Algebra & Number Theory

Volume 12
2018
No. 6

Bases for quasisimple linear groups

Melissa Lee and Martin W. Liebeck

msp

ALGEBRA AND NUMBER THEORY 12:6 (2018)
dx.doi.org/10.2140/ant.2018.12.1537

Bases for quasisimple linear groups

Melissa Lee and Martin W. Liebeck

Let V be a vector space of dimension d over $\mathbb{F}_q$, a finite field of q elements, and let $G \le \mathrm{GL}(V) \cong \mathrm{GL}_d(q)$ be a linear group. A *base* for G is a set of vectors whose pointwise stabilizer in G is trivial. We prove that if G is a quasisimple group (i.e., G is perfect and $G/Z(G)$ is simple) acting irreducibly on V, then excluding two natural families, G has a base of size at most 6. The two families consist of alternating groups Alt_m acting on the natural module of dimension $d = m-1$ or $m-2$, and classical groups with natural module of dimension d over subfields of $\mathbb{F}_q$.

1. Introduction

Let G be a permutation group on a finite set Ω of size n. A subset of Ω is said to be a *base* for G if its pointwise stabilizer in G is trivial. The minimal size of a base for G is denoted by $b(G)$ (or sometimes $b(G, \Omega)$ if we wish to emphasize the action). It is easy to see that $|G| \le n^{b(G)}$, so that $b(G) \ge \log|G|/\log n$. A well known conjecture of Pyber [1993] asserts that there is an absolute constant c such that if G is primitive on Ω, then $b(G) < c\log|G|/\log n$. Following substantial contributions by a number of authors, the conjecture was finally established in [Duyan et al. 2018] in the following form: there is an absolute constant C such that for every primitive permutation group G of degree n,

$$b(G) < 45\frac{\log|G|}{\log n} + C. \tag{1}$$

To obtain a more explicit, usable bound, one would like to reduce the multiplicative constant 45 in the above, and also estimate the constant C.

Most of the work in [Duyan et al. 2018] was concerned with affine groups contained in $\mathrm{AGL}(V)$, acting on the set of vectors in a finite vector space V (since the conjecture had already been established for nonaffine groups elsewhere). For these, one needs to bound the base size for a linear group $G \le \mathrm{GL}(V)$ that acts irreducibly on V. One source for the undetermined constant C in the bound (1) comes from a key result in this analysis, namely Proposition 2.2 of [Liebeck and Shalev 2002], in which quasisimple linear groups are handled. This result says that there is a constant C_0 such that if G is a quasisimple group acting irreducibly on a finite vector space V, then either $b(G) \le C_0$, or G is a classical or alternating

This paper represents part of the PhD work of Lee under the supervision of Liebeck. Lee acknowledges the support of an EPSRC International Doctoral Scholarship at Imperial College London. We are grateful to the referee for several helpful comments and suggestions.
MSC2010: primary 20C33; secondary 20B15, 20D06.
Keywords: linear groups, simple groups, representations, primitive permutation groups, bases of permutation groups.

group and V is the natural module for G; here by the natural module for an alternating group Alt_m over $\mathbb{F}_{p^e}$ (p prime) we mean the irreducible "deleted permutation module" of dimension $m-\delta(p,m)$, where $\delta(p,m)$ is 2 if $p \mid m$ and is 1 otherwise. This result played a major role in the proof of Pyber's conjecture for primitive linear groups in [Liebeck and Shalev 2002; 2014], which was heavily used in the final completion of the conjecture in [Duyan et al. 2018].

The main result in this paper shows that the constant C_0 just mentioned can be taken to be 6. Recall that for a finite group G, we denote by $E(G)$ the subgroup generated by all quasisimple subnormal subgroups of G. Also write $V_d(q)$ to denote a d-dimensional vector space over $\mathbb{F}_q$.

Theorem 1. *Let $V = V_d(q)$ ($q = p^e$, p prime) and $G \leq \mathrm{GL}(V)$, and suppose that $E(G)$ is quasisimple and absolutely irreducible on V. Then one of the following holds*:

(i) $E(G) = \mathrm{Alt}_m$ *and V is the natural* Alt_m*-module over $\mathbb{F}_q$ of dimension $d = m - \delta(p,m)$.*

(ii) $E(G) = \mathrm{Cl}_d(q_0)$, *a classical group with natural module of dimension d over a subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$.*

(iii) $b(G) \leq 6$.

This result has been used in [Halasi et al. 2018] to improve the bound (1), replacing the multiplicative constant 45 by 2, and the constant C by 24.

With substantially more effort, it should be possible to reduce the constant 6 in part (iii) of theorem, and work on this by the first author is in progress.

The paper is organized as follows. In Section 2 we present some preliminary results needed for the proof of Theorem 1. Section 3 contains the proof of Theorem 3.1, a result that bounds the base size for various actions of classical groups on orbits of nondegenerate subspaces. The proof of Theorem 1 follows in Section 4, where crucial use of Theorem 3.1 is made in Lemmas 4.7 and 4.8.

2. Preliminary lemmas

If G is a finite classical group with natural module V, we define a *subspace action* of G to be an action on an orbit of subspaces of V, or, in the case where $G = \mathrm{Sp}_{2m}(q)$ with q even, the action on the cosets of a subgroup $O^{\pm}_{2m}(q)$.

Lemma 2.1. *Let G be an almost simple group with socle G_0 and suppose G acts transitively on a set Ω.*

(i) *If G_0 is exceptional of Lie type, or sporadic, then $b(G) \leq 7$, with equality only if $G = M_{24}$.*

(ii) *If G_0 is classical, and the action of G on Ω is primitive and not a subspace action, then $b(G) \leq 5$, with equality if and only if $G = U_6(2).2$, $\Omega = (G : U_4(3).2^2)$.*

Proof. Part (i) follows from [Burness et al. 2009, Corollary 1] and [Burness et al. 2010, Corollary 1]. Part (ii) is [Burness 2007c, Theorem 1.1]. □

For a simple group G_0, and $1 \neq x \in \mathrm{Aut}(G_0)$, define $\alpha(x)$ to be the minimal number of G_0-conjugates of x required to generate the group $\langle G_0, x\rangle$, and define

$$\alpha(G_0) = \max\{\alpha(x) \mid 1 \neq x \in \mathrm{Aut}(G_0)\}.$$

Lemma 2.2. *Let $G_0 = \mathrm{Cl}_n(q)$, a simple classical group over $\mathbb{F}_q$ with natural module of dimension n. Then one of the following holds*:

(i) $\alpha(G_0) \le n$.

(ii) $G_0 = \mathrm{PSp}_n(q)$ *(q even) and* $\alpha(G_0) \le n+1$.

(iii) $G_0 = L_2(q)$ *and* $\alpha(G_0) \le 4$.

(iv) $G_0 = L_3(q)$ *and* $\alpha(G_0) \le 4$.

(v) $G_0 = L_4^\epsilon(q)$ *and* $\alpha(G_0) \le 6$.

(vi) $G_0 = \mathrm{PSp}_4(q)$ *and* $\alpha(G_0) \le 5$.

(vii) $G_0 = L_2(9), U_3(3)$ *or* $L_4^\epsilon(2)$.

Proof. This is [Guralnick and Saxl 2003, 3.1 and 4.1]. □

To state the next result, let $\overline{G}$ be a simple algebraic group over an algebraically closed field K of characteristic p, and let $V = V(\lambda)$ be an irreducible $K\overline{G}$-module of p-restricted highest weight λ. Let Φ be the root system of $\overline{G}$, with simple roots $\alpha_1, \dots, \alpha_l$, and let $\lambda_1, \dots, \lambda_l$ be the corresponding fundamental dominant weights. Denote by Φ_S and Φ_L the set of short and long roots in Φ, respectively, and if all roots have the same length, just write $\Phi_S = \Phi$ and $\Phi_L = \varnothing$. Let $W = W(\Phi)$ be the Weyl group, and for $\alpha \in \Phi$, let $U_\alpha = \{u_\alpha(t) : t \in K\}$ be a corresponding root subgroup with respect to a fixed maximal torus.

Now let μ be a dominant weight of $V = V(\lambda)$, write $\mu = \sum_{j=1}^{l} c_j \lambda_j$, and let $\Psi = \langle \alpha_i \mid c_i = 0\rangle_{\mathbb{Z}} \cap \Phi$, a subsystem of Φ. Define

$$r_\mu = \frac{|W : W(\Psi)| \cdot |\Phi_S \setminus \Psi_S|}{2|\Phi_S|} \quad \text{and} \quad r'_\mu = \frac{|W : W(\Psi)| \cdot |\Phi_L \setminus \Psi_L|}{2|\Phi_L|}$$

(the latter only if $\Phi_L \neq \varnothing$). Let

$$s_\lambda = \sum_\mu r_\mu \quad \text{and} \quad s'_\lambda = \sum_\mu r'_\mu \ \text{ (if } \Phi_L \neq \varnothing\text{)},$$

where each sum is over the dominant weights μ of $V(\lambda)$.

For $g \in \overline{G} \setminus Z(\overline{G})$ and $\gamma \in K^*$, let $V_\gamma(g) = \{v \in V : vg = \gamma v\}$, and write

$$\operatorname{codim} V_\gamma(g) = \dim V - \dim V_\gamma(g).$$

Lemma 2.3. *Let $V = V(\lambda)$ be as above.*

(i) *If $g \in \overline{G} \setminus Z(\overline{G})$ is semisimple and $\gamma \in K^*$, then* $\operatorname{codim} V_\gamma(g) \ge s_\lambda$.

(ii) *If $\alpha \in \Phi_S$, then* $\operatorname{codim} V_1(u_\alpha(1)) \ge s_\lambda$.

(iii) *If $\Phi_L \neq \varnothing$ and $\beta \in \Phi_L$, then* $\operatorname{codim} V_1(u_\beta(1)) \ge s'_\lambda$.

(iv) *For any nonidentity unipotent element $u \in \overline{G}$, we have* $\operatorname{codim} V_1(u) \ge \min(s_\lambda, s'_\lambda)$.

