Pacific Journal of Mathematics

CHERLIN'S CONJECTURE FOR SPORADIC SIMPLE GROUPS

FRANCESCA DALLA VOLTA, NICK GILL AND PABLO SPIGA

Volume 297 No. 1 November 2018

PACIFIC JOURNAL OF MATHEMATICS
Vol. 297, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.297.47

CHERLIN'S CONJECTURE FOR SPORADIC SIMPLE GROUPS

FRANCESCA DALLA VOLTA, NICK GILL AND PABLO SPIGA

We prove Cherlin's conjecture, concerning binary primitive permutation groups, for those groups with socle isomorphic to a sporadic simple group.

1. Introduction

In this paper we consider the following conjecture which was given first in [Cherlin 2000]:

Conjecture 1.1. *A finite primitive binary permutation group must be one of*:

(1) *A symmetric group Sym*(n) *acting naturally on n elements.*

(2) *A cyclic group of prime order acting regularly on itself.*

(3) *An affine orthogonal group* $V \cdot O(V)$ *with* V *a vector space over a finite field equipped with an anisotropic quadratic form acting on itself by translation, with complement the full orthogonal group* $O(V)$.

Thanks to work of Cherlin himself [2016], and of Wiscons [2016], Conjecture 1.1 has been reduced to a statement about almost simple groups. In particular, to prove Conjecture 1.1 it would be sufficient to prove the following statement.

Conjecture 1.2. *If* G *is a binary almost simple primitive permutation group on the set* Ω, *then* $G = \mathrm{Sym}(\Omega)$.

In this paper, we prove this conjecture for almost simple groups with sporadic socle. Formally, our main result is the following:

Theorem 1.3. *Let* G *be an almost simple primitive permutation group with socle isomorphic to a sporadic simple group. Then* G *is not binary.*

Note that we include the group ${}^2F_4(2)'$ in the list of sporadic groups — this group is sometimes considered "the 27-th sporadic group" — so Theorem 1.3 applies to this group too.

The terminology of Theorem 1.3 and the preceding conjectures is all fairly standard in the world of group theory, with the possible exception of the word

MSC2010: 03C13, 20B15, 20D08.

Keywords: primitive permutation group, relational complexity, binary action, sporadic group, almost simple group.

"binary". Roughly speaking an action is binary if the induced action on ℓ-tuples can be deduced from the induced action on pairs (for any integer $\ell > 2$); a formal definition of a "binary permutation group" is given in Section 2.

1A. ***Context and methods.*** We will not spend much time here trying to motivate the study of binary permutation groups. As will be clear on reading the definition of binary in Section 2, this notion is a particular instance of the more general concept of "arity" or "relational complexity". These notions, which we define below in group theoretic terms, can also be formulated from a model theoretic point of view where they are best understood as properties of "relational structures". These connections, which run very deep, are explored at length in [Cherlin 2000], to which we refer the interested reader.

Theorem 1.3 settles Conjecture 1.2 for one of the families given by the classification of finite simple groups. It is the third recent result in this direction: Conjecture 1.2 has also been settled for groups with alternating socle [Gill and Spiga 2016], and for groups with socle a rank 1 group of Lie type [Gill et al. 2017]. Work is ongoing for the groups that remain (groups with socle a group of Lie type of rank at least 2) [Gill et al. $\geq$ 2018].

Our proof of Theorem 1.3 builds on ideas developed in [Gill and Spiga 2016] and [Gill et al. 2017], in particular the notion of a "strongly nonbinary action". In addition to this known approach, we also make use of a number of new lemmas — we mention, in particular, Lemma 2.7, which connects the "binariness" of an action to a bound on the number of orbits in the induced action on ℓ-tuples. These lemmas are gathered together in Section 2.

In addition to these new lemmas, though, this paper is very focused on adapting known facts about binary actions to create computational tests that can be applied using a computer algebra package like GAP or Magma. This process of developing tests is explained in great detail in Section 3.

In the final two sections we describe the outcome of these computations. In Section 4 we are able to give a proof of Theorem 1.3 for all of the sporadic groups barring the Monster. In Section 5 we give a proof of Theorem 1.3 for the Monster. The sheer size of the Monster means that some of the computational procedures that we exploit for the other groups are no longer available to us, and so our methods need to be refined to deal with this special case.

2. Definitions and lemmas

Throughout this section G is a finite group acting (not necessarily faithfully) on a set Ω of cardinality t. Given a subset Λ of Ω, we write

$$G_\Lambda := \{g \in G \mid \lambda^g \in \Lambda, \text{ for all } \lambda \in \Lambda\}$$

for the set-wise stabilizer of Λ, $G_{(\Lambda)} := \{g \in G \mid \lambda^g = \lambda, \text{ for all } \lambda \in \Lambda\}$ for the

pointwise stabilizer of Λ, and G^Λ for the permutation group induced on Λ by the action of G_Λ. In particular, $G^\Lambda \cong G_\Lambda / G_{(\Lambda)}$.

Given a positive integer r, the group G is called *r-subtuple complete* with respect to the pair of n-tuples $I, J \in \Omega^n$, if it contains elements that map every subtuple of length r in I to the corresponding subtuple in J, i.e.,

$$\text{for every } \{k_1, k_2, \ldots, k_r\} \subseteq \{1, \ldots, n\},$$
$$\text{there exists } h \in G \text{ with } I_{k_i}^h = J_{k_i}, \text{ for every } i \in \{1, \ldots, r\}.$$

Here I_k denotes the k-th element of tuple I and I_k^g denotes the image of I_k under the action of g. Note that n-subtuple completeness simply requires the existence of an element of G mapping I to J.

Definition 2.1. The action of G is said to be of *arity r* if, for all $n \in \mathbb{N}$ with $n \geq r$ and for all n-tuples $I, J \in \Omega^n$, r-subtuple completeness (with respect to I and J) implies n-subtuple completeness (with respect to I and J). Note that in the literature the concept of "arity" is also known by the name "relational complexity".

When the action of G has arity 2, we say that the action of G is *binary*. If G is given to us as a permutation group, then we say that G is a *binary permutation group*.

A pair (I, J) of n-tuples of Ω is called a *nonbinary witness for the action of G on Ω* if G is 2-subtuple complete with respect to I and J, but not n-subtuple complete, that is, I and J are not G-conjugate. To show that the action of G on Ω is nonbinary it is sufficient to find a nonbinary witness (I, J).

We now recall some useful definitions introduced in [Gill et al. 2017]. We say that the action of G on Ω is *strongly nonbinary* if there exists a nonbinary witness (I, J) such that

- I and J are t-tuples where $|\Omega| = t$;
- the entries of I and J comprise all the elements of Ω.

We give a standard example, taken from [Gill et al. 2017], showing how strongly nonbinary actions can arise.

Example 2.2. Let G be a subgroup of $\mathrm{Sym}(\Omega)$, let $g_1, g_2, \ldots, g_r$ be elements of G, and let $\tau, \eta_1, \ldots, \eta_r$ be elements of $\mathrm{Sym}(\Omega)$ with

$$g_1 = \tau\eta_1, \;\; g_2 = \tau\eta_2, \;\; \ldots, \;\; g_r = \tau\eta_r.$$

Suppose that, for every $i \in \{1, \ldots, r\}$, the support of τ is disjoint from the support of η_i; moreover, suppose that, for each $\omega \in \Omega$, there exists $i \in \{1, \ldots, r\}$ (which may depend upon ω) with $\omega^{\eta_i} = \omega$. Suppose, in addition, $\tau \notin G$. Now, writing $\Omega = \{\omega_1, \ldots, \omega_t\}$, observe that

$$((\omega_1, \omega_2, \ldots, \omega_t), (\omega_1^\tau, \omega_2^\tau, \ldots, \omega_t^\tau))$$

is a nonbinary witness. Thus the action of G on Ω is strongly nonbinary.

The following lemma, taken from [Gill et al. 2017], shows a crucial property of the notion of strongly nonbinary action: it allows one to argue "inductively" on set-stabilizers (see also Lemma 2.8).

