Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

On base sizes for symmetric groups

Timothy C. Burness, Robert M. Guralnick and Jan Saxl

Abstract

A base of a permutation group G on a set Ω is a subset B of Ω such that the pointwise stabilizer of B in G is trivial. The base size of G, denoted by $b(G)$, is the minimal cardinality of a base. Let $G = S_n$ or A_n acting primitively on a set with point stabilizer H. In this note we prove that if H acts primitively on $\{1, \ldots, n\}$, and does not contain A_n, then $b(G) = 2$ for all $n \geq 13$. Combined with a theorem of James, this completes the classification of primitive actions of alternating and symmetric groups which admit a base of size two.

1. *Introduction*

Let G be a transitive permutation group on a finite set Ω with point stabilizer H. A *base* for G is a subset B of Ω such that the pointwise stabilizer of B in G is trivial. The *base size* of G, denoted by $b(G)$, is the minimal cardinality of a base for G. Equivalently, $b(G)$ is the minimal cardinality of a set of conjugates of H such that their intersection is trivial. Bases arise in estimating the orders of primitive permutation groups (see [**1**], for example) and in more recent years they have played an essential role in the computational study of groups (see [**17**] and [**18**], for example).

According to a theorem of Liebeck and Shalev [**15**, Theorem 1.3], there is a constant c such that if G is an almost simple primitive permutation group on a set Ω then either $b(G) \leq c$, or G and Ω belong to a short explicit list of exceptions. The exceptions involve the action of A_n or S_n on subsets or partitions of $\{1, \ldots, n\}$, and the action of classical groups on subspaces of the natural module. In general, $b(G)$ is unbounded in these cases since $|G|$ is not bounded above by a fixed polynomial of $|\Omega|$.

This theorem had first been conjectured by Cameron and Kantor in [**10**], where they prove the conjecture in the alternating group case by establishing a strong asymptotic result with the constant c taken to be 2. More precisely, they prove that if $G = S_n$ or A_n, and the stabilizer

2000 *Mathematics Subject Classification* 20B15 (primary), 20B30, 20D06, 20P05 (secondary).

The second author was partially supported by the NSF grant DMS 0653873.

of a point acts primitively on $\{1,\ldots,n\}$ and does not contain A_n, then the probabiity that a random pair of points in Ω form a base for G tends to 1 as n tends to infinity. In particular, there exists a constant N such that $b(G) = 2$ for all $n \geq N$.

Our main theorem reveals that $N = 13$ is best possible.

THEOREM 1. *Let $G = S_n$ or A_n acting primitively on a set with point stabilizer H. Assume that H acts primitively on $\{1,\ldots,n\}$ and does not contain A_n. Then $b(G) \leq 3$ for all $n \geq 11$, with equality if and only if $(G,H) = (A_{11}, \mathrm{M}_{11})$ or $(A_{12}, \mathrm{M}_{12})$.*

For such actions, close inspection of the small degree groups yields the following the result.

COROLLARY 2. *If $n \geq 5$ and $b(G) > 2$ then $(b(G), G, H)$ is listed in Table 1.*

REMARK 3. In the terminology of [**4**, **7**, **8**], Corollary 2 implies that $b(G) \leq 3$ for any *non-standard* permutation group with socle A_n, with equality only possible if $n \leq 12$. Indeed, the examples with $b(G) > 3$ in the statement of Corollary 2 are isomorphic to standard permutation groups. For instance, $A_8 \cong \mathrm{PSL}_4(2)$ and the action of A_8 on the cosets of $\mathrm{AGL}_3(2)$ is equivalent to the action of $\mathrm{PSL}_4(2)$ on 1-dimensional subspaces of the natural module.

In [**14**], James studies the primitive action of S_n on partitions of $\{1,\ldots,n\}$. Combined with Theorem 1, this yields a classification of the primitive actions of symmetric groups which admit a base of size two (see Corollary 4). In his thesis [**13**], James extends his analysis of partition actions to the alternating groups, and using [**13**, Theorem 1.1.13] we deduce Corollary 5 below.

COROLLARY 4. *Let $G = S_n$ with $n \geq 5$ acting primitively on a set with point stabilizer H. Then either $b(G) = 2$, or (n,H) is one of the following:*

TABLE 1. *Some primitive actions with $b(G) > 2$*

$b(G)$	(G,H)
5	$(S_6, \mathrm{PGL}_2(5))$
4	$(A_8, \mathrm{AGL}_3(2)), (A_6, \mathrm{PSL}_2(5))$
3	$(A_{12}, \mathrm{M}_{12}), (A_{11}, \mathrm{M}_{11}), (S_{10}, \mathrm{P\Gamma L}_2(9)), (S_9, \mathrm{AGL}_2(3)), (A_9, \mathrm{P\Gamma L}_2(8))$
	$(S_8, \mathrm{PGL}_2(7)), (A_7, \mathrm{PSL}_2(7)), (S_5, 5{:}4), (A_5, D_{10})$

