Computing in the Monster

Robert A. Wilson

July 17, 2002

Abstract

We give a survey of computational methods and results concerning the Monster sporadic simple group.

There are now three computer constructions of the Monster which are proving effective in answering real questions about this group. The first construction over the field of two elements is the fastest for calculations, and has been used to show the group is a Hurwitz group.

The second construction over the field of three elements, uses an involution centralizer as the heart of the construction, and has proved to be the most useful as far as calculations with subgroups is concerned. P. E. Holmes has used this construction to find explicitly four new conjugacy classes of maximal subgroups, as well as to eliminate various other possibilities for maximal subgroups.

The third construction over the field of seven elements uses the same generators as the first construction, which means that elements given as words in these generators can be investigated modulo 2 and modulo 7 simultaneously. This gives enough information in most cases to determine the conjugacy class of the element.

1 Introduction

The Monster is the largest of the 26 sporadic simple groups, and is of great interest for a variety of reasons, not least its still mysterious connections with modular forms, and quantum field theories. Until recently, its immense size has been a serious barrier to computation in the group. Thus it was too big for a computational existence proof, and its existence had to be proved 'by hand' [2] (see also [1]). Determination of maximal subgroups also had to proceed by theoretical arguments [15, 11, 12, 14].

The smallest matrix representations of the Monster have dimension 196882 in characteristics 2 and 3, and dimension 196883 in all other characteristics. Thus the smallest matrices which we could conceivably use to generate the Monster would require around 5GB of storage each, and on modern workstations with

the best available algorithms it would take several weeks of processor time to multiply two such matrices.

Despite these obvious difficulties, I decided some years ago to attempt an explicit construction of these matrices, with no hope of ever being able to use them for any serious calculation. With the collaboration of Richard Parker, Peter Walsh and Steve Linton, this project was eventually successful [10]. The generating matrices were stored in a compact way, so that all the information and special programs needed would fit onto a single 1.44MB floppy disk. This construction was in characteristic 2 for speed, and therefore proceeded by gluing together 3-local subgroups.

However, it soon transpired that these 3-local subgroups were too small to contain many useful subgroups with which to attack the maximal subgroup problem, so I began an analogous construction in characteristic 3, using the much larger 2-local subgroups. This was eventually completed by Beth Holmes [6], who then used the construction to obtain a complete classification of subgroups of the Monster isomorphic to $L_2(23)$. This major achievement was then quickly followed by 10 more such classifications, each more astonishing than the last, including the discovery of four previously unknown maximal subgroups [7, 8, 3].

In the meantime, I had produced a third construction, in characteristic 7, again using the 3-local subgroups. The idea behind this is that the generators are the same as in the characteristic 2 construction, so that one can obtain information about elements 'modulo 14'. In particular, one can calculate character values modulo 14, in order to provide good conjugacy class invariants.

2 The 2-local construction

We present first the 2-local construction, as it is easier to describe than the earlier 3-local construction, and is closely related to the Griess construction [2]. We give only an overview, and refer the reader to [6] for details. The idea is to start with a subgroup $2^{1+24}{\cdot}Co_1$, which is one of the involution centralizers in the Monster. The 3-modular irreducible representation of degree 196882 for the Monster restricts to this subgroup as the direct sum of three irreducibles, of degrees 98304, 98280 and 298. The constituent of degree 298 is a representation of the quotient Co_1, obtained from the 24-dimensional Leech lattice representation of the double cover $2{\cdot}Co_1$ by taking a trivial representation off the top and bottom of the symmetric square. The constituent of degree 98280 is monomial, and can easily be constructed again from the Leech lattice. Finally, the constituent of degree 98304 is the tensor product of representations of the double cover, of degrees 24 (the Leech lattice again) and 4096 (obtained by a Clifford algebra construction from the Leech lattice).

Thus an element of this subgroup can be specified by three matrices (over $GF(3)$, or more generally, any field of characteristic not 2), of sizes 24, 4096, and

298, and a monomial permutation on 98280 points. In particular, the storage requirement for each element is around 3.6MB, rather than the 7.4GB required for a 196882×196882 matrix over $GF(3)$. Moreover, elements of this subgroup can be multiplied together relatively easily—the most time-consuming part of the calculation is multiplying together the 4096×4096 matrices, which takes around a minute, depending on hardware and software. Most importantly for the sequel, however, is that there is an easy algorithm for calculating the image of a vector of length 196882, under one of these elements. This takes less than a second.

