Bases of primitive linear groups II

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2BZ
England

Aner Shalev
Mathematics Institute
Hebrew University
Jerusalem 91904
Israel

Abstract

We correct and improve a result in [3], giving the structure of finite primitive linear groups of unbounded base size. This confirm a well-known conjecture of Pyber on base sizes of primitive permutation groups in the case of affine groups whose associated linear group is primitive.

1 Introduction

Let V be a finite vector space, and H a subgroup of $GL(V)$. A *base* for H is a subset of V whose pointwise stabilizer in H is trivial. Denote by $b(H)$ the minimal size of a base for H. Theorem 1 of [3] gives an upper bound for $b(H)$ in the case where H acts irreducibly and primitively on V, of the form $b(H) \leq \frac{18\log|H|}{\log|V|} + c$, where c is an explicit absolute constant. This confirms part of a well-kown conjecture of Pyber [4] on base sizes of primitive permutation groups.

The proof of [3, Theorem 1] relied on Theorem 2 of that paper, a result which gives the structure of primitive linear groups of unbounded base size. Unfortunately this theorem is not correctly stated: the tensor product in part (i) of the conclusion is supposed to be defined over the prime field $\mathbb{F}_p$, but this is not possible in general, as a tensor decomposition of a vector space over an extension of $\mathbb{F}_p$ does not yield a tensor decomposition over $\mathbb{F}_p$. The purpose of this paper is to prove a corrected and improved version of [3, Theorem 2]. This is done in Theorem 1 and Proposition 2 below: these correspond to parts (i) and (ii) of [3, Theorem 2].

Corollary 3, which is a very slightly amended version of Theorem 1 of [3], can readily be deduced from these results, and we do this at the end of the paper.

Before stating the results we need a few definitions. If $V = V_d(q)$ is a vector space of dimension d over the finite field $\mathbb{F}_q$ of characteristic p, and $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$, then $\mathrm{Cl}_d(q_0)$ denotes the normalizer in $GL_d(q)$ of one of the insoluble classical groups $SL_d(q_0)$, $SU_d(q_0^{1/2})$, $Sp_d(q_0)$, $\Omega_d(q_0)$ (where in the last case q_0 is odd if d is odd, and both types $\Omega_d^{\pm}(q_0)$ are included if d is even). For the symmetric group $\mathrm{Sym}(m)$ of degree m, by the natural module over $\mathbb{F}_q$ we mean the nontrivial irreducible constituent of the usual m-dimensional permutation module over $\mathbb{F}_q$; it has dimension $m' = m - \delta(p,m)$, where $\delta(p,m)$ is 2 if $p|m$ and 1 otherwise. We denote by $\mathrm{Alt}(m)$ the alternating group of degree m.

For $H \leq GL(V)$, define $b^*(H)$ to be the minimal size of a set B of vectors such that any element of H which fixes every 1-space $\langle v \rangle$ with $v \in B$ is necessarily a scalar multiple of the identity. By [3, 3.1] we have $b(H) \leq b^*(H) \leq b(H)+1$. Also $H^{(\infty)}$ denotes the last term in the derived series of H.

Let $V = V_d(q)$ have a tensor decomposition $V = V_1 \otimes \cdots \otimes V_t$ over $\mathbb{F}_q$. For subgroups $H_i \leq GL(V_i)$ $(1 \leq i \leq t)$, define $H_1 \otimes \cdots \otimes H_t = \bigotimes_{i=1}^t H_i$ to be the subgroup of $GL(V)$ consisting of all elements $h_1 \otimes \cdots \otimes h_t$ $(h_i \in H_i)$, defined by setting

$$(v_1 \otimes \cdots \otimes v_t)(h_1 \otimes \cdots \otimes h_t) = v_1h_1 \otimes \cdots \otimes v_th_t$$

for $v_i \in V_i$.

