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

A CORRECTION TO THE 41-STRUCTURE OF THE MONSTER, A CONSTRUCTION OF A NEW MAXIMAL SUBGROUP $L_2(41)$, AND A NEW MOONSHINE PHENOMENON

SIMON P. NORTON AND ROBERT A. WILSON

Abstract

We correct the result of a previous paper which purported to show that $L_2(41)$ was not a subgroup of $\mathbb{M}$. Our main result is that there is exactly one conjugacy class of subgroups $L_2(41)$ in the Monster. Such subgroups are self-normalizing and maximal. This leads to a new unexplained Moonshine phenomenon.

1. *Introduction*

In [**2**, **10**, **12**] it was stated that $L_2(41)$ is not a subgroup of the Fischer–Griess Monster $\mathbb{M}$. The following argument, due to the first author, was given in [**10**] and [**12**] (with Atlas [**2**] notation used throughout):

(1) The 5-elements of any $L_2(41) < \mathbb{M}$ must have class $5B$ (stated without proof in Section 6 of [**10**], Theorem 20 of [**12**]).
(2) If $L_2(41) < \mathbb{M}$, then any 8-element t of the (unique up to conjugation) subgroup 41.8 of $\mathbb{M}$ must have class $8D$. (This can be seen from step 1 above, using the subgroup $41.40 < \mathbb{M}$ and the fact that any 8-element centralizing a $5B$-element has class $8D$.)
(3) Between 41.8 and $\mathbb{M}$ lies the group $G = 3^8{\cdot}O_8^-(3){\cdot}2$, a known maximal subgroup of $\mathbb{M}$, which is a non-split extension of $O = O_8^-(3){\cdot}2_3$ acting on its natural representation over GF(3). As t permutes the eigenspaces of a 41-element which it normalizes, it must act regularly on $O_3(G) \cong 3^8$, and therefore it inverts a unique subgroup of order 3 inside this group.
(4) This subgroup must correspond to a non-isotropic vector under the orthogonal form, as any eigenspace of an element that preserves the orthogonal form must be an orthogonal direct summand of the 8-space. The elements of $O_3(G)$ corresponding to non-isotropic vectors have class $3A$.
(5) However it can be seen from the fusion map of $N_{\mathbb{M}}(3A) = 3{\cdot}\mathrm{Fi}_{24}$ in $\mathbb{M}$ that no $8D$-element can invert a $3A$-element. This completes the proof.

However, it was recently pointed out to the authors by Andrei Zavarnitsine [**15**] that the argument of step (4) is invalid, because the outer elements of G, such as t, do not preserve the orthogonal form but negate it. Indeed no outer element of G can invert (or fix) a $3A$-element in $O_3(G)$ because it takes non-isotropic vectors of norm 1 to non-isotropic vectors of norm 2 and vice versa. So the 3-elements centralized and inverted by t must have class $3B$.

In this paper we resolve the re-opened question of whether $L_2(41)$ is a subgroup of the Monster, by explicit computations. Moreover, we completely determine the conjugacy classes of subgroups isomorphsic to $L_2(41)$. These computations were carried out by the second author. We use the computer construction described in [**5**], in which the Monster is generated by a subgroup $\langle a, b\rangle \cong 2^{1+24}{\cdot}\mathrm{Co}_1$, together with a 'triality element' T which centralizes a subgroup $2^{11}{\cdot}\mathrm{M}_{24}$ of $\langle a, b\rangle$.

2000 *Mathematics Subject Classification* 00000.

One possible strategy is to use the methods of [**7**], and try to generate $\mathrm{L}_2(41)$ by two copies of A_5 intersecting in D_{10}. However, the records we kept of these calculations are inadequate to allow us to repeat them easily. Thus we decided instead to adopt a different strategy. The 'obvious' way to generate $\mathrm{L}_2(41)$ is with a Borel subgroup, of shape 41:20, and the normaliser D_{40} of a torus of order 20 inside this Borel subgroup.

In order to find a copy of 41:20 inside the Monster, we have to take a somewhat circuitous route, since the only maximal subgroup containing it (apart from a putative $\mathrm{L}_2(41)$) is 41:40. First we find a subgroup $3^{8}{\cdot}\mathrm{O}_8^-(3){\cdot}2$, and then find 41:8 inside that. Next we find the centralizer in the Monster of an element of order 8 inside 41:8, and search through this centralizer to find an element of order 5 extending 41:8 to 41:40.

After this, it is relatively easy to find the normaliser of the element of order 20, and to run through the involutions which invert it, to see whether any of them extends 41:20 to $\mathrm{L}_2(41)$. It turns out that there are just 12 ways of extending this C_{20} to a D_{40}, interchanged in pairs by the element of order 40, making just six cases to check.

Our main theorem is as follows:

THEOREM 1. *There is exactly one conjugacy class of subgroups* $\mathrm{L}_2(41)$ *in the Monster. Each such subgroup is self-normalizing, and maximal.*

For the record, we note that the remaining cases of simple groups which might possibly be normal in still unknown almost simple maximal subgroups of the Monster are: $\mathrm{L}_2(13)$, $\mathrm{U}_3(4)$, $\mathrm{U}_3(8)$, and $\mathrm{Sz}(8)$. We hope to address these questions in forthcoming work.

The existence of maximal subgroups isomorphic to $\mathrm{L}_2(41)$ shows that the maximal 41-local subgroup 41:40 contains elements of classes $40C$ and $40D$, a fact we first prove theoretically. This in turn leads to uniform statements about pure Fricke elements of prime order, as in Theorem 4 below. A conceptual rather than case-by-case proof of these results would be of great interest in Monstrous Moonshine [**3**].

The paper is organised as follows. Sections 2 and 3 determine the class fusion in $\mathbb{M}$ from the subgroup 41.40, and from any $\mathrm{L}_2(41)$. Section 4 gives an overview of computational techniques, including some improvements to earlier methods of working in the Monster. Sections 5, 6 and 7 describe the calculations in enough detail for anyone with the requisite software to check the results in full. Finally, in Sections 8 and 9 we prove the new Moonshine observations and discuss their implications.

2. *The* 41*-local subgroup of* $\mathbb{M}$

THEOREM 2. *The* 40*-elements normalizing a* 41*-element* s *have class* $40C$ *or* $40D$*.*

REMARK 1. *Note that classes* $40C$ *and* $40D$ *belong to the same class of cyclic subgroups. The* 8*-elements in these subgroups have class* $8D$*, so it* is *possible that* $\mathbb{M}$ *does after all contain a subgroup of type* $\mathrm{L}_2(41)$*.*

Proof. We start by arguing, as in step (3) above, that as t permutes the eigenspaces of s it must act regularly on the 8-space on which O acts.

We next show that the "direct summand" argument is valid for the 2-space containing the vectors fixed and inverted by t, as follows. Let us extend the ground field for our 8-space so that it splits completely into eigenspaces under the action of t. Then, because t negates the orthogonal form, the space with eigenvalue 1 is orthogonal to all the eigenspaces (including itself) except that with eigenvalue -1, and vice versa; so the sum of the spaces with eigenvalues 1 and -1 is orthogonal to the sum of the spaces with the other six eigenvalues.

It therefore follows that the sum and difference of non-zero vectors fixed and negated by t (in the original 8-space over GF(3)) must be non-isotropic. In other words, in $O_3(G)$, the corresponding 3^2 has two cyclic subgroups generated by $3B$-elements (those corresponding to the vectors fixed and negated by t) and two generated by $3A$-elements (corresponding to their sum and difference).

