Forum of Mathematics, Sigma (2024), **Vol. 12**:e2 1–43
doi:10.1017/fms.2023.121

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Base sizes of primitive groups of diagonal type

Hong Yi Huang

University of Bristol, Bristol, BS8 1UG, UK; E-mail: hy.huang@bristol.ac.uk.

Received: 28 March 2023; **Revised:** 19 October 2023; **Accepted:** 6 November 2023

2020 Mathematics Subject Classification: *Primary* – 20B15; *Secondary* – 20B05, 20P05

Abstract

Let G be a permutation group on a finite set Ω. The base size of G is the minimal size of a subset of Ω with trivial pointwise stabiliser in G. In this paper, we extend earlier work of Fawcett by determining the precise base size of every finite primitive permutation group of diagonal type. In particular, this is the first family of primitive groups arising in the O'Nan–Scott theorem for which the exact base size has been computed in all cases. Our methods also allow us to determine all the primitive groups of diagonal type with a unique regular suborbit.

Contents

1. Introduction

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω of size n. A subset of Ω is called a *base* for G if its pointwise stabiliser in G is trivial. The minimal size of a base, denoted $b(G)$, is called the *base size* of G. Equivalently, if G is transitive with point stabiliser H, then $b(G)$ is the smallest number b such

that the intersection of some b conjugates of H in G is trivial. This classical concept has been studied since the early years of permutation group theory in the 19th century, finding natural connections to other areas of algebra and combinatorics. For example, see [3] for details of the relationship between the metric dimension of a finite graph and the base size of its automorphism group and [52, Section 4] for an account of the key role played by bases in the computational study of finite groups. We refer the reader to survey articles [9, Section 5] and [44] for further connections.

In general, determining $b(G)$ is a difficult problem and there are no efficient algorithms for computing $b(G)$, or constructing a base of minimal size. Blaha [4] proves that determining whether G has a base of size a given constant is an NP-complete (nondeterministic polynomial-time complete) problem. Historically, there has been an intense focus on studying the base sizes of finite primitive groups (recall that a transitive permutation group is *primitive* if its point stabiliser is a maximal subgroup). A trivial lower bound is $b(G) \geqslant \log_n |G|$ and it turns out that all primitive groups admit small bases in the sense that there is an absolute constant c such that $b(G) \leqslant c \log_n |G|$ for every primitive group G. This was originally conjectured by Pyber [51] in the 1990s and the proof was completed by Duyan et al. in [23]. It was subsequently extended by Halasi et al. [35], who show that

$$b(G) \leqslant 2 \log_n |G| + 24$$

and the multiplicative constant 2 is best possible. In fact, one can prove stronger bounds in special cases. For example, Seress [54] proves that $b(G) \leqslant 4$ if G is soluble, and this result was recently extended by Burness [8] who shows that $b(G) \leqslant 5$ if G has a soluble point stabiliser (both bounds in [8] and [54] are best possible).

The O'Nan–Scott theorem divides the finite primitive groups into several families that are defined in terms of the structure and action of the socle of the group (recall that the *socle* of a group is the product of its minimal normal subgroups). Following [42], these families are: affine, almost simple, diagonal type, product type and twisted wreath products. There are partial results on base sizes when G is affine, product type or a twisted wreath product. For example, if $G = VH \leqslant \mathrm{AGL}(V)$ is affine, then Halasi and Podoski [36] show that $b(G) \leqslant 3$ if $(|V|, |H|) = 1$, and we refer the reader to [16, 24] for some results on base sizes of product type groups and twisted wreath products. In recent years, base sizes of almost simple primitive groups have been intensively studied (recall that G is called *almost simple* if there exists a nonabelian simple group G_0 such that $G_0 \lhd G \leqslant \mathrm{Aut}(G_0)$). Roughly speaking, such a group is said to be *standard* if $G_0 = A_m$ and Ω is a set of subsets or partitions of $\{1, \ldots, m\}$, or G_0 is a classical group and Ω is a set of subspaces of the natural module for G_0, otherwise G is *nonstandard* (see [11, Definition 1] for the formal definition). A conjecture of Cameron [21, p. 122] asserts that $b(G) \leqslant 7$ if G is nonstandard, with equality if and only if $G = \mathrm{M}_{24}$ in its natural action of degree 24. This conjecture was proved in a sequence of papers by Burness et al. [11, 14, 18, 20]. In addition, the precise base sizes of all nonstandard groups with alternating or sporadic socle are computed in [14] and [20, 50], respectively.

In this paper, we focus on bases for primitive diagonal type groups. Here, $G \leqslant \mathrm{Sym}(\Omega)$ has socle T^k, where T is a nonabelian simple group and $k \geqslant 2$ is an integer. More precisely, we have $|\Omega| = |T|^{k-1}$ and

$$T^k \lhd G \leqslant T^k.(\mathrm{Out}(T) \times S_k).$$

The primitivity of G implies that the subgroup $P \leqslant S_k$ induced by the conjugation action of G on the set of factors of T^k is either primitive, or $k = 2$ and $P = A_2 = 1$. The group P is called the *top group* of G and we note that

$$T^k \lhd G \leqslant T^k.(\mathrm{Out}(T) \times P). \tag{1}$$

The first systematic study of bases for diagonal type groups was initiated by Fawcett in [25]. Here, she shows that $b(G) = 2$ if $P \notin \{A_k, S_k\}$, and in the general setting she determines the exact base size of G up to one of two possibilities (see Theorem 2.3). One of the key ingredients in [25] is a theorem of Seress [53], which asserts that if $k > 32$ and $P \notin \{A_k, S_k\}$, then there exists a subset of $\{1, \ldots, k\}$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

with trivial setwise stabiliser in P. However, this does not hold if $P \in \{A_k, S_k\}$, and hence a different approach is required. In this paper, we extend Fawcett's work by determining the exact base size in all cases (see Theorem 3 below).

In recent years, there has been significant interest in studying the base-two primitive groups (we say G is *base-two* if $b(G) = 2$). Indeed, a project with the ambitious aim of classifying these groups was initiated by Jan Saxl in the 1990s and it continues to be actively pursued, with many interesting applications and open problems. For example, Burness and Giudici [12] define the *Saxl graph* of a base-two group $G \leqslant \mathrm{Sym}(\Omega)$ to be the graph with vertex set Ω, with two vertices adjacent if they form a base for G. It is easy to see that the Saxl graph of a base-two primitive group is connected and an intriguing conjecture asserts that its diameter is at most 2 (see [12, Conjecture 4.5]). This has been verified in several special cases (for example, see [16, 17, 22, 40]), but it remains an open problem.

Returning to a diagonal type group G as in (1), recall that Fawcett [25] has proved that $b(G) = 2$ if $P \notin \{A_k, S_k\}$. Our first result resolves the base-two problem for diagonal type groups in full generality.

Theorem 1. *Let G be a diagonal type primitive group with socle T^k and top group $P \leqslant S_k$. Then $b(G) = 2$ if and only if one of the following holds:*

(i) $P \notin \{A_k, S_k\}$.
(ii) $3 \leqslant k \leqslant |T| - 3$.
(iii) $k \in \{|T| - 2, |T| - 1\}$ *and G does not contain S_k.*

Note that $b(G) \leqslant 2$ if and only if G has a regular suborbit, and there is a natural interest in studying the finite primitive groups with a unique regular suborbit. For example, notice that G has a unique regular suborbit if and only if the Saxl graph of G is G-arc-transitive. In this direction, we refer the reader to [17, Theorem 1.6] for a classification of the relevant almost simple primitive groups with soluble point stabilisers, and [16, Corollary 5] for partial results on product type groups. Here, we resolve this problem for diagonal type groups.

Theorem 2. *Let G be a diagonal type primitive group with socle T^k. Then G has a unique regular suborbit if and only if $T = A_5$, $k \in \{3, 57\}$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.*

We now present our main result, which determines the precise base size of every primitive group of diagonal type. This is the first family of primitive groups arising in the O'Nan–Scott theorem for which the exact base sizes are known.

Theorem 3. *Let G be a diagonal type primitive group with socle T^k and top group $P \leqslant S_k$.*

(i) *If $P \notin \{A_k, S_k\}$, then $b(G) = 2$.*
(ii) *If $k = 2$, then $b(G) \in \{3, 4\}$, with $b(G) = 4$ if and only if $T \in \{A_5, A_6\}$ and $G = T^2.(\mathrm{Out}(T) \times S_2)$.*
(iii) *If $k \geqslant 3$, $P \in \{A_k, S_k\}$ and $|T|^{\ell-1} < k \leqslant |T|^{\ell}$ with $\ell \geqslant 1$, then $b(G) \in \{\ell + 1, \ell + 2\}$. Moreover, $b(G) = \ell + 2$ if and only if one of the following holds:*
  (a) $k = |T|$.
  (b) $k \in \{|T| - 2, |T|^{\ell} - 1, |T|^{\ell}\}$ *and $S_k \leqslant G$.*
  (c) $k = |T|^2 - 2$, $T \in \{A_5, A_6\}$ *and $G = T^k.(\mathrm{Out}(T) \times S_k)$.*

Let us briefly discuss the methods we will use to establish our main theorems. Focusing first on Theorem 1, recall that the *holomorph* of a nonabelian finite simple group T is the group

$$\mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T),$$

which can be viewed as a primitive diagonal type group (with $k = 2$ and top group $P = 1$) in terms of its natural action on T. We write $\mathrm{Hol}(T, S)$ for the setwise stabiliser of $S \subseteq T$ in $\mathrm{Hol}(T)$. A key observation is Lemma 2.15, which implies that

$$b(G) = 2 \text{ if there exists } S \subseteq T \text{ such that } |S| = k \text{ and } \mathrm{Hol}(T, S) = 1.$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

This essentially reduces the proof of Theorem 1 to the cases where $3 \leqslant k \leqslant |T|/2$. However, it is rather difficult to directly construct an appropriate subset S of T such that $\mathrm{Hol}(T, S) = 1$.

To overcome this difficulty, we adopt a probabilistic approach for $k \geqslant 5$ in the proof of Theorem 1 (see Section 3 for more details). More specifically, we estimate the probability that a random k-subset S of T satisfies $\mathrm{Hol}(T, S) = 1$, and we also use fixed point ratios to study the probability that a random pair in Ω is a base for G. The former is a new idea, which involves computing

$$\max\{|C_T(x)| : 1 \neq x \in \mathrm{Aut}(T)\}$$

in Theorem 2.12, while the latter is a widely used technique in the study of base sizes introduced by Liebeck and Shalev [45]. The cases where $k = 3$ or 4 will be treated separately in Section 4.1. Here, we use the fact that T is invariably generated by two elements (which is proved in [34] and [38], independently), and a theorem of Gow [32] on the products of regular semisimple classes in groups of Lie type. We will use a very similar approach to establish Theorem 2.

The proof of Theorem 3 will be completed in Section 5, and the main step involves constructing a base of size $\ell + 1$ when $|T|^{\ell-1} < k \leqslant |T|^{\ell} - 3$ for some $\ell \geqslant 2$. Once again, our construction requires the existence of a suitable subset S of T such that $\mathrm{Hol}(T, S) = 1$. We will treat the case where $k = 2$ separately, working with a theorem of Leemans and Liebeck [41] on the existence of a generating pair of T with a certain property (see Theorem 5.2).

As described above, a key ingredient in our study of bases for diagonal type groups is the following result, which may be of independent interest.

Theorem 4. *Let T be a nonabelian finite simple group, and suppose $3 \leqslant m \leqslant |T| - 3$. Then there exists $S \subseteq T$ such that $|S| = m$ and $\mathrm{Hol}(T, S) = 1$.*

Similarly, let $\mathrm{Aut}(T, S)$ be the setwise stabiliser of $S \subseteq T^{\#}$ in $\mathrm{Aut}(T)$, where $T^{\#} = T \setminus \{1\}$. Note that $\mathrm{Aut}(T, S) = \mathrm{Aut}(T, T^{\#} \setminus S)$. By Theorem 4 and the transitivity of $\mathrm{Hol}(T)$, if $3 \leqslant m \leqslant |T| - 3$, then there exists $S \subseteq T$ containing 1 such that $|S| = m$ and $\mathrm{Hol}(T, S) = 1$. This implies that $\mathrm{Aut}(T, S \setminus \{1\}) = 1$ and we have the following corollary.

Corollary 5. *Let T be a nonabelian finite simple group, and suppose $2 \leqslant m \leqslant |T| - 3$. Then there exists $S \subseteq T^{\#}$ such that $|S| = m$ and $\mathrm{Aut}(T, S) = 1$.*

To conclude this section, we highlight a connection to some interesting problems in algebraic combinatorics. A digraph Γ is said to be a *digraphical regular representation (DRR)* of a group X if $\mathrm{Aut}(\Gamma) \cong X$ acts regularly on the vertex set of Γ. In particular, if Γ is a DRR of X, then Γ is isomorphic to a Cayley digraph $\mathrm{Cay}(X, S)$ for some $S \subseteq X^{\#}$ with $\mathrm{Aut}(X, S) = 1$. A classical result of Babai [1] shows that a finite group X admits a DRR if and only if X is not a quaternion group nor one of four elementary abelian groups. Moreover, it was conjectured by Babai and Godsil [2, 30] that if X is a group of order n, then the proportion of subsets $S \subseteq X^{\#}$ such that $\mathrm{Cay}(X, S)$ is a DRR tends to 1 as $n \to \infty$. This conjecture has been proved recently by Morris and Spiga [49].

Given a finite group X, it is natural to consider the existence of a DRR with a prescribed valency, noting that the valency of $\mathrm{Cay}(X, S)$ is $|S|$. Recently, there are some results concerning this problem in relation to finite simple groups (for example, see [58, 61] for the existence of some families of DRRs with a fixed valency $k \leqslant 3$, and [60] for $k \geqslant 5$). However, there appear to be no asymptotic results in the literature concerning the proportion of DRRs of a fixed valency of a given finite group. With this problem in mind, let $\mathbb{Q}_k(X)$ be the probability that a random k-subset of $X^{\#}$ has a nontrivial setwise stabiliser in $\mathrm{Aut}(X)$. That is,

$$\mathbb{Q}_k(X) = \frac{|\{R \in \mathcal{S}_k : \mathrm{Aut}(X, R) \neq 1\}|}{|\mathcal{S}_k|},$$

where $\mathcal{S}_k$ is the set of k-subsets of $X^{\#}$. In Section 6, we will prove the following results.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Theorem 6. *Let $k \geqslant 4$ be an integer and let (T_n) be a sequence of nonabelian finite simple groups such that $|T_n| \to \infty$ as $n \to \infty$. Then $\mathbb{Q}_k(T_n) \to 0$ as $n \to \infty$.*

Theorem 7. *Let T be a nonabelian finite simple group and let k be an integer such that $5\log_2|T| < k < |T| - 5\log_2|T|$. Then $\mathbb{Q}_k(T) < 1/|T|$.*

We anticipate that these two results will be useful in studying the abundance of fixed-valent DRRs of nonabelian finite simple groups.

Notation

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group and $\Delta \subseteq \Omega$. Then the pointwise and setwise stabilisers of Δ in G are sometimes denoted $G_{(\Delta)}$ and $G_{\{\Delta\}}$, respectively. We adopt the standard notation for simple groups of Lie type from [39]. All logarithms, if not specified, are in base two. Finally, if k is a positive integer, then we write $[k]$ for the set $\{1, \ldots, k\}$.

2. Preliminaries

2.1. Diagonal type groups

Here, we adopt the notation in [25]. Let $k \geqslant 2$ be an integer, and let T be a nonabelian finite simple group. Define

$$\begin{aligned} W(k,T) &:= \{(\alpha_1, \ldots, \alpha_k)\pi \in \mathrm{Aut}(T) \wr_k S_k : \alpha_1\mathrm{Inn}(T) = \alpha_i\mathrm{Inn}(T) \text{ for all } i\}, \\ D(k,T) &:= \{(\alpha, \ldots, \alpha)\pi \in \mathrm{Aut}(T) \wr_k S_k\}, \\ \Omega(k,T) &:= [W(k,T) : D(k,T)]. \end{aligned}$$

Then $|\Omega(k,T)| = |T|^{k-1}$ and $W(k,T) = T^k.(\mathrm{Out}(T) \times S_k)$ acts faithfully on $\Omega(k,T)$. We say that a group $G \leqslant \mathrm{Sym}(\Omega)$ with $\Omega = \Omega(k,T)$ is of *diagonal type* if

$$T^k \lhd G \leqslant T^k.(\mathrm{Out}(T) \times S_k).$$

Let P_G denote the subgroup of S_k induced by the conjugation action of G on the set of factors of T^k. That is,

$$P_G = \{\pi \in S_k : (\alpha_1, \ldots, \alpha_k)\pi \in G \text{ for some } \alpha_1, \ldots, \alpha_k \in \mathrm{Aut}(T)\}.$$

Then naturally we have $G \leqslant T^k.(\mathrm{Out}(T) \times P_G)$ as in (1). Moreover, G is primitive if and only if either P_G is primitive on $[k] = \{1, \ldots, k\}$, or $k = 2$ and $P_G = 1$. From now on, if G is clear from the context, we denote $P = P_G$ and

$$\begin{aligned} W &:= T^k.(\mathrm{Out}(T) \times P), \\ D &:= \{(\alpha, \ldots, \alpha)\pi : \alpha \in \mathrm{Aut}(T), \pi \in P\}, \\ \Omega &:= \Omega(k,T) = [W : D]. \end{aligned}$$

We write $\varphi_t \in \mathrm{Inn}(T)$ for the inner automorphism such that $x^{\varphi_t} = t^{-1}xt$ for any $x \in T$. Thus,

$$\Omega = \{D(\varphi_{t_1}, \ldots, \varphi_{t_k}) : t_1, \ldots, t_k \in T\}.$$

The action of G on Ω is given by

$$D(\varphi_{t_1}, \ldots, \varphi_{t_k})^{(\alpha_1,\ldots,\alpha_k)\pi} = D(\varphi_{t_{1\pi^{-1}}}\alpha_{1\pi^{-1}}, \ldots, \varphi_{t_{k\pi^{-1}}}\alpha_{k\pi^{-1}}),$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

and the stabiliser of $D \in \Omega$ in W is D itself. In particular, for any element $(\alpha, \dots, \alpha)\pi \in D$, we have

$$D(\varphi_{t_1}, \dots, \varphi_{t_k})^{(\alpha,\dots,\alpha)\pi} = D(\varphi_{t_{1\pi^{-1}}^{\alpha}}, \dots, \varphi_{t_{k\pi^{-1}}^{\alpha}}),$$

noting that $\alpha^{-1}\varphi_t\alpha = \varphi_{t^\alpha}$ for all $t \in T$.

We begin by recording some preliminary results on bases for diagonal type groups from [25]. We start with [25, Lemma 3.4].

Lemma 2.1. *Let $t_1, \dots, t_k$ be elements of T such that the following two properties are satisfied:*

(i) *At least two of the t_i are trivial and at least one is nontrivial.*
(ii) *If t_i and t_j are nontrivial and $i \neq j$, then $t_i \neq t_j$.*

Then $(\alpha, \dots, \alpha)\pi \in G$ fixes $D(\varphi_{t_1}, \dots, \varphi_{t_k})$ only if $t_i^\alpha = t_{i\pi}$ for all i.

For any $\mathbf{x} = (\varphi_{t_1}, \dots, \varphi_{t_k}) \in \mathrm{Inn}(T)^k$, we define an associated partition $\mathcal{P}_\mathbf{x} = \{\mathcal{P}_t : t \in T\}$ of $[k]$ such that $i \in \mathcal{P}_t$ if $t_i = t$. Note that some parts $\mathcal{P}_t$ in $\mathcal{P}_\mathbf{x}$ might be empty. The following lemma is an extension of Lemma 2.1, which will be useful later in Section 5. Recall that $P_{\{\mathcal{P}_\mathbf{x}\}}$ is the setwise stabiliser of the partition $\mathcal{P}_\mathbf{x}$ in P. In particular, if $t_{i\pi} = t_{j\pi}$ whenever $t_i = t_j$, then we have $\pi \in P_{\{\mathcal{P}_\mathbf{x}\}}$.

Lemma 2.2. *Let $\mathbf{x} = (\varphi_{t_1}, \dots, \varphi_{t_k}) \in \mathrm{Inn}(T)^k$, $\omega = D\mathbf{x} \in \Omega$ and let $\mathcal{P}_\mathbf{x} = \{\mathcal{P}_t : t \in T\}$ be the associated partition of $[k]$ as above. Suppose $(\alpha, \dots, \alpha)\pi \in G_\omega$. Then*

(i) *$\pi \in P_{\{\mathcal{P}_\mathbf{x}\}}$;*
(ii) *If $0 < |\mathcal{P}_1| \neq |\mathcal{P}_t|$ for all $t \neq 1$, then $t_i^\alpha = t_{i\pi}$ for all i.*

Proof. As $(\alpha, \dots, \alpha)\pi$ fixes $\omega = D(\varphi_{t_1}, \dots, \varphi_{t_k})$, there exists a unique $g \in T$ such that $t_i^\alpha = g t_{i\pi}$ for all $i \in \{1, \dots, k\}$. Suppose $t_i = t_j$ for some $i \neq j$ (so i and j are in the same part of $\mathcal{P}_\mathbf{x}$). Then $t_{i\pi} = g^{-1}t_i^\alpha = g^{-1}t_j^\alpha = t_{j\pi}$. This gives part (i).

For part (ii), it suffices to show that $g = 1$. If $t_i = 1$, then $t_{i\pi} = g^{-1}$, and we get $t_{j\pi} = g^{-1}t_j^\alpha \neq g^{-1}$ if $t_j \neq 1$. This implies that $|\mathcal{P}_{g^{-1}}| = |\mathcal{P}_1|$, so $g = 1$ by our assumption. □

The following theorem combines Fawcett's main results on base sizes of diagonal type groups from [25].

Theorem 2.3. *Let G be a diagonal type primitive group with socle T^k and top group $P \leqslant S_k$.*

(i) *If $P \notin \{A_k, S_k\}$, then $b(G) = 2$.*
(ii) *If $k = 2$, then $b(G) = 3$ if $P = 1$, and $b(G) \in \{3, 4\}$ if $P = S_2$.*
(iii) *If $k \geqslant 3$, $P \in \{A_k, S_k\}$ and $|T|^{\ell-1} < k \leqslant |T|^\ell$ with $\ell \geqslant 1$, then $b(G) \in \{\ell + 1, \ell + 2\}$. Moreover, if either $k = |T|$, or $k \in \{|T|^\ell - 1, |T|^\ell\}$ and $S_k \leqslant G$, then $b(G) = \ell + 2$.*

Corollary 2.4. *If $P \in \{A_k, S_k\}$ and $b(G) = 2$, then $2 < k < |T|$.*

The following is [25, Lemma 3.11].

Lemma 2.5. *Suppose $P \in \{A_k, S_k\}$ and there exists an odd integer $3 \leqslant s \leqslant k$ that is relatively prime to the order of every element of $\mathrm{Out}(T)$. Then G contains A_k.*

Corollary 2.6. *If $P \in \{A_k, S_k\}$ and $k \geqslant |T| - 3$, then G contains A_k.*

Proof. We have $|\mathrm{Out}(T)| < |T|^{1/3}$ by Lemma 2.9 below. In particular, $|\mathrm{Out}(T)| < |T|/3$, so there exists a prime s such that $|\mathrm{Out}(T)| < s < k$ (Bertrand's postulate). Now, apply Lemma 2.5. □

The following extends [25, Proposition 3.3], which asserts that $b(G) = 2$ if $k > 32$ and $P \notin \{A_k, S_k\}$. Here, $r(G)$ is the number of regular suborbits of G, noting that $r(G) \geqslant 1$ if and only if $b(G) \leqslant 2$.

Proposition 2.7. *If $k > 32$ and $P \notin \{A_k, S_k\}$, then $r(G) \geqslant 2$.*

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Proof. We use the same construction as in the proof of [25, Proposition 3.3]. By [53, Theorem 1], there exists a partition $\mathcal{P} = \{\Pi_1, \Pi_2, \Pi_3\}$ of $[k]$ such that each Π_i is nonempty, $|\Pi_1|$, $|\Pi_2|$ and $|\Pi_3|$ are distinct, and

$$\bigcap_{m=1}^{3} P_{\{\Pi_m\}} = 1. \tag{2}$$

Let $x_1, x_2 \in T$ be nontrivial elements of distinct orders. By the main theorem of [33], there exist $y_1, y_2 \in T$ such that $\langle x_i, y_i \rangle = T$. Let $\Delta_i = \{D, D(\varphi_{t_{i,1}}, \ldots, \varphi_{t_{i,k}})\}$ for $i \in \{1, 2\}$, where $t_{i,j} = 1$ if $j \in \Pi_1$, $t_{i,j} = x_i$ if $j \in \Pi_2$, and $t_{i,j} = y_i$ if $j \in \Pi_3$. As explained in the proof of [25, Proposition 3.3], both Δ_1 and Δ_2 are bases for G.