Lemma 2.3. *Let Ω be a G-set and let $\Lambda \subseteq \Omega$. If G^Λ is strongly nonbinary, then G is not binary in its action on Ω.*

Proof. Write $\Lambda := \{\lambda_1, \dots, \lambda_\ell\}$ and assume that G^Λ is strongly nonbinary. Then there exists $\sigma \in \mathrm{Sym}(\ell)$ with $I := (\lambda_1, \lambda_2, \dots, \lambda_\ell)$ and $J := (\lambda_{1^\sigma}, \lambda_{2^\sigma}, \dots, \lambda_{\ell^\sigma})$ a nonbinary witness for the action of G_Λ on Λ. Now, observe that (I, J) is also a nonbinary witness for the action of G on Ω because any (putative) element g of G mapping I to J fixes Λ set-wise and hence $g \in G_\Lambda$. □

Next we need an observation, made first in [Gill et al. 2017], that the existence of a strongly nonbinary witness is related to the classic concept of 2-*closure* introduced by Wielandt [1964]: given a permutation group G on Ω, the 2-closure of G is the set

$$G^{(2)} := \{\sigma \in \mathrm{Sym}(\Omega) \mid \text{ for all } (\omega_1, \omega_2) \in \Omega \times \Omega, \text{ there exists } g_{\omega_1\omega_2} \in G \text{ with } \omega_1^\sigma = \omega_1^{g_{\omega_1\omega_2}}, \omega_2^\sigma = \omega_2^{g_{\omega_1\omega_2}}\},$$

that is, $G^{(2)}$ is the largest subgroup of $\mathrm{Sym}(\Omega)$ having the same orbitals as G. The group G is said to be 2-*closed* if and only if $G = G^{(2)}$.

Lemma 2.4. *Let G be a permutation group on Ω. Then G is strongly nonbinary if and only if G is not 2-closed.*

Proof. Write $\Omega := \{\omega_1, \dots, \omega_t\}$. If G is not 2-closed, then there exists $\sigma \in G^{(2)} \setminus G$. Set $I := (\omega_1, \dots, \omega_t)$ and $J := I^\sigma = (\omega_1^\sigma, \dots, \omega_t^\sigma)$; observe that I and J are 2-subtuple complete (because $\sigma \in G^{(2)}$) and are not G-conjugate (because $\sigma \notin G$). Thus (I, J) is a strongly nonbinary witness. The converse is similar. □

Our next two lemmas make use of Lemma 2.3 and Example 2.2 to yield easy criteria for showing that a permutation group is not binary.

Lemma 2.5. *Let G be a transitive permutation group on Ω, let $\alpha \in \Omega$ and let p be a prime with p dividing both $|\Omega|$ and $|G_\alpha|$ and with p^2 not dividing $|G_\alpha|$. Suppose that G contains an elementary abelian p-subgroup $V = \langle g, h\rangle$ with $g \in G_\alpha$, with h and gh conjugate to g via G. Then G is not binary.*

Proof. Let $g \in G_\alpha$ and let $h \in g^G$ with $\langle g, h\rangle$ an elementary abelian p-subgroup of G of order p^2 with gh also conjugate to g via G. In particular, $h = g^x$, for some $x \in G$. Write $\alpha_0 := \alpha$ and $\alpha_p := \alpha^x$.

Since $g \in G_{\alpha_0}$ and $h \in G_{\alpha_p}$ commute, $\alpha_0^{h^i}$ is fixed by g and $\alpha_p^{g^i}$ is fixed by h, for every i. Write $\alpha_i := \alpha_0^{h^i}$ and $\alpha_{p+i} := \alpha_p^{g^i}$, for every $i \in \{0, \dots, p-1\}$. Moreover, g acts as a p-cycle on $\{\alpha_p, \dots, \alpha_{2p-1}\}$ and h acts as a p-cycle on $\{\alpha_0, \dots, \alpha_{p-1}\}$.

Since gh is conjugate to g via an element of G, there exists $y \in G$ with $gh = g^y$. Write $\alpha_{2p} = \alpha^y$. Observe that gh fixes $(\alpha_{2p})^{g^{-i}} = \alpha_{2p}^{h^i}$ for every i. Write

$\alpha_{2p+i} := \alpha_{2p}^{g^i}$, for every $i \in \{0, \ldots, p-1\}$. Thus g and h act as inverse p-cycles on $\{\alpha_{2p}, \ldots, \alpha_{3p-1}\}$.

Write $\Lambda := \{\alpha_0, \ldots, \alpha_{3p-1}\}$. We have

$$g^\Lambda = (\alpha_p, \ldots, \alpha_{2p-1})(\alpha_{3p-1}, \ldots, \alpha_{2p}),$$
$$h^\Lambda = (\alpha_0, \ldots, \alpha_{p-1})(\alpha_{2p}, \ldots, \alpha_{3p-1}),$$
$$(gh)^\Lambda = (\alpha_0, \ldots, \alpha_{p-1})(\alpha_p, \ldots, \alpha_{2p-1}).$$

If G^Λ is strongly nonbinary, then G is not binary by Lemma 2.3. Assume that G^Λ is not strongly nonbinary. Then, in view of Example 2.2, there exists $f \in G$ with $f^\Lambda = (\alpha_p, \ldots, \alpha_{2p-1})$. This is a contradiction, because by hypothesis $|G_\alpha|$ is not divisible by p^2 but $\langle g, f\rangle$ has order divisible by p^2 and fixes $\alpha_0 = \alpha$. □

Lemma 2.6. *Let G be a permutation group on Ω and suppose that g and h are elements of G of order p where p is a prime such that g, h and gh^{-1} are all G-conjugate. Suppose that $V = \langle g, h\rangle$ is elementary abelian of order p^2. Suppose, finally, that G does not contain any elements of order p that fix more points of Ω than g. If $|\mathrm{Fix}(V)| < |\mathrm{Fix}(g)|$, then G is not binary.*

We remark that there are well-known formulae that we can use to calculate $\mathrm{Fix}(V)$ and $|\mathrm{Fix}(g)|$ when G is transitive (see for instance [Liebeck and Saxl 1991, Lemma 2.5]). Suppose that M is the stabilizer of a point in Ω; then we have

$$|\mathrm{Fix}_\Omega(g)| = \frac{|\Omega| \cdot |M \cap g^G|}{|g^G|}, \quad |\mathrm{Fix}_\Omega(V)| = \frac{|\Omega| \cdot |\{V^g \mid g \in G, V^g \le M\}|}{|V^G|}. \tag{2-1}$$

Proof. We let

$$\Lambda := \mathrm{Fix}(g) \cup \mathrm{Fix}(h) \cup \mathrm{Fix}(gh^{-1}).$$

Observe, first, that Λ, $\mathrm{Fix}(g)$, $\mathrm{Fix}(h)$ and $\mathrm{Fix}(gh^{-1})$ are g-invariant and h-invariant. Observe, second, that

$$\mathrm{Fix}(g) \cap \mathrm{Fix}(h) = \mathrm{Fix}(g) \cap \mathrm{Fix}(gh^{-1}) = \mathrm{Fix}(h) \cap \mathrm{Fix}(gh^{-1}) = \mathrm{Fix}(V).$$

Write τ_1 for the permutation induced by g on $\mathrm{Fix}(gh^{-1})$, τ_2 for the permutation induced by g on $\mathrm{Fix}(h)$, and τ_3 for the permutation induced by h on $\mathrm{Fix}(g)$ (observe that τ_i's are non trivial as gh^{-1}, h and g are conjugate). Since $|\mathrm{Fix}(V)| < |\mathrm{Fix}(g)|$, we conclude that τ_1, τ_2 and τ_3 are disjoint nontrivial permutations. What is more, g induces the permutation $\tau_1\tau_2$ on Λ, while h induces the permutation $\tau_1\tau_3$ on Λ.

