Base sizes for sporadic simple groups

Timothy C. Burness
Institute of Mathematics
Hebrew University of Jerusalem
Jerusalem 91904
Israel

E.A. O'Brien
Department of Mathematics
University of Auckland
Auckland
New Zealand

Robert A. Wilson
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS
UK

July 6, 2009

Abstract

Let G be a permutation group acting on a set Ω. A subset of Ω is a base for G if its pointwise stabilizer in G is trivial. We write $b(G)$ for the minimal size of a base for G. We determine the precise value of $b(G)$ for every primitive almost simple sporadic group G, with the exception of two cases involving the Baby Monster group. As a corollary, we deduce that $b(G) \leqslant 7$, with equality if and only if G is the Mathieu group M_{24} in its natural action on 24 points. This settles a conjecture of Cameron.

1 Introduction

If G is a permutation group on a set Ω then a subset $B \subseteq \Omega$ is a *base* for G if the pointwise stabilizer of B in G is trivial. We write $b(G)$ for the minimal size of a base for G. This notion dates back to the early days of group theory in the nineteenth century. For instance, a classical result of Bochert [4] states that $b(G) \leqslant n/2$ if G is a primitive permutation group of degree n not containing A_n.

In more recent years, following the seminal work of Sims [28] in the early 1970s, bases have been used extensively in the computational study of finite permutation groups. For example, we observe that the elements of G are uniquely determined by their action on a base B, hence each element can be stored as a $|B|$-tuple, rather than a $|\Omega|$-tuple. Consequently, small bases are particularly important from a computational point of view. For further discussion of this topic, see, for example, [26, Chapter 4].

Base sizes for almost simple primitive permutation groups have been much studied in recent years (see [8, 10, 11, 18, 19, 20], for example). A major motivation comes from a well-known conjecture of Cameron and Kantor [12, 14] on *non-standard actions*. Roughly speaking, if G is a finite almost simple group with socle G_0 then a primitive G-set Ω is *standard* if either $G_0 = A_n$ and Ω is an orbit of subsets or partitions of $\{1, \ldots, n\}$, or G is a classical group in a subspace action, i.e. Ω is an orbit of subspaces of the natural G-module, or pairs of subspaces of complementary dimension. Non-standard (primitive) actions are defined accordingly.

E-mail: burness@math.huji.ac.il, e.obrien@auckland.ac.nz, r.a.wilson@qmul.ac.uk

The Cameron-Kantor Conjecture asserts that there exists an absolute constant c such that $b(G) \leqslant c$ for every almost simple group G in a faithful primitive non-standard action. This conjecture was finally settled by Liebeck and Shalev [22, 1.3] but their proof does not yield an explicit value for c. However, there has been much recent progress towards an explicit constant. Indeed, if $G_0 = A_n$ then Guralnick and Saxl have proved that $b(G) \leqslant 3$ for all non-standard actions, with equality only if $n \leqslant 12$ (see [10]). For groups of Lie type, the main results of [8] and [11] imply that $b(G) \leqslant 6$.

In this paper we obtain precise base size results for primitive actions of almost simple sporadic groups. Our main result is the following.

Theorem 1. *Let G be a finite almost simple sporadic group and let Ω be a faithful primitive G-set with point stabilizer $H = G_\alpha$. One of the following holds:*

(i) $b(G) = 2$*;*

(ii) $(G, H, b(G))$ *is listed in Table 1 or 2;*

(iii) G *is the Baby Monster,* $H = 2^{2+10+20}.(\mathrm{M}_{22} : 2 \times S_3)$ *or* $[2^{30}].\mathrm{L}_5(2)$*, and* $b(G) \leqslant 3$*.*

The following corollary is immediate.

Corollary 1. *We have $b(G) \leqslant 7$, with equality if and only if $G = \mathrm{M}_{24}$ in its natural action on 24 points.*

In the light of the results of [8, 10, 11], we deduce that Corollary 1 holds for every finite almost simple group in a faithful primitive non-standard action. In particular, we conclude that $c = 7$ is the best possible constant in the statement of the Cameron-Kantor Conjecture. This confirms an additional conjecture of Cameron (see [13, p. 122]).

Theorem 2. *Let G be a finite almost simple group and let Ω be a faithful primitive non-standard G-set. Then $b(G) \leqslant 7$, with equality if and only if $G = \mathrm{M}_{24}$ in its natural action of degree 24.*

Remark 1. We have been unable to determine the precise value of $b(G)$ when G is the Baby Monster group and H is one of the two 2-local subgroups listed in part (iii) of Theorem 1; our methods only yield $b(G) \leqslant 3$. Since $b(G) = 2$ if and only if H has a regular orbit on Ω, it may be possible to use the GAP [17] package orb [25] to compute the lengths of the H-orbits on Ω, or to at least account for sufficiently many 'large' H-orbits to allow one to decide if $b(G) = 2$ or 3. We refer the reader to [24, Table 2] for the case $(G, H) = (\mathbb{B}, \mathrm{Fi}_{23})$, and to [23, Table 1] for $(G, H) = (\mathbb{B}, 2^{1+22}.\mathrm{Co}_2)$.

Notation. We adopt the standard Atlas [16] notation. In particular, $N.H$ denotes an arbitrary extension of a group N by a group H; we write $N : H$ if the extension is split and $N \cdot H$ if it is non-split. The direct product of m copies of H is denoted H^m, while we write n for a cyclic group of order n. In particular, if p is prime then p^a is the elementary abelian group of order p^a. In addition, $[n]$ denotes an arbitrary group of order n. For classical groups, $\mathrm{S}_n(q)$ is the projective symplectic group $\mathrm{PSp}_n(q)$, while $\mathrm{O}^\epsilon_n(q)$ is the projective orthogonal group denoted by $\mathrm{P\Omega}^\epsilon_n(q)$ in [21]. As usual, S_n and A_n are respectively the symmetric and alternating groups on n letters, and D_n is the dihedral group of order n. We write $i_r(G)$ for the number of elements of order r in the group G.

Layout. In Section 2 we describe the probabilistic, character theoretic and computational techniques which we use to prove Theorem 1. In particular, in Section 2.1 we explain the connection between base sizes and fixed point ratios which plays a key role in our proof. Next, in Section 3 we record numerous results on the subgroup structure and representation

theory of the almost simple sporadic groups. The Web Atlas [32] and the GAP Character Table Library [7] are our main sources here. We provide more detailed information on the Baby Monster and the Monster in Sections 3.2 and 3.3, respectively. Finally, Section 4 is devoted to the proof of Theorem 1.

Acknowledgements. Burness acknowledges the support of a Lady Davis Fellowship from the Hebrew University of Jerusalem. O'Brien acknowledges the support of the Marsden Fund of New Zealand via grant UOA 0412. Wilson acknowledges the support of EPSRC grant GR/S41319. We thank John Bray for constructing some of the representations used, Thomas Breuer for his assistance in using GAP to study some of the character tables used, and Derek Holt for suggesting to us the double coset approach.

2 Techniques

The proof of Theorem 1 uses a combination of probabilistic, character theoretic and computational methods. In this section we introduce these techniques.

2.1 Probabilistic methods

Let G be a permutation group on a finite set Ω and let $b(G) = b(G,\Omega)$ be the minimal size of a base for G. As observed in the introduction, if $B \subseteq \Omega$ is a base then each element of G is uniquely determined by its action on B. This observation yields the following useful lower bound.

Proposition 2.1. *If G is a permutation group on a finite set Ω, then $b(G) \geqslant \lceil \log|G|/\log|\Omega| \rceil$.*

Probabilistic methods, based on fixed point ratio estimates, play an important role in the proof of Theorem 1. Recall that the *fixed point ratio* of $x \in G$, which we denote by $\mathrm{fpr}(x,\Omega)$, is the proportion of points in Ω which are fixed by x. In other words, $\mathrm{fpr}(x,\Omega)$ is the probability that a random $\alpha \in \Omega$ is fixed by x. If Ω is a transitive G-set, then it is easy to see that

$$\mathrm{fpr}(x,\Omega) = \frac{|x^G \cap H|}{|x^G|}, \tag{1}$$

where $H = G_\alpha$ is the G-stabilizer of a point $\alpha \in \Omega$.

Definition 2.2. Let G be a permutation group on a finite set Ω, with point stabilizer $H = G_\alpha$. For $c \in \mathbb{N}$ define

$$\widehat{Q}(G,c) = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i,\Omega)^c,$$

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

Proposition 2.3. *Let G be a transitive permutation group on a finite set Ω. Let c be a positive integer and let $Q(G,c)$ be the probability that a randomly chosen c-tuple of points in Ω is not a base for G. Then $Q(G,c) \leqslant \widehat{Q}(G,c)$.*

Proof. As observed in the proof of [22, 1.3], a c-tuple in Ω fails to be a base for G if and only if it is fixed by $x \in G$ of prime order, and the probability that a random c-tuple is fixed by x is at most $\mathrm{fpr}(x,\Omega)^c$. Since G is transitive, $\mathrm{fpr}(x,\Omega) = \mathrm{fpr}(y,\Omega)$ for all $y \in x^G$ (see (1)) and thus

$$Q(G,c) \leqslant \sum_{x \in \mathscr{P}} \mathrm{fpr}(x,\Omega)^c = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i,\Omega)^c = \widehat{Q}(G,c),$$