Suppose $\Delta_1^{(\alpha,\ldots,\alpha)\pi} = \Delta_2$. Then there exists $g \in T$ such that $t_{1,j}^{\alpha} = g t_{2,j^\pi}$ for all $j \in [k]$. If $t_{1,j} = t_{1,j'}$ for some $j' \in [k]$, then $t_{2,j} = t_{2,j'}$ and

$$t_{2,j^\pi} = g^{-1} t_{1,j}^{\alpha} = g^{-1} t_{1,j'}^{\alpha} = t_{2,(j')^\pi}.$$

Hence, $\pi \in P_{\{\mathcal{P}\}}$, and so $\pi \in P_{\{\Pi_m\}}$ for each $m \in \{1, 2, 3\}$ as $|\Pi_1|$, $|\Pi_2|$ and $|\Pi_3|$ are distinct. This implies that $\pi = 1$ by (2), and so $g = 1$. However, it follows that $x_1^{\alpha} = x_2$, which is incompatible with $|x_1| \neq |x_2|$. We conclude that Δ_1 and Δ_2 are in distinct G_D-orbits, and thus $r(G) \geqslant 2$. □

Remark 2.8. In fact, as we will show in Section 4, we have $r(G) \geqslant 1$ whenever $3 \leqslant k \leqslant |T| - 3$, with equality if and only if $T = A_5$, $k \in \{3, 57\}$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$. In particular, it follows that $r(G) \geqslant 2$ if $k \leqslant 32$ and $P \notin \{A_k, S_k\}$.

2.2. Simple groups

In this section, we record some properties of finite simple groups that will be used to prove our main results. In the whole paper, T is a nonabelian finite simple group. We start with [25, Lemma 4.8].

Lemma 2.9. *We have* $|\mathrm{Out}(T)| < |T|^{1/3}$.

Let T be a finite simple group of Lie type defined over $\mathbb{F}_q$, where $q = p^f$ and p is a prime. Then we may write $T = O^{p'}(Y_\sigma)$, where Y is the ambient simple algebraic group over the algebraic closure K of $\mathbb{F}_q$ and σ is an appropriate Steinberg endomorphism. Note that $Y_\sigma = \mathrm{Inndiag}(T)$ is the group of inner-diagonal automorphisms of T.

Lemma 2.10. *Let* $d = \frac{1}{2} \cdot \dim Y$ *if* $T \in \{{}^2B_2(q), {}^2G_2(q)', {}^2F_4(q)'\}$ *and* $d = \dim Y$ *otherwise. Then* $\frac{1}{2} q^d < |\mathrm{Inndiag}(T)| < q^d$.

Proof. This is [10, Proposition 3.9(i)] when T is a classical group, and the bounds for exceptional groups are clear. □

Recall that a semisimple element $x \in T$ is *regular* if the connected component of $C_Y(x)$ is a maximal torus of Y. Equivalently, $x \in T$ is regular semisimple if and only if $|C_T(x)|$ is indivisible by p. In particular, if T is a classical group with natural module V, then a semisimple element $x \in T$ is regular if a preimage $\widehat{x} \in \mathrm{GL}(\overline{V})$ has distinct eigenvalues on $\overline{V} = V \otimes K$. And if T is an orthogonal group, then x is also regular if $\widehat{x}$ has a two-dimensional (± 1)-eigenspace and all the other eigenvalues are distinct.

We say that a subset $\{t_1, \ldots, t_m\}$ of T is an *invariable* generating set if $\langle t_1^{g_1}, \ldots, t_m^{g_m} \rangle = T$ for any $g_1, \ldots, g_m \in T$. It has been proved in [34] and [38], independently, that every nonabelian finite simple group is invariably generated by two elements.

Theorem 2.11. *Suppose* $T \notin \{\mathrm{L}_2(5), \mathrm{L}_2(7), \Omega_8^+(2), \mathrm{P}\Omega_8^+(3)\}$ *is a finite simple group of Lie type. Then there exist regular semisimple elements* x *and* y *of distinct orders such that* T *is invariably generated by* $\{x, y\}$.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Proof. If T is an exceptional group, then we take x and y to be t_1 and t_2 in [38, Table 2], respectively, noting that t_1 is a generator of the maximal torus T_1 in that table. It is evident that $|t_1| \neq |t_2|$ in each case, and $\{t_1, t_2\}$ invariably generates T by [38] (see [38, p. 312]). Moreover, we observe that $\langle t_1 \rangle$ and $\langle t_2 \rangle$ are both maximal tori, which implies that each t_i is regular semisimple.

To complete the proof, we may assume T is a classical group. Here, we will work with the corresponding quasisimple group $Q \in \{\mathrm{SL}_n^\varepsilon(q), \mathrm{Sp}_n(q), \Omega_n^\varepsilon(q)\}$, noting that if Q is invariably generated by $\{t_1, t_2\}$, with t_1 and t_2 regular semisimple, then T is invariably generated by $\{x, y\}$, where x and y are the images of t_1 and t_2 in T, respectively (so x and y are also regular semisimple). Moreover, $|x| = |t_1|/a$ and $|y| = |t_2|/b$ for some integers a, b dividing $|Q|/|T|$, so $|x| \neq |y|$ if

$$|t_1| \text{ is indivisible by } |t_2||Q|/|T| \text{ and } |t_2| \text{ is indivisible by } |t_1||Q|/|T|. \tag{3}$$

First, assume $Q \notin \{\mathrm{SL}_2(q), \Omega_8^+(q)\}$. Here, we use the same t_1 and t_2 as presented in [38, Table 1]. In each case, it is clear that t_1 and t_2 are semisimple elements satisfying (3), and $\{t_1, t_2\}$ invariably generates Q by [38, Lemma 5.3]. Thus, it suffices to show that t_1 and t_2 are regular in every case, which is a straightforward exercise (for instance, we can work with the criterion for regularity in terms of the eigenvalues on $\overline{V}$ discussed as above). For example, consider the element $t_2 \in Q = \Omega_{4m}^+(q)$. Here, t_2 lifts to an element $\widehat{t_2} \in \mathrm{GL}(V)$ of the form

$$\widehat{t_2} = \begin{pmatrix} A & \\ & B \end{pmatrix}^\delta$$

with respect to a standard basis (see [39, Proposition 2.5.3]), where $\delta \in \{1, 2\}$, $A \in \mathrm{SO}_{4m-4}^-(q)$ has order $q^{2m-2} + 1$ and $B \in \mathrm{SO}_4^-(q)$ has order $q^2 + 1$. We only deal with the case where $\delta = 1$ since a similar argument holds for $\delta = 2$. Then the eigenvalues of A over the algebraic closure K of $\mathbb{F}_q$ are

$$\lambda, \lambda^q, \ldots, \lambda^{q^{4m-3}}$$

for some $\lambda \in K$ of order $q^{2m-2} + 1$. Similarly, the set of eigenvalues of B over K is $\{\mu, \mu^q, \mu^{q^2}, \mu^{q^3}\}$ for some $\mu \in K$ of order $q^2 + 1$. If $\mu = \lambda^{q^i}$ for some $i \in \{0, \ldots, 4m-3\}$, then $\lambda^{q^i(q^2+1)} = 1$ and so $q^{2m-2} + 1$ divides $q^i(q^2 + 1)$, which implies that $q^{2m-2} + 1$ divides $q^2 + 1$ since $(q^{2m-2} + 1, q^i) = 1$. However, since $m \geqslant 3$, this is impossible. It follows that the eigenvalues of $\widehat{t_2}$ over K are distinct, and so t_2 is a regular semisimple element.

Finally, let us handle the two excluded cases above. If $Q = \mathrm{SL}_2(q)$ with $q \notin \{4, 5, 7, 9\}$, then we take the same t_1 and t_2 as indicated in the proof of [38, Lemma 5.3]. The group $\mathrm{L}_2(4)$ is invariably generated by an element of order 3 and an element of order 5, and if $q = 9$, then we take x and y to be of order 4 and 5, respectively. If $Q = \Omega_8^+(q)$ with $q \notin \{2, 3\}$, then we take t_1 as in [38, Table 1], and t_2 an element of order $(q^3 - 1)/(2, q - 1)$ as described in the proof of [38, Lemma 5.4], where it is denoted t_3. □

It is worth noting that the excluded groups $\mathrm{L}_2(5)$, $\mathrm{L}_2(7)$, $\Omega_8^+(2)$ and $\mathrm{P}\Omega_8^+(3)$ in Theorem 2.11 are not invariably generated by any pair of regular semisimple elements of distinct orders. This is can be checked using Magma V2.26-11 [5]. More specifically, we find the set of maximal overgroups of an element $x \in T$ up to T-conjugacy using the method as in [15, Section 1.2], noting that x and y do not invariably generate T if they have a common maximal overgroup in T up to T-conjugacy.

From now on, we will assume $n \geqslant 3$ if $T = \mathrm{U}_n(q)$, $n \geqslant 4$ is even if $T = \mathrm{PSp}_n(q)$, and $n \geqslant 7$ if $T = \mathrm{P}\Omega_n^\varepsilon(q)$. We will also exclude the groups

$$\mathrm{L}_2(4), \mathrm{L}_2(5), \mathrm{L}_2(9), \mathrm{L}_3(2), \mathrm{L}_4(2), \mathrm{U}_4(2), \mathrm{Sp}_4(2)', G_2(2)', {}^2G_2(3)' \tag{4}$$

as each of them is isomorphic to one of the following groups:

$$A_5, A_6, A_8, \mathrm{L}_2(7), \mathrm{L}_2(8), \mathrm{U}_3(3), \mathrm{PSp}_4(3).$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Table 1. *$h(T)$ in Theorem 2.12*

T	$h(T)$	x	Conditions
A_n	$(n-2)!$	$(1,2)$	
M_{11}	48	2A	
M_{12}	240	2A	
M_{22}	1344	2B	
M_{23}	2688	2A	
M_{24}	21504	2A	
J_1	120	2A	
J_2	1920	2A	
J_3	2448	2B	
J_4	21799895040	2A	
HS	40320	2C	
McL	40320	2A	
Suz	9797760	3A	
He	161280	2A	
HN	177408000	2A	
Ru	245760	2A	
Ly	2694384000	3A	
Co_1	1345036492800	3A	
Co_2	743178240	2A	
Co_3	2903040	2A	
Th	92897280	2A	
O′N	175560	2B	
Fi_{22}	18393661440	2A	
Fi_{23}	129123503308800	2A	
Fi'_{24}	4089470473293004800	2C	
$\mathbb{B}$	306129918735099415756800	2A	
$\mathbb{M}$	8309562962452852382355161088000000	2A	
$E_8(q)$	$q^{57}\lvert E_7(q)\rvert(2,q-1)$	u_α	
$E_7(q)$	$q^{33}\lvert \mathrm{SO}^+_{12}(q)\rvert/(2,q)$	u_α	
$E_6^\varepsilon(q)$	$q^{21}\lvert \mathrm{SL}^\varepsilon_6(q)\rvert/(3,q-\varepsilon)$	u_α	
$F_4(q)$	$q^{15}\lvert \mathrm{Sp}_6(q)\rvert$	u_α	
$G_2(q)$	$q^5\lvert \mathrm{SL}_2(q)\rvert$	u_α	
${}^3D_4(q)$	$q^{12}(q^6-1)$	u_α	
${}^2F_4(q)$	$q^{10}\lvert {}^2B_2(q)\rvert$	u_α	$q>2$
${}^2F_4(2)'$	10240	u_α	
${}^2G_2(q)$	q^3	u_α	
${}^2B_2(q)$	q^2	u_α	
$L_n^\varepsilon(q)$	$\lvert \mathrm{PGL}_2(q^{1/2})\rvert$	$\phi^{f/2}$	$n=2$, f is even
	$q+1$	s	$n=2$, f is odd
	$\lvert \mathrm{PGL}_3(q^{1/2})\rvert$	$\phi^{f/2}$	$n=3$, $\varepsilon=+$, f is even, $3 \mid q^{1/2}+1$
	$\lvert \mathrm{PGU}_3(q^{1/2})\rvert$	$\phi^{f/2}\gamma$	$n=3$, $\varepsilon=+$, f is even, $3 \nmid q^{1/2}+1$
	$(2,q-\varepsilon)\lvert \mathrm{PGSp}_4(q)\rvert/(4,q-\varepsilon)$	γ_1	$n=4$
	$\lvert \mathrm{GU}_{n-1}(q)\rvert/(n,q+1)$	$[\omega I_1, I_{n-1}]$	$n\geqslant 6$ is even, $\varepsilon=-$
	$q^{2n-3}\lvert \mathrm{GL}^\varepsilon_{n-2}(q)\rvert/(n,q-\varepsilon)$	u_α	otherwise
$\mathrm{PSp}_n(q)$	$\lvert \mathrm{Sp}_2(q^2)\rvert$	t_1	$n=4$, q is odd
	$q^{n-1}\lvert \mathrm{Sp}_{n-2}(q)\rvert$	u_α	otherwise
$P\Omega^\varepsilon_n(q)$	$\lvert \mathrm{SO}^-_{n-1}(q)\rvert$	t'_1	n is odd
	$\lvert \mathrm{Sp}_{n-2}(q)\rvert$	b_1	q is even
	$\lvert \Omega_{n-1}(q)\rvert$	γ_1	n is even, q is odd

As mentioned in Section 1, one of our probabilistic approaches in Section 3 relies on computing

$$h(T) := \max\{|C_T(x)| : 1 \neq x \in \mathrm{Aut}(T)\}$$

for every nonabelian finite simple group T.

Theorem 2.12. *Let T be a nonabelian finite simple group. Then $h(T)$ is listed in Table 1.*

Remark 2.13. Let us briefly comment on the notation we adopt in the third column of Table 1, where we record an element $x \in \mathrm{Aut}(T)$ with $|C_T(x)| = h(T)$.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

(i) We adopt the notation in [59] for labelling conjugacy classes when T is a sporadic group. If T is Lie type, then we write u_α for a long root element.
(ii) When $T = \mathrm{L}_n(q)$, we write ϕ for a field automorphism of order $f = \log_p q$, where p is the characteristic of the field $\mathbb{F}_q$.
(iii) If $T = \mathrm{L}_2(q)$, then let H be the normaliser in $\mathrm{PGL}_2(q)$ of a nonsplit maximal torus of T, so $H \cong D_{2(q+1)}$. We then define $s \in H$ to be the central involution if q is odd, and an arbitrary element of odd prime order if q is even.
(iv) We adopt the notation in [13, Chapter 3] for elements of classical groups. For example, if $T = \mathrm{P}\Omega_n^\varepsilon(q)$, where n is even and q is odd, then a preimage in $\mathrm{O}_n^\varepsilon(q)$ of an element of type γ_1 is an involution of the form $[-I_1, I_{n-1}]$ (see [13, Section 3.5.2.14]).

Proof of Theorem 2.12. First, observe that we only need to consider prime order elements in $\mathrm{Aut}(T)$, since $C_T(x) \leqslant C_T(x^m)$ for any integer m and $x \in \mathrm{Aut}(T)$.

Assume $T = A_n$ is an alternating group. If $n = 5$ or 6, then the result can be checked using Magma. Now, assume $n \geqslant 7$, so $\mathrm{Aut}(T) = S_n$. It is easy to see that $|C_T(x)|$ is maximal when x is a transposition, in which case $C_{S_n}(x) \cong S_2 \times S_{n-2}$ and thus $|C_T(x)| = (n-2)!$. Hence, $h(T) = (n-2)!$. If T is a sporadic group, then $|C_T(x)|$ can be read off from the character table of T, which can be accessed computationally via the GAP Character Table Library [6].

For the remainder, we may assume T is a simple group of Lie type over $\mathbb{F}_q$, where $q = p^f$ with p a prime. Assume $x \in \mathrm{Aut}(T)$ is of prime order r. If $x \in \mathrm{Inndiag}(T)$, then x is semisimple if $p \neq r$, otherwise x is unipotent. And if $x \notin \mathrm{Inndiag}(T)$, then x is a field, graph or graph-field automorphism. Here, if x is a graph or graph-field automorphism, then $r \in \{2, 3\}$.

Assume T is an exceptional group. Here, we assume $T \neq {}^2G_2(3)' \cong \mathrm{L}_2(8)$ and $T \neq G_2(2)' \cong \mathrm{U}_3(3)$ as noted in (4). By [19, Proposition 2.11], $|C_T(x)|$ is maximal when $x \in T$ is a long root element. Now, assume $x \in T$ is a long root element. If T is not ${}^3D_4(q)$ or ${}^2B_2(q)$, then $|C_T(x)|$ can be read off from the tables in [43, Chapter 22], noting that $x^{\mathrm{Inndiag}(T)} = x^T$ by [43, Corollary 17.10]. If $T = {}^3D_4(q)$ or ${}^2B_2(q)$, then we can find $|C_T(x)|$ in [55, p. 677] and [57], respectively.

For the remainder of the proof, we assume T is a classical group defined over $\mathbb{F}_q$. Let V be the natural module of T, and write $\overline{V} = V \otimes K$, where K is the algebraic closure of $\mathbb{F}_q$. For $x \in \mathrm{PGL}(V)$, let $\widehat{x}$ be a preimage of x in $\mathrm{GL}(V)$. Following [10, Definition 3.16], we define

$$\nu(x) = \min\{\dim[\overline{V}, \lambda\widehat{x}] : \lambda \in K^*\},$$

where $[\overline{V}, \lambda\widehat{x}] = \{v - \lambda\widehat{x}v : v \in \overline{V}\}$. That is, $\nu(x)$ is the codimension of the largest eigenspace of $\widehat{x}$ on $\overline{V}$, noting that $\nu(x)$ is independent of the choice of the preimage $\widehat{x}$. Upper and lower bounds on $|x^T|$ in terms of n, q and $\nu(x)$ are given in [10, Section 3]. Similarly, if x is a field, graph or graph-field automorphism, then lower bounds for $|x^T|$ can be read off from [10, Table 3.11]. In addition, $|C_{\mathrm{Inndiag}(T)}(x)|$, and a description of the splitting of $x^{\mathrm{Inndiag}(T)}$ into distinct T-classes, can be found in [13, Chapter 3]. In particular, note that if $x \in \mathrm{Inndiag}(T)$ is a semisimple element of prime order, then $x^{\mathrm{Inndiag}(T)} = x^T$ (see [31, Theorem 4.2.2(j)], also recorded as [13, Theorem 3.1.12]).

We start with the case where $T = \mathrm{L}_2(q)$. Let H be the normaliser in $\mathrm{PGL}_2(q)$ of a nonsplit maximal torus of T, so $H \cong D_{2(q+1)}$. If q is odd, then we let x be the central involution in H, and if q is even, let $x \in H$ be an element of odd prime order. Then $|C_T(x)| = q + 1$, so $h(T) \geqslant q + 1$. Let $y \in \mathrm{Aut}(T)$ be an element of prime order. Note that if y is unipotent, then $|C_T(y)| = q$, and $|C_T(y)|$ divides $q + 1$ or $q - 1$ if y is semisimple. Thus, we only need to consider field automorphisms, noting that $|C_{\mathrm{PGL}_2(q)}(y)| = |\mathrm{PGL}_2(q^{1/r})|$ if y is a field automorphism of prime order r. It follows that $|C_{\mathrm{PGL}_2(q)}(y)| > q + 1$ only if $r = 2$ (so f is even). Indeed,

$$|C_T(y)| = |C_{\mathrm{PGL}_2(q)}(y)| = |\mathrm{PGL}_2(q^{1/2})| > q + 1$$

if y is an involutory field automorphism, and so we conclude that $h(T) = |\mathrm{PGL}_2(q^{1/2})|$ if f is even, and $h(T) = q + 1$ if f is odd.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

To complete the proof for linear and unitary groups, we assume $T = \mathrm{L}_n^\varepsilon(q)$ with $n \geqslant 3$. Let $x \in T$ be a unipotent element with Jordan form $[J_2, J_1^{n-2}]$ on the natural module, noting that x is a long root element. Then $|C_{\mathrm{PGL}_n^\varepsilon(q)}(x)|$ can be read off from [13, Tables B.3 and B.4], and we have $x^{\mathrm{PGL}_n^\varepsilon(q)} = x^T$ by [13, Propositions 3.2.7 and 3.3.10]. More specifically,

$$|C_T(x)| = (n, q-\varepsilon)^{-1} q^{2n-3} |\mathrm{GL}_{n-2}^\varepsilon(q)|$$

and

$$|x^T| = |x^{\mathrm{PGL}_n^\varepsilon(q)}| = \frac{|\mathrm{PGL}_n^\varepsilon(q)|}{q^{2n-3}|\mathrm{GL}_{n-2}^\varepsilon(q)|} < \frac{2q^{2n-1}}{q-1}.$$

The cases where $n \in \{3, 4\}$ require special attention, which will be treated separately.

Assume $T = \mathrm{L}_3^\varepsilon(q)$, so $|C_T(x)| = (3, q-\varepsilon)^{-1} q^3 (q-\varepsilon)$, and let y be an element in $\mathrm{Aut}(T)$ of prime order that is not of Jordan form $[J_2, J_1]$. If y is unipotent or semisimple and $\nu(y) = 2$, then either y has Jordan form $[J_3]$ or $|y|$ is odd, so by [10, Propositions 3.22 and 3.36],

$$|y^T| > \frac{1}{2(3, q-\varepsilon)} \left(\frac{q}{q+1} \right) q^6 > (q^2-1)(q^2+\varepsilon q+1) = |x^T|.$$

If $\nu(y) = 1$ and y is semisimple, then a preimage $\widehat{y}$ of y in $\mathrm{GL}(V)$ is $[\omega I_1, I_2]$, so $|C_T(y)| = (3, q-\varepsilon)^{-1} |\mathrm{GL}_2^\varepsilon(q)|$. It is easy to see that $|C_T(y)| < |C_T(x)|$. If y is a graph automorphism, then $|C_{\mathrm{PGL}_3^\varepsilon(q)}(y)| = |\mathrm{SL}_2(q)|$, so $|C_T(y)| < |C_T(x)|$ evidently. If y is a field automorphism of odd prime order r, then by [13, Propositions 3.2.9 and 3.3.12],

$$|C_{\mathrm{PGL}_3^\varepsilon(q)}(y)| = |\mathrm{PGL}_3^\varepsilon(q^{1/r})| \leqslant q(q^{2/3}-1)(q-\varepsilon),$$

so $|C_T(y)| \leqslant |C_{\mathrm{PGL}_3^\varepsilon(q)}(y)| < |C_T(x)|$. Thus, we only need to consider involutory field or graph-field automorphisms, so we can assume $\varepsilon = +$ and f is even. Let y_1 be an involutory field automorphism. Then by [13, Proposition 3.2.9],

$$|C_T(y_1)| = \frac{(3, q^{1/2}+1)}{(3, q-1)} |\mathrm{PGL}_3(q^{1/2})|.$$

Similarly, if y_2 is a graph-field automorphism, then

$$|C_T(y_2)| = \frac{(3, q^{1/2}-1)}{(3, q-1)} |\mathrm{PGU}_3(q^{1/2})|$$

by [13, Proposition 3.2.15]. Note that

$$|\mathrm{PGL}_3(q^{1/2})| < q^3(q-1) < |\mathrm{PGU}_3(q^{1/2})| < 3|\mathrm{PGL}_3(q^{1/2})|.$$

Therefore, $h(T) = |C_T(x)|$ if f is odd or $\varepsilon = -$, $h(T) = |C_T(y_1)|$ if $\varepsilon = +, f$ is even and $3 \mid q^{1/2}+1$, otherwise $h(T) = |C_T(y_2)|$.

