Computer construction of the Monster

Stephen Linton
(Department of Computer Science, University of St. Andrews)
Richard Parker
(UK Online Ltd, Shepton Mallet)
Peter Walsh and Robert Wilson
(School of Mathematics and Statistics,
The University of Birmingham)

published in J. Group Theory 1 (1998), 307–337

Abstract

In this paper we describe our computer construction of the largest of the 26 sporadic simple groups, the so-called Monster.

1 Preliminaries

1.1 Introduction

Many of the sporadic simple groups were originally constructed on a computer, for example as groups of matrices or as groups of permutations, but the Monster was far too big to be constructed in this way, so had to be done by hand [3].

By now matrix representations are available on computers for 25 of the 26 sporadic simple groups [14], but the Monster is still too big for a simple-minded computer construction. Its smallest faithful representation is of degree 196882 over $GF(2)$, which would require approximately 10GB to store two generators as matrices.

In this paper, we describe a method for constructing this representation in a more compact form, which will enable some calculations to be performed in

the Monster. It is enormously faster than matrix multiplication, but rather less flexible, and it remains to be seen how effective it will be in helping to answer real questions about the Monster.

The bulk of the paper is divided into five parts. In Sections 2 and 3 we present a variety of background material, theoretical, algorithmic and computational. In Section 4 we construct the appropriate representation of the maximal subgroup $N(3A) \cong 3^{1+12}{\cdot}2{\cdot}Suz{:}2$, and in Section 5 we study the restriction to the subgroup $3^{2+5+10}{:}(M_{11} \times 2^2)$. Finally in Section 6 we find an automorphism which normalizes the subgroup $3^{2+5+10}{:}(M_{11} \times 2^2)$ to $3^{2+5+10}{:}(M_{11} \times D_8)$, and extends $3^{1+12}{\cdot}2{\cdot}Suz{:}2$ to the Monster.

1.2 The general strategy

Our choice of construction method was based on three overiding considerations. Firstly, the huge size of the group meant that the extra efficiency of calculations over $GF(2)$ would be absolutely crucial, and could make the difference between success and failure. Second, we could never afford the time to perform a single matrix multiplication, and therefore everything should be based on acting on vectors by matrices. Third, we cannot afford the time to read in a 5GB matrix for each vector-matrix operation, so a compact way of storing at least the generators is necessary.

It seemed to us that all these conditions could be satisfied by utilizing a 3-local analogue of the 2-local Griess construction [3].

We recall first the basic ideas of the 2-local construction. We start with the involution centralizer, a subgroup of the shape $2_+^{1+24}{\cdot}Co_1$. The desired 196884-dimensional ordinary representation of the Monster restricts to this group as

$$(2^{12} \otimes 24) \oplus 98280 \oplus 300.$$

Here the 2^{12} denotes the natural (i.e. the faithful irreducible) representation of 2_+^{1+24}, extended to a group $2_+^{1+24}{\cdot}Co_1$ (*not* isomorphic to the involution centralizer in the Monster), and 24 denotes the representation of $2{\cdot}Co_1$ on the Leech lattice. The representation 98280 is a monomial representation of $2^{24}{\cdot}Co_1$ which can be obtained from the $196560 = 2 \times 98280$ minimal vectors of the Leech lattice, while the final 300 is simply the symmetric square of the Leech lattice representation.

We now imagine restricting this representation to a subgroup $2^{2+11+11+11}.M_{24}$, obtained by centralizing a second involution. We find that both the repre-

sentations 2^{12} and 24, and therefore also the 300, are monomial for this subgroup. The actual decomposition is as follows:

$$(2^{11}a \otimes 24) \oplus (2^{11}b \otimes 24) \oplus 49152 \oplus 48576 \oplus 276a \oplus 276b \oplus 276c \oplus 24.$$

This subgroup has index 2 in its normalizer in $2^{1+24}{\cdot}Co_1$, which fuses the constituents $2^{11}a \otimes 24$ with $2^{11}b \otimes 24$, and $276a$ with $276b$. The problem now is to find another invertible linear map which normalizes the subgroup, and permutes these constituents in the correct way, that is, extending the action from S_2 to S_3 on the three constituents of degree $2^{11}.24 = 49152$, and on the three of degree 276. If one utilizes all the available information, it can be shown that there is a unique such extension—this is essentially Thompson's proof of the uniqueness of the Monster, assuming the existence of this representation [9].

In the 3-local version of this, we start with the $3A$-normalizer, which is a group of the shape $3^{1+12}{\cdot}2{\cdot}Suz{:}2$. The representation restricts to this subgroup in a similar way to the above, although it is technically more complicated for at least three independent reasons.

First, we really want to work over the field of order 4, in order to be able to write elements of the normal 3-subgroup as monomial matrices, but then the required outer automorphism of $3^{1+12}{\cdot}2{\cdot}Suz$ acts *semi-linearly* on the space. (In other words, if $g \in 3^{1+12}{\cdot}2{\cdot}Suz{:}2 \setminus 3^{1+12}{\cdot}2{\cdot}Suz$, then $g(\lambda v + w) = \overline{\lambda}g(v) + g(w)$ for all vectors v and w, and all scalars $\lambda \in GF(4)$, where $\overline{\lambda} = \lambda^2$.) We solve this problem by translating between several different notations for the same thing, according to context: thus a particular space may be regarded simultaneously as an n-dimensional space over $GF(4)$, a $2n$-dimensional space over $GF(2)$, or (the span of) a collection of n 2-dimensional spaces over $GF(2)$.

Second, the representation of $6{\cdot}Suz$ which corresponds to the Leech lattice representation of $2{\cdot}Co_1$ in the 2-local construction is not irreducible, but turns out to be a uniserial module with composition factors 12, 66, 12 in order. Here the 12 denotes a reduction modulo 2 of the complex Leech lattice, and the 66 denotes the skew-square of its dual. We shall prove later on that there is (up to automorphisms) a unique module of this shape, and show how it can be constructed.

Third, the tensor product corresponding to $2^{12} \otimes 24$ is now $3^{\begin{smallmatrix}12\\6\\12\end{smallmatrix}} \otimes 66$ over $GF(4)$, but both factors have a Frobenius automorph (or dual), so there

are four representations of this shape. If we forget the $GF(4)$ structure and regard the module as having twice the dimension over $GF(2)$, this has the effect of fusing these four cases in pairs. There remains the question, which is the correct one of the two cases? It turns out that these two cases represent non-isomorphic groups of the shape $3^{1+12}{\cdot}2{\cdot}Suz$, one of which is a subgroup of the Monster, while the other one is not. We show later (in Section 5.2) how to distinguish these two groups and how we ensure that we have the right one.

We can now describe the structure of the representation restricted to the subgroup $3^{1+12}{\cdot}2{\cdot}Suz$ as

$$\begin{pmatrix} & 12 & \\ 3^6 \otimes & 66 & \\ & 12 & \end{pmatrix} \oplus 32760 \oplus 142.$$

Here the final 142 is a $GF(2)$-irreducible for Suz obtained by tensoring the reduction modulo 2 of the complex Leech lattice with its dual, and removing a trivial module from the top and the bottom. The other modules are all $GF(4)$-modules as loosely interpreted above. The 32760 is a 'semilinear-monomial' representation of $3^{12}{\cdot}2{\cdot}Suz$, again obtained from the $196560 = 6 \times 32760$ minimal vectors of the (complex) Leech lattice. (All dimensions given here, except 142, are over $GF(4)$.)

Restricting further to $3^{1+1+5+5+5}M_{11}$, we find that $3^6 = 729$ breaks up as $243a + 243b + 243c$, while 12 and 66 remain irreducible. From [11] we see that the semi-linear monomial 32760 breaks up as $16038 + 2916a^2 + 1782 + 8910 + 198$ (again, dimensions are given over $GF(4)$), while the 142 breaks up as $132 + 10$. Roughly speaking, we now have to fuse together the 16038 with one of the $243 \otimes 66$ modules, and both the 2916 modules with $243 \otimes 12$, as well as mixing the 198-dimensional $GF(4)$ semilinear part with the 132-dimensional $GF(2)$ part. (A more mathematical description will be given below.)

In fact, we decided to keep as many automorphisms of these groups as possible, in order to reduce the number of cases to consider at the end. Thus we constructed first the representation of $3^{1+12}{\cdot}2{\cdot}Suz{:}2$, then restricted to the subgroup $3^{1+1+5+5+5}{:}(M_{11} \times 2^2)$, and adjoined an automorphism extending this to $3^{2+5+10}{:}(M_{11} \times D_8)$. The precise structures of the modules for these groups are given in Section 5.4.

Before we embark on the details of the construction, we describe some of the important concepts and techniques which play a significant role. The first of these concerns the interplay between $GF(2)$ and $GF(4)$-vector spaces, and

the vital but technical 'semilinear-monomial' (a particular type of induced representation) and 'semitensor product' (a particular direct summand of a tensor product). The second concerns the adaptation of the concept of a standard (or canonical) basis to deal with such representations.

2 Background

2.1 Some representation theory

If we have a group G containing a subgroup H, with N normal in H and $H/N \cong S_3$, then we can take the 2-dimensional irreducible representation of S_3 (over $GF(2)$), lift to H, and then induce to G. The resulting representation is what we shall call a 'semilinear-monomial representation', and it has the following properties. First, each element of G can be represented as the product of a block-diagonal matrix with 2×2 blocks on the diagonal, and a permutation of these blocks. Second, each of the 2×2 blocks occurring is an element of $S_3 \cong GL_2(2) \cong \Gamma L_1(4)$. The underlying $GF(2)$-vector space has a natural decomposition as a direct sum of $|G : H|$ two-dimensional subspaces. We can identify each of these 2-spaces with a 1-space over $GF(4)$, and then identify the 2×2 matrices with semilinear maps on this 1-space. Hence the name 'semilinear-monomial'.

We apply this construction to the group $G \cong 3^{12}{:}2{\cdot}Suz{:}2$ and the subgroup $H \cong 3.3^{10}(S_3 \times U_5(2){:}2)$. The latter has a unique S_3 quotient, and if we lift and induce its 2-dimensional irreducible representation we obtain a 'semilinear-monomial representation' on $|G : H| = 32760$ 'points'. Thus the underlying space may be regarded either as a 65520-dimensional space over $GF(2)$ on which G acts linearly, or as a 32760-dimensional space over $GF(4)$ on which G acts 'semilinearly'—unfortunately the meaning of the term 'semilinear' in this context is more general than the usual meaning. That is, a given element of G will act linearly on part of the space, and semilinearly on another part. So in the expression 'semilinear-monomial representation' it should be understood that 'semilinear' governs 'monomial' and not 'representation'.