Proof. Parts (i)–(iii) are [Guralnick and Lawther $\geq$ 2018, Proposition 2.2.1]. For part (iv), note that [Guralnick and Malle 2004, Corollary 3.4] shows that $\dim V_1(u)$ is bounded above by the maximum of $\dim V_1(u_\alpha(1))$ and $\dim V_1(u_\beta(1))$; hence (iv) follows from (ii) and (iii). □

For $\overline{G}$ of type D_5 or D_6 and V a half-spin module for $\overline{G}$, we shall need the following sharper result. Note that the root system $D_n (n \geq 5)$ has two subsystems of type A_1^2 (up to conjugacy in the Weyl group); with the usual labeling of fundamental roots, we denote these by $(A_1^2)^{(1)} = \langle \alpha_1, \alpha_3 \rangle$ and $(A_1^2)^{(2)} = \langle \alpha_{n-1}, \alpha_n \rangle$.

Lemma 2.4. *Let $\overline{G} = D_n$ with $n \in \{5, 6\}$, and let $V = V(\lambda)$ be a half-spin module for $\overline{G}$ with $\lambda = \lambda_n$ or λ_{n-1}. Let $s \in \overline{G} \setminus Z(\overline{G})$ be a semisimple element, and $u \in \overline{G}$ a unipotent element of order p.*

(i) *Suppose $n = 6$. Then* $\operatorname{codim} V_\gamma(s) \geq 12$ *for any $\gamma \in K^*$; and* $\operatorname{codim} V_1(u) \geq 12$ *provided u is not a root element.*

(ii) *Suppose $n = 5$.*

   (a) *If $C_{\overline{G}}(s)' \neq A_4$ then* $\operatorname{codim} V_\gamma(s) \geq 8$ *for any $\gamma \in K^*$ and if $C_{\overline{G}}(s)' = A_4$ then* $\operatorname{codim} V_\gamma(s) \geq 6$.

   (b) *Provided u is not a root element and also does not lie in a subsystem subgroup $(A_1^2)^{(1)}$, we have* $\operatorname{codim} V_1(u) \geq 8$.

Proof. For semisimple elements s, we follow the method of [Guralnick and Lawther $\geq$ 2018, §2.6] (originally in [Kenneally 2010]). Let Ψ be a closed subsystem of the root system Φ of $\overline{G}$, and define an equivalence relation on the set of weights of $V(\lambda)$ by saying that two weights are related if their difference is a sum of roots in Ψ. Call the equivalence classes Ψ-*nets*.

Now define $\Phi_s = \{\alpha \in \Phi \mid \alpha(s) = 1\}$, the root system of $C_{\overline{G}}(s)$. If $\Phi_s \cap \Psi = \varnothing$, then any two weights in a given Ψ-net that differ by a root in Ψ correspond to different eigenspaces for s.

The subsystem Φ_s is contained in a proper subsystem spanned by a subset of the nodes of the extended Dynkin diagram of $\overline{G}$. Suppose $\Phi_s \neq A_{n-1}$. Then it is straightforward to check that there is a subsystem Ψ that is W-conjugate to $(A_1^2)^{(2)}$ such that $\Phi_s \cap \Psi = \varnothing$. For this Ψ there are 2^{n-2} Ψ-nets of size 2, and so it follows from the observation in the previous paragraph that $\operatorname{codim} V_\gamma(s) \geq 2^{n-2}$ for any $\gamma \in K^*$.

Now suppose $\Phi_s = A_{n-1}$. Here there is a subsystem Ψ that is W-conjugate to $(A_1^2)^{(1)}$ such that $\Phi_s \cap \Psi = \varnothing$. For this Ψ there are 2^{n-5}, 2^{n-3} or 2^{n-3} Ψ-nets of size 4, 2 or 1, respectively, and hence $\operatorname{codim} V_\gamma(s) \geq 2^{n-4} + 2^{n-3}$ for any $\gamma \in K^*$. This lower bound is 12 when $n = 6$, and 6 when $n = 5$. This proves (i) and (ii) for semisimple elements.

Now consider unipotent elements $u \in \overline{G}$ of order p. Assume first that p is odd. Recall that the Jordan form of a unipotent element $u \in D_n$ on the natural module determines a partition ϕ of $2n$ having an even number of parts of each even size; moreover, each such partition corresponds to a single conjugacy class, except when all parts of ϕ are even, in which case there are two classes, interchanged by a graph automorphism of D_n (see [Liebeck and Seitz 2012, Chapter 3]). Denote by u_ϕ (and by u_ϕ, u'_ϕ for the exceptional partitions) representatives of the unipotent classes in $\overline{G}$. By [Spaltenstein 1982, §4], if μ and ϕ are partitions and $\mu < \phi$ in the usual dominance order, then u_μ lies in the closure of the class $u_\phi^{\overline{G}}$ (or $u_\phi'^{\overline{G}}$).

Suppose u is not a root element, and also is not in a subsystem subgroup $(A_1^2)^{(1)}$ when $n = 5$. Then it follows from the above that the closure of $u^{\bar{G}}$ contains $u' = u_\mu$ with $\mu = (3, 1^{2n-3})$ or $(2^4, 1^{2n-8})$, the latter only if $n = 6$. Moreover, codim $V_1(u) \geq$ codim $V_1(u')$ (see the proof of [Guralnick and Malle 2004, 3.4]). If $\mu = (3, 1^{2n-3})$, then u' lies in the B_1 factor of a subgroup $B_1 \times B_{n-2}$ of $\bar{G}$, and the restriction of V to this subgroup is given by [Liebeck and Seitz 2012, 11.15(ii)]; it follows that u' acts on V with Jordan form $J_2^{2^{n-2}}$, giving the conclusion in this case. And if $\mu = (2^4, 1^4)$ with $n = 6$, then u' is in $(A_1^2)^{(1)}$, which is contained in a subsystem A_4, and the restriction of the half-spin module V to A_4 can be deduced from [Liebeck and Seitz 2012, 11.15(i)]; the lower bound on codim $V_1(u')$ in (i) follows easily from this.

It remains to consider unipotent involutions with $p = 2$. The conjugacy classes of these in $\bar{G}$ are described in [Aschbacher and Seitz 1976, §7] (alternatively in [Liebeck and Seitz 2012, Chapter 6]). Adopting the notation of [Aschbacher and Seitz 1976], representatives are a_l, c_l (l even, $2 \leq l \leq n$), and also a_6' in D_6 (which is conjugate to a_6 under a graph automorphism). These are regular elements of Levi subsystem subgroups S, as follows:

u	a_2	c_2	a_4	c_4	a_6	a_6'	c_6
S	A_1	$(A_1^2)^{(2)}$	$(A_1^2)^{(1)}$	$A_1(A_1^2)^{(2)}$	$(A_1^3)^{(1)}$	$(A_1^3)^{(2)}$	A_1^4

where $(A_1^3)^{(1)} = \langle \alpha_1, \alpha_3, \alpha_5 \rangle$ and $(A_1^3)^{(2)} = \langle \alpha_1, \alpha_3, \alpha_6 \rangle$. The restrictions $V \downarrow S$ can be worked out using [Liebeck and Seitz 2012, 11.15], from which we calculate $\dim C_V(u)$ for all the representatives:

u	a_2	c_2	a_4	c_4	a_6	a_6'	c_6
$\dim C_V(u), n = 5$	12	8	10	8	–	–	–
$\dim C_V(u), n = 6$	24	16	20	16	20	16	16

The conclusion of the lemma follows. □

3. Bases for some subspace actions

Let $G = \mathrm{Cl}(V)$ be a simple symplectic, unitary or orthogonal group over $\mathbb{F}_q$, with natural module V of dimension n. For $r < n$, denote by $\mathcal{N}_r$ an orbit of G on the set of nondegenerate r-subspaces of V. The main result of this section gives an upper bound for the base size of the action of G on $\mathcal{N}_r$ when r is very close to $\frac{n}{2}$. This will be used in the next section in the proof of Theorem 1 (see Lemmas 4.7 and 4.8).

Theorem 3.1. *Let $G_0 = \mathrm{PSp}_n(q) (n \geq 6)$, $\mathrm{PSU}_n(q) (n \geq 4)$ or $P\Omega_n^\epsilon(q) (n \geq 7, q$ odd$)$, and let G be a group with socle G_0 such that $G \leq \mathrm{PGL}(V)$, where V is the natural module for G_0. Define*

$$r = \begin{cases} \frac{1}{2}(n - (n, 4)) & \text{if } G_0 = \mathrm{PSp}_n(q), \\ \frac{1}{2}(n - (n, 2)) & \text{if } G_0 = \mathrm{PSU}_n(q) \text{ or } P\Omega_n^\epsilon(q). \end{cases}$$

Then $b(G, \mathcal{N}_r) \leq 5$.

Theorem 3.1 will follow quickly from the following result. The deduction is given in Section 3B.

Type of element x	N_x
semisimple of odd prime order	$\frac{1}{2}\dim x^{\bar{G}}+\frac{1}{4}(n-l_0)+m^2$
semisimple involutions	$\left(\frac{1}{2}+\frac{2m}{n}\right)\dim x^{\bar{G}}$
unipotent of odd prime order	$\frac{1}{2}\dim x^{\bar{G}}+\frac{1}{4}\left(n-\sum_{i \text{ odd}} r_i\right)+m^2$
unipotent involutions of types b_l, c_l	$\left(\frac{1}{2}+\frac{2m+1}{n+2}\right)\dim x^{\bar{G}}$
unipotent involutions of type a_l	$\left(\frac{1}{2}+\frac{3m}{2n}\right)\dim x^{\bar{G}}$

Table 3.1. Bounds on $\dim(x^{\bar{G}} \cap \bar{H})$ for elements x of prime order. Here, l_0 is the multiplicity of the eigenvalue 1 in the action of x on V, and r_i is the number of Jordan blocks of size i in the Jordan form of x.

Theorem 3.2. *Let G and r be as in Theorem 3.1, and let H be the stabilizer in G of a nondegenerate r-subspace in $\mathcal{N}_r$. Let $x \in G$ be an element of prime order. Then one of the following holds*:

(i) $\log|x^G \cap H|/\log|x^G| < \frac{1}{2}+\frac{7}{30}$.

