A computer-friendly construction of the monster

by Martin Seysen

May 14, 2020

Preliminary version

Abstract

Let $\mathbb{M}$ be the monster group which is the largest sporadic finite simple group, and has first been constructed in 1982 by Griess. In 1985, Conway has constructed a 196884-dimensional representation ρ of $\mathbb{M}$ with matrix coefficients in $\mathbb{Z}[\frac{1}{2}]$. So these matrices may be reduced modulo any (not necessarily prime) odd number p, leading to representations of $\mathbb{M}$ in odd characteristic. The representation ρ is based on representations of two maximal subgroups G_{x0} and N_0 of $\mathbb{M}$. In ATLAS notation, G_{x0} has structure $2^{1+24}_+.\text{Co}_1$ and N_0 has structure $2^{2+11+22}.(M_{24} \times S_3)$. Conway has constructed an explicit set of generators of N_0, but not of G_{x0}.

This paper is essentially a rewrite of Conway's construction augmented by an explicit construction of an element of $G_{x0} \setminus N_0$. This gives us a complete set of generators of $\mathbb{M}$. It turns out that the matrices of all generators of $\mathbb{M}$ consist of monomial blocks, and of blocks which are essentially Hadamard matrices scaled by a negative power of two. Multiplication with such a generator can be programmed very efficiently if the modulus p is of shape $2^k - 1$.

So this paper may be considered a as programmer's reference for Conway's construction of the monster group $\mathbb{M}$. We have implemented representations of $\mathbb{M}$ modulo 3, 7, 15, 31, 127, and 255.

1 Introduction

Let $\mathbb{M}$ be the monster group, which is the largest sporadic finite simple group, and has first been constructed by Griess [9]. That construction has been greatly simplified by Conway [5], leading to a rational representation ρ of $\mathbb{M}$ of dimension 196883+1. This paper is essentially a rewrite of Conway's construction of $\mathbb{M}$, augmented by an explicit construction of the representations of a complete set of generators of $\mathbb{M}$. Here all generators of $\mathbb{M}$ have coefficients in $\mathbb{Z}[\frac{1}{2}]$ as in [5], and they can be computed very efficiently. So a programmer may use this paper as a reference for implementing the representation ρ of $\mathbb{M}$ modulo a small odd number p.

The success of the construction in [5] is due to the fact that the representation $\rho(N_{x0})$ of a large subgroup N_{x0} of $\mathbb{M}$ of structure $2^{1+24+11}.M_{24}$ can be made explicit and monomial. We use the notation in the ATLAS [6] for describing the structure of a group, so M_{24} is the Mathieu group acting as a permutation group on 24 elements. There is a maximal subgroup

N_0 of $\mathbb{M}$ with $N_0 : N_{x0} = 3$. For a so-called triality element $\tau \in N_0 \setminus N_{x0}$ the (non-monomial) representation $\rho(\tau)$ is given explicitly in [5], so that we can effectively compute in $\rho(N_0)$.

There is another maximal subgroup G_{x0} of $\mathbb{M}$ of structure $2^{1+24}.\mathrm{Co}_1$. Here 2^{1+24} is an extraspecial 2-group, and the simple group Co_1 is the automorphism group of the 24-dimensional Leech lattice Λ modulo 2, see e.g. [7].

The group N_{x0} is a maximal subgroup of G_{x0}. So an explicit description of $\rho(\xi)$ for any $\xi \in G_{x0} \setminus N_{x0}$ gives us the capability to compute in $\rho(\mathbb{M})$. Holmes and Wilson [13] have used similar ideas to construct the representation of the Monster in characteristic 3. Their construction uses non-monomial matrices with blocks of size up to 276×276. In [5] no explicit construction of $\rho(\xi)$ is given for any $\xi \in \mathbb{M} \setminus N_0$.

The essential new result in this paper is a computer-free explicit construction of $\rho(\xi)$ for such a generator ξ in section 9.4 ff.

The construction [5] of $\mathbb{M}$ uses the Parker loop, which is a non-associative loop of order 2^{1+12}. For computations in the Parker loop a cocycle can be used, see e.g. Aschbacher [2], Chapter 4. Such a cocycle is not unique. While the choice of that cocycle is not too important for computing in the subgroup N_0 of $\mathbb{M}$, we have to select a specific cocycle for the Parker loop in such a way that the (non-monomial) representation of a certain element ξ of $G_{x0} \setminus N_{x0}$ obtains a reasonably simple structure.

In our construction we take the notation from [5], except for two explicitly stated sign changes required for the construction of a generator $\xi \in G_{x0} \setminus N_{x0}$. One of these changes is explained in section 5 and motivated by Ivanov's construction of $\mathbb{M}$ in [14]. This leads to simpler relations in the group N_0.

The other sign change is explained in section 7.2). Therefore we remark that another group $N(4096_x)$ of structure $2^{1+24}.\mathrm{Co}_1$, but not isomorphic to G_{x0}, plays an important role in Conway's construction. $N(4096_x)$ is a subgroup of the Clifford group $\mathcal{C}_{12}$ of structure $2^{1+24}_+.\mathrm{O}^+_{24}(2)$. Nebe, Rains, and Sloane [15] have constructed the group $\mathcal{C}_{12}$ as the automorphism group of $M_1^{\otimes 12}$, where M_1 is a certain 2-dimensional $\mathbb{Z}[\sqrt{2}]$-lattice. This construction leads to a 4096-dimensional real representation of $\mathcal{C}_{12}$ and also of its subgroup $N(4096_x)$, which is called 4096_x in [5]. Selecting two orthogonal short rational vectors in M_1 as a basis of the vector space $M_1 \otimes \mathbb{R}$, we also obtain a basis of the real vector space $4096_x = (M_1 \otimes \mathbb{R})^{\otimes 12}$ in the usual way. We change some signs of the basis vectors of 4096_x used in [5], so that they are compatible with the signs of the basis vectors of 4096_x, when constructed as a tensor product. We will not show this compatibility, since we do not need it explicitly in this paper. We claim that this compatibility greatly simplifies the construction of a $\xi \in G_{x0} \setminus N_{x0}$.

It is worth noting that the complex analogue $\mathcal{X}_n$ of the real Clifford group $\mathcal{C}_n$, also defined in [15], plays an important role in the theory of quantum computing. A general quantum circuit with n qubits is modelled using a dense subgroup of the complex unitary group $U(2^n, \mathbb{C})$ and cannot be simulated in polynomial time on a classical computer. There is an important class of quantum circuits with n qubits called *stabilizer circuits*, which can be modelled using the discrete subgroup $\mathcal{X}_n$ of $U(2^n, \mathbb{C})$. Here all quantum gates can be modelled by tensor products of certain well-behaved monomial and of Hadamard matrices. The Gottesman-Knill theorem states that stabilizer circuits can be simulated in polynomial time, see e.g. [1] for background. This 'explains' in a way, why choosing the signs of the basis vectors of 4096_x to be compatible with [15] and with the simulation in [1] may simplify computations in the subgroup $2^{1+24}.\mathrm{Co}_1$ of $\mathcal{X}_{12}$.

The hard part of Conway's construction [5] was to find an algebra invariant under $\rho(\mathbb{M})$, similar to the Griess algebra defined in [9]. Therefore Conway defined an algebra visibly invariant under $\rho(G_0)$ and showed that this algebra is also invariant under $\rho(N_0)$, using a basis of ρ where N_0 has a simple representation. In this paper we need an explicit representation $\rho(\xi)$ of a $\xi \in G_0 \setminus N_{x0}$. So we adjust the signs of that basis in order to simplify $\rho(G_0)$.

Define a Hadamard step on $\rho(\mathbb{M})$ to be a multiplication with a matrix that contains just monomial blocks and blocks of 2×2-Hadamard matrices, i.e. matrices of shape $c\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ for

$c \in \{\frac{1}{2}, 1\}$. We will see that the representations of all our generators of $\mathbb{M}$ can be decomposed into at most 6 Hadamard steps plus some monomial operations.

For any odd natural number p let ρ_p be the representation ρ of the monster, where all coefficients are taken modulo p. Computations in ρ_p are very efficient if $p+1$ is a reasonably small power 2^k of two. In this case we may represent an integer modulo p with k bits, putting $(1, ..., 1)_2 = (0, ..., 0)_2 = 0$. Then negation can be done by complementing all bits, halving can be done by right rotation, and the carry bit of an addition has the same valence as the least significant bit. Using integer additions, and bitwise and shift operations on a 32-bit or 64-bit computer, several components of a vector in ρ_p can be negated, halved, or added modulo a small number $p = 2^k - 1$ simultaneously in a single register.

We have implemented the representations ρ_p of the monster for $p = 3, 7, 15, 31, 127$, and 255, see [16]. Calculating in the monster modulo different numbers is useful e.g. for distinguishing between classes in $\mathbb{M}$ of the same order, see [4].

Let $g \in \mathbb{M}$ be the product of an arbitrary element of G_{x0} with a power of ξ. On the author's 64-bit Windows computer, the operation of $\rho_p(g)$ on a single vector costs 0.73 ms for $p = 3$ and 1.35 ms for $p = 255$. That computer has an Intel Core i7-8750H CPU running at up to 4.0 GHz. These benchmarks are single-threaded.

2 The Golay code $\mathcal{C}$ and its cocode $\mathcal{C}^*$

2.1 Description of the Golay code $\mathcal{C}$ and its cocode $\mathcal{C}^*$

Let $\tilde{\Omega}$ be a set of size 24 and construct the vector space $\mathbb{F}_2^{24}$ as $\prod_{i \in \tilde{\Omega}} \mathbb{F}_2$. A *Golay code* $\mathcal{C}$ is a 12-dimensional linear subspace of $\mathbb{F}_2^{24}$ whose smallest weight is 8. This characterizes the Golay code up to permutation. A Golay code has weight distribution $0^1 8^{759} 12^{2576} 16^{759} 24^1$. We identify the power set of $\tilde{\Omega}$ with $\mathbb{F}_2^{24}$ by mapping each subset of $\tilde{\Omega}$ to its characteristic function, which is a vector in $\mathbb{F}_2^{24}$. So we may write $\tilde{\Omega}$ for the Golay code word containing 24 ones, and for elements d, e of $\mathbb{F}_2^{24}$ we write $d \cup e$, $d \cap e$ for their union and intersection and $d + e$ for their symmetric difference. Golay code words of length 8 and 12 are called *octads* and *dodecads*, respectively.

The Golay cocode $\mathcal{C}^*$ corresponding to a Golay code $\mathcal{C}$ is the 12-dimensional quotient space $\mathbb{F}_2^{24}/\mathcal{C}$. For each $\delta \in \mathcal{C}^*$ define the weight of δ to be the weight of its lightest representative in $\mathbb{F}_2^{24}$. Then $\mathcal{C}^*$ has weight distribution $0^1 1^{24} 2^{276} 3^{2024} 4^{1771}$. Here the lightest representative is unique if its weight is less than 4. If δ has weight 4, there is a set of six mutually disjoint lightest representatives of δ, and any such subset of $\mathbb{F}_2^{24}$ is called a *tetrad*. The parity of a cocode element δ is defined as the parity of its weight $|\delta|$.

There is a natural scalar product $\langle , \rangle$ on $\mathcal{C} \times \mathcal{C}^*$ given by $\langle d, \delta \mathcal{C} \rangle = |d \cap \delta| \bmod 2$ for any $d \in \mathcal{C}$, $\delta \in \mathbb{F}_2^{24}$. As usual, a subspace X^* of $\mathcal{C}^*$ is *orthogonal* to a subspace X of $\mathcal{C}$ if $\langle d, \delta \rangle = 0$ for all $d \in X$, $\delta \in X^*$.

The automorphism group of a Golay code $\mathcal{C}$ is the Mathieu group M_{24}. M_{24} also preserves $\mathcal{C}^*$, see [7]. For our construction of the Monster we need a specific instance $\mathcal{C}$ of a Golay code. Therefore we assume that the reader is familiar with [7], Chapter 11, section 1–7 and 9.

There is a 3-dimensional linear code of length 6 over $\mathbb{F}_4$ with weight distribution $0^1 4^{45} 6^{18}$ called the *hexacode*. A detailed description of one instance $\mathcal{H}_6$ of the hexacode is given in [7], Chapter 11. To be concrete, let $\mathbb{F}_4 = \{0, 1, \alpha, \bar{\alpha}\}$ with $\alpha^2 = \bar{\alpha} = 1 + \alpha$, and let $\mathcal{H}_6$ be the subspace of $\mathbb{F}_4^6$ spanned by $(1001\bar{\alpha}\alpha, 0101\alpha\bar{\alpha}, 001111)$ as in [7].

We number the elements of $\tilde{\Omega}$ from 0 to 23. and arrange them in a table with 4 rows and 6 columns. We also assign an element of $\mathbb{F}_4$ and a colour to each row as follows:

white	0	0	4	8	12	16	20
red	1	1	5	9	13	17	21
green	α	2	6	10	14	16	22
blue	$\bar{\alpha}$	3	7	11	15	19	23

(2.1.1)

This table is called MOG (Miracle Octad Generator) in [7]. We start row and column numbers with 0, so element $m + 4 \cdot n$ of $\tilde{\Omega}$ corresponds to row m, column n. This is bad for Fortran and good for C programmers.

Each element x of $\mathbb{F}_2^{24}$ has a *hexacode value* $\mathfrak{h}(x) \in \mathbb{F}_4^6$ which is calculated as follows. We write the entries of x into the MOG. Then for each column of the MOG we compute a weighted sum of its nonzero entries, where each entry of the MOG has weight corresponding to the element of $\mathbb{F}_4$ associated with its row. The result $\mathfrak{h}(x)$ is a vector in $\mathbb{F}_4^6$.

Also, for each row or column in the MOG the parity of x in that row or column is the number of the nonzero entries in that row or column taken modulo 2.

Definition 2.2. *Let $\mathcal{C}$ be the linear subspace of $\mathbb{F}_2^{24}$ characterized by the following properties:*
x is in $\mathcal{C}$ if and only if $\mathfrak{h}(x) \in \mathcal{H}_6$ and for all columns of the MOG the parity of x in that column is equal to the parity of x in row 0.

In [7], Chapter 11 it is shown that $\mathcal{C}$ is indeed a Golay code. We call an element of $\mathcal{C}$ *odd* or *even*, depending on its parity in row 0.

2.2 The 'grey' and the 'coloured' subspaces of $\mathcal{C}$ and of $\mathcal{C}^*$

This subsection contains material which is not covered by [2], [5], [7] or [14], and which we need in section 9 for the first time. So it may be skipped at first reading.

The construction of the Golay code in [7], Chapter 11.5 motivates the construction of the Golay code as a direct sum $\mathcal{C} = \mathcal{G} \oplus \mathcal{H}$. For reasons to be explained below, the elements of $\mathcal{G}$ and $\mathcal{H}$ will be called *grey* and *coloured*, respectively. We also give a similar decomposition $\mathcal{C}^* = \mathcal{G}^* \oplus \mathcal{H}^*$ of the Golay cocode $\mathcal{C}^*$ into a direct sum of a grey and a coloured subspace.

In section 6 we will embed both, the Golay code $\mathcal{C}$ and its cocode $\mathcal{C}^*$, into the 24–dimensional Leech lattice Λ modulo 2. Loosely speaking, we will construct an automorphism ξ of $\Lambda/2\Lambda$ that fixes $\mathcal{H}$ and $\mathcal{H}^*$, and exchanges $\mathcal{G}$ with $\mathcal{G}^*$. By construction, ξ is in the automorphism group Co_1 of $\Lambda/2\Lambda$, but not in the automorphism group M_{24} of $\mathcal{C}$. Thus ξ can be lifted to an element of the monster group in $2^{1+24}.\mathrm{Co}_1 \setminus 2^{1+24+11}.M_{24}$ as required. We remark that our construction of ξ can also be achieved by embedding two orthogonal copies of the 12-dimensional Coxeter-Todd lattice K_{12} into the Leech lattice, as outlined in [7], Ch. 4.9. Here one copy of K_{12} corresponds to $\mathcal{G} \oplus \mathcal{G}^*$, and the other copy to $\mathcal{H} \oplus \mathcal{H}^*$.

We call an element d of $\mathcal{C}$ *grey* if in each column of the MOG all entries of d in that column in rows 1–3 are equal. Different columns may have different entries in rows 1–3. Imagine that each nonzero entry in the MOG switches on a light with a colour as given for its row in the MOG, and that the lights in each column are mixed to a common single colour. Then d is grey if none of these 6 mixed lights switched on by d shows any colour apart from white or black.

The even grey elements of $\mathcal{C}$ are precisely those with equal entries in each column, so that the number of nonzero columns is even. So there are 32 of them and they form a 5-dimensional subspace $\mathcal{G}^0$ of $\mathcal{C}$. There is also an odd grey element of $\mathcal{C}$, e.g.:

$$
g_0 = \begin{array}{|c|c|c|c|c|c|}
\hline
0 & 1 & 1 & 1 & 1 & 1 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 \\
\hline
\end{array}.
\tag{2.2.1}
$$

Thus the grey elements form a 6-dimensional subspace $\mathcal{G}$ of $\mathcal{C}$.

We define a monomorphism $\mathfrak{h}^* : \mathbb{F}_4^6 \to \mathbb{F}_2^{24}$ with $\mathfrak{h}(\mathfrak{h}^*(h)) = h$ for $h \in \mathbb{F}_4^6$ ($\mathbb{F}_4^6$ being considered as a vector space over $\mathbb{F}_2$) as follows. For $h \in \mathbb{F}_4^6$ let $\mathfrak{h}^*(h)$ be the unique element x of $\mathbb{F}_2^{24}$ that has zeros in row 0 of the MOG and exactly 0 or 2 nonzero elements in each column of the MOG such that the hexacode value $\mathfrak{h}(x)$ is equal to h. We put $\mathcal{H} = \{\mathfrak{h}^*(x) \mid x \in \mathcal{H}_6\}$. Then we have $\mathcal{C} = \mathcal{G} \oplus \mathcal{H}$. The elements of $\mathcal{H}$ are called *coloured*. So the coloured Golay

4

code words are those without any white light and with an even number of coloured lights in each column of the MOG.

Let $\mathcal{G}^*$ be the orthogonal complement of $\mathcal{H}$ and let $\mathcal{H}^*$ be the orthogonal complement of $\mathcal{G}$ in $\mathcal{C}^*$. Elements of $\mathcal{G}^*$ and $\mathcal{H}^*$ are also called grey and coloured, respectively. The monomorphism $\mathfrak{h}^*$ yields a natural isomorphism $\mathbb{F}_4^6/\mathcal{H}_6 \to \mathcal{H}^*$. Since more than half of the codewords in $\mathcal{H}_6$ have weight 4, the following lemma is obvious:

Lemma 2.3. $\mathcal{H}$ *is generated by* $\mathfrak{h}^*(h)$, *where h runs over the code words in $\mathcal{H}_6$ of weight 4.* $\mathcal{H}^*$ *is generated by* $\mathfrak{h}^*(h)$, *where h runs over the basis vectors of $\mathbb{F}_4^6$ and their scalar multiples.*

Let ω_∞ be the element of $\mathbb{F}_2^{24}$ with entries 1 in MOG row 0 and zeros in the other rows. Let ω_i, $i = 0, \ldots, 5$ be the element of $\mathbb{F}_2^{24}$ with entries 1 in MOG column i and zeros in the other columns. Put $g_i = \omega_i + \omega_\infty$. Then g_0 is as in (2.2.1) and g_i is obtained form g_0 by exchanging column 0 with column i in the MOG. $g_0, \ldots, g_5$ is a basis of $\mathcal{G}$. So $\omega_0, \ldots, \omega_5$ and ω_∞ represent the same element of the cocode C^*, which we will demote by ω. ω has minimum weight 4 in C^* and the tetrad corresponding to ω is $\{\omega_0, \ldots, \omega_5\}$. Then $d \in \mathcal{C}$ is even if and only if $\langle d, \omega \rangle = 0$.

Let $\gamma_n \in \mathcal{C}^*$ correspond the vector with an entry 1 in MOG row 0, column n, and entries 0 elsewhere. Then $(\gamma_0, \ldots, \gamma_5)$ is a basis of $\mathcal{G}^*$.

Definition 2.4. *For $d \in \mathcal{G}$ and $\delta \in \mathcal{G}^*$ let $w(d)$ and $w(\delta)$ be the weight of d and δ with respect to the basis $(g_0, \ldots, g_5)$ and $(\gamma_0, \ldots, \gamma_5)$, respectively.*

Then $\tilde{\Omega} = \sum_{n=0}^5 g_n$, $\omega = \sum_{n=0}^5 \gamma_n$ and we have $w(\tilde{\Omega}) = w(\omega) = 6$. For $d \in \mathcal{G}$, $\delta \in \mathcal{G}^*$, the weights $w(d)$ and $w(\delta)$ determine the weight $|d|$ and the minimum weight $|\delta|$ as follows:

$w(d), w(\delta)$	0	1	2	3	4	5	6
$|d|$	0	8	8	12	16	16	24
$\min |\delta|$	0	1	2	3	4	3	4

(2.5.1)

By definition of $g_0, \ldots, g_5$ and $\gamma_0, \ldots, \gamma_5$ we have:

$$\langle g_m, \gamma_n \rangle = 0 \quad \text{if} \quad m = n \quad \text{and} \quad \langle g_m, \gamma_n \rangle = 1 \quad \text{otherwise} .\tag{2.5.2}$$

Thus the reciprocal basis of $(g_0, \ldots, g_5)$ is $(\gamma_0 + \omega, \ldots \gamma_5 + \omega)$ and the reciprocal basis of $(g_0 + \tilde{\Omega}, \ldots, g_5 + \tilde{\Omega})$ is $(\gamma_0, \ldots \gamma_5)$.

