manuscripta math. 149, 523–546 (2016)

Nguyen Ngoc Hung · Mark L. Lewis · Amanda A. Schaeffer Fry

Finite groups with an irreducible character of large degree

Received: 1 April 2015
Published online: 1 October 2015

Abstract. Let G be a finite group and d the degree of a complex irreducible character of G, then write $|G| = d(d + e)$ where e is a nonnegative integer. We prove that $|G| \leq e^4 - e^3$ whenever $e > 1$. This bound is best possible and improves on several earlier related results.

1. Introduction

Let d be the degree of a complex irreducible character of a finite group G. Since d divides $|G|$ and $d^2 \leq |G|$, one can write $|G| = d(d + e)$ for some nonnegative integer e. It is clear that the largest possible value of d is $\sqrt{|G|}$ and $d = \sqrt{|G|}$ if and only if G is trivial.

The extremal situations where d is close to $\sqrt{|G|}$ or equivalently e is small have been studied considerably in the literature. In [1], Berkovich showed that $e = 1$ if and only if G is either a cyclic group of order 2 or a 2-transitive Frobenius group. Going further, Snyder [31] classified the finite groups with $e = 2$ or 3, and as a consequence of his classification, $|G| \leq 8$ when $e = 2$ and $|G| \leq 54$ when $e = 3$. This naturally leads Snyder to the observation that $|G|$ is bounded in terms of e whenever $e > 1$ and, indeed, he managed to prove that $|G| \leq ((2e)!)^2$.

Finding the best bound for $|G|$ in terms of e has become a problem of interest in many recent papers. Isaacs [16] was the first to improve Snyder's factorial bound to a polynomial one of the form Be^6 where B is a large enough constant. However his proof relied on a result of Larsen et al. [19, Theorem 1.1] on bounding the largest irreducible character degree in terms of smaller degrees in a simple group, which in turn replied on the classification of finite simple groups. Later on, Durfee and

Nguyen N. Hung is partially supported by the NSA Young Investigator Grant #H98230-14-1-0293 and a Faculty Scholarship Award from the Buchtel College of Arts and Sciences, The University of Akron.

N. N. Hung (✉): Department of Mathematics, The University of Akron, Akron, OH 44325, USA. e-mail: hn10@uakron.edu; hungnguyen@uakron.edu

M. L. Lewis: Department of Mathematical Sciences, Kent State University, Kent, OH 44242, USA. e-mail: lewis@math.kent.edu

A. A. Schaeffer Fry: Department of Mathematical and Computer Sciences, Metropolitan State University of Denver, Denver, CO 80217, USA. e-mail: aschaef6@msudenver.edu

Mathematics Subject Classification: Primary 20C15; Secondary 20C30, 20C33, 20C34

DOI: 10.1007/s00229-015-0793-z

Jensen [8] were able to obtain the bound of $e^6 - e^4$ without using the classification. This bound was further improved to $e^4 + e^3$ by the second author in [20].

In [16], Isaacs pointed out that the group of 3×3 matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & t \end{pmatrix},$$

where x, y, z, t are elements in a field of order q and $t \neq 0$, has order $q^3(q-1)$ and an irreducible character of degree $q(q-1)$. These groups show that the best possible bound one can achieve is $e^4 - e^3$ and, in fact, this bound holds when G has a nontrivial abelian normal subgroup, as shown in [20, Theorem 1]. We note that these groups had earlier appeared in [11, p. 383] in a slightly different context.

The aim of the present paper is to prove the optimal bound of $e^4 - e^3$ for arbitrary finite groups.

Theorem 1.1. *Let $|G| = d(d+e)$ where $e > 1$ and d is the degree of some irreducible character of G. Then $|G| \leq e^4 - e^3$.*

In light of [20], to prove Theorem 1.1 it suffices to assume that G has a trivial solvable radical. Indeed, we can do a bit more.

Theorem 1.2. *Let $|G| = d(d+e)$ where d is the degree of some irreducible character of G. If G has a non-abelian minimal normal subgroup, then $|G| < e^4 - e^3$.*

Theorem 1.2 convinces us that those groups with $|G| = e^4 - e^3$ are necessarily solvable. It would be interesting to confirm this, or to even classify them completely, a task that seems nontrivial to us. In Sect. 7, we show that they must be the so-called Gagola groups of specific type and present some of their examples.

Let $\mathbf{F}(G)$ and $b(G)$ respectively denote the Fitting subgroup and the largest degree of an irreducible character of G. An old (and still open) conjecture of Gluck [12] asserts that $|G : \mathbf{F}(G)| \leq b(G)^2$ whenever G is solvable. In a recent extension of Gluck's conjecture to arbitrary finite groups [6], it has been predicted that $|G : \mathbf{F}(G)| \leq b(G)^3$. This means that, when G has a trivial solvable radical, it is expected that $|G| \leq b(G)^3$. In the course of proving Theorem 1.2, we in fact prove that $e > \sqrt{b(G)} + 1$, and this, on the other end, provides a *lower bound* for $|G|$ in terms of $b(G)$ in those groups.

Theorem 1.3. *Let G be a finite group with a non-abelian minimal normal subgroup. Then*

$$|G| > b(G)\left(b(G) + \sqrt{b(G)} + 1\right).$$

Theorem 1.3 is not true for non-solvable groups in general, as shown by the non-solvable 2-transitive Frobenius groups (there are three of them, see [29, Proposition 20.2]). We should also mention that we know of no finite groups G with a non-abelian minimal normal subgroup such that $|G| \leq 2b(G)^2$. In fact, we are able to prove the following, which solves a weak form of a prediction of Isaacs raised in [16], see Sect. 3 for a detailed discussion.

Theorem 1.4. *Let S be a finite non-abelian simple group. Then $|S| > 2b(S)^2$. Consequently, if $|S| = d(d+e)$ where d is the degree of some irreducible character of S then $|S| < 2e^2$.*

We note that Theorem 1.4 implies Theorem 1.2 for simple groups and more generally characteristically simple groups. Also, its proof makes use of recent results [14,19] on bounding the largest character degree in terms of smaller degrees in finite simple groups, see Sect. 3.

Our proof of Theorem 1.2 is fundamentally different from those in [8,16,20] and, as expected, relies on the classification of finite simple groups. Let N be a non-abelian minimal normal subgroup of G and suppose that S is a simple direct factor of N. The proof is divided in two main cases, according to whether or not S is isomorphic to $\mathrm{PSL}_2(q)$.

The key to the proof in the case $S \ncong \mathrm{PSL}_2(q)$ is to show that S possesses an irreducible character θ extendible to $\mathrm{Aut}(S)$ of 'very large' degree, namely $\theta(1) > |S|^{3/8}$, see Theorem 2.1. This result helps us to reduce Theorem 1.2 to a question on characteristically simple groups, which are then handled in Theorem 1.4 as mentioned above. We believe that Theorem 2.1 will have other applications in problems involving characters of large degree. The case $S \cong \mathrm{PSL}_2(q)$ turns out to be surprisingly complicated and requires delicate treatment, and is done in Sects. 5 and 6.

2. Extendible characters of simple groups

In this section we will show that a non-abelian simple group $S \ncong \mathrm{PSL}_2(q)$ has an irreducible character extendible to $\mathrm{Aut}(S)$ of very large degree. The following theorem is a key tool toward the proof of Theorem 1.2 in the case $S \ncong \mathrm{PSL}_2(q)$.

Theorem 2.1. *Let S be a non-abelian simple group not isomorphic to $\mathrm{PSL}_2(q)$ where q is a prime power. Then S has an irreducible character θ extendible to $\mathrm{Aut}(S)$ such that $\theta(1) > |S|^{3/8}$.*

Remark. The exclusion of $\mathrm{PSL}_2(q)$ in the theorem is necessary since $|\mathrm{PSL}_2(q)| = q(q^2-1)/(2, q-1)$ and $b(\mathrm{PSL}_2(q)) = q$ or $q+1$ for $q \geq 5$.

In the study of Gluck's conjecture [6] concerning the largest character degree and the index of the Fitting subgroup in a finite group, the first author along with J. P. Cossey, Z. Halasi, and A. Maróti have proved that every non-abelian simple group S possesses an irreducible character extendible to $\mathrm{Aut}(S)$ with degree at least $|S|^{1/3}$. Unfortunately this bound is not enough for our current purpose. However, the ideas in the proof of [6, Theorem 12] can be further developed to prove Theorem 2.1.

For the reader's convenience and to prove Theorem 2.1 for the alternating groups, we recall some combinatorics concerning partitions, Young diagrams, and representation theory of the alternating and symmetric groups.

Let n be a positive integer. A finite sequence $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ for some k such that $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$ and $\lambda_1 + \lambda_2 + \cdots + \lambda_k = n$ is said to be a partition of

n. The Young diagram associated to λ, denoted by Y_λ, is defined to be the finite subset of $\mathbb{N} \times \mathbb{N}$ such that $(i, j) \in Y_\lambda$ if and only if $i \leq \lambda_j$.

When two Young diagrams can be transformed into each other when reflected about the line $y = x$, we say that the associated partitions are conjugate. The partition conjugate to λ is denoted by $\overline{\lambda}$. If $\lambda = \overline{\lambda}$ then Y_λ is symmetric and we say that λ is self-conjugate. For each node $(i, j) \in Y_\lambda$, we define the so-called *hook length* $h(i, j)$ to be the number of nodes that are directly above it, directly to the right of it, or equal to it. That is,

$$h(i, j) := 1 + \lambda_j + \overline{\lambda}_i - i - j.$$

It is well-known that there are bijective correspondences between the partitions of n, the Young diagrams of cardinality n, and the irreducible complex characters of S_n. Denote by χ_λ or χ_{Y_λ} the irreducible character of S_n corresponding to λ and Y_λ. The degree of χ_λ is given by the *hook-length formula* of Frame et al. [10]:

$$\chi_\lambda(1) = \chi_{Y_\lambda}(1) = \frac{n!}{\prod_{(i,j)\in Y_\lambda} h(i, j)}.$$

The irreducible characters of A_n can be obtained by restricting those of S_n to A_n. More explicitly, $\chi_\lambda \downarrow_{\mathsf{A}_n} = \chi_{\overline{\lambda}} \downarrow_{\mathsf{A}_n}$ is irreducible of degree $\chi_{\lambda_1}(1)$ if λ is not self-conjugate. Otherwise, $\chi_\lambda \downarrow_{\mathsf{A}_n}$ splits into two different irreducible characters of the same degree $\chi_{\lambda_1}(1)/2$.

Define $A(\lambda)$ to be the set of nodes that can be added to Y_λ to obtain another Young diagram of size $n + 1$. It is known (see [19, §2] for instance) that

$$|A(\lambda)| < \sqrt{2n} + 1.$$

Similarly, define $R(\lambda)$ to be the set of nodes that can be removed from Y_λ to obtain another Young diagram of size $n - 1$. We have

$$|R(\lambda)| < \sqrt{2n}.$$

The branching rule [17, §9.2] asserts that the restriction $\chi_\lambda \downarrow_{\mathsf{S}_{n-1}}$ of χ_λ to S_{n-1} is a sum of irreducible characters $\chi_{Y_\lambda \setminus \{(i,j)\}}$ as (i, j) runs over all nodes in $R(\lambda)$; and the induction $\chi_\lambda^{\mathsf{S}_{n+1}}$ of χ_λ to S_{n+1} is a sum of irreducible characters $\chi_{Y_\lambda \cup \{(i,j)\}}$ as (i, j) runs over all nodes in $A(\lambda)$.

