

The Order of the Monster Finite Simple Group

Gerald Höhn* and Martin Seysen†

August 1, 2025

In memory of John Conway and Simon Norton, whose work continues to inspire.

Abstract

We determine the order of the largest of the twenty-six sporadic simple groups known as the Monster, using a straightforward computational approach. The Monster is here defined as a subgroup of the symmetry group of the 196884-dimensional Griess algebra generated by a group of type $2_+^{1+24}.\text{Co}_1$ and an additional triality automorphism. Our approach is based on counting arguments for certain idempotents of the Griess algebra called *axes*. Our proof is self-contained, requiring only established properties of the Conway group as the automorphism group of the Leech lattice, and some of its subgroups.

Although our approach is conceptually simple, it requires extensive calculation inside a 196884-dimensional matrix group that current computer algebra systems cannot easily handle directly. Instead, we use the software package *mmgroup*, developed by the second author, which supports fast calculations inside the Monster. To our knowledge, this paper contains the first self-contained computation of the order of the Monster.

The Monster also acts on the Moonshine module V^\natural , which is a vertex operator algebra of central charge $c = 24$. We provide a new proof that the Monster is the *full automorphism group* of the Griess algebra and of the Moonshine module using Borcherds' proof of the Monstrous Moonshine conjectures. In addition, we show that the Monster has exactly two conjugacy classes of involutions. The order of the Baby Monster, the second largest of the sporadic simple groups, is also determined.

1 Introduction

In this paper, we will determine the order of the Monster finite group \mathbb{M} assuming only established properties of the Leech lattice and its automorphism group, and using extensive computations performed with the software package *mmgroup* [Sey20b] developed by the second author.

The Monster is the largest of the twenty-six sporadic finite simple groups. Its existence was predicted independently at the end of 1973 by Bernd Fischer and Robert Griess. Shortly afterwards, its presumptive order was computed to be

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

*Department of Mathematics, Kansas State University, USA, gerald@monstrous-moonshine.de

†München, Germany, m.seysen@gmx.de

$$= 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.$$

The Monster was first constructed by Griess in 1982 [Gri82] as a group of automorphisms of a 196884-dimensional non-associative algebra, called the *Griess algebra* and denoted by \mathcal{B} . It was later discovered that the Griess algebra is part of a larger infinite-dimensional structure called the *Moonshine module* and denoted by V^\natural [Bor86,FLM88]. The Moonshine module is an extremal vertex operator algebra of central charge 24 with the Monster as its symmetry group. Vertex operator algebras are a mathematical formalization of two-dimensional conformal field theories first studied in mathematical physics.

The automorphism group of the Griess algebra — or, alternatively, the Moonshine module — is known to contain a visible subgroup G_{x_0} of type $2_+^{1+24}.\text{Co}_1$ (the centralizer of an involution x_{-1}) and an additional *triality automorphism* τ of order 3. The Monster is defined as the subgroup generated by these:

$$\mathbb{M} = \langle G_{x_0}, \tau \rangle \subseteq \text{Aut}(\mathcal{B}).$$

Several group-theoretical properties of the Monster, like its finiteness, can be understood in terms of vertex operator algebras. Carnahan has recently provided upper and lower bounds for the order using basic group theory, the theory of orbifolds of vertex operator algebras, and Borchers' proof of the Monstrous Moonshine conjectures [Car23]. However, the order of the Monster has never been determined directly by using only properties of the Griess algebra or the Moonshine module alone.

The only published proof for the order given above of the Monster can be found in [GMS89], Corollary 3.7.3. One starts by identifying the double cover $2.B$ of the Baby Monster as the centralizer of an involution in \mathbb{M} . Then the order of the Monster is obtained by enumerating the nine double cosets in $2.B \backslash \mathbb{M} / 2.B$, and by computing the number of cosets in $2.B \backslash \mathbb{M}$ contained in each of these double cosets. In [GMS89], properties of the Baby Monster B as well as of two Conway groups Co_1 and Co_2 , the Thompson group Th , the Harada-Norton group HN , and the two Fischer groups Fi_{22} and Fi_{23} were used. In particular, their orders are assumed to be known in advance. The obvious disadvantage is that all of these groups have to be studied beforehand, either theoretically or computationally.

A strategy for computing the order of the Monster. Our approach in this paper is conceptually much simpler. We consider the permutation action of \mathbb{M} on certain idempotents in \mathcal{B} called *axes* — or *Ising vectors* if considered in V^\natural . Associated with each axis is a $2A$ involution in \mathbb{M} .

Denote by \mathbb{M}_u the stabilizer of an axis u in \mathbb{M} . Let X^+ be the \mathbb{M} -orbit of an explicitly given axis v^+ and let X^- be the \mathbb{M}_{v^+} -orbit of an explicitly given axis v^- in X^+ orthogonal to v^+ . We will determine the sizes of X^+ and X^- . Using the fact that the common stabilizer $\mathbb{M}_{v^+} \cap \mathbb{M}_{v^-}$ of v^+ and v^- is contained in G_{x_0} , one shows $\mathbb{M}_{v^+} \cap \mathbb{M}_{v^-} \cong 2^{1+23}.\text{Co}_2$. It follows that

$$|\mathbb{M}| = |X^+| \cdot |\mathbb{M}_{v^+}| = |X^+| \cdot |X^-| \cdot |2^{1+23}.\text{Co}_2|.$$

The basic strategy to determine the size of X^+ and similarly X^- is as follows. The decomposition of X^+ into twelve G_{x0} -orbits and the structure of their stabilizers has been given in [Nor98] without proof. One can decompose these orbits further into orbits under the group $N_{x0} \cong 2_+^{1+24} \cdot (2^{11} : M_{24}) \cong 2^{2+11+22} \cdot (M_{24} \times 2) < G_{x0}$ by considering the action of stabilizers of the twelve G_{x0} -orbits on $\Lambda/2\Lambda \cong 2^{24}$, where Λ denotes the Leech lattice. Using the software package `mmgroup`, we provide explicit representatives of axes in the Griess algebra for each of these N_{x0} -orbits and explicit generators for the stabilizers of the twelve G_{x0} -orbits.

The group N_{x0} is a subgroup of index 3 in the group $N_0 = \langle N_{x0}, \tau \rangle$ of structure $2^{2+11+22} \cdot (M_{24} \times S_3)$. Let N_{xyz} be the subgroup of N_{x0} of index 2 and structure $2^{2+11+22} \cdot M_{24}$. Then N_{xyz} is normal in both N_{x0} and N_0 ; but N_{x0} is not normal in N_0 , see e.g. [Con85].

Since $N_{xyz} \triangleleft N_0$, the factor group $N_0/N_{xyz} \cong S_3$ permutes the N_{xyz} -orbits contained in an N_0 -orbit. This fact will help us to show that there are 251 N_{x0} -orbits on the axes fusing into 123 N_0 -orbits and twelve G_{x0} -orbits. Those orbits fuse into a single orbit X^+ of axes closed under the action of both G_{x0} and the triality automorphism τ .

A counting argument allows us to determine the sizes of the twelve G_{x0} -orbits and of X^+ . We also show that our explicit elements inside the stabilizers of each of the twelve G_{x0} -orbits actually generate the whole stabilizer.

An analogous approach is then taken for the action of \mathbb{M}_{v+} on X^- . There are ten $(\mathbb{M}_{v+} \cap G_{x0})$ -orbits in X^- and the triality automorphism stabilizes v^+ and fuses the ten orbits.

These calculations depend extensively on calculations in `mmgroup` describing the action of G_{x0} and the triality automorphism on the Griess algebra \mathcal{B} . We also use calculations in G_{x0} done with the software package `Magma` [BCP97]. The only information from other sporadic groups used is the knowledge of the Conway groups Co_1 and Co_2 obtained from the automorphism group of the Leech lattice, and of the Mathieu group M_{24} as the automorphism group of the binary Golay code of length 24.

Our approach is analogous to Conway's original approach to the construction of Co_0 and the computation of its order [Con69], and it generalizes this method to the third generation of the happy family [Gri82].

It may be possible to simplify our approach further by using additional structure-theoretical results about vertex operator algebras. For example, if it can be shown directly that the twelve G_{x0} -orbits contain all axes of V_2^\natural , one can use arguments similar to those in [Con69] that these orbits must fuse under the additional triality automorphism.

Combining our result with the result of Carnahan [Bor86, Car23], we also show that the Monster is the full automorphism group of \mathcal{B} and V^\natural . The previous proofs of this result given by Tits [Tit83, Tit84] all depend on certain group-theoretic characterizations of the Monster.

Outline. The paper is organized as follows. In the next section, we review basic properties of the Griess algebra and of the Moonshine module and discuss the visible parts of their automorphism groups. In Section 3, we describe the 251 different N_{x0} -orbits on the axes and how these orbits fuse under G_{x0} and N_0 . In particular, we obtain the

number $|X^+|$ of axes in the Griess algebra. In Section 4, we repeat a similar analysis for the stabilizers \mathbb{M}_{v^+} of v^+ acting on X^- . In particular, we obtain the number $|X^-|$ of axes in the \mathbb{M}_{v^+} -orbit of an axis orthogonal to a given axis v^+ . In the final Section 5, we provide several applications, including the computation of the order of the Monster and the Baby Monster. The appendices provide details of the mmgroup calculations. In Appendix C, the orbits under the action of the maximal subgroup N_0 on the axes are listed.

As a supplement to this paper, we provide the programs [HS24] which allow to verify all computational results obtained with mmgroup.

2 Construction of the Monster

The Monster can be defined either as a group of automorphisms of the 196884-dimensional Griess algebra \mathcal{B} as in [Gri82, Con85] or as a group of automorphisms of the Moonshine module vertex operator algebra V^\natural of central charge 24 as in [Bor86, FLM88]. In both approaches, the Monster is defined as the subgroup generated by two “visible” subgroups G_{x_0} and N_0 .

In the first subsection, we will review the construction of the Monster and the Griess algebra as in Conway’s paper [Con85]. We also provide proofs for certain properties of involutions and their centralizers in the Monster. Although these properties can also be deduced more abstractly from the theory of vertex operator algebras, we prefer to provide full proofs to make our computations of the order of the Monster more self-contained.

In the second subsection, we will review the construction of the Monster in terms of the Moonshine module. We need this description to be able to provide a new proof of the result of Tits that the Monster is the full automorphism group of the Griess algebra and of the Moonshine module. We will also explain how the above-mentioned properties of centralizers of involutions can be shown using vertex operator algebras.

In the final subsection, we identify the automorphism group of the Griess algebra with the automorphism group of the Moonshine module.

2.1 The Monster and the Griess algebra

We first define a 196884-dimensional common rational representation \mathcal{B} of two groups G_{x_0} of structure $2_+^{1+24}.\text{Co}_1$ and N_0 of structure $2^{2+11+22}.(M_{24} \times S_3)$ with matrix entries in $\mathbb{Z}[\frac{1}{2}]$, as in [Con85]. The Monster \mathbb{M} is defined to be the group generated by G_{x_0} and N_0 . The group $N_{x_0} = N_0 \cap G_{x_0}$ has structure $2^{1+24+11}.M_{24}$ and index 3 in N_0 , see [Con85]. We write Q_{x_0} for the normal subgroup of G_{x_0} of structure 2_+^{1+24} , which is extraspecial of plus type, and x_{-1} for the unique central involution in Q_{x_0} . We write Λ for the Leech lattice and $\Lambda/2\Lambda$ for the Leech lattice mod 2. Then $\text{Aut}(\Lambda/2\Lambda)$ is the simple group Co_1 ; and $\text{Aut}(\Lambda)$ is the group Co_0 of structure $2.\text{Co}_1$. Since Co_1 is simple, x_{-1} is also the unique central involution in G_{x_0} .

There is a natural homomorphism from $Q_{x_0} \cong 2_+^{1+24}$ to $\Lambda/2\Lambda$ with kernel $\{1, x_{-1}\}$. The *type* of a vector in $\Lambda/2\Lambda$ is the halved squared norm of its shortest preimage in Λ ; possible types are 0, 2, 3, and 4. The type of an element of Q_{x_0} is the type of its image in $\Lambda/2\Lambda$. The group Co_1 is transitive on the vectors of any given type in $\Lambda/2\Lambda$. For

$r \in Q_{x0}$ we write x_r when we consider r as an element of G_{x0} or \mathbb{M} via the injective mappings $Q_{x0} \hookrightarrow G_{x0} \hookrightarrow \mathbb{M}$, as in [Con85, Sey20a]; and we write λ_r for the image of r in $\Lambda/2\Lambda$.

Elements of $\Lambda/2\Lambda$ or Q_{x0} of type 2 are called *short*. For a short $r \in Q_{x0}$ we also write λ_r for a shortest vector in the Leech lattice that maps to the same element of $\Lambda/2\Lambda$ as r ; so λ_r has squared norm 4 in Λ . By standard properties of the Leech lattice, λ_r as an element of Λ is defined up to sign only; but $\lambda_r \otimes \lambda_r$ is uniquely defined as an element of the symmetric tensor square $S^2(\Lambda \otimes_{\mathbb{Z}} \mathbb{Q})$.

Let the element x_{Ω} of Q_{x0} be as in [Con85] and [Sey20a]. Then x_{Ω} is of type 4; and the image λ_{Ω} of x_{Ω} in $\Lambda/2\Lambda$ is equal to $v + 2\Lambda$ for any primitive $v \in \Lambda$ proportional to a standard basis vector of Λ . Let $x_{\pm\Omega}$ be the two preimages of λ_{Ω} in Q_{x0} . As in [Con85], we embed N_0 into \mathbb{M} so that the characteristic subgroup of structure 2^2 of N_0 is equal to $\{x_{\pm 1}, x_{\pm\Omega}\}$.

We take for granted all theorems proved in [Con85], §§ 1–12, and Appendices 1–7. Apart from this, we use well-known facts about the Mathieu group M_{24} and the Leech lattice and its automorphism group as stated e.g. in [CS99], Ch. 4.11, and 10–12, or [Iva09], Ch. 1. We also assume that character information for the group Co_1 and for its sections Co_2 and M_{24} from the ATLAS [CCN⁺85] is available. But we do not use the character information for the Monster or the Baby Monster in [CCN⁺85], since it is difficult to understand how this information is obtained without assuming the existence of the Monster.

Our proof relies on explicit computations in the representation \mathcal{B} of \mathbb{M} , which is called 196884_x in [Con85]. For computations in \mathcal{B} we use the mmgroup package [Sey20b, Sey21], which supports computations in \mathcal{B} . We also adopt the notation from [Sey20a], where \mathcal{B} is called ρ , and explicit generating systems for G_{x0} , N_0 , and \mathbb{M} are given. Computations in \mathcal{B} are done modulo 15. This is possible because the denominators of the entries of the matrices representing elements of \mathbb{M} are powers of 2, see e.g. [Con85, Sey20a]. For a detailed discussion of why computation modulo 15 is preferred, we refer to [Sey24].

The Monster representation. To construct the representation \mathcal{B} of the Monster we start with a representation of the group G_{x0} on the rational vector space

$$\mathcal{B} = 300_x \oplus 98280_x \oplus 98304_x, \quad \text{where}$$

300_x is the symmetric tensor square $S^2(24_x)$ of 24_x,

24_x is the representation $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ of Co_0 as the automorphism group of Λ ,

98280_x is the monomial representation of G_{x0} acting on short elements of Q_{x0} ,

98304_x is the tensor product $4096_x \otimes 24_x$ with 4096_x as in [Con85, Sey20a].

A basis vector of 98280_x is denoted by X_r , where r is a short element of Q_{x0} . We identify $X_{r \cdot x_{-1}}$ with $-X_r$. As in [Con85], we write $\tilde{\Omega}$ for the set of size 24 on which the Mathieu group M_{24} acts, and \mathcal{P} for the *Parker loop*. There the natural basis vectors of 24_x are denoted by i_1, j_1, \dots , for $i, j, \dots \in \tilde{\Omega}$. So we have the following basis vectors of

\mathcal{B} :

$$\begin{aligned}
\text{for } 300_x : \quad (ii)_1 &:= i_1 \otimes i_1, & (i \in \tilde{\Omega}), & \text{of norm } 1, \\
& (ij)_1 &:= i_1 \otimes j_1 + j_1 \otimes i_1, & (i, j \in \tilde{\Omega}, i \neq j), \text{ of squared norm } 2, \\
\text{for } 98280_x : \quad X_r, & (r \in Q_{x0} \text{ short}), & \text{of norm } 1, \\
\text{for } 98304_x : \quad d_1^\pm \otimes i_1, & (d \in \mathcal{P}, i \in \tilde{\Omega}), & \text{of norm } 1.
\end{aligned}$$

For the definitions of the basis vectors of 98304_x we refer to [Sey20a]. These basis vectors are orthogonal, except when equal or opposite. The basis vectors of $300_x \oplus 98280_x$ in [Con85] agree with those in [Sey20a]; the other basis vectors of \mathcal{B} agree up to sign.

