BULL. AUSTRAL. MATH. SOC. 20D60
VOL. 48 (1993) [495–521]

ON THE ORDERS OF PRIMITIVE LINEAR P'-GROUPS

A. GAMBINI WEIGEL AND T.S. WEIGEL

A group $G \leqslant GL_K(V)$ is called K-primitive if there exists no non-trivial decomposition of V into a sum of K-spaces which is stabilised by G. We show that if V is a finite vector space and G a K-primitive subgroup of $GL_K(V)$ whose order is coprime to $|V|$, we can bound the order of G by $|V|\log_2(|V|)$ apart from one exception. Later we use this result to obtain some lower bounds on the number of p-singular elements in terms of the group order and the minimal representation degree.

1. INTRODUCTION

Let G be a finite group and V a finite dimensional K vector space for some field K. Assume further that V is an irreducible KG-module and that G is acting faithfully on V. Similarly to permutation groups, we call the representation $\phi : G \hookrightarrow GL_K(V)$ imprimitive if there exist non-trivial subspaces $W_i \neq V$; $i = 1, \ldots, r$ of V such that $V = W_1 \oplus \ldots \oplus W_r$ and G is acting on the set $\{ W_i \mid 1 \leqslant i \leqslant r \}$. Accordingly we call the representation primitive if the representation is faithful and not imprimitive. So primitive representations have to be irreducible by definition, but the converse is not true. A primitive representation can be thought of as a representation for which Clifford theory cannot be applied to simplify the representation via a permutation representation.

Our main purpose in the following section is to consider the case where V is a finite vector space over some finite field $\mathbb{F}_q$ of characteristic p and G is some finite p'-group, that is, $(|G|, p) = 1$. An example of this situation is the vector space $V = F$, where $F = \mathbb{F}_{2^n}$ is the extension field of $\mathbb{F}_2$ of degree n and $G = F^* \rtimes \mathrm{Aut}_f(F)$, the semidirect product of the group of units of F with the group of field automorphisms of F. In this case we have

$$|G| = (|V| - 1) \cdot \log(|V|),$$

where $\log : \mathbb{R}^+ \longrightarrow \mathbb{R}$ denotes the logarithm function to the base 2, that is, $2^{\log(x)} = x$. We shall show that asymptotically this is the maximal possible order of a primitive linear p'-group acting on a finite vector space V.

Received 13th January, 1993

https://doi.org/10.1017/S0004972700015951 Published online by Cambridge University Press

THEOREM A. *Let G be a finite K-primitive linear group acting on a finite vector space V over some finite field K of characteristic p. Assume further that $(|G|, p) = 1$ and define $E := \mathrm{End}_{KG}(V)$. Then*

$$|G| \leqslant |V| \cdot \dim_E(V) \cdot \log(p)$$

or $G \simeq Sp_4(3)$, $K = \mathbb{F}_7$ and V is an irreducible 4-dimensional KG-module.

Some work has been done on bounding the order of arbitrary primitive linear groups G in terms of the finite vector space V they are acting on [**16**]. But in general one cannot expect to obtain a polynomial bound for $|G|$. However it was proved by Pàlfy that for soluble G one can bound $|G|$ by $|V|^{3.25}$ [**16**].

Also Theorem A may be interesting in itself as it has a nice application. For a finite group G we define

$$\mu(G) := \min\{\, n \in \mathbb{N} \mid \exists \phi \in \mathrm{Hom}(G, S_n),\ \phi \text{ injective} \,\}$$

to be the minimal faithful representation degree of G as a permutation group. An element of G is called *p-singular* if its order is divisible by p. Let p be a divisor of the order of G. Then it is natural to ask what the distribution of p-singular elements looks like. Let us define

$$\mathcal{A}_p(G) := \{\, g \in G \mid p \,|\, \mathrm{ord}(g) \,\}.$$

In section 3 and 4 we prove the following theorem:

THEOREM B. *Let G be a finite group and p a non-trivial prime divisor of $|G|$. Then one has*

$$\frac{|G|}{|\mathcal{A}_p(G)|} \leqslant 2 \cdot \mu(G) \cdot \log(\mu(G)).$$

Easy examples show that $I_p(G) := |G| / (|\mathcal{A}_p(G)|)$ cannot be bounded by a constant, for example, for $G_n = (Z_p)^n \rtimes Z_{p^n-1}$ one gets $I_p(G) = p^n$. As G_n has exactly one minimal normal subgroup the minimal faithful permutation representation of G_n must be transitive. This implies $\mu(G_n) = p^n$. So the best possible result one can expect is that $I_p(G)$ is bounded by $\mu(G)$.

The motivation for describing the distribution of p-singular elements in terms of the minimal faithful representation degree has its origin in "Computational Group Theory". Although there exists a polynomial time algorithm for finding elements of order p (see [**11**]), this problem is usually solved on computers simply by choosing elements at random and checking their orders. Simplicity of implementation and success in many applications justify this treatment. Theorem B gives an explanation for this success. By choosing $\mu(G)^{1+\epsilon}$ many elements there is a 'high' possibility in finding an element of order p.

This paper was written while the first author was working on her dissertation [**8**], in which she also discussed this problem in detail. Recently the authors have heard of a similar version of our Theorem by Isaacs, Kantor and Spaltenstein [**10**] which was found independently. In our treatment Theorem A is the keypoint for a good reduction to the almost simple case, while they chose a different approach with the advantage that they obtained a bound linear in $\mu(G)$.

Finally we want to mention that the proofs of Theorem A and Theorem B make use of the classification of finite simple groups. All notations we shall use are standard; most of them can be found in [**5**, **3**, or **4**].

2. Primitive Linear p'-Groups

The proof of Theorem A will be given in two steps. First we reduce the problem to the almost simple case, second we prove the assertion for all almost simple groups. The reduction follows a similar argument to that used in the classification of maximal subgroups due to Aschbacher [**1**].

For this we extend the notation of primitive linear groups to semi-linear groups. For this let us define $\Gamma L_K(V) := GL_K(V).\mathrm{Aut}_f(K)$ and $P\Gamma L_K(V) := PGL_K(V).\mathrm{Aut}_f(K)$. A group $G \leqslant \Gamma L_K(V)$ is called *K-imprimitive* if there exist non-trivial K-subspaces $W_1, \dots, W_n$ such that $V = W_1 \oplus \dots \oplus W_n$ and G is acting on the set $\{W_1, \dots, W_n\}$. Accordingly we call a group *K-primitive* if such a decomposition does not exist. Similarly $H \leqslant P\Gamma L_K(V)$ is called *K-primitive* if $G = Z.H$ is *K-primitive* on V where $Z := Z(GL_K(V))$.

We call the K-primitive group $G \leqslant \Gamma L_K(V)$ *reduced* if

(1) $(F^*(G))/(Z(G))$ is simple and non-abelian,
(2) V is an absolutely irreducible $KF^*(G)$-module,
(3) V as a $KF^*(G)$-module is defined over no proper subfield of K.

Here $F^*(G)$ denotes the generalised Fitting subgroup of G. The following lemma will reduce the proof to the almost simple case:

Lemma 2.1. *Let K be a finite field of characteristic p. Assume that for every reduced K-semilinear p'-group $H \leqslant \Gamma L_K(W)$ one has*

$$|H| \leqslant |W| \cdot \dim_E(W) \cdot \log(p)$$

where $E = \mathrm{End}_{\mathbb{F}_p H}(W)$ or $H = Sp_4(3)$, $K = \mathbb{F}_7$ and W is an irreducible 4-dimensional KH-module. Then for every K-primitive p'-group $G \leqslant \Gamma L_K(V)$ one has

$$|G| \leqslant |V| \cdot \dim_{E'}(V) \cdot \log(p)$$

where $E' = \mathrm{End}_{\mathbb{F}_p G}(V)$ or $G = Sp_4(3)$, $K = \mathbb{F}_7$ and V is an irreducible 4-dimensional KG-module.

PROOF: Let $G \leqslant \Gamma L_K(V)$ be a primitive p'-group. Without loss of generality one may assume $Z = Z(GL_K(V)) \leqslant G$. We put

$$\mathcal{N}_G := \{\, N \trianglelefteq G \mid Z < N \trianglelefteq G \cap GL_K(V) \,\}.$$

As G is K-primitive there is only one isomorphism type of irreducible KN-submodule of V for each $N \in \mathcal{N}_G$. To see this assume that there are two non-isomorphic non-trivial irreducible KN-submodules W_1, $W_2 \in Irr_{KN}(V)$, that is, $W_1 \not\simeq_{KN} W_2$. As $Z \leqslant N$ every $\mathbb{F}_p N$-submodule of V is also a KN-submodule. This shows also that two KN-submodules of V are isomorphic as KN-modules if and only if they are isomorphic as $\mathbb{F}_p N$-modules. So let X_1 (respectively X_2) be the homogeneous components of V that contain the $\mathbb{F}_p N$-submodules W_1 (respectively W_2). Now one may apply Clifford theory to the irreducible $\mathbb{F}_p G$-module V, the normal subgroup N and the homogeneous component X_1 (see [**9**, p.565]). This yields $V = \bigoplus_{g \in G} X_1^g$. But by the previously mentioned argument X_1^g is also a KN-module and we obtain a contradiction to the K-primitivity of G. Let us define $W_N \leqslant V$ to be a non-trivial irreducible KN-submodule of V.

The proof of Lemma 2.1 will be done by induction on $(\dim_K(V), |K : \mathbb{F}_p|)$ endowed with the lexicograhical order, that is, $(2,1) > (1,2)$.

For $\dim_K(V) = 1$ one has $G \leqslant \Gamma L_K(K) = K^* \rtimes \mathrm{Aut}_f(K)$. Let $A \leqslant \mathrm{Aut}_f(K) := Im(G \longrightarrow \mathrm{Aut}_f(K))$. Then $E := \mathrm{End}_{\mathbb{F}_p G}(K) = \mathrm{Fix}_A(K)$ is the fixed subfield of K under the action of A. By elementary Galois theory one has $|A| = |K : E| = \dim_E(K)$ and the assertion follows in this case.

So assume that the assertion holds for K_0-primitive p'-groups $G_0 \leqslant \Gamma L_{K_0}(V_0)$ where $(\dim_{K_0}(V_0), |K_0 : \mathbb{F}_p|) < (\dim_K(V), |K : \mathbb{F}_p|)$.

