JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 12, Number 2, April 1999, Pages 497–520
S 0894-0347(99)00288-X

SIMPLE GROUPS, PERMUTATION GROUPS, AND PROBABILITY

MARTIN W. LIEBECK AND ANER SHALEV

1. Introduction

In recent years probabilistic methods have proved useful in the solution of several problems concerning finite groups, mainly involving simple groups and permutation groups. In some cases the probabilistic nature of the problem is apparent from its very formulation (see [KL], [GKS], [LiSh1]); but in other cases the use of probability, or counting, is not entirely anticipated by the nature of the problem (see [LiSh2], [GSSh]).

In this paper we study a variety of problems in finite simple groups and finite permutation groups using a unified method, which often involves probabilistic arguments. We obtain new bounds on the minimal degrees of primitive actions of classical groups, and prove the Cameron-Kantor conjecture that almost simple primitive groups have a base of bounded size, apart from various subset or subspace actions of alternating and classical groups. We use the minimal degree result to derive applications in two areas: the first is a substantial step towards the Guralnick-Thompson genus conjecture, that for a given genus g, only finitely many non-alternating simple groups can appear as a composition factor of a group of genus g (see below for definitions); and the second concerns random generation of classical groups. Our proofs are largely based on a technical result concerning the size of the intersection of a maximal subgroup of a classical group with a conjugacy class of elements of prime order.

We now proceed to describe our results in detail.

1.1. Intersections of maximal subgroups and conjugacy classes of classical groups.

Let G be a finite almost simple group with socle G_0, a classical group with natural module V over a field of characteristic p. We say that a maximal subgroup M of G is a *subspace subgroup* if it is reducible on V, or is an orthogonal group on V embedded in a symplectic group with $p = 2$; more specifically, M is a subspace subgroup if one of the following holds:

(1) $M = G_U$ for some proper non-zero subspace U of V, where U is totally singular, non-degenerate, or, if G is orthogonal and $p = 2$, a non-singular 1-space (U is any subspace if $G_0 = PSL(V)$);

Received by the editors May 14, 1998 and, in revised form, August 26, 1998.

1991 *Mathematics Subject Classification.* Primary 20D06; Secondary 20P05.

The second author acknowledges the support of the Israel Science Foundation, administered by the Israeli Academy of Sciences and Humanities.

(2) $G_0 = PSL(V)$, G contains a graph automorphism of G_0, and $M = G_{U,W}$ where U, W are proper non-zero subspaces of V, $\dim V = \dim U + \dim W$ and either $U \subseteq W$ or $V = U \oplus W$;

(3) $G_0 = Sp_{2m}(q)$, $p = 2$ and $M \cap G_0 = O^{\pm}_{2m}(q)$.

Note that in (3), if we regard G_0 as the isomorphic orthogonal group $O_{2m+1}(q)$, then $M \cap G_0 = O^{\pm}_{2m}(q)$ is the stabilizer of a subspace of the natural module of dimension $2m + 1$.

If M is a subspace subgroup, we call the action of G on the coset space $(G : M)$ a *subspace action* of the classical group G.

All the results in this paper rely on the following theorem, which for sentimental reasons we do not number, but refer to as $(\star)$.

Theorem $(\star)$**.** *There is a constant $\epsilon > 0$, such that if G is any almost simple classical group, M is a maximal subgroup of G which is not a subspace subgroup, and $x \in G$ is an element of prime order, then*

$$|x^G \cap M| \;<\; |x^G|^{1-\epsilon}.$$

1.2. **Minimal degrees.** Let G be a permutation group on a set Ω. We let $\mathrm{fix}(g)$ denote the number of fixed points of an element $g \in G$. Let $G^\sharp = G \setminus \{1\}$. The *fixity* $\mathrm{fix}(G)$ of G is defined by $\mathrm{fix}(G) = \max\{\mathrm{fix}(g) : g \in G^\sharp\}$. The *minimal degree* $m(G)$ of G is defined by $m(G) = |\Omega| - \mathrm{fix}(G)$, and coincides with the minimal support of a non-identity element of G. The *fixity ratio* (or *fixed point ratio*) $\mathrm{rfix}(g)$ of an element $g \in G$ is defined by $\mathrm{rfix}(g) = \mathrm{fix}(g)/|\Omega|$. We also set $\mathrm{rfix}(G) = \mathrm{fix}(G)/|\Omega|$. If G is an abstract group and M is a subgroup of G, then we let $\mathrm{fix}(G, M)$ and $\mathrm{rfix}(G, M)$ denote the fixity and the fixity ratio of the permutation group obtained from the action of G on the cosets of M. For $g \in G$, $\mathrm{fix}(g, M)$ and $\mathrm{rfix}(g, M)$ are defined in a similar manner.

The fixity and the minimal degree of primitive permutation groups have been studied extensively since the days of Jordan, with numerous applications. The best elementary (i.e. classification-free) bound was obtained by Babai [Ba], who showed that if G is a primitive group on a set Ω of size n, then $m(G) \geq (\sqrt{n}-1)/2$, provided G does not contain the alternating group on Ω. Using the Classification Theorem, Liebeck and Saxl [LS] showed that $\mathrm{rfix}(G) \leq 2/3$ with some known exceptions (the 2/3 bound has recently been improved to 1/2 by Guralnick and Magaard [GM]). In fact the principal result of [LS] deals with almost simple groups, showing that if G is an almost simple group of Lie type over $\mathbb{F}_q$, then for every primitive action of G we have $\mathrm{rfix}(G) \leq \frac{4}{3q}$ (with a few exceptions when $\mathrm{soc}(G) = L_2(q), L_4(2)$ or $PSp_4(3)$).

The following result gives a much stronger bound for classical groups, provided subspace actions are excluded.

Theorem 1.1. *There is a constant $\epsilon > 0$ such that if G is an almost simple classical group over $\mathbb{F}_q$, with natural module of dimension n, and M is a maximal subgroup of G which is not a subspace subgroup, then*

$$\mathrm{rfix}(G, M) < q^{-\epsilon n}.$$

Note that such a result is not valid for subspace actions, where the fixity ratio is sometimes as large as q^{-1} (roughly). However, results from [Shi] and [GK] show that similar bounds also hold if M is a subspace subgroup, provided the subspace stabilized is not of dimension less than δn (or $> n - \delta n$), where $\delta = \delta(\epsilon)$.

1.3. **The genus conjecture.** The bound obtained in Theorem 1.1 can be applied in several contexts. First, we use it in order to obtain a partial solution to the genus conjecture of Guralnick and Thompson [GT].

To state this, let G be a finite group acting faithfully and transitively on a set Ω of size n, and let $E = \{x_1, \dots, x_k\}$ be a generating set for G with $x_1 \dots x_k = 1$. If $x \in G$ has cycles of length $r_1, \dots, r_l$ in its action on Ω, define the *index* $\mathrm{ind}(x) = \sum_1^l (r_i - 1)$. The *genus* $g = g(G, \Omega, E)$ is defined by

$$2(n + g - 1) = \sum_{i=1}^{k} \mathrm{ind}(x_i),$$

and the genus $g(G, \Omega)$ of the permutation group (G, Ω) is the minimum value of $g(G, \Omega, E)$ over all such generating sets E. We say that G is a group of genus g if there is a faithful transitive G-set Ω such that $g(G, \Omega) \le g$. Such a group is the monodromy group of a cover $X \to Y$, where X is a compact connected Riemann surface of genus g and Y is the Riemann sphere (see [Gu] for background). Groups of genus g (particularly the case $g = 0$) have been extensively studied; for a survey, see [Gu]. The main conjecture in the subject, the Guralnick-Thompson genus conjecture [GT], states that if $\mathcal{E}(g)$ is the set of non-abelian, non-alternating composition factors of groups of genus g, then $\mathcal{E}(g)$ is finite for each g.

The genus conjecture was reduced to the almost simple case in [Gu, 5.1]. More specifically, one is required to show that only finitely many almost simple groups of Lie type have primitive permutation representations of given genus g.

Thus let G be an almost simple group of Lie type over the field $\mathbb{F}_q$. It is shown in [LS] that if G has genus g, then q is bounded in terms of g. Therefore, in order to prove the conjecture it suffices to deal with classical groups in arbitrarily large dimension. The case $g = 0$ and $G = L_n(q)$ was settled by Shih [Shi]. Recently it has been shown in [LP] that only finitely many classical groups G have primitive permutation representations of genus g provided the point-stabilizer M lies in the class $\mathcal{S}$ in Aschbacher's classification of maximal subgroups of classical groups (see [As, KLi]). Here we extend this result to all but subspace actions.

Theorem 1.2. *For any integer $g \ge 0$ there are only finitely many classical groups in non-subspace actions having genus g.*

Therefore, in order to complete the proof of the genus conjecture, it remains to deal with subspace actions of classical groups.

1.4. **Base size.** Recall that a *base* of a permutation group G on a set Ω is a subset $B \subseteq \Omega$ whose pointwise stabilizer $G_{(B)}$ is trivial. Bases arise in estimating the orders of primitive permutation groups, and also play an important role in computational group theory (in various polynomial-time algorithms). Denote by $b(G)$ the minimal size of a base for G. There are several conjectures suggesting upper bounds on $b(G)$. A conjecture of Cameron and Kantor [Ca1, Conjecture 3.4, p. 343], [CK, p. 260], [Ca2, p. 638] concerns almost simple primitive groups G; it states that for such groups, $b(G)$ is bounded by some absolute constant, unless G lies in a prescribed list of exceptions. Our next result settles this conjecture in the affirmative.

Theorem 1.3. *There exists an absolute constant c such that for any almost simple primitive permutation group G, one of the following holds:*

(i) *G is A_n or S_n acting on k-subsets of $\{1, \ldots, n\}$ or on partitions of $\{1, \ldots, n\}$ into k parts of size n/k;*
(ii) *G is a classical group in a subspace action;*
(iii) *$b(G) \leq c$.*

Furthermore, excluding G as in (i) or (ii), the probability that a random c-tuple of elements from the permutation domain forms a base for G tends to 1 as $|G| \to \infty$.

We note that $b(G)$ is unbounded for the groups in parts (i)–(ii), since the orders of these groups are not bounded by a fixed polynomial function of their degree. The last statement in Theorem 1.3 is in fact conjectured explicitly in [CK].

Another conjecture concerning base size was recently settled in [GSSh]. It was shown there that, if G is a primitive permutation group not involving A_d (that is, having no section isomorphic to A_d), then $b(G) \leq f(d)$ for some function of f depending only on d. The function obtained in [GSSh] is quadratic, and it was asked whether a similar result holds with a linear function. The answer is provided by

Theorem 1.4. *Let G be a primitive permutation group not involving A_d. Then $b(G)$ is bounded above by a linear function of d.*

1.5. **Random generation.** In spite of considerable progress in the study of generation, and random generation, of finite simple groups, some natural problems still remain open.

