BASE SIZES OF IMPRIMITIVE LINEAR GROUPS AND ORBITS OF GENERAL LINEAR GROUPS ON SPANNING TUPLES

JOANNA B. FAWCETT, CHERYL E. PRAEGER

Abstract. For a subgroup L of the symmetric group S_ℓ, we determine the minimal base size of $\mathrm{GL}_d(q) \wr L$ acting on $V_d(q)^\ell$ as an imprimitive linear group. This is achieved by computing the number of orbits of $\mathrm{GL}_d(q)$ on spanning m-tuples, which turns out to be the number of d-dimensional subspaces of $V_m(q)$. We then use these results to prove that for certain families of subgroups L, the affine groups whose stabilisers are large subgroups of $\mathrm{GL}_d(q) \wr L$ satisfy a conjecture of Pyber concerning bases.

1. Introduction

Bases are a fundamental tool in permutation group theory and are used extensively in computational group theory (cf. [16]). For a permutation group G on Ω, a *base* is a subset B of Ω with the property that only the identity of G fixes every point of B. The *base size* of G on Ω, denoted by $b_\Omega(G)$ or $b(G)$, is the minimal size of a base for G. In this paper, we study the base sizes of imprimitive linear groups.

Let $V_d(q)$ denote a d-dimensional vector space over the finite field $\mathbb{F}_q$. For any positive integer ℓ and subgroup L of the symmetric group S_ℓ, the wreath product $\mathrm{GL}_d(q) \wr L$ acts naturally on $V_d(q)^\ell$ as an imprimitive linear group (cf. Section 2). In our first result, we determine the base size of $\mathrm{GL}_d(q) \wr L$ in terms of the *distinguishing number* of L on $[\ell] := \{1, \ldots, \ell\}$; this latter quantity, denoted by $d_{[\ell]}(L)$ or $d(L)$, is the minimal number of parts in a partition of $[\ell]$ for which only the identity of L fixes every part.

Theorem 1.1. *Let d and ℓ be positive integers and q a prime power. Let $V := V_d(q)^\ell$. For $L \leqslant S_\ell$,*

$$\begin{aligned} b_V(\mathrm{GL}_d(q) \wr L) &= d + \min\left\{ s : \tbinom{d+s}{d}_q \geqslant d_{[\ell]}(L) \right\} \\ &= d + \left\lceil \frac{\log d_{[\ell]}(L)}{d \log q} \right\rceil + c, \end{aligned}$$

where $c = -1$ or 0.

Theorem 1.1 gives an upper bound on the base size of any irreducible imprimitive linear group, for we may view such a group H as a subgroup of $\mathrm{GL}_d(q) \wr L$ where L is the transitive group induced by H on the d-dimensional $\mathbb{F}_q$-vector spaces of a direct sum decomposition preserved by H (cf. Lemma 2.4). In fact, if the decomposition preserved by H is as coarse as possible, then the group L is primitive (cf. Lemma 2.4), and if L is not the full symmetric or alternating group, then $d(L) \leqslant 4$ by [4, 6, 15] (cf. Theorem 2.3), so we obtain the following consequence of Theorem 1.1.

Corollary 1.2. *Let V be a finite-dimensional $\mathbb{F}_q$-vector space and $H \leqslant \mathrm{GL}(V)$ where H is irreducible and imprimitive. Let $V = V_1 \oplus \cdots \oplus V_\ell$ be a decomposition preserved by H, chosen so that ℓ is minimal subject to $\ell \geqslant 2$. If the permutation group induced by H on $\{V_1, \ldots, V_\ell\}$ is not S_ℓ or A_ℓ, then $b_V(H) \leqslant \dim_{\mathbb{F}_q}(V_1) + 1$.*

Key words and phrases. permutation group, base size, general linear group, imprimitive linear group, spanning sequence.

Theorem 1.1 is proved using a result of Bailey and Cameron [1] that describes the base size of $\mathrm{GL}_d(q) \wr L$ in terms of the number of orbits of $\mathrm{GL}_d(q)$ on *spanning m-tuples*, which are m-tuples $(v_1, \ldots, v_m) \in V_d(q)^m$ such that $v_1, \ldots, v_m$ span $V_d(q)$ (such sequences are referred to as ordered multi-bases in the more general setting of [1]).