Proof of Theorem 2.1. If S is one of 26 sporadic simple groups or the Tits group, the proof is a case-by-case check from the Atlas [5]. For instance, if $S = M_{12}$—the second Mathieu group—we can choose θ to be the unique irreducible character of degree 176 of S. If S is a simple group of Lie type in characteristic p and $S \ncong \mathrm{PSL}_2(q)$ where q is a prime power, we then realize that S has the so-called *Steinberg character* St_S of degree $\mathrm{St}_S(1) = |S|_p$, the p-part of the order of S. Furthermore, St_S is extendible to $\mathrm{Aut}(S)$ (see [9] for instance). Now we can check the inequality $|S|_p > |S|^{3/8}$ easily by consulting the list of families of simple groups and their orders, see [5, p. xvi] for instance. As an example, when $S = \mathrm{PSL}_n(q)$ with $n \geq 3$, we see that $|S|_p = q^{n(n-1)/2}$ and it is easily checked that

$$|\mathrm{PSL}_n(q)|^{3/8} < q^{3(n^2-1)/8} \leq q^{n(n-1)/2}.$$

So for the rest of this proof we assume that $S = \mathsf{A}_n$ is an alternating group of degree $n \geq 7$. Note that $\mathsf{A}_5 \cong \mathrm{PSL}_2(5)$ and $\mathsf{A}_6 \cong \mathrm{PSL}_2(9)$ are not in our consideration. Let $\rho(\mathsf{A}_n)$ be the largest degree of an irreducible character of A_n that can be extended to S_n. We aim to show that $\rho(\mathsf{A}_n) > (n!/2)^{3/8}$ when $n \geq 7$.

First the theorem can be checked directly by computer for small n, namely $n < 75$. We describe here how it is done. A partition corresponding to a character of S_n of the largest degree is available in [25]. If this partition is not self-conjugate, then the required character θ can be chosen to be the character associated to this partition. So let us assume that this partition is self-conjugate and let Y be the corresponding Young diagram. We consider all the possible Young diagrams obtained from Y by moving one node from one row to another. For all those Young diagrams the degrees of the corresponding irreducible characters are computed and θ can be chosen to be the character of the largest degree among these characters.

Now we may assume that $n \geq 75$. In fact, we will prove by induction on $n \geq 75$ that $\rho(\mathsf{A}_{n+1}) \geq (n+1)^{3/8}\rho(\mathsf{A}_n)$ and this implies that $\rho(\mathsf{A}_n) > (n!/2)^{3/8}$ immediately.

Let ψ be an irreducible character of A_n with $n \geq 75$ such that ψ is extendible to S_n and $\psi(1) = \rho(\mathsf{A}_n)$. Let χ be an extension of ψ to S_n and let λ and Y be respectively the partition and the Young diagram associated to χ. By the branching rule, we have

$$\chi^{\mathsf{S}_{n+1}} = \sum_{(i,j)\in A(\lambda)} \chi_{Y\cup\{(i,j)\}}.$$

Assume that all the Young diagrams in $\{Y \cup \{(i, j)\} | (i, j) \in A(\lambda)\}$ are non-symmetric. Then all the irreducible characters $\chi_{Y\cup\{(i,j)\}}$ where $(i, j) \in A(\lambda)$ restrict irreducibly to A_{n+1}, and thus

$$\chi_{Y\cup\{(i,j)\}}(1) \leq \rho(\mathsf{A}_{n+1}).$$

We therefore deduce that

$$\chi^{\mathsf{S}_{n+1}}(1) \leq |A(\lambda)|\rho(\mathsf{A}_{n+1}).$$

Since $|A(\lambda)| < \sqrt{2n} + 1$ and $\chi^{\mathsf{S}_{n+1}}(1) = (n+1)\rho(\mathsf{A}_n)$, it follows that $(n+1)\rho(\mathsf{A}_n) < (\sqrt{2n}+1)\rho(\mathsf{A}_{n+1})$, and hence

$$\rho(\mathsf{A}_{n+1}) > \frac{n+1}{\sqrt{2n}+1}\rho(\mathsf{A}_n).$$

When $n \geq 75$, we can check that $(n+1)/(\sqrt{2n}+1) > (n+1)^{3/8}$. Therefore we conclude that $\rho(\mathsf{A}_{n+1}) > (n+1)^{3/8}\rho(\mathsf{A}_n)$, as desired.

It remains to assume that there is a symmetric Young diagram of the form $Y \cup \{(i, j)$ with $(i, j) \in A(\lambda)$. Then there is exactly one such diagram and at most $\sqrt{2n}$ non-symmetric diagrams in $\{Y \cup \{(i, j)\} | (i, j) \in A(\lambda)\}$. Let Y' be that symmetric Young diagram and μ be the corresponding partition. By the branching rule, we have

$$\chi_{Y'}\downarrow_{\mathsf{S}_n} = \sum_{(i,j)\in R(\mu)} \chi_{Y'\setminus\{(i,j)\}}.$$

We distinguish two cases:

(1) All the Young diagrams of the form $Y'\backslash\{(i,\ j)\}$ where $(i,\ j) \in R(\mu)$ are non-symmetric. Then the characters associated to these diagrams restrict irreducibly to A_n and thus their degrees are at most $\rho(\mathsf{A}_n)$. As $|R(\mu)| < \sqrt{2n+2}$, we deduce that

$$\chi_{Y'}(1) = \sum_{(i,j)\in R(\mu)} \chi_{Y'\backslash\{(i,j)\}}(1) < \sqrt{2n+2}\rho(\mathsf{A}_n).$$

We then have

$$\begin{aligned}(n+1)\rho(\mathsf{A}_n) &= \sum_{(i,j)\in A(\lambda)} \chi_{Y\cup\{(i,j)\}}(1)\\ &= \chi_{Y'}(1) + \sum_{(i,j)\in A(\lambda), Y\cup\{(i,j)\}\neq Y'} \chi_{Y\cup\{(i,j)\}}(1)\\ &< \sqrt{2n+2}\rho(\mathsf{A}_n) + \sum_{(i,j)\in A(\lambda), Y\cup\{(i,j)\}\neq Y'} \chi_{Y\cup\{(i,j)\}}(1).\end{aligned}$$

Since $\chi_{Y\cup\{(i,j)\}}(1) \leq \rho(\mathsf{A}_{n+1})$ whenever $Y \cup \{(i,\ j)\} \neq Y'$, it follows that

$$\begin{aligned}(n+1)\rho(\mathsf{A}_n) &< \sqrt{2n+2}\rho(\mathsf{A}_n) + (|\mathsf{A}(\lambda)| - 1)\,\rho\,(\mathsf{A}_{n+1})\\ &< \sqrt{2n+2}\rho(\mathsf{A}_n) + \sqrt{2n}\rho\,(\mathsf{A}_{n+1})\,.\end{aligned}$$

Thus

$$\rho\,(\mathsf{A}_{n+1}) > \frac{n+1-\sqrt{2n+2}}{\sqrt{2n}}\rho\,(\mathsf{A}_n)\,.$$

Again, as $n \geq 75$ we now can easily deduce that $\rho(\mathsf{A}_{n+1}) > (n+1)^{3/8}\rho(\mathsf{A}_n)$.

(2) There is a symmetric Young diagram of the form $Y'\backslash\{(i,\ j)\}$ where $(i,\ j) \in R(\mu)$. Let Y'' be this symmetric Young diagram and ν be the associated partition. Then Y'' is the only one symmetric diagram and there are at most $\sqrt{2n+2}-1$ non-symmetric diagrams in $\{Y'\backslash\{(i,\ j)\}|(i,\ j) \in R(\mu)\}$. So we have two symmetric Young diagrams Y' and Y'' and Y'' is obtained from Y' by removing a node. Therefore, if another node is removed from Y'' to get a Young diagram (of size $n-1$), the resulting diagram cannot be symmetric. Therefore, by the branching rule,

$$\chi_{Y''}(1) < \sqrt{2n}\rho\,(\mathsf{A}_{n-1})\,.$$

It follows that

$$\chi_{Y'}(1) < \sqrt{2n}\rho\,(\mathsf{A}_{n-1}) + \left(\sqrt{2n+2}-1\right)\rho(\mathsf{A}_n).$$

Therefore,

$$\begin{aligned}(n+1)\rho(\mathsf{A}_n) &= \chi_{Y'}(1) + \sum_{(i,j)\in A(\lambda), Y\cup\{(i,j)\}\neq Y'} \chi_{Y\cup\{(i,j)\}}(1)\\ &< \sqrt{2n}\rho(\mathsf{A}_{n-1}) + \left(\sqrt{2n+2}-1\right)\rho(\mathsf{A}_n) + \sqrt{2n}\rho(\mathsf{A}_{n+1}).\end{aligned}$$

Using the induction hypothesis that $\rho(\mathsf{A}_{n-1}) \leq n^{-3/8}\rho(\mathsf{A}_n)$, we then have

$$\rho\left(\mathsf{A}_{n+1}\right) > \frac{n+2-\sqrt{2n+2}-\sqrt{2n}n^{-3/8}}{\sqrt{2n}}\rho\left(\mathsf{A}_n\right).$$

Now with $n \geq 75$ we can check that

$$\frac{n+2-\sqrt{2n+2}-\sqrt{2n}n^{-3/8}}{\sqrt{2n}} > (n+1)^{3/8},$$

and the proof is complete. □

3. Simple groups

In this section we prove Theorem 1.4, and then deduce Theorems 1.2 and 1.3 for characteristically simple groups. This will be used in the proof for arbitrary groups. We restate Theorem 1.4 here.

Theorem 3.1. *Let S be a non-abelian simple group. Then $|S| > 2b(S)^2$. Consequently, if $|S| = d(d+e)$ where d is the degree of some irreducible character of S then $|S| < 2e^2$.*

Let $\mathrm{Irr}(G)$ denote the set of irreducible character of G. Motivated by the problem of improving Snyder's bound, Isaacs [16] introduced and studied the invariant

$$\varepsilon(S) := \frac{\sum_{\chi\in\mathrm{Irr}(S),\chi(1)<b(S)}\chi(1)^2}{b(S)^2}$$

for non-abelian simple groups S. He raised the question whether the largest character degree of S can be bounded in terms of smaller degrees in the sense that $\varepsilon(S) \geq \varepsilon$ for some universal constant $\varepsilon > 0$ and for all non-abelian simple groups S. This was answered in the affirmative in [19] with the bounding constant ε taken to be $2/(120{,}000!)$. We note that this rather small bound comes from the alternating groups, see [19, Theorem 2.1 and Corollary 2.2] for more details.

To further improve the bound from Be^6 to e^6+e^4, Isaacs even predicted that $\varepsilon(S) > 1$ for every non-abelian simple group S. This was in fact confirmed in [19] for the majority of simple classical groups, and for all simple exceptional groups of Lie type as well as sporadic simple groups. Recently, Z. Halasi, C. Hannusch, and the first author have confirmed that indeed $\varepsilon(\mathsf{A}_n) > 1$ for every $n \geq 5$, see [14].

One easily sees that if $\varepsilon(S) > 1$ then $e > b(S) \geq d$ so that $2b(S)^2 < |S| < 2e^2$, and Theorem 3.1 is proved for the simple group S. Furthermore, when S has a unique irreducible character of the largest degree $b(S)$, $|S| > 2b(S)^2$ is equivalent to $\varepsilon(S) > 1$. Therefore Theorem 3.1 can be viewed as a weak form of Isaacs's prediction.