M_{11}	$A_6.2$	4	J_1	$L_2(11)$	3	McL.2	$U_4(3):2$	5
	$L_2(11)$	4					$U_3(5):2$	3
	$M_9:2$	3	J_2	$U_3(3)$	4		$3^{1+4}:4.S_5$	3
	S_5	3		$3.A_6.2$	3		$3^4:(M_{10}\times 2)$	3
				$2^{1+4}.A_5$	3		$L_3(4):2:2$	3
M_{12}	M_{11}	5		$2^{2+4}:(3\times S_3)$	3		$2.S_8$	3
	$A_6.2^2$	4		$A_4\times A_5$	3		$M_{11}\times 2$	3
	$L_2(11)$	3		$A_5\times D_{10}$	3			
	$3^2:2.S_4$	3				Co_3	McL.2	6
	$2\times S_5$	3	$J_2.2$	$U_3(3):2$	4		HS	4
	$2^{1+4}:S_3$	3		$3.A_6.2.2$	3		$U_4(3).2.2$	3
	$4^2:D_{12}$	3		$2^{1+4}.A_5.2$	3		M_{23}	3
				$2^{2+4}:(3\times S_3).2$	3		$3^5:(2\times M_{11})$	3
$M_{12}.2$	$L_2(11).2$	3		$(A_4\times A_5):2$	3		$2.S_6(2)$	3
	$(2\times 2\times A_5).2$	3		$(A_5\times D_{10}).2$	3		$U_3(5):S_3$	3
	$2^{1+4}:S_3.2$	3		$L_3(2):2\times 2$	3		$3^{1+4}:4.S_6$	3
	$4^2:D_{12}.2$	3					$2^4.A_8$	3
	$3^{1+2}:D_8$	3	J_3	$L_2(16):2$	3			
						Co_2	$U_6(2):2$	6
M_{22}	$L_3(4)$	5	$J_3.2$	$L_2(16):4$	3		$2^{10}:M_{22}:2$	4
	$2^4:A_6$	4		$(3\times M_{10}):2$	3		McL	4
	A_7	3					$2^{1+8}:S_6(2)$	4
	$2^4:S_5$	3	HS	M_{22}	5		$HS:2$	3
	$2^3:L_3(2)$	3		$U_3(5):2$	4		$(2^4\times 2^{1+6}).A_8$	3
	M_{10}	3		$L_3(4):2$	3		$U_4(3):D_8$	3
	$L_2(11)$	3		S_8	3		$2^{4+10}.(S_5\times S_3)$	3
				$2^4.S_6$	3		M_{23}	3
$M_{22}.2$	$L_3(4).2_2$	5		$4^3:L_3(2)$	3			
	$2^4:S_6$	4		M_{11}	3	He	$S_4(4):2$	4
	$2^5:S_5$	3		$4.2^4.S_5$	3		$2^2.L_3(4).S_3$	3
	$2^3:L_3(2)\times 2$	3					$2^6:3.S_6$	3
	$A_6.2^2$	3	HS.2	$M_{22}:2$	5			
	$L_2(11).2$	3		$L_3(4).2.2$	4	He.2	$S_4(4):4$	4
				$S_8\times 2$	4		$2^2.L_3(4).D_{12}$	3
M_{23}	M_{22}	6		$2^5.S_6$	3			
	$L_3(4).2b$	4		$4^3.(2\times L_3(2))$	3	Suz	$G_2(4)$	4
	$2^4:A_7$	4		$2^{1+6}.S_5$	3		$3.U_4(3):2$	3
	A_8	3		$(2\times A_6.2.2).2$	3		$U_5(2)$	3
	M_{11}	3					$2^{1+6}.U_4(2)$	3
	$2^4:(3\times A_5):2$	3	McL	$U_4(3)$	5		$3^5.M_{11}$	3
				M_{22}	4		$J_2:2$	3
M_{24}	M_{23}	7		$U_3(5)$	3		$2^{4+6}:3.A_6$	3
	$M_{22}.2$	4		$3^{1+4}:2.S_5$	3		$(A_4\times L_3(4)):2$	3
	$2^4.A_8$	4		$3^4:M_{10}$	3		$2^{2+8}:(A_5\times S_3)$	3
	$M_{12}.2$	3		$L_3(4):2$	3			
	$2^6:3.S_6$	3		$2.A_8$	3			
	$L_3(4):S_3$	3		$2^4.A_7$	3			
	$2^6:(L_3(2)\times S_3)$	3						
	$L_2(23)$	3						

Table 1: Primitive actions with $b(G) > 2$, Part I

Suz.2	$G_2(4):2$	4	Co_1	Co_2	5
	$3.U_4(3).2.2$	3		$3.Suz:2$	4
	$U_5(2):2$	3		$2^{11}:M_{24}$	3
	$2^{1+6}.U_4(2).2$	3		Co_3	3
	$3^5.(M_{11}\times 2)$	3		$2^{1+8}.O_8^+(2)$	3
	$J_2:2\times 2$	3		$U_6(2):S_3$	3
	$2^{4+6}:3.S_6$	3		$(A_4\times G_2(4)):2$	3
	$(A_4\times L_3(4):2):2$	3		$2^{2+12}:(A_8\times S_3)$	3
	$2^{2+8}:(S_5\times S_3)$	3		$2^{4+12}.(S_3\times 3.S_6)$	3
	$M_{12}:2\times 2$	3			
			HN	A_{12}	3
Fi_{22}	$2.U_6(2)$	5		$2.HS.2$	3
	$O_7(3)$	4		$U_3(8):3$	3
	$O_8^+(2):S_3$	4			
	$2^{10}:M_{22}$	3	HN.2	S_{12}	3
	$2^6:S_6(2)$	3		$4.HS.2$	3
	$(2\times 2^{1+8}):(U_4(2):2)$	3		$U_3(8):6$	3
	$U_4(3):2\times S_3$	3			
	${}^2F_4(2)'$	3	O′N	$L_3(7):2$	3
	$2^{5+8}:(S_3\times A_6)$	3			
	$3^{1+6}:2^{3+4}:3^2:2$	3	O′N.2	$4.L_3(4).2.2$	3
$Fi_{22}.2$	$2.U_6(2).2$	6	Th	${}^3D_4(2):3$	3
	$O_8^+(2):S_3\times 2$	4		$2^5.L_5(2)$	3
	$2^{10}:M_{22}:2$	4			
	$2^7:S_6(2)$	3	Fi_{24}'	Fi_{23}	5
	$(2\times 2^{1+8}:U_4(2):2):2$	3		$2.Fi_{22}:2$	3
	$U_4(3).2.2\times S_3$	3		$(3\times O_8^+(3):3):2$	3
	${}^2F_4(2)$	3		$O_{10}^-(2)$	3
	$2^{5+8}:(S_3\times S_6)$	3		$3^7.O_7(3)$	3
	$3^5:(2\times U_4(2):2)$	3		$3^{1+10}:U_5(2):2$	3
	$3^{1+6}:2^{3+4}:3^2.2.2$	3		$2^{11}.M_{24}$	3
	$G_2(3):2$	3			
			Fi_{24}	$Fi_{23}\times 2$	5
Ru	${}^2F_4(2)$	4		$(2\times 2.Fi_{22}):2$	3
	$2^6.U_3(3).2$	3		$S_3\times O_8^+(3):S_3$	3
	$(2^2\times Sz(8)):3$	3		$O_{10}^-(2):2$	3
	$2^{3+8}:L_3(2)$	3		$3^7.O_7(3):2$	3
	$U_3(5):2$	3		$3^{1+10}:(U_5(2):2\times 2)$	3
	$2^{1+4+6}.S_5$	3		$2^{12}.M_{24}$	3
				$(2\times 2^2.U_6(2)):S_3$	3
Fi_{23}	$2.Fi_{22}$	5			
	$O_8^+(3):S_3$	4	$\mathbb{B}$	$2.{}^2E_6(2):2$	4
	$2^2.U_6(2).2$	3		$2^{1+22}.Co_2$	3
	$S_8(2)$	3		Fi_{23}	3
	$\Omega_7(3)\times S_3$	3		$2^{9+16}.S_8(2)$	3
	$2^{11}.M_{23}$	3		Th	3
	$3^{1+8}.2^{1+6}.3^{1+2}.2S_4$	3		$(2^2\times F_4(2)):2$	3
J_4	$2^{11}:M_{24}$	3	$\mathbb{M}$	$2.\mathbb{B}$	3
	$2^{1+12}.3.M_{22}:2$	3			
	$2^{10}:L_5(2)$	3			
Ly	$G_2(5)$	3			
	$3.McL:2$	3			

Table 2: Primitive actions with $b(G)>2$, Part II

where $\mathscr{P}$ is the set of elements of prime order in G, and $x_1, \ldots, x_k$ represent the distinct G-classes of elements of prime order in $H = G_\alpha$ (note that $\mathrm{fpr}(x, \Omega) = 0$ if $x^G \cap H$ is empty). $\square$

Corollary 2.4. *Let G be a transitive permutation group on a finite set Ω, with point stabilizer $H = G_\alpha$, and let c be a positive integer. If $\widehat{Q}(G, c) < 1$ then $b(G) \leqslant c$.*

We use the next result to derive an effective upper bound for $\widehat{Q}(G, c)$.

Proposition 2.5. *Let G be a transitive permutation group on a finite set Ω, with point stabilizer $H = G_\alpha$. Suppose $x_1, \ldots, x_m$ represent distinct G-classes such that $\sum_i |x_i^G \cap H| \leqslant A$ and $|x_i^G| \geqslant B$ for all $1 \leqslant i \leqslant m$. Then*

$$\sum_i |x_i^G| \cdot \mathrm{fpr}(x_i, \Omega)^c \leqslant B(A/B)^c$$

for any positive integer c.

