For each $c \geq 1$ there are constants $\hat{m} = \hat{m}(c)$, $\hat{d} = \hat{d}(c)$, $\hat{p} = \hat{p}(c)$ and $\hat{r} = \hat{r}(c)$, all in $[1, \infty)$, as well as a monotonically increasing function $f_c : [1, \infty) \rightarrow [1, \infty)$ with $f_c(x) \rightarrow \infty$ as $x \rightarrow \infty$ such that $\mathcal{H}^{(c)} \subseteq \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}, \hat{r}, f_c}$.*

Proof. Let $H \in \mathcal{H}^{(c)}$, i.e., H is a finite semisimple group with $\mathfrak{q}(H) \leq c$. By Lemma 5.5.3, we can fix constants $\hat{m}, \hat{d}, \hat{p} \geq 1$, all depending on c , such that $H \in \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}}$. Write $\text{Soc}(H) = S_1^{n_1} \times \cdots \times S_r^{n_r}$, where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$. By Lemma 5.7.5, for all socle cosets C in H , we have that

$$\mathfrak{q}_H(C) \geq D'(c)^{-1} \Gamma(C) \geq D'(c)^{-1} r,$$

so letting $\hat{r}(c) := cD'(c)$, we have that $\text{Soc}(H)$ has at most $\hat{r}(c)$ nonisomorphic nonabelian simple factors.

It remains to prove the existence of f_c . Note that by Lemma 5.3.8(3), there is a monotonically increasing function $F : [1, \infty) \rightarrow [1, \infty)$ with $F(x) \rightarrow \infty$ as $x \rightarrow \infty$ such that

$$\mathfrak{q}(\text{Soc}(H)) \geq F(|\text{Soc}(H)|). \quad (5.8.1)$$

Moreover, let $\hat{h} = \hat{h}(c)$ be so large that $\mathfrak{q}_H(C) > c$ for every \hat{h} -large socle coset C in H . Finally, denote by $N(H)$ the composition length of $\text{Soc}(H)$.

By definition, for each socle coset $C = \text{Soc}(H)\vec{\alpha}\vec{\psi}$ of H , where $\vec{\psi} = (\psi_1, \dots, \psi_r)$, we have $\text{cl}(C) = \text{cl}(\vec{\psi}) = (\text{cl}(\psi_1), \dots, \text{cl}(\psi_r))$, and, for $i = 1, \dots, r$,

$$\text{cl}(\psi_i) \subseteq \{1, \dots, n_i\} \subseteq \{1, \dots, N(H)\},$$

where the last inclusion uses that $N(H) = \sum_{j=1}^r n_j \geq n_i$. So $\text{cl}(C)$ is always an r -tuple of subsets of $\{1, \dots, N(H)\}$, and so the number of distinct cl -values of socle cosets in H is at most

$$2^{N(H)r} \leq 2^{N(H)\hat{r}(c)}. \quad (5.8.2)$$

By Formula (5.8.2) and Lemma 5.7.4, if we denote by U the union of all \hat{h} -small socle cosets in H , then

$$\text{o}(U) \leq D(c) \cdot 2^{N(H)\hat{r}(c)}. \quad (5.8.3)$$

Set $M := \text{Soc}(H) \cup U$, $M_{\text{good}} := \text{Soc}(H)$ and $M_{\text{bad}} := M \setminus \text{Soc}(H)$. By Formula (5.8.3),

$$\text{o}(M_{\text{bad}}) \leq D(c) \cdot 2^{N(H)\hat{r}(c)}. \quad (5.8.4)$$

In view of Formulas (5.8.1) and (5.8.4), an application of Lemma 5.2.3 yields that

$$\mathfrak{q}_H(M) \geq \frac{F(|\text{Soc}(H)|)}{1 + D(c) \cdot 2^{N(H)\hat{r}(c)}} \quad (5.8.5)$$

