REGULAR ORBITS OF SPORADIC SIMPLE GROUPS

JOANNA B. FAWCETT, JÜRGEN MÜLLER, E. A. O'BRIEN, AND ROBERT A. WILSON

Abstract. Given a finite group G and a faithful irreducible FG-module V where F has prime order, does G have a regular orbit on V? This problem is equivalent to determining which primitive permutation groups of affine type have a base of size 2. Let G be a covering group of an almost simple group whose socle T is sporadic, and let V be a faithful irreducible FG-module where F has prime order dividing $|G|$. We classify the pairs (G, V) for which G has no regular orbit on V, and determine the minimal base size of G in its action on V. To obtain this classification, for each non-trivial $g \in G/Z(G)$, we compute the minimal number of T-conjugates of g generating $\langle T, g\rangle$.

1. Introduction

A *base* B for a group X acting faithfully on a finite set Ω is a subset of Ω with the property that only the identity of X fixes every element of B. The *base size* of X, denoted by $b(X)$, is the minimal cardinality of a base for X. Recently, much work has been done to classify the finite primitive permutation groups of almost simple, diagonal and twisted wreath type with base size 2 (see [6–8, 11, 12]). For groups of affine type, this problem is equivalent to the regular orbit problem for fields with prime order.

Given a finite group G, a field F and a faithful FG-module V, we say that G has a *regular orbit* on V if there exists $v \in V$ such that only the identity of G fixes v; in other words, $\{v\}$ is a base for G. Hall, Liebeck and Seitz [19, Theorem 6] proved that if G is a finite quasisimple group with no regular orbit on a faithful irreducible FG-module V where F is a field of characteristic p, then either G is of Lie type in characteristic p, or $G = A_n$ where $p \leqslant n$ and V is the fully deleted permutation module, or (G, V) is one of finitely many exceptional pairs. While these exceptional pairs are unknown in general, they have been determined when F is the field $\mathbb{F}_p$ of order p and either $p \nmid |G|$ (see [16, 26]), or $p \mid |G|$ and $G/Z(G) = A_n$ (see [13]). In this paper, we consider the case where $G/Z(G)$ is a sporadic simple group whose order is divisible by p. We also consider the covering groups of the automorphism groups of the sporadic groups, and for those groups G with no regular orbit on V, we determine the base size of G in its action on V.

Theorem 1.1. *Let G be a covering group of an almost simple group whose socle is sporadic. Let V be a faithful irreducible $\mathbb{F}_pG$-module where p is a prime dividing $|G|$. If G has no regular orbit on V, then $(G, p, \dim_{\mathbb{F}_p}(V), b(G))$ is listed in Table 1.*

If there are exactly m faithful irreducible $\mathbb{F}_pG$-modules with dimension d on which G has no regular orbit and $m > 1$, then we write $d^{(m)}$ in Table 1. Except for the case $(G, p, \dim_{\mathbb{F}_p}(V)) = (\mathrm{M}_{11}, 3, 10)$, this is sufficient to identify the non-regular modules. However, there are three faithful irreducible $\mathbb{F}_3\,\mathrm{M}_{11}$-modules of dimension 10, only one of which

Key words and phrases. regular orbit; base size; sporadic simple group; primitive affine group.

Fawcett was supported by the Australian Research Council Discovery Project grant DP130100106, the London Mathematical Society, and the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 746889. O'Brien was supported by a University of Auckland Hood Fellowship. Both they and Wilson were supported by the Marsden Fund of New Zealand via grant UOA 1323. We thank the referees for their helpful and insightful comments.

has base size 2: the $\mathbb{F}_3 \mathrm{M}_{11}$-module with the property that an involution of M_{11}, viewed as an element of $\mathrm{GL}_{10}(3)$, has trace $-1 \in \mathbb{F}_3$.

There are $\mathbb{F}_p G$-modules in Table 1 (indicated by $^\sharp$) that are not absolutely irreducible; these all split into absolutely irreducible $\mathbb{F}_{p^2} G$-modules. In particular, when $G = 3.\mathrm{J}_3$, there is a unique faithful irreducible but not absolutely irreducible $\mathbb{F}_2 G$-module with dimension 18, corresponding to the two absolutely irreducible $\mathbb{F}_4 G$-modules with dimension 9 that cannot be realised over $\mathbb{F}_2$; this module should not be confused with the four faithful absolutely irreducible $\mathbb{F}_4 G$-modules with dimension 18 that cannot be realised over $\mathbb{F}_2$ (see [24]).

G	p	$\dim_{\mathbb{F}_p}(V)$	$b(G)$	G	p	$\dim_{\mathbb{F}_p}(V)$	$b(G)$
M_{11}	2	10	2	HS	2	20	2
	3	$5^{(2)}$, 10	2	HS :2	2	20	2
M_{12}	2	10	3	McL	2	22	2
	3	$10^{(2)}$	2		3	21	2
M_{12} :2	2	10	3	McL :2	2	22	2
$2.\mathrm{M}_{12}$	3	$6^{(2)}$	3		3	$21^{(2)}$	2
		$10^{(2)}$	2	Ru	2	28	2
$2.\mathrm{M}_{12}.2^+$	3	12, $10^{(4)}$	2	$2.\mathrm{Suz}$	3	12	3
$2.\mathrm{M}_{12}.2^-$	3	12	2	$2.\mathrm{Suz}.2^+$	3	$12^{(2)}$	3
M_{22}	2	$10^{(2)}$	3	$2.\mathrm{Suz}.2^-$	3	$24^\sharp$	2
M_{22} :2	2	$10^{(2)}$	3	$3.\mathrm{Suz}$	2	$24^\sharp$	2
$3.\mathrm{M}_{22}$	2	$12^\sharp$	3	$6.\mathrm{Suz}$	7	$12^{(2)}$	2
M_{23}	2	$11^{(2)}$	3		13	$12^{(2)}$	2
M_{24}	2	$11^{(2)}$	3	Co_3	2	22	2
J_1	2	20	2		3	22	2
J_2	2	$12^\sharp$	2	Co_2	2	22	3
J_2 :2	2	12	2		3	23	2
$2.\mathrm{J}_2$	3	$12^\sharp$, 14	2	Co_1	2	24	3
	5	6	2	$2.\mathrm{Co}_1$	3	24	2
$2.\mathrm{J}_2.2^+$	3	12	2		5	24	2
$2.\mathrm{J}_2.2^-$	3	$12, 14^{(2)}$	2		7	24	2
$3.\mathrm{J}_3$	2	$18^\sharp$	2				

TABLE 1. $\mathbb{F}_p G$-modules V on which G has no regular orbit

A finite primitive permutation group X is of *affine type* if its socle V is an $\mathbb{F}_p$-vector space for some prime p, in which case $X = V{:}X_0$ and V is a faithful irreducible $\mathbb{F}_p X_0$-module, where X_0 denotes the stabiliser of the vector 0 in X. Now $b(X) = b(X_0) + 1$, so classifying the primitive permutation groups of affine type with a base of size 2 amounts to determining which finite groups G, primes p, and faithful irreducible $\mathbb{F}_p G$-modules V are such that G has a regular orbit on V. Thus, as an immediate consequence of Theorem 1.1, we obtain the following.

Corollary 1.2. *Let X be a primitive permutation group of affine type with socle $V \simeq \mathbb{F}_p^d$ where p is a prime dividing $|X_0|$ and X_0 is a covering group of an almost simple group whose socle is sporadic. If $b(X) > 2$, then (G, p, d) is listed in Table 1 where $G = X_0$, and $b(X) = b(G) + 1$. In particular, $b(X) \leqslant 4$.*

The proof of Theorem 1.1 proceeds as follows. If G has no regular orbit on V, then the dimension of V is bounded above by some integer $u(G,p)$ (see Lemma 3.3). If $u(G,p)$ is less than the minimal dimension $m(G',p)$ of a faithful irreducible representation of the derived subgroup G' in characteristic p (given by [23]), then we have a contradiction. Otherwise, in most cases, the p-modular Brauer character table of G is known, so we can determine the possible dimensions for V. We then use a variety of computational techniques in GAP [14] and MAGMA [4] to determine the base size $b(G)$ of G in its action of V. For those cases where the p-modular Brauer character table of G is not known—namely when (G,p) is one of $(\mathrm{J}_4,2)$, $(\mathrm{Co}_1,2)$, $(2.\mathrm{Co}_1,3)$ or $(2.\mathrm{Co}_1,5)$—we use other methods to determine the possible dimensions for V (see §4).