Now to produce an element of the Monster not in this subgroup, we first centralize a second involution, and use a 'standard basis' method to conjugate the first involution to the second, normalizing the four-group they generate. It turns out that the conjugating matrix can be chosen to be one of two particular matrices, and it is easy to check that one of them does not extend our involution centralizer to the Monster, and therefore the other one does. This of course relies on the existence of the Monster, and of this particular representation. An independent existence proof using this explicit construction has not been attempted.

By careful change of basis in the representations described above, we can ensure that the final element is reasonably sparse. It turns out that we can write it as a monomial permutation on 147456 points, followed by 759 identical 64×64 matrices, and an 850×850 matrix. This takes up around 0.7MB, and the image of a vector under this element can be calculated in a fraction of a second.

It is important to realise that only the generators of the Monster can be stored in one of these two compact formats. For this purpose, we can regard every element of the involution centralizer $2^{1+24} \cdot Co_1$ as a generator. But every element of the Monster outside this subgroup has to be stored as a word in these generators and the final generator. Thus multiplying group elements together involves concatenating words, and can be problematical as unrestrained multiplication rapidly results in words which are too long to be useful. We shall see in Section 6 some techniques we have used to get around this major problem.

3 The 3-local constructions

The first computer construction of the Monster [10] was designed to produce the matrices over $GF(2)$, since calculation with such matrices is much faster than with matrices over any other field. The disadvantage, however, is that the maximal 2-local subgroups are no longer available as ingredients of the construction. Thus we decided to use maximal 3-local subgroups instead. Here again we give only a sketch of the construction, and refer to [10] for details.

We began with the normalizer of a cyclic group of order 3, generated by a $3B$-element. This group has the shape $3^{1+12} \cdot 2 \cdot Suz{:}2$. The restriction of the representation to this subgroup consists again of a tensor product part, a monomial part, and a small part. The small part is obtained by tensoring the complex

Leech lattice with its dual, reducing modulo 2, and taking a trivial module off the top and bottom—the result is an irreducible representation of degree 142 over $GF(2)$.

The 'monomial' part is really only monomial for a subgroup of index 2, over the extension field $GF(4)$. Thus for the whole group it is induced from a 2-dimensional representation of a subgroup of index 32760.

The 'tensor product' part is again not exactly a tensor product: if we restrict to the subgroup of index 2, it is the direct sum of two (dual) tensor products over $GF(4)$, each tensor being the product of one 90-dimensional and one 729-dimensional representation. The latter is the natural irreducible representation of the split extension $3^{1+12}{:}2{\cdot}Suz$, while the former is an indecomposable unitary module for $6{\cdot}Suz$, with constituents of degrees 12, 66 and 12.

These technicalities greatly complicate the construction, as the underlying field is sometimes of order 2, and sometimes of order 4, and the field automorphism needs special treatment. Moreover, the construction of the 90-dimensional indecomposable module was quite difficult. Once these technical difficulties were overcome, however, we ended up with an efficient calculating tool for the Monster. The storage requirement for an element in our subgroup is around 270kB, as opposed to around 5GB for a full-size matrix.

As in the case of the 2-local construction, we can treat all elements of the subgroup $3^{1+12}{\cdot}2{\cdot}Suz{:}2$ as generators, and we just need to find one other generator for the Monster. We chose another element of class $3B$, inside the normal 3-subgroup, and used a standard basis technique to find an involution swapping these two elements of order 3. By testing random products, we found the one possibility (out of 8) which extended our 3-normalizer to the Monster.

Again, by careful choice of basis we were able to write this extra element as a combination of a 'monomial' permutation on 87480 subspaces of dimension 2, two 324×324 matrices (repeated 11 and 55 times respectively), and a 538×538 matrix. The storage requirement is around 420kB for this generator.

A similar calculation can be done over any field of characteristic not 3, although it is easier if there is a cube root of unity in the field. For this reason, we repeated the calculations over the field of order 7, and obtained the same set of generators for the Monster in this different representation [17]. Over fields of characteristic bigger than 3, the dimension is 196883, as there is only one copy of the trivial module in the tensor product of the complex Leech lattice with its dual, modulo primes bigger than 3.

4 Basic calculations

In any of the above constructions, the basic operation that we can perform is to multiply a vector by a generator of the Monster. We can also work inside our chosen maximal subgroup to create new generators in this subgroup. An element

of the Monster is stored as a word $x_1 t_1 x_2 t_2 \ldots$, where the x_i are in our maximal subgroup, and the t_i are equal to the extra generator (or its inverse, in the 2-local version).