Now it is known that the $\mathbb{M}$-normalizer of any such 3^2 is a group of shape $3^2.3^6.2U_4(3).D_8$ (which is in fact a subgroup of G). The action of t on the 3^2 shows that it belongs to the outer half of a subgroup $U = 3^3.2U_4(3).2_3$, and the fact that t is regular on $O_3(G)$ implies that it has class $8G$ in the quotient group $U_4(3).2_3$, so that t^2 has class $4A$ in this group. This in turn means that the value of a 6-character of $3^2.2U_4(3)$ on t^2 is ± 2; therefore the 12-character of 6.Suz, which is the sum of two 6-characters of its subgroup $3^2.2U_4(3)$, which must have the same sign on t^2, has value ± 4. It then follows that t^2 has 6.Suz-class $4A$, so t has 6.Suz-class $8A$. Finally, the product of t with the central 3 of 6.Suz has $\mathbb{M}$-class $24H$, so t has $\mathbb{M}$-class $8D$ and the 40-elements normalizing s have $\mathbb{M}$-class $40C$ or $40D$. □

3. *Is* $L_2(41)$ *a subgroup of* $\mathbb{M}$*?*

We start by noting that although the above question is now still open, we *can* prove quite easily that $PGL_2(41) \cong L_2(41).2$ is not a subgroup, which implies that 41.40 is maximal. For $PGL_2(41)$ contains a dihedral group of order 80, whereas the 40-elements of 41.40 belong to classes $40C$ and $40D$, and are not inverted by any element of $\mathbb{M}$. It follows at once that any $L_2(41)$ in $\mathbb{M}$ is necessarily maximal.

THEOREM 3. *In any* $L_2(41)$ *inside* $\mathbb{M}$*, all elements belong to one of the classes* $(1A, 2B, 3B, 4C, 5B, 7B, 10E, 20F, 2$

Proof. For elements of order dividing 20, this follows from Theorem 2. For elements of order 3 this follows from Theorem 20 of [**12**]. As there is a unique class of elements of order 21 whose 3-part is $3B$, the theorem is true for elements of orders 21 and 7. Finally, there is a unique class of elements of order 41. □

We also note that structure constant calculations show that any element of class $20F$ is contained in exactly 12 dihedral groups of order 40. This means that there are at most 12 possibilities for building a group $L_2(41)$ by starting with a group 41.20 and extending the 20 to a dihedral group of order 40. Moreover, the elements of order 40 which normalize our group of order 41 cannot normalize any of these dihedral groups, so fuse the 12 cases into six conjugate pairs.

4. *Computational techniques*

We turn now to the computational techniques which we used to resolve the question posed in the title of the previous section. In carrying out these computations, some small improvements to the methods of [**7**] have been obtained. These will be described in this section.

4.1. *Navigating around* 2^{1+24}

Part of the construction of the Monster in [**5**] involved making the natural representation of 2^{1+24} of dimension 2^{12}, by taking 24 generators which were tensor products of 2×2 permutation or diagonal matrices. In order that we can use this information to translate from the Monster to the 24-dimensional representation of Co_1, we begin by reconstructing these 24 generators as words in the generators a and b of $2^{1+24}\cdot Co_1$.

First we made an involution $j_0 = a^2$ inside 2^{1+24}, and then made $j_i = (j_0)^{(ab)^i}$ for $i \leq 22$. These turned out to be independent, and are completed to a basis $\{j_0, j_1, \ldots, j_{23}\}$ by adjoining $j_{23} = (j_1)^b$.

Now for each generator j_i ($0 \leq i \leq 23$), we can determine which element of 2^{1+24} it is by inspecting the top row of the $2^{12} \times 2^{12}$ matrix (in order to read off the permutation) and 12 more rows (in order to read off the 12 signs). This expresses our generators in terms of the standard basis of permutations and diagonal matrices, so by inverting the resulting 24×24 matrix, we express the standard basis in terms of the above generators. The results are given in Table 1.

This gives us an explicit map from 2^{1+24} to $\mathrm{GF}(2)^{24}$ which enables us to translate problems about conjugacy in the group to (much easier) problems of linear algebra.

Moreover, since the 2^{12}-dimensional representation tensored with a 24-dimensional representation of $2{\cdot}\mathrm{Co}_1$ is a constituent of the 196882-dimensional representation, we can read off the required information about the former by calculating in the latter: again, we only need to compute the images of 13 carefully selected basis vectors in order to do this. With the numbering of coordinates as in [**5**] these were coordinates $298 + 98280 + 2^i$, for $0 \leq i \leq 12$.

4.2. *Obtaining the quotient* Co_1 *of the involution centralizer*

Given any element g of the centralizer $2^{1+24}\mathrm{Co}_1$ of the involution z, we can now compute its action on $\mathrm{GF}(2)^{24}$ as follows. For each of the 24 generators $p_1, \ldots, p_{12}, d_1, \ldots, d_{12}$ of 2^{1+24}, compute its image under conjugation by g, and read off the resulting element of $2^{1+24}/2$ as described in Sectionnavextra. Then we can write down a 24×24 matrix representing the image of g in Co_1.

This can even be done for elements of the Monster which centralize z, but which are only given as a word w in a, b, T: for each generator d_i or p_i of 2^{1+24} we apply the word $w^{-1}d_i w$

TABLE 1. *The standard generators of* 2^{1+24}.

p_1	1	0	1	1	0	0	0	1	1	1	1	0	1	1	1	0	1	1	1	1	1	0	1	1
p_2	0	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	0	1	0	0	1	0	0	1
p_3	0	0	1	1	1	0	1	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	1	1
p_4	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	1
p_5	0	0	1	1	0	0	1	1	1	0	1	1	0	1	0	0	1	1	0	1	1	1	1	1
p_6	1	0	1	1	0	0	0	1	0	0	0	1	1	1	0	1	1	1	1	0	0	1	1	1
p_7	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
p_8	1	1	1	0	1	0	0	1	0	0	1	1	1	0	1	1	0	1	0	0	1	0	1	0
p_9	0	1	1	1	1	1	0	1	1	0	1	0	0	0	1	1	1	0	1	1	1	1	1	1
p_{10}	1	0	1	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	1	0	1	0	1	0
p_{11}	1	1	1	1	0	0	1	1	0	0	0	1	0	1	0	0	1	1	1	1	1	0	0	0
p_{12}	1	0	1	1	0	1	1	0	0	0	0	0	1	0	0	0	0	1	0	1	1	0	0	0
d_1	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	0	0	0	0	1	0	0	1	1
d_2	1	0	1	1	0	1	0	1	0	1	1	0	1	1	1	0	0	1	0	1	0	0	1	0
d_3	1	1	1	0	1	0	1	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0
d_4	0	1	1	0	1	0	0	0	0	1	1	0	1	0	1	0	1	0	1	0	0	0	0	0
d_5	1	0	0	0	1	1	1	1	1	0	1	0	0	0	1	1	1	0	0	1	1	0	1	0
d_6	1	1	1	0	0	0	0	0	1	0	0	1	0	0	1	0	0	0	1	0	1	1	1	0
d_7	1	1	1	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	0	1	1	0
d_8	1	0	0	1	0	1	0	0	0	1	1	1	1	0	0	1	0	0	1	1	0	0	0	1
d_9	0	1	0	0	0	1	0	1	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	1
d_{10}	0	1	1	1	0	0	1	0	0	1	1	1	1	0	0	1	1	1	0	1	0	1	0	0
d_{11}	0	1	1	0	1	0	1	1	0	0	1	1	0	0	1	0	1	1	0	0	0	1	1	1
d_{12}	1	1	0	0	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0	1	0

The rows of this table correspond in order to the generators $p_1 \ldots, p_{12}, d_1, \ldots, d_{12}$ of 2^{1+24}. (Mnemonic: p for permutation, d for diagonal.) The columns correspond to the generators $j_0, \ldots, j_{23}$, and each row expresses one of the new generators as a product of the original generators (modulo the central involution).

or $w^{-1}p_iw$ to the 13 carefully selected basis vectors of 196882-space, and read off the result as above.

4.3. *Obtaining* $2{\cdot}\mathrm{Co}_1$

A similar process can be used to obtain elements of $2{\cdot}\mathrm{Co}_1$ as 24×24 matrices over $\mathbb{F}_3$, corresponding in pairs (modulo sign) to elements of the quotient of $2^{1+24}{\cdot}\mathrm{Co}_1$ by the normal 2-subgroup. To do this, we select 24 suitable rows of the tensor product space and extract the 24×24 matrix from them.

As in the previous case, this process can be carried out for any element of the Monster which commutes with the central element z of $2^{1+24}\mathrm{Co}_1$, even if it is only given as a word in the generators of the Monster.