The upper bound $u(G,p)$ is defined in terms of a well-known parameter. Let G be an almost simple group with socle T, and for each non-trivial $g \in G$, define $r(g)$ to be the minimal number of T-conjugates of g that generate $\langle T, g\rangle$. When T is sporadic, upper bounds on $r(G) := \max\{r(g) : g \in G \setminus \{1\}\}$ were determined in [18] (see [18, Table 1] and the proof of [18, Lemma 7.6]), but these are not always sufficient for our purposes. To determine the best possible bound on the dimension of V, we compute the exact values of the $r(g)$ and record these in the following theorem. In particular, this result considerably improves the upper bounds of [18] on $r(G)$ and may be of independent interest.

Theorem 1.3. *Let G be an almost simple group whose socle is sporadic, and let $g \in G$ be non-trivial. Either $g^2 = 1$ and $r(g) = 3$, or $g^2 \neq 1$ and $r(g) = 2$, or the class name of g is listed in Table 2.*

G	$r(g)=3$	$r(g)=4$	$r(g)=5$	$r(g)=6$
$\mathrm{M}_{22}(:2)$		2B		
$\mathrm{J}_2(:2)$	3A	2A		
$\mathrm{HS}(:2)$	4A	2C		
$\mathrm{McL}(:2)$	3A			
$\mathrm{Suz}(:2)$		3A		
Co_2		2A		
Co_1	3A			
$\mathrm{Fi}_{22}(:2)$	3A, 3B	2D		2A
Fi_{23}	3A, 3B			2A
$\mathrm{Fi}'_{24}(:2)$	3A, 3B		2C	
$\mathrm{HN}(:2)$	4D			
Ly	3A			
$\mathbb{B}$		2A		

TABLE 2. Exceptional values of $r(g)$

This paper is organised as follows. In §2 we collect some notation, definitions and basic facts. In §3 we determine bounds both for the dimensions of faithful irreducible representations admitting no regular orbit and for base sizes. In §4 we address the "dimension gaps" that occur when $m(G',p) \leqslant u(G,p)$ and the p-modular Brauer character table of G is not known. In §5 we briefly discuss computational aspects, and in §6 and §7 we prove Theorems 1.3 and 1.1, respectively.

2. Preliminaries

Let G be a finite group. We denote the derived subgroup of G by G', the centre of G by $Z(G)$, and the conjugacy class of $g \in G$ by g^G. A finite group G is *almost simple* if

$T \trianglelefteq G \leqslant \mathrm{Aut}(T)$ for some non-abelian simple group T. The subgroup of G generated by the minimal normal subgroups of G is the *socle* of G, and G is almost simple precisely when its socle is a non-abelian simple group. If $G = G'$ and $G/Z(G)$ is simple, then G is *quasisimple*.

A finite group L is a *covering group* of G (by a group M) if $L/M \simeq G$ where $M \leqslant Z(L) \cap L'$. Every finite group G has a *universal covering group* [17, Theorem 4.226], which is a covering group of G by $M(G)$, the Schur multiplier of G (see [17, §4.15] for a definition). If L is a covering group of G by a group M, then L is a homomorphic image of some universal covering group of G and M is a homomorphic image of $M(G)$ (see [17, Proposition 4.227]). Universal covering groups are determined up to isoclinism in general, and up to isomorphism when G is simple [10, Chap. 4, §1]. A finite group L is a covering group of an almost simple group G precisely when $L/Z(L) \simeq G$ and $Z(L) \leqslant L'$.

Let T be one of the 26 sporadic simple groups. A wealth of information about these groups may be found in [10], with which our notation is (more or less) consistent. It is well known that $M(T)$ is cyclic (see, for example, [25, Theorem 5.1.4]), and also that $\mathrm{Aut}(T) = T$ or $T{:}2$. If $\mathrm{Aut}(T) = T{:}2$, then $M(\mathrm{Aut}(T)) \leqslant M(T)$. (To see this, observe that the derived subgroup of a covering group of $T{:}2$ is perfect with central quotient T.) Thus by [10], $M(\mathrm{Aut}(T)) = C_s$ where $s = (2, |M(T)|)$, and if $s = 2$, then $\mathrm{Aut}(T)$ has exactly two universal covering groups. The ordinary character table of one of these groups is listed in [10], and we denote this group by $2.T.2^+$. We denote the other universal covering group by $2.T.2^-$; its character table is easily derived from that of $2.T.2^+$ (see [10, Chap. 6, §6]). In Table 3, for the convenience of the reader, we list the orders of T, its Schur multiplier $M(T)$, and its outer automorphism group $\mathrm{Out}(T)$.

For a prime p, the (p-modular) Brauer character table of G encodes information about the absolutely irreducible representations of G in characteristic p by lifting the eigenvalues of the matrices representing G to a field of characteristic 0 (see [24, §4] for a definition). We often use the known Brauer character tables of the sporadic simple groups. For those sporadic simple groups T whose order is at most $|\,\mathrm{McL}\,|$, the Brauer Atlas [24] contains the Brauer character tables of all bicyclic extensions of T for primes p dividing $|T|$; these tables are known for some larger groups, see [33] for the available data.

Let F be a field. We denote the group algebra of G over F by FG. All FG-modules in this paper are finite-dimensional, and we denote the dimension or degree of an FG-module V by $\dim_F(V)$. An irreducible FG-module V is *absolutely irreducible* if the extension of scalars $V \otimes_F E$ is irreducible for every field extension E of F, and this occurs precisely when $\mathrm{End}_{FG}(V) = F$ (see [3, Lemma VII.2.2]), where $\mathrm{End}_{FG}(V)$ denotes the set of FG-endomorphisms of V. We denote the finite field of order q by $\mathbb{F}_q$.

Let V be an irreducible $\mathbb{F}_pG$-module where p is prime, and let $k := \mathrm{End}_{\mathbb{F}_pG}(V)$. Now k is a finite division ring and therefore a field, so V is an absolutely irreducible kG-module where scalar multiplication is evaluation. Let χ be the Frobenius character of V as a kG-module, and let H be the Galois group of the field extension $k/\mathbb{F}_p$. By [3, Theorem VII.1.16], $k = \mathbb{F}_p(\{\chi(g) : g \in G\})$ and $V \otimes_{\mathbb{F}_p} k = \bigoplus_{\gamma \in H} V_\gamma$, where the V_γ are pairwise non-isomorphic absolutely irreducible kG-modules with character ${}^\gamma\chi : G \to k : g \mapsto \gamma(\chi(g))$ which cannot be realised over any proper subfield of k. Now $\dim_k(V)$ is given by the p-modular Brauer character table of G, and we can use this table to determine $\{\chi(g) : g \in G\}$ (see [24, §§2-5]) and therefore the $\mathbb{F}_pG$-module V.