Assume that there exists a normal subgroup $M \in \mathcal{N}_G$ with $S := \mathrm{End}_{KM}(W_M) > K$. For all irreducible KM-submodules $W \in Irr_{KM}(V)$ of V one has $W \simeq_{KM} W_M$ and $\mathrm{End}_{KM}(W) \simeq S$. By some standard arguments (see [**1**, (3.11.)] one has

$$C_{GL_K(V)}(M) \simeq GL_S(U), \text{ for } U \in \mathrm{Hom}_{KM}(W_M, V).$$

So put $F^\natural := Z\big(C_{GL_K(V)}(M)\big) \simeq S^*$, and $F := F^\natural \cup \{0\} \subseteq \mathrm{End}_K(V)$. Clearly $F \simeq S$ and V is a homogeneous F-module; in particular V is an F vector space. Let $v \in V$, $g \in G$, $c \in C$, $m, m' \in M$ such that $gm = m'g$. Then

$$v.m(g^{-1}cg) = v.g^{-1}m'cg = v.g^{-1}cm'g = v.(g^{-1}cg)m$$

https://doi.org/10.1017/S0004972700015951 Published online by Cambridge University Press

and G acts on $C_{GL_K(V)}(M)$ by conjugation; in particular G acts on $F \subseteq \mathrm{End}_K(V)$ by conjugation $\mathbb{F}_p$-linearly. Let $N := \ker(G \longrightarrow \mathrm{Aut}_f(F))$ be the kernel of this action. As $N \leqslant C_{GL_K(V)}(F^\natural)$ one gets $N \leqslant GL_F(V)$. For $v \in V$, $f \in F$ and $G \in G$ one gets $(v.f).g = (v.g).f^g$ and thus G is F-semi-linear, that is, $G \leqslant \Gamma L_F(V)$. But G is K-primitive and therefore F-primitive on V. As $(\dim_F(V), |F:\mathbb{F}_p|) < (\dim_K(V), |K:\mathbb{F}_p|)$ we may apply induction. As $|F:\mathbb{F}_p| \geqslant 2$ one can exclude the case $(G,V) = \left(Sp_4(3), (\mathbb{F}_7)^4\right)$. Thus induction implies $|G| \leqslant |V| \cdot \dim_E(V) \cdot \log(p)$. So in the following we may assume that $\mathrm{End}_{KM}(W_M) = K$ for all $M \in \mathcal{N}_G$.

Now assume that V is a reducible KN-module for some $N \in \mathcal{N}_G$. Let $W \in Irr_{KN}(V)$, $W \neq V$. By the previously mentioned arguments (see [1, (3.11)]) one has

$$\mathrm{End}_{KN}(V) \simeq \mathrm{End}_K(U), \text{ where } U := \mathrm{Hom}_{KN}(W,V),$$

and G is acting on $C_{GL_K(V)}(N) \simeq GL_K(U)$ by conjugation. As $V \simeq \bigoplus_{1\leqslant i\leqslant n} W$ one gets

$$C_{GL_K(V)}\big(C_{GL_K(V)}(N)\big) = GL_K(W),$$

where $GL_K(W)$ is embedded diagonally in $GL_K(V)$. Let

$$\begin{aligned} H := N_{GL_K(V)}\big(C_{GL_K(V)}(N)\big) &= C_{GL_K(V)}\big(C_{GL_K(V)}(N)\big) \circ C_{GL_K(V)}(N) \\ &\simeq GL_K(W) \circ GL_K(U). \end{aligned}$$

The sign "$\circ$" stands for the central product of normal subgroups, that is, $A \circ B$ is a group where $A, B \trianglelefteq A \circ B$ and $A \cap B \leqslant Z(A \circ B)$. As G normalises $C_{GL_K(V)}(N)$ one has $G_0 := G \cap GL_K(V) \leqslant H$. For H it follows that $V \simeq_{KH} W \otimes_K U$. So V is an absolutely irreducible KH-module and this implies $C_{GL_K(V)}(H) = Z$. But G is also acting on Z by conjugation with kernel G_0. This implies $G \leqslant (GL_K(W) \circ GL_K(U)).\mathrm{Aut}_f(K)$, where the action of $\mathrm{Aut}_f(K)$ is diagonal on $GL_K(W)$ and $GL_K(U)$. Let

$$\begin{aligned} \alpha &: G \longrightarrow \Gamma L_K(U) =: H_1 \\ \beta &: G \longrightarrow \Gamma L_K(W) =: H_2 \end{aligned}$$

be the canonical homomorphisms. Further let $A := Im(G \longrightarrow \mathrm{Aut}_f(K))$ and $r := |A|$. Then G^α (respectively G^β) are K-primitive subgroups of H_1 (respectively H_2) and we may apply induction. This yields

$$|G^\alpha| \leqslant \frac{1}{|Z|} \cdot \log(p) \cdot |U| \cdot \dim_K(U) \cdot r$$

and

$$|G^\beta| \leqslant \frac{1}{|Z|} \cdot \log(p) \cdot |W| \cdot \dim_K(W) \cdot r$$

or $K = \mathbb{F}_7$ and G^α or G^β is isomorphic to $PSp_4(3)$ and U or W is 4-dimensional. Let $\gamma := \alpha \times \beta$. Then the diagram

$$\begin{array}{ccccc} G & \longrightarrow & H_1 \times H_2 & \longrightarrow & H_1 \\ & & \downarrow & & \downarrow \\ & & H_2 & \longrightarrow & \mathrm{Aut}_f(K) \end{array}$$

commutes and one gets $\left|G^\alpha \times G^\beta : G^\gamma\right| \geqslant r$. This yields

$$|G| = |Z| \cdot |G^\gamma| \leqslant \frac{|Z|}{r} \cdot |G^\alpha| \cdot \left|G^\beta\right|.$$

As $2^{n-1} = 1 + (n-1) + \binom{n-1}{2} + \ldots + 1 \geqslant n$ for $n \in \mathbb{N}$, one has $\log(p) \leqslant |Z|$. This yields for the first case

$$|G| \leqslant \frac{\log(p)}{|Z|} \cdot \dim_K(U \otimes_K W) \cdot r \cdot |U| \cdot |W|$$

and the desired result holds. If $G^\alpha = G^\beta = PSp_4(3)$ and U and W are the 4-dimensional modules of $Sp_4(3)$ one can check the inequality by an easy calculation. Now assume that $G^\alpha = PSp_4(3)$ and $\dim_{\mathbb{F}_7}(U) = 4$ and $(G^\beta, W) \not\simeq \left(PSp_4(3), (\mathbb{F}_7)^4\right)$. Then induction implies

$$|G| \leqslant \log(7) \cdot \dim_{\mathbb{F}_7}(W) \cdot |G^\alpha|.$$

Now one uses the estimate $|PSp_4(3)| \leqslant 4 \cdot 7^5$ and the fact that $\dim_{\mathbb{F}_7}(W) \geqslant 2$. This implies $|W| \cdot |G^\alpha| \leqslant 4 \cdot 7^{5+\dim_K(W)} \leqslant \dim_K(U) \cdot 7^{4 \cdot \dim_K(W)}$ and the assertion follows in this case too. So we may assume that V is an absolutely irreducible KN-module for all $N \in \mathcal{N}_G$.

Now assume that for some $N \in \mathcal{N}_G$, V is defined over some proper subfield $K_0 < K$, that is, there exists an irreducible K_0N-module $W \in Irr_{K_0N}(V)$, such that $V \simeq_{KN} K \otimes_{K_0} W$. As V is an absolutely irreducible KN-module W has to be an absolutely irreducible K_0N-module. The same arguments as in the previous case show that

$$\mathrm{End}_{K_0N}(V) \simeq \mathrm{End}_{K_0}(U), \text{ for } U = \mathrm{Hom}_{K_0N}(W, V),$$

and $$N_{GL_{K_0}(V)}(N) \leqslant C_{GL_{K_0}(V)}\left(C_{GL_{K_0}(V)}(N)\right) \circ C_{GL_{K_0}(V)}(N) =: H_2 \circ H_1.$$

where $H_1 := C_{GL_{K_0}(V)}(N) \simeq GL_{K_0}(U)$. As Z is contained in $H_1 = C_{GL_{K_0}(V)}(N)$, one has $H_2 \leqslant C_{GL_{K_0}(V)}(Z) = GL_K(V)$. This implies that $(H_1 \circ H_2) \cap GL_K(V) = H_2 \circ$

$(H_1 \cap GL_K(V))$. But V is an irreducible KN-module and therefore $H_1 \cap GL_K(V) = Z$. Thus one has $G \leqslant (Z \circ GL_{K_0}(W)).\mathrm{Aut}_f(K)$, where the action of $\mathrm{Aut}_f(K)$ is the diagonal one. Now define $A := Im(G \longrightarrow \mathrm{Aut}_f(K))$, $A_0 := Im(G \longrightarrow \mathrm{Aut}_f(K_0))$, $r := |A|$ and $r_0 := |A_0|$. Let $\phi : G \longrightarrow \Gamma L_{K_0}(W)$ be the canonical projection. Then G^ϕ has to be a K_0-primitive subgroup of $\Gamma L_{K_0}(W)$ and we may apply induction as $(\dim_{K_0}(W), |K_0 : \mathbb{F}_p|) < (\dim_K(V), |K : \mathbb{F}_p|)$, that is,

$$|G^\phi| \leqslant \frac{\log(p)}{|K_0^*|} \cdot \dim_{K_0}(W) \cdot |W| \cdot r_0,$$

or $K_0 = \mathbb{F}_7$, $G^\phi \simeq PSp_4(3)$, $W \simeq (\mathbb{F}_7)^4$. But $\ker(\phi) = K^* \rtimes D$, where $D := \mathrm{Fix}_A(K_0)$; in particular $r = |D| \cdot r_0$. In the first case this implies

$$|G| \leqslant \log(p) \cdot \dim_K(V) \cdot \frac{|K^*|}{|K_0^*|} \cdot |W| \cdot r$$

and using the isotony of the function $f(x) = x^n/(x-1)$ for $x \geqslant 2$ this yields the desired inequality. For $G^\phi = S_4(3)$, $W = (\mathbb{F}_7)^4$ one can use the estimate $|G^\phi| \leqslant 4 \cdot 7^5$ to obtain the assertion in this case. So we may assume that for all $N \in \mathcal{N}_G$ the KN-module V is defined over no proper subfield of K.

Let M be a minimal element of $\mathcal{N}_G$. Then M/Z is characteristically simple and either elementary abelian or a direct product of copies of some finite non-abelian simple group X.