In our next result, we determine the number of orbits of $\mathrm{GL}_d(q)$ in its natural action on the set of spanning m-tuples; here we find another interpretation for the Gaussian binomial coefficient $\binom{m}{d}_q$, which equals, for instance, the number of d-dimensional subspaces of an m-dimensional $\mathbb{F}_q$-vector space.

Theorem 1.3. *Let d and m be positive integers and q a prime power. Then $\mathrm{GL}_d(q)$ has exactly $\binom{m}{d}_q$ orbits on the set of spanning m-tuples in $V_d(q)^m$.*

As an application, we use Theorem 1.1 to prove a conjecture of Pyber for certain affine groups. Given a permutation group G of degree n, there is a trivial lower bound on $b(G)$, namely $\log |G| / \log n$, as each element of G is uniquely determined by its action on a base. Pyber conjectured in [13] that there exists an absolute constant C such that $b(G) \leqslant C \log |G| / \log n$ for every primitive permutation group G of degree n. This conjecture has now been verified for all non-affine groups [2, 3, 7, 9], as well as for affine groups that are soluble [14] or coprime [8], or those whose stabilisers are primitive linear groups [10, 11].

Thus the remaining open case for Pyber's conjecture consists of affine groups whose stabilisers are imprimitive linear groups. Here $G = V : G_0$ and acts on V, where V is an $\mathbb{F}_p$-vector space for some prime p and the stabiliser G_0 is an irreducible imprimitive subgroup of $\mathrm{GL}(V)$. We focus on (not necessarily primitive) affine groups G for which G_0 is a large subgroup of $\mathrm{GL}_d(q) \wr L$ where L is one of several families of groups.

Theorem 1.4. *Let d and ℓ be positive integers and q a prime power. Let $L \leqslant S_\ell$ and $V := V_d(q)^\ell$. Let G_0 be a group for which $\mathrm{SL}_d(q)^\ell \leqslant G_0 \leqslant \mathrm{GL}_d(q) \wr L$ and suppose that G_0 induces the group L on the ℓ factors of the decomposition of V. Let $G := V : G_0$. Suppose that one of the following holds.*

(i) *$d_{[\ell]}(L) \leqslant c$ where c is an absolute constant.*
(ii) *L acts primitively on $[\ell]$.*
(iii) *L acts semiregularly on $[\ell]$.*
(iv) *$L = S_m \wr S_r$ in its imprimitive action on $[\ell]$ where $\ell = mr$ and $m, r \geqslant 2$.*

Then there exists an absolute constant C such that

$$b_V(G) \leqslant C \frac{\log |G|}{\log n} + C + 2,$$

where $n = q^{d\ell}$ is the degree of G. Moreover, we can take $C = \max\{2, \frac{\log 2c}{\log 2}\}$ when (i) holds, $C = 3$ when (ii) holds, and $C = 2$ when (iii) or (iv) hold.

More precise estimates for C may be deduced from the proof of Theorem 1.4 in Section 5. For $\ell \geqslant 2$, the affine groups $V : G_0$ of Theorem 1.4 are primitive precisely when L is transitive and $(d, q) \neq (1, 2)$ (cf. Lemma 2.4), so Theorem 1.4 includes genuine primitive affine groups.

Condition (i) of Theorem 1.4 holds for many permutation groups, including those that are primitive but not S_ℓ or A_ℓ, as previously mentioned. Indeed, Dolfi proves in [6] that if L is a (not necessarily transitive) permutation group on $[\ell]$ for which no primitive constituent contains A_ℓ, then $d(L) \leqslant 5$.

It would be interesting to prove Theorem 1.4 for all transitive subgroups L of S_ℓ. In order to apply our methods in general (cf. Lemma 5.1), it would suffice to prove that $\log d(L) \leqslant (C/\ell) \log |L| + (C-1) \log 2$ for some absolute constant C where $C > 1$.