Let N be a subgroup of G with index 2. Let V be an irreducible FG-module, and let W be an irreducible FN-submodule of $V|_N$, the restriction of V to N. It is well known from Clifford theory that either $V|_N = W$, or $V|_N = W \oplus Wg$ for all $g \in G \setminus N$. We frequently use the following observations without reference. If $V|_N = W \oplus Wg$ and W is

T	$\lvert M(T)\rvert$	$\lvert\mathrm{Out}(T)\rvert$	$\lvert T\rvert$
M_{11}	1	1	$2^4.3^2.5.11$
M_{12}	2	2	$2^6.3^2.5.11$
M_{22}	12	2	$2^7.3^2.5.7.11$
M_{23}	1	1	$2^7.3^2.5.7.11.23$
M_{24}	1	1	$2^{10}.3^3.5.7.11.23$
J_1	1	1	$2^3.3.5.7.11.19$
J_2	2	2	$2^7.3^3.5^2.7$
J_3	3	2	$2^7.3^5.5.17.19$
J_4	1	1	$2^{21}.3^3.5.7.11^3.23.29.31.37.43$
HS	2	2	$2^9.3^2.5^3.7.11$
McL	3	2	$2^7.3^6.5^3.7.11$
He	1	2	$2^{10}.3^3.5^2.7^3.17$
Ru	2	1	$2^{14}.3^3.5^3.7.13.29$
Suz	6	2	$2^{13}.3^7.5^2.7.11.13$
O'N	3	2	$2^9.3^4.5.7^3.11.19.31$
Co_3	1	1	$2^{10}.3^7.5^3.7.11.23$
Co_2	1	1	$2^{18}.3^6.5^3.7.11.23$
Co_1	2	1	$2^{21}.3^9.5^4.7^2.11.13.23$
Fi_{22}	6	2	$2^{17}.3^9.5^2.7.11.13$
Fi_{23}	1	1	$2^{18}.3^{13}.5^2.7.11.13.17.23$
Fi'_{24}	3	2	$2^{21}.3^{16}.5^2.7^3.11.13.17.23.29$
HN	1	2	$2^{14}.3^6.5^6.7.11.19$
Ly	1	1	$2^8.3^7.5^6.7.11.31.37.67$
Th	1	1	$2^{15}.3^{10}.5^3.7^2.13.19.31$
$\mathbb{B}$	2	1	$2^{41}.3^{13}.5^6.7^2.11.13.17.19.23.31.47$
$\mathbb{M}$	1	1	$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$

TABLE 3. The sporadic simple groups T

a faithful FN-module, then the base sizes of N on W and Wg are equal, and this base size is at least $b(G)$ (since $N \neq 1$). If instead $V|_N = W$ and V is a faithful FG-module, then $b(N) \leqslant b(G)$.

3. Some useful bounds

If G acts faithfully on a finite set Ω, then $|G| \leqslant |\Omega|^{b(G)}$ since, for every base B of G, each $g \in G$ is uniquely determined by $\{\alpha^g : \alpha \in B\}$. Thus we have the following elementary but useful result.

Lemma 3.1. *Let G be a finite group and F a finite field. If V is a faithful FG-module, then $|G| \leqslant (|V|-1)^{b(G)}$.*

For a group G, field F and FG-module V, define $C_V(g) := \{v \in V : vg = v\}$ for all $g \in G$. The following generalises [13, Lemma 3.3].

Lemma 3.2. *Let G be a finite group and F a finite field. Let V be a faithful FG-module. Let X be a set of representatives for the conjugacy classes of elements of prime order in G.*

If n is a positive integer for which

$$|V|^n > \sum_{g \in X} |g^G||C_V(g)|^n, \tag{3.1}$$

then $b(G) \leqslant n$.

Proof. Let Y be the set of elements of prime order in G, and let W be a faithful FG-module. If G has no regular orbit on W, then $W = \bigcup_{g \in Y} C_W(g)$, so $|W| \leqslant \sum_{g \in X} |g^G||C_W(g)|$. The base size of G on V is at most n if and only if G has a regular orbit on the faithful FG-module V^n. Since $C_{V^n}(g) = C_V(g)^n$, the result follows. □

Let G be a finite group such that $G/Z(G)$ is almost simple with socle T, and let $g \in G \setminus Z(G)$. Now $\langle T, Z(G)g\rangle$ is generated by the T-conjugates of $Z(G)g$, so we may define $r(g)$ to be the minimal number of T-conjugates of $Z(G)g$ generating $\langle T, Z(G)g\rangle$. This extends the definition given in §1. The following generalises [13, Lemma 3.5].

Lemma 3.3. *Let G be a finite group with $G/Z(G)$ almost simple and V a faithful irreducible $\mathbb{F}_qG$-module where q is a prime power. Let X be a set of representatives for the conjugacy classes of non-central elements of prime order in G, and let $u(G, q)$ be the largest integer such that*

$$1 \leqslant \sum_{g \in X} |g^G|(1/q)^{u(G,q)/r(g)}.$$

If G has no regular orbit on V, then $\dim_{\mathbb{F}_q}(V) \leqslant u(G, q)$.

Proof. Let $d := \dim_{\mathbb{F}_q}(V)$. Note that $C_V(g) = \{0\}$ for $g \in Z(G) \setminus \{1\}$. If G has no regular orbit on V, then by Lemma 3.2 and [13, Lemma 3.4],

$$q^d \leqslant \sum_{g \in X} |g^G||C_V(g)| \leqslant \sum_{g \in X} |g^G|q^{d-d/r(g)},$$

so $d \leqslant u(G, q)$. □

4. Dimension gaps

In this section we consider those cases where the upper bound $u(G, p)$ for the dimension of a faithful irreducible $\mathbb{F}_pG$-module on which G has no regular orbit (as given by Lemma 3.3) is at least the minimal dimension of a faithful irreducible representation of G' in characteristic p (as given by [23]), but the p-modular Brauer character table of G is not yet known. These "dimension gaps" occur when (G, p) is one of $(\mathrm{J}_4, 2)$, $(\mathrm{Co}_1, 2)$, $(2.\mathrm{Co}_1, 3)$ or $(2.\mathrm{Co}_1, 5)$. For each, we first compute $u(G, p)$ using the ordinary character table of G and Theorem 1.3, and then determine the representations whose dimensions are at most $u(G, p)$. Note that these results (for the dimension bound of 250) are stated in [21], but explicit proofs, which often depend on computations with the MOC system [20], are omitted.

Lemma 4.1. *There is a unique faithful irreducible 2-modular representation of Co_1 of degree at most $u(\mathrm{Co}_1, 2) = 117$. This representation has degree 24.*

Proof. Recall from the list of maximal subgroups in [10] (as corrected in [24]) that Co_1 can be generated by subgroups $3^6{:}2.\mathrm{M}_{12}$ and $3.\mathrm{Suz}:2$, intersecting in $3^5{:}(2 \times \mathrm{M}_{11})$. The 2-modular irreducibles of $3.\mathrm{Suz}:2$ of degree at most 117 have degrees 1 and 24. Hence every irreducible character of Co_1 of degree at most 117 has character restriction composed of 1 and 24. Restricting to $3^5{:}(2 \times \mathrm{M}_{11})$, the 24 remains irreducible. Since the orbits of

$2.\mathrm{M}_{12}$ on the linear characters of 3^6 are $1 + 24 + 264 + 440$, the only possible character restriction to $3^6{:}2.\mathrm{M}_{12}$ is $24^k + 1^j$.

The 24 is not in the principal block of either $3.\mathrm{Suz}:2$, or of $3^6{:}2.\mathrm{M}_{12}$. Hence the principal and non-principal block components of the restrictions to these subgroups coincide. If $j > 0$, then the perfect group $3^6{:}2.\mathrm{M}_{12}$ acts trivially on the non-zero principal block component, a contradiction. Hence $j = 0$. Since the irreducible 24 for $3.\mathrm{Suz}:2$ has no non-splitting self-extensions, $3.\mathrm{Suz}:2$ acts completely reducibly, so there is a 24-dimensional subspace invariant under Co_1, implying $k = 1$. Finally, for every irreducible representation of degree 24, there is a unique amalgamation inside $\mathrm{GL}_{24}(2)$, so there is a unique such representation of Co_1. □

Lemma 4.2.

(1) *There is a unique faithful irreducible* 3*-modular representation of* $2.\mathrm{Co}_1$ *of degree at most* $u(2.\mathrm{Co}_1, 3) = 74$. *This representation has degree* 24.
(2) *There is a unique faithful irreducible* 5*-modular representation of* $2.\mathrm{Co}_1$ *of degree at most* $u(2.\mathrm{Co}_1, 5) = 50$. *This representation has degree* 24.

Proof. In each case, we can construct such a representation from two copies of $2^{12}{:}\,\mathrm{M}_{24}$, intersecting in $2^{6+12}{:}3.S_6$. Since the orbits of M_{24} on the linear characters of 2^{12} are $1 + 24 + 276 + 1771 + 2024$, the only faithful irreducible representation of $2^{12}{:}\,\mathrm{M}_{24}$ of degree less than 276 in odd characteristic is the monomial 24. This remains irreducible on restriction to $2^{6+12}{:}3.S_6$.