Assume that the first case holds and that $M/Z \simeq (\mathbb{Z}_l)^n$. Let L^* be the l-Sylow subgroup of M. Then L^* is of symplectic type (see [**19**, p.75ff]), that is, every abelian characteristic subgroup is cyclic. Define

$$L := \{g \in L^* \mid \mathrm{ord}(g) = l\}, \text{ for } l \text{ odd}$$

and

$$L := \{g \in L^* \mid \mathrm{ord}(g) = 4\}, \text{ for } l = 2.$$

Then L is a characteristic subgroup of M of symplectic type of exponent l, (respectively 4). The structure of L and further information concerning $Z(L)$ and $C_{\mathrm{Aut}(L)}(Z(L))$ can be read from the following table (see [**13**, (4.6.)]):

structure of L	notation	$\lvert Z(L)\rvert$	$C_{Aut(L)}(Z(L))$
$\overbrace{L_0 \circ \ldots \circ L_0}^{m \text{ times}}$	l^{2m+1}, l odd	l	$l^{2m} \rtimes Sp_{2m}(l)$
$\overbrace{D_8 \circ \ldots \circ D_8}^{m \text{ times}}$	2_+^{1+2m}	2	$2^{2m} \rtimes O_{2m}^+(2)$
$\overbrace{D_8 \circ \ldots \circ D_8}^{(m-1) \text{ times}} \circ Q_8$	2_-^{1+2m}	2	$2^{2m} \rtimes O_{2m}^-(2)$
$Z_4 \circ \overbrace{D_4 \circ \ldots \circ D_4}^{m \text{ times}}$	$Z_4 \circ 2^{1+2m}$	4	$2^{2m} \rtimes Sp_{2m}(2)$

Here L_0 denotes the extraspecial group of order l^3 and exponent l, Q_8 the quarternion group and D_8 the dihedral group of order 8. The absolutely irreducible representations of L over a field of characteristic $p \neq l$ are well known (see [**13**, Proposition 4.6.3.]): L has $|Z(L) - 1|$ inequivalent absolutely irreducible representations of degree l^m, where $2m = n$. Further the smallest field over which they can be realised is $\mathbb{F}_{p^e}$, where e is the smallest integer for which $p^e \equiv 1(\operatorname{mod}|Z(L)|)$. Now let $G_0 = G \cap GL_K(V)$. Then

$$G_0 \leqslant N_{GL_K(V)}(L) \leqslant C_{Aut(L)}(Z(L)) =: C.$$

In nearly all cases one has already $|C| \leqslant |V| \cdot \dim_K(V) \cdot \log(p)$. To see this let $q = |K|$. Then it follows that

$$|C| \leqslant (q-1) \cdot l^{2m^2+3m} \leqslant l^m \cdot q^{2m^2+2m+1}.$$

Thus for $l \geqslant 5$, $l = 3$ and $m \geqslant 4$, or $l = 2$ and $m \geqslant 7$, one gets $2 \cdot m^2 + 2 \cdot m + 1 \leqslant l^m$ and therefore $C \leqslant \dim_K(V) \cdot |V|$. Similar arguments show that $|C| \leqslant |V| \cdot \dim_K(V) \cdot \log(p)$ provided $(l, m, q) \neq (3,1,4)$, $(3,1,7)$, $(3,2,4)$, $(2,1,2)$, $(2,2,q)$ and $q = 3,5,7,9$; $(2,3,q)$ and $q = 3,5,7$; $(2,4,3)$, $(2,4,5)$, $(2,5,3)$.

Let $l = 3$. In all three open cases one easily verifies that

$$|C|_{p'} \leqslant |V| \cdot \dim_K(V) \log(p),$$

where $|C|_{p'}$ denotes the p'-part of the group order of C and thus the assertion follows in this case. So from now on we may assume that $l = 2$. Let $d = \left|(\mathbb{Z}_4 \circ 2^{1+2m}) \rtimes Sp_{2m}(2)\right|$. Then $d_{p'} \leqslant |V| \cdot \dim_K(V) \cdot \log(p)$ except the cases $(m, q) = (2,3)$, $(2,5)$, $(2,7)$, $(3,3)$, $(3,5)$, $(4,3)$. These cases now have to be analysed one by one.

Let $(m,q)=(2,7)$. As $|Z(L)|\,|(q-1)$ it follows that $|Z(L)|=2$ and thus

$$C = Z \circ 2_{\pm}^{1+4} \rtimes O_4^{\pm}(2),$$

in particular $|C| \leqslant |V| \cdot \dim_K(V) \cdot \log(p)$.

Let $q=3$. Then the previously mentioned argument shows that

$$C = 2^{1+2m} \rtimes O_{2m}^{\pm}(2)$$

and $|C|_{3'} \leqslant |V| \cdot \dim_K(V) \cdot \log(p)$ except in the cases

$$\begin{aligned} 2_+^{1+6} &\rtimes O_6^+(2) \leqslant GL_8(3) \\ 2_-^{1+8} &\rtimes O_8^-(2) \leqslant GL_{16}(3). \end{aligned}$$

Let $d_{p'}^* = \max\{\,|M|_{p'} \mid M \text{ a maximal subgroup of } C\,\}$. The maximal subgroups of $O_6^+(2)$ (respectively $O_8^-(2)$) can be found in [5] and so $d_{p'}^*$ can be determined in both cases. An easy calculation shows that $d_{p'}^* \leqslant |V| \cdot \dim_K(V) \cdot \log(p)$. This argument can also be used to handle the cases

$$\begin{aligned} G_0 &\leqslant \mathbb{Z}_4 \circ 2^{1+4} \rtimes Sp_4(2) \leqslant GL_4(5) \\ G_0 &\leqslant \mathbb{Z}_4 \circ 2^{1+6} \rtimes Sp_6(2) \leqslant GL_8(5). \end{aligned}$$

This shows that $|G_0| \leqslant |V| \cdot \dim_K(V) \cdot \log(p)$. As $|G/G_0| = \dim_E(K)$ one obtains the desired result in the case that M/Z is elementary abelian. From now on we may assume that each $N \in \mathcal{N}_G$ is non-soluble. Let

$$M/Z = \underbrace{X \times \ldots \times X}_{t \text{ times}},$$

where X denotes some finite simple non-abelian group and $t \geqslant 2$. Further let $Y = Z.X$. As V is an absolutely irreducible $K(Y \times \ldots \times Y)$-module, elementary character theory implies that $V \simeq_{KM} W \otimes \ldots \otimes W$ for some absolutely irreducible KY-module W. As $C_{GL_K(V)}(M) = Z$ it follows that

$$N_{GL_K(V)}(M) \simeq \big(N_{GL_K(W)}(Y) \circ \ldots \circ N_{GL_K(W)}(Y)\big) \rtimes S_t,$$

where S_t denotes the symmetric group on t letters. Let $B := N_{GL_K(W)}(Y) \circ \cdots \circ N_{GL_K(W)}(Y)$ and $H := (G_0B)/B$. Then by assuming that G has maximal order it follows that

$$G_0 \cap B = A \circ \ldots \circ A$$

for some $A \leqslant N_{GL_K(W)}(Y)$. As $Y \leqslant A \leqslant GL_K(W)$ and W is an absolutely irreducible KY-module one gets that A is a K-primitive subgroup of $GL_K(W)$ and we may apply induction.

First let us assume that $K = \mathbb{F}_7$, $W = (\mathbb{F}_7)^4$ and $A = Y \simeq \mathbb{Z}_6 \circ Sp_4(3)$. Then $|G_0| \leqslant (|K|-1) \cdot |PSp_4(3)|^t \cdot t!$ and using the estimates $t! \leqslant 7^{2^t}$ and $|PSp_4(3)| \leqslant 4 \cdot 7^5$ one gets the desired result.

So let us assume that $|A| \leqslant |W| \cdot \dim_K(W) \cdot \log(p)$. Then one obtains

$$|G_0| \leqslant \frac{\log(p)^t}{(|K|-1)^{t-1}} \cdot |W|^t \cdot \dim_K(W)^t \cdot t!.$$

As before one has $\log(p) \leqslant |K| - 1$. Put $q := |K|$. If $q^{a^t} \geqslant q^{at} \cdot t!$ for $a = \dim_K(W)$ the desired inequality holds. Thus let us define

$$E := \{\, (q,a,t) \in \{\, n \in \mathbb{N} \mid n \geqslant 2 \,\} \mid q^{a^t} < q^{at} \cdot t! \}.$$

A lengthy but elementary calculation shows that $E = \{\, (q,2,2) \mid q \geqslant 2\} \cup \{(2,2,3)\}$. But for $(q,a,t) = (2,2,3)$ one gets $G_0 \leqslant GL_2(2) \wr S_3$. Thus G_0 is a $(2,3)$-group and therefore soluble. Here "$\wr$" denotes the wreath product with the permutation representation of S_3 on 3 letters. Thus this case can be excluded by hypothesis. Let us assume that $(a,t) = (2,2)$. This implies

$$G_0 \simeq (A \circ A) \rtimes \mathbb{Z}_2 \leqslant (GL_2(q) \circ GL_2(q)) \rtimes \mathbb{Z}_2$$

for some non-soluble p'-group A of $GL_2(q)$. Now Dickson's Theorem [**9**, p.213] implies that $X \simeq A_5$ and $A \leqslant 2.S_5$. In particular the assertion follows for $q > 19$. The cases which remain to be considered are values for q such that $q \equiv \pm 1 (\mathrm{mod}\, 5)$, $(q, 60) = 1$ and $q \leqslant 19$. Thus $q = 11$ and $q = 19$ has to be analysed some more. For $q = 19$ one can check the desired inequality; for $q = 11$ one has to use additionally that $2.A_5$ is maximal in $GL_2(11)$ (see [**5**]).

So if the assertion were false one must have $t = 1$ and $F^*(G) = Y$ for some quasisimple group Y. So the hypothesis applies. This finishes the proof of the lemma. ∎

Next we have to show that the assertion of Theorem A holds for reduced primitive groups. Therefore we define for any finite simple group X and any set M of prime numbers or zero

$$R_M(X) := \min\{\, n \in \mathbb{N} \mid X \hookrightarrow PGL_n(F), F \text{ a field with } char(F) \in M \,\}$$

to be the minimal faithful projective representation degree over a field whose characteristic lies in M. For simplicity we write $R_p(X) = R_{\{p\}}(X)$. We prove the following lemma:

https://doi.org/10.1017/S0004972700015951 Published online by Cambridge University Press

Lemma 2.2. *Let X be some finite non-abelian simple group and $q = p^f$ some prime power with $(q, |X|) = 1$. Then one has*

$$|\mathrm{Aut}\,(X)| \leqslant R_0(X) \cdot q^{R_0(X)-1} \cdot \log(p)$$

or $X \simeq A_5$, A_6, $L_3(2)$, $PSp_4(3) = U_4(2)$, $U_4(3)$, $\Omega_8^+(2)$.

Proof: It suffices to show that $|\mathrm{Aut}\,(X)| \leqslant R_0(X) \cdot p^{R_0(X)-1} \cdot \log(p)$, where $p = p_X$ is the smallest prime number not dividing $|X|$, that is, $(p, |X|) = 1$. The proof now will be done by a case by case analysis of all finite simple groups.

Let $X = A_k$ be an alternating group. Then for $k \geqslant 7$ one has $R_0(A_k) = k - 1$ (see [**5**, **13**, Proposition 5.3.5]). This yields

$$R_0(X) \cdot p^{R_0(X)-1} \geqslant (k-1) \cdot (k+1)^{k-2} \geqslant k! = |\mathrm{Aut}\,(X)|.$$

Thus the desired inequality holds in this case.