To prove Theorem 3.1, we will use Lusztig's classification of complex irreducible characters of finite groups of Lie type (see [7, Chapter 13] and [4, §13.8]) and detailed structure of the centralizers of semisimple elements in finite classical groups (see for instance [32, Section 3], [28, Section 2], and [3, Section 2]). We first record two observations.

Lemma 3.2. *Let $q \geq 2$. Then* $\prod_{i=2}^{\infty}(1 - 1/q^i) > 9/16$.

Proof. This is [19, Lemma 4.1(ii)]. □

Let $f \in \mathbb{F}_q[t]$ be an irreducible monic polynomial. In what follows, we will write $\widetilde{f}$ for the polynomial over $\mathbb{F}_q[t]$ whose roots are $\{\alpha^{-1} | \alpha \text{ is a root of } f\}$. Note that if $f = \widetilde{f}$, then the $\deg(f)$ is necessarily even. Moreover, [26, Theorem 3] gives a formula for the number of f satisfying $f = \widetilde{f}$, which yields the following lemma.

Lemma 3.3. *Let $S_2(d)$ be the number of irreducible monic polynomial over $\mathbb{F}_2$ of degree $2d$ satisfying $f = \widetilde{f}$. Then $S_2(1) = S_2(2) = S_2(3) = 1$; $S_2(4) = 2$; $S_2(5) = 3$; $S_2(6) = 5$; $S_2(7) = 9$; and $S_2(d) \geq 16$ for $d \geq 8$.*

Proof. This is straightforward from [26, Theorem 3]. □

Proof of Theorem 3.1. Since the inequality $\varepsilon(S) > 1$ has been established for all the simple exceptional groups of Lie type, the sporadic simple groups, and the alternating groups, it remains to prove the theorem for the simple classical groups.

Further, we note that we only need to consider those classical groups of Lie type excluded from [19, Theorem 4.7]. That is, we must consider the simple groups found in the following list:

$$\begin{aligned}
&\mathrm{SL}_n(2),\ \mathrm{Sp}_{2n}(2),\ \Omega^{\pm}_{2n}(2),\\
&\mathrm{PSL}_n(3) \text{ with } 5 \leq n \leq 14,\ \mathrm{PSU}_n(2) \text{ with } 7 \leq n \leq 14,\\
&\mathrm{PSp}_{2n}(3) \text{ or } \Omega_{2n+1}(3) \text{ with } 4 \leq n \leq 17,\ \mathrm{P}\Omega^{\pm}_{2n}(3) \text{ with } 4 \leq n \leq 30,\\
&\mathrm{P}\Omega^{\pm}_{8}(7),\ \text{ and } \mathrm{P}\Omega^{\pm}_{2n}(5) \text{ with } 4 \leq n \leq 6.
\end{aligned}$$

We will make use of some of the ideas used in [19], as well as the list of character degrees of small rank groups of Lie type available on Lübeck's website [22].

When the rank is at most 8 all the character degrees of the simply connected group G of the same type as S in this list can be found from [22], and one can use this to check that in fact $|S| > 2b(G)^2 \geq 2b(S)^2$, which implies that $e > b(S)$ and hence $|S| < 2e^2$. So we assume that S is one of the groups listed above with $n \geq 9$ (and $n \geq 10$ for type A).

(1) First, let S be $\mathrm{PSL}_n(3)$, $\mathrm{PSU}_n(2)$, $\mathrm{PSp}_{2n}(3)$, $\Omega_{2n+1}(3)$, $\mathrm{P}\Omega^{\pm}_{2n}(3)$, $\mathrm{P}\Omega^{\pm}_{8}(7)$, or $\mathrm{P}\Omega^{\pm}_{2n}(5)$, with n as above, but larger than 8. Note that by Seitz [30, Theorem 2.1],

$$b(S) \leq b(G) \leq |G : T|_{q'},$$

where q is the size of the underlying field for S, G is the group of fixed points for the simple simply connected algebraic group corresponding to S, and T is a maximal torus of G of minimal order. The size of T is $(q-1)^n$ (or $(q-1)^{n-1}$ for $\mathrm{PSL}_n(q)$) if S is of untwisted type, and can be found, for example, in [19, Table 1]

if S is of twisted type. We may check directly using this bound for $b(S)$ that in fact, $|S| > 2b(S)^2$ for each group in this finite list. This shows that if S is one of

$$\begin{aligned}&\mathrm{PSL}_n(3) \text{ with } 5 \le n \le 14,\ \mathrm{PSU}_n(2) \text{ with } 7 \le n \le 14,\\ &\mathrm{PSp}_{2n}(3) \text{ or } \Omega_{2n+1}(3) \text{ with } 4 \le n \le 17,\ \mathrm{P}\Omega^{\pm}_{2n}(3) \text{ with } 4 \le n \le 30,\\ &\mathrm{P}\Omega^{\pm}_{8}(7),\ \text{and } \mathrm{P}\Omega^{\pm}_{2n}(5) \text{ with } 4 \le n \le 6,\end{aligned}$$

then $2b(S)^2 < |S| < 2e^2$.

(2) Now let S be one of the groups $\mathrm{SL}_n(2)$, $\mathrm{Sp}_{2n}(2)$, or $\Omega^{\pm}_{2n}(2)$, and assume $n \ge 10$ in the first case and $n \ge 9$ in the latter two cases. Then $S^* \cong S$ is self-dual and the center of the corresponding algebraic group is trivial. We make the identification $S^* \cong S$, and hence by Lusztig's classification of complex irreducible characters of finite groups of Lie type, $\mathrm{Irr}(S)$ is parametrized by pairs $((s), \theta)$, where (s) is a semisimple conjugacy class in S and $\theta \in \mathrm{Irr}(\mathbf{C}_S(s))$ is a unipotent character. Further, the character parametrized by $((s), \theta)$ has degree

$$[S : \mathbf{C}_S(s)]_{2'}\theta(1).$$

Notice that if there are at least two $\chi \in \mathrm{Irr}(S)$ satisfying $\chi(1) = b(S)$, then certainly $|S| > 2b(S)^2$, and hence $|S| < 2e^2$. Therefore, we may further assume that there is a unique such χ.

Notice that the centralizer of a semisimple element s of S is of the form

$$\mathbf{C}_S(s) \cong K \times H_1 \times \cdots \times H_r,$$

where each H_i is of the form $\mathrm{GL}^{\epsilon_i}_{k_i}(2^{d_i})$, ϵ_i is $+$ in the linear case and $\pm$ for the symplectic and orthogonal cases, K is trivial in the linear case, $\mathrm{Sp}_{2m}(2)$ in the symplectic case, and in the orthogonal case, we may assume by the argument toward the beginning of [19, Part (3) of Proof of Theorem 4.8] that K is $\Omega^{\pm}_{2m}(2)$. (Indeed, by Tiep and Zalesskiĭ [32, Theorem 3.7], $\mathbf{C}_S(s) \cong K_1 \times H_2 \times \cdots \times H_r$ where each H_i is as described above, and K_1 has a normal subgroup isomorphic to $\Omega^{\pm}_{2m}(2)$ with either trivial quotient or quotient isomorphic to $\mathrm{GU}_2(2)$. Since St_{K_1} in the latter case has degree $2^{m(m-1)+1}$, there is no loss in assuming $\mathbf{C}_S(s) \cong K \times H_1 \times H_2 \times \cdots \times H_r$ with K as stated.) Note that we use the notation $\mathrm{GL}^{+}_{k}(2^d) := \mathrm{GL}_k(2^d)$ and $\mathrm{GL}^{-}_{k}(2^d) := \mathrm{GU}_k(2^d)$. Further, $\sum k_i d_i + m = n$, and the K and H_i are determine by the elementary divisors of s acting on the natural module $\mathbb{F}_2^n$ or $\mathbb{F}_2^{2n}$ for S. Namely, if $S = \mathrm{Sp}_{2n}(2)$ or $\Omega^{\pm}_{2n}(2)$, a factor of $H_i \cong \mathrm{GL}_{k_i}(2^{d_i})$ corresponds to a pair of monic polynomials $g_i(t)\widetilde{g}_i(t)$ in $\mathbb{F}_2[t]$ with multiplicity k_i, where $g_i \ne \widetilde{g}_i$ are irreducible of degree d_i. Moreover, $H_i \cong \mathrm{GU}_{k_i}(d^{d_i})$ corresponds to a monic irreducible $f_i(t) \ne t - 1$ with degree $2d_i$ and multiplicity k_i, where $f = \widetilde{f}$. In these cases, K corresponds to the elementary divisor $t - 1$, with multiplicity $2m$. If $S = \mathrm{SL}_n(2)$, each elementary divisor $f_i(t)$ with degree d_i and multiplicity k_i yields a factor $H_i \cong \mathrm{GL}_{k_i}(2^{d_i})$.

Let $\chi \in \mathrm{Irr}(S)$ satisfying $\chi(1) = b(S)$ be parametrized by $((s), \theta)$. Then by Larsen et al. [19, Theorem 1.2], θ must be the Steinberg character $\mathrm{St}_{\mathbf{C}_S(s)}$ of $\mathbf{C}_S(s)$. Recall that the Steinberg character of $\mathrm{GL}^{\pm}_{k}(2^d)$ has degree $2^{dn(n-1)/2}$, the Steinberg

character of $\mathrm{Sp}_{2m}(2)$ has degree 2^{m^2}, and the Steinberg character of $\Omega^{\pm}_{2m}(2)$ has degree $2^{m(m-1)}$.

Moreover, by our assumption that χ is the unique member of $\mathrm{Irr}(S)$ satisfying $\chi(1) = b(S)$, we see that it must be the case that every polynomial of a given degree and type as described above must appear as an elementary divisor of s with the same multiplicity. (Indeed, otherwise, we may find another semisimple element $s' \in S$ not conjugate to s with $\mathbf{C}_S(s) \cong \mathbf{C}_S(s')$, and hence the character parametrized by $((s'), \mathrm{St}_{\mathbf{C}_S(s')})$ has degree $b(S)$ as well.)

We will proceed using some estimates for the number of monic irreducible polynomials of a given type as above.

Let $S = \Omega^{\epsilon}_{2n}(2)$. We present the complete proof in this case and note that the proof in the other two cases are similar, though less complicated.