It has recently been shown [Di, KL, LiSh1] that a randomly chosen pair of elements of a finite simple group G generates G with probability $\to 1$ as $|G| \to \infty$. An interesting related problem, which first arose in [KL], deals with generation by a fixed element and a randomly chosen one. Given an element $x \in G$, let $P_x(G)$ denote the probability that $\langle x, y\rangle = G$, where $y \in G$ is randomly chosen, and set $P^-(G) = \min\{P_x(G) : x \in G^{\#}\}$. It was conjectured in [KL] that $P^-(G) \to 1$ as $|G| \to \infty$, but this was refuted in [GKS]. While the cases of alternating groups and groups of Lie type over fields of bounded size are now well-understood ($P^-(G)$ is bounded away from 1 in these cases), the behaviour of $P^-(G)$ for classical groups G over unbounded fields is still unclear. We settle this as follows.

Theorem 1.5. *Let G be a classical simple group in dimension n over the field $\mathbb{F}_q$. Suppose $q \to \infty$. Then $P^-(G) \to 1$, regardless of n.*

If n is bounded, then the result is proved in [GKS], so it remains to consider the case where both q and n tend to infinity, which is what we do here. We note that the case $G = L_n(q)$ is settled in [Sh1] using different methods.

The next problem, posed by G. Robinson, deals with random generation of simple groups by two conjugate elements. Suppose we choose at random $x \in G$ and then we choose at random a conjugate x^y of x. What can be said of the probability that $\langle x, x^y\rangle = G$?

Theorem 1.6. *Let G be a classical simple group, and let x, y be randomly chosen elements of G. Then the probability that $\langle x, x^y\rangle = G$ tends to 1 as $|G| \to \infty$.*

This extends results from [Sh2]. In fact Theorem 1.6 has recently been extended to all simple groups G in [GLSS].

1.6. **Structure of the paper.** There are three further sections. In the first, we assume Theorem ($\star$) to be true, and deduce Theorems 1.1–1.6. The second and third comprise the proof of Theorem ($\star$).

2. Proofs of the main results

In this section we assume that Theorem ($\star$) holds, and use it to derive Theorems 1.1–1.6.

Denote by $\mathrm{Cl}(n,q)$ the set of almost simple groups whose socle is a classical group over $\mathbb{F}_q$ with natural module of dimension n, and by $Cl_n(q)$ a quasisimple group with central factor group in $\mathrm{Cl}(n,q)$.

Proof of Theorem 1.1. Let $G \in \mathrm{Cl}(n,q)$, and let M be a maximal subgroup of G which is not a subspace subgroup. Write Ω for the coset space $(G : M)$. Let $x \in G$ be a non-trivial element with a maximal number of fixed points on Ω. Then $\mathrm{fix}(x) = \mathrm{fix}(G)$, and by replacing x with a non-trivial power if necessary, we can assume that x has prime order. We have

$$\mathrm{rfix}(G) = \mathrm{fix}(x)/|\Omega| = |x^G \cap M|/|x^G|.$$

By Theorem ($\star$), therefore, $\mathrm{rfix}(G) < |x^G|^{-\epsilon}$. Now all conjugacy classes of G have size greater than $P(G)$, the smallest degree of a faithful permutation representation of G, and lower bounds for $P(G)$ are given in [KLi, 5.2.2]. In particular we see that, excluding a finite number of possibilities for G, we have $P(G) > q^{n/2}$. Consequently $\mathrm{rfix}(G) < q^{-\epsilon n/2}$, proving Theorem 1.1.

Proof of Theorem 1.2. Fix an integer $g \geq 0$. Let $G \in \mathrm{Cl}(n,q)$ act faithfully and primitively on a set Ω of size m, where (G,Ω) is not a subspace action, and suppose $g(G,\Omega) = g$.

Assume $\mathrm{rfix}(G) \leq \frac{1}{86}$. Then $\mathrm{fix}(x) \leq m/86$ for all $1 \neq x \in G$, whence $\mathrm{ind}(x) \geq (85(d-1)m)/(86d)$, where d is the order of x (and $\mathrm{ind}(x)$ is as defined in §1.3). Now G has a generating set $x_1, \dots, x_k$ such that $x_1 \dots x_k = 1$ and $\sum \mathrm{ind}(x_i) = 2m - 2 + 2g$. Therefore, writing d_i for the order of x_i, we have

$$\frac{85}{86} m \sum \frac{d_i - 1}{d_i} \leq 2m - 2 + 2g.$$

If $\sum (d_i - 1)/d_i \geq 85/42$, it follows that $m < cg$ for some constant c. Otherwise, one of the following holds:

(1) $k = 4$, $(d_1, d_2, d_3, d_4) = (2,2,2,2)$;
(2) $k = 3$, $\sum (1/d_i) \geq 1$;
(3) $k \leq 2$.

In each case G is either solvable or isomorphic to A_5 (see [Ma, Chapter II]).

We conclude that there are only finitely many possibilities for non-subspace actions (G,Ω) satisfying $g(G,\Omega) = g$ and $\mathrm{rfix}(G) \leq 1/86$. On the other hand, by Theorem 1.1 there are also only finitely many possibilities for non-subspace actions (G,Ω) of classical groups G such that $\mathrm{rfix}(G) > 1/86$. Theorem 1.2 follows.

Proof of Theorem 1.3. Let G be an almost simple primitive permutation group on a set Ω, and suppose (G,Ω) is not as in (i) or (ii) of Theorem 1.3. We shall show that for a suitably chosen constant b, almost every b-tuple of elements of Ω forms a base for G. If G is alternating or symmetric, this holds with $b = 2$, by [CK, Theorem 2.2]. If G is a group of Lie type in bounded dimension, the assertion follows from [GSSh]. Thus it remains to deal with classical groups $G \in \mathrm{Cl}(n,q)$ of large dimension. Let $Q(G,b)$ denote the probability that a randomly chosen b-tuple from Ω does not form a base for G. Let P denote the set of elements of prime order in G, and let $x_1, \dots, x_r$ be a set of representatives for the G-conjugacy classes of elements of P. Let M be the stabilizer of a point in Ω (so that M is a maximal subgroup of G).

Note that, for a given $x \in G$, the probability that a randomly chosen point of Ω is fixed by x is $\mathrm{rfix}(x)$. Therefore the probability that a randomly chosen b-tuple of elements of Ω is fixed by x is $\mathrm{rfix}(x)^b$. Now, if a b-tuple is not a base, then it is fixed by some element $x \in G$ of prime order. This yields

$$Q(G,b) \le \sum_{x\in P} \mathrm{rfix}(x)^b = \sum_{i=1}^{r} |x_i^G| \cdot (|M \cap x_i^G|/|x_i^G|)^b = \sum_{i=1}^{r} |M \cap x_i^G|^b/|x_i^G|^{b-1}.$$

Since by assumption, (G,Ω) is not a subspace action, Theorem ($\star$) gives

$$|M \cap x_i^G| \le |x_i^G|^{1-\epsilon} \ \ (1 \le i \le r).$$

Combining the above inequalities we find that

$$Q(G,b) \le \sum_{i=1}^{r} |x_i^G|^{b(1-\epsilon)-(b-1)} = \sum_{i=1}^{r} |x_i^G|^{1-b\epsilon}.$$

Suppose $b > \epsilon^{-1}$. Then $1 - b\epsilon < 0$, and

$$Q(G,b) < r \cdot |C|^{1-b\epsilon},$$

where C is a conjugacy class of minimal size in G. As observed in the proof of 1.1, we have $|C| \ge q^{n/2}$ (recall $G \in \mathrm{Cl}(n,q)$). On the other hand, if l is the (untwisted) Lie rank of G, and $k(G)$ is the number of conjugacy classes in G, then by [LPy, Theorem 1] we have

$$r \le k(G) \le (6q)^l |G : \mathrm{soc}(G)|,$$

and this is less than q^{4n} (note that $|G : \mathrm{soc}(G)| \le |\mathrm{Out}(\mathrm{soc}(G))|$).

Hence, letting $b \ge 11\epsilon^{-1}$, say, we have $1 - b\epsilon \le -10$, so

$$Q(G,b) \le r|C|^{-10} \le q^{4n}q^{-5n} = q^{-n}.$$

Thus $Q(G,b) \to 0$ as $|G| \to \infty$. Hence, with this choice of b, almost all b-tuples form a base, and the Cameron-Kantor conjecture follows. Note that in [CK] this conjecture is already formulated in the probabilistic form established here.

Proof of Theorem 1.4. For $d \ge 5$, let Γ_d denote the class of finite groups which do not involve A_d. Let $G \in \Gamma_d$ be a primitive permutation group. We have to bound $b(G)$ by a linear function of d. The proof in [GSSh] shows that it suffices to consider two cases:

(1) the case where G is almost simple, and
(2) the case where $G = VH \le AGL(V)$ is of affine type and H is a primitive (irreducible) subgroup of $GL(V)$.

Indeed, if the base size of G is bounded by $f(d)$ in these two case, then [GSSh] shows that the base size of a general primitive group G in Γ_d will be at most $20 + 2\log d + f(d)$.

We first handle case (1). Suppose $G \in \Gamma_d$ is almost simple. By Theorem 1.3, we may assume G is as in (i) or (ii) of 1.3, since otherwise the base size of G is bounded. It is shown in [GSSh] that if $\mathrm{soc}(G)$ is alternating, then $b(G)$ is bounded by a linear function of d (this follows from known bounds on the maximal length of a chain of subgroups in G). Therefore we can assume that G is as in 1.3(ii), namely a subspace action of a classical group $G \in \mathrm{Cl}(n,q)$. Since $G \in \Gamma_d$, we have $n = O(d)$, so it suffices to show that $b(G) \leq cn$. This is done by explicit construction in [Li2, p. 14].

This completes the proof in the almost simple case.

Now consider the affine case (2). Here $G = VH \leq AGL(V)$ is of affine type, acting on the set of vectors in V, where H is a primitive subgroup of $GL(V) = GL_n(q)$ ($q = p^a$). Observe that $AGL(V)$ itself has a base of size $n+1$; hence we may assume that n is large. In order to resolve this case we need some preparations.

Lemma 2.1. *Let H be a primitive irreducible subgroup of $GL(V) = GL_n(q)$ (with n large). Then one of the following holds:*

(i) $|H| < |V|^3$;

(ii) *H stabilizes a tensor product decomposition $V = V_1 \otimes V_2$: here $H \leq GL_{n_1}(q) \circ GL_{n_2}(q)$ with $n = n_1 n_2$ and $n_1, n_2 > 1$;*

(iii) *H lies between a quasisimple subgroup S and its normalizer in $GL(V)$: either S is an alternating group A_k and V is a minimal module for S (of dimension $k-1$ or $k-2$), or S is a classical group in $\mathrm{Cl}(\frac{n}{t}, q_0)$ for some t dividing n and some subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_{q^t}$.*

Proof. Choose t maximal such that H lies in a subgroup $X = GL_{n/t}(q^t).t$ of $GL_n(q)$ (in its natural embedding). Observe that (i) holds if $n/t = 1$; hence we may assume that $n/t \geq 2$. Now choose a classical group $Y = Cl_{n/t}(q_0) \leq X$ ($\mathbb{F}_{q_0} \subseteq \mathbb{F}_{q^t}$), minimal such that $H \leq N_X(Y)$.