The representation 300_x of G_{x0} has a natural interpretation as the space of symmetric matrices over 24_x . It has a decomposition $300_x = 1_x \oplus 299_x$, where 1_x is the space spanned by the unit matrix, and 299_x is the space of the symmetric matrices of trace zero. We write $1_{\mathcal{B}}$ for the element of 300_x corresponding to the unit matrix divided by four.

To obtain a representation \mathcal{B} of the Monster \mathbb{M} , we also have to describe the action of a *triality* element τ on \mathcal{B} , such that N_0 is generated by N_{x0} and τ . For details we refer to [Con85, Sey20a]. Then \mathbb{M} fixes $1_{\mathcal{B}}$ in \mathcal{B} ; so we have a decomposition

$$\mathcal{B} = 1_x \oplus 196883_x, \quad \text{with } 196883_x = 299_x \oplus 98280_x \oplus 98304_x,$$

where $1_x = \text{Span}(1_{\mathcal{B}})$ and 196883_x are representations of \mathbb{M} .

We write (a, b) for the Monster-invariant scalar product of two elements a, b of \mathcal{B} as defined in [Con85]. This is to be distinguished from the scalar product $\langle \cdot, \cdot \rangle$ in $\Lambda/2\Lambda$. We also need an algebra structure on \mathcal{B} called the *Griess algebra*, which is invariant under the action of \mathbb{M} . We adopt the definition of the Griess algebra from [Sey20a], which is compatible with the corresponding definition in [Con85], § 12. We denote the algebra product of a and b by $a * b$. That product is commutative, but not associative. We write (a, b, c) for $(a * b, c)$. Then (a, b, c) is a symmetric trilinear form on \mathcal{B} . The element $1_{\mathcal{B}}$ of squared norm $\frac{3}{2}$ acts as the identity of the Griess algebra. We write $\text{ad } a$ for the endomorphism $v \mapsto a * v$ of the vector space \mathcal{B} .

Involutions and axes. By standard properties of Q_{x0} and the Leech lattice, all short elements in Q_{x0} are in the same conjugacy class in G_{x0} .

Lemma 2.1. *The centralizer of x_r (with $r \in Q_{x0}$ short) in G_{x0} fixes precisely the subspace of \mathcal{B} spanned by $1_{\mathcal{B}}$, $\lambda_r \otimes \lambda_r$, and X_r .*

Proof: Write C_r for the centralizer of x_r in G_{x0} and \mathcal{B}_r for the subspace of \mathcal{B} fixed by C_r . Obviously, $1_{\mathcal{B}}$, $\lambda_r \otimes \lambda_r$, and X_r are in \mathcal{B}_r . The element x_{-1} of C_r negates 98304_x ; hence $\mathcal{B}_r \subset 300_x \oplus 98280_x$. Assume that $v \in \mathcal{B}_r$ has a nonzero co-ordinate at the basis vector X_s , $s \neq r$, $r \in Q_{x0}$ short. Then we can find a $t \in Q_{x0}$ (with image λ_t in $\Lambda/2\Lambda$) such that $\langle \lambda_t, \lambda_r \rangle = 0$, $\langle \lambda_t, \lambda_s \rangle = 1 \pmod{2}$. Since Λ is transitive on pairs of short vectors with a given scalar product, it suffices to find suitable elements t of Q_{x0} for one pair λ_r, λ_s with each possible scalar product $\langle \lambda_r, \lambda_s \rangle$. Possible scalar products are 0, ± 1 , ± 2 , and ± 4 ; so we can find suitable $t \in Q_{x0}$ computationally by checking random

elements of Q_{x0} . Any such t fixes X_r (so it also centralizes x_r) and negates X_s . So the co-ordinate of v at the basis vector X_s must be zero, a contradiction. Thus C_r fixes at most $300_x \oplus \langle X_r \rangle$.

The centralizer of λ_r in $\text{Co}_1 = G_{x0}/Q_{x0}$ is the simple group Co_2 . The preimage of Co_2 in G_{x0} either fixes or negates λ_r . Thus 300_x is also a representation of Co_2 . Character calculations in Co_1 and Co_2 show that the character of 300_x as a character of Co_2 is a sum $\chi_1 \oplus \chi_1 \oplus \chi_{23} \oplus \chi_{275}$ of the irreducible characters χ_1 , χ_{23} , and χ_{275} of Co_2 of dimensions 1, 23, and 275. Thus the subspace of 300_x fixed by C_r has dimension 2. \square

Corollary 2.2. *The centralizer of x_r (with $r \in Q_{x0}$ short) in \mathbb{M} fixes a one- or two-dimensional subspace of \mathcal{B} spanned by $1_{\mathcal{B}}$ and, possibly, another vector $\lambda_r \otimes \lambda_r - 4X_r$.*

Proof: The Monster \mathbb{M} fixes $1_{\mathcal{B}}$. Since all involutions x_r in Q_{x0} with r short are conjugate in G_{x0} , we may assume $x_r = x_{ij}$ in the notation of [Con85, Sey24]. The triality element τ centralizes x_{ij} . In that notation we have $\lambda_r \otimes \lambda_r = 2(ii)_1 + 2(jj)_1 - 2(ij)_1$. Let $V = \text{Span}(1_{\mathcal{B}}, \lambda_r \otimes \lambda_r, X_r) \subset \mathcal{B}$. From the action of τ described in [Sey24], Section 8.1, we see that the subspace of V fixed by τ is just the space $\text{Span}(1_{\mathcal{B}}, \lambda_r \otimes \lambda_r - 4X_r)$. \square

We want to show that the subspace fixed by the centralizer of x_r in the Corollary is in fact 2-dimensional.

Definition 2.3. *The axis of x_r (with $r \in Q_{x0}$ short) is the vector $\text{ax}(x_r) = \frac{1}{2}\lambda_r \otimes \lambda_r - 2X_r$ in \mathcal{B} .*

Lemma 2.4. *Let $v = \text{ax}(x_r)$ (with $r \in Q_{x0}$ short). Then $v*v = 16v$ and $(v, v) = 8$. The endomorphism $\text{ad } v$ of \mathcal{B} has eigenvalues 16, 0, 4, and $\frac{1}{2}$ with eigenspaces of dimensions 1, 96256, 4371, and 96256, respectively. The involution x_r negates the eigenspace of the eigenvalue $\frac{1}{2}$ and fixes the other eigenspaces of $\text{ad } v$.*

Proof: The proof is similar to the proof in [Con85], Appendix 6. Since all involutions x_r in Q_{x0} with r short are conjugate in G_{x0} , we may assume $x_r = x_{ij}$, $i, j \in \tilde{\Omega}$ in the notation of [Con85]. Then x_{ij} either fixes or negates a basis vector of \mathcal{B} . A simple calculation shows $(v, v) = 8$ for $v = \text{ax}(x_{ij})$.

Let V_X , V_Y , and V_Z be the subspaces of \mathcal{B} defined in [Con85], §11. Then V_X is the space spanned by the basis vectors X_s of 98280_x with $\langle \lambda_{\Omega}, \lambda_s \rangle = 1 \pmod{2}$. We also have $V_Y = (V_X)^{\tau}$, $V_Z = (V_X)^{\tau^{-1}}$, and $98304_x = V_Y \oplus V_Z$, see [Con85], §11. Here τ is the triality element in \mathbb{M} as above. We define V_0 to be the subspace of $300_x \oplus 98280_x$ spanned by 300_x and the basis vectors of 98280_x with $\langle \lambda_{\Omega}, \lambda_s \rangle = 0 \pmod{2}$. So we obtain the following decomposition of \mathcal{B} :

$$\left| \begin{array}{c|c|c|c} 300_x & 98280_x & 98304_x & \\ \hline V_0 & V_X & V_Y & V_Z \end{array} \right|.$$

Direct calculation shows that $\text{ad } v$ has the following eigenvalues and eigenvectors

where r, s , and $t \in Q_{x_0}$ are short and disjoint:

eigen- value	eigenvectors	dimension of subspace	
		in V_0	in V_X
16	$\frac{1}{2}\lambda_r \otimes \lambda_r - 2X_r$	1	
0	$\frac{1}{2}\lambda_r \otimes \lambda_r + 2X_r$	1	
4	$\lambda_r \otimes \lambda_s + \lambda_s \otimes \lambda_r$ if $\langle \lambda_r, \lambda_s \rangle = 0$	23	
0	$\lambda_s \otimes \lambda_t + \lambda_t \otimes \lambda_s$ if $\langle \lambda_r, \lambda_s \rangle = \langle \lambda_r, \lambda_t \rangle = 0$	$\binom{24}{2} = 276$	
0	$X_s + X_t$ if $rst = 1$	1276	1024
4	$X_s - X_t$ if $rst = 1$	1276	1024
$\frac{1}{2}$	X_s if $\langle \lambda_r, \lambda_s \rangle = \pm 1$	22528	24576
0	X_s if $\langle \lambda_r, \lambda_s \rangle = 0$	24047	22528

The scalar product $\langle \lambda_r, \lambda_s \rangle$ is 0, ± 1 , ± 2 , or ± 4 . It is ± 4 in case $r = \pm s$. If it is ± 2 then there is a short t in Q_{x_0} with $rst = 1$. Thus any vector w in $300_x \oplus \text{span}(\{X_s \mid s \in Q_{x_0} \text{ short}\})$ is a linear combination of the eigenspaces of $\text{ad } v$ stated in the table above. So these vectors w span $300_x \oplus 98280_x$.

In the subspace $300_x \oplus 98280_x$ of \mathcal{B} the involution x_r negates precisely the subspace spanned by basis vectors X_s of 98280_x with $\langle \lambda_r, \lambda_s \rangle = 1 \pmod{2}$. From the table above we see that the negated basis vectors are in the eigenspace of the eigenvalue $\frac{1}{2}$ of $\text{ad } v$, and that the fixed basis vectors are linear combinations of the other eigenspaces. Since τ centralizes x_{ij} , and the basis vectors of 98304_x are images of the basis vectors in 98280_x under $\tau^{\pm 1}$, this is true for all basis vectors of \mathcal{B} .

So the dimensions of the intersections of the eigenspaces of $\text{ad } v$ with $V_0 \oplus V_X$ can be obtained from the table above by summing up all entries of the last column for each eigenvalue. Since x_r commutes with τ , the intersections of an eigenspace of $\text{ad } v$ with V_X, V_Y , and V_Z all have the same dimension. So we have to count the entries marked as ‘in V_X ’ in the last column three times in order to obtain the dimension of an eigenspace of $\text{ad } v$. The entries for the basis vectors X_s have been computed with the Python script `eigenspaces_axis.py` in the accompanying program code; but they can also be obtained from standard properties of the Leech lattice. \square

Remark: As a byproduct of the proof of Lemma 2.4 we have obtained the dimensions of the eigenspaces of $\text{ad } v$. These dimensions have also been computed in [Iva09], Ch. 8.4. We have scaled the largest eigenvalue of $\text{ad } v$ to 16 as in [Sey24]. That eigenvalue is scaled to 64 in [Con85], and to 1 in [Iva09].

Lemma 2.5. *The centralizer $C_{\mathbb{M}}(x_r)$ of the involution x_r where $r \in Q_{x_0}$ is short fixes a two-dimensional subspace of \mathcal{B} spanned by $1_{\mathcal{B}}$ and the vector $\text{ax}(x_r)$. The vector $\text{ax}(x_r)$ is the unique vector v in that subspace satisfying $v * v = 16 \cdot v$ and $(v, v) = 8$.*

Proof: Let V^- be the -1 eigenspace of x_r . For any $w \in V^-$ of norm 1 one has $(w * w, 1_{\mathcal{B}}) = (w, w * 1_{\mathcal{B}}) = (w, w) = 1$. By Lemma 2.4 we have $(w * w, \text{ax}(x_r)) = (w, w * \text{ax}(x_r)) = \frac{1}{2}(w, w) = \frac{1}{2}$. Averaging $w * w$ over all vectors w in V^- of norm 1 yields a linear form on \mathcal{B} corresponding to a vector $u \in \mathcal{B}$ invariant under $C_{\mathbb{M}}(x_r)$ with $(u, 1_{\mathcal{B}}) = 1$ and $(u, \text{ax}(x_r)) = \frac{1}{2}$. On the other hand we have $(1_{\mathcal{B}}, 1_{\mathcal{B}}) = \frac{3}{2}$ and

$(1_{\mathcal{B}}, \text{ax}(x_r)) = \frac{1}{2}$. So u and $1_{\mathcal{B}}$ are not proportional; hence the subspace V_2 of \mathcal{B} fixed by $C_{\mathbb{M}}(x_r)$ has dimension at least 2. By Corollary 2.2 that dimension must be equal to 2.

Put $v' = \text{ax}(x_r)/16$. Then $1_{\mathcal{B}}, v'$, and $1_{\mathcal{B}} - v'$ are idempotents in V_2 with norms $\frac{3}{2}$, $\frac{1}{32}$, and $\frac{3}{2}$, respectively. Since $v' * (1_{\mathcal{B}} - v') = 0$, there are no further idempotents in V_2 . Thus $v = \text{ax}(x_r)$ is the unique vector in V_2 with $v * v = 16 \cdot v$ and $(v, v) = 8$. \square

We remark that the proof of the corresponding statement in [Con85], § 14 uses the character table of the Monster. We may now define:

Definition 2.6. (a) A 2A *involution* of the Monster is an element conjugate in \mathbb{M} to x_r for a short element $r \in Q_{x0}$.

(b) The *axis* $\text{ax}(t)$ of a 2A involution t is the unique vector $v \in \mathcal{B}$ that is fixed by $C_{\mathbb{M}}(t)$ and satisfies $v * v = 16 \cdot v$ and $(v, v) = 8$.

(c) The set of all such vectors $\text{ax}(t)$ forms the set of *axes* of \mathcal{B} .

The axis of a 2A involution is well-defined by Lemma 2.5. By Lemma 2.4 a 2A involution t can be recovered from its axis $\text{ax}(t)$ as the map that negates the $\frac{1}{2}$ eigenspace of $\text{ad}(\text{ax}(t))$ and fixes the remaining eigenspaces. This establishes a one-to-one correspondence between the 2A involutions and their axes.

Recall that the involutions x_r for short elements $r \in Q_{x0}$ are conjugate in G_{x0} and hence in \mathbb{M} . Thus all 2A involutions are conjugate in \mathbb{M} . However, we cannot exclude yet that the conjugacy class of a 2A involution in $\text{Aut}(\mathcal{B})$ is greater than the class of 2A involutions in \mathbb{M} .

It is well known that the quotient of the centralizer of a 2A involution t in \mathbb{M} by the subgroup $\langle t \rangle$ is a simple group B , known as the *Baby Monster*, the second largest of the sporadic simple groups; cf. [Gri82], Lemmas 13.2 and 13.3. In this paper, we define B as this quotient, without assuming *a priori* that B is simple.

As an application, we show:

Theorem 2.7. *The automorphism group of the Griess algebra and hence the Monster is finite.*

Proof: The same proof as in [Con85], § 13, and Appendix 6 works. The images of an axis $\text{ax}(x_r)$ in \mathbb{M} span $300_x \oplus 98280_x$, since $\text{ax}(x_r) + \text{ax}(x_r x_{-1}) = \lambda_r \otimes \lambda_r$, $\text{ax}(x_r) - \text{ax}(x_r x_{-1}) = 4X_r$. The images of 98280_x under $\tau^{\pm 1}$ cover 98304_x ; hence the images of an axis span \mathcal{B} .

So it suffices to show that an axis v has only finitely many images under the automorphism group. Otherwise there would be an axis v' very close to v that we can write as $v' = v + \theta w + O(\theta^2)$, with w a nonzero vector orthogonal to v and θ small. Since $v * v = 16v$, we obtain

$$\begin{aligned} v' * v' &= 16v + 2\theta v * w + O(\theta^2), \\ 16v' &= 16v + 16\theta w + O(\theta^2). \end{aligned}$$

Since $|v * w| < 4|w|$ by Lemma 2.4, these two equations prohibit $v' * v' = 16v'$ for sufficiently small θ . \square

Recall that x_{-1} is the (unique) central involution in G_{x0} .

Definition 2.8. A 2B *involution* of the Monster is an element conjugate in \mathbb{M} to x_{-1} .

From the construction, the trace of a 2B involution on \mathcal{B} is 276; by Lemma 2.4, the trace of a 2A involution on \mathcal{B} is 4372. Thus, 2A and 2B involutions are not conjugate in \mathbb{M} . We will see later in Theorem 5.8 that every involution of the Monster is either a 2A or a 2B involution.

