Proceedings of the Royal Society of Edinburgh, **153**, 115–136, *2023*
DOI:10.1017/prm.2021.74

On the number of conjugacy classes of a primitive permutation group

Daniele Garzoni
School of Mathematical Sciences, Tel Aviv University, Tel Aviv, Israel
(danieleg@mail.tau.ac.il)

Nick Gill
School of Mathematics and Statistics, The Open University, Walton Hall, Milton Keynes MK7 6AA, UK (nick.gill@open.ac.uk)

(Received 2 August 2021; accepted 28 October 2021)

Let G be a primitive permutation group of degree n with nonabelian socle, and let $k(G)$ be the number of conjugacy classes of G. We prove that either $k(G) < n/2$ and $k(G) = o(n)$ as $n \to \infty$, or G belongs to explicit families of examples.

Keywords: Conjugacy classes; permutation groups

2020 *Mathematics Subject Classification:* 20B05

1. Introduction

Throughout, $k(G)$ denotes the number of conjugacy classes of a finite group G. Maróti [20] proved that if G is a primitive permutation group of degree n, then $k(G) \leqslant p(n)$, where $p(n)$ denotes the number of partitions of n. This bound is attained by S_n in its action on n points. Moreover, he proved that if the socle of G is not a direct product of alternating groups, then $k(G) \leqslant n^6$.

In this paper, we want to improve this bound under the assumption that G has nonabelian socle. In § 1.2, we will give more context and review more results in this area.

There are two special types of primitive groups which we wish to single out.

(A) Let G be the symmetric group S_d or the alternating group A_d on $d \geqslant 5$ letters. For every $1 \leqslant k < d/2$, G acts primitively on the set of k-subsets of $\{1, \ldots, d\}$. These are in number $\binom{d}{k}$.

(B) Let G be an almost simple group with socle $\mathrm{PSL}_d(q)$, and assume that $G \leqslant \mathrm{P\Gamma L}_d(q)$. Then G acts primitively on the set of 1-subspaces of $\mathbf{F}_q^d$. These are in number $(q^d - 1)/(q - 1)$.

Our main result says that, if G is a primitive group with nonabelian socle, then either G has very few conjugacy classes, or else the action of G is 'related' to (A)

Table 1. *Almost simple primitive permutation groups G of degree n (up to equivalence) for which $k(G) \geqslant \frac{n}{2}$, and for which the action is not isomorphic to an action in (A) or (B)*

G	n	$k(G)$
M_{11}	11,12	10
M_{12}	12,12	15
M_{22}	22	12
$M_{22}.2$	22	21
M_{23}	23	17
M_{24}	24	26
A_7	15,15	9
$S_8 \cong \mathrm{SL}_4(2).2$	35	22
$\mathrm{PSL}_2(11)$	11,11	8
$\mathrm{SO}_8^-(2)$	119	60
$\mathrm{Sp}_8(2)$	120,136	81
$\mathrm{SO}_8^+(2)$	120	67
$\mathrm{Sp}_6(2)$	28, 36	30
$\mathrm{PSp}_4(3) \cong \mathrm{SU}_4(2)$	27,36,40,40	20
$\mathrm{PSp}_4(3).2$	27,36,40,40,45	25
$\mathrm{PSU}_4(3).(2 \times 2)$	112	59
$\mathrm{P\Gamma U}_4(3)$	112	61
$\mathrm{SU}_3(3)$	28	14
$\mathrm{SU}_3(3).2$	28	16

or (B) or to a further finitely many almost simple primitive permutation groups. The precise statement is as follows.

THEOREM 1.1. *Let G be a primitive permutation group of degree n with non-abelian socle, so $\mathrm{Soc}(G) \cong S^r$, with S nonabelian simple and $r \geqslant 1$. Then one of the following holds.*

(1) *$k(G) < n/2$, and $k(G) = O(n^\delta)$ for some absolute $\delta < 1$.*

(2) *$G \leqslant A \wr S_r$, A is an almost simple primitive permutation group of degree m with socle S, G acts in product action on $n = m^r$ points, and one of the following holds:*

  (i) *The action of A on m points is equivalent to an action in table 1, and $k(G) < n^{1.31}$.*

  (ii) *The action of A on m points is isomorphic to an action described in (A) or (B). In the (B)-case, $k(G) < n^{1.9}$.*

On the way, we remark that theorem 1.1 is a key ingredient of the paper [9], where we study a problem of invariable generation of symmetric groups.

We will first prove theorem 1.1 in case G is almost simple, and then deduce the general case. For convenience, we state separately the almost simple case (where we also give an explicit estimate for δ).

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

Theorem 1.2. *Let G be an almost simple primitive permutation group of degree n. Then one of the following holds.*

(1) *$k(G) < n/2$, and $k(G) = O(n^{3/4})$.*

(2) *Either the action of G is equivalent to an action in table 1, or the action of G is isomorphic to an action described in (A) or (B). In the (B)-case, $k(G) < 100n$.*

In item (1), the exponent 3/4 is sharp, although in most cases $k(G) = o(n^{3/4})$ as $n \to \infty$; see remark 2.14 for a precise statement.

In the proof of theorem 1.2, an essential ingredient is the work of Fulman–Guralnick [**6**], which gives upper bounds for the number of conjugacy classes of almost simple groups of Lie type.

We immediately make some clarifications regarding the statement of theorem 1.1.

Remark 1.3.

(i) We are not asserting that every case appearing in theorem 1.1(2) does not satisfy item (1). For instance, assume that $m = n$, and consider $G = S_d$ acting on $n = \binom{d}{k}$ points as in (A), and assume that $cd \leqslant k \leqslant \frac{d}{2}$ for some fixed constant c. Then it is well known that $n = \binom{d}{k}$ is exponential in d, while the number of conjugacy classes of $G = S_d$ is of the form $O(1)^{\sqrt{d}}$. In particular $k(G) = n^{o(1)}$ as $d \to \infty$.

(ii) In theorem 1.1(2)(ii), we can be more precise about the adjective *isomorphic*, as follows. If A is A_d or S_d, then either the action of A is *equivalent* to the action on k-subsets; or else $(d, m) = (6, 6)$ or $(6, 15)$. Moreover, if A is almost simple with socle $\mathrm{PSL}_d(q)$ and $A \leqslant \mathrm{P\Gamma L}_d(q)$, then the action of A is equivalent to the action on the 1-subspaces or $(d-1)$-subspaces of $\mathbf{F}_q^d$. For this, see lemmas 2.8 and 2.12.

(iii) Whenever G is almost simple with socle isomorphic to both A_d and $\mathrm{PSL}_f(q)$, we have excluded from table 1 both the groups in (A) and (B). For instance, $G = S_6$ has 11 conjugacy classes, and contains a subgroup $S_3 \wr S_2$ of index 10 acting transitively on 6 points; but this does not appear in table 1 in view of the isomorphism $S_6 \cong \mathrm{P\Sigma L}_2(9)$. The same reasoning applies to the isomorphisms $\mathrm{SL}_2(4) \cong \mathrm{PSL}_2(5) \cong A_5$, $\mathrm{PSL}_2(7) \cong \mathrm{SL}_3(2)$ and $\mathrm{SL}_4(2) \cong A_8$.

1.1. When is $k(G) = o(n)$?

Theorem 1.1 implies in particular that, if the socle of G is nonabelian, then either $k(G) = o(n)$, or G is 'known'. Can we prove that $k(G) = o(n)$ in further cases?

We are particularly interested in the cases contemplated in theorem 1.1(2)(i), for which we show $k(G) < n^{1.31}$. We first note that there are examples in which $k(G) > n^{1.08}$ for arbitrarily large n, in contrast to item (1); see lemma 4.1.

Still, it would be interesting to understand precisely when this happens (since there are only finitely many almost simple groups to handle).

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

Question 1. Let A be an almost simple primitive group on m points appearing in table 1. Determine whether *every* primitive subgroup G of $A \wr S_r$ on $n = m^r$ points is such that $k(G) = o(m^r)$ as $r \to \infty$.

This should be related to estimating the number of conjugacy classes in wreath products, and we refer to § 4 for comments in this direction. See in particular conjecture 4.2, which would provide an answer to question 1.

1.2. Context

There are many results in the literature which give upper bounds to the number of conjugacy classes of a finite groups in terms of various parameters. We recall some of these, focusing on permutation groups.

Kovács–Robinson [**16**] proved that every permutation group of degree n has at most 5^{n-1} conjugacy classes. This estimate was subsequently improved by Liebeck–Pyber, Maróti, and Garonzi–Maróti, as follows:

$$k(G) \leqslant 2^{n-1} \quad ([17])$$

$$k(G) \leqslant 3^{(n-1)/2} \text{ for } n \geqslant 3 \quad ([20])$$

$$k(G) \leqslant 5^{(n-1)/3} \text{ for } n \geqslant 4 \quad ([11]).$$

We should mention that, in [**16**, **17**], various other upper bounds to $k(G)$ are proved, where G is not necessarily a permutation group.

