Bases of primitive permutation groups

Martin W. Liebeck and Aner Shalev

1 Introduction

Let G be a permutation group on a finite set Ω of size n. A subset of Ω is said to be a *base* for G if its pointwise stabilizer in G is trivial. The minimal size of a base for G is denoted by $b(G)$. Bases have been studied since the early years of permutation group theory, particularly in connection with orders of primitive groups and, more recently, with computational group theory. In this paper we survey some of the recent developments in this area, with particular emphasis on some well known conjectures of Babai, Cameron and Pyber.

We begin with a number of examples.

(1) Obviously $b(S_n) = n-1$ and $b(A_n) = n-2$.

(2) At the other extreme, $b(G) = 1$ if and only if G has a regular orbit on Ω.

(3) Let $G = S_k$ acting on the set Ω of pairs in $\{1, \dots k\}$. Write $k = 3l + r$ with $0 \leq r \leq 2$, and define B to be the subset of Ω consisting of the pairs $\{1,2\}, \{2,3\}, \{4,5\}, \{5,6\}, \dots, \{3l-2, 3l-1\}, \{3l-1, 3l\}$ (adding also $\{3l, 3l+1\}$ if $r = 2$). It is easy to see that B is a base so that $b(G) \leq \frac{2}{3}k + 1$ in this example.

(4) If $G = PGL_d(q)$ acting on the set Ω of 1-spaces in the underlying vector space $V_d(q)$, then $b(G) = d+1$, a minimal base being $\{\langle v_1\rangle, \dots, \langle v_d\rangle, \langle v_1 + \dots + v_d\rangle\}$, where $v_1, \dots, v_d$ is a basis for $V_d(q)$.

(5) Let G be the affine group $AGL_d(q)$ acting on $V_d(q)$, of degree q^d. Then $b(G) = d+1$.

(6) Let $G = S_2 \wr C_k$ in its natural imprimitive, transitive representation of degree $2k$ having k blocks of imprimitivity of size 2. Then $b(G) = k$.

If $\{\omega_1, \dots, \omega_b\}$ is a base for G of size $b = b(G)$, then

$$|G| = |G : G_{\omega_1 \dots \omega_b}| = |G : G_{\omega_1}|\, |G_{\omega_1} : G_{\omega_1\omega_2}| \dots |G_{\omega_1 \dots \omega_{b-1}} : G_{\omega_1 \dots \omega_b}|.$$

Each term on the right hand side is at most n and at least 2, and so we have

Proposition 1.1 *We have* $2^{b(G)} \leq |G| \leq n^{b(G)}$. *Consequently*

$$\log_2 |G| \geq b(G) \geq \frac{\log |G|}{\log n}.$$

In examples (1), (3), (4) and (5) above we see that $b(G) \sim \frac{\log |G|}{\log n}$ (where $f \sim g$ means that f/g is bounded between two positive constants); whereas in example (6), $b(G) \sim \log |G|$.

Despite the elementary nature of Proposition 1.1, the connection it gives between the order of G and the value of $b(G)$ has been much exploited, leading to a number of important results and conjectures which we shall discuss below.

2 General bounds

The problem of bounding the order of a primitive permutation group of degree n not containing A_n is one of the oldest in permutation group theory, going back to the 19th century. One of the principal methods is to bound $b(G)$ and use Proposition 1.1. The most striking early result is due to Bochert:

Theorem 2.1 (Bochert [5]) *If G is a primitive permutation group of degree n not containing A_n, then $b(G) \leq \frac{n}{2}$.*

Using Proposition 1.1 it follows from this that $|G| \leq n^{n/2}$.

Almost a hundred years later, Babai proved the first substantial improvement of Bochert's result:

Theorem 2.2 (Babai [1, 2]) *Let G a primitive permutation group of degree n not containing A_n.*

(i) *If G is not 2-transitive then $b(G) < 4\sqrt{n} \log n$.*

(ii) *If G is 2-transitive then $b(G) < c^{\sqrt{\log n}}$, where c is an absolute constant.*

The 2-transitive case was improved by Pyber:

Theorem 2.3 (Pyber [16]) *If G is a 2-transitive group of degree n not containing A_n, then $b(G) < c \log^2 n$, where c is an absolute constant.*

Note that Example (3) in the Introduction gives a primitive, not 2-transitive group of base size $c\sqrt{n}$; and Examples (4), (5) give 2-transitive groups of base size $c \log n$. This shows that the bounds in Theorems 2.2(i) and 2.3 are not far off best possible.

The above results were proved using combinatorial methods, in particular not using the classification of finite simple groups.

