Journal of Algebra 375 (2013) 302–321

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

The base size of a primitive diagonal group

Joanna B. Fawcett [1]

Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, United Kingdom

ARTICLE INFO

Article history:
Received 9 May 2012
Available online 30 November 2012
Communicated by Martin Liebeck

Keywords:
Finite permutation groups
Primitive groups
Diagonal actions
Base size

ABSTRACT

A base $\mathscr{B}$ for a finite permutation group G acting on a set Ω is a subset of Ω with the property that only the identity of G can fix every point of $\mathscr{B}$. We prove that a primitive diagonal group G has a base of size 2 unless the top group of G is the alternating or symmetric group acting naturally, in which case the minimal base size of G is determined up to two possible values. We also prove that the minimal base size of G satisfies a well-known conjecture of Pyber. Moreover, we prove that if the top group of G does not contain the alternating group, then the proportion of pairs of points that are bases for G tends to 1 as $|G|$ tends to infinity. A similar result for the case when the degree of the top group is fixed is given.

1. Introduction

Let G be a finite permutation group acting on a set Ω. A *base* $\mathscr{B}$ for G is a non-empty subset of Ω whose pointwise stabiliser is trivial. The *base size* of G is the minimal cardinality of a base for G, and we denote this by $b(G)$. Bases have been very useful in group theory, both theoretically in bounding the size of a primitive permutation group (e.g. [2]) and computationally (surveyed in [38]). Accordingly, much research has been done on bounding the base size of a primitive permutation group (e.g. [23]).

Recently, it has been proved in [5,8–10,12,20,27] that if G is a finite almost simple primitive permutation group, then $b(G) \leqslant 7$ unless the action of G is standard, in which case the base size is unbounded in general. (G has a *standard action* if G either has socle A_m and acts on the set of k-subsets or partitions of $\{1, \ldots, m\}$, or is a classical group that acts primitively on an orbit of subspaces of its natural module.) This was conjectured to be the case by Cameron [11]. In fact, it is

E-mail address: j.b.fawcett@dpmms.cam.ac.uk.

[1] The author was supported in part by the Cambridge Commonwealth Trust, the NSERC, and St John's College, Cambridge.

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2012.11.020

proved in [8] that if G is A_m or S_m acting primitively on a set of size n, then $b(G) = 2$ unless the action of G is standard or G is one of 12 listed exceptions. Together with the work of J. James [21], this classifies the primitive actions of A_m and S_m with base size 2. A similar result for primitive actions of almost simple classical groups is forthcoming in [6,7]. With the goal in mind of a theorem classifying the primitive permutation groups that admit a base of size 2, we must therefore consider the other types of primitive permutation groups as classified by the O'Nan–Scott Theorem [24]. These types broadly consist of diagonal groups, twisted wreath products, wreath products, and affine groups. In this paper, we focus on groups of diagonal type. These primitive permutation groups are not often studied, but they are important, especially to the base size 2 problem. This is because the base size of a primitive diagonal group behaves much like the base size of an almost simple primitive permutation group, in that the base size is either 2, or, for several explicitly given classes of groups, can be unbounded.

Let T be a finite non-abelian simple group, and let k be an integer that is at least 2. A group of diagonal type G with socle T^k acts primitively on a set $\Omega(k, T)$ with degree $|T|^{k-1}$ and is a (not necessarily split) extension of T^k by a subgroup of $\mathrm{Out}(T) \times S_k$; precise definitions will be given in Section 2. The permutation group induced from the conjugation action of G on the k factors of T^k is called the top group of G and is denoted by P_G. The group P_G is either primitive in its action on k points, or possibly trivial when $k = 2$, and it plays an important role in determining the base size of G. Observe that if the top group P_G does not contain the alternating group A_k, then we necessarily have $k \geqslant 5$ since A_k and S_k are the only primitive permutation groups of degree k when $k < 5$ (and the only permutation groups when $k = 2$).

Theorem 1.1. *Let G be a group of diagonal type with socle T^k for some finite non-abelian simple group T. If the top group P_G is not the alternating group A_k or the symmetric group S_k, then $b(G) = 2$.*

This is the best result we could hope for since a group of diagonal type never has a base of size 1. The proof of Theorem 1.1 is constructive, though it depends on a non-constructive result in [37] which determines exactly when a primitive permutation group has a regular orbit on the power set of the domain of its action. Note that as a consequence of [37], [20, Lemma 4.2] of Gluck, Seress and Shalev constructs a base of size 3 for a group of diagonal type whose top group is neither alternating, symmetric nor of degree less than 32.

The situation is markedly different, however, when the top group P_G is either the alternating group A_k or the symmetric group S_k. Observe that groups of diagonal type can be constructed for any finite non-abelian simple group T and for arbitrarily large k.

Theorem 1.2. *Let G be a group of diagonal type with socle T^k for some finite non-abelian simple group T where the top group P_G contains the alternating group A_k. If $k \geqslant 3$ then*

$$b(G) = \left\lceil \frac{\log k}{\log |T|} \right\rceil + a_G$$

where $a_G \in \{1, 2\}$ and $a_G = 1$ if $|T|^l < k \leqslant |T|^l + |T| - 1$ for some positive integer l. If $k = 2$, then $b(G) = 3$ when $P_G = 1$, and $b(G) \in \{3, 4\}$ otherwise.

We will see in Proposition 3.12 that if either $k = |T|$, or if $\mathrm{Inn}(T)^k \rtimes S_k \leqslant G$ and k is $|T|^l$ or $|T|^l - 1$ for some positive integer l, then $a_G = 2$. Also, we give examples when $k = 2$ and $P_G = S_2$ of two groups G with $b(G) = 3$ and two groups G with $b(G) = 4$ (see the end of Section 3). Thus Theorem 1.2 is essentially best possible. However, it remains unclear precisely when the two possibilities occur. In particular, we do not know when $b(G) = 2$, though $2 < k < |T|$ is a necessary condition.

Theorems 1.1 and 1.2 also allow us to prove a well-known conjecture of Pyber in the case of diagonal type groups. For any finite permutation group G of degree n, it is easy to see that $\lceil \log |G| / \log n \rceil \leqslant b(G)$; simply show that $|G| \leqslant n^{b(G)}$ by considering an appropriate chain of pointwise stabilisers of base elements. Pyber [35] conjectured that there exists an absolute constant c for

which the base size of a primitive permutation group G of degree n is at most $c \log|G|/\log n$. For example, almost simple groups with non-standard primitive actions satisfy Pyber's conjecture because their base sizes are bounded above by an absolute constant [12,20,27], and Benbenishty has verified the conjecture for standard actions of almost simple groups (see [28] for a reference). Moreover, soluble primitive permutation groups satisfy Pyber's conjecture [36], as do certain other affine primitive permutation groups [19,29].

Theorem 1.3. *Let G be a group of diagonal type. Then G satisfies Pyber's conjecture. In fact,*

$$b(G) \leqslant \left\lceil \frac{\log|G|}{\log n} \right\rceil + 2$$

where n is the degree of G.

We remark that although mention is made in [29] of a forthcoming paper by Seress in which Pyber's conjecture is proved for various primitive permutation groups including groups of diagonal type, this paper did not appear. Moreover, in Gluck, Seress and Shalev [20], a base for groups of diagonal type is constructed and it is claimed there that the argument can be improved to construct a base of size $\lceil \log|G|/\log n \rceil + 3$ (where G is a group of diagonal type with degree n), but the details of the proof of this weaker result are not given.

Now we consider the probabilistic side of the theory. The result of [5,8–10,12,20,27] that $b(G) \leqslant 7$ when G is an almost simple primitive permutation group with a non-standard action actually has a stronger form. Cameron and Kantor [12] conjectured that for such groups G there exists an absolute constant c with the property that the probability that a random c-tuple of points is a base for G tends to 1 as the order of G tends to infinity. In the same paper, Cameron and Kantor proved that their conjecture is true with $c = 2$ when the socle of G is alternating. Liebeck and Shalev [27] then proved the general conjecture for some undetermined constant c by using [20] and counting fixed points of elements. The constant $c = 6$ was finally established through work in [9,30]. We have an analogous result for groups of diagonal type. The proof uses the method of counting fixed points of elements as in [27].

Theorem 1.4. *Let G be a group of diagonal type with socle T^k for some finite non-abelian simple group T, and suppose that the top group P_G does not contain the alternating group A_k. Then the proportion of pairs of points from $\Omega(k, T)$ that are bases for G tends to 1 as $|G| \to \infty$.*

Similarly, we have a partial result that includes the case when the top group P_G contains the alternating group A_k. One consequence of this result is that for any fixed k at least 5, there are only finitely many groups of diagonal type with a degree k top group which do not have base size 2.

Theorem 1.5. *Let G be a group of diagonal type with socle T^k for some finite non-abelian simple group T where $k \geqslant 5$. The proportion of pairs of points from $\Omega(k, T)$ that are bases for G tends to 1 if k is fixed as $|G| \to \infty$.*

Explicitly, Theorems 1.4 and 1.5 say the following. Let δ denote either the symbol ∞, or an integer that is at least 5. If $\delta = \infty$, let $\mathscr{D}_\delta$ be the collection of those groups of diagonal type whose top group is not alternating or symmetric, and if δ is an integer, let $\mathscr{D}_\delta$ be the collection of those groups of diagonal type whose top group has degree δ. For each δ, and for each $G \in \mathscr{D}_\delta$ with socle T^k (where $k = \delta$ if δ is an integer), let $n_\delta(G)$ denote the proportion of ordered pairs (ω_1, ω_2) in $\Omega(k, T)^2$ for which $\{\omega_1, \omega_2\}$ is a base for G. Fix δ. Then for every $\varepsilon > 0$, there exists a natural number N such that $n_\delta(G) > 1 - \varepsilon$ for every $G \in \mathscr{D}_\delta$ satisfying $|G| > N$.

This paper is organised as follows. Section 2 gives some basic notation and describes the groups of diagonal type in detail. Theorems 1.1, 1.2 and 1.3 are then proved in Section 3: Theorem 1.1 follows from Propositions 3.3 and 3.7, while Theorem 1.2 essentially follows from Propositions 3.8, 3.10

and 3.12. The proof of Theorem 1.4 will take up most of Section 4, and the proof of Theorem 1.5 comes at the end of that section. Note that Sections 3 and 4 are essentially independent of each other. Note also that most of the results presented in this paper depend upon the classification of the finite simple groups.

2. Preliminaries

In this paper, all groups are finite and all actions and group homomorphisms are performed on the right. Note that the CFSG refers to the classification of the finite simple groups and that the notation used to denote the finite simple groups is consistent with that of [22].

First we have some basic notation. Let X and Y be groups. We denote the semidirect product of X and Y by $X \rtimes Y$; note that under this notation, X is a normal subgroup of $X \rtimes Y$, Y acts on X, and $(x_1, y_1^{-1})(x_2, y_2) = (x_1 x_2^{y_1}, y_1^{-1} y_2)$ for all (x_1, y_1^{-1}) and (x_2, y_2) in $X \rtimes Y$. If Y acts on $[m] := \{1, \dots, m\}$, then Y acts on X^m by permuting the coordinates; that is, the element y^{-1} of Y maps $(x_1, \dots, x_m)$ to $(x_{1^y}, \dots, x_{m^y})$ for all $(x_1, \dots, x_m) \in X^m$. This action defines the wreath product $X^m \rtimes Y$, which we denote by $X \wr_m Y$. Moreover, if X is a permutation group on a set Ω, then $X \wr_m Y$ acts on Ω^m by sending $(\omega_1, \dots, \omega_m)$ to $(\omega_{1^y}^{x_{1^y}}, \dots, \omega_{m^y}^{x_{m^y}})$ for each $(x_1, \dots, x_m)y^{-1} \in X \wr_m Y$. This is called the *product action*. As is standard, we denote the stabiliser in X of the point $\omega \in \Omega$ by X_ω, the conjugacy class of $x \in X$ by x^X, and the set of right cosets of the subgroup Y of X by $(X : Y)$. Note that A_m and S_m respectively denote the alternating group and the symmetric group on the set $[m]$. Also, if $x, y \in X$, then $[x, y] = x^{-1} y^{-1} x y$, and if $\alpha \in \mathrm{Aut}(X)$, we write $\overline{\alpha}$ for the coset $\alpha \,\mathrm{Inn}(X)$ in the outer automorphism group $\mathrm{Out}(X)$. Lastly, the function $\log x$ denotes the natural logarithm unless otherwise specified.