Theorem 2.9 (see [Con85], § 13). *Let x_{-1} be the central involution in $G_{x0} \cong 2_+^{1+24}.\text{Co}_1$. The centralizer of x_{-1} in $\text{Aut}(\mathcal{B})$ and hence in \mathbb{M} is G_{x0} .* \square

For computing the order of \mathbb{M} we use two specific 2A involutions $\beta^+ = x_{ij}$ with $i = 2, j = 3$, and $\beta^- = \beta^+ \cdot x_{-1}$. We have $\beta^+, \beta^- \in Q_{x0}$. We abbreviate λ_{β^+} to λ_β . Then $\lambda_{\beta^-} = \lambda_{\beta^+} = \lambda_\beta \in \Lambda/2\Lambda$. We define the axes v^+, v^- introduced in Section 1 by $v^+ = \text{ax}(\beta^+)$, $v^- = \text{ax}(\beta^-)$. Then the group $\mathbb{M}_{v^+} \cap \mathbb{M}_{v^-}$ fixing both axes, v^+ and v^- , also fixes the 2B involution x_{-1} . Hence $\mathbb{M}_{v^+} \cap \mathbb{M}_{v^-}$ is isomorphic to the subgroup of G_{x0} of structure $2^{1+23}.\text{Co}_2$ fixing β^+ . The mmgroup package provides support for computing with axes v^+, v^- , since they are used for shortening a word of generators of \mathbb{M} .

2.2 The Monster and the Moonshine Module

In this section, we revisit the construction of the Monster from the more advanced perspective of vertex operator algebras. This allows us to provide more conceptual proofs of the results from the last section and sometimes to obtain stronger results. We assume here that the reader is familiar with vertex operator algebras and the construction of the Moonshine module.

The Monster representation. The Moonshine module V^\natural is a vertex operator algebra of central charge 24 having as conformal character $\chi_{V^\natural} = q^{-1} \sum_{n=0}^{\infty} \dim V_n^\natural q^n$ the elliptic modular function $j - 744 = q^{-1} + 196884q + 21493760q^2 + \dots$. It was constructed in [FLM88] (see also [Bor86]) as a \mathbf{Z}_2 -orbifold of the lattice vertex operator algebra V_Λ associated to the Leech lattice Λ . The algebra induced on the degree-two part V_2^\natural can be identified with the Griess algebra \mathcal{B} (see [FLM88], Prop. 10.3.6).

The -1 automorphism of Λ has an up-to-conjugation unique lift x_{-1} (cf. [DGH98]) to V_Λ whose \mathbf{Z}_2 -orbifold $V_\Lambda^+ \oplus V_\Lambda^{T,+}$ is the Moonshine module. It follows from the construction that the group $G_{x0} \cong 2_+^{1+24}.\text{Co}_1$ acts by automorphisms on V^\natural such that the subspaces V_Λ^+ and $V_\Lambda^{T,+}$ are the $+1$ and -1 eigenspaces of the action of the central element x_{-1} of G_{x0} .

The Leech lattice Λ can be constructed from the Golay code, which allows one to construct the additional triality automorphism τ of V^\natural . If $G_{24} \subset \mathbb{F}^{24}$ is the Golay code, then the index 2 sublattice Λ_0 of Λ consists of the vectors $\frac{1}{\sqrt{2}}v \in \mathbb{R}^{24}$ such that v has integer coordinates and the sum of the 24 coordinates of v is even. The fixed-point vertex operator algebra $V_\Lambda^{++} := V_{\Lambda_0}^+ \subset V_\Lambda^+ \subset V^\natural$ has 16 irreducible modules, and the associated modular tensor category $\mathcal{T}(V_\Lambda^{++})$ is isomorphic to the modular tensor category associated to the direct sum $H \oplus H$ of two hyperbolic planes [AD04, ADL05].

For the automorphism group of V_Λ^{++} we have the short exact sequence

$$1 \longrightarrow \text{Aut}(V_\Lambda^{++})_0 \longrightarrow \text{Aut}(V_\Lambda^{++}) \longrightarrow \overline{\text{Aut}}(V_\Lambda^{++}) \longrightarrow 1,$$

where $\overline{\text{Aut}}(V_\Lambda^{++}) \subset O(H \oplus H)$ is the induced permutation group permuting the irreducible modules of V_Λ^{++} . The 16 elements of $H \oplus H$ form three orbits under the orthogonal group $O(H \oplus H)$ of order 96: two orbits of isotropic vectors of size 1 and 9, and one orbit of size 6. The 16 modules of V_Λ^{++} have 4 different conformal characters: the orbit of size 9 splits into two orbits of size 3 and 6 under $\overline{\text{Aut}}(V_\Lambda^{++})$. More precisely, $\overline{\text{Aut}}(V_\Lambda^{++})$ is a dihedral group of order 12, and $\text{Aut}(V_\Lambda^{++})_0 \cong 2^{22} \cdot (2^{11} : M_{24})$; cf. [Shi04].

There are three orbits of 2-dimensional isotropic subspaces A in $H \oplus H$ under $\overline{\text{Aut}}(V_\Lambda^{++})$: Extending V_Λ^{++} by the simple currents in A results in one of the three self-dual vertex operator algebras $V_{N(A_1^{24})}$ (the lattice vertex operator algebra associated to the Niemeier lattice with root system A_1^{24}), V_Λ , or V^\natural . The setwise stabilizer of A in $\overline{\text{Aut}}(V_\Lambda^{++})$ for the case V^\natural is an S_3 . It can be shown that $\text{Aut}(V^\natural)$ has a subgroup $N_0 \cong 2^2 \cdot 2^{11+22} \cdot (M_{24} \times S_3)$, where the 2^2 is the dual group \hat{A} of A and the S_3 is the induced action on A ; cf. [FLM88].

One checks that the definitions of G_{x0} and N_0 on V^\natural agree with the definitions in Section 2.1 when restricted to the Griess algebra $\mathcal{B} = V_2^\natural$. Let $\mathbb{M}' = \langle G_{x0}, N_0 \rangle \subseteq \text{Aut}(V^\natural)$. It was shown in [FLM88] that $\mathbb{M}' = \mathbb{M}$. The result also follows from the more general Theorem 2.16 proven below. This allows us to define the Monster \mathbb{M} also as the group of automorphisms of V^\natural generated by G_{x0} and N_0 .

Involutions and Ising vectors. We study involutions in \mathbb{M} and $\text{Aut}(V^\natural)$ from the viewpoint of vertex operator algebras. Recall that to an automorphism of order n of a self-dual vertex operator algebra one can assign its *type* $h \pmod{n}$, where $h|n$, cf. [EMS20].

Lemma 2.10. *Let t be an involution in $\text{Aut}(V^\natural)$ of type 0. Then the vector-valued character $\text{Ch}_{(V^\natural)^t}$ of the fixed-point vertex operator algebra $(V^\natural)^t$ is given either by*

$$\text{Ch}_{(V^\natural)^t} = \begin{pmatrix} q^{-1} + 100628q + O(q^2) \\ 96256q + O(q^2) \\ 96256q + O(q^2) \\ q^{-1/2} + 4372q^{1/2} + O(q^{3/2}) \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} q^{-1} + 98580q + O(q^2) \\ 24 + 98304q + O(q^2) \\ 98304q + O(q^2) \\ 4096q^{1/2} + O(q^{3/2}) \end{pmatrix}.$$

Proof: The general formula for the vector-valued character of the fixed-point vertex operator algebra V^t of a type 0 involution on a self-dual vertex operator algebra V of central charge $c = 24$ is given in [HM23], Section 3.5. Since $V_1^\natural = (V_1^\natural)^t = 0$, it follows that the three parameters are $a = 24$, $b = 24 - \dim(\widetilde{V}^\natural_1)$ (where \widetilde{V}^\natural is the orbifold vertex operator algebra of V^\natural with respect to t), and $\ell = b/24$. Also, ℓ is the dimension of a vector space, i.e., has to be a non-negative integer. Hence, the only two possibilities are $b = 24$ or $b = 0$, and the result follows. \square

Definition 2.11. An involution t of $\text{Aut}(V^\natural)$ of type 0 is called a *2A-like involution* respectively a *2B-like involution* if the vector-valued character of $(V^\natural)^t$ is the first respectively the second of the two characters given in Lemma 2.10.

We see from Lemma 2.10 that the trace of a 2A like involution on the Griess algebra \mathcal{B} is 4372 and that the trace of a 2B like involution is 276. We will see in the last section

that all involutions t in $\text{Aut}(V^\natural)$ are of type 0. For the 2A and 2B involutions of the Monster, this can be checked explicitly using a decomposition of V^\natural with respect to a Virasoro frame.

Definition 2.12. An *Ising vector* of a vertex operator algebra V is a vector $x \in V_2$ which generates a simple Virasoro vertex operator subalgebra of central charge $c = 1/2$.

A vector $x \in V_2$ generates a Virasoro vertex subalgebra if

$$x_1x = 2 \cdot x, \quad x_2x = 0, \quad \text{and} \quad x_3x = \frac{c}{2} \cdot \mathbf{1}.$$

The third equation is equivalent to $\langle x, x \rangle = \frac{c}{2}$, where $\langle \cdot, \cdot \rangle$ is the natural invariant bilinear form on V . In the case of the Moonshine module V^\natural , one has $x_2x \in V_1^\natural = 0$ so that the second equation is automatically satisfied. Also, because V^\natural has a positive definite invariant bilinear form, the Virasoro vertex operator subalgebra is automatically simple, i.e., isomorphic to the minimal model $L(1/2, 0)$. Thus a vector x in \mathcal{B} is an Ising vector if $x * x = 2x$ and $\langle x, x \rangle = \frac{1}{4}$.

Theorem 2.13. *There exists a natural bijection between 2A like involutions in $\text{Aut}(V^\natural)$ and Ising vectors in V^\natural .*

Proof: This is a special case of the correspondence between involutions of type 0 in the automorphism group of self-dual vertex operator algebras of central charge $8d$ and self-dual vertex operator superalgebras of charge less than or equal to $8d$ as established in [HM23].

In the case of a 2A like involution t in $\text{Aut}(V^\natural)$, the vertex operator superalgebra extension V of the fixed-point subalgebra $(V^\natural)^t$ has as character the sum of the first and last component of the vector-valued modular function:

$$\chi_V = q^{-1} + q^{-1/2} + 4372q^{1/2} + 100628q + O(q^{3/2}).$$

In particular, one has $\ell = \dim V_{1/2} = 1$. It follows that the vertex operator subalgebra $\langle V_{1/2} \rangle$ of V is isomorphic to the “single Fermion” $L(1/2, 0) \oplus L(1/2, 1/2)$, and thus one canonically has the vertex operator subalgebra $L(1/2, 0) \subset (V^\natural)^t \subset V^\natural$. The Virasoro element of $L(1/2, 0)$ is the associated Ising vector x in V^\natural .

Conversely, given an Ising vector x in V^\natural , it generates a subalgebra $L(1/2, 0) \subset V^\natural$. One has a natural decomposition (cf. [Höh95])

$$V^\natural = VB_{(0)}^\natural \otimes L(1/2, 0) \oplus VB_{(1)}^\natural \otimes L(1/2, 1/2) \oplus VB_{(2)}^\natural \otimes L(1/2, 1/16).$$

Then t is defined as the involution acting by $+1$ on the first two terms of this sum and by -1 on the third. From the fusion rules of $L(1/2, 0)$, it follows that t is an automorphism of V^\natural called the Miamoto involution associated to x , and one sees that t is of type 0. From the known characters of the $L(1/2, h)$ for $h = 0, 1/2$, and $1/16$ and the character of $VB^\natural = VB_{(0)}^\natural \oplus VB_{(1)}^\natural$ as an extremal self-dual vertex operator superalgebra of central charge $c = 23\frac{1}{2}$, one sees that t has to be 2A like.

One also checks that the provided maps between 2A like involutions and Ising vectors are inverse to each other. \square

The VOA $L(1/2, 0)$ has three isomorphism classes of irreducible modules: $L(1/2, 0)$, $L(1/2, 1/2)$, and $L(1/2, 1/16)$, of conformal weight 0, $1/2$, and $1/16$, respectively. It follows that the endomorphism $x_1 = \text{ad } x$ of V_2 has eigenvalues 0, $1/2$, $1/16$, and 2.

The connection to 2A and 2B involutions in the Monster as defined in the previous subsection is explained by the following two results.

Lemma 2.14. *Let t be a 2A involution of the Monster. Then t is a 2A like involution of $\text{Aut}(V^\natural)$, and the axis associated to t is, up to a scaling factor, an Ising vector of V^\natural .*

Proof: An axis v in \mathcal{B} was normalized by $v * v = 16v$ and $(v, v) = 8$. Thus $x = v/8$ satisfies $x * x = 2x$ and $(x, x) = 1/8$. The scalar product (\cdot, \cdot) on \mathcal{B} is normalized such that for the identity element $1_{\mathcal{B}}$ one has $(1_{\mathcal{B}}, 1_{\mathcal{B}}) = 3/2$, i.e., $(\omega, \omega) = 6$ for the Virasoro element $\omega = 2 \cdot 1_{\mathcal{B}}$ of V^\natural , whereas $\langle \omega, \omega \rangle = 12$. Hence $\langle x, x \rangle = 1/4$ and x is an Ising vector.

By Lemma 2.4, the involution associated to v negates the eigenspace of $\text{ad } v$ for the eigenvalue $1/2$. Thus $\text{ad } x$ negates the eigenspace for the eigenvalue $1/16$ in agreement with the definition for the associated 2A like involution given in the proof of Theorem 2.13. \square

We will see in the last section that every 2A like involution of $\text{Aut}(V)$ is actually a 2A involution of the Monster, or, equivalently, that every Ising vector in V^\natural is, up to scaling, an axis in \mathcal{B} .

Theorem 2.15. *Let t be a 2B like involution of $\text{Aut}(V^\natural)$. Then t is conjugated in $\text{Aut}(V^\natural)$ to a 2B involution of the Monster, and the centralizer of t in $\text{Aut}(V^\natural)$ is conjugated to G_{x0} .*

Proof: The fixed-point vertex operator algebra $(V^\natural)^t$ of an involution of type 0 has as its modular tensor category the tensor category associated to a hyperbolic plane as the quadratic space. This allows one to construct the orbifold vertex operator algebra \widetilde{V}^\natural by extending $(V^\natural)^t$ with the $(V^\natural)^t$ module of conformal weight 0 (mod 1) not contained in V^\natural . From Lemma 2.10, it follows that \widetilde{V}^\natural has the character $q^{-1} + 24 + 196884q + O(q^2)$. It is well known that the Leech lattice vertex operator algebra V_Λ is, up to isomorphism, the unique self-dual vertex operator algebra V of central charge $c = 24$ with $\dim V_1 = 24$. Since a lift of the -1 involution on Λ to V_Λ is, up to conjugacy, the unique involution of V_Λ having V^\natural as its orbifold (cf. [HM23], Table 9, entry #968), one has $\widetilde{V}^\natural \cong V_\Lambda$ and hence $(V^\natural)^t \cong V_\Lambda^+$. It follows that t is conjugated to z in $\text{Aut}(V^\natural)$.

Using [Shi04], we have that the fixed-point vertex operator algebra V_Λ^+ has the automorphism group $2^{24}.\text{Co}_1 \cong G_{x0}/\langle z \rangle$. Since the centralizer of z in $\text{Aut}(V^\natural)$ has to respect the decomposition of V^\natural into the z eigenspaces V_Λ^+ and $V_\Lambda^{T,+}$, it follows from Schur's Lemma that the centralizer of z is contained in $\mathbb{C}^*.2^{24}.\text{Co}_1$. Using the fusion rules for V_Λ^+ , it follows that the centralizer is equal to $G_{x0} \cong 2_+^{1+24}.\text{Co}_1$. \square

We note that Theorem 2.15 provides a vertex operator algebra proof of Lemma 2.9.

2.3 Identification of $\text{Aut}(\mathcal{B})$ and $\text{Aut}(V^\natural)$

We will show in Section 5 that the Monster is the full automorphism group of the Moonshine module and the Griess algebra. For this, we will need the following general result.

Theorem 2.16. *The map $\rho : \text{Aut}(V^\natural) \longrightarrow \text{Aut}(\mathcal{B})$, which restricts a vertex operator algebra automorphism of V^\natural to an algebra automorphism of its degree-two part $V_2^\natural = \mathcal{B}$, is an isomorphism.*

Here, an automorphism of \mathcal{B} is understood to also respect the invariant bilinear form on \mathcal{B} .

For the proof, one could try to proceed as in [FLM88] and relate the algebra structure on \mathcal{B} (together with the invariant bilinear form) and the vertex operator algebra structure on V^\natural by utilizing the *affine Griess algebra* $\hat{\mathcal{B}}$. Instead, we make use of the axes in \mathcal{B} . A system of 48 pairwise-orthogonal axes was first found in [MN93]. This motivated the notion of a *Virasoro frame* of a vertex operator algebra in [DGH98].