(3) First, if no factors of the form $\mathrm{GL}^{\pm}_{k_i}(2^{d_i})$ appears in $\mathbf{C}_{G^*}(s)$, then we see that $\chi = \mathrm{St}$ has degree $2^{n(n-1)}$. Otherwise, write $\mathbf{C}_S(s) \cong \Omega^{\beta}_{2m}(2) \times \mathrm{GL}^{\epsilon_1}_{k_1}(2^{d_1}) \times \mathrm{GL}^{\epsilon_2}_{k_2}(2^{d_2}) \times \cdots \times \mathrm{GL}^{\epsilon_r}_{k_r}(2^{d_r})$ with $r \geq 1$. In this case,

$$\begin{aligned}
\chi(1) &= 2^{m(m-1)+\sum_{\ell=1}^{r} d_\ell k_\ell (k_\ell-1)/2} \frac{(2^n-\epsilon)\prod_{j=m}^{n-1}\left(2^{2j}-1\right)}{(2^m-\beta)\prod_{\ell=1}^{r}\left(\prod_{i=1}^{k_\ell}\left(2^{id_\ell}-\epsilon_\ell^i\right)\right)} \\
&= 2^{m(m-1)+\sum_{\ell=1}^{r} d_\ell k_\ell (k_\ell-1)/2} \frac{(2^m+\beta)\prod_{j=m+1}^{n}\left(2^{2j}-1\right)}{(2^n+\epsilon)\prod_{\ell=1}^{r}\left(\prod_{i=1}^{k_\ell}\left(2^{id_\ell}-\epsilon_\ell^i\right)\right)} \\
&= \frac{2^{m(m-1)+\sum_{\ell=1}^{r} d_\ell k_\ell (k_\ell-1)/2}}{2^{\sum_{\ell=1}^{r} d_\ell k_\ell (k_\ell+1)/2}} \frac{(2^m+\beta)\prod_{j=m+1}^{n}\left(2^{2j}-1\right)}{(2^n+\epsilon)\prod_{\ell=1}^{r}\left(\prod_{i=1}^{k_\ell}\left(1-\left(\epsilon_\ell/2^{d_\ell}\right)^i\right)\right)} \\
&\leq \left(\frac{16}{9}\right)^r \left(\frac{2^m+1}{2^n-1}\right) \frac{2^{n(n+1)-m(m+1)+m(m-1)+\sum_{\ell=1}^{r} d_\ell k_\ell (k_\ell-1)/2}}{2^{\sum_{\ell=1}^{r} d_\ell k_\ell (k_\ell+1)/2}} \\
&= \left(\frac{16}{9}\right)^r \left(\frac{1+1/2^m}{1-1/2^n}\right) \frac{2^{m+n(n+1)-m(m+1)+m(m-1)+\sum_{\ell=1}^{r} d_\ell k_\ell (k_\ell-1)/2}}{2^{n+\sum_{\ell=1}^{r} d_\ell k_\ell (k_\ell+1)/2}} \\
&= \left(\frac{16}{9}\right)^r \left(\frac{1+1/2^m}{1-1/2^n}\right) 2^{n(n-1)} \\
&\leq \left(\frac{16}{9}\right)^r \left(\frac{3}{2}\right)\left(\frac{512}{511}\right) 2^{n(n-1)}.
\end{aligned}$$

Note that the bound remains true if $m = 0$, and that we have used Lemma 3.2 and the fact that $n \geq 9$. If $0 \leq r \leq 3$, this calculation (together with the first observation for the case $r = 0$) yields that

$$\chi(1) < 9 \cdot 2^{n(n-1)},$$

so we see

$$\frac{|S|}{\chi(1)^2} > \left(\frac{1}{9}\right)^2 \frac{(2^n-1)\prod_{i=1}^{n-1}\left(2^{2i}-1\right)}{2^{n(n-1)}} = \frac{1}{81}\frac{(2^n-1)\,2^{n(n-1)}\prod_{i=1}^{n-1}\left(1-1/2^{2i}\right)}{2^{n(n-1)}}$$

and by Lemma 3.2,

$$\frac{|S|}{\chi(1)^2} > \left(\frac{1}{81}\right)\left(\frac{9}{16}\right)\left(2^n-1\right),$$

which is larger than 2 since $n \geq 9$. Hence we see that $|S| > 2\chi(1)^2 = 2b(S)^2$ if $r \leq 3$. We may therefore assume that

$$\mathbf{C}_S(s) \cong \Omega_{2m}^{\beta}(2) \times \mathrm{GL}_{k_1}^{\epsilon_1}\left(2^{d_1}\right) \times \mathrm{GL}_{k_2}^{\epsilon_2}\left(2^{d_2}\right) \times \cdots \times \mathrm{GL}_{k_r}^{\epsilon_r}\left(2^{d_r}\right)$$

with $r \geq 4$, and assume $d_1k_1 \geq d_2k_2 \geq \cdots \geq d_rk_r$.

(4) Our strategy for the remainder of the proof is to consider semisimple elements $t \in S$ and the characters ψ corresponding to $(t, \mathrm{St}_{\mathbf{C}_S(t)})$. We will show that there are a sufficient number of such semisimple elements with $\psi(1)/\chi(1)$ large enough to imply that $\epsilon(S) > 1$, and therefore that $|S| < 2e^2$.

Let $\mathfrak{F}$ denote the set of all monic polynomials $f \neq t-1$ over $\mathbb{F}_2$ which are either irreducible satisfying $f = \widetilde{f}$ or of the form $f = g\widetilde{g}$ where $g \neq \widetilde{g}$ are irreducible. For $f \in \mathfrak{F}$, write $\epsilon_f = -1$ if f is irreducible and $\epsilon_f = 1$ if $f = g\widetilde{g}$, and write d_f for the degree of f. Then given that $\kappa : \mathfrak{F} \to \mathbb{N}$ is a function satisfying $n-m = \frac{1}{2}\sum_{f\in\mathfrak{F}} d_f\kappa(f)$ and $\prod_{f\in\mathfrak{F}}(\epsilon_f)^{\kappa_f} = \prod_{i=1}^{r}(\epsilon_i)_i^k$, there exists a semisimple $t \in S$ with corresponding multiplicities $\kappa(f)$ for the polynomials f as elementary divisors, and hence

$$\mathbf{C}_S(t) \cong \Omega_{2m}^{\beta}(2) \times \prod_{f\in\mathfrak{F}} \mathrm{GL}_{\kappa(f)}^{\epsilon_f}\left(2^{d_f/2}\right).$$

Now, notice that there are at least two pairs (i, j) with $4 \geq i > j \geq 1$ such that $d_ik_i + d_jk_j$ is even. Moreover, these pairs satisfy $d_ik_i + d_jk_j \geq 4$ since the combination $(d_\ell, k_\ell) = (1, 1)$ can occur at most once. Also note that if a factor of the form $\mathrm{GL}_k^{\pm}(2^{k_id_i+k_jd_j})$ appears in $\mathbf{C}_S(s)$, it must be that $(k, k_id_i + k_jd_j) = (k_1, d_1)$ or (k_2, d_2) and if $\mathrm{GU}_k(2^{(k_id_i+k_jd_j)/2})$ appears, then $(k_id_i + k_jd_j)/2 \in \{d_1, \ldots, d_4\}$ (and correspondingly $k \in \{k_1, \ldots, k_4\}$).

We consider four situations:

(i) $\mathrm{GL}_k^{\epsilon}(2^{k_id_i+k_jd_j})$ is not a factor of $\mathbf{C}_S(s)$, in which case we will consider a semisimple element $t \in S$ with

$$\mathbf{C}_S(t) \cong \Omega_{2m}^{\beta}(2) \times \mathrm{GL}_1^{\epsilon}\left(2^{k_id_i+k_jd_j}\right) \times \prod_{\ell\in\{1,\ldots,r\}\setminus\{i,j\}} \mathrm{GL}_{k_\ell}^{\epsilon_\ell}\left(2^{d_\ell}\right).$$

(ii) $\mathrm{GL}_k^{\epsilon}(2^{k_id_i+k_jd_j})$ is a factor of $\mathbf{C}_S(s)$, in which case we will consider a semisimple element $t \in S$ with

$$\mathbf{C}_S(t) \cong \Omega_{2m}^{\beta}(2) \times \mathrm{GL}_{k+1}^{\epsilon}\left(2^{k_id_i+k_jd_j}\right) \times \mathrm{GL}_{k_\ell}^{\epsilon_\ell}\left(2^{d_\ell}\right) \times \mathrm{GL}_{k_5}^{\epsilon_5}\left(2^{d_5}\right) \cdots \times \mathrm{GL}_{k_r}^{\epsilon_r}\left(2^{d_r}\right)$$

where we write $\ell \in \{1, \ldots, 4\}$ so that $\ell \neq i, j$, or the index corresponding to $(k, k_id_i + k_jd_j)$.

(iii) $\mathrm{GU}_k(2^{(k_id_i+k_jd_j)/2})$ is not a factor of $\mathbf{C}_S(s)$, in which case we consider a semisimple element $t \in S$ with

$$\mathbf{C}_S(t) \cong \Omega^{\beta}_{2m}(2) \times \mathrm{GU}_2\left(2^{(k_id_i+k_jd_j)/2}\right) \times \prod_{\ell \in \{1,\ldots,r\}\setminus\{i,j\}} \mathrm{GL}^{\epsilon_\ell}_{k_\ell}\left(2^{d_\ell}\right).$$

(iv) $\mathrm{GU}_k(2^{(k_id_i+k_jd_j)/2})$ is a factor of $\mathbf{C}_S(s)$, in which case we consider a semisimple element $t \in S$ with

$$\begin{aligned}\mathbf{C}_S(t) \cong \Omega^{\beta}_{2m}(2) \times \mathrm{GU}_{k+2}\left(2^{(k_id_i+k_jd_j)/2}\right) \times \mathrm{GL}^{\epsilon_\ell}_{k_\ell}\left(2^{d_\ell}\right)\\ \times \mathrm{GL}^{\epsilon_5}_{k_5}\left(2^{d_5}\right) \cdots \times \mathrm{GL}^{\epsilon_r}_{k_r}\left(2^{d_r}\right)\end{aligned}$$

where we write $\ell \in \{1, \ldots, 4\}$ so that $\ell \neq i, j$, or the index corresponding to $(k, (k_id_i + k_jd_j)/2)$.

Note that for situations (iii) and (iv), it must be that $\epsilon_i^{k_i}\epsilon_j^{k_j} = 1$. In each situation, we will let $\psi \in \mathrm{Irr}(S)$ correspond to $(t, \mathrm{St}_{\mathbf{C}_S(t)})$, and arrive at lower bounds for $\frac{\psi(1)}{\chi(1)}$. Note that from the last paragraph of part (3) of the proof of [19, Theorem 4.8], we have that in situation (i), $\psi(1)/\chi(1) > \frac{81}{320}$. We use similar arguments in the remaining situations.

Consider situation (ii). For simplicity in the calculation, rewrite (i, j) as $(1, 2)$ and write $d_0 := d_1k_1 + d_2k_2$. Then

$$\begin{aligned}\frac{\psi(1)}{\chi(1)} &= \frac{2^{d_0k(k+1)/2}\prod_{\nu=1}^{k_1}\left(2^{\nu d_1} - (\epsilon_1)^\nu\right)\prod_{\nu=1}^{k_2}\left(2^{\nu d_2} - (\epsilon_2)^\nu\right)\prod_{\nu=1}^{k}(2^{\nu d_0} - \epsilon^\nu)}{2^{d_0k(k-1)/2+d_1k_1(k_1-1)/2+d_2k_2(k_2-1)/2}\prod_{\nu=1}^{k+1}\left(2^{\nu d_0} - \epsilon^\nu\right)}\\
&= \frac{2^{d_0k}\prod_{\nu=1}^{k_1}\left(2^{\nu d_1} - (\epsilon_1)^\nu\right)\prod_{\nu=1}^{k_2}\left(2^{\nu d_2} - (\epsilon_2)^\nu\right)}{2^{d_1k_1(k_1-1)/2+d_2k_2(k_2-1)/2}(2^{kd_0+d_0} - \epsilon^{k+1})}\\
&> \frac{4}{5}\cdot\frac{\prod_{\nu=1}^{k_1}\left(2^{\nu d_1} - (\epsilon_1)^\nu\right)\prod_{\nu=1}^{k_2}\left(2^{\nu d_2} - (\epsilon_2)^\nu\right)}{2^{d_1k_1(k_1-1)/2+d_2k_2(k_2-1)/2+d_0}}\\
&= \frac{4}{5}\cdot\frac{2^{d_1k_1(k_1+1)/2+d_2k_2(k_2+1)/2}\prod_{\nu=1}^{k_1}\left(1 - \left(\epsilon_1/2^{d_1}\right)^\nu\right)\prod_{\nu=1}^{k_2}\left(1 - \left(\epsilon_2/2^{d_2}\right)^\nu\right)}{2^{d_1k_1(k_1-1)/2+d_2k_2(k_2-1)/2+d_0}}\\
&= \frac{4}{5}\cdot 2^{d_1k_1+d_2k_2-d}\cdot\prod_{\nu=1}^{k_1}\left(1 - \left(\epsilon_1/2^{d_1}\right)^\nu\right)\prod_{\nu=1}^{k_2}\left(1 - \left(\epsilon_2/2^{d_2}\right)^\nu\right)\\
&> \frac{4}{5}\cdot(9/16)^2 = \frac{81}{320}\end{aligned}$$

by Lemma 3.2, since $(d_j, \epsilon_j) \neq (1, 1)$ for any j. In the third line, we have also used the fact that $2^{kd+d} + 1 \leq \frac{5}{4}2^{kd_0+d_0}$ since certainly $kd + d \geq 2$.