The following definitions for groups of diagonal type can be found in [24]. For an integer $k \geqslant 2$ and a finite non-abelian simple group T, we define

$$
\begin{aligned}
W(k, T) &:= \left\{(\alpha_1, \dots, \alpha_k)\pi \in \mathrm{Aut}(T) \wr_k S_k \colon \overline{\alpha}_1 = \overline{\alpha}_i \text{ for all } i\right\},\\
D(k, T) &:= \left\{(\alpha, \dots, \alpha)\pi \in \mathrm{Aut}(T) \wr_k S_k\right\},\\
\Omega(k, T) &:= \big(W(k, T) : D(k, T)\big),\\
A(k, T) &:= W(k, T) \cap \mathrm{Aut}(T)^k.
\end{aligned}
$$

Note that $W(k, T) = A(k, T) \rtimes S_k$ and that $W(k, T)$ is an extension of T^k by $\mathrm{Out}(T) \times S_k$. Moreover, $W(k, T)$ acts faithfully on the right coset space $\Omega(k, T)$ since $\mathrm{Inn}(T)^k$ is the unique minimal normal subgroup of $W(k, T)$.

We say that a group G has *diagonal type* if there exist an integer k and a finite non-abelian simple group T such that $\mathrm{Inn}(T)^k \leqslant G \leqslant W(k, T)$ and G acts primitively on $\Omega(k, T)$. Any such G has socle T^k and degree $n := |T|^{k-1}$. Let G be a subgroup of $W(k, T)$ containing $\mathrm{Inn}(T)^k$, and let P_G denote the subgroup of S_k consisting of those $\pi \in S_k$ for which there exists $(\alpha_1, \dots, \alpha_k) \in A(k, T)$ such that $(\alpha_1, \dots, \alpha_k)\pi \in G$. Then G is a group of diagonal type if and only if either (i) P_G is primitive on $[k]$, or (ii) $k = 2$ and $P_G = \{1\}$ (see [15, Theorem 4.5A]). In particular, $W(k, T)$ is a group of diagonal type. Note that P_G is permutation isomorphic to the image of the action of G on $\{T_1, \dots, T_k\}$ by conjugation, where T_i is the i-th direct factor of $\mathrm{Inn}(T)^k$, since for any $w := (\alpha_1, \dots, \alpha_k)\pi \in W(k, T)$, we have $w^{-1} T_i w = T_{i\pi}$ for all $i \in [k]$. The group P_G is referred to as the *top group* of G. As long as the context prevents any confusion, we write D, W and Ω for $D(k, T)$, $W(k, T)$ and $\Omega(k, T)$ respectively.

Let us briefly examine Ω. Its elements have the form $\omega := D(\alpha_1, \dots, \alpha_k)\pi$ for some $(\alpha_1, \dots, \alpha_k)\pi \in W$. Now $(\alpha_i, \dots, \alpha_i)\pi \in D(k, T)$ for any $i \in [k]$, so fixing i we see that $\omega = D(\alpha_{i\pi^{-1}}^{-1}\alpha_{1\pi^{-1}}, \dots, 1, \dots, \alpha_{i\pi^{-1}}^{-1}\alpha_{k\pi^{-1}})$ where 1 is in the i-th coordinate. Since $\overline{\alpha}_l = \overline{\alpha}_j$ for all l and j, elements of Ω actually have the form $D(\varphi_{t_1}, \dots, \varphi_{t_k})$, where for each $t \in T$, the map $\varphi_t : T \to T$ is defined to be conjugation by t. Moreover, every element of Ω has $|T|$ representatives in $\mathrm{Inn}(T)^k$, and for each element of Ω, we may choose one coordinate to be any element of $\mathrm{Inn}(T)$ should we wish to do so.

In particular, fixing the same coordinate and element of $\mathrm{Inn}(T)$ and allowing all $(k-1)$-tuples with entries in $\mathrm{Inn}(T)$ yields the $|T|^{k-1}$ elements of Ω.

3. Base sizes for diagonal type groups

For this section, let G be a group of diagonal type with socle T^k where T is a finite non-abelian simple group. Note that for $g \in G$ and $\mathscr{B} \subset \Omega$, the set $\mathscr{B}^g$ is a base for G precisely when $\mathscr{B}$ is a base. (Indeed, this is true for any action.) Thus by transitivity there is no loss of generality in restricting our attention to those subsets of Ω that contain D. We begin by determining the pointwise stabiliser in G of any two-element subset of Ω containing D.

Lemma 3.1. *Let $\omega := D(\varphi_{t_1}, \ldots, \varphi_{t_k}) \in \Omega$ and write $t^{i,j}$ for $t_i^{-1}t_j$. Then for any $j_0 \in [k]$, we have $G_\omega \cap D = \{(\alpha, \ldots, \alpha)\pi \in G\colon\ t^{i,j_0}\alpha = t^{i\pi,j_0\pi}$ for all $i\}$.*

Proof. Fix $j_0 \in [k]$. Then $(\alpha, \ldots, \alpha)\pi \in G$ fixes ω if and only if $\varphi_{t_{j_0}}\alpha\varphi_{t_{j_0\pi}}^{-1} = \varphi_{t_i}\alpha\varphi_{t_{i\pi}}^{-1}$ for all i. This is equivalent to $\varphi_{t^{i,j_0}}\alpha = \alpha\varphi_{t^{i\pi,j_0\pi}}$ for all i. Evaluating this last expression at t for each $t \in T$, we see that it is equivalent to the statement that $(t^{i,j_0}\alpha)(t^{i\pi,j_0\pi})^{-1}$ centralises $t\alpha$ for all $t \in T$. Since the centre of T is trivial, the proof is complete. □

Lemma 3.1 then has the following useful, easy corollary.

Lemma 3.2. *Suppose that $(\alpha, \ldots, \alpha)\pi \in G$ fixes $D(\varphi_{t_1}, \ldots, \varphi_{t_k}) \in \Omega$. If there exists j_0 for which t_{j_0} and $t_{j_0\pi}$ are trivial, then $t_i\alpha = t_{i\pi}$ for all i.*

Lemma 3.1 motivates the following notation. For $\omega := D(\varphi_{t_1}, \ldots, \varphi_{t_k}) \in \Omega$, let $\mathcal{O}_\omega$ denote the $k \times k$ matrix whose (i, j)-th entry is the order of $t^{i,j} = t_i^{-1}t_j$. If $(\alpha, \ldots, \alpha)\pi \in G_\omega$, then since $t^{i,j_0}\alpha = t^{i\pi,j_0\pi}$ for all i and for any fixed j_0 by Lemma 3.1, the $j_0\pi$-th column of $\mathcal{O}_\omega$ must be a permutation of the entries of the j_0-th column. Note that $\mathcal{O}_\omega$ is a symmetric matrix whose diagonal entries are all 1.

Now we prove Theorem 1.1 for $k > 32$. The proof relies mainly on a theorem of Seress [37] which determines precisely when a regular orbit on the power set of the domain of a primitive action exists; his work is based on work by Cameron, Neumann and Saxl [13] who proved using the CFSG that such a regular orbit exists for all but finitely many degrees so long as the action is not the natural action of the alternating or symmetric group. Note that the result of [37], as mentioned in the Introduction, can be applied to [20, Lemma 4.2] of Gluck, Seress and Shalev to construct a base of size 3 for a group of diagonal type whose top group has degree at least 33 and does not contain the alternating group (and a larger base otherwise). However, the proof of Proposition 3.3 below proceeds somewhat differently to construct a base of size 2.

Proposition 3.3. *If $A_k \nleqslant P_G$ and $k > 32$, then $b(G) = 2$.*

Proof. Since P_G is primitive and does not contain A_k, and also since $k > 32$, [37, Theorem 1] implies that $[k]$ can be partitioned into two non-empty subsets Δ and Γ such that the setwise stabiliser of Δ in P_G is trivial. Since the setwise stabiliser of Γ must then also be trivial, we may assume without loss of generality that $|\Delta| \geqslant |\Gamma|$. Clearly $|\Delta| \geqslant 4$, so we may partition Δ into two non-empty subsets Δ_1 and Δ_2 such that neither $|\Delta_1|$ nor $|\Delta_2|$ is $|\Gamma|$. Let x and y be generators for T (which is possible by [1]), and define t_i to be 1 if $i \in \Delta_1$, x if $i \in \Delta_2$, and y if $i \in \Gamma$. Let $\omega := D(\varphi_{t_1}, \ldots, \varphi_{t_k})$.

Let $(\alpha, \ldots, \alpha)\pi$ be an element of G fixing ω. Define a function $g : \{1, \ldots, k\} \to \mathbb{N}$ by mapping i to the number of entries in column i of $\mathcal{O}_\omega$ that are 1, where $\mathcal{O}_\omega$ is as defined above. Writing $\Delta_3 = \Gamma$, we have $g(i) = |\Delta_j|$ if $i \in \Delta_j$. Then $g(i) \neq g(j)$ for all $i \in \Gamma$ and $j \in \Delta$, but $g(i) = g(i\pi)$ for all i since by Lemma 3.1, the entries of column $i\pi$ are a permutation of the entries of column i. Hence $\Gamma\pi = \Gamma$, so π is the identity. But then for any $i \in \Delta_1$, $t_{i\pi} = t_i = 1$, so by Lemma 3.2, α must fix both x and y and is therefore the identity. Thus $\{D, D(\varphi_{t_1}, \ldots, \varphi_{t_k})\}$ is a base for G. □

As for k smaller than 32, we need some more lemmas. This first lemma will also be useful in the case when the top group is alternating or symmetric.

Lemma 3.4. *Let $t_1, \ldots, t_k$ denote elements of T such that at least two of the t_i are trivial, at least one is non-trivial, and if t_i and t_j are non-trivial and $i \neq j$ then $t_i \neq t_j$. If $(\alpha, \ldots, \alpha)\pi \in G$ fixes $D(\varphi_{t_1}, \ldots, \varphi_{t_k})$, then $t_i\alpha = t_{i\pi}$ for all i.*

Proof. Let $\omega := D(\varphi_{t_1}, \ldots, \varphi_{t_k})$, and let r_i denote the order of t_i. Also, let m be the number of non-trivial t_i. To begin, assume that $t_i \neq 1$ if $i \in [m]$ and that $t_i = 1$ otherwise. Then

$$\mathcal{O}_\omega = \begin{pmatrix} A & B \\ B^T & 1_{k-m} \end{pmatrix},$$

where A is a symmetric $m \times m$ matrix whose diagonal entries are 1 and whose remaining entries are integers at least 2, B is an $m \times (k-m)$ matrix with i-th row $(r_i, \ldots, r_i)$, and 1_{k-m} is a $(k-m) \times (k-m)$ matrix in which every entry is 1. Since $k - m \geqslant 2$, columns $m+1$ through k each have at least two entries that are 1, and these are the only such columns; hence π must permute these columns, which implies that $t_{i\pi} = 1$ for $i \geqslant m+1$. The result then follows from Lemma 3.2. The proof of the general case is essentially the same since then the entries in each column of $\mathcal{O}_\omega$ will be a permutation of the entries in a column of the matrix above. □

A result of Malle, Saxl and Weigel [31] states that every finite non-abelian simple group other than $U_3(3)$ is generated by an involution and a strongly real element, which is an element that can be conjugated to its inverse by an involution. Since $U_3(3)$ is generated by an involution and an element of order 6 by [14], it follows that every finite non-abelian simple group is generated by two elements, one of which can be taken to be an involution. Since two involutions generate a dihedral group, the two generators must have different orders. This makes the next two lemmas useful. For $x, y \in T$, let $T(x, y)$ denote the set of non-trivial elements of T whose orders are different to the orders of x and y.

Lemma 3.5. *Suppose that $T = \langle x, y \rangle$ where x and y have different orders, and suppose that $k \geqslant 4$ and $P_G \neq S_k$. If P_G has base size at most $|T(x, y)| + 2$ in its action on $[k]$, then $b(G) = 2$.*

Proof. We may assume without loss of generality that $\{1, 2, \ldots, m\}$ is a base of minimal size for P_G. Since P_G is primitive and $P_G \neq S_k$, it follows that P_G contains no transpositions; thus we may conclude that $k \geqslant m + 2$. Let $t_1 := x$, $t_2 := y$, $t_i := 1$ for $\max\{3, m+1\} \leqslant i \leqslant k$, and when $m \geqslant 3$, choose $t_3, \ldots, t_m$ to be distinct elements of $T(x, y)$. Suppose that $(\alpha, \ldots, \alpha)\pi \in G$ fixes $D(\varphi_{t_1}, \ldots, \varphi_{t_k})$. Then the conditions of Lemma 3.4 are met, so $t_i\alpha = t_{i\pi}$ for all i. But α preserves order, so α fixes x and y and is therefore the identity. Then since the t_i are distinct for $i \in [m]$, π is the identity on $[m]$. Hence π is the identity, and it follows that $\{D, D(\varphi_{t_1}, \ldots, \varphi_{t_k})\}$ is a base for G. □

There is a classical result of Bochert [4] from the nineteenth century which states that every primitive permutation group of degree k that does not contain A_k has a base of size at most $k/2$ (see [15, Theorem 3.3B] for a proof). This makes the following consequence of Lemma 3.5 possible.