We apply Aschbacher's theorem [As] to the subgroup H of the classical group $N_X(Y)$. According to this, either H contains Y, or H lies in a subgroup in one of the families $\mathcal{C}_i$ ($1 \leq i \leq 8$), or H is the normalizer of an irreducible quasisimple subgroup (we say $H \in \mathcal{S}$ in the latter case); see [KLi] for detailed descriptions of these families.

If H contains Y, then (iii) holds. If $H \in \mathcal{S}$, then by [Li1, 4.1], either (i) holds, or (iii) holds with $S = A_k$.

Now suppose $H \leq M$ with M a subgroup in the family $\mathcal{C}_i$. As H is primitive and irreducible, $i \neq 1, 2$; by choice of X and Y, $i \neq 3, 5, 8$. If $i = 4$, then M is a tensor product subgroup, and (ii) holds. If $i = 6$, then $M \leq (\mathbb{F}_{q^t}^* \circ r^{1+2a}).Sp_{2a}(r).x$, where $n/t = r^a$, r is prime and x divides n. This yields

$$|H| < q^n r^{3a} r^{2a^2} n \leq q^n n^3 n^{2\log n + 1} < q^{3n},$$

provided n is large (as assumed). Finally, if H is contained in a member of $\mathcal{C}_7$, then there are $a, t > 1$ with $n = a^t$ and $H \leq (GL_a(q) \circ \ldots \circ GL_a(q)).S_t$; this yields

$$|H| < q^{a^2 t} t! \leq q^{3a^t} = q^{3n}.$$

Thus (i) holds. ♠

A sequence of vectors $v_1, \ldots, v_k$ will be called a *strong base* for H if the only elements of H which leave the subspaces $\langle v_1 \rangle, \ldots, \langle v_k \rangle$ invariant are scalars. Define $b^*(H)$ to be the minimal size of a strong base for H.

Lemma 2.2. *There exists a constant c such that, if $H \in \Gamma_d$ is a primitive subgroup of $GL(V)$, then $b^*(H) \leq cd$.*

Proof. It is shown in [GSSh, Theorem 5.3] that there is an absolute constant c_1 such that if $G = VH \leq AGL(V)$, where $H \in \Gamma_d$ is a primitive subgroup of $GL(V)$, then in the action on V,

$$\mathrm{rfix}(G) \leq |V|^{-1/c_1 d}.$$

This shows that, if $h \in H$ is fixed and is not scalar, and $v \in V$ is randomly chosen, then the probability P_h that h leaves $\langle v \rangle$ invariant is at most $\sum_{\lambda \in \mathbb{F}_q^*} \mathrm{rfix}(\lambda h) < q\mathrm{rfix}(G) \leq q|V|^{-1/c_1 d}$.

Suppose $V = (\mathbb{F}_q)^n$, and proceed by induction on $n = \dim V$. Note that $b^*(GL(V)) = \dim V + 1$, so the result follows if $n = O(d)$. We can therefore assume that $n > 2c_1 d$, where c_1 is as above. Hence $q < |V|^{1/2c_1 d}$, so

$$P_h \leq q|V|^{-1/c_1 d} < |V|^{-1/2c_1 d}.$$

Now choose at random $v_1, \ldots, v_k \in V$, and let $Q^*(H,k)$ denote the probability that $v_1, \ldots, v_k$ do not form a strong base for H. Then

$$Q^*(H,k) \leq \sum_{h \in H \setminus Z(H)} P_h^k < |H||V|^{-k/2c_1 d}.$$

It follows that, if $|H| < |V|^3$, and $k \geq 6c_1 d$, then $Q^*(H,k) < 1$, so $b^*(H) \leq 6c_1 d$.

We now apply Lemma 2.1. If H satisfies 2.1(i), then the linear bound on $b^*(H)$ is already obtained.

Now suppose H satisfies 2.1(ii). Then we have $n = n_1 n_2$ for some $n_1, n_2 > 1$ and $H \leq GL_{n_1}(q) \circ GL_{n_2}(q)$. Let H_i be the projection of H to $GL_{n_i}(q)$ $(i = 1,2)$. Then $H_i \leq GL(V_i)$, $H_i \in \Gamma_d$ and $H \leq H_1 \circ H_2$. By induction on $\dim V$ we have $b^*(H_i) \leq cd$ $(i = 1,2)$.

We now claim that

$$b^*(H_1 \circ H_2) \leq \max\{b^*(H_1), b^*(H_2)\}$$

(where $b^*(H_i)$ refers to the minimal strong base size of H_i on V_i). To show this, let $b = \max\{b^*(H_1), b^*(H_2)\}$ and let $v_{ij} \in V_i$ $(j = 1, \ldots, b)$ be a strong base for H_i $(i = 1,2)$. Set $v_j = v_{1j} \otimes v_{2j}$. We assert that $v_1, \ldots, v_b$ is a strong base for $H_1 \otimes H_2$. Indeed, let $h = h_1 h_2$ where $h_i \in H_i$, and suppose h keeps all the subspaces $\langle v_j \rangle$ invariant. Then

$$h(v_j) = h_1(v_{1j}) \otimes h_2(v_{2j}) = \lambda v_{1j} \otimes v_{2j},$$

for some $\lambda \in \mathbb{F}_q$. This implies $h_i(v_{ij}) \in \langle v_{ij} \rangle$ for all i, j. Thus h_1, h_2 are scalars, and so is h. This establishes the claim.

Applying the claim we now obtain $b^*(H) \leq cd$ as required.

Finally, consider H as in 2.1(iii). Suppose first that $S = A_k$. Then $k < d$ and $n \in \{k-1, k-2\}$, so $n \leq d+1$. Therefore $b^*(H) \leq d+2$ in this case.

To conclude, suppose $S \in \mathrm{Cl}(n/t, q_0)$, where t divides n and $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_{q^t}$. From the proof of 2.1, we see that, viewing V as an n/t-dimensional space over $\mathbb{F}_{q^t}$, V is a natural module for S. Therefore H admits a strong base of size at most $(n/t)+1$ (the extra 1 to take care of field automorphisms). Since $n/t = O(d)$, the result follows. ♠

Since a strong base for H is also a base for H, Theorem 1.4 follows from 2.2.

Proof of Theorem 1.5. Let $G \in \mathrm{Cl}(n,q)$, and suppose $q \to \infty$. We can assume that $n \to \infty$, since otherwise the conclusion follows from [GKS]. Let $\mathcal{M}$ be a set of representatives for the conjugacy classes of the maximal subgroups of G. As in the proof of [GKS, Theorem II] we have

$$1 - P^{-}(G) \leq \sum_{M \in \mathcal{M}} \mathrm{rfix}(G, M).$$

Write $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_3$ where $\mathcal{M}_1$ consists of subspace subgroups, $\mathcal{M}_2$ consists of the subgroups lying in the Aschbacher classes $\mathcal{C}_i$ ($2 \leq i \leq 8$), together with A_k, S_k in minimal representations, and $\mathcal{M}_3$ consists of the remaining subgroups in $\mathcal{S}$.

For $i = 1, 2, 3$ write

$$E_i = \sum_{M \in \mathcal{M}_i} \mathrm{rfix}(G, M).$$

Then

$$1 - P^{-}(G) \leq E_1 + E_2 + E_3,$$

so it suffices to show that, for each i, $E_i \to 0$ as $q, n \to \infty$.

Let $M \in \mathcal{M}_1$ be the stabilizer of a k-dimensional subspace of the natural module V, where $k \leq n/2$. It follows from results of Guralnick and Kantor [GK, §3] that

$$\mathrm{rfix}(G, M) \leq q^{-\delta k},$$

where $\delta > 0$ is some absolute constant. Hence the contribution of these subgroups to E_1 is at most

$$\sum_{k \geq 1} 2q^{-\delta k} = 2q^{-\delta}(1 - q^{-\delta})^{-1},$$

which tends to 0 as $q \to \infty$. This shows that $E_1 \to 0$, except possibly in the case where G is symplectic in characteristic 2. In this case there are two additional subgroups in $\mathcal{M}_1$, namely $O_n^{+}(q)$ and $O_n^{-}(q)$. If M is one of these subgroups, then $\mathrm{rfix}(G, M) \leq 4/3q$ by [LS], and so the contribution of these subgroups to E_1 is at most $8/3q$, which tends to 0 as $q \to \infty$. Therefore $E_1 \to 0$ in any case.

Let $M \in \mathcal{M}_2$. Then by Theorem 1.1 we have

$$\mathrm{rfix}(G, M) \leq q^{-\epsilon n}.$$

On the other hand we have

$$|\mathcal{M}_2| \leq cn \log\log q$$

by [GKS, 2.2]. Therefore

$$E_2 \leq cn \log\log q \cdot q^{-\epsilon n} \to 0$$

as n or q tend to infinity.

Let $M \in \mathcal{M}_3$. By the proof of Lemma 4.1 below,

$$\mathrm{rfix}(G, M) \leq q^{-cn^{3/2}}.$$

On the other hand, as in [LiSh2, p. 89] we have

$$|\mathcal{M}_3| \leq 6n^2 q^{6n} \log q.$$

Therefore

$$E_3 \leq 6n^2 q^{6n} \log q \cdot q^{-cn^{3/2}} \to 0$$

as $n \to \infty$.

The theorem is proved.

Proof of Theorem 1.6. We adopt the notation of the previous proof. Let G be a simple group in $\mathrm{Cl}(n,q)$. We can assume that $n \to \infty$, since otherwise the conclusion follows from [Sh2].

We need some notation. Let $Q_c(G)$ denote the probability that $\langle x, x^y\rangle \neq G$. Let $\{C_i\}_{i\in I}$ be the conjugacy classes of G. Suppose $C_1 = \{1\}$ and let $I^\# = I \setminus \{1\}$. For each $i \in I$ fix a representative $g_i \in C_i$.

By [Sh2, p. 572] we have

$$Q_c(G) \leq |G|^{-1} + \sum_{i\in I^\#, M\in\mathcal{M}} \frac{|C_i \cap M|^2}{|C_i||M|} = |G|^{-1} + \sum_{i\in I^\#, M\in\mathcal{M}} \frac{|C_i\cap M|}{|M|}\mathrm{rfix}(g_i, M).$$

Let $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$ be as in the preceding proof. For $M \in \mathcal{M}$ let $\mathrm{rank}(G, M)$ denote the rank of the corresponding permutation group. Fix $M \in \mathcal{M}_1$. As in [Sh2, p. 574] we have

$$\sum_{i\in I} \frac{|C_i\cap M|}{|M|}\mathrm{rfix}(g_i, M) = |G : M|^{-1} \cdot \frac{1}{|M|}\sum_{i\in I} |C_i \cap M| \mathrm{fix}(g_i, M)$$

$$= |G : M|^{-1} \cdot \mathrm{rank}(G, M).$$

For $M \in \mathcal{M}_2 \cup \mathcal{M}_3$ we use the inequality (see [Sh2, p. 573])

$$\sum_{i\in I^\#} \frac{|C_i\cap M|}{|M|}\mathrm{rfix}(g_i, M) \leq \mathrm{rfix}(G, M).$$

Define

$$D_1 = \sum_{M\in\mathcal{M}_1} \mathrm{rank}(G, M)|G : M|^{-1},$$

and let E_2, E_3 be as in the proof of Theorem 1.5. It then follows that

$$Q_c(G) \leq |G|^{-1} + D_1 + E_2 + E_3.$$

In order to show that $Q_c(G) \to 0$, we bound each of the partial sums D_1, E_2, E_3 separately. First, since $n \to \infty$, it follows from the previous proof that $E_2, E_3 \to 0$. So it remains to consider D_1. To bound this, we need the following result bounding the ranks of subspace actions.