There are easy examples showing that these estimates are somewhat close to best possible, even for transitive groups. Indeed, the subgroup $S_4^{n/4} \leqslant S_n$ has $5^{n/4}$ conjugacy classes; and the transitive subgroup $G = S_4 \wr C_{n/4} \leqslant S_n$ has $5^{n/4-o(n)}$ conjugacy classes (more precisely, $k(G)$ is asymptotic to $4 \cdot 5^{n/4}/n$; see lemma 4.3).

For primitive groups, the situation is very different. Let G be a primitive permutation group of degree n. Liebeck–Pyber [**17**, corollary 2.15] proved the following:

(i) $k(G) \leqslant p(n)$ if n is sufficiently large;

(ii) $k(G) \leqslant n^{11}$ if the socle of G is not a direct product of alternating groups.

(Recall that $p(n) = O(1)^{\sqrt{n}}$, and in fact the asymptotic behaviour of $p(n)$ is known by famous work of Hardy–Ramanujan.) Maróti [**20**] improved these results. He showed that item (i) holds for every positive integer n and, moreover, the bound $k(N) \leqslant p(n)$ holds for every normal subgroup N of G. He also showed that, in item (ii), one can replace n^{11} by n^6.

Theorem 1.1 can be regarded as an improvement of these statements, for the case where the socle of G is nonabelian.

1.3. Abelian socle

In this paper we do not address the case in which the socle of G is abelian. In this case, we still have the bound $k(G) \leqslant n^6$ from [**20**].

There is a deep problem, known as the *non-coprime* $k(GV)$*-problem*, which was addressed by Guralnick–Tiep [**13**] and which asks (in particular) for a characterization of the affine primitive permutation groups of degree n for which $k(G) > n$.

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

A resolution of this problem, if combined with the main result of this paper, would give a characterization of all primitive permutation groups of degree n for which $k(G) > n$. We refer to Guralnick–Tiep [13], Guralnick–Maróti [10] and the references therein for results in this direction, partly motivated by Brauer's celebrated $k(B)$-conjecture.

The organization of the paper is as follows. In § 2 we prove theorem 1.2, in § 3 we prove theorem 1.1, and in § 4 we discuss question 1 and make further comments.

2. Almost simple groups

In this section we prove theorem 1.2. Regarding item (1), we prove the inequality $k(G) < n/2$ in §2.2–2.4, and then we prove the asymptotic inequality $k(G) = O(n^{3/4})$ in § 2.5.

2.1. Some preliminary lemmas

We begin with a lemma from [7]. We will often apply this lemma with no mention.

Lemma 2.1. *If G is a finite group and H is a subgroup of G, then*

$$k(H)/|G:H| \leqslant k(G) \leqslant |G:H| \cdot k(H).$$

If moreover H is normal in G, then

$$k(G) \leqslant k(H) \cdot k(G/H).$$

In one occasion, we will need the following variant (see [16, p. 447]).

Lemma 2.2. *Let G be a finite group and let N be a normal subgroup of G. Then*

$$k(G) \leqslant |G:N| \cdot \#\{G\text{-conjugacy classes of } N\}.$$

We are now ready to begin the proof of theorem 1.2.

2.2. Sporadic groups

Lemma 2.3. *Let G be almost simple with socle S, a sporadic simple group. Let M be a core-free maximal subgroup of G, and write $n = |G:M|$. If $k(G) \geqslant \frac{n}{2}$, then G and n are listed in table 2.*

Note that repeated values of n in table 2 signify the existence of more than one action, up to equivalence, of the given degree. The same convention applies to later tables pertaining to the alternating groups and the groups of Lie type.

Proof. We go through the ATLAS [3]. □

2.3. Alternating groups

We recall some results that we will use. The first is an inequality of Pribitkin [22], as follows.

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

Table 2. *Faithful primitive permutation representations of degree n for sporadic almost simple groups G such that* $k(G) \geqslant \frac{n}{2}$

G	n	$k(G)$
M_{11}	11,12	10
M_{12}	12,12	15
M_{22}	22	12
$M_{22}.2$	22	21
M_{23}	23	17
M_{24}	24	26

Lemma 2.4. *Let $p(d)$ be the number of partitions of the integer d. Then*

$$p(d) < \frac{e^{\pi\sqrt{2d/3}}}{d^{3/4}}.$$

We will need the following pair of inequalities which are an easy consequence of work of Robbins on the Stirling approximations [24].

Lemma 2.5. *Let $d \geqslant 2$ be an integer. Then*

$$\sqrt{2\pi} d^{d+1/2}\, e^{-d} \leqslant d! \leqslant e\, d^{d+1/2}\, e^{-d}.$$

We will also need the following result of Praeger and Saxl [23].

Lemma 2.6. *Let $G \leqslant S_d$ and suppose that G is primitive and does not contain A_d. Then $|G| < 4^d$.*

Finally, we will need an elementary lemma. For a proof, see for instance [13, lemma 6.2].

Lemma 2.7. *For every positive integer d, $k(A_d) \leqslant k(S_d)$.*

Now we can prove the main result of this subsection.

Lemma 2.8. *Let G be almost simple with socle $S \cong A_d$. Let M be a core-free maximal subgroup of G, and write $n = |G : M|$. If $k(G) \geqslant \frac{n}{2}$, then one of the following holds.*

(1) *G and n are listed in table 3.*

(2) *M is intransitive in its action on d points, thus $n = \binom{d}{k}$ for some integer k such that $1 \leqslant k < \frac{1}{2}d$.*

(3) *$(d, n) = (6, 6)$ or $(6, 15)$, and the action of G on the cosets of M is isomorphic, but not equivalent, to the action on the coset of a maximal intransitive subgroup.*

In item (3), if $(d, n) = (6, 6)$ we have $G = A_6$ or S_6, and $M = S_5 \cap G$, where S_5 is a subgroup of S_6 acting primitively on 6 points. If $(d, n) = (6, 15)$, again $G = A_6$

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

Table 3. *Faithful primitive permutation representations of degree n for almost simple groups G with socle A_d such that $k(G) \geqslant \frac{n}{2}$, and the action is not isomorphic to an action in (A)*

G	n	$k(G)$
A_5	6	5
S_5	6	7
$A_6 = \mathrm{PSL}_2(9)$	10	7
$A_6.2 = \mathrm{PGL}_2(9)$	10	11
$A_6.2 = S_6$	10	11
$A_6.2 = M_{10}$	10	8
$A_6.(2 \times 2) = \mathrm{P\Gamma L}_2(9)$	10	13
A_7	15,15	9
A_8	15,15	14
S_8	35	22

or S_6, and $M = (S_2 \wr S_3) \cap G$, where $S_2 \wr S_3$ acts transitively (and imprimitively) on 6 points. (Note that in the latter case, if $G = A_6$ then $k(G) < n/2$.)

Proof. For $d \leqslant 8$, we use the ATLAS [3] together with GAP [8] to obtain the given list. For $9 \leqslant d \leqslant 20$ we use GAP to check that no examples occur. Assume, then, that $d > 20$.

Let us suppose, first, that M is primitive in its action on d points. Then lemmas 2.4–2.7 imply that it is sufficient to prove the following

$$\frac{\mathrm{e}^{\pi\sqrt{2d/3}}}{d^{3/4}} < \frac{\sqrt{2\pi}d^{d+1/2}}{4 \cdot \mathrm{e}^d \cdot 4^d}.$$

If we assume that the other inequality holds, we get

$$\begin{aligned} \mathrm{e}^{\pi\sqrt{2d/3}} &\geqslant \frac{\sqrt{2\pi} \cdot d^{d+5/4}}{4 \cdot \mathrm{e}^d \cdot 4^d} \\ \implies 2 \cdot \mathrm{e}^{\pi\sqrt{2d/3}} \cdot (4e)^d &\geqslant d^{d+5/4} \\ \implies 2 \cdot \mathrm{e}^{2.6\sqrt{d}} \cdot (4e)^d &\geqslant d^{d+5/4} \\ \implies 2 \cdot (5e)^{d+\sqrt{d}} &\geqslant d^{d+5/4} \\ \implies d &\leqslant 20. \end{aligned}$$

Since $d > 20$, the result follows.