An estimate of the order of the element represented by such a word is obtained by taking a 'random' vector, and applying the letters of the word in order, repeatedly until the original vector is returned. The number of times the word is scanned is then a divisor of the order of the element, and is extremely likely to be exactly that order.

To improve this estimate to an exact calculation, we pre-calculate two vectors, one of which is fixed by an element of order 71, while the other is fixed by an element of order 47 but not by an element of order 94. These were found by finding elements whose estimated orders were 71 and 94, so that their exact orders are also 71 and 94 (as the Monster has no elements of order more than 119), and adding up the 71 images of a random vector under the first, and the 47 images of a vector under the square of the second element. Now it is easy to show that no non-trivial element of the Monster fixes both of these vectors. Therefore the exact order of an element can be calculated by passing both of these vectors through the given word.

5 Random searches

The first serious calculations we attempted with the first (3-local) construction were to try to improve estimates for the symmetric genus of the Monster. By character calculations and using partial information on maximal subgroups, Thompson had shown that the Monster was a quotient of the triangle group $\Delta(2,3,29) = \langle x, y, z \mid x^2 = y^3 = z^{29} = xyz = 1 \rangle$, but the challenge was to find the minimal value of n such that the Monster is a quotient of $\Delta(2,3,n)$.

It was easy enough to find elements of orders 2 and 3, in classes $2B$ and $3B$, inside our maximal subgroup. We then wrote down a long list of conjugates of these two elements, and checked the order of the product in each case. It did not take long to find products of order less than 29, and then to check many words in the given conjugates, to verify that they did in fact generate the Monster. By this method we quickly reduced the value of n to around 17.

The ultimate aim, however, was to reduce n to 7: from Norton's work on maximal subgroups [12] it seemed very likely that this was the minimal possible value. However, the probability that a random pair has product of order 7 is of the order of 10^{-8}, so we would need to look at around 100 million pairs to have a reasonable chance of success. This we did, using some 10 years of processor time. See [16] for more details.

6 Advanced calculations

The main difference between calculating in a group given by generators as matrices or permutations, and calculating in the Monster where elements are given as words in the generators, is that if you are not careful the elements you need are given by words whose length increases exponentially with time. Without a method of shortening words it is impossible to use standard methods for finding elements and subgroups with the required properties. This is the main reason, apart from sheer size, why we originally considered serious calculation in this group to be essentially impossible.

However, with experience, we found two methods of overcoming this obstacle. The first trick is a method of conjugating one involution to a commuting involution, by a short word. As we were initally tied to the given involution centralizer, this was called the 'post', so this method of conjugating one involution to another was dubbed 'changing post'.

The second trick, which is really the crucial ingredient which enables us to calculate in the Monster almost as easily as in a small matrix group, is a method of shortening words. Specifically, if we find a word in the generators, which commutes with the original $2B$-element, then it belongs to the original subgroup $2^{1+24}{\cdot}Co_1$. Therefore it can be written in the shorthand form as a combination of a 24×24 matrix, a 4096×4096 matrix, a monomial permutation on 98280 points, and a 298×298 matrix. It turns out that this shorthand form can be determined by calculating just 36 rows of the full 196882×196882 matrix for this element. Thus provided the word for this element is not too long, this standard form can be calculated fairly quickly.

By combining this trick with Ryba's method [5] for conjugating an involution in a group to an involution in a known subgroup, we can in principle shorten any word to one of length less than about 20. In practice, however, this is still too slow for arbitrary words, and its effective use is confined to the case described above. Details can be found in Holmes's Ph. D. thesis [3] (see also [7]).

The first trick is less elegant, but no less effective. It relies on the fact that all $2B$-elements in $2^{1+24}{\cdot}Co_1$ can be obtained from the central involution by a subset of the operations: (1) conjugate by t to make it a non-central involution of 2^{1+24}, (2) conjugate by an element of $2^{1+24}{\cdot}Co_1$, (3) conjugate by t again to move it outside 2^{1+24}, and (4) conjugate again by an element of $2^{1+24}{\cdot}Co_1$. The method of conjugating an arbitrary $2B$-element in this group to the central involution, basically consists of one application of the well-known dihedral group trick to conjugate our involution to a pre-calculated one in the quotient Co_1, and one random search in the Leech lattice, to find the correct conjugating elements to reverse the above operation. See [3] or [8] for details.

Another important principle for calculating in large groups is to do the required calculations in a proper subgroup if at all possible. In many places we need to work in particular subgroups to search for the particular elements we require.

