Proceedings of the Edinburgh Mathematical Society (2021) **64**, 408–426
doi:10.1017/S0013091521000237

ON THE INVOLUTION FIXITY OF SIMPLE GROUPS

TIMOTHY C. BURNESS[1] AND ELISA COVATO[2]

[1] *School of Mathematics, University of Bristol, Bristol BS8 1UG, UK* (t.burness@bristol.ac.uk)
[2] *Bristol, UK* (elisa.covato@gmail.com)

(Received 2 July 2020; first published online 4 June 2021)

Abstract Let G be a finite permutation group of degree n and let $\mathrm{ifix}(G)$ be the involution fixity of G, which is the maximum number of fixed points of an involution. In this paper, we study the involution fixity of almost simple primitive groups whose socle T is an alternating or sporadic group; our main result classifies the groups of this form with $\mathrm{ifix}(T) \leqslant n^{4/9}$. This builds on earlier work of Burness and Thomas, who studied the case where T is an exceptional group of Lie type, and it strengthens the bound $\mathrm{ifix}(T) > n^{1/6}$ (with prescribed exceptions), which was proved by Liebeck and Shalev in 2015. A similar result for classical groups will be established in a sequel.

Keywords: Primitive groups; simple groups; involution fixity

2020 *Mathematics subject classification:* Primary 20B15; 20D06;
Secondary 20B35; 20D08

1. Introduction

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω. Let $\mathrm{fix}(g)$ be the number of elements in Ω fixed by $g \in G$ and set

$$\mathrm{fpr}(g, \Omega) = \frac{\mathrm{fix}(g)}{|\Omega|},$$

which is called the *fixed point ratio* of g. This is a classical concept in permutation group theory and bounds on fixed point ratios find a wide range of applications, especially in the context of primitive groups. For instance, we refer the reader to the recent survey article [5] for a discussion of some powerful applications concerning bases for permutation groups, the random generation of simple groups and the structure of monodromy groups of coverings of the Riemann sphere.

In this paper, we study $\mathrm{fix}(g)$ in the setting where G is an almost simple primitive permutation group and $g \in G$ is an involution. We call

$$\mathrm{ifix}(G) = \max\{\mathrm{fix}(g) : \ g \in G \text{ is an involution}\}$$

the *involution fixity* of G and we are interested in comparing $\mathrm{ifix}(G)$ with the degree of G. This is closely related to the more general concept of *fixity*, which is defined to be the maximal number of points fixed by a non-identity element. The latter notion was originally introduced by Ronse [21] in 1980 and there are more recent papers by Liebeck, Saxl and Shalev [17, 22] on the fixity of primitive groups (also see [18], where the transitive groups with fixity at most 2 are studied). Let us also highlight the work of Bender [2] from the early 1970s, which determines the finite transitive groups G with $\mathrm{ifix}(G) = 1$.

Our main motivation stems from [17], where Liebeck and Shalev use the O'Nan–Scott theorem to investigate the structure of the primitive groups of degree n with fixity at most $n^{1/6}$. Their main result for an almost simple group G with socle T shows that $\mathrm{ifix}(T) > n^{1/6}$, with specified exceptions (see [17, Theorem 4]). With a view towards applications, it is desirable to strengthen this lower bound (at the expense of some additional exceptions). The first step in this direction was taken by Burness and Thomas in [8], where the almost simple groups with socle an exceptional group of Lie type T and $\mathrm{ifix}(T) \leqslant n^{4/9}$ are determined. In this paper, we extend the analysis in [8] to the almost simple groups with socle an alternating or sporadic group. The remaining classical groups will be handled in a sequel, which will complete our study of involution fixity for almost simple primitive groups.

Our main result is the following. In the statement, $\mathcal{S}$ denotes the set of finite simple groups that are either alternating or sporadic.

Theorem 1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive permutation group of degree n with socle $T \in \mathcal{S}$ and point stabilizer H. Set $H_0 = H \cap T$. Then one of the following holds*:

(i) $\mathrm{ifix}(T) > n^{4/9}$.

(ii) *H_0 has odd order and* $\mathrm{ifix}(T) = 0$.

(iii) $(T, n) = (A_5, 5)$ *and* $\mathrm{ifix}(T) = 1$.

(iv) $n^{\alpha} \leqslant \mathrm{ifix}(T) \leqslant n^{4/9}$ *and* $(T, H_0, \mathrm{ifix}(T), n, \alpha)$ *is recorded in Table 1.*

Remark 1. Let us make some comments on the statement of Theorem 1.

(a) The groups arising in part (ii) with $|H_0|$ odd are determined in [15, Theorem 2] (also see [17, Lemma 2.1]). The possibilities are as follows:

T	H_0	Conditions
A_p	$\mathrm{AGL}_1(p) \cap T$	p prime, $p \equiv 3 (\mathrm{mod}\ 4)$, $G = S_p$ if $p = 7, 11, 23$
J_3, O'N	19:9, 31:15 (resp.)	$G = T.2$
M_{23}, Th, $\mathbb{B}$	23:11, 31:15, 47:23 (resp.)	

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

(b) The number α recorded in the fifth column of Table 1 is equal to $\log \mathrm{ifix}(T)/\log n$, expressed to three significant figures.

(c) The theorem reveals that there are only finitely many groups of the given form with $1 \leqslant \mathrm{ifix}(T) \leqslant n^{4/9}$. However, it is straightforward to show that there are infinitely many with $1 \leqslant \mathrm{ifix}(T) \leqslant n^{1/2}$. For example, we can take $T = A_p$ and $H = \mathrm{AGL}_1(p) \cap G$, where p is any prime with $p \equiv 1 (\mathrm{mod}\ 4)$ (see Remark 2.10).

(d) Theorem 1 already has an application in finite geometry. Indeed, we refer the reader to [1, Section 6], where the result is used to study point-primitive generalized quadrangles.

By combining Theorem 1 with [8, Theorem 1], we get the following corollary.

Corollary 2. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive permutation group of degree n with socle T and point stabilizer H. Set $H_0 = H \cap T$ and assume $|H_0|$ is even and T is not isomorphic to a classical group. Then one of the following holds*:

(i) $\mathrm{ifix}(T) > n^{1/3}$.

(ii) $(T, n) = ({}^2B_2(q), q^2 + 1)$ *and* $\mathrm{ifix}(T) = 1$.

(iii) $(T, H_0, \mathrm{ifix}(T), n) = (A_9, 3^2{:}\mathrm{SL}_2(3), 8, 840)$ *or* $(\mathrm{J}_1, 2^3{:}7^3{:}3, 5, 1045)$.

The proof of Theorem 1 is presented in § 2 and § 3, where we handle the groups with an alternating and sporadic socle, respectively. We freely employ computational methods, using GAP [10] and MAGMA [3], when it is feasible to do so. In particular, the argument for sporadic groups in § 3 makes extensive use of the character tables (and associated fusion maps) that are available in the GAP Character Table Library [4]. As one might expect, the O'Nan–Scott theorem provides a framework for our proof when the socle T is an alternating group. Indeed, this key result divides the possibilities for the point stabilizer H into several families and we proceed by considering each family in turn.

The notation we use in this paper is fairly standard. We will write C_n, or just n, for a cyclic group of order n and G^n denotes the direct product of n copies of G. An unspecified extension of G by a group H will be denoted by $G.H$; if the extension splits then we write $G{:}H$. We adopt the standard notation for simple groups of Lie type from [13], which differs slightly from the notation in [9]. All logarithms are in the natural base, unless stated otherwise.