Now let X be sporadic. Then from [5] one can determine $R_0(X)$, which is listed together with p_X in Table 2.

Table 2.

X	M_{11}	M_{12}	M_{22}	M_{23}	M_{24}	J_1	J_2	J_3	J_4
$R_0(X)$	10	10	10	22	23	56	6	18	1333
p_X	7	7	13	13	13	13	11	7	13

X	HS	M^cL	He	Ru	Suz	$O'N$	Co_1	Co_2	Co_3
$R_0(X)$	22	22	51	28	12	342	24	23	23
p_X	13	13	11	11	17	13	17	13	13

X	Fi_{22}	Fi_{23}	Fi'_{24}	HN	Ly	Th	BM	M
$R_0(X)$	22	782	783	133	2480	248	4371	196883
p_X	17	19	19	13	13	11	29	37

Then in all cases one can check the inequalitiy $|\mathrm{Aut}\,(X)| \leqslant R_0(X) \cdot p_X^{R_0(X)-1} \cdot \log(p_X)$.

Finally let X be a simple group of Lie type. Now we may apply a theorem of Landazuri and Seitz [**14**] which gives a lower bound $e(X)$ for the minimal faithful

Table 3.

X		$e(X)$	exceptions
$L_2(s)$		$\frac{s-1}{(2,s-1)}$	$L_2(4), L_2(9)$
$L_k(s)$	$k \geqslant 3$	$s^{k-1}-1$	$L_3(2), L_3(4)$
$PSp_{2k}(s), k \geqslant 2$	s odd s even	$1/2\,(s^k-1)$ $1/2\,(s^{k-1}-1)(s-1)$	$Sp_4(2)', Sp_6(2)$
$U_k(s), k \geqslant 3$	k odd k even	$s(s^{k-1}-1)/(s+1)$ $(s^k-1)/(s+1)$	$U_4(2), U_4(3)$
$P\Omega^+_{2k}(s), k \geqslant 4$	$s \neq 2,3,5$ $s = 2,3,5$	$(s^{k-1}-1)(s^{k-2}-1)$ $s^{k-2}(s^{k-1}-1)$	$\Omega^+_8(2)$
$P\Omega^-_{2k}(s), k \geqslant 4$		$(s^{k-1}+1)(s^{k-2}-1)$	
$P\Omega_{2k+1}(s), k \geqslant 3$	s odd, $s > 5$ $s = 3,5$	$s^{2(k-1)}-1$ $s^{k-1}(s^{k-1}-1)$	$P\Omega_7(3)$
$E_6(s)$		$s^9(s^2-1)$	
$E_7(s)$		$s^{15}(s^2-1)$	
$E_8(s)$		$s^{27}(s^2-1)$	
$F_4(s)$	s odd s even	$s^6(s^2-1)^*$ $1/2\,s^7(s^3-1)(s-1)$	$F_4(2)$
$G_2(s)$		$s(s^2-1)$	$G_2(3), G_2(4)$
${}^2E_6(s)$		$s^9(s^2-1)^*$	
${}^3D_4(s)$		$s^3(s^2-1)$	
${}^2B_2(s)$		$\sqrt{s/2}\,(s-1)$	${}^2B_2(8)$
${}^2G_2(s)$		$s(s-1)$	
${}^2F_4(s)$		$\sqrt{s/2}\,s^4(s-1)$	${}^2F_4(2)'$

The * indicates deviations to the list of [14].

projective representation degree in non-natural characteristic. In Table 3 we give an overview of these lower bounds. The table can be found in this form in [**13**, Table 5.3.A].

We give a complete proof for the case $X \simeq L_k(s)$. The same arguments yield the

https://doi.org/10.1017/S0004972700015951 Published online by Cambridge University Press

desired result in the other cases. First let $k \geqslant 3$. Then $R_0(X) \geqslant s^{k-1} - 1$, $p = p_X \geqslant 5$ and $|\mathrm{Aut}\,(X)| = |X| \cdot (k, s-1) \cdot f_0 \cdot 2$, where $s = s_0^{f_0}$ for some prime number s_0; in particular one has $|\mathrm{Aut}\,(X)| \leqslant s^{k^2}$. Now we claim that

$$s^{k^2} \leqslant 5^{s^{k-1}-2} \cdot \left(s^{k-1} - 1\right)$$

provided $(s,k) \neq (2,3)$. Let us assume that the opposite holds. This yields that there exist s, k such that $s^{k^2-k+2} > 5^{s^{k-1}-2}$ or

$$(s-1) \cdot \left(k^2 - k + 2\right) > 2 \cdot s^{k-1} - 4.$$

For $k = 3$ this implies $s^2 - 4 \cdot s + 2 < 0$ and thus $s = 2$ or $s = 3$. For $k = 4$ one gets $s^3 - 7 \cdot s + 5 < 0$ and therefore $s = 2$. For $k \geqslant 5$ one can use the fact that $f(x) = \left(x^{k-1} - 2\right)/(x-1)$ is isotonic for $x \geqslant 2$, and this yields $k^2 - k + 2 > 2^k - 4$, a contradiction for $k \geqslant 5$. An easy calculation shows that only the case $(s,k) = (2,3)$ remains and the claim is proved. For $X = L_3(4)$ one can use the character table (see [5]) to deduce that $R_0(L_3(4)) = 6$ and $p = 11$. Then one easily checks the assertion of Lemma 2.2. It remains to consider the case $k = 2$. First let $s > 13$. Then $2^s > 4 \cdot s^3$ and therefore

$$\frac{1}{2} \cdot 5^{(s-3)/2} \cdot (s-1) \cdot \log(p) > 2^{s-3} \cdot (s-1) > \frac{1}{2} \cdot s^3 \cdot (s-1) \geqslant |\mathrm{Aut}\,(X)|.$$

As $L_2(2)$ and $L_2(3)$ are soluble, $L_2(4) = L_2(5) = A_5$, $L_2(7) = L_3(2)$, $L_2(9) = A_6$; only the cases $X = L_2(8)$, $L_2(11)$, $L_2(13)$ remain. For $X = L_2(8)$ one has $R_0(X) = 8$, $p_X = 5$, for $X = L_2(11)$ one gets $R_0(X) = 5$, $p_X = 7$ and for $X = L_2(13)$, $R_0(X) = 6$ and $p = 5$ [5] and the assertion follows by elementary calculations. This proves the lemma for groups of type A_l. For finite simple groups of different Lie-type one can use the estimate $e(X)$ given in Table 3. In these cases one obtains as exceptions the groups $X = PSp_4(3) = U_4(2)$, $U_4(3)$ and $\Omega_8^+(2)$. $\square$

Proof of Theorem A: Let K be a finite field of characteristic p and let $G \leqslant \Gamma L_K(V)$ be a reduced primitive p'-group. Then $H := F^*(G) \leqslant GL_K(V)$ is a quasisimple group and V is an absolutely irreducible KH-module defined over no proper subfield of K. Let $G_0 := G \cap GL_K(V)$ and $X := H/Z$. Then $|G : G_0| \leqslant \left|K : \mathrm{End}_{\mathbf{F}_p}(V)\right|$. As $G_0/Z \leqslant \mathrm{Aut}\,(X)$ it follows from Lemma 2.2. that either

$$|G_0| \leqslant |V| \cdot \dim_K(V) \cdot \log(p)$$

or $H/Z \simeq A_5$, A_6, $L_3(2)$, $PSp_4(3)$, $U_4(3)$ or $\Omega_8^+(2)$. Let us assume that

$$|\mathrm{Aut}\,(H/Z)| > |K|^{\dim_K(V)-1} \cdot \dim_K(V) \cdot \log(p).$$

Then an easy calculation shows that one of the following must hold:

(i) $X = A_5$, $\dim_K(V) = 2$, $|K| = 7, 11, 13, 17$,
(ii) $X = A_6$, $\dim_K(V) = 3$, $|K| = 7, 11$,
(iii) $X = L_2(7) = L_3(2)$, $\dim_K(V) = 3$, $|K| = 5$,
(iv) $X = U_4(2) = PSp_4(3)$, $\dim_K(V) = 4$, $|K| = 7, 11, 13$,
$\dim_K(V) = 5$, $|K| = 7$,
(v) $X = U_4(3)$, $\dim_K(V) = 6$, $|K| = 11, 13$,
(vi) $X = \Omega_8^+(2)$, $\dim_K(V) = 8$, $|K| = 11$.

Let $X = A_5$. The group A_5 is a subgroup of $L_2(q)$ if and only if $5 \big| q$ or $q \equiv \pm 1 (\bmod 5)$ (see [**9**, p.213]). So only the case $q = 11$ remains to be considered. But A_5 is a maximal subgroup of $PGL_2(11)$ (see [5]) and therefore one gets

$$|G_0| \leqslant 600 < 11^2 \cdot 2 \cdot \log(11).$$

The group A_6 is not isomorphic to a subgroup of $L_3(7)$ or $L_3(11)$ (see [5]) and thus we may exclude the case $X = A_6$. The same holds for $L_3(2)$ as $L_3(2)$ is not a subgroup of $L_3(5)$ (see [5]).

Let $X = PSp_4(3)$. Then $PSp_4(3)$ is a subgroup of $L_4(p)$ if and only if $p \equiv 1 (\bmod 6)$ (see [**12**]). This excludes the case $(n, p) = (4, 11)$. The character table of $GSp_4(3)$ (see [5]) shows that $N_{PGL_4(p)}(X) = X$. Thus one has for $(n, p) = (4, 13)$

$$|G_0| \leqslant 12 \cdot |X| < 13^4 \cdot 4 \cdot \log(13).$$

The character table also shows that $N_{PGL_5(7)}(X) = X$ and therefore

$$|G_0| \leqslant 6 \cdot |X| < 7^5 \cdot 5 \cdot \log(7).$$

Let $X = U_4(3)$. $U_4(3)$ has a projective 6-dimensional representation over an algebraically closed field of characteristic 0. But the linear representation is only defined for $6.U_4(3)$ (see [5]). Thus one has $6 \big| |Z| = q - 1$ and this excludes the case $q = 11$. The character table also shows that $\big(N_{PGL_6(13)}(X)\big)/X$ is a subgroup of $\mathbb{Z}_2$, so one has

$$|G_0| \leqslant 24 \cdot |X| < 13^6 \cdot 6 \cdot \log(13).$$

Let $X = \Omega_8^+(2)$. Then X has a 8-dimensional projective representation over $\mathbb{F}_{11}$. But the corresponding linear representation is only defined for $2.\Omega_8^+(2)$. Thus one has $\big(N_{PGL_8(11)}(X)\big)/X = \mathbb{Z}_2$ and this yields

$$|G_0| \leqslant 12 \cdot |X| < 11^8 \cdot 8 \cdot \log(11).$$

Thus we have proved the assertion of Theorem A for all reduced primitive groups and the only exception to the estimate is the group $Sp_4(3)$ acting on $V = \mathbb{F}_7^4$. But then Lemma 2.1. implies that the estimate holds for all groups except $G = Sp_4(3)$ acting on $V = \mathbb{F}_7^4$ and Theorem A is proved. $\square$

https://doi.org/10.1017/S0004972700015951 Published online by Cambridge University Press

3. The Distribution of p-singular Elements in Finite Groups

In this section we shall prove Theorem B. As in the previous section we divide the proof in two parts: The first part is a reduction to the almost simple case and in the second we prove a slightly stronger version of Theorem B for almost simple groups. For the reduction part we use some well-known result of Easdown and Praeger which will be stated now.

