Uniqueness of the Leech lattice

Abstract

We give Conway's proof for the uniqueness of the Leech lattice.

1 Uniqueness of the Leech lattice

Theorem 1.1 *There is a unique even unimodular lattice* Λ *in* $\mathbf{R}^{24}$ *without vectors of squared length 2. It is known as the Leech lattice. The group* .0 *of automorphisms fixing the origin has order* 8315553613086720000.

Let Λ be an even unimodular lattice in $\mathbf{R}^n$ where $n < 32$.

('Unimodular' is the same as 'self-dual', and says that the volume of the fundamental domain is 1. In other words, the lattice has one point per unit volume. 'Even' means that the squared length $|x|^2 = (x, x)$ is an even integer for each $x \in \Lambda$. It follows that all inner products (x, y) with $x, y \in \Lambda$ are integers: $(x, y) = \frac{1}{2}(|x + y|^2 - |x|^2 - |y|^2)$.)

The *theta function* θ_Γ of a lattice Γ is defined by $\theta_\Gamma(z) = \sum_{x\in\Gamma} q^{\frac{1}{2}(x,x)}$, where $q = e^{2\pi iz}$.

A code has a weight enumerator, and the MacWilliams relation describes the relation between a weight enumerator of a linear code and its dual. If the code is self-dual, this yields an invariance property for the weight enumerator. For lattices similar things are true: there is a relation between the theta function of a lattice and the theta function of its dual, and if the lattice is self-dual its theta function has an invariance proterty. We quote Hecke's theorem.

Theorem 1.2 *Let* Γ *be an even unimodular lattice in* $\mathbf{R}^n$*. Then*
(i) $n \equiv 0 \pmod 8$*, and*
(ii) θ_Γ *is a modular form of weight* $\frac{1}{2}n$*.*

Let M_k be the vector space of modular forms of weight $2k$, and let M_k^0 be the subspace consisting of cusp forms, that is, of modular forms that vanish at $i\infty$. The following theorem says that there are not too many modular forms, so that one has very strong information when something is a modular form of low weight.

Theorem 1.3 *(i)* $M_k = 0$ *for* $k < 0$ *and* $k = 1$.
(ii) For $k = 0, 2, 3, 4, 5$ *we have* $\dim M_k = 1$ *and* $\dim M_k^0 = 0$.
(iii) $M_{k-6} \simeq M_k^0$.
(iv) For $k \geq 2$ *we have* $\dim M_k = \dim M_k^0 + 1$.

(The proof is easy, but belongs elsewhere.)

Look at our even unimodular lattice Λ in $\mathbf{R}^n$ with $n < 32$. We have $8|n$ and $\theta_\Gamma \in M_{n/4}$. Let N_m be the number of vectors of squared length m, so that $N_0 = 1$ and $N_2 = 0$, and $\theta_\Gamma(z) = \sum_m N_m q^{m/2}$.

If $n = 8$ then θ_Γ is uniquely determined by $N_0 = 1$, since $\dim M_2 = 1$. We already know an even unimodular lattice in $\mathbf{R}^8$, namely E_8. It is a root lattice, that is, is generated by vectors of squared length 2, so certainly $N_2 \neq 0$. (In fact $N_2 = 240$.)

If $n = 16$ then again θ_Γ is uniquely determined by $N_0 = 1$, since $\dim M_4 = 1$. And the lattice $E_8 \oplus E_8$ shows that $N_2 \neq 0$ also here.

So $n = 24$. Here $\dim M_6 = 2$, and the two conditions $N_0 = 1$, $N_2 = 0$ determine the function uniquely. Computing the coefficients one finds $N_4 = 196560$, $N_6 = 16773120$, $N_8 = 398034000$.

(In fact, $N_{2m} = \frac{65520}{691}(\sigma_{11}(m) - \tau(m))$ for $m > 0$, where $\sigma_h(m) = \sum_{d|m} d^h$ and $\tau(m)$ is Ramanujan's function, defined by $q\prod_{m=1}^{\infty}(1-q^m)^{24} = \sum_{m=1}^{\infty} \tau(m)q^m$.)

Call $x \in \Lambda$ *short* if $(x,x) \leq 8$.

