On fixed points of elements in primitive permutation groups

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2AZ
UK

Aner Shalev
Institute of Mathematics
Hebrew University
Jerusalem 91904
Israel

Dedicated to the memory of Ákos Seress

Abstract

The *fixity* of a finite permutation group is the maximal number of fixed points of a non-identity element. We study the fixity of primitive groups of degree n, showing that apart from a short list of exceptions, the fixity of such groups is at least $n^{1/6}$. We also prove that there is usually an involution fixing at least $n^{1/6}$ points.

1 Introduction

If G is a permutation group on a finite set Ω of size n, we define the *fixity* $f(G)$ to be the maximal number of fixed points of a non-identity element of G. For example, transitive groups of fixity 0 are regular, those of fixity 1 are Frobenius groups, and doubly transitive groups of fixity at most 2 are Zassenhaus groups. The general concept of fixity was introduced in [19], and further studied in [20]. The corresponding notion for linear groups is the subject of [16, 18, 21, 22, 23].

There is an obvious relationship between fixity and the classical notion of the *minimal degree* $\mu(G)$ of G (the minimal number of points moved by any non-identity element) – namely, $f(G) = n - \mu(G)$. Much of the literature on minimal degrees focusses on lower bounds for $\mu(G)$ when G is primitive, going back to classical work of Bochert, Jordan and Manning (see [24, Section 15]); an example of a post-classification result can be found in [12] where it is shown that with some standard exceptions, $\mu(G) \geq \frac{1}{3}n$ for

The authors are grateful for the support of an EPSRC grant. The second author acknowledges the support of grants from the Israel Science Foundation and ERC.

2010 *Mathematics Subject Classification:* 20D06, 20E05, 20E26, 20P05.

primitive groups G of degree n. Correspondingly, one has upper bounds on the fixity $f(G)$.

In this paper we focus on lower bounds for the fixity of primitive groups. The results in [20] are concerned with groups of bounded fixity: Theorem 1.3 of [20] shows that if G is a primitive group of fixity f, then either G has a soluble subgroup of index bounded by a function of f, or the socle $\mathrm{Soc}(G)$ of G is $L_2(q)$ or $Sz(q)$ in its doubly transitive representation of degree $q+1$ or q^2+1, respectively. Here we take this study much further and analyse the structure of primitive permutation groups whose fixity may be unbounded, and even a rather large function of the degree. Our first result shows that with specified exceptions, the fixity of primitive groups is large. In the statement, $R(G)$ denotes the soluble radical of G – that is, the largest soluble normal subgroup of G.

Theorem 1 *If G is a primitive permutation group of degree n with point-stabilizer H, then one of the following holds:*

(i) $f(G) \geq n^{1/6}$;

(ii) *G is affine and* $|G/R(G)| \leq 120$;

(iii) $\mathrm{Soc}(G) = L_2(q)$ *or* $Sz(q)$ *in the* 2*-transitive action of degree* $n = q+1$ *or* q^2+1*, respectively;*

(iv) $G = A_p$ *and* $H = p.(\frac{p-1}{2})$ *for some prime* $p \geq 19$ *with* $p \equiv 3 \bmod 4$;

(v) $\mathrm{Soc}(G) = L_p^{\epsilon}(q)$ $(\epsilon = \pm 1)$ *and* $H \cap \mathrm{Soc}(G) = (\frac{q^p-\epsilon}{(q-\epsilon)(p,q-\epsilon)}).p$*, where p is an odd prime;*

(vi) *G is one of the sporadic groups M_{23} or BM, and* $H = 23.11$ *or* 47.23*, respectively.*

In cases (iv), (v) *and* (vi), $|H|$ *is odd.*

Remarks 1. The condition $|G/R(G)| \leq 120$ in (ii) just says that either G is soluble or $G/R(G)$ is A_5 or S_5.

2. There are examples of groups in (ii)-(vi) for which $f(G)$ is much less than $n^{1/6}$. Under (ii) there are soluble Frobenius groups and also Frobenius groups with Frobenius complement $SL_2(5)$, for example. For the groups in (iii), every non-identity element of $\mathrm{Soc}(G)$ fixes at most 2 points. In (iv) the value of $f(G)$ depends on the arithmetic nature of the number $(p-1)/2$; for example if it is prime, then $f(G) = (p-1)(p-3)/4$ while $n = (p-2)!$. Similar comments apply to (v), and in (vi) the fixities of M_{23} and BM are 5 and 22. Details of all these assertions are given in Section 5.

3. It may be that the constant $\frac{1}{6}$ in part (i) of the theorem can be improved, but only slightly. Indeed, for infinitely many natural numbers

n there is a primitive group of degree n of fixity $n^{1/5}$ which is not of type (ii)-(vi). For example, let $p \geq 5$ be a prime, let $H = L_2(p)$ and let V be the irreducible 5-dimensional $\mathbb{F}_pH$-module (so $V \cong S^4W$, where W is the natural 2-dimensional module for $SL_2(p)$). Then since non-identity semisimple (respectively, unipotent) elements of H have fixed space on V of dimension at most 1 (respectively, exactly 1), the affine group $VH \leq S_{p^5}$ has fixity $p = n^{1/5}$.

A more detailed analysis of the fixity of the groups in parts (iv) and (v) (see Section 5) of the theorem yields an interesting dichotomy for the fixity of primitive groups.

Corollary 2 *There is an absolute constant $c > 0$ such that if G is a non-affine primitive permutation group of degree n, then one of the following holds:*

(i) $f(G) > (\frac{c \log n}{\log \log n})^2$;

(ii) $\mathrm{Soc}(G) = L_2(q)$ *or* $Sz(q)$ *in the 2-transitive action of degree* $n = q+1$ *or* q^2+1.

We shall deduce Theorem 1 from the following two results. The first is a reduction to affine and almost simple groups.

Theorem 3 *If G is a primitive permutation group of degree n such that $f(G) < n^{1/3}$, then G is either affine or almost simple.*

The affine case of Theorem 1 is taken care of by the main result of [16], which states that if H is a finite group satisfying $|H/R(H)| > 120$, then for any field K and any KH-module V, there exists a non-identity element $h \in H$ such that $\dim C_V(h) \geq \frac{1}{6} \dim V$.

The next theorem covers almost simple groups. It shows that not only do almost simple primitive groups of degree n have non-identity elements fixing at least $n^{1/6}$ points (with specified exceptions), but that this fixed point number can usually be achieved by an involution. In fact the *involution fixity* of permutation groups (the maximal number of fixed points of an involution) has been studied in a number of papers, going back to the celebrated result of Bender [3] classifying transitive groups with involution fixity 1; these are groups for which a point-stabilizer is a "strongly embedded" subgroup.

Theorem 4 *Let G be an almost simple primitive permutation group of degree n, with socle T and point-stabilizer H. Then one of the following holds.*

(i) *There is an involution $t \in T$ such that* $\mathrm{fix}(t) > n^{1/6}$.

(ii) *$H \cap T$ has odd order.*

(iii) *$T = L_2(q)$, $Sz(q)$ or $U_3(q)$ (with q even in the last case) in the 2-transitive action of degree $n = q+1$, q^2+1 or q^3+1, respectively.*

Remarks 1. For groups satisfying (ii) of the theorem, involutions in T are fixed point free; such groups are known (see Lemma 2.1).

2. Notice the extra group $U_3(q)$ (q even) which appears in part (iii) but not in Theorem 1(iii); the involutions in this group fix only one point, but there are elements of odd order fixing $q+1$ points.

3. It is possible that the constant $\frac{1}{6}$ in part (i) of the theorem could be improved, perhaps to around $\frac{1}{3}$. We have not attempted to do this here since we only need $\frac{1}{6}$ for the application to Theorem 1, but we leave it for a future project.

The following result can be deduced fairly quickly from Theorem 4.

Corollary 5 *If G is an almost simple primitive permutation group of degree n, then one of the following holds:*

(i) *there is an involution in G which fixes at least $n^{1/6}$ points;*

(ii) *every involution in G fixes at most 2 points.*

This result reveals a remarkable dichotomy in the involution fixity of almost simple primitive groups. We can extend this to all non-affine groups, as follows.