Let us suppose, next, that M is imprimitive in its action on d points. Then

$$n = \frac{d!}{(k!)^\ell \ell!},$$

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

where $d = k\ell$ and $k, \ell \geqslant 2$. Now lemma 2.5 implies that

$$\begin{aligned} n &\geqslant \frac{\sqrt{2\pi}\cdot d^{d+1/2}\cdot \mathrm{e}^{-d}}{(ek^{k+1/2}\mathrm{e}^{-k})^{\ell}\cdot e\cdot \ell^{\ell+1/2}\cdot \mathrm{e}^{-\ell}} = \frac{\sqrt{2\pi}\cdot d^{d+1/2}}{e\cdot k^{(k+1/2)\ell}\cdot \ell^{\ell+1/2}} \\ &= \frac{\sqrt{2\pi}}{e}\cdot\frac{\ell^{d-\ell}}{k^{(\ell-1)/2}} \\ &\geqslant \frac{\ell^{d-\ell}}{k^{\ell/2}} \\ &= \frac{\ell^{d-\ell}}{(d/\ell)^{\ell/2}}, \end{aligned}$$

which implies that

$$\begin{aligned} (d-\ell)\log(\ell) - \frac{\ell}{2}\log(d) + \frac{\ell}{2}\log(\ell) \leqslant \log(n) \\ \implies \left(d - \frac{\ell}{2}\right)\log(\ell) - \frac{\ell}{2}\log(d) \leqslant \log(n). \end{aligned}$$

(In this proof, all logarithms are base two.) If we fix d and set $f(\ell)$ to be the function on the left-hand side of the final inequality, with $\ell \in (0, d)$, then one computes that $f'(\ell)$ is a decreasing function. In particular, $f(\ell)$ takes its minimum value in the range $\ell \in (0, d)$ either when ℓ is as large as possible or as small as possible.

If ℓ is as small as possible, then $\ell = 2$ and we obtain that

$$f(2) \leqslant \log(n) \iff d - \log(d) - 1 \leqslant \log(n).$$

If ℓ is as large as possible, then $\ell = \frac{d}{2}$ and we obtain that

$$f\left(\frac{d}{2}\right) \leqslant \log(n) \iff \frac{d}{2}\log(d) - \frac{3d}{4} \leqslant \log(n).$$

Now it is easy to check that, for $d \geqslant 4$,

$$d - \log(d) - 1 \leqslant \frac{d}{2}\log(d) - \frac{3d}{4},$$

and we conclude that

$$d - \log(d) - 1 \leqslant \log(n). \tag{2.1}$$

On the other hand, if $k(G) \geqslant \frac{n}{2}$, then lemmas 2.4 and 2.7 imply that

$$\frac{n}{2} < \frac{\mathrm{e}^{\pi\sqrt{2d/3}}}{d^{3/4}}.$$

Taking logs and using (2.1), we get

$$d < \frac{1}{4}\log d + \pi\sqrt{\frac{2d}{3}}\log e + 2,$$

which, since $d > 20$, is false. This concludes the proof. □

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

2.4. Groups of Lie type

For groups of Lie type, we will use results of Fulman and Guralnick giving bounds on the number of conjugacy classes.

Theorem 2.9 [**6**, theorem 1.1]. *Let G be a connected simple algebraic group of rank r over a field of positive characteristic. Let F be a Steinberg endomorphism of G with G^F a finite group of Lie type over the field $\mathbf{F}_q$. Then*

$$k(G^F) \leqslant \min\{27.2q^r, q^r + 68q^{r-1}\}.$$

Theorem 2.10 [**6**, corollary 1.2]. *Let G be an almost simple group with socle S, a simple group of Lie type of untwisted rank r defined over $\mathbf{F}_q$. Then $k(G) \leqslant 100q^r$.*

We also introduce the following notation. For a finite group G, let $P(G)$ be the minimal degree of a faithful permutation representation of G. If G is almost simple with socle S, then $P(G)$ coincides with the minimal degree of a faithful transitive permutation representation of G, and moreover $P(S) \leqslant P(G)$. The values of $P(G)$ for G a finite simple group are known; they are listed for instance in [**12**, table 4].

Now we deal with exceptional groups.

Lemma 2.11. *Let G be almost simple with socle S, a simple exceptional group of Lie type. Then $k(G) < \frac{1}{2}|G : M|$ for all core-free maximal subgroups M of G.*

Proof. We prove the stronger inequality $k(G) < P(S)/2$. We use the values for $P(S)$ given in [**12**], as well as the fact that $k(G) \leqslant 100q^r$ (from theorem 2.10).

If S is not a Suzuki group, then the value of $P(S)$ given in [**12**] is sufficient to prove that $k(G) < P(S)/2$, except for the groups with socle $G_2(3)$, $G_2(4)$, $G_2(5)$, ${}^3D_4(2)$, ${}^2F_4(2)'$ and ${}^2G_2(3^3)$. In these cases, we can verify $k(G) < P(S)/2$ using the ATLAS [**3**].

If S is a Suzuki group, then [**25**] tells us that $k(S) = q + 3$, and lemma 2.1 implies that $k(G)$ is at most $(q + 3)f$, where $q = 2^f$. On the other hand, $P(S) = q^2 + 1$ by [**12**]. Then $(q + 3)f \geqslant \frac{1}{2}(q^2 + 1)$ if and only if $q = 8$ (recall that f is odd and $f \geqslant 3$). But if $q = 8$, [**3**] tells us that $S.3$ has 17 conjugacy classes and in this case, too, we have $k(G) < P(S)/2$. □

Next we deal with the case in which G has socle $\mathrm{PSL}_d(q)$.

Lemma 2.12. *Let G be almost simple with socle $S \cong \mathrm{PSL}_d(q)$. Let M be a core-free maximal subgroup of G, and write $n = |G : M|$. If $k(G) \geqslant \frac{n}{2}$, then one of the following holds.*

1. *G and n are listed in table 4.*
2. *$G \leqslant \mathrm{P\Gamma L}_d(q)$ and M stabilizes a 1-dimensional or a $(d-1)$-dimensional subspace of $\mathbf{F}_q^d$, thus $n = \frac{q^d-1}{q-1}$.*

Note that, in table 4, in order to ensure that the lemma is true, $n = 6$ appears for $G = \mathrm{SL}_2(4)$, but not for $G = \mathrm{PSL}_2(5)$ (even though $\mathrm{SL}_2(4) \cong \mathrm{PSL}_2(5)$). Similarly,

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

Table 4. *Faithful primitive permutation representations of degree n for almost simple groups G with socle* $\mathrm{PSL}_d(q)$ *such that* $k(G) \geqslant \frac{n}{2}$, *and the action is not isomorphic to an action in (B) (see the remark after the statement of lemma 2.12)*

G	n	$k(G)$
$\mathrm{SL}_2(4) = A_5$	6,10	5
$\mathrm{SL}_2(4).2 = S_5$	6,10	7
$\mathrm{PSL}_2(5) = A_5$	5,10	5
$\mathrm{PGL}_2(5) = S_5$	5,10	7
$\mathrm{PSL}_2(7)$	7,7	6
$\mathrm{PSL}_2(9) = A_6$	6,6	7
$\mathrm{PSL}_2(9).2 = S_6$	6,6,15,15	11
$\mathrm{PSL}_2(11)$	11,11	8
$\mathrm{SL}_3(2)$	8	6
$\mathrm{SL}_3(2).2$	8	9
$\mathrm{SL}_4(2) = A_8$	8, 28	14
$\mathrm{SL}_4(2).2 = S_8$	8,28,35	22

$n = 5$ appears for $\mathrm{PSL}_2(5)$, but not for $\mathrm{SL}_2(4)$. Similar considerations apply for the isomorphic groups $\mathrm{PSL}_2(7)$ and $\mathrm{SL}_3(2)$.

Proof. In this proof we use [14]. The main theorem of this paper, together with theorem 2.10, implies that, if $k(G) \geqslant n/2$, then either $d \leqslant 4$, or

$$(d, q) \in \{(5, 2), (5, 4), (5, 8), (6, 2), (7, 2)\}, \tag{2.2}$$

or $H := M \cap \mathrm{P\Gamma L}_d(q)$ is reducible, or H normalizes $\mathrm{PSp}_d(q)$.

Assume first that $d \geqslant 5$. This rules out the case in which H normalizes $\mathrm{PSp}_d(q)$. Let us now consider the case where H is reducible, stabilizing a subspace of dimension m.

Assume first that $2 \leqslant m \leqslant d-2$. Then $n = |G : M| > q^{m(d-m)} \geqslant q^{2d-4}$. If $k(G) \geqslant \frac{n}{2}$ then, using theorem 2.10, we deduce that $q^{d-3} < 200$. We want to whittle down the possibilities, as follows. [6, proposition 3.6] states that $k(\mathrm{PSL}_d(q)) \leqslant 2.5q^{d-1}$. This, together with the knowledge of $|\mathrm{Out}(S)|$ and lemma 2.1, reduces easily to the cases $(d, q) = (5, 2), (5, 3), (5, 4), (6, 2)$. The same argument and [14] rule out the cases $(d, q) = (5, 8), (7, 2)$ in (2.2). We can deal with the remaining cases with GAP [8].

Assume now that $m \in \{1, d-1\}$. The case in which $G \leqslant \mathrm{P\Gamma L}_d(q)$ appears in item (2) of the statement. If $G \not\leqslant \mathrm{P\Gamma L}_d(q)$, then M is a novelty and $|G : M| \geqslant q^{2d-3}$, and the GAP calculation from the previous paragraph rules out all possibilities.

Let us turn, then, to study what happens when $d \in \{2, 3, 4\}$. We make use of the counts given in [19].