(ii) $G_0 = \mathrm{PSp}_8(q)$ *and x is a unipotent element with Jordan form* $(2, 1^6)$.

Our proof is modeled on that of [Burness 2007b, Theorem 1.1], where a similar conclusion is obtained for the action of G on the set of pairs $\{U, U^{\perp}\}$ of nondegenerate $n/2$-spaces.

3A. ***Proof of Theorem 3.2.*** We shall give a proof of the theorem just for the case where G_0 is a symplectic group $\mathrm{PSp}_n(q)$. The proofs for the orthogonal and unitary groups run along entirely similar lines.

We begin with a lemma on the corresponding algebraic groups. Let $K = \bar{\mathbb{F}}_q$ and $\bar{G} = \mathrm{PSp}_n(K)$, and let $V = V_n(K)$ be the underlying symplectic space. As in Theorem 3.2, write $r = \frac{1}{2}(n-(n,4)) = \frac{1}{2}n - m$, where $m = \frac{1}{2}(n,4)$. Let $\bar{H}$ be the stabilizer in $\bar{G}$ of a nondegenerate r-subspace, so that $\bar{H} = (\mathrm{Sp}_{n/2-m}(K) \times \mathrm{Sp}_{n/2+m}(K))/\{\pm I\}$.

Write $p = \mathrm{char}(K)$. When $p = 2$, the classes of involutions in $\bar{G}$ are determined by [Aschbacher and Seitz 1976]: For any odd $l \le n/2$, there is one class with Jordan form of type $(2^l, 1^{n-2l})$, with representative denoted by b_l. For any nonzero even $l \le n/2$ there are two such classes, with representatives denoted by a_l, c_l. These are distinguished by the fact that $(v, va_l) = 0$ for all $v \in V$.

Lemma 3.3. *With the above notation, if x is an element of prime order in $\bar{H}$, then* $\dim(x^{\bar{G}} \cap \bar{H}) \le N_x$, *where N_x is given in Table 3.1.*

Proof. Denote by V_1 and $V_2 = V_1^{\perp}$ the $(n/2-m)$- and $(n/2+m)$-dimensional subspaces of V preserved by $\bar{H}$. First suppose $x \in \bar{H}$ is a semisimple element of odd prime order t. Define ω to be a t-th root of unity and let l_i be the multiplicity of ω^i $(0 \le i \le t-1)$ as an eigenvalue of x in its action on V. Then

$$\dim x^{\bar{G}} = \frac{n^2+n}{2} - \left(\frac{l_0}{2}+\frac{1}{2}\sum_{i=0}^{t-1} l_i^2\right),$$

and furthermore, $x^{\bar{G}} \cap \bar{H}$ is a union of a finite number of $\bar{H}$-classes, from which we see that

$$\begin{aligned}\dim(x^{\bar{G}} \cap \bar{H}) &\le \tfrac{1}{4}(n^2+2n)+m^2-\left(\tfrac{1}{2}l_0+\tfrac{1}{4}\sum_{i=0}^{t-1} l_i^2\right)\\ &= \tfrac{1}{2}\dim x^{\bar{G}}+\tfrac{1}{4}(n-l_0)+m^2\\ &\le \left(\tfrac{1}{2}+\tfrac{1}{n+2}\right)\dim x^{\bar{G}}+m^2.\end{aligned}$$

Now suppose that x is a semisimple involution. Here $C_{\bar{G}}(x)^0$ is the image modulo $\pm I$ of either $\mathrm{GL}_{n/2}(K)$ or $\mathrm{Sp}_l(K) \times \mathrm{Sp}_{n-l}(K)$, for some even $l \le n/2$. In the first case, $\dim x^{\bar{G}} = n^2/4+n/2$ and so

$$\dim(x^{\bar{G}} \cap \bar{H}) = \tfrac{1}{2}\dim x^{\bar{G}}+\tfrac{n}{4}+\tfrac{m^2}{2} = \left(\tfrac{1}{2}+\tfrac{1}{n}\right)\dim x^{\bar{G}}+\tfrac{1}{2}(m^2-1) \le \left(\tfrac{1}{2}+\tfrac{2}{n}\right)\dim x^{\bar{G}}.$$

Now consider the second case, where $C_{\bar{G}}(x)^0 = \mathrm{Sp}_l(K)\times \mathrm{Sp}_{n-l}(K)$. Here x is $\bar{G}$-conjugate to $[-I_l, I_{n-l}]$, and $\dim x^{\bar{G}} = nl-l^2 = l(n-l)$. For $j=1,2$, the restriction of x to V_j is $\mathrm{Sp}(V_j)$-conjugate to $[-I_{l_j}, I_{d_j-l_j}]$ for some even integer $l_j \ge 0$, where $d_j = \dim V_j$. Noting that $l = l_1+l_2$, we then have

$$\dim(x^{\bar{G}} \cap \bar{H}) = l_1\left(\tfrac{n}{2}-m-l_1\right)+l_2\left(\tfrac{n}{2}+m-l_2\right) \le \tfrac{1}{2}\dim x^{\bar{G}}+m(l_2-l_1) \le \left(\tfrac{1}{2}+\tfrac{2m}{n}\right)\dim x^{\bar{G}}.$$

Now suppose that x is a unipotent element of odd prime order p and that x has Jordan form on V corresponding to the partition $(p^{r_p}, \dots, 1^{r_1}) \vdash n$. By [Lawther et al. 2002, 1.10],

$$\dim x^{\bar{G}} = \tfrac{1}{2}(n^2+n)-\tfrac{1}{2}\sum_{i=1}^{p}\left(\sum_{k=i}^{p} r_k\right)^2-\tfrac{1}{2}\sum_{i \text{ odd}} r_i.$$

Hence, using [Burness 2007b, p.698], we have

$$\dim(x^{\bar{G}} \cap \bar{H}) \le \tfrac{1}{2}\dim x^{\bar{G}}+\tfrac{1}{4}\left(n-\sum_{i \text{ odd}} r_i\right)+m^2 \le \left(\tfrac{1}{2}+\tfrac{1}{n+2}\right)\dim x^{\bar{G}}+m^2.$$

Finally, we consider the case where x is a unipotent involution. First suppose that x is $\bar{G}$-conjugate to either b_l or c_l (as described in the preamble to the lemma). Then [Lawther et al. 2002, 1.10] implies that $\dim x^{\bar{G}} = l(n-l+1)$. Let x act on V_i with associated partition $(2^{l_i}, 1^{d_i-2l_i})$ for $i=1,2$, where $d_1 = n/2-m$ and $d_2 = n/2+m$. Then

$$\dim(x^{\bar{G}} \cap \bar{H}) \le \tfrac{1}{2}\dim x^{\bar{G}}+\tfrac{l}{2}+m(l_2-l_1) \le \left(\tfrac{1}{2}+\tfrac{2m+1}{n+2}\right)\dim x^{\bar{G}}.$$

Lastly, if x is $\bar{G}$-conjugate to a_l for some $2 \le l \le n/2$, then by [Lawther et al. 2002, 1.10], $\dim x^{\bar{G}} = l(n-l)$. By the definition of an a-type involution, if $y \in x^{\bar{G}} \cap \bar{H}$ fixes a subspace V_i, then the restriction of y to V_i is conjugate to a_{l_i} for some even integer $l_i \ge 0$. Therefore

$$\dim(x^{\bar{G}} \cap \bar{H}) \le \tfrac{1}{2}\dim x^{\bar{G}}+m(l_2-l_1).$$

Since $l_2 \le \frac{d_2}{2}$ and $l_1 = l-l_2$, we see that $l_2-l_1 \le 3l(n-l)/(2n)$, so

$$\dim(x^{\bar{G}} \cap \bar{H}) \le \left(\tfrac{1}{2}+\tfrac{3m}{2n}\right)\dim x^{\bar{G}}.$$

This completes the proof of the lemma. □

Now we embark on the proof of Theorem 3.2, considering in turn the various types of elements x of prime order in the symplectic group G. We shall frequently use the notation for such elements given in [Burness and Giudici 2016, §3.4]. Our approach in general is to find a function $\kappa(n)$ such that

$$\frac{\log|x^G \cap H|}{\log|x^G|} < \frac{1}{2} + \kappa(n), \tag{2}$$

where $\kappa(n) < \frac{7}{30}$ except possibly for some small values of n; these small values are then handled separately, usually by direct computation.

Lemma 3.4. *The conclusion of Theorem 3.2 holds when x is a semisimple element of odd prime order.*

Proof. Suppose $x \in H$ is a semisimple element of odd prime order r. Let $\mu = (l, a_1, \dots, a_k)$ be the tuple associated to x (as defined in [Burness 2007a, Definition 3.27]), and define i to be the smallest natural number such that $r \mid q^i - 1$. According to [Burness 2007a, 3.30] this means that

$$|C_G(x)| = \begin{cases} |\mathrm{Sp}_l(q)| \prod_{j=1}^{k} |\mathrm{GL}_{a_j}(q^i)| & i \text{ odd}, \\ |\mathrm{Sp}_l(q)| \prod_{j=1}^{k} |\mathrm{GU}_{a_j}(q^{i/2})| & i \text{ even}. \end{cases}$$

Let d be the number of nonzero a_j, and further define e to be equal to 1 or 2 when i is even or odd, respectively. By Lemma 3.3 and adapting the argument given in [Burness 2007b, p.720], we have

$$|x^G \cap H| < \left(\frac{n-l}{di} + 1\right)^{d/e} 2^{d(e-1)} q^{\dim x^{\bar{G}}/2 + (n-l)/4 + m^2}. \tag{3}$$

Furthermore, [Burness 2007a, 3.27] implies that

$$|x^G| \geq \frac{1}{2}\left(\frac{q}{q+1}\right)^{d(2-e)} q^{\dim x^{\bar{G}}}, \tag{4}$$

and [Burness 2007a, 3.33] gives the lower bound

$$\dim x^{\bar{G}} \geq \tfrac{1}{2}\big(n^2 + n - l^2 - l - \tfrac{1}{ei}(n - l - i(d-e))^2 - i(d-e)\big). \tag{5}$$