Set $M' := H \setminus M$. Then M' is an $\text{Aut}(H)$ -invariant union of \hat{h} -large socle cosets, and so by the choice of \hat{h} from above and Lemma 5.2.2, we have

$$\mathfrak{q}_H(M') > c.$$

But we are assuming that $\mathfrak{q}(H) \leq c$, so we must have $\mathfrak{q}_H(M) \leq c$ (otherwise, an application of Lemma 5.2.2 with $\mathfrak{P} := \{M, M'\}$ yields that $\mathfrak{q}_H(H) = \mathfrak{q}(H) > c$). Together with Formula (5.8.5), this yields that

$$c \geq \frac{F(|\text{Soc}(H)|)}{1 + D(c) \cdot 2^{N(H)\hat{r}(c)}}$$

or equivalently

$$N(H) \geq \frac{\log \frac{F(|\text{Soc}(H)|) - c}{cD(c)}}{\hat{r}(c) \log 2}.$$

Hence, denoting by $h(x)$ the smallest order of the socle of a finite semisimple group H with $|H| \geq x$ (note that the function h is also monotonically increasing), we find that

$$f_c(x) := \frac{\log \frac{F(h(x)) - c}{cD(c)}}{\hat{r}(c) \log 2}$$

defines a suitable choice for f_c in the statement of Lemma 5.8.2. \square

Recall that by Remark 5.5.2, our goal is to show that for each $c \geq 1$, the class $\mathcal{H}^{(c)}$, of finite semisimple groups H with $\mathfrak{q}(H) \leq c$, is finite. Now Lemma 5.8.2 tells us that $\mathcal{H}^{(c)}$ can also be written as the intersection of itself with one of the classes $\mathcal{H}_{\hat{m}, \hat{d}, \hat{p}, \hat{r}, f}$ from Notation 5.8.1. And the following lemma says that each such intersection is finite:

Lemma 5.8.3. *For all constants $c, \hat{m}, \hat{d}, \hat{p}, \hat{r} \geq 1$ and all functions $f : [1, \infty) \rightarrow [1, \infty)$ with $f(x) \rightarrow \infty$ as $x \rightarrow \infty$, the intersection $\mathcal{H}^{(c)} \cap \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}, \hat{r}, f}$ is finite.*

Proof. We begin by declaring some parameters:

- Let $\hat{h} = \hat{h}(c)$ be so large that for all finite semisimple groups H and all \hat{h} -large (see Notation 5.7.2) socle cosets C in H , we have $\mathfrak{q}_H(C) > c$ (this is possible by Lemma 5.7.3).
- Let $D' = D'(\hat{m}, \hat{d}, \hat{p})$ be as in Lemma 5.7.5.
- Set $\tilde{D} := D(\hat{m}, \hat{d}, \hat{p}, \hat{h}(c))$, where the quaternary function D is as in Lemma 5.7.4.
- Let $A = A(\hat{m}, \hat{d}, \hat{p}, c)$ be so large that $\min\{\frac{A}{D'(\hat{m}, \hat{d}, \hat{p})}, g_{\hat{m}, \hat{d}, \hat{p}, \hat{h}(c)}(A)\} > c$, where $g_{\hat{m}, \hat{d}, \hat{p}, \hat{h}(c)}$ is as in Lemma 5.7.9.
- Let $N_0 = N_0(\hat{m}, \hat{d}, \hat{p}, \hat{r}, c) \geq A(\hat{m}, \hat{d}, \hat{p}, c)$ be so large that for all $N \in \mathbb{N}^+$ with $N > N_0$, we have

$$\frac{N}{D'(1 + A(1 + \log_2 N)\tilde{D})(1 + \tilde{D}(\hat{r}A(1 + \log_2 N))^A)} > c.$$

We claim that if $H \in \mathcal{H}^{(c)} \cap \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}, \hat{r}, f}$ has socle $\text{Soc}(H) = S_1^{n_1} \times \dots \times S_r^{n_r}$, where S_1, \dots, S_r are pairwise nonisomorphic nonabelian finite simple groups and $n_1, \dots, n_r \in \mathbb{N}^+$, then $n(H) := \max\{n_i \mid i = 1, \dots, r\}$ is at most N_0 .