When $d = 2$, [19] implies that

$$k(\mathrm{PSL}_2(q)) = \frac{1}{(q-1, 2)}\,(q + 4(q-1, 2) - 3) \;\text{ and }\; k(\mathrm{PGL}_2(q)) = q + (2, q-1).$$

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

Table 5. *Faithful primitive permutation representations of degree n for almost simple classical groups G with socle $S \ncong \mathrm{PSL}_d(q)$ such that $k(G) \geqslant \frac{n}{2}$*

G	n	$k(G)$
$\mathrm{SO}_8^-(2)$	119	60
$\mathrm{Sp}_8(2)$	120,136	81
$\mathrm{SO}_8^+(2)$	120	67
$\mathrm{Sp}_6(2)$	28, 36	30
$\mathrm{PSp}_4(3) = \mathrm{PSU}_4(2)$	27,36,40,40	20
$\mathrm{PSp}_4(3).2 = \mathrm{PSU}_4(2).2$	27,36,40,40,45	25
$\mathrm{PSU}_4(3).(2 \times 2)$	112	59
$\mathrm{P\Gamma U}_4(3)$	112	61
$\mathrm{SU}_3(3)$	28	14
$\mathrm{SU}_3(3).2$	28	16

We use this in combination with the explicit list of maximal subgroups in $\mathrm{PSL}_2(q)$ to conclude that either

(1) $q \leqslant 11$; or

(2) $q = 16$ and M is the normalizer of a torus, or a subfield subgroup such that $M \cap S \cong \mathrm{PGL}_2(\sqrt{q})$; or

(3) $q \in \{25, 49, 81, 64, 256\}$ and M is a subfield subgroup such that $M \cap S \cong \mathrm{PGL}_2(\sqrt{q})$.

Using [8] we get the possibilities in table 4.

Next assume that $d = 3$. If q is odd, then using [19] we see that $k(\mathrm{PSL}_3(q)) \leqslant q^2 + q$, and this, along with [14], allows us to conclude that $q \leqslant 9$. These possibilities can all be excluded using [3]. If q is even, then [19] implies that $k(G) \leqslant 2f(q^2 + q + 10)$ where $q = 2^f$. Using the list of subgroups in [2] this is enough to conclude that $q \leqslant 16$. Now [8] excludes the remainder.

Finally, assume that $d = 4$. If q is odd, then [19] implies that $k(G) \leqslant 2f(q^3 + q^2 + 5q + 21)$ where $q = p^f$. We use [14] to conclude that $q = 3$. This final case is ruled out with [3]. If q is even, then [19] implies that $k(\mathrm{SL}_4(q)) = q^3 + q^2 + q$ and, again, we use the list of subgroups in [2] to conclude that $q \leqslant 16$. Now [2, 3, 8] rule out all except the listed exceptions for $q = 2$. □

Finally we deal with almost simple classical groups with socle S not isomorphic to $\mathrm{PSL}_d(q)$. Note that to deal with this class of groups it is sufficient to consider $S = \mathrm{PSU}_d(q)$ with $d \geqslant 3$ and $(d, q) \neq (3, 2)$; $S = \mathrm{PSp}_d(q)$, with $d \geqslant 4$ and $(d, q) \neq (4, 2)$; and $S = \mathrm{P\Omega}_d^{\varepsilon}(q)$ with $d \geqslant 7$.

Lemma 2.13. *Let G be almost simple with classical socle S, $S \ncong \mathrm{PSL}_d(q)$. Let M be a core-free maximal subgroup of G, and write $n = |G : M|$. If $k(G) \geqslant \frac{n}{2}$, then G and n are listed in table 5.*

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

Proof. In order to exclude some potential examples, our basic strategy will be to use the bound $k(G) \leqslant |G : S| k(S)$ from lemma 2.1, and try to show that this is smaller than $P(S)/2$. In order to bound $k(S)$, we will use the results in [6] for specific families, as follows.

Suppose that $S \cong \mathrm{PSU}_d(q)$. In this case [6, proposition 3.10] implies that $k(S) \leqslant 8.26 q^{d-1}$, and we use the values for $P(S)$ given in [12] to obtain that either S is in

$$\{\mathrm{PSU}_5(2), \mathrm{PSU}_6(2), \mathrm{PSU}_7(2), \mathrm{PSU}_5(3), \mathrm{PSU}_5(4)\}$$

or else $d \leqslant 4$. Groups with the five possible socles with $d > 4$ can be ruled out using [8].

If $S = \mathrm{PSU}_4(q)$, then [19] implies that

$$k(S) = \begin{cases} \frac{1}{4}(q^3+q^2+7q+23), & q \equiv 3 \pmod 4; \\ \frac{1}{2}(q^3+q^2+7q+9), & q \equiv 1 \pmod 4; \\ q^3+q^2+3q+2, & q \equiv 0 \pmod 2). \end{cases}$$

Thus, in any case, $k(G) \leqslant 2f(q^3+q^2+7q+23)$ where $q = p^f$. Since $P(S) = (q+1)(q^3+1)$, by [12], we conclude that $q \in \{2,3,4,5,8,16\}$. If $q \leqslant 5$, then [8] yields the listed cases. If $q \in \{8,16\}$, then $G = \mathrm{P\Gamma U}_4(q)$. The case $q = 8$ is eliminated by [1]; we now consider the case $q = 16$. We want to apply lemma 2.2 with $G = \mathrm{P\Gamma U}_4(16)$ and $N = \mathrm{SU}_4(16)$. Consider the split torus T of N of order 17^3, which intersects 284 nontrivial N-classes. By looking at eigenvalues, we see that none of these classes is fixed by the standard field automorphism σ of order 8 normalizing T. We deduce from lemma 2.2 that $k(G) \leqslant 8(q^3+q^2+3q+2-284/2) = 34080$, which is enough to conclude that $k(G) < P(S)/2$.

If $G = \mathrm{PSU}_3(q)$, then [19] implies that

$$k(S) = \begin{cases} q^2+q+2, & q \not\equiv 2 \pmod 3; \\ \frac{1}{3}(q^2+q+12), & q \equiv 2 \pmod 3). \end{cases}$$

Thus, in any case, $k(G) \leqslant 2f(q^2+q+12)$ where $q = p^f$. Since $P(S) = q^3+1$ if $q \neq 5$, by [12], we conclude that $q \leqslant 9$ or $G = \mathrm{P\Gamma U}_3(16)$. For $q \leqslant 9$, we obtain the listed examples using [3, 8]. For $G = \mathrm{P\Gamma U}_3(16)$, the same argument used for the case $\mathrm{P\Gamma U}_4(16)$ works.

Suppose that $S \cong \mathrm{PSp}_d(q)$. If $d \geqslant 6$, then we use [6, theorems 3.12 and 3.13] along with the values for $P(S)$ given in [12] to conclude that S is one of the following:

$$\{\mathrm{PSp}_6(3), \mathrm{Sp}_6(2), \mathrm{Sp}_8(2), \mathrm{Sp}_{10}(2)\}.$$

We use [3, 8] to check these cases and obtain the listed examples.

If $S = \mathrm{PSp}_4(q)$, then we use [26] (for q odd) and [5] (for q even) to establish that

$$k(\mathrm{Sp}_4(q)) = \begin{cases} q^2+5q+10, & q \text{ odd}; \\ q^2+2q+3, & q \text{ even}. \end{cases}.$$

This, combined with [12], implies that $q \leqslant 9$. Now [3, 8] yield the listed examples.

Suppose that $S \cong \mathrm{P}\Omega_{2\ell+1}(q)$. Here we assume that $\ell \geqslant 3$ and that q is odd. Now [6, theorem 3.19] along with the values for $P(S)$ given in [12] imply that $S = \mathrm{P}\Omega_7(3)$. This final case can be excluded using [3].

Suppose that $S \cong \mathrm{P}\Omega^{\pm}_{2\ell}(q)$ **with** q **odd.** We make use of [6, theorems 3.16 and 3.18] along with the values for $P(S)$ given in [12] to obtain that

$$S \in \{\mathrm{P}\Omega^{\pm}_{10}(3), \mathrm{P}\Omega^{\pm}_{8}(3), \mathrm{P}\Omega^{+}_{8}(5), \mathrm{P}\Omega^{+}_{8}(7)\}.$$

In $\mathrm{P}\Omega^{+}_{8}(5)$ and $\mathrm{P}\Omega^{+}_{8}(7)$, the outer automorphism group is S_4, and a subgroup of S_4 has at most 5 conjugacy classes, therefore by lemma 2.1 we get $k(G) \leqslant 5k(S)$, which is enough to rule out these possibilities.

We use [1, 8] to rule out the cases where $S = \mathrm{P}\Omega^{\pm}_{10}(3)$ or $\mathrm{P}\Omega^{\pm}_{8}(3)$.