The following fact is rather obvious:

$$\forall\, d \in \mathcal{G} : \quad w(d + \tilde{\Omega}) = 6 - w(d), \quad w(d) = \text{parity}(d) \pmod 2 .\tag{2.5.3}$$

3 The Parker loop $\mathcal{P}$

3.1 The definition of the Parker loop

The Parker loop $\mathcal{P}$ is a non-associative Moufang loop written multiplicatively and operating on the set $\mathcal{P} = \mathcal{C} \times \mathbb{F}_2$, see [2, 5, 14]. For any element d of $\mathcal{P}$ we write $\bar{d}$ for the loop inverse of d in $\mathcal{P}$ and we write $\tilde{d}$ for the projection of d into $\mathcal{C}$ obtained by dropping the second component of d. This projection is a homomorphism from $\mathcal{P}$ to the additive group $(\mathcal{C}, +)$. We also write 1, -1, Ω and $-\Omega$ for the elements $(0, 0)$, $(0, 1)$, $(\tilde{\Omega}, 0)$ and $(\tilde{\Omega}, 1)$ of $\mathcal{P}$. Let $d, e, f \in \mathcal{P}$. Then the following property characterizes the Parker loop up to isomorphism:

$$d^2 = (-1)^{P(\tilde{d})} \quad \text{with} \quad P(\tilde{d}) = \tfrac{1}{4}|\tilde{d}| ,$$
$$(de)(ed)^{-1} = (-1)^{C(\tilde{d}, \tilde{e})} \quad \text{with} \quad C(\tilde{d}, \tilde{e}) = \tfrac{1}{2}|\tilde{d} \cap \tilde{e}| ,\tag{3.1.1}$$
$$(d(ef))((de)f)^{-1} = (-1)^{A(\tilde{d}, \tilde{e}, \tilde{f})} \quad \text{with} \quad A(\tilde{d}, \tilde{e}, \tilde{f}) = |\tilde{d} \cap \tilde{e} \cap \tilde{f}| .$$

5

In [2] the mappings $P : \mathcal{C} \to \mathbb{F}_2$, $C : \mathcal{C}^2 \to \mathbb{F}_2$ and $A : \mathcal{C}^3 \to \mathbb{F}_2$ given by (3.1.1) are called *power map*, *commutator* and *associator*, respectively. Recall that $'+'$ denotes the symmetric difference of two sets. By [2], Lemma 11.1 and Lemma 11.8 or by direct calculation using the identity

$$|\tilde{d} + \tilde{e}| = |\tilde{d}| + |\tilde{e}| - 2|\tilde{d} \cap \tilde{e}| \,,$$

for finite sets $\tilde{d}, \tilde{e}$ we obtain:

Lemma 3.2. *The associator A is a symmetric trilinear form on $\mathcal{C}$, and we have:*

$$P(\tilde{d} + \tilde{e}) = P(\tilde{d}) + P(\tilde{e}) + C(\tilde{d}, \tilde{e}) \,, \tag{3.2.1}$$

$$C(\tilde{d} + \tilde{e}, \tilde{f}) = C(\tilde{d}, \tilde{f}) + C(\tilde{e}, \tilde{f}) + A(\tilde{d}, \tilde{e}, \tilde{f}) \,. \tag{3.2.2}$$

We obviously have $C(\tilde{d}, \tilde{e}) = C(\tilde{e}, \tilde{d})$ and by Lemma 3.2 we have $A(\tilde{d}, \tilde{d}, \tilde{e}) = 0$. This implies that $\mathcal{P}$ is *diassociative*, i.e. any subloop of $\mathcal{P}$ generated by two elements is a group, see [2, 14]. This saves a few brackets in some cases.

From now on we follow the convention in [5], using the same notation for elements of $\mathcal{P}$ and of $\mathcal{C}$. If a function F has domain $\mathcal{C}^n$ then $F(d, e, f, \ldots)$ will mean $F(\tilde{d}, \tilde{e}, \tilde{f}, \ldots)$ for $d, e, f, \ldots \in \mathcal{P}$. E.g. $A(d, e, f)$ means $A(\tilde{d}, \tilde{e}, \tilde{f})$, $\langle d, \delta \rangle$ means $\langle \tilde{d}, \delta \rangle$ for $\delta \in \mathcal{C}^*$. But we still distinguish between $d \in \mathcal{P}$ and $\tilde{d} \in \mathcal{C}$ whenever we consider d as a pair $d = (\tilde{d}, \lambda) \in \mathcal{C} \times \mathbb{F}_2$. We use this convention also for functions defined on subsets of $\tilde{\Omega}$, with the embedding $\mathcal{C} \to \tilde{\Omega}$. So $i \in d$ means $i \in \tilde{d}$, $\frac{1}{2}|d \cap e|$ means $\frac{1}{2}|\tilde{d} \cap \tilde{e}|$, etc. We also use the conventions in [5] for denoting elements of $\mathcal{P}$, $\mathcal{C}$ and $\mathcal{C}^*$:

a, b, c, d, e, f, h denote elements of $\mathcal{P}$ or, loosely, of $\mathcal{C}$,
$\delta, \epsilon, \varphi, \eta$ denote elements of $\mathcal{C}^*$,
i, j, k denote elements of $\tilde{\Omega}$, also considered as elements of $\mathcal{C}^*$ of weight 1,
ij and $d \cap e$ denote the sets $\{i, j\}$ and $\tilde{d} \cap \tilde{e}$, considered as elements of $\mathcal{C}^*$.

We will also write $\bar{d}$ for the inverse d^{-1} of d in $\mathcal{P}$. We have $\bar{d} = (-1)^{|d|/4} d$.
-

3.2   Cocycles for the Parker loop

Let V be an n-dimensional vector space over $\mathbb{F}_2$ and $q : V \to \mathbb{F}_2$ be a function with $q(0) = 0$. Let $\beta_q : V \times V \to \mathbb{F}_2$ be given by $\beta_q(x, y) = q(x + y) + q(x) + q(y)$. If β_q is bilinear then q is called a *quadratic form* on V and β_q is the bilinear form *associated* with q. Two quadratic forms on V have the same associated bilinear form if they differ by a linear function on V. The bilinear form β_q associated with q is *alternating*, i.e. $\beta_q(x, x) = 0$ for all $x \in V$. Any alternating bilinear form on V is also symmetric.

For computations in $\mathcal{P}$ it is convenient to use a cocycle $\theta : \mathcal{C} \times \mathcal{C} \to \mathbb{F}_2$ such that for $\mathcal{P} = \mathcal{C} \times \mathbb{F}_2$ we have:

$$(\tilde{d}_1, \lambda_1) \cdot (\tilde{d}_2, \lambda_2) = (\tilde{d}_2 + \tilde{d}_2, \lambda_1 + \lambda_2 + \theta(d_1, d_2)) \,, \qquad \tilde{d}_1, \tilde{d}_2 \in \mathcal{C}, \ \lambda_1, \lambda_2 \in \mathbb{F}_2 \,. \tag{3.2.3}$$

Cocycles for certain types of loops have been studied in [2, 8, 11]. A cocycle for $\mathcal{P}$ satisfying 3.1.1, which is quadratic in the first and linear in the second argument, has been constructed in [7], Ch. 29, Appendix 2. This can be summarized as follows:

Lemma 3.3. *There is a cocycle $\theta : \mathcal{C} \times \mathcal{C} \to \mathbb{F}_2$ for $\mathcal{P}$ with the following properties:*

$$P(d) = \theta(d, d) \,, \tag{3.3.1}$$

$$C(d, e) = \theta(d, e) + \theta(e, d) \,, \tag{3.3.2}$$

$$\theta(d + e, f) = \theta(d, f) + \theta(e, f) + A(d, e, f) \,, \tag{3.3.3}$$

$$\theta(d, e + f) = \theta(d, e) + \theta(d, f) \,. \tag{3.3.4}$$

6

Sketch Proof

Let $b_0, \ldots, b_{11}$ be a basis of $\mathcal{C}$. Define

$$\theta(b_i, b_j) = \begin{cases} 0 & \text{if } i < j \\ P(b_i) & \text{if } i = j \\ C(b_i, b_j) & \text{if } i > j \end{cases}$$

Then $\theta(b_i, f)$, $f \in \mathcal{C}$ is uniquely determined by $\theta(b_i, e + f) = \theta(b_i, e) + \theta(b_i, f)$. We put

$$\theta(\textstyle\sum_i \mu_i b_i, f) = \left(\textstyle\sum_i \mu_i \theta(b_i, f) \right) + \textstyle\sum_{i<j} \mu_i \mu_j A(b_i, b_j, f) \,.$$

By construction of θ and trilinearity of A, cocycle θ satisfies (3.3.4). Put $d = \sum_i \mu_i b_i$, $e = \sum_i \nu_i b_i$. By construction of θ and trilinearity of A we have

$$\theta(d + e, f) + \theta(d, f) + \theta(e, f) = \textstyle\sum_{i \neq j} \mu_i \nu_j A(b_i, b_j, f) \,,$$

so together with $A(b_i, b_i, f) = 0$, we obtain (3.3.3).

Put $C'(d, e) = \theta(d, e) + \theta(e, d)$. (3.3.3) and (3.3.4) imply $C'(d+e, f) = C'(d, f) + C'(e, f) + A(d, e, f)$. We have $C'(b_i, b_j) = C(b_i, b_j)$. So by (3.2.2) and induction over the basis vectors we obtain $C' = C$, i.e. (3.3.2). A similar argument using $\theta(b_i, b_i) = P(b_i)$, (3.2.1) and induction over the basis vectors establishes (3.3.1).
□

An immediate consequence of Lemma 3.3 is:

Lemma 3.4. *Let θ_1 be a fixed cocycle satisfying Lemma 3.3. Then the cocycles satisfying Lemma 3.3 are precisely the functions $\theta_1 + \beta$, with β an alternating bilinear form on $\mathcal{C}$.*

Since a cocycle given by Lemma 3.3 is linear in its second argument, it may also be interpreted as a function $\mathcal{C} \to \mathcal{C}^*$, and we let $\theta(d_1)$ be the element of $\mathcal{C}^*$ such that $\langle e, \theta(d) \rangle = \theta(d, e)$ holds for all $e \in \mathcal{C}$. Similarly, we let $A(d, e)$ be the element of $\mathcal{C}^*$ such that $\langle f, A(d, e) \rangle = A(d, e, f)$ holds for all $f \in \mathcal{C}$. Then for $d, e \in \mathcal{C}$ (or $d, e \in \mathcal{P}$) we have:

$$\theta(d + e) = \theta(d) + \theta(d) + A(d, e), \quad \text{with } A(d, e) = d \cap e \in \mathcal{C}^* \,. \tag{3.5.1}$$

There are cocycles satisfying (3.2.3) but not Lemma 3.3. But we only consider coycles which satisfy Lemma 3.3.

3.3 Selecting a suitable cocycle for the Parker loop

In this subsection we extend the decomposition of $\mathcal{C}$ into a grey and a coloured subspace to the Parker loop $\mathcal{P}$. Then we construct a cocycle for $\mathcal{P}$ that has some specific properties regarding that decomposition as stated in Lemma 3.9. This is needed in section 9 for the first time and may be skipped at first reading.

We also talk about *grey* and *coloured* elements of $\mathcal{P}$. Let $\mathcal{P}_{\mathcal{G}}$ and $\mathcal{P}_{\mathcal{H}}$ be the set of elements of $\mathcal{P}$ that are mapped to $\mathcal{G}$ and $\mathcal{H}$, respectively, by the homomorphism $\tilde{} : \mathcal{P} \to \mathcal{C}$.

We need a cocycle such that in our representation of $\mathbb{M}$ the non-monomial generator ξ of the monster $\mathbb{M}$ to be constructed in section 9 becomes as simple as possible. More specifically, we will select a cocycle that is related to the decomposition of $\mathcal{C}$ and $\mathcal{C}^*$ into a grey and a coloured subspace as indicated below.

Let $\gamma_{(m,i)}$ be the element of $\mathbb{F}_2^{24}$ with an entry 1 in MOG row m, column i and zero elsewhere. Thus $\gamma_{(m,0)} = \gamma_m$. We define a function $\gamma : \mathbb{F}_2^{24} \to \mathbb{F}_2^{24}$ by:

$$\gamma \left(\sum_{i=0}^{5} \sum_{m=0}^{3} \mu_{m,i} \gamma_{(m,i)} \right) = \sum_{i=0}^{5} \binom{\mu_{1,i} + \mu_{2,i} + \mu_{3,i}}{2} \gamma_i \,, \qquad \text{for} \quad \mu_{m,i} \in \{0, 1\} \,. \tag{3.5.2}$$

So $\gamma(x)$ has entry one in row 0, column n of the MOG, if x has at least two nonzero entries in column n, ignoring the entry in row 0. We usually consider γ as a function $\mathcal{C} \to \mathcal{G}^*$ with $\gamma(d)$ equal to the coset $\mathcal{C}\gamma(d)$. But we occasionally write $\gamma(d) \cap \gamma(e)$, which is meaningful only for $\gamma(d)$ and $\gamma(e)$ considered as elements of $\mathbb{F}_2^{24}$. The restriction of γ to $\mathcal{G}$ is an linear bijection $\mathcal{G} \to \mathcal{G}^*$ with $\gamma(g_m) = \gamma_m$. We have

$$\gamma(g_i) = \gamma(\omega_i) = \gamma_i \ . \tag{3.5.3}$$

Lemma 3.6. $\gamma(d + e) = \gamma(d) + \gamma(e)$ for $d \in \mathcal{C}$, $e \in \mathcal{G}$.

Proof

Let $\phi_j : \mathbb{F}_2^{24} \to \mathbb{F}_2$ be the function that maps $x \in \mathbb{F}_2^{24}$ to the coefficient of the function $\gamma(x)$ corresponding to γ_j. Then $\gamma = \sum_{j=0}^{5} \gamma_j \phi_j$. Since $(g_0, \ldots g_5)$ is a basis of $\mathcal{G}$, it suffices to show

$$\phi_j(d + g_i) = \phi_j(d) + \phi_j(g_i) \ , \qquad \text{for} \quad i, j = 0, \ldots, 5 \ . \tag{3.6.1}$$

ϕ_j depends only on the co-ordinates of $\mathbb{F}_2^{24}$ corresponding to $\gamma_{(m,j)}$ for $m = 1, 2, 3$, Since all these coordinates of g_i are zero in case $i \neq j$, (3.6.1) is established for $i \neq j$.

Assume $i = j$. Then by definition of ϕ_j we have:

$$\phi_j\left(\mu_1\gamma_{(1,j)} + \mu_2\gamma_{(2,j)} + \mu_3\gamma_{(3,j)}\right) = \binom{\mu_1 + \mu_2 + \mu_3}{2} \ , \qquad \text{for} \quad \mu_1, \mu_2, \mu_3 \in \{0, 1\} \ .$$

These three co-ordinates of g_j corresponding to $\gamma_{(1,j)}, \gamma_{(2,j)}, \gamma_{(3,j)}$ are all equal to one. Thus (3.6.1) follows from $\binom{3-k}{2} = \binom{k}{2} + \binom{3}{2} \pmod 2$, for $k \in \{0, 1, 2, 3\}$.
$\square$

Define $w_2 : \mathcal{G} \cup \mathcal{G}^* \to \mathbb{F}_2$ by

$$w_2(d) = \binom{w(d)}{2} \pmod 2 \ , \qquad \text{with } w \text{ as in Definition 2.4.} \tag{3.7.1}$$

Since $w(\Omega + d) = 6 - w_2(d)$ we have

$$w_2(\Omega + d) = w_2(d) + w(d) + 1 \ , \quad \text{for} \quad d \in \mathcal{G} \ . \tag{3.7.2}$$

A quadratic form $q : \mathbb{F}_2^n \to \mathbb{F}_2$ is called non-singular if its associated form β_q is non-singular, i.e. $\det(\beta(v_i, v_j)) = 1$ for a basis $(v_1, \ldots, v_n)$ of $\mathbb{F}_2^n$. A bilinear form which is non-singular and alternating is called *symplectic*.

Lemma 3.8. *Define* $\langle\!\langle ., . \rangle\!\rangle : \mathcal{G} \times \mathcal{G} \to \mathbb{F}_2$ *by* $\langle\!\langle d, e \rangle\!\rangle = \langle e, \gamma(d) \rangle$. *Then* $\langle\!\langle ., . \rangle\!\rangle$ *is symplectic and it is the bilinear form associated with the quadratic form* w_2 *on* $\mathcal{G}$. *We also have:*

$$\langle e, \gamma(d) \rangle = w(\gamma(d)) \cdot w(\gamma(e)) + w(\gamma(d) \cap \gamma(e)) \qquad \text{for} \quad d \in \mathcal{C}, e \in \mathcal{G} \tag{3.8.1}$$

Proof

Both sides of (3.8.1) are linear in $\gamma(d)$ and also in e. So it suffices to show (3.8.1) for $e = g_i$ and $\gamma(d)$ being substituted by γ_i. Thus we have to show $\langle g_i, \gamma_j \rangle = 1 - \delta_{i,j}$, with $\delta_{i,j}$ the Kronecker delta. But this is an immediate consequence of (2.5.2).

Hence $\langle\!\langle g_i, g_j \rangle\!\rangle = 1 - \delta_{i,j}$. For $i = 1, 2$ assume $d_i = \sum_{n=0}^{5} \mu_{i,n} g_n$, $\mu_{i,n} \in \{0, 1\}$. Since $\binom{n}{2} = \sum_{m=0}^{n-1} m$, we have $w_2(d_i) = \sum_{0 \leq m < n \leq 5} \mu_{i,m}\mu_{i,n}$. So w_2 is a quadratic from on $\mathcal{G}$. Let $\beta' : \mathcal{G} \times \mathcal{G} \to \mathbb{F}_2$ be given by $(d_1, d_2) \mapsto w_2(d_1) + w_2(d_2) + w_2(d_1 + d_2)$. Then $\beta'(d_1, d_2) = \sum_{m \neq n} \mu_{1,m}\mu_{2,n}$. Thus β' is linear in both arguments and we have $\beta'(g_m, g_n) = 1 - \delta_{m,n}$. Hence $\langle\!\langle ., . \rangle\!\rangle = \beta'$, i.e. $\langle\!\langle ., . \rangle\!\rangle$ is associated with w_2.

We have just shown that $\det \beta'$ (with respect to the basis $g_1 \ldots, g_5$) has entry $1 - \delta_{m,n}$ in row m, column n, so direct calculation yields $\det \beta' = 1 \pmod 2$.
$\square$

We claim the existence of a specific cocycle for $\mathcal{P}$ as follows:

Lemma 3.9. *There is a cocycle θ for $\mathcal{P}$ satisfying Lemma 3.3 with the following properties:*

$$
\begin{array}{llll}
\theta(d + \tilde{\Omega}) & = & \theta(d) & \text{for} \quad d \in \mathcal{C} \; , \\
\theta(e) & = & (w(e) - 1)\gamma(e) + w_2(e)\omega & \text{for} \quad e \in \mathcal{G}, \quad \omega \text{ as in section 2,} \\
\theta(e, h) & = & 0 & \text{for} \quad e \in \mathcal{G}, \ h \in \mathcal{H} \; , \\
\theta(h, e) & = & \langle e, \gamma(h) \rangle & \text{for} \quad e \in \mathcal{G}, \ h \in \mathcal{H} \; .
\end{array}
$$

Proof

Choose a basis $(b_0, ..., b_{11})$ of $\mathcal{C} = \mathcal{G} \oplus \mathcal{H}$ with $b_m = g_m \in \mathcal{G}$ for $m = 0, \ldots, 5$, $b_6, \ldots, b_{11} \in \mathcal{H}$, and g_m as in section 2. Since two cocycles for $\mathcal{C}$ differ by an alternating bilinear form, a cocycle θ is uniquely determined by decreeing the values $\theta(b_m, b_n)$ for all $0 \le m < n < 12$. So we put $\theta(b_m, b_n) = 0$ for $m < n$. We have $|g_m \cap g_n| = 4$ for $m \ne n$ So for $0 \le m < n < 6$ we have:

$$
\theta(b_m, b_n) + \theta(b_n, b_m) = C(g_m, g_n) = \tfrac{1}{2}|g_m \cap g_n| = 0 \pmod 2 \; ,
$$

by (3.1.1) and Lemma 3.3. For $m < 6$ we have $\theta(b_m, b_m) = P(g_i) = \tfrac{1}{4}|g_m| = 0 \pmod 2$. Thus $\theta(b_m, b_n) = 0$ for all $m < 6, n < 12$. Hence $\theta(b_m) = 0$ for $m < 6$. Thus by (3.5.1) the restriction of θ (as a mapping $\mathcal{C} \to \mathcal{C}^*$) to $\mathcal{G}$ is symmetric under permutations of the basis vectors $b_0, \ldots, b_5$. $\theta(e)$ can be computed for all $e \in \mathcal{G}$ by (3.5.1) Due to the permutation symmetry of θ it suffices to verify the formula for $\theta(e)$ for the cases $\theta(e_m)$ with $e_m = \sum_{n=0}^{m} g_n$, $m = 1, \ldots 5$. This can easily be done by hand calculation. (Row 0 of $\theta(e_m)$ in the MOG is 000000, 001111, 111111, 111100, 000000 for $m = 1, \ldots, 5$; the other rows are zero.)

That way we obtain $\theta(\Omega) = 0$, so we have $\theta(d + \Omega) = \theta(d)$ by (3.5.1). We have $\theta(e, h) = 0$ for $e \in \mathcal{G}, h \in \mathcal{H}$, by construction of θ. Thus $\theta(h, e) = C(e, h) = \tfrac{1}{2}|e \cap h|$. Note that $e \cap h$ has 0 or 2 nonzero entries in each column of the MOG and zeros in row 0. Hence

$$
\theta(h, e) = \frac{1}{2}|e \cap h| = |\gamma(e) \cap \gamma(h)| = w(\gamma(e) \cap \gamma(h)) = \langle e, \gamma(h) \rangle + w(\gamma(e)) \cdot w(\gamma(h)) \; .
$$

by definition of γ and (3.8.1). Since $\gamma(h)$ is even, this proves the formula for $\theta(h, e)$.
$\square$

Corollary 3.10. *For every $h \in \mathcal{H}$ there is a cocycle θ on $\mathcal{C}$ satisfying Lemma 3.9 with $\theta(h) = \gamma(h) \in \mathcal{G}^*$.*

Proof

In the proof of Lemma 3.9 we simply choose a basis $b_0, \ldots, b_{11}$ of $\mathcal{C}$ with $b_6 = h$.
$\square$

(2.5.1) and Lemma 3.9 imply that for every $e \in \mathcal{G}, h \in \mathcal{H}$ we have:

$$
P(e) = w(e) \cdot w_2(e) \, , \ \ P(h) = w_2(\gamma(h)) \, , \ \ C(e, h) = \langle e, \gamma(h) \rangle \; . \tag{3.10.1}
$$

From now on we assume that the cocycle for $\mathcal{P}$ satisfies the conditions in Lemma 3.9.