First suppose $m = 1$ (so that $n \equiv 2 \bmod 4$). Then (3)–(5) imply that the inequality (2) holds with $\kappa(n) = \frac{3}{n} + \frac{1}{n+1}$. Note that $\kappa(n) < \frac{7}{30}$ for $n \geq 18$. For $n = 6, 10, 14$, we must either adjust our value of $\kappa(n)$ or compute $|x^G \cap H|$ and $|x^G|$ explicitly, since here $\frac{3}{n} + \frac{1}{n+1} > \frac{7}{30}$. For $n = 14$, we find that (2) holds with $\kappa(n) = \frac{7}{30}$ for all choices of (l, i, d) except $(l, i, d) = (0, 1, 2)$. In the latter case, $H = (\mathrm{Sp}_8(q) \times \mathrm{Sp}_6(q))/\{\pm I\}$ and $|C_G(x)| = |\mathrm{GL}_{a_1}(q)||\mathrm{GL}_{a_2}(q)|$ with $a_1 + a_2 = 7$. Hence

$$|x^G \cap H| = \sum_{\substack{b_i \leq a_i \\ b_1 + b_2 = 4}} |\mathrm{Sp}_8(q) : \mathrm{GL}_{b_1}(q) \times \mathrm{GL}_{b_2}(q)| + |\mathrm{Sp}_6(q) : \mathrm{GL}_{a_1 - b_1}(q) \times \mathrm{GL}_{a_2 - b_2}(q)|,$$

and explicit computation gives $\log|x^G \cap H| / \log|x^G| < \frac{1}{2} + \frac{7}{30}$. For $n = 10$, (2) holds with $\kappa(n) = \frac{7}{30}$ for all valid choices of (l, i, d) except $(l, i, d) = (0, 1, 2)$ or $(0, 1, 4)$, and again explicit calculations as above give $\log|x^G \cap H|/\log|x^G| < \frac{1}{2} + \frac{7}{30}$. Finally, for $n = 6$, we find that $\log|x^G \cap H|/\log|x^G| < \frac{1}{2} + \frac{7}{30}$ for all choices of x with associated parameters (l, i, d).

Now suppose $m = 2$. Then (3)–(5) imply that (2) holds with $\kappa(n) = \frac{79}{20(n+1)}$ (when $e = 1$), and with $\kappa(n) = \frac{22}{5(n+2)}$ (when $e = 2$). We have $\kappa(n) < \frac{7}{30}$ for $n \geq 20$. For $n < 20$, explicit calculations of $|x^G \cap H|$ as above yield the conclusion. □

Lemma 3.5. *The conclusion of Theorem 3.2 holds when x is a semisimple involution.*

Proof. Suppose that $x \in H$ is a semisimple involution. Denote by s the codimension of the largest eigenspace of x on $V = V_n(K)$. By [Burness 2007a, 3.37], $|C_G(x)|$ is equal to $|\mathrm{Sp}_s(q)||\mathrm{Sp}_{n-s}(q)|$, $|\mathrm{Sp}_{n/2}(q)|^2.2$, $|\mathrm{Sp}_{n/2}(q^2)|.2$ or $|\mathrm{GL}^{\epsilon}_{n/2}(q)|.2$, with $s < \frac{n}{2}$ in the first case, and $s = \frac{n}{2}$ in the latter three cases. Suppose x is as in one of the first two cases. Adapting the analogous argument given in [Burness 2007b, p.720], we deduce that

$$|x^G \cap H| < 4\left(\frac{q^2+1}{q^2-1}\right)q^{s(n-s)/2-m(1-m)} \quad \text{and} \quad |x^G| > \tfrac{1}{2}q^{s(n-s)}$$

(the constant $\frac{1}{2}$ in the second inequality should be replaced by $\frac{1}{4}$ when $s = \frac{n}{2}$). These bounds imply that (2) holds with

$$\kappa(n) = \begin{cases} \frac{2}{n} & \text{if } s < \frac{n}{2}, m = 1, \\ \frac{3}{n+1} & \text{if } s < \frac{n}{2}, m = 2, \\ \frac{3}{2n} & \text{if } s = \frac{n}{2}, n \geq 12. \end{cases}$$

For $n \geq 12$ we have $\kappa(n) < \frac{7}{30}$, giving the conclusion. And for smaller values of n, we obtain the conclusion by explicit calculation of the values of $|x^G \cap H|$ and $|x^G|$.

Next suppose $|C_G(x)| = 2|\mathrm{Sp}_{n/2}(q^2)|$. Then $|x^G| > \frac{1}{4}q^{n^2/4}$ by [Burness 2007a, 3.37]. If $\frac{n}{4}$ is even then $x^G \cap H = \varnothing$, so assume $\frac{n}{4}$ is odd. An argument analogous to that at the top of p.722 of [Burness 2007b] for this case gives $|x^G \cap H| < \frac{1}{4}q^{(n^2/8)+2}$. These bounds imply that (2) holds with $\kappa(n) = \frac{2}{n}$, and this is less than $\frac{7}{30}$ for all $n \geq 12$.

Finally, suppose that $|C_G(x)| = 2|\mathrm{GL}^{\epsilon}_{n/2}(q)|$. Again [Burness 2007a, 3.37] and arguments of [Burness 2007b, p.722] give

$$|x^G| > \tfrac{1}{4}\left(\tfrac{q}{q+1}\right)q^{n(n+2)/4} \quad \text{and} \quad |x^G \cap H| < \tfrac{1}{4}q^{n^2/8+n/2+m^2/2}.$$

Hence (2) holds with $\kappa(n) = \frac{5}{2n}$, which is less than $\frac{7}{30}$ for $n > 10$, and for $n \leq 10$ we obtain the conclusion as usual by explicit calculation of $|x^G \cap H|$ and $|x^G|$. □

Lemma 3.6. *The conclusion of Theorem 3.2 holds when x is a unipotent element of odd prime order.*

Proof. Let $x \in H$ be a unipotent element of order p, and suppose p is odd. Let the Jordan form of x on V correspond to the partition $\lambda \vdash n$. By Lemma 3.3,

$$\dim x^{\bar{H}} \leq \tfrac{1}{2}\dim x^{\bar{G}} + \tfrac{1}{4}(n-e) + m^2, \tag{6}$$

where e is the number of odd parts in λ.

Case $\lambda = (k^{n/k})$: Since k must divide both $\frac{n}{2} - m$ and $\frac{n}{2} + m$, we have $k = 2$ or 4 (the latter only if $m = 2$). Arguing as at the bottom of p.722 of [Burness 2007b], we have $\dim x^{\bar{G}} \geq \frac{1}{4}n(n+2)$, and also

$$|x^G| > \frac{q}{q+1} q^{\dim x^{\bar{G}}} \quad \text{and} \quad |x^G \cap H| = |x^H| < 4q^{\dim x^{\bar{H}}} \leq 4q^{\dim x^{\bar{G}}/2 + (n-e)/4 + m^2}.$$

These bounds imply that (2) holds with $\kappa(n) = \frac{3}{n+1}$, which is less than $\frac{7}{30}$ for $n \geq 12$. As usual, for smaller values of n we obtain the result by explicit computation of $|x^G \cap H|$ and $|x^G|$.

Case $\lambda = (2^j, 1^{n-2j})$, $n - 2j > 0$: First suppose $j = 1$. Then $|x^G| > \frac{1}{4}q^n$ and $|x^G \cap H| < q^{n/2+m} + q^{n/2-m}$. This implies that $\log|x^G \cap H|/\log|x^G| < \frac{1}{2} + \frac{7}{30}$ for all values of $n \geq 6$ except $n = 8$. The case $n = 8$ is the exception in part (ii) of Theorem 3.2.

Next suppose that $j = 2$. Here $|x^G| > \frac{1}{4(q+1)} q^{2n-1}$. Since the two Jordan blocks of size 2 can lie in the two different subspaces V_1 and V_2, or in the same one, we have

$$|x^G \cap H| < q^{(n-2m)/2 + (n+2m)/2} + 2q^{n-4+m(m-1)} + 2q^{n+m(m-1)}.$$

Hence (2) holds with $\kappa(n) = \frac{3}{n+1}$, which is less than $\frac{7}{30}$ for $n \geq 12$. For smaller values of n we obtain the conclusion by explicit computations of $|x^G \cap H|$ and $|x^G|$.

Finally, assume $j \geq 3$ (and so $n \geq 8$ since $n - 2j > 0$). The number of ways to distribute the j Jordan blocks of size 2 amongst the subspaces V_1 and V_2 is at most $j + 1$. Then, adapting the analogous bound in [Burness 2007b, p.723] and making use of Lemma 3.3, we have

$$|x^G \cap H| < 4(j+1) q^{\dim x^{\bar{G}}/2 + j/2 + m^2}$$

and as in [Burness 2007b, p.723], we have $|x^G| > \frac{1}{4} q^{\dim x^{\bar{G}}} = \frac{1}{4} q^{j(n-j+1)}$. This yields (2) with $\kappa(n) = \frac{4}{n+2}$, which is less than $\frac{7}{30}$ for $n \geq 16$. As usual, smaller values of n are handled by direct computation.

Case $\lambda = (k^{a_k}, \ldots, 2^{a_2}, 1^l)$, $k \leq n/2 + m$: In the computations below, we adapt the arguments on p.723 of [Burness 2007b]. Let d be the number of nonzero a_i. Then

$$|x^G| > \frac{1}{2^{d+1}} \left(\frac{q}{q+1} \right)^d q^{\dim x^{\bar{G}}}.$$

If $d = 1$ then $\lambda = (k^{(n-l)/k}, 1^l)$, and we can take $k > 2$ by the previous case. By [Lawther et al. 2002, 1.10], we have

$$\dim x^{\bar{G}} = \frac{n^2}{2} + \frac{n}{2} - \frac{l(n-l)}{k} - \frac{l^2}{2} - \frac{1}{2k}(n-l)^2 - \frac{l}{2} - \frac{\alpha}{2k}(n-l),$$

where α is zero if k is even and one if k is odd. Arguing as in [Burness 2007b, p.723] we also have

$$|x^G \cap H| < \left(\frac{n-l}{k} + 1 \right) 2^2 q^{\dim x^{\bar{G}}/2 + (n-l)(1-\alpha/k)/4 + m^2}.$$

These bounds imply (2) with $\kappa(n) = \frac{3}{n-3}$, which is less than $\frac{7}{30}$ for $n \geq 16$, and smaller values of n are handed by explicit computation.