Proposition 2.3. *Let M be a subspace subgroup of the classical simple group $G \in \mathrm{Cl}(n,q)$.*

(i) *If M is the stabilizer of a totally singular subspace (any subspace if $G = L_n(q)$), then* $\mathrm{rank}(G, M) < cn^2$.

(ii) *If M is the stabilizer of a non-degenerate k-space ($k \leq n/2$, $G \neq L_n(q)$), then* $\mathrm{rank}(G, M) < ck^2q^{k^2}$*, and also* $\mathrm{rank}(G, M) < ck^2q^{k^2-k/2+3}$.

(iii) *If M is the stabilizer of a nonsingular 1-space with G orthogonal and $p = 2$, or if $(G, M, p) = (Sp_{2m}(q), O^{\pm}_{2m}(q), 2)$, then* $\mathrm{rank}(G, M) < cq$.

(iv) *In all cases,* $\mathrm{rank}(G, M)|G : M|^{-1} \leq cn^2q^{-n/5}$.

Proof. (i) In this case M is a parabolic subgroup of G; say $M = P_k$, the stabilizer of a k-space. It is well known (see [CIK]) that $\mathrm{rank}(G, P_k)$ is the same as $\mathrm{rank}(W, W_k)$, where W is the Weyl group of G and W_k the parabolic subgroup of W corresponding to P_k. If $G = L_n(q)$, then $W = S_n, W_k = S_k \times S_{n-k}$ and the rank is $k + 1$. If G is symplectic, unitary or orthogonal in odd dimension or of type O^-, then $W = 2^l.S_l$ (of type B_l) and $W_k = S_k \times 2^{l-k}.S_{l-k}$. In this case consider W acting in the natural imprimitive action on $\{\pm 1, \dots, \pm n\}$, with W_k the stabilizer of $\{1 \dots, k\}$, to see that $\text{rank}(W, W_k) < ck^2$ (in fact it is equal to $(k+1)(k+2)/2$). Finally, if G is orthogonal of type O^+, then $W = 2^{l-1}.S_l$ of type D_l (index 2 in type B_l) and the same considerations as above give $\text{rank}(W, W_k) < ck^2$.

(ii) Let V be the natural module for G, and let $G_1 = N_{PGL(V)}(G)$ (so that $|G_1 : G| \leq 8$; see [KL, Chapter 2]). Observe that $\text{rank}(G_1, M)$ is equal to the number of orbits of G_1 on pairs (U, W) of non-degenerate k-spaces.

Suppose first that G is not an orthogonal group in characteristic 2. Let (U, W) be a pair of non-degenerate k-spaces. Let $X = U \cap W$. The G_1-orbit of X is specified by $\dim X$ and $\dim(\text{rad}(X))$. Say $\text{rad}(x) = \langle e_1, \dots, e_r \rangle$. Then X has a (standard) basis $e_1, \dots, e_r, e_{r+1}, f_{r+1}, \dots, e_s, f_s$ (possibly with an additional nonsingular vector d if G is orthogonal), with inner products as given in [KL, §§2.4, 2.5]. Up to G_1-action, the number of possibilities for X is at most ck^2 (as there are at most k choices for r and s). Extend the above basis of X to standard bases of U and W:

$$\begin{array}{ll} \text{basis of } U: & e_1, \dots, e_r, e_{r+1}, f_{r+1}, \dots, e_s, f_s, f_1, \dots, f_r, e_{s+1}, f_{s+1}, \dots, (d, d_1) \\ \text{basis of } W: & e_1, \dots, e_r, e_{r+1}, f_{r+1}, \dots, e_s, f_s, f_1', \dots, f_r', e_{s+1}', f_{s+1}', \dots, (d, d_1') \end{array}$$

where d, d_1, d_1' are non-singular vectors which may or may not be present. Now observe that by Witt's theorem, the G_1-orbit of (U, W) is determined by the inner products of the above basis vectors of U with those of W. There are at most k^2 such inner products, so it follows that

$$\text{rank}(G_1, M) < ck^2 q^{k^2}.$$

Write $e_j' = e_j$ for $j \leq s$. We may choose the $e_i' (i \geq s+1)$ so that $(e_1, e_i') = 0$ for all but at most one value of i (take the e_i' to include a basis for the kernel of the map $v \to (e_1, v)$ from the space spanned by the e_i' to the field). Thus the G_1-orbit of (U, W) is specified by the above k^2 inner products, but excluding the (e_1, e_i') which equal zero. There are at least $(k-2)/2$ such e_i', so the orbit is specified by $k^2 - (k-2)/2 - 1$ inner products. The last part of (ii) follows.

When G is an orthogonal group in characteristic 2, the above proof goes through with minor changes. There are two possibilities for $\text{rad}(X)$ of a given dimension r, namely $\langle e_1, \dots, e_r \rangle$ and $\langle e_1 + f_1, e_2, \dots, e_r \rangle$ (the first being totally singular, the second not); and $X/\text{rad}(X)$ may be of type O^+ or O^-. There may also be up to 4 extra vectors $d, d_1, \dots$ to add to the bases of U, W. Apart from these changes, the above proof goes through.

(iii) This follows from the proof of [LPS, Proposition 1].

(iv) This is immediate from the previous parts. ♠

Since $|\mathcal{M}_1| \leq cn$, Proposition 2.3(iv) gives

$$D_1 \leq cn \cdot cn^2 q^{-n/5} = c^2 n^3 q^{-n/5} \to 0$$

as n or q tend to infinity.

Theorem 1.6 follows.

We note that the lower bounds on the various generation probabilities obtained in the proofs of 1.5 and 1.6 for classical groups in general are significantly better than the ones given in [Sh1], [Sh2] for $G = L_n(q)$.

3. Proof of Theorem ($\star$): preliminary lemmas

This section and the next are devoted to the proof of Theorem ($\star$).

Let G be an almost simple group with socle G_0, a classical group with natural module V of dimension n over a finite field $\mathbb{F} = \mathbb{F}_{q^u}$, where $u = 2$ if G_0 is unitary and $u = 1$ otherwise. Let p be the characteristic of $\mathbb{F}$.

We are required to produce a constant $\epsilon > 0$ such that, for any element $x \in G$ of prime order, and any maximal subgroup M of G which is not a subspace subgroup,

$$|x^G \cap M| < |x^G|^{1-\epsilon}.$$

Define

$$f(x, M) = \frac{\log |x^G \cap M|}{\log |x^G|}.$$

We have to show that $f(x, M) < 1 - \epsilon$.

Let G, M and x be as above. Observe first that by [LS], $|x^G \cap M|/|x^G| < \min\{2/q^{1/2}, 3/4\}$, and hence Theorem ($\star$) follows if the dimension n is bounded. Thus we may assume that n is unbounded.

By [As], the maximal subgroup M is either in one of the Aschbacher families $\mathcal{C}_i$ ($1 \leq i \leq 8$), or it lies in collection $\mathcal{S}$ of almost simple, irreducible subgroups (satisfying various other conditions); see [KLi] for descriptions of all these families.

Throughout the section, we adopt the following notation:

$o(1) = o_n(1)$;

$c, c', \ldots$ are positive constants;

$\delta, \delta', \ldots$ are small positive constants.

For a finite group M, $i_2(M)$ denotes the number of involutions in M.

Lemma 3.1. *We have $|M| < |G|^{\frac{1}{2}+o(1)}$. Moreover, there exists $\delta > 0$ such that if $|M| > |G|^{\frac{1}{2}-\delta}$, then M is of one of the following types:*

$M \in \mathcal{C}_2$: $Cl_{n/2}(q)$ *wr* S_2, $GL_{n/2}(q^u)$ ($G_0 \neq L_n(q)$)
$M \in \mathcal{C}_3$: $Cl_{n/2}(q^2).2$, $GU_{n/2}(q)$ (*G orthogonal or symplectic*)
$M \in \mathcal{C}_5$: $Cl_n(q^{1/2})$, $Sp_n(q)$ *or* $SO_n(q)$ (*G unitary*)
$M \in \mathcal{C}_8$: $Sp_n(q)$, $SO_n(q)$ *or* $SU_n(q^{1/2})$ ($G_0 = L_n(q)$).

Proof. For $M \in \mathcal{C}$ this follows by inspection of [KLi, Chap. 4] (recall M is not a subspace subgroup). For $M \in \mathcal{S}$ it follows from [Li1]. ♠

In what follows we let ($\star$) denote the conclusion of Theorem ($\star$).

Lemma 3.2. *If $|C_G(x)| < |G|^{\frac{1}{2}-\delta'}$, then ($\star$) holds.*

Proof. The hypothesis implies that $|x^G| > |G|^{\frac{1}{2}+\delta'}$, giving ($\star$) by 3.1 (first assertion). ♠

Lemma 3.3. *If $x \notin PGL(V)$, then ($\star$) holds.*

Proof. As $x \notin PGL(V)$ and has prime order, it is a field, graph or graph-field automorphism of G_0 (in the sense of [GL, §7]).

If $o(x) \geq 3$, then x is a field automorphism, and $|C_G(x)| < |G|^{\frac{1}{3}+o(1)}$, giving the result by 3.2.

Now assume $o(x) = 2$. Then $|x^G| > |G|^{\frac{1}{2}-o(1)}$ (see [LiSh2, 4.4] for example). Hence the result is immediate unless $|M| > |G|^{\frac{1}{2}-\delta}$, so assume the latter holds. Then M is given by 3.1. In each case we see using [LiSh2, 4.1, 5.4, 5.5] that $i_2(M) <$

$|M|^{\frac{1}{2}+o(1)}$. Using 3.1 we obtain $i_2(M) < |M|^{\frac{1}{2}+o(1)} < (|G|^{1/2+o(1)})^{1/2+o(1)} < |G|^{\frac{1}{4}+o(1)}$. It follows that

$$|x^G \cap M| \leq i_2(M) \leq |x^G|^{1/2+o(1)}.$$

♠

In view of 3.2 and 3.3, we assume from now on that $x \in PGL(V)$ and $|C_G(x)| > |G|^{\frac{1}{2}-o(1)}$.

Let $\bar{\mathbb{F}}$ be the algebraic closure of $\mathbb{F} = \mathbb{F}_{q^u}$, and let $\bar{V} = V \otimes \bar{\mathbb{F}}$. Let $\hat{x}$ be a preimage of x in $GL(V)$. Define

$$\nu(x) = \nu_{V,\bar{\mathbb{F}}}(x) = \min\{\dim[\bar{V}, \lambda\hat{x}] : \lambda \in \bar{\mathbb{F}}^*\}.$$

Note that $\nu(x) > 0$ if $x \neq 1$. Take $\bar{G}$ to be one of the classical algebraic groups $SL(\bar{V}), Sp(\bar{V}), SO(\bar{V})$, such that there is a Frobenius morphism σ of $\bar{G}$ satisfying $G_0 = \bar{G}_\sigma/Z(\bar{G}_\sigma)$.