Remark 1.5. As stated, our main results on base sizes only apply to linear groups, but each result can be interpreted for the appropriate semilinear groups, for if $H \leqslant \Gamma\mathrm{L}(V)$, then $b_V(H) \leqslant b_V(H \cap \mathrm{GL}(V)) + 1$. To see this, let B be a base for $H \cap \mathrm{GL}(V)$. Choose a primitive element $\zeta \in \mathbb{F}_q$ and a non-zero vector $v \in B$. Then $B \cup \{\zeta v\}$ is a base for H.

Both Corollary 1.2 and Theorem 1.4(ii) depend on the classification of the finite simple groups, for their proofs rely on the result referred to above concerning the distinguishing numbers of primitive permutation groups.

This paper is organised as follows. In Section 2, we state some definitions, notation and preliminary results. In Section 3, we prove Theorem 1.3; in Section 4, we prove Theorem 1.1 and Corollary 1.2; and in Section 5, we prove Theorem 1.4.

2. Preliminaries

Let H and K be groups. We denote a semidirect product of H and K (in which H is normal) by $H : K$. If K acts on $[\ell] := \{1, \ldots, \ell\}$, then K acts on H^ℓ by permuting coordinates, and this action defines the *wreath product* $H^\ell : K$, which we denote by $H \wr K$. Suppose in addition that H acts on Ω. Now $H \wr K$ has two natural actions. One is the *product action* on Ω^ℓ, in which K acts by permuting coordinates and $(h_1, \ldots, h_\ell) \in H^\ell$ maps $(\alpha_1, \ldots, \alpha_\ell) \in \Omega^\ell$ to $(\alpha_1^{h_1}, \ldots, \alpha_\ell^{h_\ell})$. The other is the *imprimitive action* on $\Omega \times [\ell]$, in which $(h_1, \ldots, h_\ell)k \in H \wr K$ maps $(\alpha, i) \in \Omega \times [\ell]$ to (α^{h_i}, i^k); if H and K are transitive on Ω and $[\ell]$ respectively, then $H \wr K$ acts transitively on $\Omega \times [\ell]$ with blocks of imprimitivity $\{(\alpha, i) : \alpha \in \Omega\}$ for $i \in [\ell]$.

Let m be a positive integer. For a group H acting on Ω, an *ordered multi-base of length* m is an m-tuple $(\alpha_1, \ldots, \alpha_m) \in \Omega^m$ for which $\{\alpha_1, \ldots, \alpha_m\}$ is a base for H. Now H acts naturally on Ω^m and preserves the set of ordered multi-bases. The following is a result of Bailey and Cameron [1, Theorem 2.13].

Proposition 2.1 ([1]). *Let ℓ be a positive integer, and let H and K be permutation groups on Ω and $[\ell]$ respectively. Then $H \wr K$ has a base of size m under the product action if and only if the number of orbits of H on ordered multi-bases of length m is at least $d_{[\ell]}(K)$.*

In [5], Chan determines the distinguishing number of a wreath product $H \wr K$ in its imprimitive action. In particular, she proves that for positive integers m and r, the distinguishing number of $S_m \wr S_r$ on $[m] \times [r]$ is the minimum d such that $\binom{d}{m}$ is at least r. The following observation is a simple consequence of this result.

Lemma 2.2. *Let m and r be positive integers, and let $\Delta := [m] \times [r]$. Then*

$$d_\Delta(S_m \wr S_r) \leqslant \left\lceil m r^{1/m} \right\rceil.$$

Proof. By [5, Corollary 2.4], $d_\Delta(S_m \wr S_r) = \min\{d : \binom{d}{m} \geqslant r\}$. In particular, $d \geqslant m$. Now

$$\left(\frac{d}{m}\right)^m \leqslant \frac{d}{m}\frac{d-1}{m-1}\cdots\frac{d-m+1}{1} = \binom{d}{m},$$

so $d_\Delta(S_m \wr S_r) \leqslant \min\{d : (d/m)^m \geqslant r\} = \lceil m r^{1/m} \rceil$. □

In contrast, the distinguishing numbers of most primitive permutation groups are very small. Cameron, Neumann and Saxl [4] proved that all but finitely many primitive subgroups of S_ℓ not containing A_ℓ have distinguishing number 2 (using different terminology), after which Seress [15] classified the exceptions. Dolfi [6, Lemma 1] then proved that the distinguishing numbers of the exceptions are at most 4. We state this result here for convenience.