2. Symmetric and alternating groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive permutation group of degree n with socle T and point stabilizer H. Set $H_0 = H \cap T$ and note that H is a maximal subgroup of G such that $G = HT$. Then $n = |T : H_0|$ and

$$\mathrm{fix}(t) = \frac{|t^T \cap H_0|}{|t^T|} \cdot n \tag{1}$$

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

Table 1. *The cases with* $n^{\alpha} \leqslant \text{ifix}(T) \leqslant n^{4/9}$ *in Theorem 1(iv)*

T	H_0	$\text{ifix}(T)$	n	α	Conditions
A_5	S_3	2	10	0.301	
	D_{10}	2	6	0.386	
A_6	$3^2{:}4$	2	10	0.301	
	A_5	2	6	0.386	$G = A_6$ or S_6
	D_{10}	4	36	0.386	$G = \mathrm{M}_{10}$, $\mathrm{PGL}_2(9)$ or $A_6.2^2$
	S_4	3	15	0.405	$G = A_6$ or S_6
	D_8	5	45	0.422	$G = \mathrm{M}_{10}$, $\mathrm{PGL}_2(9)$ or $A_6.2^2$
A_7	$\mathrm{L}_2(7)$	3	15	0.405	$G = A_7$
A_9	$3^2{:}\mathrm{SL}_2(3)$	8	840	0.308	
	$\mathrm{L}_2(8){:}3$	8	120	0.434	$G = A_9$
A_{10}	M_{10}	24	2520	0.405	
A_{11}	M_{11}	24	2520	0.405	$G = A_{11}$
J_1	$2^3{:}7{:}3$	5	1045	0.231	
	$11{:}10$	12	1596	0.336	
	$7{:}6$	20	4180	0.359	
	$19{:}6$	20	1540	0.408	
	$\mathrm{L}_2(11)$	10	266	0.412	
J_2	A_5	60	10080	0.444	
J_3	$2^4{:}(3 \times A_5)$	50	17442	0.400	
	$2^{2+4}{:}(3 \times S_3)$	85	43605	0.415	
	$3^2.3^{1+2}{:}8$	80	25840	0.431	
McL	$3^{1+4}{:}2S_5$	56	15400	0.417	
He	$7^2{:}2.\mathrm{L}_2(7)$	64	244800	0.335	
O'N	$3^4{:}2^{1+4}D_{10}$	1064	17778376	0.417	
Co_1	$5^2{:}2A_5$	3244032	1385925602181120	0.430	
HN	$\mathrm{U}_3(8){:}3$	800	16500000	0.402	
Th	$2^5.\mathrm{L}_5(2)$	2169	283599225	0.394	
	$7^2{:}(3 \times 2S_4)$	645120	12860819712000	0.443	

for all $t \in T$, where t^T denotes the conjugacy class of t in T. We will adopt this notation for the remainder of the paper.

In this section, we prove Theorem 1 for the groups with socle $T = A_m$. Recall that if $t \in T$ is an involution with cycle-shape $(2^k, 1^{m-2k})$, then

$$|t^T| = \frac{m!}{k!(m-2k)!2^k}.$$

We begin by handling the groups with $m \leqslant 25$.

Proposition 2.1. *The conclusion to Theorem 1 holds if* $m \leqslant 25$.

Proof. This is a straightforward Magma [3] computation. First assume $G = A_m$ or S_m. Working in the natural permutation representation of degree m, we use the function MaximalSubgroups to construct a set of representatives of the conjugacy classes of maximal

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

subgroups H of G. Given an involution $t \in T$, we can then compute $|t^T \cap H_0|$ and $|t^T|$, which gives $\mathrm{fix}(t)$ via (1). We then obtain $\mathrm{ifix}(T)$ by taking the maximum over a set of representatives of the conjugacy classes of involutions in T and the desired result quickly follows. Finally, if $T = A_6$ and G is one of $\mathrm{PGL}_2(9)$, M_{10} or $A_6.2^2$ then we can proceed in an entirely similar manner, working with a permutation representation of G of degree 10. □

For the remainder of this section, we may assume $G = A_m$ or S_m with $m > 25$. Our aim is to establish the bound $\mathrm{ifix}(T) > n^{4/9}$.

The possibilities for H are described by the O'Nan–Scott theorem (see [14], for example), which divides the maximal subgroups of G into the following families (in parts (e) and (f), S denotes a non-abelian finite simple group):

(a) *Intransitive*: $H = (S_k \times S_{m-k}) \cap G$, $1 \leqslant k < m/2$.

(b) *Imprimitive*: $H = (S_k \wr S_r) \cap G$, $m = kr$, $1 < k < m$.

(c) *Affine*: $H = \mathrm{AGL}_d(p) \cap G$, $m = p^d$, p prime, $d \geqslant 1$.

(d) *Product-type*: $H = (S_k \wr S_r) \cap G$, $m = k^r$, $k \geqslant 5$, $r \geqslant 2$.

(e) *Diagonal-type*: $H = (S^k.(\mathrm{Out}(S) \times S_k)) \cap G$, $m = |S|^{k-1}$, $k \geqslant 2$.

(f) *Almost simple*: $S \leqslant H \leqslant \mathrm{Aut}(S)$, $m = |H : K|$ for some maximal subgroup K of H.

We will consider each family of subgroups in turn. Before we begin the analysis of case (a), let us record some useful preliminary lemmas.

Lemma 2.2. *Suppose $|H_0|$ is even, $|H_0| \leqslant |T|^\alpha$ and $|t^T| \leqslant |T|^\beta$ for every involution $t \in H_0$. Then $\mathrm{ifix}(T) > n^{4/9}$ if $5 - 5\alpha - 9\beta > 0$.*

Proof. Let $t \in H_0$ be an involution. Then $|t^T \cap H_0| \geqslant 1$ and $|t^T| \leqslant |T|^\beta$, so $\mathrm{fix}(t) \geqslant n|T|^{-\beta}$ and thus $\mathrm{ifix}(T) > n^{4/9}$ if $n > |T|^{9\beta/5}$. The result now follows since $n = |T : H_0| \geqslant |T|^{1-\alpha}$. □

Lemma 2.3. *If $T = A_m$ and $m > 20$, then $|t^T| < |T|^{11/20}$ for every involution $t \in T$.*

Proof. The groups with $m \leqslant 54$ can be checked using Magma, so let us assume $m \geqslant 55$. Recall that if G is a finite group and $\mathcal{I}(G)$ is the set of involutions in G, then $|\mathcal{I}(G)|^2 < k(G) \cdot |G|$, where $k(G)$ is the number of conjugacy classes of G (see [12, Chapter 4], for example). As a special case, we deduce that

$$|\mathcal{I}(S_m)|^2 < m!p(m),$$

where $p(m)$ is the partition function, and thus it suffices to show that

$$2^{11}p(m)^{10} < m!. \tag{2}$$

Indeed, if this inequality holds then $|\mathcal{I}(S_m)| < |T|^{11/20}$ and the desired bound follows.

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

By the main theorem of [19], we have $p(m) < m^{-3/4}e^{c\sqrt{m}}$, where $c = \pi\sqrt{2/3}$, so (2) holds if $f(m) > 1$, where

$$f(m) := \frac{m^{15/2}m!}{2^{11}e^{10c\sqrt{m}}}.$$

For $m \geqslant 55$ we have

$$\frac{f(m+1)}{f(m)} = \frac{\left(1+\frac{1}{m}\right)^{15/2}(m+1)}{e^{10c(\sqrt{m+1}-\sqrt{m})}} \geqslant \frac{m}{6} > 1,$$

so f is an increasing function and the result follows since $f(55) > 1$. □

Lemma 2.4. *Let $T = A_m$ with $m > 20$. If $|H_0|$ is even and $|H_0|^{100} < |T|$, then* $\mathrm{ifix}(T) > n^{4/9}$.