Lemma 3.6. *Suppose that $T = \langle x, y \rangle$ where x and y have different orders, and let C be a non-trivial conjugacy class of T with minimal cardinality. If $A_k \not\leqslant P_G$ and $k \leqslant 2|C| + 4$, then $b(G) = 2$.*

Proof. Certainly $|C| \leqslant |T(x, y)|$ since 3 distinct primes divide $|T|$, while P_G has a base of size at most $k/2$ by Bochert [4]. Thus the assumption that $k \leqslant 2|C| + 4$ implies that P_G has base size at most $|T(x, y)| + 2$ in its action on $[k]$. Note that $k \geqslant 5$ since $A_k \not\leqslant P_G$ and P_G is primitive. Hence we may apply Lemma 3.5. □

Proposition 3.7. *If $A_k \not\leqslant P_G$ and $k \leqslant 32$, then $b(G) = 2$.*

Proof. By Malle, Saxl and Weigel [31, Theorem B], T is generated by elements x and y with different orders. Let $p(T)$ denote the minimal index of a proper subgroup of T. Then by Lemma 3.6, G has base size 2 if $32 \leqslant 2p(T) + 4$, so we may assume that $p(T) \leqslant 13$. Note that $|T| \leqslant 13!/2$ since T can be embedded in the alternating group on $p(T)$ points. If T is a classical group of Lie type, then values for $p(T)$ can be found in [33,42], and if T is an exceptional group of Lie type, then values for $p(T)$ can be found in [39–41]. Of course $p(A_m) = m$, and if T is sporadic (and of order less than $13!/2$), then values for $p(T)$ can be found in [14]. Using these, we see that T must be one of $L_2(7)$, $L_2(8)$, $L_2(11)$, $L_3(3)$, M_{11}, M_{12} or A_m for $5 \leqslant m \leqslant 13$. However, it can be seen using [14] that, with the exception of A_5, none of these groups has a conjugacy class of size less than 13, and so $b(G) = 2$ by Lemma 3.6. Lastly, A_5 is $(2, 3)$-generated and has 24 elements of order 5, while P_G has a base of size at most $32/2$ by Bochert [4], so $b(G) = 2$ by Lemma 3.5. □

Together, Propositions 3.3 and 3.7 imply that $b(G) = 2$ when $A_k \not\leqslant P_G$, which establishes Theorem 1.1. Note that Pyber's conjecture (Theorem 1.3) is therefore true when $A_k \not\leqslant P_G$.

We now move on to consider those diagonal type groups G for which P_G does contain the alternating group A_k. Here it is readily seen that we will not always have base size 2: if $k > |T|$, then every element of $\Omega \setminus \{D\}$ is determined by a k-tuple of elements of T whose coordinates contain at least one repeat, and so $W(k, T)$ does not have base size 2. In fact, we will see that $b(G) \neq 2$ when $k \geqslant |T|$. We begin by constructing a base for G.

Proposition 3.8. *G has a base of size*

$$\left\lceil \frac{\log(k - |T| + 1)}{\log |T|} \right\rceil + 2$$

if $k > |T|$, and a base of size 3 if $5 \leqslant k \leqslant |T|$.

Proof. Assume that $k \geqslant 5$. Then $m := \min(|T| - 1, k - 2)$ is at least 3. Define the positive integer

$$r := \begin{cases} \left\lceil \frac{\log(k-|T|+1)}{\log |T|} \right\rceil & \text{if } k > |T|, \\ 1 & \text{if } k \leqslant |T|. \end{cases}$$

For j such that $m < j \leqslant k$, let $d_{j,0}, \ldots, d_{j,r-1}$ denote the first r digits of the base $|T|$ representation of $j - m - 1$; this is reasonable since $|T|^{r-1} \leqslant k - m - 1 < |T|^r$. Let x and y be generators for T (by [1]). Since $|T|$ is divisible by at least 3 distinct primes, we may choose some non-trivial z from T whose order is different to that of x and y. Enumerating the elements of T as $t_0, \ldots, t_{|T|-1}$ where $t_0 := 1$, $t_1 := x$, $t_2 := y$ and $t_3 := z$, we may define

$$u_{i,j} := \begin{cases} t_j & \text{if } i = 2 \text{ and } 1 \leqslant j \leqslant m, \\ x & \text{if } i = 3 \text{ and } j = 1, \\ z & \text{if } i = 3 \text{ and } j = 2, \\ t_{d_{j,i-3}} & \text{if } 3 \leqslant i \leqslant r + 2 \text{ and } m < j \leqslant k, \\ 1 & \text{otherwise,} \end{cases}$$

where $1 \leqslant i \leqslant r + 2$ and $1 \leqslant j \leqslant k$. For $1 \leqslant i \leqslant r + 2$, let ω_i denote the element $D(\varphi_{u_{i,1}}, \ldots, \varphi_{u_{i,k}})$ of Ω. We claim that $\mathscr{B} := \{\omega_1, \ldots, \omega_{r+2}\}$ is a base for G. Note that $|\mathscr{B}| = r + 2$, for if $\omega_i = \omega_{i'}$ for some distinct i and i', then there exists $t \in T$ for which $u_{i,j} = t u_{i',j}$ for all j. But then we must have $i, i' \geqslant 4$, which implies that $t = 1$, and so $d_{j,i-3} = d_{j,i'-3}$ for every $j > m$. This is certainly not the case; for example, take $j = |T|^{i-3} + m + 1$.

Let $(\alpha, \ldots, \alpha)\pi$ be an element of G_{ω_1} that fixes ω_i for all $2 \leqslant i \leqslant r + 2$. Since $u_{2,1}, \ldots, u_{2,k}$ satisfy the conditions of Lemma 3.4, we get that $u_{2,j}\alpha = u_{2,j\pi}$ for all j, and so $[m]\pi = [m]$. Now $u_{2,3} = z$

has order different to that of $u_{2,1} = x$ and $u_{2,2} = y$, so $3 \leqslant 3\pi \leqslant m$. Hence $u_{3,3\pi} = 1 = u_{3,3}$, which implies that $u_{3,j}\alpha = u_{3,j\pi}$ for all j by Lemma 3.2. But $1\pi \leqslant m$, so $u_{3,1\pi} \in \{x, z, 1\}$; this together with the fact that $u_{3,1}\alpha = u_{3,1\pi}$ forces $1\pi = 1$. Similarly, $2\pi = 2$, but then $u_{2,j}\alpha$ equalling $u_{2,j\pi}$ for $j \in \{1, 2\}$ implies that $x\alpha = x$ and $y\alpha = y$, so α is the identity. Moreover, for any $i \geqslant 4$ we have that $u_{i,1\pi} = u_{i,1} = 1$, so it follows from Lemma 3.2 that $u_{i,j\pi} = u_{i,j}$ for all i and j. In other words, for every j, the j-th and $j\pi$-th columns of the $(r + 2) \times k$ matrix whose (i, j)-th entry is $u_{i,j}$ are the same. However, by construction columns $1, \ldots, m$ are distinct from one another, as are columns $m + 1, \ldots, k$. Recalling that $[m]\pi = [m]$, it follows that π is the identity. □

Note that the CFSG was only used in the proof above to obtain that T is 2-generated. This assumption can be removed if k is sufficiently larger than $|T|$: let $x_1, \ldots, x_s$ be a set of generators for T, and in the construction of $\mathscr{B}$ above, change x to x_1, y to x_2, and $u_{i+1,2}$ to x_i for $3 \leqslant i \leqslant s$. The proof remains unchanged until we obtain $x_1\alpha = x_1$ and $x_2\alpha = x_2$. Since $u_{i,1\pi} = u_{i,1} = 1$ for $i \geqslant 4$, Lemma 3.2 implies that $u_{i,j}\alpha = u_{i,j\pi}$ for all i and j, but $2\pi = 2$, so $x_i\alpha = x_i$ for all i. The remainder of the proof is the same. To get a crude idea of how large k needs to be, note that T has a generating set of size at most $\log_2 |T|$ (as any finite group does), so we need $\log_2 |T| + 1$ to be at most $r + 2$ for this argument to work. Hence for $k \geqslant |T|^{\log_2 |T|}$, the upper bound on the base size of G in Proposition 3.8 is obtained without the CFSG.

Now we consider small values for k. The following will be used when $k = 2$.

Lemma 3.9. *If $\{D, D(\varphi_{t_1}, \ldots, \varphi_{t_k})\}$ is a base of size 2 for G, then $\bigcap_{i=1}^{k} C_T(t_i) = \{1\}$.*

Proof. If $t \in \bigcap_{i=1}^{k} C_T(t_i)$, then $(t_i^{-1}t_1)\varphi_t = t_i^{-1}t_1$ for all i. But $(\varphi_t, \ldots, \varphi_t) \in G$, and $(\varphi_t, \ldots, \varphi_t)$ fixes $D(\varphi_{t_1}, \ldots, \varphi_{t_k})$ by Lemma 3.1, so $t = 1$. □

Proposition 3.10. *If $P_G = A_k$, then $b(G) = 3$ when $k = 2$, and $b(G) = 2$ when k is 3 or 4. If $P_G = S_k$, then $b(G) \in \{3, 4\}$ when $k = 2$, and $b(G) \in \{2, 3\}$ when k is 3 or 4.*

Proof. Let x and y be generators for T (by [1]). First assume that $k = 2$. Then $\{D, D(\varphi_x, 1), D(\varphi_y, 1)\}$ or $\{D, D(\varphi_x, 1), D(\varphi_y, 1), D(\varphi_{xy}, 1)\}$ is a base for G when P_G is 1 or S_2 respectively by Lemma 3.1. Moreover, $b(G) \neq 2$ in these cases since $\{D, D(\varphi_t, 1)\}$ is not a base for G for any $t \in T$ by Lemma 3.9. Let z be a non-trivial element of T with order different to that of x and y, and suppose that k is 3 or 4. Then Lemma 3.4 implies that $\{D, D(\varphi_x, 1, 1), D(1, \varphi_y, 1)\}$ or $\{D, D(\varphi_x, \varphi_z, 1, 1), D(1, 1, \varphi_y, 1)\}$ is a base for G when P_G is S_3 or S_4 respectively. Since the natural action of A_4 has base size 2, it follows from Lemma 3.5 and [31, Theorem B] that $b(G) = 2$ when $k = 4$ and $P_G = A_4$. This leaves us with the case $k = 3$ and $P_G = A_3$. By [31, Theorem B], we may assume that y is an involution. Then a consideration of the matrix $\mathcal{O}_{D(\varphi_x, \varphi_y, 1)}$ shows that $\{D, D(\varphi_x, \varphi_y, 1)\}$ is a base for G. □

We are now able to prove Pyber's conjecture for groups of diagonal type.

Proof of Theorem 1.3. Let G be a group of diagonal type with socle T^k. It is well known that $k^k/e^{k-1} \leqslant k!$ for any integer $k \geqslant 2$. If $A_k \leqslant P_G$, then

$$\left(\frac{k|T|}{e}\right)^{k-1} \leqslant \frac{1}{2}\left(\frac{k^k}{e^{k-1}}\right)|T|^{k-1} \leqslant |P_G||T|^{k-1} \leqslant |G_D||T|^{k-1} = |G|,$$

from which we obtain

$$\frac{\log(k|T|/e)}{\log|T|} \leqslant \frac{\log|G|}{\log|T|^{k-1}}.$$

But $k - |T| + 1 \leqslant k|T|/e$, so when $A_k \leqslant P_G$ and $k > |T|$, Proposition 3.8 implies that G satisfies Pyber's conjecture and, in particular, the bound in the statement of Theorem 1.3. Since $b(G)$ is constant and

at most 4 when $A_k \not\leqslant P_G$ or $k \leqslant |T|$ by Propositions 3.3, 3.7, 3.8 and 3.10, and since we always have $\lceil \log|G| / \log|T|^{k-1} \rceil \geqslant 2$, the proof is complete. □

In fact, since $\log|G| / \log|T|^{k-1} \leqslant b(G)$ (see the Introduction), this proof provides a lower bound for $b(G)$ whose value is the case $a_G = 1$ of Theorem 1.2 when $e|T|^l < k \leqslant |T|^{l+1}$ for some non-negative integer l. However, this can be improved upon. To do so, we need to know more about the structure of G.