Now, consider situation (iii), and again for simplicity rewrite (i, j) as $(1, 2)$ and write $d_0 := d_1k_1 + d_2k_2$. Then

$$\begin{aligned}\frac{\psi(1)}{\chi(1)} &= \frac{2^{d_0/2}\cdot\prod_{\nu=1}^{k_1}\left(2^{\nu d_1}-(\epsilon_1)^\nu\right)\prod_{\nu=1}^{k_2}\left(2^{\nu d_2}-(\epsilon_2)^\nu\right)}{2^{d_1k_1(k_1-1)/2+d_2k_2(k_2-1)/2}\cdot\left(2^{d_0/2}+1\right)\left(2^{d_0}-1\right)}\\ &> \frac{2^{d_0/2}}{2^{d_0/2}+1}\cdot\frac{\prod_{\nu=1}^{k_1}\left(2^{\nu d_1}-(\epsilon_1)^\nu\right)\prod_{\nu=1}^{k_2}\left(2^{\nu d_2}-(\epsilon_2)^\nu\right)}{2^{d_1k_1(k_1-1)/2+d_2k_2(k_2-1)/2+d_0}}\\ &> \frac{81}{256}\cdot\frac{2^{d_0/2}}{2^{d_0/2}+1}\\ &\geq \frac{81}{256}\cdot\frac{4}{5}=\frac{81}{320}\end{aligned}$$

where the last inequality is since $d_0 \geq 4$, and the second-to-last is by the same argument as situation (ii).

Finally, consider situation (iv). As before, write (i, j) as $(1, 2)$, and $d_0 := d_1k_1 + d_2k_2$. We have

$$\begin{aligned}&\frac{\psi(1)}{\chi(1)}\\ &= \frac{2^{d_0(k+2)(k+1)/4}\cdot\prod_{\nu=1}^{k_1}(2^{\nu d_1}-(\epsilon_1)^\nu)\prod_{\nu=1}^{k_2}\left(2^{\nu d_2}-(\epsilon_2)^\nu\right)\prod_{\nu=1}^{k}\left(2^{\nu d/2}-(-1)^\nu\right)}{2^{dk(k-1)/4+d_1k_1(k_1-1)/2+d_2k_2(k_2-1)/2}\cdot\prod_{\nu=1}^{k+2}\left(2^{\nu d_0/2}-(-1)^\nu\right)}\\ &= \frac{2^{d_0(k+2)(k+1)/4}\cdot\prod_{\nu=1}^{k_1}\left(2^{\nu d_1}-(\epsilon_1)^\nu\right)\prod_{\nu=1}^{k_2}\left(2^{\nu d_2}-(\epsilon_2)^\nu\right)}{2^{d_0k(k-1)/4+d_1k_1(k_1-1)/2+d_2k_2(k_2-1)/2}\cdot\left(2^{d_0(k+1)/2}-(-1)^{k+1}\right)\left(2^{d_0(k+2)/2}-(-1)^{k+2}\right)}\end{aligned}$$

Now, notice that one of $k + 1$ and $k + 2$ is even, so that

$$\left(2^{d_0(k+1)/2}-(-1)^{k+1}\right)\left(2^{d_0(k+2)/2}-(-1)^{k+2}\right)\leq\frac{17}{16}2^{d_0(k+1)/2+d_0(k+2)/2}$$

since $d_0(k + 1)/2$ and $d_0(k + 2)/2$ are at least 4. Hence

$$\begin{aligned}\frac{\psi(1)}{\chi(1)} &\geq \left(\frac{16}{17}\right)\frac{2^{d_0(k+2)(k+1)/4}\cdot\prod_{\nu=1}^{k_1}\left(2^{\nu d_1}-(\epsilon_1)^\nu\right)\prod_{\nu=1}^{k_2}\left(2^{\nu d_2}-(\epsilon_2)^\nu\right)}{2^{d_0k(k-1)/4+d_1k_1(k_1-1)/2+d_2k_2(k_2-1)/2}\cdot 2^{d_0(k+1)/2+d_0(k+2)/2}}\\ &= \left(\frac{16}{17}\right)\cdot\frac{\prod_{\nu=1}^{k_1}\left(2^{\nu d_1}-(\epsilon_1)^\nu\right)\prod_{\nu=1}^{k_2}\left(2^{\nu d_2}-(\epsilon_2)^\nu\right)}{2^{d_1k_1(k_1-1)/2+d_2k_2(k_2-1)/2+d_0}}\\ &> \left(\frac{16}{17}\right)\left(\frac{81}{256}\right)=\frac{81}{272}.\end{aligned}$$

Hence, in each situation, we see that $\psi(1)/\chi(1) \geq 81/320$. Now, let $d_0 := d_ik_i + d_jk_j$ as above. Suppose that $\epsilon_i^{k_i}\epsilon_j^{k_j} = -1$. Note that for every $f \in \mathfrak{F}$ which is irreducible of degree $2d_0$, we can identify a semisimple element t as in situation (i) or (ii) with $\epsilon = -1$. By Lemma 3.3, there are at least 16 such f as long as $d_0 \geq 8$, yielding at least 16 characters $\psi \in \mathrm{Irr}(S)$ satisfying $\psi(1)/\chi(1) \geq 81/320$ when $d_0 \geq 8$. Hence if $d_0 \geq 8$, we see that $\epsilon(S) \geq 16(81/320)^2 > 1$, and $|S| < 2e^2$.

Now suppose $\epsilon_i^{k_i}\epsilon_j^{k_j} = -1$. Define $\mathfrak{F}_{d_0} \subset \mathfrak{F}$ to be the set of monic polynomials of the form $g\widetilde{g}$ where $g \neq \widetilde{g}$ are irreducible of degree d_0 together with the monic

irreducible polynomials $f \neq t-1$ of degree d_0 such that $f = \widetilde{f}$. Notice that if n_{d_0} is the number of irreducible monic polynomials over $\mathbb{F}_2$ of degree d_0, then $|\mathfrak{F}_{d_0}| \geq n_{d_0}/2$. Moreover, for each choice of $\mathfrak{f} \in \mathfrak{F}_{d_0}$, we can identify a semisimple element $t \in S$ as in one of the cases (i)–(iv), with $\epsilon = 1$ in cases (i) and (ii). This yields at least $n_{d_0}/2$ characters ψ satisfying $\psi(1)/\chi(1) \geq 81/320$. Note that by Larsen et al. [19, (5.1)], if $d_0 \geq 3$, then $n_{d_0} \geq \frac{3\cdot 2^{d_0}}{4d_0}$. Then certainly $|\mathfrak{F}_{d_0}| \geq \frac{n_{d_0}}{2} \geq \frac{3\cdot 2^{d_0}}{8d_0}$ as long as $d_0 \geq 3$, which is at least 12 if $d_0 \geq 8$.

So, if $d_0 \geq 8$ for both choices of (i, j) (recall there must be at least two pairs (i, j) with $d_0 = d_i k_i + d_j k_j$ even), then there are at least 24 characters ψ satisfying $\psi(1)/\chi(1) \geq 81/320$, so that $\epsilon(S) \geq 24 \cdot (81/320)^2 > 1$, and we see in this case that $|S| < 2e^2$.

Finally, considering each possibility for $\mathrm{GL}_{k_i}^{\epsilon_i}(2^{d_i}) \times \mathrm{GL}_{k_j}^{\epsilon_j}(2^{d_j})$ satisfying $d_i k_i + d_j k_j = 4$ or 6, we can use similar (but now more explicit) calculations to show that in each case, $\epsilon(S) > 1$, completing the proof for $\Omega_{2n}^{\pm}(2)$.

We make a final remark about the proofs for $\mathrm{Sp}_{2n}(2)$ and $\mathrm{SL}_n(2)$. In either case, calculations analogous to those in part (3) above yield similar results. The remainder of the proof for $\mathrm{Sp}_{2n}(2)$ follows directly from the calculations in part (4) above for $\Omega_{2n}^{\pm}(2)$, replacing $\Omega_{2m}^{\beta}(2)$ with $\mathrm{Sp}_{2m}(2)$. The analogue to part (4) for $\mathrm{SL}_n(2)$ is similar, but requires only considering case (i) above, with $\epsilon = 1$, together with the estimate for n_d, since each elementary divisor of s yields a factor $\mathrm{GL}_{k_i}(2^{d_i})$ in this case. □

The next observation is useful in the proofs of the main results.

Lemma 3.4. *Let N be a nontrivial proper normal subgroup of G. Assume that $b(G) \leq b(N)b(G/N)$. Then* Theorem 1.2 *is true for G. Furthermore, if $|G| = b(G)(b(G)+e)$ then $e > 2\sqrt{b(G)}$.*

Proof. Write $|N| = b(N)(b(N)+e(N))$, $|G/N| = b(G/N)(b(G/N)+e(G/N))$, and recall that $|G| = b(G)(b(G)+e)$. Then

$$b(G)(b(G)+e) = b(N)b(G/N)(b(N)+e(N))\,(b(G/N)+e(G/N))\,.$$

As $b(G) \leq b(N)b(G/N)$, we deduce that

$$\begin{aligned} e &\geq e(N)e(G/N) + e(N)b(G/N) + b(N)e(G/N) \\ &> e(N)b(G/N) + b(N)e(G/N) \\ &\geq 2\sqrt{b(N)b(G/N)} \\ &\geq 2\sqrt{b(G)}. \end{aligned}$$

Note that, as both N and G/N are nontrivial, $e(N) > 0$ and $e(G/N) > 0$. We now easily deduce that $|G| < e^4 - e^3$. □

Corollary 3.5. Theorems 1.2 *and* 1.3 *are true for every finite group which is direct product of non-abelian simple groups. In particular, they are true for all characteristically simple groups.*

Proof. This follows from Theorem 3.1 and Lemma 3.4. □

4. The case $S \ncong \mathrm{PSL}_2(q)$

With Theorem 2.1 in hand, we are now ready to prove the main results in the case $S \ncong \mathrm{PSL}_2(q)$. First, we recall the following lemma, which will be frequently used from now on.