We define a constant C just as in [3, p.98], as follows. First, it is shown in [3, 3.6] that if H is a primitive subgroup of $GL(V)$ such that the Fitting subgroup $F(H)$ is irreducible on V, then $b^*(H)$ is bounded above by an absolute constant; define C_1 to be the maximum value of $b^*(H)$ over all such H, V. Next, [3, 2.2] shows that if $H \leq GL(V)$ with $E(H)$ quasisimple and absolutely irreducible on V (where $E(H)$ is the group generated by all quasisimple subnormal subgroups of H), and $E(H)$ is not $\mathrm{Alt}(m)$ or $\mathrm{Cl}_d(q_0)$ with V the natural module over $\mathbb{F}_q$, then $b^*(H)$ is bounded above by an absolute constant; define C_2 to be the maximum value of $b^*(H)$ over all such H, V. Finally, set

$$C = \max\{C_1, C_2, 33\}.$$

Theorem 1 *Let $V = V_d(q)$, and let H be a subgroup of $\Gamma L(V)$ such that H acts primitively on V and $H^0 := H \cap GL(V)$ is absolutely irreducible on V. Suppose that $b^*(H^0) > C$. Then*

$$H^0 \leq H_0 \otimes \bigotimes_{i=1}^{s} \mathrm{Sym}(m_i) \otimes \bigotimes_{i=1}^{t} \mathrm{Cl}_{d_i}(q_i),$$

where $s+t \geq 1$ and the following hold:

(i) $H_0 \leq GL_{d_0}(q)$ with $b^*(H_0) \leq C$

(ii) each factor $\mathrm{Sym}(m_i) < GL_{m_i'}(q)$, where $m_i' = m_i - \delta(p, m_i)$ as above

(iii) each factor $\mathrm{Cl}_{d_i}(q_i) \leq GL_{d_i}(q)$ as above

(iv) $d = d_0 \cdot \prod_1^s m_i' \cdot \prod_1^t d_i$

(v) the integers $m_1', \ldots, m_s', d_1, \ldots, d_t$ are all distinct

(vi) $F^*(H^0)$ contains $\prod_1^s \mathrm{Alt}(m_i) \cdot \prod_1^t \mathrm{Cl}_{d_i}(q_i)^{(\infty)}$.

Note that any irreducible primitive linear group $H \leq GL_n(p)$ (p prime) satsifies the hypotheses of the first sentence of this theorem: for if we choose $q = p^r$ maximal such that $H \leq \Gamma L_d(q) \leq GL_n(p)$, where $n = dr$, then $H^0 := H \cap GL_d(q)$ is absolutely irreducible on $V_d(q)$ by [2, 12.1].

Proposition 2 *Let H, H^0 be as in Theorem 1, with $b^*(H^0) > C$. Take $m_s' = \max(m_i' : 1 \leq i \leq s)$ and $d_t = \max(d_i : 1 \leq i \leq t)$ (define these to be 0 if $s = 0$ or $t = 0$, respectively).*

(i) Suppose $t \geq 1$ and $m_s' \leq d_t$, and let $q = q_t^r$. Then $d < d_t^2$, and

$$b^*(H^0) \leq b^*(GL_{d/d_t}(q) \otimes GL_{d_t}(q_t)) \leq \frac{9d_t^2}{dr} + 22.$$

(ii) Suppose $s \geq 1$ and $m'_s > d_t$, and let $q = p^r$. Then $d < (m'_s)^2$, and

$$b^*(H^0) \leq b^*(GL_{d/m'_s}(q) \otimes \mathrm{Sym}(m_s)) \leq \frac{3m_s \log_p m_s}{dr} + 22.$$

Corollary 3 *Suppose $H \leq GL(V)$ is an irreducible, primitive linear group on a finite vector space V. Then either*

(i) $b(H) \leq C + 1$, or

(ii) $b(H) < 18\frac{\log |H|}{\log |V|} + 30$.

2 Proofs

Proof of Theorem 1

The proof goes by induction on $\dim V$. Assume first that there is a tensor decomposition $V = V_1 \otimes V_2$ over $\mathbb{F}_q$ with $\dim V_i > 1$ such that $H \leq N_{\Gamma L(V)}(GL(V_1) \otimes GL(V_2)) := N$. For $i = 1, 2$ let ϕ_i be the natural map $N \to P\Gamma L(V_i)$, define H^i to be the full preimage in $\Gamma L(V_i)$ of $H\phi_i$, and let $H^{0,i} := H^i \cap GL(V_i)$, so that $H^0 \leq H^{0,1} \otimes H^{0,2}$.