Lemma 3.11. *Suppose that $A_k \leqslant P_G$. If there exists an odd integer s with $1 < s \leqslant k$ such that s is relatively prime to the order of every element of* $\mathrm{Out}(T)$, *then* $\mathrm{Inn}(T)^k \rtimes A_k \leqslant G$.

Proof. If π is an s-cycle, then $\pi \in A_k \leqslant P_G$, so $(\alpha, \ldots, \alpha)\pi \in G$ for some $\alpha \in \mathrm{Aut}(T)$ whose image $\bar{\alpha}$ in $\mathrm{Out}(T)$ has order r, say. Certainly $(\alpha^r, \ldots, \alpha^r)\pi^r \in G$, but G contains $\mathrm{Inn}(T)^k$, so π^r is an element of G. Hence π is as well. As π was an arbitrary s-cycle, the group G contains every s-cycle. But the s-cycles generate A_k, so $\mathrm{Inn}(T)^k \rtimes A_k \leqslant G$. □

The next result provides a lower bound on $b(G)$ which will allow us to prove that $b(G) \geqslant \lceil \log k / \log|T| \rceil + 1$ for Theorem 1.2. In fact, several other lower bounds are proved under somewhat specialised conditions; this is done to show that Theorem 1.2 is essentially best possible.

Proposition 3.12. *Suppose that $A_k \leqslant P_G$, and let l be a positive integer. Suppose that either $k > |T|^l$, or $l = 1$ and $k = |T|$, or $\mathrm{Inn}(T)^k \rtimes S_k \leqslant G$ and k is $|T|^l$ or $|T|^l - 1$. Then $b(G) \geqslant l + 2$.*

Proof. Suppose that one of the four assumptions on k and G in the statement of the proposition is true. Then certainly $k \geqslant |T| - 1$, but $|\mathrm{Out}(T)|$ is much smaller than $|T|$ by the CFSG (see Lemma 4.8, for example), so we may take the s of Lemma 3.11 to be $|\mathrm{Out}(T)| + 1$ if $|\mathrm{Out}(T)|$ is even and $|\mathrm{Out}(T)| + 2$ otherwise. Thus $\mathrm{Inn}(T)^k \rtimes A_k \leqslant G$.

For ease of notation, let $\mathscr{C}$ denote the set of the $|T|^l$ columns of length l with entries in T, and for M an $l \times m$ matrix with entries in T, let $\mathscr{C}_M$ denote the subset of $\mathscr{C}$ whose elements are the columns of M. Note that $\mathrm{Aut}(T)$ acts naturally on $\mathscr{C}$. Suppose that the columns of M are pairwise distinct. If $\mathscr{C}_M^\alpha = \mathscr{C}_M$ for some $\alpha \in \mathrm{Aut}(T)$, then α determines a permutation on $[m]$; this we denote by $\pi_{\alpha,M}$. Note that for each row $(t_1, \ldots, t_m)$ of M, we have $t_i\alpha = t_{i\pi_{\alpha,M}}$ for all i.

Choose l distinct elements $\omega_1, \ldots, \omega_l$ from $\Omega \setminus \{D\}$, and let $\mathscr{B}$ be the set $\{\omega_i\colon\ 1 \leqslant i \leqslant l\}$. We must show that $\mathscr{B}$ is not a base for G_D. For each i, let $(t_{i,1}, \ldots, t_{i,k})$ be one of the $|T|$ choices of k-tuples of elements in T that correspond to ω_i. Let B be the $l \times k$ matrix whose (i, j)-th entry is $t_{i,j}$. Note that for each i, $(t, \ldots, t)\omega_i = \omega_i$ for any $t \in T$. This allows us either to choose one element from $\mathscr{C}$ to be column j of B for any one $j \in [k]$, or, when an element of $\mathscr{C}$ is not in $\mathscr{C}_B$, to choose any one element from $\mathscr{C}$ to be in $\mathscr{C} \setminus \mathscr{C}_B$ (with appropriate repercussions for the columns of B in either case).

Suppose that B has three identical columns, say j_1, j_2 and j_3. Then $(1, \ldots, 1)(j_1\ j_2\ j_3)$ is an element of G_D that fixes $\mathscr{B}$ pointwise, so $\mathscr{B}$ is not a base for G_D. Similarly, if B has two pairs of identical columns, then $\mathscr{B}$ is not a base for G_D, so we may assume that neither scenario occurs in B. In particular, $k \leqslant |T|^l + 1$.

Suppose that B has exactly one pair of repeated columns. By relabelling if necessary, we may assume that the indices of these columns are $k - 1$ and k. If $\mathrm{Inn}(T)^k \rtimes S_k \leqslant G$, then clearly $\mathscr{B}$ is not a base for G_D, so assume otherwise, in which case $k = |T|^l + 1$, or $l = 1$ and $k = |T|$. Then $\mathscr{C}_B$ is $\mathscr{C}$ in the former case and $\mathscr{C} \setminus \{(t)\}$ for some $t \in T$ in the latter. We may assume by the note above that every entry of column $k - 1$ is the identity, and therefore the same is true for column k. Let B^* be the $l \times (k - 2)$ matrix whose j-th column is the j-th column of B for $1 \leqslant j \leqslant k - 2$. If $k = |T|^l + 1$, let α be any non-trivial element of $\mathrm{Inn}(T)$, and if $l = 1$ and $k = |T|$, let α be any non-trivial element of $\mathrm{Inn}(T)$ that fixes t. Then $\mathscr{C}_{B^*}^\alpha = \mathscr{C}_{B^*}$ in either case. Since the columns of B^* are pairwise distinct by assumption, the permutation π_{α,B^*} on $[k - 2]$ exists as defined above. Moreover, π_{α,B^*} can be made into an even permutation π of $[k]$ by either fixing or interchanging $k - 1$ and k.

Then $(\alpha,\dots,\alpha)\pi \in G_D$. Since $t_{i,j}\alpha = t_{i,j\pi}$ for all i and j, Lemma 3.1 implies that $(\alpha,\dots,\alpha)\pi$ fixes $\mathscr{B}$ pointwise. Thus $\mathscr{B}$ is not a base for G_D.

Hence we may assume that the columns of B are pairwise distinct. Then $k \leqslant |T|^l$. If $k = |T|^l$, then $\mathscr{C}_B = \mathscr{C}$, and if $k = |T|^l - 1$, then $\mathscr{C}_B = \mathscr{C} \setminus \{c\}$ for some $c \in \mathscr{C}$; we may assume that all the entries of c are the identity. Let α be an element of $\mathrm{Inn}(T)$ for which $\alpha^2 \neq 1$. Then $\mathscr{C}_B^{\alpha} = \mathscr{C}_B$ in either case. Again, since the entries of B are pairwise distinct, we have a permutation $\pi := \pi_{\alpha,B}$ of $[k]$. Since $t_{i,j}\alpha = t_{i,j\pi}$ for all i and j, Lemma 3.1 implies that $(\alpha,\dots,\alpha)\pi \in D$ fixes $\mathscr{B}$ pointwise; hence the non-trivial element $(\alpha,\dots,\alpha)^2\pi^2$ of $\mathrm{Inn}(T)^k \rtimes A_k$ does so as well, and thus $\mathscr{B}$ is not a base for G_D. □

Proof of Theorem 1.2. By Propositions 3.8 and 3.10, we have the desired result if $k \leqslant |T|$, so we may assume that $|T|^l < k \leqslant |T|^{l+1}$ for some positive integer l. It follows immediately from Proposition 3.8 that $b(G) \leqslant \lceil \log k/\log|T| \rceil + 2$. Moreover, $b(G) \geqslant l+2$ by Proposition 3.12, so $b(G) \geqslant \lceil \log k/\log|T| \rceil + 1$. If we also assume that $k \leqslant |T|^l + |T| - 1$, then the upper bound of Proposition 3.8 is equal to $\lceil \log k/\log|T| \rceil + 1$ since $k > |T|^l$ implies that $k - |T| + 1 > |T|^{l-1}$, so $a_G = 1$ and the proof is complete. □

Note that Proposition 3.12 provides several infinite classes of groups for which the a_G of Theorem 1.2 is 2; namely, $a_G = 2$ when $k = |T|$ or when G contains $\mathrm{Inn}(T)^k \rtimes S_k$ and k is $|T|^l$ or $|T|^l - 1$ for any positive integer l. Additionally, it can be shown that if m is 5 or 6, then $b(\mathrm{Inn}(A_m)^2 \rtimes S_2) = 3$ while $b(W(2, A_m)) = 4$. (GAP [18] was used to verify this when $m = 6$.) Thus Theorem 1.2 is essentially best possible.

Furthermore, Proposition 3.12 implies that $b(G) \neq 2$ when $k \geqslant |T|$, and if $2 < k < |T|$, then we know that $b(G) \in \{2, 3\}$ by Propositions 3.8 and 3.10. At this stage, it remains unclear whether we can determine when $b(G) = 2$ more precisely than this. The main difficulty here lies in the possibility of the existence of two groups of diagonal type with the same socle and top group but different base sizes; indeed, none of the methods we have seen so far can distinguish the base sizes of two such groups. However, as mentioned in the Introduction, we will see in Section 4 that for a particular fixed k that is at least 5, there are only finitely many groups of diagonal type with a degree k top group which do not have base size 2.

4. Probabilistic results

In this section, let T be a finite non-abelian simple group. The following argument has been made by Liebeck and Shalev [27]. Let G be a transitive permutation group on Ω. Let $Q(G, b)$ denote the proportion of b-tuples in Ω^b that are not (ordered) bases for G. If $x \in G$, the proportion of points in Ω that are fixed by x is $|\mathrm{fix}(x)|/|\Omega|$, so the proportion of b-tuples that are fixed by x is $(|\mathrm{fix}(x)|/|\Omega|)^b$. Moreover, if a b-tuple is not a base for G, then it is fixed by some element in G of prime order. Let X be the set of elements in G of prime order, and let $x_1,\dots,x_l$ be a set of representatives for the G-conjugacy classes of elements in X. Then since $|\mathrm{fix}(x)|/|\Omega| = |G_\omega \cap x^G|/|x^G|$ for any $\omega \in \Omega$ by transitivity, we have

$$Q(G, b) \leqslant \sum_{x\in X}\left(\frac{|\mathrm{fix}(x)|}{|\Omega|}\right)^b = \sum_{x\in X}\left(\frac{|G_\omega \cap x^G|}{|x^G|}\right)^b = \sum_{i=1}^{l}\frac{|G_\omega \cap x_i^G|^b}{|x_i^G|^{b-1}}.$$

In particular, it follows that if

$$\sum_{i=1}^{l}\frac{|G_\omega \cap x_i^G|^2|C_G(x_i)|}{|G|} \to 0$$

as $|G| \to \infty$ for some $\omega \in \Omega$, then almost any pair of elements in Ω forms a base for G. Note that we may choose $x_1,\dots,x_l$ to be elements of G_ω since $|G_\omega \cap x_i^G| = 0$ if no G-conjugate of x_i lies in G_ω.

Let G be a group of diagonal type with socle T^k. Choose a set $R(G)$ of representatives for the G-conjugacy classes of elements in the stabiliser G_D of $D = D(k, T)$ in G which have prime order. Define

$$R_1(G) := \{(\alpha, \dots, \alpha)\pi \in R(G) \colon \pi \text{ is fixed-point-free on } [k]\},$$
$$R_2(G) := \{(\alpha, \dots, \alpha)\pi \in R(G) \colon \pi = 1\},$$
$$R_3(G) := \{(\alpha, \dots, \alpha)\pi \in R(G) \colon \pi \neq 1 \text{ and } i\pi = i \text{ for some } i \in [k]\},$$

and for $1 \leqslant i \leqslant 3$, define

$$r_i(G) := \sum_{x \in R_i(G)} \frac{|G_D \cap x^G|^2 |C_G(x)|}{|G|}.$$

Thus $Q(G, 2) \leqslant r_1(G) + r_2(G) + r_3(G)$. We write $\vec{\alpha}$ for the tuple $(\alpha, \dots, \alpha)$ and C for some absolute constant which need not and will not be determined (though it could be). Such methodology will also apply to another absolute constant $c > 1$, though it will be obvious what c needs to be.

We need to prove the following three lemmas; for the second, note that $p(T)$ denotes the minimal index of a proper subgroup of T.

Lemma 4.1. *Let P be a primitive subgroup of S_k that does not contain A_k, and let $G := A(k, T) \rtimes P$. Then*

$$r_1(G) \leqslant \frac{C}{c^k |T|^{\frac{1}{6}}}$$

for some absolute constants C and $c > 1$.