It is necessary therefore to find suitably small representations of these subgroups in which to perform such calculations. In some cases we created a permutation representation by permuting the images of a carefully chosen vector. In most cases, however, we chopped a suitable submodule out of the 196882-dimensional module using a type of condensation technique specifically adapted for the special form of the representation.

7 Maximal subgroups

The most effective method of classifying maximal subgroups of large simple groups in a computational setting is to choose an abstract amalgam generating the desired isomorphism type of subgroup, and to classify all embeddings of that amalgam in the large simple group. We then look at each embedding to decide whether it indeed generates the required subgroup.

For example, if we wish to classify subgroups isomorphic to $L_2(23)$, we use the fact that this group can be generated by the Borel subgroup 23:11 and the normalizer D_{22} of a torus, intersecting in the torus (of order 11). Thus we first find all types of 23:11 in the Monster (there is only one, up to conjugacy, and it can be found inside the involution centralizer). Next we find the normalizer of the cyclic group of order 11. This is in general not so easy, but in this case we find that, by choosing the element of order 23 carefully, it is generated by the part which is in the involution centralizer, and the extra generator t of the Monster. It is therefore possible to generate all necessary elements, that is the involutions inverting the element of order 11, by short words in the Monster generators. As a result we are able to investigate with relative ease the groups so generated, and find the unique conjugacy class of subgroups of the Monster which are isomorphic to $L_2(23)$. Moreover, we can use the normalizer of the cyclic group of order 23 to show that every $L_2(23)$ in the Monster centralizes a group S_3, and therefore its normalizer is inside the maximal subgroup $3{\cdot}Fi_{24}$.

Other isomorphism types of simple subgroups of the Monster are not so easy to classify. The most successful calculation so far has been the classification of subgroups generated by two copies of A_5 intersecting in D_{10} (see [3, 8, 9]). This amalgam can generate $L_2(q)$, for any $q \equiv \pm 1 \pmod 5$, as well as $L_3(4)$, so if we can successfully classify such amalgams then we will have dealt with many of the remaining cases. Indeed, the cases $L_2(q)$ for $q = 9, 11, 19, 29, 31, 59, 71$ are all of this type, so eight cases can be dealt with in this manner. (In fact, the case $L_2(29)$ was treated earlier in a different way.)

This is easier said than done, however. It is hard to find representatives of the two classes of A_5 that need to be considered—eventually we found them by making a copy of $L_2(11) \times M_{12}$ in the Monster, itself no small undertaking, and taking suitable diagonal A_5s therein. Finding the normalizer in the Monster of the subgroup D_{10} was even more difficult, and involved working inside several

different involution centralizers to find various parts of the required subgroup.

At the end of the calculation, after several months work, we found four new maximal subgroups by this method. In particular, we found explicitly maximal subgroups $L_2(59)$ and $L_2(71)$, thus answering a long-standing question as to whether these groups were subgroups of the Monster. This shows also that the maximal local subgroups 59:29 and 71:35 are not maximal subgroups of the Monster. In addition, we found new maximal subgroups $L_2(29)$:2 and $L_2(19)$:2.

To summarise the calculations to date, we have completely classified maximal subgroups of the Monster whose socle is isomorphic to one of the 11 simple groups $L_2(q)$, for $q = 9, 11, 19, 23, 29, 31, 59, 71$, $L_3(4)$, M_{11} or $U_4(2)$. This leaves just 11 cases to consider, namely $L_2(q)$, for $q = 7, 8, 13, 16, 17, 27$, $L_3(3)$, $U_3(3)$, $U_3(4)$, $U_3(8)$ and $Sz(8)$.

8 Traces and conjugacy classes

We tend to think of the trace of a matrix as being easy and quick to calculate, but that is only true if we actually have the matrix in front of us. To calculate the trace of a matrix which is only given as a word in some generators is a much more challenging problem. Indeed, the only reasonable method we could think of is essentially to calculate the matrix one row at a time, and extract the diagonal entries. This leads to a time of around 1 hour per letter of the word (depending of course on hardware and software) for the trace modulo 2.

On the other hand, the trace modulo 2 is not a very good conjugacy class invariant. It can only ever distinguish between different $2'$-parts of elements, since modulo 2 we have $Tr(x) = Tr(x^2)$. However, if we combine this invariant with the order, and the traces of powers of the elements, we can distinguish between most classes of odd-order elements in the Monster. The exceptions are irrational classes, where we cannot distinguish between elements which generate the same cyclic subgroup, and two other cases: we cannot distinguish between $3B$ and $3C$, or between $27A$ and $27B$.