Theorem 6 *Let G be a non-affine primitive permutation group of degree n. Then one of the following holds:*

(i) *G has an involution fixing at least $n^{1/6}$ points;*

(ii) *every involution in G has at most 2 fixed points;*

(iii) *$G \leq P\Gamma L_2(q) \wr S_m$ in the product action of degree $(q+1)^m$, where $\mathrm{Soc}(G) = L_2(q)^m$ and $q \equiv 3 \bmod 4$.*

The rest of the paper is divided into five further sections. After some preliminaries in Section 2, Theorem 4 is proved in Section 3, and Theorem 3 in Section 4. Section 5 contains the deduction of Theorem 1 and Corollaries 2 and 5, and Theorem 6 is proved in the final section. We make use of Magma [4] for routine computations in some of our proofs.

2 Preliminaries

We begin with a result taken from [11, Theorem 2], which describes the almost simple primitive permutation groups in which all involutions are fixed point free.

Lemma 2.1 *Let G be a finite almost simple group with non-abelian simple socle T, and suppose H is a maximal subgroup of G such that $|H \cap T|$ is odd. Then the possibilities for T and $H \cap T$ are as in Table* 1.

Table 1:

T	$H \cap T$	Conditions
A_p	$p.(\frac{p-1}{2})$	p prime, $p \equiv 3 \bmod 4$,
		$G = S_p$ if $p = 7, 11, 23$
$L_2(q)$	$\mathbb{F}_q^+.(\frac{q-1}{2})$	$q \equiv 3 \bmod 4$
$L_p^\epsilon(q)$ $(\epsilon = \pm)$	$(\frac{q^p-\epsilon}{(q-\epsilon)(p,q-\epsilon)}).p$	p odd prime,
		$T \neq U_3(3), U_5(2)$,
		$G \geq T.3$ if $T = L_3(4), U_3(5)$
M_{23}, Th, BM	23.11, 31.15, 47.23 (resp.)	
J_3, $O'N$	19.9, 31.15 (resp.)	$G = T.2$

Proof. Theorem 2 of [11] lists all maximal subgroups H of odd order in almost simple groups with socle T. Inspection of the proof shows that we get the same list, with the addition of the J_3 and $O'N$ examples in the last row of Table 1, if we merely assume that $H \cap T$ has odd order. Hence $T, H \cap T$ are in the list in [11, Theorem 2] (together with the J_3, $O'N$ examples). This is the list in the conclusion of the lemma, except that it also includes subgroups 59.29 and 71.35 in the Monster M; these have subsequently been shown to lie in subgroups $L_2(59)$ and $L_2(71)$ (see [7, 8]), so are omitted. ∎

Next we give an elementary but useful result on fixed points.

Lemma 2.2 *Let G be a transitive permutation group on a set Ω of degree n with point-stabilizer H, and let $x \in H$.*

(i) *Then*

$$\frac{\text{fix}(x)}{n} = \frac{|x^G \cap H|}{|x^G|}.$$

(ii) *We have* $\text{fix}(x) \geq |C_G(x) : C_H(x)|$, *with equality if and only if* $x^G \cap H = x^H$.

(iii) *If* $\mathrm{fix}(x) \leq n^{1/6}$, *then*

$$|H| \geq \frac{|C_G(x)|^{6/5}}{|G|^{1/5}}.$$

(iv) *If* $\mathrm{fix}(x) \leq n^{1/6}$ *and* $|x^G| < |G|^{5/9}$, *then* $|H| > |G|^{1/3}$.

Proof. Part (i) is well-known (see for example [12, 2.5]), and (ii) follows from (i). For (iii), note that if $\mathrm{fix}(x) \leq n^{1/6}$ then by (ii) we have $|C_G(x)|/|H| \leq |G : H|^{1/6}$, and the conclusion of (iii) follows from this. Finally, (iv) is a consequence of (iii). ∎

Our proof of Theorem 4 will make use of the bounds on the sizes of involution classes and centralizers in finite simple groups given in the next two results.

Proposition 2.3 *If* T *is a simple group of Lie type, then one of the following holds:*

(i) $|u^T| < |T|^{5/9}$ *for all involutions* $u \in T$;

(ii) T *is a classical group of type* A_1, $B_m\,(m \leq 4)$, $C_m\,(m \leq 4)$, D_4 *or* ${}^2D_4$;

(iii) T *is an exceptional group of type* G_2, ${}^2G_2$, ${}^3D_4$ *or* ${}^2B_2$;

(iv) $T = L_3(4)$ *or* ${}^2F_4(2)'$.

Proof. For T classical this follows from the proof of [15, 4.1], keeping track of the precise involution centralizers given in the references quoted there. Similarly, for T of exceptional type, the conclusion follows from the proof of [15, 4.3]. ∎

Proposition 2.4 *If* T *is a non-abelian simple group, and* α *is an involutory automorphism of* T, *then* $|C_T(\alpha)| > |T|^{1/3}$.

Proof. This is a routine calculation for the alternating groups, and follows from the information on involution centralizers in [6] for the sporadic groups. For the groups of Lie type the proof is as in the previous proposition, using [15, 4.1,4.3] for inner automorphisms and [15, 4.4] for outer automorphisms. ∎

3 Proof of Theorem 4

Let G be an almost simple primitive permutation group of degree n on a set Ω with point-stabilizer H, and let $T = \mathrm{Soc}(G)$. Assume that (i) and (ii) of Theorem 4 do not hold, that is, $|H \cap T|$ is even, and

$$\mathrm{fix}(t) \leq n^{1/6} \text{ for all involutions } t \in T. \tag{1}$$

By Lemma 2.2, it follows that

$$|C_G(t) : C_H(t))| \leq n^{1/6} \text{ for all involutions } t \in H \cap T. \tag{2}$$

We aim to show that (iii) of Theorem 4 holds.

The proof is divided into subsections covering the cases where the socle T is alternating or sporadic, classical, or exceptional of Lie type.

3.1 Alternating and sporadic groups

Here we handle the case where T is an alternating or sporadic group.

Proposition 3.1 *T is not a sporadic group.*

Proof. This is a routine Magma computation with the following steps. Suppose T is sporadic. If $t \in T$ is an involution with minimal centralizer order, then by Lemma 2.2(iii) we have

$$|H| > \frac{|C_T(t)|^{6/5}}{|T|^{1/5}}.$$

The maximal subgroups H satisfying this inequality are known and are in [6], and for each it can be checked that there is an involution $t \in H \cap T$ violating (1) or (2). ∎

Proposition 3.2 *If T is an alternating group, then $T = A_5 \cong L_2(4)$ and $n = 5$, as in* (iii) *of Theorem* 4.

Proof. Let $T = A_l$. The conclusion is clear if $l = 5$, and it is easily checked that (1) fails if $l = 6$, so assume that $l > 6$. Then $G = A_l$ or S_l. As H is maximal in G, one of the following holds:

(1) $H = (S_k \times S_{l-k}) \cap G$, where $1 \leq k < l/2$,

(2) $H = (S_k \wr S_r) \cap G$, where $kr = l$ and $1 < k < l$,

(3) H acts primitively on the set $\{1, \ldots, l\}$.

Consider case (1). Here G is acting on the set Ω of k-subsets of $\{1,\dots,l\}$. Let t be the involution $(1\,2)\,(3\,4)$. Then t fixes all k-subsets that contain$\{1,2\}$ or $\{3,4\}$, or are disjoint from both, so

$$\mathrm{fix}_\Omega(t) \geq 2\binom{l-4}{k-2} + \binom{l-4}{k}.$$

One checks that this is greater than $\binom{l}{k}^{1/6} = n^{1/6}$, contradicting (1).

Now consider (2). Here the action of G is on the set of (k,r)-partitions of $\{1,\dots,l\}$ – that is, partitions into r subsets of size k, and

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

If we again let $t = (1\,2)\,(3\,4)$, then t fixes all partitions with one part containing $\{1,2\}$ and another containing $\{3,4\}$, so

$$\mathrm{fix}_\Omega(t) \geq \binom{l-4}{k-2} \times \binom{l-k-2}{k-2} \times f(k,r-2).$$

It is straightforward to verify that this is greater than $n^{1/6}$.