The first general result on base sizes using the classification was the following:

Theorem 2.4 (Liebeck [11]) *If G is a primitive group of degree n, then either*

(i) *$b(G) < 9 \log_2 n$, or*

(ii) *G is a subgroup of $S_m \wr S_r$ containing $(A_m)^r$, where the action of S_m is on k-sets and the wreath product has the product action of degree $\binom{m}{k}^r$.*

Using this one can easily deduce a sharp result of the form $b(G) \leq c\sqrt{n}$ for primitive groups and $b(G) < c \log n$ for 2-transitive groups (where $G \not\geq A_n$), somewhat improving the classification-free results 2.2 and 2.3.

3 Conjectures of Babai and Cameron

In this section we discuss some conjectures and results concerning base sizes of some important classes of primitive permutation groups. The first conjecture stems from the following well known result.

Theorem 3.1 (Babai-Cameron-Pálfy [3]) *Let d be a positive integer, and let G be a primitive group of degree n not involving A_d as a section. Then $|G| < n^{f(d)}$, where $f(d)$ depends only on d.*

The function $f(d)$ obtainable from the proof in [3] is of the form $O(d \log d)$. A new proof by Pyber (unpublished) shows that $f(d)$ can be chosen to be linear in d.

Seeking a structural explanation of this result in the light of Proposition 1.1, Babai conjectured that any group G as in the statement has a base of size bounded in terms of d alone. The first indication that this might be true came from analysis of the solvable case:

Theorem 3.2 (Seress [18]) *If G is a solvable primitive permutation group, then $b(G) \leq 4$.*

This corresponds very closely to the rather tight bound $|G| < 24^{-1/3} n^{3.244}$ on the order of a primitive solvable group G obtained in [15, 20]; indeed, the bound of 4 in Theorem 3.2 is best possible, since there are primitive solvable groups of order larger than n^3.

Babai's conjecture was finally proved:

Theorem 3.3 (Gluck-Seress-Shalev [10]) *There exists a function $g(d)$ such that if G is a primitive group not involving A_d, then $b(G) < g(d)$.*

The proof in [10] shows that $g(d)$ can be chosen as a quadratic function of d. This is improved to a linear function in [13, 1.4].

The other class of primitive groups we shall discuss in this section are the almost simple primitive groups. Here again there is a result on orders:

Theorem 3.4 (Liebeck [11]) *If G is an almost simple primitive permutation group of degree n, then one of the following holds:*

(i) $|G| < n^9$;

(ii) $F^*(G) = A_m$ *acting on k-subsets or an orbit of partitions of $\{1, \ldots, m\}$;*

(iii) $F^*(G)$ *is a classical group in a subspace action.*

In (iii), a *subspace* action of a classical group $G_0 = F^*(G)$ with natural module V is a primitive action on an orbit of subspaces of V, or pairs of subspaces of complementary dimensions (when $G_0 = PSL(V)$ and G contains a graph automorphism), or on the cosets of an orthogonal subgroup $O^{\pm}_{2m}(q) < G_0 = Sp_{2m}(q)$ with q even.

A version of this result with n^c in (i) (c unspecified) appeared in [6, 6.1]; and an improvement with n^5 replacing n^9 in (i), allowing also the exceptions $G = M_n$ with $n \in \{23, 24\}$, appears in [12, Proposition 2].

Definition We call primitive actions of groups as in (ii) or (iii) of Theorem 3.4 *standard* actions.

It is natural to ask whether there is a base-size analogue of Theorem 3.4, and indeed the following conjecture was posed by Cameron.

Conjecture 3.5 (Cameron [7, 3.4]) *There is a constant c such that if G is an almost simple primitive group in a non-standard action, then $b(G) < c$.*

In [8], Cameron and Kantor suggested a probabilistic strengthening of this conjecture: if G is as above, then almost every c-tuple is a base for G. This has now been established:

Theorem 3.6 (Liebeck-Shalev [13, 1.3]) *There is a constant c such that if G is an almost simple primitive group in a non-standard action, then the probability that a random c-tuple of points from the permutation domain forms a base for G tends to 1 as $|G| \to \infty$. In particular, Cameron's conjecture holds.*

For G an alternating or symmetric group, Theorem 3.6 was proved by Cameron and Kantor [8] with $c = 2$.

The proofs of Theorems 3.3 and 3.6 use results on fixed point ratios as a main tool, as we shall now discuss. For a permutation group G on a set Ω of size n, and an element $x \in G$, define $\mathrm{fix}(x)$ to be the number of fixed points of x and $\mathrm{rfix}(x) = \mathrm{fix}(x)/n$. Thus $\mathrm{rfix}(x)$ is the probability that a random point of Ω is fixed by x. Therefore the probabilibity that a random k-tuple is fixed by x is $\mathrm{rfix}(x)^k$. If a given k-tuple is not a base, then it is fixed by some element $x \in G$ of prime order. Hence if $Q(G,k)$ is the probability that a random k-tuple is not a base for G, then

$$Q(G,k) \leq \sum \mathrm{rfix}(x)^k, \qquad (\dagger)$$

the sum being over elements $x \in G$ of prime order.