Proof. This follows by combining Lemmas 2.2 and 2.3. □

2.1. Intransitive subgroups

In this section, we will assume $H = (S_k \times S_{m-k}) \cap G$ is a maximal intransitive subgroup of G, where $1 \leqslant k < m/2$. We may identify Ω with the set of k-element subsets of $\{1, \ldots, m\}$. In particular, $n = \binom{m}{k}$.

Proposition 2.5. *If $m \geqslant 7$, then* $\mathrm{ifix}(T) > n^{1/2}$.

Proof. We claim that $\mathrm{fix}(t) > n^{1/2}$, where $t = (1,2)(3,4) \in T$. If $k = 1$ then $n = m$, $\mathrm{fix}(t) = m - 4$ and the result follows. Now assume $k \geqslant 2$. Clearly, t fixes a k-set Γ if and only if $\Gamma \cap \{1,2,3,4\}$ is either empty, or one of $\{1,2\}$, $\{3,4\}$ or $\{1,2,3,4\}$. Therefore,

$$\mathrm{fix}(t) = \binom{m-4}{k} + 2\binom{m-4}{k-2} + \binom{m-4}{k-4}$$

where the final term is 0 if $k = 2$ or 3. The cases with $m < 10$ can be checked directly, so let us assume $m \geqslant 10$. We claim that

$$\binom{m-4}{k} + 2\binom{m-4}{k-2} > \binom{m}{k}^{1/2}, \tag{3}$$

which implies that $\mathrm{fix}(t) > n^{1/2}$.

To see this, we first express the binomial coefficients $\binom{m-4}{k}$ and $\binom{m-4}{k-2}$ in terms of $\binom{m}{k}$ and we deduce that it suffices to show that

$$\binom{m}{k}^{1/2}\left(\frac{f(k)g(k)}{m(m-1)(m-2)(m-3)}\right) > 1,$$

where $f(k) = (m-k)(m-k-1)$ and $g(k) = 2k(k-1) + (m-k-2)(m-k-3)$. Since $k \leqslant \frac{1}{2}(m-1)$, we calculate that $f(k) \geqslant \frac{1}{4}(m^2-1)$ and $g(k) \geqslant \frac{2}{3}m^2 - 4m + \frac{21}{4}$. In addition, we have $\binom{m}{k} \geqslant \binom{m}{2}$ and thus (3) holds if $h(m) > 1$, where

$$h(m) := \frac{\binom{m}{2}^{\frac{1}{2}}(m+1)\left(\frac{2}{3}m^2 - 4m + \frac{21}{4}\right)}{4m(m-2)(m-3)}.$$

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

Now

$$\frac{h(m+1)}{h(m)} = \left(\frac{m+1}{m-1}\right)^{1/2} \cdot \frac{h_1(m)}{h_2(m)}$$

with

$$h_1(m) = m(m+2)(m-3)\left(\frac{2}{3}m^2 - \frac{8}{3}m + \frac{23}{12}\right) = h_2(m) + \frac{11}{2}m^2 - \frac{41}{4}m + \frac{21}{4} > h_2(m),$$

so $h(m)$ is an increasing function and the result follows since $h(10) > 1$. □

2.2. Imprimitive subgroups

Next, we turn to the imprimitive subgroups of the form $H = (S_k \wr S_r) \cap G$, where $m = kr$ and $1 < k < m$. We identify Ω with the set of partitions of $\{1, \dots, m\}$ into r subsets of size k. Note that

$$n = |\Omega| = \frac{(kr)!}{k!^r r!} =: f(k, r).$$

Proposition 2.6. *If $m \geqslant 9$, then* $\mathrm{ifix}(T) > n^{1/2}$.

Proof. We claim that $\mathrm{fix}(t) > n^{1/2}$ for $t = (1, 2)(3, 4) \in T$.

First assume $k = 2$, so $r \geqslant 5$. Clearly, t stabilizes a partition in Ω if and only if the partition contains $\{1, 2\}$ and $\{3, 4\}$, or $\{1, 3\}$ and $\{2, 4\}$, or $\{1, 4\}$ and $\{2, 3\}$. Therefore, $\mathrm{fix}(t) = 3f(2, r-2)$ and it suffices to show that $g(r) > 1$, where

$$g(r) := \frac{9f(2, r-2)^2}{f(2, r)}.$$

Now

$$\frac{g(r+1)}{g(r)} = \frac{(2r-3)^2}{2r+1} > 1,$$

so $g(r)$ is an increasing function and the result follows since $g(5) > 1$.

Now assume $k \geqslant 3$. A partition in Ω is fixed by t if and only if it has a part containing $\{1, 2\}$ and another containing $\{3, 4\}$, or $k \geqslant 4$ and it has a part containing $\{1, 2, 3, 4\}$. Therefore,

$$\mathrm{fix}(t) = \binom{m-4}{k-2}\binom{m-k-2}{k-2} f(k, r-2) + \binom{m-4}{k-4} f(k, r-1)$$

and it suffices to show that

$$g(k, r) := \binom{kr-4}{k-2}^2 \binom{kr-k-2}{k-2}^2 \frac{f(k, r-2)^2}{f(k, r)} > 1.$$

We claim that if k is fixed then $g(k, r)$ is increasing as a function of r. To see this, first observe that

$$\frac{g(k, r+1)}{g(k, r)} = \frac{r}{(r-1)^2}\binom{kr+k-4}{k}\frac{(m-1)(m-2)(m-3)}{(m+k-1)(m+k-2)(m+k-3)}$$

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

and we have the bounds

$$\binom{kr+k-4}{k} \geqslant \left(r+1-\frac{4}{k}\right)^k \geqslant \left(r-\frac{1}{3}\right)^k$$

and

$$\frac{(m-1)(m-2)(m-3)}{(m+k-1)(m+k-2)(m+k-3)} \geqslant \left(\frac{m-3}{m+k-3}\right)^3 \geqslant \left(\frac{k}{6}+1\right)^{-3}$$

since $k \geqslant 3$ and $m \geqslant 9$. It is routine to check that

$$\left(r-\frac{1}{3}\right)^k \geqslant (r-1)\left(\frac{k}{6}+1\right)^3$$

and this justifies the claim.

Therefore, for $k \geqslant 4$, we have

$$g(k,r) \geqslant g(k,2) = \binom{2k-4}{k-2}^2 \frac{1}{f(k,2)}$$

and

$$\frac{g(k+1,2)}{g(k,2)} = \frac{2(2k-3)^2(k+1)}{(k-1)^2(2k+1)} > 1,$$

so $g(k,r) \geqslant g(4,2) > 1$. Similarly, if $k = 3$ then $r \geqslant 3$ and $g(3,r) \geqslant g(3,3) > 1$. The result follows. □

2.3. Affine subgroups

In this section, we assume $H = \mathrm{AGL}_d(p) \cap G$ and $m = p^d$, where p is a prime and $d \geqslant 1$. Note that

$$n = |\Omega| \geqslant \frac{|T|}{|\mathrm{AGL}_d(p)|} = \frac{(p^d-1)!}{2|\mathrm{GL}_d(p)|}.$$

Write $\mathrm{AGL}_d(p) = V{:}L$, where $V = (\mathbb{F}_p)^d$ and $L = \mathrm{GL}(V)$. Now $\mathrm{AGL}_d(p)$ acts faithfully on V by affine transformations $(v,x) : u \mapsto v + u^x$ and this embeds $\mathrm{AGL}_d(p)$ in S_m. Note that if $t = (v,x) \in \mathrm{AGL}_d(p)$ then $t^2 = 1$ if and only if $v^x = -v$ and $x^2 = 1$.