4 Automorphisms of the Parker loop $\mathcal{P}$

The *center $Z(G)$* of a group or a loop G is the set of elements d of G such that d commutes and associates with all elements of G. Any element of the Parker loop $\mathcal{P}$ squares to ± 1 and we have $Z(\mathcal{P}) = \{\pm 1, \pm \Omega\}$. Thus any automorphism π of $\mathcal{P}$ fixes $\{\pm 1\}$ and maps Ω to $\pm \Omega$. π is called *even* if $\pi(\Omega) = \Omega$ and *odd* if $\pi(\Omega) = -\Omega$. Since π fixes $\{\pm 1\}$, it maps to a unique automorphism $\tilde{\pi}$ of $\mathcal{C} = \mathcal{P}/\{\pm 1\}$. Then $\tilde{\pi}$ preserves power map P, commutator C and associator A, but it need not preserve the Golay code on the vector space $\mathcal{C}$. An automorphism π of $\mathcal{P}$ is called a *standard automorphism* in [5], if $\tilde{\pi}$ preserves the Golay code. E.g. for a nonzero even $\delta \in \mathcal{C}^*$ the mapping $d \mapsto d \cdot \Omega^{\langle d, \delta \rangle}$ is a non-standard automorphism of $\mathcal{P}$, see [14], section 1.6 for background. In the sequel we only deal with the group $\mathrm{Aut}_{\mathrm{St}} \mathcal{P}$

of standard automorphisms π of $\mathcal{P}$. For any $\pi \in \mathrm{Aut}_{\mathrm{St}}\mathcal{P}$ we have $\tilde{\pi} \in M_{24}$. For any $\tilde{\pi} \in M_{24}$ there are precisely 2^{12} standard automorphisms π of $\mathcal{P}$ mapping to $\tilde{\pi}$, see [5, 7].

Fix a cocycle θ for $\mathcal{P}$ that satisfies Lemma 3.3. For any $\pi \in \mathcal{P}$ define $\theta_\pi : \mathcal{C} \times \mathcal{C} \to \mathbb{F}_2$ by

$$\theta_\pi(d, e) = \theta(d^\pi, e^\pi) + \theta(d, e) . \qquad (4.0.1)$$

Then the following lemma is useful for effective computations in the group $\mathrm{Aut}_{\mathrm{St}}\mathcal{P}$:

Lemma 4.1. *For any standard automorphism π of $\mathcal{P}$ the mapping θ_π is a alternating bilinear form on $\mathcal{C}$ depending on $\tilde{\pi}$ only. There is a unique quadratic form q_π on $\mathcal{C}$ with associated bilinear form θ_π, such that for any $d = (\tilde{d}, \lambda) \in \mathcal{P}$, $\tilde{d} \in \mathcal{C}$, $\lambda \in \mathbb{F}_2$ we have*

$$(\tilde{d}, \lambda)^\pi = (\tilde{d}^\pi, \lambda + q_\pi(\tilde{d})) .$$

Proof

Define $\theta^{(\pi)} : \mathcal{C} \times \mathcal{C} \to \mathbb{F}_2$ by $\theta^{(\pi)}(d, e) = \theta(d^\pi, e^\pi)$. Since M_{24} acts as a group of linear transformations on $\mathcal{C}$ and preserves P, C and A, the function $\theta^{(\pi)}$ satisfies the conditions for a cocycle in Lemma 3.3. So $\theta_\pi = \theta^{(\pi)} + \theta$ is an alternating bilinear form by Lemma 3.4. By construction, θ_π depends on $\tilde{\pi}$ only. Let q_π be any quadratic from with associated form θ_π. Write $(\tilde{d}, \lambda)^{\pi, q_\pi}$ for $(\tilde{d}^\pi, \lambda + q_\pi(\tilde{d}))$. For $\tilde{d}, \tilde{e} \in \mathcal{C}$ and $\lambda, \mu \in \mathbb{F}_2$ we have:

$$\begin{aligned}
(\tilde{d}, \lambda)^{\pi, q_\pi} \cdot (\tilde{e}, \mu)^{\pi, q_\pi} &= \left(\tilde{d}^\pi + \tilde{e}^\pi, \lambda + q_\pi(\tilde{d}) + \mu + q_\pi(\tilde{e}) + \theta(d^\pi, e^\pi)\right) \\
&= \left(\tilde{d}^\pi + \tilde{e}^\pi, \lambda + \mu + q_\pi(\tilde{d} + \tilde{e}) + \theta_\pi(d, e) + \theta(d^\pi, e^\pi)\right) \\
&= \left(\tilde{d}^\pi + \tilde{e}^\pi, \lambda + \mu + \theta(d, e) + q_\pi(\tilde{d} + \tilde{e})\right) \\
&= \left(\tilde{d} + \tilde{e}, \lambda + \mu + \theta(d, e)\right)^{\pi, q_\pi} \\
&= (\tilde{f}, \nu)^{\pi, q_\pi} , \qquad \text{with} \quad (\tilde{f}, \nu) = (\tilde{d}, \lambda) \cdot (\tilde{e}, \mu) .
\end{aligned}$$

So the mapping $(\tilde{d}, \lambda) \mapsto (\tilde{d}, \lambda)^{\pi, q_\pi}$ is a standard automorphism of $\mathcal{P}$ which maps to the element $\tilde{\pi}$ of M_{24}. There are 2^{12} different standard automorphisms π of $\mathcal{P}$ mapping to the same element $\tilde{\pi}$ of M_{24}, and there are 2^{12} different quadratic forms on $\mathcal{C}$ with the same associated bilinear form θ_π. Hence for any such π there is a unique q_π satisfying the lemma. $\square$

A standard automorphism δ of $\mathcal{P}$ that maps to the neutral element $\tilde{\delta} = 1$ of M_{24} is called a *diagonal automorphism*. In that case the bilinear form θ_δ in Lemma 4.1 is 0 and a quadratic form associated with the bilinear form 0 is a linear form in $\hom(\mathcal{C}, \mathbb{F}_2) \cong \mathcal{C}^*$, which we also denote by δ. So a diagonal automorphism $\delta \in \mathcal{C}^*$ maps d to $d \cdot (-1)^{\langle d, \delta \rangle}$. The parity of δ as a diagonal automorphism agrees with the parity of δ as an element of $\mathcal{C}^*$.

$\mathrm{Aut}_{\mathrm{St}}\mathcal{P}$ is a non-split extension with normal subgroup $\mathcal{C}^*$ and factor group M_{24}. Even if we assume that calculations in $\mathcal{C}, \mathcal{C}^*, \mathcal{P}$ and M_{24} are easy, the calculations in $\mathrm{Aut}_{\mathrm{St}}\mathcal{P}$ are still quite technical. In the remainder of this section we study such calculations.

Using Lemma 4.1, calculation in $\mathrm{Aut}_{\mathrm{St}}\mathcal{P}$ can be done as follows. Choose a basis $(\tilde{b}_0, \ldots, \tilde{b}_{11})$ of $\mathcal{C}$ and for $\pi \in M_{24}$ let $[\pi] \in \mathrm{Aut}_{\mathrm{St}}\mathcal{P}$ be defined by

$$(\tilde{b}_i, 0) \xmapsto{[\pi]} (\tilde{b}_i^\pi, 0) , \quad i = 0, \ldots, 11 .$$

Then any element of $\mathrm{Aut}_{\mathrm{St}}\mathcal{P}$ can uniquely by written in the form $\delta \cdot [\pi]$, $\delta \in \mathcal{C}^*$, $\pi \in M_{24}$, and we have $[\pi] \cdot \delta^\pi = \delta \cdot [\pi]$.

For $\pi, \pi' \in M_{24}$ we have $[\pi\pi'] = \vartheta(\pi, \pi') \cdot [\pi\pi']$, where $\vartheta(\pi, \pi') \in \mathcal{C}^*$ is given by

$$\langle \tilde{b}_i, \vartheta(\pi, \pi') \rangle = q_{[\pi']}(b_i^\pi) , \quad i = 0, \ldots, 11 , \qquad (4.2.1)$$

and $q_{[\pi']}$ is the unique quadratic form on $\mathcal{C}$ with associated bilinear form $\theta_{\pi'}$ satisfying $q_{[\pi']}(\tilde{b}_i) = 0$ for $i = 0, \ldots, 11$. Here $\theta_{\pi'}$ is as in (4.0.1). Note that $\theta_{\pi'}$ and hence also $q_{[\pi']}$ can easily be computed from $\theta(b_i)$ and $\theta(b_i^{\pi'})$, $i = 0, \ldots, 11$.

The proof of (4.2.1) is a simple calculation based on the equation

$$(\tilde{d}, \lambda)^{[\pi][\pi']} = (\tilde{d}^{\pi\pi'}, \lambda + q_{[\pi]}(\tilde{d}) + q_{[\pi']}(\tilde{d}^\pi)) \,, \quad \tilde{d} \in \mathcal{C}, \ \lambda \in \mathbb{F}_2, \ \pi, \pi' \in \mathrm{Aut}_{\mathrm{St}}\mathcal{P} \,, \qquad (4.2.2)$$

with $q_{[\pi]}$ and $q_{[\pi']}$ as in Lemma 4.1. (4.2.2) is a consequence of Lemma 4.1.

5 The code loop group N_0 of the Parker loop $\mathcal{P}$

We define a group N which acts as a permutation group on the elements of $\mathcal{P}^3$. It will turn out that N is a fourfold cover of a maximal subgroup N_0 of the monster $\mathbb{M}$. The elements of $\mathcal{P}^3$ are called *triples*. N_0 has structure $2^2.2^{11}.2^{22}.(S_3 \times M_{24})$ and is the normalizer of a certain four-group $\{1, x, y, z\}$ in $\mathbb{M}$, see [5]. Following Conway's construction of the Monster $\mathbb{M}$ in [5], we define maximal subgroups G_{x0}, G_{y0} and G_{z0} of $\mathbb{M}$, each of structure $2^{1+24}_+.\mathrm{Co}_1$, which centralize the elements x, y and z of the four-group, respectively.

We use the ATLAS conventions [6] for group structures. $G_1.G_2$ denotes a group extension with normal subgroup G_1 and factor group G_2, $G_1 : G_2$ denotes a split extension and $G_1 \times G_2$ a direct product. All these operators associate to the left with the same precedence, and they imply that the given decomposition is invariant. E.g. $G = G_1 \times G_2 : G_3 . G_4$ means $G = ((G_1 \times G_2) : G_3) . G_4$ and implies the existence of normal subgroups G_1 and $G_1 \times G_2$ of G. 2^n is an elementary Abelian group of order 2^n, S_n is the symmetric permutation group of n elements, Co_1 is the automorphism group of the Leech lattice Λ modulo 2, and $\mathrm{Co}_0 = 2.\mathrm{Co}_1$ is the automorphism group of Λ.

The Leech lattice Λ is discussed in section 6. Following [5] we construct a 196884-dimensional real monomial representation 196884_x of the group $N_{x0} = N_0 \cap G_{x0}$, with $|N_0|/|N_{x0}| = 3$, in section 7. Then in section 8 we extend 196884_x to a representation of N_0 by adding a *triality* element τ which (by conjugation) cyclically exchanges the elements x, y, z of the four-group and also their centralizers G_{x0}, G_{y0}, G_{z0}.

The group 2^{1+24}_+ is an extraspecial 2-group, which we will discuss in section 9. There we explicitly construct the representation of an element $\xi \in G_{x0} \setminus N_{x0}$ in the N_0-module 196884_x. Since N_{x0} is a maximal subgroup of G_{x0}, this extends 196884_x to a representation of a group generated by G_{x0} and N_0, which is visibly equivalent to the representation of $\mathbb{M}$ in [5]. Essentially, the main added value of this paper compared to [5] is an explicit description of the representation of an element ξ of $G_{x0} \setminus N_{x0}$ of the Monster, so that a programmer may implement this construction with not too much effort.

As in [5], we define various subgroups of $\mathbb{M}$ shown in Figure 1 . All these subgroups of $\mathbb{M}$ agree with the corresponding subgroups of $\mathbb{M}$ in [5]. In our construction we change a few signs compared to [5] in order to simplify the representation of the element ξ.

We start with the definition of a group $\hat{N}$ which has a simpler structure than N and we will define N as a subgroup of $\hat{N}$ of index 2. We define the following generators $x_d, y_d, z_d, \nu_\pi, \tau, x_\tau, y_\tau, z_\tau$ of $\hat{N}$ by their action on a triple (a, b, c) in $\mathcal{P}^3$:

$$x_d : (\bar{d}ad, \bar{d}b, cd) \qquad y_d : (ad, \bar{d}bd, \bar{d}c) \qquad z_d : (\bar{d}a, bd, \bar{d}cd) \,,$$
$$\nu_\pi : (a^\pi, b^\pi, c^\pi) \qquad \tau : (c, a, b) \,,$$
$$x_\tau : (\bar{a}, \bar{c}, \bar{b}) \qquad y_\tau : (\bar{c}, \bar{b}, \bar{a}) \qquad z_z : (\bar{b}, \bar{a}, \bar{c}) \,,$$

with d ranging over $\mathcal{P}$ and π ranging over $\mathrm{Aut}_{\mathrm{St}}\mathcal{P}$. We put

$$x_\pi = x_\tau^{|\pi|}\nu_\pi, \quad y_\pi = y_\tau^{|\pi|}\nu_\pi, \quad z_\pi = z_\tau^{|\pi|}\nu_\pi, \quad \text{with } |\pi| = 1 \text{ for odd and } |\pi| = 0 \text{ for even } \pi.$$

So e.g. x_π maps (a, b, c) to $(\bar{a}^\pi, \bar{c}^\pi, \bar{b}^\pi)$ for odd π. We define N to be the subgroup of $\hat{N}$ generated by $x_d, y_d, z_d, x_\pi, y_\pi, z_\pi$.

Next we show some relations in $\hat{N}$. For elements u, v of a group we write $[u, v]$ for the commutator $u^{-1}v^{-1}uv$ and u^v for $v^{-1}uv$. We abbreviate x_{-1}, y_{-1} and z_{-1} to x, y and z,
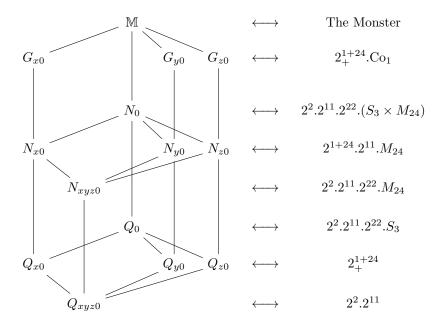
11

$$\mathbb{M} \longleftrightarrow \text{The Monster}$$

$$G_{x0} \quad G_{y0} \; G_{z0} \longleftrightarrow 2^{1+24}_{+}.\mathrm{Co}_1$$

$$N_0 \longleftrightarrow 2^2.2^{11}.2^{22}.(S_3 \times M_{24})$$

$$N_{x0} \quad N_{y0} \; N_{z0} \longleftrightarrow 2^{1+24}.2^{11}.M_{24}$$

$$N_{xyz0} \longleftrightarrow 2^2.2^{11}.2^{22}.M_{24}$$

$$Q_0 \longleftrightarrow 2^2.2^{11}.2^{22}.S_3$$

$$Q_{x0} \quad Q_{y0} \; Q_{z0} \longleftrightarrow 2^{1+24}_{+}$$

$$Q_{xyz0} \longleftrightarrow 2^2.2^{11}$$

Figure 1: Some subgroups of the Monster $\mathbb{M}$.

respectively, as in [5]. The groups $\hat{N}$ and N have a visible symmetry with respect to cyclic permutations of the letters x, y and z, which we will call *triality*. Conjugation with τ just performs such a cyclic permutation. We often just write only one of the three possible cyclic permutations in a formula or a definition, and we state that the others are obtained by triality. We use the symbol $(\&\,\widehat{xyz})$ to indicate that a relation remains valid if the letters x, y, z are cyclically exchanged, e.g.:

$$x_d y_d = z_d z^{P(d)} \;(\&\,\widehat{xyz}) \qquad \text{means} \quad x_d y_d = z_d z^{P(d)}, \; y_d z_d = x_d x^{P(d)}, \; z_d x_d = y_d y^{P(d)}\,.$$

Theorem 5.1. *The following relations define the group $\hat{N}$:*

$$\left.\begin{array}{lll}
x_d x_e = x_{de} x_{A(d,e)}, & \nu_\delta \nu_\epsilon = \nu_{\delta\epsilon}, & [x_d, \nu_\delta] = x^{\langle d, \delta\rangle}, \\
[x_d, y_e] = \nu_{A(d,e)} z^{C(d,e)}, & x_d y_d z_d = 1, & \\
x_d \nu_\pi = \nu_\pi x_{d^\pi}, & \nu_\pi \nu_{\pi'} = \nu_{\pi\pi'}, & \\
\tau^3 = x_\tau^2 = 1, & \tau = y_\tau x_\tau, & x_\tau \tau = \tau^2 x_\tau, \\
[\nu_\pi, \tau] = 1, & x_d \tau = \tau y_d, & x_d \tau^2 = \tau^2 z_d, \\
[\nu_\pi, x_\tau] = [x_d, x_\tau] = 1, & x_\tau y_d = z_d x_\tau, & x_\tau z_d = y_d x_\tau\,.
\end{array}\right\} (\&\,\widehat{xyz}).$$

Proof

Most of these relations can be shown by calculations within associative subloops of $\mathcal{P}$ generated by two elements, which we leave to the reader. We first show $x_d x_e = x_{de} x_{A(d,e)}$. We have

$$(a, b, c) \xmapsto{x_d x_e} \left(\bar{e}(\bar{d}ad)e, \bar{e}(\bar{d}b), (cd)e\right)$$

$$= \left((-1)^{C(a,d)+C(a,e)}a, \; (-1)^{A(b,d,e)}\overline{(de)}b, \; (-1)^{A(c,d,e)}c(de)\right)$$

$$= \left((-1)^{C(a,d+e)+A(a,d,e)}a, \; (-1)^{A(b,d,e)}\overline{(de)}b, \; (-1)^{A(c,d,e)}c(de)\right)$$

$$= \left((-1)^{A(a,d,e)}\overline{(de)}a(de), \; (-1)^{A(b,d,e)}\overline{(de)}b, \; (-1)^{A(c,d,e)}c(de)\right)\,.$$

For the last step, note that $C(a, d) + C(a, e) = C(a, d + e) + A(a, d, e)$ by (3.2.2) Clearly, $x_{de} x_{A(d,e)}$ maps (a, b, c) to the same triple.

12

We also show $[x_d, y_e] = z_{A(d,e)} z^{C(d,e)}$. We have

$$(a, b, c) \overset{[x_d, y_e]}{\longmapsto} \left((-1)^{C(a,d)+C(a+e,d)} a, (-1)^{C(b+d,e)+C(b,e)} b, \bar{e}\left((e(c\bar{d}))d \right) \right)$$

$$= \left((-1)^{C(d,e)+A(a,d,e)} a, (-1)^{C(d,e)+A(b,d,e)} b, (-1)^{A(c,d,e)} c \right) .$$

Note that $A(c + d, d, e) = A(c, d, e)$. Clearly, $z_{A(d,e)} z^{C(d,e)}$ maps (a, b, c) to the same triple.

Using the relations shown we may convert any word in the generators of $\hat{N}$ to the form:

$$x_d y_e x_\pi \tau^m x_\tau^n, \quad 0 \le m < 3, \, 0 \le n < 2 .$$

Such a word with $(m, n) \ne (0, 0)$ does not fix a triple $(1, \Omega, d)$ with $d \notin \{\pm 1, \pm \Omega\}$. A word of shape $x_d y_e x_\pi$, permutes the elements of each component $\mathcal{P}$ in $\mathcal{P}^3$. The stabilizers of components 1, 2 and 3 of $\mathcal{P}^3$ are $\{x_{\pm 1}, x_{\pm \Omega}\}$, $\{y_{\pm 1}, y_{\pm \Omega}\}$ and $\{z_{\pm 1}, z_{\pm \Omega}\}$. The intersection of these stabilizers is $\{1\}$.
$\square$

An immediate consequence of Theorem 5.1 is:

$$[x_d, x_e] = x^{C(d,e)}, \quad x_d^2 = x^{P(d)}, \quad \nu_\delta^2 = [\nu_\delta, \nu_\epsilon] = 1 . \quad (\& \, x\widehat{y}z) \tag{5.2.1}$$

Note that $[x_d, x_e] = (x_e x_d)^{-1} x_d x_e = x_{A(d,e)} (x_{ed})^{-1} x_{de} x_{A(d,e)} = x^{C(d,e)}$.

In order to make calculations in $\hat{N}$ and N easy, we have stated more relations than necessary. From Theorem 5.1 and its proof we see that $\hat{N}$ has structure $2^2.2^{12}.2^{24}.(S_3 \times M_{24})$.

Assigning "odd" parity to x_τ, y_τ, z_τ and to ν_π, π odd, and "even" parity to the other generators of $\hat{N}$, we see that the generators of N have even parity and that the relations in Theorem 5.1 preserve that parity. Thus N is the subgroup of the "even" elements of $\hat{N}$ and we have $|\hat{N}/N| = 2$. Note also that $\tau \in N$.

Our generators of N agree with Conway's generators in [5] with the following exceptions: Our generators x_d, y_d, z_d, correspond to $x_d \cdot z_{-1}^{P(d)}, \, y_d \cdot x_{-1}^{P(d)} \, z_d \cdot y_{-1}^{P(d)}$ in [5]. But our group N agrees with that in [5]. Our definition of x_d, y_d, z_d leads to simpler relations in N, and it agrees with Ivanov's construction of G_2 in [14], section 2.7, with G_2 in [14] corresponding to Conway's and our group N_0.

As in [5], we define $\mathcal{K}_1 = y_\Omega z_{-\Omega}$, $\mathcal{K}_2 = z_\Omega x_{-\Omega}$, $\mathcal{K}_3 = x_\Omega y_{-\Omega}$, and we put:

$$K_1 = \{1, \mathcal{K}_1\}, \quad K_2 = \{1, \mathcal{K}_2\}, \quad K_3 = \{1, \mathcal{K}_3\}, \quad K_0 = \{1, \mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3\}, .$$

Then K_0 is normal in N and $N_0 = N/K_0$ is the normalizer of a certain fourgroup in $\mathbb{M}$. For a subgroup Γ of N we define $\Gamma_n = \Gamma/\Gamma \cap K_n$, $n = 0, 1, 2, 3$. Note that K_0 is not normal in $\hat{N}$. The symbol $(\& \, x\widehat{y}z)$ will also indicate that a statement remains valid if the indices $1, 2, 3$ in the definitions above are cyclically permuted together with x, y, z. E.g.

$$\mathcal{K}_1 = x_\Omega z \in K_1 \, (\& \, x\widehat{y}z) \quad \text{implies} \quad \mathcal{K}_2 = y_\Omega x \in K_2 \quad \text{and} \quad \mathcal{K}_3 = z_\Omega y \in K_3 .$$

As a corollary of the proof of Theorem 5.1 we obtain the following structure of N:

$$N = \underbrace{2^2}_{\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3} \times \underbrace{2^2}_{x, y, z} . \underbrace{2^{11}}_{\substack{x_\delta = y_\delta = z_\delta \\ \delta \text{ even}}} . \underbrace{2^{22}}_{x_d, y_d, z_d} . \left(\underbrace{S_3}_{\substack{x_\delta, y_\delta, z_\delta \\ \delta \text{ odd}}} \times \underbrace{M_{24}}_{\substack{x_\pi = y_\pi = z_\pi \\ \pi \text{ even}}} \right) . \tag{5.3.1}$$

By omitting the M_{24} generators we obtain a normal subgroup Q and by omitting the S_3 generators we obtain a normal subgroup N_{xyz} of N.