Next, assume $T = \mathrm{L}_4^\varepsilon(q)$ and let z be a graph automorphism of type γ_1 (see [13, Sections 3.2.5 and 3.3.5]), so by [13, Propositions 3.2.14 and 3.3.17], we have

$$|C_T(z)| = \frac{(2, q-\varepsilon)}{(4, q-\varepsilon)} |\mathrm{PGSp}_4(q)| > \frac{1}{(4, q-\varepsilon)} q^6 (q^2-1)(q-\varepsilon) = |C_T(x)|$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

and we claim that $h(T) = |C_T(z)|$. Note that

$$|z^T| = \frac{q^2(q^3-\varepsilon)}{(2, q-\varepsilon)}.$$

By [10, Propositions 3.22, 3.36, 3.37 and 3.48], we have

$$|y^T| > \frac{1}{2}\left(\frac{q}{q+1}\right)q^6$$

for any unipotent, semisimple, field or graph-field element $y \in \mathrm{Aut}(T)$ of prime order. Hence, $|y^T| > |z^T|$ if $q \geqslant 4$, and for $q \in \{2, 3\}$ we can check that $|y^T| > |z^T|$ using Magma. Similarly, if y is a graph automorphism, then $|y^T| \geqslant |z^T|$ by inspecting [13, Tables B.3 and B.4].

Finally, assume $T = \mathrm{L}_n^\varepsilon(q)$ and $n \geqslant 5$. Then by applying the bounds in [10, Table 3.11] we see that

$$|y^T| > \frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{1}{2}(1-\varepsilon)} q^{\frac{1}{2}(n^2-n-4)} > \frac{2q^{2n-1}}{q-1} > |x^T|$$

if y is a field, graph or graph-field automorphism, unless $(n, q) = (5, 2)$ or $(6, 2)$, in which cases one can check that $|y^T| > |x^T|$ with the aid of Magma. If y is a unipotent or semisimple element with $\nu(y) \geqslant 2$, then

$$|y^T| > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{4n-8} > \frac{2q^{2n-1}}{q-1} > |x^T|$$

by [10, Proposition 3.36]. Thus, we only need to consider the cases where $\nu(y) = 1$ and y is not $\mathrm{Aut}(T)$-conjugate to x. In this setting, y is semisimple, and a preimage $\widehat{y}$ of y in $\mathrm{GL}(V)$ is $[\omega I_1, I_{n-1}]$, where ω is a nontrivial r-th root of unity in $\mathbb{F}_q$ if $\varepsilon = +$, or $\mathbb{F}_{q^2}$ if $\varepsilon = -$, for some prime r. It follows that

$$|C_T(y)| = (n, q-\varepsilon)^{-1}|\mathrm{GL}_{n-1}^\varepsilon(q)|.$$

Note that $|C_T(y)| > |C_T(x)|$ if and only if $\varepsilon = -$ and n is even. This implies that

$$h(T) = (n, q-\varepsilon)^{-1}|\mathrm{GL}_{n-1}^\varepsilon(q)|$$

if $\varepsilon = -$ and n is even, otherwise $h(T) = |C_T(x)|$.

This concludes the proof of Theorem 2.12 for linear and unitary groups. We can use a very similar approach to handle the symplectic and orthogonal groups and we omit the details. But let us remark that if $T = \mathrm{PSp}_n(q)$ is a symplectic group, then $|C_T(x)|$ is maximal when x is a long root element, unless $n = 4$ and q is odd, where an involution of type t_1 gives the maximal centraliser. If $T = \mathrm{P}\Omega_n^\varepsilon(q)$, where n is odd or q is even, then $|C_T(x)|$ is maximal when x is an involution of type t_1' or b_1, respectively. Finally, if $T = \mathrm{P}\Omega_n^\varepsilon(q)$ with n even and q odd, then a graph automorphism of type γ_1 has the maximal centraliser. All the relevant information about these elements can be found in [13, Chapter 3]. □

An immediate corollary is the following, which will be useful in Section 3.

Corollary 2.14. *We have $h(T) \leqslant |T|/10$ for any nonabelian finite simple group T.*

2.3. Holomorph of simple groups

Recall that $\mathrm{Hol}(T) = T{:}\mathrm{Aut}(T)$ is the *holomorph* of T, which acts faithfully and primitively on T (in fact, $\mathrm{Hol}(T) = T^2.\mathrm{Out}(T)$ is a diagonal type primitive group). Note that every element in $\mathrm{Hol}(T)$ can be uniquely written as $g\alpha$, where $g \in T$ acts on T by left translation and $\alpha \in \mathrm{Aut}(T)$ acts naturally on T. That is,

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

$$t^{g\alpha} = (g^{-1}t)^{\alpha}$$

for every $t \in T$. Let $\mathrm{Hol}(T, S)$ be the setwise stabiliser of $S \subseteq T$ in $\mathrm{Hol}(T)$. Throughout this section, we assume $P = S_k$, so $W = T^k.(\mathrm{Out}(T) \times S_k)$. The following result is a key observation.

Lemma 2.15. *The following statements are equivalent.*

(i) $\{D, D(\varphi_{t_1}, \dots, \varphi_{t_k})\}$ *is a base for* W*;*
(ii) $t_1, \dots, t_k$ *are distinct and* $\mathrm{Hol}(T, \{t_1, \dots, t_k\}) = 1$.

Proof. First, assume (i) holds. If $t_i = t_j$ for some $i \neq j$, then $(i, j) \in W$ stabilises D and $D(\varphi_{t_1}, \dots, \varphi_{t_k})$, which is incompatible with (i). Thus, $t_1, \dots, t_k$ are distinct. Suppose $g\alpha \in \mathrm{Hol}(T, \{t_1, \dots, t_k\})$. Then for any i we have

$$t_j = t_i^{g\alpha} = (g^{-1}t_i)^{\alpha} = (g^{-1})^{\alpha} t_i^{\alpha} \tag{5}$$

for some j. That is, $g\alpha$ induces a permutation $\pi \in S_k$ by $(g^{-1})^{\alpha} t_i^{\alpha} = t_{i^{\pi}}$. Now, it is easy to see that $(\alpha, \dots, \alpha)\pi$ fixes $D(\varphi_{t_1}, \dots, \varphi_{t_k})$. Hence, $\alpha = 1$ and $\pi = 1$, which implies that $g = 1$ by (5), noting that $i = j$ since $\pi = 1$.

Conversely, suppose (ii) holds and $(\alpha, \dots, \alpha)\pi$ fixes D and $D(\varphi_{t_1}, \dots, \varphi_{t_k})$. Then there exists $g \in T$ such that $t_{i^{\pi}} = g^{-1} t_i^{\alpha}$ for all i. It follows that $g^{\alpha^{-1}} \alpha \in \mathrm{Hol}(T, \{t_1, \dots, t_k\})$, which implies that $g = 1$ and $\alpha = 1$. As $t_1, \dots, t_k$ are distinct, this gives $\pi = 1$ and so (i) holds. □

Let $\mathscr{P}_k(T)$ (or just $\mathscr{P}_k$ if T is clear from the context) be the set of k-subsets of T. Recall that $r(G)$ is the number of regular suborbits of G.

Lemma 2.16. *The number of regular orbits of* $\mathrm{Hol}(T)$ *on* $\mathscr{P}_k$ *or* $\mathscr{P}_{|T|-k}$ *is* $r(W)$*. In particular,* $b(W) = 2$ *if and only if* $\mathrm{Hol}(T)$ *has a regular orbit on* $\mathscr{P}_k$ *or* $\mathscr{P}_{|T|-k}$.

Proof. This follows directly from Lemma 2.15, noting that $\mathrm{Hol}(T, S) = \mathrm{Hol}(T, T \setminus S)$. □

Given a subset $S \subseteq T$, it is difficult to determine $\mathrm{Hol}(T, S)$. In particular, it is difficult to construct a subset $S \subseteq T$ such that $\mathrm{Hol}(T, S) = 1$. By the transitivity of $\mathrm{Hol}(T)$ on T, we may assume $1 \in S$.

Lemma 2.17. *Let* S_1 *and* S_2 *be subsets of* T *such that* $1 \in S_1 \cap S_2$ *and* $S_1^{g\alpha} = S_2$*. Then* $g \in S_1$.

Proof. We have $g^{-1}S_1 = S_2^{\alpha^{-1}}$, so $1 \in g^{-1}S_1$ and thus $g \in S_1$. □

Now, we give some sufficient conditions that allow us to deduce that $\mathrm{Hol}(T, S) = 1$ for a subset $S \subseteq T$ containing 1. Here, we write $\mathrm{Aut}(T, R)$ for the setwise stabiliser of $R \subseteq T^{\#}$ in $\mathrm{Aut}(T)$.

Lemma 2.18. *Let* $S = \{t_1, \dots, t_k\} \in \mathscr{P}_k$ *with* $t_1 = 1$*. Then* $\mathrm{Hol}(T, S) = 1$ *if the following conditions are satisfied:*

(i) $\mathrm{Aut}(T, \{t_2, \dots, t_k\}) = 1$*;*
(ii) *for all* $2 \leqslant i \leqslant k$, $\{|t_i^{-1}t_1|, \dots, |t_i^{-1}t_k|\} \neq \{1, |t_2|, \dots, |t_k|\}$.

Proof. Suppose $g\alpha \in \mathrm{Hol}(T, S)$, where $g \in T$ and $\alpha \in \mathrm{Aut}(T)$. By Lemma 2.17, we have $g \in S$. If $g = t_1 = 1$, then $\alpha \in \mathrm{Aut}(T, \{t_2, \dots, t_k\})$ and the condition (i) forces $\alpha = 1$. If $g = t_i$ for some $2 \leqslant i \leqslant k$, then $t_i^{-1}S = S^{\alpha^{-1}}$, which implies that $\{|t_i^{-1}t_1|, \dots, |t_i^{-1}t_k|\} = \{1, |t_2|, \dots, |t_k|\}$, which is incompatible with the condition (ii). □

Corollary 2.19. *Let* $S = \{t_1, \dots, t_k\} \in \mathscr{P}_k$ *with* $t_1 = 1$*. If* $\mathrm{Out}(T) = 1$*, then* $\mathrm{Hol}(T, S) = 1$ *if all the following conditions are satisfied:*

(i) $t_2, \dots, t_k$ *have distinct orders;*
(ii) $M = \langle t_2, \dots, t_k \rangle$ *is a maximal subgroup of* T *such that* $Z(M) = 1$*;*
(iii) *for all* $2 \leqslant i \leqslant k$, $\{|t_i^{-1}t_1|, \dots, |t_i^{-1}t_k|\} \neq \{1, |t_2|, \dots, |t_k|\}$.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Proof. In view of Lemma 2.18, it suffices to show that the conditions (i) and (ii) imply that $\mathrm{Aut}(T, \{t_2, \ldots, t_k\}) = 1$. Suppose $\alpha \in \mathrm{Aut}(T, \{t_2, \ldots, t_k\})$. Then $\alpha \in C_{\mathrm{Aut}(T)}(t_i)$ for each i, as $t_2, \ldots, t_k$ have distinct orders. It follows that α centralises $\langle t_2, \ldots, t_k \rangle = M$ and so $\alpha \in C_{\mathrm{Aut}(T)}(M)$. Since $\mathrm{Out}(T) = 1$, this implies that $\alpha \in C_T(M) \leqslant N_T(M) = M$ since M is maximal, so $\alpha \in Z(M) = 1$. This completes the proof. □

Lemma 2.20. *Let $S_1 = \{t_1, \ldots, t_k\}$ and $S_2 = \{s_1, \ldots, s_k\}$ be elements in $\mathscr{P}_k$ such that $1 \in S_1 \cap S_2$ and $\mathrm{Hol}(T, S_j) = 1$ for each $j \in \{1, 2\}$. Then S_1 and S_2 are in distinct $\mathrm{Hol}(T)$-orbits if*

$$\{|t_i^{-1}t_1|, \ldots, |t_i^{-1}t_k|\} \neq \{|s_1|, \ldots, |s_k|\}$$

for any $i \in [k]$.

Proof. This follows immediately from Lemma 2.17. □

Remark 2.21. Let us briefly discuss the main computational techniques we will use to prove $r(W) \geqslant 2$ for some suitable T and k.

(i) Let S_1 and S_2 be k-element subsets of T containing 1, and let $O_j = \{|t| : t \in S_j\}$. Assume that $|O_j| = k$, $\langle S_j \rangle = T$ and

$$O_j \neq \{|x^{-1}t| : t \in S_j\}$$

for any $x \in S_j \setminus \{1\}$. Then $\mathrm{Hol}(T, S_j) = 1$ by Lemma 2.18, noting that the first two conditions imply that $\mathrm{Aut}(T, S_j \setminus \{1\}) = 1$. Combining Lemmas 2.16 and 2.20, we have $r(W) \geqslant 2$ if

$$O_2 \neq \{|x^{-1}t| : t \in S_1\}$$

for any $x \in S_1$. For suitable T and k, we can construct T with an appropriate permutation representation in Magma and implement this approach to find k-subsets S_1 and S_2 of T with these properties by random search. We will only need to use this method for $k \leqslant 11$.

(ii) In some cases where $\mathrm{Out}(T) = 1$, we will work with a centreless maximal subgroup M of T, rather than T itself. More precisely, if S_1 and S_2 are k-element subsets of M containing 1 and $O_j = \{|t| : t \in S_j\}$, then by Corollary 2.19, we have $\mathrm{Hol}(T, S_j) = 1$ if $|O_j| = k$, $\langle S_j \rangle = M$ and

$$O_j \neq \{|x^{-1}t| : t \in S_j\}$$

for any $S_j \setminus \{1\}$. Again, by Lemmas 2.16 and 2.20, we have $r(W) \geqslant 2$ if

$$O_2 \neq \{|x^{-1}t| : t \in S_1\}$$

for any $x \in S_1$. For example, if $T = \mathbb{M}$ is the monster sporadic group and $3 \leqslant k \leqslant 5$, then we will work with a maximal subgroup M of T isomorphic to $\mathrm{L}_2(71)$ (this case arises in the proofs of Lemma 4.1 and Proposition 4.8).

3. Probabilistic methods

In this section, we assume $G = T^k.(\mathrm{Out}(T) \times S_k)$ with $2 < k < |T|$. By Lemma 2.16, we have $r(G) \geqslant 2$ for $k = m$ if and only if $r(G) \geqslant 2$ for $k = |T| - m$, so we will assume $5 \leqslant k \leqslant |T|/2$ throughout this section (we will treat the cases where $k \in \{3, 4\}$ separately in Section 4).

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

In Section 3.1, we will estimate the probability $\mathrm{Pr}_k(T)$ that a random k-subset of T has nontrivial setwise stabiliser in $\mathrm{Hol}(T)$, noting that

$$\mathrm{Pr}_k(T) = \frac{|\{S \in \mathscr{P}_k : \mathrm{Hol}(T,S) \neq 1\}|}{\binom{|T|}{k}}. \tag{6}$$

As noted above, we have $r(G) \geqslant 2$ if and only if

$$\mathrm{Pr}_k(T) < 1 - \frac{|\mathrm{Hol}(T)|}{\binom{|T|}{k}}. \tag{7}$$

To establish this inequality, we will give upper bounds on $\mathrm{Pr}_k(T)$ in Section 3.1. In particular, we will show that $r(G) \geqslant 2$ if $4\log|T| < k \leqslant |T|/2$ (see Proposition 3.7).

Finally, to handle certain cases where k is small, we will consider the probability that a random pair of elements in Ω is not a base for G in Section 3.2, which is a widely used method in the study of base sizes.

3.1. Holomorph and subsets

We first consider $\mathrm{Pr}_k(T)$ defined as in (6). Let $\mathcal{F} = \{S \in \mathscr{P}_k : \mathrm{Hol}(T,S) \neq 1\}$ and suppose $S \in \mathcal{F}$. Then there exists $\sigma \in \mathrm{Hol}(T,S)$ of prime order. In other words, $S \in \mathrm{fix}(\sigma, \mathscr{P}_k)$, where

$$\mathrm{fix}(\sigma, \mathscr{P}_k) = \{S \in \mathscr{P}_k : \sigma \in \mathrm{Hol}(T,S)\}$$

is the set of fixed points of σ on $\mathscr{P}_k$. It follows that

$$|\mathcal{F}| = \left|\bigcup_{\sigma\in\mathcal{R}} \mathrm{fix}(\sigma,\mathscr{P}_k)\right| \leqslant \sum_{\sigma\in\mathcal{R}} |\mathrm{fix}(\sigma,\mathscr{P}_k)|,$$

where $\mathcal{R}$ is the set of elements of prime order in $\mathrm{Hol}(T)$. As discussed above, we have $r(G) \geqslant 2$ if and only if (7) holds. Thus, $r(G) \geqslant 2$ if

$$\sum_{\sigma\in\mathcal{R}} |\mathrm{fix}(\sigma,\mathscr{P}_k)| < \binom{|T|}{k} - |\mathrm{Hol}(T)|.$$

Moreover, since $5 \leqslant k \leqslant |T|/2$, we note that $|\mathrm{Hol}(T)| < \frac{1}{2}\binom{|T|}{k}$ by Lemma 2.9. This observation yields the following result.

Lemma 3.1. *We have $r(G) \geqslant 2$, and hence $b(G) = 2$, if*

$$\binom{|T|}{k} > 2\sum_{\sigma\in\mathcal{R}} |\mathrm{fix}(\sigma,\mathscr{P}_k)|. \tag{8}$$

In order to apply Lemma 3.1, we need to derive a suitable upper bound for the summation appearing on the right-hand side of (8).

Lemma 3.2. *Let $\sigma \in \mathrm{Hol}(T)$ be of prime order r with cycle shape $[r^m, 1^{|T|-mr}]$. Then*

$$|\mathrm{fix}(\sigma,\mathscr{P}_k)| = \sum_{u=0}^{\lfloor k/r\rfloor} \binom{m}{u}\binom{|T|-mr}{k-ru}.$$

Proof. This follows by noting that any subset fixed by σ is a union of some cycles comprising σ. □

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

If $\sigma \in \mathrm{Hol}(T)$ is an element as described in Lemma 3.2, then $|T| - mr$ is the number of elements in T fixed under σ. It follows that $|T| - mr \leqslant \mathrm{fix}(\mathrm{Hol}(T))$, where $\mathrm{fix}(\mathrm{Hol}(T))$ is the fixity of $\mathrm{Hol}(T)$ (the *fixity* of a permutation group is the maximum number of elements fixed by a nonidentity permutation). Recall that

$$h(T) = \max\{|C_T(x)| : 1 \neq x \in \mathrm{Aut}(T)\},$$

which has been determined in Theorem 2.12.

Lemma 3.3. *We have* $\mathrm{fix}(\mathrm{Hol}(T)) = h(T)$.

Proof. Let $\sigma \in \mathrm{Hol}(T)$ be such that it fixes at least one element in T. We may assume σ fixes $1 \in T$ by the transitivity of $\mathrm{Hol}(T)$. Thus, $\sigma \in \mathrm{Aut}(T)$ and hence $C_T(\sigma)$ is the set of fixed points of σ, which completes the proof. □

Corollary 3.4. *Let* $\sigma \in \mathrm{Hol}(T)$ *be of prime order r. Then*

$$|\mathrm{fix}(\sigma, \mathscr{P}_k)| \leqslant \sum_{u=0}^{\lfloor k/r \rfloor} \binom{|T|/r}{u} \binom{h(T)}{k - ru}.$$

The following bounds on binomial coefficients come from [56, Theorem 2.6], where e is the exponential constant.

Lemma 3.5. *Let* ℓ, m, n *be positive integers with* $n > m$. *Then*

$$e^{-\frac{1}{8\ell}} a(\ell, m, n) < \binom{n\ell}{m\ell} < a(\ell, m, n),$$

where

$$a(\ell, m, n) = \frac{1}{\sqrt{2\pi}} \ell^{-\frac{1}{2}} \left(\frac{n}{(n-m)m}\right)^{\frac{1}{2}} \left(\frac{n^n}{(n-m)^{n-m} m^m}\right)^{\ell}.$$

Corollary 3.6. *Suppose* $n = tm$ *for some integer* $t \geqslant 2$. *Then*

$$e^{-\frac{1}{8}} \left(\frac{t^2}{(t-1)n}\right)^{\frac{1}{2}} \left(\frac{t^t}{(t-1)^{t-1}}\right)^{\frac{n}{t}} < \sqrt{2\pi} \binom{n}{m} < \left(\frac{t^2}{(t-1)n}\right)^{\frac{1}{2}} \left(\frac{t^t}{(t-1)^{t-1}}\right)^{\frac{n}{t}}. \tag{9}$$

Proof. Put $\ell = 1$ and $m = n/t$ in Lemma 3.5. □

Proposition 3.7. *If* $4 \log |T| < k \leqslant |T|/2$, *then* $r(G) \geqslant 2$. *In particular,* $b(G) = 2$.

Proof. First, if $T = A_5$, then we construct the permutation group $\mathrm{Hol}(T)$ on T using the function `Holomorph` in Magma. Then we find two random k-subsets of T lying in distinct regular $\mathrm{Hol}(T)$-orbits by random search.

Hence, we may assume $|T| \geqslant 168$ and thus $4 \log |T| < |T|/4$. First, assume $|T|/4 \leqslant k \leqslant |T|/2$. By Corollary 3.4, we have

$$|\mathrm{fix}(\sigma, \mathscr{P}_k)| \leqslant \sum_{u=0}^{\lfloor k/r \rfloor} \binom{|T|/r}{u} \binom{h(T)}{\lfloor h(T)/2 \rfloor} \leqslant 2^{|T|/r} \binom{h(T)}{\lfloor h(T)/2 \rfloor} \leqslant 2^{|T|/2} \binom{h(T)}{\lfloor h(T)/2 \rfloor}$$

for every element $\sigma \in \mathrm{Hol}(T)$ of prime order. Hence, (8) holds if

$$\binom{|T|}{k} > |\mathrm{Hol}(T)| 2^{|T|/2+1} \binom{h(T)}{\lfloor h(T)/2 \rfloor}, \tag{10}$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

and it suffices to consider $k = |T|/4$. Now, we apply (9), which gives

$$\binom{|T|}{|T|/4} > \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{8}} \frac{4}{\sqrt{3|T|}} \left(\frac{4}{3^{3/4}}\right)^{|T|}$$

and

$$\binom{h(T)}{\lfloor h(T)/2 \rfloor} < \frac{1}{\sqrt{2\pi}} \cdot \sqrt{\frac{4}{h(T)}} \cdot 2^{h(T)} \leqslant \frac{1}{\sqrt{2\pi}} \cdot \sqrt{\frac{40}{|T|}} \cdot 2^{|T|/10}$$

as $h(T) \leqslant |T|/10$ by Corollary 2.14. Combining the inequalities above, we see that (10) holds for $k = |T|/4$ if

$$\frac{1}{\sqrt{2\pi}} e^{-\frac{1}{8}} \frac{4}{\sqrt{3|T|}} \left(\frac{4}{3^{3/4}}\right)^{|T|} > |\mathrm{Hol}(T)| \cdot 2^{|T|/2+1} \cdot \frac{1}{\sqrt{2\pi}} \cdot \sqrt{\frac{40}{|T|}} \cdot 2^{|T|/10}.$$

Finally, since $|\mathrm{Out}(T)| < |T|^{1/3}$ by Lemma 2.9, it suffices to show that

$$t_0^{|T|} > \sqrt{30} e^{\frac{1}{8}} |T|^{\frac{7}{3}}, \tag{11}$$

where

$$t_0 = 4 \cdot 3^{-\frac{3}{4}} \cdot 2^{-\frac{1}{2}-\frac{1}{10}} = 1.1577....$$

and it is easy to check that the inequality in (11) holds for all $|T| \geqslant 168$.

Now, assume $4 \log |T| < k < |T|/4$ and let $\sigma \in \mathrm{Hol}(T)$ be of prime order r. Observe that $ru \leqslant k < |T|/4$ for all $u \in \{0, \dots, \lfloor k/r \rfloor\}$, so

$$\begin{aligned}\sum_{u=0}^{\lfloor k/r \rfloor} \binom{|T|/r}{u}\binom{h(T)}{k-ru} &< \sum_{u=0}^{\lfloor k/r \rfloor} \binom{|T|/2}{u}\binom{h(T)}{k-ru} \\ &< \sum_{u=0}^{\lfloor k/r \rfloor} \binom{|T|/2}{ru}\binom{h(T)}{k-ru} \\ &< \binom{|T|/2+h(T)}{k},\end{aligned}$$

noting that the third inequality follows from the Vandermonde's identity. Thus, (8) holds if

$$\binom{|T|}{k} > 2|\mathrm{Hol}(T)| \binom{|T|/2+h(T)}{k}. \tag{12}$$

It is easy to see that (12) is equivalent to

$$\frac{|T|!}{(|T|-k)!} > 2|\mathrm{Hol}(T)| \frac{(|T|/2+h(T))!}{(|T|/2+h(T)-k)!}.$$

Now,

$$\frac{|T|-m}{|T|/2+h(T)-m} \geqslant \frac{|T|}{|T|/2+h(T)} =: t$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

for every $m \in \{0, \dots, k-1\}$ and thus (12) holds if $t^k > 2|\mathrm{Hol}(T)|$. By Corollary 2.14, we have $|T|/h(T) \geqslant 10$, and hence $t \geqslant 5/3$. Therefore, (12) holds if $(5/3)^k > |T|^{8/3}$ (by applying Lemma 2.9), which implies the desired result. □

Now, we turn to the cases where $5 \leqslant k \leqslant 4\log|T|$. We will give some sufficient conditions for $r(G) \geqslant 2$.

