

Conway's group and octonions

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

Submitted 17th March 2009

Abstract

We give a description of the double cover of Conway's group in terms of right multiplications by 3×3 matrices over the octonions. This leads to simple sets of generators for many of the maximal subgroups, including a uniform construction of the Suzuki chain of subgroups.

1 Introduction

In [12] I showed how to construct a 3-dimensional octonionic Leech lattice, based on Coxeter's non-associative ring of integral octonions [5], which is an algebraic version of the E_8 lattice. The automorphism group of the Leech lattice is Conway's group Co_0 , which is a double cover of the sporadic simple group Co_1 (see [2]). In this paper I show how to write generators for Co_0 , and many of its maximal subgroups, in terms of 3×3 octonion matrices (suitably interpreted).

We begin by summarising the notation and results of [12]. The octonions are an 8-dimensional real vector space, with basis $\{i_t : t \in PL(7)\}$, where $PL(7) = \{\infty\} \cup \mathbb{F}_7$ is the projective line of order 7, such that $i_\infty = 1$ and the multiplication is given by the images under the subscript permutations $t \mapsto t + 1$ and $t \mapsto 2t$ of $i_0 i_1 = -i_1 i_0 = i_3$. The lattice L is defined to be the copy of E_8 whose roots are $\pm i_t \pm i_u$ for $t \neq u$ and $\frac{1}{2} \sum_t (\pm i_t)$ with an odd number of minus signs. Let $s = \frac{1}{2}(-1 + i_0 + \dots + i_6)$ and $R = \bar{L}$.

Writing $B = \frac{1}{2}LR$ we proved in [12] that B is a copy of the E_8 lattice whose roots are $\pm i_t$ and the images under $t \mapsto t + 1$ of $\frac{1}{2}(\pm 1 \pm i_0 \pm i_1 \pm i_3)$ and $\frac{1}{2}(\pm i_2 \pm i_4 \pm i_5 \pm i_6)$. Thus Coxeter's non-associative ring of integral octonions (see [5] and [3]) is $\frac{1}{2}(1 + i_0)B(1 + i_0)$, which is closed under multiplication. Moreover, using the Moufang laws we showed that $L\bar{s} = 2B$ and $BL = L$. The important content of [12] is the following definition.

Definition 1 The octonionic Leech lattice $\Lambda = \Lambda_{\mathbb{O}}$ is the set of triples (x, y, z) of octonions, with the norm $N(x, y, z) = \frac{1}{2}(x\bar{x} + y\bar{y} + z\bar{z})$, such that

- (i) $x, y, z \in L$,
- (ii) $x + y, x + z, y + z \in L\bar{s}$, and
- (iii) $x + y + z \in Ls$.

The main result of [12] is that Λ is isometric to the Leech lattice.

2 The monomial subgroup

The reflection in any vector r of norm 1 in the octonions can be expressed as the map

$$x \mapsto -r\bar{x}r.$$

In particular, since $1 + i_t$ is perpendicular to s we have $s = -\frac{1}{2}(1 + i_t)\bar{s}(1 + i_t)$. Using R_a to denote the map $x \mapsto xa$, the Moufang law $((xa)b)a = x(aba)$ can be expressed as $R_a R_b R_a = R_{aba}$. In particular $R_s = -\frac{1}{2}R_{1+i_t}R_{\bar{s}}R_{1+i_t}$, which is equivalent to each of the following:

$$\begin{aligned} R_s R_{-1+i_t} &= R_{1+i_t} R_{\bar{s}}, \\ R_{-1+i_t} R_s &= R_{\bar{s}} R_{1+i_t}. \end{aligned}$$

Combining two such relations gives

$$R_s R_{1-i_0} R_{1+i_t} = -R_{1+i_0} R_{\bar{s}} R_{1+i_t} = R_{1+i_0} R_{1-i_t} R_s.$$

Therefore

$$\begin{aligned} (L(1 - i_0))(1 + i_t) &= (LR)L = 2BL = 2L \\ (B(1 - i_0))(1 + i_t) &= (BL)R = LR = 2B \\ ((Ls)(1 - i_0))(1 + i_t) &= ((L(1 + i_0))(1 - i_t))s = 2Ls. \end{aligned}$$

These three equations imply that the map $\frac{1}{2}R_{1-i_0}R_{1+i_t}$ acting simultaneously on all three coordinates preserves the octonion Leech lattice Λ .