For the sake of precision, we give here our identifications of the various fields, spaces and groups. Many other identifications are possible, but all

give equivalent results.

$GF(2)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$GF(4)$	0	1	ω	$\overline{\omega}$

$GL_2(2)$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$
$\Gamma L_1(4)$	1	ω	$\overline{\omega}$	1^*	ω^*	$\overline{\omega}^*$

Now we are in a position to describe our various different notations for representations of groups G of the shape $G \cong 3.H.2$. To exclude degenerate cases we assume that G has trivial centre, while $3.H = N$, say, has centre of order at least 3. We let w be a particular element of order 3 in the centre of N, and suppose that we are given a $GF(2)$-representation of G in which w acts fixed-point-freely. Then restricting to N, we may identify w with scalar multiplication by $\omega \in GF(4)$. This gives the underlying n-dimensional $GF(2)$-space the structure of an $n/2$-dimensional $GF(4)$-space, on which N acts linearly, and the elements of $G \setminus N$ act semilinearly, in the usual sense that $(\lambda v)g = \overline{\lambda}(vg)$ for $g \in G \setminus N$ and scalars $\lambda \in GF(4)$.

In practice we can perform this translation by using a standard basis algorithm for w (see Section 2.3), so that w is represented by a block diagonal matrix with $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ on the diagonal. Then we divide the matrices for elements g of G into 2×2 blocks, and each non-zero block is either one of $\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}$ (if $g \in N$), or one of $\begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$ (if $g \notin N$). We then translate the notation using the above tables.

The two cases where we carried out this procedure (in both directions!) were the representation of $3^{1+12}{:}2{\cdot}Suz{:}2$ of degree $2 \times 3^6 = 1458$ over $GF(2)$, and the 180-dimensional representation of $6{\cdot}Suz{:}2$. If we regard these both as (non-faithful) representations of $3^{1+12}{:}6{\cdot}Suz{:}2$, then we can imagine tensoring them together.

For clarity, we return to our general notation, and suppose that we have two suitable representations of G, of dimensions $2k$ and $2m$, treated in the above way, for possibly different central elements w_1 and w_2 of N. Then these correspond to $GF(4)$-representations of N of dimensions k and m, whose tensor product has dimension km over $GF(4)$, or $2km$ over $GF(2)$. It follows that the $GF(2)$ tensor product, which has dimension $4km$, splits as the direct sum of two submodules of dimension $2km$. We call these the two 'semitensor products' of the original representations. In general these two

submodules are not isomorphic—indeed they may have completely different structures.

There remains the question, how do we find these submodules in practice? One of them corresponds to identifying w_1 and w_2 with the *same* element of $GF(4)$ (so that $w_1 w_2^{-1}$ is in the kernel of the representation), while the other corresponds to identifying them with *different* elements of $GF(4)$ (so that $w_1 w_2$ is in the kernel).

Replacing w_2 by its inverse if necessary we may assume that we are in the first case, and that in the first representation w_1 is represented by a block diagonal matrix with $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ on the diagonal, and similarly for w_2 in the second representation. Then elements of N are represented by matrices whose non-zero 2×2 blocks are identified with $GF(4)$-elements as above. Thus to obtain the desired semitensor product we simply multiply all the 2×2 blocks in the first matrix by all the 2×2 blocks in the second matrix, and arrange them in the usual form of a tensor product.

The elements of $G \setminus N$, on the other hand, are represented by matrices whose non-zero 2×2 blocks are of the form λ^*, for $\lambda \in GF(4)$. Now we want to interpret the semitensor product of λ^* and μ^* as $(\lambda\mu)^*$, because the effect should be to multiply by the scalars λ and $\mu \in GF(4)$, and then apply the field automorphism. Since we are interpreting * as the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, this translates to multiplying the 2×2 blocks together with $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in between them—in either order, since all three elements are involutions.

This 'semitensor' construction can be interpreted in the language of the representation theory of $3^2{:}2 \cong \frac{1}{2}(S_3 \times S_3)$. The 2×2 blocks in the two representations of G correspond to elements in two different 2-dimensional representations of $3^2{:}2$. Now the latter group has exactly four 2-dimensional irreducible representations, and the tensor product of any two of them is the direct sum of the other two. We simply need to make a consistent choice of one of these direct summands. (We neglect the degenerate case when $w_1 = w_2^{\pm 1}$, which can be simply explained by the representation theory of S_3.)

We apply this construction to certain 180- and 1458-dimensional representations of $3^{1+12}{:}6{\cdot}Suz{:}2$. The only problem (which is solved in Section 5.2 below) is that there is no distinction between w_1 and w_1^{-1}, or between w_2 and w_2^{-1}, so that until we consider them both together we cannot tell which of

w_1w_2 or $w_1w_2^{-1}$ should act trivially. All we know is that the tensor product of the two representations is the direct sum of two indecomposable modules of degree 131220, one of which represents the $3A$-normalizer of the Monster, while the other represents a different group.

2.2 Standard basis algorithms

We will use many variants of the standard basis algorithm throughout the construction, for purposes as diverse as:

1. converting $GF(2)$ representations to $GF(4)$ representations, and *vice versa*;
2. adjoining outer automorphisms to groups;
3. finding invariant symplectic forms;
4. constructing (split or non-split) extensions of a vector space by a group acting on it.

In this section we describe the original matrix-group standard-basis algorithm of [7], and the modifications of it that we have used for other types of representations, and for specific purposes. In the following section we describe briefly the main types of applications that we have used.

The original motivation for the standard basis algorithm was to provide an isomorphism test for simple modules (i.e. irreducible group representations). The idea is to take 'standard' (i.e. fixed, or determined up to isomorphism) generators for the group, and construct a 'standard' (i.e. determined up to isomorphism) basis, with respect to which the matrices representing the group generators assume a 'standard' form. Isomorphism can then be tested by comparing these standard forms. In practice, the usefulness of this algorithm lies mainly in the fact that it produces an explicit isomorphism when one exists.

We describe first the corresponding algorithm for primitive permutation groups G, as this is technically simpler. Suppose G permutes n points, and is generated by the 'standard' generators (or indeed, any generators) $g_1, \ldots, g_k$, and that one of the point stabilizers is generated by $h_1, \ldots, h_m$, where the h_i are given by certain words in the g_j, say $h_i = w_i(g_1, \ldots, g_k)$. Then we may take the fixed point P_1 of $\langle h_1, \ldots, h_m \rangle$ as a 'seed' point. (If there is more than one fixed point, then the fixed points form a block, but G acts primitively,

and therefore regularly, so has prime order, and we neglect this trivial case.) Then we 'spin' this point under the group generators, in some fixed order, until we have all the n points: for example, we may define inductively P_i to be the first point distinct from $P_1, \ldots, P_{i-1}$ in the list

$$P_1, P_1g_1, P_1g_2, \ldots, P_1g_k, P_2g_1, \ldots, P_2g_k, \ldots.$$

(Of course, many other orderings are possible, as we shall see later on.) If we now write the generators $g_1, \ldots, g_k$ as permutations of the subscripts of $P_1, \ldots, P_n$, then they assume a standard form. Thus running the algorithm twice produces an explicit isomorphism between two equivalent permutation representations of a given abstract group (with a fixed set of generators).

Next we may generalize to arbitrary transitive permutation groups G on n points. In this case the stabilizer H of a point will in general have d fixed points, where $d = |N_G(H) : H|$ is the index of H in its G-normalizer. But now the centralizer in S_n of G is a group of order d, isomorphic to $N_G(H)/H$, and acting regularly on these d points. It follows therefore that we can take any one of them as the seed point, and the standard form will be the same in each case. Sometimes this is an advantage, in that we can choose the seed point arbitrarily, and sometimes a disadvantage, if all possible seed points need to be checked, as happens for example in Section 6.2.

Finally we generalize to arbitrary permutation groups by working in each orbit separately, and then concatenating the orbits in a suitable order.

The second type of standard basis algorithm applies to matrix groups, or matrix representations of abstract groups. There are several extra complications here. Firstly, there are more ways of choosing a suitable seed vector v_1. The original version (which is particularly useful if little is known about the group beforehand) took v_1 to be the (or a) nullvector of a suitable linear combination of words in $g_1, \ldots, g_k$. In this context, 'suitable' means one with smallest possible non-zero nullity. Later enhancements using characteristic polynomials provide good ways of finding such linear combinations of words quickly. It is also possible to use fixed vectors of subgroups as in the permutation group case. Secondly, in the 'spinning' part of the algorithm we define v_i to be the first vector in the list

$$v_1, v_1g_1, \ldots, v_1g_k, v_2g_1, \ldots$$

which is *linearly independent* of $\{v_1, \ldots, v_{i-1}\}$. Thirdly, not all modules are direct sums of simple modules, and to produce a suitable standard basis for

a module with a complicated structure it may be necessary to use more than one seed vector. (This last problem does not arise in our context.)

So far in this section we have only described what is well known. Now we need to generalize the methods to our 'semilinear-monomial' representations. In fact there are two quite distinct problems we need to solve. Both problems are to construct isomorphisms, just as in the previous cases. However, one considers isomorphism within the category of 'semilinear-monomial' representations, while the other considers isomorphism in the wider category of matrix representations.

The first problem can be solved by a combination of the algorithms already described. Moreover, the method applies to an arbitrary induced representation. Thus we let $G = \langle g_1, \ldots, g_k \rangle$ be a group, $H = \langle h_1, \ldots, h_m \rangle$ be a subgroup of G with $h_i = w_i(g_1, \ldots, g_k)$, and U be a fixed H-module of dimension d. We write the action of an element of G on the induced module $U \uparrow^G$ as a permutation of the n images of U, followed by a list of n $d \times d$ matrices giving the action on the appropriate image of U. Our task now is to put such a representation into a standard form, in order to construct an explicit isomorphism between two equivalent representations.

First we consider the permutation action of G on the n images of U. In this action H is by definition a point stabilizer, and we choose U_1 (the 'seed point') to be one of the fixed points of H. Next we use the matrix version of the standard basis algorithm to determine a standard basis B_1 for U_1 (as a module for H, with standard generators $h_1, \ldots, h_m$). Finally, we use the permutation version to order the 'points' as $U_1, \ldots, U_n$, with standard bases attached. More explicitly, we may define B_i to be the first basis in the list

$$B_1, B_1g_1, \ldots, B_1g_k, B_2g_1, \ldots$$

with the property that $\langle B_i \rangle$ is distinct from each of $\langle B_1 \rangle, \ldots, \langle B_{i-1} \rangle$.