A Virasoro frame of a vertex operator algebra W of central charge $c = n/2$ is a set $\{\omega_1, \dots, \omega_n\} \subset W_2$ of mutually orthogonal Ising vectors with $\omega_1 + \dots + \omega_n = \omega$, the Virasoro element of W . Such a Virasoro frame generates a vertex operator subalgebra $T_n \cong L(1/2, 0)^{\otimes n}$ inside a sufficiently regular W , where $L(1/2, 0)$ is the $c = 1/2$ Virasoro minimal model vertex operator algebra. It was shown in [DGH98] that such a subalgebra T_n in the vertex operator algebra W defines two linear binary codes \mathcal{C} and \mathcal{D} of length n which are orthogonal to each other.

Proof of injectivity of ρ : A Virasoro frame $\{\omega_1, \dots, \omega_{48}\} \subset V^\natural$ was found in [DGH98] such that \mathcal{C} is the lexicographic code of length 48 and minimal weight 4. The dimension of \mathcal{C} is 41 and the code $\mathcal{D} = \mathcal{C}^\perp$ has dimension 7 and minimal weight 16. Furthermore, \mathcal{C} is generated by its weight 4 codewords.

Let ψ be an automorphism of V^\natural in the kernel of ρ . Since ψ fixes \mathcal{B} , it fixes the Virasoro frame and hence the vertex operator algebra T_{48} it generates.

The simple vertex operator subalgebra $M_{\mathcal{C}} \cong \bigoplus_{c \in \mathcal{C}} M(c)$ of V^\natural is a simple current extension of T_{48} by the simple currents $M(c)$, $c \in \mathcal{C}$, and the fusion rules among the $M(c)$ are those for the group \mathcal{C} . A codeword c of weight 4 in \mathcal{C} corresponds to a T_{48} -module $M(c)$ with a lowest-weight vector u in $V_2^\natural = \mathcal{B}$. Thus ψ fixes such u and the T_{48} -module $M(c)$. Since \mathcal{C} is generated by its weight 4 codewords, ψ acts trivially on all of $M_{\mathcal{C}}$.

Similarly, $\bigoplus_{I \in \mathcal{D}} M^I \cong V^\natural$ is a simple current extension. The M^I are irreducible $M_{\mathcal{C}}$ -modules, and the fusion rules among the M^I , $I \in \mathcal{D}$, are those for the group \mathcal{D} . Furthermore, \mathcal{D} is generated by codewords $I \in \mathcal{D}$ with the property that the $M_{\mathcal{C}}$ -module M^I contains a lowest-weight vector u in V_2^\natural , cf. [DGL07]. This implies that ψ acts trivially on those M^I and thus on all of V^\natural . \square

For the proof of the surjectivity of ρ , we use the following result from [DGL07], which was also proven with the help of the above Virasoro frame.

Theorem 2.17 ([DGL07], Thm. 1). *Let V be a C_2 -cofinite self-dual extremal vertex operator algebra of central charge 24 such that the degree-two part V_2 with the induced algebra structure is isomorphic to the Griess algebra \mathcal{B} . Then V is isomorphic to V^\natural .*

An analysis of the proof shows that the following more precise result can be deduced:

Proposition 2.18. *Let V be a C_2 -cofinite self-dual extremal vertex operator algebra of central charge 24. Let $\varphi : \mathcal{B} \longrightarrow V_2$ be an algebra isomorphism. Then φ can be extended to a vertex operator algebra isomorphism $\hat{\varphi} : V^\natural \longrightarrow V$.*

Proof: Let $\{\varphi(\omega_1), \dots, \varphi(\omega_{48})\}$ be the image of the Virasoro frame $\{\omega_1, \dots, \omega_{48}\}$ of \mathcal{B} under φ . This is a Virasoro frame in V_2 because φ is an algebra isomorphism, and thus preserves the product relations defining a frame. It generates a vertex operator subalgebra $T'_{48} \cong L(1/2, 0)^{\otimes 48} \subset V$, see [DGL07]. This allows us to extend φ from $\{\omega_1, \dots, \omega_{48}\} \subset V_2^\natural$ to a vertex operator algebra isomorphism $\hat{\varphi} : T_{48} \longrightarrow T'_{48}$.

The vertex operator subalgebra T'_{48} of V defines the two associated binary codes \mathcal{C}' and \mathcal{D}' . The codewords c of weight 4 in \mathcal{C} correspond to T_{48} -modules $M(c)$ with a lowest-weight vector u in $V_2^\natural = \mathcal{B}$. Since φ is an algebra isomorphism, it preserves the correspondence between weight 4 codewords and their associated lowest-weight vectors in the degree-two space. This establishes a canonical identification between the weight 4 codewords of \mathcal{C} and \mathcal{C}' . As both codes are generated by their weight 4 codewords, φ induces a canonical identification between \mathcal{C} and \mathcal{C}' . The two vertex operator subalgebras

$$M_{\mathcal{C}} \cong \bigoplus_{c \in \mathcal{C}} M(c) \quad \text{and} \quad M_{\mathcal{C}'} \cong \bigoplus_{c \in \mathcal{C}'} M(c)$$

of V^\natural and V , respectively, are therefore isomorphic since they are both simple current extensions of $L(1/2, 0)^{\otimes 48}$ by corresponding simple currents. This allows us to extend the given algebra isomorphism $\varphi : \bigoplus_{c \in \mathcal{C}} M(c) \cap \mathcal{B} \longrightarrow \bigoplus_{c \in \mathcal{C}'} M(c) \cap V_2$ to a vertex operator algebra isomorphism $\hat{\varphi} : M_{\mathcal{C}} \longrightarrow M_{\mathcal{C}'}$.

It is shown in [DGL07], Thm. 6.10, that all irreducible $M_{\mathcal{C}}$ -modules are simple currents. It follows that one has simple current extensions

$$V^\natural \cong \bigoplus_{I \in \mathcal{D}} M^I \quad \text{and} \quad V \cong \bigoplus_{I \in \mathcal{D}'} M^I,$$

where M^I is an irreducible $M_{\mathcal{C}}$ -module corresponding to a codeword $I \in \mathcal{D}$ and the fusion rules among the M^I are the ones for the group \mathcal{D} . Analogous properties hold for the $M_{\mathcal{C}'}$ -modules. Furthermore, \mathcal{D} is generated by codewords $I \in \mathcal{D}$ with the property that M^I contains an $M_{\mathcal{C}}$ -lowest-weight vector u in V_2^\natural . Since φ is an algebra isomorphism, these vectors u are mapped to $M_{\mathcal{C}'}$ -lowest-weight vectors $\varphi(u)$ in V_2 . The code $\mathcal{D}' = \mathcal{C}'^\perp$ is, like \mathcal{D} , generated by codewords I' for which the corresponding $M_{\mathcal{C}'}$ -modules $M^{I'}$ contain a lowest-weight vector in V_2 . The isomorphism φ ensures that the set of such generating modules for V^\natural corresponds exactly to that for V . This allows us to extend the vertex operator algebra isomorphism $\hat{\varphi} : M_{\mathcal{C}} \longrightarrow M_{\mathcal{C}'}$ to a vertex operator algebra isomorphism $\hat{\varphi} : V^\natural \longrightarrow V$. \square

Taking $V = V^\natural$ in Proposition 2.18 shows that any automorphism of \mathcal{B} can be extended to an automorphism of V^\natural . Therefore, the map ρ is surjective. Together with the already proven injectivity, this completes the proof of Theorem 2.16.

3 Counting the axes in the Griess algebra

In this section, we compute the number of axes in the Griess algebra \mathcal{B} by decomposing them into twelve orbits under the group G_{x0} . The result is shown in Table 1. In particular, as the number of all axes in \mathcal{B} is the sum of the sizes of all orbits, we will obtain:

Proposition 3.1. *There are 97 239 461 142 009 186 000 axes in the Griess algebra \mathcal{B} .*

The number of axes in each orbit was first determined by Norton, cf. [Nor98], Table 2, where the relevant information is given without proof. The main objective of this section is to recompute the information in that table using the mmgroup package [Sey20b] without assuming any further properties of the Monster or its character table.

G_{x0} -orbit	No. suborbits		G_{x0} -orbit size	Stabilizer C of an axis in the orbit	
	N_{x0}	N_{xyz}		$C \cap Q_{x0}$	$C/(C \cap Q_{x0})$
2A	3	3	196560	2^{1+23}	Co_2
2B	5	6	11935123200	2^{1+16}	$2^{1+8} \cdot O_8^+(2)$
4A	9	11	1630347264000	2^{12}	$2^{11} \cdot M_{23}$
4B	16	21	1466587938816000	2^7	$2^{1+8} \cdot S_6(2)$
4C	14	17	6599645724672000	2^5	$2^{1+8+6} \cdot A_8$
6A	10	14	1896194506752000	2^2	$U_6(2).2$
6C	23	35	438020931059712000	2^2	$2^{1+8} \cdot (3 \times U_4(2)).2$
8B	37	64	8601138282627072000	1	$2^{1+10} \cdot M_{11}$
6F	8	12	1501786049347584000	1	$2^{1+8} \cdot A_9$
10A	23	36	786389785840189440	2	$\text{HS}.2$
10B	38	68	37845008443559116800	1	$2^{1+8} \cdot (A_5 \times A_5).2$
12C	65	118	48057153579122688000	1	$2 \cdot S_6(2)$
Total	251	405	97239461142009186000		

Table 1: Sizes of G_{x0} -orbits on axes and stabilizers in G_{x0} of an axis in the orbit.

We also use the MAGMA algebra system [BCP97] for obtaining the structure of certain groups.

3.1 The strategy for counting the axes

Identifying the G_{x0} -orbits. We can find at least twelve orbits.

Lemma 3.2. *There exist at least twelve orbits on the axes under G_{x0} , distinguished by the conjugacy class of tx_{-1} in \mathbb{M} where t is the 2A involution associated to an axis.*

Proof: Starting with the axis v^+ , we compute samples of axes by repeatedly transforming an axis with a random element of G_{x0} and with a power of the triality element τ . The first transformation does not change the G_{x0} -orbit of the axis, but the second transformation may do so. In principle, we could compute traces of powers of tx_{-1} in \mathcal{B} with the mmgroup package for distinguishing between conjugacy classes in \mathbb{M} . But for reasons of speed, we use a watermarking technique explained below for distinguishing between orbits of axes. This way we obtain representatives of twelve different orbits of axes. The Python script `orbit_classes.py` computes orders and traces in \mathcal{B} of the elements tx_{-1} (and also of some powers of tx_{-1}), where t runs through the involutions corresponding to the axes found. That way, twelve different conjugacy classes of elements tx_{-1} have been found. \square

Remark: In [Nor98] and [Sey24], the G_{x0} -orbit of a 2A involution t is labeled by the conjugacy class of tx_{-1} in the Monster. The character information computed by the script `orbit_classes.py` in the accompanying code is sufficient to match our representatives of the orbits on the axes with the orbits described in [Nor98]. Here the character table

of the Monster in the ATLAS [CCN⁺85] is only used for adjusting our notation for the orbits to the notation used in [Nor98].

We choose representatives for the axes for each of the twelve cases as in Lemma 3.2. To confirm that a given axis belongs to one of the corresponding twelve G_{x0} -orbits, we proceed as follows using a watermarking technique to identify the likely orbit.

The subspace 300_x of \mathcal{B} can be identified with the symmetric 24×24 matrices. An element of G_{x0} acts as a rational orthogonal transformation on the symmetric 24×24 matrices. Thus the eigenvalues and dimensions of the eigenspaces of such a matrix depend therefore only on the G_{x0} -orbit. We project the given axis to 300_x , obtaining a symmetric 24×24 matrix. Table 1 in [Sey24] shows that the algebraic information obtained in that way is sufficient to distinguish between the putative twelve G_{x0} -orbits. A slightly more sophisticated disambiguation of the G_{x0} -orbits of the axes based on their entries in \mathcal{B} (modulo 15) is given in [Sey24], Section 8.4.

Having identified the likely orbit of an axis, we want to show that the axis is actually in that orbit. Therefore, we compute an element of G_{x0} that maps the axis to the corresponding representative. For the details of this computation, we refer to Appendix A.1.

The triality transition matrix. Our objective is to compute the transition matrix M for the operation of the triality element τ on the G_{x0} -orbits, as shown in Table 2. The rows and columns of M are labeled by the names of the G_{x0} -orbits on the axes. An entry in row i , column j indicates the number of axes in orbit j that are mapped to orbit i by the triality element τ , up to a factor depending on the column j only and chosen such that the total of each column is 16584750. Thus the matrix $M/16584750$ is column-stochastic, and one checks that it is regular.

From the Perron–Frobenius theorem, we conclude that the column vector containing the sizes of the G_{x0} -orbits is the unique eigenvector of M for the eigenvalue 16584750. For computing the sizes of the G_{x0} -orbits on the axes from the matrix M , it, therefore, suffices to know the size of one of these orbits.

Lemma 3.3. *The orbit labeled '2A' and containing the axis v^+ has size 196560.*

Proof: The 2A involution β^+ corresponding to the axis v^+ in the orbit labeled '2A' is contained in Q_{x0} . The element λ_β of $\Lambda/2\Lambda$ is short and has precisely the two preimages β^+ and β^- in Q_{x0} . Since there are 98280 short vectors in $\Lambda/2\Lambda$, the size of the G_{x0} -orbit on the axes labeled '2A' is $2 \cdot 98280$. \square

So given M , we may compute the sizes of all G_{x0} -orbits on the axes, as shown in Table 1.

To compute the transition matrix M , we utilize that the triality element τ normalizes a large subgroup of G_{x0} . The group $N_{x0} = G_{x0} \cap N_0$ has a subgroup N_{xyz} of index 2 with structure $2^{2+11+22}.M_{24}$. The triality element τ normalizes N_{xyz} . Thus, for any $g \in G_{x0}$ and axis v , the G_{x0} -orbit of $vg\tau$ depends on the left coset gN_{xyz} only. The index of N_{xyz} in G_{x0} is 16584750. Thus a left transversal \mathcal{T} of N_{xyz} in G_{x0} can be effectively computed. For computing the transition matrix, it suffices to transform a representative of each G_{x0} -orbit with all elements $\{g \cdot \tau \mid g \in \mathcal{T}\}$, and to determine the G_{x0} -orbit of the transformed axes.

	2A	2B	4A	4B	4C	6A
2A	93150	135	1	.	.	.
2B	8197200	64935	3542	63	15	.
4A	8294400	483840	35927	2232	240	891
4B	.	7741440	2007808	137367	33600	74844
4C	.	8294400	971520	151200	54255	.
6A	.	.	1036288	96768	.	133731
6C	.	.	7254016	2225664	860160	2020788
8B	.	.	5275648	3870720	430080	8382528
6F	522240	.
10A	.	.	.	2064384	491520	953856
10B	.	.	.	1548288	7311360	.
12C	.	.	.	6488064	6881280	5018112

	6C	8B	6F	10A	10B	12C
2A
2B
4A	27	1
4B	7452	660	.	3850	60	198
4C	12960	330	2295	4125	1275	945
6A	8748	1848	.	2300	.	198
6C	321003	134024	.	284900	59520	72450
8B	2631744	2217999	483840	3010000	1375680	1399104
6F	.	84480	486135	.	271200	274320
10A	511488	275200	.	411775	131520	106992
10B	5142528	6052992	6834240	6329400	6435735	6543936
12C	7948800	7817216	8778240	6538400	8309760	8186607

Table 2: Action of the triality element τ on the G_{x0} -orbits in the axes. The entry in row i , column j is the number of N_{xyz} -orbits in the G_{x0} -orbit j that are mapped to G_{x0} -orbit i . The total of each column is $|G_{x0}/N_{xyz}| = 16584750$.

Such a computation is lengthy, but doable with a modern PC, and has been done in an early stage of the mmgroup project using the identification of an orbit via watermarking. We have $\mathbb{M} = \langle G_{x0}, \tau \rangle$. Therefore, if every orbit obtained by watermarking in this way is one of the twelve G_{x0} -orbits given by Lemma 3.2, then this calculation also shows that we have found all G_{x0} -orbits.

It thus remains to verify that the orbit of an axis identified by watermarking is indeed in that G_{x0} -orbit. Here, in principle, the method discussed in Appendix A.1 can be used. However, we have to transform almost 200 million axes to the representative of their G_{x0} -orbit. Finding a suitable transformation takes much longer than identifying an orbit via watermarking, so this approach is presently not feasible. In the next section, we will discuss how to reduce the required amount of computation significantly.

Once the data for matrix M have been computed, their correctness can be verified by a much simpler computation. For details, we refer to Appendix D.

3.2 Speeding up the counting of the axes

In this subsection, we explain how to speed up the counting of the axes so that this can be done in practice. Our primary objective is to compute Table 2. Let v_i be the chosen representative of the G_{x0} -orbit i on the axes, and let C_i be the stabilizer of v_i in G_{x0} . As discussed in the previous subsection, we want to compute the axes $v_i g \tau$, where g runs through a left transversal \mathcal{T} of N_{xyz} in G_{x0} .