Theorem 2.3 ([4, 6, 15]). *If L is a primitive subgroup of S_ℓ not containing A_ℓ, then $d_{[\ell]}(L) \leqslant 4$.*

Let V be a finite-dimensional $\mathbb{F}_q$-vector space where q is a power of a prime p. A subgroup H of $\mathrm{GL}(V)$ is *irreducible* if it does not preserve any proper non-zero subspaces of V, and *imprimitive* if it preserves a decomposition $V = V_1 \oplus \cdots \oplus V_\ell$ where V_i is an $\mathbb{F}_q$-subspace of V for $1 \leqslant i \leqslant \ell$. If L is the group induced by H on $\{V_1, \ldots, V_\ell\}$ and $\dim_{\mathbb{F}_q}(V_i) = d$ for $1 \leqslant i \leqslant \ell$, then we may assume that $H \leqslant \mathrm{GL}_d(q) \wr L$; in particular, this occurs whenever L is transitive. Note that the action of the imprimitive linear group $\mathrm{GL}_d(q) \wr L$ on $V_d(q)^\ell$ is precisely the product action defined above.

An *affine* group with socle V and stabiliser H is the group $G = V : H$ arising from the natural action of H on V. Note that H is the stabiliser of the 0 vector. The action of G on V is primitive precisely when H is an irreducible subgroup of $\mathrm{GL}(V)$ with V viewed as an $\mathbb{F}_p$-vector space.

The following is a collection of basic results concerning imprimitive linear groups.

Lemma 2.4. *Let V be a finite-dimensional $\mathbb{F}_q$-vector space and $H \leqslant \mathrm{GL}(V)$ where H is imprimitive. Let $V = V_1 \oplus \cdots \oplus V_\ell$ be a decomposition preserved by H where $\ell \geqslant 2$, and let L be the subgroup of S_ℓ induced by H on $\{V_1, \ldots, V_\ell\}$. Let $d := \dim_{\mathbb{F}_q}(V_1)$.*

(i) *If H is irreducible, then L is transitive and $(d, q) \neq (1, 2)$.*
(ii) *If the decomposition of V is chosen so that ℓ is minimal, then L is primitive.*
(iii) *If $V_i = V_d(q)$ for $1 \leqslant i \leqslant \ell$ and $S \leqslant \mathrm{GL}_d(q)$ such that $S^\ell \leqslant H \leqslant \mathrm{GL}_d(q) \wr L$ and S is transitive on $V_d(q) \setminus \{0\}$, then $V : H$ is primitive if and only if L is transitive and $(d, q) \neq (1, 2)$.*

Proof. (i) If H is irreducible and I is an orbit of L on $[\ell]$, then $\oplus_{i \in I} V_i$ is a subspace of V preserved by H, so L is transitive. If also $(d, q) = (1, 2)$, then the set of vectors in $V \simeq \mathbb{F}_2^\ell$ with an even number of non-zero entries is preserved by H, a contradiction.

(ii) If L is not primitive, then H preserves a coarser decomposition of V.

(iii) If $V : H$ is primitive, then H is irreducible and we may apply (i). Conversely, suppose that L is transitive and $(d, q) \neq (1, 2)$. Let U be a non-zero $\mathbb{F}_p$-subspace of V preserved by H where p is the characteristic of $\mathbb{F}_q$. Let $0 \neq u = (u_1, \ldots, u_\ell) \in U$. Without loss of generality, we may assume that $u_1 \neq 0$. Since $(d, q) \neq (1, 2)$, there exists $v_1 \in V_1 \setminus \{0, u_1\}$. Since H contains a subgroup S that is transitive on $V_1 \setminus \{0\}$ and fixes V_i pointwise for $2 \leqslant i \leqslant \ell$, the vector $v := (u_1 - v_1, u_2, \ldots, u_\ell) \in U$. Thus $(v_1, 0, \ldots, 0) = u - v \in U$, and it follows as above that $(w_1, 0, \ldots, 0) \in U$ for all $w_1 \in V_1$. Since L is transitive on $[\ell]$, we conclude that $U = V$. Hence $V : H$ is primitive. □