Suppose that $S \cong \Omega^{\pm}_{2\ell}(q)$ **with** q **even.** We make use of [6, theorem 3.22] along with the values for $P(S)$ given in [12] to obtain that

$$S \in \{\Omega^{\pm}_{10}(2), \Omega^{\pm}_{8}(2), \Omega^{+}_{8}(4)\}.$$

We use [3] for the groups with $q = 2$, and we get the listed examples. We can rule out $\Omega^{+}_{8}(4)$ using [1]. □

2.5. Proof of theorem 1.2

Let G be an almost simple primitive permutation group of degree n. Putting together lemmas 2.3, 2.8, 2.11, 2.12 and 2.13, we get that either $k(G) < n/2$, or we are in case (2) of theorem 1.2 (regarding table 1, recall remark 1.3(iii)).

Note that, if the action of G is isomorphic to an action in (B), then $k(G) < 100n$ follows immediately from theorem 2.10.

It remains to prove the asymptotic statement, that is, either $k(G) = O(n^{3/4})$, or the action of G is isomorphic to an action in (A) or (B). We assume that this latter condition does not hold, and we want to show $k(G) = O(n^{3/4})$.

We may assume that G is sufficiently large along the proof. Let M be the stabilizer of a point in the action of G on n points; in particular $|G : M| = n$. Write $S = \mathrm{Soc}(G)$.

Assume first that $S \cong A_d$, and assume that M is transitive on d points; we will show that $k(G) = n^{o(1)}$ as d tends to infinity. By lemma 2.4 (or by the Hardy–Ramanujan asymptotic formula), we have $k(G) = O(1)^{\sqrt{d}}$. On the other hand, by lemmas 2.5 and 2.6, if M is primitive on d points then $n \geqslant (d/O(1))^d$; and by (2.1) in the proof of lemma 2.8, if M is imprimitive then $n \geqslant c^d$ for some constant c. Therefore $k(G) = n^{o(1)}$ if $S \cong A_d$.

Assume now that $S \cong \mathrm{PSL}_d(q)$. We have $k(G) = O(q^{d-1})$ by theorem 2.10. If $H := M \cap \mathrm{P\Gamma L}_d(q)$ is reducible in the action on $\mathbf{F}_q^d$, one possibility is that it stabilizes a k-space for some $2 \leqslant k \leqslant d-2$, and so $n > q^{2d-4}$. If $d \to \infty$, we see that $k(G) = o(n^{3/4})$; and if d is bounded, we see that $k(G) = O(n^{3/4})$ (we actually have $k(G) = o(n^{3/4})$ as $q \to \infty$ except for the case $(d, k) = (4, 2)$). The remaining possibility is that $G \not\leqslant \mathrm{P\Gamma L}_d(q)$ and M is the stabilizer of a flag (pair of incident point-hyperplane) or antiflag (pair of complementary point-hyperplane). But in this case $n > q^{2d-3}$, and the previous computation is sufficient for $d \geqslant 4$; and for $d = 3$, $k(G) = O(n^{2/3})$.

If $d = 2m \geqslant 4$ and H normalizes $\mathrm{PSp}_{2m}(q)$, then

$$n \geqslant \frac{1}{(m, q-1)} \cdot q^{m^2-m}(q^3-1)(q^5-1)\cdots(q^{2m-1}-1)$$

and we can easily check that $k(G) = O(q^{d-1}) = o(n^{3/4})$.

If now H is irreducible and does not normalize $\mathrm{PSp}_d(q)$, we can apply the main theorem of [14]. We see easily that $k(G) = o(n^{3/4})$ as $d \to \infty$. If d is bounded instead, then we can assume that q is large and in particular [14] implies that $n \geqslant q^{(d-1)(d-2)/2}$, which proves $k(G) = o(n^{3/4})$ in case $d \geqslant 5$. In case $d \leqslant 4$, we can use the list of maximal subgroups of $\mathrm{PSL}_d(q)$ given in [2] in order to prove $k(G) = o(n^{3/4})$ (if H is irreducible, $n \gg q^{3/2}$ for $d = 2$; $n \gg q^4$ for $d = 3$; and $n \gg q^5$ for $d = 4$).

Assume finally that S is a group of Lie type and that $S \not\cong \mathrm{PSL}_d(q)$. In this case we want to show $k(G) = O(P(S)^{3/4})$, which implies the statement, since $P(S) \leqslant n$. This can be checked combining $k(G) = O(q^r)$ (where r is the untwisted rank of S) with the value of $P(S)$ given in [12]. In fact, we get $k(G) = o(P(S)^{3/4})$ unless $S \cong \mathrm{PSU}_4(q)$. (We remark that, in the latter case, $P(S)$ is equal to the number of totally singular 2-subspaces of $\mathbf{F}_{q^2}^4$; we also use [2] in order to see that $n \gg q^5$ for every other primitive action of G.)

This concludes the proof of theorem 1.2.

Remark 2.14. In theorem 1.2(1), we actually showed that $k(G) = o(n^{3/4})$ as $n \to \infty$ unless $S \cong \mathrm{PSL}_4(q)$ and G acts on the set of 2-subspaces of $\mathbf{F}_q^4$, or $S \cong \mathrm{PSU}_4(q)$ and G acts on the set of totally singular 2-subspaces of $\mathbf{F}_{q^2}^4$. In these cases, we have $n \sim q^4$ and $k(S) \asymp q^3$, therefore $k(S) \asymp n^{3/4}$. (Recall that $f \asymp g$ means that $c_1 f \leqslant g \leqslant c_2 f$ for positive constants c_1 and c_2.)

3. The general case

In this section we prove theorem 1.1. We first prove a lemma.

Lemma 3.1. *Let G be a finite almost simple group with socle S. Then either $S \cong A_5, A_6, \mathrm{PSL}_2(7), \mathrm{PSL}_2(11)$, or $4 \cdot k(G)^2 < |S|$. Moreover, $k(G)^3 = O(|S|)$.*

We note that we actually have $k(G)^3 = o(|S|)$ as $|S| \to \infty$, except for the case $S \cong \mathrm{PSL}_2(q)$.

Proof. We first prove $4 \cdot k(G)^2 < |S|$, with the listed exceptions.

Assume first that $S \cong A_d$. Then lemmas 2.4, 2.5 and a straightforward computation imply that it is sufficient to show

$$3.2 \cdot e^{5.2\sqrt{d}+d} < d^{d+2},$$

which is true for $d \geqslant 10$. For $d \leqslant 9$, direct check gives the exceptions in the statement.

Assume now that $S \cong \mathrm{PSL}_d(q)$. Using the bound $k(S) \leqslant 2.5q^{d-1}$ from [6], lemma 2.1, and the fact that $|G : S| \leqslant 2f(d, q-1)$, with $q = p^f$, we see that it is sufficient to show

$$100f^2(d,q-1)^3 < q^{d(d-1)/2-2d+2}(q^2-1)\cdots(q^d-1).$$

If $d \geqslant 4$, we can easily verify that this is true. For $d=3$, [19] tells us that $k(S) \leqslant q^2+q$. We compute that it is enough to show

$$16f^2(3,q-1)^3(q+1) < q(q-1)(q^3-1),$$

which can be verified unless $q=2,4$. The case $q=2$ is in the statement (since $\mathrm{SL}_3(2) \cong \mathrm{PSL}_2(7)$), while the case $q=4$ can be excluded with [8].

If $d=2$, we use the exact value of $k(S)$ (recalled in the proof of lemma 2.12), in order to reduce to the cases $q \leqslant 16$ or $q=25,27,32,64,81,128,256$. Then we use [8] and we get the cases $q=4,5,7,9,11$ in the statement.

Assume that S is classical and that $S \ncong \mathrm{PSL}_d(q)$. Here one can prove that $4k(G)^2 < |S|$ using the upper bounds for $k(S)$ given in [6]. One can also argue as follows (but this is not necessary). If G appears in table 1, we can make a direct check. If G is not in table 1, then theorem 1.2 tells us that $k(G) < P_m(G)/2$, where $P_m(G)$ denotes the smallest index of a core-free maximal subgroup of G. Now it is known (see [15, p. 178]) that $P(S) \leqslant |S|^{1/2}$. In particular, whenever $P_m(G)=P(S)$, we can immediately conclude $4k(G)^2 < |S|$. Certainly we have $P(S) \leqslant P_m(G)$. Using the value of $P(S)$ given in [12] (see also [4], where an explicit M for which $|S:M|=P(S)$ is given), and consulting [15], we deduce that $P_m(G)=P(S)$ unless $S \cong \mathrm{PSU}_3(5)$, $S \cong \mathrm{Sp}_4(q)$ with q even, $S \cong \mathrm{P\Omega}_8^+(q)$, or $S \cong \mathrm{P\Omega}_{2m}^+(3)$ with $m \geqslant 4$. (If $S \cong \mathrm{PSU}_3(5)$, $|S:M|=P(S)$ where M is isomorphic to A_7; if $S \cong \mathrm{P\Omega}_{2m}^+(3)$, M is the stabilizer of a nondegenerate 1-space.) We can exclude the unitary case with [3]; in the symplectic case we can use $k(\mathrm{Sp}_4(q)) = q^2+2q+3$ (see the proof of lemma 2.13); in the orthogonal cases we can use the bound $k(\mathrm{P\Omega}_{2m}^+(q)) \leqslant 14q^m$ given in [6].