Observe that the roots $1 - i_t$ for $t = 0, 1, 2, 3, 4, 5, 6$ form a copy of the root system of type A_7 , whose Weyl group is the symmetric group S_8 . Now the product of the reflections in $1 - i_0$ and $1 - i_t$ is the map

$$x \mapsto \frac{1}{4}(1 - i_t)((1 + i_0)x(1 + i_0))(1 - i_t)$$

which can be expressed as $\frac{1}{2}B_{1+i_0}\frac{1}{2}B_{1-i_t}$, where B_r denotes the bi-multiplication map $x \mapsto rxr$. These elements act as 3-cycles $(\infty, 0, t)$, so generate the rotation

subgroup A_8 of the Weyl group. Finally we apply the triality automorphism which takes bimultiplications $B_{\bar{u}}$ by units \bar{u} of norm 1 to right-multiplications R_u by the octonion conjugate u , and deduce that the maps $\frac{1}{2}R_{1-i_0}R_{1+i_t}$ generate $2 \cdot A_8$, the double cover of A_8 .

Adjoining the coordinate permutations and sign changes to this group gives a group $2 \cdot A_8 \times S_4$. Adjoining also the symmetry $r_0 : (x, y, z) \mapsto (x, yi_0, zi_0)$ described in [12] gives a group of shape $2^{3+12}(A_8 \times S_3)$. The latter group is in fact a maximal subgroup of the automorphism group $2 \cdot Co_1$ of the Leech lattice (see [11]), so we only need one more (non-monomial) symmetry to generate the whole of $2 \cdot Co_1$.

3 A complex reflection group

In order to construct a non-monomial symmetry, we regard s as a complex number $\frac{1}{2}(-1 + \sqrt{-7})$ and consider the subset of the octonionic Leech lattice which lies inside the 3-dimensional vector space over $\mathbb{Q}(s) = \mathbb{Q}(\sqrt{-7})$. This is a lattice spanned over $\mathbb{Z}[s]$ by the vectors $(\pm 2s, 0, 0)$, $(\pm 2, \pm 2, 0)$ and $(\pm s^2, \pm s, \pm s)$. Dividing through by s we obtain a well-known lattice (see for example [4, p. 3]) which has 42 vectors of norm 4, and the 21 reflections in these vectors generate the automorphism group of the lattice, which is isomorphic to $2 \times L_3(2)$. More explicitly, this automorphism group is generated by the monomial subgroup $2^3:S_3 \cong 2 \times S_4$ together with the matrix

$$\frac{1}{2} \begin{pmatrix} 0 & \bar{s} & \bar{s} \\ s & -1 & 1 \\ s & 1 & -1 \end{pmatrix},$$

which is the negative of reflection in $(s, 1, 1)$.

Now this matrix represents the map

$$(x, y, z) \mapsto \frac{1}{2}((y+z)s, x\bar{s} - y + z, x\bar{s} + y - z) \quad (1)$$

on the given complex vector space. But this can also be interpreted as a map on triples (x, y, z) of octonions. We show next that, with this interpretation, it is also a symmetry of the octonion Leech lattice. To prove this claim, it is useful first to prove the following lemma.

Lemma 1 $(x, y, z) \in \Lambda$ if and only if the following three conditions hold:

- (i) $x \in L$;
- (ii) $x + y \in L\bar{s} = 2B$;
- (iii) $x\bar{s} + y + z \in 2L$.

Proof. We use repeatedly the properties $2L \subset Ls \subset L$ and $2L \subset L\bar{s} \subset L$. Suppose the three conditions of the lemma hold. Then $y = (x + y) - x \in L$ so $z = (x\bar{s} + y + z) - y - x\bar{s} \in L$. Also $y + z = (x\bar{s} + y + z) - x\bar{s} \in L\bar{s}$, and therefore $x + z = (x + y) - (y + z) + 2z \in L\bar{s}$. Finally $x + y + z = (x\bar{s} + y + z) + xs + 2x \in Ls$.

