An octonionic Leech lattice

Robert A. Wilson

15/12/08, QMUL, Pure Mathematics Seminar

1 Introduction

This is the last talk in a series of five. In this talk I want to bring together the various strands—E_8 and octonions on the one hand, the Golay code and the Leech lattice on the other. The result of this is an octonionic *definition* of the Leech lattice which to my mind has certain advantages over the Leech–Conway definition (though certainly some disadvantages as well). In particular, many of the maximal subgroups of Conway's group are much easier to describe in my formulation.

Let me begin with some revision of the salient points from the last four talks.

E_8 is an 8-dimensional *lattice* spanned by 240 *roots* of norm 2 (though often scaled to a different norm). Four different coordinate systems are of interest to us:

- **L**, with roots $(\pm 2^2, 0^6)$ and $(\pm 1^8)$ (odd sign combination);
- **R**, the same but with an even sign combination;
- **B**, with roots $(\pm 2, 0^7)$ and $(\pm 1^4, 0^4)$, with support $\infty 013$ or 2456 or an image under $t \mapsto t + 1$ mod 7 on subscripts;
- **E**, the same but with ∞ and 0 swapped afterwards.

Octonions form an 8-dimensional *non-associative algebra* spanned by $1 = i_\infty, i_0, \ldots, i_6$ with product given by $i_0 i_1 = -i_1 i_0 = i_3$ and images under $t \mapsto t + 1$ and $t \mapsto 2t$ on subscripts (modulo 7).

- **E** scaled to norm 1 is closed under multiplication: it is essentially the Coxeter–Dickson integral octonions;
- **L** scaled to norm 2 is $(1 + i_0)\mathbf{E}$;
- **R** scaled to norm 2 is $\mathbf{E}(1 + i_0)$;

- **B** scaled to norm 1 is $\frac{1}{2}(1+i_0)\mathbf{E}(1+i_0)$.

We used the Moufang laws $(xy)(zx) = x(yz)x$ etc. to prove that $\mathbf{LR} = 2\mathbf{B}$, $\mathbf{BL} = \mathbf{L}$ and $\mathbf{RB} = \mathbf{R}$.

The Golay code is a subspace of dimension 12 in $\mathbb{F}_2^{24}$ spanned by the vectors 'one column plus a hexacode word', in the 4×6 MOG (Miracle Octad Generator0 array: we can take a basis of 12 vectors by taking

- six vectors of the form 'one column plus the top row';
- six vectors of the form 'first column plus one of six basis vectors for the hexacode as an $\mathbb{F}_2$ vector space'.

It has weight distribution $0^1 8^{759} 12^{2576} 16^{759} 24^1$, and the 759 *octads* are as follows:

- a pair of columns: 15 of these;
- a column plus a hexacode word: $6.2^6 = 384$ of these;
- top row plus a hexacode word of weight 4, plus an even number of the corresposnding four columns: $45.2^3 = 360$ of these.

The Leech lattice consists of vectors $(x_1, \ldots, x_{24})$ in $\mathbb{Z}^{24}$ satisfying:

$$\begin{array}{rcl} x_i & \equiv & m \pmod 2 \\ (x_i - m)/2 \bmod 2 & \text{is} & \text{in the Golay code} \\ \sum x_i/4 & \equiv & m \pmod 2 \end{array}$$

The vectors of minimal norm are as follows:

- $(\pm 4, \pm 4, 0^{22})$: there are 1104 of these;
- $(\pm 2^8, 0^{16})$: there are $759.2^7 = 97152$ of these;
- $(-3, 1^{23})$ with sign-changes on a Golay-codeword: there are $24.2^{12} = 98304$ of these.

2 Octonion coordinates

The MOG array naturally divides into three 'bricks' of two columns each. The (minimal norm) Leech lattice vectors lying in one brick are of shape $(\pm 4^2, 0^6)$ or $(\pm 2^8)$ in that brick: that is, they are the roots of a suitably scaled copy of E_8. If we label the 8 coordinates by octonions as follows:

-1	i_0
i_4	i_5
i_2	i_6
i_1	i_3

then these vectors give a copy of $\mathbf{L}$.

This labelling was arrived at after much experimentation, and seems to give the nicest description of the Leech lattice.