The centralizer of x in N is called N_x and has structure

$$N_x = \underbrace{2}_{\mathcal{K}_1} \times \underbrace{2}_{\mathcal{K}_2, \mathcal{K}_3} : \underbrace{2_+^{1+24}}_{x_d, x_\delta} . \underbrace{2^{11}}_{y_d, z_d} . \underbrace{M_{24}}_{x_\pi} \quad (\& \, x\widehat{y}z). \tag{5.3.2}$$
$$\underbrace{\phantom{2 \times 2 : 2_+^{1+24}}}_{(\text{This is } Q_x)}$$

Let Q_x be the subgroup of N_x generated by x_d, x_δ with $d \in \mathcal{P}, \delta \in \mathbb{C}^*$. Then $Q_x \cap K_0 = 1$, so we have $Q_x \cong Q_{x1} \cong Q_{x0}$. Q_x is not normal in N_x, but $K_1 Q_x$ is. To see this, it suffices to verify $[x_\delta, \mathcal{K}_1] = 1$ and $\mathcal{K}_2 x_\delta = x_\delta \mathcal{K}_3$ for odd δ (apart from trivial checks).

The defining relations in the group Q_x given by Theorem 5.1 and (5.2.1) simplify to:

$$x_d^2 = x^{P(d)}, \ x_\delta^2 = 1, \ x_d x_e = x_{de} x_{A(d,e)}, \ x_\delta x_\epsilon = x_{\delta+\epsilon}, \ [x_d, x_\delta] = x^{\langle d, \delta \rangle}, \qquad (5.3.3)$$

so every element of Q_x can uniquely be written in the form $x_d x_\delta$. We often write $x_r, x_s, \ldots$ for elements of Q_x. We put

$$\tilde{x}_d = x_{-1}^\mu x_d x_{\theta(d)} \quad \text{for } d = (\tilde{d}, \mu) \in \mathcal{P}, \ \tilde{d} \in \mathcal{C}, \ \mu \in \mathbb{F}_2, \text{ and cocyle } \theta, \text{ i.e. } \theta(d) \in \mathcal{C}^*. \quad (5.3.4)$$

$\tilde{x}_d$ does not depend on the sign of d, so $\tilde{x}_d$ is also well defined for $d \in \mathcal{C}$. Then the group Q_x generated by x_d, x_δ, $d \in \mathcal{P}, \delta \in \mathcal{C}^*$ is also generated by $\tilde{x}_d, x_\delta$. It is visibly extraspecial of type 2_+^{1+24}, satisfying the even simpler relations:

$$\tilde{x}_d^2 = x_\delta^2 = 1, \ \tilde{x}_d \tilde{x}_e = \tilde{x}_{de}, \ x_\delta x_\epsilon = x_{\delta\epsilon}, \ [\tilde{x}_d, x_\delta] = x^{\langle \tilde{d}, \delta \rangle}, \qquad (5.3.5)$$

which are easy consequences of (3.2.3) (3.3) and (5.3.3). We will discuss extraspecial 2-groups in section 9.1. So the structure description (5.3.2) of N_x should now be clear.

Similarly, we let N_y and N_z be the centralizers of y and z in N. We let Q_y and Q_z be the subgroups of N_y and N_z generated by y_d, y_δ and z_d, z_δ, respectively.

Our definition of Q_x differs from that in [5], since the definition of N in [5] does not easily lead to a split extension corresponding to our extension $K_0 : Q_x$. We put

$$Q_{xyz} = K_0 Q_x \cap K_0 Q_y \cap K_0 Q_z \ .$$

Q_{xyz} is elementary Abelian of structure $2^2.2^2.2^{11}$ and generated by K_0, x, y, z and x_δ, δ even.

6 The relation between Q_x and the Leech lattice Λ

6.1 The homomorphism from Q_x to the $\Lambda/2\Lambda$

The 24-dimensional Leech lattice Λ is defined as follows. Consider an Euclidean vector space $\mathbb{R}^{24}$ with scalar product $\langle ., . \rangle$ and basis vectors labelled by the elements of $\tilde{\Omega}$. Assume that a Golay code $\mathcal{C}$ is given on $\mathbb{F}_2^{24} = \prod_{i \in \tilde{\Omega}} \mathbb{F}_2$. Then the Leech lattice is the set of vectors u in $\mathbb{R}^{24}$ with co-ordinates $(u_i, i \in \tilde{\Omega})$, such that there is an $m \in \{0, 1\}$ and a $d \in \mathcal{C}$ with

$$\begin{aligned} \forall i \in \tilde{\Omega}: \quad u_i &= m + 2 \cdot \langle d, i \rangle \quad &&(\text{mod } 4), \\ \sum_{i \in \tilde{\Omega}} u &= 4m \quad &&(\text{mod } 8). \end{aligned}$$

See e.g. [7], Chapter 4, section 11 for background. The Leech lattice Λ is an even unimodular lattice, i.e. $\langle u, u \rangle$ is even for all $u \in \Lambda$ and $\det \Lambda = 1$. Therefore we have to scale the basis vectors of the underlying space $\mathbb{R}^{24}$ so that they have norm $1/\sqrt{8}$, not 1. Then for vectors u, v with co-ordinates u_i, v_i (where i ranges over $\tilde{\Omega}$) we have $\langle u, v \rangle = \frac{1}{8} \sum u_i v_i$. For $u \in \Lambda$ we define $\text{type}(u) = \frac{1}{2} \langle u, u \rangle = \frac{1}{16} \sum u_i^2$. The Leech lattice can be characterized as the (unique) 24-dimensional even unimodular lattice without any vectors of type 1, see e.g. [7].

Theorem 6.1. *There is an isomorphism from $Q_x/\{1, x\}$ to $\Lambda/2\Lambda$ given by:*

$$\begin{aligned} x_i &\mapsto \lambda_i = (-3_{\text{on } i}, 1_{\text{elsewehere}}) \ , \\ x_d &\mapsto \lambda_d = (2_{\text{on } d}, 0_{\text{elsewehere}}) \qquad \text{if } |d| = 0 \bmod 8 \ , \\ x_d &\mapsto \lambda_d = (0_{\text{on } d}, 2_{\text{elsewehere}}) \qquad \text{if } |d| = 4 \bmod 8 \ , \end{aligned}$$

which satisfies $[x_r, x_s] = x^{\langle \lambda_r, \lambda_s \rangle}, \quad x_r^2 = x^{\text{type}(\lambda_r)}, \quad \text{with } \text{type}(\lambda_r) = \frac{1}{2} \langle \lambda_r, \lambda_r \rangle \ .$

Our homomorphism $Q_x \to \Lambda/2\Lambda$ differs slightly from the corresponding homomorphism in [5], Theorem 2, where x_d is mapped to $(2_{\text{on } d}, 0_{\text{elswehere}})$ for all $d \in \mathcal{P}$. But it agrees with the isomorphism $W_{24} \to \Lambda/2\Lambda$ in [14], Lemma 1.8.3, which leads to a simpler set of relations in the group N. Note that W_{24} in [14] corresponds to $Q_x/\{1, x\}$ in this paper.

Proof of Theorem 6.1

The proof is along the lines of the proof of Theorem 2 in. [5]. The definitions of λ_i, λ_d imply:

$$x_\Omega \mapsto -2\lambda_i + \lambda_\Omega = (8_{\text{on } i}, 0_{\text{elswehere}}) \qquad \text{for any } i \in \tilde{\Omega} \ ,$$

$$x_d x_\Omega^{|d|/4} \mapsto (2_{\text{on } d}, 0_{\text{elswehere}}) \ ,$$

$$x_\delta x_\Omega^{|\delta|/2} \mapsto (4_{\text{on } \delta}, 0_{\text{elswehere}}) \qquad \text{for any } \delta \subset \tilde{\Omega} \text{ with } |\delta| \text{ even } .$$

For any $d \in \mathcal{C}$ the value $|d|/2$ is even, so that the product $\Pi_{i \in d} x_i$ maps to $2 \cdot \lambda_d$ or to $2 \cdot \lambda_{d+\Omega}$. Thus for any $\delta \in \mathcal{C}^*$ the image of x_δ is well defined in $\Lambda/2\Lambda$, even if δ is defined modulo $\mathcal{C}$ only. To show that the mapping $x_r \mapsto \lambda_r$ is a homomorphism, it suffices to check that it preserves the relations 5.3.3. Since x_{-1} is mapped to 0, all these checks are easy except for the relation $x_d x_e = x_{de} x_{A(d,e)}$. We have

$$x_d x_\Omega^{|d|/4} x_e x_\Omega^{|e|/4} \mapsto (4_{\text{on } d \cap e}, \ 2_{\text{on } d+e}, \ 0_{\text{elswehere}}) \ .$$

Clearly, $x_{d+e} x_\Omega^{|d+e|/4} x_{d \cap e} x_\Omega^{|d \cap e|/2}$ maps to the same element of $\Lambda/2\Lambda$. Thus the relation $x_d x_e = x_{de} x_{A(d,e)} x_\Omega^m$ is preserved for $m = |d+e|/4 + |d|/4 + |e|/4 + |d \cap e|/2 = 0 \pmod 2$. The mapping $x_r \mapsto \lambda_r$ is surjective by construction and both, its origin and its image, have size 2^{24}; hence it is an isomorphism.

In an extraspecial 2 group the commutator is bilinear and we have $\text{type}(u+v) = \text{type}(u) + \text{type}(v) + \langle u, v \rangle$ and $(x_r x_s)^2 = x_r^2 x_s^2 [x_r, x_s]$. So it suffices to check $x_r^2 = x^{\text{type}(\lambda_r)}$ and $[x_r, x_s] = x^{\langle \lambda_r, \lambda_s \rangle}$, with x_r, x_s running through all the generators x_d, x_δ given in the Theorem. All these checks can be done by easy calculations using 5.3.3.
□

An immediate consequence of Theorem 6.1 is $P(d) = \text{type}(\lambda_d) \pmod 2$ for all $d \in \mathcal{P}$.

We will abbreviate $x_d \cdot x_\delta$ to $x_{d \cdot \delta}$ and $\lambda_d + \lambda_\delta$ to $\lambda_{d \cdot \delta}$ for $d \in \mathcal{P}, \delta \in \mathcal{C}^*$ as in [5]. For $r = (d, \delta) \in \mathcal{P} \times \mathcal{C}^*$ we will define $x_r = x_{d \cdot \delta}$, and for $f \in \{\pm 1, \pm \Omega\}$ we put $x_{f \cdot r} = x_f \cdot x_r$. (The more relaxed condition $f \in \mathcal{P}$ could have the funny effect $x_{f \cdot d} = x_f x_d \ne x_{fd}$).

6.2 Short vectors in $\Lambda/2\Lambda$

A vector in $\Lambda/2\Lambda$ is called *short*, if it is congruent modulo 2Λ to a vector of type 2 in Λ, i.e. to a shortest nonzero vector in Λ. x_r is called short if its image λ_r in $\Lambda/2\Lambda$ is short. We define x_r^+ to be $x_{\Omega \cdot r}$ if this is short and x_r otherwise. The short vectors in $\Lambda/2\Lambda$ are given as follows, see [5] or [7], Ch. 4.11.

$$\lambda_{ij} : (4_{\text{on } i}, -4_{\text{on } j}, 0_{\text{else}}),$$

$$\lambda_{ij}^+ = \lambda_{\Omega \cdot ij} : (4_{\text{on } i,j}, 0_{\text{else}}), \tag{6.1.1}$$

$$\lambda_{d \cdot \delta}^+ = \lambda_{\Omega^n d \cdot \delta} : (-2_{\text{on } \delta}, 2_{\text{on } d \backslash \delta}, 0_{\text{else}}), \quad n = |\delta|/2, |d| = 8, \text{and } \delta \text{ is an even subset of } d,$$

$$\lambda_{d \cdot i}^+ = \lambda_{\Omega^m d \cdot i} : (\mp 3_{\text{on } i}, \pm 1_{\text{else}}), \ m = \langle d, i \rangle + P(d), \text{ and the lower sign is taken on } d.$$

For d in $\mathcal{C}$ (or in $\mathcal{P}$) with $|d| = 8$ we define $A(d, \mathcal{C}) = \{A(d, c) \mid c \in \mathcal{C}\}$. It follows from standard facts about the Golay code that $A(d, \mathcal{C})$ is the set of all even elements of $\mathcal{C}^*$ which can be represented as a subset of d. An element of $A(d, \mathcal{C})$ has exactly two representatives δ and $d + \delta$ which are subsets of d. If δ, ϵ are given as elements of $A(d, \mathcal{C})$, then the expressions $|\delta|/2$ and $|\delta \cap \epsilon|$ are well defined (modulo 2) under the assumption that subsets of d are

15

chosen as representatives of δ and ϵ. Thus $\lambda_{d\cdot\delta}^+$, $|d| = 8$, δ even, is short if and only if $\delta \in A(d, \mathcal{C})$. For each octad d (i.e. $d \in \mathcal{C}$, $|d| = 8$) there are 64 short vectors of that shape.

We obviously have $\lambda_{-r} = \lambda_r$ for all short vectors λ_r. We also have $\lambda_{d\cdot i}^+ = \lambda_{\Omega d\cdot i}^+$. $\mathcal{C}$ contains 759 octads. So the numbers of the short vectors as given above are:

$$|\lambda_{ij}| = |\lambda_{ij}^+| = \binom{24}{2} = 276, \ |\lambda_{d\cdot\delta}^+| = 759 \cdot 64 = 48576, \ |\lambda_{d\cdot i}^+| = 2048 \cdot 24 = 49152 \,.$$

Altogether we have 98280 short vectors in $\Lambda/2\Lambda$.

7 Representations of the groups N_{x0}, N_{y0}, N_{z0}

In this section we construct a 196884-dimensional real monomial representation 196884_x of the group $N_{x0} = N_0 \cap G_{x0}$. We give a basis of the vector space 196884_x and we state the operations of the generators of N_{x0}. In section 8 we extend 196884_x to N_0 and in section 9 we extend 196884_x to G_{x0} so that we eventually obtain a representation of the monster $\mathbb{M}$. Similar representations 196884_y and 196884_z of N_{y0} and N_{z0} may be obtained in the same way.

7.1 Representations 98280_x, 98280_y, 98280_z of N_{x0}, N_{y0}, N_{z0}

Since $Q_{x0} \cong Q_x$ and Q_{x0} is normal in N_{x0}, the group N_{x0} acts on Q_x via conjugation, preserving the paring between x_r and x_{-r} in Q_x. This leads to a representation of N_{x0} on a real vector space 98280_x of dimension 98280 spanned by short vectors X_r, $r \in \mathcal{P} \times \mathcal{C}^*$ with the relation $-(X_r) = X_{-r}$, so that N_{x0} acts on X_r in the same way as on x_r by conjugation. We will use the same symbol 98280_x for that vector space and the action of the group N_{x0} on that vector space. Since N_{x0} is a quotient of N_{x1} and N_x, this gives us also a representation on N_{x1} and N_x.

We give 98280_x the structure of an Euclidean space by assigning norm 1 to all vectors X_r, and by declaring all pairs of such vectors perpendicular unless they are equal or opposite.

Considering 98280_x as a representation of N_x, its kernel is the group generated by K_0 and x. The elements y and z of N_x act on the basis vector $X_{d\cdot\delta}$ of 98280_x as $(-1)^{|\delta|}$. Using triality, we may define similar representations 98280_y and 98280_z of N_y and N_z.

7.2 Representations 4096_x, 4096_y, 4096_z of N_{x1}, N_{y2}, N_{z3}

In this section we construct representations 4096_x, 4096_y and 4096_z of the groups N_{x1}, N_{y2} and N_{z3}. On the way we also obtain a representation $(6\cdot2048)_N$ of N which will be useful for combining the first three representations to a representation of N_0.

We construct these representations from the action of N on $\mathcal{P}^3$ given in section 5. We augment $\mathcal{P}$ by an element 0 by decreeing $0 \cdot d = d \cdot 0 = 0 \cdot 0 = 0$, $d \in \mathcal{P}$ and we write $\mathcal{P}_0$ for $\mathcal{P} \cup 0$ with that operation. Put $\mathcal{P}_0^{(3)} = \{(d, 0, 0), (0, d, 0), (0, 0, d) \mid d \in \mathcal{P}\}$. By definition N acts as a permutation group on $\mathcal{P}_0^{(3)}$. The action of N on $\mathcal{P}_0^{(3)}$ preserves the pairing between (a, b, c) and $(-a, -b, -c)$. So we have a monomial representation of N on the real vector space $(6\cdot2048)_N$ spanned by the basis vectors in $\mathcal{P}_0^{(3)}$ with the identification $-(a, b, c) = (-a, -b, -c)$. Let K_0, K_1, and K_2 be as in section 5. We prefer a different basis of $(6\cdot2048)_N$, so that we can easily identify the subspaces of $(6\cdot2048)_N$ where the representation of K_0, K_1, or K_2 is trivial. For all $d \in \mathcal{P}$ we define

$$\begin{aligned}
d_1^- &= (0, d, 0) + (0, -\Omega d, 0)\,, & d_1^+ &= (0, 0, \bar{d}) + (0, 0, \Omega \bar{d})\,, \\
d_2^- &= (0, 0, d) + (0, 0, -\Omega d)\,, & d_2^+ &= (\bar{d}, 0, 0) + (\Omega \bar{d}, 0, 0)\,, \\
d_3^- &= (d, 0, 0) + (-\Omega d, 0, 0)\,, & d_3^+ &= (0, \bar{d}, 0) + (0, \Omega \bar{d}, 0)\,.
\end{aligned}$$

Here we make another deviation from Conway's original definition in [5]: d_m^+ in [5] corresponds to our $\bar{d}_m^+$. The motivation for this change is given in section 1. This change greatly simplifies the representation of the element ξ of $G_{x0} \setminus N_{x0}$ in 4096_x, as stated in Corollary 9.16.

The set $(d_m^\pm)$, $d \in \mathcal{P}$, $m = 1, 2, 3$ is a basis of $(6 \cdot 2048)_N$ with the obvious identifications

$$(d)_m^- = -(-d)_m^- = -(\Omega d)_m^- = (-\Omega d)_m^- \, , \ (d)_m^+ = -(-d)_m^+ = (\Omega d)_m^+ = -(-\Omega d)_m^+ \, . \quad (7.1.1)$$

For $m = 1, 2, 3$ we write $\langle d_m^+ \rangle$ and $\langle d_m^- \rangle$ for the subspaces of $(6 \cdot 2048)_N$ generated by the corresponding basis vectors. All these 2048-dimensional subspaces are invariant under the action of N_{xyz}. They are permuted by the cosets of N_{xyz} as indicated in Table 1 for the coset representatives x_i and τ.

We give $(6 \cdot 2048)_N$ the structure of an Euclidean space by assigning the norm $1/\sqrt{2}$ to all vectors $(d, 0, 0)$, $(0, d, 0)$, and $(0, 0, d)$ and by declaring all pairs of such vectors perpendicular unless they are equal or opposite. Then all vectors $(d_m^\pm)$, $m = 1, 2, 3$ have norm 1 and pairs such vectors are also perpendicular unless they are equal or opposite. In the sequel $(6 \cdot 2048)_N$ means the representation of N on this Euclidean space with orthonormal basis vectors taken from the vectors $(d_m^\pm)$, $m = 1, 2, 3$. Then $(6 \cdot 2048)_N$ is an orthogonal and monomial representation of N.

We define the representations 4096_x, 4096_y and 4096_z of N_x, N_y and N_z, respectively, by their natural action on the following subspaces of $(6 \cdot 2048)_N$:

$$4096_x : \langle d_1^- \rangle \oplus \langle d_1^+ \rangle \, , \quad 4096_y : \langle d_2^- \rangle \oplus \langle d_2^+ \rangle \, , \quad 4096_z : \langle d_3^- \rangle \oplus \langle d_3^+ \rangle \, ,$$

where $\oplus$ denotes the direct sum. The kernels of 4096_x, 4096_y, 4096_z, and elements acting as -1 are displayed in Table 1. From these kernels we see that 4096_x, 4096_y, 4096_z are also representations of N_{x1}, N_{y2}, N_{z3}, respectively.

Subspace of $(6 \cdot 2048)_N$	4096_x		4096_y		4096_z	
	$\langle d_1^- \rangle$	$\langle d_1^+ \rangle$	$\langle d_2^- \rangle$	$\langle d_2^+ \rangle$	$\langle d_3^- \rangle$	$\langle d_3^+ \rangle$
Kernel of $4096_{x,y,z}$	$1, \mathcal{K}_1, y_\Omega, z_{-\Omega}$		$1, \mathcal{K}_2, z_\Omega, x_{-\Omega}$		$1, \mathcal{K}_3, x_\Omega, y_{-\Omega}$	
Elements acting as -1	$x_{-1}, \mathcal{K}_2, \mathcal{K}_3$		$y_{-1}, \mathcal{K}_1, \mathcal{K}_3$		$z_{-1}, \mathcal{K}_1, \mathcal{K}_2$	
x_i maps subspace to	$\langle d_1^+ \rangle$	$\langle d_1^- \rangle$	$\langle d_3^+ \rangle$	$\langle d_3^- \rangle$	$\langle d_2^+ \rangle$	$\langle d_2^- \rangle$
τ maps subspace to	$\langle d_2^- \rangle$	$\langle d_2^+ \rangle$	$\langle d_3^- \rangle$	$\langle d_3^+ \rangle$	$\langle d_1^- \rangle$	$\langle d_1^+ \rangle$

Table 1: The kernels of and the action of S_3 on the subspaces of $(6 \cdot 2048)_N$

7.3 Representations $24_x, 24_y, 24_z$ of N_{x1}, N_{y2}, N_{z3}

In this section we construct representations 24_x, 24_y and 24_z of the groups N_{x1}, N_{y2} and N_{z3}. On the way we also obtain a representation $(3 \cdot 24)_N$ of N which will be useful for combining the first three representations to a representation of N_0.

Now we construct a representation $(3 \cdot 24)_N$ of N. For each $i \in \tilde{\Omega}$ we define i_1 by:

$$i_1 = \sum_{d \in \mathcal{P}} (-1)^{\langle d, i \rangle} (d, 0, 0) \, ,$$

without any identification of $(d, 0, 0)$ and $(-d, 0, 0)$.