3. Orbits on spanning tuples

Recall that for non-negative integers m and d and a prime power q, the *Gaussian binomial coefficient* is defined by

$$\binom{m}{d}_q := \begin{cases} \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-d+1}-1)}{(q^d-1)(q^{d-1}-1)\cdots(q-1)} & \text{if } d \leqslant m \\ 0 & \text{if } d > m. \end{cases}$$

Recall also that $\binom{m}{d}_q$ is precisely the number of d-dimensional subspaces of $V_m(q)$.

Proof of Theorem 1.3. Let $\mathcal{S}_{m,d}$ denote the set of spanning m-tuples of $\mathrm{GL}_d(q)$ on $V_d(q) = \mathbb{F}_q^d$ (viewed as row vectors). If $d > m$, then $\mathcal{S}_{m,d}$ is empty, so we may assume that $d \leqslant m$. Let $\mathcal{M}_{m,d}$ denote the set of $(m \times d)$-matrices over $\mathbb{F}_q$ with rank d. There is a natural bijection between $\mathcal{S}_{m,d}$ and $\mathcal{M}_{m,d}$ defined by mapping $(v_1, \ldots, v_m)$ to the $(m \times d)$-matrix

with rows $v_1, \ldots, v_m$. Now $\mathrm{GL}_d(q)$ acts on $\mathcal{M}_{m,d}$ by right multiplication, and the actions of $\mathrm{GL}_d(q)$ on $\mathcal{S}_{m,d}$ and $\mathcal{M}_{m,d}$ are equivalent under the bijection above, so the numbers of orbits of $\mathrm{GL}_d(q)$ on $\mathcal{S}_{m,d}$ and $\mathcal{M}_{m,d}$ are the same.

Let $\mathcal{O}_{m,d}$ be the set of orbits of $\mathrm{GL}_d(q)$ on $\mathcal{M}_{m,d}$. Define a map φ from $\mathcal{O}_{m,d}$ to the set of d-dimensional subspaces of $\mathbb{F}_q^m$ (viewed as column vectors) by mapping the orbit $\{Ag : g \in \mathrm{GL}_d(q)\}$, for $A \in \mathcal{M}_{m,d}$, to the column space of A. Now φ is well-defined since A and Ag have the same column space for all $g \in \mathrm{GL}_d(q)$. Clearly φ is surjective; it is also injective, for if A and B are elements of $\mathcal{M}_{m,d}$ with the same column space, then there exists $g \in \mathrm{GL}_d(q)$ such that $Ag = B$. Thus $|\mathcal{O}_{m,d}| = \binom{m}{d}_q$, as desired. □

Next we give a simple estimation for the Gaussian binomial coefficient.

Lemma 3.1. *Let d and s be positive integers and q a prime power. Then*

$$q^{ds} \leqslant \binom{d+s}{d}_q \leqslant \left(1 - \frac{1}{q} - \frac{1}{q^2}\right)^{-1} q^{ds}.$$

Proof. Observe that

$$q^s \leqslant \frac{q^{s+i}-1}{q^i-1} = q^s \frac{q^i - \frac{1}{q^s}}{q^i - 1} = q^s \frac{1 - \frac{1}{q^{s+i}}}{1 - \frac{1}{q^i}}$$

for $1 \leqslant i \leqslant d$. In particular, the lower bound holds. Moreover,

$$\binom{d+s}{d}_q = q^{ds} \frac{\prod_{i=1}^{d} \left(1 - \frac{1}{q^{s+i}}\right)}{\prod_{i=1}^{d} \left(1 - \frac{1}{q^i}\right)}.$$

Since $\prod_{i=1}^{d}(1 - 1/q^{s+i}) < 1$ and $\prod_{i=1}^{d}(1 - 1/q^i) \geqslant 1 - 1/q - 1/q^2$ by [12, Lemma 3.5], the upper bound holds. □

4. Base sizes of imprimitive linear groups

We begin by establishing the first equality of Theorem 1.1.

