$L_2(59)$ is a subgroup of $\mathbb{M}$.

Petra E. Holmes

and

Robert A. Wilson

School of Mathematics and Statistics,
University of Birmingham,
Edgbaston, Birmingham B15 2TT

July 17, 2002

1 Introduction

All the maximal subgroups of the 25 smallest sporadic simple groups have been determined. This only leaves the Monster to consider.

The only remaining candidates for maximal subgroups of the Monster are the normalisers of some non-abelian simple groups. Approximately 20 isomorphism types of simple groups remain to be considered (see [11]). These include $L_2(19)$ and $L_2(59)$. In some of these cases it is not known whether the simple group on question is or is not contained in $\mathbb{M}$. The group $L_2(59)$ is one of these but $L_2(19)$ is known to be contained in the $3C$ normaliser $S_3 \times Th$ [8].

The groups $L_2(59)$ and $L_2(19)$ can be generated by an A_5 intersecting a D_{20} in a D_{10}. All classes of A_5's in $\mathbb{M}$ are classified in [10]. Below is a list of these classes of A_5's. The information is taken from Table 3 of [10]. The A_5's in the first six rows are denoted by their class fusions and those in the last two rows by T and B respectively.

$(2,3,5)$ classes	$C_{\mathbb{M}}(C_{\mathbb{M}}(\mathrm{A}_5))$	$C_{\mathbb{M}}(\mathrm{A}_5)$	$C_{\mathbb{M}}(\mathrm{D}_{10})$
AAA	A_5	A_{12}	HN
BAA	$2 \times \mathrm{A}_5$	$2.\mathrm{M}_{22}.2$	2.HS.2
BBA	$\mathrm{S}_6.2$	M_{11}	2.HS.2
ACA	A_5	$\mathrm{U}_3(8).3$	HN
BCA	$2 \times \mathrm{A}_5$	$2^{1+4}(\mathrm{A}_4 \times \mathrm{A}_5)$	$2^{1+8}(\mathrm{A}_5 \times \mathrm{A}_5).2$
BCB	$5^3.(4 \times \mathrm{A}_5)$	D_{10}	$5^3.(4 \times \mathrm{A}_5)$
BBB	Th	S_3	$5^3.(4 \times \mathrm{A}_5)$
BBB	2B	2	$5^3.(4 \times \mathrm{A}_5)$

In [11], it is shown that in any subgroup of $\mathbb{M}$ isomorphic to $\mathrm{L}_2(q)$ for $q \in \{19, 27, 29, 31, 41, 49, 59, 71\}$ the elements of orders 2, 3 and 5 are in classes $2B$, $3B$ and $5B$. So their A_5's must be from the last two rows of the above list, *i.e.* of types T and B.

We consider the case where the A_5 is of T-type and prove the following results:

Theorem 1.1 *There is exactly one class of subgroups of* $\mathbb{M}$ *isomorphic to* $\mathrm{L}_2(59)$*. Each subgroup in this class is a new maximal subgroup*

and

Lemma 1.2 *All subgroups of* $\mathbb{M}$ *isomorphic to* $\mathrm{L}_2(19)$ *and containing* T*-type* A_5*'s are contained in a copy of the maximal subgroup* $\mathrm{S}_3 \times \mathrm{Th}$.

Note that it is easy to prove that there is at most one class of subgroups of $\mathbb{M}$ isomorphic to $\mathrm{L}_2(59)$, so that once we have found one containing T-type A_5's it follows immediately that there is no $\mathrm{L}_2(59)$ with B-type A_5's. We consider subgroups of $\mathbb{M}$ containing B-type A_5's in [3]. This includes the remaining possibilities for $\mathrm{L}_2(19)$'s.

1.1 Strategy

The work described here was performed using the computer construction of the Monster described in [4]. This construction allows us to calculate easily inside G, a $2B$ centraliser, but does not allow multiplication of elements outside G.

Recall that $\mathrm{L}_2(59)$ and $\mathrm{L}_2(19)$ can both be generated by an A_5 and a D_{20} intersecting in a D_{10}.

First we will find a suitable A_5 which we call A. We then find a subgroup of A isomorphic to a D_{10}, which we call D, and finally we look at all involutions extending D to a D_{20} to find which (if any) extend A to an $\mathrm{L}_2(59)$ or an $\mathrm{L}_2(19)$.

The T-type A_5's are contained in Thompson groups and all copies of Th in $\mathbb{M}$ centralise $3C$ elements [1], so we can begin by finding the $3C$ element that A centralises. We look for the $3C$-element in $G \cap C_{\mathbb{M}}(t)$ so that we generate a nice copy of Th using t and two length 0 generators for $2^{1+8} \cdot \mathrm{A}_9$. We convert these generators to their images in the representation of Th of degree 248 over $GF(3)$, then find A as a subgroup of Th generated by short words and containing an element x of order 5 given by a word of length 0.

Now consider the normaliser $D \cong \mathrm{D}_{10}$ of this 5-element in A. If we think of D_{20} as $\mathrm{D}_{10} \times 2$, it becomes clear that all the D_{20}'s which contain D can be obtained by running through the involutions in $C = C_{\mathbb{M}}(D)$. The centraliser of D is contained in the normaliser of our element x of order 5, namely $5^{1+6}{:}4\mathrm{J}_2 2$. Fortunately, we can find C without generating the latter group — all we need is a few elements inside it. Using these and an involution r inside D, we centralise r inside $N_{\mathbb{M}}(x)$ to find words generating C.