We define i_2, i_3 similarly by using the triples $(0, d, 0)$ and $(0, 0, d)$. Then it is easy to check that the subgroup $Q_{xyz}^{(-)}$ of Q_{xyz} generated by x_δ, x, y, z, δ even, preserves i_1, i_2, i_3 and that N operates on i_1 as follows:

$$i_1 \xmapsto{x_d} i_1 \, , \quad i_1 \xmapsto{y_d, z_d} (-1)^{\langle d, i \rangle} i_1 \, , \quad i_1 \xmapsto{x_\pi} i_1^\pi \, , \quad i_1 \xmapsto{\tau} i_2 \, , \quad (\& \widehat{xyz}) \, .$$

Here the symbol $(\& \widehat{xyz})$ means that x, y, z and indices $1, 2, 3$ must be cyclically permuted. We define 24_x to be the representation of N_x with basis $i_1, i \in \tilde{\Omega}$. Representations 24_z and 24_y are defined similarly, based on i_2 and i_3. Then

$$(3{\cdot}24)_N = 24_x \oplus 24_y \oplus 24_z$$

is a representation of N with kernel $Q_{xyz}^{(-)}$. x_δ preserves i_1 and exchanges i_2 with i_3 for odd δ, and τ cyclically permutes i_1, i_2 and i_3.

We declare $\{i_m | i \in \tilde{\Omega}, m = 1, 2, 3\}$ to be an orthonormal basis of the Euclidean space $(3{\cdot}24)_N$. Then N acts orthogonally and monomially on that space.

Representations $24_x, 24_y, 24_z$ are invariant under the action of N_{xyz}. But they are permuted by the cosets of N_{xyz} in N, as indicated by the action of the coset representatives x_i and τ in the following Table 2. This table also displays the kernels of these representations and the elements acting as -1.

Subspace of $(3{\cdot}24)_N$	24_x	24_y	24_z
basis vectors	$i_1, i \in \tilde{\Omega}$	i_2	i_3
Kernel generated by	$\mathcal{K}_1, x_d, x_\delta, y, z$	$\mathcal{K}_2, y_d, y_\delta, x, z$	$\mathcal{K}_3, z_d, z_\delta, x, y$
Elements acting as -1	$\mathcal{K}_2, \mathcal{K}_3, y_\Omega, z_\Omega$	$\mathcal{K}_1, \mathcal{K}_3, x_\Omega, z_\Omega$	$\mathcal{K}_1, \mathcal{K}_2, x_\Omega, y_\Omega$
x_i maps subspace to	24_x	24_z	24_y
τ maps subspace to	24_y	24_z	24_x

Table 2: Kernels of and action of S_3 on the subspaces of $(3{\cdot}24)_N$

7.4 Representation 196884_x, 196884_y, 196884_z of N_{x0}, N_{y0}, N_{z0}

We will now construct a representation 196384_x of subgroup $N_{x0} = N_x/K_0$ of the monster $\mathbb{M}$ from the representations 24_x, 4096_x and 98280_x. We define the representation

$$196884_x = 300_x \oplus 98280_x \oplus 98304_x$$

of N_{x0} to be the direct sum of representations 300_x, 98280_x 98304_x, where

300_x is the symmetric tensor square $24_x \otimes_{\text{sym}} 24_x$ of 24_x ,

98280_x is defined as above ,

98304_x is the tensor product $4096_x \otimes 24_x$.

98280_x is a representation of N_{x0} by construction. For both representations, 300_x and 98304_x, the group K_1 is in their kernel, and $\mathcal{K}_2, \mathcal{K}_3$ act as -1. Thus K_0 is contained in the kernel of the tensor products $24_x \otimes 24_x$ and $4096_x \otimes 24_x$, so that 300_x and 98304_x are indeed representations of N_{x0}.

We introduce some abbreviations for the basis vectors that we will use for 196884_x:

for 300_x : $(ii)_1 = i_1 \otimes i_1$, of norm 1,

$(ij)_1 = i_1 \otimes j_1 + j_1 \otimes i_1$ $(i \neq j)$, of squared norm 2,

for 98280_x : X_r $(r$ short$)$, of norm 1,

for 98304_x : $d^{\pm} \otimes_1 i = d_1^{\pm} \otimes i_1$ $(d \in \mathcal{P}, i \in \tilde{\Omega})$, of norm 1.

These basis vectors are mutually orthogonal, except when equal or opposite. For representations 196884_y and 196884_z we use the corresponding notation $(\& \widehat{xyz})$ obtained by cyclically permuting (x, y, z) and $(1, 2, 3)$. The action of the generators of N on the basis vectors of 196884_x, 196884_y and 196884_z can be obtained from Table 3.

g	Action of g on the basis vectors				
	i_1	d_1^-	d_1^+	$X_{d\cdot\delta}$, δ even	$X_{d\cdot i}^+$, $i \in \tilde{\Omega}$
x_e	i_1	$(\bar{e}d)_1^-$	$(\bar{e}d)_1^+$	$(-1)^n X_{d\cdot\delta}$	$(-1)^{\langle e,i\rangle} X_{\bar{e}de\cdot i}^+$
y_e	$(-1)^{\langle e,i\rangle} i_1$	$(\bar{e}de)_1^-$	$(de)_1^+$	$(-1)^{\langle e,\delta\rangle} X_{\Omega^n d\cdot\delta\delta'}$	$X_{de\cdot i}^+$
z_e	$(-1)^{\langle e,i\rangle} i_1$	$(de)_1^-$	$(\bar{e}de)_1^+$	$(-1)^{C(d,e)} X_{\Omega^n d\cdot\delta\delta'}$	$(-1)^{\langle e,i\rangle} X_{\bar{e}d\cdot i}^+$
x_π, π even	$(i^\pi)_1$	$(d^\pi)_1^-$	$(d^\pi)_1^+$	$X_{d^\pi\cdot\delta^\pi}$	$X_{d^\pi\cdot i^\pi}^+$
x_π, π odd	$(i^\pi)_1$	$(d^\pi)_1^+$	$(d^\pi)_1^-$	$X_{d^\pi\cdot\delta^\pi}$	$(-1)^m X_{d^\pi\cdot i^\pi}^+$
y_π, π odd	$(i^\pi)_3$	$(d^\pi)_3^+$	$(d^\pi)_3^-$	$Z_{d^\pi\cdot\delta^\pi}$	$(-1)^m Z_{d^\pi\cdot i^\pi}^+$
z_π, π odd	$(i^\pi)_2$	$(d^\pi)_2^+$	$(d^\pi)_2^-$	$Y_{d^\pi\cdot\delta^\pi}$	$(-1)^m Y_{d^\pi\cdot i^\pi}^+$
τ	i_2	d_2^-	d_2^+	$Y_{d\cdot\delta}$	$Y_{d\cdot i}^+$
τ^2	i_3	d_3^-	d_3^+	$Z_{d\cdot\delta}$	$Z_{d\cdot i}^+$

Table 3: Action of the generators of N on 24_x, 4096_x and 98280_x.
Notation: $n = C(d,e) + \langle e,\delta\rangle$, $\delta' = A(d,e)$, $X_{d\cdot i}^+ = X_{\Omega^m d\cdot i}$, with $m = P(d) + \langle d,i\rangle$.

The action of the generating elements g of N on the basis vectors $i_2, d_2^\pm, Y_{d\times\delta}$ and $i_3, d_3^\pm, Z_{d\times\delta}$ can by obtained by applying the triality operation ($\&\,\widehat{xyz}$) to the corresponding entries in Table 3. E.g. from the action of z_e on d_1^+ and i_1 we may deduce

$$d_2^+ \otimes i_2 \xmapsto{x_e} (-1)^{\langle e,i\rangle}(\bar{e}de)_2^+ \otimes i_2 \qquad \text{and} \qquad d_3^+ \otimes i_3 \xmapsto{y_e} (-1)^{\langle e,i\rangle}(\bar{e}de)_3^+ \otimes i_3$$

by applying the triality operation ($\&\,\widehat{xyz}$). In the sequel the phrase "from Table 3 we obtain ..." means that the reader has to apply the triality operation ($\&\,\widehat{xyz}$) by himself, if necessary.

The action of g on the basis vectors $X_{d\cdot\delta}, X_{d\cdot i}$ is obtained by conjugation of the corresponding basis vector with g and taking the result modulo the kernel K_1.

The basis vector $X_{d\cdot i}^+$ in Table 3 is short for all $d \in \mathcal{P}, i \in \tilde{\Omega}$ and all short basis vectors $X_{d\cdot\delta}$ for odd δ are of that shape. We have $X_{d\cdot i}^+ = X_{\Omega d\cdot i}^+$. The notation $X_{d\cdot i}^+$ in Table 3 is consistent with the notation $x_{d\cdot i}^+$ in section 6.2.

The following table is helpful for computing the last two columns in Table 3:

g	Value of $g^{-1}Bg$ for			
	$B = x_d$	$B = x_\delta, \delta$ even	$B = x_i, i \in \tilde{\Omega}$	Remarks
x_e	$x^{C(d,e)} x_d$	$x^{\langle e,\delta\rangle} x_\delta$	$x^{\langle e,i\rangle}$	
y_e	$z^{C(d,e)} x_d x_{A(d,e)}$	$y^{\langle e,\delta\rangle} x_\delta$	$z^{P(e)+\langle e,i\rangle} x_e x_i$	$y = x_{-\Omega}, z = x_\Omega$
z_e	$y^{C(d,e)} x_d x_{A(d,e)}$	$z^{\langle e,\delta\rangle} x_\delta$	$y^{P(e)+\langle e,i\rangle} x_e x_i$	$(\mathrm{mod}\ K_1)$
x_π	x_{d^π}	x_{δ^π}	x_{i^π}	
y_π	z_{d^π}	x_{δ^π}	z_{i^π}	π odd
z_π	y_{d^π}	x_{δ^π}	y_{i^π}	π odd

Table 4: Action of generators of N by conjugation

8 Extending the representation 196884_x from N_{x0} to N_0

8.1 The action of the triality element τ on 196884_x

In order to extend the representation 196884_x from N_{x0} to N_0 it suffices to state the action of the triality element τ on the basis vectors of 196884_x. We first state the result, which

is the most important information for a programmer. Proofs are deferred to the next two subsections.

The operation of τ on the basis vectors $(ij)_1$, X_{ij} and X_{ij}^+ is given by:

$$(ii)_1 \overset{\tau}{\longmapsto} (ii)_1 \,, \tag{8.1.1}$$

$$(ij)_1 \overset{\tau}{\longmapsto} X_{ij} - X_{ij}^+ \overset{\tau}{\longmapsto} X_{ij} + X_{ij}^+ \overset{\tau}{\longmapsto} (ij)_1 \,, \quad i \neq j \,. \tag{8.1.2}$$

The operation of τ on the basis vectors $X_{d,i}^+$ and $d^\pm \otimes_1 i$ is given by:

$$X_{d,i}^+ = X_{\Omega^{\langle d,i \rangle}+P(d)d,i} \overset{\tau}{\longmapsto} (-1)^{\langle d,i \rangle} \cdot d^- \otimes_1 i \overset{\tau}{\longmapsto} \bar{d}^+ \otimes_1 i \overset{\tau}{\longmapsto} X_{d,i}^+. \tag{8.1.3}$$

Now we specify the action of τ on the remaining basis vectors $X_{d \cdot \delta}$ of 196884_x. We put $X_{d \cdot \delta}^+ = X_{\Omega^n d \cdot \delta}$ for $n = |\delta|/2$, $|d| = 8$, $\delta \in A(d, \mathcal{C})$, with $A(d, \mathcal{C}) = \{A(d, c) \mid c \in \mathcal{C}\}$, in accordance with the notation in section 6.2. Clearly all remaining basis vectors are of that shape. Let V_T be the subspace of 196884_x generated by these basis vectors. We extend V_T from a representation of N_x, with kernel K_T generated by x_f, y_f, z_f for $f \in \{-1, \pm\Omega\}$, to a representation of $\hat{N}$. Then V_T is also a representation of N. It is also a representation of N_0, because K_0 is in the kernel of V_T.

The operations of the generators $x_e, y_e, z_e, \nu_\pi, x_\tau, y_\tau$ of $\hat{N}$ on the basis vector $X_{d \cdot \delta}^+$ of V_T are given by:

$$\begin{array}{llll}
x_e: & (-1)^{C(d,e)+\langle e,\delta \rangle} X_{d \cdot \delta}^+ \,, & y_e: & (-1)^{\langle e,\delta \rangle} X_{d \cdot \delta \delta'}^+ \,, & \text{with} \quad \delta' = A(d,e) \,, \\
z_e: & (-1)^{C(d,e)} X_{d \cdot \delta \delta'}^+ \,, & \nu_\pi: & (-1)^{|\delta| \cdot |\pi|/2} X_{d^\pi \cdot \delta^\pi}^+ \,, \\
x_\tau: & (-1)^{|\delta|/2} X_{d \cdot \delta}^+ \,, & y_\tau: & \frac{1}{8} \sum_{\epsilon \in A(d,\mathcal{C})} (-1)^{|\delta \cap \epsilon|} X_{d \cdot \epsilon}^+ \,.
\end{array} \tag{8.1.4}$$

Here $|\delta|/2$ and $|\delta \cap \epsilon|$ are defined (modulo 2) for δ and ϵ as even subsets of d as in section 6.2, and $|\pi|$ is equal to 1 for odd and to 0 for even π. The sum in the expression for y_τ runs over all even subsets ϵ of d, identifying $d \setminus \epsilon$ with ϵ, so that it has 64 terms. x_τ is monomial and the action of y_τ resembles that of a Hadamard matrix, thus allowing a very efficient implementation.

The operations of x_e, y_e, z_e and x_π are obviously equal to the corresponding operations in Table 3. In section 8.3 we will show that the remaining operations in V_T a are consistent with the relations in $\hat{N}$. By Theorem 5.1 we have $\tau = y_\tau x_\tau$ and $\tau^2 = \tau^{-1} = x_\tau y_\tau$. We obtain the operation of x_π in Table 3 by using $x_\pi = x_\tau^{|\pi|} \nu_\pi$.

The operation of the triality element τ leads to an identification of the three spaces 196884_x, 196884_y and 196884_z, which is called the *dictionary* in [5], Table 2. In our notation we have the following identification of these three spaces:

Subspace	198664_x		198664_y		198664_z
V_A	$(ij)_1$	$=$	$Y_{ij} + Y_{ij}^+$	$=$	$Z_{ij} - Z_{ij}^+$
V_B	$X_{ij} - X_{ij}^+$	$=$	$(ij)_2$	$=$	$Z_{ij} + Z_{ij}^+$
V_C	$X_{ij} + X_{ij}^+$	$=$	$Y_{ij} - Y_{ij}^+$	$=$	$(ij)_3$
V_D	$(ii)_1$	$=$	$(ii)_2$	$=$	$(ii)_3$
V_X	$X_{d \cdot i}^+$	$=$	$\bar{d}^+ \otimes_2 i$	$=$	$(-1)^{\langle d,i \rangle} d^- \otimes_3 i$
V_Y	$(-1)^{\langle d,i \rangle} d^- \otimes_1 i$	$=$	$Y_{d \cdot i}^+$	$=$	$\bar{d}^+ \otimes_3 i$
V_Z	$\bar{d}^+ \otimes_1 i$	$=$	$(-1)^{\langle d,i \rangle} d^- \otimes_2 i$	$=$	$Z_{d \cdot i}^+$
V_T	$X_{d,\delta}^+$	$=$	$\frac{1}{8} \sum (-)_{\epsilon,\delta} Y_{d,\delta}^+$	$=$	$\frac{1}{8} \sum (-)_{\delta,\epsilon} Z_{d,\delta}^+$
V_T	$\frac{1}{8} \sum (-)_{\delta,\epsilon} X_{d,\delta}^+$	$=$	$Y_{d,\delta}^+$	$=$	$\frac{1}{8} \sum (-)_{\epsilon,\delta} Z_{d,\delta}^+$
V_T	$\frac{1}{8} \sum (-)_{\epsilon,\delta} X_{d,\delta}^+$	$=$	$\frac{1}{8} \sum (-)_{\delta,\epsilon} Y_{d,\delta}^+$	$=$	$Z_{d,\delta}^+$

Table 5: The dictionary

Here $(-)_{\delta,\epsilon} = (-1)^{|\delta \cap \epsilon| + |\delta|/2}$ and the sum in the last three lines runs over $\epsilon \in A(d,\mathcal{C})$.

Following [5], we also give names to the subspaces of 196884_x as indicated in table 5.

8.2 Proofs for the monomial and almost-monomial actions of τ

The purpose of this subsection is to establish (8.1.1), (8.1.2) and (8.1.3).

Using the information in Table 3, it is easy to check that the identification $(ii)_1 = (ii)_2 = (ii)_3$ in line 4 of Table 5 is compatible with the action of N_{x0}. Together with the obvious action $(ii)_1 \overset{\tau}{\mapsto} (ii)_2 \overset{\tau}{\mapsto} (ii)_3 \overset{\tau}{\mapsto} (ii)_1$ we obtain (8.1.1).

Next we show (8.1.2). The group ring $\mathbb{R}Q_{xyz0}$ is the real algebra with basis vectors labelled by Q_{xyz0}, and multiplication of the basis vectors given by the group operation in Q_{xyz0}. Since Q_{xyz0} is normal in N_0, the group N_0 operates on $\mathbb{R}Q_{xyz0}$ by conjugation.

Let V be the subspace of $98280_x \oplus 98280_y \oplus 98280_z$ spanned by $X_{f\cdot\delta}, Y_{f\cdot\delta}, Z_{f\cdot\delta}$, $f \in \{\pm 1, \pm\Omega\}$, δ even. We define a linear mapping $V \to \mathbb{R}Q_{xyz0}$ by:

$$X_{f\cdot\delta} \to x_{f\cdot\delta} - x_{-f\cdot\delta}, \quad Y_{f\cdot\delta} \to y_{f\cdot\delta} - y_{-f\cdot\delta}, \quad Z_{f\cdot\delta} \to z_{f\cdot\delta} - z_{-f\cdot\delta}.$$

The restriction of this mapping to 98280_x, to 98280_y and to 98280_z is injective and the mapping preserves the operation of N_0. So we may identify the basis vectors of V with their images in $\mathbb{R}Q_{xyz0}$. Using the relations in $Q_{xyz0} = Q_{xyz}/K_0$ given by K_0 and $x_{(ij)} = y_{(ij)} = z_{(ij)}$ we obtain:

$$
\begin{aligned}
Y_{ij} + Y_{ij}^+ = Y_{ij} + Y_{\Omega\cdot ij} &= y_{1\cdot(ij)} + y_{\Omega\cdot(ij)} - y_{-1\cdot(ij)} - y_{-\Omega\cdot(ij)} \\
&= z_{1\cdot(ij)} + z_{-\Omega\cdot(ij)} - z_{\Omega\cdot(ij)} - z_{-1\cdot(ij)} \quad = \quad Z_{ij} - Z_{ij}^+ \\
&= x_{1\cdot(ij)} + x_{-1\cdot(ij)} - x_{-\Omega\cdot(ij)} - x_{\Omega\cdot(ij)} \quad .
\end{aligned}
$$

Hence we may identify $Y_{ij} + Y_{ij}^+$ with $Z_{ij} - Z_{ij}^+$. A similar calculation yields $Z_{ij} + Z_{ij}^+ = X_{ij} - X_{ij}^+$ and $X_{ij} + X_{ij}^+ = Y_{ij} - Y_{ij}^+$. Put $(X_{ij}) = x_{1\cdot(ij)} + x_{-1\cdot(ij)} - x_{\Omega\cdot(ij)} - x_{-\Omega\cdot(ij)}$, and define (Y_{ij}), (Z_{ij}) similarly, using triality. From Table 3 we see that the action of the generators x_d, x_π and τ of N_{x0} on the vectors (X_{ij}), (Y_{ij}) and (Z_{ij}) is the same as their action on $(ij)_1$, $(ij)_2$ and $(ij)_3$, respectively. So we have just established the identifications in the first three lines of Table 5. Using these identifications and the obvious action $(ij)_1 \overset{\tau}{\mapsto} (ij)_2 \overset{\tau}{\mapsto} (ij)_3 \overset{\tau}{\mapsto} (ij)_1$ we obtain (8.1.2).

Next we show (8.1.3). This is a consequence of lines 5–7 of the dictionary in Table 5 and of the obvious operation of the triality element τ. Lines 5–7 in Table 5 are direct consequences of the following two lemmas.

Lemma 8.2. *The group N_0 has a monomial representation $(3{\cdot}49152)_N$ with basis vectors $d^\pm \otimes_m i$, $d \in \mathcal{P}$, $i \in \tilde{\Omega}$, $m = 1, 2, 3$, and the identifications*

$$(-d)^\pm = -(d^\pm), \quad (\pm\Omega d)^\pm = d^\pm, \quad \bar{d}^+ \otimes_m i = (-1)^{\langle d,i \rangle} d^- \otimes_{m+1} i,$$

where m is to be taken modulo 3, and the action of the generators of N_0 is given by table 3 and triality.

Proof

For $m = 1, 2, 3$ let $\langle d^+ \otimes_m i \rangle$ and $\langle d^- \otimes_m i \rangle$ be the vector spaces spanned by the basis vectors $d^+ \otimes_m i$ and $d^- \otimes_m i$, respectively, for $d \in \mathcal{P}$, $i \in \tilde{\Omega}$, with the identifications given by (7.1.1). Define $(6{\cdot}49152)_N$ by:

$$(6{\cdot}49152)_N = \langle d^+ \otimes_1 i \rangle \oplus \langle d^- \otimes_1 i \rangle \oplus \langle d^+ \otimes_2 i \rangle \oplus \langle d^- \otimes_2 i \rangle \oplus \langle d^+ \otimes_3 i \rangle \oplus \langle d^- \otimes_3 i \rangle$$

The six subspaces in the definition of $(6{\cdot}49152)_N$ are invariant under N_{xyz}, and the action of the kernel elements in tables 1 and 2 show that K_0 acts as identity everywhere, so $(6{\cdot}49152)_N$ is a representation of N_{xyz0}. From the actions of τ and x_i in these tables we see that both of them preserve $(6{\cdot}49152)_N$ so that this is indeed a representation of N_0.

Let $\imath$ be the involution on $(6{\cdot}49152)_N$ given by:

$$d^\pm \otimes_m i \overset{\imath}{\longmapsto} (-1)^{\langle d,i \rangle} \bar{d}^\mp \otimes_{m\pm 1} i, \quad \text{with } m \text{ to be taken modulo 3},$$

Involution $\imath$ trivially preserves the identification between $(-d)^\pm \otimes_m i$ and $-(d^\pm \otimes_m i)$. Since $\langle \Omega, i \rangle = 1$, we have

$$\imath((\Omega d)^+ \otimes_m i) = (-1)^{\langle \Omega d, i \rangle} \Omega \bar{d}^- \otimes_{m+1} i = (-1)^{\langle d, i \rangle} (-\Omega \bar{d})^- \otimes_{m+1} i$$
$$= (-1)^{\langle d, i \rangle} \bar{d}^- \otimes_{m+1} i \quad = \imath(d^+ \otimes_m i) \,.$$

A similar calculation shows $\imath(-\Omega d_m^- \otimes i_m) = \imath(d_m^- \otimes i_m)$. Thus the identifications $(\Omega d)_m^+ = d_m^+$ and $(-\Omega d)_m^- = d_m^-$ are also preserved, so that $\imath$ is well defined on $(6{\cdot}49152)_N$.