Now assuming G is primitive and M is a point stabilizer, we have $\mathrm{rfix}(x) = |x^G \cap M|/|x^G|$. In the crucial case where G is an almost simple group of Lie type in a non-standard action, it is established in [13, Theorem (*)] that this ratio is bounded above by $|x^G|^{-\epsilon}$, where ϵ is a positive constant. Plugging this into (†) and choosing k large enough (greater than $11/\epsilon$ will do), it is possible to deduce that $Q(G,k) \to 0$ as $|G| \to \infty$, which is enough to prove Theorem 3.6.

As for Theorem 3.3, the proof starts with a far from straightforward reduction to the cases where G is almost simple, or of affine type with a point stabilizer G_0 being a primitive linear group. Define $\mathrm{rfix}(G)$ to be the maximum value of $\mathrm{rfix}(x)$ for $1 \neq x \in G$. Then (†) gives

$$Q(G,k) \leq |G|\mathrm{rfix}(G)^k.$$

In the two cases above, it is shown in [10] that the right hand side tends to 0 as $|G| \to \infty$ for a suitable choice of $k = g(d)$. Thus in fact a stronger, probabilistic form of Theorem 3.3 holds for these types of primitive groups.

4 Pyber's Conjecture

A conjecture for arbitrary primitive groups which generalizes the conjectures in the previous section was formulated by Pyber in [17]:

Conjecture 4.1 (Pyber) *There is a constant c, such that if G is a primitive permutation group of degree n, then*

$$b(G) < c\frac{\log |G|}{\log n}.$$

Note that this conclusion does not hold for all transitive groups G, as is shown by Example (6) of the Introduction.

Seress [19] has shown that to prove Pyber's conjecture, it is sufficient to establish it in the cases where G is either almost simple or of affine type.

Suppose first that G is almost simple. If the action is non-standard, then by Theorem 3.6, $b(G)$ is bounded above by a constant, and so Pyber's conjecture holds in this case. For standard actions, Benbenishty [4] has verified that Pyber's conjecture holds. Hence we have

Theorem 4.2 *Pyber's conjecture holds for almost simple groups.*

Now suppose that G is affine. Here $G \leq AGL(V)$, where V is a finite vector space of order $n = p^d$ (p prime); identifying V with the group of translations we have $G = VH$, where the point stabilizer $H = G_0$ is an irreducible subgroup of $GL(V)$, and $b(G) = 1 + b(H)$ (where $b(H)$ is the minimal size of a base for H in its action on vectors).

A couple of special cases of the problem have appeared: the solvable case (see Theorem 3.2), and the case where H is a p'-group. In the latter case Gluck and Magaard [9] show that $b(H) \leq 95$.

Recently we have solved the case in which H acts primitively as a linear group on V (in other words, H does not preserve any non-trivial direct sum decomposition of V).

Theorem 4.3 (Liebeck-Shalev [14]) *There is a constant c such that if $H \leq GL(V)$ is an irreducible, primitive linear group on a finite vector space V, then either*

(i) $b(H) < c$, *or*

(ii) $b(H) < 18\frac{\log |H|}{\log |V|} + 27$.

In proving this result, we study the structure of primitive linear groups which have unbounded base sizes. The first step is to analyse quasisimple linear groups. Here are some obvious examples of such groups having unbounded base sizes.

(1) Let $H = Cl_d(q)$, a classical group with natural module V of dimension d over $\mathbb{F}_q$. Then in its action on V, we have $b(H) \sim d$.

(2) Let $H = Cl_d(q^{1/r})$, where $\mathbb{F}_{q^{1/r}}$ is a subfield of $\mathbb{F}_q$, and take H to act naturally on $V = V_d(q)$. If $v_1, \ldots, v_d$ is an $\mathbb{F}_q$-basis of V, and $\lambda_1, \ldots, \lambda_r$ is a basis

for $\mathbb{F}_q$ over $\mathbb{F}_{q^{1/r}}$, then $\sum_1^r \lambda_i v_i, \sum_1^r \lambda_i v_{r+i}, \ldots$ is a base for H, and hence we see that $b(H) \sim d/r$ in the unbounded case.

(3) Let $H = A_{d+\delta}$ ($\delta = 1$ or 2) acting on its irreducible deleted permutation module $V = V_d(q)$ over $\mathbb{F}_q$. It is straightforward to see that $b(H) \sim \log d / \log q$ in the unbounded case.