Lemma 3.8. *Suppose* $5 \leqslant k \leqslant 4\log|T|$. *Then* $r(G) \geqslant 2$, *and hence* $b(G) = 2$, *if*

$$\binom{|T|}{k} > 2|\mathrm{Hol}(T)| \sum_{u=0}^{\lfloor k/2 \rfloor} \binom{|T|/2}{u}\binom{h(T)}{k-2u}. \tag{13}$$

Proof. If $8\log|T| < h(T)$, then $k < h(T)/2$ and (8) follows via (13) and Corollary 3.4. By inspecting Table 1, we see that $8\log|T| \geqslant h(T)$ only if T is isomorphic to one of the following groups:

$$\mathrm{M}_{11},\ \mathrm{J}_1,\ {}^2B_2(8),\ \mathrm{L}_3(3),\ \mathrm{L}_2(q)\ (q \leqslant 167). \tag{14}$$

Assume T is one of the groups in (14), and suppose $\sigma \in \mathrm{Hol}(T)$ has prime order r. We claim that

$$|\mathrm{fix}(\sigma, \mathscr{P}_k)| < \sum_{u=0}^{\lfloor k/2 \rfloor} \binom{|T|/2}{u}\binom{h(T)}{k-2u}. \tag{15}$$

To see this, first assume σ is fixed-point-free on T. Here, $|\mathrm{fix}(\sigma, \mathscr{P}_k)| = 0$ if $r \nmid k$, and

$$|\mathrm{fix}(\sigma, \mathscr{P}_k)| = \binom{|T|/r}{k/r}$$

otherwise. In particular, the inequality in (15) holds. Now, assume σ has a fixed point on T. Since σ is conjugate to an element fixing the identity element in T, we may assume $\sigma \in \mathrm{Aut}(T)$. Then with the aid of Magma and Corollary 3.4, it is easy to check that (15) holds when T is one of the groups in (14).

We conclude that the proof is complete by combining (13) and (15) with Lemma 3.1. □

Lemma 3.9. *The inequality (13) holds if*

$$2^u u^u |T|^{k-u} > 2|\mathrm{Hol}(T)|\lfloor k/2 \rfloor k^{2u} e^{k+u} h(T)^{k-2u} \tag{16}$$

for every $u \in \{0, \dots, \lfloor k/2 \rfloor\}$, *where we define* $u^u = 1$ *if* $u = 0$.

Proof. First, observe that (13) holds if

$$\binom{|T|}{k} > 2|\mathrm{Hol}(T)|\lfloor k/2 \rfloor \binom{|T|/2}{u}\binom{h(T)}{k-2u} \tag{17}$$

for every $u \in \{0, \dots, \lfloor k/2 \rfloor\}$. Now,

$$\left(\frac{k}{k-2u}\right)^{k-2u} < e^{2u}$$

for all such u. Therefore, (17) follows by combining (16) and the well-known bounds on binomial coefficients

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

$$\frac{n^m}{m^m} < \binom{n}{m} < \frac{(en)^m}{m^m}$$

for any integers $n \geqslant m \geqslant 0$, where we define $m^m = 1$ if $m = 0$. □

We conclude this section by establishing two more technical lemmas, which will play a key role in Section 4.

Lemma 3.10. *Suppose* $|T| > 4080$ *and* $5 \leqslant k \leqslant 4\log|T|$. *Then (13) holds if there exists an integer* k_0 *such that* $5 \leqslant k_0 \leqslant k$,

$$|T|^{k_0} > |\mathrm{Hol}(T)|^2 k_0^{2+k_0} e^{3k_0} \tag{18}$$

and

$$h(T)^2 < k_0|T|. \tag{19}$$

Proof. We first prove that (13) holds if $k = k_0$. In view of Lemma 3.9, it suffices to verify the inequality in (16) for all $u \in \{0, \dots, \lfloor k/2 \rfloor\}$ and we will do this by induction. First assume $u = \lfloor k/2 \rfloor$ and note that (18) is equivalent to (16) if k is even. For k odd, we have $u = (k-1)/2$ and the inequality in (16) is as follows:

$$\left(\frac{|T|(k-1)}{k^2e^3}\right)^k |T| > \frac{k-1}{k^2e} \cdot 4|\mathrm{Hol}(T)|^2 \left(\frac{k-1}{2}\right)^2 h(T)^2. \tag{20}$$

In view of (19), we see that (20) holds if

$$\left(\frac{|T|}{ke^3}\right)^k \left(\frac{k-1}{k}\right)^{k-1} e > k^2|\mathrm{Hol}(T)|^2,$$

which is implied by (18) since $(\frac{k-1}{k})^{k-1} > e^{-1}$. Therefore, (16) holds for $u = \lfloor k/2 \rfloor$ and we have established the base case for the induction. Now, suppose (16) holds for $u = u_0$, where $1 \leqslant u_0 \leqslant \lfloor k/2 \rfloor$. It suffices to show that (16) holds for $u = u_0 - 1$. Here, the desired inequality holds if

$$2^{-1}|T| \cdot \frac{(u_0-1)^{u_0-1}}{u_0^{u_0}} > k^{-2}e^{-1} \cdot h(T)^2,$$

but this is implied by (19), noting that $(\frac{u_0-1}{u_0})^{u_0-1} > e^{-1}$ and $2u_0 \leqslant k$. In conclusion, if $k = k_0$, then (16) holds for all $u \in \{0, \dots, \lfloor k/2 \rfloor\}$ and thus (13) holds by Lemma 3.9.

Finally, we need to show that (13) holds when $k_0 < k$. By (19), we have $h(T)^2 < k_0|T| < k|T|$, and by arguing as above, it suffices to show that

$$|T|^k > |\mathrm{Hol}(T)|^2 k^{2+k} e^{3k}. \tag{21}$$

Since $|T| > 4080$ and $5 \leqslant k \leqslant 4\log|T|$, we get

$$|T| > 2e^4(4\log|T| + 1) \geqslant 2e^4(k+1) > \left(\frac{k+1}{k}\right)^{k+2} e^3(k+1).$$

Therefore, (21) holds for all $k_0 \leqslant k \leqslant 4\log|T|$ by induction on k, and the proof is complete. □

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Lemma 3.11. *Suppose* $5 \leqslant k \leqslant 4\log|T|$. *Then (13) holds if there exists an integer* k_0 *such that* $5 \leqslant k_0 \leqslant k$,

$$|T|^{k_0} > 2|\mathrm{Hol}(T)|\lfloor k_0/2\rfloor e^{k_0} h(T)^{k_0} \tag{22}$$

and

$$2h(T)^2 > (4\log|T|)^2 e|T|. \tag{23}$$

Proof. This is similar to the proof of Lemma 3.10, working with Lemma 3.9 to establish the inequality in (13). First, assume $k = k_0$ and note that (22) is equivalent to (16) with $u = 0$. We now use induction to show that (16) holds for all $u \in \{0, \ldots, \lfloor k/2\rfloor\}$. To do this, suppose (16) holds for $u = u_0$, where $0 \leqslant u_0 \leqslant \lfloor k/2\rfloor - 1$. Then (23) implies that

$$2|T|^{-1} \cdot \frac{(u_0+1)^{u_0+1}}{u_0^{u_0}} > k^2 e \cdot h(T)^{-2},$$

and thus (16) holds for $u = u_0 + 1$ and the result follows.

Finally, let us assume $k_0 < k$. It suffices to show that

$$|T|^k > 2|\mathrm{Hol}(T)|\lfloor k/2\rfloor e^k h(T)^k$$

for all $k_0 \leqslant k \leqslant 4\log|T|$. This is clear by induction on k, since we have

$$|T| > 2eh(T)$$

for every T by Corollary 2.14. □

3.2. Fixed point ratios

Now, we turn to another powerful probabilistic approach to study $b(G)$, where $G = T^k.(\mathrm{Out}(T) \times S_k)$, which was initially introduced by Liebeck and Shalev [45]. Here, we will estimate the probability $\mathbb{P}_k(T)$ that a random element in Ω is in a regular orbit of $G_D = D$, noting that $b(G) = 2$ if and only if $\mathbb{P}_k(T) > 0$. Equivalently,

$$\mathbb{P}_k(T) = \frac{r(G)|G|}{|T|^{2k-2}}$$

is the probability that a random pair of elements in Ω is a base for G.

Clearly, $\{\omega_1, \omega_2\} \subseteq \Omega$ is not a base for G if and only if there exists an element $x \in G_{\omega_1} \cap G_{\omega_2}$ of prime order. Now, the probability that $x \in G$ fixes a random element in Ω is given by the *fixed point ratio*

$$\mathrm{fpr}(x) = \frac{|\mathrm{fix}(x,\Omega)|}{|\Omega|} = \frac{|x^G \cap D|}{|x^G|},$$

where $\mathrm{fix}(x,\Omega)$ is the set of fixed points of x on Ω. Hence, we have

$$1 - \mathbb{P}_k(T) \leqslant \sum_{x \in R(G)} |x^G| \cdot \mathrm{fpr}(x)^2 = \sum_{x \in R(G)} \frac{|x^G \cap D|^2 |C_G(x)|}{|G|},$$

where $R(G)$ is the set of representatives for the G-conjugacy classes of elements in the stabiliser D in G which have prime order. We adopt the notation from [25] and define

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

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

and

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

It follows that

$$1 - \frac{r(G)|G|}{|T|^{2k-2}} = 1 - \mathbb{P}_k(T) \leqslant r_1(G) + r_2(G) + r_3(G), \tag{24}$$

which gives a lower bound on $r(G)$. In particular, $b(G) = 2$ if $r_1(G) + r_2(G) + r_3(G) < 1$. Thus, we need to bound each $r_i(G)$ above.

Lemma 3.12. *We have* $r_1(G) < (k!)^2 |T|^{8/3 - \lceil k/2 \rceil}$.

Proof. This is established in the proof of Theorem 1.5 in [25]. □

Lemma 3.13. *We have* $r_2(G) < (|T|/h(T))^{4-k}$.

Proof. Let $f_p(\mathrm{Aut}(T))$ be the number of conjugacy classes of elements of prime order in $\mathrm{Aut}(T)$. It follows from the proof of [25, Lemma 4.2] that

$$r_2(G) \leqslant |\mathrm{Out}(T)| f_p(\mathrm{Aut}(T)) \left(\frac{h(T)}{|T|}\right)^{k-2}.$$

Thus, it suffices to show that

$$|\mathrm{Out}(T)| f_p(\mathrm{Aut}(T)) < \left(\frac{|T|}{h(T)}\right)^2. \tag{25}$$

First, assume $T = A_n$ is an alternating group. Then as discussed in the proof of [25, Lemma 4.2], we have $f_p(\mathrm{Aut}(T)) < \frac{n^2}{2}$. This implies (25) since $h(T) = (n-2)!$ by Theorem 2.12.

Next, assume T is a sporadic group. Then $f_p(\mathrm{Aut}(T))$ can be read off from the character table of $\mathrm{Aut}(T)$ and it is easy to check that (25) holds in every case.

Finally, assume T is a simple group of Lie type over $\mathbb{F}_q$. Let $f(T)$ be the number of conjugacy classes in T. As noted in [28], we have $f_p(\mathrm{Aut}(T)) \leqslant |\mathrm{Out}(T)| f(T)$. Thus, it suffices to show that

$$|\mathrm{Out}(T)|^2 f(T) < \left(\frac{|T|}{h(T)}\right)^2. \tag{26}$$

We divide the proof into several cases.

Case 1. $T \neq \mathrm{L}_n^{\varepsilon}(q)$.

In this setting, [29, Theorem 1.2] implies that $f(T) < |T|/h(T)$, so in view of (26), it suffices to show that

$$h(T)|\mathrm{Out}(T)|^2 < |T|. \tag{27}$$

First, we assume $T \neq \mathrm{P}\Omega_8^+(q)$. Here, $|\mathrm{Out}(T)| \leqslant 8 \log q$ and by inspecting Table 1, one can see that $|T|/h(T) \geqslant q^3/2$. It is straightforward to check that if $q \geqslant 13$, then $128(\log q)^2 < q^3$, which implies that (27) holds for $q \geqslant 13$. Then there are only finitely many exceptional groups of Lie type to consider, and

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

in each case we can use the precise value of $h(T)$ in Table 1 to verify (27). Hence, we may assume $q \leqslant 11$ and T is a classical group. By our assumption, $T = \mathrm{PSp}_n(q)$, $\Omega_n(q)$, $\mathrm{P}\Omega_n^-(q)$, or $\mathrm{P}\Omega_n^+(q)$ with $n \geqslant 10$ in the latter case. In each case, we have $|T|/h(T) > q^{n-2}$ by inspecting Table 1, so if $n \geqslant 8$ we have

$$|\mathrm{Out}(T)|^2 \leqslant 64(\log q)^2 \leqslant q^6 \leqslant q^{n-2} < |T|/h(T)$$

and thus (27) holds. There are finitely many groups remaining and we can check that (27) holds in each case.

Now, assume $T = \mathrm{P}\Omega_8^+(q)$. Here, $|T|/h(T) > q^6$ and $|\mathrm{Out}(T)| \leqslant 24f \leqslant 24\log q$. This shows that (27) holds for $q \geqslant 4$ since we have $24^2(\log q)^2 < q^6$. If $q = 2$, then $|\mathrm{Out}(T)|^2 = 36 < 120 = |T|/h(T)$, while if $q = 3$, then $|\mathrm{Out}(T)|^2 = 576 < 1080 = |T|/h(T)$.

Case 2. $T = \mathrm{U}_n(q)$, $n \geqslant 3$.

In this case, [29, Theorem 1.2] implies that $f(T) < \frac{1}{2}|T|/h(T)$, except when $(n, q) = (3, 3)$ or $(4, 3)$. In the latter two cases, it is easy to check (26). In other cases, we have $|T|/h(T) > q^n$ by inspecting Table 1, so (26) holds if

$$|\mathrm{Out}(T)|^2 < 2q^n. \tag{28}$$

Notice that $|\mathrm{Out}(T)| \leqslant 2(q+1)\log q < q^2$ for $q \geqslant 7$, and for $q \in \{3, 5\}$ we still have $|\mathrm{Out}(T)| \leqslant 2(q+1) < q^2$. This implies that if $q \notin \{2, 4\}$ and $n \geqslant 4$, then we have

$$|\mathrm{Out}(T)|^2 < q^4 \leqslant q^n < 2q^n$$

and so (28) is satisfied. If $q = 2$, then $|\mathrm{Out}(T)| \leqslant 6$, so (28) holds if $n \geqslant 5$, and if $q = 4$, then $|\mathrm{Out}(T)| \leqslant 20$, and thus (28) holds for $n \geqslant 4$. It is straightforward to check (26) when $T = \mathrm{U}_4(2)$, where we have $f(T) = 20$.

Finally, assume $n = 3$, so $|\mathrm{Out}(T)| \leqslant 6\log q$. Here, (28) is satisfied for all $q > 4$ since $(6\log q)^2 < 2q^3$. By our assumption, the only remaining cases are $T = \mathrm{U}_3(3)$ with $f(T) = 14$ and $T = \mathrm{U}_3(4)$ with $f(T) = 22$, so the inequality in (26) holds.

Case 3. $T = \mathrm{L}_n(q)$.

Here, we assume $(n, q) \neq (2, 4), (2, 5), (2, 9), (3, 2), (4, 2)$ as noted in (4). If $n = 2$ and $q \in \{7, 11\}$, then an easy computation using Magma shows that (25) holds, and the result follows.

In each of the remaining cases, we have $|T|/h(T) > q^{n-1}$ by inspecting Table 1. Moreover, [27, Corollary 1.2] implies that $f_p(\mathrm{Aut}(T)) < 100|T|/h(T)$, so (25) holds if

$$100|\mathrm{Out}(T)| < q^{n-1}. \tag{29}$$

Since $|\mathrm{Out}(T)| \leqslant 2(q-1)\log q < q^2$ for all q, (29) holds if $n \geqslant 10$. Moreover, if $n \geqslant 4$, then (29) holds if $q > 100$, while for $q < 100$ it is easy to check that (29) still holds in each case, unless $q = 2$ and $n \leqslant 8$, or $n \in \{5, 6\}$ and $q \leqslant 4$, or $n = 4$ and $q \leqslant 9$. But in each of these cases, it is straightforward to check that (25) is satisfied, so to complete the proof we may assume $n \in \{2, 3\}$

Suppose $n = 3$, so $|\mathrm{Out}(T)| \leqslant 6\log q$, and (29) holds if $600\log q < q^2$. The latter holds if $q > 59$. In fact, by working with the precise value of $|\mathrm{Out}(T)|$ we see that (29) holds if $q > 25$. Finally, if $q \leqslant 25$, then we can check (25) using Magma.

To complete the proof, we may assume $T = \mathrm{L}_2(q)$, so $|\mathrm{Out}(T)| \leqslant 2\log q$ and $|T|/h(T) \geqslant (q+1)q^{1/2}/2$. Thus, (25) holds if

$$800\log q < (q+1)^2$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

since we have $f_p(\mathrm{Aut}(T)) < 100q$ by [27, Corollary 1.2]. In this way, we deduce that (25) holds if $q \geqslant 71$. And for $q < 71$, we can check that (25) holds with the aid of Magma. □

Lemma 3.14. *We have*

$$r_3(G) < \binom{k}{2}\left(\frac{1}{|T|} + \frac{|\mathrm{Out}(T)|h(T)^{k-3}}{|T|^{k-3}}\right) + \frac{k!}{|T|^{\frac{4}{3}}} + |T|^{-\frac{1}{3}}\left(2\binom{k}{3} + \frac{1}{2}\binom{k}{2}\binom{k-2}{2}\right).$$

Proof. First, let

$$R_4(G) = \{(\alpha, \ldots, \alpha)\pi \in R_3(G) : \pi = (1,2)\},$$
$$R_4(T) = \{\alpha \in \mathrm{Aut}(T) : (\alpha, \ldots, \alpha)\pi \in R_4(G)\}$$

as in the proof of [25, Theorem 1.5]. Set $P = S_k$ and

$$r_4(G) := |(1,2)^P| \sum_{\alpha \in R_4(T)} \frac{|\alpha^{\mathrm{Aut}(T)}|}{|T|}\left(\frac{|C_{\mathrm{Inn}(T)}(\alpha)|}{|T|}\right)^{k-3}.$$

Then we have

$$\begin{aligned} r_4(G) &= \binom{k}{2}\left(\frac{1}{|T|} + \sum_{\alpha \in R_4(T)\setminus\{1\}} \frac{|\alpha^{\mathrm{Aut}(T)}|}{|T|}\left(\frac{|C_{\mathrm{Inn}(T)}(\alpha)|}{|T|}\right)^{k-3}\right) \\ &\leqslant \binom{k}{2}\left(\frac{1}{|T|} + |\mathrm{Out}(T)|\left(\frac{h(T)}{|T|}\right)^{k-3}\right). \end{aligned} \tag{30}$$

As noted in the proof of [25, Theorem 1.5], we have

$$r_3(G) \leqslant r_4(G) + \sum_{\pi \in R\setminus\{(1,2)\}} \frac{|\pi^P|}{|T|^{k-r_\pi-\frac{5}{3}}}, \tag{31}$$

where R is a set of representatives for the conjugacy classes of elements of prime order in P and r_π is the number of $\langle\pi\rangle$-orbits in $[k]$. Without loss of generality, we may assume $(1,2) \in R$.

Let $x, y \in R$ be the representatives the P-classes $(1,2,3)^P$ and $(1,2)(3,4)^P$, respectively. Note that $r_x = r_y = k-2$ and $r_z \leqslant k-3$ for all $z \in R \setminus \{(1,2), x, y\}$. Then

$$\begin{aligned} \sum_{\pi \in R\setminus\{(1,2)\}} \frac{|\pi^P|}{|T|^{k-r_\pi-\frac{5}{3}}} &= \sum_{\pi \in R\setminus\{(1,2),x,y\}} \frac{|\pi^P|}{|T|^{k-r_\pi-\frac{5}{3}}} + |T|^{-\frac{1}{3}}\left(2\binom{k}{3} + \frac{1}{2}\binom{k}{2}\binom{k-2}{2}\right) \\ &< \frac{k!}{|T|^{\frac{4}{3}}} + |T|^{-\frac{1}{3}}\left(2\binom{k}{3} + \frac{1}{2}\binom{k}{2}\binom{k-2}{2}\right) \end{aligned}$$

and so the lemma follows by combining (30) and (31). □

Now, we define

$$Q_1(G) := (k!)^2|T|^{\frac{8}{3}-\frac{k}{2}-\frac{1}{2}\delta_{5,k}} + \frac{k!}{|T|^{\frac{4}{3}}} + \frac{k^4}{2|T|^{\frac{1}{3}}}, \tag{32}$$

where $\delta_{5,k} = 1$ if $k = 5$ and $\delta_{5,k} = 0$ otherwise, and

$$Q_2(G) := \left(\frac{|T|}{h(T)}\right)^{4-k} + \binom{k}{2}|\mathrm{Out}(T)|\left(\frac{|T|}{h(T)}\right)^{3-k}. \tag{33}$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

By Lemmas 3.12, 3.13 and 3.14, we have

$$r_1(G) + r_2(G) + r_3(G) < Q_1(G) + Q_2(G). \tag{34}$$

Lemma 3.15. *If $Q_1(G) + Q_2(G) < 1/2$ and $5 \leqslant k \leqslant 4\log|T|$, then $r(G) \geqslant 2$. In particular, $b(G) = 2$.*

Proof. By (24) and (34), we have

$$\frac{1}{2} > Q_1(G) + Q_2(G) > 1 - \frac{r(G)|G|}{|T|^{2k-2}} = 1 - \frac{r(G)|\mathrm{Out}(T)| \cdot k!}{|T|^{k-2}}.$$

It suffices to prove that

$$2|\mathrm{Out}(T)| \cdot k! \leqslant |T|^{k-2},$$

which is clear since $k \leqslant 4\log|T|$. □

4. Proofs of Theorems 1, 2 and 4

In this section, we will establish Theorems 1, 2 and 4. We will consider the following cases in turn:

(a) $P \in \{A_k, S_k\}$ and $k \in \{3, 4, |T| - 4, |T| - 3\}$;
(b) $P \in \{A_k, S_k\}$ and $k \in \{|T| - 2, |T| - 1\}$;
(c) $P = S_k$, $5 \leqslant k \leqslant |T|/2$ and $G = W$.

More specifically, we will prove that $r(G) \geqslant 2$ for every group in cases (a) and (c), with the exception of the two special cases arising in the statement of Theorem 2 (in both cases, $b(G) = 2$ and $r(G) = 1$). Then Lemma 2.16 shows that $b(G) = 2$ if $P \in \{A_k, S_k\}$ and $3 \leqslant k \leqslant |T| - 3$, as in part (ii) of Theorem 1, which also establishes Theorem 4. In particular, we deduce that $r(G) \geqslant 2$ if $P \notin \{A_k, S_k\}$ and $k \leqslant 32$, as noted in Remark 2.8.

As explained in Section 2, we will exclude the simple groups listed in (4), due to the existence of isomorphisms.

4.1. The groups with $k \in \{3, 4, |T| - 4, |T| - 3\}$

We start with case (a).