Lemma 4.2. *Let P be a primitive subgroup of S_k where $k \geqslant 5$, and let $G := A(k, T) \rtimes P$. Then*

$$r_2(G) \leqslant \frac{C}{p(T)^{k - \frac{19}{4}}}$$

for some absolute constant C.

Lemma 4.3. *Let P be a primitive subgroup of S_k that does not contain A_k, and let $G := A(k, T) \rtimes P$. Then*

$$r_3(G) \leqslant \frac{C}{|T|^{\frac{1}{3}}} \left(\frac{1}{c^k} + \frac{1}{\sqrt{k}} \right)$$

for some absolute constants C and $c > 1$.

In fact, Lemma 4.3 is primarily a consequence of the following more general result, which we record here and prove separately from Lemma 4.3 as it has applications to the probabilistic side of the base size problem for other types of primitive permutation groups, such as the groups of twisted wreath type (in [16]).

Lemma 4.4. *Let P be a primitive subgroup of S_k that does not contain A_k, and let T be a finite non-abelian simple group. Then for some absolute constants C and $c > 1$, we have*

$$\sum_{\pi \in R(P)} \frac{|\pi^P|}{|T|^{k - r_\pi - \frac{5}{3}}} \leqslant C \left(\frac{1}{c^k} + \frac{1}{\sqrt{k}} \right)$$

where $R(P)$ denotes a set of representatives for the conjugacy classes of elements of prime order in P, and r_π denotes the number of cycles in the full cycle decomposition of π in S_k, including fixed points.

If we assume that Lemmas 4.1, 4.2 and 4.3 are true, then Theorem 1.4 can be proved easily, as we now see.

Proof of Theorem 1.4. Note that $k \geqslant 5$ since for $k \leqslant 4$ the only primitive permutation groups of degree k are A_k and S_k. Then by Lemmas 4.1, 4.2 and 4.3,

$$Q\left(\left(A(k,T) \rtimes P_G\right), 2\right) \leqslant C\left(\frac{1}{c^k |T|^{\frac{1}{6}}} + \frac{1}{p(T)^{k-\frac{19}{4}}} + \frac{1}{|T|^{\frac{1}{3}} c^k} + \frac{1}{|T|^{\frac{1}{3}}\sqrt{k}}\right)$$

for some absolute constants C and $c > 1$. Because T can be embedded in the alternating group on $p(T)$ points, it follows that $p(T) \to \infty$ as $|T| \to \infty$. Thus $Q((A(k,T) \rtimes P_G), 2)$ converges to 0 as $|T| \to \infty$ or $k \to \infty$. Since $G \leqslant A(k,T) \rtimes P_G \leqslant W(k,T)$, any base for $A(k,T) \rtimes P_G$ is also a base for G. Thus $Q(G,2) \leqslant Q((A(k,T) \rtimes P_G), 2)$. Also, clearly $|G| \leqslant |\operatorname{Aut}(T)||T|^{k-1}|P_G| \leqslant |T|!|T|^{k-1}k!$, so $|T| \to \infty$ or $k \to \infty$ when $|G| \to \infty$. Thus $Q(G,2)$ will indeed converge to 0 as $|G|$ tends to infinity. □

In order to prove the three lemmas, we first need to calculate the sizes of conjugacy classes and centralisers of various elements of $D(k,T)$.

Lemma 4.5. *Let P be a subgroup of S_k, let $G := A(k,T) \rtimes P$, and let $(\alpha,\dots,\alpha)\pi \in G$ where π has a fixed point on $[k]$. Then*

$$(\alpha,\dots,\alpha)\pi^G \cap G_D = \left\{(\alpha',\dots,\alpha')\pi' \colon \alpha' \in \alpha^{\operatorname{Aut}(T)},\ \pi' \in \pi^P\right\}.$$

In particular, $|(\alpha,\dots,\alpha)\pi^G \cap G_D| = |\alpha^{\operatorname{Aut}(T)}||\pi^P|$.

Proof. Suppose that $\alpha' := \beta^{-1}\alpha\beta$ for any $\beta \in \operatorname{Aut}(T)$ and $\pi' := \sigma^{-1}\pi\sigma$ for any $\sigma \in P$. Then $(\beta,\dots,\beta)\sigma$ conjugates $(\alpha,\dots,\alpha)\pi$ to $(\alpha',\dots,\alpha')\pi'$ in G. On the other hand, if $(\alpha_1,\dots,\alpha_k)\sigma$ conjugates $(\alpha,\dots,\alpha)\pi$ to $(\alpha',\dots,\alpha')\pi'$ in G, then $\sigma^{-1}\pi\sigma = \pi'$ and $\alpha_i^{-1}\alpha\alpha_{i\pi} = \alpha'$ for all i. Since π has a fixed point, the result follows. □

The proof of Lemma 4.5 should give the reader some indication of why it is not only convenient to work with the group $A(k,T) \rtimes P$ but also necessary, as we lose control of the sizes of $R_2(G)$ and $R_3(G)$ for an arbitrary group of diagonal type G.

Lemma 4.6. *Let P be a subgroup of S_k, let $G := A(k,T) \rtimes P$, and let $(\alpha,\dots,\alpha)\pi$ be an element of G of prime order p. Then $|C_G((\alpha,\dots,\alpha)\pi)|$ is either*

$$\left|C_P(\pi)\right|\left|C_{\operatorname{Out}(T)}(\overline{\alpha})\right||T|^{\frac{k}{p}} \tag{1}$$

if π is fixed-point-free on $[k]$, or

$$\left|C_P(\pi)\right|\left|C_{\operatorname{Aut}(T)}(\alpha)\right|\left|C_{\operatorname{Inn}(T)}(\alpha)\right|^{\operatorname{fix}_{[k]}(\pi)-1}|T|^{\frac{1}{p}(k-\operatorname{fix}_{[k]}(\pi))} \tag{2}$$

if π has a fixed point on $[k]$.

Note that the division into two cases in Lemma 4.6 is necessary because there exist $\alpha, \beta \in \mathrm{Aut}(T)$ for which $\overline{\beta} \in C_{\mathrm{Out}(T)}(\overline{\alpha})$ but $\beta \notin C_{\mathrm{Aut}(T)}(\alpha)$. In fact, if π is fixed-point-free, then the two expressions for $|C_G((\alpha,\dots,\alpha)\pi)|$ agree precisely when $C_{\mathrm{Aut}(T)}(\alpha)/C_{\mathrm{Inn}(T)}(\alpha)$ is isomorphic to $C_{\mathrm{Out}(T)}(\overline{\alpha})$.

Proof of Lemma 4.6. Let $f_\pi := \mathrm{fix}_{[k]}(\pi)$, let c_π be the number of non-trivial cycles of π so that $c_\pi = (k - f_\pi)/p$, and let $r_\pi := c_\pi + f_\pi$. The element $(\alpha_1,\dots,\alpha_k)\sigma \in \mathrm{Aut}(T)^k \wr S_k$ is in G and centralises $(\alpha,\dots,\alpha)\pi$ if and only if all three of the following conditions occur: σ centralises π in P, $\alpha^{-1}\alpha_i\alpha = \alpha_{i\pi}$ for all i, and α_i and α_j are in the same coset of $\mathrm{Inn}(T)$ for all i and j. There are precisely $|C_P(\pi)|$ elements of P satisfying the first condition, and this condition is independent of the other two, so we assume that σ is fixed and count how many occurrences of the latter conditions are possible.

Note that if α is trivial, then $\alpha^{-1}\alpha_i\alpha = \alpha_{i\pi}$ for all i if and only if $\alpha_i = \alpha_j$ whenever i and j are in the same cycle of the full cycle decomposition of π. Thus there are $|\mathrm{Out}(T)||T|^{r_\pi}$ tuples $(\alpha_1,\dots,\alpha_k)$ satisfying both conditions. The desired equality then follows in either case for π, so we may assume that α is non-trivial, in which case α has prime order p.

Suppose, first of all, that i_0 is moved by π. Then i_0 is contained in a p-cycle in the full cycle decomposition of π as π must have the same prime order as α. Let us assume that this p-cycle is $(12\cdots p)$ and that i_0 is 1. If $\alpha^{-1}\alpha_i\alpha = \alpha_{i\pi}$ and $\overline{\alpha}_1 = \overline{\alpha}_i$ for all i, then, in particular, $[\alpha_1,\alpha] \in \mathrm{Inn}(T)$ and the elements $\alpha_2,\dots,\alpha_p$ are determined by α_1 and α. Conversely, if we are given $\alpha_1 \in \mathrm{Aut}(T)$ such that $[\alpha_1,\alpha] \in \mathrm{Inn}(T)$, define $\alpha_{i+1} := \alpha^{-i}\alpha_1\alpha^i$ for each $i \in [p-1]$. Then $\alpha^{-1}\alpha_i\alpha = \alpha_{i\pi}$ for all $i \in [p]$ since α has order p. Moreover, $[\alpha_1,\alpha^i] \in \mathrm{Inn}(T)$ for all $i \in [p]$ since $[\alpha_1,\alpha^i] = [\alpha_1,\alpha^{i-1}]\alpha^{1-i}[\alpha_1,\alpha]\alpha^{i-1}$ for all such i; thus $\overline{\alpha}_1 = \overline{\alpha}_i$ for all $i \in [p]$. Since this argument does not depend on the choice of i_0 or on the letters of the p-cycle, and since for $\beta \in \mathrm{Aut}(T)$, $[\beta,\alpha] \in \mathrm{Inn}(T)$ if and only if $\overline{\beta} \in C_{\mathrm{Out}(T)}(\overline{\alpha})$, it follows that there are at most $|C_{\mathrm{Out}(T)}(\overline{\alpha})|$ choices for the coset of $\mathrm{Inn}(T)$ from which the α_i may be chosen, and for each such coset there are at most $|T|$ choices corresponding to each non-trivial cycle of π. If π is fixed-point-free, then all these choices are possible. Since $c_\pi = k/p$, Eq. (1) follows.

Suppose then that π has a fixed point i_0. Certainly $\alpha^{-1}\alpha_i\alpha = \alpha_{i\pi}$ and $\overline{\alpha}_{i_0} = \overline{\alpha}_i$ for all fixed points i if and only if $\alpha_{i_0} \in C_{\mathrm{Aut}(T)}(\alpha)$ and $\alpha_{i_0}^{-1}\alpha_i \in C_{\mathrm{Inn}(T)}(\alpha)$ for all fixed points $i \neq i_0$. Hence there are at most $|C_{\mathrm{Aut}(T)}(\alpha)||C_{\mathrm{Inn}(T)}(\alpha)|^{f_\pi - 1}$ choices for $\{\alpha_i\colon\ i\pi = i\}$, and if π is trivial, then all these choices are possible, in which case Eq. (2) is true. Suppose that $\pi \neq 1$, and let $\{\alpha_i\colon\ i\pi = i\}$ be one of the choices described above. Then since $\overline{\alpha}_{i_0} \in C_{\mathrm{Out}(T)}(\overline{\alpha})$ for any i_0 fixed by π, any element of the coset $\overline{\alpha}_{i_0}$ may be chosen to determine the α_j corresponding to any non-trivial cycle of π as above. Thus each of the choices for $\{\alpha_i\colon\ i\pi = i\}$ not only occurs but does so $|T|^{c_\pi}$ times. Eq. (2) then follows. □

There are several occasions when we will need to bound the number of conjugacy classes of elements of prime order in a group, so we set up some notation for this. Let X be a finite group. If $\mathcal{C}$ is a union of conjugacy classes of X, we write $f_{\mathcal{C}}(X)$ for the number of conjugacy classes contained in $\mathcal{C}$. Also, we write $f(X)$ for $f_X(X)$, and when $\mathcal{C}$ consists of the elements of prime order in X, we write $f_p(X)$ for $f_{\mathcal{C}}(X)$. Let Y be a subgroup of X. Gallagher noted in [17] that $f(X) \leqslant [X:Y]f(Y)$ and $f(Y) \leqslant [X:Y]f(X)$ and gave elementary proofs of these facts. The latter can easily be generalised to $f_{\mathcal{C}}(Y)$ for any union of conjugacy classes $\mathcal{C}$ in Y, which we now do.