Assume that S is exceptional. In the proof of lemma 2.11 we actually proved $k(G) < P(S)/2$, therefore we conclude by the argument of the previous paragraph.

Assume finally that S is sporadic. We use [3] to conclude $4k(G)^2 < |S|$.

It remains to prove the asymptotic statement, that is, $k(G)^3 = O(|S|)$ (and indeed $k(G)^3 = o(|S|)$ if $S \ncong \mathrm{PSL}_2(q)$). We may assume that S is sufficiently large, and the statement is easy to check, using lemma 2.4 and theorem 2.10. □

We need three technical lemmas.

Lemma 3.2. *Assume that $S \cong A_d$, or that S is the socle of some group appearing in table 1. If $S \leqslant B \leqslant A \leqslant \mathrm{Aut}(S)$, then $k(B) \leqslant k(A)$, unless $A = \Omega_8^+(2).S_3$.*

Proof. If $S \cong A_d$, the statement follows from lemma 2.7, and by direct check in case $d=6$. If S is the socle of some group appearing in table 1, we use [3]. □

Lemma 3.3. *Assume that G is almost simple with socle $S \cong \mathrm{PSL}_d(q)$, with $d \geqslant 3$, and let m denote the number of flags (that is, pairs of incident point-hyperplane) in $\mathbf{F}_q^d$. Then, $k(G) < m/2$ and $k(G) = O(m^{2/3})$.*

We note that we actually have $k(G) = o(m^{2/3})$ as $m \to \infty$, except in case $d=3$.

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

Proof. We begin with the inequality $k(G) < m/2$. If $G \nleqslant \mathrm{P\Gamma L}_d(q)$, then G acts primitively on the set of flags, and the statement follows from theorem 1.2. Assume now that $G \leqslant \mathrm{P\Gamma L}_d(q)$. Then G acts primitively on the set of 2-subspaces of $\mathbf{F}_q^d$. It is easy to see that the number of 2-subspaces is smaller than the number of flags. Assume that $d \geqslant 4$. Then, by lemma 2.12, either $k(G) < m/2$, or G appears in table 4. Examining table 4, we see that $k(G) < m/2$ also in the latter case.

We are left with the case $d = 3$. We have $k(G) \leqslant 100q^2$ by theorem 2.10, and moreover $m > q^3$. In particular, if $k(G) \geqslant m/2$ then $q < 200$. We whittle down a bit the possibilities. Write $a = (3, q-1)$. By [**19**] and lemma 2.1, we deduce $k(G) \leqslant |G : S| \cdot (q^2 + q + 5a - 5)/a < 2|G : S| \cdot q^2$. Therefore, if $q = p^f$, we have $q < 8af$. Using $q < 200$, we see that we are reduced to the cases $q \leqslant 27$ and $q = 32, 64$, which can be checked with [**8**] (if $q \neq 2, 4, 8, 16$, it is enough to show that $4f(q^2 + q + 5a - 5)$ is smaller than m, without computing the actual value of $k(G)$).

The asymptotic statement $k(G) = O(m^{2/3})$ can be checked easily using $k(G) = O(q^{d-1})$. □

Lemma 3.4. *Let A be an almost simple primitive group of degree m with socle S, and assume that A is not in the possibilities of theorem 1.2(2). Let $S \leqslant B \leqslant A$. Then, $k(B) < m/2$. Moreover, for every fixed $\alpha > 3/4$, if S is sufficiently large then $k(B) < m^\alpha$.*

Proof. We begin with the inequality $k(B) < m/2$. Write $m = |A : M|$ for some core-free maximal subgroup M of A. If $B = A$, the claim is true by theorem 1.2. Assume, for a contradiction, that there exists B such that $k(B) \geqslant m/2 = |B : B \cap M|/2$. Let T be a core-free subgroup of B, maximal with respect to the property that $B \cap M \leqslant T$ and that T is core-free in B (that is, T does not contain S).

Note that, by the maximality of T, the subgroups of B properly containing T must contain S. Then choose C such that $T < C \leqslant B$ and T is maximal in C. In particular, C acts primitively on the cosets of T, and moreover, by lemma 2.1,

$$|B : C| \cdot k(C) \geqslant k(B) \geqslant \frac{|B : C||C : T|}{2},$$

whence $k(C) \geqslant |C : T|/2$. Therefore we can apply theorem 1.2. The first possibility is that C appears in table 1. By lemma 3.2 and $k(B) \geqslant m/2$, we deduce $A = \Omega_8^+(2).S_3$. Then by [**3**] $m \geqslant 3600$, which contradicts $k(B) \geqslant m/2$. By lemma 3.2, we also see that it cannot be $S \cong A_d$. By theorem 1.2 and lemma 2.12, the only remaining possibility is that $S \cong \mathrm{PSL}_d(q)$, $C \leqslant \mathrm{P\Gamma L}_d(q)$ and T is the stabilizer of a 1-space or $(d-1)$-space. In particular, $B \cap M$ stabilizes a 1-space or a $(d-1)$-space.

Assume first that $A \leqslant \mathrm{P\Gamma L}_d(q)$. By assumption, M is not the stabilizer of a 1-space or $(d-1)$-space. Then, there is no other possibility for M (in such a way that $B \cap M$ fixes a 1-space or $(d-1)$-space), which is a contradiction. Assume finally that $A \nleqslant \mathrm{P\Gamma L}_d(q)$. Then the only possibility is that M is the stabilizer of a flag or antiflag. In particular, m is larger than the number of flags in $\mathbf{F}_q^d$, which contradicts lemma 3.3. This final contradiction proves that $k(B) < m/2$ for every $S \leqslant B \leqslant A$.

Now we want to show that, for every fixed $\alpha > 3/4$, if S is sufficiently large then $k(B) < m^\alpha$ for every $S \leqslant B \leqslant A$.

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

By theorem 1.2, we have $k(A) = O(m^{3/4})$. Assume that $k(B) \geqslant m^\alpha$. We want to show that S has bounded order (in other words, we want to show that, if S is sufficiently large, we get a contradiction). By taking S large, we have $k(B) > k(A)$. Much of the argument of the first part of the proof carries unchanged, except that we have the inequality

$$|B : C| \cdot k(C) \geqslant k(B) \geqslant |B : C|^\alpha \cdot |C : T|^\alpha,$$

from which $k(C) \geqslant |C : T|^\alpha \cdot |B : C|^{\alpha-1}$. Note that $|B : C| \leqslant |\mathrm{Out}(S)|$ and $|C : T| \geqslant P(S)$. Using [**12**, table 4], we easily see that $|\mathrm{Out}(S)| = P(S)^{o(1)}$ as $|S| \to \infty$ (the statement being obvious in case $S \cong A_d$), from which we get that, for every fixed $\beta < \alpha$,

$$k(C) \geqslant |C : T|^\alpha \cdot |B : C|^{\alpha-1} > |C : T|^\beta$$

if S is sufficiently large. In particular we may take $\beta > 3/4$, and by theorem 1.2, we deduce that C and $|C : T|$ must appear in item (2) of the theorem. Then, the argument that we used in the first part of the proof, together with lemma 3.3, gives a contradiction. □

3.1. Proof of theorem 1.1

We can now prove theorem 1.1. We will apply many times lemma 2.1, usually with no mention. Moreover, we will often use the following theorem from [**17**], which we recalled in the introduction.

Theorem 3.5. *Let $r \geqslant 1$ and let $P \leqslant S_r$. Then, $k(P) \leqslant 2^{r-1}$.*

Let G be a primitive permutation group of degree n with nonabelian socle $\mathrm{Soc}(G) \cong S^r$, with S simple.

In the following proof, a permutation group G of degree n in *product action* refers to a group $G \leqslant A \wr S_r$, where A is almost simple primitive on m points with socle S and G acts on $n = m^r$ points (so we do not include the actions that sometimes are called *holomorph compound* and *compound diagonal*; see [**18**, **21**] for descriptions and terminology for finite primitive permutation groups).

Proof of theorem 1.1. **Assume first** that the action of G is not product action; we want to show $k(G) < n/2$ and $k(G) = O(n^\delta)$ for some absolute $\delta < 1$. We begin with the first inequality.