Moreover, every relevant faithful irreducible representation of $2.\mathrm{Co}_1$ must have character restriction 24^k to each of these subgroups. Since the irreducible 24 for $2^{12}{:}\,\mathrm{M}_{24}$ has no non-splitting self-extensions, the subgroups in question act completely reducibly, implying that $k = 1$. Since every matrix that commutes with the action of $2^{6+12}{:}3.S_6$ commutes with the action of both copies of $2^{12}{:}\,\mathrm{M}_{24}$, there is a unique amalgamation of groups into $\mathrm{GL}_{24}(3)$, or $\mathrm{GL}_{24}(5)$, and so a unique representation of $2.\mathrm{Co}_1$ of dimension 24. □

Our proof for $(\mathrm{J}_4, 2)$ is motivated by the approach of [23, §4.3.21], which in turn is based on [2, Chap. 6].

Lemma 4.3. *There is a unique faithful irreducible* 2*-modular representation of* J_4 *of degree at most* $u(\mathrm{J}_4, 2) = 129$. *This representation has degree* 112.

Proof. Let V be a faithful irreducible 2-modular representation of $G := \mathrm{J}_4$ of degree at most 129. Recall that G can be generated by subgroups $K := U_3(11){:}2$ and $L := 11^{1+2}{:}(5 \times 2.S_4)$, intersecting in $H := 11^{1+2}{:}(5 \times 8{:}2)$. Also, $K' = U_3(11)$ and L generate G and intersect in $H_1 := 11^{1+2}{:}(5 \times 8)$; see [2, p. 63]. In particular, there exists an involution $z \in H \setminus H_1$ where $z \in L$ and $K = \langle K', z\rangle$.

The 2-modular Brauer character table of K shows that V has character restriction $110 + 1^k$ to K. Similarly, V has character restriction $110' + \lambda$ to L, where $110'$ is one of the three irreducible Brauer characters of this degree, and λ has constituents of degree 1 and 2. By considering the unique conjugacy class of elements of order 3 in G, we deduce that $k \geqslant 2$, the irreducible Brauer character of degree 110 occurring in the restriction to L is one of the non-rational ones, and λ has a unique constituent of degree 2 apart from $k - 2$ linear ones.

By considering the unique conjugacy class of elements of order 5 in G, we deduce that the constituents of λ are necessarily rational, so are uniquely determined by their degree. The 2-modular Brauer character table of H shows that the irreducible Brauer characters of degree 110 of K and L restrict irreducibly to H. A consideration of 2-blocks yields the

block decomposition of the various restrictions as

$$V|_K \sim (110 + 1^k) \quad \text{and} \quad V|_L \sim 110' \oplus (2 + 1^{k-2}) \quad \text{and} \quad V|_H \sim 110 \oplus (1^k).$$

Hence there is a unique L-submodule U_{110} of V of dimension 110, which cannot be K-invariant, so the unique 110-local K-submodule of V is reducible. (Here we freely use terminology from [27].) By computing suitable cohomology groups, we determine all possible downward K-extensions of 110 with kernel having only trivial constituents. This shows that the local submodule in question, say U_{111}, is uniserial with descending composition series 110/1. In particular, this specifies a trivial K-submodule U_1 of V. Moreover, $(V/U_{111})|_K \sim 1^{k-1}$; thus K', being perfect, acts trivially on this quotient.

Observe that $[L{:}H] = 3$, where the action of L on the cosets of H is equivalent to the natural action of $S_3 \cong S_4/V_4$; thus the associated permutation module is semisimple of shape $2 \oplus 1$. Since U_1 cannot be L-invariant, the L-submodule U_1^L generated by U_1 is either irreducible of degree 2, or semisimple of shape $2 \oplus 1$. Hence we get an L-submodule $110' \oplus U_1^L$, which contains U_{111}, and so is K'-invariant. Hence $110' \oplus U_1^L = V$, implying that $\dim_{\mathbb{F}_2}(V) \in \{112, 113\}$; in other words, $k = 2$ or $k = 3$.

Let $X \leqslant V$ be the image of the action of $1 + z$, where we view the latter as an element of both $\mathbb{F}_2K$ and $\mathbb{F}_2L$. Since $1 + z$ has an image of dimension 55 on 110, both cases for $V|_L$ yield $\dim_{\mathbb{F}_2}(X) = 56$, where X intersects non-trivially with the irreducible direct summand 2.

Next, again using a cohomological approach, we determine all indecomposable K-modules (up to isomorphism) having the constituent 110 once, and the trivial constituent 1 with multiplicity at most 3, where we restrict to those modules having 110 neither in their head nor in their socle. This yields two isomorphism types V_{112} and $V_{112'}$ of modules, both uniserial with descending composition series 1/110/1, a module V_{113} of dimension 113 with head of shape $1 \oplus 1$ and socle of shape 1, and the dual V_{113}^* of V_{113}. In all cases the unique 110-local submodule is isomorphic to U_{111}.

Suppose that $k = 3$. If $V|_K = V_{113}$, for which $1 + z$ has image of dimension 56, then $X \leqslant U_{111}$. This implies that $110' \oplus 2$ contains U_{111}. Since the latter coincides with the radical of V_{113}, we conclude that $110' \oplus 2$ is K'-invariant, a contradiction. Similarly, if $V|_K = V_{113}^*$, then, since $V|_L$ is self-dual, we obtain a contradiction by dualising the picture. Finally, let $V|_K$ have a direct summand isomorphic to V_{112} or $V_{112'}$. Now $1 + z$ has an image of dimension 55 on $V_{112'}$, say, and $1 + z$ has an image of dimension 56 on V_{112}. Hence $V|_K = V_{112} \oplus 1$, where again $X \leqslant U_{111}$, yielding a contradiction as above. This excludes the case $k = 3$.

Hence $k = 2$, so $\dim_{\mathbb{F}_2}(V) = 112$. By the above, $V|_K = V_{112}$. The arguments of [2, pp. 63ff.] now imply that V is uniquely determined up to isomorphism. □

5. Comments on computations

We usually used the Atlas database [32] to access explicit matrix and permutation representations on standard generators, and straight line programs on these for conjugacy class representatives. In GAP we accessed this data through the AtlasRep package [31]. The ordinary and Brauer character tables from [10, 24, 33] are available through the Character Table Library [5] of GAP.

We used the Orb package [29] available through GAP. It has highly optimised techniques to enumerate orbits of vectors or subspaces in a G-module V. It can be used directly to enumerate a G-orbit point-by-point. But a critical feature is that it can also enumerate a G-orbit in larger pieces consisting of suborbits with respect to a helper subgroup $U \leqslant G$. During the enumeration process, to recognise quickly whether a U-suborbit has been

encountered before, helper U-sets, homomorphic images of the given ones, are used; for example, if the G-orbit consists of vectors in a G-module V, then the helper U-set may consist of the vectors in an epimorphic image of the U-module $V|_U$. To fully utilise the helper U-sets, these must be enumerated in turn, which is done using the same process, giving rise to a divide-and-conquer strategy. A detailed account of this approach is given in [28], whose terminology we freely borrow here.

Magma has an implementation of an algorithm of Cannon and Holt [9] which constructs faithful irreducible representations defined over a given finite field of a finite permutation group; we used this to construct representations, either all or those of specified degree, of certain small degree permutation groups. Occasionally, we used our implementation in Magma of the algorithm of [15] to conjugate a given representation to one defined over a subfield.

Applications of Lemma 3.2 require knowledge of conjugacy classes of G. To compute these, we sometimes used the infrastructure of [1] available in Magma; classes in J_4 were written down directly using the results of [22] as summarised at [32].

6. Proof of Theorem 1.3

Let G be an almost simple group whose socle T is sporadic. First suppose that $T \neq \mathbb{M}$; we address this case in Lemma 6.2.

(i) Using explicit words given on standard generators from the Atlas database, or the general purpose algorithm available in GAP, we determine representatives of conjugacy classes of G.

(ii) For each class representative g, we perform a random search through g^G for a subset S generating G or T. If G has a "small degree" permutation representation, then we check generation by S directly. For J_4, HN, Ly, Th and $\mathbb{B}$, we use instead a faithful matrix representation and a different generation check: we select a set of primes whose product divides the order of T, but of none of its maximal subgroups, and now search randomly in $\langle S\rangle$ for elements having these orders. Hence, for each class representative g, we obtain an upper bound $u(g)$ to $r(g)$.