Proposition 3.1. (See [7, Proposition 1.3.]) Let G be a finite group and N be an abelian (elementary abelian) normal subgroup of G. Then there exists an abelian (elementary abelian) normal subgroup L of G containing N having the same prime divisors as N such that $\mu(G/L) \leqslant \mu(G)$.

For $N \trianglelefteq G$ one has $|\mathcal{A}_p(G)| \leqslant |N| \cdot |\mathcal{A}_p(G/N)| + |\mathcal{A}_p(N)|$. For this reason Proposition 3.1. will be an important tool in the reduction step. Let E be some non-abelian finite simple group. We put $Out(E) := (\mathrm{Aut}\,(E))/E$. For our purpose we need the following facts about minimal representation degrees:

Proposition 3.2.

(a) *Let $H = E_1 \times \ldots \times E_r$ for some finite non-abelian simple groups E_i. Then one has*

$$\mu(H) = \mu(E_1) + \ldots + \mu(E_r).$$

(b) *Let E be some finite simple group. Then $|Out(E)| \leqslant \mu(E)$.*

(c) *Let S be a normal subgroup of G with*

$$S \simeq \underbrace{E_1 \times \ldots \times E_1}_{n_1 \text{times}} \times \ldots \times \underbrace{E_r \times \ldots \times E_r}_{n_r \text{times}},$$

where the E_i's are finite simple groups and $E_i \not\simeq E_j$, for all $i \neq j$. Assume further that $C_G(S) = 1$. Then

$$\mu\left(\frac{G}{S}\right) \leqslant \mu(S) \leqslant \mu(G).$$

Proof: (a) See [7, Theorem 3.1]

(b) By the classification of finite simple groups it suffices to consider a finite simple group of Lie type G. For p-subgroups $P \leqslant S_n$ it is shown in [2] that $\left|P/[P,P]\right| \leqslant p^{n/p}$. This implies that $P/(\mathrm{Frat}(P))$ is elementary abelian of rank less than or equal to $(\mu(P))/p$. Thus one gets $\mu(G) \geqslant p \cdot f \cdot l$, where $p^f = q$ is the order of the field of definition and l is the Lie rank of the corresponding simple algebraic group, for

https://doi.org/10.1017/S0004972700015951 Published online by Cambridge University Press

example, for $G = {}^2B_2(2^{2k+1})$ we let $f = (2k+1)/2$. By a theorem of Steinberg one knows that $|Out(G)| = d \cdot f \cdot g$, where d denotes the order of the diagonal, f the order of the field automorphism and g the order of the graph automorphisms. This argument therefore shows that $Out(G) \leqslant \mu(G)$ provided $G \neq A_l(2^k)$, $l \geqslant 2$; ${}^2A_l(2^k)$, $l \geqslant 2$, $D_4(3^k)$. For these remaining cases one may consult Table 5.2.A of [13] to verify that $|Out(G)| \leqslant \mu(G)$.

(c) Put

$$N_i := \underbrace{E_i \times \cdot \times E_i}_{n_i \text{times}}.$$

Then one has

$$\operatorname{Aut}(S) = \prod_{i=1}^{r} \operatorname{Aut}(N_i) = \prod_{i=1}^{r} \operatorname{Aut}(E_i) \wr S_{n_i}.$$

This yields

$$\frac{G}{S} \leqslant \Big(\prod_{i=1}^{r} \operatorname{Aut}(N_i)\Big)/S \leqslant \prod_{i=1}^{r} \frac{\operatorname{Aut}(N_i)}{N_i} \simeq \prod_{i=1}^{r} Out(N_i) \wr S_{n_i}.$$

Here the wreath product is build via the canonical permutation representation of S_n. Now applying part (c) one gets

$$\mu\Big(\frac{G}{S}\Big) \leqslant \sum_{i=1}^{r} \mu(Out(E_i) \wr S_{n_i}) \leqslant \sum_{i=1}^{r} n_i \cdot |Out(E_i)| \leqslant \sum_{i=1}^{r} n_i \cdot \mu(E_i) = \mu(S).$$

□

We prove the following intermediate result to Theorem B.

Lemma 3.3. *Let $G \leqslant S_n$ be a finite group, p a prime divisor of $|G|$ and $n = \mu(G)$. We assume that for all simple groups X and all almost simple groups F with $X \leqslant S \leqslant \operatorname{Aut}(X)$, one has*

$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{2 \cdot \mu(X) \cdot \log(\mu(X))}$$

for all non-trivial prime divisors of $|X|$. Then one has

$$\frac{|\mathcal{A}_p(G)|}{|G|} \geqslant \frac{1}{2 \cdot \mu(G) \cdot \log(\mu(G))}.$$

Proof: Let $G \leqslant Sym(\Omega)$, $|\Omega| = n$. We proceed by induction on $|G|$.

Assume that G acts intransitively on Ω and let $B_1, \dots, B_k$ be the orbits of G. Then G does not act faithfully on any orbit as $|B_i| < n$. Further G embeds in the direct product of its transitive constituents, that is, $G \leqslant \prod_{i=1}^{k} \left(G/G_{(B_i)}\right)$. So there exists an $i \in \{1, \dots, k\}$ such that $p \,\Big|\, \left|G/\left(G_{(B_i)}\right)\right|$. Using induction we may conclude that

$$\frac{|\mathcal{A}_p(G)|}{|G|} \geqslant \frac{|G_{(B_i)}|\,|\mathcal{A}_p(G/G_{(B_i)})|}{|G_{(B_i)}|\,|G/G_{(B_i)}|} \geqslant \frac{1}{2 \cdot \mu(G/G_{(B_i)}) \cdot \log\left(\mu(G/G_{(B_i)})\right)}$$

and the assertion holds as $\mu(G) > |B_i| \geqslant \mu\left(G(G_{(B_i)})\right)$. Thus we may assume that G is acting transitively on Ω.

Assume G has an abelian normal subgroup N whose order is coprime to p. Using Proposition 3.1 we find an abelian normal subgroup L of G whose order is coprime to p such that $\mu(G/L) \leqslant \mu(G)$. So induction implies

$$\frac{|\mathcal{A}_p(G)|}{|G|} \geqslant \frac{|L|\,|\mathcal{A}_p(G/L)|}{|L|\,|G/L|} \geqslant \frac{1}{2 \cdot \mu(G/L) \cdot \log\left(\mu(G/L)\right)} \geqslant \frac{1}{2 \cdot \mu(G) \cdot \log\left(\mu(G)\right)}$$

and we may assume that $O_{p'}(G) = 1$.

Now assume that G has an elementary abelian normal p-subgroup N. By Proposition 3.1. we may assume that $\mu(G/N) \leqslant \mu(G)$. If $p \big| |G/N|$ one concludes as before. So we may assume that $\left(|N|, |G/N|\right) = 1$. By the Schur-Zassenhaus Theorem there exists a complement C to N in G. As $|C|$ is coprime to p, N is a completely reducible $\mathbb{F}_p C$-module, that is, $N \simeq N_1 \times \dots \times N_r$ and each N_i is a minimal $\mathbb{F}_p C$-submodule of N. If $r > 1$ then N_1 is complementable by $U := N_2 \times \dots \times N_r \times C$ and $p \big| |G/N_1|$. As $G/N_1 \simeq U \leqslant G$, one has $\mu(G/N_1) \leqslant \mu(G)$ and one may conclude as before. So $r = 1$ and $N = Fit(G)$, the largest nilpotent normal subgroup of G. Let H be the stabiliser of an element $\alpha \in \Omega$.

Assume that $M := N \cap H \neq 1$. Then $M \neq N$, because $\mathrm{Core}_G(H) = 1$. N is a completely reducible $\mathbf{F}_p H$-module, so let M_0 be an H-invariant complement of M in N. Put $U := H \cdot M_0 < G$ and we get $|M_0| < |G : H| = n$. As $\mathcal{A}_p(U) \subseteq \mathcal{A}_p(G)$ it follows that

$$\frac{|\mathcal{A}_p(G)|}{|G|} \geqslant \frac{|\mathcal{A}_p(U)|}{|U|} \cdot \frac{|H|\,|M_0|}{|G|} = \frac{|\mathcal{A}_p(U)|}{|U|} \cdot \frac{|M_0|}{n}.$$

But $p \big| |U/(\mathrm{Core}_U(H))|$ and

$$\mu(U/\,\mathrm{Core}_U(H)) \leqslant |U : H| = |M_0|.$$

If we use the fact that $|\mathcal{A}_p(U)| \geqslant |\mathrm{Core}_U(H)|\,|\mathcal{A}_p(U/\,\mathrm{Core}_U(H))|$ and apply the induction hypothesis for $U/(\mathrm{Core}_U(H))$ we get

$$\frac{|\mathcal{A}_p(G)|}{|G|} \geqslant \frac{1}{2 \cdot |M_0| \cdot \log\left(|M_0|\right)} \cdot \frac{|M_0|}{n}$$

and the desired result follows by isotony.

So let us assume that $H \cap N = 1$. Then $|G| \geqslant |H|\,|N|$ and $n \geqslant |N|$. Since p does not divide $|G/N|$, N has a complement S in G. Put $C = C_S(N)$ then we have $C \triangleleft G$ and G/C acts faithfully and $\mathbb{F}_p$-linearly on N. Then $\mu(G/C) \leqslant |N| \leqslant n$ and $p \big| |G/C|$. So if $C \neq 1$ we may apply induction again and obtain the desired result. Thus we may assume that $C = 1$. Then N is a faithful and irreducible $\mathbb{F}_p S$-module and it is a well-known fact that S is a subgroup of the wreath product $GL(\beta, p) \wr S_r$, where $|N| = p^\alpha = p^{\beta \cdot r}$ [18]. If S does not act $\mathbb{F}_p$-primitively on N one has $\beta < \alpha$. In this case it follows either $(\alpha, p) = (2,2), G \simeq A_4$ and $S \simeq \mathbb{Z}_3$ acts primitively on $N \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ or

$$n = \mu(G) \leqslant r \cdot p^\beta < p^\alpha \leqslant n,$$

a contradiction. So S is a $\mathbb{F}_p$-linear p'-group acting on the $\mathbb{F}_p$-vector space N and Theorem A applies. The following two cases arise: Either $|S| \leqslant |N| \cdot \log(|N|)$ so that

$$\frac{|\mathcal{A}_p(G)|}{|G|} \geqslant \frac{(|N|-1)}{|N|} \cdot \frac{1}{|S|} \geqslant \frac{1}{2 \cdot |N| \cdot \log(|N|)}$$

or $S \leqslant \mathbb{Z}_6 \circ Sp_4(3)$ and $|N| = 7^4$.