Lemma 3.4. *Suppose $\nu(x) = s$. Then the following hold.*

(i) *If $G_0 = L_n^\epsilon(q)$, we have*

$$cq^{s(2n-s)} > |x^G| > c' \max(q^{2s(n-s)}, q^{ns}).$$

(ii) *If $G_0 = PSp_n(q)$ or $P\Omega_n^\epsilon(q)$, then*

$$cq^{s(2n-s+1)/2} > |x^G| > c' \max(q^{s(n-s)}, q^{ns/2}).$$

Proof. (i) Assume first that x is semisimple and $\nu(x) = s$. Then $C_{\bar{G}}(\hat{x})$ lies in a σ-stable subgroup $((GL_{n-s})^k \times GL_{n-k(n-s)}) \cap \bar{G}$ for some $k \geq 1$, and contains GL_{n-s}. Hence

$$c|GL_{n-s}^\epsilon(q)| \leq |C_{GL_n^\epsilon(q)}(\hat{x})| \leq c'|GL_{n-s}^\epsilon(q) \times GL_s^\epsilon(q)|,$$

which yields $cq^{s(2n-s)} > |x^G| > c'q^{2s(n-s)}$. This also implies $|x^G| > c'q^{ns}$ if $s \leq n/2$; and if $s > n/2$, then $|C_{GL_n^\epsilon(q)}(\hat{x})| \leq |GL_{n-s}^\epsilon(q)|^{n/(n-s)} < cq^{n(n-s)}$, giving $|x^G| > cq^{ns}$.

Now assume x is unipotent (of order p). For each i, let n_i be the number of Jordan blocks in x of size i, so that $\sum in_i = n$, $\sum n_i = n - s$. By [Wa, p. 34] we have

$$|x^G| \sim q^{n^2 - 2\sum_{i<j} in_in_j - \sum in_i^2}.$$

Define

$$f = 2\sum_{i<j} in_in_j + \sum in_i^2.$$

We claim

(1) $f \geq (n-s)^2 + s$;
(2) if $s \leq n/2$, then $f \leq (n-s)^2 + s^2$; and
(3) if $s > n/2$, then $f \leq n(n-s)$.

Conclusion (i) follows from these assertions.

For (1), observe that $\sum(i-1)n_i = s$, so

$$f = (\sum n_i)^2 + \sum(i-1)n_i^2 + 2\sum_{i<j}(i-1)n_in_j$$

$$\geq (\sum n_i)^2 + \sum(i-1)n_i = (n-s)^2 + s.$$

For (2), note that

$$s^2 = \sum (i-1)^2 n_i^2 + 2\sum_{i<j}(i-1)(j-1)n_i n_j \geq \sum (i-1)n_i^2 + 2\sum_{i<j}(i-1)n_i n_j,$$

and hence $f = (n-s)^2 + \sum(i-1)n_i^2 + 2\sum_{i<j}(i-1)n_i n_j \leq (n-s)^2 + s^2$.

Finally, for (3), the fact that $\sum n_i = n-s$, $\sum(i-1)n_i = s$ gives

$$\begin{aligned} s(n-s) &= \sum (i-1)n_i^2 + \sum_{i<j}((i-1)+(j-1))n_i n_j \\ &\geq \sum (i-1)n_i^2 + 2\sum_{i<j}(i-1)n_i n_j = f - (n-s)^2. \end{aligned}$$

(ii) Assume first that $G_0 = PSp_n(q)$ (with n even), and x is semisimple with $\nu(x) = s$. Let $\bar{V}_\lambda$ be an eigenspace of $\hat{x}$ of maximal dimension $n-s$, corresponding to eigenvalue λ. If $\lambda = \pm 1$, then $\bar{V}_\lambda$ is non-degenerate, and $Sp_{n-s} \leq C_{\bar{G}}(\hat{x}) \leq Sp_{n-s} \times Sp_s$ (all σ-stable subgroups); otherwise, $\bar{V}_\lambda$ is totally singular and $GL_{n-s} \leq C_{\bar{G}}(\hat{x}) \leq (GL_{n-s})^k \times Sp_{n-2k(n-s)}$ for some $k \geq 1$. It follows that

$$|Sp_{n-s}(q)| \leq |C_{Sp_n(q)}(\hat{x})| \leq |Sp_{n-s}(q) \times Sp_s(q)|,$$

whence

$$cq^{s(2n-s+1)/2} > |x^G| > c' q^{s(n-s)}.$$

This also gives $|x^G| > c' q^{ns/2}$ unless $s \geq n/2$, in which case, as above,

$$|x^G| > c|Sp_n(q)|/|Sp_{n-s}(q)|^{n/n-s} > c' q^{ns/2}.$$

Now suppose x is unipotent, of order p. Let n_i be the number of Jordan blocks of size i in x. Then $\sum i n_i = n, \sum n_i = n-s$. Suppose $p \neq 2$. Then by [Wa, p. 37], n_i is even if i is odd, and

$$|C_{Sp_n(q)}(\hat{x})| = q^{\sum_{i<j} i n_i n_j + \sum (i-1)n_i^2/2} \prod_{i \text{ odd}} |Sp_{n_i}(q)| \prod_{i \text{ even}} q^{n_i/2}|O_{n_i}(q)|.$$

Hence

$$|x^G| \sim q^{(n^2+n-2\sum_{i<j} i n_i n_j - \sum i n_i^2 - \sum_{i \text{ odd}} n_i)/2}.$$

Define

$$g = 2\sum_{i<j} i n_i n_j + \sum i n_i^2 + \sum_{i \text{ odd}} n_i.$$

We claim that

(1) $g \geq (n-s)^2 + n - s$;
(2) if $s \leq n/2$, then $g \leq (n-s)^2 + s^2 + n$; and
(3) if $s > n/2$, then $g \leq (n-s)^2 + s(n-s) + n$.

Conclusion (ii) (for $p \neq 2$) follows from these assertions.

To see (1), observe

$$g = (\sum n_i)^2 + \sum (i-1)n_i^2 + 2\sum_{i<j}(i-1)n_i n_j + \sum_{i \text{ odd}} n_i.$$

Hence $g \geq (n-s)^2 + \sum_{i \text{ even}} n_i + \sum_{i \text{ odd}} n_i = (n-s)^2 + n - s$.

For (2), note that

$$s^2+n=(\sum(i-1)n_i)^2+\sum in_i$$

$$\geq \sum(i-1)n_i^2+2\sum_{i<j}(i-1)n_in_j+\sum_{i \text{ odd}} n_i = g-(n-s)^2.$$

And for (3),

$$s(n-s)+n=(\sum(i-1)n_i)(\sum n_i)+\sum in_i$$

$$\geq \sum(i-1)n_i^2+2\sum_{i<j}(i-1)n_in_j+\sum_{i \text{ odd}} n_i = g-(n-s)^2.$$

Finally, if $p=2$, we see from [AS, §7] that, writing $n=2m$,

$$cq^{m^2+(m-s)^2+m} > |C_G(x)| > c'q^{m^2+(m-s)^2+m-s},$$

giving $cq^{s(n-s+1)} > |x^G| > c'q^{s(n-s)}$. Since $\nu(x) \leq n/2$ in this case (as x is an involution), the conclusion follows. This completes the proof for $G_0 = PSp_n(q)$.

The proof for $G_0 = P\Omega_n(q)$ is entirely similar and is left to the reader. ♠

Lemma 3.5. *If $\nu(x) > (\frac{1}{2}+\delta)n$ (where δ is a small positive constant), then $(\star)$ holds.*

Proof. The hypothesis implies by 3.4 that $|x^G| > |G|^{\frac{1}{2}+\delta}$, giving $(\star)$ by 3.1. ♠

Assume from now on that $\nu(x) < (\frac{1}{2}+\delta)n$, where δ is a small positive constant.

For a positive integer s, and a subgroup H of $PGL(V)$, define

$$n_s(H) = |\{h \in H : o(h) \text{ prime and } \nu(h)=s\}|.$$

For a prime r, let $k_r(H)$ be the number of conjugacy classes of elements of order r in H, and define

$$k_{pr}(H) = \max\{k_r(H) : r \text{ prime}\}.$$

Lemma 3.6. (i) *If $G_0 = L_n^\epsilon(q)$, then $n_s(G) < cnq^{n+s(2n-s)}$ and $k_{pr}(G) < cnq^n$. Also, if $s < (1/2+\delta)n$, then $n_s(G) < cnq^{s+s(2n-s)}$.*

(ii) *If G_0 is a symplectic or orthogonal group, then $n_s(G) < cq^{(n+s(2n-s+1))/2}$ and $k_{pr}(G) < cq^n$. Also if $s < (1/2+\delta)n$, then $n_s(G) < cq^{s(2n-s+5)/2}$.*

Proof. (i) Let $k_{s,u}$ (resp. $k_{s,s}$) denote the number of conjugacy classes in $PGL_n^\epsilon(q)$ of unipotent (resp. semisimple) elements h of prime order such that $\nu(h)=s$. Such a unipotent class is determined by a partition of n into $n-s$ parts (each part being the size of a Jordan block). Subtracting 1 from each part gives a partition of s. Letting $P(s)$ denote the number of partitions of s we obtain

$$k_{s,u} \leq P(s) < 2^s.$$

A semisimple element h of prime order r is conjugate to the image (modulo scalars) of a matrix $\mathrm{diag}(A_1,\dots,A_l,I_m)$, where each A_j is an irreducible $i \times i$ block (and $il+m=n$, r divides q^i-1). If $\nu(h)=s$, then the largest eigenspace of h on $\bar{V}$ (of dimension $n-s$) is either the 1-eigenspace of dimension m, or is the eigenspace of an eigenvalue of some A_j. In the first case, $m = n - s$; and in the second, $l \geq n - s$ and $l \leq n/i$. Thus

$$k_{s,s} \leq r^{s/i} + \sum_{n/i \geq l \geq n-s} r^l \leq q^s + (n/i)(q^i)^{n/i} < cnq^n.$$

It now follows from 3.4 that

$$n_s(PGL_n^\epsilon(q)) < c(k_{s,u} + k_{s,s})q^{s(2n-s)} < c'nq^{n+s(2n-s)}.$$

Note that $k_{pr}(PGL_n^\epsilon(q)) \leq \sum_{s \leq n}(k_{s,u} + k_{s,s})$, and from the above this is less than cnq^n. Finally, if $s < n/2$, then in the second case above, $n/i \geq n - s$ implies $i = 1$ and $\hat{x}$ conjugate to the image of $\mathrm{diag}(I_{n-s}, \lambda_1, \ldots, \lambda_s)$, whence $k_{s,s} \leq q^s$. This gives $n_s(PGL_n^\epsilon(q)) < c'nq^{s+s(2n-s)}$. And if $n/2 \leq s < (1/2 + \delta)n$, then either $i = 1$ as before, or $i = 2$, in which case we obtain $k_{s,s} < c((q+1)/2)^{n/2}$ ($n/2$ 2-blocks, at most $q + 1/2$ choices for each A_i up to conjugacy), whence $k_{s,s} < cq^s$ giving the result as before.