(iii) Clearly $r(g) \geqslant 3$ if g is an involution, and $r(g) \geqslant 2$ otherwise. If $u(g)$ equals this lower bound, then $r(g) = u(g)$. This leaves unresolved the cases listed in Table 2. (Since in all cases $u(g) = r(g)$, the random search achieved the best possible outcome.)

(iv) Since no non-trivial element of $\mathrm{Aut}(G)$ stabilises a generating $\ell(g)$-tuple of distinct elements of g^G, we deduce that

$$\prod_{i=0}^{\ell(g)-1} (|g^G| - i) \geqslant |\mathrm{Aut}(G)|.$$

This provides a new lower bound $\ell(g)$ for $r(g)$, and resolves the following cases where $\ell(g) = u(g)$:

$$(\mathrm{J}_2, 3\mathrm{A}),\ (\mathrm{McL}, 3\mathrm{A}),\ (\mathrm{Co}_1, 3\mathrm{A}),\ (\mathrm{Fi}_{22}, 3\mathrm{A}),\ (\mathrm{Fi}_{23}, 3\mathrm{A}),$$

$$(\mathrm{Fi}'_{24}, 3\mathrm{A}),\ (\mathrm{Fi}'_{24}, 3\mathrm{B}),\ (\mathrm{Fi}'_{24}{:}2, 2\mathrm{C}),\ (\mathrm{HN}{:}2, 4\mathrm{D}),\ (\mathrm{Ly}, 3\mathrm{A}),\ (\mathbb{B}, 2\mathrm{A}).$$

(v) In most cases, a search through a set of representatives $g_1, \ldots, g_{u(g)-1}$ of the G-orbits on the set of $(u(g)-1)$-tuples of g^G is feasible. These are found readily as follows. Fixing $g_1 := g$, we let g_2 run through a set of representatives of the $C_G(g_1)$-orbits in g^G, for fixed g_2 we let g_3 run through a set of representatives of

the $C_G(g_1, g_2)$-orbits in g^G, and so on. We check directly the order of the subgroup generated by each tuple. This resolves the cases

$$(\mathrm{M}_{22}{:}2, 2\mathrm{B}),\ (\mathrm{J}_2, 2\mathrm{A}),\ (\mathrm{HS}, 4\mathrm{A}),\ (\mathrm{HS}{:}2, 2\mathrm{C}),\ (\mathrm{Suz}, 3\mathrm{A}),$$
$$(\mathrm{Co}_2, 2\mathrm{A}),\ (\mathrm{Fi}_{22}, 2\mathrm{A}),\ (\mathrm{Fi}_{22}{:}2, 2\mathrm{D}),\ (\mathrm{Fi}_{23}, 2\mathrm{A}).$$

We now resolve the remaining cases.

Lemma 6.1.

(1) *Let* $G = \mathrm{Fi}_{22}$. *If* $g \in G$ *is in class* 3B, *then* $r(g) = 3$.
(2) *Let* $G = \mathrm{Fi}_{23}$. *If* $g \in G$ *is in class* 3B, *then* $r(g) = 3$.

Proof. In each case we know from (ii) that $r(g) \leqslant 3$. Hence we must show that there is no $h \in g^G$ such that $\{g, h\}$ generates G. It suffices to let h run through a set of representatives of the $C_G(g)$-orbits on g^G. Moreover, if $\{g, h\}$ generates G, then $C_G(g) \cap C_G(h) = Z(G) = \{1\}$, so h belongs to a regular $C_G(g)$-orbit. Thus it suffices to find representatives of the regular $C_G(g)$-orbits on g^G. The latter are found, or their non-existence proved, by an application of Orb with helper subgroups. If there are relevant $C_G(g)$-orbits, then we determine the order of the subgroups thus generated, and verify that none is G.

We summarise the details of our Orb computations.

(1) $G = \mathrm{Fi}_{22}$ has a faithful permutation representations on 3510 points. The action of G on its conjugacy class g^G, which has size 25 625 600, is equivalent to its action on the cosets of $C_G(g) \cong 3^{1+6}.2^{3+4}.3^2$, where $N_G(\langle g \rangle) \cong 3^{1+6}.2^{3+4}.3^2.2$ is a maximal subgroup of G. There is a vector v in the absolutely irreducible $\mathbb{F}_3 G$-module V of dimension 924 which is fixed precisely by $C_G(g)$, so v^G is equivalent to g^G as a G-set. Using the permutation character of the action of G on the cosets of $C_G(g)$, we find that $C_G(g)$ has 64 orbits in v^G. We use the chain of helper subgroups $\{1\} = U_0 < U_1 = U_2 < U_3 = G$ specified in Table 4, where we also list the dimension d_i of the various helper quotients of V. In particular, we choose $U_1 = U_2 = C_G(g)$, but use distinct helper quotients. To find all regular $C_G(g)$-orbits in the G-orbit v^G, we must enumerate at least $1 - |C_G(g)|/|v^G| \sim 90\%$ of it. Enumerating a total of 23 471 749 vectors in v^G, that is $\sim 91\%$ of v^G, we find 37 orbits, precisely 5 of which are regular $C_G(g)$-orbits. Translating back to g^G, we find that none gives rise to a two-element generating set of G, generating instead either $G_2(3)$ or A_9.

i	U_i	$\lvert U_i \rvert$	$[U_i{:}U_{i-1}]$	d_i
3	Fi_{22}	64 561 751 654 400	25 625 600	924
2	$3^{1+6}.2^{3+4}.3^2$	2 519 424	1	17
1	$3^{1+6}.2^{3+4}.3^2$	2 519 424	2 519 424	5

Table 4. Helper subgroups for Fi_{22}

(2) $G = \mathrm{Fi}_{23}$ has a faithful permutation representations on 31671 points. The action of G on its conjugacy class g^G, which has size 2 504 902 400, is equivalent to its action on the cosets of $C_G(g) \cong 3^{1+8}.2^{1+6}.3^{1+2}.2A_4$, where $N_G(\langle g \rangle) \cong 3^{1+8}.2^{1+6}.3^{1+2}.2S_4$ is a maximal subgroup of G. There is a vector v in the absolutely irreducible $\mathbb{F}_3 G$-module V of dimension 528 which is fixed precisely by $N_G(\langle g \rangle)$, so v^G has length 1 252 451 200, and is equivalent to the action of G on the cosets of $N_G(\langle g \rangle)$. Since a regular $C_G(g)$-orbit in g^G implies a $C_G(g)$-orbit in v^G of length divisible by $|C_G(g)|/2$, we must find representatives of the latter. Using the permutation

character of the action of G on the cosets of $N_G(\langle g\rangle)$, we find that $C_G(g)$ has 37 orbits in v^G. We use the chain of helper subgroups $\{1\} = U_0 < U_1 < U_2 < U_3 < U_4 < U_5 = G$ specified in Table 5, where we also list the dimension d_i of the various helper quotients of V. In particular, we choose $U_4 = C_G(g)$, and use the same helper quotient for all the helper subgroups. To find all relevant $C_G(g)$-orbits in the G-orbit v^G, we must enumerate at least $1 - |C_G(g)|/(2 \cdot |v^G|) \sim 35\%$ of it. Enumerating a total of 1 157 675 328 vectors in v^G, that is $\sim 90\%$ of v^G, we find 13 orbits, none of which has length divisible by $|C_G(g)|/2$. □

i	U_i	$\lvert U_i\rvert$	$[U_i{:}U_{i-1}]$	d_i
5	Fi_{23}	4 089 470 473 293 004 800	2 504 902 400	528
4	$3^{1+8}.2^{1+6}.3^{1+2}.2A_4$	1 632 586 752	24	13
3	$3^{1+8}.2^{1+6}.3^{1+2}$	68 024 448	27	13
2	$3^{1+8}.2^{1+6}$	2 519 424	128	13
1	3^{1+8}	19 683	19 683	13

TABLE 5. Helper subgroups for Fi_{23}

Lemma 6.2. *If $g \in \mathbb{M}$ is in class* 2A *or* 2B *then $r(g) = 3$; all other non-trivial elements satisfy $r(g) = 2$.*

Proof. From the (almost complete) classification of the maximal subgroups of $\mathbb{M}$ (see [30, Table 5.6]), we deduce that, for both $p = 59$ and 71, there is a unique conjugacy class of maximal subgroups of order divisible by p, the groups in question being isomorphic to $\mathrm{L}_2(p)$. A consideration of class multiplication coefficients, computed from the ordinary character table of $\mathbb{M}$, shows that these are non-zero for all conjugacy class triples $(\mathrm{X}, \mathrm{X}, 71\mathrm{A})$ and $(\mathrm{X}, \mathrm{X}, 59\mathrm{A})$, where X runs through all conjugacy classes except 1A, 2A, and 2B. Hence $r(g) = 2$ for all conjugacy classes containing elements g of order at least 3 and not fusing into both $\mathrm{L}_2(59)$ and $\mathrm{L}_2(71)$.