In view of Example 2.2, G^Λ is strongly nonbinary provided there is no element $f \in G_\Lambda$ that induces the permutation τ_1. Arguing by contradiction, if such an element f exists, then f has order divisible by p and $f^{o(f)/p}$ is a p-element fixing more points than g, which is a contradiction. Thus G^Λ is strongly nonbinary and G is not binary by Lemma 2.3. □

For the rest of this section we assume that G is transitive. Given $\ell \in \mathbb{N} \setminus \{0\}$, we denote by $\Omega^{(\ell)}$ the subset of the Cartesian product Ω^ℓ consisting of the ℓ-tuples $(\omega_1, \dots, \omega_\ell)$ with $\omega_i \neq \omega_j$, for every two distinct elements $i, j \in \{1, \dots, \ell\}$. We denote by $r_\ell(G)$ the number of orbits of G on $\Omega^{(\ell)}$.

Let $\pi : G \to \mathbb{N}$ be the permutation character of G, that is, $\pi(g) = \mathrm{fix}_\Omega(g)$ where $\mathrm{fix}_\Omega(g)$ is the cardinality of the fixed point set $\mathrm{Fix}_\Omega(g) := \{\omega \in \Omega \mid \omega^g = \omega\}$ of g. From the orbit counting lemma, we have

$$\begin{aligned} r_\ell(G) &= \frac{1}{|G|} \sum_{g \in G} \mathrm{fix}_\Omega(g)(\mathrm{fix}_\Omega(g) - 1) \cdots (\mathrm{fix}_\Omega - (\ell - 1)) \\ &= \langle \pi(\pi - 1) \cdots (\pi - (\ell - 1)), 1 \rangle_G, \end{aligned}$$

where 1 is the principal character of G and $\langle \cdot, \cdot \rangle_G$ is the natural Hermitian product on the space of $\mathbb{C}$-class functions of G.

Lemma 2.7. *If G is transitive and binary, then $r_\ell(G) \leq r_2(G)^{\ell(\ell-1)/2}$ for each $\ell \in \mathbb{N}$.*

Note that this lemma is, in effect, an immediate consequence of the fact that, for a binary action, the orbits on pairs "determine" orbits on ℓ-tuples. Thus, to uniquely determine the orbit of a particular ℓ-tuple, it is enough to specify the orbits of all $\binom{\ell}{2}$ pairs making up the ℓ-tuple.

Proof. We write $r_2 := r_2(G)$ and $r_\ell := r_\ell(G)$ and we assume that $r_\ell > r_2^{(\ell-1)\ell/2}$ for some $\ell \in \mathbb{N}$. Clearly, $\ell > 2$.

Let

$$(\omega_{1,1}, \dots, \omega_{1,\ell}), \dots, (\omega_{r_\ell,1}, \dots, \omega_{r_\ell,\ell})$$

be a family of representatives for the G-orbits on $\Omega^{(\ell)}$. From the pigeon-hole principle, at least r_ℓ/r_2 of these elements have the first two coordinates in the same G-orbit. Formally, there exists $\kappa \in \mathbb{N}$ with $\kappa \geq r_\ell/r_2$ and a subset $\{i_1, \dots, i_\kappa\}$ of $\{1, \dots, r_\ell\}$ of cardinality κ such that the κ pairs

$$(\omega_{i_1,1}, \omega_{i_1,2}), \dots, (\omega_{i_\kappa,1}, \omega_{i_\kappa,2})$$

are in the same G-orbit. By considering all possible pairs of coordinates, this argument can be easily generalized. Indeed, from the pigeon-hole principle, there exists κ with $\kappa \geq r_\ell/r_2^{(\ell-1)\ell/2} > 1$ and a subset $\{i_1, \dots, i_\kappa\}$ of $\{1, \dots, r_\ell\}$ of cardinality κ such that, for each $1 \leq u < v \leq \ell$, the κ pairs

$$(\omega_{i_1,u}, \omega_{i_1,v}), \dots, (\omega_{i_\kappa,u}, \omega_{i_\kappa,v})$$

are in the same G-orbit. In other words, the ℓ-tuples

$$(\omega_{i_1,1}, \dots, \omega_{i_1,\ell}), \dots, (\omega_{i_\kappa,1}, \dots, \omega_{i_\kappa,\ell})$$

are 2-subtuple complete. Since G is binary, these ℓ-tuples must be in the same G-orbit, contradicting $\kappa > 1$. □

Observe that when $r_2(G) = 1$, that is, G is 2-transitive, Lemma 2.7 yields $r_\ell(G) = 1$ for every $\ell \in \{2, \dots |\Omega|\}$. Therefore $G = \mathrm{Sym}(\Omega)$ is the only 2-transitive binary group.

Lemma 2.8. *Let G be transitive, let α be a point of Ω and let $\Lambda \subseteq \Omega$ be a G_α-orbit. If G is binary, then G_α^Λ is binary. In particular, if $g \in G$ and the action of G_α on the right cosets of $G_\alpha \cap G_\alpha^g$ in G_α is not binary, then G is not binary.*

Proof. Assume that G is binary. Let $\ell \in \mathbb{N}$ and let $I := (\lambda_1, \lambda_2, \dots, \lambda_\ell)$ and $J := (\lambda'_1, \lambda'_2, \dots, \lambda'_\ell)$ be two tuples in Λ^ℓ that are 2-subtuple complete for the action of G_α on Λ. Clearly, $I_0 := (\alpha, \lambda_1, \lambda_2, \dots, \lambda_\ell)$ and $J_0 := (\alpha, \lambda'_1, \lambda'_2, \dots, \lambda'_\ell)$ are 2-subtuple complete for the action of G on Ω. As G is binary, I_0 and J_0 are in the same G-orbit; hence I and J are in the same G_α-orbit. From this we deduce that G_α^Λ is binary.

Suppose now that $g \in G$ and that the action of G_α on the right cosets of $G_\alpha \cap G_\alpha^g$ in G_α is not binary. Set $\beta := \alpha^g$ and $\Lambda := \beta^{G_\alpha}$. Now Λ is a G_α-orbit contained in $\Omega \setminus \{\alpha\}$ and the action of G_α on Λ is permutation isomorphic to the action of G_α on the right cosets of $G_\alpha \cap G_\beta = G_\alpha \cap G_\alpha^g$ in G_α. Therefore, G_α^Λ is not binary and hence G is not binary. □

3. On computation

In this section we explain how to make use of the lemmas given in the previous section in a computational setting. The computational problem we are faced with is as follows: given a transitive action of a group G on a set Ω, we wish to show that the action is nonbinary; in some cases we will require more, namely that the action is strongly nonbinary. If the set Ω is small enough, then we can often exhibit G as a permutation group in the computer algebra package Magma and compute explicitly; when Ω gets too large, then this may be infeasible and we may know only the isomorphism type of G and the isomorphism type of a point-stabilizer.

3A. ***Test 1*: *using Lemma 2.7.*** In some cases, Lemma 2.7 is very efficient for dealing with some primitive actions of almost simple groups G with socle a sporadic simple group. In particular, whenever the permutation character of G is available in GAP or in Magma, we can simply check directly the inequality in Lemma 2.7. For instance, using this method it is easy to verify that each faithful primitive action of M_{11} is nonbinary.

For practical purposes, it is worth mentioning that apart from

- the Monster,
- the action of the Baby Monster on the cosets of a maximal subgroup of type $(2^2 \times F_4(2)) : 2$,

each permutation character of each primitive permutation representation of an almost simple group with socle a sporadic simple group is available in GAP via the package

"The GAP Character Table Library". Therefore, for the proof of Theorem 1.3, we can quickly and easily use Lemma 2.7 except for the Monster. To give a rough idea of the time to perform this test, in the Baby Monster (except for the action on the cosets on a maximal subgroup of type $(2^2 \times F_4(2)) : 2$), it takes less than two minutes to perform this checking. (The permutation character of the Baby Monster G on the cosets of a maximal subgroup M of type $(2^2 \times F_4(2)) : 2$ is missing from the GAP library because the conjugacy fusion of some of the elements of M in G remains a mystery: this information is vital for computing the permutation character.)