Claim *Each coset of* 2Λ *inside* Λ *contains a short vector. The classes that contain more than a single pair* $\pm x$ *of short vectors are precisely the classes that contain vectors of length* $\sqrt{8}$*, and these contain* 48 *short vectors, namely* 24 *mutually orthogonal pairs* $\pm x$ *of vectors of length* $\sqrt{8}$.

Indeed, let x, y be short vectors with $y \neq \pm x$ and $y - x \in 2\Lambda$. We may suppose $(x,y) \geq 0$. (Otherwise, replace y by $-y$.) Now $|y-x|^2 \leq |y|^2 + |x|^2 \leq 16$, but for nonzero vectors $u \in 2\Lambda$ we know $|u|^2 \geq 16$, so equality must hold everywhere, and x and y are orthogonal. In $\mathbf{R}^{24}$ we can have at most 24 mutually orthogonal pairs of vectors $\pm x$. The number of cosets that contain short vectors is at least $\frac{N_0}{1} + \frac{N_4}{2} + \frac{N_6}{2} + \frac{N_8}{48} = 2^{24}$, but since this is the total number of cosets, we must have equality everywhere. This proves the claim.

Fix one set of 24 mutually orthogonal pairs of vectors of length $\sqrt{8}$ to define a basis of $\mathbf{R}^{24}$. Then Λ contains the vectors $\frac{1}{\sqrt{8}}(\pm 8, 0^{23})$ and their halved differences $\frac{1}{\sqrt{8}}((\pm 4)^2, 0^{22})$ (where this notation means that there are 2 places with ± 4 and 22 places with 0, in any order). These vectors generate a sublattice Λ_0 of Λ, and $\Lambda_0 = \{\frac{1}{\sqrt{8}}(x_1, \ldots, x_{24}) \mid 4|x_i \text{ for all } i \text{ and } 8|\sum x_i\}$.

Consider an arbitrary vector $x = \frac{1}{\sqrt{8}}(x_1, \ldots, x_{24}) \in \Lambda$. Since the inner products with vectors in Λ_0 must be integers, it follows that the x_i must be integers, all of the same parity (all even or all odd). If there is such a vector with all x_i odd, then pick one and make sure that for that one $x_i \equiv 1 \pmod 4$ for all i, by changing the sign of some coordinates, if necessary.

The next step identifies the extended binary Golay code inside the lattice. Consider the sublattice Λ_1 of Λ consisting of the vectors for which all x_i are even, and let C be the image of Λ_1 in $\{0,1\}^{24}$ under the map defined coordinatewise by sending $0 \pmod 4$ to 0 and $2 \pmod 4$ to 1. Note that if $x \mapsto c$ then also $x + x_0 \mapsto c$ for any $x_0 \in \Lambda_0$ (since such x_0 has all coordinates divisible by 4).

Claim *C is the extended binary Golay code.*

There is a unique linear code with word length 24, dimension 12 and minimum distance 8. Clearly, C is a linear code with word length 24. Suppose $c \in C$, $c \neq 0$. Then c is the image of some $x \in \Lambda$, and by subtracting a vector in Λ_0 we may assume that $x_i \in \{0, 2\}$ for all i except one, and $x_i \in \{-2, 2\}$ for the last i. Now $4 \leq (x, x) = \frac{4}{8}\mathrm{wt}(c)$, so that $\mathrm{wt}(c) \geq 8$. This shows that C has minimum distance at least 8.

Look at the supports of code words of weight 8. No 5-set can be covered twice, otherwise the minimum distance would be smaller than 8. Since each 8-set covers $\binom{8}{5}$ 5-sets, and there are $\binom{24}{5}$ 5-sets altogether, there cannot be more than $\binom{24}{5}/\binom{8}{5} = 759$ words of weight 8 in C.

The balls of radius 4 around code words cover the words at distance less than 4 to C precisely once, and the words at distance 4 to C at most six times: if a word w has distance 4 to distinct code words c_1 and c_2, then $c_1 - w$ and $c_2 - w$ are vectors of weight 4 with disjoint supports (since c_1 and c_2 have distance 8), and there are at most six disjoint 4-sets in a 24-set. Since $1 + 24 + \binom{24}{2} + \binom{24}{3} + \frac{1}{6}\binom{24}{4} = 2^{12}$, there can be at most $2^{24}/2^{12} = 2^{12}$ code words, i.e. C has dimension at most 12.