Finally, consider case (3). Let $t \in H \cap T$ be an involution, and suppose that t is in the conjugacy class of cycle-shape $(2^m, 1^f)$, where $2m + f = l$. By our assumption (1) together with Lemma 2.2(iii), we have

$$|H| > \frac{|C_G(t)|^{6/5}}{|G|^{1/5}} \geq \frac{(2^{m-1}m!f!)^{6/5}}{(l!)^{1/5}}. \tag{3}$$

If we define $g(m,f) = 2^{m-1}m!f!$, then $\frac{g(m-1,f+2)}{g(m,f)} = \frac{(f+2)(f+1)}{2m}$, so the minimal value of $g(m,f)$ is attained when $(f+2)(f+1)$ is roughly equal to $2m$. Combining this with the well-known inequalities $(\frac{s}{e})^s < s! < se(\frac{s}{e})^s$ for any positive integer s, we see that the right hand side of the inequality (3) is greater than 2^l for $l > 24$. This conflicts with the result of Maroti [17, 1.2] which states that a primitive subgroup of S_l $(l > 24)$ not containing A_l has order less than 2^l.

Hence $l \leq 24$. At this point, a Magma computation using the list of maximal primitive groups of degree $l \leq 24$ shows that each such group has an involution t which violates the inequality (2). This completes the proof.

■

3.2 Classical groups

Continue with the assumptions at the beginning of this section: G is an almost simple primitive permutation group of degree n on a set Ω with point-stabilizer H and socle T, and (i) and (ii) of Theorem 4 do not hold. In this subsection we prove

Proposition 3.3 *If T is a classical group, then $T = L_2(q)$ or $U_3(q)$ (with q even in the latter case) in the 2-transitive action of degree $n = q+1$ or q^3+1.*

Let us embark on the proof of this. Suppose that $T = Cl_d(q)$, where $Cl_d(q)$ stands for one of the groups $L_d(q)$, $U_d(q)$, $PSp_d(q)$, $P\Omega_d^\epsilon(q)$ (d odd or even); we refer to these as cases L,U,S,O respectively. Write V for the natural d-dimensional module for T over $\mathbb{F}_{q^u}$ (where $u = 2$ in case U and $u = 1$ otherwise), and let p be the characteristic of the field $\mathbb{F}_q$.

First we pin down the possibilities for the maximal subgroup H. In the following result, we use Aschbacher's classification [2] of maximal subgroups of classical groups into families $\mathcal{C}_i$ ($1 \le i \le 8$) and $\mathcal{S}$: the families $\mathcal{C}_i$ are called geometric subgroups, and the family $\mathcal{S}$ consists of almost simple subgroups acting absolutely irreducibly on V. Detailed descriptions of these families can be found in [9].

Define the following collections of simple groups:

$\mathcal{L}_1 = \{L_3(4),\, L_4(5),\, U_3(5),\, U_4(3),\, U_4(7)\}$,
$\mathcal{L}_2 = \{L_3(4),\, L_4(2),\, L_4(7),\, L_5(3),\, U_3(3),\, U_3(5),\, U_4(3),\, U_4(5),\, U_5(2),\, U_6(2)\}$.

Lemma 3.4 *Assume that T is not of type A_1, $B_m\,(m \le 4)$, $C_m\,(m \le 4)$, D_4 or ${}^2D_4$. Then one of the following holds:*

(i) *$H \in \mathcal{C}_1 \cup \mathcal{C}_1'$ (the reducible maximal subgroups);*

(ii) *$H \in \mathcal{C}_8$ (the classical maximal subgroups);*

(iii) *$H \in \mathcal{C}_6$ and $T \in \mathcal{L}_1$;*

(iv) *$H \in \mathcal{C}_i$ ($2 \le i \le 5$) is as in Table 2;*

(v) *$H \in \mathcal{S}$ and either $T \in \mathcal{L}_2$ or H, T are as in Table 3.*

Proof. By assumption there is an involution $t \in H \cap T$ such that $\mathrm{fix}(t) \le n^{1/6}$. Also (excluding $T = L_3(4)$) we have $|t^T| < |T|^{5/9}$ by Proposition 2.3, and so $|H \cap T| > |T|^{1/3}$ by Lemma 2.2(iv). Maximal subgroups satisfying this bound are classified in [1], and the conclusion follows from this. ■

We now consider the various possiblities in Lemma 3.4, starting with the case where H is a parabolic subgroup (which is part of the case where $H \in \mathcal{C}_1 \cup \mathcal{C}_1'$).

Lemma 3.5 *The conclusion of Proposition 3.3 holds if H is a parabolic subgroup.*

Table 2:

Family $\mathcal{C}_i$	Type of H	Possibilities
$\mathcal{C}_2$	$Cl_{d/k}(q) \wr S_k$	$k \leq 3$
		$k = d$ (Cases U,O)
		$k = \frac{d}{2} \leq 5$ (Cases S,O)
	$GL_{d/2}(q^u)$	Cases U,S,O
$\mathcal{C}_3$	$Cl_{d/k}(q^k)$	$k \leq 3$
	$GU_{d/2}(q)$	Cases S,O
$\mathcal{C}_4$	$Sp_2(q) \otimes Sp_{d/2}(q)$	Case O^+
$\mathcal{C}_5$	$Cl_d(q^{1/k})$	$k \leq 3$
	$Sp_d(q)$, $O^{\epsilon}_d(q)$	Case U

Table 3:

Soc(H)	T
$A_{d+\alpha}$ $(\alpha \in \{1,2\})$	$Sp_d(2)$ or $\Omega^{\epsilon}_d(2)$, $10 \leq d \leq 22$
A_{12}	$P\Omega^+_{10}(3)$
M_{12}	$\Omega^-_{10}(2)$

Proof. Suppose H is parabolic. The cases where $T = L_2(q)$ or $T = U_3(q)$ (q even) are in conclusion (iii) of Proposition 3.3, so exclude these groups from consideration.

Consider first $T = L_d(q)$. Here $d \geq 3$ by the assumption in the previous paragraph. There are two possibilities:

(a) $H = P_i$, the stabilizer in G of an i-space $V_i \subset V$; here

$$n = f_{d,i}(q) := \frac{(q^d-1)(q^{d-1}-1)\cdots(q^{d-i+1}-1)}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}.$$

(b) $H = P_{i,d-i}$, the stabilizer of a flag $V_i \subset V_{d-i}$ with $d-i > i$, and G contains a graph automorphism of T; here

$$n = f_{d,i}(q) f_{d-i,d-2i}(q).$$

Choose an involution $t \in T$ that fixes pointwise a $(d-2)$-subspace of V; specifically, choose

$$t = \mathrm{diag}(A, I_{d-2}) \tag{4}$$

where $A = -I_2$ if q is odd and $A = J_2$, a 2×2 unipotent Jordan block matrix, if q is even.

In case (a) we may assume that $i \leq d/2$ as the permutation character of T on P_i is the same as that on P_{d-i}. Since t fixes every i-space in the $(d-2)$-space it fixes pointwise, we have $\text{fix}(t) \geq f_{d-2,i}(q)$. When $i < d-2$ it is easy to check that $f_{d-2,i}(q)^6 > f_{d,i}(q)$, which contradicts (1). And if $i \geq d-2$ we must have $(i,d) = (1,3)$ or $(2,4)$; in the first case t fixes at least $q+1$ 1-spaces, and in the second case it fixes at least q^2+q+1 2-spaces, and again (1) is contravened.

In case (b) with $i \geq 2$, the element t fixes all flags $V_i \subset V_{d-i}$ such that V_i contains the 2-space spanned by the first 2 basis vectors (on which t acts as the matrix A above), so $\text{fix}(t) \geq f_{d-2,i-2}(q) f_{d-i,d-2i}(q)$. One checks that $(f_{d-2,i-2}(q) f_{d-i,d-2i}(q))^6 > f_{d,i}(q) f_{d-i,d-2i}(q)$, contradicting (1). Finally, if $i=1$ and $d \geq 4$ then $\text{fix}(t) \geq f_{d-2,1}(q)$; and if $i=1, d=3$ then a calculation gives $\text{fix}(t) \geq q$. Both cases give a contradiction to (1). This completes the analysis when $T = L_d(q)$.