This leaves the non-involutory conjugacy classes 3B, 5B, and 6E. Since the squares of the elements of 6E belong to 3B, it suffices to deal with the first two. For each conjugacy class, X say, we compute the number of pairs of elements of X whose product belongs to 71A, and compare this with the number of such pairs contained in some maximal subgroup isomorphic to $\mathrm{L}_2(71)$. In each case there are (many) more pairs in $\mathbb{M}$ than are accounted for by these maximal subgroups. This implies that $r(g) = 2$ for elements g belonging to either 3B or 5B.

It remains to consider the involutory conjugacy classes 2A and 2B. The class multiplication coefficients associated with the conjugacy class triples $(2\mathrm{B}, 2\mathrm{B}, 41\mathrm{A})$ and $(2\mathrm{B}, 41\mathrm{A}, 71\mathrm{A})$ are both non-zero. Similarly, the class multiplication coefficients associated with the conjugacy class triples $(2\mathrm{A}, 2\mathrm{A}, 5\mathrm{A})$ and $(2\mathrm{A}, 5\mathrm{A}, 71\mathrm{A})$ are both non-zero; moreover conjugacy class 5A does not fuse into $\mathrm{L}_2(71)$. This implies that $r(g) = 3$ for elements g belonging to either 2A or 2B. □

7. Proof of Theorem 1.1

Let T be a sporadic simple group, and let G be a covering group of an almost simple group with socle T. Let V be a faithful irreducible $\mathbb{F}_pG$-module where p is a prime dividing $|G|$. Let $k := \mathrm{End}_{\mathbb{F}_pG}(V)$. Note that $p \nmid |Z(G)|$ since $Z(G) \leqslant k^*$.

Suppose that G has no regular orbit on V, so $b(G) > 1$. Let $m(G, p)$ denote the minimal dimension of a faithful irreducible representation of G in characteristic p. Let $u(G, p)$ be

as defined in Lemma 3.3. Recall that G' denotes the derived subgroup of G. Observe that

$$m(G', p) \leqslant m(G, p) \leqslant \dim_k(V) \leqslant \dim_{\mathbb{F}_p}(V) \leqslant u(G, p).$$

Lemma 7.1. $(G, p, \dim_{\mathbb{F}_p}(V))$ *is listed in Table* 6.

Proof. We use the ordinary character table of G and Theorem 1.3 to compute the upper bound $u(G, p)$. By [23], $m(G', p)$ is known. If $m(G', p) > u(G, p)$, then we have a contradiction. If (G, p) is one of $(\mathrm{J}_4, 2)$, $(\mathrm{Co}_1, 2)$, $(2.\mathrm{Co}_1, 3)$ or $(2.\mathrm{Co}_1, 5)$, then $\dim_{\mathbb{F}_p}(V)$ is determined by Lemmas 4.1–4.3. Otherwise, we use the p-modular Brauer character table of G to determine the possibilities for $\dim_{\mathbb{F}_p}(V)$. □

We adopt several conventions in Table 6. The dimensions in bold are precisely those listed in Table 1. We write $d^{(m)}$ when there are exactly m d-dimensional $\mathbb{F}_pG$-modules and $m > 1$, except for the case $(G, p, \dim_{\mathbb{F}_p}(V)) = (\mathrm{M}_{11}, 3, 10)$. Here we write **10** and $10^{(2)}$; the one in bold denotes the unique faithful irreducible 10-dimensional $\mathbb{F}_3\,\mathrm{M}_{11}$-module with the property that an involution, viewed as an element of $\mathrm{GL}_{10}(3)$, has trace $-1 \in \mathbb{F}_3$.

Lemma 7.2. *If* $\dim_{\mathbb{F}_p}(V)$ *is not bold in Table* 6*, then* $b(G) = 1$.

Proof.

(i) If $(G, p, \dim_{\mathbb{F}_p}(V))$ is one of

$$(\mathrm{M}_{11}, 3, 10),\ (2.\mathrm{M}_{22}.2^+, 7, 10),\ (2.\mathrm{M}_{22}, 7, 10),\ (\mathrm{HS}{:}2, 3, 22),\ (\mathrm{HS}, 3, 22),$$

then we use Magma to prove that $b(G) = 1$.

(ii) If $(G, p, \dim_{\mathbb{F}_p}(V))$ is $(\mathrm{M}_{24}, 3, 22)$ or $(3.\mathrm{Fi}_{22}, 2, 54)$, then we use Orb directly to prove that $b(G) = 1$.

(iii) If $(G, p, \dim_{\mathbb{F}_p}(V)) = (\mathrm{Co}_2, 5, 23)$, then we use Orb with helper subgroup $2^4 \times 2^{1+6}.A_8$ to prove that $b(G) = 1$.

Otherwise, we use Magma to prove that inequality (3.1) holds with $n = 1$, in which case $b(G) = 1$ by Lemma 3.2. □

Lemma 7.3. *If* $\dim_{\mathbb{F}_p}(V)$ *is bold in Table* 6*, then one of the following holds.*

(1) $(G, p, \dim_{\mathbb{F}_p}(V), b(G))$ *is correctly listed in Table* 1.
(2) $(G, p, \dim_{\mathbb{F}_p}(V)) = (2.\mathrm{Co}_1, 3, 24)$ *and* $b(G) \in \{2, 3\}$.
(3) $(G, p, \dim_{\mathbb{F}_p}(V)) = (2.\mathrm{Co}_1, 7, 24)$ *and* $b(G) \leqslant 2$.

Proof. Let $\ell := \lceil (\log |G|)/\log(|V| - 1) \rceil$, and recall that $b(G) \geqslant \ell$ by Lemma 3.1. Let n be the least positive integer such that (3.1) holds, so $b(G) \leqslant n$ by Lemma 3.2. For each relevant group we compute n using Magma.

(i) If $(G, p, \dim_{\mathbb{F}_p}(V))$ is one of

$$(\mathrm{M}_{11}, 3, 5),\ (\mathrm{M}_{23}, 2, 11),\ (\mathrm{M}_{24}, 2, 11),\ (\mathrm{J}_2, 2, 12),\ (\mathrm{J}_2{:}2, 2, 12),$$
$$(3.\mathrm{Suz}, 2, 24),\ (\mathrm{Co}_3, 2, 22),\ (\mathrm{Co}_1, 2, 24),$$

then we use Magma to prove that $b(G) = \ell$.

(ii) If $(G, p, \dim_{\mathbb{F}_p}(V))$ is one of

$$(\mathrm{M}_{11}, 3, 10),\ (\mathrm{M}_{12}, 2, 10),\ (\mathrm{M}_{12}{:}2, 2, 10),\ (2.\mathrm{M}_{12}, 3, 6),\ (2.\mathrm{M}_{12}.2^{\pm}, 3, 12),$$
$$(\mathrm{M}_{22}, 2, 10),\ (3.\mathrm{M}_{22}, 2, 12),\ (\mathrm{J}_1, 2, 20),\ (2.\mathrm{J}_2, 3, 14),\ (2.\mathrm{J}_2.2^-, 3, 14),$$

then $n > \ell$, and we use Magma to prove that $b(G) = n$.

(iii) If $(G, p, \dim_{\mathbb{F}_p}(V)) = (\mathrm{M}_{22}{:}2, 2, 10)$, then $\ell = 2$ and $n = 4$. We use Magma to prove that $b(G) = 3$.