Since C_i centralizes v_i , it suffices to consider a transversal of the double coset space $C_i \backslash G_{x0} / N_{xyz}$, provided that we know the number of right cosets of C_i in G_{x0} in each double coset in $C_i \backslash G_{x0} / N_{xyz}$. So we need a fast method to find the transversal of the double coset space $C_i \backslash G_{x0} / N_{xyz}$ and to count the right cosets of C_i in each of these double cosets. Therefore, it would be helpful to find a permutation representation of G_{x0} acting on the cosets in G_{x0} / N_{xyz} . The group G_{x0} acts on $\Lambda / 2\Lambda$ via the natural action of its factor group Co_1 . The centralizer of λ_Ω (with λ_Ω as in Section 2.1) in G_{x0} is N_{x0} . Since λ_Ω is a type 4 vector, and Co_1 is transitive on the type 4 vectors, there is a one-to-one correspondence between the left cosets G_{x0} / N_{x0} and the type 4 vectors in $\Lambda / 2\Lambda$. Since N_{xyz} has index 2 in N_{x0} , this is almost what we need.

There is an $a \in N_{x0} \setminus N_{xyz}$ with $a^{-1} \tau a = \tau^{-1}$; we may take, e.g., $a = x_\delta$ with $\delta = \{0\} \in \mathcal{C}^*$ in the notation of [Sey20a]. So instead of inspecting the representatives $v_i g \tau$ and $v_i g a \tau$ of two different cosets in G_{x0} / N_{xyz} , we may inspect $v_i g \tau$ and $v_i g \tau^{-1}$ instead, where g runs through a transversal of $C_i \backslash G_{x0} / N_{x0}$.

We first model the stabilizer C_i in G_{x0} of an axis v_i , or at least a large subgroup of C_i . For this, we create a set of generators of C_i as elements of the group G_{x0} . The easiest way to create a generator of C_i is to multiply v_i with a random element g_1 of G_{x0} , and to find an element $g_2 \in G_{x0}$ that reduces the axis $v_i g_1$ to v_i , i.e., $(v_i g_1) g_2 = v_i$. Then $g_1 g_2$ centralizes v_i . We may obtain a suitable element g_2 by the method discussed in Appendix A.1. That way, we have computed 10 random generators of the stabilizer C_i . There is a very small probability that these generators generate a proper subgroup of C_i . For computing Table 2, this may cause some more overhead, but not any error. For simplicity, we also write C_i for the group generated by these generators.

We model the action of the subgroup C_i of G_{x0} on $\Lambda / 2\Lambda$ by using the class `Orbit_Lin2` in the `mmgroup` package. This class implements the action of a general group C_i (given by generators) on the vector space \mathbb{F}_2^n , $n \leq 24$, or, more specifically, on $\Lambda / 2\Lambda$. The key ingredient of the class `Orbit_Lin2` is a fast algorithm for finding orbits on $\Lambda / 2\Lambda$ under the group C_i . That class contains a member function for computing a list of representatives of the orbits under C_i on $\Lambda / 2\Lambda$ and the sizes of these orbits. Since $C_i \subset G_{x0}$, all elements of such an orbit have the same type in $\Lambda / 2\Lambda$, and we are only interested in orbits on vectors of type 4.

For any $\lambda \in \Lambda / 2\Lambda$ of type 4, we may compute a $g_\lambda \in G_{x0}$ that maps λ to λ_Ω with `mmgroup`. Let L_i be a set of representatives of all orbits of type 4 vectors under C_i on $\Lambda / 2\Lambda$. Then the set $\{g_\lambda \mid \lambda \in L_i\}$ is a transversal of the double coset space $C_i \backslash G_{x0} / N_{x0}$. We compute the G_{x0} -orbits on the axes $v_i g_\lambda \tau^{\pm 1}$, where λ runs through L_i , as discussed in Section 3.1. In the course of this computation, we also verify that all these axes are in one of the twelve orbits given by Lemma 3.2. This proves:

Lemma 3.4. *There are precisely twelve orbits on the axes under G_{x0} .*

We compute the column of Table 2 corresponding to the orbit $v_i G_{x0}$ as follows. For

each $\lambda \in L_i$ and $\varepsilon = \pm 1$, we add the size of the orbit of λ under C_i on $\Lambda/2\Lambda$ to the row in the table corresponding to the orbit of the axis $v_i g_\lambda \tau^\varepsilon$.

Having computed Table 2, we may compute column 4 of Table 1, as discussed in Section 3.1; in particular, Proposition 3.1 is proven.

3.3 Decomposition of the G_{x0} orbits into N_{xyz} orbits

Let the axis v_i be a representative of the orbit $v_i G_{x0}$ as above. Once the size of that orbit is known (as shown in column 4 of Table 1), we may compute the decomposition of the orbit $v_i G_{x0}$ into N_{x0} -orbits and also the structures of the stabilizers in N_{x0} of representatives of these orbits.

In the previous subsection, we have computed a set of random elements of the stabilizer C_i of v_i in G_{x0} . There is a very small probability that this set generates a proper subgroup of C_i . For computing the N_{x0} -orbits on the axes in the orbit $v_i G_{x0}$, we need a set generating the whole group C_i . In Appendix B, we will show how to check that a computed set of elements of C_i actually generates C_i . In the remainder of this section, we assume that a generating set of the whole group C_i is available.

If C_i is the stabilizer of an axis v_i in G_{x0} , then the number of N_{x0} -orbits on the axes contained in the orbit $v_i G_{x0}$ is equal to the number of double cosets in $C_i \backslash G_{x0} / N_{x0}$. As we have seen in the previous subsection, the left cosets G_{x0} / N_{x0} correspond to the type 4 vectors in $\Lambda/2\Lambda$. Thus, the double cosets in $C_i \backslash G_{x0} / N_{x0}$ correspond to the orbits of the type 4 vectors in $\Lambda/2\Lambda$ under C_i . These orbits can easily be enumerated with the technique used in the previous subsection, so we may compute column 2 in Table 1. Clearly, the total of that column is equal to the number of orbits on axes under N_{x0} , and hence also to the number of double cosets in $\mathbb{M}_{v^+} \backslash \mathbb{M} / N_{x0}$. The stabilizer \mathbb{M}_{v^+} is of structure $2.B$. Thus, we have shown:

Proposition 3.5. *There are precisely 251 double cosets in $2.B \backslash \mathbb{M} / N_{x0}$. The number of double cosets in $2.B \backslash \mathbb{M} / N_{x0}$ contained in a double coset in $2.B \backslash \mathbb{M} / G_{x0}$ is given by Table 1, Column 2.*

We remark that the number of double cosets in $2.B \backslash \mathbb{M} / N_{x0}$ (with N_{x0} of structure $2^{2+11+22} \cdot (M_{24} \times 2)$) has not been computed before.

The last two columns of Table 1 describe the structure of the stabilizer in G_{x0} of an axis in a given G_{x0} -orbit. The computation of this structure is described in Appendix B. We also list the number of double cosets in $2.B \backslash \mathbb{M} / N_{xyz}$ in column 3 for each of the twelve G_{x0} -orbits. The computation of these numbers is described in Appendix C.1.

We have verified all the entries of Table 1. We also determined the N_0 -orbits on the axes, and the result is shown in Appendix C.1.

4 Counting the feasible axes

In this section we compute the number of feasible axes. Recall that β^+ and β^- are the $2A$ involutions in \mathbb{M} corresponding to the specific axes v^+ and v^- as defined in Section 2.1. We define the set of *feasible axes*, denoted X^- , as the orbit of the axis v^- under the stabilizer \mathbb{M}_{v^+} of axis v^+ , i.e.

$$X^- = \{v^- h \mid h \in \mathbb{M}_{v^+}\}.$$

We write H for the stabilizer $\mathbb{M}_{v^+} \cap G_{x0}$ of v^+ in G_{x0} , as in [Sey24]. The group H is also the centralizer of β^+ in G_{x0} , and of structure $2^{1+23}.\text{Co}_2$. Since the triality element τ centralizes β^+ , it must also fix its corresponding axis v^+ and we have $\tau \in \mathbb{M}_{v^+}$. Our strategy for counting the feasible axes is analogous to the method for counting the axes in Section 3: we first decompose X^- into orbits under the action of H and then compute a transition matrix describing how τ acts on these orbits. We will just summarize this briefly. We will show:

Proposition 4.1. *There are 11 707 448 673 375 feasible axes.*

We use a method similar to that in Section 3 for disambiguating orbits on the feasible axes under H . We adopt the naming conventions for these orbits from [Sey24], Section 9.

Lemma 4.2. *There exist at least ten orbits on the feasible axes under H . These axes are distinguished by the conjugacy class of tx_{-1} in \mathbb{M} where t is the $2A$ involution associated to an axis, and by the norm of the projection of the axis onto the subspace of 300_x spanned by $\lambda_\beta \otimes \lambda_\beta$.*

Proof: We generate a large sample of feasible axes by applying random elements of H and powers of the triality element τ to the initial axis v^- . A similar watermarking strategy as in the proof of Lemma 3.2 allows to disambiguate ten different H -orbits on the feasible axes. Those can be distinguished by the two invariants described in the statement of the lemma. \square

Remark: Müller [Mül08] has enumerated the ten orbits on the feasible axes under the action of $H = \mathbb{M}_{v^+} \cap G_{x0}$ on X^- and computed their sizes in [Mül08], Table 3. However, that paper uses properties of the Baby Monster and its character table. We will confirm these results with `mmgroup` and provide some additional information for each orbit in our Table 3.

We choose representatives for the feasible axes for each of the ten potential orbits found in Lemma 4.2. To confirm that a given feasible axis belongs to one of these potential H -orbits we use a watermarking technique to identify the likely orbit, similar to the watermarking used in Section 3.1. (A slightly more sophisticated method for the disambiguation of the H -orbits of the feasible axes is discussed in [Sey24], Section 9.2.)

Having identified the likely orbit of a feasible axis, we compute an element of H that maps the axis to the corresponding representative, as discussed in Appendix A.2.

The triality transition matrix for X^- . Our objective is to compute the transition matrix M' for the operation of the triality element τ on the H -orbits on the feasible axes, as shown in Table 4. Matrix M' agrees with the matrix shown in [Mül08], Table 3. Rows and columns of M' correspond to the H -orbits on the feasible axes; entries are interpreted as the entries of matrix M in Table 2. The columns in the table are normalized so that they sum to $|H:H \cap N_{xyz}| = 93150$. The computation of M' will be discussed below.

Using the same argument based on Markov chains as in Section 3.1 we may compute a vector containing the sizes of the H -orbits on the feasible axes (up to a scalar multiple) from matrix M' . We have:

Lemma 4.3. *The orbit labeled with '2A1' and containing the axis v^- has size 1.*

H -orbit	No. suborbits		H -orbit size	Stabilizer C of an axis in the orbit	
	$H \cap N_{x0}$	$H \cap N_{xyz}$		$C \cap Q_{x0}$	$C/(C \cap Q_{x0})$
2A1	1	1	1	2^{1+23}	Co_2
2A0	5	6	93150	2^{1+22}	$2^{10}.M_{22}.2$
2B1	4	5	7286400	2^{1+16}	$2^{1+8}.S_6(2)$
2B0	6	8	262310400	2^{1+15}	$2^{1+4+6}.A_8$
4A1	9	12	4196966400	2^{12}	$2^{9+1}.L_3(4).2$
4B1	12	18	470060236800	2^7	$2^{1+8+5}.S_6$
4C1	6	9	537211699200	2^5	$2^{1+4+6}.A_8$
6A1	3	5	9646899200	2^2	$U_6(2).2$
6C1	8	14	6685301145600	2^2	$2^{1+8}.U_4(2).2$
10A1	5	9	4000762036224	2	HS.2
Total	59	87	11707448673375		

Table 3: Sizes of H -orbits on feasible axes (with $H = \mathbb{M}_{v+} \cap G_{x0}$), and stabilizers in H of an axis in the orbit.

	2A1	2A0	2B1	2B0	4A1	4B1	4C1	6A1	6C1	10A1
2A1	.	1
2A0	93150	925	63	15	1
2B1	.	4928	63	120	42	1
2B0	.	42240	4320	1815	420	30	15	.	.	.
4A1	.	45056	24192	6720	1807	272	120	891	27	.
4B1	.	.	64512	53760	30464	10287	5040	24948	3060	3850
4C1	.	.	.	30720	15360	5760	3495	.	4320	4125
6A1	2048	512	.	891	36	100
6C1	43008	43520	53760	24948	53451	53900
10A1	32768	30720	41472	32256	31175

Table 4: Action of the triality element τ on the H -orbits in the feasible axes.

The entry in row i , column j is the number of $(H \cap N_{xyz})$ -orbits in H -orbit j that are mapped to H -orbit i . The total of each column is $|H:H \cap N_{xyz}| = 93150$.

Proof: The group H fixes the two involutions β^+ and x_{-1} , and hence also their product β^- and the axis $v^- = \text{ax}(\beta^-)$. Axis v^- is in orbit 2A1; so orbit 2A1 has size 1. \square

Thus we may compute the sizes of all H -orbits on the feasible axes, as shown in Table 3, column 4.

For computing the transition matrix M' we use the fact that the triality element τ normalizes the group $H \cap N_{xyz}$ with structure $2^{2+11+20}.M_{22}.2$. Thus for any $g \in H$ and feasible axis v the H -orbit of $vg\tau$ depends only on the left coset $g(H \cap N_{xyz})$. The index $|H:H \cap N_{xyz}|$ is equal to 93150; hence a left transversal \mathcal{T}' of $H/(H \cap N_{xyz})$ in H can be effectively computed. For computing the transition matrix M' it suffices to transform a representative of each H -orbit with all elements $\{g \cdot \tau \mid g \in \mathcal{T}'\}$ and to determine the H -orbits of the transformed axes.

In Appendix A.2 we will discuss how to effectively determine the H -orbit of a feasible axis. We may speed up the computation of M' using a similar technique as described in

Section 3.2. We also verify that the images of all feasible axes obtained in the course of this computation are in one of the ten orbits given by Lemma 4.2. This proves:

Lemma 4.4. *There are precisely ten orbits on the feasible axes under H .*

Having computed matrix M' in Table 4, we may compute column 4 of Table 3, as discussed above; in particular, Proposition 4.1 is proven.

For obtaining the last two columns of Table 3 we compute the structure of the stabilizer C_i of a feasible axis v_i in H , where v_i runs through the representatives of the H -orbits on the feasible axes. We may compute random elements of C_i as follows. We multiply v_i by a random element g_1 of H . Then we use the technique described in Appendix A.2 to compute a $g_2 \in H$ that maps $v_i g_1$ to v_i ; i.e. $g_1 g_2$ centralizes v_i . That way we have computed 10 random elements of the stabilizer C_i . These elements generate the whole group C_i with a very high probability. The method discussed in Appendix B can be used to check if a set of elements of C_i actually generates C_i .

So we have a generating system for the stabilizer in H of a feasible axis, for each H -orbit on the feasible axes. The structures of these stabilizers have been computed with MAGMA and mmgroup, similar to the corresponding computation in Appendix B for the G_{x0} -orbits. These structures are displayed in the last two columns of Table 3.

It remains to compute columns 2 and 3 of Table 3. As in [Sey24], we call a vector $\lambda \in \Lambda/2\Lambda$ *feasible* if λ is of type 2 and $\lambda + \lambda_\beta$ is of type 4. Then $H \cap N_{x0}$ is the stabilizer of the feasible vector $\lambda_\beta + \lambda_\Omega$, see [Sey24], Section 9.1. Hence there is a one-to-one correspondence between the left cosets $H/(H \cap N_{x0})$ and the feasible type 2 vectors in $\Lambda/2\Lambda$.

Let C_i be the stabilizer of a feasible axis v_i in H . Since the left cosets $H/(H \cap N_{x0})$ correspond to the feasible type 2 vectors in $\Lambda/2\Lambda$, the double cosets in $C_i \backslash H/(H \cap N_{x0})$ correspond to the orbits in the feasible type 2 vectors in $\Lambda/2\Lambda$ under C_i . These orbits can easily be enumerated with the technique described in Section 3.3; so we may compute column 2 in Table 3. Clearly, the total of that column is equal to the number of orbits on feasible axes under $H \cap N_{x0}$, and hence also to the number of double cosets in $H \backslash \mathbb{M}_{v+}/(H \cap N_{x0})$. The stabilizer \mathbb{M}_{v+} is of structure 2.B. Thus we have shown:

Proposition 4.5. *There are precisely 59 double cosets in $H \backslash 2.B/(H \cap N_{x0})$. The number of double cosets in $H \backslash 2.B/(H \cap N_{x0})$ contained in a double coset in $H \backslash 2.B/H$ is given by Table 3, Column 2.*

It is well known that the group H of structure $2^{1+23}.\text{Co}_2$ is a maximal subgroup of 2.B, and that the group $H \cap N_{x0}$ of structure $2^{2+11+20}.(M_{22} : 2 \times 2)$ is maximal in H , see, e.g., [CCN⁺85]. We also list the number of double cosets in $H \backslash 2.B/(H \cap N_{xyz})$ in column 3 for each of the ten H -orbits. The computation of these numbers is described in Appendix C.2.