Definition 2.7. Fix a basis $\{e_1,\ldots,e_d\}$ for V. With respect to this basis, let us define $x_k = [-I_k, I_{d-k}]$ if $p \neq 2$ and $x_k = [A^k, I_{d-2k}]$ if $p = 2$, where $A = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$. In particular, if $p = 2$ then $1 \leqslant k \leqslant d/2$ and x_k is a block-diagonal matrix with k blocks equal to A. For $k \geqslant 1$ set $t_k = (v, x_k) \in \mathrm{AGL}_d(p)$, where $v = e_1$ if $p \neq 2$, otherwise $v = 0$. Note that t_k is an involution.

Lemma 2.8. *Let $t = t_k \in \mathrm{AGL}_d(p)$. Then t has cycle-shape $(2^{p^{d-k}(p^k-1)/2}, 1^{p^{d-k}})$ as an element of S_m and we have $|C_{\mathrm{AGL}_d(p)}(t)| = p^{d-k}|C_{\mathrm{GL}_d(p)}(x_k)|$.*

Proof. First consider the cycle-shape of t. Since t is an involution, it suffices to show that it fixes exactly p^{d-k} vectors in V. Suppose $w = \sum_i a_i e_i \in V$ is fixed by t.

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

First assume $p \neq 2$. Here $w = w^t = w^{x_k} + e_1$ and thus

$$\sum_{i=1}^{d} a_i e_i = (-a_1 + 1)e_1 + \sum_{i=2}^{k}(-a_i)e_i + \sum_{i=k+1}^{d} a_i e_i,$$

so $a_1 = \frac{1}{2}$ and $a_i = 0$ for $2 \leqslant i \leqslant k$. There are no conditions on the coefficients a_i for $i > k$, so t fixes precisely p^{d-k} vectors and the result follows. Similarly, if $p = 2$ then $w = w^t = w^{x_k}$ and

$$\sum_{i=1}^{d} a_i e_i = \sum_{i=1}^{k}(a_{2i}e_{2i-1} + a_{2i-1}e_{2i}) + \sum_{i=2k+1}^{d} a_i e_i,$$

which implies that $a_{2i-1} = a_{2i}$ for $1 \leqslant i \leqslant k$. Therefore, t fixes $2^k 2^{d-2k} = 2^{d-k}$ vectors as claimed.

Now let us consider the centralizer of t. Suppose $p \neq 2$ and $(u, y) \in \mathrm{AGL}_d(p)$. Then (u, y) centralizes t if and only if $y \in C_{\mathrm{GL}_d(p)}(x_k) = \mathrm{GL}_k(p) \times \mathrm{GL}_{d-k}(p)$ and $u + e_1^y = e_1 + u^{x_k}$. Given $y \in C_{\mathrm{GL}_d(p)}(x_k)$, a straightforward calculation shows that there are p^{d-k} vectors $u \in V$ such that $u + e_1^y = e_1 + u^{x_k}$ and thus

$$|C_{\mathrm{AGL}_d(p)}(t)| = p^{d-k}|C_{\mathrm{GL}_d(p)}(x_k)| = p^{d-k}|\mathrm{GL}_k(p)||\mathrm{GL}_{d-k}(p)|.$$

Similarly, if $p = 2$ then $(u, y) \in \mathrm{AGL}_d(2)$ centralizes t if and only if $y \in C_{\mathrm{GL}_d(2)}(x_k)$ and $u^{x_k} = u$. Since the 1-eigenspace of x_k on V is $(d-k)$-dimensional, we get

$$|C_{\mathrm{AGL}_d(2)}(t)| = 2^{d-k}|C_{\mathrm{GL}_d(2)}(x_k)| = 2^{d-k+2dk-3k^2}|\mathrm{GL}_k(2)||\mathrm{GL}_{d-2k}(2)|$$

and the result follows. □

Proposition 2.9. *If $d = 1$ then one of the following holds:*

(i) $p \equiv 3 \pmod 4$ *and* $\mathrm{ifix}(T) = 0$.

(ii) $p = 5$, $n = 6$ *and* $\mathrm{ifix}(T) = 2$.

(iii) $p \equiv 1 \pmod 4$, $p \geqslant 13$ *and* $\mathrm{ifix}(T) > n^{4/9}$.

Proof. First note that $H_0 = p{:}\frac{1}{2}(p-1)$ and $n = (p-2)!$. In particular, if $p \equiv 3 (\mathrm{mod}\ 4)$ then $|H_0|$ is odd and thus $\mathrm{ifix}(T) = 0$ as claimed. Now assume $p \equiv 1 (\mathrm{mod}\ 4)$. If $p = 5$ then $H_0 = D_{10}$ and $\mathrm{ifix}(T) = 2$, so let us assume $p \geqslant 13$. Let $t \in H_0$ be an involution. By applying Lemma 2.8, noting that H_0 has a unique conjugacy class of involutions, we deduce that

$$|t^T \cap H_0| = p, \quad |t^T| = \frac{p!}{2^{(p-1)/2}\left(\frac{1}{2}(p-1)\right)!}$$

and thus (1) gives

$$\mathrm{ifix}(T) = \mathrm{fix}(t) = \frac{2^{(p-1)/2}\left(\frac{1}{2}(p-1)\right)!}{p-1}. \tag{4}$$

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

It follows that $\mathrm{ifix}(T) > n^{4/9}$ if and only if $f(p) > 1$, where

$$f(p) := \frac{2^{(p-1)/2}\left(\frac{1}{2}(p-1)\right)!}{(p-1)(p-2)!^{4/9}}.$$

The result now follows since $f(p+2) = (p-1)^{5/9}p^{-4/9}f(p) > f(p)$ and $f(13) > 1$. □

Remark 2.10. The proof of Proposition 2.9 reveals that there are infinitely many groups G as in Theorem 1 with $1 \leqslant \mathrm{ifix}(T) \leqslant n^{1/2}$. Indeed, if we take $T = A_p$ and $H = \mathrm{AGL}_1(p) \cap G$, where p is a prime such that $p \equiv 1 (\mathrm{mod}\ 4)$, then $\mathrm{ifix}(T)$ is given in (4) and we deduce that $\mathrm{ifix}(T) > n^{1/2}$ if and only if $g(p) > 1$, where

$$g(p) := \frac{2^{(p-1)/2}\left(\frac{1}{2}(p-1)\right)!}{(p-1)(p-2)!^{1/2}}.$$

Since $g(p+2) < (p/(p-1))^{1/2}g(p+2) = g(p)$ and $g(5) < 1$, it follows that $\mathrm{ifix}(T) \leqslant n^{1/2}$ for every prime p with $p \equiv 1(\mathrm{mod}\ 4)$.

Proposition 2.11. *If $d \geqslant 2$ then either $\mathrm{ifix}(T) > n^{4/9}$ or $(d, p, \mathrm{ifix}(T), n) = (2, 3, 8, 840)$.*

Proof. First assume $d = 2$, so $m = p^2$ and p is odd. If $p = 3$ or 5 then the result follows from Proposition 2.1, so let us assume $p \geqslant 7$. As in Definition 2.7, set $t = t_2 = (e_1, x_2) \in H_0$. By applying Lemma 2.8, we deduce that

$$|t^T \cap H_0| \geqslant |t^{H_0}| = p^2, \quad |t^T| = \frac{(p^2)!}{2^{(p^2-1)/2}\left(\frac{1}{2}(p^2-1)\right)!}$$

and thus $\mathrm{ifix}(T) > n^{4/9}$ if $f(p) > 1$, where

$$f(p) := \frac{2^{(p^2-1)/2}p^{1/3}\left(\frac{1}{2}(p^2-1)\right)!}{(p-1)^{5/9}(p^2-1)^{5/9}(p^2)!^{4/9}}.$$