Lemma 4.1. *Let d and ℓ be positive integers and q a prime power. Let $V := V_d(q)^\ell$ and $L \leqslant S_\ell$. Then $b_V(\mathrm{GL}_d(q) \wr L) = d + \min\{s : \binom{d+s}{d}_q \geqslant d_{[\ell]}(L)\}$.*

Proof. For $\mathrm{GL}_d(q)$ acting on $V_d(q)$, a multi-base of length m is a spanning m-tuple for each positive integer m. Thus we may apply Theorem 1.3 and Proposition 2.1. □

Next we establish some bounds on the base size of $\mathrm{GL}_d(q) \wr L$; these we will use to determine the second equality of Theorem 1.1.

Lemma 4.2. *Let d and ℓ be positive integers and q a prime power. Let $V := V_d(q)^\ell$ and $L \leqslant S_\ell$. Then*

$$d + \left\lceil \frac{\log c(q) d_{[\ell]}(L)}{d \log q} \right\rceil \leqslant b_V(\mathrm{GL}_d(q) \wr L) \leqslant d + \left\lceil \frac{\log d_{[\ell]}(L)}{d \log q} \right\rceil$$

where $c(q) := 1 - \frac{1}{q} - \frac{1}{q^2}$.

Proof. By Lemmas 3.1 and 4.1,

$$b(\mathrm{GL}_d(q) \wr L) \leqslant d + \min\{s : q^{ds} \geqslant d(L)\} = d + \left\lceil \tfrac{\log d(L)}{d \log q} \right\rceil,$$

as desired. Similarly, again by Lemmas 3.1 and 4.1,

$$b(\mathrm{GL}_d(q) \wr L) \geqslant d + \min\{s : c(q)^{-1} q^{ds} \geqslant d(L)\} = d + \left\lceil \tfrac{\log c(q) d(L)}{d \log q} \right\rceil,$$

as desired. □

Proof of Theorem 1.1. The first equality is Lemma 4.1, so we focus on the second. For $(d,q) = (1,2)$, by Lemma 4.1,

$$b(\mathrm{GL}_1(2) \wr L) \geqslant 1 + \min\{s : 2^{s+1} \geqslant d(L)\} = 1 + \left\lceil \tfrac{\log d(L)}{\log 2} \right\rceil - 1,$$

so by Lemma 4.2, the assertion of Theorem 1.1 holds. For $(d,q) \neq (1,2)$, by Lemma 4.2, it suffices to show that $-1 \leqslant \log c(q)/(d \log q)$, where $c(q) = 1 - 1/q - 1/q^2$. This is equivalent to proving that $q^d \geqslant c(q)^{-1}$. If $q \geqslant 3$, then $q^d \geqslant 3 \geqslant 9/5 \geqslant c(q)^{-1}$, and if $q = 2$, then $d \geqslant 2$, so $q^d \geqslant 4 = c(2)^{-1}$, as desired. □

Proof of Corollary 1.2. Let L be the subgroup of S_ℓ induced by H on the set $\{V_1, \ldots, V_\ell\}$, and let $d := \dim_{\mathbb{F}_q}(V_1)$. By Lemma 2.4, the group L is primitive and $(d,q) \neq (1,2)$. In particular, we may assume that $V_i = V_d(q)$ for $1 \leqslant i \leqslant \ell$ and $H \leqslant \mathrm{GL}_d(q) \wr L$. By assumption, L is not S_ℓ or A_ℓ, so $d(L) \leqslant 4$ by Theorem 2.3. Since $\binom{d+1}{d}_q = q^d + q^{d-1} + \cdots + q + 1 \geqslant 4$, we may take $s = 1$ in Theorem 1.1. Thus $b(H) \leqslant d + 1$. □

5. Pyber's conjecture

We begin with a sufficient condition for Pyber's Conjecture in the case of affine groups with specified stabilisers.