Proof. For $1 \leqslant i \leqslant m-1$ set $a_i = |x_i^G \cap H|$ and $b_i = |x_i^G| - B$. Since G is transitive, $\mathrm{fpr}(x_i, \Omega) = |x_i^G \cap H|/|x_i^G|$, hence

$$\begin{aligned}\sum_{i=1}^{m} |x_i^G| \cdot \mathrm{fpr}(x_i, \Omega)^c &\leqslant B\left(\frac{A - \sum_{i=1}^{m-1} a_i}{B}\right)^c + \sum_{i=1}^{m-1} (B + b_i)\left(\frac{a_i}{B + b_i}\right)^c \\ &\leqslant B^{1-c}\left((A - \sum_{i=1}^{m-1} a_i)^c + \sum_{i=1}^{m-1} a_i^c\right)\end{aligned}$$

and the result follows. $\square$

Corollary 2.6. *Let G be a transitive permutation group on a finite set Ω, with point stabilizer $H = G_\alpha$. Let $\mathcal{R}$ be the set of distinct prime divisors of $|H|$, let $\mathcal{S} \subseteq \mathcal{R}$ and let X be a set of representatives of the distinct G-classes of elements of order $r \in \mathcal{S}$. Let c be a positive integer. Then $b(G) \leqslant c$ if*

$$\sum_{x \in X} |x^G| \cdot \mathrm{fpr}(x, \Omega)^c + \sum_{r \in \mathcal{R} \setminus \mathcal{S}} b_r (a_r/b_r)^c < 1,$$

where $i_r(H) \leqslant a_r$, and $|x^G| \geqslant b_r$ for all $x \in G$ of order r.

Corollary 2.7. *Let G be a transitive permutation group on a finite set Ω, with point stabilizer $H = G_\alpha$. If $|H|^2 < |x^G|$ for all $x \in H$ of prime order then $b(G) = 2$.*

Proof. Set $A = |H|$ and $B = \min |x^G|$, where the minimum is over all $x \in H$ of prime order. Proposition 2.5 yields $\widehat{Q}(G, 2) \leqslant A^2/B$. $\square$

2.2 Character theoretic methods

We begin with a classical result of Frobenius (see [2, 10.1, p. 43] or [27, 7.2.1], for example).

Lemma 2.8. *Let G be a finite group, let z be a fixed element of G, and for $1 \leqslant i \leqslant t$ let C_i be a conjugacy class in G with representative x_i. The number of solutions to the equation $\prod_{i=1}^t y_i = z$ with $y_i \in C_i$ is equal to*

$$\frac{|C_1| \cdots |C_t|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x_1) \cdots \chi(x_t)\chi(z^{-1})}{\chi(1)^{t-1}},$$

where $\mathrm{Irr}(G)$ is the set of ordinary irreducible characters of G.

Definition 2.9. Let G be a finite group and let X and C be conjugacy classes in G with representatives x and z, respectively. For $t \in \mathbb{N}$ define

$$m(X, C, t) = \frac{|X|^t}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)^t \chi(z^{-1})}{\chi(1)^{t-1}},$$

where $\mathrm{Irr}(G)$ is the set of ordinary irreducible characters of G.

Let G be a transitive permutation group on a finite set Ω, with point stabilizer $H = G_\alpha$. Suppose $H = C_G(x)$ for some $x \in G$. Then the action of G on Ω is equivalent to the action of G on $X = x^G$ by conjugation. Let C be a conjugacy class in G, set $X_C = \{y \in X \mid xy \in C\}$ and note that X_C is a union of H-orbits. Fix $z \in C$ and observe that

$$|X_C| = |C||X|^{-1} \cdot |\{(a, b) \in X \times X \mid ab = z\}|,$$

hence Lemma 2.8 yields

$$|X_C| = |C||X|^{-1} m(X, C, 2),$$

where $m(X, C, 2)$ is defined as in Definition 2.9.

Proposition 2.10. *With the notation established, if $|X_C| < |H|$ for each conjugacy class C in G, then $b(G) > 2$.*

Proof. Observe that $b(G) = 2$ if and only if there exists a conjugacy class C such that H has a regular orbit on X_C. Of course, if H has a regular orbit on X_C then $|X_C| \geqslant |H|$. □

Proposition 2.11. *Let G be a transitive permutation group on a finite set Ω, with point stabilizer $H = G_\alpha$. Assume $H = C_G(x)$ for an involution $x \in G$. Set $X = x^G$ and suppose there exists a conjugacy class $C = c^G$ with $m(X, C, t) > 0$, where $t = 2$ or 3, and c is self-centralizing of order r. Then $b(G) \leqslant 2$ if $t = 2$ and r is odd, and $b(G) \leqslant 3$ if $t = 3$ and r is an odd prime.*

Proof. Since $m(X, C, t) > 0$, there exist $x_1, \ldots, x_t \in X$ such that $\prod_i x_i = z \in C$. Set $K = \bigcap_i C_G(x_i)$. Then $K \leqslant C_G(z)$ and $C_G(z) = \langle z \rangle$ since z is self-centralizing in G. Suppose $t = 2$ and assume $z^i \in K$, for some $1 \leqslant i \leqslant r - 1$. Then $(x_1x_2)^i x_1 = x_1(x_1x_2)^i = (x_2x_1)^{i-1}x_2$, so $z^i = z^{-i}$ and thus $z^{2i} = 1$, a contradiction since r is odd. Therefore K is trivial. Similarly, if $t = 3$ and $z \in K$ then $(x_1x_2x_3)x_i = x_i(x_1x_2x_3)$, hence $z = x_1x_2x_3 = x_2x_3x_1 = x_3x_1x_2$ and $[x_1x_3, x_2] = 1$, so

$$z^3 = (x_1x_2x_3)(x_3x_1x_2)(x_2x_3x_1) = x_1(x_2x_1x_3)x_1 = x_3x_2x_1 = z^{-1},$$

a contradiction since r is odd. Therefore K is a proper subgroup of $\langle z \rangle$, hence K is trivial since r is prime. We conclude that $b(G) \leqslant t$ since there exist $g_i \in G$ such that $C_G(x_i) = H^{g_i}$. □

2.3 Computational methods

2.3.1 Random search

Let $G = \langle x_1, \ldots, x_k \rangle$ be a finite group and let H be a core-free subgroup of G, so $\bigcap_{g \in G} H^g = 1$. Assume that we have an explicit faithful permutation representation ρ for G. We can now construct $G \cong \langle \rho(x_1), \ldots, \rho(x_k) \rangle$ as an explicit permutation group on n letters. Further, let us assume that $H = \langle y_1, \ldots, y_l \rangle$, where each y_i is a known word in the given generators for G, and so we know H as an explicit subgroup of G.

Let Ω be the set of right cosets of H in G. We can now view G as a transitive permutation group on Ω, with point stabilizer $H = G_\alpha$ (the fact that H is core-free

implies that Ω is a faithful G-set). As before, let $b(G) = b(G, \Omega)$ be the minimal size of a base for G with respect to Ω. If $c \in \mathbb{N}$, then $b(G) \leqslant c$ if and only if there exist $g_2, \ldots, g_c \in G$ such that $\bigcap_{i=1}^{c} H^{g_i} = 1$, where $g_1 = 1$. We can try to find such elements by a random search, using our explicit constructions of G and H. If this procedure terminates, then $b(G) \leqslant c$. In particular, if it terminates with $c = \lceil \log |G| / \log |\Omega| \rceil$ then Proposition 2.1 implies that $b(G) = c$.

We exploited this random search approach using MAGMA [5]. For practical reasons, we limit its use to those groups which admit a faithful permutation representation of degree at most 2×10^6.

2.3.2 Stabilizer analysis

Suppose G, H, ρ and Ω are as before, so G and H are explicit permutation groups on n letters. We can explicitly construct G as a permutation group on Ω. One can then compute the size of all possible c-point stabilizers, for any $c \geqslant 2$, and the precise value of $b(G)$ quickly follows. Here we only need to consider stabilizers corresponding to a suitable system of orbit representatives. More precisely, we note that the size of any c-point stabilizer is of the form $|G_{\alpha_1,\ldots,\alpha_c}|$ with $\alpha_1 = \alpha$ fixed, while α_i represents a $G_{\alpha_1,\ldots,\alpha_{i-1}}$-orbit on Ω for $2 \leqslant i \leqslant c$.

We implemented this technique in MAGMA using the command `CosetAction`. For practical reasons, we only use this technique if $|\Omega| \leqslant 3 \times 10^6$.

2.3.3 Double coset enumeration

Again, G, H, ρ and Ω are as before. Suppose we want to show that $b(G) > 2$. Observe that $b(G) = 2$ if and only if H has a regular orbit on Ω. Further, the H-orbit of the coset $Hx \in \Omega$ can be identified with the double coset HxH in G. Therefore, in order to show that $b(G) > 2$, it is sufficient to find a set $T \subset G$ of distinct (H, H) double coset representatives such that:

(i) $|HxH| < |H|^2$ for all $x \in T$; and

(ii) $\sum_{x \in T} |HxH| > |G : H| - |H|^2$.

We have implemented this technique in MAGMA. First, we find a set $S \subset G$ of 'large' (H, H) double coset representatives; S is chosen at random, noting that $|HxH| = |H|^2/|H \cap H^x|$. Next we attempt to find a subset $T \subseteq S$ of *distinct* double coset representatives, satisfying (i) and (ii) above. To do this, we use the fact that $HxH = HyH$ if and only if $yh^{-1}n^{-1}x^{-1} \in H$ for some $n \in N_H(H \cap H^x)$, where $h \in H$ satisfies $(H \cap H^x)^h = H \cap H^y$. (Note that if $H \cap H^x$ and $H \cap H^y$ are not H-conjugate then $HxH \neq HyH$.)

