New computations in the Monster

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

February 23, 2006

Abstract

We survey recent computational results concerning the Monster sporadic simple group. The main results are: progress towards a complete classification of the maximal subgroups, including showing that $L_2(27)$ is not a subgroup; showing that the 196882-dimensional module over $GF(2)$ supports a quadratic form; a complete set of explicit conjugacy class representatives; small representations of most of the maximal subgroups; and a partial classification of the 'nets' (in the sense of Norton).

1 Introduction

Our aim in this paper is to update the survey [26] by describing the various explicit computations which have been performed in the Monster group, and the new information about the Monster which has resulted from these calculations. We begin by summarising [26] for the benefit of readers who do not have that paper to hand.

The smallest matrix representations of the Monster have dimension 196882 in characteristics 2 and 3, and dimension 196883 in all other characteristics. Three of these representations (over the fields of orders 2, 3, and 7) are now available explicitly [14, 8, 24]. It is hoped that the data and programs to manipulate them will be made available in the next release of Magma [15]. The generating matrices are stored in a compact way, and never written out in full. The basic operation of the system is to calculate the action of a generator on a vector of the underlying module.

Our first construction [14] was carried out over the field $GF(2)$ of two elements in the interests of speed, and proceeded by amalgamating various 3-local subgroups. Unfortunately, these 3-local subgroups are too small to contain many

useful subgroups, so we embarked on a second construction [8] over $GF(3)$, in order to utilise the much larger 2-local subgroups. In [26] we described how Beth Holmes used this construction to find four new maximal subgroups, and obtain a complete classification of subgroups of the Monster isomorphic to one of 11 listed simple groups (out of 22 still unclassified). The third construction [24] was over $GF(7)$, again using the 3-local subgroups, and the same generators as in the $GF(2)$ case. Thereby one can calculate character values modulo 14, and obtain good conjugacy class invariants.

2 The 2-local construction

The 2-local construction, although not the first, is easier to describe than the 3-local constructions, and is closely related to the Griess construction [5]. We shall not describe the construction itself, merely the outcome, and refer the reader to [8] for details. The idea is first to construct the involution centralizer $2^{1+24}{\cdot}Co_1$, in such a way that we can both calculate in this subgroup, and calculate its action on the module of dimension 196882 over $GF(3)$. Then we make a special 'triality' element which normalizes a subgroup $2^2.2^{11}.2^{22}.M_{24}$, the centralizer of a 4-group.

Now the 3-modular irreducible representation of degree 196882 for the Monster restricts to the subgroup $2^{1+24}{\cdot}Co_1$ as the direct sum of three constituents, of degrees 98304, 98280 and 298. The constituent of degree 98280 is monomial, and that of degree 98304 is a tensor product of representations of the double cover, of degrees 24 and 4096. Any element of this subgroup can therefore 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. (Note however that this representation is not unique: negating the matrices of size 24 and 4096 gives a second representation of the same element.)

By careful choice of basis we can ensure that the triality element can be written as a monomial permutation on 147456 points, followed by 759 identical 64×64 matrices, and an 850×850 matrix. In particular its action on a vector can be quickly computed.

It is important to realise that the only elements of the Monster which are stored in one of these two compact formats are the elements of $2^{1+24}{\cdot}Co_1$ and the triality element (or rather, eight triality elements, being the elements of order 3 in the A_4 generated by the normal 2^2 and a triality element). Every other element of the Monster is stored as a word in these generators. (Some improvements on this are possible, but seem not to be worth the extra effort. For example, it would be possible to devise a compact format for most if not all of the subgroup $2^2.2^{11}.2^{22}.(M_{24} \times S_3)$.)

3 The 3-local constructions

When we first seriously considered a computer construction of the Monster some ten years ago, we decided to produce 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 [14] for details.

The role of the involution centralizer is now taken by a maximal subgroup of shape $3^{1+12}{\cdot}2{\cdot}Suz{:}2$. The restriction of the representation to this subgroup consists again of a 'tensor product' part, of dimension 131220, a 'monomial' part, of dimension 65520, and a 'small' part. The small part has dimension 142 over $GF(2)$, or dimension 143 in any characteristic bigger than 3. The 'monomial' part is in reality 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.