The problem now is that, although we have words generating C, we cannot easily work with these words until we convert them to their images in a more manageable representation. But since D contains the $2B$ element r it is obvious that C is contained in a $2B$ centraliser. And we know that we can calculate easily in G, the centraliser of a different $2B$ element. So if we can find a word k conjugating r to z, then we can use the word-shortening trick to get length zero words for C^k and do all our calculations in here. Section 2 gives a trick for doing just that.

Now that we can work in C, we can look for involutions extending D to a D_{20}. From [11], we know that new copies of $\mathrm{L}_2(59)$ and $\mathrm{L}_2(19)$ can only contain $2B$ elements. So we only need consider those D_{20}'s which contain only $2B$ involutions. We find all 500 of these $2B$ involutions in $C_{\mathbb{M}}(\mathrm{D}_{10})$, and use vectors to test the orders of elements in the group generated by the involution being tested and A. Twelve of the cases give us a copy of $\mathrm{L}_2(59)$, but these are all in the same class as they are conjugate under $N_{\mathbb{M}}(A) \cong \mathrm{S}_5 \times \mathrm{S}_3$.

The rest of this section gives background material from [4] and [5]. In Section 3 we describe in detail how we find the subgroup $3 \times$ Th, and in Section 4 we find the subgroup A_5. In Section 5 we find the normaliser of the D_{10}, and in Section 6 we run through the cases and draw our conclusions. Notation can be found in Section 7.

1.2 Summary of the construction

Here we recap some of the necessary material from [4].

The construction uses the 2-local subgroups and is over $GF(3)$. We first constructed two generators, c and d, for $G \cong 2_+^{1+24} {}^{\cdot}\mathrm{Co}_1$, the centraliser of an element z in class $2B$. We then restricted this group to $K \cong 2^{2+11+22} {}^{\cdot}\mathrm{M}_{24}$, the centraliser of a second involution and then extended that to $2^{2+11+22} {}^{\cdot}(\mathrm{M}_{24} \times 3)$ by adjoining an extra generator, t, which cycles the three involutions in $Z(K)$. We use five generators for K. These are a and b, which together generate $C_G(t) \cong 2^{11} {}^{\cdot}\mathrm{M}_{24}$, and three involutions u, v and w in $O_2(K)$.

Modulo the normal 2^{2+11}, the group K is isomorphic to $(2^{11} \times 2^{11})$:M_{24}. We defined three subgroups U, V and W of K so that their images in this quotient group were the two direct factors and the diagonal subgroup of the $2^{11} \times 2^{11}$. The third generator t permutes the three subgroups U, V and W, and so the involutions u, v and w were chosen from the three subgroups so that they would also be permuted by t.

The module for G has shape

$$\mathbf{298} \oplus \mathbf{98280} \oplus \mathbf{98304} \cong \mathbf{298} \oplus \mathbf{98280} \oplus (\mathbf{24} \otimes \mathbf{4096})$$

so we store each element $g \in G$ as a file containing four matrices: $g_{\mathbf{24}}$, $g_{\mathbf{298}}$, $g_{\mathbf{98280}}$ and $g_{\mathbf{4096}}$. But the restriction of **196882** to the 4-group normaliser gives a module

$$\mathbf{22} \oplus \mathbf{828} \oplus \mathbf{48576} \oplus \mathbf{147456},$$

so T could not be stored in the same format as elements of G.

Thus we store arbitrary elements as words in T and elements of G. In [5] we defined the *length* of such a word as the number of occurrences of T in it. It takes approximately six seconds × word length to multiply a vector by a word using a Pentium II/450MHz processor with 384 MB of RAM.

1.3 Shortening words

Any word w in $\mathbb{M}$ which centralises z can be written in the same format as our generators for G, *i.e.* as a file containing four matrices, $w_{\mathbf{24}}$, $w_{\mathbf{298}}$, $w_{\mathbf{4096}}$ and $w_{\mathbf{98280}}$. But these elements are frequently found as much longer words. In [5] we gave a method for converting a word w of nonzero length in $C_{\mathbb{M}}(z)$ to the corresponding length zero word given in the more useful format. This trick is of fundamental importance in our work, as it is the only method we have for shortening words and hence preventing exponential growth of the words that we need.

In [4], we constructed generators of $2_+^{1+24} \cdot \mathrm{Co}_1$ as preimages of standard generators for Co_1 in **24f2**. Then in [5] we showed how we can find $w_{\mathbf{24f2}}$ and then use the same method to give a preimage of $w_{\mathbf{24f2}}$ in **196882**. Of course, this lift will probably not be equal to w, but it can be corrected using only 13 images of vectors under w. In total, the process requires 36 vector-word multiplications - in other words, it allows us to determine the matrix $w_{\mathbf{196882}}$ by calculating less than 0.02% of its rows.

In the Section 2 we extend this trick to one which can be used to change from the centraliser of one $2B$ elmenent to another.

1.4 Condensation in the Monster

We also showed in [5] how the usual method of using condensation [9] to obtain small representations of groups from large ones can be adapted for use in our Monster construction. This relies on the subgroup to be condensed having a fair sized 2-group with a central $2B$ element.

The process of *condensation* is frequently used when computing with large modules. It replaces a module for a group algebra by a much smaller module for a related algebra, such that much of the module structure is preserved. In [5] we used the method to find a vector in a 782-dimensional submodule of the 196882-dimensional $GF(3)\mathbb{M}$-module.