We claim that $f(p+2) > f(p)$. To see this, set $k = (p^2+4p+3)/2$ and observe that

$$\frac{f(p+2)}{f(p)} = \alpha \cdot 2^{2p+1}\frac{k!}{(k-2p-2)!}\left(\frac{(2k-4p-3)!}{(2k+1)!}\right)^{4/9}$$

where

$$\alpha = 2\left(\frac{p-1}{p+1}\right)^{5/9}\left(\frac{p+2}{p}\right)^{1/3}\left(\frac{p^2-1}{2k}\right)^{5/9} > 1.$$

By taking logarithms and using the bound $-x/(1-x) < \log(1-x) < -x$ for all $0 < x < 1$, it is straightforward to show that

$$a^b e^{-b(b-1)/2(a-b)} \leqslant \frac{a!}{(a-b)!} \leqslant a^b e^{-b(b-1)/2a} \tag{5}$$

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

for all integers $1 \leqslant b < a$. This implies that

$$\frac{f(p+2)}{f(p)} > \frac{1}{2}e^{\beta}\left(\frac{2k}{(2k+1)^{8/9}}\right)^{2p+2},$$

where

$$\beta = \frac{4}{9}\cdot\frac{(4p+4)(4p+3)}{4k+2} - \frac{(2p+2)(2p+1)}{2(k-2p-2)}.$$

One checks that this lower bound is minimal when $p=7$, which gives $f(p+2) > f(p)$ as claimed. Moreover, since $f(7) > 1$, we conclude that $\mathrm{ifix}(T) > n^{4/9}$.

Now assume $d \geqslant 3$. If $p=2$ and $d \leqslant 6$, then a Magma calculation gives $\mathrm{ifix}(T) > n^{4/9}$. Similarly, one can check that the same conclusion holds if $p=3$ and $d \leqslant 4$. In order to establish the desired bound in the remaining cases, set $t = t_2 \in H_0$ and note that t has cycle-shape $(2^{p^{d-2}(p^2-1)/2}, 1^{p^{d-2}})$ by Lemma 2.8. Now $|t^T \cap H_0| \geqslant 1$ and $|\mathrm{GL}_d(p)| < p^{d^2}$, so $n > (p^d)!p^{-d(d+1)}$ and it follows that $\mathrm{ifix}(t) > n^{4/9}$ if $g(d,p) > 1$, where

$$g(d,p) := \frac{(\frac{1}{2}p^{d-2}(p^2-1))!\,\left(p^{d-2}\right)!2^{p^{d-2}(p^2-1)/2}}{p^{5d(d+1)/9}\,(p^d)!^{4/9}}.$$

If d is fixed, then by arguing as above one can show that $g(d,p)$ is an increasing function in p. Similarly, one checks that if p is fixed, then $g(d,p)$ is increasing as a function of d (here we are assuming that $d \geqslant 7$ if $p=2$ and $d \geqslant 5$ if $p=3$, which is valid in view of the above remarks). Therefore, for $p \geqslant 5$, we have $g(d,p) \geqslant g(3,5) > 1$. Similarly, if $p=3$ and $d \geqslant 5$ then $g(d,p) \geqslant g(5,3) > 1$ and for $p=2$ with $d \geqslant 7$ we get $g(d,p) \geqslant g(7,2) > 1$. We conclude that $\mathrm{ifix}(T) > n^{4/9}$ if $d \geqslant 3$ and the proof of the proposition is complete. □

2.4. Product-type subgroups

Now assume H is a product-type subgroup of G, so $H = (S_k \wr S_r) \cap G$ and $m = k^r$, where $k \geqslant 5$ and $r \geqslant 2$. Set $\Gamma = \{1,\ldots,k\}$ and note that the embedding of H in G arises from the product action of H on the Cartesian product Γ^r. That is, for every $(x_1,\ldots,x_r)\sigma \in H$ and $(\gamma_1,\ldots,\gamma_r) \in \Gamma^r$ we have

$$(\gamma_1,\ldots,\gamma_r)^{(x_1,\ldots,x_r)\sigma} = (\gamma_1^{x_1},\ldots,\gamma_r^{x_r})^{\sigma} = \left(\gamma_{1^{\sigma^{-1}}}^{x_{1^{\sigma^{-1}}}},\ldots,\gamma_{r^{\sigma^{-1}}}^{x_{r^{\sigma^{-1}}}}\right).$$

In particular, let us observe that

$$n \geqslant \frac{(k^r)!}{2(k!)^r r!}.$$

Proposition 2.12. *If H is a product-type subgroup of G, then* $\mathrm{ifix}(T) > n^{4/9}$.

Proof. Fix the involution $t = (t_1, 1, \ldots, 1) \in (A_k)^r < H_0$, where $t_1 = (1,2)(3,4) \in A_k$. By considering the action of H on Γ^r, it is easy to see that t has exactly $(k-4)k^{r-1}$

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

fixed points and so it has cycle-shape $(2^{2k^{r-1}}, 1^{(k-4)k^{r-1}})$ as an element of T. Therefore,

$$|t^T| = \frac{(k^r)!}{2^{2k^{r-1}}(2k^{r-1})!((k-4)k^{r-1})!}$$

and using the trivial bound $|t^T \cap H_0| \geqslant 1$ we deduce that $\mathrm{fix}(t) > n^{4/9}$ if $f(k,r) > 1$, where

$$f(k,r) := \frac{2^{18k^{r-1}-5}(2k^{r-1})!^9((k-4)k^{r-1})!^9}{(k^r)!^4(k!)^{5r}(r!)^5}.$$

A routine calculation shows that if k is fixed, then $f(k,r)$ is an increasing function in r, so we may assume $r=2$. If $k=5$ then $m=25$ and so this case was handled in Proposition 2.1. Similarly, if $k=6$ then an easy Magma computation shows that $\mathrm{ifix}(T) > n^{4/9}$. Finally, if $k \geqslant 7$ then

$$\frac{f(k+1,2)}{f(k,2)} = 2^{27}\frac{(2k+1)^9}{k+1}\left(\frac{(k^2)!}{(k^2+2k+1)!}\right)^4\left(\frac{(k^2-2k-3)!}{(k^2-4k)!}\right)^9$$

and by applying the bounds in (5) it is straightforward to show that this ratio is greater than 1. In particular, $f(k,2)$ is an increasing function in k and the result follows since $f(7,2) > 1$. □

2.5. Diagonal-type subgroups

Here $H = (S^k.(\mathrm{Out}(S) \times S_k)) \cap G$ and $m = |S|^{k-1}$, where $k \geqslant 2$ and S is a non-abelian finite simple group. The embedding of H in G is afforded by a natural (faithful) action of H on the set of cosets of the diagonal subgroup $\{(s,\dots,s) : s \in S\}$ of S^k.

Proposition 2.13. *If H is a diagonal-type subgroup of G, then* $\mathrm{ifix}(T) > n^{4/9}$.

Proof. First assume $m < 200$, so $k=2$ and S is isomorphic to A_5 or $\mathrm{L}_2(7)$. In both cases, we can use the database of primitive groups in Magma to construct H as a subgroup of S_m and then it is a routine computation to check that $5-5\alpha-9\beta > 0$ for constants α and β such that $|H_0| \leqslant |T|^\alpha$ and $|t^T| \leqslant |T|^\beta$ for every involution $t \in H_0$. Therefore, $\mathrm{ifix}(T) > n^{4/9}$ by Lemma 2.2.