To generate the Monster, we adjoined a 'duality' element normalizing a certain subgroup of shape $3^2.3^5.3^{10}.(M_{11} \times 2^2)$. 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.

In fact these calculations are considerably simplified 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 [24].

4 Basic calculations

There are just two basic operations available to us in any of the constructions we have described. The first is to multiply together elements in our chosen maximal subgroup to create new generators in this subgroup. The second is to act on a vector by one of these generators, or by the extra 'triality' or 'duality' element.

An element of the Monster is stored as a word $x_1t_1x_2t_2\ldots$, where the x_i are in our maximal subgroup, and the t_i are equal to the extra generator (or possibly its inverse, in the 2-local version). If we take a 'random' vector v in the underlying module, the chances are extremely good that it lies in a regular orbit under the Monster. Thus the order of an element x is, with probability very close to 1, equal to the smallest positive integer n such that $vx^n = v$. In [14, 26] we described how to improve this probability to exactly 1 at the expense of taking two (carefully

chosen) vectors instead of one.

The first serious calculations we attempted used the $GF(2)$ construction to try to improve estimates for the symmetric genus of the Monster. By character calculations alone, Thompson had shown that the Monster was a quotient of the triangle group $\Delta(2,3,29) = \langle x, y, z \mid x^2 = y^3 = z^{29} = xyz = 1\rangle$, and the challenge was to find the minimal value of n such that the Monster is a quotient of $\Delta(2,3,n)$. From Norton's work on maximal subgroups [17] it seemed very likely that this minimal value was 7. However, the probability that a random pair of elements of orders 2 and 3 has product of order 7 is around 10^{-8}, so we would need to look at something like 100 million pairs to have a reasonable chance of finding $(2,3,7)$-generators for the Monster. This took some 10 years of processor time. See [23] for more details.

5 The quadratic form

The 196882-dimensional representation of the Monster over the field of two elements is self-dual, so the Monster preserves a symplectic form on the module, and embeds in the symplectic group $Sp_{196882}(2)$. The question as to whether the Monster also preserves a quadratic form seems difficult to answer from a theoretical perspective. Beth Holmes and Steve Linton (and independently Jon Thackray) calculated explicitly a quadratic form which is invariant. They did not determine whether this form is of $+$ or $-$ type.

6 Traces and conjugacy classes

The trace of a matrix is easy to calculate, but it is less obvious how to calculate the trace of a linear transformation given in the form of a computer program. Ultimately it seems to be necessary to calculate the corresponding matrix, and extract the diagonal entries. This is obviously rather time-consuming compared to the tracing of individual vectors we have been doing up till now.

Now if p is any prime, the trace modulo p can only distinguish between different p'-parts of elements, since modulo p we have $Tr(x^p) = Tr(x)$. Thus in order to distinguish conjugacy classes, it is necessary to calculate traces modulo two distinct primes. Since we used exactly the same generators in the representations over $GF(2)$ and over $GF(7)$, we can calculate the trace mod 2 and the trace mod 7 for the same element of the group, thus obtaining the value of the degree 196883 character modulo 14. Combining this invariant with the order of the element and the traces of its powers, we are able to identify the conjugacy class of any element, up to a few ambiguities.

With this apparatus Richard Barraclough has produced a list of conjugacy class representatives [2]. To do this, he first improved the efficiency of our pro-

grams so that a trace modulo 7 now takes only a few hours to calculate. Then he conducted a wide search through words of length 1 and 2. Most classes turned up in this way, and the few that did not had representatives in the subgroup $3^{1+12}{\cdot}2{\cdot}Suz{:}2$. Thus a more targeted search was conducted in this subgroup. For example, this subgroup contains representatives of both classes $27A$ and $27B$, lying above class $9A$ in Suz. By finding elements of this type, and explicitly calculating their centralizers, it was possible to find representatives of classes $27A$ and $27B$, since they have different centralizer orders in the Monster.

7 Shortening words

As is well-known, the main difficulty in computing with a group whose elements are given as words is in preventing the words getting too long. We were able to find two tricks which in combination overcome this obstacle in most cases. The first trick takes two commuting $2B$-involutions, and produces a short word conjugating one to the other. The second trick is a method of rewriting a word known to be in the involution centralizer $2^{1+24}{\cdot}Co_1$, as a word of length 1.