Conversely if (x, y, z) satisfies the conditions of the original definition, then $x\bar{s} + y + z = (x + y + z)\bar{s} + (y + z)s + 2(y + z) \in 2L$.

For convenience, write (x', y', z') for the image of (x, y, z) under the octonion map given by (1), and note that $s = \frac{1}{2}(-1 + \sqrt{-7})$ satisfies $s^2 + s + 2 = 0$, so that $s + \bar{s} = -1$, $s^2 = -2 - s = \bar{s} - 1$ and $\bar{s}^2 = -2 - \bar{s} = s - 1$. Now we compute

- (i) $x' = \frac{1}{2}(y + z)s \in L$;
- (ii) $x' + y' = \frac{1}{2}(x\bar{s} + y(-1 + s) + z(1 + s)) = \frac{1}{2}(x + y\bar{s} - z)\bar{s} \in L\bar{s}$, using the fact that Λ is invariant under coordinate permutations and sign-changes;
- (iii) $x'\bar{s} + y' + z' = (y + z) + x\bar{s} \in 2L$;

and the claim is proved.

We summarise our results in the following theorem.

Theorem 1 *The full automorphism group $2 \cdot Co_1$ of the Leech lattice is generated by the following symmetries:*

- (i) *an S_3 of coordinate permutations;*
- (ii) *the map $r_0 : (x, y, z) \mapsto (x, yi_0, zi_0)$;*
- (iii) *the maps $\frac{1}{2}R_{1-i_0}R_{1+i_t}$ for $t = 1, 2, 3, 4, 5, 6$;*
- (iv) *the map $(x, y, z) \mapsto \frac{1}{2}((y + z)s, x\bar{s} - y + z, x\bar{s} + y - z)$.*

4 The normaliser of the complex reflection group

We have described the subgroup $2 \cdot A_8$ generated by the maps $\frac{1}{2}R_{1-i_0}R_{1+i_t}$ as the double cover of the group of even permutations of $\{\infty, 0, 1, 2, 3, 4, 5, 6\}$. The stabiliser of ∞ is a subgroup $2 \cdot A_7$ generated by the elements $\frac{1}{2}R_{i_1-i_0}R_{i_t-i_0}$ for $t = 2, 3, 4, 5, 6$. Since the roots $i_t - i_0$ are perpendicular to s , we know that $(i_t - i_0)\bar{s}(i_t - i_0) = -2s$ and therefore $R_{i_t-i_0}R_s = R_{\bar{s}}R_{i_t-i_0}$. It follows that this group $2 \cdot A_7$ commutes with the reflection group $2 \times L_3(2)$ just described, giving rise to a subgroup $L_3(2) \times 2 \cdot A_7$.

It is well-known (see [11]) that this group has index 2 in a maximal subgroup of shape $(L_3(2) \times 2 \cdot A_7).2$. To obtain the latter group we may adjoin an element such as $\frac{1}{2}R_{i_0-i_1}R_s^*$, where

$$R_s^* = R_s \frac{1}{2} \begin{pmatrix} s & 1 & 1 \\ 1 & s & 1 \\ 1 & 1 & s \end{pmatrix}.$$

Using the fact that $R_{i_1-i_0}R_s = R_{\bar{s}}R_{i_1-i_0}$ we can re-write this element in various ways such as

$$\frac{1}{2}R_{\bar{s}}R_{i_0-i_1}\frac{1}{2}\begin{pmatrix} s & 1 & 1 \\ 1 & s & 1 \\ 1 & 1 & s \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \bar{s} & 1 & 1 \\ 1 & \bar{s} & 1 \\ 1 & 1 & \bar{s} \end{pmatrix}\frac{1}{2}R_{\bar{s}}R_{i_0-i_1}.$$

In particular, it squares to minus the identity.