Now suppose that $d \geq 2$. By [Burness 2007b, p.723],

$$\dim x^{\bar{G}} \geq \tfrac{1}{4}n^2 + \tfrac{1}{4}(d^2 - d + 2) - \tfrac{1}{16}d^4 - \tfrac{1}{24}d^3 + \tfrac{3}{16}d^2 - \tfrac{1}{3}d - \tfrac{1}{4}l^2 - \tfrac{1}{2},$$

and adapting the analogous bound given in [Burness 2007b, p.723] and referring to Lemma 3.3, we have

$$|x^G \cap H| < 4^d \left(\frac{\frac{n}{2} - \frac{d^2}{4} + \frac{d}{4} - \frac{l}{2} - 1}{d} + 1 \right)^d q^{\dim x^{\bar{G}}/2 + (n-l)/4 + m^2}.$$

These bounds give (2) with $\kappa(n) = \frac{4}{n}$, which is less than $\frac{7}{30}$ for $n \geq 18$, and smaller values of n are handed by explicit computation. □

Lemma 3.7. *The conclusion of Theorem 3.2 holds when x is a unipotent involution.*

Proof. Let $p = 2$, and recall the description of the involution class representatives a_l, b_l, c_l of G in the preamble to Lemma 3.3.

First assume that x is conjugate to a_l for some even integer l with $2 \leq l \leq \frac{n}{2}$. If $l = 2$, then by [Lawther et al. 2002, 1.10] and [Burness 2007a, Proposition 3.9] we have

$$|x^G \cap H| < 2q^{2(n/2-m-2)} + 2q^{2(n/2+m-2)}. \tag{7}$$

If $l \geq 4$ then we may adapt the analogous equation in [Burness 2007b, p.723] and obtain

$$|x^G \cap H| < \left(\tfrac{l}{2} + 1\right) 2^2 q^{(1/2+3m/(2n))l(n-l)}.$$

Furthermore, for all l, by [Burness 2007b, p.723]

$$|x^G| > \tfrac{1}{2} q^{l(n-l)}.$$

These bounds imply that $\log|x^G \cap H| / \log|x^G| < \frac{1}{2} + \frac{7}{30}$, provided $n \geq 14$ when $l = 2$, and $n \geq 24$ when $l \geq 4$. Smaller values of n can be dealt with by explicit computation of $|x^G \cap H|$ and $|x^G|$.

Now suppose that x is conjugate to either a b_l- or c_l-type involution. If $l = 1$ then by [Lawther et al. 2002, 1.10] and [Burness 2007a, Proposition 3.9]

$$|x^G \cap H| < q^{n/2-m} + q^{n/2+m}, \tag{8}$$

and if $l = 2$, then

$$|x^G \cap H| < q^n + q^{2(n/2-m-1)} + q^{2(n/2+m-1)}. \tag{9}$$

If $l \geq 3$, then by adapting the analogous argument in [Burness 2007b, p.724], we deduce

$$|x^G \cap H| < 4\left(\frac{q^2+1}{q^2-1}\right)\left(q^{\dim x^{\bar{G}}/2+2m-1} + q^{\dim x^{\bar{G}}/2+m-1}\right) + 4\left(\frac{q^2+1}{q^2-1}\right) q^{\dim x^{\bar{G}}/2+l/2+m}$$

where $\dim x^{\bar{G}} = l(n-l+1)$. Lastly, [Burness 2007b, p.724] gives

$$|x^G| > \tfrac{1}{2} q^{l(n-l+1)}.$$

As usual, these bounds imply that $\log|x^G \cap H|/\log|x^G| < \frac{1}{2} + \frac{7}{30}$ for $n \geq 14$, and explicit computations give the same conclusion for smaller values of n. □

This completes the proof of Theorem 3.2.

3B. ***Deduction of Theorem 3.1.*** The deduction of Theorem 3.1 from Theorem 3.2 proceeds along the lines of the proof of [Burness 2007c, 1.1].

First we shall require a small extension of [Burness 2007c, Proposition 2.2]. For a finite group G, define

$$\eta_G(t) = \sum_{C \in \mathcal{C}} |C|^{-t},$$

where $\mathcal{C}$ is the set of conjugacy classes of elements of prime order in G.

Lemma 3.8. *Let G be a finite classical group as in Theorem 3.1, with $n \geq 6$.*

(i) *Then $\eta_G\left(\frac{1}{3}\right) < 1$.*

(ii) *Let $G = \mathrm{PGSp}_8(q)$. Then $\eta_G\left(\frac{1}{3}\right) < 0.396$.*

Proof. (i) This is [Burness 2007c, Proposition 2.2].

(ii) We compute the sizes of the conjugacy classes with each centralizer type using [Burness and Giudici 2016, Table B.7], and bound the number of classes with each centralizer type using the same arguments as those given in the proof of [Burness 2007c, Lemma 3.2]. The result follows from these computations. □

We also need to cover separately the two cases of Theorem 3.1 for dimensions less than 6.

Lemma 3.9. *Theorem 3.1 holds for $G_0 = \mathrm{PSU}_4(q)$ or $\mathrm{PSU}_5(q)$.*

Proof. Consider the first case. Here $G = \mathrm{PGU}_4(q)$ acting on $\mathcal{N}_1$, the set of nondegenerate 1-spaces. Let $v_1, \ldots, v_4$ be an orthonormal basis of the natural module for G. If q is odd, then $\langle v_1\rangle$, $\langle v_2\rangle$, $\langle v_3\rangle$, $\langle v_1+v_2+v_3+v_4\rangle$ is a base for the action of G; and if q is even, then $\langle v_1\rangle$, $\langle v_2\rangle$, $\langle v_3\rangle$, $\langle v_1+v_2+v_3\rangle$, $\langle v_2+v_3+v_4\rangle$ is a base.

Now let $G = \mathrm{PGU}_5(q)$ acting on $\mathcal{N}_2$. Let $v_1, \ldots, v_5$ be an orthonormal basis. Any element of G that fixes the three nondegenerate 2-spaces $\langle v_1, v_2\rangle$, $\langle v_2, v_3\rangle$ and $\langle v_3, v_4\rangle$ also fixes $\langle v_1, v_5\rangle$ and $\langle v_4, v_5\rangle$ (as these are $\langle v_2, v_3, v_4\rangle^\perp$ and $\langle v_1, v_2, v_3\rangle^\perp$), hence fixes all the 1-spaces $\langle v_1\rangle, \ldots, \langle v_5\rangle$. Hence adding two further nondegenerate 2-spaces intersecting in $\langle v_1+\cdots+v_5\rangle$ to the first three gives a base of size 5. □

Proof of Theorem 3.1. Let G and r be as in the statement of Theorem 3.1, and let H be the stabilizer of a nondegenerate r-subspace in $\mathcal{N}_r$. In view of Lemma 3.9, we may assume that the dimension $n \geq 6$.

For a positive integer c, let $Q(G, c)$ be the probability that a randomly chosen c-tuple of elements of $\mathcal{N}_r$ does not form a base for G. Then

$$Q(G,c) \leq \sum_{x \in X} |x^G| \left(\frac{\mathrm{fix}_{\mathcal{N}_r}(x)}{|\mathcal{N}_r|}\right)^c = \sum_{x \in X} |x^G| \left(\frac{|x^G \cap H|}{|x^G|}\right)^c, \tag{10}$$

where X is a set of conjugacy class representatives of the elements of G of prime order. Clearly G has a base of size c if and only if $Q(G, c) < 1$.

Assume for the moment that $G_0 \neq \mathrm{PSp}_8(q)$. Then by Theorem 3.2 we have

$$\frac{|x^G \cap H|}{|x^G|} < |x^G|^{-1/2+7/30}$$

for all elements $x \in G$ of prime order. Hence it follows from (10) that

$$Q(G,5) < \sum_{x \in X} |x^G|^{1+5(-1/2+7/30)} = \eta_G\big(\tfrac{1}{3}\big).$$

Therefore by Lemma 3.8(i), G has a base of size 5, as required.

It remains to consider the case where $G_0 = \mathrm{PSp}_8(q)$. Here Theorem 3.2(ii) gives $|x^G \cap H|/|x^G| < |x^G|^{-1/2+7/30}$ for all elements $x \in G$ of prime order, except when x is a unipotent element with Jordan form $(2, 1^6)$. In the latter case $|x^G| = q^8 - 1$ and $|x^G \cap H| = q^6 + q^2 - 2$. Hence

$$Q(G,5) < \eta_G\big(\tfrac{1}{3}\big) + (q^8 - 1)\left(\frac{q^6 + q^2 - 2}{q^8 - 1}\right)^5,$$

and this is less than 1 for all q, by Lemma 3.8(ii).

This completes the proof of Theorem 3.1. □

4. Proof of Theorem 1

Assume the hypotheses of Theorem 1. Thus $G \leq \mathrm{GL}(V) = \mathrm{GL}_d(q)$, and $E(G)$ is quasisimple and absolutely irreducible on V. Then the group $Z := Z(G)$ consists of scalars, and G/Z is almost simple. Let G_0 be the socle of G/Z. Note that $G_0 = E(G)/(Z \cap E(G))$.