Lemma 4.1. *Suppose $k \in \{3, 4\}$, $P = S_k$ and T is a sporadic simple group. Then $r(G) \geqslant 2$.*

Proof. If $T \notin \{\mathrm{Ly}, \mathrm{Th}, \mathrm{J}_4, \mathbb{B}, \mathbb{M}\}$, then we can construct T as a permutation group in Magma using the function `AutomorphismGroupSimpleGroup`. Then the result follows by random search (see Remark 2.21(i)). If $T \in \{\mathrm{Ly}, \mathrm{Th}, \mathrm{J}_4, \mathbb{B}, \mathbb{M}\}$, then $|\mathrm{Out}(T)| = 1$. Let M be a maximal subgroup of T with

$$(T, M) \in \{(\mathrm{Ly}, G_2(5)),\ (\mathrm{Th}, \mathrm{AGL}_2(5)),\ (\mathrm{J}_4, \mathrm{M}_{22}.2),\ (\mathbb{B}, \mathrm{Fi}_{23}),\ (\mathbb{M}, \mathrm{L}_2(71))\}. \tag{35}$$

In view of Corollary 2.19, the result follows by random search as in Remark 2.21(ii). □

We define the following set of finite simple groups of Lie type:

$$\begin{aligned}\mathcal{C} := \{&{}^2B_2(8), {}^2B_2(32), G_2(3), G_2(4), {}^2F_4(2)', {}^3D_4(2), F_4(2), \mathrm{L}_2(7), \mathrm{L}_2(8),\\ &\mathrm{L}_2(11), \mathrm{L}_2(13), \mathrm{L}_2(16), \mathrm{L}_2(27), \mathrm{L}_2(32), \mathrm{L}_3^{\varepsilon}(3), \mathrm{L}_3^{\varepsilon}(4), \mathrm{U}_3(5), \mathrm{U}_3(8), \mathrm{L}_4^{\varepsilon}(3),\\ &\mathrm{PSp}_4(3), \mathrm{Sp}_4(4), \mathrm{L}_5^{\varepsilon}(2), \mathrm{U}_6(2), \mathrm{Sp}_6(2), \mathrm{PSp}_4(3), \mathrm{Sp}_8(2), \Omega_8^{\varepsilon}(2), \mathrm{P}\Omega_8^{+}(3)\}.\end{aligned}$$

Recall that an element x of a simple group of Lie type T defined over a field of characteristic p is regular semisimple if and only if $|C_T(x)|$ is indivisible by p.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Lemma 4.2. *Suppose $T \notin \mathcal{C}$ is a finite simple group of Lie type. Then T has at least eight regular semisimple* $\mathrm{Aut}(T)$*-classes.*

Proof. Suppose T is a Lie type group defined over $\mathbb{F}_q$, where $q = p^f$ for some prime p. We will work with a quasisimple group Q with $Q/Z(Q) = T$. Let m be the number of regular semisimple conjugacy classes in Q. Then T has at least $m|T|/|Q|$ regular semisimple T-classes, and thus T has at least eight regular semisimple $\mathrm{Aut}(T)$-classes if

$$m|T| \geqslant 8|\mathrm{Out}(T)||Q|. \tag{36}$$

First, assume Q is a simply connected quasisimple exceptional group. Then m has been computed by Lübeck [46], and one can see that (36) holds for every $T \notin \mathcal{C}$ by inspecting [46].

Next, assume $Q \in \{\mathrm{SL}_n^\varepsilon(q), \mathrm{Sp}_n(q)\}$, so m is given in [26]. The result now follows by inspecting [26]. For example, if $Q = \mathrm{SL}_2(q)$, then $|Q|/|T| = (2, q-1)$, $|\mathrm{Out}(T)| = (2, q-1)f$ and

$$m = q - 3 + (2, q)$$

by [26, Theorem 2.4]. Thus, (36) is valid if

$$q - 3 + (2, q) \geqslant 8(2, q-1)^2 f,$$

which holds for all $q > 81$. For the cases where $q \leqslant 81$ and $T \notin \mathcal{C}$, one can check using Magma that there are at least eight regular semisimple $\mathrm{Aut}(T)$-classes. We use an entirely similar argument to treat all the other cases and we omit the details.

To complete the proof, we assume $Q = \Omega_n^\varepsilon(q)$, so Q has index 2 in $\mathrm{SO}_n^\varepsilon(q)$. First, assume q is even. Here, $Q = T$ and every semisimple element in $\mathrm{SO}_n^\varepsilon(q)$ has odd order, and so lies in Q. This implies that m is at least the number of regular semisimple $\mathrm{SO}_n^\varepsilon(q)$-classes in $\mathrm{SO}_n^\varepsilon(q)$, which is computed in [26, Theorem 5.12], and the result follows by arguing as above.

Finally, assume $Q = \Omega_n^\varepsilon(q)$ and q is odd. Write $d = \lceil n/2 \rceil - 1$. Let $A \in \mathrm{GL}_d(q)$ be of order $q^d - 1$ and let

$$x = \begin{pmatrix} A & & \\ & (A^{-1})^T & \\ & & I_{n-2d} \end{pmatrix}$$

with respect to a standard basis (see [39, Proposition 2.5.3]). Then $x \in \mathrm{SO}_n^\varepsilon(q)$, so $y := x^2 \in \Omega_n^\varepsilon(q)$, noting that

$$y = \begin{pmatrix} B & & \\ & (B^{-1})^T & \\ & & I_{n-2d} \end{pmatrix},$$

where $B = A^2$. Let μ be an eigenvalue of B of order $(q^d - 1)/2$ in the algebraic closure K of $\mathbb{F}_q$. Then it is easy to show that $\mu \neq \mu^{\pm q^t}$ for any $1 \leqslant t \leqslant d-1$, and the set of eigenvalues of y is

$$\{\mu, \mu^q, \ldots, \mu^{q^{d-1}}, \mu^{-1}, \mu^{-q}, \ldots, \mu^{-q^{d-1}}, 1\},$$

where 1 has multiplicity $n - 2d \in \{1, 2\}$ and any other eigenvalue has multiplicity 1. It follows that y^i is regular semisimple if $(i, (q^d - 1)/2) = 1$. This gives at least

$$\frac{\phi\big((q^d - 1)/2\big)}{2d}$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

regular semisimple $\mathrm{GO}_n^\varepsilon(q)$-classes in Q, where ϕ is the Euler's totient function (note that two elements are not conjugate in $\mathrm{GL}_n(q)$ if they have distinct sets of eigenvalues). By arguing as above, T has at least eight regular semisimple $\mathrm{Aut}(T)$-classes if

$$\phi\Big((q^d-1)/2\Big) \geqslant 32d \cdot |\mathrm{Aut}(T) : \mathrm{PGO}_n^\varepsilon(q)|, \tag{37}$$

noting that $|\mathrm{Aut}(T) : \mathrm{PGO}_n^\varepsilon(q)| \leqslant f \leqslant \log q$ if $d \neq 3$, while $|\mathrm{Aut}(T) : \mathrm{PGO}_n^\varepsilon(q)| \leqslant 3f \leqslant 3\log q$ if $d = 3$. It is easy to check that (37) holds unless

$$(d,q) \in \{(6,3),(5,3),(4,3),(4,5),(4,7),(3,3),(3,5),(3,7)\}.$$

For these remaining cases, one can use Magma to obtain m and so (36) holds unless $Q \in \{\Omega_{10}^-(3), \Omega_8^+(5), \Omega_8^\varepsilon(3), \Omega_7(3)\}$, where we can directly check that there are at least eight regular semisimple $\mathrm{Aut}(T)$-classes in T with the aid of Magma. □

We remark that $\mathrm{P}\Omega_8^+(3)$ has exactly eight regular semisimple $\mathrm{Aut}(T)$-classes in T. If $T \in \mathcal{C}$ and $T \neq \mathrm{P}\Omega_8^+(3)$, then the number of $\mathrm{Aut}(T)$-classes of regular semisimple elements in T is strictly less than 8, which can be checked using Magma. We include $\mathrm{P}\Omega_8^+(3)$ in $\mathcal{C}$ in view of Theorem 2.11, so if $T \notin \mathcal{C}$, then T is invariably generated by a pair of regular semisimple elements of distinct orders.

Lemma 4.3. *Suppose $k = 3$, $P = S_k$ and $T \notin \mathcal{C}$ is a simple group of Lie type. Then $r(G) \geqslant 2$.*

Proof. Let x and y be as described in Theorem 2.11. Let z_1 and z_2 be semisimple elements in T lying in distinct $\mathrm{Aut}(T)$-classes and

$$z_1, z_2 \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)}.$$

Note that the existence of z_1 and z_2 follows from Lemma 4.2. Then by applying [32, Theorem 2], which asserts that the product of any two regular semisimple T-classes contains all semisimple elements in T, there exist g_i and h_i in T such that $z_i = x^{g_i} y^{h_i}$, and without loss of generality we may assume $g_i = 1$, so $z_i = xy^{h_i}$. It is easy to see that $\mathrm{Hol}(T, \{1, x^{-1}, y^{h_i}\}) = 1$, and so $b(G) = 2$. By Lemma 2.16, it suffices to show that $S_1 = \{1, x^{-1}, y^{h_1}\}$ and $S_2 = \{1, x^{-1}, y^{h_2}\}$ are in distinct $\mathrm{Hol}(T)$-orbits. Suppose $S_1^{g\alpha} = S_2$ for some $g\alpha \in \mathrm{Hol}(T)$, and note that $g \in S_1$ by Lemma 2.17. If $g = 1$, then $(x^{-1})^\alpha = x^{-1}$ and $(y^{h_1})^\alpha = y^{h_2}$. However, this implies that

$$z_1^\alpha = (xy^{h_1})^\alpha = xy^{h_2} = z_2,$$

which is incompatible with our assumption $z_1^{\mathrm{Aut}(T)} \neq z_2^{\mathrm{Aut}(T)}$. If $g = x^{-1}$, then $(y^{h_1})^g = xy^{h_1} = z_1$, which is not $\mathrm{Aut}(T)$-conjugate to any element in S_2, a contradiction. Finally, if $g = y^{h_1}$, then $(x^{-1})^g = y^{-h_1}x^{-1} = z_1^{-1}$. With the same reason, this is impossible. Therefore, there is no $g\alpha \in \mathrm{Hol}(T)$ such that $S_1^{g\alpha} = S_2$, which completes the proof. □

Lemma 4.4. *Suppose $k = 4$, $P = S_k$ and $T \notin \mathcal{C}$ is a simple group of Lie type. Then $r(G) \geqslant 2$.*

Proof. Let x and y be as in Theorem 2.11. By [32, Theorem 2], every semisimple element in T lies in $x^T y^T$, so we may assume that

$$x^{-1}y \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)}. \tag{38}$$

Additionally, using Lemma 4.2, let z_0 be a regular semisimple element such that

$$z_0 \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)} \cup (x^{-1}y)^{\mathrm{Aut}(T)} \cup (y^{-1}x)^{\mathrm{Aut}(T)}. \tag{39}$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Again, [32, Theorem 2] implies that $x^T z_0^T$ contains all semisimple elements in T. Thus, by Lemma 4.2, there exists $z \in z_0^T$ such that

$$z^{-1}x \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)} \cup (x^{-1}y)^{\mathrm{Aut}(T)} \cup (y^{-1}x)^{\mathrm{Aut}(T)}. \tag{40}$$

Set $S_1 = \{1, x, y, z\}$ and suppose $g\alpha \in \mathrm{Hol}(T, S_1)$. If $g = 1$, then $\alpha \in \mathrm{Aut}(T, S_1) = 1$ as $\langle x, y\rangle = T$ and x, y, z are in distinct $\mathrm{Aut}(T)$-classes. If $g = x$, then $x^{-1}y \in x^{-1}S_1 = S_1^{\alpha^{-1}}$, which is incompatible with either (38) or (39). The case where $g = y$ can be eliminated using the same argument. If $g = z$, then $z^{-1}S_1 = S_1^{\alpha^{-1}}$, and by using (39) and (40), both z^{-1} and $z^{-1}x$ are $\mathrm{Aut}(T)$-conjugate to z, which yields $z^{-1} = z^\alpha = z^{-1}x$, a contradiction. Thus, we have $b(G) = 2$.

Similarly, Lemma 4.2 implies that there exists a regular semisimple element $w \in T$ such that $w \neq z$,

$$w \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)} \cup (x^{-1}y)^{\mathrm{Aut}(T)} \cup (y^{-1}x)^{\mathrm{Aut}(T)}$$

and

$$w^{-1}x \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)} \cup (x^{-1}y)^{\mathrm{Aut}(T)} \cup (y^{-1}x)^{\mathrm{Aut}(T)}.$$

Set $S_2 = \{1, x, y, w\}$. By arguing as above, we have $\mathrm{Hol}(T, S_2) = 1$ and it suffices to show that S_1 and S_2 are in distinct $\mathrm{Hol}(T)$-orbits. Suppose $S_1^{g\alpha} = S_2$, and note that $g \in S_1$ by Lemma 2.17. If $g = 1$, then $x^\alpha = x$ and $y^\alpha = y$, which implies that $\alpha = 1$. However, this is incompatible with $z \neq w$. If $g = x$, then

$$1^g = x^{-1},\ y^g = x^{-1}y \text{ and } z^g = x^{-1}z.$$

Thus, one of the above is $\mathrm{Aut}(T)$-conjugate to w, which has to be $z^g = x^{-1}z$ by our assumption. However, this gives a contradiction since $y^g = x^{-1}y$ is not $\mathrm{Aut}(T)$-conjugate to x or y by (38). The case where $g = y$ can be eliminated similarly. Finally, if $g = z$, then

$$x^g = z^{-1}x,\ y^g = z^{-1}y \text{ and } 1^g = z^{-1}.$$

Once again, the only possibility is $x^{g\alpha} = w$ by (40). But this leaves $(z^{-1})^\alpha = 1^{g\alpha} \in \{x, y\}$, which is incompatible with (39). □

We can now establish Theorems 1 and 2 for $k \in \{3, 4, |T| - 4, |T| - 3\}$.

Proposition 4.5. *If $k \in \{3, 4, |T| - 4, |T| - 3\}$, then $r(G) \geqslant 1$, with equality if and only if $T = A_5$, $k \in \{3, 57\}$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.*

Proof. By Proposition 2.7, we may assume $P \in \{A_k, S_k\}$. First, assume $k \in \{3, 4\}$ and $P = S_k$. The groups where T is sporadic have been treated in Lemma 4.1. If $T \notin \mathcal{C}$ is Lie type, then by Lemmas 4.3 and 4.4, we have $r(G) \geqslant 2$ as desired. The cases where $T \in \mathcal{C}$ can be handled by random search (see Remark 2.21(i)).

Thus, to complete the proof for $k \in \{3, 4\}$ and $P = S_k$ we may assume $T = A_n$ is an alternating group. First, assume $k = 3$ and $T = A_5$. One can check using Magma that $\mathrm{Hol}(T)$ has a unique regular orbit on $\mathcal{P}_k$, so $r(G) = 1$ if $G = W = A_5^3.(2 \times S_3)$. With the aid of Magma, one can show that $r(G) \geqslant 2$ if $G < W$. Here, we obtain the permutation group G in Magma by accessing the primitive group database, noting that $|\Omega| = |A_5|^2 = 3600$.

Next, assume $P = S_3$ and $T = A_n$ with $n \geqslant 6$. The cases where $n \leqslant 8$ can be easily handled using Magma (see Remark 2.21(i)). Now, assume $n \geqslant 9$, so by [48], there exist $x_1, y_1 \in T$ such that $|x_1| = 2$, $|y_1| = 3$ and $\langle x_1, y_1\rangle = T$. Note that if $|x_1y_1| = 2$ or 3, then $\langle x_1, y_1\rangle = S_3$ or A_4 respectively, so we must have $|x_1y_1| \geqslant 4$. Hence, $\mathrm{Hol}(T, \{1, x_1, y_1\}) = 1$ by Lemma 2.18, and thus $b(G) = 2$. Let $x_2 = (1, 2, \ldots, n)$ if n is odd, while $x_2 = (1, 2)(3, \ldots, n)$ if n is even, and let $y_2 = (1, 2, 3)x_2^{-1}$. Then $\langle x_2, y_2\rangle = T$ and Lemma 2.18 implies that $\mathrm{Hol}(T, \{1, x_2, y_2\}) = 1$, so we have $r(G) \geqslant 2$ by Lemma 2.20.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Now, assume $P = S_4$ and $T = A_n$. The cases where $n \leqslant 11$ can be handled using Magma as noted in Remark 2.21(i). Assume $n \geqslant 12$, and let $x = (1,2)(3,4)$. Let C_1 and C_2 be the set of involutions moving 8 and 12 points in $[n]$, respectively. Note that there exist $y_1 \in C_1$ and $y_2 \in C_2$ such that $xy_i \neq y_i x$. Moreover, by [7, Theorem 1.2], there exist z_1 and z_2 such that

$$T = \langle x, z_1 \rangle = \langle y_1, z_1 \rangle = \langle x, z_2 \rangle = \langle y_2, z_2 \rangle.$$

In particular, $2 \notin \{|z_i|, |xz_i|, |y_i z_i|\}$. Set $S_1 = \{1, x, y_1, z_1\}$ and $S_2 = \{1, x, y_2, z_2\}$. We first prove that $\mathrm{Hol}(T, S_i) = 1$. Suppose $g\alpha \in \mathrm{Hol}(T, S_i)$. If $g = 1$, then $\alpha \in \mathrm{Aut}(T, S) = 1$ since $\langle x, z_i \rangle = T$ and x, y_i, z_i are in distinct $\mathrm{Aut}(T)$-classes. If $g = x$, then $2 \notin \{|y_i^g|, |z_i^g|\} = \{|xy_i|, |xz_i|\}$, which is impossible. The cases where $g \in \{y_i, z_i\}$ can be eliminated similarly. This implies that $b(G) = 2$. By applying Lemma 2.17, one can show that S_1 and S_2 are in distinct $\mathrm{Hol}(T)$-orbits.

Therefore, we have $r(G) \geqslant 1$ if $k \in \{3, 4\}$, with equality if and only if $G = A_5^3.(2 \times S_3)$. By Lemma 2.16, it suffices to consider the case where $T = A_5$ and $k = |A_5| - 3 = 57$. Note that $r(G) = 1$ if $G = W = A_5^{57}.(2 \times S_{57})$, and G has at least $|W : G|$ regular suborbits if $G < W$. □

4.2. The groups with $P \in \{A_k, S_k\}$ and $k \in \{|T| - 2, |T| - 1\}$

Lemma 4.6. *Suppose $m \in \{2, 3\}$. Then there exist $S_1, S_2 \subseteq T^{\#}$ such that $|S_i| = m$, $\mathrm{Aut}(T, S_i) = 1$ and $S_1^{\mathrm{Aut}(T)} \neq S_2^{\mathrm{Aut}(T)}$.*

Proof. First, observe that if $S_1 \cup \{1\}$ and $S_2 \cup \{1\}$ are in distinct regular $\mathrm{Hol}(T)$-orbits, then all conditions in the statement of the lemma are satisfied. Hence, the result follows from Lemma 2.16 and Proposition 4.5, except when $T = A_5$ and $m = 2$. In the latter case, we can verify the lemma using Magma. □

Proposition 4.7. *Assume $k = |T| - 1$ or $|T| - 2$.*

(i) *If G contains S_k, then $b(G) = 3$.*
(ii) *If G does not contain S_k, then $r(G) \geqslant 2$.*

Proof. Recall that $b(G) \in \{2, 3\}$ by Theorem 2.3(iii). First, assume G contains S_k. It suffices to show that $b(G) = 3$ if $G = T^k{:}S_k$. Suppose $\{D, D(\varphi_{t_1}, \ldots, \varphi_{t_k})\}$ is a base for G. If $t_i = t_j$ for some $i \neq j$, then $(i, j) \in G$ stabilises D and $D(\varphi_{t_1}, \ldots, \varphi_{t_k})$ pointwise. Therefore, $t_1, \ldots, t_k$ are distinct. Let $S = T \setminus \{t_1, \ldots, t_k\}$, so $|S| \in \{1, 2\}$. Without loss of generality, we may also assume $1 \in S$. Thus, there exists $1 \neq t \in T$ such that $S^{\varphi_t} = S$, and hence $\varphi_t \in \mathrm{Hol}(T, T \setminus S)$, which is incompatible with Lemma 2.15.

Now, we turn to the case where G does not contain S_k. Recall that $T^k{:}A_k \leqslant G$ by Corollary 2.6. From Lemma 4.6, there are subsets $S_1, S_2 \subseteq T^{\#}$ of size $|T| - k + 1$ lying in distinct regular $\mathrm{Aut}(T)$-orbits. Write $T^{\#} \setminus S_i = \{t_{i,1}, \ldots, t_{i,k-2}\}$, and consider $\Delta_i = \{D, D(\varphi_{t_{i,1}}, \ldots, \varphi_{t_{i,k}})\}$, where $t_{i,k-1} = t_{i,k} = 1$. Suppose $x = (\alpha, \ldots, \alpha)\pi \in G_{(\Delta_i)}$. By Lemma 2.1, $t_{i,j}^{\alpha} = t_{i,j^{\pi}}$ for all j. It follows that $\alpha \in \mathrm{Aut}(T, S_i)$ and thus $\alpha = 1$. Hence, $x = \pi \in \langle (k-1, k) \rangle$, and so $x = 1$ since G does not contain S_k. This shows that $b(G) = 2$. Finally, if Δ_1 and Δ_2 are in the same G_D-orbit, then

$$D(\varphi_{t_{1,1}}, \ldots, \varphi_{t_{1,k}})^{(\alpha, \ldots, \alpha)\pi} = D(\varphi_{t_{2,1}}, \ldots, \varphi_{t_{2,k}})$$

for some $\alpha \in \mathrm{Aut}(T)$ and $\pi \in S_k$. This implies that $S_1^{\alpha} = S_2$, which is incompatible with our assumption. Therefore, $r(G) \geqslant 2$ and the proof is complete. □

4.3. The groups with $P = S_k$, $5 \leqslant k \leqslant |T|/2$ and $G = W$

Finally, let us turn to case (c) mentioned in the beginning of this section. Note that if $r(G) \geqslant 2$ in every case, then the proofs of Theorems 1 and 2 are complete by combining Corollary 2.4 with Propositions 2.7, 4.5 and 4.7. By Proposition 3.7, it suffices to consider the cases where $5 \leqslant k \leqslant 4 \log |T|$. Recall that $r(G) \geqslant 2$ if (13) holds or $Q_1(G) + Q_2(G) < 1/2$ (see Lemmas 3.8 and 3.15).

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Proposition 4.8. *The conclusions to Theorems 1 and 2 hold when T is a sporadic simple group.*

Proof. As noted above, we may assume $5 \leqslant k \leqslant 4\log|T|$. With the aid of Magma, it is easy to check that (13) holds for all k in this range unless T is one of the following groups:

$$\mathrm{Suz}, \mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Fi}_{22}, \mathrm{Fi}_{23}, \mathrm{Fi}'_{24}, \mathbb{B}, \mathbb{M}.$$

Assume $T \in \{\mathrm{Suz}, \mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Fi}_{22}, \mathrm{Fi}_{23}, \mathrm{Fi}'_{24}\}$. Here, we can construct T as a permutation group in Magma using the function `AutomorphismGroupSimpleGroup`, and we can then check that (13) holds for $9 \leqslant k \leqslant 4\log|T|$. The cases where $5 \leqslant k \leqslant 8$ can be handled by random search using Magma (see Remark 2.21(i)).

Finally, if $T \in \{\mathbb{B}, \mathbb{M}\}$, then (13) holds unless $k = 5$ or $(T, k) = (\mathbb{B}, 6)$. In each case, we can verify that $r(G) \geqslant 2$ by random search as described in Remark 2.21(ii), with the same centreless maximal subgroup M of T chosen in (35). □

Proposition 4.9. *The conclusions to Theorems 1 and 2 hold when $T = A_n$ is an alternating group.*

Proof. Once again, we may assume $5 \leqslant k \leqslant 4\log|T|$. The cases where $n \in \{5, 6\}$ can be easily handled using Magma, so we also assume $n \geqslant 7$. First, assume $n \leqslant k \leqslant 4\log|T|$. With the aid of Magma, it is easy to check (13) holds for all $7 \leqslant n \leqslant 29$. Note that $h(T) = (n-2)!$ and thus (23) holds. By Lemma 3.11, it suffices to establish the inequality in (22) for $k_0 = n$. Thus, we only need to show that

$$\left(\frac{n(n-1)}{2e}\right)^n > \frac{n(n!)^2}{2},$$

which holds for all $n \geqslant 30$.