G	$p=2$	$p=3$	$p=5$	$p=7$	$p=11$	$p=13$	$p=23$
M_{11}	**10**	**5**$^{(2)}$, **10**, 10$^{(2)}$	10				
M_{12}	**10**, 32	**10**$^{(2)}$, 15$^{(2)}$	11$^{(2)}$				
$M_{12}:2$	**10**, 32	20					
$2.M_{12}$		**6**$^{(2)}$, **10**$^{(2)}$	12				
$2.M_{12}.2^+$		**10**$^{(4)}$, **12**			10$^{(4)}$		
$2.M_{12}.2^-$		**12**, 20$^{(2)}$					
M_{22}	**10**$^{(2)}$, 34	21					
$M_{22}:2$	**10**$^{(2)}$, 34	21$^{(2)}$					
$2.M_{22}$		20		10	10$^{(2)}$		
$2.M_{22}.2^+$		20$^{(2)}$		10$^{(2)}$	10$^{(4)}$		
$2.M_{22}.2^-$		20$^{(2)}$					
$3.M_{22}$	**12**, 30						
M_{23}	**11**$^{(2)}$, 44$^{(2)}$	22					
M_{24}	**11**$^{(2)}$, 44$^{(2)}$	22					
J_1	**20**				7		
J_2	**12**, 28, 36		14				
$J_2:2$	**12**, 28, 36		14$^{(2)}$				
$2.J_2$		**12**, **14**	**6**, 14	12			
$2.J_2.2^+$		**12**	12	12			
$2.J_2.2^-$		**12**, **14**$^{(2)}$	12	12			
$3.J_3$	**18**, 36$^{(2)}$						
J_4	112						
HS	**20**	22	21				
HS:2	**20**	22$^{(2)}$	21$^{(2)}$				
McL	**22**	**21**	21				
McL:2	**22**	**21**$^{(2)}$	21$^{(2)}$				
He	51$^{(2)}$						
Ru	**28**						
$2.Ru$			28$^{(2)}$				
$2.Suz$		**12**					
$2.Suz.2^+$		**12**$^{(2)}$					
$2.Suz.2^-$		**24**					
$3.Suz$	**24**						
$6.Suz$			24	**12**$^{(2)}$		**12**$^{(2)}$	
Co_3	**22**	**22**	23	23			
Co_2	**22**	**23**	23	23	23		
Co_1	**24**						
$2.Co_1$		**24**	**24**	**24**	24	24	24
Fi_{22}	78						
$Fi_{22}:2$	78						
$3.Fi_{22}$	54						

TABLE 6. $\mathbb{F}_pG$-modules with $\dim_{\mathbb{F}_p}(V) \leqslant u(G,p)$

(iv) If $(G, p, \dim_{\mathbb{F}_p}(V)) = (2.\mathrm{Co}_1, 3, 24)$, then $\ell = 2$ and $n = 3$, so (2) holds. Similarly, if $(G, p, \dim_{\mathbb{F}_p}(V)) = (2.\mathrm{Co}_1, 7, 24)$, then $\ell = 1$ and $n = 2$, so (3) holds.

(v) If $(G, p, \dim_{\mathbb{F}_p}(V))$ is one of

$$(\mathrm{McL}, 3, 21),\ (\mathrm{McL}:2, 3, 21),\ (6.\mathrm{Suz}, 13, 12),$$

then $\ell = 1$ and $n = 2$. We use ORB and helper subgroups $\mathrm{M}_{11}, \mathrm{M}_{11}.2$, and $6.3^{(2+4)}.[48]$ respectively to prove that $b(G) = 2$.

In all other cases, $n = \ell$ so $b(G) = \ell$. □

Lemma 7.4. *If* $(G, p, \dim_{\mathbb{F}_p}(V)) = (2.\mathrm{Co}_1, 3, 24)$, *then* $b(G) = 2$.

Proof. By Lemma 7.3, $b(G) \geqslant 2$. Let $M \cong 2^{12}{:}\,\mathrm{M}_{24}$ be a maximal subgroup of G and let $H \cong \mathrm{M}_{24}$ be a fixed complement of $O_2(M) \cong 2^{12}$. As an $\mathbb{F}_2 H$-module, $O_2(M)$ is isomorphic to the binary Golay code, and so is uniserial with descending composition series 11/1. Thus all subgroups of M properly containing H necessarily contain $Z(M) = Z(G)$. Moreover, by [10], every maximal subgroup $\tilde{M}$ of G containing H is G-conjugate to M, so we may assume that $\tilde{M} = M$.

We show that there exist $v, w \in V$ such that $C_G(v) = H$ and $C_H(w) = \{1\}$. The restriction of V to H is isomorphic to the natural permutation $\mathbb{F}_3 H$-module, which is uniserial with descending composition series 1/22/1. Hence there exists $0 \neq v \in V$ fixed by H. Every subgroup of G properly containing H necessarily contains $Z(G)$, so it does not fix v. This shows that $C_G(v) = H$. Lemma 7.2 shows that the irreducible H-subquotient of dimension 22 of V has a regular vector. Hence $b(G) = 2$. □

Lemma 7.5. *If* $(G, p, \dim_{\mathbb{F}_p}(V)) = (2.\mathrm{Co}_1, 7, 24)$, *then* $b(G) = 2$.

Proof. By Lemma 7.3, $b(G) \leqslant 2$. To show that G does not have a regular orbit on V, we use ORB with the chain of helper subgroups $\{1\} = U_0 < U_1 < U_2 < U_3 < U_4 = G$ specified in Table 7; these are chosen so that $Z(G) < U_1$. The helper quotients of V, associated with the various helper subgroups, have dimension d_i.

i	U_i	$\lvert U_i\rvert$	$[U_i{:}U_{i-1}]$	d_i
4	$2.\mathrm{Co}_1$	8 315 553 613 086 720 000	46 621 575	24
3	$(2 \times 2^{1+8}_+).O^+_8(2)$	178 362 777 600	270	16
2	$(2^2.2^7).2^6.A_8$	660 602 880	560	8
1	$[2^{17}]{:}3^2$	1 179 648	1 179 648	8

TABLE 7. Helper subgroups for G

Since the Cauchy-Frobenius Lemma shows that there are 1097 G-orbits on V, it is infeasible to enumerate sufficiently many (randomly chosen) orbits to rule out the existence of a regular orbit. Instead, we consider the projective space $\mathbb{P}(V)$, the set of 1-spaces in V, which we view as a $G/Z(G)$-set. Observe that $|\mathbb{P}(V)| = (7^{24} - 1)/6 \sim 3.2 \cdot 10^{19}$; to exclude a regular $G/Z(G)$-orbit on $\mathbb{P}(V)$ we must enumerate $1 - |G|/(2 \cdot |\mathbb{P}(V)|) \sim 87\%$ of it. With a random search we find representatives of 75 G-orbits covering $\sim 90\%$ of $\mathbb{P}(V)$ without detecting a regular $G/Z(G)$-orbit.

But there might exist $v \in V$ having stabiliser $C_G(v) = \{1\}$ such that the 1-space $\langle v \rangle \in \mathbb{P}(V)$ has non-trivial stabiliser $C_G(\langle v \rangle) \cong \mathbb{F}_7^*$. Hence we must also exclude G-orbits of length $|G|/6$. To do this by an exhaustive enumeration of $\mathbb{P}(V)$, we must cover $1 - |G|/(6 \cdot |\mathbb{P}(V)|) \sim 96\%$ of the space. The Cauchy-Frobenius Lemma shows that there are 382 G-orbits on $\mathbb{P}(V)$, some of which may escape a random search.