4.4. *Changing post*

In our computations we are often 'tied to the post', in the sense that we can really only compute elements in the subgroup

$$C_{\mathbb{M}}(z) \cong 2^{1+24}{\cdot}\mathrm{Co}_1.$$

However, a method was given in [**6**] for 'changing post', specifically, finding a word in the generators of the Monster which conjugates any given $2B$-element in $2^{1+24}{\cdot}\mathrm{Co}_1$ to the central involution. In principle, we pre-compute some representatives for the conjugacy classes of $2B$-elements in this group, as words in the generators. Then we conjugate our arbitrary $2B$-element to one of these by the usual dihedral group method. In practice, however, it turns out not to be too hard to deal with each case as it arises.

In fact, there are just five conjugacy classes of $2B$-involutions in $2^{1+24}{\cdot}\mathrm{Co}_1$, as follows:

(1) the central involution z,
(2) the conjugates of $T^{-1}zT$, which lie in the normal 2^{1+24},
(3) two classes mapping to Co_1-class $2A$,
(4) one class mapping to Co_1-class $2C$.

Given any $2B$-element x of type (2), we can convert both x and $T^{-1}zT$ to vectors v_1, v_2 in $\mathrm{GF}(2)^{24}$, as described in Section 4.1. There are 8292375 vectors in this orbit under Co_1, so if we make a few thousand images of each vector under known elements of Co_1, the chances are we will find elements $g_1, g_2 \in \mathrm{Co}_1$ such that $v_1g_1 = v_2g_2$, so that $v_1g_1g_2^{-1} = v_2$. (Sorting the vectors makes it easy to find such coincidences.) Lifting back to $2^{1+24}\mathrm{Co}_1$ we have that $g_1g_2^{-1}$ conjugates x to $T^{-1}zT$ or TzT^{-1}, and we have found an element conjugating x to z.

Working inside $2^{1+24}.2^{11}\mathrm{M}_{24}$ we can find elements y_1, y_2, y_3 in the other three $2B$-classes, such that T or T^{-1} conjugates y_i into the 2^{1+24}. Thus each y_i can be conjugated to z by the above method. Now any involution y conjugate to one of the y_i can be so conjugated by finding g such that y_iy^g has odd order, say $2k+1$, as then $y^{(y_iy^g)^k} = y_i$. (If this proves too difficult, one can do the conjugation in the quotient Co_1 first, and then lift to $2^{1+24}\mathrm{Co}_1$.)

4.5. *Applying the formula*

Observe that if x, y are two conjugate elements of order 3 in A_4, then $x^{yx} = y$. Hence the same is true in any group which has an abelian normal 2-subgroup of index 3. By iterating this procedure, one can obtain a conjugating element in the non-abelian case also. Moreover, if g is any element of any group G which commutes with x of order 3 modulo an abelian normal 2-subgroup, then xx^g conjgates x^g to x, so gxx^g centralizes x. Similarly, if g inverts x modulo the 2-group, then $x^{-1}x^g$ conjugates x^g to x^{-1}, so $gx^{-1}x^g$ conjugates x to x^{-1}. Again these procedures can be iterated in the non-abelian case.

These formulas can be easily generalised to elements of order p, where p is any odd prime: in this case we have

$$x^{(yx)^{(p-1)/2}} = y.$$

5. *Finding the maximal subgroup* $3^8{\cdot}\mathrm{O}_8^-(3){\cdot}2$

We turn now to the actual computations, and for clarity we divide these into three main phases. In the first phase (Section 5) we find a copy of the maximal subgroup $3^8{\cdot}\mathrm{O}_8^-(3){\cdot}2$ of $\mathbb{M}$. In the second phase (Section 6) we find a subgroup 41:8 of this, and extend to a maximal subgroup 41:40 of $\mathbb{M}$. In the third phase (Section 7) we find the normalizer of the element of order 20 and complete the determination of the subgroups isomorphic to $\mathrm{L}_2(41)$.

Since the only subgroup of the Monster in which we can easily work is the subgroup $2^{1+24}{\cdot}\mathrm{Co}_1$, that is, the centralizer of a $2B$-involution z, we aim to generate other subgroups by involution centralizers wherever possible. Now $\mathrm{O}_8^-(3)$ has just three conjugacy classes of involutions, whose fixed spaces on the 3^8 are non-singular subspaces of dimensions 2, 4 or 6, and of type $+$, $-$, $+$ respectively. Their centralizers are respectively of shapes

$$3^2.2.\mathrm{U}_4(3).D_8$$
$$(3^4 \times 2^{1+4}.3^2).A_6.D_8$$
$$3^6(2 \times \mathrm{L}_4(3)).D_8$$

and from this it is clear that they fuse to classes $2B$, $2B$ and $2A$ respectively in the Monster.

Now to generate this subgroup in the most effective manner we may consider two commuting involutions x, z whose fixed spaces are disjoint 2-spaces. Then their centralizers have shape $(3^2 \times 2){\cdot}\mathrm{U}_4(3).D_8$ and together generate the group.

5.1. *Finding the first involution centralizer*

We begin therefore by locating a group of this shape inside $2^{1+24}{\cdot}\mathrm{Co}_1$. In fact, for simplicity, we just took the words from [**13**] for the maximal subgroup $3{\cdot}\mathrm{Suz}{:}2$ of Co_1, and then for the maximal subgroup $\mathrm{U}_4(3).2^2$ in Suz:2. This gives a subgroup of index 2 in the desired involution centralizer, which turns out to be sufficient for our purposes.

Specifically, in the generators a, b of the involution centralizer we make the elements

$$c = (ab)^{38}a(ab)^2$$
$$d = (ab^2)^{38}((ababab^2)^2ab)^8(ab^2)^2$$
$$e = d(cd^2)^4(cd)^3$$
$$f = ((ce)^2(cece^2)^2)^{14}$$

and then, modulo the 2-group,

$$\langle c, d\rangle \to 3{\cdot}\mathrm{Suz}{:}2$$
$$\langle c, e\rangle \to 3^2{\cdot}\mathrm{U}_4(3).2^2.$$

In order to get subgroups $6{\cdot}\mathrm{Suz}{:}2$ and $(2 \times 3^2){\cdot}\mathrm{U}_4(3).2^2$ when we lift to $2^{1+24}{\cdot}\mathrm{Co}_1$, we 'apply the formula', using the element f, which lies in the centre of $3{\cdot}\mathrm{Suz}$, so is in class $3A$ in the Conway group. This means replacing c and d by

$$c' = cf^{-1}c^{-1}fc = cf^2c^3fc$$
$$d' = dfd^{-1}fd = dfd^5fd$$

respectively. (These two formulae are different, because c inverts f modulo the 2-group, whereas d centralizes f modulo the 2-group.) We now calculate

$$e' = d'(c'd'^2)^4(c'd')^3,$$

that is, using the same formula as for e, but using c', d' in place of c, d.

5.2. *Finding the centralizer of* 2^2

Having obtained the group

$$\langle c', e' \rangle \cong (2 \times 3^2) \cdot U_4(3).2^2$$

which has index 2 in our desired centralizer of z, we need to pick a suitable involution for x in $\langle c', e' \rangle$. One slight problem here is that we cannot distinguish x from $y = xz$ abstractly, although they are completely different in the Monster. Thus we were forced to try both cases to find out which was the right one. The two cases may be taken as e'^5 and $e'^5 z$. The former turns out to be the correct one. In the sequel, we work with $y = e'^5 z$ rather than x.

In any case, both these elements have the same centralizer in $C(z)$, and we easily find generators e' and

$$g = (e'^5 (e'^{c'})^5)^2 = (e'^5 c'^3 e'^5 c')^2$$

for this common centralizer.