In the latter case one has $S \simeq A \times Sp_4(3)$ where $A \simeq \mathbb{Z}_3$ or $A = 1$. From the list of maximal subgroups of $Sp_4(3)$ [5] we conclude that $\mu(N \rtimes S) = 280 \cdot |A|$. From the character table of $Sp_4(3)$ we can read off the characteristic polynomial of the conjugacy class $3A$ which equals $(x^2 + x + 1)(x-1)^2$. This shows that for an element g of this conjugacy class one gets $|C_N(g)| = 49$ and so one has at least 23040 many elements of order 21 in $N \rtimes Sp_4(3)$. This yields the desired inequality in this case too.

So we may assume that $Fit(G) = 1$. Let $S = soc(G) = L_1 \times \ldots \times L_r$, where L_i is a minimal non-abelian normal subgroup of G, that is, a direct product of n_i copies of a non-abelian simple group E_i. Since the Fitting group of G is trivial, S equals the generalised Fitting subgroup, in particular $C_G(S) = 1$. If $p \big| |G/S|$ one can use Proposition 3.2.(c) and apply induction to obtain the desired inequality. For $p \nmid |G/S|$ we may assume without loss of generality that $p \big| |L_1|$, in particular $p \big| |E_1|$. Put

$$\begin{aligned} C_1 &= C_G(L_1), \\ N/C_1 &= N_{G/C_1}(E_1 C_1/C_1) \end{aligned}$$

and

$$C_2/C_1 = C_{N/C_1}(E_1 C_1/C_1).$$

So G/C_1 acts transitively and faithfully on the direct factors of $L_1 C_1/C_1 \simeq L_1$ isomorphic to E_1, for example,

$$|G/C_1| = |G/C_1 : N/C_1|\,|N/C_1| = n_1\,|N/C_1|.$$

https://doi.org/10.1017/S0004972700015951 Published online by Cambridge University Press

Since N/C_2 is a quasisimple group containing $E_1C_2/C_2 \simeq E_1$ we may apply the hypothesis to conclude that

$$\frac{|\mathcal{A}_p(N/C_2)|}{|N/C_2|} \geqslant \frac{1}{2\cdot\mu(E_1)\cdot\log(\mu(E_1))}.$$

This yields

$$\begin{aligned}\frac{|\mathcal{A}_p(G)|}{|G|} &\geqslant \frac{|\mathcal{A}_p(G/C_1)|}{|G/C_1|} \geqslant \frac{1}{n_1}\,\frac{|C_2/C_1|\,|\mathcal{A}_p(N/C_2)|}{|C_2/C_1|\,|N/C_2|}\\ &\geqslant \frac{1}{n_1}\cdot\frac{1}{2\cdot\mu(E_1)\cdot\log(\mu(E_1))} \geqslant \frac{1}{2\cdot\mu(G)\cdot\log(\mu(G))}\end{aligned}$$

and the lemma is proved. ∎

4. The Distribution of p-singular Elements in Quasisimple Groups

The results we prove in this section make use of the classification of finite simple groups using the completeness of the list, the character tables for some simple groups as reported in the Atlas, [5], and bounds on the orders of maximal subgroups of the simple groups. To complete the proof of Theorem B it suffices to prove the following lemma.

Lemma 4.1. *Let S be a quasisimple group, that is, $X \leqslant S \leqslant \mathrm{Aut}(X)$ and X is a finite non-abelian simple group. Let p be a prime divisor of $|X|$. Then the following inequality holds*

$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{2\cdot\mu(X)\cdot\log(\mu(X))}.$$

For $X \neq A_6$, $L_{l+1}(q)$, $U_4(5)$, $U_4(7)$, $P\Omega_8^+(4)$, $P\Omega_8^+(5)$ this bound can be improved to

$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{\mu(X)}.$$

Proof: The proof of Lemma 4.1 will be done in four steps. First we consider the case when X is an alternating group. Then $X = L_n(q)$ and X a finite group of Lie type is treated. Finally we have to look at the 26 sporadic groups.

Let $X \simeq A_n$. Then for $n \neq 6$ one has $S = A_n$, S_n. Each element $x \in S$ has a unique representation as a product of disjoint cycles, that is, $x = x_1 \cdots x_r$, such that $supp(x_i) \cap supp(x_j) = \emptyset$ for $i \neq j$. The prime p divides $\mathrm{ord}(x)$ if and only if there exists an i such that $p \big| |supp(x_i)|$. For $S = S_n$ we can count the number of elements $x = x_1x_2$ where $supp(x_1) \cap supp(x_2) = \emptyset$, $1 \in supp(x_1)$, $\mathrm{ord}(x_1) = p$. One gets

$$\mathcal{A}_p(S_n) \geqslant \binom{n-1}{p-1}\cdot(p-1)!\cdot(n-p)! = (n-1)!.$$

With a similar procedure one concludes that $\mathcal{A}_p(A_n) \geqslant (n-1)/2!$. As $\mu(A_n) = n$ the assertion follows in this case. For $S \leqslant \mathrm{Aut}(A_6)$ one uses $\mathcal{A}_p(A_6) \subseteq \mathcal{A}_p(S)$.

In the following we consider quasisimple groups S where X is a finite group of Lie type. Therefore we recall some well known facts about finite groups of Lie type. We use substantially the same notation as in [3] and [4]. Let $\mathbf{G}$ be an algebraic group and F a Frobenius automorphism of $\mathbf{G}$. Then $\mathbf{G}^F$ will denote the finite group of Lie type obtained as the fixed point set of F, that is, $\mathbf{G}^F = \{g \in \mathbf{G} \mid F(g) = g\}$. An element $g \in \mathbf{G}$ is called a *regular* element of $\mathbf{G}$ if the dimension of $C_{\mathbf{G}}(g)$ equals the rank of $\mathbf{G}$, which is the dimension of a maximal torus of $\mathbf{G}$. ▯

Proposition 4.2. (See [4, (5.1.9)]) *Let $\mathbf{G}$ be a connected, reductive group and F a Frobenius automorphism of $\mathbf{G}$. Then $\mathbf{G}^F$ contains $\left(|\mathbf{G}^F|\right)\Big/\left(\left|(Z^0)^F\right| q^l\right)$ regular unipotent elements, where Z^0 denotes the connected component of the centre of $\mathbf{G}$, l is the semisimple rank of $\mathbf{G}$ and q is defined as in* [4, p.35].

Proposition 4.3. (See [4, (6.6.1)]) *Let $\mathbf{G}$ be a connected, reductive group and F a Frobenius automorphism of $\mathbf{G}$. Then the number of unipotent elements in $\mathbf{G}^F$ is $\left|\mathbf{G}^F\right|_p^2$.*

Now consider the quasisimple group S where $L_{l+1}(q) \leqslant S \leqslant \mathrm{Aut}(L_{l+1}(q))$, $q = \pi^f$.

Let $X = L_2(q)$, $q = \pi^f$. A famous theorem of Galois asserts that $\mu(X) = q+1$, or X is one of the following [9, p.214]: $L_2(2)$, $L_2(3)$, $L_2(5)$, $L_2(7)$, $L_2(9)$, $L_2(11)$. The groups $L_2(2)$ and $L_2(3)$ are soluble and therefore may be discarded. Further $L_2(5) \simeq A_5$, $L_2(9) \simeq A_6$ have already been considered. The group $L_2(7) \simeq L_3(2)$ will be discussed in the next paragraph. Thus the only group which has to be considered separately is $X = L_2(11)$. In this case one has $\mu(L_2(11)) = 11$.

Therefore let us assume that $X = L_2(q)$, $q \neq 2,3,5,7,9,11$. If $p = \pi$ there exist $(q+1)$ trivial intersecting Sylow p-subgroups of X. So

$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{(2,q-1)\cdot f} \cdot \frac{|\mathcal{A}_p(X)|}{|X|} \geqslant \frac{1}{q\cdot f} > \frac{1}{\mu(X)\cdot \log(\mu(X))}.$$

Let $p \neq \pi$. Then there exists a cyclic self-centralising subgroup T of order $(q+1)/d$ or $(q-1)/d$ where $d = (2,q-1)$, such that $p \big| |T|$. This implies

$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{d\cdot f} \cdot \frac{|\mathcal{A}_p(X)|}{|X|} \geqslant \frac{1}{(q+1)\cdot f} \geqslant \frac{1}{\mu(X)\cdot \log(\mu(X))}.$$

For $X = L_2(11)$ one can use the same arguments and this yields

$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{2\cdot \mu(X)\cdot \log(\mu(X))}$$

in this case.

Now assume $X = L_{l+1}(q)$, $l > 1$, $q = \pi^f$. If one excludes the case $X = L_4(2) \simeq A_8$ which was already treated before one gets for $l > 1$

$$\mu(L_{l+1}(q)) = \frac{(q^{l+1}-1)}{(q-1)}.$$

This result is based on the work of Cooperstein [**6**] and Patton [**17**] and is reported in full detail in [**13**, Table 5.2.A].

Let $p = \pi$. As $L_{l+1}(q) \simeq \mathbf{G}^F/Z(\mathbf{G}^F)$, where $\mathbf{G}$ is a simply connected algebraic group of type A_l, one may apply Proposition 4.3 to deduce that in $\mathbf{G}^F$ and therefore in X there are at least $|\mathbf{G}^F|_p^2$ elements of p-power order. This yields

$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{2\cdot(q-1,l+1)\cdot f} \cdot \frac{|\mathcal{A}_p(X)|}{|X|} \geqslant \frac{1}{2\cdot f} \cdot \frac{|\mathbf{G}^F|_p}{|\mathbf{G}^F|_{p'}}.$$

But
$$\frac{|\mathbf{G}^F|_p}{|\mathbf{G}^F|_{p'}} = \frac{q^{l(l+1)/2}}{(q^2-1)\cdot \ldots \cdot (q^{l+1}-1)} \geqslant \frac{1}{q^l}$$

and thus
$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{2\cdot f} \cdot \frac{1}{\mu(X)} \geqslant \frac{1}{2\cdot \mu(X)\cdot \log(\mu(X))}.$$

For $p \neq \pi$ we have to consider three cases: (1) $p \big| |Z(\mathbf{G}^F)|$, (2) $p | (q-1)$, but $p \nmid |Z(\mathbf{G}^F)|$ and (3) $p \nmid (q-1)$. Let $k = \min\{ m \in \mathbb{N} \mid p | q^m - 1\}$. By Λ we denote a partition of $l+1$ consisting of two integers r_1 and r_2 such that $l+1 = r_1 + r_2$. To Λ there corresponds a decomposition $V \simeq V_1 \oplus V_2$, where $\dim_{\mathbb{F}_q}(V_i) = r_i$, for $i = 1,2$.