Given a group algebra FG, a module V and an idempotent $e \in FG$, we construct the module eV for the algebra $eFGe$. The idempotent is usually taken to be the average of the elements in a *condensation subgroup* K, where the average is defined as $\frac{1}{|K|}\sum_{k \in K} k$. In this case, the subspace eV of V is fixed by K, as $ke = e$ and hence $keV = eV \ \forall k \in K$. Note that condensation is a functor and not a homomorphism, so condensing a generating set for FG will not necessarily give a generating set for $eFGe$. A more detailed description of condensation can be found in, for example, [9].

In our case, it is best to choose our condensation subgroup to be a subgroup of E containing z, as then the fixed subspace of **196882** has a basis of single coordinate vectors which can easily be written down. All the elements of E fix **298** and as the central element z acts as -1 on **98304**, any group containing it fixes nothing here. This only leaves **98280** to consider, but as the elements of E act as diagonal matrices on our basis for this module we can see a basis of single coordinate vectors for the fixed space here. The action of any element of G on this space can then be written down by deleting the appropriate rows and columns. This method can also be used to condense any element of $\mathbb{M}$ for which we know a word in c, d and t, as the n-th row of the matrix representing it can be obtained by multiplying row n of the identity matrix by the given word.

2 Changing post

Suppose we want to work in the centraliser of a $2B$ element i, where i is not our favourite involution z. Then we can do all calculations inside G instead of $C_{\mathbb{M}}(i)$, as long as we know a word k which conjugates i to z. We call $C_{\mathbb{M}}(i)$ the *i-post*, and *changing post* is the process of changing from one $2B$ centraliser to another.

The obvious way to find a word conjugating one involution to another is to use the dihedral trick [6]. This uses the fact that all involutions in a dihedral group of order $4n + 2$ are conjugate, and if g and h are two of these involutions then $(gh)^n$ conjugates h to g. But this method leads to excessively long words. We show below that a word of length at most 2 can be found which will conjugate i to z for any $2B$ element $i \in G$.

2.1 A conjugating word of length 2 exists

First we consider the case where $i \in E = O_2(G)$. There is a $2B$ pure 2^2 in E which contains z and whose non-trivial elements are permuted by T. This group is the centre of the group $K \cong 2^{2+11+22\cdot}\mathrm{M}_{24}$. The $2B$ elements in E lie in two orbits under G [12], both of which contain one element of $Z(K)$, so for any of these there is an element $g \in G$ which maps it into the four-group. Then we can map i to any of the three distinct elements of $Z(K)$ by using the correct one of g, gt and gt^{-1}. So conjugating i by one of the two length 1 words gt or gt^{-1} will map it to z.

Now assume $i \in G \setminus E$. We show that i can be mapped into E using a word of length 1. As we have seen, the subgroup of G which is normalised by T has shape $2^{2+11+22}\mathrm{M}_{24}$. In [4] we find three subgroups U, V and W of index 2^{11} in $O_2(K)$ which are permuted by T. These contain the three elements u, v and w. One of these subgroups, W, is contained in E but the other two both contain $2B$ elements of all the G classes which are not contained in E. So there exists an element of G which conjugates i into either U or V, then one application of T or T^{-1} will conjugate it into W, and therefore E.

We now see that a length 1 word exists which conjugates any $2B$ element of G to some element of E, and also one which will conjugate any $2B$ element of E to z. Then the product of these two words gives the length 2 word that we want.

2.2 Finding the conjugating word

Assume $i \in G \setminus E$. Here we give details on how to find the length 2 word conjugating i to z that we now know must exist.

We first find a word of length 1 which will conjugate it into E.

We use the two involutions u and $u^{(ab)^3}u$ in U. Modulo E, these elements are in Co_1 classes $2c$ and $2a$ respectively, which are the only possibilities for $2B$ elements of $G \setminus E$. We test the nullity of $i_{\mathbf{298}} + I_{\mathbf{298}}$ to find the Co_1 class of its image modulo E. The dihedral trick gives a word k_1' conjugating i to either uu'' or $u^{(ab)^3}uu''$ for some $u'' \in E$.

What we want is to conjugate i to an element of either U or V, so we now need to replace u'' by an element $u' \in (U \cup V) \cap E$. In practice this step is almost always unnecessary as we can usually take $u' = u''$ and therefore $k_1 = k_1'$, but if this method were to fail we could work in **24f2** to find an element in $C_G(u)$ (or $C_G(u^{(ab)^3}u)$) mapping the vector corresponding to u'' to an element of the spaces corresponding to U or V. The element k_1' can then be post multiplied by the new conjugator to give k_1.

Next we multiply random vectors (one will usuallly suffice!) whose first 298 coordinates are not all zeroes by both i^{k_1T} and $i^{k_1T^{-1}}$ until we find which of the two is an element of E. Denote the correct choice of conjugator by $k_1T^{\varepsilon_1}$. We then use the word-shortener to shorten $i' = i^{k_1T^{\varepsilon_1}}$ to see this element of E as a word of length zero.

This involution i' can now be converted to a vector of **24f2** using the method of [5], then we search in **24f2** to find the element $k_{2_{\mathbf{24f2}}}$ mapping it to the vector corresponding to the non-trivial element of $Z(K)/\langle z\rangle$. This element lifts to the element k_2 of G, with $i^{k_1t^{-1}k_2}$ in $Z(K)$. It then takes one application of t^{ε_2} to conjugate $i^{k_1t^{-1}k_2}$ to z, where $\varepsilon_2 = \pm 1$.

So we now have a word of length 2 given by $k = k_1t^{\varepsilon_1}k_2t^{\varepsilon_2}$ which conjugates i to z.

