The Leech lattice

Robert A. Wilson

08/12/08, QMUL, Pure Mathematics Seminar

1 Introduction

This is the fourth talk in a projected series of five. Today my plan is to describe (more or less) Conway's construction of the Leech lattice and the Conway groups, using the Golay code. If you missed last week's talk on the Golay code, I hope it won't matter too much, as I'll remind you of the important points as we go along. (And some of the things we are going to use I didn't have time for last week anyway!) Next week I shall describe my new construction of the Leech lattice and the Conway groups using octonions and E_8 instead.

The Leech lattice is special for many reasons. Aside from its huge automorphism group, which is of great interest to group theorists, it turns up in number theory, coding theory, and theoretical physics, among other places.

It was first constructed as a solution to a sphere-packing problem: how many spheres of equal size can touch a given one? In one dimension the answer is 2, and in two dimensions it is 6, as everybody knows. In three dimensions there was much controversy as to whether the answer is 12 or 13. Apparently this is now settled as 12, but of course there is quite a bit of play in the system: it is not rigid. In eight dimensions, the answer is 240, and the E_8 root system describes the unique, rigid, solution. And the only other dimension in which the answer is known is 24, where the answer is 196560 and the Leech lattice provides the unique, rigid, solution.

We saw that E_8 is a self-dual even lattice in 8 dimensions—it is in fact the unique such. It turns out that for such an even self-dual lattice to exist, the dimension must be divisible by 8. There is a unique 16-dimensional example. In 24 dimensions there are exactly 24—and the Leech lattice is the only one which does not have any vectors of norm 2 (i.e. roots).

2 The Hamming code and E_8

Before I describe the construction of the Leech lattice, let me remind you of the connection between the E_8 lattice and the extended binary Hamming code of length 8. If we label the 8 coordinates $\infty, 0, 1, \ldots, 6$ then the Hamming code has words (0^8), (1^8) and 14 words of shape $(1^4 0^4)$ with the 1s either on ∞ together with a line, or the complement of a line, in the projective plane.

The norm 1 copy of E_8 has roots $(\pm 1, 0^7)$ and $\frac{1}{2}(\pm 1^4, 0^4)$ with the same rule for where the four coordinates $\pm\frac{1}{2}$ go. Let us double the coordinates so they are all integers; then the lattice consists of all $(x_\infty, \ldots, x_6)$ with integer coordinates, such that $(x_i \bmod 2)$ is in the extended Hamming code.

A norm 2 copy of E_8 has roots (doubled again to make the coordinates integers) $(\pm 2, 0^7)$ and $(\pm 1^8)$ with an odd number of minus signs: the conditions now are

$$\begin{aligned} x_i &\equiv m \pmod 2 \\ \sum x_i &\equiv 2m \pmod 4 \end{aligned}$$

3 Definition of the Leech lattice

Recall the (extended) binary Golay code, of length 24, consisting of 2^{12} words, with weight distribution $0^1 8^{759} 12^{2576} 16^{759} 24^1$. (We don't need the details of its construction just at the moment.)

Define the Leech lattice to consist of integer vectors $(x_1, \ldots, x_{24})$ such that

$$\begin{aligned} x_i &\equiv m \pmod 2 \\ (x_i - m)/2 \bmod 2 &\ \text{is}\ \text{in the Golay code} \\ \sum x_i &\equiv 4m \pmod 8 \end{aligned}$$

The vectors of minimal norm are easy to classify.

If $m = 0$, suppose first that the codeword $(x_i - m)/2 \bmod 2$ is the zero word. Then all the coordinates are divisible by 4, and their sum is divisible by 8. So the shortest possibility is $(\pm 4, \pm 4, 0^{22})$, that is norm 32.

If the codeword is non-zero, there are at least 8 coordinates congruent to 2 mod 4, and the smallest possibility is $(\pm 2^8, 0^{16})$. Moreover, the sum of the coordinates is divisible by 8, so there is an even number of minus signs.

If $m = 1$, suppose that the codeword is zero. Then not all coordinates can be $+1$, since $24 \not\equiv 4 \bmod 8$, so the shortest possibility is $(-3, 1^{23})$.

Then changing sign on a Golay codeword gives the corresponding codeword in the definition.