The cases where $T = U_d(q)$ or $PSp_d(q)$ are similar. In these cases $H = P_i$, the stabilizer of a totally singular i-space, and $n = g_{d,i}(q)$ or $h_{d,i}(q)$ respectively, where

$$g_{d,i}(q) := \frac{\prod_{r=d-2i+1}^{d}(q^r - (-1)^r)}{\prod_{r=1}^{i}(q^{2r}-1)}, \quad h_{d,i}(q) := \frac{\prod_{r=0}^{i-1}(q^{d-2r}-1)}{\prod_{r=1}^{i}(q^r-1)}.$$

Define an involution $t \in T$ as in (4). Then $\text{fix}(t)$ is at least $g_{d-2,i}(q)$ or $h_{d-2,i}(q)$ respectively, which contradicts (1) except in the cases where $(d,i) = (4,2)$ or $(3,1)$; in these cases we calculate that $\text{fix}(t)$ is greater than q^2 or q respectively (noting that q is odd in the latter case as $T = U_3(q)$, q even is excluded by assumption), again contradicting (1).

The case where $T = P\Omega_d^{\epsilon}(q)$ with $H = P_i$ is very similar, but using instead the involution

$$t = \text{diag}(B, I_{d-4}), \tag{5}$$

where $B = -I_4 \in \Omega_4^+(q)$ if q is odd, and $B = J_2 \otimes I_2 \in SL_2(q) \otimes SL_2(q) = \Omega_4^+(q)$ if q is even. We leave the details to the reader.

There are two remaining parabolic cases: these are the cases where $T = P\Omega_8^+(q)$ or $Sp_4(q)$ (q even), G contains a graph automorphism of order 3 or 2, and $H = P_{134}$ (obtained by deleting nodes 1,3,4 from the D_4 Dynkin diagram) or B (a Borel subgroup), respectively. In the first case, we regard points as flags $V_1 \subset V_3 \subset V_4$ of singular subspaces, and the involution defined as in (5) fixes at least $(q+1)^2$ of these (this is the number of singular 1-spaces in an O_4^+-space on which t acts trivially); and in the second case, regarding points as flags $V_1 \subset V_2$, the involution defined in (4) fixes at least $2q$ of these. Hence (1) is contradicted as usual. ■

Lemma 3.6 *The conclusion of Proposition* 3.3 *holds if* $H \in \mathcal{C}_1 \cup \mathcal{C}_1'$.

Proof. These are the cases in which H is a reducible maximal subgroup of G. Since we have covered the parabolics in the previous lemma, the remaining cases are those in which $H \cap T = N_i$, where N_i is the stabilizer of a non-degenerate i-space in cases U,S,O, or a nonsingular 1-space in case O with q even, or a decomposition $V = V_i \oplus V_{d-i}$ in case L where G contains a graph automorphism.

The proof follows along the same lines as that of the previous lemma. Define an involution $t \in T$ as in (4) or (5). If we set $n = |T : N_i| := s_{d,i}(q)$, then t fixes at least $s_{d-r,i}(q)$ points, where $r = 4$ in case O and $r = 2$ otherwise, and we check that this number is greater than $s_{d,i}(q)^{1/6}$, apart from a few cases with small d, i for which slightly better estimates of fix(t) are required to violate the inequality (1). ■

Lemma 3.7 *The conclusion of Proposition* 3.3 *holds if* $H \in \mathcal{C}_8$.

Proof. In this case T and H are as follows:

T	Type of H
$L_d(q)$	$Sp_d(q)$, $U_d(q^{1/2})$, $O_d^\epsilon(q)$
$Sp_d(q)$ (q even)	$O_d^\epsilon(q)$

In all cases there is an involution $t = \mathrm{diag}(A, I_{d-2}) \in H \cap T$ defined as in (4). We proceed by computing a lower bound for $|C_G(t) : C_H(t)|$ and checking that it is greater than $n^{1/6}$, contradicting (2).

First consider the case where $T = L_d(q)$ and H is of type $Sp_d(q)$. Write $d = 2l$, so $l \geq 2$. We have $|C_G(t) : C_H(t)| \geq |SL_{2l-2}(q) : Sp_{2l-2}(q)|$, and this is greater than $n^{1/6}$ unless $l = 2$. Now let $l = 2$. If q is even then $|C_G(t) : C_H(t)| = q^5\,|SL_2(q)|\,/q^3\,|SL_2(q)| = q^2$ which is again greater than $n^{1/6}$. And if q is odd we regard T as the orthogonal group $P\Omega_6^+(q)$ acting on nonsingular 1-spaces, and $t = (-I_2, I_4)$, from which we see that fix(t) is at least the number of nonsingular 1-spaces in the 4-space on which it acts trivially; this is greater than $n^{1/6}$, contradicting (1).

The cases where $T = L_d(q)$ and H is of type $U_d(q^{1/2})$ or $O_d^\epsilon(q)$ are very similar to the one in the previous paragraph. Finally, if $T = Sp_d(q)$ and $H \cap T = O_d^\epsilon(q)$ with q even and $d = 2l \geq 4$, then t is a reflection in $O_{2l}^\epsilon(q)$, so $|C_{H\cap T}(t)| = 2|SO_{2l-1}(q)|$. Hence we have $n = \frac{1}{2}q^l(q^l + \epsilon)$ and $|C_T(t) : C_{H\cap T}(t)| = \frac{1}{2}q^{2l-1}$, contradicting (2). ■

Lemma 3.8 *The conclusion of Proposition* 3.3 *holds if* T *is not of type* A_1, B_m $(m \leq 4)$, C_m $(m \leq 4)$, D_4 *or* ${}^2D_4$.

Proof. Assume T is not one of the types in the statement. By Lemma 3.4 together with Lemmas 3.5, 3.6 and 3.7, H is as in (iii), (iv) or (v) of Lemma 3.4.

If H is as in Lemma 3.4(iii) then $H \in \mathcal{C}_6$ and $T \in \mathcal{L}_1$. A Magma computation shows that in each case there is an involution $t \in H$ violating the bound (1).

Now suppose H is as in Lemma 3.4(v). Again a Magma computation rules out $T \in \mathcal{L}_2$, so assume H, T are as in Table 3. In all cases except the last row of the table, V is the fully deleted permutation module for $\mathrm{Soc}(H) = A_{d+\alpha}$ ($\alpha = 1$ or 2) over $\mathbb{F}_2$ or $\mathbb{F}_3$. Let $t = (1\,2)\,(3\,4) \in \mathrm{Soc}(H)$. If $q = 2$ then in the notation of [14, Chapter 4], t is an involution in $T = Cl(V) = Sp(V)$ or $\Omega(V)$ with $V \downarrow t = V(2)^2 + W(1)^{(d-4)/2}$, and the centralizer $C_T(t)$ can be read off from [14, Theorem 4.2]. In all cases it follows that $|C_T(t) : C_{H\cap T}(t)| > n^{1/6}$, contrary to (2): for example, if $T = \Omega^-_{10}(2)$ and $\mathrm{Soc}(H) = A_{12}$, then $|C_T(t)| = 2^8|Sp_6(2)|$ and $|C_{S_{12}}(t)| = 4|S_8|$, while $n \leq |T : S_{12}|$. If $q = 3$ then from Table 3 we have $T = P\Omega^+_{10}(3)$, $\mathrm{Soc}(H) = A_{12}$; here t acts on V as $(-I_2, I_8)$, and again we find that $|C_T(t) : C_{H\cap T}(t)| > n^{1/6}$. For the last row of Table 3, $\mathrm{Soc}(H) = M_{12}$, $T = \Omega^-_{10}(2)$ and again V is the fully deleted permutation module, dealt with in similar fashion.o

It remains to consider the case where H is as in (iv) of Lemma 3.4, so that H is as in Table 2. We shall give the arguments for cases L and O, and leave the similar cases U and S to the reader.

Suppose then that $T = L_d(q)$ and H is as in Table 2. First let $H \in \mathcal{C}_2$, so that H is of type $GL_{d/k}(q) \wr S_k$ with $k \leq 3$, the stabilizer of a decomposition of V as a direct sum of k subspaces of dimension d/k. Then H contains a conjugate of the involution $t = \mathrm{diag}(A, I_{d-2})$ defined as in (4). Write $V = V_2 \oplus V_{d-2}$, where t acts on V_2 as the matrix A, and t acts trivially on V_{d-2}. If $k = 2$, set $l := d/2 \geq 2$, and observe that t fixes all decompositions of the form $(V_2 \oplus V_{l-2}) \oplus V_l$, where $V_{l-2} \oplus V_l = V_{d-2}$. Hence $\mathrm{fix}(t) \geq |GL_{2l-2}(q) : GL_{l-2}(q) \times GL_l(q)| > q^{2l(l-2)}$, while $n < q^{2l^2}$. Therefore (1) fails for $l > 2$, while if $l = 2$ then it is easy to see that $\mathrm{fix}(t) \geq q^2$, again contradicting (1). The case $k = 3$ is similar.