We have $r \geqslant 2$ and either $n = |S|^r$, or $r = \ell t$ with $\ell \geqslant 2$, $t \geqslant 1$ and $n = |S|^{(\ell-1)t}$. In particular $n \geqslant |S|^{r/2}$. Furthermore, $G \leqslant \mathrm{Aut}(S) \wr S_r$. Then, by lemma 2.1 and theorem 3.5, $k(G) \leqslant k(G \cap \mathrm{Aut}(S)^r) \cdot 2^{r-1}$. Now $G \cap \mathrm{Aut}(S)^r$ admits a normal series of length r in which every factor is almost simple with socle S; therefore, by theorem 3.5, $k(G \cap \mathrm{Aut}(S)^r) \leqslant f(S)^r$, where $f(S) = \max\{k(A) : S \leqslant A \leqslant \mathrm{Aut}(S)\}$. We deduce that it is enough to show that

$$2f(S) < |S|^{1/2}.$$

By lemma 3.1, this is true unless $S \cong A_5, A_6, \mathrm{PSL}_2(7), \mathrm{PSL}_2(11)$. Assume then that we are in one of these cases. If $n = |S|^r$ or $n = |S|^{(\ell-1)t}$ with $\ell \geqslant 3$, then $n \geqslant |S|^{2r/3}$,

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

hence by the same argument as above we have $k(G) < n/2$ provided

$$2f(S) < |S|^{2/3}.$$

We can check that this is true. Therefore we are reduced to the case in which $S \in \{A_5, A_6, \mathrm{PSL}_2(7), \mathrm{PSL}_2(11)\}$, $r = 2t$ and $n = |S|^t$.

Assume first that $t = 1$, and let $h(S)$ be the maximum number of conjugacy classes of a primitive group on $|S|$ points with socle S^2. We can use [8] in order to compute that $h(S) < |S|/2$.

Next we deal with any $t \geqslant 1$. We have $G \leqslant D \wr S_t$, where D has socle S^2 and is primitive on $|S|$ points. Then $k(G) \leqslant k(G \cap D^t) \cdot 2^{t-1}$. Now $G \cap D^t$ admits a normal series of length t in which every factor has socle S^2 and is primitive on $|S|$ points; in particular $k(G \cap D^t) \leqslant h(S)^t < (|S|/2)^t$ and therefore $k(G) < |S|^t/2 = n/2$, as wanted.

We turn now to the asymptotic statement; namely, $k(G) = O(n^\delta)$ for an absolute $\delta < 1$. We assume that n is sufficiently large and we show $k(G) \leqslant n^\delta$ (which is equivalent up to enlarging δ). We will show in various places that $k(G) \leqslant n^{\delta'}$ for various δ'. In order to simplify notation, we will always use the same symbol δ—one should just take the maximum.

Assume first that S is sufficiently large. By lemma 3.1, we have $f(S) < |S|^{0.35}/2$. Using $n \geqslant |S|^{r/2}$, we deduce $k(G) < n^{0.7}$.

Assume now that S has bounded order. If $S \ncong A_5, A_6, \mathrm{PSL}_2(7), \mathrm{PSL}_2(11)$, by lemma 3.1 we have $2f(S) < |S|^{1/2}$, and in particular

$$k(G) < (2 \cdot f(S))^r < |S|^{r\delta/2} \leqslant n^\delta$$

for some $\delta < 1$ absolute (since $|S|$ is bounded).

Assume then that $S \cong A_5, A_6, \mathrm{PSL}_2(7), \mathrm{PSL}_2(11)$. If $n = |S|^r$ or $n = |S|^{(\ell-1)t}$ with $\ell \geqslant 3$, then $n \geqslant |S|^{2r/3}$ and, as already observed, $f(S) < |S|^{2/3}/2$; therefore the same argument as above applies. The remaining case is $\ell = 2$ and $r = 2t$. We already observed that $2h(S) < |S|$, from which we get

$$k(G) < (2 \cdot h(S))^t < |S|^{t\delta} = n^\delta$$

for some $\delta < 1$ absolute.

Assume now that the action of G is product action, and assume that we are not in case (2) of the statement. We want to show $k(G) < n/2$ and $k(G) = O(n^\delta)$ for some $\delta < 1$ absolute. We begin with the first inequality. We have $G \leqslant A \wr S_r$, $n = m^r$, and A is an almost simple group with socle S admitting a primitive action on m points, which is not among the possibilities of theorem 1.2(2).

Note that $k(G) \leqslant k(G \cap A^r) \cdot 2^{r-1}$, and $G \cap A^r$ admits a normal series of length r in which each factor is isomorphic to a subgroup $S \leqslant B \leqslant A$. By lemma 3.4, $k(B) < m/2$ for every $S \leqslant B \leqslant A$, and therefore $k(G \cap A^r) < (m/2)^r$ and $k(G) < n/2$, as wanted.

The asymptotic statement $k(G) = O(n^\delta)$ for some $\delta < 1$ is proved as we did for the case in which $n = |S|^r$ or $n = |S|^{(\ell-1)t}$, dividing the cases $|S|$ sufficiently large and $|S|$ bounded. If S is sufficiently large, by lemma 3.4 we have $k(B) < m^{0.8}/2$ for every $B \leqslant S \leqslant A$, and therefore $k(G) < n^{0.8}/2$. If S has bounded order, we

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

only need to use $k(B) < m/2$ for every $S \leqslant B \leqslant A$, which holds again in view of lemma 3.4.

Assume now that we are in case (2)(i) of the statement; we want to show $k(G) < n^{1.31}$. We have $G \leqslant A \wr S_r$ and A is almost simple acting primitively on m points.

Let us consider first the case in which $A = M_{12}$ acting primitively on $m = 12$ points. If $r \geqslant 4$, [**11**] tells us that a subgroup of S_r has at most $5^{(r-1)/3} < 5^{r/3}$ conjugacy classes. In particular, using that $k(A) = 15$, we deduce that $k(G) < 15^r \cdot 5^{r/3}$, which we verify to be at most $n^{1.31}$. If $r \leqslant 3$, we use that a subgroup of S_r has at most r conjugacy classes, so $k(G) \leqslant 15^r \cdot r$, which is less than $n^{1.31}$ for $r \leqslant 3$.

Let us consider now all other cases. By lemma 3.2 we have $k(B) \leqslant k(A)$ for every $S \leqslant B \leqslant A$. Then $k(G) \leqslant k(A)^r \cdot 2^{r-1} < (2k(A))^r$, so we only need to show that $2k(A) \leqslant m^{1.31}$. This can be checked easily going through all cases in table 1 (but leaving out the case of M_{12} acting on 12 points).

Assume finally that we are in case (2)(ii) of the statement, and the action of A is isomorphic to an action in (B); in particular $m = (q^d - 1)/(q - 1)$. We want to show $k(G) < n^{1.9}$.

If $r \geqslant 4$, by theorem 2.10 we have

$$k(G) \leqslant (100q^{d-1})^r \cdot 5^{(r-1)/3} < (100 \cdot 5^{1/3})^r \cdot n,$$

hence we are done provided $100 \cdot 5^{1/3} \leqslant m^{0.9}$, that is, $m \geqslant 303$. If $r \leqslant 3$, we use $k(G) \leqslant (100q^{d-1})^r \cdot r$, and we see that $m \geqslant 303$ is enough also in these cases.

Therefore we assume that $m < 303$; this leaves us with the cases $d = 6, 7, 8$ and $q = 2$; or $d = 5$ and $q \leqslant 3$; or $d = 4$ and $q \leqslant 5$, or $d = 3$ and $q \leqslant 16$; or $d = 2$ and $q < 302$.

We whittle down slightly the possibilities for $d = 2$. In the proof of lemma 2.12, we recalled the exact value of $k(\mathrm{PSL}_2(q))$ and $k(\mathrm{PGL}_2(q))$. Using this and $q < 302$, it is easy to deduce that $k(A) \leqslant 8(q + 1) = 8m$. By the same computation as above, we are done provided $8 \cdot 5^{1/3} \leqslant m^{0.9}$, that is, $m \geqslant 19$. Therefore if $d = 2$ then we may assume that $q \leqslant 17$.

Now we deal with all the remaining cases (for $d \leqslant 8$). We only need to show that $k(A) \cdot 5^{1/3} \leqslant m^{1.9}$, which can be checked with [**8**]. □

4. Further comments

4.1. Theorem 1.1(2)(i)

In theorem 1.1(2)(i), we proved $k(G) < n^{1.31}$. Can we get better bounds? Since we have finitely many possibilities for the almost simple primitive group A of degree m, we fix A and m, and we want to estimate $k(G)$ where $G \leqslant A \wr S_r$ is primitive, mainly when r is large.

First, we show that it is not always true that $k(G) = o(n)$ as $n \to \infty$ (and in fact it is not even true that $k(G) = O(n)$).