Lemma 4.1. *Let $N = S \times \cdots \times S$, a direct product of copies of a non-abelian simple group S, be a minimal normal subgroup of G. Assume that $\theta \in \mathrm{Irr}(S)$ is extendible to $\mathrm{Aut}(S)$. Then the product character $\psi := \theta \times \cdots \times \theta \in \mathrm{Irr}(N)$ is extendible to G. Consequently, if $\chi \in \mathrm{Irr}(G)$ is an extension of ψ, then there is a bijection $\beta \leftrightarrow \beta\chi$ between $\mathrm{Irr}(G/N)$ and the set of irreducible characters of G lying above ψ.*

Proof. The first statement of the lemma is well known (see for instance [2, Lemma 5] or [27, Lemma 1]). The second statement follows by Gallagher's theorem, see [15, Corollary 6.17]. □

Theorem 4.2. *Let G be a finite group with a minimal normal subgroup $N = S \times \cdots \times S$, where S is a non-abelian simple group different from $\mathrm{PSL}_2(q)$ for every prime power q. Let $|G| = b(G)(b(G)+e)$. Then $e > \sqrt{b(G)}+1$ and, in particular, $|G| < e^4 - e^3$.*

Proof. Let θ be a character of S found in Theorem 2.1, i.e. θ is extendible to $\mathrm{Aut}(S)$ and $\theta(1) > |S|^{3/8}$. Let $\psi := \theta \times \cdots \times \theta \in \mathrm{Irr}(N)$. Using Lemma 4.1, we deduce that ψ is extended to a character $\chi \in \mathrm{Irr}(G)$ and the mapping $\beta \mapsto \beta\chi$ is a bijection between $\mathrm{Irr}(G/N)$ and the set of irreducible characters of G lying above $\psi \in \mathrm{Irr}(N)$. This implies in particular that $\chi(1)b(G/N)$ is a character degree of G, and whence $b(G) \geq \chi(1)b(G/N)$.

If $b(G) = \chi(1)b(G/N)$, then $b(G) \leq b(N)b(G/N)$ and we are done by Lemma 3.4. So for the rest of the proof we assume that $b(G) > \chi(1)b(G/N)$. This means that the degree of any irreducible character of G lying above ψ is $<b(G)$. We therefore deduce that

$$b(G)e = |G| - b(G)^2 \geq \sum_{\beta \in \mathrm{Irr}(G/N)} (\chi(1)\beta(1))^2 = \chi(1)^2|G/N|.$$

Using the fact that $\chi(1) = \theta(1)^k > |S|^{3k/8} = |N|^{3/8}$, we then obtain

$$b(G)e > |N|^{3/4}|G/N| = |G|/|N|^{1/4}.$$

As the case $G = N$ has been already handled in Corollary 3.5, we may assume that $|G/N| \geq 2$. Also note that $|G| \geq 2|N| \geq 5040$ as 2520 is the size of the smallest simple group not isomorphic to $\mathrm{PSL}_2(q)$. We now easily see that $|G|/|N|^{1/4} > |G|^{3/4} + |G|^{1/2}$. This and the above inequality imply that

$$b(G)e > |G|^{3/4} + |G|^{1/2}.$$

Since $b(G) \leq |G|^{1/2}$, it follows that

$$b(G)e > b(G)^{3/2} + b(G),$$

or equivalently

$$e > b(G)^{1/2} + 1.$$

This implies that $b(G) < e^2 - e$, which in turn implies that

$$|G| = b(G)(b(G) + e) < \left(e^2 - e\right) e^2 = e^4 - e^3,$$

and the theorem is completely proved. □

5. The case $S \cong \mathrm{PSL}_2(q)$ with q even

Characters of the linear groups in dimension 2 are well known and we will use [33] as the main source. In particular, we will follow the notation there.

According to [33, p. 8], when q is even, $\mathrm{SL}_2(q) \cong \mathrm{PSL}_2(q)$ has the following irreducible characters

(i) $1_{\mathrm{SL}_2(q)}$ of degree 1,
(ii) $\mathrm{St}_{\mathrm{SL}_2(q)}$ of degree q,
(iii) χ_i, $1 \leq i \leq (q-2)/2$, of degree $q+1$, and
(iv) θ_j, $1 \leq j \leq q/2$, of degree $q-1$.

Let $q = 2^f$ and φ the field automorphism of order f of $\mathrm{SL}_2(q)$. Then, by White [33, Lemma 4.8], the character $\chi_i \in \mathrm{Irr}(\mathrm{SL}_2(q))$ is invariant under φ^k where $1 \leq k \leq f$ if and only if $(2^f - 1)|i(2^k - 1)$ or $(2^f - 1)|i(2^k + 1)$; and the character $\theta_j \in \mathrm{Irr}(\mathrm{SL}_2(q))$ is invariant under φ^k if and only if $(2^f + 1)|j(2^k - 1)$ or $(2^f + 1)|j(2^k + 1)$. Using this, we can deduce that $\mathrm{SL}_2(2^f)$ has a non-principal irreducible character besides the Steinberg character that is extendible to $\mathrm{Aut}(\mathrm{SL}_2(2^f))$.

Lemma 5.1. *The simple groups* $\mathrm{SL}_2(q)$ *with* $q \geq 8$ *even always have an irreducible character* θ *of degree* $q-1$ *or* $q+1$ *such that* θ *is extendible to* $\mathrm{Aut}(\mathrm{SL}_2(q))$.

Proof. Assume that $q = 2^f$ with $f \geq 3$. From the above discussion, we observe that when f is odd then $3|(2^f + 1)$ and $\theta_{(2^f+1)/3}$ is invariant under φ. On the other hand, when f is even then $3|(2^f - 1)$ and $\chi_{(2^f-1)/3}$ is invariant under φ. So in any case, there is always an irreducible character $\theta \in \mathrm{Irr}(\mathrm{SL}_2(q))$ of degree $q-1$ or $q+1$ such that θ is invariant in $\mathrm{Aut}(\mathrm{SL}_2(q))$. Note that $\mathrm{Aut}(\mathrm{SL}_2(2^f)) = \mathrm{SL}_2(2^f) \rtimes \langle\varphi\rangle$. Thus θ is extendible to $\mathrm{Aut}(\mathrm{SL}_2(q))$, as wanted. □

Lemma 5.2. *Let* $N = \mathrm{PSL}_2(q) \times \cdots \times \mathrm{PSL}_2(q)$, *a direct product of* k *copies of the simple linear group* $\mathrm{PSL}_2(q)$, *is a normal subgroup of* G. *Then*

$$b(G) \leq \min\left\{|G|^{1/2}, (q+1)^k |G/N|\right\}.$$

Proof. It is clear that $b(G) \leq |G|^{1/2}$, so it remains to show that $b(G) \leq (q+1)^k |G/N|$. But this is also clear since $b(\mathrm{PSL}_2(q)) \leq q+1$ for every prime power $q \geq 8$. □

We are now ready to prove Theorems 1.2 and 1.3 in the case $S \cong \mathrm{PSL}_2(q)$ with q even. Since $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$, we will assume that $q \geq 8$.

Theorem 5.3. *Assume that $N = \mathrm{PSL}_2(q) \times \cdots \times \mathrm{PSL}_2(q)$, a direct product of k copies of $\mathrm{PSL}_2(q)$ where $q \geq 8$ is even, is a minimal normal subgroup of a finite group G. Let $|G| = b(G)(b(G)+e)$. Then $e > \sqrt{b(G)} + 1$ and, in particular, $|G| < e^4 - e^3$.*

Proof. Let $\theta \in \mathrm{Irr}(\mathrm{SL}_2(q))$ be an irreducible character of degree $q-1$ or $q+1$ such that θ is extendible to $\mathrm{Aut}(\mathrm{SL}_2(q))$, as its existence is guaranteed by Lemma 5.1. Using Lemma 4.1, we obtain a bijection $\beta \leftrightarrow \beta\chi$ between $\mathrm{Irr}(G/N)$ and the set of irreducible characters of G lying above $\theta \times \cdots \times \theta \in \mathrm{Irr}(N)$, where χ is an extension of $\theta \times \cdots \times \theta$ to G.

Consider the case $b(G) = \chi(1)b(G/N)$. We then have $b(G) \leq b(N)b(G/N)$ and as in the proof of Theorem 4.2, we are done by Lemma 3.4. So we can assume that $b(G) > \chi(1)b(G/N)$. In other words, all the irreducible characters of G lying above $\theta \times \cdots \times \theta \in \mathrm{Irr}(N)$ have degree smaller than $b(G)$.

Repeat the above arguments for the Steinberg character $\mathrm{St}_{\mathrm{SL}_2(q)}$ in place of θ, we also can assume that all irreducible characters of G lying above $\mathrm{St}_{\mathrm{SL}_2(q)} \times \cdots \times \mathrm{St}_{\mathrm{SL}_2(q)} \in \mathrm{Irr}(N)$ have degree smaller than $b(G)$. Note that these characters are of the form $\beta\chi_1$ where $\beta \in \mathrm{Irr}(G/N)$ and χ_1 is an extension of $\mathrm{St}_{\mathrm{SL}_2(q)} \times \cdots \times \mathrm{St}_{\mathrm{SL}_2(q)} \in \mathrm{Irr}(N)$ to G.

The conclusions of the last two paragraphs imply that

$$\begin{aligned} b(G)e = |G| - b(G)^2 &> \sum_{\beta \in \mathrm{Irr}(G/N)} \left(\beta(1)^2\chi(1)^2 + \beta(1)^2\chi_1(1)^2\right) \\ &= \left(\chi(1)^2 + \chi_1(1)^2\right)|G/N| \\ &\geq \left((q-1)^{2k} + q^{2k}\right)|G/N|. \end{aligned}$$

It is straightforward to check that

$$\left((q-1)^{2k} + q^{2k}\right)|G/N| \geq |G|^{3/4} + |G|^{1/2}$$

if $|G/N| \geq q^k$, and

$$\left((q-1)^{2k} + q^{2k}\right)|G/N| \geq (q+1)^{3k/2}|G/N|^{3/2} + (q+1)^k|G/N|$$

if $|G/N| < q^k$. Therefore, it follows from Lemma 5.2 that

$$\left((q-1)^{2k} + q^{2k}\right)|G/N| \geq b(G)^{3/2} + b(G).$$

We finally deduce that $b(G)e > b(G)^{3/2} + b(G)$, and the desired inequality follows. □

6. The case $S \cong \mathrm{PSL}_2(q)$ with q odd

We now turn to the most complicated case, namely $S \cong \mathrm{PSL}_2(q)$ with odd q. This will be achieved in Theorems 6.1 and 6.3.

Theorem 6.1. *Assume that $N = \mathrm{PSL}_2(q) \times \cdots \times \mathrm{PSL}_2(q)$, a direct product of k copies of $\mathrm{PSL}_2(q)$ where $q \geq 5$ is an odd prime power, is a minimal normal subgroup of a finite group G such that $|G/N| \geq q^k$. Let $|G| = b(G)(b(G)+e)$. Then $e > \sqrt{b(G)} + 1$ and, in particular, $|G| < e^4 - e^3$.*

Proof. Write $N = S_1 \times \cdots \times S_k$ where $S_i \cong \mathrm{PSL}_2(q)$ for every $i = 1, 2, \ldots, k$. As before, we apply Lemma 4.1 to have a bijective map $\beta \mapsto \beta\chi$ from $\mathrm{Irr}(G/N)$ to the set of irreducible characters of G lying above $\mathrm{St}_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k} \in \mathrm{Irr}(N)$, where χ is an extension of $\mathrm{St}_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k}$ to G. The case $b(G) = \chi(1)b(G/N) = q^k b(G/N)$ can be argued as before by using Lemma 3.4. So we may assume that $b(G) > q^k b(G/N)$. Equivalently, every irreducible character of G lying above $\mathrm{St}_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k} \in \mathrm{Irr}(N)$ has degree smaller than $b(G)$. It follows in particular that

$$b(G)e = |G| - b(G)^2 \geq q^{2k}|G/N|. \tag{1}$$

Let $M := S_2 \times \cdots \times S_k$. Let $T := \mathbf{N}_G(M)$, so $|G : T| = k$. Furthermore M can be considered as a subgroup of $T/\mathbf{C}_G(M)$, which in turn is isomorphic to a subgroup of $\mathrm{Aut}(M) \cong \mathrm{Aut}(\mathrm{PSL}_2(q)) \wr \mathsf{S}_{k-1}$. Using [24, Lemma 1.3], we have that $\mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k} \in \mathrm{Irr}(M)$ is extendible to $\mathrm{Aut}(M)$, and hence is extendible to $T/\mathbf{C}_G(M)$. It follows that $\mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k} \in \mathrm{Irr}(M)$ is extended to an irreducible character of T whose kernel contains $\mathbf{C}_G(M)$. Now since $S_1 \subseteq \mathbf{C}_G(M)$, we conclude that the character $1_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k} \in \mathrm{Irr}(N)$ is extendible to T. Assume that χ_1 is an extension of $1_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k}$ to T.