For reasons that will be more clear later, for the proof of Theorem 1.3, we need to prove the nonbinariness of permutation groups $G \leq \mathrm{Sym}(\Omega)$ that are not necessarily almost simple, let alone having socle a sporadic simple group. When $|\Omega|$ is relatively small (for practical purposes, here relatively small means at most 10^9), we can afford to compute the permutation character and check the inequality in Lemma 2.7.

3B. ***Test 2*: *using Lemma 2.4.*** By connecting the notion of strong-nonbinariness to 2-closure, Lemma 2.4 yields an immediate computational dividend: there are built-in routines in GAP and Magma to compute the 2-closure of a permutation group.

Thus if Ω is small enough, say $|\Omega| \leq 10^6$, then we can easily check whether or not the group G is 2-closed. Thus we can ascertain whether or not G is strongly nonbinary.

3C. ***Test 3*: *a direct analysis.*** The next test we discuss is feasible once again provided $|\Omega| \leq 10^6$. It simply tests whether or not 2-subtuple-completeness implies 3-subtuple completeness, and the procedure is as follows:

We fix $\alpha \in \Omega$, we compute the orbits of G_α on $\Omega \setminus \{\alpha\}$ and we select a set of representatives $\mathcal{O}$ for these orbits. Then, for each $\beta \in \mathcal{O}$, we compute the orbits of $G_\alpha \cap G_\beta$ on $\Omega \setminus \{\alpha, \beta\}$ and we select a set of representatives $\mathcal{O}_\beta$. Then, for each $\gamma \in \mathcal{O}_\beta$, we compute $\gamma^{G_\alpha} \cap \gamma^{G_\beta}$. Finally, for each $\gamma' \in \gamma^{G_\alpha} \cap \gamma^{G_\beta}$, we test whether the two triples (α, β, γ) and (α, β, γ') are G-conjugate. If the answer is "no", then G is not binary because by construction (α, β, γ) and (α, β, γ') are 2-subtuple complete. In particular, in this circumstance, we can break all the "for loops" and deduce that G is not binary.

If the answer is "yes", for every β, γ, γ', then we cannot deduce that G is binary, but we can keep track of these cases for a deeper analysis. We observe that, if the answer is "yes", for every β, γ, γ', then 2-subtuple completeness implies 3-subtuple completeness.

3D. ***Test 4*: *using Lemma 2.8.*** The next test is particularly useful in cases where Ω is very large, since its computational complexity is independent of $|\Omega|$. Let us

suppose that G and its subgroup M are stored in a library as abstract groups (or as matrix groups or as permutation groups). When $|G : M|$ is too large, it is impractical (and sometimes impossible) to construct G as a permutation group on the coset space $\Omega := G/M$ with point stabilizer M. However, using Lemma 2.8, we can still prove that G acting on Ω is nonbinary: all we need is $g \in G$ such that the action of M on $M \cap M^g$ is nonbinary. Now, for carefully chosen g, $|M : M \cap M^g|$ might be much smaller than $|G : M|$ and we can use one of the previous tests to ascertain whether or not M in its action on $M/(M \cap M^g)$ is binary.

3E. ***Test 5*: *a new lemma.*** Our final test requires an extra lemma which we include here, rather than in the earlier section, as its computational aspect is somehow inherent in its very statement.

Lemma 3.1. *Let G be a primitive group on a set Ω, let α be a point of Ω, let M be the stabilizer of α in G and let d be an integer with $d \geq 2$. Suppose $M \neq 1$ and, for each transitive action of M on a set Λ such that*

(1) $|\Lambda| > 1$,

(2) *every composition factor of M is isomorphic to some section of M^Λ,*

(3) *either $M_{(\Lambda)} = 1$ or, given $\lambda \in \Lambda$, the stabilizer M_λ has a normal subgroup N with $N \neq M_{(\Lambda)}$ and $N \cong M_{(\Lambda)}$, and*

(4) *M is binary in its action on Λ,*

we have that d divides $|\Lambda|$. Then either d divides $|\Omega| - 1$ or G is not binary.

Proof. Suppose that G is binary. Since $\{\beta \in \Omega \mid \beta^m = \beta, \text{ for all } m \in M\}$ is a block of imprimitivity for G and since G is primitive, we obtain that either M fixes each point of Ω or α is the only point fixed by M. The former possibility is excluded because $M \neq 1$ by hypothesis. Therefore α is the only point fixed by M. Let $\Lambda \subseteq \Omega \setminus \{\alpha\}$ be an M-orbit. Thus $|\Lambda| > 1$ and (1) holds. Since G is a primitive group on Ω, from [Dixon and Mortimer 1996, Theorem 3.2C], we obtain that every composition factor of M is isomorphic to some section of M^Λ and hence (2) holds. From Lemma 2.8, the action of M on Λ is binary and hence (4) holds. Let now $\lambda \in \Lambda$ and consider the orbital graph $\Gamma := (\alpha, \lambda)^G$. Observe that Γ is connected because G is primitive. Let $g \in G$ with $\alpha^g = \lambda$. Clearly, Λ is the set of out-neighbors of α in Γ and $\Lambda' := \Lambda^g$ is the set of out-neighbors of $\alpha^g = \lambda$ in Γ. Set $N := (G_\lambda)_{(\Lambda')}$. Clearly, $(G_\alpha)_{(\Lambda)} = M_{(\Lambda)}$ and $(G_{\alpha^g})_{(\Lambda^g)} = (G_\lambda)_{(\Lambda')} = N$ are isomorphic because they are G-conjugate via the element g. Moreover, $M_{(\Lambda)} = (G_\alpha)_{(\lambda^{G_\alpha})}$ is normalized by G_α and, similarly, N is normalized by G_λ; therefore they are both normalized by

$$G_\alpha \cap G_\lambda = M \cap G_\lambda = M_\lambda.$$

If $M_{(\Lambda)}$ and N are equal, an easy connectedness argument yields that $M_{(\Lambda)} = 1$. Therefore (3) also holds.

Since the four hypotheses in the statement of this lemma hold for the action of $M = G_\alpha$ on its G_α-orbit Λ, we get d divides $|\Lambda|$. Since this argument does not depend on the G_α-orbit $\Lambda \subseteq \Omega \setminus \{\alpha\}$, we obtain that $\Omega \setminus \{\alpha\}$ has cardinality divisible by d. Thus $|\Omega| - 1$ is divisible by d. □

When it comes to implementing Lemma 3.1 on a computer, it is important to observe that we do *not* need to construct the embedding of $M = G_\alpha$ in G; indeed we do not need the group G stored in our computer at all. Instead we need only the index $|G : M| = |\Omega|$ and the abstract group M (given as a group of matrices, or as a permutation group, or as a finitely presented group).

Given $|\Omega|$ and M, we may choose a prime p (typically $p = 2$) with p not dividing $|\Omega| - 1$ and we construct all the transitive permutation representations of degree greater than 1 and relatively prime to p of M satisfying (1), (2) and (3). If none of these permutation representations is binary (and we can use any of Tests 1 to 4 to test this), we infer that every transitive permutation representation of M of degree greater than 1 satisfying (1), (2), (3) and (4) has degree divisible by p. Now, from Lemma 3.1, we get that G in its action on the set M of right cosets of M in G is not binary because p does not divide $|\Omega| - 1$.

We give an explicit example to show how easily Lemma 3.1 can be applied. The Monster G has a maximal subgroup M isomorphic to $\mathrm{PGL}_2(19)$. The index of M in G is

$$11813120245533813974948244224586414576107520000000 0 \sim 10^{50}$$

and we can easily observe that this number is even. After implementing Lemma 3.1 on a computer, it takes the blink of an eye to prove that each permutation representation of M of degree at least 1 and odd is nonbinary. Thus G acting on the cosets of M is nonbinary. Observe that besides $|G : M|$ and the isomorphism class of M, no information about G is needed.

4. The non-Monster groups

The centerpiece of this section is Table 1; it summarizes the results of applying the tests described in the previous section to all almost simple groups with a sporadic socle, barring the Monster.