For the proof of the Lemma is suffices to show that $\imath$ commutes with the action of the generators of N_0. Using Table 3, it is trivial to check that $\imath$ commutes with τ and x_π for even π. So it remains to check that $\imath$ commutes with x_e and x_ϵ for odd ϵ, which is a tedious but straightforward calculation using Table 3. The relevant action of x_e is given in Table 6. $\square$

Lemma 8.3. *The subspace of $196884_x \oplus 196884_y \oplus 196884_z$ spanned by the basis vectors $X_{d \cdot i}$, $Y_{d \cdot i}$ and $Z_{d \cdot i}$, $d \in \mathcal{P}$, $i \in \tilde{\Omega}$, i odd, $\langle d, i \rangle = P(d)$ is a monomial representation of N_0. There is an isomorphism from that space into $(3{\cdot}49152)_N$ given by*

$$X_{d \cdot i} \mapsto \bar{d}^+ \otimes_2 i \,, \quad Y_{d \cdot i} \mapsto \bar{d}^+ \otimes_3 i \,, \quad Z_{d \cdot i} \mapsto \bar{d}^+ \otimes_1 i \,.$$

Proof

Let V be the space spanned by $X_{d \cdot i}$, $Y_{d \cdot i}$ and $Z_{d \cdot i}$. The last column in Table 3 shows that V is a representation of N_0. So we have to show that the mapping $V \to (3{\cdot}49152)_N$ given in the Lemma preserves the action of the generators, say, x_e, x_π and τ of N_0. This is trivial for τ and x_π. The operation of x_e on V and on $(3{\cdot}49152)_N$ is stated in Table 6. $\square$

Operation $B \mapsto Bx_e$ of the element x_e of N_0 on basis vectors B		
$B \mapsto Bx_e$	$B \mapsto Bx_e$	$B \mapsto Bx_e$
$X_{d \cdot i}^+ \mapsto (-1)^{\langle e, i \rangle} X_{\bar{e}de \cdot i}^+$	$\bar{d}^+ \otimes_2 i \mapsto (-1)^{\langle e, i \rangle} (\bar{e}\bar{d}e)^+ \otimes_2 i$	$d^- \otimes_3 i \mapsto (-1)^{\langle e, i \rangle} (\bar{e}de)^- \otimes_3 i$
$Y_{d \cdot i}^+ \mapsto (-1)^{\langle e, i \rangle} Y_{\bar{e}d \cdot i}^+$	$\bar{d}^+ \otimes_3 i \mapsto (-1)^{\langle e, i \rangle} (\bar{d}e)^- \otimes_3 i$	$d^- \otimes_1 i \mapsto (\bar{e}d)^- \otimes_1 i$
$Z_{d \cdot i}^+ \mapsto Z_{de \cdot i}^+$	$\bar{d}^+ \otimes_1 i \mapsto (\bar{e}\bar{d})^+ \otimes_1 i$	$d^- \otimes_2 i \mapsto (-1)^{\langle e, i \rangle} (de)^- \otimes_2 i$

Table 6: Operation of x_e on some basis vectors of $196884_x \oplus 196884_y \oplus 196884_z$.
Entries in the same row are equivalent (up to sign) with respect to the dictionary in Table 5.

8.3 The proof for the non-monomial action of τ

In this subsection we will show that V_T is a representation of $\hat{N}$ with the operation of the generators of $\hat{N}$ given by (8.1.4). We already know from section 8.1 that V_T represents N_x with kernel K_T. In the sequel the generators $x_d, y_d, z_d, x_\delta, x_\tau, y_\tau$ denote the linear operation of the corresponding generator on V_T, and we put $\nu_\pi = x_\pi x_\tau^{|\pi|}$. Our goal is to establish the defining relations for $\hat{N}/K_T$ in V_T, with the relations between the generators of N_x already established in V_T.

By construction x_τ and y_τ act as real symmetric orthogonal matrices on V_T, establishing $x_\tau^2 = y_\tau^2 = 1$. Note that y_τ consists of 64×64 blocks, one for each d, and each of these blocks can easily be checked to by symmetric and orthogonal.

From $\nu_\pi = x_\pi x_\tau^{|\pi|}$ and the operation of x_π and x_τ in (8.1.4) we conclude that ν_π maps $X_{d \cdot \delta}^+$ to $X_{d^\pi \cdot \delta^\pi}^+$ also for odd $\pi \in \mathrm{Aut}_{\mathrm{St}} \mathcal{P}$, Thus for any odd diagonal automorphism $\varphi \in \mathcal{C}^*$ the element ν_φ acts by multiplication with ± 1 on each 64-dimensional block of V_T corresponding to a fixed d. Thus ν_φ commutes with x_d, y_d, z_d, x_δ for all $d \in \mathcal{C}$, $\delta \in \mathcal{C}^*$ and also with x_τ and y_τ. From the operation of ν_π on $X_{d \cdot \delta}^+$ in V_T we conlude $\nu_\pi \nu_{\pi'} = \nu_{\pi\pi'}$ for all $\pi, \pi' \in \mathrm{Aut}_{\mathrm{St}} \mathcal{P}$. With this information we easily check that the involution ν_φ acts on the representation V_T

of N_x by conjugation in the same way the element ν_φ of $\hat{N}$ acts on the group N_x. Thus V_T represents the subgroup $\hat{N}_x$ of $\hat{N}$ generated by N_x and ν_φ, φ odd.

So V_T also represents the normal subgroup $\hat{N}_{xyz}$ of $\hat{N}$ generated by N_{xyz} and ν_φ, φ odd. We claim that the involution y_τ acts on the representation V_T of $\hat{N}_{xyz}$ by conjugation in the same way as the element y_τ of $\hat{N}$ acts on the normal subgroup $\hat{N}_{xyz}$ of $\hat{N}$. By (8.1.4), y_τ commutes with all x_π, π even. We have already shown that y_τ commutes with an odd x_φ, hence it commutes with all ν_π, establishing the claim for all generators ν_π.

To prove our claim, we will show that $y_\tau x_e = z_e y_\tau$ holds in V_T. To see this, note that

$$X_{d\cdot\delta}^+ \overset{x_e y_\tau z_e}{\longmapsto} \tfrac{1}{8} \sum_{\epsilon \in A(d,\mathcal{C})} (-1)^{\langle e,\delta\rangle + |\delta \cap \epsilon|} X_{d\cdot\epsilon A(d,e)}^+ = \tfrac{1}{8} \sum_{\epsilon \in A(d,\mathcal{C})} (-1)^{m(\epsilon)} X_{d\cdot\epsilon}^+,$$

with $m(\epsilon) = |\delta \cap (\epsilon + A(d,e))| + \langle e, \delta\rangle = |\delta \cap \epsilon| + |\delta \cap d \cap e| + |\delta \cap e| = |\delta \cap \epsilon|$ (mod 2). Hence $x_e y_\tau z_e = y_\tau$, implying $y_\tau x_e = z_e y_\tau$. Together with the relations already established in V_T we obtain $y_\tau x_e y_\tau = z_e$, $y_\tau z_e y_\tau = x_e$ and $y_\tau y_e y_\tau = y_e$, implying our claim. So V_T also represents the group $\hat{N}_y$ generated by $\hat{N}_{xyz}$ and y_τ.

Thus V_T represents an extension with normal subgroup $\hat{N}_{xyz}$ and factor group generated by the involutions x_τ and y_τ, where x_τ and y_τ operate on $\hat{N}_{xyz}$ by conjugation in V_T in the same way as in $\hat{N}$. $\hat{N}$ has structure $\hat{N}_{xyz} : S_3$ with S_3 the symmetric permutation group of three elements generated by x_τ and y_τ. So in order to show that V_T represents $\hat{N}$ it suffices to show $\tau^3 = 1$ (with $\tau = x_\tau y_\tau$) in V_T.

Since $\tau^3 = 1$ in $\hat{N}$ and conjugation with τ in V_T is the same as in $\hat{N}$, the matrix τ^3 in V_T centralizes all generators in V_T. By construction the generators x_e, y_e and τ consist of blocks of 64×64 matrices, with one block for each octad d. Thus for each d the block of τ^3 corresponding to d centralizes the blocks of all matrices x_e and y_e corresponding to the same d. It is easy to see that for any such d the corresponding blocks of the matrices x_e and y_e generate the complete ring of all 64×64 matrices. So the block of τ^3 corresponding to d is a multiple of the identity matrix, and since τ is orthogonal, that block of matrix τ^3 is equal to ± 1. The trace of that block of matrix τ is equal to $\tfrac{1}{8} \sum_{\epsilon \in A(d,\mathcal{C})} (-1)^{|\epsilon|/2} = \tfrac{1}{8}(36 - 28) = 1$. It is easy to check that a real 64×64-matrix τ with $\tau^3 = -1$ has eigenvalues $-1, (1 \pm \sqrt{-3})/2$ and hence trace equal to -1 (mod 3). This establishes $\tau^3 = 1$ in V_T.
$\square$

9 Extending representation 196884_x from N_{x0} to $2_+^{1+24}.\mathbf{Co}_1$

In this section we extend the representation of 196884_x from N_{x0} to a maximal subgroup G_{x0} (with structure $2_+^{1+24}.\mathrm{Co}_1$) of the monster $\mathbb{M}$. It turns out that such an extension is possible for each of the building blocks 24_x, 4096_x and 98280_x of 196884_x. For an optimized computer construction of $\mathbb{M}$ we need an explicit representation of a $\xi \in G_{x0} \setminus N_{x0}$ in all these building blocks such that N_{x0} and ξ generate G_{x0}. Note that [5] contains an explicit construction of N_0, but no construction any specific $\xi \in \mathbb{M} \setminus N_0$. Here the hardest part is the extension of N_0 to G_{x0} and the construction of a suitable element ξ in the representation 4096_x.

We first describe the representation theory of the extraspecial 2 group 2_+^{1+2n} and of certain extensions of such groups called *holomorphs* in [12] and [14]. In section 9.2 we present N_{x0} as a central quotient of a fiber product corresponding to the faithful representation $4096_x \otimes 24_x$ of N_{x0}. In section 9.3 we extend that fiber product to the group G_{x0}. In sections 9.4 ff. we give an explicit construction of a suitable $\xi \in G_{x0} \setminus N_{x0}$ of order 3 and of its representation. The action of ξ and ξ^2 on the components of 196884_x is stated in Lemma 9.5 for 98304_x, in Corollary 9.11 for 24_x, and in in Corollary 9.16 for 4096_x.

9.1 Extraspecial 2-groups and their representations

Recall the definition of quadratic, bilinear any symplectic forms on vector spaces over $\mathbb{F}_2$ from section 3.3. Symplectic bilinear or non-singular quadratic forms exist only on spaces $\mathbb{F}_2^{2n}$ of even dimension. A quadratic form q on $\mathbb{F}_2^{2n}$ is of *plus type* if it is non-singular and there is an n-dimensional subspace V of $\mathbb{F}_2^{2n}$ with $q(x) = 0$ for all $x \in V$. It is known that all quadratic forms of plus type on $\mathbb{F}_2^{2n}$ are equivalent under the linear group $\mathrm{SL}_{2n}(2)$.

A finite 2-group E is said to be *extraspecial* if its center $Z(E)$ has order 2, the factor group $E/Z(E)$ is elementary abelian, and the commutator group $[E, E]$ of E is contained in $Z(E)$. We usually write -1 for the non-identity element in $Z(E)$, so $Z(E) = \{\pm 1\}$. The elementary Abelian 2-group $E/\{\pm 1\}$ may be regarded as vector space over $\mathbb{F}_2$.

Define $P : E/\{\pm 1\} \to \mathbb{F}_2$ by $x^2 = (-1_E)^{P(x)}$, $x \in E$. Then P is well-defined on $E/\{\pm 1\}$, and by (23.10) in [3], P is a non-singular quadratic form on the vector space $E/\{\pm 1\}$, and we have $[x, y] = (-1)^{\beta_P(x,y)}$ for all $x, y \in E$, with β_P symplectic. Thus E has order 2^{2n+1}.

An extraspecial 2-group E is of plus type if the corresponding quadratic form P on $E/\{\pm 1\}$ is of plus type. For any $n \in \mathbb{N}$ there is a unique extraspecial 2-group of order 2^{1+2n} of plus type denoted by 2_+^{1+2n}.

The remainder of this subsection deals with the representation theory of 2_+^{1+2n} and of certain extensions of that group.

Let E be an extraspecial 2-group of type 2_+^{1+2n}. We write $\mathbb{R}E$ for the group ring of E over the real field $\mathbb{R}$. So $\mathbb{R}E$ is a real algebra with the elements of E as basis vectors, and the basis vectors are multiplied as in E. Let $\mathbb{R}E^{\pm}$ be the quotient algebra of $\mathbb{R}E$, where we identify the real number -1 with element -1 of $Z(E)$. It is well known that the irreducible complex representations of the group 2_+^{1+2n} consist of a unique faithful real 2^n-dimensional representation and of 2^{2n} real one-dimensional representations of the elementary Abelian 2 group $G/\{\pm 1\}$, see e.g. [10]. So it is obvious that $\mathbb{R}E^{\pm}$ is isomorphic to the unique faithful irreducible real representation of E.

A *holomorph* of a group E is an extension with normal subgroup E and factor group $\mathrm{Out}\, E$, where $\mathrm{Out}\, E$ is the group of outer automorphisms of E, see [10, 12, 14]. We remark that the meaning of the term 'holomorph' in [12] and [14] differs from the meaning of that term in the older group-theoretic literature. If E is of type 2_+^{1+2n}, the group $\mathrm{Out}\, E$ is the orthogonal group $\mathrm{O}_{2n}^+(2)$. Here the orthogonal group $\mathrm{O}_{2n}^+(2)$ preserves the quadratic form P of plus type on the vector space $E/\{\pm 1\}$ defined above. There is a unique holomorph $\mathfrak{H}(E)$ of the group $E = 2_+^{1+2n}$ which has a faithful 2^n-dimensional real representation, called the *standard holomorph* of E, see [10], Appendix 1 or [14], Lemma 1.4.2. Since $\mathbb{R}E^{\pm}$ is isomorphic to the unique faithful irreducible representation of E of dimension 2^n, it is the restriction of the 2^n–dimensional real representation of $\mathfrak{H}(E)$ to E. Schur's lemma implies that an element of $\mathbb{R}E^{\pm}$ which acts as an automorphism on E is determined by that action up to a scalar multiple, which must be ± 1.

The following lemma helps us to construct elements of the standard holomorph $\mathfrak{H}(E)$:

Lemma 9.1. *Let $E = 2_+^{1+2n}$ and $H \subset E$ an elementary Abelian 2-group not containing -1. We consider H and $E/\{\pm 1\}$ as vector spaces over $\mathbb{F}_2$. Let*

$$\xi = |H|^{-1/2} \sum_{z \in H} (-1)^{q(z)} z$$

be an element of $\mathbb{R}E^{\pm}$, with q a non-singular quadratic form on H with associated bilinear form β_q.

Then $\xi^2 = 1$ and there is a unique linear mapping $\phi : E/\{\pm 1\} \to H$ with $[x, y] = (-1)^{\beta_q(\phi(x), y)}$ for all $x \in E$, $y \in H$. For all $x \in E$ we have

$$[x, \xi] = (-1)^{q(\phi(x))} \phi(x) \in Z(E) \cdot H .$$

Proof

$$|H|x^{-1}\xi x\xi = \sum_{y,z\in H} x^{-1}(-1)^{q(y)}yx(-1)^{q(z)}z = \sum_{y,z\in H}(-1)^{q(y)+q(z)}[x,y]yz$$

$$= \sum_{y,z\in H}(-1)^{q(y)+q(yz)}[x,y]z = \sum_{z\in H}(-1)^{q(z)}z\sum_{y\in H}(-1)^{\beta_q(z,y)+C(x,y)}\ ,$$

where C is the bilinear form on $E/\{\pm 1\}$ with $[x.y] = (-1)^{C(x,y)}$. Since both, $\beta_q(z,y)$ and $C(x,y)$ are linear in y, the last sum over y is equal to $|H|$ if $\beta_q(z,y) = C(x,y)$ for all $y \in H$ and zero otherwise. Since β_q is non-singular, it follows from linear algebra that for each $x \in E/\{\pm 1\}$ there is a unique $z \in H$ with $\beta_q(z,y) = C(x,y)$ for all $y \in H$, and that the mapping ϕ which maps each $x \in E/\{\pm 1\}$ to that value z is linear. This proves $x^{-1}\xi x\xi = (-1)^{q(z)}z$, with $z = \phi(x)$. In case $x = 1$ we have $\phi(x) = 0$, obtaining $\xi^2 = 1$, and hence $[x,\xi] = (-1)^{q(z)}z$.

□

Conjugation with an element ξ of $\mathbb{R}E^{\pm}$ constructed in Lemma 9.1 is an automorphism of E, since $[x,\xi] \in E$ for all $x \in E$. Hence ξ represents an element of $\mathfrak{H}(E)$. $\mathbb{R}E^{\pm}$ is a faithful irreducible representation of E and also of $\mathfrak{H}(E)$. So we may identify the element ξ of $\mathbb{R}E^{\pm}$ with the element of $\mathfrak{H}(E)$ represented by ξ.

Remark

In Lemma 9.1, ξ operates on the vector space $V = E/\{\pm 1\}$ by conjugation as an orthogonal transformation with $\operatorname{im}(\xi - 1) = H$. The coset ξE of E can be considered as an element of $\mathfrak{H}(E)/E \cong O_{2n}^+$, and the bilinear form β_q is uniquely determined by the coset ξE. For each element X of an orthogonal group operating on a vector space V, Wall [17] has defined a nondegenerate bilinear form F_X on the image of $X - 1$ in V called the *parametrization* of X. It can be shown that β_q is just Wall's parametrization of ξE.

9.2 N_{x0} is a central quotient of a fiber product

In section 7 we have constructed representations 4096_x and 24_x of the group N_x which both are also representations of $N_{x1} = N_x/K_1$. By Tables 1 and 2 the kernels $K(4096_x)$ and $K(24_x)$ of these two representations of N_x intersect in K_1. Let $N(4096_x) = N_x/K(4096_x)$ and $N(24_x) = N_x/K(24_x)$ be the quotients of N_x for which the representations 4096_x and 24_x are faithful. Put $N_x^* = N_x//(K(4096_x)K(24_x))$. Then

$$N_x^* \cong N(4096_x)/(K(24_x)/K_1) \cong N(24_x)/(K(4096_x)/K_1)\,,$$
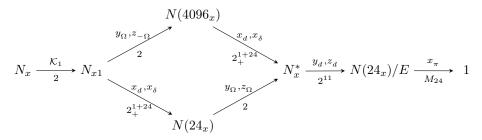
where e.g. the natural injection from $K(24_x)/K_1$ into $N(4096_x)$ is obtained by extending the coset xK_1 to xK_{4096} for $x \in K(24_x)$.

Then N_{x1} is isomorphic to the fiber product $N(4096_x) \triangle_{N_x^*} N(24_x)$. If G_1, G_2 are groups with a common factor group H and homomorphisms $\phi_i : G_i \to H$, $i = 1,2$, then the fiber product $G_1 \triangle_H G_2$ is the subgroup of the direct product $G_1 \times G_2$ defined by:

$$G_1 \triangle_H G_2 = \{(x,y) \in G_1 \times G_2 \mid \phi_1(x) = \phi_2(y)\}\ .$$

If G_i has a center $\{\pm 1_i\}$ of order 2 for $i = 1,2$, then we write $\frac{1}{2}(G_1 \triangle_H G_2)$ for the quotient of $G_1 \triangle_H G_2$ by $\{(1_1, 1_2), (-1_1, -1_2)\}$ as in [6]. Since $\mathcal{K}_2$ and $\mathcal{K}_3$ act as -1 in both, 4096_x and 24_x, the group N_{x0} is isomorphic to $\frac{1}{2}(N(4096_x) \triangle_{N_x^*} N(24_x))$.

The following diagram, which is essentially a copy of Fig. 2 in [5], depicts the homomorphisms from N_x to the various factor groups of N_x defined above. For each homomorphism we show a generating system and the structure of the corresponding factor group.

$$
\begin{array}{ccccccccc}
&& N(4096_x) &&&&&& \\
& \nearrow{\scriptstyle y_\Omega, z_{-\Omega}} \atop {\scriptstyle 2} && \searrow{\scriptstyle x_d, x_\delta} \atop {\scriptstyle 2^{1+24}_+} &&&& \\
N_x \xrightarrow[2]{\;\mathcal{K}_1\;} N_{x1} &&&& N_x^* \xrightarrow[2^{11}]{\;y_d, z_d\;} N(24_x)/E \xrightarrow[M_{24}]{\;x_\pi\;} 1 \\
& \searrow{\scriptstyle x_d, x_\delta} \atop {\scriptstyle 2^{1+24}_+} && \nearrow{\scriptstyle y_\Omega, z_\Omega} \atop {\scriptstyle 2} &&&& \\
&& N(24_x) &&&&&&
\end{array}
$$

From (5.3.2) we see that $N(4096_x)$ has structure $2^{1+24}_+.2^{11}.M_{24}$, $N(24_x)$ has structure $2^{12} : M_{24}$ and N_x^* has structure $2^{11} : M_{24}$. The relations (5.3.5) show that the subgroup Q_x of N_x generated by x_d, x_δ has structure 2^{1+24}_+. Note that $|Q_x \cap K_1| = 1$, so Q_x is also isomorphic to a subgroup of N_{x1}.

By construction, $N(24_x)$ acts as a matrix group on $\mathbb{R}^{24}$ with coordinates labelled by $\tilde{\Omega}$. $N(24_x)$ has an elementary Abelian normal subgroup E of order 2^{12}. An element of E corresponds to the negation of the coordinates given by a codeword of $\mathcal{C}$, hence $E \cong \mathcal{C}$. The permutation representation of M_{24} acts as a complement of E in $N(24_x)$.