Observe that the stabilizer of $1_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k}$ normalizes M, and $1_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k}$ has exactly k conjugates under the action of G. Thus, T must be the stabilizer of $1_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k}$ in G.

Now we apply Gallagher's theorem to obtain a bijection $\beta_1 \mapsto \beta_1\chi_1$ between $\mathrm{Irr}(T/N)$ and the set of irreducible characters of T lying above $1_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k} \in \mathrm{Irr}(N)$. Moreover, by Clifford's theorem, each irreducible character of T lying above $1_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k} \in \mathrm{Irr}(N)$ induces irreducibly to G. Therefore, the map $\beta_1 \mapsto (\beta_1\chi_1)^G$ is a bijection between $\mathrm{Irr}(T/N)$ and the set of irreducible characters of G lying above $1_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k} \in \mathrm{Irr}(N)$. We note that

$$(\beta_1\chi_1)^G(1) = |G : T|\chi_1(1)\beta_1(1) = kq^{k-1}\beta_1(1)$$

and

$$kq^{k-1}\beta_1(1) \leq kq^{k-1}b(T/N) \leq kq^{k-1}|T/N|^{1/2} = k^{1/2}q^{k-1}|G/N|^{1/2}.$$

If $b(G) = kq^{k-1}b(T/N)$ then it follows that

$$b(G)^{3/2} + b(G) \leq k^{3/2}q^{3(k-1)/2}|G/N|^3/4 + k^{1/2}q^{k-1}|G/N|^{1/2}.$$

Using the hypothesis $|G/N| \geq q^k$, one can easily check that

$$k^{3/2}q^{3(k-1)/2}|G/N|^3/4 + k^{1/2}q^{k-1}|G/N|^{1/2} < q^{2k}|G/N|$$

and therefore we have

$$b(G)^{3/2} + b(G) < q^{2k}|G/N|.$$

This and (1) imply that $b(G)^{3/2} + b(G) < b(G)e$. As in the proof of Theorem 4.2, we deduce that $|G| < e^4 - e^3$ as required.

So from now on to the end of the proof we assume that $b(G) > kq^{k-1}b(T/N)$. In other words, the irreducible characters of G of the form $(\beta_1\chi_1)^G$ where $\beta_1 \in \mathrm{Irr}(T/N)$ all have degree smaller than $b(G)$. Recall from the second paragraph that all irreducible characters of G lying above $\mathrm{St}_{S_1} \times \cdots \times \mathrm{St}_{S_k}$ also have degree smaller than $b(G)$. Therefore we obtain

$$\begin{aligned} b(G)e &\geq \sum_{\beta \in \mathrm{Irr}(G/N)} \beta(1)^2\chi(1)^2 + \sum_{\beta_1 \in \mathrm{Irr}(T/N)} \Big((\beta_1\chi_1)^G(1)\Big)^2 \\ &= q^{2k}|G/N| + k^2q^{2(k-1)}|T/N| \\ &= q^{2k}|G/N| + kq^{2(k-1)}|G/N|. \end{aligned}$$

Using the hypothesis that $|G/N| \geq q^k$ and the fact that $|N| = |\mathrm{PSL}_2(q)|^k < q^{3k}$, we easily check that

$$q^{2k}|G/N| > |G|^{3/4}$$

and

$$kq^{2(k-1)}|G/N| > |G|^{1/2}.$$

Therefore we deduce that $b(G)e > |G|^{3/4} + |G|^{1/2}$. Since $b(G) \leq |G|^{1/2}$, it follows that $b(G)e > b(G)^{3/2} + b(G)$ and the theorem follows as before. □

Unlike the groups in even characteristic, $\mathrm{PSL}_2(q)$ with odd q may have the Steinberg character as the only one that is extendible to $\mathrm{Aut}(\mathrm{PSL}_2(q))$. According to White [33, p. 8], when q is odd, $\mathrm{PSL}_2(q)$ has the following irreducible characters:

(i) $1_{\mathrm{PSL}_2(q)}$ of degree 1,
(ii) $\mathrm{St}_{\mathrm{PSL}_2(q)}$ of degree q,
(iii) χ_i, $1 \leq i \leq (q-3)/2$ and i even, of degree $q+1$,
(iv) θ_j, $1 \leq j \leq (q-1)/2$ and j even, of degree $q-1$,
(v) ξ_1 and ξ_2 of degree $(q+1)/2$, if $q \equiv 1 (\mathrm{mod}\ 4)$, and
(vi) η_1 and η_2 of degree $(q-1)/2$, if $q \equiv -1 (\mathrm{mod}\ 4)$.

Let $q = p^f$ where p is an odd prime. Let φ be the field automorphism of order f of $\mathrm{PSL}_2(q)$ and δ be the diagonal automorphism of order 2 of $\mathrm{PSL}_2(q)$. Then, by White [33, Lemma 4.8], the character $\chi_i \in \mathrm{Irr}(\mathrm{PSL}_2(q))$ is invariant under φ^k where $1 \leq k \leq f$ if and only if $(p^f - 1)|i(p^k - 1)$ or $(p^f - 1)|i(p^k + 1)$; and the character $\theta_j \in \mathrm{Irr}(\mathrm{PSL}_2(q))$ is invariant under φ^k if and only if $(p^f + 1)|j(p^k - 1)$ or $(p^f + 1)|j(p^k + 1)$. Contrary to the even characteristic case, we now show that $\mathrm{PSL}_2(p^f)$ has an irreducible character of degree $q-1$ whose stabilizer in $\mathrm{Aut}(\mathrm{PSL}_2(q))$ is $\mathrm{PGL}_2(q)$, which is as small as possible.

Lemma 6.2. *Let $q = p^f \geq 5$ be an odd prime power and let θ_2 be defined as above. Then*

$$\mathrm{Stab}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\theta_2) = \mathrm{PGL}_2(q).$$

Proof. We observe that $(p^f + 1)|2(p^k - 1)$ or $(p^f + 1)|2(p^k + 1)$ if and only if $k = f$. That means $\theta_2 \in \mathrm{Irr}(\mathrm{PSL}_2(q))$ is not invariant under φ^k for every $1 \leq k < f$. It is well known that every irreducible character of $\mathrm{PSL}_2(q)$ of degree $q \pm 1$ is invariant under the diagonal automorphism δ. Therefore

$$\mathrm{Stab}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\theta_2) = \mathrm{PSL}_2(q) \rtimes \langle \delta \rangle = \mathrm{PGL}_2(q),$$

as claimed. □

Theorem 6.3. *Assume that $N = \mathrm{PSL}_2(q) \times \cdots \times \mathrm{PSL}_2(q)$, a direct product of k copies of $\mathrm{PSL}_2(q)$ with $q \geq 5$, is a minimal normal subgroup of a finite group G such that $|G/N| < q^k$. Let $|G| = b(G)(b(G) + e)$. Then $e > \sqrt{b(G)} + 1$ and, in particular, $|G| < e^4 - e^3$.*

Proof. Arguing as in the proof of Theorem 6.1, we can assume that every irreducible character of G lying above $\mathrm{St}_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k} \in \mathrm{Irr}(N)$ has degree smaller than $b(G)$.

By Lemma 6.2, we have $\mathrm{Stab}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\theta_2) = \mathrm{PGL}_2(q)$. Let $\psi := \theta_2 \times \cdots \times \theta_2 \in \mathrm{Irr}(N)$. Then we have $\mathrm{Stab}_{\mathrm{Aut}(N)}(\psi) = \mathrm{PGL}_2(q) \wr \mathsf{S}_k$. Set $\overline{H} := \mathrm{PGL}_2(q) \wr \mathsf{S}_k$.

Consider N as a subgroup of $G/\mathbf{C}_G(N)$, which in turn can be considered as a subgroup of $\mathrm{Aut}(N)$. Then the stabilizer of ψ in $G/\mathbf{C}_G(N)$ is $\overline{H} \cap G/\mathbf{C}_G(N)$. Let H be the preimage of $\overline{H} \cap G/\mathbf{C}_G(N)$ in G. Then we have $\mathrm{Stab}_G(\psi) = H$.

Recall that $\mathrm{PGL}_2(q) = \mathrm{PSL}_2(q) \rtimes \langle \delta \rangle$ where δ the diagonal automorphism of degree 2 of $\mathrm{PSL}_2(q)$. Therefore θ is extendible to $\mathrm{PGL}_2(q)$. Thus $\psi \in \mathrm{Irr}(N)$ is extendible to $\overline{H}$ so that it is extendible to $\overline{H} \cap G/\mathbf{C}_G(N)$ as well. We deduce that ψ is extendible to H. Let χ be an extension of ψ to H.

The conclusions of the last two paragraphs, together with Gallagher's theorem and Clifford's theorem, imply that $\beta \mapsto (\beta\chi)^G$ is a bijection between $\mathrm{Irr}(H/N)$ and the set of irreducible characters of G lying above $\psi \in \mathrm{Irr}(N)$. Note that

$$(\beta\chi)^G(1) = \beta(1)\chi(1)|G/H| = (q-1)^k\beta(1)|G/H|.$$

We come up with two cases:

Case $b(G) = (q-1)^k b(H/N)|G/H|$: Then we have $b(G) \leq (q-1)^{|}G/N|$. Recall that every irreducible character of G lying above $\mathrm{St}_{S_1} \times \mathrm{St}_{S_2} \times \cdots \times \mathrm{St}_{S_k} \in \mathrm{Irr}(N)$ has degree smaller than $b(G)$. Therefore $b(G)e \geq q^{2k}|G/N|$. This and the inequality $b(G) \leq (q-1)^{|}G/N|$, together with the hypothesis that $|G/N| < q^k$ imply that $b(G)e > b(G)^{3/2} + b(G)$, and we are done as before.

Case $b(G) > (q-1)^k b(H/N)|G/H|$: Then every irreducible character of G of the form $(\beta\chi)^G$ where $\beta \in \mathrm{Irr}(H/N)$ has degree smaller than $b(G)$. Therefore

$$\begin{aligned} b(G)e &\geq q^{2k}|G/N| + \sum_{\beta \in \mathrm{Irr}(H/N)} \left((\beta\chi)^G(1)\right)^2 \\ &= q^{2k}|G/N| + (q-1)^{2k}|H/N||G/H|^2 \\ &\geq q^{2k}|G/N| + (q-1)^{2k}|G/N|. \end{aligned}$$

Using $|G/N| < q^k$, we can check that

$$q^{2k}|G/N| + (q-1)^{2k}|G/N| > (q+1)^{3k/2}|G/N|^{3/2} + (q+1)^k|G/N|.$$

It follows from Lemma 5.2 that

$$q^{2k}|G/N| + (q-1)^{2k}|G/N| > b(G)^{3/2} + b(G).$$

This and the above inequality $b(G)e \geq q^{2k}|G/N| + (q-1)^{2k}|G/N|$ imply that $b(G)e > b(G)^{3/2} + b(G)$, which in turn implies that $b(G) < e^2 - e$ and the theorem follows. □

Theorems 1.2 and 1.3 now are consequences of Theorems 4.2, 5.3, 6.1, and 6.3.