In our case, $d = 2$, and each B_i can be represented as an invertible 2×2 matrix over $GF(2)$, i.e. as an element of $GL_2(2) \cong S_3$.

Our final version of the standard basis algorithm concerns the case where the module U which is induced up, or the subgroup H from which it is induced, may not be fixed by the G-isomorphism which we are trying to construct. In other words, we need to work in the category of all modules, rather than the category of induced modules. In this case our method is somewhat *ad hoc*, and may not generalize very easily. We merely refer to Section 6.3 for a description.

2.3 Application of standard basis algorithms

There are many situations where the construction of an explicit isomorphism between two different G-modules is useful. We describe a few which we will use later on, namely:

1. finding G-invariant forms;
2. adjoining an outer automorphism to G;
3. constructing non-split extensions of a vector space V by G;
4. extending or restricting the underlying field of a representation.

Our first application is to finding G-invariant forms. Suppose we have a self-dual G-module V, and for each group generator g_i let M_i be the matrix giving its action on a standard basis of V. Then the inverse-transposed matrices $(M_i^{-1})^t$ give an equivalent action of G, which therefore has the same standard form. In other words, if S is a standard basis matrix obtained by applying the algorithm to the matrices $(M_i^{-1})^t$, then

$$S(M_i^{-1})^t S^{-1} = M_i$$

or equivalently

$$M_i S M_i^t = S.$$

Thus S is the matrix of a bilinear form invariant under G. By letting S run through all possible standard basis matrices, we obtain all G-invariant bilinear forms on V. In particular, if V is a simple module, we obtain the G-invariant symplectic form, or symmetric bilinear form.

Similarly, if V is unitary, then with the same notation the matrices $(\overline{M}_i^{-1})^t$ give an action of G equivalent to that of the M_i, where $\overline{}$ denotes the field automorphism of order 2. In this case, the standard basis matrix S has the property that

$$S(\overline{M}_i^{-1})^t S^{-1} = M_i$$

or equivalently

$$M_i S \overline{M}_i^t = S.$$

Our second application, which is crucial and which we use frequently, is to adjoin outer automorphisms to groups. Suppose we have as usual a group G with standard generators $g_1, \ldots, g_k$, in a representation which is invariant

under an outer automorphism τ. We first have to find words $w_i(g_1, \ldots, g_k)$ for $1 \leq i \leq k$ such that the k-tuple $(w_1(g_1, \ldots, g_k), \ldots, w_k(g_1, \ldots, g_k))$ is conjugate in G to $(\tau(g_1), \ldots, \tau(g_k))$. For this reason it is important to choose our generators in such a way that such words will be easy to find. See [13] for a fuller discussion.

Now suppose that $g_1, \ldots, g_k$ are represented by (matrices, permutations or whatever) $M_1, \ldots, M_k$ with respect to a suitable standard basis. Then we apply the standard basis algorithm again to $w_1(M_1, \ldots, M_k), \ldots, w_k(M_1, \ldots, M_k)$. The resulting standard basis matrix/permutation/etc. will then conjugate $M_1, \ldots, M_k$ to $w_1(M_1, \ldots, M_k), \ldots, w_k(M_1, \ldots, M_k)$, so realises an automorphism $\tau\alpha$ of G, where α is an inner automorphism. As in many applications of the algorithm, we may need to consider all possible standard bases in order to find one with the properties we require. In this case, all standard bases will give a group *isoclinic* to $G.\langle\tau\rangle$, but in general not all (or even, not any) will give a group *isomorphic* to $G.\langle\tau\rangle$.

While the above construction produces upward extensions of a group G, our third application produces downward extensions. Specifically, we produce (split or non-split) extensions $V.G$ where V is some specified G-module. In the general construction, V is a tensor product module, but since every module is a tensor product of itself with the trivial module, this is not a restriction in principle. However, sometimes we need not just to get the group extension $V.G$ correct, but also its representation. Thus it may be useful to construct a group of the form $W.G$, where W is a proper submodule of a non-trivial tensor product V, and this may not be easy to find.

We first consider the easiest case, where matrices M_i representing the action of the group generators g_i on V are available. Then the matrices

$$\begin{pmatrix} M_i & 0 \\ v & 1 \end{pmatrix},$$

where v ranges over all row vectors in V, generate a split extension $V{:}G$, in which the matrices with $v = 0$ generate a subgroup isomorphic to G.

Now the same group $V{:}G$ is represented by the inverse transpose matrices

$$\left(\begin{pmatrix} M_i & 0 \\ v & 1 \end{pmatrix}^{-1}\right)^t = \begin{pmatrix} M_i^{-1} & 0 \\ -vM_i^{-1} & 1 \end{pmatrix}^t = \begin{pmatrix} (M_i^{-1})^t & -(M_i^{-1})^t v^t \\ 0 & 1 \end{pmatrix}.$$

which on moving the last coordinate to the beginning becomes

$$\begin{pmatrix} 1 & 0 \\ -(M_i^{-1})^t v^t & (M_i^{-1})^t \end{pmatrix}.$$

Suppose now that V is self-dual, so that by the above method we can find a matrix S conjugating $(M_i^{-1})^t$ to M_i for all i. Thus conjugating the above matrices by

$$\begin{pmatrix} 1 & 0 \\ 0 & S \end{pmatrix}$$

we obtain

$$\begin{pmatrix} 1 & 0 \\ 0 & S^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -(M_i^{-1})^t v^t & (M_i^{-1})^t \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & S \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -M_i S^{-1} v^t & M_i \end{pmatrix},$$

since $S^{-1}(M_i^{-1})^t S = M_i$. What happens if we now paste these matrices together, overlapping on the M_i? We obtain matrices of the form

$$\left(\begin{array}{c|cc} 1 & 0 & | \\ \hline -M_i S^{-1} v^t & M_i & | \; 0 \\ \hline & v & 1 \end{array}\right),$$

and clearly the top-right matrix entry should be 0. Thus by assigning all possible values to the bottom-left entry we obtain a group $F.V.G$, where F is the underlying field.

In the case when S is a symplectic form, and the underlying field has characteristic not 2, we find that this is a non-split extension, since the fact that $S^t = -S$ implies that the commutator of the two matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ -S^{-1} v^t & I & 0 \\ 0 & v & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ -S^{-1} w^t & I & 0 \\ 0 & w & 1 \end{pmatrix}$$

is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ -vS^{-1}w^t + wS^{-1}v^t & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ 2wS^{-1}v^t & 0 & 1 \end{pmatrix}.$$

For example, if V is a $2n$-dimensional representation over $GF(p)$, where p is a prime bigger than 2, then we obtain a $(2n+2)$-dimensional representation of a group $p_+^{1+2n}{:}G$ in this way.

A generalization of this construction takes a subgroup of $V{:}G$ rather than the whole group. For example, it may be possible to take a representation of G itself in this form, and then the construction gives rise to a representation of $F.G$, which may or may not be split.

A further generalization can be obtained by replacing the trivial representation of G by some other representation, or indeed by two distinct representations. Thus we may have a group G with two modules, such that a submodule of one is isomorphic to a quotient of the other. Using the standard basis algorithm very much as above, we can obtain the matrices representing the group generators in the forms

$$\begin{pmatrix} A_i & 0 \\ B_i & C_i \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} C_i & 0 \\ D_i & E_i \end{pmatrix}.$$

Then we can paste them together to form matrices

$$\begin{pmatrix} A_i & 0 & 0 \\ B_i & C_i & 0 \\ * & D_i & E_i \end{pmatrix},$$

where $*$ denotes an unknown part of the matrix. If all possibilities for $*$ are taken, then an extension $V.G$ is formed (where V is the appropriate G-module), which again may be either split or non-split.

Our final application of the standard basis method is to change the field of definition for a matrix representation.

If a matrix representation is written over a large field F, but is equivalent to a representation over a subfield F_0, than an appropriate base-change can be found by use of the standard basis algorithm. Provided the seed vector is found by a process which does not involve the use of any elements of $F \setminus F_0$, the standard basis matrix will automatically conjugate the group generators to matrices over F_0. This is the case, for example, if the seed vector is the nullvector of an F_0-linear combination of words in the group generators, or a fixed vector of a subgroup which has fixed space of dimension 1.

On the other hand, if a matrix representation is written over a small field F_0, but is equivalent to a representation of smaller dimension over an extension field F, then we can first use the standard basis algorithm to find the centralizer of the representation. Then we can choose an appropriate identification of a fixed-point-free element X of the centralizer with a generator ξ for the multiplicative group of F. Now we use the standard basis algorithm again, this time applied to the element X alone, so that X is conjugated into block diagonal form, with all diagonal blocks equal to x, say. This implies that the group generators are conjugated into a form in which all the blocks of the matrices are either zero or powers of x. Thus the blocks can be identified with (zero or) the corresponding powers of ξ in F.

A slight generalization of this method will work when the representation is only semilinear over F, rather than linear.

3 The Suzuki group

3.1 Standard generators

In order to understand the details of the construction of the Monster below, we need a fair amount of detailed information about the Suzuki group, and the action of its sixfold cover on the complex Leech lattice. Many of these details can be found in [11]. For example, the orbits of the monomial subgroup on the minimal vectors of the lattice are described in Table 1(a) of [11], and will be important later on.

In addition, it is worth here describing the 'standard generators' that we use, and the details of the technique employed to adjoin outer automorphisms. These will be used in several places later on. We follow [13] in defining standard generators for the simple group Suz to be elements $a \in 2B$, $b \in 3B$, with ab of order 13 and $abab^2$ of order 15. Such generators are unique up to automorphisms, which means there are two conjugacy classes of such pairs in the group itself. We now take pre-images A, B, of these generators in the various covering groups that we need, and in order to specify them up to automorphisms in each case we demand that A has order 2 or 4, B has order 3, and AB has order 13.

Similarly, we define standard generators for the automorphism group $Suz{:}2$ to be $c \in 2C$, $d \in 3B$, with cd of order 28. In the group $6{\cdot}Suz{:}2$ we take pre-images C and D with D of order 3 and $CDCD^2$ of order 7. Note that this group is the one whose character table is printed in the Atlas [2], rather than the isoclinic one. An equivalent definition of standard generators for this group is as follows. First, C is in class $2C$, and D is in class $+3B$, that is, that pre-image of class $3B$ in Suz which has order 3 and character value 3 on the degree 12 characters. Finally, CD has order 56. It is not hard to show that this defines the pair of generators (C, D) up to automorphisms. It must however be borne in mind that the outer automorphism group of $6{\cdot}Suz{:}2$ has order 2, and acts by multiplying elements in the outer half of the group by the central involution. In terms of the standard generators, this can be expressed by replacing C by C^3. Since this outer automorphism does not preserve the 12-dimensional representation, it is necessary to make

a consistent choice of C in the different representations.