Finally, let us assume $5 \leqslant k < n$ and define $Q_1(G)$ and $Q_2(G)$ as in (32) and (33), respectively. Then

$$Q_1(G) = (k!)^2|T|^{\frac{8}{3}-\frac{k}{2}-\frac{1}{2}\delta_{5,k}} + \frac{k!}{|T|^{\frac{4}{3}}} + \frac{k^4}{2|T|^{\frac{1}{3}}} < (6!)^2\left(\frac{2}{n!}\right)^{\frac{1}{3}} + \frac{2^{\frac{4}{3}}}{(n!)^{\frac{1}{3}}} + \frac{2^{\frac{1}{3}}n^4}{2(n!)^{\frac{1}{3}}}$$

and

$$Q_2(G) = \left(\frac{|T|}{h(T)}\right)^{4-k} + \binom{k}{2}|\mathrm{Out}(T)|\left(\frac{|T|}{h(T)}\right)^{3-k} < \frac{2}{n(n-1)} + 20\left(\frac{2}{n(n-1)}\right)^2.$$

Given these bounds, it is easy to check that $Q_1(G) + Q_2(G) < 1/2$ for all $n \geqslant 21$. Finally, for the cases where $7 \leqslant n \leqslant 20$ and $5 \leqslant k < n$, one can use Magma to check that either (13) holds, or $Q_1(G)+Q_2(G) < 1/2$, or $\mathrm{Hol}(T)$ has at least two regular orbits on $\mathscr{P}_k$ (for the latter, we use the random search approach as in Remark 2.21(i)). □

To complete the proofs of Theorems 1 and 2, we may assume T is a finite simple group of Lie type. First, we consider some low rank groups, where $h(T)$ is small and Lemma 3.10 can be applied.

Lemma 4.10. *Suppose $T = \mathrm{L}_2(q)$ and $5 \leqslant k \leqslant 4\log|T|$. Then $r(G) \geqslant 2$.*

Proof. If $|T| \leqslant 4080$, then $q \leqslant 13$ and one can check the result using Magma. More precisely, we first check (13), and if it fails, then we construct the permutation group $\mathrm{Hol}(T)$ on T using the function `Holomorph` and use random search to find two k-subsets S_1 and S_2 of T lying in distinct regular $\mathrm{Hol}(T)$-orbits (this is a viable approach since $|T|$ is small).

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Thus, we may assume $q \geqslant 16$. First, assume $k \geqslant 6$ and set $k_0 = 6$. For $q \leqslant 733$, one can check (13) using Magma. Assume $q > 733$, and note that $h(T) \leqslant q^{1/2}(q-1)$ by Theorem 2.12, so (19) holds. Moreover, as $|\mathrm{Out}(T)| \leqslant 2\log q$, we can check that (18) holds if

$$q^2(q^2-1)^2 > 16(\log q)^2 6^8 e^{18},$$

which holds true for all $q > 733$. Now, apply Lemma 3.10.

To complete the proof, we assume $k = 5$. By Lemma 3.9, $r(G) \geqslant 2$ if (16) holds for every $u \in \{0,1,2\}$. If $u = 2$, then (16) holds if

$$q^{1/2}(q+1) > 5^4 e^7 \log q,$$

which holds for all $q > 48449$. With the same method, one can check that (16) holds for $u \in \{0,1\}$ if $q > 48449$. With the aid of Magma, we see that (13) holds for all $16 \leqslant q \leqslant 48449$, unless $q \in \{16, 25, 49, 81\}$, and the remaining cases can be handled using Magma and random search, utilising the method in Remark 2.21(i). □

Lemma 4.11. *Suppose* $T \in \{\mathrm{L}_3^{\varepsilon}(q), {}^2B_2(q), {}^2G_2(q)\}$ *and* $5 \leqslant k \leqslant 4\log|T|$. *Then* $r(G) \geqslant 2$.

Proof. Note that $|T| > 4080$ and $h(T)^2 < 5|T|$ by Theorem 2.12. Thus, in view of Lemma 3.10, we only need to prove (18) for $k_0 = 5$. Assume $T = \mathrm{L}_3^{\varepsilon}(q)$, so $|T| \geqslant q^3(q^2-1)(q^3-1)/3$ and $|\mathrm{Out}(T)| \leqslant 6\log q$. Thus, (18) holds if

$$q^3(q^2-1)(q^3-1) > 3(6\log q)^2 5^7 e^{15},$$

which is true for all $q > 73$. By applying the precise values of $h(T)$ and $|\mathrm{Out}(T)|$, we see that (13) holds unless $\varepsilon = -$, $k = 5$ and $q \in \{3,5,8\}$, or $\varepsilon = +$ and

$$(q,k) \in \{(3,5),(3,6),(4,5),(13,5)\},$$

all of which cases can be handled easily by random search as discussed in Remark 2.21(i). We can apply the same method to the cases where $T = {}^2B_2(q)$ or ${}^2G_2(q)$, where (18) holds if $T \neq {}^2G_2(27)$, ${}^2B_2(8)$, ${}^2B_2(32)$ or ${}^2B_2(128)$ (we are excluding the group ${}^2G_2(3)'$ as noted in (4)). In the remaining four cases, one can check (13) directly. □

Proposition 4.12. *The conclusions to Theorems 1 and 2 hold when T is an exceptional group of Lie type.*

Proof. Once again, by the previous results, we may assume $5 \leqslant k \leqslant 4\log|T|$. In view of Lemma 4.11, we may also assume $T \neq {}^2B_2(q)$ or ${}^2G_2(q)$. Note that

$$\frac{|T|}{h(T)} > 10|\mathrm{Out}(T)| \geqslant 10$$

and $|T| > \frac{1}{6}q^d$, where d is as defined in Lemma 2.10.

First, assume $5 \leqslant k \leqslant 8$. Then

$$Q_2(G) < \frac{h(T)}{|T|} + 10|\mathrm{Out}(T)| \cdot \frac{h(T)^2}{|T|^2} < \frac{1}{10} + \frac{1}{10} = \frac{1}{5}$$

and

$$Q_1(G) < \frac{(6!)^2}{|T|^{\frac{1}{3}}} + \frac{8!}{|T|^{\frac{4}{3}}} + \frac{8^4}{2|T|^{\frac{1}{3}}} < \frac{6^{\frac{1}{3}}(6!)^2}{q^{\frac{d}{3}}} + \frac{6^{\frac{4}{3}}\cdot 8!}{q^{\frac{4d}{3}}} + \frac{6^{\frac{1}{3}}8^4}{2q^{\frac{d}{3}}} < \frac{3}{10}$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

unless $T \in \{{}^2F_4(2)', {}^3D_4(2), {}^3D_4(3), {}^3D_4(4), F_4(2)\}$ or $T = G_2(q)$ for $q \leqslant 23$. In this cases, one can check (13) with the aid of Magma unless $T = {}^3D_4(q)$ and $k = 5$, or $T = F_4(2)$ and $k \in \{5, 6\}$. In the latter cases, we can do random search using Magma as in Remark 2.21(i).

To complete the proof, we assume $9 \leqslant k \leqslant 4 \log |T|$. The groups with $q = 2$ can be handled by verifying (13) directly, so we now assume $q \geqslant 3$. We first prove (22) for $k_0 = 9$. By inspecting Table 1, we have

$$2^9 \left(\frac{|T|}{h(T)} \right)^9 > |T|^2 q^{22}. \tag{41}$$

For example, if $T = E_8(q)$, then

$$\frac{|T|}{h(T)} = \frac{(q^{30}-1)(q^{24}-1)(q^{20}-1)}{(q^{10}-1)(q^6-1)} > \frac{1}{2} q^{58}$$

and $|T| < q^{248}$ by Lemma 2.10, which implies (41). Since $|\mathrm{Out}(T)| \leqslant 6 \log q$, it follows that (22) holds for $k_0 = 9$ if

$$q^{22} > 48 \log q \cdot (2e)^9$$

and one can check that this inequality holds for $q \geqslant 3$. By Lemma 3.11, it suffices to prove (23). Here, we only give a proof for the case where $T = G_2(q)$, as all the other cases are very similar. First, note that $|T| = q^6(q^6-1)(q^2-1) < q^{14}$ and $h(T) = q^6(q^2-1) > \frac{1}{2} q^8$. Then (23) holds if

$$q^2 > 56^2 (\log q)^2 e,$$

which holds true for all $q > 907$. One can also check that (23) holds for all $601 < q \leqslant 907$. If $q \leqslant 601$, then we can use the precise values of $|T|$, $h(T)$ and $|\mathrm{Out}(T)|$ to check (13) for all $9 \leqslant k \leqslant 4 \log |T|$. This completes the proof. □

Lemma 4.13. *Suppose* $T = \mathrm{L}_4^{\varepsilon}(q)$ *and* $5 \leqslant k \leqslant 4 \log |T|$. *Then* $r(G) \geqslant 2$.

Proof. Recall that $h(T) = (2, q-\varepsilon)|\mathrm{PGSp}_4(q)|/(4, q-\varepsilon)$ by Theorem 2.12. First, assume that $k \geqslant 7$ and set $k_0 = 7$. For $q \leqslant 89$, one can check (13) with the aid of Magma. Now, assume $q > 89$. It is easy to see that

$$q^5 > \max\{48(4e)^7 \log q, 4e \cdot 60^2 (\log q)^2\},$$

which implies (22) and (23).

Now, assume $k \in \{5, 6\}$. Note that $|T|/h(T) > 10|\mathrm{Out}(T)| \geqslant 10$, so $Q_2(G) < \frac{1}{5}$. Moreover,

$$Q_1(G) < \frac{(6!)^2}{|T|^{\frac{1}{3}}} + \frac{6!}{|T|^{\frac{4}{3}}} + \frac{6^4}{2|T|^{\frac{1}{3}}},$$

so we have $Q_1(G) < \frac{3}{10}$ if $q \geqslant 19$ and thus $Q_1(G) + Q_2(G) < 1/2$. Finally, if $q \leqslant 17$, then we can use Magma (via random search as in Remark 2.21(i)) to check that $r(G) \geqslant 2$. □

Lemma 4.14. *Suppose* $T = \mathrm{PSp}_4(q)$ *and* $5 \leqslant k \leqslant 4 \log |T|$. *Then* $r(G) \geqslant 2$.

Proof. As noted in (4), we assume $q \geqslant 3$. First, assume $k \geqslant 6$. It can be checked using Magma that (13) holds for $q \leqslant 607$, unless $(k, q) = (6, 3)$, in which case we can verify the result using Magma and random search as in Remark 2.21(i). Now, assume $q > 607$. By applying the bounds $|T| < q^{10}$, $h(T) > q^6/2$ and $q^4/2 < |T|/h(T) < 2q^4$, we see that (22) holds for $k_0 = 6$ if

$$q^4 > 6(2e)^6 \log q,$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

while (23) holds if

$$q^2 > 40^2(\log q)^2 e.$$

Note that both inequalities hold for all $q > 607$.

Finally, assume $k = 5$. Once again, we have $|T|/h(T) > 10|\mathrm{Out}(T)| \geqslant 10$ and thus $Q_2(G) < \frac{1}{5}$. Additionally,

$$Q_1(G) = \frac{(5!)^2}{|T|^{\frac{1}{3}}} + \frac{5!}{|T|^{\frac{4}{3}}} + \frac{5^4}{2|T|^{\frac{1}{3}}} < \frac{3}{10}$$

for all $q \geqslant 27$. The remaining groups with $q \leqslant 25$ can be handled with the aid of Magma via random search (see Remark 2.21(i)). □

Proposition 4.15. *The conclusions to Theorems 1 and 2 hold when T is a classical group.*

Proof. Let T be a classical group over $\mathbb{F}_q$, and let n be the dimension of the natural module. Note that $|T| > \frac{1}{8}q^{n(n-1)/2}$ by Lemma 2.10. As explained above, we may assume $5 \leqslant k \leqslant 4\log|T|$. In addition, we may also assume $n \geqslant 5$ by Lemmas 4.10, 4.11, 4.13 and 4.14. Then

$$\frac{|T|}{h(T)} > 10|\mathrm{Out}(T)| \geqslant 10$$

by inspecting Table 1, and thus

$$Q_2(G) < \frac{h(T)}{|T|} + 10|\mathrm{Out}(T)| \cdot \frac{h(T)^2}{|T|^2} < \frac{1}{10} + \frac{1}{10} = \frac{1}{5}.$$

First, assume $5 \leqslant k \leqslant n+3$. Then

$$\begin{aligned} Q_1(G) &< \frac{(6!)^2}{|T|^{\frac{1}{3}}} + \frac{(n+3)!}{|T|^{\frac{4}{3}}} + \frac{(n+3)^4}{2|T|^{\frac{1}{3}}} \\ &< \frac{8^{\frac{1}{3}}(6!)^2}{q^{\frac{n(n-1)}{6}}} + \frac{8^{\frac{4}{3}}(n+3)!}{q^{\frac{2n(n-1)}{3}}} + \frac{8^{\frac{1}{3}}(n+3)^4}{2q^{\frac{n(n-1)}{6}}} =: Q(n,q). \end{aligned}$$

Evidently, $Q(n,q)$ is a decreasing function of q. In addition, if q is fixed, then each summand is a decreasing function of n. Thus, $Q(n,q)$ is also decreasing of n. Note that $Q(n,q) < \frac{3}{10}$ if

$$(n,q) \in \{(12,2),(10,3),(9,4),(8,7),(7,9),(6,23),(5,97)\} =: \mathcal{B}.$$

Hence, we only need to consider the cases where $n < n_0$ or $q < q_0$ for some $(n_0,q_0) \in \mathcal{B}$. For these groups, we can show that $r(G) \geqslant 2$ either by checking $Q_1(G) + Q_2(G) < 1/2$ or (13), or by random search as explained in Remark 2.21(i). This shows that $r(G) \geqslant 2$ if $5 \leqslant k \leqslant n+3$.

To complete the proof, assume $n+4 \leqslant k \leqslant 4\log|T|$ and let $k_0 = n+4$. We first consider the case where $T = \mathrm{L}_n^{\varepsilon}(q)$. Note that $|T| < q^{n^2-1}$ and

$$\frac{|T|}{h(T)} \geqslant \frac{|\mathrm{PGL}_n^{\varepsilon}(q)|}{|\mathrm{GU}_{n-1}(q)|} > \frac{1}{2}q^{2n-2}$$

by Lemma 2.10 and Theorem 2.12. Hence, (22) holds if

$$q^{6n-8} > 2(n+4)(2e)^{n+4}$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

since $|\mathrm{Out}(T)| \leqslant 2(q+1)\log q < 2q^2$. This inequality holds if $q \geqslant 3$ or $n \geqslant 7$, while we can check (22) directly when $(n,q) = (5,2)$ or $(6,2)$. Thus, we have (22) for all $n \geqslant 5$ and $q \geqslant 2$. By Lemma 3.11, it suffices to prove (23). To do this, first note that

$$h(T) \geqslant q^{2n-3}|\mathrm{PGL}^{\varepsilon}_{n-2}(q)| > \frac{1}{2}q^{2n-3}q^{(n-2)^2-1} = \frac{1}{2}q^{n^2-2n}$$

by Lemma 2.10 and Theorem 2.12, so (23) holds if

$$q^{n^2-4n-1} > 32e(n^2-1)^2$$

since $\log q < q$. One can easily check that the above inequality holds for all $n \geqslant 5$ and $q \geqslant 2$, unless $n = 5$ and $q \leqslant 13$, or $(n,q) = (6,2)$, in which cases we can verify (23) directly. This completes the proof for linear and unitary groups.

Next, assume $T = \mathrm{PSp}_n(q)$ with $n \geqslant 6$. Here $|T| < q^{n(n+1)/2}$ by Lemma 2.10 and

$$\frac{|T|}{h(T)} = \frac{q^n-1}{(2,q-1)} > q^{n-1}.$$

Since $|\mathrm{Out}(T)| \leqslant 2\log q$, we see that (22) holds if

$$q^{2n-4} > 2\log q \cdot (n+4)e^{n+4}$$

and one checks that this inequality is valid unless $q = 2$ and $n \leqslant 28$, $n = 6$ and $q \leqslant 5$, or $(n,q) \in \{(8,3),(10,3)\}$. In these remaining cases, one can also check (22) by applying the precise values of $|T|$, $h(T)$ and $|\mathrm{Out}(T)|$, so as above, it just remains to verify (23). To do this, first note that

$$h(T) = q^{n-1}|\mathrm{Sp}_{n-2}(q)| > \frac{1}{2}q^{n(n-1)/2},$$

so it suffices to show that

$$q^{n(n-3)/2} > 8en^2(n+1)^2(\log q)^2.$$

The latter holds unless $(n,q) = (6,2)$ or $(6,3)$, in which cases one can directly verify (23). The result now follows from Lemma 3.11.

Finally, assume $T = \mathrm{P}\Omega^{\varepsilon}_n(q)$ is an orthogonal group, so $n \geqslant 7$, and q is odd if n is odd. In this setting, $|T| < q^{n(n-1)/2}$ and

$$\frac{|T|}{h(T)} > \frac{1}{2}q^{n-1}$$

by Lemma 2.10 and Theorem 2.12. In addition, (22) holds if

$$q^{4n-4} > 24\log q \cdot (n+4)(2e)^{n+4}$$

since $|\mathrm{Out}(T)| \leqslant 24\log q$, which is valid unless $q = 2$ and $n \leqslant 14$. In the remaining cases, (22) can be checked directly. Finally, to prove (23), note that

$$h(T) > \frac{1}{4}q^{(n-1)(n-2)/2}$$

by Lemma 2.10 and Theorem 2.12, so we only need to show that

$$q^{(n-1)(n-4)/2} > 32en^2(n-1)^2(\log q)^2.$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

This holds unless $(n, q) = (7, 3)$ or $(8, 2)$, and in these special cases we can verify (23) directly. We now complete the proof by applying Lemma 3.11. □

We conclude that the proofs of Theorems 1 and 2 are complete by combining Propositions 4.8, 4.9, 4.12 and 4.15. As noted in the beginning of this section, the proof of Theorem 4 is also complete.

5. Proof of Theorem 3

In this section, we prove Theorem 3, which is our main result. By Theorems 1, 2.3, and Proposition 4.7, we only need to consider the cases where $k = 2$, or $k > |T|$ and $P \in \{A_k, S_k\}$.

5.1. The groups with $k = 2$

We first consider the case where $k = 2$. As recorded in Theorem 2.3(ii), we have $b(G) = 3$ if $P = 1$, and $b(G) \in \{3, 4\}$ if $P = S_2$.

Lemma 5.1. *Suppose* $W = T^2.(\mathrm{Out}(T) \times S_2)$ *and* $s, t \in T$. *Then* $\{D, D(1, \varphi_s), D(1, \varphi_t)\}$ *is a base for* W *if and only if:*

(i) $C_{\mathrm{Aut}(T)}(s) \cap C_{\mathrm{Aut}(T)}(t) = 1$;
(ii) *there is no* $\alpha \in \mathrm{Aut}(T)$ *such that* $s^\alpha = s^{-1}$ *and* $t^\alpha = t^{-1}$.

Proof. This can be deduced from [47, Lemma 3.5]. □

The following is [41, Theorem 1.1].

Theorem 5.2. *Suppose* T *is not* A_7, $\mathrm{L}_2(q)$ *or* $\mathrm{L}_3^\varepsilon(q)$ *for some prime power* q. *Then there exists a generating pair* (s, t) *of* T *such that* $|s| = 2$ *and there is no* $\alpha \in \mathrm{Aut}(T)$ *with* $s^\alpha = s^{-1}$ *and* $t^\alpha = t^{-1}$.

It has been proved recently that each of the excluded groups A_7, $\mathrm{L}_2(q)$ and $\mathrm{L}_3^\varepsilon(q)$ does not have a generating pair described as in Theorem 5.2 (see [37, Theorem 1.3]).

Proposition 5.3. *The conclusion to Theorem 3 holds for* $k = 2$.

Proof. Recall that $b(G) = 3$ if $P = 1$ by Theorem 2.3(ii). Thus, we may assume $P = S_2$. By Lemma 5.1 and Theorem 5.2, we have $b(G) = 3$ if $T \notin \{A_7, \mathrm{L}_2(q), \mathrm{L}_3^\varepsilon(q)\}$. The case where $T = A_7$ can be easily handled using Magma and we deduce that $b(W) = 3$.

Assume $T = \mathrm{L}_2(q)$, so $\mathrm{Aut}(T) = \mathrm{P\Gamma L}_2(q)$. If $q \in \{4, 5, 9\}$, then T is isomorphic to A_5 or A_6 and we can prove the proposition with the aid of Magma, noting that $b(W) = 4$ and $b(G) = 3$ if $G < W$. Now, we consider the cases where $q \notin \{4, 5, 9\}$. Let s be an element in T of order $(q-1)/(2, q-1)$. Then we have $N_{\mathrm{PGL}_2(q)}(\langle s \rangle) \cong D_{2(q-1)}$ and

$$C_{\mathrm{P\Gamma L}_2(q)}(s) = C_{\mathrm{PGL}_2(q)}(s) \cong C_{q-1}.$$

One can show that $\mathrm{PGL}_2(q)$ is base-two on $[\mathrm{PGL}_2(q) : N_{\mathrm{PGL}_2(q)}(\langle s \rangle)]$ (see, for example, [8, Lemma 4.7]), which implies that there exists $g \in \mathrm{PGL}_2(q)$ such that

$$N_{\mathrm{PGL}_2(q)}(\langle s \rangle) \cap N_{\mathrm{PGL}_2(q)}(\langle s^g \rangle) = 1.$$

We claim that the pair (s, s^g) satisfies the conditions (i) and (ii) in Lemma 5.1. Indeed, (i) is clear since $C_{\mathrm{P\Gamma L}_2(q)}(s) = C_{\mathrm{PGL}_2(q)}(s)$ and so it suffices to check (ii). To do this, first note that there exists an element $\beta \in \mathrm{PGL}_2(q)$ such that $s^\beta = s^{-1}$. Therefore, if $\alpha \in \mathrm{P\Gamma L}_2(q)$ and $s^\alpha = s^{-1}$, then α is contained in the coset $C_{\mathrm{P\Gamma L}_2(q)}(s)\beta$. In particular, $\alpha \in \mathrm{PGL}_2(q)$ as $C_{\mathrm{P\Gamma L}_2(q)}(s) \leqslant \mathrm{PGL}_2(q)$. It follows that $\alpha \in N_{\mathrm{PGL}_2(q)}(\langle s \rangle)$. Similarly, if $(s^g)^\alpha = (s^g)^{-1}$, then $\alpha \in N_{\mathrm{PGL}_2(q)}(\langle s^g \rangle)$, which yields $\alpha = 1$. This leads to a contradiction as s is not an involution. Thus, $b(G) = 3$ by Lemma 5.1.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Finally, let us turn to the case where $T = \mathrm{L}_3^{\varepsilon}(q)$. One can easily check the proposition for $q = 3$ using Magma, and we will assume $q \neq 2$ as $\mathrm{L}_3(2) \cong \mathrm{L}_2(7)$ has been handled above, and $\mathrm{U}_3(2)$ is not simple. Let N be a subgroup of $\mathrm{Aut}(T)$ of type $\mathrm{GL}_1^{\varepsilon}(q^3)$. Then N is a maximal subgroup of $\mathrm{Aut}(T)$, and $N \cap T \cong \langle s \rangle{:}C_3$, where $|s| = (q^3 - \varepsilon)/d(q - \varepsilon)$ and $d = (3, q - \varepsilon)$ (see [39, Proposition 4.3.6]). Note that $N = N_{\mathrm{Aut}(T)}(\langle s \rangle)$. By [8, Lemma 6.4], $\mathrm{Aut}(T)$ is base-two on $[\mathrm{Aut}(T) : N]$, so there exists $g \in \mathrm{Aut}(T)$ such that $N_{\mathrm{Aut}(T)}(\langle s \rangle) \cap N_{\mathrm{Aut}(T)}(\langle s^g \rangle) = 1$. By repeating the above argument, we deduce that the conditions (i) and (ii) in Lemma 5.1 are satisfied if we take $t = s^g$, which completes the proof. □

The following corollary will be useful in Section 5.3.

Corollary 5.4. *Suppose $T \notin \{A_5, A_6\}$. Then there exist $x, y \in T$ such that $C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) = 1$ and there is no $\alpha \in \mathrm{Aut}(T)$ with $(x, y)^{\alpha} = (x^{-1}, y^{-1})$.*

Proof. Proposition 5.3 implies that the group $W = T^2.(\mathrm{Out}(T) \times S_2)$ has a base of size 3. Now, apply Lemma 5.1. □

5.2. *The groups with $|T|^{\ell-1} < k \leqslant |T|^{\ell} - 3$*

Next, we assume $P \in \{A_k, S_k\}$ and $|T|^{\ell-1} < k \leqslant |T|^{\ell} - 3$ for some integer $\ell \geqslant 1$. The groups with $\ell = 1$ have been handled in Theorem 1 and Proposition 5.3, so we may assume $\ell \geqslant 2$. In this setting, Theorem 2.3(iii) implies that $b(G) \in \{\ell + 1, \ell + 2\}$, and we will show that $b(G) = \ell + 1$ by constructing a base for G of size $\ell + 1$. We may assume $G = T^k.(\mathrm{Out}(T) \times S_k)$ throughout.