Indeed, assume one could have an $H \in \mathcal{H}^{(c)} \cap \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}, \hat{r}, f}$ with $n(H) > N_0$. We will show that $\mathfrak{q}(H) > c$, and thus a contradiction. By choice of \hat{h} , all \hat{h} -large socle cosets C in H satisfy $\mathfrak{q}_H(C) > c$, and so do all socle cosets C whose cycle type $\text{ct}(C)$ is A -good, by choice of A and Lemma 5.7.5. Therefore, it is only the \hat{h} -small socle cosets with an A -bad cycle type that we need to worry about – the idea is to carefully join unions of such “bad” socle cosets with unions of previously mentioned “good” socle cosets such that each “mixed” union still has \mathfrak{q}_H -value strictly larger than c , using Lemmas 5.2.2 and 5.2.3 for this.

Assume that in a first step, we take care of the \hat{h} -small socle cosets with a cycle type that is A -bad of the first kind by joining each socle coset union $W_{\vec{\epsilon}}^{(\hat{h})}(H)$, where $\vec{\epsilon} \in \text{CT}_{\text{bad},1}^{(A)}(H)$, with the union $V_{\beta_H^{(A)}(\vec{\epsilon})}(H)$ of socle cosets with the A -good cycle type $\beta_H^{(A)}(\vec{\epsilon})$. This results in a partition of

$$H \setminus \bigcup_{\vec{\epsilon} \in \text{CT}_{\text{bad},2}^{(A)}(H)} W_{\vec{\epsilon}}^{(\hat{h})}(H)$$

into blocks of the form

$$B_{\vec{\delta}} := V_{\vec{\delta}}(H) \cup \bigcup \{W_{\vec{\epsilon}}^{(\hat{h})}(H) \mid \vec{\epsilon} \in (\beta_H^{(A)})^{-1}[\{\vec{\delta}\}]\},$$

where $\vec{\delta}$ ranges over the A -good cycle types of socle cosets of H . Lemma 5.7.9 and the choice of A guarantee us that

$$\mathfrak{q}_H(B_{\vec{\delta}}) > c \tag{5.8.6}$$

for all $\vec{\delta} \in \text{CT}_{\text{good}}^{(A)}(H)$.

It remains to deal with the part

$$\bigcup_{\vec{\epsilon} \in \text{CT}_{\text{bad},2}^{(A)}(H)} W_{\vec{\epsilon}}^{(\hat{h})}(H),$$

consisting of all \hat{h} -small socle cosets whose cycle type is A -bad of the second kind. Denote by $\vec{\delta}_0 := \text{ct}(\text{Soc}(H))$ the trivial cycle type, which is A -good because

$$\Gamma(\vec{\delta}_0) = \sum_{i=1}^r n_i \geq n(H) > N_0 \geq A.$$

One of the blocks of the partition of $H \setminus \bigcup_{\vec{\epsilon} \in \text{CT}_{\text{bad},2}^{(A)}(H)} W_{\vec{\epsilon}}^{(\hat{h})}(H)$ mentioned just above is

$$B_{\vec{\delta}_0} := V_{\vec{\delta}_0}(H) \cup \bigcup \{W_{\vec{\epsilon}}^{(\hat{h})}(H) \mid \epsilon \in (\beta_H^{(A)})^{-1}[\{\vec{\delta}_0\}]\},$$

and we claim that the union

$$B'_{\vec{\delta}_0} := B_{\vec{\delta}_0} \cup \bigcup_{\vec{\epsilon} \in \text{CT}_{\text{bad},2}^{(A)}(H)} W_{\vec{\epsilon}}^{(\hat{h})}(H)$$

still has \mathfrak{q}_H -value strictly larger than c .