Finally, we note that we can recover standard generators for $6{\cdot}Suz$ from those of $6{\cdot}Suz{:}2$ by putting $A = (CDD)^{-2}(CD)^{-14}(CDD)^2$ and $B = D$. (Note however, that (due to carelessness) in later sections, in particular Section 3.3, we actually used the inverse of this A instead. This change only ever has the effect of multiplying elements by the central involution of $6{\cdot}Suz{:}2$ so has little impact. We felt it safer not to try to change the words we used, for fear of introducing fresh mistakes.)

3.2 Adjoining outer automorphisms

For technical reasons we need to adjoin an outer automorphism to many of the groups constructed below. The main reason is to ensure that the various representations are absolutely irreducible over $GF(2)$, in order to minimize the number of cases we need to consider later on.

The method is standard, and is described in Section 2.3 above. If we take a, b as standard generators for the Suzuki group, then it turns out that the pair a', b' given by $a' = (ab)^{-2}a(ab)^2$ and $b' = (ab^2)^{-2}b(ab^2)^2$ is a pair of standard generators in the other conjugacy class. Therefore we can use the standard basis algorithm to conjugate the pair (a, b) to the pair (a', b'), thereby obtaining a matrix which realises the outer automorphism of Suz. Adjoining this matrix to the group Suz therefore generates a group which is isoclinic to, but not necessarily isomorphic to, $Suz{:}2$. Therefore we may need to multiply this matrix by some element which centralizes the given representation of Suz. But these elements are usually easy to write down.

The same method works for all the covering groups of Suz, by replacing a, b by the standard pre-images A, B.

The most important example of this method in the sequel is however adjoining a specified automorphism to $3^{2+5+10}(M_{11} \times 2^2)$. This is in principle the same, though in practice much more complicated: we have 6 generators instead of two, 13 indecomposable summands rather than one or two, and a very large representation, and, in addition, three or four different versions of the standard basis algorithm are required.

3.3 Standard generators for $3^{1+12}{:}6{\cdot}Suz{:}2$

All the representations we are going to make will be made with a particular set of 'standard generators' for $3^{1+12}{:}6{\cdot}Suz{:}2$. Here we define these, as they

are crucial for resolving various subtle questions.

We first find a complementary subgroup $6{\cdot}Suz{:}2$ (which is unique up to conjugacy, as it is contained in the involution centralizer $(3 \times 6{\cdot}Suz){:}2$), and take standard generators C, D as defined in Section 3.1. We next make generators $A = (CDD)^{-2}(CD)^{14}(CDD)^2$ and $B = D$ for the subgroup $6{\cdot}Suz$, and find a subgroup $2 \times U_5(2)$ generated by $(AB(ABAB^2)^2)^4$ and

$$((AB)^3BAB)^9((AB)^3B(AB)^5B(AB)^2B)^6((AB)^3BAB)^{-9}.$$

Then our third generator for $3^{1+12}{:}6{\cdot}Suz{:}2$ is defined as the element E in 3^{1+12} which is centralized by the given group $U_5(2)$ and inverted by the central involution of $\langle A, B\rangle \cong 6{\cdot}Suz$. Thus E is determined up to inversion, but there is an inner automorphism which centralizes C and D, and inverts E. In other words, C, D, E are determined up to automorphisms, except for the problem mentioned earlier, that C might need to be replaced by C^3. This is equivalent to replacing the action of $6{\cdot}Suz{:}2$ on 3^{12} by the dual action.

We also denote by C, D and E the images of these generators in the various quotient groups that appear in the construction. For certain purposes we also need standard generators for the subgroup $3^{1+12}{:}6{\cdot}Suz$ of index 2, and various quotients thereof, and we take these to be A, B and E as defined above.

3.4 A 38-dimensional module for $3^{1+12}{:}6{\cdot}Suz{:}2$

Just as the 2-local construction is most easily described in terms of a double cover of the involution centralizer, so this 3-local construction is most easily described in terms of a triple cover of the $3A$-centralizer. This may be described as the split extension of an extraspecial group 3^{1+12} by the covering group $6{\cdot}Suz$ of the Suzuki group, in which the action is given by the natural action of $2{\cdot}Suz$ on the complex Leech lattice modulo $\theta = \sqrt{-3}$. Thus the commutator map in the extraspecial group corresponds to the symplectic form on the 12-space over $GF(3)$, and the central 3-element in $6{\cdot}Suz$ acts trivially. (We note in passing that the Schur multiplier of $3^{12}{:}2{\cdot}Suz$ is 3^2, since the multiplier of $2{\cdot}Suz$ is 3, and any covering of the 3^{12} corresponds to a symplectic form invariant under $2{\cdot}Suz$.)

This group has a centre of order 3^2, and therefore has four distinct quotients by cyclic groups of order 3. Clearly one of these is a split extension $3^{1+12}{:}2{\cdot}Suz$, while another has shape $3^{12}{:}6{\cdot}Suz$. The other two both have

the shape $3^{1+12}{\cdot}2{\cdot}Suz$, but it turns out that they are not isomorphic. (It is not too hard to prove this theoretically, by observing that the outer automorphism group of $3^{1+12}{:}6{\cdot}Suz$ has order 2, but we also prove it computationally in Section 5.2.) One of them is isomorphic to a subgroup of the Monster, while the other is not.

In order to study these groups closely, and find a way to distinguish them, we made a 38-dimensional representation of $3^{1+12}{:}6{\cdot}Suz{:}2$ with module structure

$$\begin{matrix} & & 1 \\ 12 & \oplus & 12 \\ 12 & & \end{matrix}$$

as follows. First, take the 24-dimensional representation of Conway's group $2{\cdot}Co_1$ on the Leech lattice, reduce modulo 3, and restrict to a subgroup $6{\cdot}Suz{:}2$. This gives a 24-dimensional representation of $6{\cdot}Suz{:}2$ over $GF(3)$, which is a uniserial module with two 12-dimensional constituents. These constituents are dual to each other, but restrict to isomorphic self-dual modules for the subgroup of index 2.

Next, we take another copy of one of these 12-dimensional constituents, and 'glue' a copy of the trivial module at top and bottom (see the next paragraph for a precise description): in principle this gives a group $3^{1+24}{:}2{\cdot}Suz{:}2$, in which we found a subgroup $3^{1+12}{:}2{\cdot}Suz{:}2$ as follows, by utilizing the symplectic form on the 12-space, which (up to sign) is preserved by the group.

Suppose that S is the matrix of the symplectic form fixed by $2{\cdot}Suz$ on the 12-space over $GF(3)$, so that $M^tSM = S$ for all elements M of $2{\cdot}Suz$ (or $M^tSM = -S$ for elements M of $2{\cdot}Suz{:}2 \setminus 2{\cdot}Suz$). Then we take all matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ v & M & 0 \\ \lambda & \pm v^tS & 1 \end{pmatrix}$$

where v is any column vector, λ is any scalar, and v^t is the transpose of v. Also, M is any element of $2{\cdot}Suz{:}2$, and the sign is $+$ if and only if M is in $2{\cdot}Suz$. All we need to check then is that this set of matrices is closed under multiplication, and so forms a group with the correct structure. (An alternative method of constructing this representation would be to use the method of Section 2.3—starting from a 13-dimensional representation of $3^{12}{:}2{\cdot}Suz{:}2$. In theoretical terms this boils down to the same thing, but the practical steps are somewhat different.)

Taking the direct sum of these two representations of dimensions 24 and 14 gives a 38-dimensional representation of $3^{1+12}{:}6{\cdot}Suz{:}2$. We use the standard generators C, D of $2{\cdot}Suz{:}2$ here to ensure that we get the correct subdirect product, rather than the full direct product, of the groups. At this stage it is not important which of C or C^3 we use, as long as we make a consistent choice later on.

Note that we have here a direct sum of 3-modular representations of the groups $3^{1+12}{:}2{\cdot}Suz{:}2$ and $6{\cdot}Suz{:}2$, while ultimately we require tensor products of 2-modular representations of these two groups.

We can now see the normal 3^2 clearly, and observe the effects of factoring out particular subgroups of it. Moreover, since we have defined standard generators for the group, we can label and eventually distinguish the elements of the centre, and decide which one must be factored out to obtain a subgroup of the Monster.

4 The representation of $3^{1+12}{:}2{\cdot}Suz{:}2$

4.1 The 3^6-dimensional module for $3^{1+12}{:}2{\cdot}Suz$

The natural representation of the extraspecial group 3^{1+12} is easy to write down. If we label the 3^6 basis vectors e_v by vectors v in $V = GF(3)^6$, then we have a group of *translations* $T_w : e_v \mapsto e_{v+w}$ for each $w \in V$, together with a group of *diagonal elements* $D_\chi : e_v \mapsto \omega^{\chi(v)} e_v$ for each linear character $\chi \in V^*$, where ω denotes a generator for the multiplicative group of $GF(4)$. Each of these groups has order 3^6, and together they generate 3^{1+12}.

The symplectic form on 3^{12} is given by $(\chi, w) = \chi(w)$, corresponding to the commutator map $[D_\chi, T_w] = \omega^{\chi(w)}$ on 3^{1+12}. For simplicity we choose a basis $w_1, \ldots, w_6$ for V and the dual basis $\chi_1, \ldots, \chi_6$ for V^*, so that $(\chi_j, w_i) = 0$ if $i \neq j$ and 1 if $i = j$.

Now we take the 12-dimensional representation of $2{\cdot}Suz$ over $GF(3)$, and write it with respect to an ordered symplectic basis which we might as well label $\{w_1, \ldots, w_6, \chi_1, \ldots, \chi_6\}$ as above. We then have to find 729×729 matrices over $GF(4)$ which act by conjugation on $\{T_{w_i}, D_{\chi_j}\}$ in the same way (modulo scalars) that our generators for $2{\cdot}Suz$ act on the given (ordered) basis.

To find such a symplectic basis for the 12-space explicitly, we first use the standard basis method to find a matrix S conjugating the group generators

to their transposed inverses: thus $S^{-1}g_iS = ((g_i)^t)^{-1}$ so $g_iS(g_i)^t = S$, and therefore S is the matrix of a symplectic form invariant under the action of the group generators g_i. Now the orthogonal space to a subspace generated by the rows of a matrix U is the span of the vectors w such that $USw^t = 0$, that is, the 'nullspace' of US. Thus we may find our symplectic basis by first choosing inductively χ_i to be any vector orthogonal to $\{\chi_1, \ldots, \chi_{i-1}\}$, then choosing w_i orthogonal to $\{w_1, \ldots, w_{i-1}, \chi_j \mid j \neq i\}$, and finally changing sign on w_i where necessary to make $\chi_i(w_i) = 1$.