We claim that H^i is primitive on V_i, and that $H^{0,i}$ is absolutely irreducible on V_i, for $i = 1, 2$. The first assertion is straightforward, since if, say, H^1 preserves a direct sum decomposition $V_1 = \bigoplus_1^r X_j$, then H preserves the decomposition $V = \bigoplus_1^r X_j \otimes V_2$, and so $r = 1$ as H is primitive. For the second assertion, observe that if $K = C_{GL(V_i)}(H^{0,i})$, then $K \otimes 1$ centralizes $H^{0,1} \otimes H^{0,2}$, hence centralizes H^0; since H^0 is absolutely irreducible this implies that $K = \mathbb{F}_q^*$, hence $H^{0,i}$ is absolutely irreducible.

By the claim, we can apply induction to the groups $H^{0,i} \leq GL(V_i)$ for $i = 1, 2$. This gives

$$\begin{aligned} H^{0,1} &\leq H_0^{(1)} \otimes \bigotimes \mathrm{Sym}(m_i) \otimes \bigotimes \mathrm{Cl}_{d_i}(q_i), \\ H^{0,2} &\leq H_0^{(2)} \otimes \bigotimes \mathrm{Sym}(m'_i) \otimes \bigotimes \mathrm{Cl}_{d'_i}(q'_i), \end{aligned}$$

where $b^*(H_0^{(i)}) \leq C$ for $i = 1, 2$. As argued on p.110 of [3], we can assume that all the numbers m_i, m'_i, d_i, d'_i are distinct; also $b^*(H_0^{(1)} \otimes H_0^{(2)}) \leq C$ by [3, 3.3(ii)]. Since $H^0 \leq H^{0,1} \otimes H^{0,2}$, the conclusion of Theorem 1 therefore holds.

Hence we may assume from now on that there is no nontrivial tensor decomposition of V over $\mathbb{F}_q$ preserved by H. By [2, 12.2], it follows that if N is a normal subgroup of H such that $N \leq H^0$ and $N \not\leq Z(H^0)$, then $V \downarrow N$ is absolutely irreducible.

Now H is insoluble, since otherwise $b(H) \leq 4$ by [5]. Let $Z = Z(H^0)$ and let S be the socle of H/Z. Write $S = M_1 \times \cdots \times M_k$ where each M_i is a minimal normal subgroup of H/Z. Let R be the full preimage of S in H, and P_i the preimage of M_i, so that $R = P_1 \dots P_k$, a commuting product. Clearly $R \cap H^0 \neq 1$, so we may take $P_1 \leq H^0$. By the previous paragraph, $V \downarrow P_1$ is absolutely irreducible.

If P_1/Z is abelian then $b^*(H^0)$ is bounded, by [3, 3.6] – indeed, $b^*(H^0) \leq C$ by definition of C, which is a contradiction.

Hence $P_1/Z \cong T^t$, where T is a non-abelian simple group. If $t > 1$, then [1, 3.16, 3.17] implies that P_1 preserves a tensor decomposition $V = V_1 \otimes \cdots \otimes V_t$ with $\dim V_i$ independent of i, and $H^0 \leq N_{GL(V)}(\bigotimes GL(V_i))$; but then $b(H^0) \leq 4$ by [3, 3.5].

Hence $t = 1$. Now [3, 2.2], together with the definition of C, implies that $E(H^0)$ is either $\mathrm{Alt}(m)$ (with $d = m - \delta(p, m)$) or $\mathrm{Cl}_d(q_0)$, as in the conclusion of Theorem 1. This completes the proof.

Proof of Proposition 2

The proof runs along similar lines to that of [3, Theorem 2(ii)], but there are a few differences, so we give it in full here. Let H, H^0 be as in Theorem 1, with $b^*(H^0) > C$. The proof goes by induction on $s + t$.

Consider the base case $s + t = 1$ we have $H^0 \leq H_0 \otimes M$ where $M = \mathrm{Cl}_{d_1}(q_1)$ or $\mathrm{Sym}(m_1)$. Write $m = d_1$ or m_1', respectively, so that $d = d_0 m$. By [3, 3.7], we have $b(M) \leq \frac{3m}{r} + 5$ (where $q = q_1^r$) or $\frac{\log_p m}{r} + 5$ (where $q = p^r$), respectively.

Assume $d_0 > m$. If $b^*(H_0) > m$ then by [3, 3.3(ii)],

$$b^*(H^0) \leq \max\{b^*(H_0), b^*(M)\} \leq \max\{b^*(H_0), m + 1\} = b^*(H_0) \leq C,$$

which is a contradiction. And if $b^*(H_0) \leq m$ then [3, 3.3(iv)] implies that $b(H^0) \leq 3$, also a contradiction.