3 Almost simple sporadic groups

3.1 The Web Atlas

Let G be an almost simple group with socle G_0, a sporadic simple group. A great deal of information on the maximal subgroups and representations of G is available in the Atlas [16], the Web Atlas [32] and the GAP Character Table Library [7]. For example, the ordinary character table of G is in [16], and is available in GAP-readable form in [7].

The maximal subgroups of each almost simple sporadic group have been determined up to conjugacy, except for the Monster group $\mathbb{M}$. Lists of the known maximal subgroups can be found in the Web Atlas.

It is well-known that every almost simple sporadic group is 2-generated, and the Web Atlas provides a black-box algorithm to construct an explicit pair of *standard generators* for each group. For details of these algorithms, see [31].

The Web Atlas also provides various permutation and matrix representations for the sporadic groups and their maximal subgroups. In particular, if $G \notin \{\mathrm{Ly}, \mathrm{J}_4, \mathrm{Th}, \mathbb{B}, \mathbb{M}\}$, then an explicit faithful permutation representation of G on $n(G)$ letters is available, where $n(G)$ is defined in Table 3. Here $\alpha = 2$ if $G = G_0.2$, otherwise $\alpha = 1$. In addition, if $G_0 \notin \{\mathrm{Fi}_{23}, \mathrm{Fi}'_{24}, \mathrm{Co}_1, \mathrm{HN}, \mathbb{B}, \mathbb{M}\}$, then explicit generators for each maximal subgroup of G are presented in [32] as words in the standard generators of G.

G_0	M_{11}	M_{12}	M_{22}	M_{23}	M_{24}	J_1	J_2	J_3	HS	McL	Suz	He
$n(G)$	11	$12 \cdot \alpha$	22	23	24	266	100	6156	100	275	1782	2058

Co_1	Co_2	Co_3	Fi_{22}	Fi_{23}	Fi'_{24}	Ru	O′N	HN
98280	2300	276	3510	31671	306936	4060	$122760 \cdot \alpha$	1140000

Table 3: Degrees of some permutation representations

Proposition 3.1. *Let G be an almost simple sporadic group with socle G_0, where $G_0 \in \{\mathrm{Fi}_{23}, \mathrm{Fi}'_{24}, \mathrm{Co}_1, \mathrm{HN}\}$. We can construct each of the maximal subgroups H of G listed in Table 4.*

G	H
Fi_{23}	$2.\mathrm{Fi}_{22},\ \mathrm{O}_8^+(3).S_3,\ [3^{10}].(\mathrm{L}_3(3) \times 2),\ S_{12},\ (2^2 \times 2^{1+8}).(3 \times \mathrm{U}_4(2)).2,\ 2^{6+8} : (A_7 \times S_3)$
Fi'_{24}	$\mathrm{Fi}_{23},\ 2^{11}.\mathrm{M}_{24},\ 2^2.\mathrm{U}_6(2) : S_3,\ 2^{1+12}.3_1.\mathrm{U}_4(3).2$
Fi_{24}	any maximal subgroup
Co_1	$2^{11} : \mathrm{M}_{24},\ \mathrm{Co}_3,\ 2^{2+12} : (A_8 \times S_3),\ 2^{4+12} : (S_3 \times 3.S_6),\ 3^2.\mathrm{U}_4(3).D_8$
HN	$2^{1+8}.(A_5 \times A_5).2,\ 2^6.\mathrm{U}_4(2),\ (A_6 \times A_6).D_8$
HN.2	any maximal subgroup

Table 4: Some 'constructible' maximal subgroups

Proof. Suppose $G = \mathrm{Fi}_{23}$. By inspecting the Web Atlas [32], we may assume $H = [3^{10}].(\mathrm{L}_3(3) \times 2)$ or $2^{6+8} : (A_7 \times S_3)$. In the first case, H contains a Sylow 3-subgroup S of G, so the subgroup $[3^{10}]$ is normal in S. Therefore, in order to construct H as a subgroup of G, we take a Sylow 3-subgroup of G, determine its normal subgroups of order 3^{10} (of which there are 13) and then consider the order of the G-normalizer of each of these subgroups. We find there is a unique normalizer of order $|H|$ and so this is the desired subgroup H. The other case is very similar: H contains a Sylow 2-subgroup of G which normalizes the subgroup 2^{6+8}.

Next assume $G = \mathrm{Co}_1$. In view of [32], we may assume $H = 2^{2+12} : (A_8 \times S_3)$, $2^{4+12} : (S_3 \times 3.S_6)$ or $3^2.\mathrm{U}_4(3).D_8$. In the first two cases, H contains a Sylow 2-subgroup of G and we proceed as before. If $H = 3^2.\mathrm{U}_4(3).D_8$ then $H = N_G(K)$, where K is an elementary abelian subgroup of order 3^2 (see [16]). Now, if S is a Sylow 3-subgroup of G, then a MAGMA calculation reveals that S has 580 elementary abelian subgroups of order 3^2; precisely four of them have a G-normalizer of order $|H|$, and these normalizers are pairwise G-conjugate so we can take H to be any one of them.

Now, if $G = \mathrm{Fi}_{24}$ or HN.2 then explicit generators for each maximal subgroup of G are in the Web Atlas. Finally, if $G = \mathrm{Fi}'_{24}$ or HN then each of the listed subgroups is of the form $H = G \cap M$, where M is a maximal subgroup of $L = \mathrm{Fi}_{24}$ or HN.2, respectively (see [16]). Therefore, we can construct L and M as permutation groups on 306936 or 1140000 points (see [32]), and then set $G = \mathrm{Socle}(L)$ and $H = M \cap G$. □

Proposition 3.2. *Suppose* $G \in \{\mathrm{Fi}_{23}, \mathrm{Fi}'_{24}, \mathrm{Co}_1, \mathrm{HN}, \mathrm{Th}, \mathrm{J}_4, \mathrm{Ly}\}$. *Both the character table of every maximal subgroup* H *of* G *and the fusion of* H*-classes in* G *are known. The same is true if* (G, H) *is one of the cases listed in Table 5.*

G	H
$\mathrm{HN}:2$	$S_{12},\ 4.\mathrm{HS}.2,\ \mathrm{U}_3(8):6,\ 2^6.\mathrm{U}_4(2).2$
$\mathbb{B}$	$2.{}^2E_6(2):2,\ \mathrm{Fi}_{23},\ \mathrm{Th},\ \mathrm{HN}:2,\ \mathrm{O}_8^+(3):S_4, (2^2 \times F_4(2)):2,\ 3^{1+8}.2^{1+6}.\mathrm{U}_4(2).2,$ $5:4 \times \mathrm{HS}:2,\ (S_3 \times \mathrm{Fi}_{22}):2,\ S_4 \times {}^2F_4(2),\ (S_5 \times \mathrm{M}_{22}):2,\ 5^2:4S_4 \times S_5$
$\mathbb{M}$	$2.\mathbb{B},\ 2^{1+24}.\mathrm{Co}_1,\ 3.\mathrm{Fi}_{24},\ 2^2.{}^2E_6(2):S_3,\ 3^{1+12}.2\mathrm{Suz}.2$

Table 5: Some cases for which the fusion of H-classes in G has been determined

Proof. All of this information is available in [7], unless $(G, H) = (\mathbb{B}, (2^2 \times F_4(2)):2)$ or $(\mathbb{M}, 3^{1+12}.2\mathrm{Suz}.2)$. In the former case, only the character table of H is in [7]; the fusion of H-classes in G were calculated directly using the GAP command `PossibleClassFusions`. The character table of $3^{1+12}.2\mathrm{Suz}.2 < \mathbb{M}$, together with the fusion of H-classes in G, were calculated by Barraclough and Wilson [3]. □

3.2 The Baby Monster

Proposition 3.3. *Let* H *be one of the following maximal subgroups of* $\mathbb{B}$*:*

(1)	$2^{2+10+20}.(\mathrm{M}_{22}:2 \times S_3)$	(2)	$[2^{35}].(S_5 \times \mathrm{L}_3(2))$	(3)	$(3^2:D_8 \times \mathrm{U}_4(3).2.2).2$
(4)	$[3^{11}].(S_4 \times 2S_4)$	(5)	$5^{1+4}.2^{1+4}.A_5.4$	(6)	$(S_6 \times \mathrm{L}_3(4):2).2$
(7)	$5^3 \cdot \mathrm{L}_3(5)$	(8)	$(S_6 \times S_6).4$	(9)	$\mathrm{L}_2(49).2_3$

Then H *has an explicit faithful permutation representation on* $n(H)$ *points, where* $n(H)$ *is defined in Table 6.*

If H *is one of the following subgroups*

$$(10)\quad 2^{9+16}.\mathrm{S}_8(2) \qquad (11)\quad [2^{30}].\mathrm{L}_5(2)$$

then there is an explicit faithful matrix representation of H *into* $\mathrm{GL}_{m(H)}(2)$*, where* $m(H) =$ 180 *and* 144*, respectively.*

H	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
$n(H)$	6144	21504	3024	26244	3250	52	3875	24	50

Table 6: Degrees of some permutation representations of maximal subgroups of $\mathbb{B}$

Proof. The representations for (3)-(5) and (7) were constructed by An and Wilson (see Section 3 of [1]). Cases (6), (8) and (9) are straightforward. For example, (9) is the unique subgroup of index 2 in $\mathrm{Aut}(\mathrm{L}_2(49))$ which has only one class of involutions, and has a natural action on the 50 points of the projective line over $\mathbb{F}_{49}$. Case (8) is the unique subgroup of index 2 in $K = \mathrm{Aut}(S_6 \times S_6) \cong (S_6 \times S_6).D_8$ which maps onto the cyclic subgroup of D_8, and we can easily construct a permutation representation of degree 24 for K. In case (6), there is a subgroup $S_5 \times \mathrm{L}_3(4).2$ which is also in the maximal subgroup $S_5 \times \mathrm{M}_{22}.2$, so H is the unique subgroup of index 2 in $S_6.2 \times \mathrm{L}_3(4).2^2$ which has shape $(S_6 \times \mathrm{L}_3(4):2_2).2$. Thus it can easily be constructed as a permutation group on $10 + 42$ points. John Bray (personal communication) provided the relevant representations for (1), (2), (10) and (11).