Now we make 729×729 matrices corresponding to our generators A and B of $2{\cdot}Suz$ by another application of the standard basis method. Note first that our basis for 729-space may be defined by choosing a seed vector such as the fixed vector of $\langle D_\chi \rangle$, and taking its images under the 3^6 elements of $\langle T_w \rangle$, in a specified order.

Given an element g of $2{\cdot}Suz$, therefore, we may write

$$\begin{aligned} g(e_i) &= \sum_{j=1}^{6} \alpha_{ij} w_j + \sum_{j=1}^{6} \beta_{ij} \chi_j \\ g(f_i) &= \sum_{j=1}^{6} \gamma_{ij} w_j + \sum_{j=1}^{6} \delta_{ij} \chi_j \end{aligned}$$

and construct corresponding elements of 3^{1+12} as

$$\begin{aligned} U_i &= \prod_{j=1}^{6} T_{w_j}^{\alpha_{ij}} . \prod_{j=1}^{6} D_{\chi_j}^{\beta_{ij}} \\ V_i &= \prod_{j=1}^{6} T_{w_j}^{\gamma_{ij}} . \prod_{j=1}^{6} D_{\chi_j}^{\delta_{ij}} \end{aligned}$$

Thus g must act on 3^{1+12} by conjugating T_{w_i} to a scalar multiple of U_i (for each i), and D_{χ_i} to a scalar multiple of V_i (for each i). Notice that we have 12 independent choices of scalars here, corresponding to multiplying g by an element of $3^{1+12}/3$.

Without loss of generality we choose all the scalars to be 1, which means that g maps the standard basis for the standard generators $\{T_{w_i}, D_{\chi_i} \mid 1 \leq i \leq 6\}$ to the standard basis for the generators $\{U_i, V_i \mid 1 \leq i \leq 6\}$. Thus the top row of the matrix for g is simply the fixed vector of $\langle V_i \mid 1 \leq i \leq 6 \rangle$ (which involves another arbitrary choice of scalar multiple, making 13 in all), and the other rows are obtained by multiplying by the elements of $\langle U_i \mid 1 \leq i \leq 6 \rangle$ in the predetermined order.

As we have seen, the elements that we make are really only defined up to 13 independent choices of scalars, and therefore we end up with an arbitrary element of the given coset of 3^{1+12}. This can be corrected afterwards, by finding standard generators A, B, E for the group as defined in Section 3.3.

Next, we need to adjoin the outer automorphism in the standard way. That is, we first make the direct sum of this representation and its dual, and then put it into standard basis with respect to the standard generators A, B, E. Then we make the elements A' and B' defined above, and find the element E' defined by putting dashes on everything in the definition of E above (Section 3.3), and find the matrix putting the representation into standard form with respect to these new generators. Correcting, if necessary, by scalars on the two constituents of the original representation, we obtain a 1458-dimensional representation of $3^{1+12}{:}2{\cdot}Suz{:}2$, written over $GF(4)$.

To write this over $GF(2)$, we use the standard basis method again, as described in Section 2.3. Then we need to find standard generators equivalent to C, D, E for the group.

Finally, we want to ensure that our basis exhibits the $GF(4)$ semilinear structure, so we arrange that a generator for the normal subgroup of order 3 in each case acts as a block diagonal matrix with 2×2 blocks $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. In technical terms, what we do here is write the representation with respect to a standard basis for the normal subgroup of order 3 (with a specified generator).

4.2 The 90-dimensional module for $6{\cdot}Suz$

This representation has to be a suitable reduction modulo 2 of the ordinary representation $12 \oplus 78$, in which the 12 denotes the natural representation of $6{\cdot}Suz$, and the 78 is the dual of its symmetric square (or the symmetric square of its dual). This implies that, modulo 2, the constituents are 12, 66, and 12. We show first that this must be a uniserial module with structure $\begin{smallmatrix} 12 \\ 66 \\ 12 \end{smallmatrix}$, and then show that there is a unique such module, up to equivalence and field automorphisms.

Now Clifford theory tells us that any representation in the given 2-block of $3^{1+12}{\cdot}2{\cdot}Suz$ can be written as the tensor product of a 3^6-dimensional representation of the split extension $3^{1+12}{:}2{\cdot}Suz$ and a faithful representationof

$6{\cdot}Suz$. Also, as we can easily check with the Meataxe, the 78 can be reduced modulo 2 both as $\begin{matrix}66\\12\end{matrix}$ and as $\begin{matrix}12\\66\end{matrix}$. Since the whole representation is unitary, the 90-dimensional factor must be symmetrical. Moreover, the central involution of $6{\cdot}Suz$ acts non-trivially, so the 90-dimensional module is either uniserial of shape $\begin{matrix}12\\66\\12\end{matrix}$, or of shape $\begin{matrix}12\\12\end{matrix} \oplus 66$.

The latter can be easily eliminated by showing that $6{\cdot}Suz$ does not have a faithful representation of shape $\begin{matrix}12\\12\end{matrix}$ over $GF(4)$. This is because the full group of matrices

$$\begin{pmatrix} M & 0 \\ A & M \end{pmatrix},$$

where M is a 12×12 matrix in a fixed representation of $3{\cdot}Suz$, has the shape $2^{288}{:}3{\cdot}Suz$. Factoring out by the centre, we obtain a group $2^{286}{:}Suz$, in which there is a unique class of complementary Suz—we calculate this explicitly by the same method used below to classify complements in $2^{1584}{:}Suz$. In particular, all such complements lift to $2^2 \times 3{\cdot}Suz$ in $2^{288}{:}3{\cdot}Suz$.

Next we show that there is a unique non-split extension $\begin{matrix}12\\66\end{matrix}$ for $3{\cdot}Suz$. By general nonsense, this is equivalent to showing that there is a unique non-split extension of $12 \otimes 66^*$ by the trivial module for Suz. This in turn is equivalent to showing that there are just four classes of subgroups isomorphic to Suz in the split extension $V{:}Suz$, where V is the module $12 \otimes 66^*$ for Suz over $GF(4)$.

We now take a, b to be standard generators for Suz acting on V, and construct this split extension $V{:}Suz$. Now any copy of Suz in $V{:}Suz$ is generated by $a' = av_1$ and $b' = v_2 b$, for some $v_1, v_2 \in V$, such that a' and b' satisfy the same relations as a and b. Moreover, ab has order 13, so by Sylow's theorem we may as well assume that $ab = a'b'$. This implies that $v_1 v_2 = 1$, so $v_1 = v_2 = v$, say. Since $a^2 = 1$, we must have $(a')^2 = 1$, which implies that $v \in C_V(a)$. Since $b^3 = 1$, we have $(b')^3 = (vb)^3 = 1$, which implies that $v \in [V, b]$. Similarly, the relation $(babab)^{15} = 1$ implies $(b'a'b'a'b')^{15} = (vbabab)^{15} = 1$, which in the more usual additive notation becomes

$$\begin{aligned} v &\in \ker(1 + (babab) + (babab)^2 + \cdots + (babab)^{14}) \\ &= \mathrm{im}(1 + babab) \end{aligned}$$

$$= \quad [V, babab].$$

Using the relations

$$(b(ab)^3)^{12} = (b(ab)^4)^{21} = (b(ab)^5)^{15} = 1$$

in a similar fashion, we deduce that

$$v \in C_V(a) \cap [V,b] \cap [V,babab] \cap [V,b(ab)^4] \cap [V,b(ab)^5] \cap \ker\left(\sum_{i=0}^{11}(b(ab)^3)^i\right).$$

We calculate this subspace W, say, of V explicitly, and find its dimension, which happens to be 61.

On the other hand, such a pair $(a' = av, b' = vb)$ with $ab = a'b'$ is conjugate to (a,b) exactly when $a' = a^w$ (or, equivalently, $b' = b^w$), for some $w \in C_V(ab)$. But $a^w = a[a,w] = a[w,a]$, so this condition is equivalent to $v \in [C_V(ab), a]$, which we denote by U. Since U has dimension 60, and the conjugacy classes of complements are in one-to-one correspondence with the vectors of W/U, it follows that there are at most 4 classes of complements. On the other hand, we already know that there is at least one non-split extension $\begin{matrix}12\\66\end{matrix}$, so the required result follows.

At this stage, therefore, we know that the 90×90 matrices for the group generators can be written in the form

$$\begin{pmatrix} M_{12} & 0 & 0 \\ A & M_{66} & 0 \\ * & B & M_{12} \end{pmatrix},$$

where M_n denotes an $n \times n$ matrix. In principle we know everything about the representation except what happens in the bottom left 12×12 block of these matrices. Unfortunately, this still leaves us with 2^{288} possibilities for each group generator, and so we had to devise a method for ruling out most of these possibilities.

To make our first approximation to this representation, we take the 12-dimensional representation of $3{\cdot}Suz$ over $GF(4)$, and make both the symmetric square of its dual, and the dual of its symmetric square. One of these has the structure $\begin{matrix}12\\66\end{matrix}$ and the other $\begin{matrix}66\\12\end{matrix}$. We use the Meataxe to put the two constituents into standard basis, so that we can paste together the matrices for these two representations, overlapping on a 66×66 block in the middle.

The resulting matrices generate some subgroup of $2^{288}{\cdot}3{\cdot}Suz$ which is likely to be nearly all of it. To find the subgroup $6{\cdot}Suz$ we adopted a somewhat inelegant approach, after failing to find any reasonable alternative.

The idea is to find generating subgroups of reasonably large odd order for $3{\cdot}Suz$, so that their centralizers in 2^{288} are reasonably small, then 'apply the formula' to find corresponding subgroups of odd order in $2^{288}{\cdot}3{\cdot}Suz$, and finally to run through all the cases which are left (given by double cosets of two of these centralizers in a third) to see which one gives $6{\cdot}Suz$. In this case, the 'formula' is as follows. If a, b are conjugate elements of odd order m in a group of the shape $2^n{:}m$, then $(ba)^{\frac{m-1}{2}}$ conjugates a to b.

We chose to generate Suz by subgroups 11:5 and 5×3 intersecting in 5. It was not easy to find such subgroups given by words in the standard generators—details can be found in [10]. Next we calculate the same words in any preimages of the standard generators in our group $2^n{\cdot}3{\cdot}Suz$, to obtain certain preimages of the subgroups 11:5 and 5×3. To remove the unwanted 2-groups, we first power up our elements until they have odd order, and then, as described above, we 'apply the formula', as follows.