We still have to show that this element is a symmetry of the octonionic Leech lattice. Writing (x', y', z') for the image of (x, y, z) under this map, we have

- (i) $x' = \frac{1}{4}((x\bar{s} + y + z)\bar{s})(i_0 - i_1) \in \frac{1}{4}(2L\bar{s})L = \frac{1}{2}(LR)L = BL = L$ and by symmetry also $y', z' \in L$;
- (ii) $s^2 - s = s(s - 1) = s\bar{s}^2 = 2\bar{s}$ and therefore $x' - y' = \frac{1}{2}((x - y)(i_0 - i_1))\bar{s} \in \frac{1}{2}((LR)L)\bar{s} = L\bar{s}$ and again by symmetry $y' - z' \in L\bar{s}$;
- (iii) $s + 2 = -s^2$ and so $x' + y' + z' = \frac{1}{4}(((x + y + z)\bar{s})(i_1 - i_0))s^2 \in \frac{1}{2}(LR)s^2 = Ls$.

Since, as remarked in [12], we can change signs arbitrarily in the definition, we have shown that the given element is a symmetry of the lattice.

Finally let us consider the action of $\frac{1}{2}R_{i_0-i_1}R_s^*$ by conjugation on $L_3(2) \times 2 \cdot A_7$. Since the factor $2 \cdot A_7$ commutes with the action of any matrix over $\mathbb{Q}(s)$, it follows easily that our element acts on the $2 \cdot A_7$ factor as the transposition $(0, 1)$. Similarly, $R_{i_0-i_1}$ acts as complex conjugation ($s \leftrightarrow \bar{s}$) so our element acts on the $L_3(2)$ factor as complex conjugation followed by conjugation by the matrix $\begin{pmatrix} s & 1 & 1 \\ 1 & s & 1 \\ 1 & 1 & s \end{pmatrix}$. More concretely, it commutes with the S_3 of coordinate permutations and maps the sign change on the last two coordinates (that is, the negative of reflection in $(2, 0, 0)$) to the negative of reflection in $(s, 1, 1)$.

5 The Suzuki chain

The so-called Suzuki chain of subgroups of $2 \cdot C_{01}$ is a series of subgroups of the following shapes:

$$\begin{aligned} 2 \cdot A_9 &\times S_3 \\ 2 \cdot A_8 &\times S_4 \\ (2 \cdot A_7 &\times L_3(2)).2 \\ (2 \cdot A_6 &\times U_3(3)).2 \\ (2 \cdot A_5 &\circ 2 \cdot J_2).2 \\ (2 \cdot A_4 &\circ 2 \cdot G_2(4)).2 \\ &6 \cdot Suz.2 \end{aligned}$$

We have already described two groups in this list, namely $2 \cdot A_8 \times S_4$ and $(2 \cdot A_7 \times L_3(2)).2$. To obtain $2 \cdot A_9 \times S_3$, we take the S_3 of coordinate permutations, together with the group $2 \cdot A_8$ which is generated by $\frac{1}{2}R_{1-i_0}R_{1+i_t}$, and extend $2 \cdot A_7$ to $2 \cdot S_7$ by adjoining the element $\frac{1}{2}R_{i_0-i_1}R_s^*$ as above. The map onto A_9 permuting the points $\{*, \infty, 0, 1, 2, 3, 4, 5, 6\}$ is then given by mapping $R_{1-i_0}R_{1+i_t}$ onto the 3-cycle $(\infty, 0, t)$, as we have already seen, and mapping the extra element to $(*, \infty)(0, 1)$. In terms of the root system of L , the factor R_s^* of the new element corresponds to the root s , and extends the root system of type A_7 spanned by $1 - i_t$ to one of type A_8 .

To obtain the remaining groups in the Suzuki chain, all we have to do is adjoin to the complex reflection group $2 \times L_3(2)$ the part of $2 \cdot A_9$ which commutes with the appropriate subgroup $2 \cdot A_n$.