5.3. *Conjugating the second involution to the first*

The next step is to 'change post', that is to conjugate the new involution $y = e'^5 z$ to z so that we can work in its centralizer to find the elements we need. (We describe the calculations that we actually did. They could be simplified slightly by using the pre-computation described in Section 4.4.) The first step is to work in the quotient Co_1 to conjugate y into the normal 2^{11} of the standard copy of $2^{11}{:}M_{24}$. Now this standard copy is generated by h and i where

$$\begin{aligned} h &= (ab)^{34}(abab^2)^3(ab)^6 \\ i &= (ab^2)^{35}((ababab^2)^2 ab)^4 (ab^2)^5 \end{aligned}$$

Now if we let

$$\begin{aligned} k_1 &= hihi^2 \\ k_2 &= hihihi^2 \\ k &= (k_1 k_2)^3 k_2 k_1 k_2 \end{aligned}$$

then k has order 22 in the quotient Co_1, so we know it powers up to an element which is conjugated by T or T^{-1} into the normal 2-subgroup. We now find that $(k^h)^{11} y$ has order 15 modulo the central involution, and therefore

$$l_0 = ((k^h)^{11} y)^7$$

conjugates y into the desired place. (In fact, since we had first done the calculation with x instead of y, we actually used $l_1 = z l_0$ instead. This makes no difference to any of the subsequent calculations.) A simple trial and error then gives us that T^{-1} conjugates this into the normal 2-group.

The second stage of the process of 'changing post' is to conjugate our element $y' = y^{l_1 T^{-1}}$ to z^T modulo $\langle z \rangle$. To do this we translate these elements of 2^{1+24} into vectors of the standard module for Co_1, as described in Section 4.1. Then we make a few thousand images of each under elements of Co_1, and sort the results in order to find coincidences. Any coincidence between the two lists of images gives us an element of Co_1 to map one to the other. We find that the element

$$l_2 = (ababab^2)^{10}(abababab^2 ab)^3 (ab^2)^4$$

conjugates y' to zz^T, and therefore

$$l = l_1 T^{-1} l_2 T$$

conjugates y to z.

5.4. *Finding the centralizer of an element of order* 10

We may also conjugate e' and g by l to obtain a subgroup of $C(z)$ containing A_6. We need to extend this to a group of shape roughly

$$3^{4\cdot}(\mathrm{O}_4^+(3) \times \mathrm{O}_4^-(3)).$$

The first step is to find the centralizer of the element $e'' = e'^l$, which has order 10. To do this, we first work in the quotient Co_1, and conduct a random search for $3A$-elements which commute with e'' in this quotient. They will generate a normal subgroup $A_5 \times A_5$ of the desired centralizer.

Specifically, we take the $3A$-element

$$m_0 = (ab(abab^2)^2)^{28}$$

and conjugate by the elements

$$c_{\alpha\beta\gamma\delta} = c_1^\alpha c_2^\beta c_3^\gamma c_4^\delta,$$

where

$$\begin{aligned} c_1 &= ab \\ c_2 &= ab^2 \\ c_3 &= ab(abab^2)^2 \\ c_4 &= ababab^2ab \end{aligned}$$

and

$$\begin{aligned} (\alpha,\beta,\gamma,\delta) = {} & (10,8,27,9), \\ & (0,21,19,6), \\ & (36,35,36,5), \\ & (16,10,13,5). \end{aligned}$$

In fact the conjugation was only done correctly modulo the 2-group, and the actual elements we made were

$$\begin{aligned} m_1 &= (c_{10,8,27,9})^{13} m_0 c_{10,8,27,9} \\ m_2 &= (c_{0,21,19,6})^{38} m_0 c_{0,21,19,6} \\ m_3 &= (c_{36,35,36,5})^{21} m_0 c_{36,35,36,5} \\ m_4 &= (c_{16.10.13.5})^{21} m_0 c_{16,10,13,5} \end{aligned}$$

whereas the orders of the conjugating elements are respectively $28, 39, 44, 44$. We have that $\langle m_1, m_2\rangle$ is one of the A_5 factors, and $\langle m_3, m_4\rangle$ is the other.

In each of these A_5s there are just two cyclic groups of order 3 which extend our A_6 to a group of shape 3^5A_6. In the first group they happen to be generated by m_1 and m_2, while in the second they are generated by

$$\begin{aligned} m_5 &= m_3^{m_4 m_3} = (m_4 m_3)^4 m_3 m_4 m_3 \\ m_6 &= m_3^{m_4^2} = m_4 m_3 m_4^2. \end{aligned}$$

It will turn out later that the ones we need are m_1 and m_5.

5.5. *Shortening the words for the conjugates of* e' *and* g

Recall that e' has order 10 and its fifth power is z. Since z commutes with y, it follows that z^l commutes with $y^l = z$, so we want to find a word in a and b which gives the element z^l. We start by identifying it in the quotient group Co_1, where we know it lies in the $A_5 \times A_5$ generated by the m_i: we find that, modulo the 2-group, it is

$$m = (m_2 m_6)^2 m_1 m_5 m_2 m_6 (m_1 m_5)^2 (m_2 m_6)^2 m_1 m_5.$$

We next find the centralizer of this involution in the Conway group: this has shape

$$2^{11}\mathrm{M}_{12}.2$$

and it, or a subgroup of index 2, is generated by the elements

$$\begin{aligned} n &= (mab^2m(ab^2)^{-1})^7 \\ o &= ab(m(ab)^{-1}mab)^{17}. \end{aligned}$$

This group is now small enough that we can conduct a random search for elements of order 5 which are equal to (powers of) e'^2 and $(e'^2)^g$. We find that the conjugates of $(no)^2$ by

$$d_{\alpha,\beta,\gamma,\delta,\epsilon,\zeta} = o^\alpha (no)^\beta (no^2)^\gamma d_4^\delta d_5^\epsilon d_5^\zeta$$

do this job, where

$$\begin{aligned} d_4 &= (no)^2(nono^2)^2no^2 \\ d_5 &= (no)^2(nono^2)^2 \\ d_6 &= no(nono^2)^2 \end{aligned}$$

and

$$\begin{aligned} (\alpha,\beta,\gamma,\delta,\epsilon,\zeta) = &(6,2,10,5,7,9), \\ &(3,2,9,3,0,5) \end{aligned}$$

respectively. Again, this conjugation is only done correctly modulo the 2-group, and the actual elements we make are

$$\begin{aligned} q_1 &= (d_{6,2,10,5,7,9})^5(no)^2 d_{6,2,10,5,7,9} \\ q_2 &= (d_{3,2,9,3,0,5})^3(no)^2 d_{3,2,9,3,0,5} \end{aligned}$$

Next we lift these elements to $2^{1+24}\cdot\mathrm{Co}_1$. In order to find out which element of 2^{1+24} to multiply q_i by, in order to get the actual element we want, we calculate the action of its quotient on the 13 basis vectors described in the previous section, and thereby read off a word for this quotient in terms of the standard generators for 2^{1+24}. We find that q_1 and q_2 need to be replaced by

$$\begin{aligned} q_1' &= p_1p_3p_5p_6p_7p_9p_{11}p_{12}d_1d_2d_3d_4d_7d_8d_9d_{10}d_{11}(q_1)^4z \\ q_2' &= p_2p_7p_9p_{10}p_{11}d_4d_5d_8d_9d_{10}q_2z \end{aligned}$$

respectively. We then have $q_1' = (e'^2)^l$ and $q_2' = (e'^2)^{gl}$.

5.6. *Generators for* $3^8\cdot\mathrm{O}_8^-(3)\cdot 2$

Now we are in a position to complete the computation of the centralizer in the Monster of the element of order 10. This element is the product of z with q_1', and we have already calculated the elements m_1, m_2, m_5, m_6 which centralize it modulo the 2-group. So we only need to 'apply the formula'. Multiplying by z where necessary to get elements of order 3 we have

$$\begin{aligned} m_1' &= q_1'm_1(q_1'q_1'^{m_1})^2z \\ m_2' &= q_1'm_2(q_1'q_1'^{m_2})^2 \\ m_5' &= q_1'm_5(q_1'q_1'^{m_5})^2 \\ m_6' &= q_1'm_6(q_1'q_1'^{m_6})^2z \end{aligned}$$

These elements together generate a group of shape $2^{1+8}(A_5\times A_5)$ which centralizes q_1'.