For the remainder, we may assume $m \geqslant 200$. We claim that $|H_0|^{100} < |T|$ and thus $\mathrm{ifix}(T) > n^{4/9}$ by Lemma 2.4. To see this, let us first observe that $|\mathrm{Out}(S)| \leqslant |S|/30$ by [20, Lemma 2.2], so $|H_0| \leqslant \ell^{k+1}k!/30$ where $\ell = |S|$. It follows that $|H_0|^{100} < |T|$ if $f(k,\ell) > 1$, where

$$f(k,\ell) := \frac{1}{2}\left(\frac{30}{\ell^{k+1}k!}\right)^{100}(\ell^{k-1})!$$

If $k=2$ then $m=\ell$ and the condition $m \geqslant 200$ implies that $\ell \geqslant 360$ since A_6 is the smallest non-abelian simple group with order at least 200 (up to isomorphism). For $\ell \geqslant$

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

360 we have

$$\frac{f(2,\ell+1)}{f(2,\ell)} = \left(\frac{\ell}{\ell+1}\right)^{300}(\ell+1) > 1,$$

so $f(2,\ell)$ is increasing as a function of ℓ and we have $f(2,360) > 1$. Similarly, if $k \geqslant 3$ then $\ell \geqslant 60$ and $f(k,\ell)$ is an increasing function in both k and ℓ. The result now follows since $f(3,60) > 1$. □

2.6. Almost simple subgroups

To complete the proof of Theorem 1 for symmetric and alternating groups, we may assume that $T = A_m$ with $m > 25$ and H is an almost simple subgroup acting primitively on $\Gamma = \{1,\ldots,m\}$. We will write S to denote the socle of H (note that $S \neq T$ since H is a core-free subgroup of G).

First we handle the low degree groups with $m \leqslant 600$.

Proposition 2.14. *If* $25 < m \leqslant 600$ *then* $\mathrm{ifix}(T) > n^{4/9}$.

Proof. To construct H as a subgroup of G we use the database of primitive groups in Magma, via the command

```
PrimitiveGroups([26..600] : Filter:="AlmostSimple").
```

Once we have removed the groups with $S = T$, we are left with 766 cases to consider. Define

$$\alpha(J) = \max\left\{\frac{|t^J|}{|t^T|} : t \in J \text{ is an involution}\right\}$$

for each subgroup J of H_0. Given a specific subgroup J, we can compute $\alpha(J)$ by finding a set of representatives for the conjugacy classes of involutions in J and then for each representative t we compute the number of fixed points of t on $\{1,\ldots,m\}$, which allows us to calculate $|t^T|$. Note that $\mathrm{ifix}(T) \geqslant \alpha(J)n$.

For $m \leqslant 60$, it is easy to check that $\alpha(H_0) > n^{-5/9}$ and thus $\mathrm{ifix}(T) > n^{4/9}$. Similarly, if $60 < m \leqslant 600$ and P is a Sylow 2-subgroup of H_0, then $\alpha(P) > n^{-5/9}$ and the result follows (this approach avoids the problem of computing a set of conjugacy class representatives in H_0, which can be expensive in terms of time and memory). □

For the remainder, we may assume $m > 600$. Our basic aim is to establish the bound

$$|H_0|^{100} < |T| \tag{6}$$

whenever possible, noting that this gives $\mathrm{ifix}(T) > n^{4/9}$ via Lemma 2.4. To do this, it will be convenient to make a distinction between the cases where H is standard or non-standard, according to the following definition.

Definition 2.15. Let $H \leqslant \mathrm{Sym}(\Gamma)$ be an almost simple primitive group with socle S and point stabilizer K. Then H is *standard* if one of the following holds:

(i) $S = A_k$ is an alternating group and Γ is a set of subsets or partitions of $\{1,\ldots,k\}$.

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

(ii) S is a classical group with natural module V and Γ is a set of subspaces (or pairs of subspaces) of V.

(iii) $S = \mathrm{Sp}_{2d}(q)$, q is even and $K \cap S = \mathrm{O}^{\pm}_{2d}(q)$.

In all other cases, H is *non-standard*.

This definition facilitates the statement of the following key result of Liebeck and Saxl (see [16, Proposition 2]).

Proposition 2.16. *Let $H \leqslant \mathrm{Sym}(\Gamma)$ be a non-standard almost simple primitive group of degree $m \geqslant 25$. Then $|H| < m^5$.*

With this proposition in hand, we can very quickly reduce the problem to the groups where H is standard.

Proposition 2.17. *If $m > 600$ and H is non-standard, then* $\mathrm{ifix}(T) > n^{4/9}$.

Proof. Here $|H| < m^5$ by Proposition 2.16 and one can check that $2m^{500} < m!$ (since $m > 600$). Therefore (6) holds and the result follows. □

Proposition 2.18. *If $m > 600$, H is standard and S is alternating, then* $\mathrm{ifix}(T) > n^{4/9}$.

Proof. Write $S = A_k$ and first assume that the embedding of H in G is afforded by the action of H on the set of ℓ-element subsets of $\{1, \ldots, k\}$, so $m = \binom{k}{\ell}$ and $2 \leqslant \ell < k/2$. Note that $k \geqslant 12$ since $m > 600$. Now $m \geqslant \binom{k}{2} = \frac{1}{2}k(k-1)$ and it is straightforward to check that

$$|H_0|^{100} \leqslant (k!)^{100} < \frac{1}{2}\left(\frac{1}{2}k(k-1)\right)! \leqslant |T|$$

for all $k \geqslant 98$. Similarly, if $k \leqslant 97$ and $\ell \geqslant 3$ then $m \geqslant \binom{k}{3}$ and one checks that (6) holds, so we may assume that $\ell = 2$, $36 \leqslant k \leqslant 97$ and $m = \frac{1}{2}k(k-1)$. Here we compute

$$\alpha = \frac{\log k!}{\log |T|}, \quad \beta = \frac{\log \gamma}{\log |T|}, \tag{7}$$

where

$$\gamma = \max\left\{\frac{m!}{2^{2j}(2j)!(m-4j)!} : 1 \leqslant j \leqslant m/4\right\}$$

is the size of the largest conjugacy class of involutions in T. One checks that $5 - 5\alpha - 9\beta > 0$ in each case, whence $\mathrm{ifix}(T) > n^{4/9}$ by Lemma 2.2.

Now assume that the embedding of H corresponds to the action on the set of partitions of $\{1, \ldots, k\}$ into r subsets of size ℓ, where $1 < \ell < k$. Here $m = k!/(\ell!)^r r!$ and the condition $m > 600$ implies that $k \geqslant 10$. It is easy to check that $m \geqslant \binom{k}{4}$ and by arguing as in the previous paragraph, we deduce that (6) holds if $k \geqslant 12$. The same bound also holds when $k = 10$ since $r = 5$, $\ell = 2$ and $m = 945$. □

In order to complete the proof of Theorem 1 for $T = A_m$, we may assume that $m > 600$ and H is an almost simple classical group over $\mathbb{F}_q$ with socle S. Let V be the natural module for S and set $\ell = \dim V$. In view of Proposition 2.17, we may also assume that $H \leqslant \mathrm{Sym}(\Gamma)$ is a *standard* group, which means that Γ is either a set of subspaces (or pairs of subspaces) of V, or $S = \mathrm{Sp}_\ell(q)$, q is even and Γ is the set of cosets of a subgroup $\mathrm{O}^{\pm}_\ell(q)$ of S (see Definition 2.15). Let K be a point stabilizer for the action of H on Γ, so $m = |H : K|$.