Table 1 consists of two columns: the first column lists all of the almost simple groups G with socle a sporadic simple group (recall that we include Tits group ${}^2F_4(2)'$ in the list of sporadic groups). In the second column, we list all pairs $(M, \circ)$, where M is a maximal subgroup of G with the property that the action of G on the set G/M of right cosets of M in G satisfies Lemma 2.7 (in other words, the action is not excluded by Test 1, and hence is a potentially binary action). We use the ATLAS [Conway et al. 1985] notation for the group M.

Now the symbol $\circ$ is either ∞ or a prime p or "?". We write $\circ = \infty$ if we have proved the nonbinariness of G in its action on G/M using Tests 2 or 3; we write $\circ = p$ if we have proved the nonbinariness of G in its action on G/M using Test 5 applied to the prime p; and we write $\circ =?$ if both methods have failed. The symbol "$-$" in the second column means that each primitive permutation representation of G is not binary via Lemma 2.7 (Test 1).

We have made use of the fact that full information on the maximal subgroups for each group in the first column of Table 1 is available: these are all stored in GAP or in Magma. To be more precise, in each case, either the maximal subgroup M is stored providing a generating set (written as words in the standard generators for G), or when such information is not available (for instance, for some of the maximal subgroups of Fi_{23}), the group M is explicitly described (for instance, as a p-local subgroup) and hence also in this case it is possible to construct M with a computer.

We are now able to prove Theorem 1.3 for all groups bar the Monster.

Proposition 4.1. *Let G be an almost simple primitive group with socle a sporadic simple group. If G is binary, then G is the Monster group.*

Proof. In view of Table 1, it suffices to consider the case that G is either Co_3, or Ru, or B: these are the only groups having a "?" symbol in one of their rows. We first assume that G is either Co_3 or Ru; here, in view of Table 1 the group G is acting on the cosets of $M = A_4 \times S_5$ when $G = \mathrm{Co}_3$, or $M = 5 : 4 \times A_5$ when $G = \mathrm{Ru}$. Given a Sylow 2-subgroup P of M, in both cases it is easy to verify with Magma that there exists $g \in \mathbf{N}_G(P)$ with $M \cap M^g = P$. When $G = \mathrm{Co}_3$, P is of type $2 \times 2 \times D_4$ and, when $G = \mathrm{Ru}$, P is of type $4 \times 2 \times 2$. Another computation shows that the actions of $A_4 \times S_5$ on the cosets of $2 \times 2 \times D_4$, and of $5 : 4 \times A_4$ on the cosets of $4 \times 2 \times 2$ are not binary. Therefore, G in its action on the cosets of M is not binary by Lemma 2.8.

Finally assume that G is the Baby Monster B. In view of Table 1, G is acting on the cosets of M where M is of one of the following types:

$$(2^2 \times F_4(2)) : 2, \quad 3^{1+8}.2^{1+6}.U_4(2).2, \quad (3^2 : D_8 \times U_4(3).2^2).2, \quad 3^2.3^3.3^6.(S_4 \times 2S_4).$$

Let Ω be the set of right cosets of M in G and let $\alpha \in \Omega$ with $G_\alpha = M$ (that is, α is the coset M). We go through the four remaining cases one at a time.

Case 1: $M \cong (3^2 : D_8 \times U_4(3).2^2).2$**.** Observe that a Sylow 7-subgroup of G has order $7^2 = 49$, that G has a unique conjugacy class of elements of order 7, and that $|M|$ and $|G : M|$ are both divisible by 7. Then Lemma 2.5 implies that G is not binary.

Case 2: $M \cong 3^{1+8}.2^{1+6}.U_4(2).2$**.** The group G has two conjugacy classes of elements of order 5, with the ATLAS notation, of type 5A and of type 5B. By

group	outcome of tests
M_{11}	–
M_{12}	–
$M_{12}.2$	–
M_{22}	–
$M_{22}.2$	–
M_{23}	–
M_{24}	$(L_2(7), \infty)$
J_1	$(D_6 \times D_{10}, \infty), (7:6, \infty)$
J_2	(A_5, ∞)
$J_2.2$	(S_5, ∞)
J_3	–
$J_3.2$	$(19:18, 3)$
J_4	$(M_{22}:2, 2),\ (11_+^{1+2}:(5\times 2S_4), 2),\ (L_2(32):5, 11),\ (L_2(23):2, 2),$ $(U_3(3), 2),\ (29:28, 2),\ (43:14, 7),\ (37:12, 2)$
${}^2F_4(2)'$	–
${}^2F_4(2)$	$(M, 2)$ where M has order 156
Suz	$(A_7, 2),\ (L_2(25), 2)$
Suz.2	$(S_7, 7)$
McL	–
McL.2	–
HS	$(M_{22}, 2)$
HS.2	$(M_{22}:2, 2)$
Co_3	$(A_4 \times S_5, ?)$
Co_2	$(5_+^{1+2}:4S_4, 2)$
Co_1	$(A_9 \times S_3, 3),\ ((A_7 \times L_2(7)):2, 2),\ ((D_{10} \times (A_5 \times A_5).2).2, 2),$ $(5_+^{1+2}:\mathrm{GL}_2(5), 2),\ (5^3:(4\times A_5).2, 2),\ (5^2:4A_4, 2),\ (7^2:(3\times 2A_4), 2)$
He	$(5^2:4A_4, 2)$
He.2	–
Fi_{22}	–
$Fi_{22}.2$	–
Fi_{23}	$(L_2(23), 2)$
Fi'_{24}	$((A_5 \times A_9):2, 3),\ (A_6 \times L_2(8):3, 2),\ (7:6\times A_7, 7),\ (U_3(3).2, 2)$ $(U_3(3).2, 2),\ (L_2(13).2, 2),\ (L_2(13).2, 2),\ (29:14, 7)$
Fi_{24}	$(S_5 \times S_9, 3),\ (S_6 \times L_2(8):3, 2),\ (7:6\times S_7, 7),\ (7_+^{1+2}:(6\times S_3).2, 2),\ (29:28, 7)$
Ru	$(L_2(13):2, 2),\ (5:4\times A_5, ?),\ (A_6.2^2, 2),\ (5_+^{1+2}:[2^5], 2),\ (3.A_6.2^2, 2)$
O'N	$(A_7, 2),\ (A_7, 2)$
O'N.2	$(31:30, 5),\ (L_2(7):2, 2),\ (A_6:2_2, 2)$
Ly	$(67:22, 11),\ (37:18, 3)$
Th	$(3^5:2S_6, 2),\ (5_+^{1+2}:4S_4, 2),\ (5^2:\mathrm{GL}_2(5), 2),\ (7^2:(3\times 2S_4), 2),$ $(L_2(19).2, 2),\ (L_3(3), 2),\ (M_{10}=A_6.2_3, 2),\ (31:15, 4),\ (S_5, 5)$
HN	$(3_+^{1+4}:4A_5, 2)$
HN.2	–
B	$((2^2\times F_4(2)):2, ?),\ (3^{1+8}.2^{1+6}.U_4(2).2, ?),\ ((3^2:D_8\times U_4(3).2^2).2, ?),$ $(5:4\times \mathrm{HS}:2, 2),\ (3^2.3^3.3^6.(S_4\times 2S_4), ?),\ (S_4\times {}^2F_4(2), 2),\ (S_5\times (M_{22}:2), 2),$ $((S_6\times (L_3(4):2)).2, 2),\ (5^3:L_3(5), 2),\ (5^{1+4}.2^{1+4}.A_5.4, 2),\ ((S_6\times S_6).4, 2),$ $((5^2:4S_4)\times S_5, 2),\ (L_2(49).2, 2),\ (L_2(31), 2),\ (M_{11}, 2),\ (L_3(3), 2),$ $(L_2(17):2, 2),\ (L_2(11):2, 2),\ (47:23, 23)$

Table 1. Disposing of some of the sporadic simple groups.

computing the permutation character of G via the package the GAP character table library, we see that an element of type 5A fixes no point and that an element of type 5B fixes 25000 points. Observe that $|M|$ is divisible by 5, but not by $5^2 = 25$. Moreover, using the ATLAS [Conway et al. 1985], we see that G contains an elementary abelian 5-group V of order 5^3 generated by three elements of type 5B; moreover, the normalizer of V is a maximal subgroup of G of type $5^3 : L_3(5)$. In particular, each nonidentity 5-element of V is of type 5B, because $L_3(5)$ acts transitively on the nonzero vectors of 5^3. Since $|M|$ is not divisible by 25, we conclude that $\mathrm{Fix}(V)$ is empty. Now we apply Lemma 2.6 to L, a subgroup of M of order 25 such that $|\mathrm{Fix}(L)| < |\mathrm{Fix}(g)|$. We conclude that G is not binary.