Lemma 4.1. *If G_0 is exceptional of Lie type or sporadic, then $b(G) \leq 6$.*

Proof. Pick $v \in V \setminus \{0\}$, and consider the action of G on the orbit $\Delta = v^G$. By Lemma 2.1(i), if $G_0 \neq M_{24}$ then there exist Z-orbits $\delta_1, \ldots, \delta_6$ such that $G_{\delta_1 \cdots \delta_6} \leq Z$. Hence $b(G) \leq 6$. The case where $G_0 = M_{24}$ is taken care of in Remark 4.3 below. □

Lemma 4.2. Theorem 1(i) *or* (iii) *holds if G_0 is an alternating group.*

Proof. This follows from [Fawcett et al. 2016, Theorem 1.1]. □

In view of the previous two lemmas, we can suppose from now on that G_0 is a classical simple group. Assume that

$$b(G) \geq 7. \tag{11}$$

We aim to show that conclusion (ii) of Theorem 1 must hold. By the above assumption, the dimension $d \geq 7$, and also every element of V^6 is fixed by some element of prime order in $G \setminus Z$, and so

$$V^6 = \bigcup_{g \in \mathcal{P}} C_{V^6}(g), \tag{12}$$

where $\mathcal{P}$ denotes the set of elements of prime order in $G \setminus Z$. Now $|C_{V^6}(g)| = |C_V(g)|^6$, and

$$\dim C_V(g) \le \left\lfloor \left(1 - \frac{1}{\alpha(g)}\right) \dim V \right\rfloor, \tag{13}$$

where $\alpha(g)$ is as defined in the preamble to Lemma 2.2 (strictly speaking, it is $\alpha(gZ)$ for $gZ \in G/Z$). Writing $\alpha = \alpha(G_0)$, it follows that

$$|V|^6 = q^{6d} \le |\mathcal{P}| q^{6\lfloor d(1-1/\alpha)\rfloor}.$$

Since $|G| = |Z||G/Z| \le (q-1)|\mathrm{Aut}(G_0)|$, we therefore have

$$q^{6\lceil d/\alpha\rceil} \le |\mathcal{P}| < |G| \le (q-1)|\mathrm{Aut}(G_0)|. \tag{14}$$

Remark 4.3. Using (14) we can handle the case $G_0 = M_{24}$ as follows, completing the proof of Lemma 4.1: we have $\alpha(M_{24}) \le 4$ by [Goodwin 2000, 2.4], so (14) yields $\frac{6}{4}d < \log_2|M_{24}|$, hence $d \le 18$. By [Hiss and Malle 2001], this forces $d = 11$ and $q = 2$, so $G = M_{24} < \mathrm{GL}_{11}(2)$. Here V or V^* is a quotient of the binary Golay code of length 24, dimension 12, by a trivial submodule, and we see from [Conway et al. 1985, p.94] that there is a G-orbit on V of size 276 or 759 on which G acts primitively. The base sizes of these actions of M_{24} are less than 7, by [Burness et al. 2010], and the conclusion follows. Similar, much simpler, computations also rule out the cases where G_0 is one of the three small groups in the conclusion of Lemma 2.2(vii).

Let $q = p^a$, where p is prime. The analysis divides naturally, according to whether or not the underlying characteristic of G_0 is equal to p — that is, whether or not G_0 is in the set $\mathrm{Lie}(p)$.

Lemma 4.4. *Under assumption* (11), G_0 *is not in* $\mathrm{Lie}(p')$.

Proof. Suppose $G_0 \in \mathrm{Lie}(p')$. Lower bounds for $d = \dim V$ are given by [Landazuri and Seitz 1974; Seitz and Zalesskii 1993], and the values of α by Lemma 2.2. Plugging these into (14) (and also using the fact that $d \ge 7$), we see that G_0 must be one of the following:

$$\begin{gathered}\mathrm{PSp}_4(3), \mathrm{PSp}_4(5), \mathrm{Sp}_6(2), \mathrm{PSp}_6(3), \mathrm{PSp}_8(3), \mathrm{PSp}_{10}(3),\\ U_3(3), U_4(3), U_5(2),\\ \Omega_7(3), \Omega_8^+(2).\end{gathered}$$

At this point we use [Hiss and Malle 2001], which gives the dimensions and fields of definition of all the irreducible projective representations of the above groups of dimension up to 250. Combining this information with (14) leaves just the following possibilities:

G_0	d	q
$U_5(2)$	10	3
$U_4(3)$	20	2
$\mathrm{Sp}_6(2)$	7, 8	$q \le 11$
	14	3
$\Omega_8^+(2)$	8	$q \le 29$

Consider first $G_0 = U_5(2)$. Here $G = \langle -I \rangle \times U_5(2).2 < \mathrm{GL}_{10}(3)$, and the Brauer character of this representation of G is given in [Conway et al. 1985]. From this we can read off the dimensions of the fixed point spaces of $3'$-elements of prime order. These are as follows, using Atlas notation:

g	$2A, -2A$	$2B, -2B$	$2C, -2C$	$5A$	$11AB$
$\dim C_V(g)$	2, 8	6, 4	5, 5	2	0

Also $\alpha \leq 5$ by Lemma 2.2, so (13) gives $\dim C_V(g) \leq 8$ for all elements $g \in G$ of order 3. At this point, the inequality $|V|^6 \leq \sum_{g \in \mathcal{P}} |C_V(g)|^6$ implied by (12) gives

$$3^{60} \leq |2A| \cdot (3^{12} + 3^{48}) + |2B| \cdot (3^{24} + 3^{36}) + |2C| \cdot (3^{30} + 3^{30}) + |5A| \cdot 3^{12} + |3ABCDEF| \cdot 3^{48},$$

where $|2A|$ denotes the size of the conjugacy class of $2A$-elements, and so on. This is a contradiction.

This method works for all the cases in the above table, except $(G_0, d, q) = (\Omega_8^+(2), 8, 3)$; in this case the crude inequality $|V|^6 \leq \sum_{g \in \mathcal{P}} |C_V(g)|^6$ implied by (12) does not yield a contradiction. Here we have $G \leq 2.\Omega_8^+(2).2 < \mathrm{GL}(V) = \mathrm{GL}_8(3)$. Observe that $\Omega_8^+(2).2$ has a subgroup $N = S_3 \times \Omega_6^-(2).2$, and N is the normalizer of $\langle x \rangle$, where x is an element of order 3. Then $C_V(x) \neq 0$, and N must fix a 1-space in $C_V(x)$. Moreover, we compute that the minimal base size of $\Omega_8^+(2).2$ acting on the cosets of N is equal to 4. It follows that there are four 1-spaces in V whose pointwise stabilizer in G is Z. Hence $b(G) \leq 4$ in this case. □

In view of the previous lemmas, from now on we may assume that $G_0 = \mathrm{Cl}_n(q_0)$, a classical simple group over a field $\mathbb{F}_{q_0}$ of characteristic p, with natural module of dimension n. There are various standard isomorphisms between classical groups of low dimensions (e.g., $L_4(q_0) \cong P\Omega_6^+(q_0)$); in such cases we adopt the notation $\mathrm{Cl}_n(q_0)$ taking n to be the minimal possible value. Recall that $G \leq \mathrm{GL}(V) = \mathrm{GL}_d(q)$ and $G_0 = \mathrm{soc}(G/Z) = E(G)/(Z \cap E(G))$. The next lemma identifies the possible highest weights for V as a module for the quasisimple classical group $E(G)$.

Lemma 4.5. *Suppose as above that $G_0 = \mathrm{Cl}_n(q_0)$, a classical group in $\mathrm{Lie}(p)$. Then $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$, and one of the following holds*:

(1) $V = V(\lambda)$, *where λ is one of the weights $\lambda_1, \lambda_2, 2\lambda_1, \lambda_1 + p^i\lambda_1$, or $\lambda_1 + p^i\lambda_{n-1} (i > 0)$ (listed up to automorphisms of G_0, the last one only for $G_0 = L_n^\epsilon(q_0)$).*

(2) $G_0 = L_n^\epsilon(q_0) (n \geq 3)$ *and* $V = V(\lambda_1 + \lambda_{n-1})$.

(3) $G_0 = L_n(q_0) (7 \leq n \leq 21)$ *and* $V = V(\lambda_3)$.

(4) $G_0 = L_6^\epsilon(q_0)$ *and* $V = V(\lambda_3)$.

(5) $G_0 = L_8^\epsilon(q_0)$ *and* $V = V(\lambda_4)$.

(6) $G_0 = \mathrm{PSp}_6(q_0)$ *and* $V = V(\lambda_3)$ *(p odd).*

(7) $G_0 = \mathrm{PSp}_8(q_0)$ *and* $V = V(\lambda_3)$ *(p odd) or* $V(\lambda_4)$ *(p odd).*

(8) $G_0 = \mathrm{PSp}_{10}(q_0)$ *and* $V = V(\lambda_3)$ $(p = 2)$.

(9) $G_0 = P\Omega_n^\epsilon(q_0) (7 \leq n \leq 20, n \neq 8)$ *and V is a spin or half-spin module.*

Proof. Assume first that $q_0 > q$. Then by [Kleidman and Liebeck 1990, 5.4.6], there is an integer $s \geq 2$ such that $q_0 = q^s$ and $d = m^s$, where m is the dimension of an irreducible module for $E(G)$. Note that $m \geq n$ (by the minimal choice of n). By (14),

$$q^{6m^s/\alpha} \leq (q-1)|\mathrm{Aut}(\mathrm{Cl}_n(q^s))|.$$

Lemma 2.2 shows that $\alpha \leq n+2$ (excluding the small groups in Lemma 2.2(vii) which were ruled out in Remark 4.3), and hence

$$q^{6m^s/(n+2)} \leq (q-1)|\mathrm{Aut}(\mathrm{Cl}_n(q^s))| < (q-1)q^{s(n^2-1)}(2s\log_p q).$$

Since $m \geq n$, it follows from this that $s = 2$ and

$$m^2 < \frac{(n+2)(2n^2+1)}{6}.$$

Now using [Lübeck 2001], we deduce that $m = n$ and so

$$E(G) \leq \mathrm{SL}_n(q^2) < \mathrm{SL}_{n^2}(q).$$

As in [Liebeck and Shalev 2002, p.104], we see that there is a vector v such that $E(G)_v \leq \mathrm{SU}_n(q)$. By Lemma 2.1, the base size of an almost simple group with socle $L_n(q^2)$ acting on the cosets of a subgroup containing $U_n(q)$ is at most 4. Hence there are 1-spaces $\delta_1, \dots, \delta_4$ whose pointwise stabilizer in G is equal to Z, and so $b(G) \leq 4$ in this case. This contradicts our initial assumption that $b(G) \geq 7$.