(ii) First consider $k_{s,u}$ for $G_0 = PSp_n(q)$. For p odd, by [Wa, p. 34], a unipotent class of elements h of order p with $\nu(h) = s$ is determined by a partition of n into $n - s$ parts, and, for each even part size, a choice of one of two orthogonal forms. Since the number of even part sizes is less than $\sqrt{s}$, it follows that $k_{s,u} < P(s)2^{\sqrt{s}} < 2^{s+\sqrt{s}}$. If $q \geq 5$, then this is less than q^n; and if $q = 3$, then $\nu(h) = s \leq 2n/3$ so $2^{s+\sqrt{s}} < q^n$. Hence $k_{s,u} < cq^n$ for all odd q; the same holds when $p = 2$, by [AS, §8].

Now consider $k_{s,s}$ for $G_0 = PSp_n(q)$. A semisimple element h of prime order r with $\nu(h) = s$ is conjugate to the image of either

$$\mathrm{diag}(I_{n-s}, -I_s) \quad \text{or} \quad \mathrm{diag}(I_m, A_1, A_1^{-T}, \ldots, A_l, A_l^{-T}),$$

where each A_j is an irreducible $i \times i$ block (matrices relative to an obvious basis) and r divides $q^i - 1$. Arguing as above, we obtain $k_{s,s} < cnq^{n/2}$ (and if $s < (1/2 + \delta)n$, $k_{s,s} < cq^s$), giving the result as in (i).

The argument for G_0 orthogonal is similar and left to the reader. ♠

The next lemma is taken from [HLS, Lemma 4.1]. As it appears there without proof (and there is some possibility of confusion over which field things are being taken over), we give a proof here.

Lemma 3.7. *Let V_a, V_b be vector spaces of dimensions a, b over $\mathbb{F}_q$, and let $g = g_1 \otimes g_2 \in GL(V_a) \otimes GL(V_b)$ acting on $V = V_a \otimes V_b$, with g of prime order. Let $s_1 = \nu(g_1)(= \nu_{V_a, \bar{\mathbb{F}}}(g_1))$, and $s_2 = \nu(g_2)$. Then*

$$\nu(g) = \nu_{V, \bar{\mathbb{F}}}(g) \geq \max(as_2, bs_1).$$

Proof. Suppose first that g is semisimple. Let g_1 have eigenvalues $\lambda_1, \ldots, \lambda_t$ with multiplicities $r_1, \ldots, r_t$ respectively, and let g_2 have eigenvalues $\mu_1, \ldots, \mu_u$ with multiplicities $s_1, \ldots, s_u$, where $r_1 \geq r_2 \geq \ldots \geq r_t$ and $s_1 \geq \ldots \geq s_u$. Then $\nu(g_1) = a - r_1, \nu(g_2) = b - s_1$.

Assume without loss that $t \geq u$. Then the maximum dimension of an eigenspace for $g = g_1 \otimes g_2$ is at most $\sum_1^t r_i s_i$. Therefore

$$\nu(g) \geq ab - \sum_1^t r_i s_i \geq ab - r_1 \sum_1^t s_i = ab - r_1 b = b\nu(g_1),$$

and similarly $\nu(g) \geq a\nu(g_2)$.

Now suppose g is unipotent of order p. In the Jordan canonical form, for $1 \le i \le p$ let the Jordan block J_i of size $i \times i$ occur with multiplicity r_i in g_1, and with multiplicity s_i in g_2.

For $i \le j \le p$, one checks that $C_{V_i \otimes V_j}(J_i \otimes J_j)$ has dimension i. Hence

$$\dim C_{V_a \otimes V_b}(g_1 \otimes g_2) \le \sum_{i,j} i r_i s_j,$$

and therefore $\nu(g_1 \otimes g_2) \ge ab - \sum_{i,j} i r_i s_j$. Consequently

$$a\nu(g_2) = a(b - \sum s_j) \le ab - (\sum i r_i)(\sum s_j) = ab - \sum_{i,j} i r_i s_j \le \nu(g_1 \otimes g_2).$$

Similarly $b\nu(g_1) \le \nu(g_1 \otimes g_2)$. ♠

4. Completion of proof of Theorem ($\star$)

Continue with the notation of the previous section. In this section we complete the proof of Theorem ($\star$) by considering the possibilities for the maximal subgroup M of the classical group G. Recall once again, that M either lies in one of the Aschbacher families $\mathcal{C}_i$ ($1 \le i \le 8$), or $M \in \mathcal{S}$; also M is not a subspace subgroup, and $\nu(x) < (\frac{1}{2} + \delta)n$, where δ is a small positive constant.

Lemma 4.1. *If $M \in \mathcal{C}_6 \cup \mathcal{C}_7 \cup \mathcal{S}$, then ($\star$) holds.*

Proof. If $M \in \mathcal{C}_6 \cup \mathcal{C}_7$, then $M \cap PGL(V)$ is primitive and tensor-indecomposable on V (since M is maximal, for instance), and hence by [HLS, Theorem 4(b)], $\nu(x) > \sqrt{n}/12$. By [HLS, Theorem 4(a) and p. 452-3], the same conclusion holds for $M \in \mathcal{S}$, excluding the case where $M = A_{n+d}$ or S_{n+d} ($d \le 2$) and V is a constituent of the permutation module. Hence, excluding this case, by 3.4 we have

$$|x^G| > q^{cn^{3/2}}.$$

However, for $M \in \mathcal{C}_6$, $|M| < cr^{2a}|Sp_{2a}(r)|$ for some prime r, where $n = r^a$; hence $|M| < cr^{2a^2+3a} < cn^{d \log n}$. For $M \in \mathcal{C}_7$, $|M| < |GL_a(q)|^b |S_b|$ with $n = a^b$, so $|M| < cq^{a^2 b} b! < c' q^{2n}$. And for $M \in \mathcal{S}$ (excluding the above exception with $M' = A_{n+d}$), we have $|M| < q^{3n}$ by [Li1]. Thus in all these cases, we have $|x^G \cap M| < |M| < |x^G|^\delta$, giving ($\star$).

Finally, suppose $M' = A_{n+d}$ with $d \le 2$, as in the case excluded above. In this case the proof of [LP, Lemma 8] supplies lower bounds for $|x^G|$ and upper bounds for $|x^G \cap M|$, from which the result follows easily. ♠

Lemma 4.2. *If $M \in \mathcal{C}_3$, then ($\star$) holds.*

Proof. Suppose $M \in \mathcal{C}_3$. Then either

(1) $M \cap PGL(V)$ lies in the image modulo scalars of a group $Cl_{n/k}(q^k).k$, where k is prime (and G is of the same type $Cl_n(q)$), or

(2) $M \cap PGL(V)$ lies in the image of $GU_{n/2}(q)$ and G is symplectic or orthogonal.

Consider case (1). Let $B = Cl_{n/k}(q^k)$. For $y \in B$, let

$$\nu_0(y) = \min\{\dim[\bar{V}_{n/k}, \lambda y] : \lambda \in \bar{\mathbb{F}}^*\}$$

and let $\nu(y)$ be defined as above (relative to $V = V_n$).

We claim that for $y \in B$ of prime order,

$$\nu(y) \ge k\nu_0(y).$$

If y is unipotent, this is clear, since $\nu(y) = n - \dim C_{V_n}(y) = k(\frac{n}{k} - \dim C_{V_{n/k}}(y)) = k\nu_0(y)$.

Now suppose y is semisimple. An element of $GL_{n/k}(q^k)$ conjugate to

$$\mathrm{diag}(\lambda_1, \dots, \lambda_{n/k}) \in GL_{n/k}(\bar{\mathbb{F}}) \qquad (\lambda_i \in \bar{\mathbb{F}}^*)$$

becomes conjugate to

$$\mathrm{diag}(\lambda_1, \lambda_1^q, \dots, \lambda_1^{q^{k-1}}, \dots, \lambda_{n/k}^{q^{k-1}}) \in GL_n(\bar{\mathbb{F}}).$$

For an eigenvalue $\lambda \in \bar{\mathbb{F}}$ of y, let V_λ be the corresponding eigenspace in $V_{n/k}$, and define

$$a = \max\{\dim V_\lambda : \lambda = \lambda^q\}, \quad b = \max\{\dim V_\mu : \mu \neq \mu^q\}.$$

Then $\nu_0(y) = \min(\frac{n}{k} - a, \frac{n}{k} - b)$. The maximum multiplicity of an eigenvalue of y on V_n is at most $\max(ak, bk)$. If $b \geq a$, then $\nu(y) \geq n - bk$ and $\nu_0(y) \leq \frac{n}{k} - b \leq \nu(y)/k$, as required. And if $b < a$, then $\nu(y) \geq n - ak$ and $\nu_0(y) \leq \frac{n}{k} - a \leq \nu_0(y)/k$. This establishes the claim.

Next, for $y \in M - B$ of prime order k, y is B-conjugate to a field automorphism of B of order k (see [GL, 7.2]). Such an element acts as a permutation with n/k k-cycles on a suitable basis of V_n, and hence $\nu(y) = n(k-1)/k$; as $\nu(x) < (\frac{1}{2}+\delta)n$, this case arises only when $k = 2$, in which case $|y^G \cap (M - B)| < c|Cl_{n/2}(q^2) : Cl_{n/2}(q)|$.

Now let $\nu(x) = s$, and assume that $(k, s) \neq (2, n/2)$. Define an integer d to be 1 if $G_0 = L_n^\epsilon(q)$, and to be 2 otherwise. Then by the above and 3.6,

$$|x^G \cap M| < n_s(B) < c \sum_{r \leq s/k} (q^k)^{r((2n/k) - r + 5)/d} \leq c\frac{s}{k}.q^{s(2n-s+5k)/kd}.$$

Therefore using 3.4, we have

$$f(x, M) \leq \frac{\log n + (s/2k)(2n - s + 5k)}{s(n - s)} = \frac{2n - s + 5k}{2k(n - s)} + o(1).$$

Denote the right hand side of the above equality by $g(k, s)$. We claim that $g(k, s) \leq 3/4 + o(1)$. Indeed, for fixed k, the function $g(k, s)$ is increasing when $s \in [0, (1/2+\delta)n]$, so its maximum is attained at the end point $s = (1/2+\delta)n$. Therefore

$$g(k, s) \leq \frac{(3/2 - \delta)n + 5k}{2k(1/2 - \delta)n}.$$

The expression on the right is maximal when $k = 2$, and so

$$g(k, s) \leq \frac{(3/2 - \delta)n + 10}{4(1/2 - \delta)n} = 3/4 + \delta',$$

as required.

Finally, assume $(k, s) = (2, n/2)$. Then

$$\begin{aligned} |x^G \cap M| &= |x^G \cap B| + |x^G \cap (M - B)| \\ &< n_s(B) + c'|Cl_{n/2}(q^2) : Cl_{n/2}(q)| < 2n_s(B), \end{aligned}$$

and the conclusion follows as before.