Suppose that e, f satisfy the relations $e^{11} \equiv f^5 \equiv 1$ and $e^f \equiv e^3$ modulo the 2-group. Then by the formula, $(e^3e^f)^5$ conjugates e^f to e^3, so that $f' = f(e^3e^f)^5$ conjugates e to e^3, whence $\langle e, (f')^2\rangle \cong 11{:}5$ (here we need to square f' since it might have order 10). The same idea applied to the other elements will produce subgroups 11:5 and 5×3 in $2^n{\cdot}3{\cdot}Suz$, intersecting in 5.

Since our generators now have odd order, and the action of the group $3{\cdot}Suz$ on the 144-dimensional $GF(4)$-module is uniserial with constituents 1, 142, 1 in order, it is easy to check that our group is now of the form $2^{286}.3{\cdot}Suz$. However, it seems to be easier not to use this knowledge in what follows.

To look at all possibilities for such configurations, we need to consider conjugates of 11:5 or 5×3 by elements of the 5-centralizer. Of course, conjugation by elements which centralize the 11 or the 3 will have no effect, so the different cases correspond to the double cosets of $C(11{:}5)$ and $C(5 \times 3)$ in $C(5)$. These centralizers are all vector subspaces of the 144-dimensional space over $GF(4)$, and their dimensions, 6, 16 and 32 respectively, can be calculated from the character table. Since the two subgroups generate $3{\cdot}Suz$, their centralizers intersect in the fixed space of $3{\cdot}Suz$, which has dimension 1, so the total number of cases left to consider is $4^{32-6-16+1} = 4^{11}$. This is a large but manageable number of cases.

We check these cases by looking at the orders of certain words in our three

generators, to see if they are compatible with the orders we already know for the same words in the corresponding generators for $6{\cdot}Suz$. Most possibilities are quickly eliminated, and we are left eventually with three generators for the required 90-dimensional representation of $6{\cdot}Suz$.

Again, we take the direct sum of this representation and its dual, and adjoin the outer automorphism by the same method as in the previous section, find standard generators for the full group and write the result over $GF(2)$. Finally, we write the representation as a $GF(4)$-semilinear representation by finding a standard basis for one of the two generators for the normal subgroup of order 3.

Note that there is now a choice involved here, which is tied up with the question of which group of order 3 to quotient out. (See Section 5.2 below.)

4.3 The semilinear-monomial representation on 32760 points

This is a representation of $3^{12}{:}2{\cdot}Suz{:}2$, so the problem of which group we have does not affect this part of the representation.

The semilinear-monomial action of $3^{1+12}{\cdot}2{\cdot}Suz{:}2$ on 32760 2-spaces can be most easily described as the action by conjugation on a certain class of 3^2-subgroups of 3^{1+12}. These are the subgroups which are stabilized by a subgroup $U_5(2)$. The three cyclic subgroups in such a 3^2 which lie outside the centre of 3^{1+12} can be identified with the three non-zero vectors of $GF(2)^2$, and any permutation of these three cyclic subgroups (realised by an element of $3^{1+12}{\cdot}2{\cdot}Suz{:}2$) can be encoded as a permutation of the three non-zero vectors of $GF(2)^2$, and therefore as a 2×2 matrix over $GF(2)$.

As we have just observed, the result is a representation of $3^{12}{:}2{\cdot}Suz{:}2$, so we can equally well start from the split extension $3^{1+12}{:}2{\cdot}Suz{:}2$ rather than one of the non-split ones. This means that there is a straightforward construction from the 14-dimensional representation described in Section 3.4.

Indeed, there is an even simpler construction from the 13-dimensional quotient thereof, which represents exactly the group $3^{12}{:}2{\cdot}Suz{:}2$ that we need. We simply take the action on a certain orbit of vectors, and interpret the results as follows. The first coordinate ($\lambda = 0$, 1 or 2) is interpreted as the non-zero scalar ω^λ in $GF(4)$ (that is, 1, ω or $\overline{\omega}$ respectively), and the remaining 12 coordinates as one of the 2×32760 minimal vectors of the complex Leech lattice modulo $\theta = \sqrt{-3}$. We choose arbitrarily one

of each pair of vectors as the 'positive' one, and interpret negation as the automorphism $\omega \mapsto \overline{\omega}$ of $GF(4)$.

5 The representation of $3^{2+5+10}{:}(M_{11} \times 2^2)$

5.1 The subgroup $3^{1+1+5+5+5}{:}(M_{11} \times 2^2)$

The next step is to find suitable 'standard generators' for the subgroup

$$3^{1+1+5+5+5}{:}(M_{11} \times 2^2)$$

of $3^{1+12}{\cdot}2{\cdot}Suz{:}2$, so that the action of the desired outer automorphism is clearly visible. We chose to take elements F, G, H, I, J, K defined as follows. First take a complement $M_{11} \times 2^2$, which is easily seen to be unique up to conjugacy, and take H, I to be standard generators for M_{11}, in the sense of [13]. That is, H has order 2 and I has order 4, with HI of order 11 and $(HI)^2(HIHI^2)^2HI^2$ of order 4. Then we take F and G to be involutions centralizing H and I. (To specify these precisely, we take F to be the central involution of $2{\cdot}Suz$, and G to be the other involution which does not centralize the second central factor of the O_3-subgroup. This ensures that the required outer automorphism interchanges F and G.)

Next, we take an element of order 8 in M_{11}, such as $(HI)^3IHI$, and consider (non-trivial) elements of the O_3-subgroup which are inverted by this element of order 8. There are just four of them, up to inversion, and we let J be the one which is centralized by F (and inverted by G), and K be the one which is centralized by G (and inverted by F). As before, there are inner automorphisms, given by G and F respectively, which swap J with J^{-1}, and K with K^{-1}, so all choices are equivalent.

To make these elements in practice, we calculated the following words in the standard generators C, D, E.

$$\begin{aligned}
\alpha &= (CD(CDCD^2)^2(CD)^2(CDCD^2)^2)^{11} \\
\beta &= (CD)^{-6}(CD(CDCD^2)^2)^2(CD)^6 \\
\gamma &= (\alpha\beta^2\alpha\beta(\alpha\beta\alpha\beta^2)^2)^{10} \\
\delta &= (\alpha\beta\alpha\beta^2)^{-4}\alpha(\alpha\beta\alpha\beta^2)^4 \\
\varepsilon &= (\alpha\beta)^{-1}((\alpha\beta)^3\beta)^3\alpha\beta \\
F &= \beta^5
\end{aligned}$$

$$\begin{aligned} G &= ((\delta\varepsilon)^3\varepsilon)^{11} \\ H &= \delta G \\ I &= \varepsilon G \\ \zeta &= (HI)^3 IHI \\ J &= (\zeta(\zeta^2\gamma)^3\zeta)^{-1}(\zeta^2\gamma)^2 \\ \eta &= (D^{-1}EDG)^2 \\ K &= (\zeta(\eta\zeta^2)^4)^{-1}(\eta\zeta^2)^4\zeta \end{aligned}$$

By construction, the outer automorphism that we need to adjoin now acts by centralizing H and I (since these generate a complementary M_{11}), swapping F with G (thereby extending 2^2 to D_8), and (consequently) swapping J with K.

5.2 Which is which?

Or, as one of us quipped, which is witch? Clearly the witch performs magic and brings forth the Monster, and we need to know therefore, which of the two almost indistinguishable groups of the shape $3^{1+12}{\cdot}2{\cdot}Suz$ is the witch?

In theoretical terms, we work as usual in the triple cover, and find the corresponding triple cover of $3^{1+1+5+5+5}{:}(M_{11}\times 2^2)$. We ask which quotient of this triple cover admits an automorphism mapping F, G, H, I, J, K in order to G, F, H, I, K, J. It turns out that only one of them does. The calculations needed to see this can be done already in the 38-dimensional representation described in Section 3.4. Here we find that the element

$$(HJIK)^6 IK(HJIK)^2 IK(HJIKIK)^2$$

has order 24, while its image under the required outer automorphism,

$$(HKIJ)^6 IJ(HKIJ)^2 IJ(HKIJIJ)^2$$

has order 8. It follows that we must quotient by

$$((HJIK)^6 IK(HJIK)^2 IK(HJIKIK)^2)^8$$

in order to get the correct group $3^{1+12}{\cdot}2{\cdot}Suz{:}2$. This relation can now be tested in any desired representation, to see if we have the correct group.

5.3 The action of $3^{1+12}{\cdot}2{\cdot}Suz$ on vectors

At this stage we know the precise action of elements of the subgroup $3^{1+12}{\cdot}2{\cdot}Suz$ on vectors, and so is possible to code it up into a procedure. To avoid some of the technical problems to do with 'semi-tensor products', we leave off the outer automorphism, so that all we need to do is to take the correct Frobenius automorphs of our representations. The changes of basis decribed below will only change the data input to this procedure, not the procedure itself.

Thus we take the $GF(4)$-representations of degree 90 and 729 for $3^{1+12}{:}6{\cdot}Suz$, and first determine which of the two tensor products $90 \otimes 729$ and $\overline{90} \otimes 729$ represents a group satisfying the relation given at the end of Section 5.2. (Here $\overline{\ }$ denotes the Frobenius automorphism $x \mapsto x^2$ of $GF(4)$.)

To describe the action of the group on $GF(2)$-vectors of length 196882, we first divide the vector into three pieces, of lengths 131220, 65520 and 142. These will be acted on by the tensor product, the semilinear monomial, and the residual 142×142 matrix, respectively. We next translate the $GF(2)$-vector of length 131220 into a $GF(4)$-vector of length 65610 in the usual way, and then fold it up into a 90×729 matrix. We can then apply an element of the group to this by multiplying on the right by the corresponding 729×729 matrix, and on the left by the *transpose* of the corresponding 90×90 matrix. Finally we translate the resulting 90×729 matrix over $GF(4)$ back into a $GF(2)$-vector of length 131220.

The semilinear-monomial part of the action can be described by a permutation of 32760 subspaces of dimension 2, followed by suitable actions on each of these 2-spaces. Finally, the last 142 coordinates of the vector are acted on by a 142×142 matrix in the usual manner.

Thus an element of $3^{1+12}{\cdot}2{\cdot}Suz$ is stored as

- a 90×90 matrix over $GF(4)$ (the transpose of our original matrix)
- a 729×729 matrix over $GF(4)$
- a permutation on 32760 points
- a list of 32760 elements of $S_3 \cong GL_2(2) \cong \Gamma L_1(4)$
- a 142×142 matrix over $GF(2)$

and the action on the space is as specified above.