3 A copy of the Thompson group

The A_5 that we want is contained in the Thompson group, so we first find our Thompson group.

We find generators for Th as short words in c, d and t. Calculating with the elements that we find is impractical, so we use condensation to help obtain their images in the 248-dimensional representation of Th.

3.1 Generators for Th

We start by looking for a group $3 \times \mathrm{Th}$. The central elements of $3 \times \mathrm{Th}$ are in class $3C$ so we choose a $3C$ element, h, and find generators for its centraliser. We want t to be the only generator of non-zero length so we look for h in $C_G(t) \cong 2^{11} {}^{\cdot} \mathrm{M}_{24} \cong \langle a, b\rangle$. We choose $h = \phi_{22}(a, b)^7$.

Next we want to find h_1 and h_2 centralising h in G such that $\langle h_1, h_2\rangle \cong 2^{1+8}\mathrm{A}_9$, the involution centraliser in Th [1], and $\langle h_1, h_2, t\rangle \cong \mathrm{Th}$. The index of $C_G(t)$ in G is too large for a random search to be feasible, so we work in the subgroup of G generated by t and the $2A$-element $m = (cd)^{30}$ to find

$$h_1'' = (m\phi_{23}(m,h)\phi_{16}(m,h)tm^2)^{10}$$

and in $\langle h, m_2 = m^d\rangle$ to find

$$h_2'' = (\phi_9(m_2,h)\phi_7(m_2,h)m_2^4)^2.$$

These are only correct modulo a subgroup of E, so we use a trick from [7] to find the correct elements. The trick says that, if g has order $2n+1$ and commutes with f modulo an elementary abelian 2-group, then g commutes with $f(gg^f)^n$. Note that although this formula has been in use for years, the first published proof of it appears in [2]. We use the formula to correct the putative generators for $2^{1+8}{}^{\cdot}\mathrm{A}_9$ to

$$h_1' = h_1''hh^{h_1''} \text{ and } h_2' = h_2''hh^{h_2''}.$$

These elements t, h_1' and h_2' generate the group $3 \times \mathrm{Th}$, but to improve our chances of finding an A_5 we move down to the subgroup Th, generated by

$$t, \quad h_1 = \phi_5(h_1', h_2')h_1' \quad \text{and} \quad h_2 = h_1'h_2'h_1'.$$

Although our set of generators for Th consists of extremely short words, they are still too cumbersome to use. So we decide to convert them to their images in a smaller representation. This can be done using condensation as in Section 1.4.

3.2 A condensation subgroup for our Thompson group

We want to work in the matrix representation of Th of degree 248, denoted **248a**. We follow the method of [5] and choose a condensation subgroup contained in $E \cap \mathrm{Th} \cong 2^{1+8}$. As the group 2^{1+8} fixes nothing in **248a** and we require our condensation subgroup to have a non-trivial fixed space in the target representation, we have to use a proper subgroup of this group instead of the whole 2^{1+8}.

We work in an isomorphic 248-dimensional module for Th, denoted **248b**, taken from [15]. In here we look for subgroups of $O_2(2^{1+8}{}^{\cdot}\mathrm{A}_9)$ with non-trivial fixed spaces.

We find that one class of subgroups of index 2 in 2^{1+8} consists of groups fixing a 3-dimensional space. A group in this class will be an ideal condensation subgroup.

Now we locate one of these subgroups in $\langle h_1, h_2\rangle$. The generating set that we have for $2^{1+8}\mathrm{A}_9$ in

248b is not isomorphic to $\{h_1, h_2\}$, so we find a pair of generators, s_1 and s_2, as words in h_1 and h_2 which are isomorphic to those that we have generating $2^{1+8\cdot}\mathrm{A}_9$ in **248b**. First we find the words $s_1' = \phi_{22}(h_1, h_2)^2$ and $s_2' = \phi_{16}(h_1, h_2)h_1$ which are correct modulo the subgroup 2^{1+8}. We also find a set of generators for 2^{1+8}, $i_n = (\phi_7(h_1, h_2)^9)^{\phi_{19}(h_1,h_2)^{2(n-1)}}, 1 \leq n \leq 8$. We then correct the approximations s_1' and s_2' to give the words $s_1 = i_3 i_4 s_1'$ and $s_2 = i_2 s_2'$. Finally we obtain seven generators for our condensation subgroup H by spinning $\phi_9(s_1, s_2)^4$ under $\phi_5(s_1, s_2)$.

3.3 Condensing our Thompson group

In **196882** H has fixed space of dimension 1042. We write down a basis for this space as described in Section 1.4. Now we will use this basis to condense the group.

Recall from Section 1.4 that condensation is a functor and not a homomorphism so we cannot assume that our group generators will condense to give generators for the condensed algebra. It is even more likely that we will only generate a subalgebra when the generators are not evenly spaced throughout the group. The generating set $\{h_1, h_2, t\}$ is heavily biased in favour of the small subgroup $2^{1+8\cdot}\mathrm{A}_9$ of Th so condensing only our three generators for Th fails to give enough elements to generate the condensed algebra, and we cannot use the usual trick of condensing random elements of large order (see [9]) as we are only able to condense short words. This means that we need to condense quite a few elements of Th to see enough of the condensed algebra. We condense the elements

$$h_1,\ h_2,\ t,\ h_1t, \quad h_2t, \quad h_1th_2t, \quad h_2th_1th_2t, \quad \text{and} \quad h_1th_1th_2t.$$

This gives a module **1042** for the condensed algebra $e\mathbf{196882}\mathbb{M}e$, where e is the average of the elements in H. We then use the Meataxe [13] to chop **1042** and find a vector in a 3 dimensional subspace. Converting this vector to an element of 196882-dimensional space and spinning this under the generators for Th gives a basis for **248a**. We then write h_1, h_2 and t with respect to this basis.