Hence we proceed differently. If v is as above, then $C_G(\langle v\rangle) = \langle tz\rangle$, where $t \in G$ has order 3, and $1 \neq z \in Z(G)$. Now v is an eigenvector for t with respect to an eigenvalue ω, where $\omega \in \mathbb{F}_7^*$ is a primitive third root of unity. By [10], there are precisely four conjugacy classes of elements of order 3 in G; see Table 8, where the associated centralisers and the dimension $d_\omega(t)$ of the eigenspace $E_\omega(t)$ of t with respect to the eigenvalue ω are given.

t	$d_\omega(t)$	$C_G(t)$	$\lvert C_G(t)\rvert$
$3A$	12	6.Suz	2 690 072 985 600
$3B$	6	$2.(3^2.U_4(3).2)$	117 573 120
$3C$	9	$2.(3^{1+4}{:}2.S_4(3))$	25 194 240
$3D$	8	$2.A_9 \times 3$	1 088 640

TABLE 8. 3-centralisers in G

Since the conjugacy classes under consideration are rational, the normaliser $N_G(\langle t\rangle)$ interchanges the eigenspaces $E_\omega(t)$ and $E_{\omega^2}(t)$, so it suffices to consider either of the primitive third roots of unity in $\mathbb{F}_7^*$. Now $C_G(t)$ acts on $E_\omega(t)$, and hence $C_G(t)/\langle tz\rangle$ acts on $\mathbb{P}(E_\omega(t))$. Since $C_{C_G(t)}(\langle v\rangle) = C_G(\langle v\rangle) = \langle tz\rangle$, we conclude that $\langle v\rangle$ belongs to a regular $C_G(t)/\langle tz\rangle$-orbit on $\mathbb{P}(E_\omega(t))$.

For conjugacy classes $3A$ and $3B$, we check that $|\mathbb{P}(E_\omega(t))| = (7^{d_\omega(t)} - 1)/6 < |C_G(t)|/6$, hence there cannot be a regular $C_G(t)/\langle tz\rangle$-orbit. To deal with classes $3C$ and $3D$, we pick a representative t, compute the action of $C_G(t)$ on $E_\omega(t)$, and enumerate $\mathbb{P}(E_\omega(t))$ completely by a standard orbit computation. For conjugacy class $3C$, none of the 21 $C_G(t)/\langle tz\rangle$-orbits in $\mathbb{P}(E_\omega(t))$ is regular; for conjugacy class $3D$ precisely one of the 26 relevant orbits is regular. We pick $\langle v\rangle$ from this unique regular $C_G(t)/\langle tz\rangle$-orbit on $\mathbb{P}(E_\omega(t))$, and use ORB to enumerate 51% of the G-orbit of $\langle v\rangle$ in $\mathbb{P}(V)$. This shows that $C_G(\langle v\rangle) \cong Z(G) \times A_4$. Hence $b(G) = 2$. □

REFERENCES

[1] BÄÄRNHIELM, H., HOLT, D., LEEDHAM-GREEN, C. R. AND O'BRIEN, E. A. A practical model for computation with matrix groups. *J. Symbolic Comput. 68* (2015), 27–60.

[2] BENSON, D. J. The simple group J_4. Ph.D. Thesis, University of Cambridge, 1981.

[3] BLACKBURN, N. AND HUPPERT, B. *Finite groups II.* Springer Verlag, Berlin, 1981.

[4] BOSMA, W., CANNON, J. AND PLAYOUST, C. The Magma algebra system. I. The user language. *J. Symbolic Comput. 24* (1997), 235–265.

[5] BREUER, T. CTblLib – *a* GAP *package, Version 1.2.2*, 2013. `http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib/`.

[6] BURNESS, T. C., GURALNICK, R. M. AND SAXL, J. On base sizes for symmetric groups. *Bull. London Math. Soc. 43* (2011), 386–391.

[7] BURNESS, T. C., GURALNICK, R. M. AND SAXL, J. Base sizes for S-actions of finite classical groups. *Israel J. Math. 199* (2014), 711–756.

[8] BURNESS, T. C., O'BRIEN, E. A. AND WILSON, R. A. Base sizes for sporadic simple groups. *Israel J. Math. 177* (2010), 307–333.

[9] CANNON, J. J., AND HOLT, D. F. Computing projective indecomposable modules and higher cohomology groups. *Exp. Math. 22* (2013), 51–59.

[10] CONWAY, J. H., CURTIS, R. T., NORTON, S. P., PARKER, R. A. AND WILSON, R. A. *Atlas of finite groups.* Clarendon Press, Oxford, 1985.

[11] FAWCETT, J. B. The base size of a primitive diagonal group. *J. Algebra 375* (2013), 302–321.

[12] Fawcett, J. B. Bases of primitive permutation groups. Ph.D. Thesis, University of Cambridge, 2013.
[13] Fawcett, J. B., O'Brien, E. A. and Saxl, J. Regular orbits of symmetric and alternating groups. *J. Algebra 458* (2016), 21–52.
[14] The GAP Group. GAP — *Groups, Algorithms, and Programming, Version 4.9.2*, 2018. http://www.gap-system.org.
[15] Glasby, S. P., Leedham-Green, C. R. and O'Brien, E. A. Writing projective representations over subfields. *J. Algebra 295* (2006), 51–61.
[16] Goodwin, D. P. M. Regular orbits of linear groups with an application to the $k(GV)$-problem, 1. *J. Algebra 227* (2000), 395–432.
[17] Gorenstein, D. *Finite simple groups: an introduction to their classification.* Plenum Press, New York, 1982.
[18] Guralnick, R. M. and Saxl, J. Generation of finite almost simple groups by conjugates. *J. Algebra 268* (2003), 519–571.
[19] Hall, J. I., Liebeck, M. W. and Seitz, G. M. Generators for finite simple groups, with applications to linear groups. *Quart. J. Math. 43* (1992), 441–458.
[20] Hiss, G., Jansen, C., Lux, K. and Parker, R. A. Computational modular character theory. http://www.math.rwth-aachen.de/~MOC/CoMoChaT.
[21] Hiss, G. and Malle, G. Low-dimensional representations of quasi-simple groups. *LMS J. Comput. Math. 4* (2001), 22–63.
[22] Janko, Z. A new finite simple group of order $86 \cdot 775 \cdot 571 \cdot 046 \cdot 077 \cdot 562 \cdot 880$ which possesses M_{24} and the full covering group of M_{22} as subgroups. *J. Algebra 42* (1976), 564–596.
[23] Jansen, C. The minimal degrees of faithful representations of the sporadic simple groups and their covering groups. *LMS J. Comput. Math. 8* (2005), 122–144.
[24] Jansen, C., Lux, K., Parker, R. A. and Wilson, R. A. *An atlas of Brauer characters.* Clarendon Press, Oxford, 1995.
[25] Kleidman, P. and Liebeck, M. W. *The subgroup structure of the finite classical groups.* Cambridge University Press, Cambridge, 1990.
[26] Köhler, C. and Pahlings, H. Regular orbits and the $k(GV)$-problem. In *Groups and Computation III: Proceedings of the International Conference at the Ohio State University, June 15-19, 1999* (2001), pp. 209–228.
[27] Lux, K., Müller, J. and Ringe, M. Peakword condensation and submodule lattices: an application of the Meat-Axe. *J. Symb. Comput. 17* (1994), 529–544.
[28] Müller, J., Neunhöffer, M. and Wilson, R. A. Enumerating big orbits and an application: B acting on the cosets of Fi_{23}, *J. Algebra 314* (2007), 75–96.
[29] Müller, J., Neunhöffer, M. and Noeske, F. Orb — *Methods to enumerate Orbits, Version 4.8.0*, 2017. https://gap-packages.github.io/orb.
[30] Wilson, R. A. *The finite simple groups.* Springer Verlag, London, 2009.
[31] Wilson, R. A., Parker, R. A., Nickerson, S., Bray, J. N. and Breuer, T. AtlasRep — *a* GAP *Interface to the Atlas of Group Representations, Version 1.5.1*, 2016. http://www.math.rwth-aachen.de/~Thomas.Breuer/atlasrep.
[32] Wilson, R. A., et al. Atlas *of finite group representations.* http://brauer.maths.qmul.ac.uk/Atlas/v3.
[33] Wilson, R. A., et al. *The* Modular Atlas *homepage.* http://math.rwth-aachen.de/~MOC.

(Fawcett) Department of Mathematics, Imperial College London, South Kensington Campus, London, SW7 2AZ, United Kingdom
E-mail address: j.fawcett@imperial.ac.uk

(Müller) Fakultät für Mathematik und Naturwissenschaften, Bergische Universität, Wuppertal, Germany
E-mail address: juergen.mueller@math.uni-wuppertal.de

(O'Brien) Department of Mathematics, University of Auckland, Auckland, New Zealand
E-mail address: e.obrien@auckland.ac.nz

(Wilson) School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London, E1 4NS, United Kingdom
E-mail address: r.a.wilson@qmul.ac.uk