An octonionic definition of the Leech lattice can be obtained as the set of triples (x, y, z) such that

- $x, y, z \in \mathbf{L}$;
- $x - y, y - z \in 2\mathbf{B}$;
- $x\overline{s} + y + z \in 2\mathbf{L}$;

where $\overline{s} = -\frac{1}{2}(1 + i_0 + \cdots + i_6)$.

Various equivalent definitions are easy to prove: since $2\mathbf{L} \subset \mathbf{B} \subset \mathbf{L}$ we see that $x - y \in 2\mathbf{B}$ is equivalent to $x + y \in 2\mathbf{B}$, and similarly we can change the signs of x, y, or z in the last condition. Moreover, $1 + \overline{s} = -s \in \mathbf{L}$, so $y + z \in 2\mathbf{B}$ implies $(y + z)(1 + \overline{s}) \in 2\mathbf{BL} = 2\mathbf{L}$, and therefore $x\overline{s} + y + z \in 2\mathbf{L}$ is equivalent to $(x + y + z)\overline{s} \in 2\mathbf{L}$. In particular the definition is invariant under sign-changes on the three coordinates, and under permutations of the three coordinates.

Proof of this can be obtained by various methods:

- An elementary but tedious proof by showing that (a) a spanning set of vectors for the Leech lattice satisfy these conditions, and (b) the minimal vectors which satisfy these conditions are in the Leech lattice.
- An easier proof by finding some nice symmetries of both versions of the lattice, to reduce the amount of computation required.
- A direct proof that the new definition, with norm of (x, y, z) defined to be $\frac{1}{2}(x\overline{x} + y\overline{y} + z\overline{z})$, is an even self-dual integral lattice in 24 dimensions with no vectors of norm 2.

Some symmetries of the lattice can be obtained as $\frac{1}{2}R_{1-i_0}R_{1+i_t}$, where R_x denotes right-multiplication by x. This symmetry maps (x, y, z) to (x', y', z') where $x' = \frac{1}{2}(x(1 - i_0))(1 + i_t)$ and similarly for y' and z'. It is easy to prove that (x', y', z') satisfies the (new) defining conditions of the Leech lattice.

- Since $1 \pm i_t \in \mathbf{L} \cap \mathbf{R}$ we have $x' \in \frac{1}{2}(\mathbf{LR})\mathbf{L} = \mathbf{BL} = \mathbf{L}$ etc.
- and $x' - y' \in \frac{1}{2}((2\mathbf{B})\mathbf{L})\mathbf{R} = \mathbf{LR} = 2\mathbf{B}$ etc.
- Also, one of the Moufang laws states $R_a R_b R_a = R_{aba}$ so in particular $\frac{1}{2} R_s R_{-1+i_t} R_s = R_{1+i_t}$ or $R_s R_{-1+i_t} = R_{1+i_t} R_{\overline{s}}$ which enables us to re-write $(x' + y' + z')\overline{s}$ as $\frac{1}{2}((x + y + z)\overline{s})$ right-multiplied by $\pm 1 \pm i_0$ and then $\pm 1 \pm i_t$ for some signs which we don't need to bother to calculate. Therefore $(x' + y' + z')\overline{s} \in \frac{1}{2}((2\mathbf{L})\mathbf{R})\mathbf{L} = 2\mathbf{BL} = 2\mathbf{L}$.

These symmetries generate $2A_8$, and together with the sign-changes and coordinate permutations we get a group $S_4 \times 2A_8$.

Adjoining $(1, R_{i_t}, R_{i_t})$ to this gives a maximal subgroup $2^{3+12}(S_3 \times A_8)$.

The Suzuki chain subgroups can all be generated easily. They are of shape

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

To get the first one, adjoin $\frac{1}{4} R_{1-i_0} \begin{pmatrix} s^2 & s & s \\ s & s^2 & s \\ s & s & s^2 \end{pmatrix}$ and remove the sign changes.

To get the third one, adjoin $\frac{1}{2} \begin{pmatrix} 0 & s & s \\ \overline{s} & 1 & -1 \\ \overline{s} & -1 & 1 \end{pmatrix}$ to extend the monomial $2 \times S_4$ to the complex reflection group $2 \times L_3(2)$, and reduce the $2A_8$ to $2A_7$ by taking only $\frac{1}{2} R_{i_0 - i_1} R_{i_0 - i_t}$ for $1 \leq t \leq 6$, and adjoin a similar element to get the outer half of the group.

Now to get the rest, delete one value of t at a time from the $2A_n$, and adjoin whatever part of the $2A_9$ commutes with this $2A_n$.