7. Groups with $|G| = e^4 - e^3$

In this section, we characterize those groups that satisfy the condition $|G| = e^4 - e^3$. To do this, we need to introduce another class of groups.

An irreducible character χ of a finite group G is said to be a *Gagola character* if it vanishes on all but two conjugacy classes of G. Groups with such a character have been studied in great depth by Gagola [11]. In particular, if G has a Gagola character, then G has a unique minimal normal subgroup N, which is necessarily elementary abelian. Furthermore, χ vanishes on all the elements in $G \setminus N$ and that χ is the unique irreducible character of G whose kernel does not contain N. In this situation, for simplicity we will say that G is a *Gagola group* and (G, N) is a *Gagola pair*.

The following lemma shows the connection between groups in consideration and Gagola groups.

Lemma 7.1. (*i*) *Let G be a finite group with a nontrivial abelian normal subgroup, and let $|G| = d(d+e)$ where d is a character degree of G and $e > 1$ is an integer. If $d \geq e^2 - e$ then G has a Gagola character $\chi \in \mathrm{Irr}(G)$ of degree d.*

(*ii*) *Let (G, N) be a Gagola pair with the associated Gagola character of degree d. Let p be the only prime divisor of $|N|$ and P a Sylow p-subgroup of G. Then $|P : N| = e^2$ and $d = e(|N| - 1)$.*

Proof. See [18, Corollary 1.4], [31, Theorem 4.1], and [20, Lemmas 2.1 and 2.2]. □

We can now characterize the groups G with $|G| = e^4 - e^3$.

Theorem 7.2. *Let G be a finite group, and let $|G| = d(d+e)$ where $d > 1$ is a character degree of G and $e > 1$ is an integer. Then $|G| = e^4 - e^3$ if and only if G has a Gagola character of degree d and a unique minimal normal subgroup N of order e.*

Proof. Suppose first that G has a Gagola character of degree d and the unique minimal normal subgroup N with $|N| = e$. Let p be the unique prime divisor of $|N|$ and let P be a Sylow p-subgroup of G. By Lemma 7.1(ii), we know that $e^2 = |P : N|$. Furthermore, from Lemma 2.1 and Corollary 2.3 of [11], we have $|G : P| = |N| - 1$. Therefore,

$$|G| = |G : P||P : N||N| = (|N| - 1)|P : N||N| = (e - 1)e^2 e = e^4 - e^3.$$

Conversely, suppose that $|G| = e^4 - e^3$. In view of Theorem 1.2, G must have a nontrivial solvable radical. In particular, G has a nontrivial abelian normal subgroup. Theorem 1.1 of [20] then implies that

$$d \leq e^2 - e.$$

If $d < e^2 - e$, then

$$|G| = d(d + e) < \left(e^2 - e\right)\left(\left(e^2 - e\right) + e\right) = \left(e^2 - e\right)e^2 = e^4 - e^3 = |G|,$$

which is a contradiction. Thus, we must have $d = e^2 - e$. We then apply Lemma 7.1(i) to see that G has a Gagola character of degree d, and hence has a unique minimal normal subgroup. Let N be the unique minimal normal subgroup of G. Applying Lemma 7.1(ii), we deduce that $d = e(|N| - 1)$. Since $d = e^2 - e$, it follows that $e(e - 1) = e(|N| - 1)$, and we easily computes that $|N| = e$. □

The groups mentioned in the introduction are not the only Gagola groups in the consideration of Theorem 7.2. Let us describe here another family of such groups, which appeared in [13, p. 409] in a different context. These groups have normal Sylow p-subgroups, where p the the prime divisor of $|N|$.

Let $\mathbb{F}$ be a field of order q where q is a power of some prime p. Take

$$K := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & d \end{pmatrix} : a, b, c \in \mathbb{F};\ d \in \mathbb{F}^* \right\}.$$

Let $\mathcal{G} := Gal(\mathbb{F}/\mathbb{F}_p)$ be the Galois group for $\mathbb{F}$ over the subfield $\mathbb{F}_p$ of order p. We define an action $\mathcal{G}$ on K as follows: if $\sigma \in \mathcal{G}$, then σ acts on a typical element of K by acting on each of the entries of K. Let

$$P := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} | a, b, c \in \mathbb{F} \right\},$$

and

$$L := \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & d \end{pmatrix} | d \in \mathbb{F}^* \right\}.$$

It is not difficult to see that P is an ultraspecial group of order q^3 and L is a cyclic group of order $q - 1$. Notice that P and L are invariant under the action

of $\mathcal{G}$. Furthermore, the semi-direct product of $\mathcal{G}$ acting on L is isomorphic to the affine group on $\mathbb{F}$. Let Γ be the semi-direct product of $\mathcal{G}$ acting on K. (We note that $\mathbf{Z}(P)L\mathcal{G}$ is isomorphic to the affine semi-linear group on $\mathbb{F}$, which has been discussed on [23, p. 38].)

Suppose $D = NH^*$ is a two-transitive Frobenius group of Dickson type of order $p^n(p^n - 1)$, where N is the Frobenius kernel and H^* is the Frobenius complement. It is well-known that H^* can be embedded in the affine group of $\mathbb{F}$ and that NH^* is isomorphic to a subgroup of the semi-linear affine group of $\mathbb{F}$. Thus, H^* is isomorphic to $H \subseteq L\mathcal{G} \subset \Gamma$ and NH is isomorphic to $\mathbf{Z}(P)H$. We set $G := PH$, and it is not difficult to see that G is a Gagola group with the desired properties.

A family of non-p-closed examples can be found in [21, Theorem 3.3] for every prime p. These groups were constructed as subgroups of index p of the group Γ defined above when $q = p^p$. Two other non-p-closed examples can be found in [11, pp. 383–384]. The first of these has a subgroup S of order 12 obtained by taking a cyclic group of order 4 acting on a group of order 3 by inverting the nontrivial elements and then having S act on the direct product of two cyclic groups of order 4. The second one has a subgroup T which is the direct product of a cyclic group of order 4 and the semi-direct product of a cyclic group of order 9 acting nontrivially on the quaternion group of order 8. The desired group is then obtained by having T act on the direct product of two cyclic groups of order 9. We refer the interested reader to [11] for detailed constructions of these groups.

It seems nontrivial to us to obtain a complete classification of those groups that satisfy the extremal condition $|G| = e^4 - e^3$. It is likely that these groups are necessarily solvable, but we are not able to confirm it at this time.

Acknowledgments The authors are grateful to the anonymous referee for several comments and suggestions that have significantly improved the exposition of the paper.

References

[1] Berkovich, Y.: Groups with few characters of small degrees. Isr. J. Math. **110**, 325–332 (1999)
[2] Bianchi, M., Chillag, D., Lewis, M.L., Pacifici, E.: Character degree graphs that are complete graphs. Proc. Am. Math. Soc. **135**, 671–676 (2007)
[3] Burkett, S.T., Nguyen, H.N.: Conjugacy classes of small sizes in the linear and unitary groups. J. Group Theory **16**, 851–874 (2013)
[4] Carter, R.W.: Finite Groups of Lie Type. Conjugacy Classes and Complex Characters, Wiley, New York (1985)
[5] Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A., Wilson, R.A.: Atlas of Finite Groups. Clarendon Press, Oxford (1985)
[6] Cossey, J.P., Halasi, Z., Maróti, A., Nguyen, H.N.: On a conjecture of Gluck. Math. Z. **279**, 1067–1080 (2015)
[7] Digne, F., Michel, J.: Representations of finite groups of Lie type. Lond. Math. Soc. Stud. Texts **21** (1991)
[8] Durfee, C., Jensen, S.: A bound on the order of a group having a large character degree. J. Algebra **338**, 197–206 (2011)

[9] Feit, W.: Extending Steinberg characters, Linear algebraic groups and their representations. Contemp. Math. **153**, 1–9 (1993)
[10] Frame, J.S., Robinson, G.B., Thrall, R.M.: The hook graphs of the symmetric group. Can. J. Math. **6**, 316–324 (1954)
[11] Gagola, S.M. Jr.: Characters vanishing on all but two conjugacy classes. Pac. J. Math. **109**, 363–385 (1983)
[12] Gluck, D.: The largest irreducible character degree of a finite group. Can. J. Math. **37**, 442–451 (1985)
[13] Goldstein, D., Guralnick, R.M., Lewis, M.L., Moretó, A., Navarro, G., Tiep, P.H.: Groups with exactly one irreducible character of degree divisible by p. Algebra Number Theory **8**, 397–428 (2014)
[14] Halasi, Z., Hannusch, C., Nguyen, H.N.: The largest character degrees of the symmetric and alternating groups. Proc. Am. Math. Soc. arXiv:1410.3055 **(to appear)**
[15] Isaacs, I.M.: Character Theory of Finite Groups. AMS Chelsea, Providence (2006)
[16] Isaacs, I.M.: Bounding the order of a group with a large character degree. J. Algebra **348**, 264–275 (2011)
[17] James, G.D.: The Representation Theory of the Symmetric Groups. Lecture Notes in Mathematics. Springer, Berlin (1978)
[18] Kuisch, E., van der Waall, R.W.: Homogeneous character induction. J. Algebra **149**, 454–471 (1992)
[19] Larsen, M., Malle, G., Tiep, P.H.: The largest irreducible representations of simple groups. Proc. Lond. Math. Soc. **106**, 65–96 (2013)
[20] Lewis, M.L.: Bounding group orders by large character degrees: a question of Snyder. J. Group Theory **17**, 1081–1116 (2014)
[21] Lewis M.L.: Camina pairs that are not p-closed. Isr. J. Math. doi:10.1007/s11856-014-1126-8
[22] Lübeck F.: Data for Finite Groups of Lie Type and Related Algebraic Groups. http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/index.html
[23] Manz, O., Wolf, T.R.: Representations of Solvable Groups. London Mathematical Society Lecture Note Series, vol. 185. Cambridge University Press, Cambridge (1993)
[24] Mattarei, S.: On character tables of wreath products. J. Algebra **175**, 157–178 (1995)
[25] McKay, J.: The largest degrees of irreducible characters of the symmetric group. Math. Comput. **30**, 624–631 (1976)
[26] Meyn, H., Götz, W.: Self-reciprocal polynomials over finite fields, Séminaire Lotharingien de Combinatoire. Publ. Inst. Rech. Math. Av. **413**, 82–90 (1990)
[27] Moretó, A., Nguyen, H.N.: On the average character degree of finite groups. Bull. Lond. Math. Soc. **46**, 454–462 (2014)
[28] Nguyen, H.N.: Low-dimensional complex characters of the symplectic and orthogonal groups. Commun. Algebra **38**, 1157–1197 (2010)
[29] Passman, D.S.: Permutation Groups. pp. vi+152 Dover, Mineola (2012)
[30] Seitz, G.M.: Cross-characteristic embeddings of finite groups of Lie type. Proc. Lond. Math. Soc. **60**, 166–200 (1990)
[31] Snyder, N.: Groups with a character of large degree. Proc. Am. Math. Soc. **136**, 1893–1903 (2008)
[32] Tiep, P.H., Zalesskiĭ, A.E.: Unipotent elements of finite groups of Lie type and realization fields of their complex representations. J. Algebra **271**, 327–390 (2004)
[33] White, D.L.: Character degrees of extensions of $\mathrm{PSL}_2(q)$ and $\mathrm{SL}_2(q)$. J. Group Theory **16**, 1–33 (2013)