In order to refine this picture further, we next need to make generators for the normal subgroup 2^{1+8}. Let

$$\begin{aligned} r_1 &= (m_2'm_6')^3 \\ r_5 &= (r_1)^{m_5'm_6'} \end{aligned}$$

$$r_{i+1} = (r_i)^{m_1' m_2'} \text{ for } i = 1, 2, 3, 5, 6, 7.$$

We then look for conjugates of $(m_1' m_5')^4$ and $(m_2' m_6')^4$ which could extend the $\langle c'^l, e'^l \rangle$ to $3^8{\cdot}\mathrm{O}_8^-(3).2$, by eliminating all cases in which we can find an element of an incompatible order. This leaves us with just the one case

$$s_1 = ((m_1' m_5')^4)^{r_7}.$$

At this stage we have generators c'^l, e'^l, s_1 for the maximal subgroup $3^8{\cdot}\mathrm{O}_8^-(3){\cdot}2$ of the Monster.

6. *Finding the maximal subgroup* 41:40

6.1. *Finding a dihedral group of order* 82

We look at the commutators of z with 'random' short words in the generators of $3^8{\cdot}\mathrm{O}_8^-(3){\cdot}2$, in order to find a commutator of order 41. After a few attempts we find that the element s_4 works, where

$$\begin{aligned} s_2 &= (c'e')^2 (c'e'^3)^2 \\ s_3 &= c'e'c'e'^3 \\ s_4 &= (s_2)^l s_1 q_2' (s_3)^l \end{aligned}$$

Thus z and z^{s_4} are involutions generating a dihedral group of order 82. Note that the word for s_4 involves four instances of l or l^{-1}, each of which involves two instances of T or T^{-1}. Thus the element zz^{s_4} of order 41 is given as a word involving 16 instances of T or T^{-1}.

6.2. *Extending to* 41:4

Next we look for elements of order 4 which lie in $3^8{\cdot}\mathrm{O}_8^-(3)$ and which square to z, with the property that they conjugate this element of order 41 to a power of itself. This latter property is equivalent to the property that the conjugate commutes with the original. This is an easier property to check. Indeed, a quicker test is to pre-compute a vector fixed by the element of order 41, and test whether the image of this vector under the element to be tested is again fixed by the element of order 41.

It turns out that there are just 2430 such cyclic groups of order 4 to test, and each test took approximately 15 seconds. Thus we were able to run the whole test in about ten hours, and find the one case which works. The element of order 4 which normalizes the given element of order 41 turns out to be

$$s = r_1 r_3 r_5 (q_1' q_2')^{s_1^2 s_5^2 q_1'^4 q_2' q_1'^4},$$

where

$$s_5 = ((m_1' m_5'^2)^2)^{r_6}.$$

We also make the following elements which will be useful later: let

$$s_6 = s_1 (m_2' m_6')^4 s_1 (m_2' m_6')^2 s_1^2 (m_2' m_6')^4$$

and

$$s_7 = (s_6 s_5^2 s_6 s_5 s_6)^{q_1'^4 q_2' q_1'^4}.$$

6.3. *Finding the* 10*-normalizer*

Before extending 41:4 to 41:8, we need to make the outer halves of the various groups which we have neglected to make so far. We begin with

$$\langle q_1', m_1', m_2', m_5', m_6' \rangle \cong 5 \times 2^{1+8}(A_5 \times A_5),$$

which has index 8 in the full 10-normalizer, and work first in the quotient Co_1. To find an element swapping the two A_5 factors we can work in

$$\langle n, o\rangle \to 2^{11}\mathrm{M}_{12},$$

and first find the centralizer of q_1' in $\langle n, o\rangle$ as

$$\langle q_1', n_1, n_2, n_3\rangle \to 5 \times 2^3,$$

modulo the 2^{1+24}, where

$$\begin{aligned} n_1 &= ((no^2)^8)^{o^2}q_1')^5, \\ n_2 &= ((nonono^2)^8q_1')^5, \\ n_3 &= (((nonono^2)^8)^o q_1')^5. \end{aligned}$$

Then we find that the last generator works, so we put

$$t_1 = (o^{10}(nonono^2)^8 o q_1')^5$$

and apply the formula to get

$$t_2 = q_1' t_1 (q_1' t_1^3 q_1' t_1)^2,$$

which extends the group to $5 \times 2^{1+8}(A_5 \times A_5).2$ as required.

Next we find that, modulo the 2-group,

$$\langle n^{o^5}, q_1'\rangle \to S_6,$$

in which

$$t_3 = ((q_1' o^6 n o^5)^2 q_1'^4 o^6 n o^5)^2 (q_1'^2 (q_1' o^6 n o^5)^2 q_1'^4 o^6 n o^5)$$

conjugates q_1' to its square. So we apply the formula (where t_3 has order 8) to get

$$t_4 = t_3((q_1')^2 t_3^7 q_1' t_3)^2,$$

which extends our group to the full 10-normalizer

$$(5 \times 2^{1+8}(A_5 \times A_5).2).4.$$

6.4. *Outer halves of* $(2^{1+4} \times 3^4)(3^2 \times A_6).D_8$

We need to adjust t_3 and t_4 so that they normalise $\langle q_1', q_2'\rangle$. First we use the formula to adjust them so that they normalize the 3^2 generated by s_1 and s_5. We put

$$\begin{aligned} t_2' &= t_2 s_5^2 t_2^3 s_5 t_2 \\ t_4' &= s_1 s_5 t_4 s_1 s_5 t_4^3 s_1 s_5 t_4 \\ t_4'' &= t_4' s_1^2 s_5 (t_4')^3 s_1 s_5^2 t_4'. \end{aligned}$$

Then t_2' and t_4'' normalise $\langle s_1, s_5\rangle$, but t_2' still does not normalise $\langle q_1', q_2'\rangle$. Indeed, only half of the normaliser of $3^2 \times 5$ normalizes this group, so we make another element which normalizes the former but not the latter. Let

$$t_6 = m_2'^2 m_1' m_2' m_1'^2 m_2'^2 m_1'$$

and then apply the formula twice to get

$$\begin{aligned} t_6' &= s_1 s_5 t_6 s_1 s_5 (s_1 s_5)^{t_6} \\ t_6'' &= t_6' (s_1^2 s_5)(s_1 s_5^2)^{t_6'}. \end{aligned}$$

Finally we find that t_4'' and $t_2'' = t_2' t_6''$ extend our group to $(2^{1+4} \times 3^4)(3^2 \times A_6).D_8$ as required.

6.5. *The* 4*-centralizer*

Next we construct the centralizer in $\langle q_1', q_2' \rangle$ of the element s of order 4. We already have the centralizer of s^2, namely the group

$$(2^{1+4} \times 3^4)(3^2 \times A_6).D_8$$

just constructed. The centralizer of s is a subgroup of order $2^9.3^2$, and structure which may be roughly described as

$$(4 \circ Q_8 \times 3^2).(3 \times D_8).2^2,$$

where the individual terms correspond to those given for the centralizer of s^2. We work our way up from the bottom, constructing a composition series as we go. The group $4 \circ Q_8$ may be generated by

$$\begin{aligned} u_3 &= r_1 r_3 r_5 \\ u_4 &= r_1 r_6 \\ u_5 &= r_2 r_3 r_5 r_7 r_8. \end{aligned}$$

The central involution of the D_8 may be taken as s, and the remaining four composition factors of order 2 are u_6, u_7, u_8, u_9 constructed as follows:

$$\begin{aligned} u_8 &= [s, q_2']^2 = (s^3 (q_2')^2 s q_2')^2 \\ u_{11} &= t_4'' t_2'' [s, t_4'' t_2''] = t_4'' t_2'' s^3 (t_4'' t_2'')^3 s t_4'' t_2'' \\ u_{12} &= r_3 r_4 r_6 r_7 s_5^2 s_7 s_5 [s, r_3 r_4 r_6 r_7 s_5^2 s_7 s_5] \\ u_7 &= [u_8, u_{11}] = u_8 u_{11}^7 u_8 u_{11} \\ u_6 &= (u_7 u_{12})^3 \\ u_9 &= (u_{11} u_6)^3. \end{aligned}$$

The normal 3^2 may be generated by

$$\begin{aligned} u_{14} &= (q_1' [s, q_1']^2)^2 = (q_1' (s^3 (q_1')^4 s q_1)^2)^2, \\ u_{15} &= (u_{14})^{u_{11}}. \end{aligned}$$

The other factor of 3 turned out not to be required.