All these vectors have norm 32, and the total number of them is

$$\binom{24}{2}.2^2 + 759.2^7 + 24.2^{12} = 196560.$$

4 Properties of the Leech lattice

The lattice is spanned by the norm 32 vectors. Given any vector in the lattice, add $(-3, 1^{23})$ if necessary to make all the coordinates even. Then add vectors of shape $(2^8, 0^{16})$ to make all the coordinates divisible by 4. (This is possible because the octads span the Golay code.) Finally, add $(\pm 4, \pm 4, 0^{22})$ to make all but at most one coordinate 0. The definition now implies this coordinate is divisible by 8, and can be made as a sum of more vectors of shape $(\pm 4^2, 0^{22})$.

All inner products are divisible by 8. The first condition of the definition is equivalent to saying that the inner product of an arbitrary lattice vector with the vectors of shape $(\pm 4^2, 0^{22})$ is divisible by 8. The last condition says the inner product with $(-3, 1^{23})$ is divisible by 8. And the other condition (using the self-duality of the Golay code) says that the inner product with all the vectors of shape $(2^8, 0^{16})$ is divisible by 8.

But these vectors span the lattice, so the result follows.

The lattice is integral and self-dual if we divide the norm by 8. This follows immediately from what we have just proved.

5 The automorphism group of the Golay code

The extended code has the following numbers of vectors at various distances:

- 1 codeword
- 24 at distance 1
- $24.23/2 = 276$ at distance 2
- $24.23.22/3.2.1 = 2024$ at distance 3
- $24.23.22.21/4.3.2 = 10626$ at distance 4

In particular, 2325 cosets of the code contain representatives of weight at most 3, so the remaining 1771 each have 6 representatives of weight 4, since $6 \times 1771 = 10626$.

Sextets are the corresponding partitions of the 24 points into six 4s. For example the six columns of our diagram (Curtis's MOG) form such a sextet, since the sum of two columns lies in the code.

The stabiliser of a sextet permutes the six columns as S_6: an A_6 from the automorphism group of the hexacode, together with swapping the last two columns and simultaneously applying the field automorphism.

Fixing all the columns setwise, we still have the additive symmetry of the hexacode. Therefore the full stabiliser has shape $2^6{:}3S_6$.

The full automorphism group of the extended Golay code is transitive on the sextets (needs to be proved!), and so has order 244823040. It is the simple Mathieu group M_{24}.

6 The Leech lattice modulo 2

Vectors of norm 6 after dividing the norm by 8. It is not hard to see these are of shape $(5, 1^{23})$, $(-3^3, 1^{21})$, $(2^{12}, 0^{12})$ and $(2^8, 4, 0^{15})$ and the numbers of each are

$$24.2^{12} + \binom{24}{3}.2^{12} + 2576.2^{11} + 759.16.2^8 = 16773120.$$

Vectors of norm 8 are of the following shapes

$$\begin{array}{r}(8, 0^{23})\\ (6, 2^7, 0^{16})\\ (4^4, 0^{20})\\ (2^8, 4^2, 0^{14})\\ (2^{12}, 4, 0^{11})\\ (2^{16}, 0^8)\\ (5, -3^2, 1^{21})\\ (-3^5, 1^{19})\end{array}$$

and we can count them and find out that there are exactly 48.8292375 of them.

The 2^{24} cosets of the lattice Λ in 2Λ contain (by Pythagoras's Theorem) at most one of the following:

- the zero vector
- a pair of a norm 4 vector and its negative
- a pair of a norm 6 vector and its negative

- at most 24 norm 8 vectors and their negatives

But

$$1 + 196560/2 + 16773120/2 + 8292375 = 2^{24}$$

so this is all, and in particular every norm 8 vector is part of a *cross* consisting of 24 mutually orthogonal norm 8 vectors and their negatives.

7 The automorphism group of the Leech lattice

It is not difficult to show that the stabilizer of a cross is $2^{12}M_{24}$. We can show that the automorphism group is transitive on the crosses, by explicitly constructing another automorphism.

Hence the order of the automorphism group is 8292375 times the order of $2^{12}M_{24}$. It has a centre of order 2 consisting of $\pm I_{24}$. Modulo this is Conway's first group, which is a simple group of order

$$4157776806543360000.$$