It follows that we can also perform multiplications in this group by a straightforward procedure—remembering, among other things, to multiply the 90×90 matrices in the reverse order, since they have been transposed.

5.4 The structure of the module

Let us now re-interpret what we have done, in the more usual language of modules for the $GF(2)$ group algebras. None of this material is required in later sections, so we do not bother to prove anything. The reader who is only interested in the proof is advised to skip this section. Nevertheless it may be helpful to see the underlying structure behind all the machinery we develop.

The module of dimension 196882 for the group $3^{1+12}{\cdot}2{\cdot}Suz{:}2$ has the following structure:

$$\begin{array}{c} 17496 \\ 96228 \oplus 65520 \oplus 142 \\ 17496 \end{array}$$

where each number stands for an absolutely irreducible module of the given dimension. It is clear therefore that the centralizer of this group in $GL_{196882}(2)$ has order 2.

Restricting to $3^{1+1+5+5+5}{:}(M_{11} \times 2^2)$, we find that 17496 becomes $5832 \oplus 11664$, while 96228 becomes $32076 \oplus 64152$. The 65520 is less easy to unravel, but with the help of [11] and the Meataxe we can show that the restriction is

$$32076 \oplus \begin{array}{c} 5832 \\ 5832 \end{array} \oplus \begin{array}{c} 1782 \\ 1782 \end{array} \oplus 17820 \oplus 264 \oplus 132.$$

Since the 142 restricts as $132 \oplus 10$, we have the complete decomposition as follows:

$$64512 \oplus 32076ab \oplus 11664aa \oplus \begin{array}{c} 5832ab \\ 5832ab \end{array} \oplus \begin{array}{c} 1782 \\ 1782 \end{array} \oplus 17820 \oplus 264 \oplus 132ab \oplus 10.$$

Note that we have not proved that the gluing of the constituents is precisely as stated here. This actually follows from explicit calculations in Sections 6.2 and 6.3, where we determine the centralizer of the module, and hence we can eliminate all other possibilities for the module structure.

Our final task is to find the correct involution which normalizes this group. It must swap the two constituents of degree 32076, and the two of degree 132, as well as the two uniserial summands of degree $11664 = 5832 + 5832$. Since there is an involution centralizing each of these two uniserial modules,

and a group $GL_2(2) \cong S_3$ centralizing the direct sum of two isomorphic modules of degree 11664, we have a total centralizer of order 48, which means that there are in principle 48 cases to consider. However, half of these give an automorphism which squares to a non-trivial automorphism of the non-irreducible summands, so can be eliminated. One-third of those that are left involve an element of order 3 in the $GL_2(2)$, so these can also be eliminated, as we are looking for an involution. Thus we are left with just 16 involutions to consider. These 16 cases reduce to 8 if we take into account the action of the centralizer of the group $3^{1+12}{\cdot}2{\cdot}Suz{:}2$.

6 The extension to $3^{2+5+10}{:}M_{11} \times D_8)$

6.1 First steps towards a standard basis

We now need to find a standard basis for the 196882-space in terms of the original list of generators F, G, H, I, J, K, and then again in terms of the automorphic list, G, F, H, I, K, J. It is neither sensible nor practical to try to use the general-purpose standard-basis programs which exist in various versions of the Meat-axe package. Instead we use various refinements of the same general principle in order to ensure that our matrices remain as 'nice' and as sparse as possible. The most important thing turns out to be to replace the usual 'depth-first' exploration of the space (i.e. applying all the generators to one vector at a time) by a 'breadth-first' approach (applying one generator at a time to all the vectors).

The first thing to note is that all the representations which go to make up the 'tensor product' part of the space, become semilinear-monomial when restricted to the subgroup. We therefore change basis on the 1548- and 180-dimensional $GF(2)$-representations to exhibit this structure. This task, like many, can be accomplished by a suitable standard basis algorithm, applied to each irreducible constituent separately. For example, on the 24-dimensional $GF(2)$-constituent, we find the fixed 2-space of a subgroup $3^5{:}L_2(11)$ of our fixed $3^5{:}M_{11}$, and find its 12 images under the latter group. On the 132-dimensional constituent we do the same with the subgroup $3^5{:}S_5$. On the 1458-space, we first need to find the unique subgroup of order 3^7 in 3^{1+12} which is invariant under our $3^5{:}M_{11}$. Then the fixed space of this 3^7 again has dimension 2, and we take the 729 images of this 2-space to form our basis.

An important question to ask here is, given a semilinear-monomial representation, is the basis with respect to which it is semilinear-monomial essentially unique? In other words, is the set of permuted subspaces determined? Such a question can be answered by looking in detail at the structure of the group, as these representations are nothing more than representations induced from the 2-dimensional representation of an S_3-quotient of a suitable subgroup. We need to know, therefore, to what extent the subgroup from which the representation is induced, and the representation which is induced, are unique.

It turns out that in some cases they are unique, while in two, namely those with $GF(2)$-dimension 3564 and 17820, they are not.

The question can be re-phrased as, to what extent is the 'diagonal' subgroup of the 'monomial' group determined? In the 5832, for example, the point stabilizer in $3^{1+1+5+5+5}{:}(M_{11} \times 2^2)$ has index 5832, and has shape $3^{1+1+5+5}{:}(L_2(11) \times 2^2)$. Now this can be re-written in the form $3^{1+10}(S_3 \times 2 \times L_2(11))$, and since $L_2(11)$ acts irreducibly on the 3^5, there is a unique S_3 quotient to induce up from. Moreover, the point stabilizer is determined by its index and the kernel of the representation, which has order 3.

In the 1782, on the other hand, the kernel of the representation has order 3^2, and modulo this the point stabilizer is $3^{5+5+1}A_6.2.2$. Thus we have again a unique S_3 quotient from which to induce up. However, this time there are four different subgroups of the same shape, permuted by the outer automorphism group, and therefore there are four different ways of writing this group as a semilinear monomial.

Each of the remaining cases is analogous to one of these.

In the cases where the basis is essentially unique, we adopt a variant of 'standard basis' similar to one that is used for permutation representations. This is described in general terms in Section 2.2, and in more detail in Section 6.2 below. In the small constituents, which have $GF(2)$-dimensions 132 and 264, we used the general purpose standard basis algorithm, on the grounds that they are small and any method would do. In the other cases, we devised an *ad hoc* method described in Section 6.3.

6.2 Semilinear-monomial standard basis

As explained in Section 2.2, this is essentially a variant of permutation standard basis. To put a permutation group into standard form with respect to a set of 'standard generators', it is first necessary to choose a word, or

set of words, in the standard generators, with the property that they have a small number (preferably 1) of fixed points in common. This fixed point (or one of these fixed points) then provides a 'seed' to the spinning algorithm, which produces the remaining points in the orbit by applying the generators in a specified order, and writing down in order all the points which are distinct from the previously obtained points. The result is a list of the points in a canonical order, which can be used to conjugate the permutations into standard form.

In our case, our 'points' are 2-dimensional spaces, so we also need to specify one of the six bases for our seed point, and carry this basis with us through the generators. The result now is a semilinear-monomial element which conjugates our representation into standard form.

One slight problem which we encountered was that it was not always possible to determine the seed point (with its basis) uniquely, and therefore our choice of standard form was a little more arbitrary than usual. This also means that in testing equivalence, or in finding all elements which exhibit an equivalence, we must try all possible seeds for one of the representations.

On the other hand, we are free to choose our generators and our spinning algorithm in any way we like, and we used this freedom to order the basis vectors in a nice way, which enabled us to simply 'write down' a large part of the extra generator for the Monster.

The representations which we have to deal with here are the semilinear-monomial representations on 32076, 11664, 16038 and 5832 points, all coming from the semitensor product, and those on 16038 and 5832 points coming from the original semilinear-monomial on 32760 points for the group $3^{1+12}{\cdot}2{\cdot}Suz{:}2$. Those on 32076 and 11664 points are fixed by the extra element which we are trying to construct, while those on 16038 and 5832 points are interchanged in pairs.

In each case we need, as far as possible, to find words in the standard generators which give the stabilizer of a point, in order to find a suitable seed point for the standard basis algorithm. In practice, we only needed a single element in the point stabilizer for these cases. The full stabilizer was needed, however, in the semilinear monomials on 1782 and 8910 points, which are discussed in the next section.

In the cases of 32076 and 16038 points, we took the element $(HI)^3((HI)^2I)^2HI^2$ of order 5, which fixes six and three points respectively, while in the cases of 11664 and 5832 points, we took the element HI of order 11, which fixes four and two points respectively. We now briefly discuss these four cases

individually.

Taking the two cases of 5832 points first, we find in one case that the two fixed points of HI are swapped by F and acted on by G as a transposition of S_3, and *vice versa* in the other case.

We take an arbitrary basis (6 choices) of an arbitrary fixed point (2 choices) as our seed in the first case, and conjugate the representation into standard form. In the second case we try all 12 possibilities, to see which ones conjugate the second representation into the same standard form. We find that exactly two of the 12 seeds work (as expected from the discussion in Section 5.4), and thus we have two possibilities for the element which interchanges the two semilinear monomials on 5832 points (since it has order 2). We can order the points in such a way that one of these elements acts by bodily interchanging the two blocks of 5832 points.

The 11664 case is very similar. In this case we have four fixed points of HI, permuted regularly by $\langle F, G\rangle \cong 2^2$. Taking an arbitrary seed for the first ordering of the generators, we now need to check 24 cases for the second ordering. It turns out that 6 cases conjugate the second representation into the standard form, so there are apparently 6 possibilities for the action of the extra element. However, two of them have order 6, while our desired element is an involution, so we are left with four cases. Each of these can be written as a semilinear monomial on 11664 points.

The 16038 case is actually the simplest. Of the three fixed points of the element $(HI)^3(HIHI^2)^2HI^2$ of order 5, just one is fixed by F, so we take one of the 6 bases for this point as our seed. Thus we only need to check 6 cases for the other ordering of the generators on the other 16038 representation, and we find that exactly one of these six cases works. Thus the element swapping the representations is uniquely determined.

Similarly on the 32076, we take one of the two fixed points of the element $FG(HI)^3(HIHI^2)^2HI^2$ of order 10 as our seed, and check 12 cases to find that again there is only one possibility.

The result of all this is that the action of the extra element on the corresponding space of $GF(4)$-dimension

$$32076 + 11664 + 2 \times (16038 + 5832) = 87480$$

(so $GF(2)$-dimension 174960) can be described as a semilinear monomial on 43740 points together with a bodily interchange of the remaining two blocks of 21870 points.