6.6. *Extending to* 41:8

In the Sylow 2-subgroup of the 4-centralizer we carried out an exhaustive search for all the elements of order 8 which square to s. Modulo s, there were just 20 such elements, in two conjugacy classes of size 4 and 16. Each one had just three conjugates under the 3-part of the group, giving us 60 cases to check in total. We rapidly found the required element of order 8 to be

$$u = u_{14}^2 u_5 u_7 u_8 u_9 u_{14}.$$

Thus

$$\langle u, z^{s_4} \rangle \cong 41{:}8.$$

6.7. *The full* 4*-centralizer*

From this point on, we have to leave the safety of the subgroup $3^8 \cdot \mathrm{O}_8^-(3) \cdot 2$, and venture out into the Monster. In order to find an element of order 5 which extends 41:8 to 41:40, we need to find the centralizer in the Monster of our element of order 8. First we find the full centralizer in the Monster of its square, s. Since $s^2 = z$, the central involution of $2^{1+24} \cdot \mathrm{Co}_1$, we work throughout in the latter group.

In effect we are looking for the centralizer of an involution in the quotient $2^{24} \cdot \mathrm{Co}_1$. The structure of this involution centralizer is $2^{16}.2^{1+8}.\mathrm{S}_6(2)$. Given the part of the centralizer we

already have, it should be sufficient to find one more generator. Unfortunately, the presence of a large normal 2-subgroup means that Bray's algorithm [**1**] is not effective, since the elements it produces are overwhelmingly likely to lie in the normal 2-group. Thus we need more subtle techniques.

We first calculate that $[s, b]$ has order 10, but only order 5 in the quotient Co_1. Therefore the element

$$v_1 = b[s, b]^2$$

commutes with s modulo the 2-group. Together with the part of the centralizer we already have, it generates a group of shape

$$2^{1+24}{\cdot}2^{1+8}{\cdot}\mathrm{O}_8^+(2).$$

Since the normalizer of s has index $2^8.120 = 30720$ in this group, a random search for elements of the normalizer is just about feasible, but we would prefer something quicker if possible.

Now it is easy to calculate from the centralizer orders given in the Atlas [**2**] that a $3E$-element in $\mathrm{O}_8^+(2)$ has a 1 in 20 chance of lying in a particular subgroup $\mathrm{S}_6(2)$. Moreover, such an element acts with a fixed 4-space on the chief factor 2^8 which we lose in going down to $N(s)$. In other words a random conjugate of such an element of order 3 in $2^{1+24}.2^{1+8}.\mathrm{O}_8^+(2)$ has a probability of 1 in $16.20 = 320$ of centralizing s. In fact we decided to be more systematic, and first make the 16 conjugates under the 2^8 factor, so that the probability of success at each stage is increased to 1 in 20.

Now it turns out that u_{14} is a 3-element in the right conjugacy class, so we first find a suitable set of 16 conjugates of it. We tried conjugating by $v_2^\alpha v_3^\beta v_4^\gamma v_5^\delta$, where

$$\begin{aligned} v_2 &= a^2, \\ v_3 &= (a^2)^{(v_1u_{15})^8}, \\ v_4 &= (a^2)^{(v_1u_{15})^{16}}, \\ v_5 &= (a^2)^{(v_1u_{15})^{24}}, \end{aligned}$$

and $\alpha, \beta, \gamma, \delta \in \{0, 1\}$, and found by brute force that these 16 conjugates lie in different cosets of the 4-normalizer. Then conjugating these 16 elements of order 3 by elements of the form

$$v_1(v_1u_{14})^\varepsilon(v_1u_{15})^{8\zeta}$$

we found that one case which works is

$$v_6 = (u_{14})^{v_2v_5v_1(v_1u_{14})^4(v_1u_{15})^{32}}.$$

Moreover, the full centralizer of s is generated by v_6u_{14} and u_{15}, and has shape

$$C(s) \cong 4.2^8.2^8.2.2^6\mathrm{S}_6(2).$$

6.8. *The* 8*-centralizer*

We now make (most of) the centralizer of the element u of order 8 by a similar method. This centralizer has order $2^{19}.3^3.5$ and shape

$$C(u) \cong 8.2^4.2^4.2^4.A_6.2.$$

First we get two generators for the centralizer modulo the 2-group. We make

$$w_1 = u_{15}[u, u_{15}] = u_{15}u^7u_{15}^2uu_{15}$$

which does in fact centralize u, and

$$w_2 = (v_6u_{14}u_{15})^3[u, (v_6u_{14}u_{15})^3],$$

which only centralizes u modulo 2^{1+24} (which is actually better than we could a priori have hoped for). Now we investigate the 2-group. First

$$w_3 = (w_2^6(v_6u_{14}u_{15}^2)^2)^7$$

is an involution in the bottom 2^8 chief factor of $C(s)$, and we make

$$\begin{aligned} w_4 &= (w_3)^{(w_1w_2)^2}, \\ w_5 &= (w_4)^{(w_1w_2)^2}, \\ w_6 &= (w_5)^{(w_1w_2)^2}. \end{aligned}$$

Next we find that

$$w_7 = w_4w_5w_6w_3^{v_6u_{14}u_{15}}$$

centralizes u, and we make the bottom 2^4 chief factor of $C(u)$ by

$$\begin{aligned} w_8 &= (w_7)^{(w_1w_2)^2}, \\ w_9 &= (w_8)^{(w_1w_2)^2}, \\ w_{10} &= (w_9)^{(w_1w_2)^2}. \end{aligned}$$

Now u_4 already centralizes u, so we make another 2^4 chief factor by

$$\begin{aligned} w_{12} &= (u_4)^{(w_1w_2)^2}, \\ w_{13} &= (w_{12})^{(w_1w_2)^2}, \\ w_{14} &= (w_{13})^{(w_1w_2)^2}. \end{aligned}$$

The next non-trivial chief factor can be made as follows:

$$\begin{aligned} w_{15} &= w_3(v_6u_{14}u_{15}^2)^{7(v_6u_{14}u_{15})}, \\ w_{16} &= w_5w_{15}^{(w_1w_2)^2}, \\ w_{17} &= w_3w_5(w_{15})^{(w_1w_2)^4}, \\ w_{18} &= w_3w_4w_5w_6(w_{15})^{(w_1w_2)^6}. \end{aligned}$$

The last non-trivial chief factor A_6 proved more elusive. Let

$$\begin{aligned} w_{19} &= ((v_6u_{14}u_{15})^3u_{15}v_6u_{14}u_{15})^2v_6u_{14}u_{15}^2 \\ w_{20} &= w_{19}^8[u, w_{19}^8]. \end{aligned}$$

Then put

$$\begin{aligned} w_{21} &= ((w_1w_2^2)^2w_1^2w_2^2w_{20})^4, \\ w_{22} &= (w_{21})^{(w_1w_2)^2}, \\ w_{23} &= (w_{22})^{(w_1w_2)^2}, \\ w_{24} &= (w_{23})^{(w_1w_2)^2} \end{aligned}$$

to get a 2^4 which commutes with u modulo the 2^{1+24}. We then find that

$$w_{25} = (w_1w_2)^{2(w_3w_4w_6w_{21}w_{23}w_{24})}$$

is an element of order 5 which commutes with u. This completes our construction of the non-trivial composition factors of $C(u)$.