Following the proof of Lemma 5.7.9 with $\vec{\delta} := \vec{\delta}_0$ and using again that $\Gamma(\vec{\delta}_0) = \sum_{i=1}^r n_i \geq \max\{n_1, \dots, n_r\} = n(H)$, we find that

$$\mathfrak{q}_H(B_{\vec{\delta}_0}) \geq \frac{n(H)}{D'(1 + \varphi_H^{(A)}(\vec{\delta}_0)\tilde{D})}.$$

Now $(\beta_H^{(A)})^{-1}[\{\vec{\delta}_0\}]$ consists only of cycle types $\vec{\epsilon}$ such that $A < \text{ord}(\vec{\epsilon}) = p$ is a prime and p divides one of the numbers $n(H), n(H) - 1, \dots, n(H) - A + 1$ (otherwise, each of the corresponding cycle types $\vec{\epsilon}$ has too many cycles to be A -bad). Moreover, each such prime p corresponds to at most one A -bad cycle type $\vec{\epsilon}$ of the first kind. It follows that

$$\varphi_H^{(A)}(\vec{\delta}_0) = |(\beta_H^{(A)})^{-1}[\{\vec{\delta}_0\}]| \leq A(1 + \log_2 n(H)),$$

and so

$$\mathfrak{q}_H(B_{\vec{\delta}_0}) \geq \frac{n(H)}{D'(1 + A(1 + \log_2 n(H))\tilde{D})}. \tag{5.8.7}$$

How many element orders are there in

$$\bigcup_{\vec{\epsilon} \in \text{CT}_{\text{bad},2}^{(A)}(H)} W_{\vec{\epsilon}}^{(\hat{h})}(H),$$

the union of all the \hat{h} -small socle cosets with an A -bad cycle type of the second kind? The number of such cycle types is at most $(\hat{r}A(1 + \log_2 n(H)))^A$ (think of length A sequences of pairs of choices of an index $i \in \{1, \dots, r\} \subseteq \{1, \dots, [\hat{r}]\}$ and of a cycle

length in $\{1, \dots, n_i\} \subseteq \{1, \dots, n(H)\}$ which is a power of a prime $p \leq A$. Hence, by Lemma 5.7.4,

$$o\left(\bigcup_{\vec{c} \in \text{CT}_{\text{bad},2}^{(A)}(H)} W_{\vec{c}}^{(\hat{h})}(H)\right) \leq \tilde{D}(\hat{r}A(1 + \log_2 n(H)))^A. \quad (5.8.8)$$

Applying Lemma 5.2.3 with

- $M := B'_{\vec{\delta}_0} = B_{\vec{\delta}_0} \cup \bigcup_{\vec{c} \in \text{CT}_{\text{bad},2}^{(A)}(H)} W_{\vec{c}}^{(\hat{h})}(H)$,
- $M_{\text{good}} := B_{\vec{\delta}_0}$ and
- $M_{\text{bad}} := \bigcup_{\vec{c} \in \text{CT}_{\text{bad},2}^{(A)}(H)} W_{\vec{c}}^{(\hat{h})}(H)$,

and using Formulas (5.8.7) and (5.8.8), we conclude that

$$\mathfrak{q}_H(B'_{\vec{\delta}_0}) \geq \frac{n(H)}{D'(1 + A(1 + \log_2 n(H))\tilde{D})(1 + \tilde{D}(\hat{r}A(1 + \log_2 n(H)))^A)} > c, \quad (5.8.9)$$

where the second inequality is by the assumption $n(H) > N_0$ and the choice of N_0 .

We are now ready to show that $\mathfrak{q}(H) > c$. Consider the partition \mathfrak{P} of H whose members are the following:

- the set $B'_{\vec{\delta}_0} = B_{\vec{\delta}_0} \cup \bigcup_{\vec{c} \in \text{CT}_{\text{bad},2}^{(A)}(H)} W_{\vec{c}}^{(\hat{h})}(H)$, and
- the sets $B_{\vec{\delta}}$ where $\vec{\delta} \in \text{CT}_{\text{good}}^{(A)}(H) \setminus \{\vec{\delta}_0\}$.

By Formulas (5.8.6) and (5.8.9), each partition member has \mathfrak{q}_H -value strictly larger than c , and so $\mathfrak{q}_H(H) = \mathfrak{q}(H) > c$ by an application of Lemma 5.2.2. This is the desired contradiction confirming that $n(H) \leq N_0$.