Now let $H \in \mathcal{C}_3$ (still with $T = L_d(q)$), so that H is of type $GL_{d/k}(q^k)$ with $k \leq 3$. Set $l = d/k$. Observe that $l > 1$: for if $l = 1$ then k must be 3, but this means that $H \cap T$ has odd order (as in row 3 of the table in Lemma 2.1). If $l \geq 3$, let $t = \mathrm{diag}(A, I_{l-2}) \in SL_l(q^k) \leq H$, where A is as defined in (4). Then t acts on V as $\mathrm{diag}(A^k, I_{(l-2)k})$ (where A^k represents k diagonal blocks A). Now $C_G(t)$ and $C_H(t)$ can be worked out using [14, 7.1], and one checks that $|C_G(t) : C_H(t)| > n^{1/6}$. If $l = 2$, let $t = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(q^k) \leq H$, acting on V as $\begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix}$ and argue similarly.

To complete the case $T = L_d(q)$, let $H \in \mathcal{C}_5$, so that H is of type $GL_d(q^{1/k})$ with $k \leq 3$. Here we define $t = \mathrm{diag}(A, I_{d-2}) \in SL_d(q^{1/k}) \leq H$ as in (4), and argue in the usual way that $|C_G(t) : C_H(t)| > n^{1/6}$.

Now suppose that $T = P\Omega_d^\epsilon(q)$ and H is as in Table 2. Assume first that $d = 2l$ and H is of type $O_l^\delta(q) \wr S_2$. Then $\epsilon = +$ and $n \leq |\Omega_{2l}^+(q)|/|SO_l(q)|^2 < 4q^{l^2}$. We can pick an involution $t = (A, I_{2l-4}) \in H$, where $A = -I_4$ if q is odd, and A has Jordan form J_2^2 if q is even (where each of the J_2's acts on a non-degenerate subspace of type O_2^+). If q is odd then we can choose t so that $|C_G(t) : C_H(t)| \geq |\Omega_4^+(q) \times \Omega_{2l-4}^+(q) : SO_2^\delta(q)^2 \times SO_{l-2}^\delta(q)^2|$, and this is greater than $n^{1/6}$; and if q is even then $C_G(t)$ and $C_H(t)$ are given by [14, 7.3], and we get the same conclusion. We use the same involution t for the cases where H is of type $O_{d/k}^\delta(q) \wr S_k$ with $k = 3, 4$ or 5. And if H is of type $O_1(q) \wr S_d$ then q is odd and we use an involution $t = (-I_2, I_{d-2})$ to obtain $|C_G(t) : C_H(t)| > n^{1/6}$. The last case with $H \in \mathcal{C}_2$ is of type $GL_{d/2}(q)$, and for this we use the usual centralizer argument taking t in $GL_{d/2}(q)$ as in (4).

For $H \in \mathcal{C}_3$ of type $O_{d/k}(q^k)$ or $GU_{d/2}$ we define $t \in H$ as in (4) and obtain $|C_G(t) : C_H(t)| > n^{1/6}$ as usual. For $H \in \mathcal{C}_4$ of type $Sp_2(q) \otimes Sp_{d/2}(q)$ we use the same definition of $t \in Sp_{d/2}(q)$. And finally the cases where $H \in \mathcal{C}_5$ are handled using t as in (5). ■

Lemma 3.9 *The conclusion of Proposition* 3.3 *holds if* T *is of type* B_3, B_4, C_3, C_4 *or* ${}^2D_4$.

Proof. Suppose T is of one of these types. The maximal subgroups of G are given by [5]. We know that H is not in $\mathcal{C}_1 \cup \mathcal{C}_1' \cup \mathcal{C}_8$ by Lemmas 3.6 and 3.7. We also have $|H| > |C_G(t)|^{6/5}/|G|^{1/5}$ for some involution $t \in T$ by Lemma 2.2(iii), and the minimal involution centralizer orders are given in the proofs of [15, 4.1, 4.3]. It follows from these observations that either H is as in Table 2, or H is in Table 4.

The subgroups in Table 2 are handled as in the previous lemma, so assume H is in Table 4. In all cases it is routine to find an involution $t \in H$ such that $|C_G(t) : C_H(t)| > n^{1/6}$. As an illustration, consider the case where $T = \Omega_7(q)$ (q odd) and $H \cap T = G_2(q)$. An involution $t \in G_2(q)$ satsifies $|C_{G_2(q)}(t)| = |SL_2(q)|^2$, while $C_T(t) = (\Omega_4^+(q) \times \Omega_3(q)).2$, so that $|C_G(t) : C_H(t)| \geq \frac{1}{2}q(q^2-1)$. Since $n = q^3(q^4-1)$, the conclusion follows in this case. ■

Lemma 3.10 *The conclusion of Proposition* 3.3 *holds if* T *is of type* A_1, C_2 *or* D_4.

Proof. Suppose $T = L_2(q)$ and H is not parabolic. When q is odd, $H \cap T$ is $D_{q\pm1}$, of type $L_2(q_0)$, or A_4, S_4 or A_5; and when q is even $H \cap T$ is $D_{2(q\pm1)}$ or $L_2(q_0)$ (where $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$). In all cases it is routine to find an involution $t \in H \cap T$ and check that $|C_G(t) : C_H(t)| > n^{1/6}$.

Likewise, when $T = PSp_4(q)$ or $P\Omega_8^+(q)$, the non-parabolic maximal subgroups H of G are given by [5, Tables 8.12-8.14, 8.50], and in all cases

Table 4:

T	$H \cap T$
$PSp_6(q)$ (q odd)	$Sp_2(q) \circ GO_3(q) \in \mathcal{C}_4$
$PSp_6(q)$ (q even)	$G_2(q) \in \mathcal{S}$
$PSp_6(3)$	$L_2(13) \in \mathcal{S}$
$PSp_6(5)$	$J_2 \in \mathcal{S}$
$Sp_8(2)$	$S_{10} \in \mathcal{S}$
$PSp_8(3)$	$2^6.U_4(2) \in \mathcal{C}_6$
$\Omega_7(q)$	$G_2(q) \in \mathcal{S}$
$\Omega_7(p)$ ($p \leq 11$)	$Sp_6(2) \in \mathcal{S}$
$\Omega_7(3)$	$S_9 \in \mathcal{S}$
$\Omega_9(3)$	$A_{10} \in \mathcal{S}$

we find an involution $t \in H \cap T$ such that $|C_G(t) : C_H(t)| > n^{1/6}$. There are numerous cases to check, but the arguments are all similar to those we have given previously and we omit the details. ■

This completes the proof of Proposition 3.3.

3.3 Exceptional groups

Continue to assume that G is an almost simple primitive permutation group of degree n on a set Ω with point-stabilizer H and socle T, and (i) and (ii) of Theorem 4 do not hold. In this subsection we prove

Proposition 3.11 *If T is an exceptional group of Lie type, then $T = {}^2B_2(q)$ in the 2-transitive action of degree q^2+1.*

Together with Propositions 3.1, 3.2 and 3.3, this will complete the proof of Theorem 4.

Let us embark upon the proof of Proposition 3.11. Assume that T is an exceptional group of Lie type over a field $\mathbb{F}_q$ of characteristic p. We know that $|H \cap T|$ is even, and the inequalities (1) and (2) hold for all involutions $t \in H \cap T$.

Lemma 3.12 *Assume T is not of type G_2, ${}^2G_2$, ${}^3D_4$ or ${}^2B_2$. Then one of the following holds:*

(i) *H is a parabolic subgroup;*

(ii) *H is as in Table 5.*

Proof. The proof is the same as that of Lemma 3.4: Proposition 2.3 and Lemma 2.2(iv) imply that $|H \cap T| > |T|^{1/3}$, and the maximal subgroups satisfying this bound are classified in [1]. ∎

Remark Most of the subgroups in Table 5 are subgroups of maximal rank in the sense of [13], and their precise structure is given in [13, Table 5.1]. All the subgroups in the table contain the group indicated there with small index (at most 3).