Now consider case (2). The argument here is similar. Let $B = GU_{n/2}(q)$. As above, if $b \in B$, we have $\nu_{V_{n/2}}(b) \leq s/2$. By [LiSh2, 4.4], $M - B$ has at most 3 B-classes of involutions y, and $|C_B(y)| > c|B : O_{n/2}(q)|$ for each of these; moreover,

$\nu(y) = n/2$ (as each such involution interchanges a pair of maximal totally singular subspaces of $V \otimes \bar{\mathbb{F}}$). Thus if $s \neq n/2$, then by 3.6,

$$|x^G \cap M| = |x^G \cap B| \leq n_s(B) < c \sum_{r \leq s/2} q^{r(n-r+1)} < c(s/2)q^{(s/2)(n-(s/2)+1)},$$

and by 3.4,

$$|x^G| > cq^{s(n-s)},$$

whence $f(x, M) < ((2n - s + 2) + \log n)/(4(n - s)) < 3/4 + o(1)$ as above. And if $s = n/2$, then $|x^G \cap M| < n_s(B) + c|B : O_{n/2}(q)| < 2n_s(B)$, giving the result as above again. ♠

Lemma 4.3. *If $M \in \mathcal{C}_4$, then $(\star)$ holds.*

Proof. Suppose $M \in \mathcal{C}_4$, so $M \cap PGL(V) < Cl_{n_1}(q) \otimes Cl_{n_2}(q) = Cl(V_1) \otimes Cl(V_2)$, where $V = V_1 \otimes V_2$, $n = n_1 n_2$ and $n_i \geq 2$. (The precise possibilities are listed in [KL, §4.3].) Write $s = \nu(x)$.

Let $x = g_1 \otimes g_2 \in M$, and write $s_i = \nu(g_i)$. Then by 3.7, $s = \nu(x) \geq \max(n_1 s_2, n_2 s_1)$. As $s < (\frac{1}{2} + \delta)n$, we have $s_1 < (\frac{1}{2} + \delta)n_1, s_2 < (\frac{1}{2} + \delta)n_2$.

By 3.6,

$$|x^G \cap M| < \max_{s_1 \leq s/b, s_2 \leq s/a} q^{(s_1/d)(2n_1 - s_1 + 5) + (s_2/d)(2n_2 - s_2 + 5)},$$

where $d = 1$ if $G_0 = L_n^\epsilon(q)$ and $d = 2$ otherwise. The maximum above is attained when $s_1 = s/n_2, s_2 = s/n_1$. Therefore, using 3.4, we have

$$f(x, M) \leq \frac{(s/n_2)(2n_1 - (s/n_2) + 5) + (s/n_1)(2n_2 - (s/n_1) + 5)}{2s(n - s)}.$$

Write $a = n_1, b = n_2$, and denote the expression on the right by $g(a, b, s)$. We claim that $g(a, b, s) \leq 3/8 + o(1)$. To show this write $s = \alpha n$, and note that

$$g(a, b, s) = \frac{\alpha a(2a - \alpha a + 5) + \alpha b(2b - \alpha b + 5)}{2\alpha n(n - \alpha n)}$$

$$= \frac{5\alpha(a + b)n^{-2} + \alpha(2 - \alpha)(a^2 + b^2)n^{-2}}{2\alpha(1 - \alpha)}.$$

This yields

$$g(a, b, s) = \frac{5(a + b)n^{-2} + (2 - \alpha)(a^2 + b^2)n^{-2}}{2(1 - \alpha)}.$$

Note that $(a + b)n^{-2} = o(1)$, and that $(a^2 + b^2)n^{-2} \leq 1/4 + o(1)$. Therefore

$$g(a, b, s) \leq \frac{(2 - \alpha)(1/4 + o(1))}{2(1 - \alpha)}.$$

For α in the interval $(0, 1/2 + \delta]$, the expression on the right attains its maximum when $\alpha = 1/2 + \delta$, giving $g(a, b, s) \leq 3/8 + \delta'$, as claimed. ♠

Lemma 4.4. *If $M \in \mathcal{C}_5$, then $(\star)$ holds.*

Proof. Suppose $M \in \mathcal{C}_5$, so either

(1) $M \cap PGL(V) \leq Cl_n(q_0)$, where $q = q_0^k$ for some prime k, or
(2) $G_0 = U_n(q)$ and $M \cap PGL(V) \leq PGSp_n(q)$ or $PGO_n(q)$.

Consider case (1). Let $s = \nu(x)$. Then by 3.4, writing $d = 1$ if $G_0 = L_n^\epsilon(q)$, $d = 2$ otherwise,

$$|x^M| \leq cq_0^{(s/d)(2n-s+1)}.$$

Hence using 3.6, we have

$$|x^G \cap M| < k_{pr}(M)|x^M| < cnq_0^{n+(s/d)(2n-s+1)}.$$

Consequently

$$f(x, M) \leq \frac{2n + s(2n - s + 1) + \log n}{2sk(n - s)}.$$

The expression on the right is increasing in $s \in (0, (1/2+\delta)n]$, and so the maximum is attained for $s = (1/2 + \delta)n$. This yields

$$f(x, M) \leq \frac{1}{2k} \frac{3/2 - \delta}{1/2 - \delta + o(1)} \leq 3/4 + \delta'.$$

Now consider case (2). Here, again using 3.4 and 3.6, we have

$$|x^G \cap M| < k_{pr}(M)|x^M| < cq^{n+(s/2)(2n-s+1)},$$

and the result follows as before. ♠

Lemma 4.5. *If $M \in \mathcal{C}_2$, then $(\star)$ holds.*

Proof. In this case, either

(1) $M \cap PGL(V)$ is contained in the image modulo scalars of a subgroup $Cl_m(q)$ *wr* S_k, where $n = km$ and $k \geq 2$, or
(2) $M \cap PGL(V)$ is contained in the image of $GL_{n/2}(q^u)$, and G_0 is unitary, symplectic or orthogonal.

Consider case (1). Write B for the image of the base group $(Cl_m(q))^k$, fixing a decomposition $V = V_1 \oplus \ldots \oplus V_k$ (where $\dim V_i = m$ for all i). Let $s = \nu(x)$. Suppose first that $x^G \cap M \subseteq B$. If $s_i = \nu_{V_i}(x^{V_i})$, then $s_1 + \ldots + s_k \leq s$. Thus by 3.6, with the usual definition of the integer d,

$$|x^G \cap M| \leq n_s(B) < \sum_{s_1+\ldots+s_k \leq s, s_i \leq m} \prod_i (cm)^{s_i} q^{(m+s_i(2m-s_i+1))/d}$$

$$\leq (cm)^s q^{n/d} \prod_i q^{s_i(2m-s_i+1)/d}.$$

The number of terms in the sum with $\sum s_i = t \leq s$ is at most $\binom{k+t-1}{k-1}$, which is less than k^t. Let $0 \leq s_1, \ldots, s_k \leq m$ with $\sum s_i = t \leq s$. Then $\sum s_i^2 \geq k(t/k)^2 = t^2/k$, and so

$$\sum_{i=1}^k s_i(2m - s_i + 1) = (2m + 1)t - \sum s_i^2 \leq (2m + 1)t - t^2/k.$$

Hence

$$n_s(B) < (cm)^s q^{n/d} \sum_{t=1}^s k^t q^{(t/d)(2m-t/k+1)} \leq (cm)^s q^{n/d} sk^s q^{(s/d)(2m-s/k+1)}.$$

It follows by 3.4 that

$$f(x,M) \le \frac{s(2(n/k)-(s/k)+1)+n+2s(\log k+\log m+c')}{2s(n-s)}$$

$$= \frac{2n-s}{2k(n-s)} + \frac{n}{2s(n-s)} + o(1).$$

If $s > 1$, then the expression on the right is maximal when $s = (1/2+\delta)n$ and $k = 2$, giving $f(x,M) < 3/4+\delta'$. And if $s = 1$, then in fact, $n_s(B) < cq^{3m/d}$, giving $f(x,M) < 3m/(2s(n-s)) + o(1) < 3/4 + o(1)$ again.

Now assume that $x^G \cap M \not\subseteq B$. We may take $x \in M - B$; say x is the image of $\hat{x} = (b_1, \ldots, b_k)\pi$, where each $b_i \in Cl_m(q)$ and $1 \ne \pi \in S_k$. Let r be the (prime) order of x, hence of π. For the purpose of estimating $\nu(x)$, we regard $\hat{x}$ as an element of $GL_n(\bar{\mathbb{F}})$, and each b_i as an element of $GL_m(\bar{\mathbb{F}})$. We have $\hat{x}^r = \lambda I$ for some scalar λ. Choose $\mu \in \bar{\mathbb{F}}$ such that $\mu^r = \lambda^{-1}$. Replacing $\hat{x}$ by $\mu\hat{x}$ (hence each b_i by μb_i), we then have $\hat{x}^r = I$.

Let π consist of h r-cycles and f fixed points, so that $k = hr + f$. Say π induces the permutation $\prod_{i=1}^{h}((i-1)r+1 \ldots ir)$ on the coordinates. As $\hat{x}^r = I$, we have

$$b_1 \ldots b_r = b_{r+1} \ldots b_{2r} = \ldots = b_{(h-1)r+1} \ldots b_{hr} = 1.$$

Define

$$\begin{aligned} g = \ & (1, b_1, b_1b_2, b_1b_2b_3, \ldots, b_1 \ldots b_{r-1}, \ldots, \\ & 1, b_{(h-1)r+1}, b_{(h-1)r+1}b_{(h-1)r+2}, \ldots, b_{(h-1)r+1} \ldots b_{hr-1}, 1, \ldots, 1). \end{aligned}$$

Then $g^{-1}\pi g = (b_1, b_2, \ldots, b_{hr}, 1, \ldots, 1)\pi$. Hence, if $b = (1, \ldots, 1, b_{hr+1}, \ldots, b_k)$, then

$$g^{-1} b\pi g = (b_1, \ldots, b_k)\pi = x.$$

Thus x is conjugate (in $GL_n(\bar{\mathbb{F}})$) to $b\pi$.

Suppose $r \ne p$, and let $\omega \in \bar{\mathbb{F}}_p$ be an r^{th} root of unity. Let $W = \sum_1^{hr} V_i$. Then there is a scalar λ such that in its action on W, $\lambda\pi$ has each of the eigenvalues ω^i $(0 \le i \le r-1)$ with multiplicity mh. Therefore

$$\nu(x) = \nu(b\pi) \ge mh(r-1).$$

Similarly, if $r = p$, then $C_W(\pi)$ has dimension mh, and the same conclusion follows.