Now that we know that $n(H) \leq N_0$, and in view of our assumption that $H \in \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}, \hat{r}, f}$, it follows that the composition length $\sum_{i=1}^r n_i$ of $\text{Soc}(H)$ is at most $\hat{r}N_0$, and so $\hat{r}N_0 \geq f(|H|)$. But $f(x) \rightarrow \infty$ as $x \rightarrow \infty$, so there are indeed only finitely many possibilities for H , as required. \square

5.9 Completing the proof of Theorem 1.1.2(2)

Let us now give a proof of Theorem 1.1.2(2) using the results developed in the previous subsections. By Remark 5.5.2, it suffices to show that for each constant $c \geq 1$, the class $\mathcal{H}^{(c)}$, defined in Notation 5.5.1(1), is finite. By Lemma 5.8.2, we find that there are

- constants $\hat{m} = \hat{m}(c)$, $\hat{d} = \hat{d}(c)$, $\hat{p} = \hat{p}(c)$, $\hat{r} = \hat{r}(c)$, all in $[1, \infty)$, as well as
- a monotonically increasing function $f_c : [1, \infty) \rightarrow [1, \infty)$ with $f_c(x) \rightarrow \infty$ as $x \rightarrow \infty$

such that $\mathcal{H}^{(c)}$ is contained in the class $\mathcal{H}_{\hat{m}, \hat{d}, \hat{p}, \hat{r}, f_c}$, as defined in Notation 5.8.1. In other words, we have

$$\mathcal{H}^{(c)} \cap \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}, \hat{r}, f_c} = \mathcal{H}^{(c)}. \quad (5.9.1)$$

But an application of Lemma 5.8.3 yields that the intersection $\mathcal{H}^{(c)} \cap \mathcal{H}_{\hat{m}, \hat{d}, \hat{p}, \hat{r}, f_c}$, i.e., the class $\mathcal{H}^{(c)}$ by Formula (5.9.1), is finite, which concludes the proof.

References

- [1] R. Abbott, J. Bray, S. Linton, S. Nickerson, S. Norton, R. Parker, I. Suleiman, J. Tripp, P. Walsh, R. Wilson, *ATLAS of Finite Group Representations – Version 3*, online resource, <http://brauer.maths.qmul.ac.uk/Atlas/v3/>.
- [2] R. Bastos and A.C. Dantas, On Finite Groups with Few Automorphism Orbits, *Comm. Algebra* **44**(7):2953–2958, 2016.
- [3] N.L. Biggs and A.T. White, *Permutation Groups and Combinatorial Structures*, Cambridge University Press (London Mathematical Society Lecture Note Series, 33), Cambridge, 1979 (reprinted 2008).
- [4] A. Bors, Finite groups with a large automorphism orbit, *J. Algebra* **521**:331–364, 2019.
- [5] R. Brandl and W.J. Shi, A characterization of finite simple groups with abelian Sylow 2-subgroups, *Ric. Mat.* **42**(1):193–198, 1993.
- [6] T.C. Burness, Fixed point ratios in actions of finite classical groups, II, *J. Algebra* **309**(1):80–138, 2007.
- [7] A.A. Buturlakin, Spectra of finite simple groups $E_6(q)$ and ${}^2E_6(q)$, *Algebra Logic* **52**(3):188–202, 2013.
- [8] A.A. Buturlakin, Spectra of finite simple groups $E_7(q)$, *Sib. Math. J.* **57**(5):769–777, 2016.
- [9] A.A. Buturlakin and M.A. Grechkoseeva, The cyclic structure of maximal tori of the finite classical groups, *Algebra Logic* **46**(2):73–89, 2007.
- [10] P.J. Cameron and C.E. Praeger, Block-transitive t -designs. I. Point-imprimitive designs, *Discrete Math.* **118**:33–43, 1993.
- [11] P.J. Cameron and C.E. Praeger, Block-transitive t -designs. II. Large t , in: F. De Clerck et al. (eds.), *Finite geometry and combinatorics*, Cambridge University Press (London Mathematical Society Lecture Note Series, 191), Cambridge, 1993.
- [12] R.W. Carter, Centralizers of semisimple elements in the finite classical groups, *Proc. London Math. Soc. (3)* **42**(1):1–41, 1981.
- [13] G. Cherlin and U. Felgner, Homogeneous finite groups, *J. London Math. Soc. (2)* **62**(3):784–794, 2000.
- [14] A.C. Dantas, M. Garonzi and R. Bastos, Finite groups with six or seven automorphism orbits, *J. Group Theory* **20**(5):945–954, 2017.
- [15] S. Das, A brief note on estimates of binomial coefficients, online note, available under <http://page.mi.fu-berlin.de/shagnik/notes/binomials.pdf>.