Lemma 4.7. *Let X be a finite group with subgroup Y. Let $\mathcal{C} \subseteq \mathcal{C}'$ be unions of conjugacy classes of Y and X respectively. Then $f_{\mathcal{C}}(Y) \leqslant [X:Y]f_{\mathcal{C}'}(X)$. In particular, $f_p(Y) \leqslant [X:Y]f_p(X)$.*

Proof. We adapt Gallagher's proof in [17] as follows. First we obtain a formula for $f_{\mathcal{C}}(Y)$:

$$\frac{1}{|Y|}\sum_{y\in\mathcal{C}}\left|C_Y(y)\right| = \sum_{y\in\mathcal{C}}\frac{1}{|y^Y|} = f_{\mathcal{C}}(Y).$$

Of course, this formula can be used to determine $f_{\mathcal{C}'}(X)$ as well. Since $\mathcal{C} \subseteq \mathcal{C}'$ and $C_Y(y) \leqslant C_X(y)$ for all $y \in \mathcal{C}$, the result follows. □

We will also need the following technical consequences of the CFSG. The first is routine to verify since $|\mathrm{Out}(T)|$ and $|T|$ are known for every simple group T (see [22, Section 5.1], for example, for lists of these quantities), so a proof is omitted. For the second, note that $l(T)$ denotes the untwisted Lie rank of a simple group T of Lie type; when T is a twisted group, this is simply the Lie rank of the corresponding untwisted group. Recall that $p(T)$ denotes the minimal index of a proper subgroup of T.

Lemma 4.8. *Let T be a non-abelian simple group. Then $|\mathrm{Out}(T)|^3 < |T|$.*

Lemma 4.9. *Let T be a simple group of Lie type over $\mathbb{F}_q$ where $T \neq L_m(2)$ for any m. Then*

$$\big|\mathrm{Out}(T)\big|^2 (6q)^{l(T)} \leqslant C p(T)^{11/4}$$

for some absolute constant C.

Proof. Note that the presence of the absolute constant C allows us to ignore finitely many T. Write $q = p^f$ where p is a prime and f is a positive integer. Values for $|\mathrm{Out}(T)|$ may be found in [22, Section 5.1], for example.

Suppose that T is an exceptional group. Since $l(T)$ is constant and $|\mathrm{Out}(T)|$ is bounded above by a constant multiple of q, it suffices to show that $l(T)+2$ is at most $(11/4)b(T)$ for some constant $b(T)$ for which $p(T) \geqslant q^{b(T)}$. If T is ${}^2B_2(q)$ or ${}^2G_2(q)$, then $l(T) = 2$ and we may take $b(T) = 2$ by [41]. Otherwise, we have $l(T) \leqslant 8$ and we may take $b(T) = 4$ by [39–41]. In both cases, the desired inequality is satisfied.

Let T be one of the following groups: $PSp_{2m}(q)$ where $m \geqslant 2$, $\Omega_{2m+1}(q)$ where $m \geqslant 3$, $P\Omega^+_{2m}(q)$ where $m \geqslant 4$, or $P\Omega^-_{2m}(q)$ where $m \geqslant 4$. Then $l(T) = m$, $p(T) \geqslant q^{2m-2}$ by [33,42], and $|\mathrm{Out}(T)|$ is at most a constant multiple of q. Since $q^2(6q)^m$ is at most $36q^{2(2m-2)}$, it follows that T satisfies the desired inequality.

Let T be $U_m(q)$ where $m \geqslant 3$. Then $l(T) = m-1$, $p(T) \geqslant q^{2m-4}$ by [33], and $|\mathrm{Out}(T)|$ is at most a constant multiple of $(q+1)f$. Since $(q+1)^2 f^2 \leqslant q^{7/2}$ and $q^{7/2}(6q)^{m-1} \leqslant 36q^{(11/4)(2m-4)}$, we have verified the desired inequality.

Finally, suppose that T is $L_m(q)$ where $m \geqslant 2$. We may assume that $T \neq L_2(9)$. Then $l(T) = m-1$, $p(T) \geqslant q^{m-1}$ by [33], and $|\mathrm{Out}(T)|$ is at most a constant multiple of $(q-1)f$. Note that $(q-1)^2 f^2 \leqslant q^{7/2}$. If $m \geqslant 3$, then since $q \geqslant 3$ (by assumption), it follows that $q^{7/2}(6q)^{m-1}$ is at most $36q^{(11/4)(m-1)}$, so T satisfies the desired inequality. If $m = 2$, then $|\mathrm{Out}(T)|$ is at most a constant multiple of f, and since $f^2 q \leqslant q^{11/4}$, the proof is complete. □

We are now in a position to prove the four lemmas.

Proof of Lemma 4.1. If $\vec{\alpha}\pi \in R_1(G)$ where π has prime order p, then k/p is an integer and is therefore bounded above by $\lfloor k/2 \rfloor$. Since $P = P_G$, Eq. (1) of Lemma 4.6 then implies that

$$\max_{\vec{\alpha}\pi \in R_1(G)} \big|C_G(\vec{\alpha}\pi)\big| \leqslant \big|\mathrm{Out}(T)\big| |P| |T|^{\lfloor \frac{k}{2} \rfloor}.$$

Note that $|G_D| = |\mathrm{Out}(T)||T||P|$ and $|G| = |G_D||T|^{k-1}$. Then

$$r_1(G) \leqslant \frac{|G_D|^2}{|G|} \max_{\vec{\alpha}\pi \in R_1(G)} \big|C_G(\vec{\alpha}\pi)\big| \leqslant \frac{|\mathrm{Out}(T)|^2 |P|^2}{|T|^{\lceil \frac{k}{2} \rceil - 2}}.$$

By a classification-free result of Praeger and Saxl [34], since P is primitive and does not contain A_k, we know that the order of P is bounded above by 4^k. Moreover, we have $|\mathrm{Out}(T)|^2 \leqslant |T|^{2/3}$ by

Lemma 4.8. Recall that $k \geqslant 5$, for if $k \leqslant 4$ then the primitivity of P implies that P is A_k or S_k; thus $\lceil k/2 \rceil - 17/6$ is positive. Suppose that T is not A_5 or $L_2(7)$. Then $|T| \geqslant 360$, so

$$\frac{|\operatorname{Out}(T)|^2|P|^2}{|T|^{\lceil \frac{k}{2} \rceil - 2}} \leqslant \frac{16^k}{|T|^{\frac{1}{6}} 360^{\lceil \frac{k}{2} \rceil - \frac{17}{6}}} \leqslant \frac{360^{\frac{17}{6}}}{|T|^{\frac{1}{6}}} \left(\frac{16}{\sqrt{360}} \right)^k,$$

which is our desired bound. Furthermore, by [3, Corollary 1.2], which is a classification-free result of Babai, again since P is primitive and does not contain A_k, we know that $|P| \leqslant \exp(4\sqrt{k}(\log k)^2)$ for sufficiently large k. Note that k is eventually larger than $8\sqrt{k}(\log k)^2$. Suppose that T is A_5 or $L_2(7)$. Then $|\operatorname{Out}(T)| = 2$, so

$$\frac{|\operatorname{Out}(T)|^2|P|^2}{|T|^{\lceil \frac{k}{2} \rceil - 2}} \leqslant \frac{4e^{8\sqrt{k}(\log k)^2}}{|T|^{\frac{1}{6}} 60^{\lceil \frac{k}{2} \rceil - \frac{13}{6}}} \leqslant \frac{4 \cdot 60^{\frac{13}{6}}}{|T|^{\frac{1}{6}}} \left(\frac{e}{\sqrt{60}} \right)^k$$

for sufficiently large k. Since only finitely many G have been omitted from our argument, the proof is complete. □

Proof of Lemma 4.2. Note that if $R(T)$ is a set of representatives for the conjugacy classes of elements of prime order in $\operatorname{Aut}(T)$, then we may assume that $R_2(G) = \{\vec{\alpha} \colon \alpha \in R(T)\}$ by Lemma 4.5. By applying Lemma 4.5 and Eq. (2) of Lemma 4.6 with $\pi = 1$, we get the following.

$$\begin{aligned} |G| r_2(G) &= \sum_{\alpha \in R(T)} \left(\left|\operatorname{Aut}(T)\right|^2 \left|C_{\operatorname{Aut}(T)}(\alpha)\right|^{-2} \right) \left(|P| \left|C_{\operatorname{Aut}(T)}(\alpha)\right| \left|C_{\operatorname{Inn}(T)}(\alpha)\right|^{k-1} \right) \\ &\leqslant \left|\operatorname{Aut}(T)\right|^2 |P| \sum_{\alpha \in R(T)} \left|C_{\operatorname{Inn}(T)}(\alpha)\right|^{k-2} \\ &\leqslant \left|\operatorname{Out}(T)\right|^2 |T|^2 |P| f_p\big(\operatorname{Aut}(T)\big) \Big(\max_{\alpha \in R(T)} \left|C_{\operatorname{Inn}(T)}(\alpha)\right| \Big)^{k-2}. \end{aligned}$$

(Recall that $f_p(X)$ denotes the number of conjugacy classes of elements of prime order in a group X.) Since $k-2$ is positive and $[T : C_{\operatorname{Inn}(T)}(\alpha)] \geqslant p(T)$ for every $1 \neq \alpha \in \operatorname{Aut}(T)$, if we divide by $|G|$, then we see that $r_2(G)$ is at most $|\operatorname{Out}(T)| f_p(\operatorname{Aut}(T)) p(T)^{2-k}$. It therefore suffices to show that

$$\left|\operatorname{Out}(T)\right| f_p\big(\operatorname{Aut}(T)\big) \leqslant C p(T)^{11/4}$$

for some absolute constant C. Note that we may ignore finitely many simple groups T should we wish to due to the presence of the constant. In particular, we may ignore the sporadic groups.

If T is the alternating group A_m, then $p(T) = m$ and $\operatorname{Out}(T)$ is constant. In fact, we have that $\operatorname{Aut}(A_m) = S_m$ if $m \neq 6$, and since

$$f_p(S_m) = \sum_{\substack{2 \leqslant p \leqslant m \\ p \text{ prime}}} \left\lfloor \frac{m}{p} \right\rfloor \leqslant \sum_{\substack{2 \leqslant p \leqslant m \\ p \text{ prime}}} \frac{m}{2} \leqslant \frac{m^2}{2},$$

it follows that $f_p(\operatorname{Aut}(T)) p(T)^{-11/4}$ is bounded above by $m^{-3/4}$.

Let us assume, then, that T is a simple group of Lie type over $\mathbb{F}_q$. As noted before Lemma 4.7, for any group X and subgroup Y, it is elementary to show that $f(X) \leqslant [X : Y] f(Y)$. (Note that Lemma 4.7 provides an upper bound on $f(Y)$ rather than on $f(X)$; see [17] for a proof of the upper bound on $f(X)$.) Hence $f_p(\operatorname{Aut}(T)) \leqslant f(T) |\operatorname{Out}(T)|$. Moreover, from [25, Theorem 1] we know that $f(T) \leqslant (6q)^{l(T)}$ where $l(T)$ is the untwisted Lie rank of T. If T is not $L_m(2)$ for any m, then $|\operatorname{Out}(T)|^2 (6q)^{l(T)} \leqslant C p(T)^{11/4}$ for some absolute constant C by Lemma 4.9, and we have verified the desired inequality.

If T is $L_m(2)$, then $|\mathrm{Out}(T)| = 2$, $p(T) \geqslant 2^{m-1}$ by [33], and $f(T) \leqslant 2^m$ by [32, Lemma 5.9], so the proof is complete. □

Proof of Lemma 4.3 assuming Lemma 4.4. Note first of all that $R_3(G)$ may be empty. If so, then the result is true, so we may assume otherwise. For $\pi \in P$ of prime order p, as in the proof of Lemma 4.6, let $f_\pi := \mathrm{fix}_{[k]}(\pi)$, let c_π be the number of non-trivial cycles of π so that $c_\pi = (k - f_\pi)/p$, and let $r_\pi := c_\pi + f_\pi$. Since $|C_{\mathrm{Inn}(T)}(\alpha)| \leqslant |T|$, Lemma 4.5 and Eq. (2) of Lemma 4.6 imply that

$$\begin{aligned} |G|r_3(G) &\leqslant \sum_{\vec{\alpha}\pi \in R_3(G)} \left|\alpha^{\mathrm{Aut}(T)}\right|^2 \left|\pi^P\right|^2 \left|C_P(\pi)\right| \left|C_{\mathrm{Aut}(T)}(\alpha)\right| |T|^{r_\pi - 1} \\ &= \left|\mathrm{Out}(T)\right| |P| \sum_{\vec{\alpha}\pi \in R_3(G)} \left|\alpha^{\mathrm{Aut}(T)}\right| \left|\pi^P\right| |T|^{r_\pi}. \end{aligned}$$

Let $R(T)$ denote a set of representatives for the conjugacy classes of elements of prime order in $\mathrm{Aut}(T)$ together with the identity, and let $R(P)$ denote a set of representatives for the conjugacy classes of elements of prime order in P that fix a point of $[k]$. Then by Lemma 4.5 we may assume without loss of generality that $R_3(G) \subseteq \{\vec{\alpha}\pi\colon\ \alpha \in R(T),\ \pi \in R(P)\}$, so

$$\sum_{\vec{\alpha}\pi \in R_3(G)} \left|\alpha^{\mathrm{Aut}(T)}\right| \left|\pi^P\right| |T|^{r_\pi} \leqslant \sum_{\alpha \in R(T)} \left|\alpha^{\mathrm{Aut}(T)}\right| \sum_{\pi \in R(P)} \left|\pi^P\right| |T|^{r_\pi} \leqslant |T|^{\frac{4}{3}} \sum_{\pi \in R(P)} \left|\pi^P\right| |T|^{r_\pi}$$

since $|\mathrm{Out}(T)| \leqslant |T|^{1/3}$ by Lemma 4.8. Then the proof is complete by Lemma 4.4. □

Proof of Lemma 4.4. For $\pi \in P$ of prime order p, as in the proof of Lemma 4.3, let $f_\pi := \mathrm{fix}_{[k]}(\pi)$, let c_π be the number of non-trivial cycles of π so that $c_\pi = (k - f_\pi)/p$, and let $r_\pi := c_\pi + f_\pi$. As in the statement of the lemma, let $R(P)$ denote a set of representatives for the conjugacy classes of elements of prime order in P. We want to prove that

$$\sum_{\pi \in R(P)} \frac{|\pi^P|}{|T|^{k - r_\pi - \frac{5}{3}}} \leqslant C\left(\frac{1}{c^k} + \frac{1}{\sqrt{k}}\right) \tag{3}$$

for some absolute constants C and $c > 1$. Note that $r_\pi = k - 1$ for some $\pi \in R(P)$ if and only if P contains a transposition, which is equivalent to P being S_k since P is primitive. Thus the exponent of $|T|$ in (3) is always positive.