For any partition $\mathcal{P}$ of $[k]$ into $|T|$ parts, where some parts are allowed to be empty, we may write $\mathcal{P} = \{\mathcal{P}_t : t \in T\}$. Recall that $\mathrm{Hol}(T, S)$ is the setwise stabiliser of $S \subseteq T$ in $\mathrm{Hol}(T)$.

Lemma 5.5. *If $\ell \geqslant 2$ and $|T|^{\ell-1} < k \leqslant |T|^{\ell} - 3$, then there exists a partition $\mathcal{P} = \{\mathcal{P}_t : t \in T\}$ of $[k]$ satisfying the following properties:*

(P1) $|\mathcal{P}_t| \leqslant |T|^{\ell-1}$ *for all* $t \in T$.
(P2) $|\mathcal{P}_1| \neq 0$ *and* $\mathrm{Hol}(T, S) = 1$, *where*

$$S = \{t \in T : |\mathcal{P}_t| = |\mathcal{P}_1|\}.$$

(P3) *There exists $x \in T^{\#}$ such that $|\mathcal{P}_x| \in \{1, |T|^{\ell-1} - 1\}$.*

Proof. First, assume $|T|^{\ell} - 2|T|^{\ell-1} < k \leqslant |T|^{\ell} - 3$. In view of Theorem 4, let S be a subset of T containing 1 with $|S| = |T| - 3$ and $\mathrm{Hol}(T, S) = 1$, and let $\{x_1, x_2, x_3\} = T \setminus S$. Now, define $\mathcal{P} = \{\mathcal{P}_t : t \in T\}$, where $|\mathcal{P}_t| = |T|^{\ell-1}$ if $t \in S$, and $|\mathcal{P}_{x_i}| \leqslant |T|^{\ell-1} - 1$ with $|\mathcal{P}_{x_1}| = |T|^{\ell-1} - 1$ and $|\mathcal{P}_{x_2}| + |\mathcal{P}_{x_3}| = k - (|T| - 2)|T|^{\ell-1} + 1$. Note that such a partition exists since

$$2 \leqslant k - (|T| - 2)|T|^{\ell-1} + 1 \leqslant 2|T|^{\ell-1} - 2.$$

It is then easy to check that $\mathcal{P}$ satisfies the conditions (P1)–(P3).

Now, assume $3|T|^{\ell-1} < k \leqslant |T|^{\ell} - 2|T|^{\ell-1}$. Then there exists an integer m such that $3 \leqslant m \leqslant |T| - 3$ and $m|T|^{\ell-1} < k \leqslant (m + 1)|T|^{\ell-1}$. By Theorem 4, there exists a subset $S \subseteq T$ containing 1 with $|S| = m$ and $\mathrm{Hol}(T, S) = 1$. Let $x_1, x_2 \in T \setminus S$, and define $\mathcal{P} = \{\mathcal{P}_t : t \in T\}$, where $|\mathcal{P}_t| = |T|^{\ell-1}$ if $t \in S$, $|\mathcal{P}_{x_1}| = 1$ and $|\mathcal{P}_{x_2}| = k - m|T|^{\ell-1} - 1$, noting that $0 \leqslant k - m|T|^{\ell-1} - 1 < |T|^{\ell-1}$. One can check (P1)–(P3) easily.

To complete the proof, we assume $|T|^{\ell-1} < k \leqslant 3|T|^{\ell-1}$ and let $S = \{t_1, t_2, t_3\} \subseteq T$ be such that $t_1 = 1$ and $\mathrm{Hol}(T, S) = 1$. In this setting, let $x_1, x_2, x_3 \in T \setminus S$ and define $\mathcal{P} = \{\mathcal{P}_t : t \in T\}$, where $|\mathcal{P}_{t_i}| = 1$, and $|\mathcal{P}_{x_i}| \leqslant |T|^{\ell-1}$ with $|\mathcal{P}_{x_i}| \neq 1$ and $|\mathcal{P}_{x_1}| + |\mathcal{P}_{x_2}| + |\mathcal{P}_{x_3}| = k - 3$. We conclude the proof by noting that $\mathcal{P}$ satisfies the conditions (P1)–(P3). □

For the remainder of this subsection, $\mathcal{P} = \{\mathcal{P}_t : t \in T\}$ is a partition of $[k]$ satisfying the conditions in Lemma 5.5, where $S \subseteq T$ and $x \in T^{\#}$ are as described in (P2) and (P3), respectively. Define $\mathbf{a}_0 = (\varphi_{t_{0,1}}, \ldots, \varphi_{t_{0,k}}) \in \mathrm{Inn}(T)^k$ by $t_{0,j} = t$ if $j \in \mathcal{P}_t$.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Lemma 5.6. *Suppose* $(\alpha, \dots, \alpha)\pi \in G_{D\mathbf{a}_0}$. *Then* $\alpha = 1$ *and* $\pi \in P_{(\mathcal{P})}$.

Proof. First, note that there exists a unique $g \in T$ such that $t_{0,j}^{\alpha} = gt_{0,j^\pi}$ for all $j \in [k]$, and we have $\pi \in P_{\{\mathcal{P}\}}$ by Lemma 2.2(i). This implies that π fixes the set $\{\mathcal{P}_t : t \in S\}$, and thus $g^{-1}t^{\alpha} \in S$ if $t \in S$, whence $g^{\alpha^{-1}}\alpha \in \mathrm{Hol}(T, S) = 1$. It follows that $g = 1$ and $\alpha = 1$, so $t_{0,j} = t_{0,j^\pi}$ for all $j \in [k]$, which concludes the proof. □

Write $T^{\ell-1} = \{\mathbf{b}_1, \dots, \mathbf{b}_{|T|^{\ell-1}}\}$, where $\mathbf{b}_h = (a_{1,h}, \dots, a_{\ell-1,h})$. If $|\mathcal{P}_x| = 1$, then we may assume $\mathbf{b}_1 = (1, \dots, 1)$, and if $|\mathcal{P}_x| = |T|^{\ell-1} - 1$, we assume $\mathbf{b}_{|T|^{\ell-1}} = (1, \dots, 1)$. Let $1 \leqslant i \leqslant \ell - 1$, and define $\mathbf{a}_i = (\varphi_{t_{i,1}}, \dots, \varphi_{t_{i,k}}) \in \mathrm{Inn}(T)^k$, where $t_{i,j} = a_{i,h}$ if j is the h-th smallest number in $\mathcal{P}_t$. Define $X_{i,t} := \{j \in \mathcal{P}_x : t_{i,j} = t\}$.

Lemma 5.7. *For any* $t \in T^{\#}$ *and* $i \in \{1, \dots, \ell - 1\}$, *we have* $|X_{i,t}| \neq |X_{i,1}|$.

Proof. If $|\mathcal{P}_x| = 1$, then $\mathbf{b}_1 = (1, \dots, 1)$, so $|X_{i,1}| = 1$ and $|X_{i,t}| = 0$ for all $t \in T^{\#}$. And if $|\mathcal{P}_x| = |T|^{\ell-1}$, then $\mathbf{b}_{|T|^{\ell-1}} = (1, \dots, 1)$, which implies that $|X_{i,1}| = |T|^{\ell-1} - 1$ and $|X_{i,t}| = |T|^{\ell-1}$ for all $t \in T^{\#}$. □

Proposition 5.8. *If* $\ell \geqslant 2$, $P \in \{A_k, S_k\}$ *and* $|T|^{\ell-1} < k \leqslant |T|^{\ell} - 3$, *then* $b(G) = \ell + 1$.

Proof. As noted above, it suffices to show that $\Delta = \{D, D\mathbf{a}_0, D\mathbf{a}_1 \dots, D\mathbf{a}_{\ell-1}\}$ is a base for $G = T^k.(\mathrm{Out}(T) \times S_k)$. Suppose $(\alpha, \dots, \alpha)\pi \in G_{(\Delta)}$. By Lemma 5.6, we have $\alpha = 1$ and $\pi \in P_{(\mathcal{P})}$. Note that for any $i \in \{1, \dots, \ell - 1\}$, there exists a unique $g_i \in T$ such that $t_{i,j} = g_i t_{i,j^\pi}$ for any $j \in [k]$. Now, $j \in X_{i,1}$ if and only if $j^\pi \in X_{i,g_i^{-1}}$. This implies that $g_i = 1$ by Lemma 5.7, and hence $t_{i,j} = t_{i,j^\pi}$ for all $i \in \{1, \dots, \ell - 1\}$ and $j \in [k]$.

From the definition of $\mathbf{a}_i$, we see that if $j, j' \in \mathcal{P}_t$ and $j \neq j'$, then there exists $i \in \{1, \dots, \ell - 1\}$ such that $t_{i,j} \neq t_{i,j'}$. This yields $j^\pi \neq j'$, so $j^\pi = j$ since $\pi \in P_{\{\mathcal{P}_t\}}$. That is, $\pi \in P_{(\mathcal{P}_t)}$ for all $t \in T$, whence $\pi = 1$. □

5.3. The groups with $|T|^{\ell} - 2 \leqslant k \leqslant |T|^{\ell}$

To complete the proof of Theorem 3, we turn to the cases where $P \in \{A_k, S_k\}$ and $k \in \{|T|^{\ell} - 2, |T|^{\ell} - 1, |T|^{\ell}\}$ for some integer $\ell \geqslant 1$. The groups with $\ell = 1$ have been treated previously, and we record the result as follows.

Proposition 5.9. *If* $k \in \{|T| - 2, |T| - 1, |T|\}$ *and* $P \in \{A_k, S_k\}$, *then*

$$b(G) = \begin{cases} 2 & \text{if } k \in \{|T| - 2, |T| - 1\} \text{ and } S_k \not\leqslant G; \\ 3 & \text{otherwise.} \end{cases}$$

Proof. Combine Theorem 2.3(iii) and Proposition 4.7. □

From now on, we assume $\ell \geqslant 2$. We start with the groups with $S_k \not\leqslant G$.

Lemma 5.10. *Suppose* $k \in \{|T|^{\ell} - 2, |T|^{\ell} - 1, |T|^{\ell}\}$ *with* $\ell \geqslant 2$, $P \in \{A_k, S_k\}$ *and* $S_k \not\leqslant G$. *Then* $b(G) = \ell + 1$.

Proof. In view of Theorem 2.3(iii), it suffices to construct a base for G of size $\ell + 1$. Note that $A_k \leqslant G$ by Corollary 2.6, so G does not contain any transposition in S_k.

By Corollary 5, there exist $x, y \in T^{\#}$ such that $\mathrm{Aut}(T, \{x, y\}) = 1$. Let $\mathcal{P} = \{\mathcal{P}_t : t \in T\}$ be a partition of $[k]$ with $|\mathcal{P}_1| = |T|^{\ell-1} + 1$, $|\mathcal{P}_x| = |T|^{\ell-1} - 1$ and $|\mathcal{P}_t| = |T|^{\ell-1}$ if $t \notin \{1, x, y\}$. Thus, $|\mathcal{P}_y| = |T|^{\ell-1} - m$ if $k = |T|^{\ell} - m$, where $m \in \{0, 1, 2\}$. Now, define $\mathbf{a}_0 = (\varphi_{t_{0,1}}, \dots, \varphi_{t_{0,k}}) \in \mathrm{Inn}(T)^k$ by setting $t_{0,j} = t$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

if $j \in \mathcal{P}_t$. We also write $T^{\ell-1} = \{\mathbf{b}_1, \dots, \mathbf{b}_{|T|^{\ell-1}}\}$, where $\mathbf{b}_h = (a_{1,h}, \dots, a_{\ell-1,h})$, and we may assume $\mathbf{b}_{|T|^{\ell-1}} = (y, \dots, y)$. Define $\mathbf{a}_i = (\varphi_{t_{i,1}}, \dots, \varphi_{t_{i,k}}) \in \mathrm{Inn}(T)^k$ for $i \in \{1, \dots, \ell-1\}$, where

$$t_{i,j} = \begin{cases} a_{i,h} & \text{if } j \text{ is the } h\text{-th smallest number in } \mathcal{P}_t; \\ 1 & \text{if } j \text{ is the largest number in } \mathcal{P}_1. \end{cases}$$

We claim that $\Delta = \{D, D\mathbf{a}_0, D\mathbf{a}_1, \dots, D\mathbf{a}_{\ell-1}\}$ is a base for G.

Suppose $(\alpha, \dots, \alpha)\pi \in G_{(\Delta)}$. By Lemma 2.2, we have $\pi \in P_{\{\mathcal{P}\}}$ and $t_{0,j}^{\alpha} = t_{0,j^\pi}$ for all $j \in [k]$. We first prove that $\alpha = 1$. To see this, note that if $k \in \{|T|^\ell - 2, |T|^\ell - 1\}$, then $\pi \in P_{\{\mathcal{P}_x \cup \mathcal{P}_y\}}$, which implies that $\alpha \in \mathrm{Aut}(T, \{x, y\})$, and thus $\alpha = 1$ since $\mathrm{Aut}(T, \{x, y\}) = 1$. Now, assume $k = |T|^\ell$. Then $\pi \in P_{\{\mathcal{P}_x\}}$ and thus $\alpha \in C_{\mathrm{Aut}(T)}(x)$. Note that for each $i \in \{1, \dots, \ell-1\}$, 1 appears exactly $|T|^{\ell-1} + 1$ times in the entries of $\mathbf{a}_i$, while φ_y appears exactly $|T|^{\ell-1} - 1$ times and every other element appears exactly $|T|^{\ell-1}$ times. By arguing as above, we have $t_{i,j}^{\alpha} = t_{i,j^\pi}$ for all $i \in \{1, \dots, \ell-1\}$, which implies that $\alpha \in C_{\mathrm{Aut}(T)}(y)$, and so $\alpha = 1$ since $\mathrm{Aut}(T, \{x, y\}) = 1$.

Finally, observe that there exists a unique pair $\{j_1, j_2\}$ of elements in $[k]$ such that $j_1 \neq j_2$ and $t_{i,j_1} = t_{i,j_2}$ for all $i \in \{0, \dots, \ell-1\}$, where we have $t_{i,j_1} = t_{i,j_2} = 1$. For each i, there exists a unique element $g_i \in T$ such that $t_{i,j} = g_i t_{i,j^\pi}$ for all $j \in [k]$, so $t_{i,j_1^\pi} = t_{i,j_2^\pi} = g_i^{-1}$. Since $\pi \in P_{\{\mathcal{P}_1\}}$, it follows that $g_i = 1$ and so $t_{i,j} = t_{i,j^\pi}$ for all $j \in [k]$. It is then easy to see that $\pi \in \langle (j_1, j_2) \rangle$, and thus $\pi = 1$ as G does not contain any transposition in S_k. □

Proposition 5.11. *If $\ell \geqslant 2$, $P \in \{A_k, S_k\}$ and $k \in \{|T|^\ell - 1, |T|^\ell\}$, then*

$$b(G) = \begin{cases} \ell + 1 & \text{if } S_k \not\leqslant G; \\ \ell + 2 & \text{if } S_k \leqslant G. \end{cases}$$

Proof. See Theorem 2.3(iii) for the groups with $S_k \leqslant G$ and Lemma 5.10 for $S_k \not\leqslant G$. □

Finally, we turn to the groups with $k = |T|^\ell - 2$ and $S_k \leqslant G$. The case where $\ell = 2$ requires special attention.

Lemma 5.12. *Suppose $k = |T|^2 - 2$, $T \in \{A_5, A_6\}$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$. Then $b(G) = 4$.*

Proof. By Theorem 2.3(iii), we have $b(G) \in \{3, 4\}$, so it suffices to show that there is no base for G of size 3.

We argue by contradiction and suppose $\Delta = \{D, D\mathbf{a}_0, D\mathbf{a}_1\}$ is a base for G, where $\mathbf{a}_i = (\varphi_{t_{i,1}}, \dots, \varphi_{t_{i,k}}) \in \mathrm{Inn}(T)^k$. If φ_t appears at least $|T| + 1$ times in the entries of $\mathbf{a}_0$ for some t, then there exist $j, j' \in [k]$ such that $j \neq j'$, $t_{0,j} = t_{0,j'} = t$ and $t_{1,j} = t_{1,j'}$, which implies that $G_{(\Delta)}$ contains the transposition (j, j'). Thus, we may assume that each φ_t appears at most $|T|$ times in the entries of $\mathbf{a}_0$. The same argument holds for $\mathbf{a}_1$. It follows that the set

$$S_i = \{t \in T : \varphi_t \text{ appears exactly } |T| \text{ times in the entries of } \mathbf{a}_i\}$$

has size at least $|T| - 2$, so $|S_i| \in \{|T| - 2, |T| - 1\}$.

First, assume either $|S_0|$ or $|S_1|$ is equal to $|T| - 1$, say $|S_0| = |T| - 1$ and $1 \notin S_0$. For the same reason as above, for any j, j' such that $j \neq j'$ and $t_{0,j} = t_{0,j'}$, we have $t_{1,j} \neq t_{1,j'}$, otherwise $(j, j') \in G_{(\Delta)}$. This implies that $|S_1| = |T| - 2$, and we may assume $T \setminus S_1 = \{1, x\}$ for some $x \neq 1$. Write $\mathbf{c}_j = (t_{0,j}, t_{1,j})$ for $j \in [k]$, noting that

$$\{\mathbf{c}_j : j \in [k]\} = T^2 \setminus \{(1, 1), (1, x)\}.$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

That is, $\{\mathbf{c}_j : j \in [k]\}$ is fixed by φ_x setwise, with the componentwise action. This induces a permutation $\pi \in S_k$, where

$$j^\pi = m \text{ if } \mathbf{c}_j^{\varphi_x} = \mathbf{c}_m.$$

In particular, $t_{i,j}^{\varphi_x} = t_{i,j^\pi}$ for each $i \in \{0,1\}$. Then

$$D\mathbf{a}_i^{(\varphi_x,\dots,\varphi_x)\pi} = D(\varphi_{t_{i,1\pi^{-1}}^{\varphi_x}}, \dots, \varphi_{t_{i,k\pi^{-1}}^{\varphi_x}}) = D(\varphi_{t_{i,1}}, \dots, \varphi_{t_{i,k}}) = D\mathbf{a}_i$$

for each $i \in \{0,1\}$, and so $(\varphi_x, \dots, \varphi_x)\pi \in G_{(\Delta)}$.

To complete the proof, we may assume $|S_0| = |S_1| = |T| - 2$, say $T \setminus S_0 = \{1, x\}$ and $T \setminus S_1 = \{1, y\}$. Write $\mathbf{c}_j = (t_{0,j}, t_{1,j})$ for $j \in [k]$ as above, and observe that

$$T^2 \setminus \{\mathbf{c}_j : j \in [k]\} = \{(1,1),(x,y)\} \text{ or } \{(1,y),(x,1)\}.$$

It is easy to check with the aid of Magma that there exists an automorphism $\alpha \in \mathrm{Aut}(T)$ such that $1 \neq \alpha \in C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y)$, or $(x,y)^\alpha = (x^{-1}, y^{-1})$.

Assume $\alpha \neq 1$ and $(x,y)^\alpha = (x,y)$. Then $\{\mathbf{c}_j : j \in [k]\}$ is fixed by α setwise, with the componentwise action. Once again, α induces a permutation $\pi \in S_k$, where

$$j^\pi = m \text{ if } \mathbf{c}_j^\alpha = \mathbf{c}_m.$$

Then by arguing as above, we deduce that $(\alpha, \dots, \alpha)\pi \in G_{(\Delta)}$.

Finally, assume $(x,y)^\alpha = (x^{-1}, y^{-1})$ and note that

$$\{\mathbf{c}_j : j \in [k]\}^\alpha = \{(x^{-1}, y^{-1})\mathbf{c}_j : j \in [k]\}.$$

Here, α also induces a permutation $\pi \in S_k$, where

$$j^\pi = m \text{ if } \mathbf{c}_j^\alpha = (x^{-1}, y^{-1})\mathbf{c}_m,$$

and thus $t_{0,j}^\alpha = x^{-1} t_{0,j^\pi}$ and $t_{1,j}^\alpha = y^{-1} t_{1,j^\pi}$ for all $j \in [k]$, noting that $\pi \neq 1$ if $\alpha = 1$. Now, we have

$$D\mathbf{a}_0^{(\alpha,\dots,\alpha)\pi} = D(\varphi_{t_{i,1\pi^{-1}}^\alpha}, \dots, \varphi_{t_{i,k\pi^{-1}}^\alpha}) = D(\varphi_{x^{-1}\varphi_{t_{i,1}}}, \dots, \varphi_{x^{-1}\varphi_{t_{i,k}}}) = D\mathbf{a}_0$$

and similarly, $D\mathbf{a}_1^{(\alpha,\dots,\alpha)\pi} = D\mathbf{a}_1$. This completes the proof. □

Proposition 5.13. *If $P \in \{A_k, S_k\}$ and $k = |T|^2 - 2$, then*

$$b(G) = \begin{cases} 4 & \text{if } T \in \{A_5, A_6\} \text{ and } G = T^k.(\mathrm{Out}(T) \times S_k); \\ 3 & \text{otherwise.} \end{cases}$$

Proof. By Lemmas 5.10 and 5.12, we may assume that $S_k \leqslant G$, and G is not $T^k.(\mathrm{Out}(T) \times S_k)$ if $T \in \{A_5, A_6\}$. That is, $G = T^k.(O \times S_k)$ for some $O \leqslant \mathrm{Out}(T)$, with $O \neq \mathrm{Out}(T)$ if $T \in \{A_5, A_6\}$. We will prove that $b(G) = 3$ by constructing a base of size 3.

Write $K = \mathrm{Inn}(T).O \leqslant \mathrm{Aut}(T)$. Note that there exist $x, y \in T$ such that $C_K(x) \cap C_K(y) = 1$ and there is no $\alpha \in K$ with $(x,y)^\alpha = (x^{-1}, y^{-1})$. This can be obtained by Corollary 5.4 when $T \notin \{A_5, A_6\}$, and the cases where $T \in \{A_5, A_6\}$ can be checked using Magma (note that $K < \mathrm{Aut}(T)$ if $T \in \{A_5, A_6\}$). Now, let $\mathcal{P} = \{\mathcal{P}_t : t \in T\}$ be a partition of $[k]$ with $|\mathcal{P}_1| = |\mathcal{P}_x| = |T| - 1$, and $|\mathcal{P}_t| = |T|$ if $t \notin \{1, x\}$. And we label the elements in T by $T = \{g_1, \dots, g_{|T|}\}$, where $g_1 = 1$ and $g_{|T|} = y$. Define

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

$\mathbf{a}_0 = (\varphi_{t_{0,1}}, \ldots, \varphi_{t_{0,k}}) \in \mathrm{Inn}(T)^k$, where $t_{0,j} = t$ if $j \in \mathcal{P}_t$, and define $\mathbf{a}_1 = (\varphi_{t_{1,1}}, \ldots, \varphi_{t_{1,k}}) \in \mathrm{Inn}(T)^k$ by setting

$$t_{1,j} = \begin{cases} g_h & \text{if } t \neq 1 \text{ and } j \text{ is the } h\text{-th smallest number in } \mathcal{P}_t; \\ g_{h+1} & \text{if } j \text{ is the } h\text{-th smallest number in } \mathcal{P}_1. \end{cases}$$

Now, we claim that $\Delta = \{D, D\mathbf{a}_0, D\mathbf{a}_1\}$ is a base for G.

Suppose $(\alpha, \ldots, \alpha)\pi \in G_{(\Delta)}$, noting that $\alpha \in K$. By Lemma 2.2(i), we have $\pi \in P_{\{\mathcal{P}\}}$, so either $\pi \in P_{\{\mathcal{P}_1\}} \cap P_{\{\mathcal{P}_x\}}$, or $\mathcal{P}_1^\pi = \mathcal{P}_x$, hence there are two cases to consider.