Lemma 5.1. *Let d and ℓ be positive integers and q a prime power. Let $L \leqslant S_\ell$ and $V := V_d(q)^\ell$. Let G_0 be a group for which $\mathrm{SL}_d(q)^\ell \leqslant G_0 \leqslant \mathrm{GL}_d(q) \wr L$ and suppose that G_0 induces the group L on the ℓ factors of the decomposition of V. Let $G := V : G_0$. If*

$$\log d_{[\ell]}(L) \leqslant C \log |L|^{\frac{1}{\ell}} + (C-1)\log 2$$

for some absolute constant C where $C > 1$, then

$$b_V(G) \leqslant C\frac{\log |G|}{\log n} + C + 2,$$

where $n := q^{d\ell}$.

Proof. Let $X_0 := \mathrm{GL}_d(q) \wr L$ and $a(d,q) := \prod_{i=1}^{d}(1 - 1/q^i)$. Now $1 \leqslant (1 - 1/q^i)q$ for $1 \leqslant i \leqslant d$, so $1 \leqslant a(d,q)q^d$, which implies that

$$0 \leqslant C \log a(d,q) + Cd \log q.$$

Note that $(C-1)\log 2 \leqslant (C-1)d^2 \log q$ since $C > 1$. Thus by our assumption on $d(L)$,

$$\log d(L) \leqslant C \log |L|^{\frac{1}{\ell}} + (C-1)d^2 \log q + C \log a(d,q) + Cd \log q.$$

Dividing both sides by $d \log q$ and adding $d + 2$, we obtain

$$\frac{\log d(L)}{d \log q} + d + 2 \leqslant C\frac{\log |L|}{d\ell \log q} + Cd + C\frac{\log a(d,q)}{d \log q} + C + 2 = C\frac{\log |X_0|}{d\ell \log q} + C + 2 \tag{1}$$

since $|X_0| = \mathrm{GL}_d(q)^\ell |L|$ and $|\mathrm{GL}_d(q)| = q^{d^2} a(d,q)$. Moreover, by Theorem 1.1,

$$b(X_0) + 1 \leqslant \left\lceil \frac{\log d(L)}{d \log q} \right\rceil + d + 1 \leqslant \frac{\log d(L)}{d \log q} + d + 2. \tag{2}$$

Note that $|G| = q^{d\ell}|G_0|$. Since L is the group induced by the action of G_0 on the ℓ factors of the decomposition of V, and since the kernel of this action contains $\mathrm{SL}_d(q)^\ell$, it follows that $|X_0| = (q-1)^\ell |\mathrm{SL}_d(q)^\ell||L| \leqslant (q-1)^\ell |G_0| \leqslant |G|$. Thus by (1) and (2),

$$b(G) \leqslant b(G_0) + 1 \leqslant b(X_0) + 1 \leqslant C\frac{\log|X_0|}{d\ell \log q} + C + 2 \leqslant C\frac{\log|G|}{d\ell\log q} + C + 2,$$

as desired. □

Recall that a permutation group $L \leqslant S_\ell$ is *semiregular* if $b(L) = 1$.

Proof of Theorem 1.4. By Lemma 5.1, it suffices to find an absolute constant C with $C > 1$ such that

$$\log d(L) \leqslant C \log |L|^{\frac{1}{\ell}} + (C-1)\log 2. \tag{3}$$

Note that for $\ell = 1$, (3) holds with $C := 2$. If (i) holds, then (3) holds with $C := \max\{2, \log(2c)/\log 2\}$. Moreover, if (iii) holds, then $d(L) \leqslant 2$, so (3) holds with $C := 2$, and if (ii) holds and L is not A_ℓ or S_ℓ, then $d(L) \leqslant 4$ by Theorem 2.3, so (3) holds with $C := 3$.

Observe that $k^k \leqslant k!^2$ for every positive integer k, for if $1 \leqslant i \leqslant k$, then $k \leqslant i(k-i+1)$, so $k^k \leqslant \prod_{i=1}^k i(k-i+1) = k!^2$.