We now have images of h_1, h_2 and t as three 248×248 matrices generating Th, and we can work in this representation to find words for the A_5 that we need.

4 Generating A and D

We find words generating a copy of A_5 in Th and also a D_{10} inside it. Both these words are impractical so we replace them with shorter ones using methods from Section 1.3.

4.1 Finding A

We to find the group $A \cong \mathrm{A}_5$ inside Th as follows.

A presentation for A_5 is $\langle X, Y | X^5, Y^2, (XY)^3 \rangle$. We look for short words satisfying this presentation. We use a length zero word $x = (\phi_4(h_1, h_2))^6$ in $\mathbb{M}$ class $5B$ as one generator and look for a conjugate z^g of the involution z to be the second generator, looking for a product xz^g of order 3. This is a large but manageable search — the probablility of success at each attempt is about 3×10^{-5}. We find the two generators for A, namely x and

$$y = z^{t\phi_4(h_1,h_2)\phi_{12}(h_1,h_2)t\phi_{13}(h_1,h_2)\phi_{15}(h_1,h_2)t^{-1}\phi_{12}(h_1,h_2)\phi_{11}(h_1,h_2)t\phi_4(h_1,h_2)h_1th_1^2t^{-1}(\phi_{22}(h_1,h_2)\phi_{13}(h_1,h_2))^{-1}}.$$

The word for y can be shortened immediately as the subword

$$y' = z^{t\phi_4(h_1,h_2)\phi_{12}(h_1,h_2)t\phi_{13}(h_1,h_2)\phi_{15}(h_1,h_2)}$$

centralises z and so is contained in G. So we can write y' as a word of length zero using the method of Section 1.3. This gives

$$y = y'^{t^{-1}\phi_{12}(h_1,h_2)\phi_{11}(h_1,h_2)t\phi_4(h_1,h_2)h_1th_1^2t^{-1}(\phi_{22}(h_1,h_2)\phi_{13}(h_1,h_2))^{-1}}.$$

We then further abbreviate y by finding the word

$$j = (u(yz)^{14})^4 t(cd)^{30}c(cd)^{-34}\phi_{14}(c, d)^{-41}t$$

(see Section 2) conjugating y to y'', a word of length zero, and we write y as $y''^{j^{-1}}$.

4.2 Generators for D

Inside A, we find an involution $r = y^{\phi_9(x,y)}$ extending x to a D_{10}, which we denote D. There are 8 occurrences of y in $\phi_9(x, y)$, so, even using the shortened version of y, this gives a word of length 32 for r. We will need to use r frequently and so we cannot possibly afford to use this word. We must find one which is much shorter.

In fact, if we can find a $2B$ element centralising both r and z then we can write r as a word of length 4. We do this by finding a length 2 word k which conjugates the new involution to z. Then we write $r' = r^k$ as a word of length zero, and hence write r as the word of length 4, $r = r'^{k^{-1}}$.

The dihedral trick [6] is a well known method of finding involutions that centralise other involutions.

A dihedral group is generated by two involutions and if it is of twice even order it has a central involution. We use this fact below.

We work inside **248a** where we find that rz has order 10, and so the element $(rz)^5$ is a $2B$ involution in $G \cap C_{\mathbb{M}}(r)$ (there are no $2A$'s in Th). We use the word-shortening trick to write $(rz)^5$ as a word of length zero. Then the method of Section 2 provides an element conjugating $(rz)^5$ to z given by the length 2 word

$$k = \phi_{12}(c,d)(u(rz^5)^{\phi_{12}(c,d)})^{10}t^{-1}\phi_{10}(c,d)^3c^2(\phi_{12}(c,d)^{11}(cd)^8c)^{-1}t^{-1}.$$

This gives us our word of length 4, $r = {r'}^{k^{-1}}$.

5 A subgroup of $C_{\mathbb{M}}(D)$ generated by involutions

We want to find all involutions extending D to a copy of D_{20}. These involutions can all be seen inside the subgroup $C \cong 5^{3{\cdot}}(2 \times \mathrm{A}_5)$ of index 2 in $C_{\mathbb{M}}(D) \cong 5^{3{\cdot}}(4 \times \mathrm{A}_5)$.

Of course, C must centralise both x and r as these two elements generate D, so we first extend D to a larger subgroup of $N_{\mathbb{M}}(x)$ then centralise r inside this subgroup. This gives a group $2 \times C$ inside which we find C. If we consider the generators of C as long words involving r then there is no obvious way to check whether or not we have generated the whole of C, so before even starting to look for C we change post to $C_{\mathbb{M}}(r)$. This post is the best vantage point from which to study C as $C \leq C_{\mathbb{M}}(r)$ and so all elements of C have length zero in the r-post.

5.1 A subgroup of $N_{\mathbb{M}}(x)$

We now find a selection of elements of $N_{\mathbb{M}}(x) \cong 5^{1+6}{:}4\mathrm{J}_2{\dot{}}2$. The easiest elements to find are those contained in the subgroup $N_G(x)$. The image of x in G/E is in Co_1 class $5a$ so $N_G(x) \cong (5 \times 2\mathrm{J}_2){:}4$.