Let $\pi \in R(P)$ have order p. We may write $pc_\pi = \mu(P) + i$ for some non-negative integer i where $\mu(P)$ denotes the minimal degree of P, which is the minimal number of points moved by an element of P. Then $c_\pi = \mu(P)/p + i/p$ and $f_\pi = k - \mu(P) - i$. Since $i/p - i \leqslant 0$ and $p \geqslant 2$, it follows that

$$\max_{\pi \in R(P)} r_\pi \leqslant \left\lfloor \frac{\mu(P)}{2} \right\rfloor + k - \mu(P) = k - \left\lceil \frac{\mu(P)}{2} \right\rceil.$$

Hence we conclude that (3) is true if the following inequality holds:

$$\frac{|P|}{|T|^{\lceil \frac{\mu(P)}{2} \rceil - \frac{5}{3}}} \leqslant C\left(\frac{1}{c^k} + \frac{1}{\sqrt{k}}\right). \tag{4}$$

It will usually be sufficient to prove this inequality. The proof now divides into two cases according to whether $\mu(P) \geqslant k/3$ or not. In the first, we bound the left-hand side of (3) or (4) by C/c^k, and in the second, we bound the left-hand side of (3) or (4) by $C/\sqrt{k}$.

Case 1: $\mu(P) \geqslant k/3$.

Suppose first of all that $|T| \geqslant |L_3(3)| = 5616$ and $k > 6$. Since $|P| \leqslant 4^k$ by [34] and $\lceil k/6 \rceil - 5/3$ is positive,

$$\frac{|P|}{|T|^{\lceil \frac{\mu(P)}{2} \rceil - \frac{5}{3}}} \leqslant \frac{4^k}{5616^{\lceil \frac{k}{6} \rceil - \frac{5}{3}}} \leqslant 5616^{\frac{5}{3}} \left(\frac{4}{\sqrt[6]{5616}} \right)^k,$$

which is the upper bound we desire. Suppose instead that $|T| < 5616$. For sufficiently large k, we know that $|P|$ is at most $\exp(4\sqrt{k}(\log k)^2)$ by [3, Corollary 1.2]. Since k is eventually larger than $24\sqrt{k}(\log k)^2$, it follows that

$$\frac{|P|}{|T|^{\lceil \frac{\mu(P)}{2} \rceil - \frac{5}{3}}} \leqslant 60^{\frac{5}{3}} \left(\frac{e^{24\sqrt{k}(\log k)^2}}{60^k} \right)^{\frac{1}{6}} \leqslant 60^{\frac{5}{3}} \left(\frac{e}{60} \right)^{\frac{k}{6}}$$

for sufficiently large k, which is again the upper bound we desire. Lastly, suppose that $k = 5$ or 6 (which we may do since P must contain A_k when $k \leqslant 4$). Note that the left-hand side of (3) is bounded above by $|P||T|^{5/3-k+r_{\pi^*}}$ where $\pi^* \in R(P)$ achieves the maximum. Since $k - r_{\pi^*} \geqslant 2$, we may replace $|T|$ by 60, and since $|P|$ and r_{π^*} are constant, this establishes Eq. (3). Only finitely many G have been excluded from our argument, so this case is complete.

Case 2: $\mu(P) < k/3$.

Let $\Omega_{m,l}$ denote the set of subsets of $[m]$ of size l. Then by Liebeck and Saxl [26, Theorem 2], our assumption on $\mu(P)$ forces P to be a subgroup of $S_m \wr_r S_r$ that contains A_m^r and acts by the product action on $\Omega_{m,l}^r$ for some $m \geqslant 5$, $r \geqslant 1$ and $1 \leqslant l < m/2$. Note that this action is primitive and faithful, that (r, l) is not $(1, 1)$ by assumption, and that $k = \binom{m}{l}^r$. Let

$$g(m, r, l) := \binom{m-2}{l-1} \binom{m}{l}^{r-1}.$$

Observe that $((12), 1, \ldots, 1) \in S_m^r$ moves $2g(m, r, l)$ points of $\Omega_{m,l}^r$ while no element of $S_m \wr_r S_r$ moves fewer; hence $g(m, r, l) \leqslant \mu(P)/2$. It is certainly true that $m^{mr} \geqslant \sqrt{k}$ and $|P| \leqslant m^{mr} r^r$, so since $g(m, r, l) \neq 1$ and $|T| \geqslant 60$, it follows that (4) is true if we can show that

$$2mr \log m + r \log r \leqslant g(m, r, l) \log 60 + C \tag{5}$$

for some absolute constant C. If $r \geqslant 3$, then Eq. (5) holds since $g(m, r, l) \geqslant m^{r-1}$; if $r = 2$ and $l \geqslant 2$, then Eq. (5) holds since $g(m, 2, l) \geqslant m^2$; and if $r = 1$ and $l \geqslant 3$, then Eq. (5) holds since $g(m, 1, l) \geqslant (m-3)^2/2$ (and since $l < m/2$ forces $m > 6$). Thus the cases when (r, l) is $(1, 2)$ or $(2, 1)$ remain; note that for either one, the left-hand side of Eq. (4) tends to infinity if T is fixed and m tends to infinity. We therefore establish Eq. (3) instead.

Suppose that (r, l) is $(1, 2)$. Recall that P is A_m or S_m acting (faithfully) on the set $\Omega_{m,2}$ of 2-subsets of $[m]$ where $m \geqslant 5$. In the proof of Lemma 4.2, we saw that $f_p(S_m) \leqslant m^2/2$, and so $f_p(P) \leqslant m^2$. But $m \geqslant \sqrt{k}$, so Eq. (3) will be true if we can show that $|\pi^P| 60^{r_\pi - k}$ is bounded above by m^{-3} for each $\pi \in R(P)$. To this end, let π be an element of P of prime order p. Then the full cycle decomposition of π in S_m consists of t cycles of length p for some t such that $1 \leqslant t \leqslant \lfloor m/p \rfloor$. Certainly $|\pi^P| \leqslant m^{pt}$. Moreover, we have $k - r_\pi = (1 - 1/p)(k - f_\pi) \geqslant (k - f_\pi)/2$ and $\log 60 > 4$, so it suffices to show that

$$(pt + 3) \log m \leqslant 2(k - f_\pi). \tag{6}$$

Let i and j be distinct points of $[m]$. Clearly π fixes $\{i, j\}$ if and only if either both i and j are members of $\mathrm{fix}_{[m]}(\pi)$, or the full cycle decomposition of π in S_m contains the transposition (ij). Hence

$$f_\pi = \left|\mathrm{fix}_{\Omega_{m,2}}(\pi)\right| = \begin{cases} \binom{m-pt}{2} & \text{if } p \geqslant 3, \\ \binom{m-2t}{2} + t & \text{if } p = 2. \end{cases}$$

By evaluating $2(k - f_\pi)$ and rearranging Eq. (6), it follows that Eq. (3) is true if

$$(pt+3)\log m + p^2t^2 + pt + \left\{ \begin{array}{l} 0 \quad \text{if } p \geqslant 3 \\ 2t \quad \text{if } p = 2 \end{array} \right\} \leqslant 2mpt \tag{7}$$

for all primes p and integers t such that $1 \leqslant t \leqslant \lfloor m/p \rfloor$. Since $pt + 1 \leqslant m + 1 \leqslant 4m/3$, it follows that $p^2t^2 + pt \leqslant 4mpt/3$. In fact, we also have $4t^2 + 4t \leqslant 8mt/3$ since $2t + 2 \leqslant m + 2 \leqslant 4m/3$ when $m \geqslant 6$, and $2t \leqslant 4$ when $m = 5$. Moreover, the fact that $3\log m \leqslant m$ implies that $(pt + 3)\log m \leqslant 2mpt/3$ when $pt + 3 \leqslant 2pt$. Thus Eq. (7) is satisfied if $p \neq 2$ or $t \neq 1$, and if $p = 2$ and $t = 1$, then it is easy to check that Eq. (7) still holds.

The remaining case to consider is when (r, l) is $(2, 1)$. Recall that here P is a subgroup of $S_m^2 \rtimes C_2$ that contains A_m^2 and acts via the product action on $[m]^2$ for $m \geqslant 5$. Let $Q := S_m^2 \rtimes C_2$ and let τ denote the generator for C_2. First we determine the conjugacy classes of elements of prime order in Q.

Let $\mathcal{C}$ be the union of those elements of prime order in Q whose projection onto C_2 is trivial, and let $\mathcal{C}_\tau$ be the union of those elements of prime order in Q whose projection onto C_2 is τ. Then the elements in $\mathcal{C}$ with order p have the form (s_1, s_2) where s_1 and s_2 are elements of S_m such that $s_i^p = 1$ for both i and s_1 or s_2 is non-trivial, and the elements of $\mathcal{C}_\tau$ have the form $(s, s^{-1})\tau$ for any $s \in S_m$. Note that both $\mathcal{C}$ and $\mathcal{C}_\tau$ are unions of conjugacy classes of Q since $S_m^2 \trianglelefteq Q$. In fact, since $(s, u)^{-1}(s, s^{-1})\tau(s, u) = (u, u^{-1})\tau$ for any $s, u \in S_m$, it follows that $f_{\mathcal{C}_\tau}(Q) = 1$.

Let $(s_1, s_2) \in \mathcal{C}$. Since we may conjugate (s_1, s_2) by (u_1, u_2) or $(u_1, u_2)\tau$ for any $u_1, u_2 \in S_m$, it follows that $(s_1, s_2)^Q = (s_1^{S_m} \times s_2^{S_m}) \cup (s_2^{S_m} \times s_1^{S_m})$. Fix a prime $p \leqslant m$. Then in Q there are $m_p := \lfloor m/p \rfloor$ conjugacy classes $(s_1, s_1)^Q$ where s_1 has order p, and since $(s_1, s_2)^Q = (s_2, s_1)^Q$, there are $\binom{m_p+1}{2}$ conjugacy classes $(s_1, s_2)^Q$ where (s_1, s_2) has order p but s_1 and s_2 have a different number of p-cycles on $[m]$ (allowing for the identity, which has no p-cycles). This accounts for all the elements in $\mathcal{C}$ with order p. Then since $m_p \leqslant m/2$ for any prime p, we obtain

$$f_{\mathcal{C}}(Q) = \sum_{\substack{2 \leqslant p \leqslant m \\ p \text{ prime}}} m_p + \binom{m_p + 1}{2} \leqslant \sum_{\substack{2 \leqslant p \leqslant m \\ p \text{ prime}}} \frac{m^2 + 6m}{8} \leqslant \frac{m^3 + 6m^2}{8}.$$

Thus $f_{\mathcal{C}}(Q) \leqslant (3/8)m^3$.