9.3   The maximal subgroup $G_{x0} = 2^{1+24}_+.\mathrm{Co}_1$ of $\mathbb{M}$

As in [5], we will enlarge $N(4096_x)$ and $N(24_x)$ to larger groups of $G(4096_x)$ and $G(24_x)$ of structure $2^{1+24}.\mathrm{Co}_1$ and $2.\mathrm{Co}_1$, respectively. From this we obtain the group $G_{x0} = \frac{1}{2}(G(4096_x) \triangle_{\mathrm{Co}_1} G(24_x))$, which is a maximal subgroup of the monster.

The group $N(4096_x) = N_{x1}/K(4096_x)$ defined in section 9.2 has the faithful irreducible real representation 4096_x. 4096_x is also faithful and irreducible for the extraspecial subgroup Q_x of type 2^{1+24}_+ of $N(4096_x)$ and hence also for the standard holomorph $\mathfrak{H}(Q_x)$ of Q_x .

By Theorem 6.1 the quotient of Q_x by its center is isomorphic to $\Lambda/2\Lambda$, and the squaring map in Q_x is equal to the mapping $\Lambda/2\Lambda \to \mathbb{F}_2$ given by $\lambda \mapsto \mathrm{type}(\lambda) = \langle \lambda, \lambda \rangle /2$. This 'type' mapping is a quadratic form on $\Lambda/2\Lambda$ by construction, which is invariant under the automorphism group Co_1 of $\Lambda/2\Lambda$. It is of plus type by (5.3.5), so Co_1 is a subgroup of $O_2^+(24)$. The factor group N_x^* of $N(4096_x)$ with structure $2^{11}.M_{24}$ is isomorphic to the monomial subgroup of the automorphism group Co_1 of $\Lambda/2\Lambda$. This leads to a chain of inclusions

$$
\begin{array}{ccccccc}
& Q_x & \subset & N(4096_x) & \subset & G(4096_x) & \subset & \mathfrak{H}(Q_x) \\
\text{with structures} & 2^{1+24}_+ & \subset & 2^{1+24}_+.2^{11}.M_{24} & \subset & 2^{1+24}_+.\mathrm{Co}_1 & \subset & 2^{1+24}_+.O_{24}^+(2)\,.
\end{array}
$$

There is a similar chain of inclusions of groups

$$
\begin{array}{ccccccc}
& E & \subset & N(24_x) & \subset & G(24_x) & \subset & \mathrm{SO}_{24}(\mathbb{R}) \\
\text{with structures} & 2^{12} & \subset & 2^{12}.M_{24} & \subset & 2.\mathrm{Co}_1 &.
\end{array}
$$

Here the group $G(24_x)$ is the automorphism group of the Leech lattice Λ, and $N(24_x)$ is the monomial subgroup of that group. So the groups $G(4096_x)$ and $G(24_x)$ possess natural homomorphisms onto Co_1 which are extensions of the homomorphisms from $N(4096_x)$ and $N(24_x)$ onto $N_x^* = 2^{12} : M_{24}$. We can therefore extend the fiber product N_{x1} of $N(4096_x)$ and $N(24_x)$ to the fiber product

$$
G_{x1} = G(4096_x) \triangle_{\mathrm{Co}_1} G(24_x)\,.
$$

This group has representations of degrees 4096 and 24 extending the representations 4096_x and 24_x, which we will also call 4096_x and 24_x. The tensor product $4096_x \otimes 24_x$ identifies the centers $\{\pm 1\}$ of both of its factors and is hence is a representation of

$$
G_{x0} = \tfrac{1}{2}\left(G(4096_x) \triangle_{\mathrm{Co}_1} G(24_x)\right)\,.
$$

The group G_{x0} is the maximal subgroup of the monster $\mathbb{M}$ constructed in [5]. The groups G_{x0} and $G(4096_x)$ are both of structure $2^{1+24}.\text{Co}_1$, but not isomorphic, see e.g. [10, 14].

We have found representations 4096_x and 24_x of G_{x1}. This leads to representations $98304_x = 4096_x \otimes 24_x$ and $300_x = 24_x \otimes_{\text{sym}} 24_x$ of G_{x0}. G_{x0} (as a extension of its normal subgroup Q_x) permutes the short elements x_r of Q_x via conjugation. Thus the representation 98280_x of N_{x0} can also be extended to a monomial representation of G_{x0}, which we will also call 98280_x. So we may build a representation 196884_x of G_{x0} from its components in the same way as in the case of N_x.

9.4 Construction of a $\xi \in G_{x0} \setminus N_{x0}$ and operation of ξ on 98280_x

It remains to construct a specific element $\xi \in G_{x0} \setminus N_{x0}$. By [6], $2^{11} : M_{24}$ is maximal in Co_1, so N_{x0} is maximal in G_{x0}, and hence any $\xi \in G_{x0} \setminus N_{x0}$ together with N_{x0} generates G_{x0}.

4096_x is also a faithful irreducible representation of $Q_x = 2^{1+24}$, so $\hom(4096_x, 4096_x)$ is isomorphic to $\mathbb{R}Q_x^\pm$ as an algebra. Thus we may define ξ as an element $\xi = \xi_{4096} \otimes \xi_{24}$ of $\mathbb{R}Q_x^\pm \otimes \hom(24_x, 24_x)$. Conjugation of Q_x with ξ_{4096} may be computed by Lemma 9.1. The action of ξ_{4096} determines the action of ξ in 98280_x uniquely and in 24_x up to sign. We will construct a specific element ξ_{4096} or order 3. Then we let ξ_{24} be the unique element of order 3 corresponding to ξ_{4096}, i.e. $-\xi_{24}$ has order 6. In the sequel we will abbreviate ξ_{4096} to ξ.

The decompositions $\mathcal{C} = \mathcal{G} \oplus \mathcal{H}$ and $\mathcal{C}^* = \mathcal{G}^* \oplus \mathcal{H}^*$ of $\mathcal{C}$ and $\mathcal{C}^*$ into grey and coloured subspaces discussed in section 2.2 is useful for describing the action of ξ.

Recall from section 2.2 that $\mathcal{G}$ has a natural basis $g_0, \ldots, g_5$ and that $\mathcal{G}^*$ has a natural basis $\gamma_0, \ldots, \gamma_5$. Let $w : \mathcal{G} \cup \mathcal{G}^* \to \mathbb{Z}$ be the weight of a vector in the corresponding natural basis, as in Definition 2.4. Let $w_2 : \mathcal{G} \cup \mathcal{G}^* \to \mathbb{F}_2$ as in (3.7.1). So $w_2(d) = \binom{w(d)}{2} \pmod 2$. Let $\gamma : \mathcal{C} \to \mathcal{G}^*$ be as in (3.5.2). By Lemma 3.8, w_2 is a non-singular quadratic form on $\mathcal{G}$ with associated bilinear form

$$\beta_{w_2} = \langle\!\langle .,. \rangle\!\rangle \,, \qquad \text{where} \quad \langle\!\langle d, e \rangle\!\rangle = \langle d, \gamma(e) \rangle = \langle e, \gamma(d) \rangle \,. \qquad (9.2.1)$$

By (3.5.3) the restriction of γ to $\mathcal{G}$ is an isomorphism $\mathcal{G} \to \mathcal{G}^*$ with $\gamma(g_i) = \gamma_i$. Thus the mapping $w_2 : \mathcal{G}^* \to \mathbb{F}_2$ is also a non-singurlar quadratic form on $\mathcal{G}^*$. We also define the bilinear form $\langle\!\langle .,. \rangle\!\rangle$ on $\mathcal{G}^*$ by decreeing $\langle\!\langle \delta, \epsilon \rangle\!\rangle = \beta_{w_2}(\delta, \epsilon)$.

For $d \in \mathcal{C}$ (or $d \in \mathcal{P}$) let $\tilde{x} = x_{(\tilde{d},0)} x_{\theta(d)}$ be as in (5.3.4). Then $\{x_\epsilon \mid \epsilon \in \mathcal{G}^*\}$ and $\{\tilde{x}_e \mid e \in \mathcal{G}\}$ are elementary Abelian subgroups of Q_x not containing the central element x_{-1} of Q_x. In order to construct the *three-bases* element ξ we put $\xi = \xi_\gamma \xi_g \in \mathbb{R}G^\pm$ with

$$\xi_\gamma = \frac{1}{8} \sum_{\epsilon \in \mathcal{G}^*} (-1)^{w_2(\epsilon)} x_\epsilon \,, \quad \xi_g = \frac{1}{8} \sum_{e \in \mathcal{G}} (-1)^{w_2(e)} \tilde{x}_e \,. \qquad (9.3.1)$$

By Lemma 3.8 and (9.2.1), w_2 is a non-singular quadratic form on $\mathcal{G}$ and also on $\mathcal{G}^*$. Thus by Lemma 9.1, ξ_γ and ξ_g are involutions in the holomorph $\mathfrak{H}(Q_x)$, so they both normalize Q_x.

ξ_γ and ξ_g are in $\mathfrak{H}(Q_x)$ but not in $G(4096_x)$. In section 9.5 we will show that the product $\xi = \xi_\gamma \xi_g$ is in $G(4096_x)$ as required. The relevant relations for ξ_γ and ξ_g are given by:

Lemma 9.4.

$$\xi_\gamma^2 = \xi_g^2 = (\xi_\gamma \xi_g)^3 = [\tilde{x}_e, \xi_g] = [x_\epsilon, \xi_\gamma] = 1 \,, \quad e \in \mathcal{C}, \, \epsilon \in \mathcal{C}^* \,;$$
$$[\tilde{x}_h, \xi_\gamma] = [x_\eta, \xi_g] = 1 \,, \quad h \in \mathcal{H}, \, \eta \in \mathcal{H}^* \,;$$
$$\tilde{x}_d^{\xi_\gamma} = x_\delta^{\xi_g} = (-1)^{w_2(d)} \tilde{x}_d x_\delta \,, \quad [\tilde{x}_d, x_\delta] = 1 \,, \quad d = \mathcal{G}, \, \delta = \gamma(d) \in \mathcal{G}^* \,.$$

Proof

We have already shown $\xi_\gamma^2 = \xi_g^2 = 1$. Put $\tilde{x}_r = \tilde{x}_{e \cdot \epsilon}$ for $r = (e, \epsilon) \in \mathcal{C} \times \mathcal{C}^*$. We define a scalar product $\langle ., . \rangle$ on $(\mathcal{C} \times \mathcal{C}^*) \times (\mathcal{C} \times \mathcal{C}^*)$ by decreeing $\langle (e, \epsilon), (f, \varphi) \rangle = \langle e, \varphi \rangle + \langle f, \epsilon \rangle$. Then (5.3.5) implies

$$[\tilde{x}_r, \tilde{x}_s] = (-1)^{\langle r, s \rangle}, \qquad \text{for} \quad r, s \in \mathcal{C} \times \mathcal{C}^* .$$

Thus $\tilde{x}_r$, $r \in \mathcal{H} \times \mathcal{C}^*$, commutes with every term $\tilde{x}_s$, $s \in \mathcal{G}^*$ in the sum that defines ξ_γ. Hence $\tilde{x}_r$ commutes with ξ_γ. A similar argument shows that $\tilde{x}_r$, $r \in \mathcal{C} \times \mathcal{H}^*$, commutes with ξ_g.

Next we show the formula for $\tilde{x}_d^{\xi_\gamma}$. Let $\phi_\gamma : Q_x / \{\pm 1\} \to \mathcal{G}^*$ be the linear mapping given by $\phi_\gamma(\tilde{x}_{g_n}) = \gamma_n$, $\phi_\gamma(\tilde{x}_r) = 0$, $r \in \mathcal{H} \times \mathcal{C}^*$. Then

$$[\tilde{x}_r, x_\delta] = (-1)^{\langle r, \delta \rangle} = (-1)^{\langle\!\langle \phi_\gamma(\tilde{x}_r), \delta \rangle\!\rangle} \qquad \text{for} \quad r \in \mathcal{C} \times \mathcal{C}^* .$$

Since $\langle\!\langle ., . \rangle\!\rangle$ is the bilinear form associated with w_2, the last equation and Lemma 9.1 imply:

$$[\tilde{x}_d, \xi_\gamma] = (-1)^{w_2(\phi_\gamma(\tilde{x}_d))} x_{\phi_\gamma(\tilde{x}_d)} = (-1)^{w_2(d)} x_\delta .$$

The proof of the formula for $x_\delta^{\xi_g}$ is similar. Let $\phi_g : Q_x / \{\pm 1\} \to \mathcal{G}$ be the linear mapping given by $\phi_g(\tilde{x}_{\gamma_n}) = g_n$, $\phi_g(\tilde{x}_r) = 0$, $r \in \mathcal{C} \times \mathcal{H}^*$. Then

$$[\tilde{x}_r, x_d] = (-1)^{\langle r, d \rangle} = (-1)^{\langle\!\langle \phi_g(\tilde{x}_r), d \rangle\!\rangle} \qquad \text{for} \quad r \in \mathcal{C} \times \mathcal{C}^* .$$

This equation together with Lemma 9.1 implies:

$$[x_\delta, \xi_\gamma] = (-1)^{w_2(\phi_g(x_\delta))} x_{\phi_g(\tilde{x}_r)} = (-1)^{w_2(\delta)} \tilde{x}_d = (-1)^{w_2(d)} \tilde{x}_d .$$

Since $\langle\!\langle ., . \rangle\!\rangle$ is associated with the quadratic form w_2 and hence alternating we have:

$$[\tilde{x}_d, x_\delta] = (-1)^{\langle d, \delta \rangle} = (-1)^{\langle\!\langle d, d \rangle\!\rangle} = 1 .$$

It remains to show $(\xi_\gamma \xi_g)^3 = 1$. This follows from $\xi_\gamma^2 = \xi_g^2 = 1$ and

$$8 \xi_g^{\xi_\gamma} = \sum_{d \in \mathcal{G}} (-1)^{w_2(d)} \tilde{x}_d^{\xi_\gamma} = \sum_{d \in \mathcal{G}} \tilde{x}_d x_\delta = \sum_{\delta \in \mathcal{G}^*} x_\delta \tilde{x}_d = \sum_{\delta \in \mathcal{G}^*} (-1)^{w_2(\delta)} x_\delta^{\xi_g} = 8 \xi_\gamma^{\xi_g} .$$

$\square$

By Lemma 9.4, $\xi = \xi_\gamma \xi_g$ operates on $\tilde{x}_d$, $\in \mathcal{G}$ by conjugation as follows:

$$\tilde{x}_d \overset{\xi}{\longmapsto} x_{\gamma(d)} \overset{\xi}{\longmapsto} (-1)^{w_2(d)} \tilde{x}_d x_{\gamma(d)} \overset{\xi}{\longmapsto} \tilde{x}_d . \tag{9.4.1}$$

Figure 2: Action of ξ_γ and ξ_g on $\tilde{x}_d \in \mathcal{G}$ and on $x_\delta = \gamma(x_d) \in \mathcal{G}^*$.

Lemma 9.5. *Let $d, e \in \mathcal{G}$, $h \in \mathcal{P}_\mathcal{H}$, $\eta \in \mathcal{H}^*$. Put $\delta = \gamma(d)$, $\epsilon = \gamma(e)$. Then ξ operates by conjugation on Q_x as follows:*

$$\tilde{x}_d \tilde{x}_h x_\epsilon x_\eta \overset{\xi}{\longmapsto} (-1)^{w_2(e) + \langle\!\langle d, e \rangle\!\rangle} \tilde{x}_e \tilde{x}_h x_{\delta \epsilon} x_\eta \tag{9.5.1}$$

$$\tilde{x}_d \tilde{x}_h x_\epsilon x_\eta \overset{\xi^2}{\longmapsto} (-1)^{w_2(d) + \langle\!\langle d, e \rangle\!\rangle} \tilde{x}_{de} \tilde{x}_h x_\delta x_\eta \tag{9.5.2}$$

$$x_h x_{\gamma(h)} \overset{\xi}{\longmapsto} x_h x_{\gamma(h)} \tag{9.5.3}$$

Proof

By Lemma 9.4, conjugation with ξ fixes $\tilde{x}_h$ and x_η. So (9.5.1) and (9.5.2) follow from (9.4.1) and from the commutator rules in (5.3.5).

ξ does not depend on the cocycle θ, provided that θ satisfies Lemma 3.9, So by Corollary 3.10 we may assume $\theta(h) = \gamma(h)$ and hence $\tilde{x}_h = x_h x_{\gamma(h)}$. Then (9.5.3) follows from (9.5.1).
$\square$

Every element x_r of Q_x is of shape $\pm\tilde{x}_d\tilde{x}_h x_\epsilon x_\eta$ as given by Lemma 9.5. So that Lemma allows us to conjugate any such x_r with ξ or ξ^2. ξ operates on the basis vector X_r of the representation 98280_x in the same way as it operates on x_r by conjugation. So Lemma 9.5 also gives us the operation of ξ and ξ^2 on 98280_x.

9.5 The operation of ξ on 24_x

We also define a linear transformation $\xi_{24} = \xi_{24a}\xi_{24b}$ on 24_x, where ξ_{24a} and ξ_{24b} are 24×24 matrices operating on 24_x by right multiplication. Matrices ξ_{24a} and ξ_{24b} consist of six identical 4×4–blocks ξ_{4a} and ξ_{4b}, respectively, where each of the 4×4–blocks transforms the four basis vectors of 24_x labelled by a column of the MOG, as given in (2.1.1). We put:

$$\xi_{4a} = \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}, \quad \xi_{4b} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{9.5.4}$$

We define $\Lambda^E = \{\lambda \in \Lambda \mid \langle \lambda_{\tilde{\Omega}}, \lambda \rangle = \langle \lambda_\omega, \lambda \rangle = 0 \pmod 2\}$, with $\tilde{\Omega} \in \mathcal{G}, \omega \in \mathcal{G}^*$ as in section 2. Then Λ^E is a sublattice of Λ of index 4.

ξ_{4a} and ξ_{4b} are orthogonal by construction. Thus ξ_{24a}, ξ_{24b} and ξ_{24} are also orthogonal. Direct calculation shows that $\xi_{4a}\xi_{4b}$ and hence also ξ_{24} has order 3. Alternatively, we may check that matrix $\xi_{4a}\xi_{4b}$ has trace 1 and eigenvectors $(0,1,-1,0)$ and $(0,1,0,-1)$ with eigenvalue 1. So orthogonality forces the other eigenvalues to $\frac{-1\pm\sqrt{-3}}{2}$ and hence order 3.

Lemma 9.6. Λ^E *is invariant under* ξ_{24a} *and* ξ_{24b}.

Proof

Using the isomorphism in Theorem 6.1 it is easy to see that Λ^E is generated by the vectors

$$\lambda_{ij}^\pm : (4_{\text{on } i}, \pm 4_{\text{on } j}, 0_{\text{else}}), \qquad i,j \in \tilde{\Omega},$$
$$\lambda_d^E : (2_{\text{on } d}, 0_{\text{else}}), \qquad d \in \mathcal{C}, \quad \langle d, \omega \rangle \text{ even}.$$

Here the condition $\langle d, \omega \rangle = 0 \pmod 2$ implies that λ_d^E has an even number of entries 2 in each column and also in row 0 of the MOG.

The operation of ξ_{24b} is negation of row 0 in the MOG. Thus $\lambda_{ij}^\pm - \xi_{24b}(\lambda_{ij}^\pm)$ has entries divisible by 8 and $\lambda_d^E - \xi_{24b}(\lambda_d^E)$ has an even number of entries divisible by 4 in row 0 of the MOG and zeros elsewhere. All these differences are in Λ^E, so Λ^E is invariant under ξ_{24b}.

Matrix $1 - \xi_{4a}$ contains entry $\frac{1}{2}$ everywhere, so the operation of $1 - \xi_{4a}$ may be described as follows: For each column of the MOG calculate half the sum of its entries and write the result into each entry of that column. Performing this operation on $\lambda_{ij}^\pm$ we obtain either one column with equal entries divisible by 4 or two columns with equal entries ± 2. These results are all in Λ^E.

Any λ_d^E has an even number of entries 2 in each MOG column and the total number of entries 2 is divisible by 4. Thus there is a vector $e \in \Lambda^E$ with an even number of nonzero entries, which are all equal to 4, such that $\lambda_d^E - e$ has the same number of entries 2 and -2 in each column of the MOG. Hence $\lambda_d^E - e$ is invariant under ξ_{4a}. We have already shown $\xi_{4a}(e) \in \Lambda^E$, thus $\xi_{24a}(\lambda_d^E) \in \Lambda^E$. Hence Λ^E is also invariant under ξ_{24a}.

□

By (2.2.1) and Theorem 6.1 we have the following Leech lattice vectors in MOG coordinates:

$$\lambda_{g_0} = \begin{array}{|c|c|c|c|c|c|} \hline 0 & 2 & 2 & 2 & 2 & 2 \\ \hline 2 & 0 & 0 & 0 & 0 & 0 \\ \hline 2 & 0 & 0 & 0 & 0 & 0 \\ \hline 2 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array} \quad , \quad \lambda_{\gamma_0} = \begin{array}{|c|c|c|c|c|c|} \hline -3 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 \\ \hline \end{array} \quad , \tag{9.7.1}$$

where $g_0, \ldots, g_5$ is the natural basis of $\mathcal{G}$ and $\gamma_0, \ldots, \gamma_5$ is the natural basis of $\mathcal{G}$. g_n and γ_n are obtained from g_0 and γ_0 by exchanging MOG column 0 with column n. We have:

$$\begin{pmatrix} -3 & 3 & 0 & 1 & 1 & -2 \\ 1 & 1 & -2 & 1 & -1 & 0 \\ 1 & 1 & -2 & 1 & -1 & 0 \\ 1 & 1 & -2 & 1 & -1 & 0 \end{pmatrix}^\top \cdot \xi_{4a} \cdot \xi_{4b} = \begin{pmatrix} 3 & 0 & -3 & 1 & -2 & 1 \\ 1 & -2 & 1 & -1 & 0 & 1 \\ 1 & -2 & 1 & -1 & 0 & 1 \\ 1 & -2 & 1 & -1 & 0 & 1 \end{pmatrix}^\top ,$$

and hence

$$\lambda_{\gamma_i} \xmapsto{\xi_{24}} \lambda_{g_i} - \lambda_{\gamma_i} \xmapsto{\xi_{24}} -\lambda_{g_i} \xmapsto{\xi_{24}} \lambda_{\gamma_i} . \tag{9.7.2}$$

Since Λ is generated by Λ^E, g_0 and γ_0, Lemma 9.6 and (9.7.2) imply:

Corollary 9.8. *The Leech lattice Λ is invariant under ξ_{24}.*

Lemma 9.9. *The isomorphism $Q_x/Z(Q_x) \to \Lambda/2\Lambda$ given by Theorem 6.1 maps conjugation with ξ on Q_x to the automorphism ξ_{24} of the Leech lattice Λ (modulo 2Λ).*

Proof

Write x_{g_i} for $x_{(g_i,0)}$, with $(g_i, 0) \in \mathcal{P}_\mathcal{G}$. We have $\theta(g_i) = 0$ by Lemma 3.9 and hence $\tilde{x}_{g_i} = x_{g_i}$ by (5.3.4). So by (9.4.1), ξ operates on x_{g_i} and x_{γ_i} by conjugation as follows:

$$x_{\gamma_i} \xmapsto{\xi} x_{\pm g_i} x_{\gamma_i} \xmapsto{\xi} x_{g_i} \xmapsto{\xi} x_{\gamma_i} .$$

Comparing this operation of ξ with the operation of of ξ_{24} on λ_{g_i} and λ_{γ_i} given by (9.7.2) we see that these operations are compatible. So by linearity the operation of ξ_{24} on λ_r (modulo 2Λ) is the compatible with the operation of ξ of x_r on Q_x (modulo the center of Q_x) for all r in $\mathcal{G} \oplus \mathcal{G}^*$.