Remark 2.19. Due to the existence of a number of exceptional isomorphisms among the low-dimensional classical groups, we may assume that S is one of the following:

$$\mathrm{L}_\ell(q),\ \ell \geqslant 2;\ \mathrm{U}_\ell(q),\ \ell \geqslant 3;\ \mathrm{PSp}_\ell(q),\ \ell \geqslant 4;\ \mathrm{P\Omega}^\epsilon_\ell(q),\ \ell \geqslant 7.$$

In addition, in view of the isomorphisms

$$\mathrm{L}_2(4) \cong \mathrm{L}_2(5) \cong A_5,\ \mathrm{L}_2(9) \cong \mathrm{PSp}_4(2)' \cong A_6,\ \mathrm{L}_3(2) \cong \mathrm{L}_2(7),$$
$$\mathrm{L}_4(2) \cong A_8,\ \mathrm{PSp}_4(3) \cong \mathrm{U}_4(2)$$

(see [13, Proposition 2.9.1]), we may assume that

$$S \neq \mathrm{L}_2(4),\ \mathrm{L}_2(5),\ \mathrm{L}_2(9),\ \mathrm{L}_3(2),\ \mathrm{L}_4(2),\ \mathrm{PSp}_4(2)',\ \mathrm{PSp}_4(3).$$

Proposition 2.20. *If* $m > 600$, H *is standard and* S *is classical, then* $\mathrm{ifix}(T) > n^{4/9}$.

Proof. We adopt the set-up introduced above, including the conditions on S presented in Remark 2.19. Write $q = p^f$, where p is a prime. We will prove that (6) holds unless $(H, m) = (\mathrm{L}_{10}(2), 2^{10} - 1)$.

Since $m = |S : S \cap K|$ it follows that $m \geqslant P(S)$, where $P(S)$ is the minimal degree of a non-trivial permutation representation of S. The minimal degrees are presented in [11, Table 4] (which corrects a couple of slight errors in [13, Table 5.2.A]) and by inspection we deduce that $m > q^{\ell-2}$. Similarly, the order of $\mathrm{Aut}(S)$ is recorded in [13, Table 5.1.A] and it is easy to see that $|H| \leqslant |\mathrm{Aut}(S)| < 2q^{\ell^2}$.

If $S = \mathrm{L}_2(q)$ then $m > \max\{600, q\}$, $|H| \leqslant q(q^2 - 1)\log_p q$ and it is routine to verify the bound in (6). Similarly, if $\ell = 3$ then $S = \mathrm{L}^\epsilon_3(q)$, $m > \max\{600, q^2 + q\}$,

$$|H| \leqslant |\mathrm{Aut}(\mathrm{U}_3(q))| = 2q^3(q^2 - 1)(q^3 + 1)\log_p q$$

and we quickly deduce that (6) holds.

Now assume $\ell \geqslant 4$. If $q \geqslant 31$ then one checks that

$$2^{101} q^{100\ell^2} < (q^{\ell-2})! \tag{8}$$

and this establishes the bound in (6). More precisely, if $\ell \geqslant 5$ then the inequality in (8) is satisfied unless (ℓ, q) is one of the following:

$$\ell = 5,\ q \leqslant 9;\ \ell = 6,\ q \leqslant 5;\ \ell = 7,\ q \leqslant 4;\ \ell = 8,\ q \leqslant 3;\ \ell = 9, 10, 11, 12,\ q = 2. \tag{9}$$

Suppose $\ell = 4$ and $q \leqslant 29$. If $S = \mathrm{PSp}_4(q)$ then $q \geqslant 4$ (see Remark 2.19), $m > \max\{600, q^2\}$ and

$$|H| \leqslant |\mathrm{Aut}(\mathrm{PSp}_4(q))| \leqslant 2q^4(q^2 - 1)(q^4 - 1)\log_p q,$$

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

which implies that (6) holds. Now assume $S = \mathrm{L}_4^{\epsilon}(q)$, so

$$|H| \leqslant |\mathrm{Aut}(\mathrm{U}_4(q))| = 2q^6(q^2-1)(q^3+1)(q^4-1)\log_p q.$$

If $m > \max\{600, q^4\}$ then (6) holds, so let us assume $600 < m \leqslant q^4$. By inspecting [6, Table 4.1.2], which records the degree of every standard classical group, we deduce that $S = \mathrm{L}_4(q)$ and $m = (q^4-1)/(q-1)$ is the only possibility, so $q \geqslant 9$ and we get $|\mathrm{Aut}(S)|^{100} < |T|$.

Very similar reasoning establishes the bound in (6) for all the remaining cases in (9) with $\ell \leqslant 9$, so to complete the proof, we may assume that $\ell \in \{10, 11, 12\}$ and $q = 2$. If $\ell \in \{11, 12\}$ and $S = \mathrm{L}_\ell^{\epsilon}(2)$ then $m \geqslant 2^\ell - 1$ and we deduce that (6) holds. Similarly, if $\ell = 12$ and $S \neq \mathrm{L}_{12}^{\epsilon}(2)$ then the bound $m > 2^{10}$ is sufficient. Finally, let us assume $\ell = 10$. If $S \neq \mathrm{L}_{10}^{\epsilon}(2)$ then $|H| \leqslant |\mathrm{Sp}_{10}(2)|$ and one checks that the condition $m > 600$ implies that $m \geqslant 2^{10} - 1$, which allows us to verify the bound in (6). Now assume $S = \mathrm{L}_{10}^{\epsilon}(2)$, so $|H| \leqslant 2|\mathrm{U}_{10}(2)|$. If $m > 2^{11}$ then $|H|^{100} < |T|$, so let us assume $m \leqslant 2^{11}$, in which case $H = \mathrm{L}_{10}(2)$ and $m = 2^{10} - 1$ (so Γ is the set 1-dimensional subspaces of V). Here $|H|^{100} > |T|$, but if we define $\alpha = \log|H|/\log|T|$ and β as in (7), then it is easy to check that $5 - 5\alpha - 9\beta > 0$ and thus $\mathrm{ifix}(T) > n^{4/9}$ by Lemma 2.2. □

3. Sporadic groups

In this final section, we complete the proof of Theorem 1 by handling the groups with socle a sporadic simple group. Our first result quickly reduces the problem to the Baby Monster and Monster (denoted by $\mathbb{B}$ and $\mathbb{M}$, respectively).

Proposition 3.1. *The conclusion to Theorem 1 holds if $T \neq \mathbb{B}, \mathbb{M}$ is a sporadic group.*

Proof. This is an easy computation using the GAP Character Table Library [4]. In each case, the character table of G is available in [4] and we use the Maxes function to access the character table of the maximal subgroup H. In addition, [4] stores the fusion map from H-classes to G-classes, which allows us to compute $\mathrm{fix}(t)$ via (1) for all $t \in G$. In particular, we can compute $\mathrm{ifix}(T)$ precisely and the result follows. □

To complete the proof of Theorem 1, we may assume that $T = \mathbb{B}$ or $\mathbb{M}$. In both cases, we claim that $\mathrm{ifix}(T) > n^{4/9}$.