- [16] J. Dénes, P. Erdős and P. Turán, On some statistical properties of the alternating group of degree n , *Enseignement Math. (2)* **15**:89–99, 1969.
- [17] H.W. Deng and W.J. Shi, The characterization of Ree groups ${}^2F_4(q)$ by their element orders, *J. Alg.* **217**(1):180–187, 1999.
- [18] D.I. Deriziotis and A.P. Fakiolas, The maximal tori in the finite Chevalley groups of type E_6 , E_7 and E_8 , *Comm. Algebra* **19**(3):889–903, 1991.
- [19] A. Devillers and J. Doyen, Homogeneous and ultrahomogeneous linear spaces, *J. Combin. Theory Ser. A* **84**(2):236–241, 1998.
- [20] P. Erdős, On an elementary proof of some asymptotic formulas in the theory of partitions, *Ann. Math.* **43**(3):437–450, 1942.
- [21] P. Erdős and P. Turán, On some problems of a statistical group theory. IV, *Acta Math. Acad. Sci. Hungar.* **19**:413–435, 1968.
- [22] J.A. Ernest, Central intertwining numbers for representations of finite groups, *Trans. Amer. Math. Soc.* **99**:499–508, 1961.
- [23] R. Fraïssé, Sur certaines relations qui généralisent l'ordre des nombres rationnels, *C. R. Acad. Sci.* **237**:540–542, 1953.
- [24] J. Fulman and R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Trans. Amer. Math. Soc.* **364**(6):3023–3070, 2012.
- [25] P.C. Gager, Maximal tori in finite groups of Lie type, PhD thesis (University of Warwick), 1973, available online under <http://wrap.warwick.ac.uk/66550/>.
- [26] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.10.2* (2019), <http://www.gap-system.org>.
- [27] The GAP Group, *GAP – Reference Manual, Release 4.10.2* (2019), <https://www.gap-system.org/Manuals/doc/ref/chap0.html>.
- [28] A. Gardiner, Homogeneous graphs, *J. Combinatorial Theory Ser. B* **20**(1):94–102, 1976.
- [29] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups, Number 3*, American Mathematical Society (Mathematical Surveys and Monographs, 40.3), Providence, 1998.
- [30] M.A. Grechkoseeva and M.A. Zvezdina, On spectra of automorphic extensions of finite simple groups $F_4(q)$ and ${}^3D_4(q)$, *J. Algebra Appl.* **15**(9):165–168, 2016.
- [31] 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):7665–7694, 2015.