By Lemma 2.3 the space $\mathcal{H}^*$ is generated by vectors $ij \in \mathbb{F}_2^{24}$, where i and j are in the same column of the MOG, and not in row 0. By Theorem 6.1, the vector λ_{ij} has entries 4 and -4 in the corresponding positions. Thus λ_{ij} is not changed by ξ_{24a} or by ξ_{24b}. By Lemma 9.4 conjugation with ξ_k or ξ_g does not change x_{ij}. So by linearity the operations of ξ_{24} on λ_δ and of ξ on x_δ are trivial for $\delta \in \mathcal{H}^*$ and and hence compatible. Hence the operations of ξ on x_r and of ξ_{24} on λ_r are compatible for all $r \in \mathcal{G} \oplus \mathcal{C}^*$.

For any $h \in \mathcal{P}_\mathcal{H}$ of weight 8 let $\hat{x}_h = x_h x_{\gamma(h)}$. Then $\hat{x}_h$ is invariant under ξ by Lemma 9.5. Let $\hat{\lambda}_h \in \Lambda$ be any representative of the image of $\hat{x}_h$ under the mapping $Q_x \to \Lambda/2\Lambda$ given by Theorem 6.1. Since the elements $\hat{x}_h, h \in \mathcal{P}_\mathcal{H}, |h| = 8$ and $x_r, r \in \mathcal{P}_\mathcal{G} \oplus \mathcal{C}^*$ generate Q_x, it suffices to show $\xi_{24}(\hat{\lambda}_h) \in \hat{\lambda}_h + 2\Lambda$. (Note that 45 of the 64 elements of $\mathcal{H}$ have weight 8; so these elements generate $\mathcal{H}$.)

By Theorem 6.1 for every $h \in \mathcal{P}_\mathcal{H}$ there is a representative λ_h of the image of x_h with precisely no or two nonzero entries of value 2 in each column of the MOG and zeros in row 0. There is also a representative $\lambda_{\gamma(h)}$ of the the image of $x_{\gamma(h)}$ with entries 4 in row 0 in the columns where λ_h does no vanish, and zero entries elsewhere. Thus $\hat{\lambda}_h = \lambda_h - \lambda_{\gamma(h)}$ is a representative of the image of $\hat{x}_h$.

For $\hat{\lambda}_h$ in each column of the MOG the sum of the entries is zero. Thus $\hat{\lambda}_h$ is invariant under ξ_{24a}. Since λ_h has zeros on row 0 of the MOG and $\lambda_{\gamma(h)}$ has nonzero entries in row 0 of the MOG only, ξ_{24b} maps $\hat{\lambda}_h = \lambda_h - \lambda_{\gamma(h)}$ to $\lambda_h + \lambda_{\gamma(h)} = \hat{\lambda}_h + 2\lambda_{\gamma(h)}$.
□

An immediate consequence of Corollary 9.8 and Lemma 9.9 is:

Theorem 9.10. $\xi \in G(4096_x)$, $\xi_{24} \in G(24_x)$, $\xi \otimes \xi_{24} \in G_{x0}$.

Using 9.5.4 and Theorem 9.10, and identifying the basis vector i_x of 24_x with the position of entry i in the MOG, we obtain the following action of ξ and ξ^2 on the space 24_x:

Corollary 9.11. *For the n-th column vector c_n in the MOG we have:*

$$c_n^\top \xrightarrow{\xi} \frac{1}{2} c_n^\top \cdot \begin{pmatrix} -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} , \quad c_n^\top \xrightarrow{\xi^2} \frac{1}{2} c_n^\top \cdot \begin{pmatrix} -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix} .$$

9.6 The operation of ξ on 4096_x

Let ξ_γ and ξ_g be as in (9.3.1). We will now derive the operation of $\xi = \xi_\gamma \xi_g$ on 4096_x. Therefore we first specify a suitable basis of 4096_x.

Definition 9.12. (9.12.1) *Let $g_0, \ldots, g_5$ be the standard basis of the grey subspace $\mathcal{G}$ of Golay code as in section 2.2. We also write g_i for the element $(\tilde{g}_i, 0)$, $i = 0, \ldots, 5$, of the grey part $\mathcal{P}_\mathcal{G}$ of the Parker loop $\mathcal{P}$.*

(9.12.2) *Let $\mathcal{P}_\mathcal{G}^0 = \left\{ \left(\prod_{1 \leq i \leq 5} \tilde{g}_i^{\alpha_i}, 0 \right) \mid \sum_{1 \leq i \leq 5} \alpha_i = 0 \pmod{2} \right\}$.*

(9.12.3) *For $d \in \mathcal{G}$ and $\sigma \in \mathbb{Z}$ let $d_1^{[\sigma]} = d_1^+$ if σ is even and $d_1^{[\sigma]} = d_1^-$ if σ is odd.*

Then $\mathcal{P}_\mathcal{G}^0$ is a subset of $\mathcal{P}_\mathcal{G}$ with 16 even elements. Any element e of $\mathcal{P}_\mathcal{G}$ has a unique decomposition $e = \pm \Omega^\sigma g_0^\kappa d$, $d \in \mathcal{P}_\mathcal{G}^0$, $\sigma, \kappa \in \{0, 1\}$. For the unit vectors $f_1^{[\sigma]}$ in 4096_x, $f \in \mathcal{P}$ we have $(\Omega f)_1^{[\sigma]} = (-1)^\sigma f_1^{[\sigma]}$. It is easy to see that we have:

Lemma 9.13. *The vectors $(g_0^\kappa dh)_1^{[\sigma]}$, $\sigma, \kappa = 0, 1$, $d \in \mathcal{P}_\mathcal{G}^0$, $h \in \mathcal{P}_\mathcal{H}$ form a basis of 4096_x, with $w(g_0^\kappa d) = \kappa \pmod{2}$, $w_2(g_0^\kappa d) = w_2(d)$, and $A(g_0, d, h) = \theta(g_0, d) = \theta(g_0, h) = \theta(d, h) = 0$.*

So the the decomposition of a basis vector of 4096_x in Lemma 9.13 is easy to compute and independent of the association of the factors given in the Lemma.

Lemma 9.14. *Let $d \in \mathcal{P}_\mathcal{G}^0$ and $h \in \mathcal{P}_\mathcal{H}$. Then ξ_g maps $(g_0^\kappa dh)_1^{[\sigma]}$ to $(-1)^{w_2(d)+1}(g_0^\kappa dh)_1^{[\sigma+\kappa+1]}$.*

Proof

For any $f \in \mathcal{P}$ put $f' = \frac{1}{2} f_1^+ + \frac{1}{2} f_1^-$. From (7.1.1) we obtain:

$$f_1^+ = f' + (\Omega f)' , \quad f_1^- = f' - (\Omega f) , \quad \text{and hence} \quad f_1^{[\sigma]} = f' + (-1)^\sigma (\Omega f)' \qquad (9.14.1)$$

Let $e \in \mathcal{G}$, $\varphi \in \mathcal{G}^*$. From Table 3 we see that x_φ maps $(eh)'$ to $(-1)^{\langle eh, \varphi \rangle}(eh)'$. We have $\langle h, \varphi \rangle = 0$. So by (9.3.1) and Lemma 3.8, we obtain:

$$(eh)' \xrightarrow{\xi_\gamma} \tfrac{1}{8}(eh)' S(e) , \quad \text{with} \quad S(e) = \sum_{\varphi \in \mathcal{G}^*} (-1)^{w_2(\varphi)+\langle e, \varphi \rangle} = \sum_{f \in \mathcal{G}} (-1)^{w_2(f)+\langle\!\langle e, f \rangle\!\rangle} .$$

By Lemma 3.8 we have $w_2(f) + \langle\!\langle e, f \rangle\!\rangle = w_2(ef) + w_2(e)$ and hence:

$$(-1)^{w_2(e)} S(e) = \sum_{f \in \mathcal{G}} (-1)^{w_2(ef)} = \sum_{f \in \mathcal{G}} (-1)^{w_2(f)} = \sum_{m=0}^{6} \binom{6}{m} (-1)^{m(m-1)/2} = -8 .$$

This proves:

$$(eh)' \xrightarrow{\xi_\gamma} (-1)^{w_2(e)+1}(eh)' . \qquad (9.14.2)$$

We have $w_2(\Omega e) = w_2(e) + w(e) + 1$ by (3.7.2) and hence:

$$(\Omega eh)' \xrightarrow{\xi_\gamma} (-1)^{w_2(e)+w(e)}(\Omega eh)' . \qquad (9.14.3)$$

From 9.14.1, (9.14.2) and (9.14.3) we obtain:

$$(eh)_1^{[\sigma]} \xrightarrow{\xi_\gamma} (-1)^{w_2(e)+1}(eh)_1^{[\sigma+\kappa+1]} , \quad \text{where } \kappa \text{ is the parity of } e.$$

Putting $e = g_0^\kappa d$, the lemma now follows from Lemma 9.13.
□

The following Lemma states the operation of ξ_g on these basis vectors:

Lemma 9.15. *Let* $d \in \mathcal{P}_{\mathcal{G}}^0$ *and* $h \in \mathcal{P}_{\mathcal{H}}$. *Then* ξ_g *maps* $(g_0^\kappa dh)_1^{[\sigma]}$ *to*

$$\tfrac{1}{4} \sum_{d \in \mathcal{P}_{\mathcal{G}}^0} (-1)^{w_2(de)}(g_0^{\kappa+\sigma+1}eh)_1^{[\sigma]} .$$

Proof

Let $\mathcal{P}_{\mathcal{G}}^+ = \{(\tilde{f}, 0) \mid f \in \mathcal{G}\}$. Then $\mathcal{P}_{\mathcal{G}}^0 \subset \mathcal{P}_{\mathcal{G}}^+ \subset \mathcal{P}_{\mathcal{G}}$. Let $e, f \in \mathcal{P}_{\mathcal{G}}^+$. By (9.3.1) and (5.3.5) we have:

$$\xi_g = \tfrac{1}{8} \sum_{e \in \mathcal{P}_{\mathcal{G}}^+} (-1)^{w_2(fe)}\tilde{x}_f\tilde{x}_e , \quad \text{for any} \quad f \in \mathcal{P}_{\mathcal{G}}^+ .$$

We have $\langle h, \theta(e)\rangle = \langle h, \theta(f)\rangle = 0$ by Lemma 3.9. Using Table 3 and $e^2 = (-1)^{\langle e, \theta(e)\rangle}$ we obtain:

$$(fh)_1^{[\sigma]} \xrightarrow{x_f} h_1^{[\sigma]} \xrightarrow{x_{\theta(f)}} h_1^{[\sigma]} \xrightarrow{x_e} (\bar{e}h)_1^{[\sigma]} \xrightarrow{x_{\theta(e)}} (-1)^{\langle e,\theta(e)\rangle}(\bar{e}h)_1^{[\sigma]} = (eh)_1^{[\sigma]} .$$

Thus $\tilde{x}_f\tilde{x}_e$ maps $(fh)_1^{[\sigma]}$ to $(eh)_1^{[\sigma]}$ and we obtain:

$$(fh)_1^{[\sigma]} \xrightarrow{\xi_g} \tfrac{1}{8} \sum_{e \in \mathcal{P}_{\mathcal{G}}^+} (-1)^{w_2(fe)}(eh)_1^{[\sigma]} . \qquad (9.15.1)$$

To finish the proof, we put $f = g_0^\kappa d$.
Case $\sigma = 1$

If fe is odd then $w_2(fe\Omega) = w_2(fe)$ by (3.7.2), and we have $(eh)_1^- = -(\Omega eh)_1^-$ by (7.1.1), so that the terms for e and Ωe in the sum (9.15.1) cancel. If fe is even, these two terms are equal. The set $\mathcal{P}_{\mathcal{G}}^0$ contains exactly one of the two elements $d, \Omega d$ for each even $d \in \mathcal{P}_{\mathcal{G}}^+$, so that summing (9.15.1) over the even elements of $\mathcal{P}_{\mathcal{G}}^+$ proves the Lemma. We remark that $w_2(g_0de) = w_2(de)$ by Lemma 9.13, for $d, e \in \mathcal{P}_{\mathcal{G}}^0$.
Case $\sigma = 0$

If fe is even then $w_2(fe\Omega) = -w_2(fe)$ by (3.7.2), and we have $(eh)_1^+ = (\Omega eh)_1^+$ by (7.1.1), so that the terms for e and Ωe in the sum (9.15.1) cancel. If fe is odd, these two terms are equal. Now the same argument as in case $\sigma = 0$ shows that summing over the odd elements of $\mathcal{P}_{\mathcal{G}}^+$ in (9.15.1) proves the Lemma.
□

We have $\xi = \xi_\gamma\xi_g$. Combining Lemmas 9.14 and 9.15, and using Lemma 3.8 we obtain:

Corollary 9.16. *Let* $d \in \mathcal{P}_{\mathcal{G}}^0, h \in \mathcal{P}_{\mathcal{H}}$. *Then:*

$$(g_0^\kappa dh)_1^{[\sigma]} \xrightarrow{\xi} \tfrac{1}{4} \sum_{d \in \mathcal{P}_{\mathcal{G}}^0} (-1)^{\langle\!\langle d,e\rangle\!\rangle+w_2(e)+1}(g_0^\sigma eh)_1^{[\kappa+\sigma+1]} ,$$

$$(g_0^\kappa dh)_1^{[\sigma]} \xrightarrow{\xi^2} \tfrac{1}{4} \sum_{d \in \mathcal{P}_{\mathcal{G}}^0} (-1)^{\langle\!\langle d,e\rangle\!\rangle+w_2(d)+1}(g_0^{\kappa+\sigma+1}eh)_1^{[\kappa]} .$$

Notation

Symbol	Description	Section
a, b, c, d, e, f, h	Elements of the Parker loop $\mathcal{P}$ or of the Golay code $\mathcal{C}$	3.1
$A(d, e, f)$	Associator map of the elements d, e, f of the Parker loop $\mathcal{P}$	3.1
$\mathrm{Aut}_{\mathrm{St}}\mathcal{P}$	The group of standard automorphisms of the Parker loop $\mathcal{P}$	4
$C(d, e)$	Commutator map of the elements d and e of the Parker loop $\mathcal{P}$	3.1
$\mathcal{C}, \mathcal{C}^*$	$\mathcal{C}$ is the 12-dimensional Golay code in $\mathbb{F}_2^{24}$, $\mathcal{C}^*$ its cocode $\mathbb{F}_2^{24}/\mathcal{C}$	2.1
$\delta, \epsilon, \varphi, \eta$	Elements of the Golay cocode $\mathcal{C}^*$	3.1
$g_0, \ldots, g_5$	Standard basis of the "grey" subspace $\mathcal{G}$ of the Golay code $\mathcal{C}$;	
	$g_i, i = 0, \ldots, 5$, is also considered as the element $(g_i, 0)$ of $\mathcal{P}_{\mathcal{G}}$.	2.2
$\mathcal{G}, \mathcal{G}^*$	The subspaces of the "grey" elements of $\mathcal{C}$ and $\mathcal{C}^*$, respectively	2.2
G_{x0}	A maximal subgroup of $\mathbb{M}$ of structure $2_+^{1+24}.\mathrm{Co}_1$	5
γ	A specific function $\mathcal{C} \to \mathcal{G}^*$, satisfying $\gamma(g_i) = \gamma_i$, $i = 0, \ldots, 5$	3.3
$\gamma_0, \ldots, \gamma_5$	Standard basis of the "grey" subspace $\mathcal{G}^*$ of the Golay cocode $\mathcal{C}^*$	2.2
$\mathcal{H}, \mathcal{H}^*$	The subspace of the "coloured" elements of $\mathcal{C}$ and $\mathcal{C}^*$, respectively	2.2
i, j, k	Elements of $\tilde{\Omega}$, also considered as elements of $\mathcal{C}^*$ of weight 1	3.1
ij	Shorthand for $i \cup j$, considered as an element of $\mathcal{C}^*$ of weight 2	3.1
Λ	The 24-dimensional Leech lattice.	6.1
$\mathbb{M}$	The monster group, i.e. the largest sporadic simple group	1
M_{24}	Mathieu group, acts on $\tilde{\Omega}$ as the automorphism group of $\mathcal{C}$.	2.1
MOG	Miracle Octad Generator; a tool for calculations in $\mathcal{C} \subset \mathbb{F}_2^{24}$.	2.1
N	A fourfold cover of the maximal subgroup N_0 of $\mathbb{M}$	5
N_0	A maximal subgroup of $\mathbb{M}$ of structure $2^{2+11+22}.(M_{24} \times S_3)$	5
N_{x0}	Subgroup of structure $2_+^{1+24}.2^{11}.M_{24}$ of $\mathbb{M}$ with $G_{x0} \cap N_0 = N_{x0}$	5
Ω	The element $(\tilde{\Omega}, 0)$ of the Parker loop $\mathcal{P}$	2.1
$\tilde{\Omega}$	A set of size 24 used for labeling the basis vectors of $\mathbb{F}_2^{24}$,	
	its power set $2^{\tilde{\Omega}}$ is identified with $\mathbb{F}_2^{24}$, and we have $\mathcal{C} \subset \mathbb{F}_2^{24}$	2.1
ω	A specific "grey" element in the subset $\mathcal{G}^*$ of the cocode $\mathcal{C}^*$	2.2
$P(d)$	The squaring map in $\mathcal{P}$, with $d^2 = (0, P(d))$ for $d \in \mathcal{P}$	3.1
$\mathcal{P}$	The Parker loop, any $d \in \mathcal{P}$ has the form $(\tilde{d}, \mu)$, $\tilde{d} \in \mathcal{C}, \mu \in \mathbb{F}_2$	3.1
$\mathcal{P}_{\mathcal{G}}, \mathcal{P}_{\mathcal{H}}$	Subsets of $\mathcal{P}$: origins of $\mathcal{G}$ and $\mathcal{H}$ of the mapping $\tilde{\ } : \mathcal{P} \to \mathcal{C}$.	3.3
π, π', π''	Standard automorphisms of the Parker Loop $\mathcal{P}$ in $\mathrm{Aut}_{\mathrm{St}}\mathcal{P}$	4
θ	Cocycle of Parker loop $\mathcal{P}$, with $(\tilde{d}, 0) \cdot (\tilde{e}, 0) = (\tilde{d} + \tilde{e}, \theta(\tilde{d}, \tilde{e}))$	3.2
$w(d)$	Weight of vector $d \in \mathcal{G}$ with respect to the basis $g_0, \ldots, g_5$	2.2
$w(\delta)$	Weight of vector $\delta \in \mathcal{G}^*$ with respect to the basis $\gamma_0, \ldots, \gamma_5$	2.2
$w_2(d), w_2(\delta)$	Equal to $\binom{w(d)}{2}$, $\binom{w(\delta)}{2}$ modulo 2	3.3
$Z(G)$	The center of a group or a loop G	4
$\tilde{\ }$	The homomorphism $\mathcal{P} \to \mathcal{C}$ with $(\tilde{d}, \mu) \mapsto \tilde{d}$, for $\tilde{d} \in \mathcal{C}, \mu \in \mathbb{F}_2$.	3.1
$\bar{\ }$	Inversion in the Parker loop $\mathcal{P}$: $\bar{d} = d^{-1}$	3.1
$\|d\|, \|\delta\|$	Weight of code word $d \in \mathcal{C}$, min. weight of cocode word $\delta \in \mathcal{C}^*$	2.1
$\langle ., . \rangle$	The scalar product, e.g. on $\mathcal{C} \times \mathcal{C}^*$	2.1
$\langle\langle d, e \rangle\rangle$	equal to $\langle d, \gamma(e) \rangle$ and to $w_2(de) + w_2(d) + w_2(e)$ for $d, e \in \mathcal{G}$	3.3

References

[1] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *CoRR*, quant-ph/0406196, 2004.

[2] M. Aschbacher. *Sporadic Groups.* Cambridge University Press, New York, 1986.

[3] M. Aschbacher. *Finite Group Theory.* Cambridge University Press, New York, 1994.

[4] R. W. Barraclough and R. A. Wilson. Conjugacy class representatives in the Monster Group. *LMS Journal of Computation and Mathematics*, 8:205–216, 2005.

[5] J. H. Conway. A simple construction of the Fischer-Griess monster group. *Inventiones Mathematicae*, 79, 1985.

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

[7] J. H. Conway and Neil J. A. Sloane. *Sphere Packings, Lattices and Groups.* Springer-Verlag, New York, 3rd edition, 1999.

[8] A. Drápal and P. Vojtěchovský. Code loops in both parities. *Journal of Algebraic Combinatorics*, 31(4):585–611, 2010.

[9] R. L. Griess. The friendly giant. *Invent. Math*, 69:1–102, 1982.

[10] R. L. Griess. The monster and its nonassociative algebra. In J. McKay, editor, *Finite Simple Groups Coming of Age, Contemp. Math 45*, pages 121–158. AMS, Providence, RI, 1982.

[11] R. L. Griess. Code loops. *J. Algebra*, 100:224–234, 1986.

[12] R. L. Griess. *Twelve Sporadic Groups.* Springer-Verlag, New York, NY, USA, 1998.

[13] P. E. Holmes and R. A. Wilson. A new computer construction of the monster using 2-local subgroups. *Journal of the London Mathematical Society*, 67(2):349–364, 2003.

[14] A. A. Ivanov. *The Monster Group and Majorana Involutions.* Cambridge University Press, April 2009.

[15] G. Nebe, E. M. Rains, and N. J. A. Sloane. The invariants of the clifford groups. *IJDCC: Designs, Codes and Cryptography*, 24, 2001.

[16] M. Seysen. `mmgroup`, a python implementation of the monster group. `https://github.com/Martin-Seysen/mmgroup`, 2020.

[17] G. E. Wall. On the conjugacy classes in the unitary, symplectic and orthogonal groups. *J. Australian Math. Soc.*, 3:1–63, 1963.