□

Proposition 3.4. *Let H be one of the following maximal subgroups of $\mathbb{B}$:*

(1) $2^{9+16}.\mathrm{S}_8(2)$ (2) $2^{2+10+20}.(\mathrm{M}_{22} : 2 \times S_3)$ (3) $[2^{30}].\mathrm{L}_5(2)$
(4) $[2^{35}].(S_5 \times \mathrm{L}_3(2))$ (5) $(3^2 : D_8 \times \mathrm{U}_4(3).2.2).2$

(i) The ordinary character table of H is known.

(ii) If C is a conjugacy class in $\mathbb{B}$ containing elements of order 2 or 3 then $|C \cap H|$ is given in Table 7.

	$\lvert 2A \cap H\rvert$	$\lvert 2B \cap H\rvert$	$\lvert 2C \cap H\rvert$	$\lvert 2D \cap H\rvert$	$\lvert 3A \cap H\rvert$	$\lvert 3B \cap H\rvert$
(1)	473400	18580575	3956490240	11549737576	17825792000	3354101022720
(2)	182584	6022239	638533632	1444090472	3238002688	103347650560
(3)	125240	2696287	383467520	880456296	1300234240	58250493952
(4)	51512	1172575	131022848	313463400	142606336	18790481920
(5)	804	4356	121392	302535	78408	350000

Table 7: Some class fusion data relating to $\mathbb{B}$

Proof. By Proposition 3.3 we have an explicit faithful permutation or matrix representation of H. The character tables can now be constructed directly using the MAGMA implementation of the algorithm of Unger [29].

Now consider (ii). First, let H be the subgroup labelled (2). By inspecting the character table of H, we deduce that

$$\chi \downarrow H = \varphi_2 + \varphi_{25} + \varphi_{76} + \varphi_{120},$$

where χ is the complex irreducible character of $\mathbb{B}$ of degree 4371 and the φ_i are irreducible characters of H with $\varphi_2(1) = 1$, $\varphi_{25}(1) = 66$, $\varphi_{76}(1) = 1232$ and $\varphi_{120}(1) = 3072$. The entries in Table 7 are easily obtained since χ takes distinct values at each class of elements of order 2 and 3. The cases (1), (3) and (4) are similar. For case (5), the fusion of H-classes in $\mathbb{B}$ were computed by Thomas Breuer. □

Remark 3.5. The character tables identified in Proposition 3.4 are now available as part of the GAP Character Table Library [7].

3.3 The Monster

Proposition 3.6. *Let H be a maximal subgroup of $\mathbb{M}$. Either H belongs to one of 43 known conjugacy classes of maximal subgroups, or $|H| \leqslant 99283968$.*

Proof. Suppose H is a maximal subgroup of $\mathbb{M}$ which is not in one of the 43 known conjugacy classes. According to [6, Section 1], H is an almost simple group with socle $\mathrm{L}_2(13)$, $\mathrm{U}_3(4)$, $\mathrm{U}_3(8)$ or $\mathrm{Sz}(8)$, and thus $|H| \leqslant |\mathrm{Aut}(\mathrm{U}_3(8))| = 99283968$ as claimed. □

Proposition 3.7. *Let H be one of the following maximal subgroups of $\mathbb{M}$:*

(1) $2^{3+6+12+18}.(\mathrm{L}_3(2) \times 3S_6)$ (2) $3^8.\mathrm{O}_8^-(3).2_3$ (3) $(3^2 : 2 \times \mathrm{O}_8^+(3)).S_4$
(4) $3^{3+2+6+6} : (\mathrm{L}_3(3) \times SD_{16})$ (5) $(7 : 3 \times \mathrm{He}) : 2$ (6) $5^{1+6} : 2\mathrm{J}_2 : 4$
(7) $3^{2+5+10}.(\mathrm{M}_{11} \times 2S_4)$ (8) $(A_5 \times A_{12}) : 2$ (9) $5^{3+3}.(2 \times \mathrm{L}_3(5))$
(10) $2^{2+11+22}.(\mathrm{M}_{24} \times S_3)$

Then H has an explicit permutation representation on $n(H)$ points, where $n(H)$ is defined in Table 8.

H	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
$n(H)$	1032192	805896	3369	85293	2065	78125	34992	17	7750	294912

Table 8: Degrees of some permutation representations of maximal subgroups of $\mathbb{M}$

Proof. See the Web Atlas [32]. We refer the reader to [6] for details on how these representations were determined. □

Proposition 3.8. *Let $H_1 = 2^{10+16}.\mathrm{O}_{10}^+(2)$ and $H_2 = 2^{5+10+20}.(S_3 \times \mathrm{L}_5(2))$. Let r be a prime divisor of $|H_i|$. Then $i_r(H_i) \leqslant a_{r,i}$, where $a_{r,i}$ is defined in Table 9.*

i	$a_{2,i}$	$a_{3,i}$	$a_{5,i}$	$a_{7,i}$
1	486009339903	237937664983040	$2^{20} \cdot 78512308224$	$2^{18} \cdot 93251174400$
2	76880543743	2284253609984	$2^{28} \cdot 666624$	$2 \cdot 2^{30} \cdot 238080$

$a_{17,i}$	$a_{31,i}$
$2 \cdot 2^{24} \cdot 460770508800$	$5 \cdot 2^{25} \cdot 758041804800$
0	$6 \cdot 2^{35} \cdot 322560$

Table 9: The bounds $i_r(H_i) \leqslant a_{r,i}$

Proof. First consider $H = H_1$. Let V_{26} be the 26-dimensional $\mathrm{O}_{10}^+(2)$-module $V_{10} \oplus V_{16}$ over $\mathbb{F}_2$, where V_{10} is the natural $\mathrm{O}_{10}^+(2)$-module, and V_{16} is one of the two irreducible spin modules for $\mathrm{O}_{10}^+(2)$. Using a combination of Magma and the Web Atlas [32], we can determine the $\mathrm{GL}_{26}(2)$-class of each $x \in \mathrm{O}_{10}^+(2)$ of prime order. By [9, 6.1] we have

$$i_2(H) \leqslant 2^{10+16} - 1 + \sum_{i=1}^{4} 2^{26-m(x_i)} |x_i^{\mathrm{O}_{10}^+(2)}|,$$

where $x_1, \ldots, x_4$ represent the distinct classes of involutions in $\mathrm{O}_{10}^+(2)$ and $m(x_i)$ is the number of Jordan 2-blocks in the Jordan form of x_i on V_{26}. We calculate that $m(2A) = 6$, $m(2B) = m(2C) = 10$ and $m(2D) = 12$, hence $i_2(H) \leqslant 486009339903 = a_{2,1}$. Similarly, if r is an odd prime, then [9, 6.1] gives

$$i_r(H) \leqslant \sum_{i=1}^{k_r} 2^{26-n(y_i)} |y_i^{\mathrm{O}_{10}^+(2)}|,$$

where $n(y_i) = \dim C_{V_{26}}(y_i)$, and $y_1, \ldots, y_{k_r}$ represent the distinct classes in $\mathrm{O}_{10}^+(2)$ containing elements of order r. (In fact, it is easy to see that equality holds here.) In this way we obtain the $a_{r,1}$.

The case $H = H_2$ is very similar. Let V_1 and V_2 denote the trivial and 2-dimensional irreducible $\mathbb{F}_2 S_3$-modules, respectively. In addition, write V_5 for the natural $\mathrm{L}_5(2)$-module and V_{10} for one of the two 10-dimensional irreducible $\mathbb{F}_2\mathrm{L}_5(2)$-modules. Now let V_{35} be the 35-dimensional $\mathbb{F}_2(S_3 \times \mathrm{L}_5(2))$-module $(V_1 \otimes V_5) \oplus (V_1 \otimes V_{10}) \oplus (V_2 \otimes V_{10})$. As before, we deduce that

$$i_2(H) \leqslant 2^{5+10+20} - 1 + \sum_{i=1}^{5} 2^{35-m(x_i)} |x_i^{\tilde{H}}|,$$

where $x_1, \ldots, x_5$ represent the distinct involution classes in $\tilde{H} = S_3 \times \mathrm{L}_5(2)$, and $m(x_i)$ is the number of Jordan 2-blocks in the Jordan form of x_i on V_{35}. It follows that $i_2(H) \leqslant 76880543743 = a_{2,2}$ as claimed. Similarly, if r is an odd prime then

$$i_r(H) = \sum_{i=1}^{k_r} 2^{35-n(y_i)} |y_i^{\tilde{H}}|,$$

where $n(y_i) = \dim C_{V_{35}}(y_i)$ and $y_1, \ldots, y_{k_r}$ represent the distinct $\tilde{H}$-classes which contain elements of order r. This gives the remaining $a_{r,2}$ terms. □

Proposition 3.9. *Let H be one of the following maximal subgroups of $\mathbb{M}$*

(1) $2^{2+11+22}.(\mathrm{M}_{24} \times S_3)$ (2) $2^{3+6+12+18}.(3S_6 \times \mathrm{L}_3(2))$
(3) $2^{10+16}.\mathrm{O}^+_{10}(2)$ (4) $2^{5+10+20}.(\mathrm{L}_5(2) \times S_3)$

and let C be a conjugacy class of involutions in $\mathbb{M}$. Then $|C \cap H|$ is given in Table 10.