- [32] B. Hartley, A general Brauer-Fowler theorem and centralizers in locally finite groups, *Pacific J. Math* **152**(1):101–117, 1992.
- [33] B. Hartley and M. Kuzucuoğlu, Centralizers of elements in locally finite simple groups, *Proc. London Math. Soc. (3)* **62**(2):301–324, 1991.
- [34] G.H. Hardy and S. Ramanujan, Asymptotic formulæ in combinatory analysis, *Proc. London Math Soc. (2)* **17**:75–115, 1918.
- [35] M. Huber, *Flag-transitive Steiner designs*, Birkhäuser (Frontiers in Mathematics), Basel, 2009.
- [36] J.E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge University Press (Cambridge studies in advanced mathematics, 29), Cambridge, 1990.
- [37] G. James and A. Kerber, *The Representation Theory of the Symmetric Group*, Addison-Wesley (Encyclopedia of Mathematics and Its Applications), Reading, 1981.
- [38] S. Kohl, A bound on the order of the outer automorphism group of a finite simple group of given order, online note (2003), available under <http://www.gap-system.org/DevelopersPages/StefanKohl/preprints/outbound.pdf>.
- [39] T.J. Laffey and D. MacHale, Automorphism orbits of finite groups, *J. Austral. Math. Soc. (Ser. A)* **40**:253–260, 1986.
- [40] C.H. Li, On isomorphisms of finite Cayley graphs – a survey, *Discrete Math.* **256**:301–334, 2002.
- [41] C.H. Li, Á. Seress and S.J. Song, s -Arc-transitive graphs and normal subgroups, *J. Algebra* **421**:331–348, 2015.
- [42] C.H. Li and C.E. Praeger, Finite groups in which any two elements of the same order are either fused or inverse-fused, *Comm. Algebra* **25**(10):3081–3118, 1997.
- [43] F. Lübeck, Data for Finite Groups of Lie Type and Related Algebraic Groups, online database, <http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/index.html>.
- [44] I.G. MacDonald, Numbers of conjugacy classes in some finite classical groups, *Bull. Austral. Math. Soc.* **23**(1):23–48, 1981.
- [45] G. Malle and D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type*, Cambridge University Press (Cambridge studies in advanced mathematics, 133), Cambridge, 2011.
- [46] A. Maróti, On elementary lower bounds for the partition function, *Integers* **3**(A10):1–9, 2003.

-
- [47] J.L. Nicolas and G. Robin, Majorations explicites pour le nombre de diviseurs de N , *Canad. Math. Bull.* **26**(4):485–492, 1983.
- [48] The On-Line Encyclopedia of Integer Sequences, A000009, <https://oeis.org/A000009>.
- [49] H. Robbins, A remark on Stirling’s formula, *Amer. Math. Monthly* **62**(1):26–29, 1955.
- [50] D.J.S. Robinson, *A Course in the Theory of Groups*, Springer (Graduate Texts in Mathematics, 80), New York, 2nd. ed. 1996.
- [51] J.S. Rose, Automorphism groups of groups with trivial centre, *Proc. London Math. Soc. (3)* **31**(2):167–193, 1975.
- [52] M.A. Shahabi and H. Mohtadifar, The characters of finite projective symplectic groups $\text{PSp}_4(q)$, in: C.M. Campbell, E.F. Robertson and G.C. Smith (eds.), *Groups St Andrews 2001 in Oxford*, vol. 2, Cambridge University Press (London Mathematical Society Lecture Note Series, 305), Cambridge, 2003.
- [53] W.J. Shi, A characterization of Suzuki’s simple groups, *Proc. Amer. Math. Soc.* **114**(3):589–591, 1992.
- [54] M. Stroppel, Locally compact groups with few orbits under automorphisms, *Top. Proc.* **26**(2):819–842, 2002.
- [55] D.M. Testerman, A_1 -type overgroups of elements of order p in semisimple algebraic groups and the associated finite groups, *J. Algebra* **177**(1):34–76, 1995.
- [56] K. Thas, Finite flag-transitive projective planes: a survey and some remarks, *Discrete Math.* **266**:417–429, 2003.
- [57] A.V. Vasil’ev and A.M. Staroletov, Recognizability of groups $G_2(q)$ by spectrum, *Algebra Logic* **52**(1):1–14, 2013.
- [58] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Aust. Math. Soc.* **3**:1–62, 1963.
- [59] R. Weiss, The non-existence of 8-transitive graphs, *Combinatorica* **3**(1):309–311, 1981.
- [60] M. Wildon, Counting partitions on the abacus, *Ramanujan J.* **17**:355–367, 2008.
- [61] J. Zhang, On Finite Groups All of Whose Elements of the Same Order Are Conjugate in Their Automorphism Groups, *J. Algebra* **153**:22–36, 1992.