We find $N_G(x)$ using the same method that we used in Section 3.1 to find $C_G(h)$. We use the element of order 2, $m_1 = (cd)^{20}$ to get the intermediate generators

$$m_2 = m_1^{\phi_{13}(c,d)dc}, \quad m_3 = m_1^{\phi_{19}(c,d)dc} \quad \text{and} \quad m_4 = m_1^{\phi_{20}(c,d)d^2}$$

which we use to find

$$n_1' = (\phi_{18}(x,m_2)xm_2x^2)^3, \quad n_2' = (\phi_{10}(x,m_3)\phi_8(x,m_3)xm_3x)^2$$

$$\text{and} \quad n_3' = \phi_{14}(x,m_4)\phi_{12}(x,m_4)\phi_{10}(x,m_4)\phi_6(x,m_4)\phi_{19}(x,m_4)\phi_{17}(x,m_4)$$

which are correct modulo E. These are corrected to give

$$n_1 = n_1'(x^{n_1'}x)^3, \quad n_2 = n_2'(x^{n_2'}x)^3 \quad \text{and} \quad n_3 = n_3'(x^{n_3'}x^2)^3,$$

which generate $N_G(x)$. The elements n_1 and n_2 both centralise x and n_3 maps x to x^2. As $r \notin G$ we have $N_G(x) < \langle n_1, n_2, n_3, r\rangle \leq N_{\mathbb{M}}(x)$

5.2 The r-post

Now we want to work in $C_{\mathbb{M}}(r)$.

In Section 2 we learn how to conjugate $2B$'s in G to z. This trick becomes even more valuable when it is used twice. If i_1 is a $2B$ in G and i_2 a $2B$ in $C_{\mathbb{M}}(i_1)$, then we can change post once to $C_{\mathbb{M}}(i_1)$, then use the trick a second time to conjugate i_2 to i_1. Now multiply the two conjugating words together, and it is clear that we have successfully found a word of length at most 4 conjugating i_2 to z.

Recall that we have an element $r' = r^k$ which centralises both r and z, and that we can conjugate any $2B$ involution in G to z using a conjugating word of length at most 2. So we use the method of Section 2 to find a length 2 word l conjugating r' to z, where l is given by

$$l = \phi_5(c,d)(u(rz^5)^{\phi_5(c,d)})^{10}t\phi_{12}(c,d)^{17}d^2c(\phi_9(c,d)^{12}(cd)^{37}c)^{-1}t.$$

Then the word kl conjugates r to z, and we can calculate in $C_{\mathbb{M}}(r)$ by working in the conjugate group $(C_{\mathbb{M}}(r))^{kl} = G$.

5.3 Generators and a representation of C

It is well known that the dihedral trick [6] can be used to find involution centralisers. All it requires is a supply of random involutions from the group that we are looking in. We can use this trick to find enough of the centraliser of r in $N_{\mathbb{M}}(x)$, using involutions from the subgroup $N_G(x)$ found above. Of course, the involutions in $N_G(x)$ are far from random as they all lie inside the same subgroup of $N_{\mathbb{M}}(x)$, but we find that they are random enough for our purposes.

Each generator that we find will be conjugated by kl and shortened. This will result in a generating set for C^{kl} consisting of length zero words, and hence an isomorphic copy of C that is easy to calculate in. The shortening process is time consuming (approximately 6 minutes × length of word to be shortened, plus 45 minutes for overheads), so it is important to discard any redundant generators before putting them into the new post. We test for redundancy of each new generator g by testing the presence of the image of the first coordinate vector v_1 under g^{kl} in the orbit of the already-found subgroup of C^{kl} on v_1, as this is an orbit that can be efficiently calculated and stored by working in **298**.

Here we find generators t, g_1', g_2', g_3', g_4' and g_5' for $2 \times C$. Two obvious generators are h and $g_1' = (rz)^5$. The dihedral trick then gives us

$$g_2' = (r((\phi_8(n_1,n_2))^{30})^{\phi_3(n_1,n_2)})^5 \qquad g_3' = (r((\phi_8(n_1,n_2))^{30})^{\phi_9(n_1,n_2)})^5$$
$$g_4' = (r((\phi_8(n_1,n_2))^{30})^{\phi_4(n_1,n_2)})^5 \qquad g_5' = (r((\phi_8(n_1,n_2))^{30})^{\phi_{11}(n_1,n_2)})^5.$$

The generators g_i', $1 \leq i \leq 5$, of the previous subsection were all found as the product of one element centralising x and one (*i.e.* r) inverting x, all raised to the power 5. Elements found in this way must invert x as 5 is odd. So we multiply these elements by r to convert them to the elements $g_i \in C_{\mathbb{M}}(D)$, $1 \leq i \leq 5$. Then C is generated by t, g_1, g_2, g_3, g_4 and g_5.

We then obtain a permutation representation **750P** of C^{kl}, a summand of dimension 750 of **196560P**. This 750 dimensional representation is faithful, as **196560P** is a faithful representation of $G/Z(G)$, and the central involution z is not contained in C^{kl}.

Now we have easy access to any involution in $C_{\mathbb{M}}(D)$ as these are all contained in C so we are ready to move on to the next section in which we search through the involutions in C for one which will extend A to a copy of $\mathrm{L}_2(59)$.

6 Finding $\mathrm{L}_2(59)$ and $\mathrm{L}_2(19)$

We can construct $\mathrm{L}_2(59)$ and $\mathrm{L}_2(19)$ as amalgams of A and a D_{20} intersecting in D. To do this we must extend D up to a D_{20}, which can be done by adjoining any involution in C as $\mathrm{D}_{20} = 2 \times \mathrm{D}_{10}$.