To distinguish classes of even order, we need traces modulo an odd prime. This was the main reason why I decided to repeat the 3-local construction over the field of order 7, using exactly the same generators, so that the same words can be used in both representations simultaneously. Thus we can calculate the trace mod 2 and the trace mod 7 for the same element of the group, thus obtaining the character value modulo 14. This gives us a much better class invariant, which when combined with the order and the traces of powers, discriminates all classes of cyclic subgroups except $27A$ and $27B$. However, it is much more expensive to calculate traces modulo 7—days just to calculate one trace—so it can take weeks to identify the conjugacy class of an element by this method. With this apparatus my research student Richard Barraclough is in the process of producing a (partial) list of conjugacy class representatives. See also [4] for a description of a

method and the results of some experiments designed to produce pseudo-random elements of the Monster for use in randomized algorithms.

9 Conclusion

At the time of writing, it is less than four years since the publication of our first paper [10] on constructing the Monster. During that time, we have effectively tamed the Monster, so that many computations are now feasible inside this huge group. This was beyond our wildest dreams in 1998, but now seems routine.

It is natural therefore to speculate on what further calculations might be possible. For example, could we provide an independent existence proof for the Monster? This seems hard at the present time, but may be possible. At least we could find elements satisfying a suitable presentation, and perhaps combine this with arguments concerning the 2-local geometry to produce an existence proof independent of [2].

Other problems worthy of attack include specific questions such as: Does the 196882-dimensional $GF(2)$-representation support an invariant quadratic form? If so, is it of $+$-type or $-$-type? There are also more speculative questions, for example concerned with classifying Norton's nets (see [13]), where computational assistance might be valuable. And, can we complete the determination of the maximal subgroups of the Monster? There are undoubtedly some hard cases still to crack, and they may take a huge amount of computer time, but it seems as though this aim is not completely unreasonable.

Many years ago, I used Moore's law (doubling of computer power every 18 months), plus a postulated doubling of software power every 18 months, and a doubling of our own brain power every 18 months (perhaps the least plausible assumption, but with hindsight the most important contribution), to estimate that we could determine the maximal subgroups of the Monster by the end of the second millenium AD. No-one seemed to take me seriously at the time, but maybe I was not so far off the mark.

References

[1] J. H. Conway, A simple construction for the Fischer–Griess monster group, *Invent. Math.* **79** (1985), 513–540.

[2] R. Griess, The friendly giant, *Invent. Math.* **69** (1982), 1–102.

[3] P. E. Holmes, Computing in the Monster, Ph. D. thesis, Birmingham, 2001.

[4] P. E. Holmes, S. A. Linton and S. H. Murray, Product replacement in the Monster, Preprint 2002/12, School of Mathematics and Statistics, The University of Birmingham.

[5] P. E. Holmes, S. A. Linton, A. J. E. Ryba and R. A. Wilson, A constructive membership test for black box groups, in preparation.

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

[7] P. E. Holmes and R. A. Wilson, A new maximal subgroup of the Monster, *J. Algebra* **251** (2002), 435–447.

[8] P. E. Holmes and R. A. Wilson, $L_2(59)$ is a subgroup of $\mathbb{M}$, in preparation.

[9] P. E. Holmes and R. A. Wilson, More new maximal subgroups of the Monster, in preparation.

[10] S. A. Linton, R. A. Parker, P. G. Walsh and R. A. Wilson, Computer construction of the Monster, *J. Group Theory* **1** (1998), 307–337.

[11] U. Meierfrankenfeld and S. V. Shpektorov, The maximal 2-local subgroups of the Monster and Baby Monster, in preparation.

[12] S. P. Norton, Anatomy of the Monster, I, in *The atlas of finite groups ten years on (ed. R. T. Curtis and R. A. Wilson)*, 198–214. Cambridge University Press, 1998.

[13] S. P. Norton, Netting the Monster, in *The Monster and Lie algebras (ed. J. Ferrar and K. Harada)*, 111–125. Ohio State Univ. Math. Res. Inst. Publ. **7**. de Gruyter, 1998.

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

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

[16] R. A. Wilson, The Monster is a Hurwitz group, *J. Group Theory* **4** (2001), 367–374.

[17] R. A. Wilson, Construction of the Monster over $GF(7)$, and an application. Preprint 2000/22, School of Mathematics and Statistics, The University of Birmingham.