We have verified all the entries of Table 3. We also determined the $(2.B \cap N_0)$ -orbits on the feasible axes and the result is shown in Appendix C.2.

5 Properties of the Monster

In this section, we use the enumeration results from Sections 3 and 4 to obtain several results about the Monster.

Theorem 5.1. *The order of the Monster \mathbb{M} equals*

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

$$= 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.$$

Proof: In Proposition 3.1, the size of the set X^+ of axes was determined. In Propositions 4.1, the size of the set X^- of feasible axes is given. Thus the order of the Monster is

$$\mathbb{M} = |X^+| \cdot |X^-| \cdot |S|$$

where S is the stabilizer in \mathbb{M} of the two axes v^+ and v^- . The product of the two 2A involutions β^+ and β^- associated with v^+ and v^- is the central 2B involution x_{-1} in G_{x_0} which must be centralized by S . By Theorem 2.9 or Theorem 2.15, it follows that S is contained in G_{x_0} . The stabilizer of v^+ and v^- in G_{x_0} can be read off from Table 3 to be $2^{1+23}.\text{Co}_2$. Since the order 42,305,421,312,000 of Co_2 is assumed to be known, the result follows. \square

Recall that $C_{\mathbb{M}}(t)/\langle t \rangle$ where t is a 2A involution in the Monster is the Baby Monster B , the second largest of the sporadic simple groups. Using $|B| = |X^-| \cdot |S|/2$ we have also shown:

Corollary 5.2. *The order of the Baby Monster B equals*

$$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 41 \cdot 47$$

$$= 4,154,781,481,226,426,191,177,580,544,000,000.$$

Next, we will prove that the Monster is simple. Our proof is along the lines of the corresponding proof in [Car23]. For a group G we write $G^\#$ for the set of non-identity elements of G . If G is a subgroup and H is a subset of an ambient group M , we write $C_G(H)$ for the centralizer of H in G .

Lemma 5.3. *If N is a normal subgroup of \mathbb{M} and z is an involution in \mathbb{M} with $C_N(z) = 1$ then N is abelian of odd order; and conjugation with z in N is equivalent to inversion in N .*

Proof: When the involution z acts by conjugation on N , it has exactly one fixed point, the identity. Thus $|N|$ is odd. Let $a, b \in N$. The mapping $N \rightarrow N$ given by $a \mapsto aza^{-1}z$ is injective (and hence bijective), since $aza^{-1}z = bzb^{-1}z$ implies $b^{-1}aza^{-1}b = z$, i.e. $a^{-1}b \in C_N(z)$. We have $(aza^{-1}z)^z = (aza^{-1}z)^{-1}$. Hence $c^z = c^{-1}$ for all $c \in N$. Since inversion is an automorphism on N , the group N is abelian. \square

Lemma 5.4. *A normal subgroup N of \mathbb{M} with $|G_{x_0} \cap N| = 1$ is trivial.*

Proof: We use the argument from the proof of Lemma 4.8 in [Car23]. Let N be a normal subgroup of \mathbb{M} with $|G_{x_0} \cap N| = 1$. Then $|C_N(x_{-1})| = 1$. Let E be the elementary abelian 2 subgroup $\{x_{\pm 1}, x_{\pm \Omega}\}$ of Q_{x_0} , with $x_{\pm 1}, x_{\pm \Omega}$ as in Section 2.1. Since conjugation with the triality element τ cyclically exchanges the three elements of $E^\#$, we have $|C_N(e)| = 1$ for all $e \in E^\#$. So by Lemma 5.3, $|N|$ is odd, and conjugation in N with any $e \in E^\#$ is equivalent to inversion in N . Thus conjugation with the product of the three elements of $E^\#$ is also inversion in N . Since that product is equal to 1, inversion is the identity map in N . Since $|N|$ is odd, this implies $|N| = 1$. \square

Lemma 5.5. *The group G_{x_0} contains the characteristic series*

$$1 \triangleleft \langle x_{-1} \rangle \triangleleft Q_{x_0} \triangleleft G_{x_0}.$$

This series contains all normal subgroups of G_{x_0} .

Proof: We may use the argument in the proof of [Car23], Lemma 4.5. By construction, $\langle x_{-1} \rangle$ is the center of G_{x_0} , and Q_{x_0} is a normal subgroup with quotient $G_{x_0}/Q_{x_0} \cong \text{Co}_1$. The series is therefore a normal series. That it contains all normal subgroups of G_{x_0} follows from the fact that Q_{x_0} is extraspecial, Co_1 is simple, and the natural 24-dimensional representation $Q_{x_0}/\langle x_{-1} \rangle \cong \Lambda/2\Lambda$ of Co_1 is irreducible over \mathbb{F}_2 . \square

Theorem 5.6. *The Monster is a simple group.*

Proof: We adapt the proof of Theorem 4.12 from [Car23] to our notation. Let N be a non-trivial normal subgroup of \mathbb{M} . By Lemma 5.4, the intersection $N \cap G_{x_0}$ must be a non-trivial normal subgroup of G_{x_0} . So by Lemma 5.5, the group $N \cap G_{x_0}$ must be one of the groups $\langle x_{-1} \rangle$, Q_{x_0} , or G_{x_0} . Suppose $N \cap G_{x_0} = \langle x_{-1} \rangle$. This would imply $x_{-\Omega} = (x_{-1})^\tau \in N$. Since $x_{-\Omega} \in G_{x_0} \setminus \langle x_{-1} \rangle$, this contradicts the assumption $N \cap G_{x_0} = \langle x_{-1} \rangle$.

Let $d \in \mathcal{P} \setminus \{\pm 1, \pm \Omega\}$, with \mathcal{P} the *Parker loop* as in [Con85, Sey20a]. Then $x_d \in Q_{x_0}$, but $x_d^\tau = y_d \in G_{x_0} \setminus Q_{x_0}$. Thus $N \cap G_{x_0} = Q_{x_0}$ would imply $y_d \in N \cap (G_{x_0} \setminus Q_{x_0})$, a contradiction.

Hence $G_{x_0} \subset N$. Let $g = x_\delta \in G_{x_0}$, for any odd element δ of the Golay cocode. Then $g^\tau g = \tau$, implying $\tau \in N$. Hence $N = \mathbb{M}$.

Note that all calculations in this proof can be done inside the group N_0 . \square

We now show that the Monster is the full automorphism group of the Griess algebra and the Moonshine module. This result was first obtained by Tits [Tit83, Tit84] by reducing it to a group-theoretical characterization of the Monster given by Smith [Smi79]. Our method utilizes results of Carnahan [Car23] on the order of $\text{Aut}(V^\natural)$ and Borchers' proof of the Conway-Norton Moonshine conjectures [Bor92].

Theorem 5.7. *The Monster is the full automorphism group of the Griess algebra and the Moonshine module, i.e., one has $\mathbb{M} = \text{Aut}(\mathcal{B}) = \text{Aut}(V^\natural)$.*

Proof: By Theorem 2.16, we have $\text{Aut}(\mathcal{B}) = \text{Aut}(V^\natural)$. In Carnahan [Car23], it was proven that $\text{Aut}(V^\natural)$ equals the order of the Monster as in Theorem 5.1 up to a factor which is a power of 11; see [Car23], Corollary 5.2 and Theorems 5.3, 5.4, and 5.5.

Thus we need to show that the Monster has no 11-Sylow subgroup of order 11^3 or larger. If this were the case, there would exist a subgroup H of order 11^3 in $\text{Aut}(\mathcal{B})$. By Borchers [Bor92], the trace of any element g of $\text{Aut}(V^\natural)$ on V^\natural is a completely replicable modular function. These functions have been classified in [ACMS92]. In particular, there is only one completely replicable function of order 11 and none of order 11^2 . Thus the exponent of the group H must be 11. In addition, the trace of an order 11 element g in $\text{Aut}(V^\natural)$ on \mathcal{B} equals 17, the coefficient of q^1 in the unique completely replicable function of order 11. For the dimension of the subspace of \mathcal{B} fixed by H we obtain

$$\dim \mathcal{B}^H = \frac{1}{|H|} \sum_{h \in H} \text{tr}(h|\mathcal{B}) = \frac{1}{11^3} (196884 + (11^3 - 1) \cdot 17) = \frac{1814}{11}$$

which is not an integer. Thus such a subgroup H cannot exist and the 11-Sylow subgroup of $\text{Aut}(V^\natural)$ must have order 11^2 .

It follows that $|\text{Aut}(V^\natural)| = |\mathbb{M}|$ and hence $\text{Aut}(V^\natural) = \mathbb{M}$. \square

We finally show that the Monster has exactly two conjugacy classes of involutions.

Theorem 5.8. *The Monster has two conjugacy classes of involutions: the 2A involutions corresponding to the axes and with centralizers isomorphic to a two-fold cover of the Baby Monster and the 2B involutions with centralizers isomorphic to $G_{x0} \cong 2_+^{1+24}.\text{Co}_1$.*

We provide two proofs, a computational one in Appendix E using mmgroup and a theoretical one using vertex operator algebras below.

Proof: It follows from Theorem 5.1 that the index of G_{x0} in \mathbb{M} is odd and hence that any involution of \mathbb{M} is conjugated to an involution in G_{x0} .

We first observe that there are no involutions of type 1 in $\text{Aut}(V^\natural)$. Indeed, by [Bor92, CKU18] the graded trace of such an involution t equals either the graded trace of a 2A like or a 2B like involution. This determines the character of $(V^\natural)^t$ and hence the whole vector-valued character of $(V^\natural)^t$. In particular, we see that $(V^\natural)^t$ has no modules of conformal weight $1/4$ or $3/4$. Thus t must be of type 0.

We know from Lemma 2.10 that every involution of $\text{Aut}(V^\natural)$ of type 0 is either 2A like or 2B like and from Theorem 2.15 that every 2B like involution is actually a 2B involution. We also know from Theorem 2.13 that every 2A like involution corresponds uniquely to an Ising vector of V^\natural . Any involution in G_{x0} is centralized by the central element x_{-1} in G_{x0} and thus the corresponding Ising vector for a 2A like involution is fixed by x_{-1} , i.e., is contained in the fixpoint vertex operator subalgebra V_Λ^+ of V^\natural . The Ising vectors of V_Λ^+ have been classified in [LS07]. They either correspond to norm 4 vectors of Λ or to embeddings of $E_8(2)$ (the root lattice E_8 rescaled such that the minimal vectors have norm 4) into Λ . One immediately verifies that those two cases correspond to the first two orbits of axes of \mathcal{B} in Table 1 and thus these Ising vectors are axes in \mathcal{B} , i.e., the 2A like involution is a 2A involution. \square

The Monster is known to have a total of 194 conjugacy classes of elements forming 172 algebraic conjugacy classes [CCN⁺85]. Besides two classes of order 27, the classes of elements g can be distinguished by the traces of g and its powers g^2 and g^3 on \mathcal{B} . Explicit representatives have been first determined in [BW05]. We provide a list of representatives of these classes for mmgroup at the first author's webpage [Höh24]. Functions for listing and identifying a class are also available on that webpage. At the moment we are unable to distinguish the two conjugacy classes of elements of order 27.

Appendix A Mapping an axis to the representative of its orbit

A.1 Mapping an axis to the representative of its G_{x0} orbit

Class `Axis` in the mmgroup package models an axis of a 2A involution. For documentation we refer to [Sey21], Chapter *Axes of 2A involutions in the Monster*. Here one of the most important functions is the member function `reduce_G_x0` of class `Axis`. This function

returns an element of the group G_{x_0} that maps the axis to the representative of its G_{x_0} -orbit. This process is called the *reduction* of an axis (in G_{x_0}), and will be discussed in this section.

We will not prove that *every* axis can be reduced as described here. It suffices that we are able to reduce all axes occurring during our practical computations. Tests with the mmgroup package have shown that our reduction method has succeeded on hundreds of thousands of random axes. A key step in the implementation of the group operation in \mathbb{M} in mmgroup is the reduction of an axis in \mathbb{M} . Reduction of an axis in \mathbb{M} is simpler than in G_{x_0} , because we may transform an axis to a 'simpler' G_{x_0} -orbit whenever possible.

We assume that an axis is given as a vector in the representation \mathcal{B} (with entries taken modulo 15). Our first step is to determine the G_{x_0} -orbit of the axis. Here we use the method in [Sey24], Section 8.4 for a quick disambiguation of the twelve orbits. (At this stage we are not yet sure that there are no more than twelve orbits; but any attempt to reduce an axis will certainly fail if the axis is not in one of these orbits.)

The next step is called the *beautifying* of an axis. In this step we try to transform the symmetric 24×24 matrix corresponding to the part 300_x of the axis into a nice form by using a transformation in G_{x_0} . The same operation is also applied to a candidate for the representative of a G_{x_0} -orbit of an axis, in order to obtain a more beautiful representative. Criteria for a beautiful symmetric matrix are:

- Few off-diagonal nonzero entries, so that eigenspaces are visible or at least easy to compute.
- The signs of the nonzero off-diagonal elements should follow an orderly pattern.

This beautification is implemented in the function `beautify_axis` in file `beautify_axis.py` in the mmgroup package. The parts 300_x of the representatives of the G_{x_0} -orbits on the axes can be displayed with the following Python script:

```
from mmgroup.axes import Axis
for name, representative in Axis.representatives().items():
    print("Name of axis orbit:", name)
    print("Part 300_x of representative of orbit:")
    representative.display_sym()
```

In all cases, after beautifying an axis, the part 300_x of the axis is equal to the corresponding part of one of those representatives. Afterwards, it suffices in all but one case to transform the axis with an element of Q_{x_0} , in order to obtain the representative of the G_{x_0} -orbit of the axis. In the case of the orbit '6F', we have to work in an extension of structure $2^{1+24+11}$ of Q_{x_0} instead.

In all cases, the reduction of the axis was achieved.

A.2 Mapping a feasible axis to the representative of its H orbit

The reduction of a feasible axis under the group $H = \mathbb{M}_{v+} \cap G_{x_0}$ follows a procedure entirely analogous to the one described for G_{x_0} -orbits in Appendix A.1. Member function `reduce_G_x0` of class `BabyAxis` in the mmgroup package uses the same principles of

orbit disambiguation, beautification, and final reduction to map a feasible axis to the pre-computed representative of its H -orbit. For details we refer again to the documentation in [Sey21], Chapter *Axes of 2A involutions in the Monster*.

As in Appendix A.1, we will not prove that *every* feasible axis can be reduced. It suffices that we are able to reduce all axes occurring during the calculation. In all cases, the reduction of the axis was achieved.

Appendix B Computing stabilizers of axes in G_{x0} -orbits

A random algorithm is called a *Monte Carlo* algorithm if it may compute a wrong result with a (usually) small probability, and a *Las Vegas* algorithm if it either succeeds or indicates failure. In Section 3.2 et seq. we have computed a generating set of the stabilizer C_i in G_{x0} of a given axis v_i using a Monte Carlo algorithm. Note that this algorithm computes a generating set of a group C'_i that might be a proper subgroup of C_i with a very small probability. In this section we will convert that algorithm to a Las Vegas algorithm. In order to detect $C'_i \subsetneq C_i$, it suffices to compute the order $|C'_i|$ of the group C'_i . Then we may multiply $|C'_i|$ by the (known) size of the G_{x0} -orbit of v_i . If this product is equal to the order of G_{x0} , then we have $C'_i = C_i$. Here it suffices to compute a lower bound for $|C'_i|$ that is sharp with high probability.

While computing the order of a subgroup is a standard feature in computer algebra systems like MAGMA [BCP97] that hardly needs a detailed discussion, the group G_{x0} is too large to be handled directly. Our approach therefore combines the strengths of mmgroup for efficient computation within G_{x0} with MAGMA's ability to analyze smaller factor groups. The computer algebra system MAGMA usually represents a finite group as a permutation group or as a matrix group over a finite field. It includes a large number of algorithms from computational group theory, such as those for computing group orders, identifying subgroups, and more; see [HEO05] for a comprehensive overview. The group G_{x0} is so large that we have not found a satisfactory way to compute with that group in MAGMA. Computing in the group G_{x0} in the mmgroup package is easy; but that package contains only a limited set of algorithms from computational group theory. It turns out that this is sufficient for computing a generating set for a subgroup C'_i of the stabilizer C_i of an axis, and also a lower bound for the order of that subgroup. In all our tests (over a dozen runs), the computed lower bound for $|C'_i|$ was equal to the expected order of C_i for all cases.