(i) $H = S_k \times S_{n-k}$ *with* $k < n/2$;

(ii) $H = S_2 \wr S_l$ *and* $n = 2l$;

(iii) $H = S_k \wr S_l$, $n = kl$ *with* $k \geq 3$ *and* $l < \max\{8, k+3\}$;

(iv) $(n, H) = (10, \mathrm{P\Gamma L}_2(9)), (9, \mathrm{AGL}_2(3)), (8, \mathrm{PGL}_2(7)), (6, \mathrm{PGL}_2(5))$ *or* $(5, 5{:}4)$.

Corollary 5. *Let* $G = A_n$ *with* $n \geq 5$ *acting primitively on a set with point stabilizer* H. *Then either* $b(G) = 2$, *or* (n, H) *is one of the following:*

(i) $H = (S_k \times S_{n-k}) \cap G$ *with* $k < n/2$;

(ii) $H = (S_2 \wr S_l) \cap G$ *and* $n = 2l$;

(iii) $H = (S_k \wr S_l) \cap G$, $n = kl$ *with* $k \geq 3$, *and either* $l < k+2$, *or* $l = k+2 \in \{5, 6\}$;

(iv) $(n, H) = (12, \mathrm{M}_{12}), (11, \mathrm{M}_{11}), (9, \mathrm{P\Gamma L}_2(8)), (8, \mathrm{AGL}_3(2)), (7, \mathrm{PSL}_2(7)), (6, \mathrm{PSL}_2(5))$ *or* $(5, D_{10})$.

Remark 6. It is interesting to consider the base size of the permutation groups arising in cases (i) - (iii) of Corollary 4.

(i) Here Ω is the set of k-element subsets of $\{1, \ldots, n\}$; in general, the exact base size is not known. Perhaps the best result to date is due to Z. Halasi [**12**], which states that

$$b(G) \geq \left\lceil \frac{2n-2}{k+1} \right\rceil,$$

with equality if $n \geq k^2 - 1$. We thank Dr Halasi for providing us with a very elegant proof of this result. Since $b(G) \geq \log_2 n$ for all k, we note that this bound is not sharp when k is large.

(ii) We claim that $b(G) = 3$. To see this, first observe that H is the centralizer of a fixed point free involution. Embed the dihedral group D of order n into S_n via the regular representation. Note that D is generated by a pair x_1, x_2 of fixed point free involutions, so $C = C_G(D)$ is isomorphic to D (its "opposite"). It is easy to produce a fixed point free involution x_3 that does not commute with any element of C (by counting, for example), so $\bigcap_i C_G(x_i)$ is trivial. Therefore $b(G) \leq 3$, and thus equality holds since $|H|^2 > |G|$.

(iii) We refer the reader to [**2**], where explicit upper bounds on $b(G)$ are given.

Remark 7. For completeness, let us consider the three additional almost simple groups with socle A_6. If $G \neq A_6, S_6$ is an almost simple group with socle A_6, acting primitively on a set with point stabilizer H, then it is easy to check that either $b(G) = 2$, or one of the following holds:

(i) $b(G) = 4$ and $(G, H) = (A_6.2^2, \mathrm{AGL}_1(9).2)$; or

(ii) $b(G) = 3$ and (G, H) is one of the following:

$$(A_6.2^2, [32]), (A_6.2^2, D_{20}.2), (\mathrm{M}_{10}, \mathrm{AGL}_1(9)), (\mathrm{PGL}_2(9), D_{20}), (\mathrm{PGL}_2(9), 3^2{:}Q_8),$$

where [32] denotes a Sylow 2-subgroup of $A_6.2^2$.

In a series of recent papers, explicit versions of the aforementioned theorem of Liebeck and Shalev have been obtained for various families of simple groups. In [**4**, **7**], it is proved that $b(G) \leq 6$ for any almost simple primitive group G of Lie type (excluding subspace actions of classical groups, of course). Precise base sizes are computed in [**8**] for sporadic groups; the main result states that $b(G) \leq 7$, with equality if and only if $G = \mathrm{M}_{24}$ acting on 24 points. In [**9**, p.122], Cameron conjectured that $c = 7$ is the best possible constant in the Liebeck-Shalev theorem, so in view of the above results we see that Corollary 2 provides the final step in the proof of this conjecture.