6.9. *Extending to* 41:40

We now need to check through all the 5-cycles in the 8-centralizer to find the one which normalizes our element of order 41. The number of cases to consider is $2^{12}.36 = 147456$. The 2^{12} conjugates by the normal 2-group are obtained by conjugating by combinations of w_i for $7 \le i \le 18$. The 36 conjugates in S_6 (modulo the 2-group) may be made as follows: let

$$w_{26} = w_1^2w_{25}^3$$

and then make a 3^2 generated modulo the 2-group by w_1 and

$$w_{27} = ((w_{25}^3 w_1 w_{25}^3)^4 w_{26} w_{25}^3 w_1 w_{25}^3)^4.$$

Let

$$\begin{aligned} w_{28} &= (w_{25}w_{26})^2 w_1 w_{25} w_{26} \\ w_{29} &= w_{25}^2 w_{26} w_1 w_{25}, \end{aligned}$$

(although these elements were not in the end required). Then the 36 conjugates of w_{25} by

$$w_{28}^{\alpha} w_{29}^{\beta} w_{27}^{\gamma} w_1^{\delta} \text{ for } 0 \le \alpha, \beta \le 1 \text{ and } 0 \le \gamma, \delta \le 2$$

will do the job. The element of order 5 which normalizes our element of order 41 turns out to be

$$w = (w_{25})^{w_{30}},$$

where

$$w_{30} = w_{27} w_1 w_{16} w_{17} w_{10} u_4.$$

Thus

$$\langle z^{s_4}, u, w \rangle \cong 41{:}40.$$

7. *Generating* $\mathrm{L}_2(41)$

7.1. *Normalizing the element of order* 20

To save time, we analysed the normalizer of $x_0 = sw_{25}$ rather than sw, and conjugated by w_{30} afterwards. First note that $C(x_0)/\langle x_0 \rangle$ has order 48. We found the following elements in the centralizer:

$$\begin{aligned} x_1 &= (u_3 w_{25})^5 \\ x_2 &= (u_4 w_{25})^5. \end{aligned}$$

Now in the quotient $\mathrm{S}_6(2)$ of the 4-centralizer, the centralizer of the element of order 5 is $5 \times S_3$. We already have a transposition of this S_3, namely u. To find another transposition, we first see that

$$x_3 = u^{(v_6 u_{14} u_{15})^3}$$

maps to a transposition which together with u generates an S_3 in the quotient $\mathrm{S}_6(2)$. Now we conjugate this by combinations of $w_{21}, w_{22}, w_{23}, w_{24}$ to find the transposition

$$x_4 = x_3^{w_{21} w_{23} w_{24}}$$

commutes with w_{25} modulo the 2-group. So we apply the formula twice, getting

$$\begin{aligned} x_5 &= w_{25} x_4 (w_{25} {w_{25}}^{x_4})^2 \\ x_6 &= w_{25} x_5 (w_{25} {w_{25}}^{x_5})^2. \end{aligned}$$

Writing

$$\begin{aligned} x_7 &= (u x_6)^4 \\ x_8 &= (x_2)^{x_7} \end{aligned}$$

gives a composition series for $C(x_0)/\langle x_0 \rangle$ of order 48 by adjoining successively x_1, x_2, x_8, x_7, u.

Now to make an element which inverts x_0 we first apply the formula to the element

$$x_9 = r_3 r_4 r_6 r_7$$

of order 4, which, modulo the 2-group, inverts s and centralizes $(w_1w_2)^2$. This gives

$$x_{10} = w_{25}x_9(w_{25}{w_{25}}^{x_9})^2.$$

Then we look in S_6 for an element which inverts the 5-element: modulo the 2-group, we find

$$x_{11} = (w_{25}w_1w_{25}^3w_1^2w_{25}^3)^2.$$

This time we have to apply the formula twice:

$$x_{12} = x_{11}((w_{25})^4{w_{25}}^{x_{11}})^2$$
$$x_{13} = x_{12}((w_{25})^4{w_{25}}^{x_{12}})^2.$$

Combining these two elements gives an element $x_{14} = x_{10}x_{13}$ which inverts x_0. Finally we have that

$$\langle u, x_0, x_1, x_2, x_8, x_7, x_{14}\rangle$$

is the group of all elements centralizing or inverting the element sw_{25} of order 20.

7.2. *Testing the six cases*

We now run through this group to find the involutions inverting the element of order 20. They turn out to be the conjugates of ux_{14}. There are exactly 12 ways of extending the cyclic group of order 20 to D_{40}, falling into six orbits of size 2 under the action of the element u of order 8.

Finally we conjugate by w_{30} and test the resulting six cases. The group generated by 41:20 and D_{40} is isomorphic to $\mathrm{L}_2(41)$ just if one of the 20 reflections in the dihedral group has product of order 3 with the element of order 41.

It turned out that exactly one of the six cases generates $\mathrm{L}_2(41)$. This is given by the involution

$$y_0 = (sw)^2(x_1x_2ux_{14})^{x_7w_{30}}.$$

7.3. *Proving the main theorem*

In fact, many of the calculations described above were done without proof, and therefore we must check certain key facts in order to prove our main results. The three elements which we showed generate $\mathrm{L}_2(41)$ are $\alpha = z^{s_4}z$, $\beta = sw$, and $\gamma = y_0$. These elements satisfy the presentation

$$\langle \alpha, \beta, \gamma \mid \alpha^{41} = \beta^{20} = \gamma^2 = (\beta\gamma)^2 = (\alpha\gamma)^3, \alpha^\beta = \alpha^2\rangle.$$

To prove this, we first showed that $z^{s_4}z$ had order divisible by 41, by showing that it brings a 'random' vector back after 41 steps. Hence it has order exactly 41. All the relations which do not involve α can be calculated inside the subgroup $2^{1+24}\mathrm{Co}_1$. The remaining relations can be checked by verifying them on two vectors carefully chosen so that the intersection of their stabilizers is trivial. This proves existence of the subgroup $\mathrm{L}_2(41)$.

The elements centralizing or inverting sw all lie inside $2^{1+24}\mathrm{Co}_1$, where we can easily check all required relations, and verify that we have indeed considered all the involutions which invert sw. This proves uniqueness.

8. *A new Moonshine phenomenon*

The discovery of Theorem 2 removes what previously appeared to be an exception to the following theorem, which may have significance in Moonshine theory. (All Moonshine related notation and terminology is as in [**3**, **4**, **11**].)

DEFINITION 1. *An element of $\mathbb{M}$ with order $n > 1$ is said to be a* pure Fricke element *of order n if the fixing group of its corresponding Classical Moonshine function, as in [**3**], can be obtained from $\Gamma_0(n)$ by adjoining the Fricke involution $z \mapsto -1/(nz)$.*

It can be seen from [**3**] that the pure Fricke classes of $\mathbb{M}$ are $2A$, $3A$, $4A$, $5A$, $6B$, $7A$, $8A$, $9A$, $10D$, $11A$, $12H$, $13A$, $14C$, $15C$, $16C$, $17A$, $18E$, $19A$, $20F$, $21D$, $23AB$, $24I$, $25A$, $26B$, $27A$, $27B$, $29A$, $31AB$, $32A$, $35B$, $36D$, $39CD$, $41A$, $47AB$, $59AB$ and $71AB$.

THEOREM 4. *Let p be a prime other than 2 or 3 dividing the order of $\mathbb{M}$, and let g be a pure Fricke element of order p. Then the following hold:*

(i) *The shape of $N_{\mathbb{M}}(g)$ is either $g.g' \times H$ or $(g.g' \times H).2$, where g' is an element of order $(p-1)/2$, according as the class of g is irrational or rational. The Frobenius group $g.g'$ is uniquely defined by this condition.*

(ii) *There is a modular function of form $2p|2+$, i.e. a square root of the Hauptmodul of $\Gamma_0(p)+$ (with z replaced by $2z$), exactly when the class of g is rational.*

(iii) *Furthermore, in the rational case the outer half of $H.2 = N_{\mathbb{M}}(g)/g.g'$ has a unique conjugacy class of involutions.*

(iv) *g' is a pure Fricke element.*

Of these (i) has long been known, and (ii) was stated in [**9**]. The first author had previously noticed that (iv) was true except when $p = 41$ and possibly when $p = 71$. The case $p = 71$ was settled when P. E. Holmes showed that $L_2(71) < \mathbb{M}$ (see [**7**]; the result is also stated in [**2**] page xl, though not in the original edition of the ATLAS), and Theorem 2 settles the case $p = 41$.

All four parts may be proved by a case by case analysis. The shapes of the various groups $N_{\mathbb{M}}(g)$ are, respectively,

$(D_{10} \times \mathrm{HN}).2$
$(7.3 \times \mathrm{He}).2$
$(11.5 \times \mathrm{M}_{12}).2$
$(13.6 \times \mathrm{L}_3(3)).2$
$(17.8 \times \mathrm{L}_2(7)).2$
$(19.9 \times A_5).2$
$23.11 \times S_4$
$(29.14 \times 3).2$
$31.15 \times S_3$
41.40
47.23×2
59.29
71.35.