Case 3: $M \cong 3^2.3^3.3^6.(S_4 \times 2S_4)$**.** From the ATLAS [Conway et al. 1985], we see that $M = \mathbf{N}_G(V)$, where V is an elementary abelian 3-subgroup of order 3^2 with $V \setminus \{1\}$ consisting only of elements of type 3B. For the proof of this case, we refer to [Wilson 1987] and [Wilson 1999]. According to Wilson [1987, Section 3], there exist three G-conjugacy classes of elementary abelian 3-subgroups of G of order 3^2 consisting only of elements of type 3B, denoted in [Wilson 1987] as having type (a) or (b) or (c). Moreover, from [Wilson 1987, Proposition 3.1], we see that only for the elementary abelian 3-groups of type (a) the normalizers are maximal subgroups of G and of shape $3^2.3^3.3^6.(S_4 \times 2S_4)$. Thus V is of type (a). Let V_1, V_2, V_3 be representatives for the conjugacy classes of elementary 3-subgroups of G of order 3^2 and consisting only of elements of type 3B. We may assume that $V_1 = V$. From [Wilson 1987] or [Wilson 1999], for $W \in \{V_1, V_2, V_3\}$, $\mathbf{N}_G(W)$ has shape $3^2.3^3.3^6.(S_4 \times 2S_4)$, $(3^2 \times 3^{1+4}).(2^2 \times 2A_4).2$, and $(3^2 \times 3^{1+4}).(2 \times 2S_4)$; in [Wilson 1987; 1999], these cases are referred to as type (a), type (b) and type (c), respectively.

Next, we consider a maximal subgroup K of G isomorphic to $\mathrm{PSL}_3(3)$. From [Wilson 1999] (pages 9 and 10 and the discussion therein on the interaction between K and the types (a), (b) and (c)), we infer that K contains a conjugate of V. In particular, replacing K by a suitable G-conjugate, we may assume that $V \leq K$, and more specifically,

$$M \cap K = \mathbf{N}_K(V).$$

Take $\Lambda := \alpha^K$ and observe that Λ is a K-orbit on Ω and that the stabilizer of the point α in K is $\mathbf{N}_K(V)$. Moreover, since K is maximal in G, we get $G_\Lambda = K$. We claim that $G^\Lambda = K^\Lambda$ is strongly nonbinary, from which it follows that G is not binary by Lemma 2.3. Observe that the action of K on Λ is permutation isomorphic to the action of K on the set of right cosets of $\mathbf{N}_K(V)$ in K.

Now, we consider the abstract group $K_0 = \mathrm{PSL}_3(3)$, we consider an elementary abelian 3-subgroup V_0 of order 9 of K_0, we compute $N_0 := \mathbf{N}_{K_0}(V_0)$ and we consider the action of K_0 on the set Λ_0 of right cosets of N_0 in K_0. A straightforward

computation shows that K_0 is not 2-closed in this action, and hence K_0 in its action on Λ_0 is strongly nonbinary by Lemma 2.4.

Case 4: $M \cong (2^2 \times F_4(2)) : 2$**.** Here we cannot invoke the GAP character table library to understand whether $F_4(2)$ contains elements of type 5A or 5B, because the fusion of M in G is (in some cases) still unknown. As we mentioned above, G has two conjugacy classes of elements of order 5, denoted by 5A and 5B; what is more the group $F_4(2)$ contains a unique conjugacy class of elements of order 5. Observe that the centralizers in G have elements of type 5A and 5B which have orders 44352000 and 6000000, respectively. Now, the centralizer in $F_4(2)$ of an element of order 5 has cardinality 3600. Since 3600 does not divide 6000000, we get that M contains only elements of type 5A; in particular elements of type 5B do not fix any element of Ω.

Using (2-1), we conclude that if g is an element of order 5 in M, then

$$|\mathrm{Fix}_\Omega(g)| = \frac{|G|}{|M|}\frac{|M : \mathbf{C}_M(g)|}{|G : \mathbf{C}_G(g)|} = \frac{|\mathbf{C}_G(g)|}{|\mathbf{C}_M(g)|} = \frac{44352000}{3600 \times 4 \times 2} = 1540.$$

Now let V be a Sylow 5-subgroup of M and observe that V has order 5^2 and $V \setminus \{1\}$ consists only of elements of type 5A. Referring to [Wilson 1987, Section 6], we see that G contains only one conjugacy class of elementary abelian groups of order 25 for which the nontrivial elements are all of type 5A. Thus V is a representative of this G-conjugacy class. Now, Theorem 6.4 in [Wilson 1987] yields $N_G(V) \cong 5^2 : 4S_4 \times S_5$. Appealing to (2-1) again, we conclude that

$$|\mathrm{Fix}_\Omega(V)| = \frac{|G|}{|M|}\frac{|M : \mathbf{N}_M(V)|}{|G : \mathbf{N}_G(V)|} = \frac{|\mathbf{N}_G(V)|}{|\mathbf{N}_M(V)|} = \frac{28800}{19200} = 15.$$

Now Lemma 2.6 implies that G is not binary. □

5. The Monster

We prove Theorem 1.3 for the Monster. Our proof will break down into several parts, and to ensure we cover all possibilities we make use of a recent account of the classification of the maximal subgroups of the sporadic simple groups in [Wilson 2017].

From [Wilson 2017, Section 3.6], we see that the classification of the maximal subgroups of the Monster G is complete except for a few small open cases. In particular, if M is a maximal subgroup of G, then either

(***a***) M is in [Wilson 2017, Section 4], or

(***b***) M is almost simple with socle isomorphic to $L_2(8)$, $L_2(13)$, $L_2(16)$, $U_3(4)$ or $U_3(8)$.

From here on G will always denote the Monster group, and M will be a maximal subgroup of G. We consider the action of G on cosets of M.

maximal subgroup	prime	maximal subgroup	prime
$2.B$	11	$(D_{10} \times \mathrm{HS}).2$	7
$2^{1+24}.\mathrm{Co}_1$	11	$(3^2 : 2 \times O_8^+(3)).S_4$	7
$3.\mathrm{Fi}_{24}$	11	$3^{2+5+10}.(M_{11} \times 2S_4)$	11
$2^2.{}^2E_6(2).S_3$	11	$5^{1+6} : 2J_2 : 4$	7
$2^{10+16}.O_{10}^+(2)$	7	$(A_5 \times A_{12}) : 2$	7
$2^{2+11+22}.(M_{24} \times S_3)$	7	$(A_5 \times U_3(8) : 3_1) : 2$	7
$3^{1+12}.2\mathrm{Suz}.2$	7	$(L_3(2) \times S_4(4) : 2).2$	7
$2^{5+10+20}.(S_3 \times L_5(2))$	7	$(5^2 : [2^4] \times U_5(5)).S_3$	7
$2^{3+6+12+18}.(L_3(2) \times 3S_6)$	7	$7^{1+4} : (3 \times 2S_7)$	5
$3^8.O_8^-(3).2_3$	7	$L_2(16).2$	5

Table 2. Primitive actions of the Monster for Lemma 5.2.

5A. ***The almost simple subgroups in (b).*** We begin by applying Test 5 to those groups in category (***b***). Provided that such a group M is not isomorphic to $L_2(16).2$, we find that, by applying Test 5 with the prime 2 or 3, we can immediately show that G in its action on G/M is not binary.