	$\lvert 2A \cap H\rvert$	$\lvert 2B \cap H\rvert$
(1)	47220432	43521572863
(2)	3573456	4026530095
(3)	76973776	$\leqslant$ 485932366127
(4)	5932752	$\leqslant$ 76874610991

Table 10: Some partial fusion data for involutions in $\mathbb{M}$

Proof. In cases (1) and (2) we use the explicit permutation representations from Proposition 3.7 to calculate the exact number of involutions in the group. Therefore it suffices to calculate the number which fuse to class $2A$ in $\mathbb{M}$. In cases (3) and (4) we again calculate the number of $2A$-involutions in the subgroup, but we do not have an explicit representation of the group with which to count the total number of involutions, so instead we use the bounds given in Proposition 3.8.

First observe that there are exactly two classes of $2B$-elements in the $2A$-element centralizer $2.\mathbb{B}$, and therefore there are exactly two classes of $2A$-elements in the $2B$-element centralizer $2^{1+24}.\mathrm{Co}_1$. Moreover, the orders of the centralizers of the 2^2-groups can be read off from the character table of $2.\mathbb{B}$. Thus it is easy to deduce that one of these classes is a class of 196560 involutions in the normal subgroup 2^{1+24}, while the other is a class of involutions mapping to elements of Co_1-class $2A$: each such coset of 2^{1+24} contains exactly 2^8 such, related to each other by elements of the 2^{1+24} corresponding to Leech lattice vectors in the 8-dimensional eigenspace of the corresponding involution in Co_1.

Now consider case (1). We restrict from Co_1 to $2^{11}.\mathrm{M}_{24}$. The orbit of length 196560 splits into three orbits, corresponding to Leech lattice vectors of shapes $(4^2, 0^{22})$, $(2^8, 0^{16})$ and $(-3, 1^{23})$, and therefore of lengths 1104, 97152 and 98304 respectively. The first of these lies inside the normal subgroup 2^{2+11} of (1): there are four such elements corresponding to each of the 276 duads under the natural action of M_{24}. Thus this orbit is fixed by the whole of (1). The elements in the other two orbits lie in just one of the three groups 2^{1+24} corresponding to the three involutions in the normal fours-group, so under the action of (1) the orbits become three times the size. In the first case, the remaining 194304 involutions in the orbit lie in the O_2-subgroup of (1), and therefore map to elements of the normal subgroup 2^{11} in $2^{11}.\mathrm{M}_{24}$. It is well-known that there are just 759 such involutions in Co_1-class $2A$, so they account for exactly these $759 \times 256 = 194304$ $2A$-involutions in $\mathbb{M}$.

There is just one other conjugacy class of elements of Co_1-class $2A$ in $2^{11}.\mathrm{M}_{24}$, represented by permutations of cycle type $(1^8 2^8)$ in M_{24}. Notice that the 8-dimensional eigenspace of this element contains no vectors with odd coordinates in the Leech lattice, so all these $2A$-elements lie in the subgroup $2^{2+11+22}.\mathrm{M}_{24}$. Since there are 759×15 such involutions in M_{24}, each lifting to 2^4 elements of Co_1-class $2A$ in $2^{11}.\mathrm{M}_{24}$, it follows that there are 46632960 involutions in this conjugacy class. Adding up the four class sizes 1104, 291456, 294912 and 46632960 gives the total 47220432 as claimed.

For future calculations it is useful to know the exact number of $2A$-involutions in a Sylow 2-subgroup of $\mathbb{M}$. It is easy to calculate that the Sylow 2-subgroup of M_{24} contains

exactly 89 involutions of cycle type $(1^8 2^8)$. Therefore the Sylow 2-subgroup of $2^{11}.\mathrm{M}_{24}$ (and therefore Co_1) contains $759+89.2^4 = 2183$ involutions of Co_1-class $2A$. Similarly the Sylow 2-subgroup of $2^{1+24}.\mathrm{Co}_1$ (and therefore $\mathbb{M}$) contains exactly $196560 + 2183.2^8 = 755408$ involutions of $\mathbb{M}$-class $2A$.

Now we are ready to consider case (2). We use the result for (1), and first restrict to the intersection of (1) and (2), which is a group of shape $2^{2+11+22}.(2^6.3S_6 \times S_3) \cong 2^{3+6+12+18}.(3S_6 \times S_4)$. Thus we restrict from M_{24} to the sextet stabilizer $2^6 : 3S_6$. By easy calculations in M_{24} we see that 1104 splits as $144+960$, according as the two non-zero coordinates lie in the same part of the sextet or not; and 291456 splits as $5760 + 138240 + 147456$, according as the octad splits across the sextet in the pattern $(4^2 0^4)$ or $(2^4 0^2)$ or (31^5). The class of size 294912 does not split at all. Finally, the involutions of M_{24}-class $2A$ in $2^6 : 3S_6$ are of three types: 45 inside the normal 2^6, and 180 mapping to involutions of cycle type $(1^2 2^2)$ in S_6, and 360 mapping to transpositions of S_6. Since each of these lifts to 2^{12} involutions of $\mathbb{M}$-class $2A$, we obtain three orbits of lengths 184320, 737280 and 1474560 respectively.

For the second part of the argument we need to consider what happens to these orbits when we extend from S_4 to $\mathrm{L}_3(2)$. Now the orbit of length 144 consists of the $2A$-elements which are in all seven of the groups 2^{1+24} corresponding to the seven involutions in the normal 2^3 of (2), so this is fixed by (2). The orbit of length 960 consists of those in the three of these groups corresponding to the involutions in the normal 2^2 of (1), and so it fuses with the orbit of length 5760 corresponding to the other six subgroups 2^2 in the 2^3. Similarly the orbit of length 138240 fuses with the orbit of length 184320.

The orbit of size 147456 corresponds to the three involutions in the normal 2^2 of S_4, while that of size 294912 corresponds to the other six involutions of S_4. Thus they fuse with a further 589824 involutions corresponding to the other twelve involutions in $\mathrm{L}_3(2)$ to make an orbit of size 1032192 in (2). This leaves just the orbits of size 737280 and 1474560, corresponding respectively to the involutions in A_6 and the transpositions of S_6. Since these elements are not diagonal in the quotient $\mathrm{M}_{24} \times S_3$ of (1), they are not diagonal in the quotient $S_6 \times S_3$ of the intersection of (1) and (2), and therefore they are not diagonal in the quotient $S_6 \times \mathrm{L}_3(2)$ of (2). In other words these orbits are invariant under (2). Adding up the orbit lengths we have calculated, we obtain the total figure of 3573456 involutions of $\mathbb{M}$-class $2A$ in case (2), as claimed.

Now consider case (3). First we work inside its intersection with the involution centralizer $2^{1+24}.\mathrm{Co}_1$. This is a group of shape $2^{1+24}.2^{1+8}.\mathrm{O}_8^+(2) \cong 2^{10+16}.2^8.\mathrm{O}_8^+(2)$. Since the subgroup 2^{1+8} of Co_1 contains exactly 271 involutions of Co_1-class $2A$, the total number of involutions of $\mathbb{M}$-class $2A$ in the O_2-subgroup is $196560 + 271.2^8 = 265936$. It is well-known that in the orthogonal group action on 2^{10}, just the 496 non-isotropic vectors are in $\mathbb{M}$-class $2A$. Moreover, the group 2^{10+16} is the centralizer in this O_2-subgroup of any $2A$-element corresponding to the central involution of the quotient $2^{1+8}.\mathrm{O}_8^+(2)$ in Co_1. Thus one can calculate that there is a further orbit of $73440 = 2295.2^5$ involutions of $\mathbb{M}$-class $2A$ in 2^{10+16}.

Next we study the embedding of $2^8.\mathrm{O}_8^+(2)$ in $\mathrm{O}_{10}^+(2)$. The normal 2^8 contains 135 elements of $\mathrm{O}_{10}^+(2)$-class $2A$ and 120 of class $2B$. In both cases, representatives can be chosen inside 2^{1+24}, and thus it is possible to deduce that the former each lift to 2^9 elements of $\mathbb{M}$-class $2A$, while the latter each lift to 2^{10} such. This accounts for all the 265936 $2A$-elements in the O_2-subgroup. Now we claim that no other $\mathrm{O}_{10}^+(2)$-class contains elements of $\mathbb{M}$-class $2A$. For a Sylow 2-subgroup of $\mathrm{O}_{10}^+(2)$ contains exactly 547 elements of class $2A$ and 392 of class $2B$, which already accounts for the full number $496+73440+547.2^9+392.2^{10} = 755408$ of $2A$-elements in the Sylow 2-subgroup of $\mathbb{M}$. Since in $\mathrm{O}_{10}^+(2)$ there are 23715 elements of class $2A$ and 63240 of class $2B$, the total number of elements of $\mathbb{M}$-class $2A$ in case (3) is $96 + 73440 + 23715.2^9 + 63240.2^{10} = 76973776$, as claimed.

Finally we consider case (4). Again we work first in the involution centralizer, which

means we have to study the embedding of the maximal subgroup $2^{2+12}.(A_8 \times S_3)$ in Co_1. We refer to [30] for details of this embedding. Certainly the three involutions in the normal fours-group are in Co_1-class $2A$. We find $420 = 3.35.2^2$ such involutions in $2^{2+12} \setminus 2^2$, and $3.105.2^5 = 10080$ corresponding to the 105 fixed-point-free involutions in A_8, and $3.2^7 = 384$ corresponding to the three involutions of S_3. Now we claim there are no more $2A$-elements in this group, since in the Sylow 2-subgroup we have already accounted for $3 + 420 + 17.3.2^5 + 2^7 = 2183$. In particular, notice that there are no $2A$-elements mapping to diagonal involutions in the quotient $A_8 \times S_3$.