Since $\nu(x) \le (\frac{1}{2}+\delta)n = (\frac{1}{2}+\delta)m(hr+f)$, it follows that $h(r-1) < (1+\delta')(h+f)$, where $1+\delta' = (1+2\delta)/(1-2\delta)$. By 3.4, we have

$$|x^G| > cq^{2mh(r-1)(n-mh(r-1))(1-\delta'')/d} = cq^{2m^2h(r-1)(h+f)(1-\delta'')/d}$$

(δ'' a small positive constant, usual definition of d). Obviously,

$$|x^G \cap M| < |M| \le |Cl_m(q)|^k k! < cq^{kc(m)}k!,$$

where $c(m) = m^2$ if $G_0 = L_n^\epsilon(q)$, $c(m) = (m^2+m)/2$ if $G_0 = PSp_n(q)$, and $c(m) = (m^2-m)/2$ if $G_0 = P\Omega_n(q)$. Hence

$$(\dagger) \qquad f(x,M) \le \frac{dkc(m) + dk\log k}{2m^2h(r-1)(h+f)(1-\delta'')}.$$

Now $k = h(r-1)+h+f$, so

$$\frac{k}{h(r-1)(h+f)} = \frac{1}{h(r-1)} + \frac{1}{h+f} \le \frac{2}{h(r-1)}.$$

Consequently

$$(1-\delta'')f(x,M) \le \frac{dc(m)}{m^2h(r-1)} + \frac{d\log k}{m^2h(r-1)} \le \frac{3}{2h(r-1)} + \frac{2\log k}{m^2h(r-1)}.$$

This yields ($\star$) (with $\epsilon = 1/8$ or so), unless one of the following holds:

(a) $h = 1, r = 2$;
(b) $m^2h(r-1) < 16\log k$.

Consider case (a). Here $k = f+2$ and $h+f = k-1$. Going back to (†) above, we find that

$$(1-\delta'')f(x,M) \le \frac{dk(c(m)+\log k)}{2m^2(k-1)} \le \frac{k}{k-1}\left(\frac{m^2+m+2\log k}{2m^2}\right).$$

This yields the conclusion (with $\epsilon = 1/8$ or so) unless either (b) above holds, or $k = 2$.

For $k = 2$ we argue as follows. Since $x \in M - B$ and x has prime order, x must be an involution. Hence $|x^G \cap M| \le i_2(M)$. It is easy to see (by direct computation or using the proof of [LiSh2, 5.4]) that $i_2(M) \le |M|^{1/2+o(1)} = q^{(1+o(1))m^2/d}$. Our above-mentioned lower bound on $|x^G|$ (with $k = r = 2, h = 1, f = 0$) yields

$$|x^G| > c'q^{2m^2(1-\delta'')/d}.$$

Hence

$$|x^G \cap M| \le |i_2(M)| \le q^{(1+o(1))m^2/d} \le |x^G|^{1/2+\delta'''}$$

where as usual, δ''' is small.

Now consider case (b). Here in particular, $m^2 < 16\log k$ and $h(r-1) < 16\log k$. The first inequality yields $n^2 = k^2m^2 < 16k^2\log k$, and so k is as large as we want (since n is). Since $h(r-1) = (k-f)(r-1)/r$, the second inequality yields $k - f < 16r\log k/(r-1) < 32\log k$, whence $f > k - 32\log k$.

We may suppose that for all $y \in x^G \cap M$, we have $y = b\phi$ with $b \in B$ and $\phi \in S_k$ having more than $k - 32\log k$ fixed points, since otherwise the above argument gives the conclusion. In other words,

$$x^G \cap M \subseteq \{B\phi : \phi \in S_k, |\operatorname{supp}(\phi)| \le 32\log k\}.$$

Now $|B| < q^{m^2k} < q^{16k\log k}$, and

$$|\{\phi \in S_k : |\operatorname{supp}(\phi)| \le 32\log k\}| \le \binom{32\log k}{k}.(32\log k)! < n^{c'\log n} < |B|^{o(1)}.$$

Hence $|x^G \cap M| < |B|^{1+o(1)}$.

For the purpose of proving ($\star$) we may therefore assume that $|x^G| < |B|^2$. Then $|x^G| < q^{32k\log k}$, whence by 3.4 we have $\nu(x) < 32\log k$.

Now fix $\phi \in S_k$ with $|\operatorname{supp}(\phi)| \le 32\log k$. We next obtain an upper bound for the number of elements h of $B\phi$ such that $\nu(h) < 32\log k$; this will then be an upper bound for $|x^G \cap B\phi|$. Let $h = (b_1, \dots, b_k)\phi$ with $\dim C_V(h) > n - 32\log k$, and say ϕ moves the points $1, \dots, t$ and fixes the rest, where $t \le 32\log k$. The number of possibilities for $b_1, \dots, b_f$ is at most $(q^{m^2})^{32\log k}$, which is less than $q^{512\log^2 k}$. Of the remaining b_i, at most $32\log k$ of them are not equal to I_m; hence the number of possibilities for $b_{t+1}, \dots, b_k$ is at most $k^{32\log k}.(q^{m^2})^{32\log k}$. We conclude that

$$|x^G \cap B\phi| < q^{512\log^2 k}.k^{32\log k}.(q^{m^2})^{32\log k} < q^{512\log^2 k}.k^{32\log k}.q^{512\log^2 k}.$$

Since the number of possibilities for ϕ is at most $k^{32\log k}(32\log k)!$, and k is large, it follows that

$$|x^G \cap M| < (q^k)^{o(1)} \leq (q^n)^{o(1)} \leq |x^G|^{o(1)},$$

giving the result.

Finally, case (2) is handled in exactly the same way as case (2) in the proof of 4.2. ♠

Lemma 4.6. *If $M \in \mathcal{C}_8$, then $(\star)$ holds.*

Proof. Recall we are excluding $M = O_n(q) < Sp_n(q)$ with q even (as this is a subspace subgroup). Thus when $M \in \mathcal{C}_8$, we have $G_0 = L_n(q)$ and M of type $PSp_n(q)$, $O_n(q)$ or $U_n(q^{1/2})$. Let $s = \nu(x)$. Then by 3.6,

$$|x^G \cap M| \leq n_s(M) < cq^{(s/2)(2n-s+5)},$$

so by 3.4,

$$f(x, M) < \frac{(s/2)(2n-s+5)}{2s(n-s)},$$

which (for $0 \leq s < (1/2+\delta)n$) is bounded above by $3/4 + \delta'$. ♠

Notice that Theorem $(\star)$ is now proved.

References

[As] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469-514. MR **86a:**20054

[AS] M. Aschbacher and G.M. Seitz, Involutions in Chevalley groups over finite fields of even order, *Nagoya Math. J.* **63** (1976), 1-91. MR **54:**10391

[Ba] L. Babai, On the order of uniprimitive permutation groups, *Annals of Math.* **113** (1981), 553-568. MR **83j:**20010

[Ca1] P.J. Cameron, Some open problems on permutation groups, in *Groups, Combinatorics and Geometry* (eds: M.W. Liebeck and J. Saxl), London Math. Soc. Lecture Note Series **165**, Cambridge University Press, Cambridge, 1992, 340-350. MR **94c:**20005

[Ca2] P.J. Cameron, Permutation groups, in *Handbook of Combinatorics* (eds: R.L. Graham et al.), Elsevier Science B.V., Amsterdam, 1995, 611-645. MR **97e:**20002

[CK] P.J. Cameron and W.M. Kantor, Random permutations: some group-theoretic aspects, *Combinatorics, Probability and Computing* **2** (1993), 257-262. MR **95b:**20006

[CIK] C.W. Curtis, N. Iwahori and R. Kilmoyer, Hecke algebras and characters of parabolic type of finite groups with BN-pairs, *IHES Publ. Math.* **40** (1972), 81-116. MR **50:**494

[Di] J.D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199-205. MR **40:**4985

[GSSh] D. Gluck, Á. Seress and A. Shalev, Bases for primitive permutation groups and a conjecture of Babai, *J. Algebra* **199** (1998), 367-378. CMP 98:06

[GL] D. Gorenstein and R. Lyons, The local structure of finite groups of characteristic 2 type, *Memoirs Amer. Math. Soc.* **42**, No. 276 (1983). MR **84g:**20025

[Gu] R.M. Guralnick, The genus of a permutation group, in *Groups, Combinatorics and Geometry* (eds: M.W. Liebeck and J. Saxl), London Math. Soc. Lecture Note Series **165** (1992), 351-363. MR **94a:**20006

[GK] R.M. Guralnick and W.M. Kantor, Probabilistic generation of finite simple groups, *J. Algebra*, to appear.

[GKS] R.M. Guralnick, W.M. Kantor and J. Saxl, The probability of generating a classical group, *Comm. in Algebra* **22** (1994), 1395-1402. MR **95a:**20030

[GLSS] R.M. Guralnick, M.W. Liebeck, J. Saxl and A. Shalev, Random generation of finite simple groups, to appear.

[GM] R.M. Guralnick and K. Magaard, On the minimal degree of a primitive permutation group, *J. Algebra* **207** (1998), 127-145. CMP 98:17

[GT] R.M. Guralnick and J.G. Thompson, Finite groups of genus zero, *J. Alg.* **131** (1990), 303-341. MR **91e:**20006

[HLS] J. Hall, M.W. Liebeck and G.M. Seitz, Generators for finite simple groups, with applications to linear groups, *Quart. J. Math.* **43** (1992), 441-458. MR **93k:**20030

[KL] W.M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Ded.* **36** (1990), 67-87. MR **91j:**20041

[KLi] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series **129**, Cambridge University Press, 1990. MR **91g:**20001

[Li1] M.W. Liebeck, On the orders of maximal subgroups of the finite classical groups, *Proc. London Math. Soc.* **50** (1985), 426-446. MR **87a:**20046

[Li2] M.W. Liebeck, On minimal degrees and base sizes of primitive permutation groups, *Arch. Math.* **43** (1984), 11-15. MR **86d:**20004

[LP] M.W. Liebeck and C.W. Purvis, On the genus of a finite classical group, *Bull. London Math. Soc.* **29** (1997), 159-164. MR **98h:**20086

[LPy] M.W. Liebeck and L. Pyber, Upper bounds for the number of conjugacy classes of a finite group, *J. Algebra* **198** (1997), 538-562. CMP 98:06

[LS] M.W. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, *Proc. London Math. Soc.* (3) **63** (1991), 266-314. MR **92f:**20003

[LiSh1] M.W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Ded.* **56** (1995), 103-113. MR **96h:**20116

[LiSh2] M.W. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the (2,3)-generation problem, *Annals of Math.* **144** (1996), 77-125. MR **97e:**20106a

[LPS] M.W. Liebeck, C.E. Praeger and J. Saxl, On the 2-closures of primitive permutation groups, *J. London Math. Soc.* **37** (1988), 241-252. MR **89b:**20009

[Ma] W. Magnus, *Non-Euclidean Tesselations and Their Groups*, Academic Press, New York – London, 1974. MR **50:**4774

[Sh1] A. Shalev, A theorem on random matrices and some applications, *J. Algebra* **199** (1998), 124-141. CMP 98:06

[Sh2] A. Shalev, Random generation of simple groups by two conjugate elements, *Bull. London Math. Soc.* **29** (1997), 571-576. MR **98h:**20122

[Shi] T. Shih, *Bounds of Fixed Point Ratios of Permutation Representations of $GL_n(q)$ and Groups of Genus Zero*, Ph.D. Thesis, California Institute of Technology, Pasadena, 1990.

[Wa] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Austral. Math. Soc.* 3 (1965), 1-62. MR **27:**212

Department of Mathematics, Imperial College, London SW7 2BZ, England
E-mail address: `m.liebeck@ic.ac.uk`

Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel
E-mail address: `shalev@math.huji.il`