Hence we may assume now that $q_0 \leq q$, so that $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$ by [Kleidman and Liebeck 1990, 5.4.6]. Now (14) gives

$$d < \tfrac{\alpha}{6}(1 + \log_q|\mathrm{Aut}(G_0)|). \tag{15}$$

Noting that apart from the case where $G_0 = P\Omega_8^+(q_0)$, we have $|\mathrm{Out}(G_0)| \leq q$, it now follows using Lemma 2.2 that $d < N$, where N is as defined in Table 4.1.

G_0	N
$L_n^\epsilon(q_0)$	$\frac{1}{6}n(1+n^2),\ n > 4$
	$\frac{1}{6}(n+2)(1+n^2),\ n \leq 4$
$\mathrm{PSp}_n(q_0),\ n \geq 4$	$\frac{1}{6}(n+1)\big(2+\frac{1}{2}n(n+1)\big),\ n > 4$
	$10,\ n = 4$
$P\Omega_n^\epsilon(q_0),\ n \geq 7$	$\frac{1}{6}n\big(2+\frac{1}{2}n(n-1)\big)+\delta$

Table 4.1. Where δ is $\log_q 6$ if $G_0 = P\Omega_8^+(q_0)$, and $\delta = 0$ otherwise.

Now applying the bounds in [Lübeck 2001] (and also the improved bound for type A in [Martínez 2017]), we see that with one possible exception, one of the cases (1)–(9) in the conclusion holds. The possible exception is $G_0 = L_4^\epsilon(q_0)$ with $p = 3$ and $V = V(\lambda_1+\lambda_2)$, of dimension 16. But in this case G does not contain a graph automorphism of G_0 (since the weight $\lambda_1+\lambda_2$ is not fixed by a graph automorphism), and so [Guralnick and Saxl 2003, 4.1] implies that we can take $\alpha = 4$ in (15), and this rules out this case. □

Lemma 4.6. *Under the above assumption* (11), G_0 *is not as in* (3)–(9) *of Lemma 4.5.*

Proof. Suppose G_0 is as in (3)–(9) of Lemma 4.5. First we consider the actions of the simple algebraic groups $\bar{G}$ over $K = \bar{\mathbb{F}}_q$ corresponding to G_0 on the $K\bar{G}$-modules $\bar{V} = V \otimes K = V_{\bar{G}}(\lambda)$. Define

$$M_\lambda = \min\{\operatorname{codim} V_\gamma(g) \mid \gamma \in K^*,\, g \in \bar{G} \setminus Z(\bar{G})\}.$$

By Lemma 2.3, a lower bound for M_λ is given by $\min(s_\lambda, s'_\lambda)$, and simple calculations give the following lower bounds:

$\bar{G}$	λ	$M_\lambda \geq$
$A_n (n \geq 5)$	λ_3	$\frac{1}{2}(n-1)(n-2)$
A_7	λ_4	20
C_3	$\lambda_3 (p > 2)$	4
C_4	$\lambda_3 (p > 2)$	13
	$\lambda_4 (p > 2)$	13
C_5	$\lambda_3 (p = 2)$	25
$D_n (n \geq 5)$	λ_{n-1}, λ_n	2^{n-3}
$B_n (n \geq 3)$	λ_n	2^{n-2}

Apart from cases (4) and (5) of Lemma 4.5, the group G/Z is contained in $\bar{G}/Z$; in cases (4) and (5), a graph automorphism of $\bar{G}$ may also be present. Thus excluding (4) and (5), we see that (12) gives

$$q^{6M_\lambda} \leq |G|. \tag{16}$$

The bounds for M_λ in the above table now give a contradiction, except when $\bar{G} = D_n (n \leq 6)$ or $B_n (n \leq 5)$.

We now consider the cases $\bar{G} = D_n (n \leq 6)$ or $B_n (n \leq 5)$. Since $B_{n-1}(q) < D_n(q) < \mathrm{GL}(V)$, it suffices to deal with $\bar{G} = D_6$, D_5 or B_3.

Suppose $G_0 = D_6^\epsilon(q_0)$ with $\mathbb{F}_{q_0} \subseteq \mathbb{F}_q$. By Lemma 2.4(i), for any element $g \in G$ that is not a scalar multiple of a root element, we have $\operatorname{codim} C_V(g) \geq 12$; and for root elements u, from the above table we have $\operatorname{codim} C_V(u) \geq 8$. The number of root elements in G_0 is less than $2q^{18}$. Hence (12) gives

$$|V|^6 = q^{32\times 6} \leq 2q^{18}(q-1)\cdot q^{24\times 6} + |G|q^{20\times 6},$$

which is a contradiction.

Now suppose $G_0 = D_5^\epsilon(q_0)$. We perform a similar calculation, using Lemma 2.4(ii). The number of semisimple elements s of G for which $C_{\bar{G}}(s)' = A_4$ is at most $|Z|\cdot(q-1)|D_5^\epsilon(q) : A_4^\epsilon(q).(q-1)| < 2q^{22}$. The number of root elements in G_0 is less than $2q^{14}$, and the number of unipotent elements in the class

$(A_1^2)^{(1)}$ is less than $2q^{20}$ (these have centralizer in $D_5^{\epsilon}(q)$ of order $q^{14}|\mathrm{Sp}_4(q)|(q-\epsilon)$, see [Liebeck and Seitz 2012, Table 8.6a]). Hence (12) together with Lemma 2.4(ii) gives

$$q^{16\times 6} \le 2(q^{14}+q^{20})(q-1)q^{12\times 6} + 2q^{22}q^{10\times 6} + |G|q^{8\times 6}.$$

This is a contradiction.

Next consider $G_0 = B_3(q_0)$. In the action on the spin module V, there is a vector v with stabilizer $G_2(q_0)$ in $B_3(q_0)$. Hence $b(G) \le 4$ in this case, by Lemma 2.1(ii).

It remains to handle cases (4) and (5), where G may contain graph automorphisms of $\bar{G}$. For $G_0 = L_6^{\epsilon}(q_0)$ or $L_8^{\epsilon}(q_0)$, the conjugacy classes of involutions in the coset of a graph automorphism are given by [Aschbacher and Seitz 1976, §19] for q even and by [Gorenstein et al. 1998, 4.5.1] for q odd. It follows that the number of such involutions is less than $2q^{21}$ or $2q^{36}$ in case (4) or (5), respectively. For such an involution g, by (13) we have $\dim C_V(g) \le 16$ or 60, respectively. All other elements of prime order in G lie in $\bar{G}Z$, hence have fixed point space of codimension at least M_λ. Hence we see that (12) gives

$$|V|^6 = \begin{cases} q^{20\times 6} \le |G|\cdot q^{14\times 6} + 2q^{21}\cdot q^{16\times 6} & \text{in case (4)},\\ q^{70\times 6} \le |G|\cdot q^{50\times 6} + 2q^{36}\cdot q^{60\times 6} & \text{in case (5)}.\end{cases}$$

Both of these yield contradictions.

This completes the proof of the lemma. □

Lemma 4.7. *The group G_0 is not as in* (2) *of Lemma 4.5.*

Proof. Here $G_0 = L_n^{\epsilon}(q_0)$ with $n \ge 3$, and $V = V(\lambda_1+\lambda_{n-1})$. Suppose first that $\epsilon = +$. Then $G/Z \le \mathrm{PGL}_n(q)$, and V can be identified with T/T_0, where

$$T = \{A \in M_{n\times n}(q) : \mathrm{Tr}(A) = 0\} \quad \text{and} \quad T_0 = \{\lambda I_n : n\lambda = 0\},$$

and the action of $\mathrm{GL}_n(q)$ is by conjugation. By [Steinberg 1962], we can choose $X, Y \in \mathrm{SL}_{n-1}(q_0)$ generating $\mathrm{SL}_{n-1}(q_0)$. Let $x = \mathrm{Tr}(X)$, $y = \mathrm{Tr}(Y)$, and define

$$A_1 = \begin{pmatrix} X & 0\\ 0 & -x\end{pmatrix}, \quad A_2 = \begin{pmatrix} Y & 0\\ 0 & -y\end{pmatrix}, \quad A_3 = \begin{pmatrix} -x & 0\\ 0 & X\end{pmatrix}, \quad A_4 = \begin{pmatrix} -y & 0\\ 0 & Y\end{pmatrix}.$$

Then $\{A_1, \dots, A_4\}$ is a base for the action of $\mathrm{GL}_n(q)$, and hence $b(G) \le 4$.

Now suppose $\epsilon = -$, so that $G/Z \le \mathrm{PGU}_n(q)$, where we take $\mathrm{GU}_n(q) = \{g \in \mathrm{GL}_n(q^2) : g^T g^{(q)} = I\}$. Then we can identify V with the $\mathbb{F}_q$-space S modulo scalars, where

$$S = \{A \in M_{n\times n}(q^2) : \mathrm{Tr}(A) = 0,\, A^T = A^{(q)}\},$$

with $\mathrm{GU}_n(q)$ acting by conjugation. As in [Liebeck and Shalev 2002, p.104], there is a vector $A \in V$ such that $\mathrm{GU}_n(q)_A \le N_r$, where N_r is the stabilizer of a nondegenerate r-space and $r = \frac{1}{2}n$ or $\frac{1}{2}(n-(n,2))$. In the first case, the base size of $\mathrm{PGU}_n(q)$ acting on $\mathcal{N}_r$ is at most 5, by Lemma 2.1(ii) (since in this case N_r is contained in a nonsubspace subgroup of type $\mathrm{GU}_{n/2}(q) \wr S_2$); and the same holds in the second case, by Theorem 3.1. It follows that $b(G) \le 5$, contradicting our assumption (11). □

The proof of Theorem 1 is completed by the following lemma.

Lemma 4.8. *If G_0 is as in* (1) *of Lemma 4.5, then conclusion* (ii) *of Theorem 1 holds.*

Proof. Here $G_0 = \mathrm{Cl}_n(q_0)$, and $V = V(\lambda)$ with $\lambda = \lambda_1, \lambda_2, 2\lambda_1, \lambda_1 + p^i\lambda_1$ or $\lambda_1 + p^i\lambda_{n-1}$.