Consider first the subgroup $2 \cdot A_6$ generated by $\frac{1}{2}R_{i_1-i_2}R_{i_1-i_t}$ for $t = 3, 4, 5, 6$. This subgroup centralizes $\frac{1}{2}R_{1-i_0}R_s^*$ as well as the complex reflection group $2 \times L_3(2)$. Together these generate the full centralizer $2 \times U_3(3)$, and by adjoining $\frac{1}{2}R_{1-i_0}R_{i_1-i_2}$ we obtain the whole group $(2 \cdot A_6 \times U_3(3)).2$, which is a maximal subgroup of $2 \cdot C_{O_1}$. An alternative generating set may be obtained by observing that the monomial subgroup of $U_3(3)$ is $4^2:S_3$ generated by $r_0 : (x, y, z) \mapsto (x, yi_0, zi_0)$ and the coordinate permutations. Then we need only adjoin the element (1) to obtain $U_3(3)$. To prove that the group is indeed $U_3(3)$, first observe that all the generating matrices are written over $\mathbb{Q}(i_0, s)$, which is an *associative* ring of quaternions. Therefore these matrices define a quaternionic representation of the group in the usual sense, and it then suffices to reduce the representation modulo 3. Since both i_0 and $s - \bar{s} = \sqrt{-7}$ map to $\pm i$ in the field $\mathbb{F}_9 = \mathbb{F}_3(i)$, it follows immediately that the generators map to unitary matrices. Notice that this is essentially the same description of the group $2 \times U_3(3)$ as Cohen's description of it as a quaternionic reflection group [1]. The reflecting vectors are, up to left quaternion scalar multiplication, the $3 + 12 + 48 = 63$ images under the monomial group of the Leech lattice vectors $(2s, 0, 0)$, $(2, 2, 0)$ and (s^2, s, s) .

The next case may be obtained by taking the subgroup $2 \cdot A_5$ generated by $\frac{1}{2}R_{i_2-i_3}R_{i_2-i_t}$ for $t = 4, 5, 6$. To extend from $U_3(3)$ to $2 \cdot J_2$ we may adjoin $\frac{1}{2}R_{1-i_0}R_{1+i_1}$, or alternatively extend the monomial subgroup from $4^2:S_3$ to $2^{3+4}:S_3$ by adjoining $r_1 : (x, y, z) \mapsto (x, yi_1, zi_1)$. Then the involution centralizer $2^{2+4}A_5$ is generated by the diagonal symmetries, the coordinate permutation $(2, 3)$, and the element $\frac{1}{2}R_{1-i_0}R'_s$, where

$$R'_s = \begin{pmatrix} s & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}.$$

This is reminiscent of, but rather different from, the description of $2 \cdot J_2$ as a quaternionic reflection group in [1, 7, 8].

The group $2 \cdot (A_4 \times G_2(4)).2$ is perhaps best described by taking the subgroup

$2 \cdot A_4$ generated by $\frac{1}{2}R_{i_0-i_3}R_{i_5-i_6}$ and $\frac{1}{2}R_{i_3-i_5}R_{i_5-i_6}$. With the quaternionic labelling

$$\begin{array}{|c|c|} \hline 1 & 1 \\ \hline k & j \\ \hline i & k \\ \hline j & i \\ \hline \end{array}$$

given in [10] of each brick of the MOG (itself originally described in [6]), these elements become left-multiplication by k and $-\omega$ respectively. As generators for $2 \cdot G_2(4)$ we may take those given above for $L_3(2)$, together with the monomial elements $\text{diag}(1, i_t, i_t)$ for $t = 1, 2, 4$, and the elements $\frac{1}{2}R_{1-i_1}R_{i_2-i_4}$ (equivalent to right multiplication by k) and $\frac{1}{2}R_{i_1-i_2}R_{i_2-i_4}$ (equivalent to right multiplication by $-\omega$), as well as $\frac{1}{2}R_{1-i_1}R_s^*$.

The last case $6 \cdot \text{Suz}$ is of particular interest. It may be taken as the centralizer of the element $\frac{1}{2}R_{i_3-i_5}R_{i_5-i_6}$ of order 6. Then it is generated by the sign-changes and coordinate permutations, together with the matrix of reflection in $(s, 1, 1)$, and $\frac{1}{2}R_{1-i_0}R_{1+i_t}$ for $t = 1, 2, 4$, as well as $\frac{1}{2}R_{1-i_1}R_s^*$. This extends to $6 \cdot \text{Suz}:2$ by adjoining $\frac{1}{2}R_{1-i_0}R_{i_5-i_6}$.

6 Some 2-local subgroups

We have already seen how to generate the maximal 2-local subgroup of Co_0 which has shape $2^{3+12}(A_8 \times S_3)$, acting monomially on the three octonion coordinates.