Corollary 8. *Cameron's base size conjecture is true.*

In the forthcoming paper [**5**] we establish an analogue of Theorem 1 for primitive actions of finite almost simple classical groups, extending the results of [**4**]. Excluding subspace actions, we show that in most cases there is a base of size 2, and we completely classify the exceptions. Following [**10**], we also obtain strong asymptotic results on the probability that a random pair of points form a base. We extend our analysis to simple algebraic groups in [**6**], where we compute the precise base size for most primitive actions of such groups (including subspace actions of classical algebraic groups). In particular, we establish an analogue of Corollary 8 for algebraic groups.

2. *Preliminaries*

Our main tool is the following easy lemma.

Lemma 2.1. *Let G be a finite group, let H be a subgroup of G with $H = N_G(H)$, and let $x_1, \ldots, x_k$ represent the distinct G-classes of elements of prime order in H. If $H \cap H^x \neq 1$ for all $x \in G$ then*

$$\sum_{i=1}^{k} |x_i^G \cap H|^2 |C_G(x_i)| \geq |G|.$$

In particular, if $H \cap H^x \neq 1$ for all $x \in G$ then

$$|H|^2 \max |C_G(x)| \geq |G|,$$

where the maximum is taken over all elements $x \in H$ of prime order.

Proof. Let $x \in H$ be an element of prime order. The number of distinct conjugates of H containing x is given by the formula

$$(|x^G \cap H|/|x^G|) \cdot |G : H|,$$

whence the number of distinct conjugates of H containing some element of $x^G \cap H$ is at most

$$|x^G \cap H|^2 \ |C_G(x)|/|H|.$$

If the first asserted inequality fails, it follows that there is a conjugate H^y which does not contain any prime order elements of H, whence $H \cap H^y = 1$. The second assertion is an obvious consequence of the first. □

Corollary 2.2. *Let G be a primitive permutation group on a finite set Ω with point stabilizer H. Then $b(G) = 2$ if*

$$\sum_{i=1}^{k} |x_i^G \cap H|^2 |C_G(x_i)| < |G|,$$

where $x_1, \ldots, x_k$ represent the distinct G-classes of elements of prime order in H.

3. *Proof of Theorem 1*

Let $G = S_n$ or A_n acting primitively on a set Ω with point stabilizer H. Assume that H acts primitively on $\{1, \ldots, n\}$ and does not contain A_n. The cases with $n < 40$ can be checked by hand, although it is convenient and straightforward to verify the results with the aid of Magma [**3**]. For the remainder we will assume $n \geq 40$.

To begin with, let us exclude the following two cases:

(a) $H = (S_l \wr S_k) \cap G$ with the natural product action on $n = l^k$ points;

(b) $H = S_l$ or A_l, acting on m-element subsets of $\{1, \ldots, l\}$ (so $n = \binom{l}{m}$).

Then by a theorem of Maróti [**16**, Theorem 1.1] we have

$$|H| \leq n^{1+\lfloor \log_2 n \rfloor}.$$

In addition, except for one family which involves the action of orthogonal groups over the field of two elements on a set of hyperplanes, the minimal degree of H is at least $n/2$ (see [**11**, Theorem 1]). Therefore, with this exception,

$$|C_G(x)| \leq 2^{n/4}\lceil n/4\rceil!\lceil n/2\rceil!$$

for all non-trivial $x \in H$. (Note that equality holds when n is divisible by 4 and x has cycle-shape $(2^{n/4}, 1^{n/2})$.) Since $n \geq 40$ we deduce that $|H|^2 \max|C_G(x)| < |G|$, whence $b(G) = 2$ by Corollary 2.2.

A similar calculation applies for the exceptional family of orthogonal groups over the field of two elements. Indeed, if H is of type $O_{2l+1}(2)$ or $O_{2l}^{+}(2)$ then $n = 2^{l-1}(2^l - 1)$ and the minimal degree of H is $n/2 - 2^{l-2}$; for $O_{2l}^{-}(2)$ we have $n = (2^l + 1)(2^{l-1} - 1)$ and the minimal degree is $n/2 - (2^{l-1} - 1)/2$ (see [**11**, Theorem 1] for these facts). The previous argument now goes through essentially unchanged. Therefore, to complete the proof, it remains to deal with the excluded cases (a) and (b) above.

First consider (a). Without loss of generality, we may assume $G = S_n$, so $H = S_l \wr S_k$ with the product action on $n = l^k$ points. We give details in the case $k = 2$ – the other cases are much easier. Here $n = l^2$ for some integer $l \geq 7$. By Corollary 2.2, it suffices to show that

$$\sum_{i=1}^{k'} |x_i^G \cap H|^2 |C_G(x_i)| + \sum_{i=k'+1}^{k} |x_i^G \cap H|^2 |C_G(x_i)| < |G|, \tag{3.1}$$

where $x_1, \ldots, x_{k'}$ represent the distinct G-classes of involutions in H, and $x_{k'+1}, \ldots, x_k$ the G-classes of elements of odd prime order. Let $i_2(H)$ denote the number of involutions in H.