The group $M = L_2(16).2$ is exceptional here: for each prime p dividing $|M|$, there exists a permutation representation of M of degree coprime to p satisfying the four conditions in Lemma 3.1; hence we cannot apply Test 5. We defer the treatment of $L_2(16).2$ to Section 5B below.

From here on we will consider those groups in category (***a***), as well as the deferred group $L_2(16).2$.

5B. ***Constructing a strongly nonbinary subset.*** For our next step, we will apply Lemma 2.5 to the remaining group, $L_2(16).2$, from category (***b***) and to the groups from category (***a***). We start with a technical lemma; this is then followed by the statement that we need, Lemma 5.2.

Lemma 5.1. *Let G be the Monster, let $p \in \{5, 7, 11\}$ and let $x \in G$ with $o(x) = p$. Then there exists $g \in G$ with $\langle x, x^g \rangle$ elementary abelian of order p^2 and with xx^g conjugate to x via an element of G.*

Proof. When $p = 11$, there is nothing to prove: G has a unique conjugacy class of elements of order 11 and a Sylow 11-subgroup of G is elementary abelian of order 11^2.

When $p \in \{5, 7\}$, it is enough to read [Conway et al. 1985, page 234]: G contains two conjugacy classes of elements of order p. Moreover, G contains two elementary abelian p-subgroups V and V' both of order p^2, with V generated by two elements of type pA and with V' generated by two elements of type pB. Moreover, $\mathbf{N}_G(V)$ and $\mathbf{N}_G(V')$ act transitively on the nonidentity elements of V and of V', respectively.

This lemma can also be easily deduced from [Wilson 1988]. □

maximal subgroup	prime	maximal subgroup	prime
$(7:3\times \mathrm{He}):2$	2	$(7^2:(3\times 2A_4)\times L_2(7)).2$	2
$(A_6\times A_6\times A_6).(2\times S_4)$	2	$(13:6\times L_3(3)).2$	2
$(5^2:[2^4]\times U_3(5)).S_3$	2	$13^{1+2}:(3\times 4S_4)$	2
$(L_2(11)\times M_{12}):2$	2	$L_2(71)$	2
$(A_7\times (A_5\times A_5):2^2):2$ [1]	2	$L_2(59)$	5
$5^4:(3\times 2L_2(25)):2$	2	$11^2:(5\times 2A_5)$	2
$7^{2+1+2}:\mathrm{GL}_2(7)$	2	$L_2(41)$	2
$M_{11}\times A_6.2^2$	2	$L_2(29):2$	2
$(S_5\times S_5\times S_5):S_3$	3	$7^2:\mathrm{SL}_2(7)$	2
$(L_2(11)\times L_2(11)):4$	2	$L_2(19):2$	2
$13^2:(2L_2(13).4)$	2	$41:40$	2

Table 3. Primitive actions of the Monster for Lemma 5.3.

Lemma 5.2. *Let G be the Monster and let M be a maximal subgroup of G. If M is as in the maximal subgroup columns of Table 2, then the action of G on the right cosets of M in G is not binary.*

Note that the final line of the table is the remaining group from category (***b***), hence, once this lemma is disposed of, we only deal with groups from category (***a***).

Proof. If suffices to compare $|G:M|$ with $|M|$ and apply Lemmas 2.5 and 5.1. For simplicity we highlight in Table 2 the prime p that we use to apply Lemma 2.5. □

5C. ***Using Test 5.*** We next apply Test 5 to the remaining maximal subgroups of G. The statement that we need is the following.

Lemma 5.3. *Let G be the Monster and let M be a maximal subgroup of G. If M is as in maximal subgroup columns of Table 3, then the action of G on the right cosets of M in G is not binary.*

Proof. Table 3 lists precisely those remaining maximal subgroups that can be excluded using Test 5, together with the prime p that has been used. □

5D. ***The remainder.*** By ruling out the groups listed in Tables 2 and 3, we are left with precisely five subgroups on Wilson's list [2017]. We now deal with these one at a time and, in so doing, we complete the proof of Theorem 1.3. The remaining groups are as follows: $S_3\times \mathrm{Th}$, $3^{3+2+6+6}:(L_3(3)\times SD_{16})$, $(7:3\times \mathrm{He}):2$, $5^{3+3}.(2\times L_3(5))$, $5^{2+2+4}:(S_3\times \mathrm{GL}_2(5))$.

[1] This action turned out to be rather problematic. Each transitive action of odd degree satisfying the conditions (1), (2), (3) in Lemma 3.1 is not binary. However, for some of these actions to witness the nonbinariness we had to resort to 4-tuples, which was particularly time consuming.

Case 1: $M \cong S_3 \times \mathrm{Th}$**.** Here we refer to [Wilson 1988, Section 2]. There are three conjugacy classes of elements of order 3 in the Monster G, of type 3A, 3B and 3C, and the normalizers of the cyclic subgroups generated by the elements of type 3C are maximal subgroups of G conjugate to M. Choose x, an element of type 3C with $M = \mathbf{N}_G(\langle x \rangle)$. We write $M := H \times K$, where $H \cong S_3$ and $K \cong \mathrm{Th}$. From the first two lines of the proof of Proposition 2.1 of [Wilson 1988], for every $y \in K$ of order 3, xy is an element of type 3C. From the subgroup structure of the Thompson group Th, the group K contains an element y of order 3 with $\mathbf{N}_K(\langle y \rangle)$ of shape $(3 \times G_2(3)) : 2$ and maximal in K. Since x and xy are in the same G-conjugacy class, there exists $g \in G$ with $x^g = xy$. Moreover, an easy computation inside the direct product $M = H \times K$ yields that $M \cap M^g = \mathbf{N}_G(\langle x \rangle) \cap \mathbf{N}_G(\langle xy \rangle) = \mathbf{N}_M(\langle xy \rangle) \cong (\langle x \rangle \times \mathbf{C}_K(y)) : 2$ has shape $(3 \times 3 \times G_2(3)) : 2$. This shows that the action of M on the right cosets of $M \cap M^g$ is permutation isomorphic to the primitive action of Th on the right cosets of $(3 \times G_2(3)) : 2$. In other words, G has a suborbit inducing a primitive action of the sporadic Thompson group. From Proposition 4.1, this action is not binary, and hence the action of G on the right cosets of M is not binary by Lemma 2.8.

Case 2: $M \cong 3^{3+2+6+6} : (L_3(3) \times SD_{16})$**.** Arguing as in the previous case, we note that M contains only elements of type 13A and no elements of type 13B. Let Q be a 13-Sylow subgroup of M and let P be a 13-Sylow subgroup of G with $Q \leq P$. Observe that P is an extraspecial group of exponent 13 of order 13^3 and that Q has order 13. Replacing P by a suitable G-conjugate we may also assume that $Q \neq \mathbf{Z}(P)$. (Observe that to guarantee that we may actually assume that $Q \neq \mathbf{Z}(P)$ we need to use [Wilson 1988, page 15], which describes how the 13-elements of type A and B are partitioned in P. Indeed, not all 13-elements of type B are in $\mathbf{Z}(P)$ and hence, if accidentally $Q = \mathbf{Z}(P)$, we may replace Q with a suitable conjugate.)

Let $\alpha \in \Omega$ with $G_\alpha = M$ and set $\Lambda := \alpha^P$. From the previous paragraph, P acts faithfully on the set Λ and $|\Lambda| = 13^2$. Now the permutation group P in its action on Λ is not 2-closed; indeed the 2-closure of P in its action on Λ is of order 13^{14}, it is a Sylow 13-subgroup of $\mathrm{Sym}(\Lambda)$ (this follows from an easy computation or directly from [Dobson and Witte 2002]). Since P embeds into G^Λ, the 2-closure of G^Λ contains the 2-closure of P, but since 13^{14} does not divide the order of $|G|$, G^Λ is not 2-closed. Lemmas 2.3 and 2.4 imply that the action is not binary.