Assume that (2) or (3) holds. Then there exists a maximal torus T_Λ of $SL_{l+1}(q)$ and an element $t \in T_\Lambda$ such that for $T_0 := \langle t \rangle$:

(a) $p | \operatorname{ord}(t)$;

(b) There exist exactly two non-trivial irreducible $\mathbb{F}_q T_0$-submodules V_1 and V_2 of V such that $\dim_{\mathbb{F}_q}(V_i) = r_i$;

(c) $C_{SL_{\mathbb{F}_q}(V)}(t) = T_\Lambda$.

If $k = 1$, that is, $p | (q-1)$, there exists a cyclic torus T_Λ corresponding to the partition $\Lambda = (l,1)$ which leaves invariant a vector subspace V_1 of dimension l and a one dimensional subspace V_2. With an appropriate base the generator t of the torus T_Λ corresponds to a matrix of the form

$$x = \begin{pmatrix} s & 0 \\ 0 & det(s)^{-1} \end{pmatrix},$$

where $\langle s \rangle$ is a Singer-cycle on V_1 (see [**9**, p.187f]). V_1 and V_2 are non-isomorphic irreducible $\mathbb{F}_q T_0$-submodules of V, and therefore the only non-trivial $\mathbb{F}_q T_0$-submodules of V.

If $k \geqslant 2$, then $p\big|(q^k-1)/(q-1)$ and p does not divide q^m-1 for all $m<k$. Consider the torus T_Λ^* of $GL_{l+1}(q)$ corresponding to the partition $\Lambda=(k,l+1-k)$: Let $V_1 \simeq \mathbb{F}_{q^k}$, $T_1 \simeq \mathbb{F}_{q^k}^*$ and $V_2 \simeq \mathbb{F}_{q^{l+1-k}}$, $T_2 \simeq \mathbb{F}_{q^{l+1-k}}^*$ and define $T_\Lambda^* := T_1 \times T_2$. If $l+1-k=1$ we are done with a similar argument as for $k=1$, so assume $k \neq l$. Thus $l+1-k>1$, in particular $T_2 \cap SL_{l+1-k}(q) \neq 1$. Denote by t_2 a generator of $T_2 \cap SL_{l+1-k}(q)$. So t_2 acts irreducibly on V_2. Let t_1 be an element of order p in the torus $T_1 \cap SL_k(q)$ of $SL_k(q)$. The choice of k implies that V_1 is an irreducible $\mathbb{F}_q\langle t_1\rangle$-module. Let $t := t_1^\alpha \times t_2^\beta \in T_\Lambda \cap SL_{l+1}(q)$, where $(\alpha,p)=1$, $(\beta,\mathrm{ord}(t_2))=1$, and $T_0 := \langle t\rangle$. Then for all choices of α and β, V_1 and V_2 are irreducible $\mathbb{F}_q T_0$ submodules of V. We claim that we can choose α and β such that V_1 and V_2 are non equivalent $\mathbb{F}_q T_0$-modules.

If $l+1-k \neq k$ then obviously V_1 is not isomorphic to V_2 as an $\mathbb{F}_q T_0$-module. So assume that $l+1=2k$. There exist $(p-1)/k$ non-equivalent irreducible representations of $\langle t_1\rangle$. So if $V_1 \simeq_{\mathbb{F}_q T_0} V_2$ for all choices of α and β one gets $1+k=p$. As the images of $T_0 \longrightarrow GL_{\mathbb{F}_q}(V_1)$ and $T_0 \longrightarrow GL_{\mathbb{F}_q}(V_2)$ must have the same order for $V_1 \simeq_{\mathbb{F}_q T_0} V_2$ this yields $p=\big(q^{p-1}-1\big)/(q-1)$. So $\big(q^{p-1}-1\big)/(q-1)$ is a prime number and thus $p-1$ is a prime. This implies $p=3$, $k=2$, $q=2$ and $X=L_4(2)$ which was excluded by hypothesis and the claim is proved. Thus in both cases (2) and (3) one finds a maximal torus $T_\Lambda := T_\Lambda^* \cap SL_{l+1}(q)$ and an element $t \in T_\Lambda$ satisfying (a) and (b). But if V_1 and V_2 are the only irreducible $\mathbb{F}_q T_0$-modules it follows easily that $\mathrm{Hom}_{\mathbb{F}_q T_0}(V,V) \simeq \mathbb{F}_{q^k} \oplus \mathbb{F}_{q^{l+1-k}}$ and thus $C_{SL_{\mathbb{F}_q}(V)}(t) = T_\Lambda$. In particular, if $\tilde{t}$ denotes the image of t in $L_{l+1}(q)$ one has

$$\left|C_{L_{l+1}(q)}\big(\tilde{t}\big)\right| = \frac{1}{(l+1,q-1)\cdot(q-1)}\cdot\left(q^{r_1}-1\right)\cdot\left(q^{r_2}-1\right).$$

This yields that

$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{2\cdot(l+1,q-1)\cdot f}\cdot\frac{|\mathcal{A}_p(X)|}{|X|} \geqslant \frac{1}{2\cdot(l+1,q-1)\cdot f}\cdot\frac{1}{\left|C_X\big(\tilde{t}\big)\right|} \geqslant \frac{1}{2\cdot f}\cdot\frac{1}{\mu(X)}$$

and the assertion follows in this case.

Now let $p\big|(q-1,l+1) = |Z(SL_{l+1}(q))|$. Let ξ denote a primitive p^{th}-root of unity in $\mathbb{F}_q$. It suffices to construct a torus T in $SL_{l+1}(q)$ and an element $g \in T$ such that $C_{SL_{l+1}(q)}(g) = T$, $p\big|\mathrm{ord}(g)$ and $\langle g\rangle \cap Z(SL_{l+1}(q)) = 1$.

Let $l=2$, then $SL_3(q)$ contains a maximally split torus T of order $(q-1)^2$ and $p^2\big|(q-1)^2$. In this case put

$$g := \begin{pmatrix} \xi & 0 & 0 \\ 0 & \xi^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \in T.$$

As $p \neq 2$ one concludes that $C_{SL_3(q)}(g) = T$. It is obvious that $\langle g \rangle \cap Z(SL_{l+1}(q)) = 1$.

Let $l > 2$ and consider the field norm $N : \mathbb{F}^*_{q^{l-1}} \to \mathbb{F}^*_q$. So N is a surjective map whose kernel has order $(q^{l-1} - 1)/(q-1)$. Thus by order arguments there exists an element $\tau \in \mathbb{F}_{q^{l-1}}$ being contained in no proper subfield of $\mathbb{F}_{q^{l-1}}$, such that $N(\tau) = \xi^{-1}$. Put

$$g := \begin{pmatrix} \xi & 0 & \dots & \dots & \dots & 0 \\ 0 & \tau & 0 & \dots & \dots & 0 \\ 0 & 0 & \tau^q & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \dots & 0 & \tau^{q^{l-2}} & 0 \\ 0 & \dots & \dots & \dots & 0 & 1 \end{pmatrix}.$$

Then $g \in T_\Lambda$ where T_Λ is a maximal torus corresponding to the partition $\Lambda = (1,1,l-1)$. Further we have $p \mid \operatorname{ord}(g)$ and $\langle g \rangle \cap Z(SL_{l+1}(q)) = 1$. As all eigenvalues of g are distinct elements in $\overline{\mathbb{F}}_q$, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$, g is a regular element in $G = SL_{l+1}(\overline{\mathbb{F}}_q)$, in particular $C_{SL_{l+1}(q)}(g) = T_\Lambda$. This implies the assertion also in this case.

Next we consider an arbitrary finite group of Lie type X.

Proposition 4.4. *Let* $\mathbf{G}$ *be an algebraic simple, simply connected group of Lie type over the algebraically closed field* $\overline{\mathbb{F}}_q$ *of characteristic* π. *Let* $F : \mathbf{G} \to \mathbf{G}$ *be a Frobenius automorphism of* $\mathbf{G}$ *and* $\mathbf{G}^F$ *be the corresponding finite group of Lie type. Let* p *be a prime divisor of the order of* $X := \mathbf{G}^F / Z(\mathbf{G}^F)$. *Then*

$$\frac{|\mathcal{A}_p(X)|}{|X|} \geqslant \frac{1}{(q+1)^l},$$

where l *denotes the Lie rank of* $\mathbf{G}$ *and* q *is defined as before.*

Proof: It is a well known fact that an element $g \in \mathbf{G}^F$ is a π-element if and only if g is unipotent and g is a π'-element if and only if g is semisimple.

(1) Let $p = \pi$. $\mathbf{G}$ is a simple algebraic group, so $Z^0(\mathbf{G}) = 1$ and Proposition 4.2 yields

$$\frac{|\mathcal{A}_p(\mathbf{G}^F)|}{|\mathbf{G}^F|} \geqslant \frac{1}{q^l}.$$

(2) Let $p \neq \pi$ and s be a semisimple element of $\mathbf{G}^F$, such that $\operatorname{ord}(s) = p^\alpha$ for some $\alpha \in \mathbb{N}$, and $s \notin Z(\mathbf{G}^F)$. So Steinberg's Theorem [**4**, Theorem 3.5.6] implies that $\mathbf{H} := C_{\mathbf{G}}(s)$ is a connected reductive group, in particular $\mathbf{H}$ has decomposition: $\mathbf{H} = [\mathbf{H},\mathbf{H}]Z^0(\mathbf{H})$.

For $[\mathbf{H},\mathbf{H}] = 1$, $\mathbf{H}$ is a maximal torus of $\mathbf{G}$. So $\mathbf{H}^F = C_{\mathbf{G}^F}(s)$ is a maximal torus of $\mathbf{G}^F$ and s is a regular semisimple element. It is a well known fact that the order of a

https://doi.org/10.1017/S0004972700015951 Published online by Cambridge University Press

maximal torus of $\mathbf{G}^F$ is bounded by $(q+1)^l$ [4, Proposition 3.3.5] and thus we obtain in this case

$$\frac{|\mathcal{A}_p(X)|}{|X|} \geqslant \frac{d}{|C_{\mathbf{G}^F}(s)|} \geqslant \frac{1}{(q+1)^l},$$

where $d = |Z(\mathbf{G}^F)|$.