To take the second part first, note that if we find a word in the generators, representing an element 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 'standard' form (in two ways) as a combination of a 24×24 matrix, a 4096×4096 matrix, a monomial permutation on 98280 points, and a 298×298 matrix. This standard form can be determined by calculating just 36 rows of the full 196882×196882 matrix for this element, so can be obtained fairly quickly. Moreover, if necessary we can even express this standard form as a word in the original generators for the subgroup.

The first trick 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 the triality element to take it to a non-central involution of 2^{1+24}, (2) conjugate by a random element of $2^{1+24}{\cdot}Co_1$, (3) conjugate by the triality element again to move it outside 2^{1+24}, and (4) conjugate again by a random element of $2^{1+24}{\cdot}Co_1$. Thus to conjugate an arbitrary $2B$-element in this group to the central involution, it suffices to conduct two random searches to find the correct conjugating elements to reverse the above operation.

Combining these tricks with Ryba's method for conjugating an involution in a group to an involution in a known subgroup [13], we can in principle shorten any word to one of length less than about 20. Specifically, given an arbitrary element g which powers to a $2B$-element x, there is a good chance that xz will power to a $2B$-element y, where z is our original $2B$-element. Since x and z both centralize y, we can use the first trick to conjugate y to z, say $y^{w_1} = z$ where w_1 has length at most 4. Using the trick again, we can conjugate x^{w_1} to z, say $x^{w_1 w_2} = z$ where $w_1 w_2$ has length at most 8. We then use the second trick to

write $g^{w_1 w_2}$ as a word of length 1, and thus obtain a word of length at most 17 for g. More generally, if h is an arbitrary word, we can multiply it by a random word of short length (preferably length 1) until we find an element g satisfying the above hypotheses. This is likely to produce a word of length at most 18 for h.

8 Maximal subgroups

A great deal of theoretical work on classifying the maximal subgroups of the Monster has been done in [22, 16, 17, 18], which reduced the problem to classifying conjugacy classes of simple subgroups of just 22 isomorphism types, subject to a variety of other conditions. In her PhD thesis [6] Beth Holmes dealt with 11 of the 22 isomorphism types, namely $L_2(q)$ for $q = 9, 11, 19, 23, 29, 31, 59, 71$ and $L_3(4)$, $U_4(2)$ and M_{11}. Since then she has completed the cases $L_2(q)$ for $q = 7, 8, 16, 17, 27$, and $L_3(3)$, $U_3(3)$, and $U_3(4)$. This leaves just the cases $L_2(13)$, $U_3(8)$ and $Sz(8)$.

The only really effective method of classifying such simple subgroups 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 Monster. We then look at each embedding to decide whether it indeed generates a subgroup of the required isomorphism type.

The most successful calculation of this type has been the classification of subgroups generated by two copies of A_5 intersecting in D_{10} (see [6]). This amalgam can generate $L_2(q)$, for any $q \equiv \pm 1 \pmod 5$, as well as $L_3(4)$, so this deals with eight of the required cases. In particular, we found four new maximal subgroups by this method, including subgroups isomorphic to $L_2(59)$ and $L_2(71)$, thus answering a long-standing question. In addition, we found new maximal subgroups $L_2(29)$:2 and $L_2(19)$:2. (In fact, the $L_2(29)$ case was done by a different method, but with hindsight it would have been easier to use this method.)

Four more of these cases, namely $L_2(7)$, $L_2(17)$, $L_3(3)$ and $U_3(3)$, were dealt with by an amalgam of two copies of S_4, intersecting in D_8 (see [7]). The case $U_3(4)$ used a subgroup $5 \times A_5$, extending a diagonal C_5 (there are two classes, so both need to be considered) to D_{10}. In the case $L_2(8)$ we can assume the 7-element is in class $7B$, so from the 2-local analysis [16] we know the 2^3:7 centralizes a $2B$-element, and most of the calculation can then be done inside the corresponding subgroup $2^{1+24}{\cdot}Co_1$.