Case 3: $M \cong (7 : 3 \times \mathrm{He}) : 2$**.** Observe that He has a unique conjugacy class of elements of order 5 and that its Sylow 5-subgroups are elementary abelian of order 5^2. Thus, we let $V := \langle g, h \rangle$ be an elementary abelian 5-subgroup of M and we note that g, h and gh are M-conjugate and hence G-conjugate. The group G has two conjugacy classes of elements of order 5, denoted 5A and 5B. We claim that M contains only elements of type 5A. Indeed, a computation inside the Held group He reveals that $\mathbf{C}_M(g)$ contains an element of order $7 \times 3 \times 5 = 105$ and hence G

contains an element x of order 105 with $x^{21} = g$ being an element of order 5. By considering the power information on the conjugacy classes of G, we see that g belongs to the conjugacy class of type 5A. Since all 5-elements are conjugate in M, we get that M contains only 5-elements of type 5A.

We now calculate the number of fixed points of g and of V on Ω, making use of (2-1). Using the information on the conjugacy classes of He and G we deduce

$$|\mathrm{Fix}_\Omega(g)| = \frac{|G|}{|M|}\frac{|M:\mathbf{C}_M(g)|}{|G:\mathbf{C}_G(g)|} = \frac{|\mathbf{C}_G(g)|}{|\mathbf{C}_M(g)|} = \frac{1365154560000000}{12600} = 108345600000.$$

Next, since V is a Sylow 5-subgroup of M, we deduce that $|\mathbf{N}_M(V)| = 50400$ using the structure of the Held group. Moreover, from [Wilson 1988, Section 9], we get that the normalizer of an elementary abelian 5-subgroup of the Monster consisting only of elements of type 5A is maximal in G and is of the form $(5^2 : 4{\cdot}2^2 \times U_3(5)) : S_3$. In particular, $|\mathbf{N}_G(V)| = 302400000$. Thus

$$|\mathrm{Fix}_\Omega(V)| = \frac{|G|}{|M|}\frac{|M:\mathbf{N}_M(V)|}{|G:\mathbf{N}_G(V)|} = \frac{|\mathbf{N}_G(V)|}{|\mathbf{N}_M(V)|} = \frac{302400000}{50400} = 6000.$$

Now Lemma 2.6 implies that G is not binary.

Case 4: $M \cong 5^{3+3}.(2 \times L_3(5))$**.** Let P be a Sylow 31-subgroup of M and observe that P is also a Sylow 31-subgroup of G. Recall that G has a maximal subgroup $K := C \times D$, where $C \cong S_3$ and $D \cong \mathrm{Th}$ (as usual Th denotes the sporadic Thompson group). Now, by considering the subgroup structure of Th, we see that D contains a maximal subgroup isomorphic to $2^5.\mathrm{L}_5(2)$ and hence D contains a Frobenius subgroup F isomorphic to $2^5 : 31$. Replacing F by a suitable conjugate we may assume that $P \leq F$.

Comparing the subgroup structure of M and of F, we deduce $M \cap F = P$. Consider $\Lambda := \alpha^F$. By construction, as $M = G_\alpha$, we get $|\Lambda| = 32$ and F acts as a 2-transitive Frobenius group of degree 32 on Λ. Since the 2-closure of a 2-transitive group of degree 32 is Sym(32) and since G has no sections isomorphic to Sym(32), we deduce from Lemma 2.4 that G^Λ is strongly nonbinary. Therefore G is not binary by Lemma 2.3.

Case 5: $M \cong 5^{2+2+4} : (S_3 \times \mathrm{GL}_2(5))$**.** For this last case we invoke again the help of a computer-aided computation based on Lemma 3.1, but applied in a slightly different way than what we have described in Test 5. (We thank Tim Dokchitser for hosting the computations required for dealing with this case.) Observe that $|\Omega| - 1$ is divisible by 5, but not by 5^2.

With Magma we construct all the transitive permutation representations on a set Λ of degree greater than 1 and with $|\Lambda|$ not divisible by 5^2 of M. (Considering that a Sylow 5-subgroup of M has index 576, this computation does require some time but it is feasible.) Next, with a case-by-case analysis we see that none of these

permutation representations satisfies (1), (2), (3) and (4). Therefore, every transitive permutation representation of M of degree greater than 1 satisfying (1), (2), (3) and (4) has degree divisible by 25. Now, from Lemma 3.1 applied with $d := 25$, we get that G in its action on the set M of right cosets of M in G is not binary because 25 does not divide $|\Omega| - 1$.

Acknowledgments

At a crucial juncture in our work on Theorem 1.3, we needed access to greater computational power — this need was met by Tim Dokchitser who patiently ran and re-ran various scripts on the University of Bristol Magma cluster. We are very grateful to Tim — without his help we would have struggled to complete this work. We are also grateful to an anonymous referee for a number of helpful comments and suggestions.

References

[Cherlin 2000] G. Cherlin, "Sporadic homogeneous structures", pp. 15–48 in *The Gelfand Mathematical Seminars, 1996-1999*, edited by I. M. Gelfand and V. S. Retakh, Birkhäuser, Boston, 2000. MR Zbl

[Cherlin 2016] G. Cherlin, "On the relational complexity of a finite permutation group", *J. Algebraic Combin.* **43**:2 (2016), 339–374. MR Zbl

[Conway et al. 1985] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford Univ. Press, 1985. MR Zbl

[Dixon and Mortimer 1996] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Math. **163**, Springer, 1996. MR Zbl

[Dobson and Witte 2002] E. Dobson and D. Witte, "Transitive permutation groups of prime-squared degree", *J. Algebraic Combin.* **16**:1 (2002), 43–69. Correction in **29**:4 (2009), 537. MR Zbl

[Gill and Spiga 2016] N. Gill and P. Spiga, "Binary permutation groups: alternating and classical groups", preprint, 2016. arXiv

[Gill et al. 2017] N. Gill, F. Hunt, and P. Spiga, "Cherlin's conjecture for almost simple groups of Lie rank 1", preprint, 2017. To appear in *Math. Proc. Cambridge Philos. Soc.* arXiv

[Gill et al. $\geq$ 2018] N. Gill, M. Liebeck, and P. Spiga, "Cherlin's conjecture for finite groups of Lie type", in preparation.

[Liebeck and Saxl 1991] M. W. Liebeck and J. Saxl, "Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces", *Proc. London Math. Soc.* (3) **63**:2 (1991), 266–314. MR Zbl

[Wielandt 1964] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964. MR Zbl

[Wilson 1987] R. A. Wilson, "Some subgroups of the Baby Monster", *Invent. Math.* **89**:1 (1987), 197–218. MR Zbl

[Wilson 1988] R. A. Wilson, "The odd-local subgroups of the Monster", *J. Austral. Math. Soc. Ser. A* **44**:1 (1988), 1–16. MR Zbl

[Wilson 1999] R. A. Wilson, "The maximal subgroups of the Baby Monster, I", *J. Algebra* **211**:1 (1999), 1–14. MR Zbl

[Wilson 2017] R. A. Wilson, "Maximal subgroups of sporadic groups", pp. 57–72 in *Finite simple groups: thirty years of the Atlas and beyond* (Princeton, 2015), edited by M. Bhargava et al., Contemp. Math. **694**, Amer. Math. Soc., Providence, RI, 2017. MR Zbl arXiv

[Wiscons 2016] J. Wiscons, "A reduction theorem for primitive binary permutation groups", *Bull. Lond. Math. Soc.* **48**:2 (2016), 291–299. MR Zbl

Received July 21, 2017. Revised April 27, 2018.

FRANCESCA DALLA VOLTA
DIPARTIMENTO DI MATEMATICA E APPLICAZIONI
UNIVERSITY OF MILANO-BICOCCA
MILAN
ITALY
francesca.dallavolta@unimib.it

NICK GILL
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTH WALES
TREFOREST
UNITED KINGDOM
nick.gill@southwales.ac.uk

PABLO SPIGA
DIPARTIMENTO DI MATEMATICA E APPLICAZIONI
UNIVERSITY OF MILANO-BICOCCA
MILANO
ITALY
pablo.spiga@unimib.it

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2018 is US $475/year for the electronic version, and $640/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 297 No. 1 November 2018

0030-8730(201811)297:1;1-R