An important intermediate result in [14] shows that these are the only examples of quasisimple groups with unbounded base sizes:

Proposition 4.4 ([14, 2.2]) *If $H \leq GL_d(q)$ with $E(H)$ quasisimple and absolutely irreducible on $V_d(q)$, then either*

(i) *$b(H) < c$ for some absolute constant c, or*

(ii) *$E(H) = Cl_d(q^{1/r})$ or $A_{d+\delta}$ as in Examples (2), (3) above.*

In the statement, $E(H)$ as usual denotes the product of all quasisimple subnormal subgroups of H.

Note that Proposition 4.4 does not require the assumption of primitivity of H as a linear group.

The next step in the proof involves analysis of tensor products, and we present another couple of examples.

(4) Let $V = V_m(q) \otimes V_m(q)$, and let $H = GL_m(q) \otimes GL_m(q)$ acting naturally on V (where $GL_m(q) \otimes GL_m(q)$ denotes the image of $GL_m(q) \times GL_m(q)$ in $GL(V)$). We claim that $b(H) \leq 3$. To see this, identify V with $M_m(q)$, the space of all $m \times m$ matrices over $\mathbb{F}_q$, with H-action $(g,h) : A \to g^T A h$ for $g, h \in GL_m(q)$, $A \in V$. Then the stabilizer of the identity matrix, $H_I = \{(h^{-T}, h) : h \in GL_m(q)\}$, and (h^{-T}, h) sends A to $h^{-1}Ah$. It is well known that $SL_m(q)$ is 2-generated, say $SL_m(q) = \langle C, D \rangle$. Then $H_{I,C,D} = 1$, proving the claim.

(5) Extending the previous example, it can be shown that if $V = V_a(q) \otimes V_b(q)$ with $a \leq b$, and $H = Cl_a(q) \otimes Cl_b(q^{1/r})$ acting naturally on V, then either $b(H)$ is bounded or $b(H) \sim b/ar$.

Here is our structure theorem, on which the proof of Theorem 4.3 is based. It is a simplified version of [14, Theorem 2].

Theorem 4.5 ([14]) *Suppose $H \leq GL_d(q)$ is primitive and absolutely irreducible. Then one of the following holds:*

(i) *$b(H) < c$ for some absolute constant c;*

(ii) *$H \leq GL_a(q) \otimes Cl_b(q^{1/r})$ ($d = ab$), H contains the factor $Cl_b(q^{1/r})'$, and $b(H) \sim b/ar$;*

(iii) *$H \leq GL_a(q) \otimes S_{b+\delta}$ ($d = ab, \delta = 1$ or 2), H contains the factor $A_{b+\delta}$, and $b(H) \sim \log b/(a \log q)$.*

In view of the above results, to complete the proof of Pyber's conjecture it remains to handle the affine case where the linear group $H = G_0$ acts imprimitively on V.

References

[1] L. Babai, On the order of uniprimitive permutation groups, *Ann. of Math.* **113** (1981), 553–568.

[2] L. Babai, On the order of doubly transitive permutation groups, *Invent. Math.* **65** (1982), 473–484.

[3] L. Babai, P.J. Cameron and P. Pálfy, On the orders of primitive groups with restricted nonabelian composition factors, *J. Algebra* **79** (1982), 161–168.

[4] C. Benbenishty, Base sizes of standard actions of alternating and classical groups, to appear.

[5] A. Bochert, Über die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann, *Math. Ann.* **33** (1889), 584-590.

[6] P.J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), 1–22.

[7] P.J. Cameron, Some open problems on permutation groups, in *Groups, combinatorics and geometry* (eds. M. Liebeck and J. Saxl), pp.340–350, London Math. Soc. Lecture Note Ser., 165, Cambridge Univ. Press, Cambridge, 1992.

[8] P.J. Cameron and W.M. Kantor, Random permutations: some group-theoretic aspects, *Combin. Probab. Comput.* **2** (1993), 257–262.

[9] D. Gluck and K. Magaard, Base sizes and regular orbits for coprime affine permutation groups, *J. London Math. Soc.* **58** (1998), 603–618.

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

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

[12] M.W. Liebeck and J. Saxl, Maximal subgroups of finite simple groups and their automorphism groups, *Contemp. Math.* **131** (1992), 243-259.

[13] M.W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497-520.

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

[15] P.P. Pálfy, A polynomial bound for the orders of primitive solvable groups, *J. Algebra* **77** (1982), 127-137.

[16] L. Pyber, On the orders of doubly transitive permutation groups, elementary estimates, *J. Combin. Theory Ser. A* **62** (1993), 361–366.

[17] 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, pp.197-219, Amer. Math. Soc., Providence, 1993.

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

[19] A. Seress, Bases for non-affine primitive groups, to appear.

[20] T.R. Wolf, Solvable and nilpotent subgroups of $\mathrm{GL}(n, q^m)$, *Canad. J. Math.* **34** (1982), 1097–1111.