In accordance with Theorem 4 it can be seen from [**4**] that Moonshine type functions of type $2p|2+$ exist when $p = 5$, 7, 11, 13, 17, 19, 29 or 41, but not when $p = 23$, 31, 47, 59 or 71. In the former case the groups $H.2$ are, respectively, HN.2, He.2, $\mathrm{M}_{12}.2$, $\mathrm{L}_3(3).2$, $\mathrm{L}_2(7).2$, $A_5.2$, 3.2 and 1.2, each of which does indeed have just one conjugacy class of involutions in its outer half.

We now look at (iv), the new result. In many cases there is a unique class of element of order $(p-1)/2$ which has elements centralizing a particular element h' of $C_{\mathbb{M}}(g)$; for $p = 5$, 7, 11, 13, 17, 19, 23, 47 and 59 we may take h' in class $19A$, $17A$, $11A$, $13B$, $7A$, $5A$, $1A$, $1A$ and $1A$ respectively to show that g' belongs to class $2A$, $3A$, $5A$, $6B$, $8A$, $9A$, $11A$, $23AB$ and $29A$ respectively. (Why does $C_{\mathbb{M}}(13A.6) = \mathrm{L}_3(3)$ contain a $13B$-element? Because as $13B$ is 13-central in $\mathbb{M}$ and has centralizer $13^{1+2}.2A_4$, it follows that there is a 13^2 where 1 cyclic

subgroup has $13B$-elements and 13 cyclic subgroups have $13A$-elements, and injecting this group into $13A.6 \times \mathrm{L}_3(3)$ shows that the 13-elements of $\mathrm{L}_3(3)$ must have class $13B$.)

The remaining cases are dealt with as follows:

29: if we take h' to have class $3A$ then we find that g' must belong to either $14A$ or $14C$. However the former is impossible as $14A$ powers to $2A$, which is a class of 6-transpositions, so does not have two elements with product of order 29.

31: the normalizer of a 31-element has shape $31.15 \times 3C.2A$. The 3-part of the 15-element cannot have class $3C$ (as elements of this class do not centralize $2A$-elements), and the 5-part cannot have class $5A$ (as elements of this class do not centralize $3C$-elements), so the only possible class for the 15-element is $15C$.

41: use Theorem 2.

71: as remarked above, Holmes has shown that 71.35 is contained in a subgroup $\mathrm{L}_2(71)$, and Theorem 20 of [**12**] shows that the 5-elements of any $\mathrm{L}_2(71)$ have class $5B$. It follows immediately that the 35-elements have class $35B$.

This completes the proof of the theorem. □

We may also note that in all the irrational cases – $p = 23$, 31, 47, 59 and 71 – the order of g' is odd. This follows from the well known observation that all the irrationalities in the character table of the Monster are imaginary.

9. *Normalizer Moonshine*

The theme of Moonshine is the search for conceptual proofs and understanding of results that had been discovered and proved by case by case analysis which, however, seem to be more than coincidences. Is there a conceptual proof of Theorem 4?

One of the consequences of the discovery of Moonshine has been the study of Moonshine type functions, i.e. modular functions that are Hauptmoduls of groups containing some $\Gamma_0(n)$ and which are in standard form (where, in the Laurent series expansion in $q = e^{2\pi iz}$, the only term with a non-positive exponent is q^{-1}). These functions are listed in [**4**, **11**].

Most of these apppear to be simple transformations of the functions that appear in Generalized Moonshine [**8**], which correspond to pairs (g, h) of commuting elements in $\mathbb{M}$. But there are some that cannot appear in Generalized Moonshine. Examples of these are $58a$ and $82a$, which are functions of type $58|2+$ and $82|2+$ in the sense described in Theorem 4.

The first author then wondered – see [**9**] – whether these functions could be made to correspond to pairs (g, h) where h normalizes but does not centralize g. This might be called "Normalizer Moonshine", and would happen as follows.

Let g be a pure Fricke element of order p, and define an element g' satisfying the condition of Theorem 4. If h normalizes g, then whenever g is irrational, and half the time when g is rational, there is an n such that $h.g'^n$ commutes with g. In this case the function we assign to the pair (g, h) is the Generalized Moonshine function associated with $(g, h.g'^n)$.

If, however, there is no such n, then in the quotient group $N_{\mathbb{M}}(g)/g.g' \cong H.2$ h will correspond to an element in the outer half of $H.2$. If this is an involution, we assign to the pair (g, h) a modular function of type $2p|2+$. (There may be more than one such function, but in such cases there usually seems to be a "good" function to assign.)

We can then hope to assign to other pairs (g, h), where h corresponds to an element in the outer half of $H.2$, other modular functions, in such a way that the coefficient of each q^m is the value of a character of $H.2$ on the relevant element.

Unfortunately this is not always possible: for example, if g has order 19 and h is an element of order 6 which inverts g, we would expect to see a function which is congruent modulo 3 to $38a$, the unique function of type $38|2+$, but there is no such function of moonshine type other than $38a$ itself.

We also note that, as stated in [**9**], even for those pairs (g, h) for which a function can be allocated, it won't behave under combinations of the braiding operations $(g, h) \mapsto (g, gh)$, $(g, h) \mapsto (gh, h)$ (and their inverses) in the manner which one might expect from Generalized Moonshine.

Of course, when one tries to generalize a result one often has to sacrifice strength, so the above is not necessarily fatal to the concept of Normalizer Moonshine.

References

1. J. N. Bray, *An improved method for generating the centralizer of an involution*, Arch. Math. (Basel) 74 (2000), 241–245.
2. J. Conway, R. Curtis, S. Norton, R. Parker and R. Wilson, *An* Atlas *of Finite Groups* (2nd edition), Oxford University Press, 2003.
3. J. Conway and S. Norton, *Monstrous Moonshine,* Bull. London Math. Soc. 11 (1979) pp. 308-339.
4. D. Ford, J. McKay and S. Norton, *More on Replicable Functions,* Comm. Alg. 22 (13) 1994, pp. 5175-5193.
5. P. E. Holmes and R. A. Wilson, *A new computer construction of the Monster using* 2*-local subgroups*, J. London Math. Soc. 67 (2003), 349–364.
6. P.E. Holmes and R. A. Wilson, *A new maximal subgroup of the Monster*, J. Algebra 251 (2002), 435–447.
7. P. E. Holmes and R. A. Wilson, *On subgroups of the Monster containing* A_5*'s,* J. Alg. 319 (2008) no 7, pp. 2653-2667.
8. S. Norton, *Generalized Moonshine,* Proc. Symp. Pure Maths 47, AMS, (1987) pp. 208-9.
9. S. Norton, *Netting the Monster,* in *The Monster and Lie Algebras Vol. 7,* (eds. Ferrar & Harada), Walter de Gruyter and Co. 1998, pp. 111-125.
10. S. Norton, *Anatomy of the Monster: I,* Proceedings of the Atlas Ten Years On conference (Birmingham 1995), pp. 198-214, Cambridge Univ. Press, 1998.
11. S. Norton, *Moonshine-type functions and the CRM correspondence,* in *Groups and Symmetries: From Neolithic Scots to John McKay* (eds. Harnad & Winternitz), CRM Proceedings and Lecture Notes Vol. 47 (2009), pp. 327-342.
12. S. Norton and R. Wilson, *Anatomy of the Monster: II,* Proc. LMS (3) 84 (2002), pp. 581-598.
13. R. A. Wilson et al., *An Atlas of Group Representations*, http://brauer.maths.qmul.ac.uk/Atlas/.
14. R. A. Wilson, *The finite simple groups*, Springer GTM 251, 2009.
15. A. Zavarnitsine, Personal communication.

Simon P. Norton
DPMMS,
Centre for Mathematical Sciences,
Cambridge University,
Wilberforce Road,
Cambridge CB3 0WB,
U.K.

S.Norton@dpmms.cam.ac.uk

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

R.A.Wilson@qmul.ac.uk