Proposition 3.2. *The conclusion to Theorem 1 holds if $T = \mathbb{B}$.*

Proof. Here $G = T$ is the Baby Monster and we proceed as in the proof of the previous proposition, noting that the character tables of G and H are available in [4] (as before, we use the Maxes function to access the character table of H). In addition, in all but one case, the fusion map from H-classes to G-classes is also stored and this reduces the analysis to the case $H = (2^2 \times F_4(2)).2$. Here we use the function PossibleClassFusions to determine a set of candidate fusion maps (there are 64 such maps in total) and for each possibility one checks that $\mathrm{ifix}(T) = 160908528\,8448 > n^{4/9}$. □

Proposition 3.3. *The conclusion to Theorem 1 holds if $T = \mathbb{M}$.*

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

Proof. Let $G = T = \mathbb{M}$ be the Monster. By inspecting the ATLAS [9], we see that G has two conjugacy classes of involutions, labelled 2A and 2B, where

$$|\mathtt{2A}| = 97239461142009186000, \quad |\mathtt{2B}| = 5791748068511982636944259375.$$

As discussed in [23], G has 44 known conjugacy classes of maximal subgroups and any additional maximal subgroup is almost simple with socle one of $\mathrm{L}_2(8)$, $\mathrm{L}_2(13)$, $\mathrm{L}_2(16)$ or $\mathrm{U}_3(4)$. Let us define the following three collections of known maximal subgroups of G:

$$\mathcal{A} = \{2^{10+16}.\Omega_{10}^{+}(2), 2^{2+11+22}.(\mathrm{M}_{24} \times S_3), 2^{5+10+20}.(S_3 \times \mathrm{L}_5(2)), 2^{3+6+12+18}.(\mathrm{L}_3(2) \times 3S_6)\}$$
$$\mathcal{B} = \{3^8.\mathrm{P}\Omega_8^{-}(3).2, (3^2{:}2 \times \mathrm{P}\Omega_8^{+}(3)).S_4, 3^{2+5+10}.(\mathrm{M}_{11} \times 2S_4), 3^{3+2+6+6}.(\mathrm{L}_3(3) \times \mathrm{SD}_{16})\}$$
$$\mathcal{C} = \{(\mathrm{L}_2(11) \times \mathrm{L}_2(11)){:}4, 11^2{:}(5 \times 2A_5), 7^2{:}\mathrm{SL}_2(7), \mathrm{L}_2(29){:}2, \mathrm{L}_2(19){:}2\}$$

First assume H belongs to one of the 44 known classes of maximal subgroups. If H is not contained in $\mathcal{A}$, $\mathcal{B}$ or $\mathcal{C}$, then we use the function NamesOfFusionSources to access the character table of H in GAP and in each case we can work with the stored fusion map from H-classes to G-classes. This allows us to compute $\mathrm{ifix}(T)$ as in the proof of Proposition 3.1 and it is straightforward to verify the desired bound.

Now assume H is one of the subgroups in $\mathcal{C}$. Here the character table of H is available in GAP, but the fusion map is not stored. So in these cases, we proceed as in the proof of Proposition 3.2, using the function PossibleClassFusions. In each case, we find that $\mathrm{ifix}(T)$ is independent of the choice of fusion map and we calculate that $\mathrm{ifix}(T) > n^{4/9}$.

Next, suppose $H \in \mathcal{A} \cup \mathcal{B}$. If $H \in \mathcal{A}$ then [7, Proposition 3.9] gives $|t^G \cap H|$, where t is contained in the 2A class of involutions in G. This allows us to compute $\mathrm{fix}(t)$ precisely and we deduce that $\mathrm{ifix}(T) > n^{4/9}$. Now assume $H \in \mathcal{B}$ and let α be the size of the largest conjugacy class of involutions in H. We use MAGMA to compute α, working with a representation of H given in [24]. For $H = 3^8.\mathrm{P}\Omega_8^{-}(3).2$, this is a matrix representation of dimension 204 over $\mathbb{F}_3$ and we use LMGClasses to compute a set of conjugacy class representatives; in the remaining cases, we work with a permutation representation of degree less than 10^5. Now, if β is the size of the 2B class of involutions in G (see above), then $\mathrm{ifix}(T) \geqslant n\alpha\beta^{-1}$ and in each case it is easy to check that this lower bound is greater than $n^{4/9}$. For example, if $H = 3^8.\mathrm{P}\Omega_8^{-}(3).2$ then $\alpha = 1982806371$ and the above bound yields $\mathrm{ifix}(T) > n^{4/9}$.

To complete the proof of the proposition, we may assume H is an almost simple maximal subgroup with socle $S = \mathrm{L}_2(8)$, $\mathrm{L}_2(13)$, $\mathrm{L}_2(16)$ or $\mathrm{U}_3(4)$. Let α be the size of the largest class of involutions in S and define $\beta = |\mathtt{2B}|$ as above. Then one checks that

$$\left(\frac{|T|}{|\mathrm{Aut}(S)|}\right)^{5/9} > \frac{\beta}{\alpha}$$

and since $H \leqslant \mathrm{Aut}(S)$, we immediately deduce that $\mathrm{ifix}(T) > n^{4/9}$ as required. □

This completes the proof of Theorem 1.

References

1. J. Bamberg, T. Popiel and C. E. Praeger, Simple groups, product actions, and generalized quadrangles, *Nagoya Math. J.* **234** (2019), 87–126.
2. H. Bender, Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festlässt, *J. Algebra* **17** (1971), 527–554.
3. W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: the user language, *J. Symb. Comput.* **24** (1997), 235–265.
4. T. Breuer, *The* GAP *Character Table Library, Version 1.2.1*, GAP package, available at http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib, 2012
5. T. C. Burness, Simple groups, fixed point ratios and applications, in *Local representation theory and simple groups*, pp. 267–322, EMS Ser. Lect. Math. (Eur. Math. Soc., Zürich, 2018).
6. T. C. Burness and M. Giudici, *Classical groups, derangements and primes*, Australian Mathematical Society Lecture Series, Volume 25 (Cambridge University Press, Cambridge, 2016).
7. T. C. Burness, E. A. O'Brien and R. A. Wilson, Base sizes for sporadic simple groups, *Israel J. Math.* **177** (2010), 307–333.
8. T. C. Burness and A. R. Thomas, On the involution fixity of exceptional groups of Lie type, *Internat. J. Algebra Comput.* **28** (2018), 411–466.
9. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups* (Oxford University Press, 1985).
10. The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.11.0, available at http://www.gap-system.org, 2020.
11. S. Guest, J. Morris, C. E. Praeger and P. Spiga, On the maximum orders of elements of finite almost simple groups and primitive permutation groups, *Trans. Amer. Math. Soc.* **367** (2015), 7665–7694.
12. I. M. Isaacs, *Character theory of finite groups*, Pure and Applied Mathematics, Volume 69 (Academic Press, New York-London, 1976).
13. P. B. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Note Series, Volume 129 (Cambridge University Press, 1990).
14. M. W. Liebeck, C. E. Praeger and J. Saxl, A classification of the maximal subgroups of the finite alternating and symmetric groups, *J. Algebra* **111** (1987), 365–383.
15. M. W. Liebeck and J. Saxl, On point stabilizers in primitive permutation groups, *Comm. Algebra* **19** (1991), 2777–2786.
16. M. W. Liebeck and J. Saxl, Maximal subgroups of finite simple groups and their automorphism groups, in *Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989)*, Contemp. Math., Volume 131, pp. 243–259 (American Mathematical Society, Providence, RI, 1992).
17. M. W. Liebeck and A. Shalev, On fixed points of elements in primitive permutation groups, *J. Algebra* **421** (2015), 438–459.
18. K. Magaard and R. Waldecker, Transitive permutation groups where nontrivial elements have at most two fixed points, *J. Pure Appl. Algebra* **219** (2015), 729–759.
19. W. Pribitkin, Simple upper bounds for partition functions, *Ramanujan J.* **18** (2009), 113–119.
20. M. Quick, Probabilistic generation of wreath products of non-abelian finite simple groups, *Comm. Algebra* **32** (2004), 4753–4768.
21. C. Ronse, On permutation groups of prime power order, *Math. Z.* **173** (1980), 211–215.

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press

22. J. Saxl and A. Shalev, The fixity of permutation groups, *J. Algebra* **174** (1995), 1122–1140.
23. R. A. Wilson, Maximal subgroups of sporadic groups, in *Finite simple groups: thirty years of the Atlas and beyond*, Contemp. Math., Volume 694, pp. 57–72 (American Mathematical Society, Providence, RI, 2017).
24. R. A. Wilson, *et al.*, *A World-Wide-Web Atlas of finite group representations*, http://brauer.maths.qmul.ac.uk/Atlas/v3/

https://doi.org/10.1017/S0013091521000237 Published online by Cambridge University Press