Lemma 4.1. *Consider $A = M_{12}$ acting primitively on 12 points, and consider $G = A \wr C_r$ acting on $n = 12^r$ points, where C_r is cyclic of order r. If r is large enough, then $k(G) > n^{1.08}$.*

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

Proof. We have

$$k(G) \geqslant \frac{k(A)^r}{r}.$$

Since $k(A) = 15$, this is easily seen to be larger than $n^{1.08}$ for r large enough. □

The same argument shows that $k(G) > n^\alpha$ for some absolute $\alpha > 1$ whenever A and m in table 1 are such that $k(A) > m$ (but in the table, A and m are replaced by G and n). This happens rarely; specifically, when

$$(A, m) \in \{(M_{12}, 12), (M_{24}, 24), (\mathrm{Sp}_6(2), 28)\}.$$

Let us consider now the case in which $k(A) \leqslant m$ (by looking at table 1, this is equivalent to $k(A) < m$). By lemma 3.2, we have $k(B) \leqslant k(A)$ for every subgroup $S = \mathrm{Soc}(A) \leqslant B \leqslant A$. We assume that $r \geqslant 4$, so that by [**11**] a subgroup of S_r has at most $5^{(r-1)/3} < 5^{r/3}$ conjugacy classes. Then, we have $k(G) < (k(A)5^{1/3})^r$, and whenever $k(A) \cdot 5^{1/3} < m$ we get $k(G) < n^\delta$ for some absolute $\delta < 1$. The condition $k(A) \cdot 5^{1/3} < m$ holds in some cases, but not quite in all.

Therefore one should try to change the argument. We make the following conjecture.

Conjecture 4.2. Let A be an almost simple primitive group on m points appearing in table 1, and assume that $k(A) < m$. Then, for every primitive subgroup $G \leqslant A \wr S_r$ on $n = m^r$ points, $k(G) = o(m^r)$ as $r \to \infty$.

In order to address conjecture 4.2, it seems relevant to estimate the number of conjugacy classes in wreath products (although G need not be a full wreath product, which is a complication).

4.2. Conjugacy classes in wreath products

Let $A \neq 1$ be a finite group, and let P be a transitive permutation group of degree r. Throughout, denote $k = k(A)$. Consider the wreath product $G = A \wr P$. By theorem 3.5, we have $k(G) \leqslant k^r \cdot 2^{r-1}$. Does a considerably better bound hold? If necessary, we may imagine that A is fixed and $r \to \infty$. In fact, we ask a question which is independent of the relation between A and r.

Question 2. Let $A \neq 1$ be a finite group, let $P \leqslant S_r$ be transitive, and set $G = A \wr P$. Is $k(G) = O(k^r)$?

We should note that a positive answer to question 2 would not necessarily provide a positive answer to conjecture 4.2 (since, in conjecture 4.2, G needs not be a wreath product).

The next lemma gives an affirmative answer to question 2 for the case where $P \leqslant S_r$ is regular. Before proving the lemma, we recall the combinatorial description of the conjugacy classes of $G = A \wr P$, in general: View the k conjugacy classes of A as k distinct colours. Let $\pi_1, \ldots, \pi_t$ be representatives for the conjugacy classes of P. For each i, colour the cycles of π_i in each possible way, and identify two colourings if one is obtained from the other by conjugation in $\mathrm{C}_P(\pi_i)$ (note that $\mathrm{C}_P(\pi_i)$ acts

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

on the cycles of π_i). In this way we get the conjugacy classes of $G = A \wr P$; these can be thought of as the conjugacy classes of P, in which each cycle has a colour, and two colourings are identified as described above.

Lemma 4.3. *Let $G = A \wr P$ with $A \neq 1$, $P \leqslant S_r$ regular, and set $k = k(A)$. Then*

$$k(G) = \frac{k^r}{r} + O(rk^{r/2}).$$

Proof. Assume that $\pi \in P$ has order at least 2; then π has at most $r/2$ cycles. Summing over all nontrivial elements $\pi \in P$, we deduce that the number of colourings of the cycles of all nontrivial elements $\pi \in P$ is at most $rk^{r/2}$.

Now we consider the colourings of the cycles of the identity element $1 \in P$. The action of $P = \mathrm{C}_P(1)$ on the cycles can clearly be identified with the action of P on the set $\{1, \dots, r\}$.

Let $\mathcal{C}$ be a colouring of $\{1, \dots, r\}$. The size of the P-orbit of $\mathcal{C}$ is strictly smaller than r if and only if $\mathcal{C}$ is stabilized by a nontrivial element $\pi \in P$, which implies that $\mathcal{C}$ has constant colours along the cycles of π. Therefore, the number of such colourings is at most $rk^{r/2}$. This implies that the number of colourings whose P-orbit has size r is at least $k^r - rk^{r/2}$, whence

$$k(G) = \frac{k^r}{r} + O(rk^{r/2}).$$

This proves the lemma. □

4.3. Theorem 1.1(2)(ii)

In this case we have $G \leqslant A \wr S_r$ where A is almost simple primitive on m points. Work of Maróti [**20**] tells us that $k(G) \leqslant p(n)$ and this bound is achieved if the action of A is isomorphic to an action in (A).

Assume instead that the action of A is isomorphic to an action in (B). We have shown that, in this case, $k(G) < n^{1.9}$. This is certainly a long way from being sharp; let us consider what might be possible.

First, recall that, if q is odd, and if $A = \mathrm{PGL}_2(q)$, then $k(A) = q + 2 > m = q + 1$. If we take for instance $q = 5$ then, by the same argument as in lemma 4.1, we see that $k(A \wr C_r) > n^{1.08}$ for r sufficiently large. Therefore it is not true in general that $k(G) = O(n)$.

However, in the other direction, observe that, for any G in the case under consideration, the usual bound $k(G) < (100q^{d-1})^r \cdot 2^r$ implies that, for every fixed $\epsilon > 0$, $k(G) < n^{1+\epsilon}$ provided $\mathrm{PSL}_d(q)$ is sufficiently large (or, equivalently, provided m is sufficiently large). We are left with the natural question:

Question 3. Let A be an almost simple primitive group isomorphic to a group in (B), and assume that $G \leqslant A \wr S_r$ is primitive on $n = m^r$ points. What is the minimum value of ϵ such that $k(G) < n^{1+\epsilon}$?

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press

References

1 W. Bosma, J. Cannon and C. Playoust. The magma algebra system. I. The user language. *J. Symb. Comput.* **24** (1997), 235–265. Computational algebra and number theory (London, 1993).

2 J. N. Bray, D. F. Holt and C. M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, vol. 407 (Cambridge: Cambridge University Press, 2013).

3 J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson. *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups, with computational assistance from J. G. Thackray* (Eynsham: Oxford University Press, 1985).

4 B. N. Cooperstein. Minimal degree for a permutation representation of a classical group. *Isr. J. Math.* **30** (1978), 213–235.

5 H. Enomoto. The characters of the finite symplectic group $\mathrm{Sp}(4, q)$, $q = 2^f$. *Osaka J. Math.* **9** (1972), 75–94.

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

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

8 The GAP Group. GAP – groups, algorithms, and programming, version 4.10.2, 2019.

9 D. Garzoni and N. Gill. Large minimal invariable generating sets in the finite symmetric groups. *Isr. J. Math.* to appear, 2021.

10 R. M. Guralnick and A. Maróti. On the non-coprime $k(GV)$-problem. *J. Algebra* **385** (2013), 80–101.

11 M. Garonzi and A. Maróti. On the number of conjugacy classes of a permutation group. *J. Comb. Theory Ser. A* **133** (2015), 251–260.

12 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. Am. Math. Soc.* **367** (2015), 7665–7694.

13 R. M. Guralnick and P. H. Tiep. The non-coprime $k(GV)$ problem. *J. Algebra* **293** (2005), 185–242.

14 W. M. Kantor. Permutation representations of the finite classical groups of small degree or rank. *J. Algebra* **60** (1979), 158–168.

15 P. Kleidman and M. W. Liebeck. *The subgroup structure of the finite classical groups*. London Mathematical Society Lecture Note Series, vol. 129 (Cambridge: Cambridge University Press, 1990).

16 L. G. Kovács and G. R. Robinson. On the number of conjugacy classes of a finite group. *J. Algebra* **160** (1993), 441–460.

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

18 M. W. Liebeck, C. E. Praeger and J. Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Aust. Math. Soc., Ser. A* **44** (1988), 389–396.

19 I. G. Macdonald. Numbers of conjugacy classes in some finite classical groups. *Bull. Aust. Math. Soc.* **23** (1981), 23–48.

20 A. Maróti. Bounding the number of conjugacy classes of a permutation group. *J. Group Theory* **8** (2005), 273–289.

21 C. E. Praeger. The inclusion problem for finite primitive permutation groups. *Proc. London Math. Soc.* **60** (1990), 68–88.

22 W. Pribitkin. Simple upper bounds for partition functions. *Ramanujan J.* **18** (2009), 113–119.

23 C. E. Praeger and J. Saxl. On the orders of primitive permutation groups. *Bull. London Math. Soc.* **12** (1980), 303–307.

24 H. Robbins. A remark on Stirling's formula. *Am. Math. Mon.* **62** (1955), 26–29.

25 M. Suzuki. On a class of doubly transitive groups. *Ann. Math.* **75** (1962), 105–145.

26 G. E. Wall. On the conjugacy classes in the unitary, symplectic and orthogonal groups. *J. Aust. Math. Soc.* **3** (1963), 1–62.

https://doi.org/10.1017/prm.2021.74 Published online by Cambridge University Press