Table 5:

T	Type of H
$E_8(q)$	$A_1(q)E_7(q)$, $D_8(q)$, $A_2^\epsilon(q)E_6^\epsilon(q)$, $E_8(q^{1/2})$
$E_7(q)$	$(q-\epsilon)E_6^\epsilon(q)$, $A_1(q)D_6(q)$, $A_7^\epsilon(q)$, $A_1(q)F_4(q)$, $E_7(q^{1/2})$
$E_6^\epsilon(q)$	$(q-\epsilon)D_5^\epsilon(q)$, $A_1(q)A_5^\epsilon(q)$, $F_4(q)$, $(q-\epsilon)^2D_4(q).S_3$, $(q^2+\epsilon q+1)\,{}^3D_4(q)$, $C_4(q)$ $(p \neq 2)$, $E_6^\pm(q^{1/2})$ $(\epsilon = +)$, $E_6^\epsilon(q^{1/3})$
$F_4(q)$	$B_4(q)$, $D_4(q).S_3$, ${}^3D_4(q).3$, $A_1(q)C_3(q)$, $F_4(q^{1/2})$, ${}^2F_4(q)$ $(q = 2^{2m+1})$, $C_2(q)^2$ $(p = 2)$, $C_2(q^2)$ $(p = 2)$
${}^2F_4(q)'$	$({}^2B_2(q))^2$, $C_2(q)$
$E_6(2)$	$(7 \times {}^3D_4(2)).3$
${}^2E_6(2)$	Fi_{22}, $\Omega_7(3)$
$F_4(3)$	${}^3D_4(2)$
$F_4(2)$	$L_4(3).2$

Lemma 3.13 *The conclusion of Proposition* 3.11 *holds if H is a parabolic subgroup.*

Proof. Consider first the cases where T is of type E_8, E_7, E_6^ϵ or F_4. Suppose $H \cap T = QL$, a parabolic subgroup with unipotent radical Q and Levi factor L. Since H is maximal in G, either $H = P_i$ for some i, or G contains a graph automorphism of T and $H = P_{ij}$ for some i, j. In any case L contains a subgroup $A \cong SL_2(q)$ generated by long root groups, which we take to be in the largest simple factor of L. The centralizer $D = C_T(A)$ is as follows (see [14, Table 11.4]):

T	$E_8(q)$	$E_7(q)$	$E_6^\epsilon(q)$	$F_4(q)$	$G_2(q)$
D	$E_7(q)$	$D_6(q)$	$A_5^\epsilon(q)$	$C_3(q)$	$A_1(q)$

Choose an involution $t \in A$; then t is a long root element if $p = 2$ and $t \in Z(A)$ if $p \neq 2$. Then $C_T(t) = AD$ if $p \neq 2$, and $C_T(t) = UD$, where U is the unipotent radical of the parabolic with Levi factor D, if $p = 2$. Likewise, if we set $L_0 = C_L(A)$ (again given by [14, Table 11.4]), then $C_L(t)$ is AL_0 if $p \neq 2$ and U_0L_0 (with unipotent radical U_0) if $p = 2$. It follows that

$|C_T(t) : C_{H\cap T}(t)| \geq |D : U_1L_0|$, where U_1 is a unipotent normal subgroup of U_1L_0. In all cases we calculate that

$$|D : U_1L_0| > |T : QL|^{1/6} = n^{1/6}, \tag{6}$$

contradicting (2). We illustrate this calculation with an example. Let $T = E_8(q)$ and $H = P_5 = QL$. Here $D = E_7(q)$ and $L = A_3(q)A_4(q)T_1$ where $|T_1| = q-1$. Then $L_0 = C_L(A) = A_3(q)A_2(q)T_2$, so

$$|D : U_1L_0| = |E_7(q) : U_1A_3(q)A_2(q)T_2|.$$

The index of an A_3A_2 parabolic in $E_7(q)$ is greater then q^{54}, while $n = |E_8(q) : P_5|$ is less than $4q^{104}$, giving (6).

Next consider $T = G_2(q)$. Here $H = P_1$, P_2 or a Borel subgroup B (the latter only if $p = 3$ and G contains a graph automorphism of T). Let $H \cap T = QL$ as above. Then L contains a long or short root involution t and $C_T(t)$ contains a subgroup $D \cong SL_2(q)$ generated by short or long root elements, respectively. It follows that we can choose t so that $|C_T(t) : C_{H\cap T}(t)|$ is at least the index of a parabolic of D, which is $q+1$, and this is greater than $n^{1/6}$.

If $T = {}^3D_4(q)$ then $H \cap T = QL$ with $L = ((q^3-1) \circ A_1(q)).d$ or $((q-1) \circ A_1(q^3)).d$, where $d = (2, q-1)$. In the first case an involution $t \in A_1(q)$ has centralizer containing $D = A_1(q^3)$ and we argue as above that $|C_T(t) : C_{H\cap T}(t)| \geq q^3+1$. In the second case, if q is odd we choose an involution $t \in L \setminus Z(L)$; and if q is even choose $t \in A_1(q^3)$. Now it is straightforward to see that $|C_T(t) : C_{H\cap T}(t)| \geq q^2 > n^{1/6}$.

Now let $T = {}^2F_4(q)'$. The case $q = 2$ is easily done using [6] so assume $q > 2$. Then $H \cap T = QL$ with $L = (q-1).A_1(q)$ or $(q-1).{}^2B_2(q)$. Choosing an involuton $t \in L$ we have $|C_T(t)| = q^9|A_1(q)|$ or $q^{10}|{}^2B_2(q)|$ respectively (see [14, Table 22.2.5]), and now we check that $|C_T(t) : C_{H\cap T}(t)| \geq q^2 > n^{1/6}$.

When $T = {}^2G_2(q)$, H is a Borel subgroup and an involution $t \in H$ has $C_T(t) = 2 \times L_2(q)$, so $|C_T(t) : C_{H\cap T}(t)| \geq q+1 > n^{1/6}$.

Finally, the case where $T = {}^2B_2(q)$ and H is parabolic is in the conclusion of Proposition 3.11. ■

Lemma 3.14 *The conclusion of Proposition* 3.11 *holds if T is not of type G_2, ${}^2G_2$, ${}^3D_4$ or ${}^2B_2$.*

Proof. Assume that T is not of one of these types. By the previous lemma, H is not parabolic, so Lemma 3.12 shows that H is as in Table 5.

Suppose first that H is as in one of the first four rows of Table 5, excluding ${}^2F_4(q) < F_4(q)$. Then $H \cap T$ contains a long root involution t of T, which we take in the larger simple factor of $H \cap T$. We have seen in the proof of Lemma 3.13 how to compute $C_G(t)$ (it is the group AD or UD in the proof, where U is the unipotent radical of the parabolic of T with Levi factor D), and similarly we can compute $C_{H \cap T}(t)$. Using this we easily check that $|C_T(t) : C_{H \cap T}(t)| > n^{1/6}$ in all these cases. And for $H \cap T = {}^2F_4(q) < F_4(q)$ we choose an involution $t \in H \cap T$ in the class $A_1\tilde{A}_1$ and read off $C_T(t)$ and $C_{H \cap T}(t)$ from [14, Tables 22.2.4, 22.2.5]. Similarly, for the cases where $T = {}^2F_4(q)$ we can use [14] to pick involutions $t \in H \cap T$ and compute centralizers, where t is in the T-class $(\tilde{A}_1)_2$ or $A_1\tilde{A}_1$ for H of type ${}^2B_2(q)^2$ or $C_2(q)$, respectively.

The remaining groups in Table 5 are handled in the usual way by choosing an involution $t \in H \cap T$ and checking (using [6] for the centralizers) that $|C_T(t) : C_{H \cap T}(t)| > n^{1/6}$. ■

Lemma 3.15 *The conclusion of Proposition* 3.11 *holds if T is of type G_2, ${}^2G_2$, ${}^3D_4$ or ${}^2B_2$.*

Proof. The non-parabolic maximal subgroups H of G are known and are listed in tables in [5, Chapter 8], and involution centralizers in T are well-known. It is routine to work through the lists and in each case find an involution $t \in H \cap T$ such that $|C_T(t) : C_{H \cap T}(t)| > n^{1/6}$. We omit the details. ■

This completes the proof of Theorem 4.

4 Proof of Theorem 3

Let G be a primitive permutation group of degree n on a set Ω, and suppose G is not affine or almost simple. Assume that every non-identity element in G fixes at most $n^{1/3}$ points.