As a subgroup of $G_{x0} \cong 2^{1+24}.\text{Co}_1$, the group C_i has a normal subgroup $C_i \cap Q_{x0}$ with factor group $\overline{C}_i = C_i / (C_i \cap Q_{x0})$. We use the mmgroup package for representing the generators of \overline{C}_i (with $\overline{C}_i \subset \text{Co}_1 \subset \text{SL}_{24}(2)$) as 24×24 matrices over \mathbb{F}_2 . Then we use MAGMA to compute the structure of the group \overline{C}_i generated by these matrices. The structure of the group \overline{C}_i obtained in this way is displayed in Column 5 of Table 1. The structure of the subgroup $C_i \cap Q_{x0}$ can easily be computed with mmgroup; it is displayed in Column 4 of Table 1.

In the remainder of this subsection we will discuss the computation of a lower bound for $|C'_i|$, with $C'_i \subset G_{x0}$ given by a set of generators. In Section 3.2 we have computed the action of such a group C'_i on the type 4 vectors in $\Lambda/2\Lambda$ by using the class `Orbit_Lin2` in the mmgroup package. This way we obtain a permutation representation of C'_i with

kernel $C'_i \cap Q_{x0}$, i.e. a faithful representation of $\overline{C'_i}$. The class `Orbit_Lin2` also supports the computation of a Schreier vector for the action of the group C'_i on the type 4 vectors in $\Lambda/2\Lambda$ as discussed in [HEO05], Section 4.1.1. Using a Schreier vector, we may compute an element of C'_i that maps a vector in $\Lambda/2\Lambda$ to any vector in the same C'_i -orbit. So, in principle, a Schreier vector may be used for computing the stabilizer of any type 4 vector in $\Lambda/2\Lambda$. For simplicity, we assume that this type 4 vector is the vector λ_Ω , as defined in Section 2.1. Let $C'_{i,1}$ be the stabilizer of λ_Ω in C'_i . Then $|C'_i|$ is the product of $|C'_{i,1}|$ and the size of the orbit of λ_Ω under the action of C'_i . Since we need just a lower bound for $|C'_i|$, it suffices to compute a set of random elements of C'_i that generates $C'_{i,1}$ with high probability. Since $C'_{i,1}$ fixes λ_Ω , it is a subgroup of the group $N_{x0} \cong 2^{1+24+11}.M_{24}$.

Let ρ_{24} be the representation of M_{24} as a subgroup of $\text{SL}_{11}(2)$ given by the action of M_{24} on the even part of the Golay cocode \mathcal{C}^* . Since the factor group $C'_i/(C'_i \cap Q_{x0})$ is a subgroup of M_{24} , the restriction of representation ρ_{24} to that factor group is also a (possibly non-faithful) representation of $C'_{i,1}$. We also write ρ_{24} for that representation of $C'_{i,1}$; and the `mmgroup` package supports computation in ρ_{24} . Considering ρ_{24} as a permutation representation of $C'_{i,1}$ in \mathbb{F}_2^{11} , we may compute the stabilizer of a vector $v \in \mathbb{F}_2^{11}$ that is not fixed by $C'_{i,1}$, using the same method as above. This way we obtain a subgroup $C'_{i,2} \subsetneq C'_{i,1}$; and the index of $C'_{i,2}$ in $C'_{i,1}$ is the size of the orbit of v under the action of $C'_{i,1}$. Again, it suffices to find a set of elements of $C'_{i,2}$ that generates $C'_{i,2}$ with high probability. Repeating this process we obtain a chain of subgroups

$$C'_i \supset C'_{i,1} \supset \dots \supset C'_{i,k},$$

such that $C'_{i,k}$ fixes all vectors in ρ_{24} . Thus $C'_{i,k}$ is contained in the normal subgroup of structure $2^{1+24+11}$ of N_{x0} . The `mmgroup` package supports computation in the subgroup $2^{1+24+11}$ of N_{x0} , so that the order of $C'_{i,k}$ can be computed.

On the authors' PCs the computation of Tables 1 and 2 (excluding the computation of the structure of the stabilizers of the axes with MAGMA) takes about a minute.

Appendix C Orbits on axes under N_0 and $N_0 \cap 2.B$

C.1 Orbits on the axes in \mathcal{B} under N_0

In Table 5 we list the 123 orbits on the 2A axes under the action of the maximal subgroup N_0 of M . Recall that N_0 has structure $2^{2+11+22}.M_{24}.S_3$, and that the normal subgroup of N_0 of structure $2^{2+11+22}.M_{24}$ is denoted by N_{xyz} .

For each N_0 -orbit on the axes, we display the structure of the stabilizer in N_0 of an axis in that orbit. This stabilizer is presented in the form $C = E.G.S$, where $E = C \cap 2^{2+11+22}$, $E.G = C \cap N_{xyz}$. More specifically, we have:

- E is the intersection of C with the normal 2-subgroup $2^{2+11+22}$ of N_0 . It is displayed in Column 2 of the table. The structure of E is given as $2^{\lambda+\mu+\nu}$, meaning that its intersections with the characteristic subgroups 2^2 and 2^{2+11} of $2^{2+11+22}$ have orders 2^λ and $2^{\lambda+\mu}$, respectively, and the total order of E is $2^{\lambda+\mu+\nu}$. Here we omit leading zero terms in the exponent describing E .

- G is the projection of $C \cap N_{xyz}$ to the factor group $N_{xyz}/2^{2+11+22} \cong M_{24}$. Its structure and order are displayed in Columns 3 and 4. Here Column 3 has been computed with the GAP computer algebra package [GAP24].
- S is the projection of C to the factor group $N_0/N_{xyz} \cong S_3$. It is displayed in Column 5.

Since $N_0/N_{xyz} \cong S_3$, an N_0 -orbit of an axis decomposes into $|S_3| : |S| = 6 : |S|$ different N_{xyz} -orbits of the same size, with S as above. Since $N_{xyz} < N_{x0} < N_0$ and $|N_0 : N_{x0}| = 3$, each N_0 -orbit decomposes into one, two, or three N_{x0} -orbits. The number of N_{x0} -orbits in a given N_0 -orbit is determined by the action of the group S on the three cosets of N_{x0} in N_0 .

- If $|S| = 1$, S fixes all three cosets, resulting in three distinct N_{x0} -orbits, each of them containing two N_{xyz} -orbits.
- If $|S| = 2$, S fixes one coset and permutes the other two, resulting in two N_{x0} -orbits. One of them contains one, and the other contains two N_{xyz} -orbits.
- If $|S| \geq 3$, S acts transitively on the three cosets, resulting in a single N_{x0} -orbit which may contain one or two N_{xyz} -orbits.

The final column, ‘ G_{x0} -orbits’ of Table 5, describes how these constituent N_{x0} -orbits are contained in the twelve G_{x0} -orbits from Table 1. For example:

- An entry ‘ $4B, 6A, 6C$ ’ indicates that the N_0 -orbit decomposes into three N_{x0} -orbits lying in those G_{x0} -orbits.
- An entry ‘ $2A, 2B^2$ ’ indicates that the N_0 -orbit decomposes into two N_{x0} -orbits. The smaller one lies in G_{x0} -orbit $2A$, while the larger one lies in G_{x0} -orbit $2B$.
- An entry ‘ $2A^3$ ’ indicates that the N_0 -orbit contains a single N_{x0} -orbit lying in the G_{x0} -orbit $2A$.

Table 5: Orbits of N_0 on axes

N_0 -orbits on the axes, and stabilizers $C = E.G.S$ of these axes in N_0					
No	E	G	$ G $	S	G_{x0} -orbits
1	$2^{2+11+20}$	$M_{22} : 2$	887040	S_3	$2A^3$
2	$2^{2+10+16}$	$2^4 : A_8$	322560	2	$2A, 2B^2$
3	$2^{1+11+11}$	M_{23}	10200960	2	$2A, 4A^2$
4	2^{2+7+14}	$2^{1+6} : \text{PSL}_3(2)$	21504	S_3	$2B^3$
5	2^{1+7+12}	$2^6 : A_5 : S_3$	23040	2	$2B, 4A^2$
6	2^{6+10}	$2^4 : A_7$	40320	S_3	$4A^3$
7	2^{1+5+11}	$2^4 : S_6$	11520	2	$2B, 4B^2$
8	2^{1+4+11}	$2^{1+6} : \text{PSL}_3(2)$	21504	2	$2B, 4C^2$
9	2^{6+6}	$2^4 : A_8$	322560	2	$4A, 4B^2$
10	2^{3+10}	$2^6 : \text{PSL}_3(2)$	10752	S_3	$4C^3$
11	2^{4+8}	$2^{1+6} : \text{PSL}_3(2)$	21504	2	$4A, 4C^2$

No	E	G	$ G $	S	G_{x0} -orbits
12	2^{2+9}	$\text{PSL}_3(4) : 2$	40320	2	$4A, 6A^2$
13	2^{4+10}	$2^4 : \text{PSL}_3(2)$	2688	2	$4A, 4B^2$
14	2^{11}	M_{11}	7920	2	$4A, 8B^2$
15	2^{2+9}	$2^4 : 3 : S_5$	5760	2	$4A, 6C^2$
16	2^{2+8}	$2^5 : S_5$	3840	S_3	$4B^3$
17	2^{3+6}	$2^6 : (S_3 \times S_3)$	2304	S_3	$4B^3$
18	2^{3+8}	$2^{2+6} : S_3$	1536	2	$4B^2, 4C$
19	2^{1+0}	M_{22}	443520	S_3	$6A^3$
20	2^{1+8}	$2^{2+6} : S_3$	1536	S_3	$4C^3$
21	2^{1+0}	$M_{22} : 2$	887040	2	$6A, 10A^2$
22	2^{1+7}	$2^4 : S_6$	11520	1	$4B, 6A, 6C$
23	2^{1+6}	$2^4 : S_6$	11520	2	$4B, 6A^2$
24	2^{2+7}	$2^{2+6} : S_3$	1536	2	$4B, 4C^2$
25	2^5	$2^{1+6} : \text{PSL}_3(2)$	21504	2	$4C, 6F^2$
26	2^{2+4}	$2^4 : 3 : S_5$	5760	2	$4B, 6C^2$
27	2^2	A_8	20160	2	$6A, 10A^2$
28	2^6	$2^4 : A_5$	960	2	$4B, 10B^2$
29	2^{1+6}	$2^{2+4} : S_3$	384	2	$4B, 6C^2$
30	2^5	$2^{2+6} : S_3$	1536	2	$4C, 8B^2$
31	2^5	$2^{2+6} : S_3$	1536	2	$4C, 10B^2$
32	2^{1+5}	S_6	720	2	$4B, 10A^2$
33	2^6	S_6	720	2	$4B, 12C^2$
34	2^4	$2^4 : \text{PSL}_3(2)$	2688	2	$4C, 6F^2$
35	2^{1+3}	$2^4 : \text{PSL}_3(2)$	2688	2	$4C, 10A^2$
36	2	A_8	20160	2	$6A, 12C^2$
37	2^4	$2^6 : D_{10}$	640	S_3	$8B^3$
38	2^6	$2^6 : S_3$	384	2	$4B, 8B^2$
39	2^{1+4}	$2^{2+5} : S_3$	768	2	$4C, 6C^2$
40	2	$2^4 : S_6$	11520	2	$6A, 12C^2$
41	2^6	$2 \times \text{PSL}_3(2)$	336	2	$4B, 12C^2$
42	2^4	$2^6 : (S_3 \times S_3)$	2304	1	$6A, 6C, 8B$
43	2	$2^4 : A_6$	5760	2	$6A, 8B^2$
44	2^{1+0}	$2^4 : S_5$	1920	S_3	$6C^3$
45	2^2	S_6	720	S_3	$6C^3$
46	1	M_{11}	7920	2	$8B^2, 10A$
47	2^{1+0}	$2^5 : S_5$	3840	2	$6C, 10A^2$
48	1	A_7	2520	S_3	$10A^3$
49	2^4	$2^{3+4} : S_3$	768	1	$6C, 6C, 8B$
50	2^{1+2}	S_6	720	2	$6C^2, 10A$
51	1	$2^4 : \text{PSL}_3(2)$	2688	3	$12C^3$
52	2	$2^4 : S_5$	1920	2	$6C, 8B^2$
53	2^4	$2^{2+4} : 3$	192	2	$4C, 10B^2$
54	2^4	$2^5 : S_3$	192	2	$4C, 12C^2$

No	E	G	$ G $	S	G_{x0} -orbits
55	2^2	$2^4 : (S_3 \times S_3)$	576	2	$6C, 10A^2$
56	2	$2^4 : S_5$	1920	1	$8B, 10A, 12C$
57	2	$2^{2+5} : S_3$	768	2	$6C, 12C^2$
58	2	$2^{2+6} : 3$	768	2	$6F, 10B^2$
59	2	$2^4 : (S_3 \times S_3) : 2$	1152	1	$8B, 10A, 12C$
60	2^2	$2^{2+3} : S_3$	192	2	$8B, 10A^2$
61	2^3	$S_3 \times S_4$	144	1	$6C, 10A, 12C$
62	1	$2^{2+3} : S_3$	192	S_3	$10B^3$
63	2	$2^{1+2+3} : S_3$	384	1	$8B, 10A, 10B$
64	2	$2^{1+4} : S_3$	192	2	$6C, 12C^2$
65	2	$2^5 : S_3$	192	2	$8B, 12C^2$
66	1	$\text{GL}_2(4) : 2$	360	2	$10A, 12C^2$
67	1	$2^5 : D_{10}$	320	2	$10B^2, 12C$
68	2^2	$2^4 : S_3$	96	1	$6C, 8B, 12C$
69	2^2	$2^4 : S_3$	96	1	$6C, 10B, 12C$
70	1	$2^{2+4} : S_3$	384	1	$8B, 8B, 12C$
71	2	$2^4 : S_3$	96	2	$6C, 8B^2$
72	2	$2^4 : S_3$	96	2	$6C, 10B^2$
73	1	$2^{2+4} : 3$	192	2	$6F^2, 8B$
74	1	$2^{2+3} : S_3$	192	2	$6F, 12C^2$
75	1	$2^{2+3} : S_3$	192	2	$10B, 12C^2$
76	1	$\text{PSL}_3(2)$	168	2	$10A, 12C^2$
77	2	2^{2+4}	64	2	$10A, 12C^2$
78	2	2^{2+4}	64	2	$10B, 12C^2$
79	2	A_5	60	2	$6C, 10B^2$
80	2	A_5	60	2	$10A, 10B^2$
81	1	S_5	120	2	$8B^2, 10A$
82	1	S_5	120	2	$10A, 12C^2$
83	2	$2^4 : S_3$	96	1	$8B, 10A, 12C$
84	2	$2^4 : S_3$	96	1	$10A, 10B, 12C$
85	1	$2^5 : S_3$	192	1	$12C, 12C, 12C$
86	1	$2^5 : 3$	96	2	$8B, 12C^2$
87	1	2^5	32	S_3	$8B^3$
88	1	2^{1+4}	32	S_3	$10B^3$
89	1	$(S_3 \times S_3) : 2$	72	2	$8B, 12C^2$
90	1	2^{2+2+3}	128	1	$8B, 10B, 12C$
91	1	2^{2+2+3}	128	1	$8B, 10B, 12C$
92	2	2^{2+3}	32	2	$6C, 12C^2$
93	1	2^{3+3}	64	2	$12C, 12C^2$
94	1	A_5	60	2	$8B^2, 12C$
95	1	$2^{1+2} : S_3$	48	2	$10A, 10B^2$
96	1	$S_3 \times S_3$	36	2	$8B^2, 12C$
97	1	A_4	12	S_3	$12C^3$

No	E	G	$ G $	S	G_{x0} -orbits
98	1	2^{3+2}	32	2	$6F, 10B^2$
99	1	2^{3+2}	32	2	$8B, 10B^2$
100	1	2^5	32	2	$8B, 12C^2$
101	1	2^{1+4}	32	2	$10B, 12C^2$
102	1	$2^{1+2} : S_3$	48	1	$8B, 8B, 10B$
103	1	2^3	8	S_3	$12C^3$
104	1	$7 : 3$	21	2	$6F, 12C^2$
105	1	$2 \times A_4$	24	1	$6F, 10B, 12C$
106	1	S_4	24	1	$8B, 12C, 12C$
107	1	S_4	24	1	$8B, 12C, 12C$
108	1	D_{12}	12	2	$12C, 12C^2$
109	1	2^2	4	S_3	$12C^3$
110	1	D_{10}	10	2	$8B, 10B^2$
111	1	3	3	S_3	$10B^3$
112	1	2^3	8	2	$10B, 10B^2$
113	1	2^3	8	2	$10B^2, 12C$
114	1	D_{12}	12	1	$8B, 10B, 12C$
115	1	S_3	6	2	$10B^2, 12C$
116	1	S_3	6	2	$12C, 12C^2$
117	1	D_{10}	10	1	$8B, 10B, 12C$
118	1	2^3	8	1	$10B, 10B, 12C$
119	1	D_8	8	1	$10B, 12C, 12C$
120	1	2^3	8	1	$10B, 12C, 12C$
121	1	2^2	4	2	$10B^2, 12C$
122	1	S_3	6	1	$10B, 12C, 12C$
123	1	3	3	2	$10B, 12C^2$

C.2 Orbits on the feasible axes in \mathcal{B} under $2.B \cap N_0$

Recall that the group \mathbb{M}_{v+} (of structure $2.B$) is the stabilizer of the specific axis v^+ , and that an axis is *feasible* if it is in the orbit of the specific axis v^- under \mathbb{M}_{v+} . In Table 6 we list the 32 orbits on the feasible axes under the action of the group $\mathbb{M}_{v+} \cap N_0 \cong 2^{2+11+20}.(M_{22} : 2).S_3$.