If $\lambda = \lambda_1$, then $d = n$ and $E(G) = \mathrm{Cl}_d(q_0)$ is as in part (ii) of Theorem 1.

Now consider $\lambda = \lambda_2$. Here we argue as in the proof of [Liebeck and Shalev 2002, 2.2] (see p.102). Assume first that $V = \wedge^2 W$ where W is the natural module for $\mathrm{Cl}_n(q_0)$ (with scalars extended to $\mathbb{F}_q$). Then $E(G)$ lies in the action of $\mathrm{SL}(W)$ on this space. If n is even, then the argument in [loc. cit.] provides a vector $v \in V$ such that $\mathrm{SL}(W)_v = \mathrm{Sp}(W)$, and so $b(G) \le b(\mathrm{PGL}(W)/\mathrm{PSp}(W))$. By Lemma 2.1(ii), this is at most 4, provided $n \ge 6$; for $n = 4$, the action $\mathrm{PGL}_4 / \mathrm{PSp}_4$ is a subspace action (it is O_6/N_1), so Lemma 2.1 does not apply — but an easy argument shows that the base size is at most 5 in this case. And if n is odd, say $n = 2k+1$, then the argument in [loc. cit.] gives three vectors with stabilizer normalizing a subgroup Sp_{2k}, and then adding three further vectors gives a base — so $b(G) \le 6$ (again, a slightly different argument is needed for the case $2k = 4$, but this is straightforward). Now assume $V \ne \wedge^2 W$. Then V is equal to $(\wedge^2 W)^+$ (which is $f^\perp$ or $f^\perp/\langle f\rangle$ in the notation of [loc. cit., p.103]), and $E(G)$ lies in the action of $\mathrm{Sp}(W)$ on this space; the argument in [loc. cit.] gives

$$b(G) \le b(\mathrm{PSp}(W), \mathcal{N}_r),$$

where $\mathcal{N}_r$ is the set of nondegenerate subspaces of dimension r and $r = \frac{1}{2}n$ or $\frac{1}{2}(n-(n,4))$. As before, Lemma 2.1(ii) (in the first case) and Theorem 3.1 (in the second) now give $b(G) \le 5$.

The case where $\lambda = 2\lambda_1$ is similar to the λ_2 case, arguing as in [loc. cit., p.103]. Note that p is odd here. If G_0 is not an orthogonal group, then $E(G) \le \mathrm{SL}(W)$ acting on $V = S^2W$, and there is a vector v such that $\mathrm{SL}(W)_v = \mathrm{SO}(W)$; hence $b(G) \le b(\mathrm{SL}(W)/\mathrm{SO}(W)) \le 4$, by Lemma 2.1(ii). And if G_0 is orthogonal, then $V = (S^2W)^+$ (of dimension $\dim S^2W - \delta$, $\delta \in \{1, 2\}$), and we see as in the previous case that $b(G) \le b(PGO(W), \mathcal{N}_r)$ with $r = \frac{1}{2}(n-(n,2))$. Hence Theorem 3.1 gives $b(G) \le 5$ again.

Finally, suppose $\lambda = \lambda_1 + p^i\lambda_1$ or $\lambda_1 + p^i\lambda_{n-1}$. Here as in [loc. cit., p.103], we have $E(G) \le \mathrm{SL}(W) = \mathrm{SL}_n(q)$ acting on $V = W \otimes W^{(p^i)}$ or $W \otimes (W^*)^{(p^i)}$. We can think of the action of $\mathrm{SL}(W)$ on V as the action on $n \times n$ matrices, where $g \in \mathrm{SL}(W)$ sends

$$A \to g^T A g^{(p^i)} \text{ or } g^{-1} A g^{(p^i)}.$$

Hence we see that the stabilizer of the identity matrix I is contained in $\mathrm{SU}_n(q^{1/2})$ or $\mathrm{SL}_n(q^{1/r})$ for some $r > 1$, and so as usual Lemma 2.1(ii) gives $b(G) \le 5$. □

This completes the proof of Theorem 1.

References

[Aschbacher and Seitz 1976] M. Aschbacher and G. M. Seitz, "Involutions in Chevalley groups over fields of even order", *Nagoya Math. J.* **63** (1976), 1–91. MR Zbl

[Burness 2007a] T. C. Burness, "Fixed point ratios in actions of finite classical groups, II", *J. Algebra* **309**:1 (2007), 80–138. MR Zbl

[Burness 2007b] T. C. Burness, "Fixed point ratios in actions of finite classical groups, III", *J. Algebra* **314**:2 (2007), 693–748. MR Zbl

[Burness 2007c] T. C. Burness, "On base sizes for actions of finite classical groups", *J. Lond. Math. Soc.* (2) **75**:3 (2007), 545–562. MR Zbl

[Burness and Giudici 2016] T. C. Burness and M. Giudici, *Classical groups, derangements and primes*, Australian Math. Soc. Lecture Series **25**, Cambridge Univ. Press, 2016. MR Zbl

[Burness et al. 2009] T. C. Burness, M. W. Liebeck, and A. Shalev, "Base sizes for simple groups and a conjecture of Cameron", *Proc. Lond. Math. Soc.* (3) **98**:1 (2009), 116–162. MR Zbl

[Burness et al. 2010] T. C. Burness, E. A. O'Brien, and R. A. Wilson, "Base sizes for sporadic simple groups", *Israel J. Math.* **177** (2010), 307–333. MR Zbl

[Conway et al. 1985] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford Univ. Press, 1985. MR Zbl

[Duyan et al. 2018] H. Duyan, Z. Halasi, and A. Maróti, "A proof of Pyber's base size conjecture", *Adv. Math.* **331** (2018), 720–747. MR Zbl

[Fawcett et al. 2016] J. B. Fawcett, E. A. O'Brien, and J. Saxl, "Regular orbits of symmetric and alternating groups", *J. Algebra* **458** (2016), 21–52. MR Zbl

[Goodwin 2000] D. P. M. Goodwin, "Regular orbits of linear groups with an application to the $k(GV)$-problem, I", *J. Algebra* **227**:2 (2000), 395–432. MR Zbl

[Gorenstein et al. 1998] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups, III*, Math. Surveys and Monographs **40.3**, Amer. Math. Soc., Providence, RI, 1998. MR Zbl

[Guralnick and Lawther] R. M. Guralnick and R. Lawther, "Generic stabilizers in actions of simple algebraic groups", in preparation.

[Guralnick and Malle 2004] R. M. Guralnick and G. Malle, "Classification of $2F$-modules, II", pp. 117–183 in *Finite groups 2003* (Gainesville, FL, 2003), edited by C. Y. Ho et al., de Gruyter, Berlin, 2004. MR Zbl

[Guralnick and Saxl 2003] R. M. Guralnick and J. Saxl, "Generation of finite almost simple groups by conjugates", *J. Algebra* **268**:2 (2003), 519–571. MR Zbl

[Halasi et al. 2018] Z. Halasi, M. W. Liebeck, and A. Maróti, "Base sizes of primitive groups: bounds with explicit constants", preprint, 2018. arXiv

[Hiss and Malle 2001] G. Hiss and G. Malle, "Low-dimensional representations of quasi-simple groups", *LMS J. Comput. Math.* **4** (2001), 22–63. Correction in **5** (2002), 95–126. MR Zbl

[Kenneally 2010] D. J. Kenneally, *On eigenvectors for semisimple elements in actions of algebraic groups*, Ph.D. thesis, University of Cambridge, 2010, Available at https://search.proquest.com/docview/1771283289.

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

[Landazuri and Seitz 1974] V. Landazuri and G. M. Seitz, "On the minimal degrees of projective representations of the finite Chevalley groups", *J. Algebra* **32** (1974), 418–443. MR Zbl

[Lawther et al. 2002] R. Lawther, M. W. Liebeck, and G. M. Seitz, "Fixed point spaces in actions of exceptional algebraic groups", *Pacific J. Math.* **205**:2 (2002), 339–391. MR Zbl

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

[Liebeck and Shalev 2002] M. W. Liebeck and A. Shalev, "Bases of primitive linear groups", *J. Algebra* **252**:1 (2002), 95–113. MR Zbl

[Liebeck and Shalev 2014] M. W. Liebeck and A. Shalev, "Bases of primitive linear groups, II", *J. Algebra* **403** (2014), 223–228. MR Zbl

[Lübeck 2001] F. Lübeck, "Small degree representations of finite Chevalley groups in defining characteristic", *LMS J. Comput. Math.* **4** (2001), 135–169. MR Zbl

[Martínez 2017] Ã. L. Martínez, “Small-dimensional representations of algebraic groups of type A_l”, preprint, 2017. arXiv

[Pyber 1993] L. Pyber, “Asymptotic results for permutation groups”, pp. 197–219 in *Groups and computation* (New Brunswick, NJ, 1991), edited by L. Finkelstein and W. M. Kantor, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **11**, Amer. Math. Soc., Providence, RI, 1993. MR Zbl

[Seitz and Zalesskii 1993] G. M. Seitz and A. E. Zalesskii, “On the minimal degrees of projective representations of the finite Chevalley groups, II”, *J. Algebra* **158**:1 (1993), 233–243. MR Zbl

[Spaltenstein 1982] N. Spaltenstein, *Classes unipotentes et sous-groupes de Borel*, Lecture Notes in Math. **946**, Springer, 1982. MR Zbl

[Steinberg 1962] R. Steinberg, “Generators for simple groups”, *Canad. J. Math.* **14** (1962), 277–283. MR Zbl

Communicated by Pham Huu Tiep
Received 2018-02-20 Revised 2018-04-10 Accepted 2018-06-06

m.lee16@imperial.ac.uk *Department of Mathematics, Imperial College, London, United Kingdom*

m.liebeck@imperial.ac.uk *Department of Mathematics, Imperial College, London, United Kingdom*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2018 is US $340/year for the electronic version, and $535/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 12 No. 6 2018

1937-0652(2018)12:6;1-B