We distinguish between the three possible types for the primitive group G, according to the O'Nan–Scott theorem (see [10]):

(1) product type

(2) simple diagonal type

(3) twisted wreath type.

Case (1). In this case, for some integer $m \geq 2$ we have

$$G \leq G_0 \wr S_m,$$

where $G_0 \leq S_{n_0}$ is primitive on Ω_0, a set of size n_0, $n_0^m = n$, and the wreath product has the product action on $\Omega = \Omega_0^m$. Moreover, in this case we have $\mathrm{Soc}(G) = \mathrm{Soc}(G_0)^m$, and either G_0 is almost simple or it is of simple diagonal type (as in case (2) below).

Since $\mathrm{Soc}(G_0)$ is not regular on Ω_0, we can choose an element $1 \neq t \in \mathrm{Soc}(G_0)$ fixing a point of Ω_0. Then the m-tuple $g = (t, 1, \ldots, 1) \in \mathrm{Soc}(G_0)^m \leq G$ fixes at least n_0^{m-1} points of Ω, and hence

$$\mathrm{fix}(g) \geq n_0^{m-1} \geq n^{\frac{1}{2}},$$

a contradiction.

Case (2). In this case, for some integer $m \geq 2$ and some simple group T we have

$$T^m \leq G \leq N_{S_n}(T^m),$$

where T^m is embedded in S_n via its action on the cosets of the diagonal subgroup $D = \{(u, \ldots, u) : u \in T\}$. In this case we have $n = |T|^{m-1}$.

Let $t \in T$ be an involution and let $x = (t, t, \ldots, t) \in D$. Then $C_{T^m}(x) = C_T(t)^m$. Noting that $|C_T(t)| > |T|^{1/3}$ by Proposition 2.4, we therefore have

$$|C_{T^m}(x) : C_D(x)| = |C_T(t)|^{m-1} \geq (|T|^{\frac{1}{3}})^{m-1}.$$

Hence by Lemma 2.2(ii),

$$\mathrm{fix}(x) \geq (|T|^{m-1})^{\frac{1}{3}} = n^{\frac{1}{3}},$$

which is a contradiction.

Case (3). Here G is a twisted wreath product of the form $T\ \mathrm{twr}_\phi H = T^m H$, where T is a non-abelian simple group, $N := \mathrm{Soc}(G) = T^m$ is regular on Ω, H (the point-stabilizer in G) is a permutation group on $\{1, \ldots, m\}$, and ϕ is a homomorphism from the point-stabilizer H_1 (in H) to $\mathrm{Aut}(T)$ whose image contains T (see [10, p.391] for more details). It is clear from the properties of ϕ that T is a section of H. Thus H has even order; let $t \in H$ be an involution. Observe that $\mathrm{fix}(t) = C_N(t)$.

Write $N = T_1 \times T_2 \times \ldots \times T_m$ where $T_j \cong T$. Then t induces a permutation on $T_1, \ldots, T_m$ of order dividing 2. Suppose that, as such, t decomposes into m_1 cycles of length 1 and m_2 cycles of length 2 (so $m_1 + 2m_2 = m$). If T_j is a cycle of length 1, then t induces an automorphism of T_j which by Proposition 2.4 has at least $|T|^{\frac{1}{3}}$ fixed points in T_j. If T_k, T_l is an orbit of length 2, then t centralizes some diagonal subgroup of $T_k \times T_l$, so it has at least $|T|$ fixed points in $T_k \times T_l$. Altogether we see that

$$\mathrm{fix}(t) = |C_N(t)| \geq (|T|^{\frac{1}{3}})^{m_1} \cdot |T|^{m_2}.$$

Since $m_1/3 + m_2 \geq m/3$ (with equality if $m_1 = m$), we conclude that

$$\mathrm{fix}(t) = |C_N(t)| \geq |T|^{\frac{m}{3}} = n^{\frac{1}{3}},$$

a contradiction.

This completes the proof of Theorem 3.

5 Deduction of Theorem 1 and corollaries

In this section we deduce Theorem 1 and Corollaries 2 and 5 from the results already proved.

We shall need a few lemmas concerning the fixity of the actions of the groups with odd order point-stabilizers in the conclusion of Lemma 2.1.

Lemma 5.1 *Let $p \geq 7$ be a prime with $p \equiv 3 \bmod 4$, let $G = S_p$ and let H be a subgroup $p.(p-1)$. Define Ω to be the set of right cosets of H in G, and let $x \in H$ be an element of prime order q dividing $p-1$. Write $p-1 = qm$.*

(i) *Then* $\mathrm{fix}(x) = (q-1)q^{m-1}(m-1)!$.

(ii) *If $q = 2$ then* $\mathrm{fix}(x) = 2^{(p-3)/2} \cdot (\frac{p-3}{2})!$.

(iii) *If $q = \frac{p-1}{2}$ then* $\mathrm{fix}(x) = \frac{1}{4}(p-1)(p-3)$.

Proof. The element x has cycle-shape $(q^m, 1)$, and all elements of order q in H are G-conjugate, so $|x^G \cap H| = p(q-1)$. Now part (i) follows from Lemma 2.2(i), and (ii) and (iii) follow from (i). ∎

Lemma 5.2 *Let G be a primitive permutation group with socle $T = L_p^{\epsilon}(q)$ and point-stabilizer H such that $H \cap T = (\frac{q^p-\epsilon}{(q-\epsilon)(p,q-\epsilon)}).p = H_0.p$, where p is an odd prime.*

(i) *If x is an element of order p in $H \cap T \setminus H_0$, then* $\mathrm{fix}(x) = \frac{p-1}{p}|C_T(x)|$.

(ii) *If $|H|$ is even and x is an involution in H, then* $\mathrm{fix}(x) = |C_T(x) : C_{H\cap T}(x)|$.

Proof. (i) Since x acts fixed-point-freely on H_0, the number of elements of order p in $H \cap T \setminus H_0$ is $|H_0|(p-1)$. These elements act as p-cycles on a basis, so are all T-conjugate. Hence $|x^T \cap H| = |H_0|(p-1)$, and now part (i) follows from Lemma 2.2(i). Part (ii) is similar. ∎

Remark In part (ii) of the lemma, x is an involutory outer automorphism of T, and the possibilities for $C_T(x)$ are well-known (see for example [15, 4.4]): they are of type $O_p(q)$, and also $L_p(q^{1/2})$, $U_p(q^{1/2})$ (the latter two only for $\epsilon = +$ and q square).

For the sporadic groups occurring in Lemma 2.1, similar arguments yield

Lemma 5.3 *For the actions of M_{23}, Th, BM, $J_3.2$ and $O'N.2$ with point-stabilizers* 23.11, 31.15, 47.23, 19.18 *and* 31.30 *respectively, the fixities are*

$$f(M_{23}) = 5,\ f(Th) = 23328,\ f(BM) = 22,$$
$$f(J_3.2) = 272,\ f(O'N.2) = 11704,$$

realised by elements of orders 11, 3, 23, 2 *and* 2.

Proof of Theorem 1

Let G be a primitive permutation group of degree n on a set Ω, and suppose that $f(G) < n^{1/6}$. Then G is affine or almost simple by Theorem 3. If G is affine then [16] shows that $|G/R(G)| \leq 120$ as in conclusion (ii) of Theorem 1, so we assume that G is almost simple. Let T be the socle of G and H a point-stabilizer. Then Theorem 4 implies that either $H \cap T$ has odd order, or T is $L_2(q)$, $Sz(q)$ or $U_3(q)$ (q even) in the 2-transitive action of degree $q+1$, q^2+1 or q^3+1, respectively. In the latter case $L_2(q)$ and $Sz(q)$ are in conclusion (iii) of Theorem 1, and for $T = U_3(q)$ an element of the form $\mathrm{diag}(\lambda, \lambda, \lambda^{-2})$ (where $\lambda^{q+1} = 1$) fixes $q+1$ points, contradicting the assumption that $f(G) < n^{1/6}$.

It remains to consider the case where $|H \cap T|$ is odd. Here T and $H \cap T$ are given by Lemma 2.1. The cases where $G = S_p$ or Th contradict $f(G) < n^{1/6}$, by Lemmas 5.1(ii) and 5.3. All the other possibilities are in the conclusion of Theorem 1.