If $[\mathbf{H},\mathbf{H}] \neq 1$, $\mathbf{H}$ contains regular unipotent elements. Let $T_1,\dots,T_k$ denote the $\mathbf{H}^F$-conjugacy classes of regular unipotent elements in $\mathbf{H}^F$ and let $u_1,\dots,u_k$ be representatives of these classes. From Proposition 4.2 we deduce that

$$\sum_{i=1}^{k} |T_i| = \frac{|\mathbf{H}^F|}{\left|Z^0(\mathbf{H})^F\right| q^{l(\mathbf{H})}},$$

where $l(\mathbf{H})$ is the semisimple rank of $\mathbf{H}$. Set $\sigma_i := s \cdot u_i$, $i = 1,\dots,k$. For these elements σ_i we claim that the $\mathbf{G}^F$-conjugacy classes $S_i := \{\sigma_i^g \mid g \in \mathbf{G}^F\}$ are disjoint and that $C_{\mathbf{G}^F}(\sigma_i) \subset C_{\mathbf{G}^F}(s) = \mathbf{H}^F$.

Let $g \in \mathbf{G}^F$ be such that $\sigma_i^g = \sigma_j$. We find an arbitrary big $k \in \mathbb{N}$ such that $p|\pi^k - 1$ and thus can choose k such that $s^{\pi^k} = s$ and $u_i^{\pi^k} = u_j^{\pi^k} = 1$. Then

$$s = (su_j)^{\pi^k} = ((su_i)^g)^{\pi^k} = \left((su_i)^{\pi^k}\right)^g = s^g$$

and $g \in C_{\mathbf{G}^F}(s) = \mathbf{H}^F$. From this we obtain $T_i = T_j$, a contradiction. The same argument also shows that $C_{\mathbf{G}^F}(\sigma_i) \leqslant \mathbf{H}^F$. Thus one even has $C_{\mathbf{G}^F}(\sigma_i) = C_{\mathbf{H}^F}(u_i)$. So

$$|S_i| = \frac{|\mathbf{G}^F|}{|C_{\mathbf{G}^F}(\sigma_i)|} = \frac{|\mathbf{G}^F|}{|C_{\mathbf{H}^F}(\sigma_i)|} = \frac{|\mathbf{G}^F|}{|\mathbf{H}^F|} \cdot |T_i|.$$

But at most d elements in $\mathbf{G}^F$ have the same image in X. Thus one gets

$$\frac{|\mathcal{A}_p(X)|}{|X|} \geqslant \frac{1/d \cdot \sum_{i=1}^k |S_i|}{1/d \cdot |\mathbf{G}^F|} = \frac{\sum_{i=1}^k |T_i|}{|\mathbf{H}^F|} = \frac{1}{\left|Z^0(\mathbf{H})^F\right| \cdot q^{l(\mathbf{H})}} \geqslant \frac{1}{(q+1)^{l(\mathbf{G})-l(\mathbf{H})} \cdot q^{l(\mathbf{H})}}$$

and the proposition is proved. ∎

Let $X \leqslant S \leqslant \mathrm{Aut}(S)$, where X is a finite simple group of Lie type. We assume further that $X \not\cong G_2(2), {}^2F_4(2)$. Then Proposition 4.4. implies that

$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{|Out(E)|} \cdot \frac{1}{(q+1)^l}.$$

Bounds for the minimal permutation representation degrees for groups of Lie type were computed for the classical groups by Cooperstein [6], and by Patton [17], and for the

Table 4.

X	$\mu(X)^*$	exceptions
$PSp_{2l}(q)$	$\dfrac{q^{2l}-1}{q-1}$	$\mu(Sp_{2l}(2)) = 2^{l-1}(2^l-1)$
		$\mu(PSp_4(3)) = 27$
$\Omega_{2l+1}(q)$ q odd	$\dfrac{q^{2l}-1}{q-1}$	$\mu(\Omega_{2l+1}(3)) = 1/2\,3^l(3^l-1)$
$P\Omega_{2l}^{+}(q)$	$\dfrac{(q^{l-1}+1)(q^l-1)}{q-1}$	$\mu(P\Omega_{2l}^{+}(2)) = 2^l(2^l-1)$
$P\Omega_{2l}^{-}(q)$	$\dfrac{(q^{l-1}-1)(q^l+1)}{q-1}$	
$U_3(q)$	q^3+1	$\mu(U_3(5)) = 50$
$U_4(q)$	$(q^3+1)(q+1)$	
$U_{l+1}(q)$	$\dfrac{\left(q^l-(-1)^l\right)\left(q^{l-1}-(-1)^{l-1}\right)}{(q^2-1)}$	$\mu(U_{6k}(2)) = 1/3\,2^{6k-1}(2^{6k}-1)$
$E_6(q)$	$q^{14}(*)$	
${}^2E_6(q)$	$q^{20}(*)$	
$E_7(q)$	$q^{27}(*)$	
$E_8(q)$	$q^{57}(*)$	
$G_2(q)$	$1/6\,q^6(*)$	
${}^3D_4(q)$	$q^7(*)$	
${}^2B_2(q)$	q^4+1	
${}^2G_2(q)$	q^6+1	
${}^2F_4(q)$	$q^{26}(*)$	$\mu({}^2F_4(2)') = 1600$

The $(*)$ indicates where we give only a lower bound.

exeptional groups in Liebeck and Saxl [15]. We list these bounds in Table 4. Using these bounds one can verify the inequality

$$(*) \qquad |Out(E)|\,(q+1)^l \leqslant \mu(E)$$

https://doi.org/10.1017/S0004972700015951 Published online by Cambridge University Press

for all simple groups of Lie type apart from the following exeptions:

$$X \simeq L_{l+1}(q), PSp_4(3), U_3(5), U_3(8), U_4(3), U_4(5), U_4(7), U_6(2), P\Omega_8^+(3), P\Omega_8^+(4), P\Omega_8^+(5).$$

Groups of tyle A_{l+1} were considered before. One can use the character tables in [5] to show that $(*)$ also holds for S provided $X = soc(S) = PSp_4(3)$, $U_3(8)$, $U_4(3)$, $U_6(2)$, $P\Omega_8^+(3)$. For the remaining groups $X \simeq U_3(5)$, $U_4(5)$, $U_4(7)$, $P\Omega_8^+(4)$, $P\Omega_8^+(5)$ one easily verifies the estimate

$$|Out(E)|\,(q+1)^l \leqslant 2 \cdot \mu(E) \cdot \log(\mu(E)).$$

Thus it remains to consider $X \simeq {}^2F_4(2)'$. In this case one has $\mu(X) = 1600$ and for each non trivial conjugacy class C of X one has $|C| \cdot \mu(X) \geqslant |X|$ and thus the assertion holds in this case too.

Finally assume that X is sporadic and S a quasisimple group which satisfies $X \leqslant S \leqslant \mathrm{Aut}(X)$. It is a trivial matter to calculate for each prime dividing $|X|$ the number $|\mathcal{A}_p(X)|$ using the character tables in [5]. There we can also find lists of all maximal subgroups of most of the sporadic groups. This we can use to calculate the minimal permutation representation degree for X. For

$$X \simeq J_4,\ Fi_{23},\ Th,\ Fi_{24}',\ BM,\ M$$

there do not exist complete lists of maximal subgroups, but we can roughly bound the minimal degree as follows:

$$\begin{array}{rl}
\mu(J_4) \geqslant 1334 & \text{as } \mu(J_4) \geqslant \chi(1)+1 \text{ for all non-trivial irreducible chracters } \chi, \\
\mu(Fi_{23}) \geqslant 3510 & \text{as } \mu(Fi_{23}) \geqslant \mu(Fi_{22}) = 3510, \\
\mu(Th) \geqslant 249 & \text{as } \mu(Th) \geqslant \chi(1)+1 \text{ for all non-trivial irreducible chracters } \chi, \\
\mu(Fi_{24}) \geqslant 2040 & \text{as } \mu(Fi_{24}') \geqslant \mu(He) \geqslant 2040, \\
\mu(BM) \geqslant 1140000 & \text{as } \mu(BM) \geqslant \mu(HN) = 1140000, \\
\mu(M) \geqslant 1140000 & \text{as } \mu(M) \geqslant \mu(HN) = 1140000.
\end{array}$$

For all simple sporadic groups X and prime divisors p of X one concludes that

$$\frac{|\mathcal{A}_p(S)|}{|S|} \geqslant \frac{1}{\mu(X)}$$

and this completes the proof of Lemma 4.1. and thus also of Theorem B. $\square$

References

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

[2] M. Aschbacher and R. Guralnick, 'On abelian quotients of primitive groups', *Proc. Amer. Math. Soc.* **107** (1989), 89–95.

[3] R.W. Carter, *Simple groups of Lie type* (Wiley-Interscience, New York, 1972).

[4] R.W. Carter, *Finite groups of Lie type: Conjugacy classes and complex characters* (Wiley-Interscience, New York, 1985).

[5] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *An Atlas of finite groups* (Oxford University Press, 1985).

[6] B.N. Cooperstein, 'Minimal degree for a permutation representation of a classical group', *Israel J. Math.* **30** (1978), 213–235.

[7] D. Easdown and C.E. Praeger, 'On minimal faithful permutation representations of finite groups', *Bull. Austral. Math. Soc.* **38** (1988), 207–220.

[8] A. Gambini Weigel, *Bemerkungen zur Komplexität einiger gruppentheoretischer Algorithmen*, Dissertation (Albert-Ludwigs-Universität Freiburg, 1992).

[9] B. Huppert, *Endliche gruppen* 1 (Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[10] I.M. Isaacs, W.M. Kantor and N. Spaltenstein, 'On the probability that a group element is p-singular'. Preprint.

[11] W.M. Kantor, 'Polynomial-time algorithms for finding elements of prime order and Sylow subgroups', *J. Algorithms* **6** (1985), 478-514.

[12] P. Kleidman, 'The low-dimensional finite classical groups and their subgroups', (to appear in Longman Research Notes).

[13] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, LMS Lecture Notes Series **129** (Cambridge University Press, 1990).

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

[15] M.W. Liebeck and J. Saxl, 'On the orders of maximal subgroups of the finite exceptional groups of Lie type', *Proc. London Math. Soc.* **55** (1987), 299–330.

[16] P.P. Pàlfy, 'A polynomial bound for the orders of primitive solvable groups', *J. Algebra* **77** (1982), 127–137.

[17] W.H. Patton, *The minimum index for subgroups in some classical groups: A generalisation of a theorem of Galois*, Ph.D.Thesis (University of Illinois at Chicago Circle, 1972).

[18] D.I. Suprunenko, *Matrix groups*, Translation of Mathematical Monographs (American Mathematical Society, 1976).

[19] M. Suzuki, *Group theory II* (Springer-Verlag, Berlin, Heidelberg, New York, 1982).

Mathematishces Institut
Albert-Ludwigs-Universität
Albertstr.23b
D78 Freiburg