Lifting to $2^{1+24}.2^{2+12}.(A_8 \times S_3)$, the orbit lengths are multiplied by 2^8 as usual, giving 768, 107520, 2580480 and 98304. It is also easy to calculate that under the action of this group the 196560 $2A$-elements in 2^{1+24} fall into three orbits, of lengths 720, 11520, and 184320. The final step is to consider the fusion of these orbits when we extend from $2^4.A_8$ to $\mathrm{L}_5(2)$.

It is not hard to deduce that the orbits of lengths 720 and 768 fuse to one of length 1488. Similarly, 11520 and 107520 fuse to one of length 119040. The orbits of lengths 184320 and 2580480 correspond respcetively to the 15 involutions in 2^4, and the 210 transvections in $2^4.A_8 \setminus 2^4$. They therefore fuse with a further 16.184320 involutions, corresponding to the 240 transvections in $\mathrm{L}_5(2) \setminus 2^4.A_8$, to make an orbit of size 5713920. Finally the orbit of length 98304 is fixed, since these involutions are not diagonal in $A_8 \times S_3$, so cannot be diagonal in $\mathrm{L}_5(2) \times S_3$. Adding up these numbers gives the total number of $2A$-elements in (4). □

4 Proof of Theorem 1

Proposition 4.1. *The conclusion to Theorem 1 holds if*

$$G_0 \in \{\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{23}, M_{24}, \mathrm{J}_1, \mathrm{J}_2, \mathrm{J}_3, \mathrm{HS}, \mathrm{McL}, \mathrm{Co}_3, \mathrm{Co}_2, \mathrm{He}, \mathrm{Suz}, \mathrm{Ru}, \mathrm{Fi}_{22}, \mathrm{O'N}\}.$$

Proof. Let G be an almost simple permutation group on a set Ω with point stabilizer $H = G_\alpha$ and socle G_0, a sporadic simple group in the above list. We use Magma to construct G and H as explicit permutation groups on $n(G)$ letters, where the integer $n(G)$ is given in Table 3. We claim that $b(G) = c$. In each case we use random search to check that $b(G) \leqslant c$ (see Section 2.3.1). Furthermore, if $\lceil \log |G| / \log |\Omega| \rceil = c$, then Proposition 2.1 yields $b(G) \geqslant c$ and thus equality holds. Therefore, it remains to deal with the cases listed in Table 11.

Let (G, H) be one of the cases in Table 11. First assume $(G, H) \notin \mathcal{A}$, where

$$\mathcal{A} = \{(\mathrm{Fi}_{22}, 3^{1+6} : 2^{3+4} : 3^2 : 2),\ (\mathrm{Fi}_{22}.2, 3^{1+6} : 2^{3+4} : 3^2.2.2),\ (\mathrm{Fi}_{22}.2, G_2(3) : 2)\}.$$

Then $|\Omega| < 3 \times 10^6$ and stabilizer analysis reveals that all $(c-1)$-point stabilizers are non-trivial (see Section 2.3.2).

Finally, suppose $(G, H) \in \mathcal{A}$. The random search method yields $b(G) \leqslant 3$. To deduce that $b(G) = 3$, we use the double coset enumeration method described in Section 2.3.3. □

Proposition 4.2. *The conclusion to Theorem 1 holds if*

$$G_0 \in \{\mathrm{Fi}_{23}, \mathrm{Fi}'_{24}, \mathrm{Co}_1, \mathrm{HN}, \mathrm{Th}, \mathrm{J}_4, \mathrm{Ly}\}.$$

Proof. Suppose (G, H) is one of the cases for which the fusion of H-classes in G has been determined (see Proposition 3.2). Let c be a positive integer and define $\widehat{Q}(G, c)$ as in Definition 2.2. We compute $\widehat{Q}(G, c)$ precisely. By applying Propositions 2.1 and Corollary 2.4 we deduce that, with few exceptions, $b(G) = \lceil \log |G| / \log |\Omega| \rceil$.

The only exceptions with $G \in \{\mathrm{Th}, \mathrm{J}_4, \mathrm{Ly}\}$ are $(G, H) = (\mathrm{Th}, 2^{1+8}.A_9)$ and $(\mathrm{Ly}, 2.A_{11})$. In both cases, we observe that $H = C_G(x)$ for an involution $x \in 2A$. In the former case,

G	H	G	H	G	H
M_{12}	$A_6.2^2$	HS	M_{22}	He.2	$\mathrm{Sp}_4(4):4$
	$2 \times S_5$	HS.2	$\mathrm{M}_{22}.2$	Suz	$(A_4 \times \mathrm{L}_3(4)):2$
	$2^{1+4}:S_3$		$\mathrm{L}_3(4).2.2$		$2^{2+8}:(A_5 \times S_3)$
	$4^2:D_{12}$		$S_8 \times 2$	Suz.2	$2^{2+8}:(S_5 \times S_3)$
$\mathrm{M}_{12}.2$	$2^{1+4}:S_3.2$		$(2 \times A_6.2^2).2$		$\mathrm{M}_{12}:2 \times 2$
	$4^2:D_{12}.2$	McL	$\mathrm{U}_4(3)$	Ru	$(2^2 \times \mathrm{Sz}(8)):3$
	$3^{1+2}:D_8$		M_{22}		$2^{3+8}:\mathrm{L}_3(2)$
M_{22}	$2^4:A_6$	McL.2	$\mathrm{U}_4(3):2$		$\mathrm{U}_3(5):2$
	$\mathrm{L}_2(11)$		$\mathrm{M}_{11} \times 2$		$2^{1+4+6}.S_5$
M_{23}	$\mathrm{L}_3(4).2b$	Co_3	McL.2	Fi_{22}	$2.\mathrm{U}_6(2)$
	$2^4:A_7$		HS		$\mathrm{O}_8^+(2):S_3$
M_{24}	$2^4.A_8$		$3^{1+4}:4.S_6$		$3^{1+6}:2^{3+4}:3^2:2$
	$\mathrm{L}_2(23)$		$2^4.A_8$	$\mathrm{Fi}_{22}.2$	$2.\mathrm{U}_6(2).2$
J_2	$\mathrm{U}_3(3)$	Co_2	$\mathrm{U}_6(2):2$		$\mathrm{O}_8^+(2):S_3 \times 2$
	$A_4 \times A_5$		$2^{10}:\mathrm{M}_{22}:2$		$2^{10}:\mathrm{M}_{22}:2$
	$A_5 \times D_{10}$		McL		$3^{1+6}:2^{3+4}:3^2.2.2$
$\mathrm{J}_2.2$	$\mathrm{L}_3(2):2 \times 2$		$2^{1+8}:\mathrm{Sp}_6(2)$		$G_2(3):2$
$\mathrm{J}_3.2$	$(3 \times \mathrm{M}_{10}):2$	He	$\mathrm{Sp}_4(4):2$	O′N.2	$4.\mathrm{L}_3(4).2.2$

Table 11: Some cases with $\lceil \log|G|/\log|\Omega| \rceil < b(G)$

by inspecting the character table of G, we calculate that $m(X, C, 2) > 0$, where $X = 2A$, $C = 19A$ and $m(X, C, 2)$ is defined as in Definition 2.9. Therefore Proposition 2.11 implies that $b(G) = 2$ since every $c \in C$ is self-centralizing in G. The same argument applies in the other case, with $C = 67A$.

The remaining exceptional cases (G, H) appear in Table 4. Following Proposition 3.1, we use Magma to construct G and H as permutation groups on $n(G)$ letters, where $n(G)$ is defined in Table 3. A combination of Proposition 2.1 and random search (see Section 2.3.1) yields $b(G) = \lceil \log|G|/\log|\Omega| \rceil$, with the exception of the following cases (G, H):

$$(\mathrm{Fi}'_{24}, 2^{11}.\mathrm{M}_{24}),\ (\mathrm{Co}_1, 2^{2+12}:(A_8 \times S_3)),\ (\mathrm{Co}_1, 2^{4+12}.(S_3 \times 3.S_6)),\ (\mathrm{Co}_1, \mathrm{Co}_2).$$

(If $(G, H) = (\mathrm{Fi}_{23}, \mathrm{O}_8^+(3):S_3)$ or $(\mathrm{Fi}'_{24}, \mathrm{Fi}_{23})$ then it is easier to use stabilizer analysis, rather than random search, to show that $b(G) = 4$ or 5, respectively (see Section 2.3.2).) In the first three cases, the previous fusion calculations yield $\widehat{Q}(G, 3) < 1$, hence $b(G) \leqslant 3$ and double coset enumeration implies that $b(G) > 2$ (see Section 2.3.3). If $(G, H) = (\mathrm{Co}_1, \mathrm{Co}_2)$ then stabilizer analysis yields $b(G) = 5$.

To complete the proof of the proposition, we may assume $G = \mathrm{Fi}_{24}$ or HN.2, and H is not one of the subgroups listed in Table 5. Following Proposition 3.1, we use Magma to construct G and H as permutation groups on $n(G)$ points, and then the usual combination of random search and Proposition 2.1 yields $b(G) = \lceil \log|G|/\log|\Omega| \rceil$, unless $G = \mathrm{Fi}_{24}$ and $H = 2^{12}.\mathrm{M}_{24}$ or $(2 \times 2^2.\mathrm{U}_6(2)):S_3)$. (If $(G, H) = (\mathrm{Fi}_{24}, \mathrm{Fi}_{23} \times 2)$, then it is easier to use stabilizer analysis to show that there is a trivial 5-point stabilizer.)