Since P has index at most 8 in Q, Lemma 4.7 implies that $f_{\mathcal{C}\cap P}(P) \leqslant 3m^3$ and that $f_{\mathcal{C}_\tau \cap P}(P) \leqslant 8$. But $m = \sqrt{k}$, so Eq. (3) is true if $|\pi^P| 60^{r_\pi - k}$ is at most a constant multiple of m^{-4} for all $\pi \in R(P) \cap \mathcal{C}$ and at most a constant multiple of m^{-1} for all $\pi \in R(P) \cap \mathcal{C}_\tau$ where both constants are absolute.

We prove the latter requirement first. Let $\pi \in \mathcal{C}_\tau \cap P$. Then $|\pi^P| \leqslant m^{m-1}$ since $|\mathcal{C}_\tau| = |S_m|$. Moreover, if $\pi = (s, s^{-1})\tau$, then the set of fixed points of π on $[m]^2$ is $\{(i, is)\colon\ i \in [m]\}$, so $2(k - r_\pi) = k - f_\pi = m^2 - m$. Since $\log m \leqslant \frac{1}{2}(m-1)\log 60$, we have that $|\pi^P| 60^{r_\pi - k}$ is bounded above by m^{-1}, as desired.

Now let $\pi = (s_1, s_2)$ be an element of prime order p in $\mathcal{C} \cap P$, and suppose that for each i the full cycle decomposition of s_i in S_m consists of t_i p-cycles where $0 \leqslant t_i \leqslant \lfloor m/p \rfloor$ and t_1 or t_2 is non-zero. Then $|(s_1, s_2)^P| \leqslant 2|s_1^{S_m}||s_2^{S_m}| \leqslant 2m^{pt_1 + pt_2}$. Moreover, the element (s_1, s_2) fixes $(i, j) \in [m]^2$ if and only

if s_1 fixes i and s_2 fixes j, so $f_{(s_1,s_2)} = (m - pt_1)(m - pt_2)$. Again, since $k - r_\pi \geqslant (k - f_\pi)/2$ and $\log 60 > 4$, if we can show that

$$(pt_1 + pt_2 + 4)\log m + 2p^2 t_1 t_2 \leqslant 2m(pt_1 + pt_2),$$

then $|\pi^P|60^{r_\pi - k}$ is bounded above by $2m^{-4}$, as desired. Since $\log m/m$ is at most $1/3$ and $x := pt_1 + pt_2$ is at least two, we obtain that $(x+4)\log m \leqslant mx$, and since $pt_i \leqslant m$ for both i, we obtain that $2p^2 t_1 t_2 \leqslant mx$. This completes the proof. □

Now we prove Theorem 1.5 by modifying the proofs of Lemmas 4.1 and 4.3.

Proof of Theorem 1.5. As in the proof of Theorem 1.4, it suffices to show that if $G = A(k,T) \rtimes P$ where P is a primitive subgroup of S_k and $k \geqslant 5$, then $r_i(G)$ converges to 0 for each i as $|T|$ tends to infinity with k fixed. In the proof of Lemma 4.1, we saw that $r_1(G) \leqslant |P|^2 |T|^{8/3 - \lceil k/2 \rceil}$ (since $|\operatorname{Out}(T)|^2 < |T|^{2/3}$ by Lemma 4.8). But k is at least 5, so $r_1(G) \to 0$ as $|T| \to \infty$ with k fixed. Moreover, by Lemma 4.2 the same is true for $r_2(G)$ since $p(T) \to \infty$ as $|T| \to \infty$. Thus it remains to consider $r_3(G)$; this will require some extra work.

For $\pi \in P$ of prime order p, as we have done before, let $f_\pi := \operatorname{fix}_{[k]}(\pi)$, $c_\pi := (k - f_\pi)/p$ and $r_\pi := c_\pi + f_\pi$. Also, let $R(P)$ denote a set of representatives for the conjugacy classes of elements of prime order in P that also fix a point. By Lemma 4.5, we may assume that if $\vec{\alpha}\pi \in R_3(G)$, then $\pi \in R(P)$; moreover, we will assume for simplicity that if π is a transposition, then $\pi = (12)$. Accordingly, let $R_4(G) := \{\vec{\alpha}\pi \in R_3(G) \colon \pi = (12)\}$, and let $r_4(G)$ be the sum of $r_3(G)$ restricted to elements of $R_4(G)$. Also, let $R_4(T) := \{\alpha \in \operatorname{Aut}(T) \colon \vec{\alpha}\pi \in R_4(G)\}$. Note that $R_4(T)$ contains the identity if it is non-empty. Suppose for the time being that $R_4(G)$ is non-empty. Then $P = S_k$. By Lemma 4.5 and Eq. (2) of Lemma 4.6, we have that

$$\begin{aligned} r_4(G) &= \left|(12)^{S_k}\right| \sum_{\alpha \in R_4(T)} \frac{|\alpha^{\operatorname{Aut}(T)}|}{|T|} \left(\frac{|C_{\operatorname{Inn}(T)}(\alpha)|}{|T|}\right)^{k-3} \\ &\leqslant \left|(12)^{S_k}\right| \left(\frac{1}{|T|} + \frac{|\operatorname{Out}(T)|}{p(T)^{k-3}}\right) \end{aligned}$$

since $[T : C_{\operatorname{Inn}(T)}(\alpha)] \geqslant p(T)$ if $\alpha \neq 1$. Then for any primitive P, the proof of Lemma 4.3 and the above inequality imply that

$$r_3(G) \leqslant \left|(12)^{S_k}\right| \left(\frac{1}{|T|} + \frac{|\operatorname{Out}(T)|}{p(T)^{k-3}}\right) + \sum_{\pi \in R(P) \setminus \{(12)\}} \frac{|\pi^P|}{|T|^{k - r_\pi - \frac{5}{3}}}.$$

But $|\operatorname{Out}(T)| \leqslant C p(T)^{11/8}$ for some absolute constant C by Lemma 4.9 since $|\operatorname{Out}(T)|$ is constant if T is either $L_m(2)$, an alternating group or a sporadic group. This then gives us the desired convergence since $k \geqslant 5$ and $k - r_\pi \geqslant 2$ when π is not a transposition. □

Note that the methods of this section can sometimes be adapted to the cases when either $k < 5$ and k is fixed as $|G| \to \infty$, or $k < |T|$ and k grows with $|T|$ as $|G| \to \infty$. These results and their proofs are not included here but can be found in [16]. For example, it is proved that if $k \geqslant 3$, then the proportion of 3-tuples that are bases for G tends to 1 if k is fixed as $|G| \to \infty$. In fact, it looks likely that a similar result holds when $k = 2$ and P_G is trivial; indeed, it is proved for such groups that the proportion of 4-tuples that are bases tends to 1 if k is fixed as $|G| \to \infty$ by using stronger bounds on the numbers of conjugacy classes of non-abelian simple groups. Lastly, it is proved that the proportion of pairs that are bases tends to 1 as $|G|$ tends to infinity if k is a non-constant function in the variable $|T|$ for which $k^4 \leqslant |T|$ for all non-abelian simple groups T.

Acknowledgments

I am grateful to Jan Saxl for his support and guidance, as well as to Ross Lawther and Peter Cameron for some helpful suggestions.

References

[1] M. Aschbacher, R. Guralnick, Some applications of the first cohomology group, J. Algebra 90 (1984) 446–460.
[2] L. Babai, On the order of uniprimitive permutation groups, Ann. Math. 113 (1981) 553–568.
[3] L. Babai, On the order of doubly transitive permutation groups, Invent. Math. 65 (1982) 473–484.
[4] A. Bochert, Ueber die Zahl der verschiedenen Werthe, die eine Function gegebener Buchstaben durch Vertauschung derselben erlangen kann, Math. Ann. 33 (1889) 584–590.
[5] T. Burness, On base sizes for actions of finite classical groups, J. London Math. Soc. 75 (2007) 545–562.
[6] T. Burness, R. Guralnick, J. Saxl, Base sizes for geometric actions of finite classical groups, in preparation.
[7] T. Burness, R. Guralnick, J. Saxl, Base sizes for S-actions of finite classical groups, Israel J. Math., in press.
[8] T. Burness, R. Guralnick, J. Saxl, On base sizes for symmetric groups, Bull. Lond. Math. Soc. 43 (2011) 386–391.
[9] T. Burness, M. Liebeck, A. Shalev, Base sizes for simple groups and a conjecture of Cameron, Proc. London Math. Soc. 98 (2009) 116–162.
[10] T. Burness, E. O'Brien, R. Wilson, Base sizes for sporadic simple groups, Israel J. Math. 177 (2010) 307–333.
[11] P. Cameron, Permutation Groups, Cambridge University Press, 1999.
[12] P. Cameron, W. Kantor, Random permutations: some group-theoretic aspects, Combin. Probab. Comput. 2 (1993) 257–262.
[13] P. Cameron, P. Neumann, J. Saxl, On groups with no regular orbits on the set of subsets, Arch. Math. 43 (1984) 295–296.
[14] J. Conway, R. Curtis, S. Norton, R. Parker, R. Wilson, Atlas of Finite Groups, Clarendon Press, Oxford, 1985.
[15] J. Dixon, B. Mortimer, Permutation Groups, Springer Verlag, New York, 1996.
[16] J. Fawcett, Bases of primitive permutation groups, PhD thesis, in preparation.
[17] P. Gallagher, The number of conjugacy classes in a finite group, Math. Z. 118 (1970) 175–179.
[18] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12, 2008, URL http://www.gap-system.org.
[19] D. Gluck, K. Magaard, Base sizes and regular orbits for coprime affine permutation groups, J. London Math. 58 (1998) 603–618.
[20] D. Gluck, Á. Seress, A. Shalev, Bases for primitive permutation groups and a conjecture of Babai, J. Algebra 199 (1998) 367–378.
[21] J. James, Partition actions of symmetric groups and regular bipartite graphs, Bull. Lond. Math. Soc. 38 (2006) 224–232.
[22] P. Kleidman, M. Liebeck, The Subgroup Structure of the Finite Classical Groups, Cambridge University Press, Cambridge, 1990.
[23] M. Liebeck, On minimal degrees and base sizes of primitive permutation groups, Arch. Math. 43 (1984) 11–15.
[24] M. Liebeck, C. Praeger, J. Saxl, On the O'Nan–Scott theorem for finite primitive permutation groups, J. Aust. Math. Soc. 44 (1988) 389–396.
[25] M. Liebeck, L. Pyber, Upper bounds for the number of conjugacy classes of a finite group, J. Algebra 198 (1997) 538–562.
[26] M. Liebeck, J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, Proc. London Math. Soc. 3 (1991) 266–314.
[27] M. Liebeck, A. Shalev, Simple groups, permutation groups, and probability, J. Amer. Math. Soc. 12 (1999) 497–520.
[28] M. Liebeck, A. Shalev, Bases of primitive permutation groups, in: Groups, Combinatorics and Geometry, Durham, 2001, World Scientific, Singapore, 2003, pp. 147–154.
[29] M. Liebeck, A. Shalev, Bases of primitive linear groups, J. Algebra 252 (2002) 95–113.
[30] M. Liebeck, A. Shalev, Character degrees and random walks in finite groups of Lie type, Proc. London Math. Soc. 90 (2005) 61–86.
[31] G. Malle, J. Saxl, T. Weigel, Generation of classical groups, Geom. Dedicata 49 (1994) 85–116.
[32] D. Maslen, D. Rockmore, Separation of variables and the computation of Fourier transforms on finite groups, J. Amer. Math. Soc. 10 (1997) 169–214.
[33] V. Mazurov, Minimal permutation representations of finite simple classical groups. Special linear, symplectic, and unitary groups, Algebra Logika 32 (1993) 142–153.
[34] C. Praeger, J. Saxl, On the orders of primitive permutation groups, Bull. Lond. Math. Soc. 12 (1980) 303–307.
[35] L. Pyber, Asymptotic results for permutation groups, in: DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, 1993, pp. 197–219.
[36] Á. Seress, The minimal base size of primitive solvable permutation groups, J. London Math. Soc. 53 (1996) 243–255.
[37] Á. Seress, Primitive groups with no regular orbits on the set of subsets, Bull. Lond. Math. Soc. 29 (1997) 697–704.
[38] Á. Seress, Permutation Group Algorithms, Cambridge University Press, Cambridge, 2003.
[39] A. Vasilyev, Minimal permutation representations of finite simple exceptional groups of types G_2 and F_4, Algebra Logika 35 (1996) 371–383.
[40] A. Vasilyev, Minimal permutation representations of finite simple exceptional groups of types E_6, E_7, and E_8, Algebra Logika 36 (1997) 518–530.
[41] A. Vasilyev, Minimal permutation representations of finite simple exceptional twisted groups, Algebra Logika 37 (1998) 17–35.
[42] V. Vasilyev, V. Mazurov, Minimal permutation representations of finite simple orthogonal groups, Algebra Logika 33 (1995) 337–350.