The involution centraliser has the shape $2^{1+8} \cdot W(E_8)'$. If we take our involution to be $r_0^2 = \text{diag}(1, -1, -1)$, then the normal subgroup 2^{1+8} is generated by $r_t = \text{diag}(1, i_t, i_t)$ for all t . Modulo this, the group $2 \cdot A_8$ together with $\text{diag}(i_t, i_t, 1)$ generate a maximal subgroup of $W(E_8)'$, which may be extended to the whole group by adjoining an element such as $\frac{1}{2}R_{1-i_0}R'_s$, where R'_s is as defined above.

Another maximal 2-local subgroup of Co_0 is $2^{12}M_{24}$. This intersects our monomial group $2^{3+12}(A_8 \times S_3)$ in a group

$$2^{12} \cdot 2^6(S_3 \times L_3(2)) \cong 2^{3+12} \cdot (2^3 L_3(2) \times S_3).$$

To make the latter group, take the normal subgroup $2^{3+12}S_3$ generated by the coordinate permutations and all r_t , and the subgroup of $2A_8$ generated by

$$\frac{1}{8}R_{1-i_2}R_{i_3-i_5}R_{i_4-i_1}R_{i_6-i_0}R_{1-i_1}R_{i_2-i_4}$$

and its images under $i_t \mapsto i_{t+1}$. Now let π be the coordinate permutation $(1, 2)$, and adjoin the element

$$r_1^{\pi R_{1-i_1}R'_s/2} = \frac{1}{4}R_{1-i_1}R'_s \text{diag}(i_1, 1, i_1)R_{1-i_1}R'_s.$$

A little calculation shows that this element lies in the subgroup $2^{12}M_{24}$ which acts monomially on the MOG described above, but does not lie in $2^{3+12}(A_8 \times S_3)$. Hence we have obtained generators for $2^{12}M_{24}$.

A similar process gives generators for the other 2-constrained maximal 2-local subgroup $2^{5+12}(S_3 \times 3S_6)$. In this case we adjoin the above element to the subgroup $2^{3+12}((A_4 \times A_4).2 \times S_3)$ obtained by restricting to the subgroup of $2 \cdot A_8$ generated by $\frac{1}{2}R_{1-i_1}R_{1+i_2}$, $\frac{1}{2}R_{1-i_1}R_{1+i_4}$, $\frac{1}{2}R_{i_0-i_3}R_{i_0-i_6}$, $\frac{1}{2}R_{i_0-i_3}R_{i_0-i_5}$ and $\frac{1}{4}R_{1-i_0}R_{i_1-i_3}R_{i_2-i_6}R_{i_4-i_5}$.

References

- [1] A. M. Cohen, Finite quaternionic reflection groups, *J. Algebra* **64** (1980), 293–324.
- [2] J. H. Conway, A group of order 8,315,553,613,086,720,000, *Bull. London Math. Soc.* **1** (1969), 79–88.
- [3] J. H. Conway and D. A. Smith, *On quaternions and octonions: their geometry, arithmetic and symmetry*, A. K. Peters (2003).
- [4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *An Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.
- [5] H. S. M. Coxeter, Integral Cayley numbers, *Duke Math. J.* **13** (1946), 567–578.
- [6] R. T. Curtis, A new combinatorial approach to M_{24} , *Math. Proc. Cambridge Philos. Soc.* **79** (1976), 25–42.
- [7] J. Tits, Quaternions over $\mathbb{Q}(\sqrt{5})$, Leech’s lattice and the sporadic group of Hall–Janko, *J. Algebra* **63** (1980), 56–75.
- [8] R. A. Wilson, The geometry of the Hall–Janko group as a quaternionic reflection group, *Geom. Dedicata* **20** (1986), 157–173.
- [9] R. A. Wilson, The complex Leech lattice and maximal subgroups of the Suzuki group, *J. Algebra* **84** (1983), 151–188.
- [10] R. A. Wilson, The quaternionic lattice for $2G_2(4)$ and its maximal subgroups *J. Algebra* **77** (1982), 449–466.
- [11] R. A. Wilson, The maximal subgroups of Conway’s group Co_1 , *J. Algebra* **85** (1983), 144–165.
- [12] R. A. Wilson, Octonions and the Leech lattice, *J. Algebra* **322** (2009), 2186–2190.