Any involution in C will extend D to a D_{20}. Recall that C has shape $5^{3\cdot}(2 \times \mathrm{A}_5)$. By looking at $C/5^3$, we can see that there are 3 classes of involutions in this group. It turns out that two of them fuse to Monster class $2B$ and one to Monster class $2A$. Any copy of $\mathrm{L}_2(59)$ can only contain elements of Monster class $2B$ so we can discard one of the three classes. This leaves us with 500 involutions to consider. We work in the permutation representation **750P** to find words for all these involutions.

The involutions lie in orbits under conjugation by $C_{\mathbb{M}}(A) \cong \mathrm{S}_3$, and all involutions in the same orbit will extend A to groups in the same conjugacy class of $\mathbb{M}$. We are only interested in involutions lying in regular orbits under the S_3, as by the orbit-stabiliser theorem these are the only ones which will extend A to a group with trivial centraliser, and all subgroups with non-trivial centraliser must already be contained in known maximal subgroups.

Before we can calculate the orbits we need to find generators for $C_{\mathbb{A}} \cong \mathrm{S}_3$ in C. We already know that the known element h centralises A and we also know that the involutions of the S_3 are all in class $2A$ of $\mathbb{M}$. We find that there is only one copy of S_3 in $C_{\mathbb{M}}(A)$ containing both h and elements in class $2A$, and we can generate this using h and the involution $s = ((g_1 g_2)^5)^{g_5 g_4 g_2 g_1}$.

We make the orbits of $\langle s, h\rangle$ on the involutions and choose a representative of each orbit as the involution to be checked. Note that each involution has the same length (four) as they are all of the form $f^{kl^{-1}}$ for some length zero word f in g_1^{kl}, g_2^{kl}, g_3^{kl}, g_4^{kl}, and g_5^{kl}.

6.1 Results

We test the cases and find one conjugacy class of $\mathrm{L}_2(59)$'s and one of $\mathrm{L}_2(19)$'s. Each of the involutions extending A to a copy of $\mathrm{L}_2(19)$ is contained in an orbit of length 1 under $C_{\mathbb{M}}(A)$, telling us that each copy of $\mathrm{L}_2(19)$ in this class has centraliser S_3 and is contained in a copy of the Thompson group. This proves Lemma 1.2.

A word for an involution extending A to $\mathrm{L}_2(59)$ is given by $i = g_2^{g_1 g_2 g_4 g_5}$. From [11], we know that if any copy of $\mathrm{L}_2(59)$ exists then it must be unique. We also know that any copy must be self-normalising [1]. So we have now proved Theorem 1.1.

We can now determine the class fusion of the class of $\mathrm{L}_2(59)$'s as there are several possible class fusions for $\mathrm{L}_2(59)$'s given in [11]. The unknown classes are those consisting of elements of orders 10 and 30. We choose an element of order 10 lying inside the D_{20} and centralising the involution that we have just found. We change post to $C_{\mathbb{M}}(i)$ so that we can see a length zero conjugate to this 10-element. We can then calculate the fixed space of the element, which shows that it is class $10E$ and that the elements of order 30 are therefore in class $30G$ as this is the only class of elements of order 30 which power up to class $10E$ and class $3B$.

7 Index of Notation

Here is a list of the notation which is used frequently throughout, together with brief definitions. All modules are over $GF(3)$ unless stated otherwise.

7.1 Modules

We denote the image of an element x in the representation $\mathbf{n}$ by $x_{\mathbf{n}}$. We also abuse notation a little by defining $x_{\mathbf{4096}}$ as “the image of some element x' in **4096**, where x' is a preimage of x in the double cover of $G = 2_+^{1+24\cdot}\mathrm{Co}_1$” for $x \in G$, and similarly for $x_{\mathbf{24}}$. This is because both of these are modules for $2G$ and not for G itself, although they are referred to because their tensor product, **98304**, is a module for G.

22	a module for M_{24}
24	a module for $2\mathrm{Co}_1$
24f2	a module for Co_1 over $GF(2)$
248a	a submodule of $\mathbf{196882}_{\mathrm{Th}}$
248b	amodule isomorphic to **248a** taken from [15]
298	a module for Co_1
750P	a permutation representation of C
850	a module for $2^{22}{:}(\mathrm{M}_{24} \times 3)$
1042	the fixed space of H
4096	a module for a group $2_+^{1+24}\mathrm{Co}_1$ not isomorphic to G
98280	a monomial representation of $2^{24\cdot}\mathrm{Co}_1$
98304	$\mathbf{24} \otimes \mathbf{4096}$
147456	a monomial representation of $2^{2+11+22\cdot}(\mathrm{M}_{24} \times 3)$
196560P	a permutation representation of $2^{24\cdot}\mathrm{Co}_1$
196882	the module for $\mathbb{M}$
P	a permutation representation of Co_1 on 98280 points