The number of involutions in S_l is equal to the sum of the degrees of the complex irreducible characters of S_l, and hence is bounded above by $p(l)l!^{1/2}$, where $p(l)$ is the number of partitions of l. In H there are precisely $l!$ involutions outside the base group S_l^2, whence

$$i_2(H) \leq (1 + p(l)l!^{1/2})^2 - 1 + l! \leq l!(1 + p(l))^2.$$

The centralizer in G of any involution in H has order at most $2^l l!(l^2 - 2l)!$, so

$$\sum_{i=1}^{k'} |x_i^G \cap H|^2 |C_G(x_i)| \leq i_2(H)^2 \max|C_G(x_i)| \leq l!^2(1 + p(l))^4 2^l l!(l^2 - 2l)! < |G|/2,$$

since

$$l!^3(1 + p(l))^4 2^{l+1} < (l - 1)^{4l} < (l^2)!/(l^2 - 2l)!.$$

Now let us turn to elements of odd order. The centralizer in G of any non-identity element of odd order in H has order at most $3^l l!(l^2 - 3l)!$, so

$$\sum_{i=k'+1}^{k} |x_i^G \cap H|^2 |C_G(x_i)| < |H|^2 3^l l!(l^2 - 3l)! < |G|/2$$

and we conclude that $b(G) = 2$, as required.

Finally, let us turn to case (b), so $H = S_l$ or A_l acting on the set of m-element subsets of $\{1, \ldots, l\}$, and thus $n = \binom{l}{m}$. Here we consider just the action on pairs of elements – the other cases are similar and easier. We have $n = l(l-1)/2$ and we proceed as in the previous case, separately estimating the contributions from involutions and elements of odd prime order. The maximal size of the centralizer in G of an involution in H is $2^{l-2}(l-2)![(l^2-5l+8)/2]!$, while that of an element of odd prime order is at most $3^{l-2}(l-2)![(l^2-7l+12)/2]!$. From these bounds we quickly deduce that (3.1) holds, hence $b(G) = 2$.

This completes the proof of Theorem 1.

References

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

2. C. Benbenishty, J. A. Cohen and A. C. Niemeyer, 'The minimum length of a base for the symmetric group acting on partitions', *European J. Combin.* 28 (2007) 1575–1581.

3. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system I: The user language', *J. Symbolic Comput.* 24 (1997) 235–265.

4. T. C. Burness, 'On base sizes for actions of finite classical groups', *J. London Math. Soc.* 75 (2007) 545–562.

5. T. C. Burness, R. M. Guralnick and J. Saxl, 'Base sizes for finite classical groups', in preparation.

6. T. C. Burness, R. M. Guralnick and J. Saxl, 'On base sizes for algebraic groups', in preparation.

7. T. C. Burness, M. W. Liebeck and A. Shalev, 'Base sizes for simple groups and a conjecture of Cameron', *Proc. London Math. Soc.* 98 (2009) 116–162.

8. T. C. Burness, E. A. O'Brien and R. A. Wilson, 'Base sizes for sporadic simple groups', *Israel J. Math.* 177 (2010) 307–334.

9. P. J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts, vol. 45 (Cambridge University Press, 1999).

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

11. R. M. Guralnick and K. Magaard, 'On the minimal degree of a primitive permutation group', *J. Algebra* 207 (1998) 127–145.

12. Z. Halasi, private communication.

13. J. P. James, 'Two point stabilisers of partition actions of symmetric, alternating and linear groups', Ph.D. thesis (University of Cambridge, 2006).

14. J. P. James, 'Partition actions of symmetric groups and regular bipartite graphs', *Bull. London Math. Soc.* 38 (2006) 224–232.

15. M. W. Liebeck and A. Shalev, 'Simple groups, permutation groups, and probability', *J. Amer. Math. Soc.* 12 (1999) 497–520.

16. A. Maróti, 'On the orders of primitive groups', *J. Algebra* 258 (2002) 631–640.

17. Á. Seress, *Permutation Group Algorithms*, Cambridge Tracts in Mathematics, vol. 152, (Cambridge University Press, Cambridge, 2003).

18. C. C. Sims, *Computation with permutation groups*, Proc. Second Sympos. on Symbolic and Algebraic Manipulation (ACM, New York, 1971), pp. 23–28.

Timothy C. Burness
School of Mathematics
University of Southampton
Southampton SO17 1BJ
UK

t.burness@soton.ac.uk

Robert M. Guralnick
Department of Mathematics
University of Southern California
Los Angeles CA 90089
USA

guralnic@usc.edu

Jan Saxl
DPMMS
University of Cambridge
Cambridge CB3 0WB
UK

j.saxl@dpmms.cam.ac.uk