6.3 A standard basis for the 1782 and 8910

In these two cases, we found that there were four essentially distinct bases with respect to which the representation appeared as a semilinear monomial (permuted by the outer automorphism group $2 \cdot S_4$ of $3^{2+5+10}{:}M_{11}$), and that therefore we had to swap two of these. For the first basis, we simply applied the same algorithm as above, with a careful choice of spinning algorithm.

In order to find the second basis, however, it was necessary to determine the seed as a vector in the entire space, no longer restricted to being in one of our favoured 2-spaces. This required a new idea.

We start by describing the 1782 case. In this case we use first the subgroup $\langle H^I, I^{(HI^2)^2} \rangle \cong A_6$ of M_{11}. This subgroup has two fixed points out of the 1782, which generate a 4-space over $GF(2)$. We can choose a basis for this space such that F and G each act as

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

and take (say) the first basis vector as our seed.

For the precise description of our spinning algorithm we need to define the elements $J_n = (HI)^{-n} J (HI)^n$ and $K_n = (HI)^{-n} K (HI)^n$. Our seed is centralized by $J = J_0$ and K_n for all n. Finally we find that the element $((HI)^3 IHI)$ extends our A_6 to M_{10} inside M_{11}. Thus by applying all the words

$$F^\alpha {J_1}^\beta {J_2}^\gamma {J_3}^\delta {J_4}^\varepsilon ((HI)^3 IHI)^\zeta (HI)^\eta$$

for $0 \leq \alpha \leq 1, 0 \leq \beta \leq 2, 0 \leq \gamma \leq 2, 0 \leq \delta \leq 2, 0 \leq \varepsilon \leq 2, 0 \leq \zeta \leq 1, 0 \leq \eta \leq 10$ to our seed vector we obtain 3564 linearly independent $GF(2)$-vectors. We take this as our standard basis, in reverse lexicographic order of the words $\alpha\beta\gamma\delta\varepsilon\zeta\eta$.

Now we need to turn our attention to the second ordering of the generators, to get the second standard basis for the space. This is no longer in the same semilinear-monomial representation, but all is not lost. Note that our first seed vector was centralized by J and K_n. Therefore our second seed vector must be centralized by K and J_n, which means that it is in the space spanned by the first 162 points (i.e. the first 324 $GF(2)$-coordinates). Moreover, it is fixed by H^I and $(HI^2)^{-2} I (HI^2)^2$, which brings us into a 4-dimensional subspace. Using the action of F and $[J_1, K_2]$ on the first seed

vector, and the action of G and $[K_1, J_2]$ on the second, we can reduce the number of possibilities to just two, which is what we would expect from Section 5.4.

In both cases, therefore, we take the images of the appropriate $GF(2)$-vector of length 324 under

$$F^\alpha {K_1}^\beta {K_2}^\gamma {K_3}^\delta {K_4}^\varepsilon ((HI)^3 IHI)^\zeta (HI)^\eta$$

for $0 \leq \alpha \leq 1$, $0 \leq \beta \leq 2$, $0 \leq \gamma \leq 2$, $0 \leq \delta \leq 2$, $0 \leq \varepsilon \leq 2$, $0 \leq \zeta \leq 1$, $0 \leq \eta \leq 10$. The fact that HI simply permutes 11 blocks of size 324 bodily, means that this part of the action can be 'hard-wired', and only a single 324×324 matrix needs to be stored.

The 8910 case is very similar. We find by a random search that the group generated by $x = (HI)^{-2}H(HI)^2$ and $y = (HI^2)^{-1}I(HI^2)$ has a unique orbit of size 2 on the 8910 points, in which y interchanges the two points, while x centralizes one and acts non-trivially on the other. We take the former as our seed point, and choose one of the two vectors in it that are swapped by F as our seed vector. To get our full standard basis, therefore, we apply the words

$$F^\alpha {J_0}^\beta {J_1}^\gamma {J_2}^\delta {J_3}^\varepsilon y^\zeta (I^{-1}HI^2)^\eta ((HI)^3 (HIHI^2)^2 HI^2)^\theta$$

for $0 \leq \alpha \leq 1$, $0 \leq \beta \leq 2$, $0 \leq \gamma \leq 2$, $0 \leq \delta \leq 2$, $0 \leq \varepsilon \leq 2$, $0 \leq \zeta \leq 1$, $0 \leq \eta \leq 10$, $0 \leq \theta \leq 5$. Now to find the automorphic basis, we first find the fixed space of J_n and x, which has dimension 3, and consider the action of the other elements on this space. Spinning up the possible seed vectors under the words automorphic to the above, we find only one case which gives rise to an involutory automorphism. Thus there is a unique possibility for the action of the automorphism on the corresponding 17820-space. Just as before, our careful choice of standard basis enables us to specify the action by a single 324×324 matrix.

6.4 The action of the standard basis elements

We have now constructed all the relevant standard bases, so we can write down all possibilities for the element which maps the old standard basis to the new one. As we have seen, such an element T_i acts on the 196882-space as follows. On the first 174960-space, it acts as a certain semilinear monomial, as calculated in Section 6.2. The next 3564-space is acted on by a block diagonal matrix, with the same 324×324 matrix repeated 11 times on the

diagonal. Similarly, the next 17820-space is determined by another 324×324 matrix, repeated 55 times. Finally we lump together the last 538 coordinates, and act on them by a 538×538 standard basis matrix in the usual way.

Thus the 16 possibilities $T_1, \ldots, T_{16}$ for the extra generator of the Monster are stored as quadruples:

- a permutation on 87480 points
- a list of 87480 elements of S_3
- a pair of 324×324 matrices over $GF(2)$
- a 538×538 matrix over $GF(2)$

and the action on the vectors of 196882-space is as described.

6.5 Investigating the 16 cases

The 16 cases arise from the following ambiguities. First, the semilinear monomial piece with $GF(2)$-dimension 3564 has the module structure of two isomorphic 1782-dimensional pieces glued one on top of the other. The standard basis is therefore only determined up to multiplication by the involution in the centralizer of this representation. Second, the two semilinear monomials with $GF(2)$-dimension 11664 each have two standard bases as defined above, so we can swap them one way round or the other. Finally, the semilinear monomial with $GF(2)$-dimension 23328 has four standard bases.

With hindsight, it is clear that these 16 cases occur in pairs, interchanged by an involution which commutes with the entire group $3^{1+12}{\cdot}2{\cdot}Suz{:}2$, and that therefore there are only 8 cases to check. This involution can be described by acting on the 90-dimensional $GF(4)$-module in the same way as the central involution of $6{\cdot}Suz$, and acting trivially on all the other representations, including the 729-dimensional $GF(4)$-representation. (Thus its action on the tensor product is *not* the same as the central involution of any copy of $6{\cdot}Suz$.) However, we actually checked all 16 cases, as follows.

We took a random vector, and applied first the element A from $3^{1+12}{\cdot}2{\cdot}Suz$, and then the extra generator T_i, and repeated 119 times, checking at each stage whether the image vector was equal to the original vector. We found that in 14 cases, the image vector was never equal to the original, which means that AT_i has order bigger than 119, so cannot be in the Monster. In

the other two cases, the 60th image was equal to the original, which strongly suggests that AT_i has order 60 in these cases. For our peace of mind, we then tested $ADET_i$, which has order (divisible by) 94, and $ADEGT_i$, which has order (divisible by) 71, in these two cases.

7 Conclusion

Since we know that the Monster does have a representation with all the properties we have used, and since we have eliminated all possibilities except one, it follows that this last case is in fact the Monster.

We can now calculate in the Monster in the following sense. We can make any element of $3^{1+12}{\cdot}2{\cdot}Suz$ quickly, and apply it to an arbitrary vector. We can also apply the extra generator T to any vector. Thus we can work with elements of the Monster written in the form $S_1TS_2T\ldots$, for arbitrary $S_i \in 3^{1+12}{\cdot}2{\cdot}Suz$, provided these words do not get too long. We can guess (correctly, we believe!) the order of such an element by acting on a random vector by S_1, then by T, then by S_2, and so on, and repeating until the vector returns to its starting point. This gives a divisor of the element order which will in practice be equal to the element order, although we cannot prove this.

We can improve these 'vector-order' calculations to real calculations of the order, at the cost of doubling the number of vectors. To do this, we use the elements of orders 71 and 94 found above. First note that if a vector is fixed by an element of order 71, than its full stabilizer is isomorphic to a subgroup of $L_2(71)$, since all maximal subgroups with order divisible by 71 are of this form. Second, a vector fixed by an element of order 47 has its full stabilizer contained in $2{\cdot}B$, for a similar reason. But if the latter vector is not fixed by the element of order 94, then its stabilizer is a proper subgroup of $2{\cdot}B$, which implies that it is a subgroup of 47:23. Now $L_2(71)$ has no elements of order 47 or 23, so the intersection of these two stabilizers is trivial.

Acknowledgements. The authors would like to thank John Bray, Klaus Lux, and Chris Parker, for many helpful comments and conversations.

References

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

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

[3] R. L. Griess, The Friendly Giant, *Invent. Math.* **69** (1982), 1–102.

[4] S. A. Linton, The art and science of computing in large groups, in *Computational algebra and number theory (W. Bosma and A. van der Poorten, eds.)*, pp. 91–109. Kluwer, 1995.

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

[6] S. P. Norton, The anatomy of the Monster. I, in *The Atlas 10 years on: Proc. Birmingham Conf., 1995, (R. T. Curtis and R. A. Wilson, eds.)*, pp. 198–214. London Math. Soc. Lecture Note Series, Cambridge University Press, 1998.

[7] 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.

[8] M. Schönert *et al.*, *GAP 3.4 Manual (Groups, Algorithms, and Programming)*, Lehrstuhl D für Mathematik, RWTH Aachen, 1994.

[9] J. G. Thompson, Finite-dimensional representations of free products with an amalgamated subgroup, *J. Algebra* **69** (1981), 146–149.

[10] P. G. Walsh, Computational study of the Monster and other sporadic simple groups, Ph. D. thesis, Birmingham, 1996.

[11] R. A. Wilson, The complex Leech lattice and maximal subgroups of the Suzuki group, *J. Algebra* **84** (1983), 151–188.

[12] R. A. Wilson, A new construction of the Baby Monster, and its applications, *Bull. London Math. Soc.* **25** (1993), 431–437.

[13] R. A. Wilson, Standard generators for sporadic simple groups, *J. Algebra* **184** (1996), 505–515.

[14] R. A. Wilson *et al.*, A world-wide-web atlas of group representations, http://www.mat.bham.ac.uk/atlas/