This completes the proof of Theorem 1.

Proof of Corollary 2

Let G be a non-affine primitive permutation group of degree n, and assume (i) and (ii) of Corollary 2 do not hold. Then G is as in (iv), (v) or (vi) of Theorem 1. If $G = A_p$ then $n = (p-2)!$, while Lemma 5.1 shows that $f(G) \geq \frac{1}{4}(p-1)(p-3)$; and if $\mathrm{Soc}(G) = L_p^{\epsilon}(q)$ then Lemma 5.2 gives $f(G) \geq \frac{p-1}{p}|C_T(x)|$ where x acts as a p-cycle on a basis, and this is at least of the order of q^{p-1}, while n is of the order of q^{p^2-p}. In both cases (i) of Corollary 2 holds.

Proof of Corollary 5

Let G be an almost simple primitive permutation group of degree n. Let H be a point-stabilizer and $T = \mathrm{Soc}(G)$. Suppose that there is no involution in G fixing at least $n^{1/6}$ points. Then (ii) or (iii) of Theorem 4 holds.

In case (ii) of Theorem 4, any involution in H (if one exists) fixes at least $n^{1/6}$ points by Lemmas 5.1(ii), 5.2(ii) and 5.3. Hence by assumption $|H|$ must be odd, so that involutions in G are fixed-point-free, and (ii) of Corollary 5 holds.

In case (iii) of Theorem 4, T is $L_2(q)$, $Sz(q)$ or $U_3(q)$ (q even) of degree $q+1$, q^2+1 or q^3+1, respectively. Then involutions in T fix at most 2 points, as in Corollary 5(ii). Finally, if G contains an involutory outer automorphism t of T, then either $T = L_2(q)$ and $\mathrm{fix}(t) = q^{1/2}+1$, or $T = U_3(q)$ and $\mathrm{fix}(t) = q+1$; in both cases $\mathrm{fix}(t) > n^{1/6}$. This completes the proof.

6 Proof of Theorem 6

Let G be a primitive permutation group of degree n on a set Ω, and suppose G is not affine, and also is not as in conclusion (iii) of Theorem 6. We may also assume that G is not almost simple, by Corollary 5.

Assume that G has an involution which is not fixed point free. We shall show that G then has an involution fixing at least $n^{1/3}$ points, which will be more than enough to establish Theorem 6.

As in the proof of Theorem 3, there are three types of primitive group to consider for G. In cases (2) (simple diagonal type) and (3) (twisted wreath type), we produced an involution fixing more than $n^{1/3}$ points. Hence it remains to handle case (1), in which $G \leq G_0 \wr S_m$ in the product action on $\Omega = \Omega_0^m$, and (G_0, Ω_0) is of simple diagonal or almost simple type.

Suppose first that $\mathrm{Soc}(G_0)$ possesses an involution t which fixes at least one point of Ω_0. Then the m-tuple $g = (t, 1, \ldots, 1) \in \mathrm{Soc}(G_0)^m \leq G$ is an involution fixing at least $n_0^{m-1} \geq n^{1/2}$ points of Ω.

Hence we may assume now that G_0 is almost simple and that every involution in $T := \mathrm{Soc}(G_0)$ is fixed point free on Ω_0; in other words, $(G_0)_\omega \cap T$ has odd order for $\omega \in \Omega_0$. Hence T, T_ω are as in the table of Lemma 2.1.

Claim Every involution in G_0 is either fixed point free on Ω_0, or fixes at least $n_0^{1/3}$ points of Ω_0.

Proof. Since involutions in T are fixed point free, we need to consider involutions $t \in G_0 \setminus T$. Recall that we have excluded the case where $T = L_2(q)$ with $n_0 = q+1$ and $q \equiv 3 \bmod 4$ (these occur in (iii) of Theorem 6). For the remaining cases in Lemma 2.1, $G_0 \setminus T$ can have involutions only when $T = A_p$, $L_p^{\pm}(q)$, J_3 or $O'N$. In the first case we need to consider $G_0 = S_p$ with point stabilizer $H_0 = p.(p-1)$. By Lemma 5.1(ii), for an involution $u \in H_0$ we have

$$\mathrm{fix}(u) = 2^{(p-3)/2}.((p-3)/2)!$$

and it it easily checked that this is greater than $n_0^{1/3}$ for $p \geq 7$ (as is the case by Lemma 2.1). For $T = L_p^{\pm}(q)$ we use Lemma 5.2 and the ensuing remark, and for $T = J_3$ or $O'N$ we use Lemma 5.3. Hence the Claim is proved.

By assumption, G possesses an involution t which is not fixed point free. Write

$$t = (g_1, \ldots, g_m)\pi$$

where each $g_i \in G_0$ and $\pi \in S_m$. Let $(\omega_1, \ldots, \omega_m)$ be a point in Ω fixed by t.

Observe that $\pi^2 = 1$. Let $\pi \in S_m$ have m_1 2-cycles and m_0 fixed points, so that $m_0 + 2m_1 = m$. If $i\pi = i$, then $g_i^2 = 1$ and g_i fixes ω_i, so by the Claim we have $\mathrm{fix}_{\Omega_0}(g_i) \geq n_0^{1/3}$. And if $i\pi = j \neq i$, then $g_i = g_j^{-1}$ and any element $(\alpha, \alpha g_i)$ $(\alpha \in \Omega_0)$ is fixed by $(g_i, g_i^{-1})(i\,j)$. It follows that

$$\mathrm{fix}_\Omega(t) \geq (n_0^{1/3})^{m_0}(n_0)^{m_1} \geq (n_0^m)^{1/3} = n^{1/3}.$$

This completes the proof of Theorem 6.

References

[1] S.H. Alavi and T.C. Burness, Large subgroups of simple groups, *J. Algebra*, to appear.

[2] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469-514.

[3] H. Bender, Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festlasst, *J. Algebra* **17** (1971), 527–554.

[4] W. Bosma, J. Cannon, and C. Playoust, The MAGMA algebra system I: The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[5] J.N. Bray, D.F. Holt and C.M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Math. Soc. Lecture Note Series **407**, Cambridge Univ. Press, 2013.

[6] J.H.Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

[7] P.E. Holmes and R.A. Wilson, $PSL_2(59)$ is a subgroup of the Monster, J. London Math. Soc. **69** (2004), 141–152.

[8] P.E. Holmes and R.A. Wilson, On subgroups of the Monster containing A_5's, J. Algebra **319** (2008), 2653–2667.

[9] P. Kleidman and M.W. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Note Series **129**, Cambridge Univ. Press, 1990.

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

[11] M.W. Liebeck and J. Saxl, On point stabilizers in primitive permutation groups, *Comm. Algebra* **19** (1991), 2777–2786.

[12] M.W. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of Riemann surfaces, *Proc. London Math. Soc.* **63** (1991), 266–314.

[13] M.W. Liebeck, J. Saxl and G.M. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type, *Proc. London Math. Soc.* **65** (1992), 297-325.

[14] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Mathematical Surveys and Monographs, Vol.180, American Math. Soc., Providence, RI, 2012.

[15] M.W. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the $(2,3)$-generation problem, *Annals of Math.* **144** (1996), 77–125.

[16] M.W. Liebeck and A. Shalev, Fixed points of elements of linear groups, *Bull. London Math. Soc.* **43** (2011), 897–900.

[17] A. Maroti, On the orders of primitive groups, *J. Algebra* **258** (2002), 631–640.

[18] M.F. Newman, E.A. O'Brien and A. Shalev, The fixity of groups of prime-power order, *Bull. London Math. Soc.* **27** (1995), 225–231.

[19] C. Ronse, On permutation groups of prime power order, *Math. Z.* **173** (1980), 211–215.

[20] J. Saxl and A. Shalev, The fixity of permutation groups, *J. Algebra* **174** (1995), 1122–1140.

[21] A. Shalev, On the fixity of linear groups, *Proc. London Math. Soc.* **68** (1994), 265–293.

[22] A. Shalev, Finite groups and almost free actions, The mathematical heritage of Sir William Rowan Hamilton (Dublin, 1993), *Proc. Roy. Irish Acad. Sect. A* **95** (1995), suppl., 67–74.

[23] A. Shalev, Modular representations and almost free actions, *Forum Math.* **7** (1995), 559–574.

[24] H. Wielandt, *Finite permutation groups*, Academic Press, 1964.