For each $(\mathbb{M}_{v+} \cap N_0)$ -orbit on the feasible axes, we display the structure of the stabilizer in $\mathbb{M}_{v+} \cap N_0$ of an axis in that orbit. This stabilizer is presented in the form $C = E.G.S$, where $E = C \cap 2^{2+11+20}$, $E.G = C \cap \mathbb{M}_{v+} \cap N_{xyz}$. The groups E , G , and S are displayed in Columns 2–5 of the table, with organization and legend as in Table 5.

We have $\mathbb{M}_{v+} \cap N_{xyz} \triangleleft \mathbb{M}_{v+} \cap N_0$ and $(\mathbb{M}_{v+} \cap N_0)/(\mathbb{M}_{v+} \cap N_{xyz}) = N_0/N_{xyz} = S_3$. So the discussion of the decomposition of the $(\mathbb{M}_{v+} \cap N_0)$ -orbits into $(\mathbb{M}_{v+} \cap N_{x0})$ -orbits and $(\mathbb{M}_{v+} \cap N_{xyz})$ -orbits can be taken verbatim from the corresponding discussion in Subsection C.1. We list the fusion of $(\mathbb{M}_{v+} \cap N_{x0})$ -orbits into $(\mathbb{M}_{v+} \cap G_{x0})$ -orbits in Column 6 of Table 6 in the same format as in the corresponding column in Table 5. Here the names of the $(\mathbb{M}_{v+} \cap G_{x0})$ -orbits are taken from Table 3.

Table 6: Orbits on feasible axes under $\mathbb{M}_{v+} \cap N_0$

$(\mathbb{M}_{v+} \cap N_0)$ -orbits on feasible axes, and stabilizers $C = E.G.S$ of these axes					
No	E	G	$ G $	S	$(\mathbb{M}_{v+} \cap G_{x0})$ -orbits
1	$2^{2+11+20}$	$M_{22} : 2$	887040	2	$2A1, 2A0^2$
2	$2^{2+11+18}$	$2^5 : S_5$	3840	S_3	$2A0^3$
3	$2^{2+10+15}$	$2^4 : S_6$	11520	2	$2A0, 2B1^2$
4	$2^{2+10+14}$	$2^4 : \text{PSL}_3(2)$	2688	2	$2A0, 2B0^2$
5	$2^{1+11+10}$	$\text{PSL}_3(4) : 2$	40320	2	$2A0, 4A1^2$
6	2^{2+7+14}	$2^4 : \text{PSL}_3(2)$	2688	2	$2B1, 2B0^2$
7	2^{2+7+12}	$2^{1+3+3} : S_3$	768	S_3	$2B0^3$
8	2^{1+7+12}	$2^5 : S_5$	3840	2	$2B1, 4A1^2$
9	2^{1+5+11}	$2^4 : S_6$	11520	2	$2B1, 4B1^2$
10	2^{1+7+11}	$2^{2+5} : S_3$	768	2	$2B0, 4A1^2$
11	2^{6+10}	$2^4 : S_5$	1920	S_3	$4A1^3$
12	2^{1+4+10}	$2^4 : \text{PSL}_3(2)$	2688	2	$2B0, 4C1^2$
13	2^{2+9}	$\text{PSL}_3(4) : 2$	40320	2	$4A1, 6A1^2$
14	2^{1+5+10}	$2^{2+5} : S_3$	768	2	$2B0, 4B1^2$
15	2^{6+6}	$2^4 : S_6$	11520	2	$4A1, 4B1^2$
16	2^{2+8}	$2^5 : S_5$	3840	S_3	$4B1^3$
17	2^{4+8}	$2^4 : \text{PSL}_3(2)$	2688	2	$4A1, 4C1^2$
18	2^{4+10}	$2^{3+3} : S_3$	384	2	$4A1, 4B1^2$
19	2^{2+9}	$2^4 : S_5$	1920	2	$4A1, 6C1^2$
20	2^{1+0}	$M_{22} : 2$	887040	2	$6A1, 10A1^2$
21	2^{1+7}	$2^4 : S_6$	11520	1	$4B1, 6A1, 6C1$
22	2^{3+8}	$2^{2+4} : S_3$	384	2	$4B1^2, 4C1$
23	2^{3+6}	$2^{3+3} : S_3$	384	S_3	$4B1^3$
24	2^{2+7}	$2^{2+5} : S_3$	768	2	$4B1, 4C1^2$
25	2^{2+4}	$2^4 : S_5$	1920	2	$4B1, 6C1^2$
26	2^{1+6}	$2^{2+4} : S_3$	384	2	$4B1, 6C1^2$
27	2^{1+5}	S_6	720	2	$4B1, 10A1^2$
28	2^{1+3}	$2^4 : \text{PSL}_3(2)$	2688	2	$4C1, 10A1^2$
29	2^{1+4}	$2^{2+5} : S_3$	768	2	$4C1, 6C1^2$
30	2^{1+0}	$2^4 : S_5$	1920	S_3	$6C1^3$
31	2^{1+0}	$2^5 : S_5$	3840	2	$6C1, 10A1^2$
32	2^{1+2}	S_6	720	2	$6C1^2, 10A1$

Appendix D A certificate for computing the order of the Monster

A key step in computing the order of the Monster is the enumeration of the G_{x0} -orbits on the axes and their sizes, as listed in Table 1. These data can be readily computed

using a suitable linear algebra program, provided that Table 2 has been established as correct. However, generating the entries in Table 2 involves sophisticated computations within the Monster group, which are carried out using the mmgroup package.

Once these data (along with certain auxiliary information) are available, their correctness can be verified through significantly simpler computations. For this reason, it is practical to store all the information required to generate Table 2 in a separate human-readable file, enabling a simple and efficient verification of its correctness. We refer to such a file as a *certificate*.

Similarly, we need the enumeration of the $(H \cap N_{xyz})$ -orbits on the feasible 2A axes and their sizes, as listed in Table 3. These data can be readily computed from Table 4. We therefore also compute a certificate for verifying the correctness of that table.

Our accompanying program code computes these certificates and stores them in the subdirectory `axis_orbits/certificates`. That subdirectory also contains Python scripts for verifying the certificates. Therefore, it suffices to check the programs and data in this subdirectory in order to verify the correctness of Tables 2 and 4. For further details we refer the reader to the program code. In the remainder of this section we focus on the verification of the certificate for Table 2. The verification of the other certificate is similar.

For verifying a certificate, we need only a tiny fraction of the functionality of the mmgroup package. For each G_{x0} -orbit on the axes we store the following information in a certificate:

- The name of the orbit.
- An element of \mathbb{M} mapping the standard axis v^+ to a representative v_i of the orbit.
- A generating system for the stabilizer of axis v_i in G_{x0} .
- A list of elements of G_{x0} mapping v_i to a set of representatives of N_{x0} -orbits contained in this orbit.

Note that mmgroup allows storing elements of \mathbb{M} in a compact form. To compute the N_{x0} -orbits (and their relative sizes) contained in the G_{x0} -orbit of an axis v_i , we analyze the action of the stabilizer of v_i in G_{x0} on the type-4 vectors in $\Lambda/2\Lambda$, as described in Section 3.2. For each case, we verify that the resulting list of N_{x0} -orbits agrees with the corresponding list of precomputed N_{x0} -orbit representatives in the certificate. For any such N_{x0} -orbit representative v_j we store the following information in the certificate:

- Orbit size (relative to $|X^+| : |G_{x0} : N_{x0}|$).
- Elements of G_{x0} mapping the axes $v_j \cdot \tau^e$ to the representatives of their G_{x0} -orbits, for $e = \pm 1$.

Given such a certificate, we may compute Table 4 as described in Sections 3.1–3.2, but with the following simplifications:

- If a representative of a G_{x0} - or N_{x0} -orbit is required, we may compute it from the data in the certificate.
- If an axis must be transformed to the representative of its G_{x0} -orbit, we may read the transformation from the certificate.

For this computation, it is sufficient to be able to perform the following operations related to the Monster with mmgroup:

- Transforming an axis in \mathcal{B} by an element of \mathbb{M} .
- Mapping an element of G_{x0} to the automorphism group Co_1 of $\Lambda/2\Lambda$.
- Computing in the natural representation of Co_1 on $\Lambda/2\Lambda$.

In particular, we do not need any word-shortening algorithm for the Monster. During such a computation we also check the internal consistency of the certificate. The size of the certificate is about 60 kBytes; its verification takes about 20 seconds on the authors' PCs.

Appendix E Classes of involutions in the Monster

It is well known that the Monster has two classes of involutions called 2A and 2B in [CCN⁺85]. In this appendix we will prove this fact using the character table of the group Co_1 and computations in `mmgroup` only.

From Theorem 5.1 it follows that G_{x0} has odd index in \mathbb{M} . Thus it suffices to show that all involutions in G_{x0} fuse either to class 2A or to class 2B in the Monster.

The Python script `involutions_G_x0.py` in the accompanying program code performs a brute-force calculation with `mmgroup` to establish this fact. It turns out that G_{x0} has seven classes of involutions, two classes fusing to class 2A in \mathbb{M} , and five classes fusing to class 2B in \mathbb{M} .

Alternatively, this last fact can be established using the character information about \mathbb{M} and G_{x0} stored in the GAP computer algebra package [GAP24] with the following GAP program:

```
LoadPackage("ctbllib");;
chM := CharacterTable("M");;
chGx0 := CharacterTable("2^1+24.Co1");;
fusion := FusionConjugacyClasses(chGx0, chM);;
involutions := Positions(OrdersClassRepresentatives(chGx0), 2);;
List(involutions, t->[ClassNames(chGx0)[t], ClassNames(chM)[fusion[t]]]);
```

References

- [ACMS92] D. Alexander, C. Cummins, J. McKay, and C. Simons. Completely replicable functions. In *Groups, combinatorics & geometry (Durham, 1990)*, volume 165 of *London Math. Soc. Lecture Note Ser.*, pages 87–98. Cambridge Univ. Press, Cambridge, 1992.
- [AD04] Toshiyuki Abe and Chongying Dong. Classification of irreducible modules for the vertex operator algebra V_L^+ : general case. *J. Algebra*, 273(2):657–685, 2004.
- [ADL05] Toshiyuki Abe, Chongying Dong, and Haisheng Li. Fusion rules for the vertex operator algebra $M(1)$ and V_L^+ . *Comm. Math. Phys.*, 253(1):171–219, 2005.

- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.
- [Bor86] R. E. Borcherds. Vertex algebras, Kac-Moody algebras, and the Monster. *Proc. Natl. Acad. Sci. USA*, 83:3068–3071, 1986.
- [Bor92] R. E. Borcherds. Monstrous moonshine and monstrous Lie superalgebras. *Invent. math.*, 109:405–444, 1992.
- [BW05] R. W. Barraclough and R. A. Wilson. Conjugacy class representatives in the Monster Group. *LMS Journal of Computation and Mathematics*, 8:205–216, 2005.
- [Car23] Scott Carnahan. Why do the symmetries of the monster vertex algebra form a finite simple group? *preprint. arXiv:2206.15391v2*, 2023.
- [CCN⁺85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of Finite Groups*. Clarendon Press, Oxford, 1985.
- [CKU18] Scott Carnahan, Takahiro Komuro, and Satoru Urano. Characterizing moonshine functions by vertex-operator-algebraic conditions. *SIGMA Symmetry Integrability Geom. Methods Appl.*, 14:Paper No. 114, 8, 2018.
- [Con69] J. H. Conway. A group of order 8, 315, 553, 613, 086, 720, 000. *Bull. London Math. Soc.*, 1:79–88, 1969.
- [Con85] J. H. Conway. A simple construction of the Fischer-Griess monster group. *Inventiones Mathematicae*, 79, 1985.
- [CS99] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*. Springer-Verlag, New York, 3rd edition, 1999.
- [DGH98] Chonying Dong, Robert Griess, and Gerald Höhn. Framed Vertex Operator Algebras, Codes and the Moonshine Module. *Comm. Math. Phys.*, 193:407–448, 1998. q-alg/9707008.
- [DGL07] Chongying Dong, Robert L. Griess, Jr., and Ching Hung Lam. Uniqueness results for the moonshine vertex operator algebra. *Amer. J. Math.*, 129(2):583–609, 2007.
- [EMS20] Jethro van Ekeren, Sven Möller, and Nils R. Scheithauer. Construction and classification of holomorphic vertex operator algebras. *J. Reine Angew. Math.*, 759:61–99, 2020.
- [FLM88] Igor Frenkel, James Lepowsky, and Arne Meurman. *Vertex Operator Algebras and the Monster*. Academic Press, San Diego, 1988.
- [GAP24] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.14.0*, 2024.

- [GMS89] Robert L. Griess, Ulrich Meierfrankenfeld, and Yoav Segev. A uniqueness proof for the monster. *Annals of Mathematics*, 130(3):567–602, 1989.
- [Gri82] R. L. Griess. The friendly giant. *Invent. Math.*, 69:1–102, 1982.
- [HEO05] Derek F. Holt, Bettina Eick, and Eamonn A. O’Brien. *Handbook of Computational Group Theory*. Chapman and Hall/CRC, Boca Raton, FL, 2005.
- [HM23] Gerald Höhn and Sven Möller. Classification of self-dual vertex operator super algebras of central charge at most 24. *preprint. arXiv:2303.17190*, 2023.
- [Höh95] Gerald Höhn. *Selbstduale Vertexoperatorsuperalgebren und das Babymonster*. PhD thesis, Universität Bonn, 1995. see: Bonner Mathematische Schriften **286**, arXiv:0706.0236.
- [Höh24] Gerald Höhn. Subgroups of the monster in mmgroup. <http://www.monstrous-moonshine.de/~gerald/monster/>, 2024. Accessed on August 1, 2025.
- [HS24] Gerald Höhn and Martin Seysen. Code accompanying this paper. https://github.com/Martin-Seysen/order_monster/, 2024. Accessed on August 1, 2025.
- [Iva09] A. A. Ivanov. *The Monster Group and Majorana Involutions*. Cambridge University Press, April 2009.
- [LS07] Ching Hung Lam and Hiroki Shimakura. Ising vectors in the vertex operator algebra V_{Λ}^+ associated with the Leech lattice Λ . *Int. Math. Res. Not. IMRN*, (24):Art. ID rnm132, 21, 2007.
- [MN93] Werner Meyer and Wolfram Neutsch. Associative Subalgebras of the Griess Algebra. *Journal of Algebra*, 158:1–17, 1993.
- [Mül08] J. Müller. On the action of the sporadic simple baby monster group on its conjugacy class 2B. *LMS Journal of Computation and Mathematics*, 11:15–27, 2008.
- [Nor98] S. P. Norton. Anatomy of the monster I. In *The Atlas of Finite Groups: Ten Years On*, pages 198–214. Cambridge University Press, 1998.
- [Sey20a] M. Seysen. A computer-friendly construction of the monster. *arXiv e-prints*, page arXiv:2002.10921, February 2020.
- [Sey20b] M. Seysen. mmgroup, a python implementation of the monster group. <https://github.com/Martin-Seysen/mmgroup>, 2020. Release mmgroup v1.0.0, accessed on August 1, 2025.
- [Sey21] M. Seysen. Welcome to mmgroup’s documentation. <https://mmgroup.readthedocs.io/en/stable>, 2021. Accessed on August 1, 2025.

- [Sey24] Martin Seysen. A fast implementation of the monster group: The monster has been tamed. *Journal of Computational Algebra*, 9:100012, 2024.
- [Shi04] Hiroki Shimakura. The automorphism group of the vertex operator algebra V_L^+ for an even lattice L without roots. *J. Algebra*, 280(1):29–57, 2004.
- [Smi79] Stephen D. Smith. Large Extraspecial Subgroups of Widths 4 and 6. *Journal of Algebra*, 58:251–281, 1979.
- [Tit83] J. Tits. Résumé de Cours. *Annuaire du Collège de France*, pages 89–102, 1982–1983.
- [Tit84] J. Tits. On R. Griess’ “Friendly giant”. *Invent. Math.*, 78:491–499, 1984.