7.2 Words

The following words are used frequently throughout. They are implemented in some versions of the MeatAxe [13], [14] in the function “fro”. These are:

$$
\begin{array}{rcl@{\qquad}rcl}
\phi_1(g,h) & = & g & \phi_{12}(g,h) & = & \phi_3(g,h)\phi_{11}(g,h) \\
\phi_2(g,h) & = & h & \phi_{13}(g,h) & = & \phi_{12}(g,h)\phi_3(g,h) \\
\phi_3(g,h) & = & gh & \phi_{14}(g,h) & = & \phi_{13}(g,h)\phi_4(g,h) \\
\phi_4(g,h) & = & gh^2 & \phi_{15}(g,h) & = & \phi_{14}(g,h)\phi_4(g,h) \\
\phi_5(g,h) & = & ghgh^2 & \phi_{16}(g,h) & = & \phi_5(g,h)\phi_{15}(g,h) \\
\phi_6(g,h) & = & (gh)^2gh^2 & \phi_{17}(g,h) & = & \phi_{16}(g,h)\phi_5(g,h) \\
\phi_7(g,h) & = & (gh)^2gh^2gh & \phi_{18}(g,h) & = & \phi_{17}(g,h)\phi_3(g,h) \\
\phi_8(g,h) & = & gh(ghgh^2)^2 & \phi_{19}(g,h) & = & \phi_4(g,h)\phi_{18}(g,h) \\
\phi_9(g,h) & = & (gh)^2(ghgh^2)^2 & \phi_{20}(g,h) & = & \phi_{19}(g,h)\phi_3(g,h) \\
\phi_{10}(g,h) & = & (gh)^2(ghgh^2)^2gh^2 & \phi_{21}(g,h) & = & \phi_{14}(g,h)\phi_{15}(g,h) \\
\phi_{11}(g,h) & = & \phi_{10}(g,h)\phi_4(g,h) & \phi_{22}(g,h) & = & \phi_9(g,h)\phi_{12}(g,h)
\end{array}
$$

$$\phi_{23}(g,h) = \phi_7(g,h)\phi_8(g,h)$$

7.3 Miscellaneous

A	an A_5
a, b	generators for $C_G(T) \cong 2^{11\cdot}\mathrm{M}_{24}$
C	a subgroup $5^{3\cdot}(2 \times \mathrm{A}_5)$ of $C_{\mathbb{M}}(D)$
c, d	generators for G
D	a D_{10} in A
E	$O_2(G) \cong 2_+^{1+24}$
G	$C_{\mathbb{M}}(z) \cong 2_+^{1+24\cdot}\mathrm{Co}_1$
$g_1, \ldots, g_5$	generators for C
H	the condensation subgroup of Th
h	a $3C$ element centralising A
h_1, h_2	centralise t and generate $2^{1+8\cdot}\mathrm{A}_9$
k	conjugates r to r'
K	$C_{\mathbb{M}}(2B^2) \cong 2^{2+11+22\cdot}\mathrm{M}_{24}$, normalised by t
l	conjugates r' to z
length	number of occurrences of t in a word
n_1, n_2, n_3	generators for $(5 \times 2\mathrm{J}_2){:}4$, a subgroup of $N_G(x)$
post	a $2B$ centraliser
r	an element of order 2 in D
r'	a length zero conjugate of r
s	a generator of $C_{\mathbb{M}}(A) \cong \mathrm{S}_3$
t	the third generator of $\mathbb{M}$
u, v, w	involutions in $O_2(K)$ extending $\langle a, b\rangle$ to K
U, V, W, Z	subgroups of $O_2(K)$ containing u, v, w
x	an element of order 5 in D
y	a generator of A
z	the central involution in G

References

[1] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson. *Atlas of finite groups.* Clarendon Press, Oxford, 1985.

[2] P.E. Holmes. Computing in the Monster. *PhD Thesis,* Birmingham 2002.

[3] P.E. Holmes. Some new subgroups of $\mathbb{M}$ with A_5's in. *in prep.*.

[4] P.E. Holmes and R.A. Wilson. A new computer construction of the Monster using 2-local subgroups. *J. London Math. Soc.,* to appear.

[5] P.E. Holmes and R.A. Wilson. A new maximal subgroup of the Monster. *J. Algebra,* to appear.

[6] P. B. Kleidman and R.A. Wilson. The maximal subgroups of J_4. *Proc. London Math. Soc.* , 56(3):484-510, 1988.

[7] S. A. Linton. The art and science of computing in large groups. *Computational algebra and number theory,* (Sydney, 1992), 91–109.

[8] S. A. Linton. The maximal subgroups of the Thompson group. *J. London Math. Soc.,* 39(2):79–88, 1989.

[9] K. Lux and M. Wiegelmann. Condensing tensor product modules. In R.A. Wilson and R.T. Curtis, editors, *The Atlas of finite groups: ten years on*, volume 249 of *London Math. Soc. Lecture Note Ser.*, pages 198–214. (CUP), 1985.

[10] S.P. Norton. Anatomy of the Monster, I. In R.A. Wilson and R.T. Curtis, editors, *The Atlas of finite groups: ten years on*, volume 249 of *London Math. Soc. Lecture Note Ser.*, pages 198–214. (CUP), 1985.

[11] S.P. Norton and R.A. Wilson. Anatomy of the Monster, II. *Proc. London Math. Soc.* 84 (2002), 581-598.

[12] S.P. Norton. Character table of $2_+^{1+24\cdot}\mathrm{Co}_1$. *Personal communication.* Now included in the GAP character table library.

[13] R.A. Parker. The computer calculation of modular characters (the Meat-Axe). In Computational Group Theory (Durham), *Editor, M.D. Atkinson, pages 267-274. Academic Press, London-New York, 1982*

[14] M. Ringe. The C MeatAxe. *Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, release 1.5 edition, 1995*

[15] R.A. Wilson *et al.* A World-Wide-Web Atlas of group representations. http://www.mat.bham.ac.uk/atlas.