Therefore $d_0 \leq m$. Also $b^*(M) > d_0$, again by [3, 3.3(iv)]. Hence [3, 3.3(iii)] gives $b(H^0) \leq 3(1 + \frac{b^*(M)}{d_0})$. If $M = \mathrm{Cl}_{d_1}(q_1)$, then $b^*(M) \leq b(M) + 1 \leq \frac{3m}{r} + 6$, so this gives

$$b(H^0) \leq 3(1 + \frac{3m + 6r}{rd_0}) \leq \frac{9m^2}{rd} + 21,$$

which yields part (i) of the proposition. Similarly part (ii) holds when $M = \mathrm{Sym}(m_1)$.

Now assume $s + t \geq 2$. Let m be the maximum of d_t and m_s', and write M for the corresponding group $\mathrm{Cl}_{d_t}(q_t)$ or $\mathrm{Sym}(m_s)$. Let N be the tensor product of H_0 and the other factors $\mathrm{Cl}_{d_i}(q_i)$, $\mathrm{Sym}(m_i)$, so that $H^0 \leq N \otimes M$. If $b^*(N) \leq C$ the conlcusion follows as in the $s + t = 1$ case, so assume $b^*(N) > C$.

Let m' be the largest among the dimensions d_i, m_i' omitting m, and write N_1 for the corresponding group $\mathrm{Cl}_{d_i}(q_i)$ or $\mathrm{Sym}(m_i)$.

Consider the case where $N_1 = \mathrm{Cl}_{d_i}(q_i)$. Let $q = q_i^u$. By induction we have

$$b^*(N) \leq 9\frac{d_i^2 m}{du} + 22 \leq 9\frac{d_i}{u} + 22.$$

Suppose $d \geq m^2$. Then $b^*(N) \geq m$ by [3, 3.3(iv)], so [3, 3.3(iii)] implies that

$$b^*(H^0) \leq 3(1 + \frac{9d_i + 22u}{um}).$$

Since $m \geq d_i$ and $m > 22$ (otherwise [3, 3.3] can easily be used to deduce that $b^*(H^0) < C$), this yields $b^*(H^0) < 33 \leq C$, a contradiction. Hence $d < m^2$ in this case. Now the conclusion of the proposition follows by the argument given for the $s + t = 1$ case.

Finally, consider the case where $N_1 = \mathrm{Sym}(m_i)$. Let $q = p^r$. By induction,

$$b^*(N) \leq \frac{(3m_i \log_p m_i) \cdot m}{dr} + 22 \leq \frac{3 \log_p m_i}{r} + 22.$$

Now the argument of the previous paragraph gives the conclusion.

This completes the proof of Proposition 2.

Proof of Corollary 3

Let $V = V_n(q_0)$, and suppose $H \leq GL(V)$ acts primitively and irreducibly on V. Choose $q = q_0^r$ maximal such that $H \leq \Gamma L_d(q) \leq GL_n(q_0)$, where $n = dr$. Write $H^0 = H \cap GL_d(q)$ and $V = V_d(q)$. By [2, 12.1], H^0 is absolutely irreducible on V.

If $b^*(H^0) \leq C$ then $b(H) \leq C+1$, as in part (i) of the corollary. So assume that $b^*(H^0) > C$. Then H^0 is given by Theorem 1 of this paper. Now the proof that H satisfies (ii) proceeds just as in [3, p.112].

Acknowledgements The authors acknowledge the support of an EPSRC grant. The second author is grateful for the support of ISF grant 754/08 and ERC Advanced Grant 247034.

References

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

[2] Arithmetic results on orbits of linear groups, M. Giudici, M.W. Liebeck, C.E. Praeger, J. Saxl and P.H. Tiep, preprint, arXiv:1203.2457.

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

[4] L. Pyber, Asymptotic results for permutation groups, in *Groups and Computation* (eds. L. Finkelstein and W. Kantor), DIMACS Series on Discrete Math. and Theor. Comp. Science, Vol. 11, Amer. Math. Soc, Providence, 1993, pp. 197-219.

[5] A. Seress, The minimal base size of primitive solvable permutation groups, *J. London Math. Soc.* **53** (1996), 243–255.