The case $L_2(27)$ relies on an amalgam of 3^3:13 and D_{26} intersecting in 13, and the fact that there are just two classes of 3^3:13 in the Monster (this follows fairly easily from the results of [22]). In one case a simple counting argument shows that there is no such $L_2(27)$, while in the other case we needed to check a handful of cases computationally. In particular, there is no subgroup isomorphic

to $L_2(27)$ in the Monster, which answers another long-standing question.

Regarding the three outstanding cases, $L_2(13)$, $U_3(8)$ and $Sz(8)$, our computers are currently working through the cases for $L_2(13)$. After that, the case of $U_3(8)$ should present no serious problems. Our strategy in this case is to take a subgroup $3 \times L_2(8)$, and extend one of the diagonal elements of order 9 to a D_{18}.

The final case, $Sz(8)$, is proving more tricky. The only approach we can think of is to start with a group 2^3:7 and extend a 7-element to D_{14}. We can use the fact that $Sz(8)$ contains 2^{3+3}:7 to reduce the number of possibilities for the 2^3:7. Nevertheless, it is not easy to classify these subgroups. We know that the involutions are in class $2B$. Now there are three classes of $2B$-pure subgroups of order 4, whose normalizers involve composition factors M_{24}, M_{12} and A_8 respectively. A fairly easy counting argument shows that the first of these cannot occur in a putative subgroup $Sz(8)$.

In the second case, the normalizer of the 4-group has the shape $(2^2 \times 2^{1+20}) \cdot (S_3 \times M_{12}{:}2)$ inside $2^{1+24} \cdot 3 \cdot Suz{:}2$ inside $2^{1+24} \cdot Co_1$. Now in $Sz(8)$ we have $2^{3+3}/2^2 \cong 4 \circ Q_8$, which embeds uniquely (up to conjugacy) in M_{12}:2. In this embedding the central involution is of M_{12}-class $2B$. Thus the 2^3 we are looking for is either entirely inside 2^{1+24}, or maps to a $2B$-element in M_{12}. In the former case, the whole of 2^{3+3}:7 must lie inside $2^{1+24} \cdot Co_1$, and it is straightforward to show that this does not happen. In the latter case it turns out that the 2^3:7 lies in the maximal subgroup $2^3.2^6.2^{12}.2^{18}.(L_3(2) \times 3S_6)$, with the 2^3 lying in the normal $2^3.2^6.2^{12}$ but not in the $2^3.2^6$. It can be shown that it is unique up to conjugacy. At this stage it seems to be necessary to resort to computer calculations.

A similar analysis of the third type of $2B^2$ is in progress.

9 Explicit representations of subgroups

The Monster contains many interesting subgroups, which it may be useful to study independently. To facilitate such study, we have tried to construct small representations of these groups, whenever such representations exist [3]. These representations are available from the Monster page of [25]. In many cases one of these subgroups may be described as a certain non-split extension of a group acting (not necessarily faithfully) on a module. While previous constructions have concentrated on representing p-local subgroups irreducibly in characteristic different from p, the smallest faithful (reducible) representations are usually to be found in characteristic p. John Bray has developed effective methods of constructing such non-split extensions explicitly by gluing together indecomposable (but reducible) modules for the quotient group. Various techniques are then employed to ensure that the group constructed is indeed isomorphic to the desired subgroup of the Monster.

In two of the larger cases, namely the 3-local subgroups $3^2.3^5.3^{10}.(M_{11} \times 2S_4)$ and $3^3.3^2.3^6.3^6.(L_3(3) \times SD_{16})$, we felt that the only reliable method of ensuring

that we obtained a group of the right isomorphism type was to find it explicitly as a subgroup of the Monster. We then employed ad hoc techniques to try to find some smaller representations—in this case permutation representations.

To date we have representations of all the maximal subgroups except some of the 2-local subgroups. The latter do not appear to have faithful permutation representations of reasonable degree, and new methods will be required for these cases.

10 Character tables

Richard Barraclough is in the process of calculating the character table of the group $3^{1+12}{\cdot}2{\cdot}Suz{:}2$ used in some of our constructions of the Monster, along with various closely related groups. There are many subtleties which make this calculation difficult, not the least of which is the fact that there are two non-isomorphic groups of this shape, whose character tables look very similar.