For these two cases, random search gives $b(G) \leqslant 3$. If $H = 2^{12}.\mathrm{M}_{24}$ then double coset enumeration yields $b(G) > 2$. In the other case, $H = C_G(x)$ for $x \in 2D$ and, by inspecting the character table of G, we deduce that $b(G) > 2$ via Proposition 2.10. □

Proposition 4.3. *The conclusion to Theorem 1 holds if $G = \mathbb{B}$.*

Proof. From the character table of G, we calculate that $|x^G| \geqslant 13571955000$ for every $x \in G$ of prime order, hence Corollary 2.7 yields $b(G) = 2$ if $|H| \leqslant 116498$. This deals with the 6 smallest maximal subgroups of G. For the remainder we assume $|H| > 116498$.

Next let H be one of the subgroups listed in Table 5. By Proposition 3.2, we can compute $\widehat{Q}(G, c)$ precisely and we deduce that $b(G) = \lceil \log|G|/\log|\Omega| \rceil$, with the exception

of the case $H = (2^2 \times F_4(2)) : 2$. Here the same method yields $b(G) \leqslant 3$ and one can check that equality holds via Proposition 2.10 since $H = C_G(x)$ for an involution $x \in 2C$. If $H = 2^{1+22}.\mathrm{Co}_2$, then $H = C_G(x)$ for an involution $x \in 2B$ and from the character table of G we calculate that $m(X, C, 3) > 0$, where $X = 2B$, $C = 47A$ and $m(X, C, 3)$ is defined in Definition 2.9. A combination of Propositions 2.1 and 2.11 yields $b(G) = 3$.

Next suppose H is one of the subgroups labelled (1)-(5) in the statement of Proposition 3.4. Let $\mathcal{R}$ be the set of distinct prime divisors of $|H|$ and set $\mathcal{S} = \{2, 3\}$. From the entries in Table 7 we can compute $\mathrm{fpr}(x, \Omega)$ precisely for every $x \in G$ of order 2 or 3. Further, it is straightforward to calculate $i_r(H)$ for every prime $r > 3$ from the character table of H (see Proposition 3.4(i)). A combination of Proposition 2.1 and Corollary 2.6 implies that $b(G) = \lceil \log |G| / \log |\Omega| \rceil$, unless $H = 2^{2+10+20}.(\mathrm{M}_{22} : 2 \times S_3)$ or $[2^{30}].\mathrm{L}_5(2)$; here the same approach only yields $b(G) \leqslant 3$. These are the two cases stated in part (iii) of Theorem 1. It is worth noting that if $x_1, \ldots, x_4$ represent the distinct involution classes in G then Proposition 3.4 implies that $\sum_i |x_i^G| \cdot \mathrm{fpr}(x_i, \Omega)^2 > 1$, hence $\widehat{Q}(G, 2) > 1$ in both of these cases.

To complete the proof, we may assume H is one of the following subgroups;

(1)	$5^3 \cdot \mathrm{L}_3(5)$	(2)	$\mathrm{L}_2(49).2_3$	(3)	$(S_6 \times S_6).4$
(4)	$[3^{11}].(S_4 \times 2S_4)$	(5)	$(S_6 \times \mathrm{L}_3(4) : 2).2$	(6)	$5^{1+4}.2^{1+4}.A_5.4$

In each case it is easy to compute $i_r(H)$ for every prime divisor r of $|H|$. Indeed, we use the permutation representation for H cited in Proposition 3.3, and compute its conjugacy classes directly using the Magma implementation of the algorithm of [15]. In all six cases, we get $b(G) = 2$ via Corollary 2.6 (setting $\mathcal{S} = \emptyset$). □

Proposition 4.4. *The conclusion to Theorem 1 holds if $G = \mathbb{M}$.*

Proof. The character table of G indicates that $|x^G| \geqslant 97239461142009186000$ for all $x \in G$ of prime order, hence Corollary 2.7 yields $b(G) = 2$ if $|H| \leqslant 9861007105$. By Proposition 3.6, this deals with all of the 'unknown' maximal subgroups of G, together with the 24 smallest cases listed in the Web Atlas [32]. By Proposition 3.2, we can compute $\widehat{Q}(G, c)$ precisely if $H = 2.\mathbb{B}$, $2^{1+24}.\mathrm{Co}_1$, $3.\mathrm{Fi}_{24}$, $2^2.{}^2E_6(2) : S_3$ or $3^{1+12}.2\mathrm{Suz}.2$. This yields $b(G) = \lceil \log |G| / \log |\Omega| \rceil$, unless $H = 2^{1+24}.\mathrm{Co}_1$. Here $H = C_G(x)$ for an involution $x \in 2B$, and we calculate that $m(X, C, 2) > 0$, where $X = 2B$, $C = 105A$ and $m(X, C, 2)$ is defined in Definition 2.9. Therefore Proposition 2.11 gives $b(G) = 2$.

Next let H be one of the maximal subgroups labelled (1)-(9) in the statement of Proposition 3.7. We use Magma to construct H as a permutation group on $n(H)$ points, where $n(H)$ is defined in Table 8. Moreover, if r is a prime divisor of H, then we can compute $i_r(H)$ directly in Magma using the algorithm of [15]. In each case, the reader can check that Corollary 2.6 yields $b(G) = 2$ (we set $\mathcal{S} = \emptyset$). If $H = S_3 \times \mathrm{Th}$ or $(D_{10} \times \mathrm{HN}).2$, then we can compute $i_r(H)$ directly and the same argument yields $b(G) = 2$. Similarly, we set $\mathcal{S} = \{2\}$ and apply Proposition 3.9 if $H = 2^{2+11+22}.(\mathrm{M}_{24} \times S_3)$. Finally, if $H = 2^{10+16}.\mathrm{O}_{10}^+(2)$ or $2^{5+10+20}.(S_3 \times \mathrm{L}_5(2))$, then a combination of Corollary 2.6 and Propositions 3.8 and 3.9 gives $b(G) = 2$. □

This completes the proof of Theorem 1.

References

[1] J. An, and R.A. Wilson, *The Alperin weight conjecture and Uno's conjecture for the Baby Monster $\mathbb{B}$, p odd*, LMS J. Comput. Math. **7** (2004), 120–166.

[2] Z. Arad, M. Herzog, and J. Stavi, *Powers and products of conjugacy classes in groups*, Products of conjugacy classes in groups (Z. Arad and M. Herzog, eds.), Lecture Notes in Math., vol. 1112, Springer Verlag, New York, 1985, pp. 6–51.

[3] R.W. Barraclough and R.A. Wilson, *The character table of a maximal subgroup of the Monster*, LMS J. Comput. Math. **10** (2007), 161–175.

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

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

[6] J.N. Bray and R.A. Wilson, *Explicit representations of maximal subgroups of the Monster*, J. Algebra **300** (2006), 834–857.

[7] T. Breuer, *Manual for the GAP Character Table Library, Version 1.1*, RWTH Aachen (2004).

[8] T.C. Burness, *On base sizes for actions of finite classical groups*, J. London Math. Soc. **75** (2007), 545–562.

[9] ———, *Fixed point ratios in actions of finite classical groups,* II, J. Algebra **309** (2007), 80–138.

[10] T.C. Burness, R.M. Guralnick, and J. Saxl, *Base sizes for actions of simple groups*, in preparation.

[11] T.C. Burness, M.W. Liebeck, and A. Shalev, *Base sizes for simple groups and a conjecture of Cameron*, submitted.

[12] P.J. Cameron, *Some open problems on permutation groups*, Groups, Combinatorics and Geometry (M.W. Liebeck and J. Saxl, eds.), London Math. Soc. Lecture Note Series, vol. 165, 1992, pp. 340–350.

[13] ———, *Permutation Groups*, London Math. Soc. Student Texts, vol. 45, Cambridge University Press, 1999.

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

[15] J.J. Cannon and D.F. Holt, *Computing conjugacy class representatives in permutation groups*, J. Algebra **300** (2006), 213–222.

[16] J. Conway, R. Curtis, S. Norton, R. Parker, and R. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

[17] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2004.

[18] D. Goldstein and R.M. Guralnick, *Alternating forms and self-adjoint operators*, J. Algebra **308** (2007), 330–349.

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

[20] ———, *Two point stabilisers of partition actions of linear groups*, J. Algebra **297** (2006), 453–469.

[21] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990.

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

[23] J. Müller, *On the action of the sporadic simple Baby Monster group on its conjugacy class* $2B$, LMS J. Comput. Math. **11** (2008), 15–27.

[24] J. Müller, M. Neunhöffer, and R.A. Wilson, *Enumerating big orbits and an application: B on the cosets of* Fi_{23}, J. Algebra **314** (2007), 75–96.

[25] J. Müller, M. Neunhöffer, and F. Noeske, *GAP 4 Package orb*, `http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Computer/Software/Gap/orb.html`.

[26] Á. Seress, *Permutation Group Algorithms*, Cambridge Tracts in Mathematics, vol. 152, Cambridge University Press, Cambridge, 2003.

[27] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Math., vol. 1, Jones and Bartlett, Boston MA, 1992.

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

[29] W.R. Unger, *Computing the character table of a finite group*, J. Symbolic Comput. **41** (2006), 847–862.

[30] R.A. Wilson, *The maximal subgroups of Conway's group* Co_1, J. Algebra **85** (1983), 144–165.

[31] R.A. Wilson, *Standard generators for sporadic simple groups*, J. Algebra **184** (1996), 505–515.

[32] R.A. Wilson et al., *A World-Wide-Web Atlas of finite group representations*, `http://brauer.maths.qmul.ac.uk/Atlas/v3/`.