First, assume that $\mathcal{P}_1^\pi = \mathcal{P}_x$. There exists a unique $g \in T$ such that $t_{0,j}^\alpha = g t_{0,j^\pi}$ for all $j \in [k]$, and by taking $j \in \mathcal{P}_1$ we have $g = x^{-1}$. This implies that $x^\alpha = x^{-1}$ by taking $j \in \mathcal{P}_x$. Let $\mathcal{Q} = \{\mathcal{Q}_t : t \in T\}$ be the partition of $[k]$ defined by setting $j \in \mathcal{Q}_t$ if $t_{1,j} = t$. Then $|\mathcal{Q}_1| = |\mathcal{Q}_y| = |T| - 1$, and $|\mathcal{Q}_t| = |T|$ if $t \notin \{1, y\}$. By arguing as above, either $\pi \in P_{\{\mathcal{Q}_1\}} \cap P_{\{\mathcal{Q}_y\}}$ or $\mathcal{Q}_1^\pi = \mathcal{Q}_y$. If the former holds, then

$$(\mathcal{P}_1 \cap \mathcal{Q}_1)^\pi = \mathcal{P}_x \cap \mathcal{Q}_1.$$

However, as can be seen from the definitions of $\mathbf{a}_0$ and $\mathbf{a}_1$, we have $|\mathcal{P}_1 \cap \mathcal{Q}_1| = 0$, while $|\mathcal{P}_x \cap \mathcal{Q}_1| = 1$. This implies that $\mathcal{Q}_1^\pi = \mathcal{Q}_y$, so $y^\alpha = y^{-1}$ as above. By our assumptions on x and y, there is no $\alpha \in K$ with $(x, y)^\alpha = (x^{-1}, y^{-1})$, which gives a contradiction.

Finally, suppose that $\pi \in P_{\{\mathcal{P}_1\}} \cap P_{\{\mathcal{P}_x\}}$. First, note that $t_{0,j}^\alpha = t_{0,j^\pi}$ for all $j \in [k]$, so $x^\alpha = x$. Similarly, we have $\pi \in P_{\{\mathcal{Q}_1\}} \cap P_{\{\mathcal{Q}_y\}}$ and $y^\alpha = y$. This implies that $\alpha \in C_K(x) \cap C_K(y) = 1$, and thus $t_{i,j} = t_{i,j^\pi}$ for all $i \in \{0, 1\}$ and $j \in [k]$, which yields $\pi = 1$ and completes the proof. □

Proposition 5.14. *If $\ell \geqslant 3$, $k = |T|^\ell - 2$ and $P \in \{A_k, S_k\}$, then $b(G) = \ell + 1$.*

Proof. In view of Theorem 2.3(iii), it suffices to construct a base for G of size $\ell + 1$. First note that there exist $x, y, z \in T$ such that

$$C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) \cap C_{\mathrm{Aut}(T)}(z) = 1$$

and there is no $\alpha \in \mathrm{Aut}(T)$ with

$$(x, y, z)^\alpha = (x^{-1}, y^{-1}, z^{-1}).$$

To see this, if $T \notin \{A_5, A_6\}$, then we apply Corollary 5.4, and if $T \in \{A_5, A_6\}$, then it can be checked using Magma. Let $\mathcal{P} = \{\mathcal{P}_t : t \in T\}$ be a partition of $[k]$ with $|\mathcal{P}_1| = |\mathcal{P}_x| = |T|^{\ell-1} - 1$ and $|\mathcal{P}_t| = |T|^{\ell-1}$ if $t \notin \{1, x\}$. Write $T^{\ell-1} = \{\mathbf{b}_1, \ldots, \mathbf{b}_{|T|^{\ell-1}}\}$, where $\mathbf{b}_h = (a_{1,h}, \ldots, a_{\ell-1,h})$, and we may assume $\mathbf{b}_1 = (1, \ldots, 1)$ and $\mathbf{b}_{|T|^{\ell-1}} = (y, z, \ldots, z)$. Now, define $\mathbf{a}_i = (\varphi_{t_{i,1}}, \ldots, \varphi_{t_{i,k}})$ for $i \in \{0, \ldots, \ell - 1\}$, where $t_{0,j} = t$ if $j \in \mathcal{P}_t$, and if $i \geqslant 1$,

$$t_{i,j} = \begin{cases} a_{i,h} & \text{if } t \neq 1 \text{ and } j \text{ is the } h\text{-th smallest number in } \mathcal{P}_t; \\ a_{i,h+1} & \text{if } j \text{ is the } h\text{-th smallest number in } \mathcal{P}_1. \end{cases}$$

We claim that $\Delta = \{D, D\mathbf{a}_0, D\mathbf{a}_1, \ldots, D\mathbf{a}_{\ell-1}\}$ is a base for G.

We argue as in the proof of Proposition 5.13. Suppose $(\alpha, \ldots, \alpha)\pi \in G_{(\Delta)}$, noting that $\pi \in P_{\{\mathcal{P}\}}$ by Lemma 2.2(i). It follows that either $\pi \in P_{\{\mathcal{P}_1\}} \cap P_{\{\mathcal{P}_x\}}$ or $\mathcal{P}_1^\pi = \mathcal{P}_x$.

First, assume that $\mathcal{P}_1^\pi = \mathcal{P}_x$. Note that there exists a unique $g \in T$ such that $t_{0,j}^\alpha = g t_{0,j^\pi}$ for all $j \in [k]$. Now, $g = x^{-1}$ by taking $j \in \mathcal{P}_1$, and thus $x^\alpha = x^{-1}$ by taking $j \in \mathcal{P}_x$. Let $\mathcal{Q} = \{\mathcal{Q}_t : t \in T\}$ be the partition of $[k]$ defined by setting $j \in \mathcal{Q}_t$ if $t_{1,j} = t$. Then $|\mathcal{Q}_1| = |\mathcal{Q}_y| = |T|^{\ell-1} - 1$, and

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

$|\mathcal{Q}_t| = |T|^{\ell-1}$ if $t \notin \{1, y\}$. By applying Lemma 2.2(i) again, we have either $\pi \in P_{\{\mathcal{Q}_1\}} \cap P_{\{\mathcal{Q}_y\}}$ or $\mathcal{Q}_1^\pi = \mathcal{Q}_y$. If $\pi \in P_{\{\mathcal{Q}_1\}} \cap P_{\{\mathcal{Q}_y\}}$, then

$$(\mathcal{P}_1 \cap \mathcal{Q}_1)^\pi = \mathcal{P}_x \cap \mathcal{Q}_1,$$

which is impossible since $|\mathcal{P}_1 \cap \mathcal{Q}_1| = |T|^{\ell-2} - 1$, while $|\mathcal{P}_x \cap \mathcal{Q}_1| = |T|^{\ell-2}$. Hence, we have $\mathcal{Q}_1^\pi = \mathcal{Q}_y$, and thus $y^\alpha = y^{-1}$ with the same argument as above. Now, suppose $i \geqslant 2$ and let $\mathcal{R} = \{\mathcal{R}_t : t \in T\}$ be the partition of $[k]$ defined by setting $j \in \mathcal{R}_t$ if $t_{i,j} = t$. Then $|\mathcal{R}_1| = |\mathcal{R}_z| = |T|^{\ell-1} - 1$, and $|\mathcal{R}_t| = |T|^{\ell-1}$ if $t \notin \{1, z\}$. By arguing as above, we have $z^\alpha = z^{-1}$. However, by our assumptions on x, y and z, there is no automorphism of T simultaneously inverting all three elements, which gives a contradiction.

It follows that $\pi \in P_{\{\mathcal{P}_1\}} \cap P_{\{\mathcal{P}_x\}}$, and with the same reason, we have $\pi \in P_{\{\mathcal{Q}_1\}}$ and $\pi \in P_{\{\mathcal{R}_1\}}$. Hence, $t_{i,j}^\alpha = t_{i,j^\pi}$ for all $i \in \{0, \dots, \ell-1\}$ and $j \in [k]$. This implies that

$$\alpha \in C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) \cap C_{\mathrm{Aut}(T)}(z),$$

so $\alpha = 1$. Moreover, note that if $j, j' \in \mathcal{P}_t$ for some $t \in T$ and $j \neq j'$, then there exists $i \in \{1, \dots, \ell-1\}$ such that $t_{i,j} \neq t_{i,j'}$. Hence, $\pi = 1$ and so Δ is a base for G. □

We conclude that the proof of Theorem 3 is complete by combining Theorem 1 with Propositions 5.3, 5.8, 5.9, 5.11, 5.13 and 5.14.

6. Proofs of Theorems 6 and 7

In this final section, we will prove Theorems 6 and 7. As introduced in Section 1, let $\mathbb{Q}_k(T)$ be the probability that a random k-element subset of $T^\#$ has a nontrivial setwise stabiliser in $\mathrm{Aut}(T)$. That is,

$$\mathbb{Q}_k(T) := \frac{|\{R \in \mathcal{S}_k(T) : \mathrm{Aut}(T, R) \neq 1\}|}{|\mathcal{S}_k(T)|},$$

where $\mathcal{S}_k(T)$ is the set of k-subsets of $T^\#$ (we will simply write $\mathcal{S}_k$ if T is clear from the context). Consider the diagonal type group $G = T^k.(\mathrm{Out}(T) \times S_k) \leqslant \mathrm{Sym}(\Omega)$, and recall that

$$\mathbb{P}_k(T) := \frac{|\{(t_1, \dots, t_{k-1}) \in T^{k-1} : \{D, D(\varphi_{t_1}, \dots, \varphi_{t_{k-1}}, 1)\} \text{ is a base for } G\}|}{|T|^{k-1}},$$

which is the probability that a random element in Ω is in a regular orbit of $G_D = D$.

The following is [25, Theorem 1.5].

Theorem 6.1. *Let $k \geqslant 5$, and let (T_n) be a sequence of nonabelian finite simple groups such that $|T_n| \to \infty$ as $n \to \infty$. Then $\mathbb{P}_k(T_n) \to 1$ as $n \to \infty$.*

Lemma 6.2. *For any $k \geqslant 4$, we have $\mathbb{Q}_k(T) \leqslant 1 - \mathbb{P}_{k+1}(T)$.*

Proof. First, by Lemma 2.15, we have $\{D, D(\varphi_{t_1}, \dots, \varphi_{t_k}, 1)\}$ is a base for G if and only if $t_1, \dots, t_k \in T^\#$ are distinct and $\mathrm{Hol}(T, \{t_1, \dots, t_k, 1\}) = 1$. The latter condition implies that $\mathrm{Aut}(T, \{t_1, \dots, t_k\}) = 1$, so

$$\mathbb{P}_{k+1}(T) \leqslant \frac{|\{(t_1, \dots, t_k) \in (T^\#)^k : t_1, \dots, t_k \text{ are distinct and } \mathrm{Aut}(T, \{t_1, \dots, t_k\}) = 1\}|}{|T|^k}.$$

Note that the numerator of the expression on the right-hand side is

$$k! \cdot |\{R \in \mathcal{S}_k : \mathrm{Aut}(T, R) = 1\}|.$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

Thus, we have

$$\mathbb{P}_{k+1}(T) \leqslant \frac{k! \cdot |\{R \in \mathcal{S}_k : \mathrm{Aut}(T,R) = 1\}|}{|T|^k}$$

and it suffices to show that

$$|T|^k \geqslant k! \cdot |\mathcal{S}_k|.$$

This is clear, as $|\mathcal{S}_k| = \binom{|T|-1}{k}$. □

Theorem 6 now follows by combining Theorem 6.1 and Lemma 6.2. Finally, we establish Theorem 7. Recall that $\mathcal{P}_k$ is the set of k-subsets of T, and

$$\mathrm{fix}(\sigma, \mathcal{P}_k) = \{S \in \mathcal{P}_k : \sigma \in \mathrm{Hol}(T,S)\}$$

is the set of fixed points of $\sigma \in \mathrm{Hol}(T)$ on $\mathcal{P}_k$.

Proposition 6.3. *Let $m > 0$ be a real number. Then $\mathbb{Q}_k(T) < 1/m$ if*

$$\binom{|T|}{k} > m \sum_{\sigma \in \mathcal{R}} |\mathrm{fix}(\sigma, \mathcal{P}_k)|, \tag{42}$$

where $\mathcal{R}$ is the set of elements of prime order in $\mathrm{Hol}(T)$.

Proof. As noted in Section 3.1, we have

$$|\{S \in \mathcal{P}_k : \mathrm{Hol}(T,S) \neq 1\}| \leqslant \sum_{\sigma \in \mathcal{R}} |\mathrm{fix}(\sigma, \mathcal{P}_k)|,$$

which implies that $\mathrm{Hol}(T)$ has

$$r > \frac{m-1}{m|\mathrm{Hol}(T)|}\binom{|T|}{k}$$

regular orbits on $\mathcal{P}_k$. Then

$$|\{R \in \mathcal{S}_k : \mathrm{Hol}(T,R) = 1\}| = r(|T|-k)|\mathrm{Aut}(T)| > \frac{(m-1)(|T|-k)}{m|T|}\binom{|T|}{k}$$

and thus

$$\mathbb{Q}_k(T) = \frac{|\{R \in \mathcal{S}_k : \mathrm{Aut}(T,R) \neq 1\}|}{|\mathcal{S}_k|} < 1 - \frac{(m-1)(|T|-k)}{m|T|} \cdot \frac{\binom{|T|}{k}}{\binom{|T|-1}{k}} = \frac{1}{m},$$

as desired. □

Proof of Theorem 7. Note that if $T = A_5$, then $5\log|T| < k < |T| - 5\log|T|$ implies that $k = 30$, in which case we can check the theorem using Magma. Now, assume $|T| \geqslant 168$, so $5\log|T| < |T|/4$. It suffices to show that (42) holds for $m = |T|$ and $5\log|T| < k \leqslant |T|/2$, and we can do this by arguing as in the proof of Proposition 3.7. More precisely, if $|T|/4 \leqslant k \leqslant |T|/2$, then (42) holds for $m = |T|$ if

$$2t_0^{|T|} > \sqrt{30}e^{\frac{1}{8}}|T|^{\frac{10}{3}},$$

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

where

$$t_0 = 4 \cdot 3^{-\frac{3}{4}} \cdot 2^{-\frac{1}{2}-\frac{1}{10}} = 1.1577....$$

This inequality is valid for all $|T| \geqslant 168$. And if $k < |T|/4$, then (42) holds for $m = |T|$ if $(5/3)^k > |T|^{10/3}$, which holds true for all $k > 5 \log |T|$. □

Remark 6.4. By Proposition 6.3, we have $\mathbb{Q}_k(T) < 1/2$ if (8) holds. We refer the reader to the proofs in Section 4 for a wider range of k satisfying (8) for each class of simple groups. For example, the proof of Proposition 4.9 shows that if $T = A_n$ and $n \geqslant 7$, then (8) holds for all $n \leqslant k \leqslant 4 \log |T|$, which implies that $\mathbb{Q}_k(T) < 1/2$ for all $n \leqslant k \leqslant |T| - n$.

Acknowledgements. The author thanks the China Scholarship Council for supporting his doctoral studies at the University of Bristol. He wishes to thank his supervisor Professor Tim Burness for his supervision and support throughout. He also thanks two anonymous referees for their helpful comments and suggestions on an earlier version of the paper.

Competing interest. The authors have no competing interest to declare.

References

[1] L. Babai, 'Finite digraphs with given regular automorphism groups', *Period. Math. Hungar.* **11** (1980), 257–270.
[2] L. Babai and C. D. Godsil, 'On the automorphism groups of almost all Cayley graphs', *European J. Combin.* **3** (1982), 9–15.
[3] R. F. Bailey and P. J. Cameron, 'Base size, metric dimension and other invariants of groups and graphs', *Bull. Lond. Math. Soc.* **43** (2011), 209–242.
[4] K. D. Blaha, 'Minimum bases for permutation groups: the greedy approximation', *J. Algorithms* **13** (1992), 297–306.
[5] W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symb. Comput.* **24** (1997), 235–265.
[6] T. Breuer, *The GAP Character Table Library, Version 1.3.1*, GAP package, 2020, http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib.
[7] T. Breuer, R. M. Guralnick and W. M. Kantor, 'Probabilistic generation of finite simple groups, II', *J. Algebra* **320** (2008), 443–494.
[8] T. C. Burness, 'Base sizes for primitive groups with soluble stabilisers', *Algebra Number Theory* **15** (2021), 1755–1807.
[9] T. C. Burness, 'Simple groups, fixed point ratios and applications', *in Local Representation Theory and Simple Groups*, EMS Ser. Lect. Math. (Eur. Math. Soc., Zürich, 2018), 267–322.
[10] T. C. Burness, 'Fixed point ratios in actions of finite classical groups. II', *J. Algebra* **309** (2007), 80–138.
[11] T. C. Burness, 'On base sizes for actions of finite classical groups', *J. Lond. Math. Soc.* **75** (2007), 545–562.
[12] T. C. Burness and M. Giudici, 'On the Saxl graph of a permutation group', *Math. Proc. Cambridge Philos. Soc.* **168** (2020), 219–248.
[13] T. C. Burness and M. Giudici, *Classical Groups, Derangements and Primes*, Australian Mathematical Society Lecture Series, vol. 25 (Cambridge University Press, Cambridge, 2016).
[14] T. C. Burness, R. M. Guralnick and J. Saxl, 'On base sizes for symmetric groups', *Bull. Lond. Math. Soc.* **43** (2011), 386–391.
[15] T. C. Burness and S. Harper, 'Computations concerning the uniform domination number of a finite simple group', http://seis.bristol.ac.uk/~tb13602/udncomp.pdf.
[16] T. C. Burness and H. Y. Huang, 'On base sizes for primitive groups of product type', *J. Pure Appl. Algebra* **227** (2023), Paper No. 107228.
[17] T. C. Burness and H. Y. Huang, 'On the Saxl graphs of primitive groups with soluble stabilisers', *Algebr. Comb.* **5** (2022), 1053–1087.
[18] T. C. Burness, M. W. Liebeck and A. Shalev, 'Base sizes for simple groups and a conjecture of Cameron', *Proc. Lond. Math. Soc.* **98** (2009), 116–162.
[19] T. C. Burness and A. R. Thomas, 'The classification of extremely primitive groups', *Int. Math. Res. Not. IMRN* 2022, 10148–10248.
[20] T. C. Burness, E. A. O'Brien and R. A. Wilson, 'Base sizes for sporadic simple groups', *Israel J. Math.* **177** (2010), 307–333.
[21] P. J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts, vol. 45 (Cambridge University Press, Cambridge, 1999).
[22] H. Chen and S. Du, 'On the Burness–Giudici conjecture', *Comm. Algebra* **51** (2023), 5019–5045.
[23] H. Duyan, Z. Halasi and A. Maróti, 'A proof of Pyber's base size conjecture', *Adv. Math.* **331** (2018), 720–747.
[24] J. B. Fawcett, 'Bases of twisted wreath products', *J. Algebra* **607** (2022), 247–271.
[25] J. B. Fawcett, 'The base size of a primitive diagonal group', *J. Algebra* **375** (2013), 302–321.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press

[26] J. Fulman and R. M. Guralnick, 'The number of regular semisimple conjugacy classes in the finite classical groups', *Linear Algebra Appl.* **439** (2013), 488–503.
[27] J. Fulman and R. M. Guralnick, 'Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements', *Trans. Amer. Math. Soc.* **364** (2012), 3023–3070.
[28] P. X. Gallagher, 'The number of conjugacy classes in a finite group', *Math. Z.* **118** (1970), 175–179.
[29] D. Garzoni and N. Gill, 'On the number of conjugacy classes of a primitive permutation group', *Proc. Roy. Soc. Edinburgh Sect. A* **153** (2023), 115–136.
[30] C. D. Godsil, 'On the full automorphism group of a graph', *Combinatorica* **1** (1981), 243–256.
[31] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups. Number 3*, Mathematical Surveys and Monographs, vol. 40 (American Mathematical Society, Providence, RI, 1998).
[32] R. Gow, 'Commutators in finite simple groups of Lie type', *Bull. London Math. Soc.* **32** (2000), 311–315.
[33] R. M. Guralnick and W. M. Kantor, 'Probabilistic generation of finite simple groups', *J. Algebra* **234** (2000), 743–792.
[34] R. M. Guralnick and G. Malle, 'Simple groups admit Beauville structures', *J. Lond. Math. Soc.* **85** (2012), 694–721.
[35] Z. Halasi, M. W. Liebeck and A. Maróti, 'Base sizes of primitive groups: bounds with explicit constants', *J. Algebra* **521** (2019), 16–43.
[36] Z. Halasi and K. Podoski, 'Every coprime linear group admits a base of size two', *Trans. Amer. Math. Soc.* **368** (2016), 5857–5887.
[37] G. A. Jones, 'Finite simple automorphism groups of edge-transitive maps', *J. Algebra* **607** (2022), 454–472.
[38] W. M. Kantor, A. Lubotzky and A. Shalev, 'Invariable generation and the Chebotarev invariant of a finite group', *J. Algebra* **348** (2011), 302–314.
[39] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129 (Cambridge University Press, Cambridge, 1990).
[40] M. Lee and T. Popiel, 'Saxl graphs of primitive affine groups with sporadic point stabilisers', *Internat. J. Algebra Comput.* **33** (2023), 369–389.
[41] D. Leemans and M. W. Liebeck, 'Chiral polyhedra and finite simple groups', *Bull. Lond. Math. Soc.* **49** (2017), 581–592.
[42] M. W. Liebeck, C. E. Praeger and J. Saxl, 'On the O'Nan–Scott theorem for finite primitive permutation groups', *J. Austral. Math. Soc.* **44** (1988), 389–396.
[43] M. W. Liebeck and G. M. Seitz, *Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie algebras*, Mathematical Surveys and Monographs, vol. 180 (Amer. Math. Soc., 2012).
[44] M. W. Liebeck and A. Shalev, 'Bases of primitive permutation groups', *in Groups, Combinatorics & Geometry (Durham, 2001)*, (World Sci. Publ., River Edge, NJ, 2003), 147–154.
[45] M. W. Liebeck and A. Shalev, 'Simple groups, permutation groups, and probability', *J. Amer. Math. Soc.* **12** (1999), 497–520.
[46] F. Lübeck, 'Centralisers and numbers of semisimple classes in exceptional groups of Lie type', http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/CentSSClasses.
[47] A. Lucchini, M. Morigi and M. Moscatiello, 'Primitive permutation IBIS groups', *J. Combin. Theory Ser. A* **184** (2021), Paper No. 105516.
[48] G. A. Miller, 'On the groups generated by two operators', *Bull. Amer. Math. Soc.* **7** (1901), 424–426.
[49] J. Morris and P. Spiga, 'Asymptotic enumeration of Cayley digraphs', *Israel J. Math.* **242** (2021), 401–459.
[50] M. Neunhöffer, F. Noeske, E. A. O'Brien and R. A. Wilson, 'Orbit invariants and an application to the Baby Monster', *J. Algebra* **341** (2011), 297–305.
[51] L. Pyber, 'Asymptotic results for permutation groups', in *Groups and Computation*, edited by L. Finkelstein and W. Kantor, DIMACS Series, vol. **11** (1993), 197–219.
[52] Á. Seress, *Permutation Group Algorithms*, Cambridge Tracts in Math. **152** (Cambridge University Press, Cambridge, 2003).
[53] Á. Seress, 'Primitive groups with no regular orbits on the set of subsets', *Bull. London Math. Soc.* **29** (1997), 697–704.
[54] Á. Seress, 'The minimal base size of primitive solvable permutation groups', *J. London Math. Soc.* **53** (1996), 243–255.
[55] N. Spaltenstein, 'Caractères unipotents de ${}^3D_4(F_q)$', *Comment. Math. Helv.* **57** (1982), 676–691.
[56] P. Stănică, 'Good lower and upper bounds on binomial coefficients', *JIPAM. J. Inequal. Pure Appl. Math.* **2** (2001), Article 30.
[57] M. Suzuki, 'On a class of doubly transitive groups', *Annals of Math.* **75** (1962), 105–145.
[58] G. Verret and B. Xia, 'Oriented regular representations of out-valency two for finite simple groups', *Ars Math. Contemp.* **22** (2022), Paper No. 7.
[59] R. A. Wilson et al., *A World-Wide-Web Atlas of Finite Group Representations*, http://brauer.maths.qmul.ac.uk/Atlas/v3/.
[60] B. Xia, 'Graphical regular representations of $(2, p)$-generated groups', Preprint, 2023, arXiv:2304.00541.
[61] B. Xia, S. Zheng and S. Zhou, 'Cubic graphical regular representations of some classical simple groups', *J. Algebra* **612** (2022), 256–280.

https://doi.org/10.1017/fms.2023.121 Published online by Cambridge University Press