It would be interesting to have the character tables of other maximal subgroups. From the representations described in the previous section, it should be possible to calculate some of these character tables without difficulty. However, the larger subgroups still present a formidable challenge.

11 Nets and their classification

Norton has generalised the ideas of Moonshine to commuting pairs of elements of the Monster, introducing functions F which are invariant under the action of the modular group via $F(g,h) = F(g^\alpha h^\beta, g^\gamma h^\delta)$ when $\alpha\delta - \beta\gamma = 1$. This even makes sense for non-commuting elements g and h, in the case when $g = ab$ and $h = bc$, and a, b, c are involutions. In this case, the action of the modular group corresponds to an action of the three-string braid group on triples of involutions.

In the case when a, b, c are in class $2A$, there are about 1.4×10^6 conjugacy classes of triples (a, b, c), which fall into about 14,000 orbits under the action of the braid group. These orbits are (roughly speaking) what Norton calls 'nets': they have a combinatorial structure of a polyhedron of genus 0 or 1. A complete classification of these nets would be of great interest in clarifying and developing the ideas of generalised moonshine.

There are various ways of dividing up the set of nets into more manageable subsets, for example according to the product abc, or the group generated by a, b, c, or the centralizer of a, b, c. So far, Richard Barraclough has a complete classification of the nets which are centralized by any element of prime order bigger than 3, and is working on the ones centralized by an element of order 3 [1].

The classification of nets with trivial centralizer will be difficult, however.

Ultimately it requires calculating the orbits of certain groups on the nearly 10^{20} involutions in class $2A$. This is a major challenge for the future.

12 A presentation for the Monster, and a new existence proof?

Norton has shown how to produce a presentation for the Monster on generators closely related to the 2-local subgroups we used in one of our constructions. The proof of this presentation, however, requires deep arguments. We hope to be able to verify that certain elements in our group satisfy the relations of this presentation. It may then be possible to provide for the first time a computational proof of existence of the Monster, independent of Griess's proof.

References

[1] R. W. Barraclough, Ph. D. thesis, Birmingham University, in preparation, 2005.

[2] R. W. Barraclough and R. A. Wilson, Conjugacy class representatives in the Monster, Preprint, QMUL, 2005.

[3] J. N. Bray and R. A. Wilson, Explicit representations of maximal subgroups of the Monster, in preparation.

[4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *An ATLAS of Finite Groups*, Oxford University Press, 1985.

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

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

[7] P. E. Holmes, On subgroups of the Monster containing S_4, Preprint, University of Birmingham.

[8] 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.

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

[10] P. E. Holmes and R. A. Wilson, $PSL_2(59)$ is a maximal subgroup of the Monster, *J. London Math. Soc.* **69** (2004), 141–152.

[11] P. E. Holmes and R. A. Wilson, On subgroups of the Monster containing A_5, to appear.

[12] P. E. Holmes and R. A. Wilson, The maximal subgroups of the Monster, in preparation.

[13] P. E. Holmes, S. A. Linton, E. A. O'Brien, A. J. E. Ryba and R. A. Wilson, Constructive recognition of black-box groups, in preparation.

[14] 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.

[15] Computational Algebra Group, School of Mathematics and Statistics, University of Sydney, *The Magma Computational Algebra System for Algebra, Number Theory and Geometry*, 2005. (`http://magma.maths.usyd.edu.au/magma/`).

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

[17] 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.

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

[19] R. A. Parker, The computer calculation of modular characters (The 'Meat-axe'), in *Computational Group Theory (ed. M. D. Atkinson)*, Academic Press, 1984, pp. 267–274.

[20] R. A. Parker and R. A. Wilson, Computer construction of matrix representations of finite groups over finite fields, *J. Symbolic Comput.* **9** (1990), 583–590.

[21] M. Ringe, *The C Meat-axe 2.3, documentation*, RWTH Aachen, 1995.

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

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

[24] 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.

[25] R. A. Wilson et al., A world-wide-web Atlas of Group Representations, http://www.mat.bham.ac.uk/atlas/

[26] R. A. Wilson, Computing in the Monster, in *Groups, Combinatorics and Geometry (ed. A. A. Ivanov, M. W. Liebeck and J. Saxl)*, 327–335. World Scientific, 2003.