Suppose that (ii) holds and L is A_ℓ or S_ℓ, in which case $d(L) = \ell - 1$ or ℓ respectively. Now $4(\ell-1)^\ell \leqslant 4(\ell-1)(\ell-1)!^2 \leqslant \ell!^2$ and $\ell^\ell \leqslant \ell!^2$, so $d(L)^\ell \leqslant |L|^2$ in either case. Hence (3) holds with $C := 2$.

If (iv) holds and $L = S_m \wr S_r$ where $\ell = mr$ and $m, r \geqslant 2$, then $d(L) \leqslant 2mr^{1/m}$ by Lemma 2.2, and $(mr^{1/m})^{mr} \leqslant (m!^r r!)^2$, so (3) holds with $C := 2$. □

Acknowledgements

This research forms part of the Discovery Project grant DP130100106 of the second author, funded by the Australian Research Council. The first author is supported by that same grant. We would like to thank Aner Shalev for suggesting we look at the remaining open case for Pyber's conjecture, and Martin Liebeck for some observations regarding Theorem 1.3.

We would especially like to give our heartfelt thanks to the group of mathematicians who, as a collective at the 2014 annual research retreat of the Centre for the Mathematics of Symmetry and Computation (CMSC), discovered and gave a recursive proof of a version of Theorem 1.3. This group includes Brian Corr, Alice Devillers, Stephen Glasby, Cai Heng Li, Dugald Macpherson and Gabriel Verret.

References

[1] Bailey, R. F., and Cameron, P. J. Base size, metric dimension and other invariants of groups and graphs. *Bull. London Math. Soc. 43* (2011), 209–242.
[2] Benbenishty, C. *On actions of primitive groups.* PhD thesis, Hebrew University, Jerusalem, 2005.
[3] Burness, T. C., and Seress, Á. On Pyber's base size conjecture. *Trans. Amer. Math. Soc. 367* (2015), 5633–5651.
[4] Cameron, P. J., Neumann, P. M., and Saxl, J. On groups with no regular orbits on the set of subsets. *Arch. Math. 43* (1984), 295–296.
[5] Chan, M. The distinguishing number of the direct product and wreath product action. *J. Algebr. Comb. 24* (2006), 331–345.
[6] Dolfi, S. Orbits of permutation groups on the power set. *Arch. Math. 75* (2000), 321–327.
[7] Fawcett, J. B. The base size of a primitive diagonal group. *J. Algebra 375* (2013), 302–321.
[8] Gluck, D., and Magaard, K. Base sizes and regular orbits for coprime affine permutation groups. *J. London Math. Soc. 58* (1998), 603–618.
[9] Liebeck, M. W., and Shalev, A. Simple groups, permutation groups, and probability. *J. Amer. Math. Soc. 12* (1999), 497–520.

[10] Liebeck, M. W., and Shalev, A. Bases of primitive linear groups. *J. Algebra 252* (2002), 95–113.
[11] Liebeck, M. W., and Shalev, A. Bases of primitive linear groups II. *J. Algebra 403* (2014), 223–228.
[12] Neumann, P. M., and Praeger, C. E. Cyclic matrices over finite fields. *J. London Math. Soc. 52* (1995), 263–284.
[13] Pyber, L. Asymptotic results for permutation groups. *DIMACS Ser. Discrete Math. Theoret. Comp. Sci. 11* (1993), 197–219.
[14] Seress, Á. The minimal base size of primitive solvable permutation groups. *J. London Math. Soc. 53* (1996), 243–255.
[15] Seress, Á. Primitive groups with no regular orbits on the set of subsets. *Bull. London Math. Soc. 29* (1997), 697–704.
[16] Seress, Á. *Permutation group algorithms*. Cambridge University Press, Cambridge, 2003.

Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia. Email: {joanna.fawcett, cheryl.praeger[†]}@uwa.edu.au,
[†] Also affiliated with King Abdulaziz University, Jeddah, Saudi Arabia.