Now count vectors of length 2. If $(x,x)=4$, then $\sum x_i^2 = 32$, and x must have one of the shapes $\frac{1}{\sqrt{8}}((\pm 4)^2, 0^{22})$ or $\frac{1}{\sqrt{8}}((\pm 2)^8, 0^{16})$ or $\frac{1}{\sqrt{8}}(\mp 3, (\pm 1)^{23})$. The number of vectors of these shapes is at most $\binom{24}{2}.2^2 + 759.2^7 + 24.2^{12} = 196560$. But this is N_4, so we must have equality everywhere.

(For the vectors of shape $\frac{1}{\sqrt{8}}((\pm 2)^8, 0^{16})$ there are 2^8 choices for the signs, but we can use only half of these, since two choices that differ in only one place would differ by a vector of squared length 2.

For the vectors of shape $\frac{1}{\sqrt{8}}(\mp 3, (\pm 1)^{23})$, subtract a vector with all coordinates 1 (mod 4) to get a vector with all x_i even. The fact that C has dimension at most 12 means that at most 2^{12} choices for the signs are possible.)

This shows that C has dimension 12, and therefore is the extended binary Golay code.

Now we can describe the Leech lattice.

Theorem 1.4 $x = \frac{1}{\sqrt{8}}(x_1, ..., x_{24}) \in \Lambda$ *if and only if*

(i) $x_i \in \mathbf{Z}$*, all* x_i *have the same parity; and*

(ii) if all x_i *are even, then* $\sum x_i \equiv 0 \pmod 8$*; if all* x_i *are odd, then then* $\sum x_i \equiv 4 \pmod 8$*; and*

(iii) $\{i \mid x_i \equiv a \pmod 4\} \in \mathcal{S}$ *for* $a = 0,1,2,3$*, where* $\mathcal{S}$ *is the collection of supports of vectors in* C.

Proof: Exercise. □

About the group of automorphisms: starting from any of the $N_8/48$ sets of 24 mutually orthogonal pairs of vectors $\pm x$ of length $\sqrt{8}$, we arrived at a unique description of Λ. That means that its group of automorphisms is transitive on these $N_8/48$ coordinate frames. If we fix a frame, then the possible automorphisms consist of sign changes and permutations of the coordinates, and correspond to automorphisms of the extended binary Golay code, which has group $2^{12}.M_{24}$. Altogether we find a group of order $(N_8/48).2^{12}.|M_{24}| = 8292375.4096.24.23.22.21.20.48 = 8315553613086720000 = 2^{22}.3^9.5^4.7^2.11.13.23$.

2 Related sporadic simple groups

Co.1 The group of the Leech lattice stabilizing the origin 0 is called .0 and was found above to have order 8315553613086720000. It has a center of order 2 (the map $x \mapsto -x$) and the quotient is a simple group called .1 or Co_1 of order $\frac{1}{2}|.0| = 2^{21}.3^9.5^4.7^2.11.13.23$.

Co.2 The subgroup of .0 fixing a vector of squared length 4 is Co_2 of order $|.0|/N_4 = 2^{18}.3^6.5^3.7.11.23$. This is the group of automorphisms of a strongly regular graph on 2300 points.

Co.3 The subgroup of .0 fixing a vector of squared length 6 is Co_3 of order $|.0|/N_6 = 2^{10}.3^7.5^3.7.11.23$. This is the group of automorphisms of a regular 2-graph on 276 points.

McL The subgroup of .0 fixing a triangle with sides of squared lengths 4, 4, 6 is McL of order $2^7.3^6.5^3.7.11$. The group $McL.2$ is the point stabilizer of Co_3 in its action on 276 points. It is the group of automorphisms of a strongly regular graph on 275 points.

HS The subgroup of .0 fixing a triangle with sides of squared lengths 4, 6, 6 is HS of order $2^9.3^2.5^3.7.11$. The group $HS.2$ is the group of automorphisms of a strongly regular graph on 100 points.

$\mathbf{M_{24}}$ The group M_{24} of order $2^{10}.3^3.5.7.11.23$ is 5-transitive on 24 points (and the subgroup fixing 5 points has order 48, so $|M_{24}| = 24.23.22.21.20.48$). It is the automorphism group of the Steiner system $S(5, 8, 24)$. The automorphism group of the extended binary Golay code (both translations and coordinate permutations) is $2^{12}.M_{24}$.

$\mathbf{M_{23}}$ A point stabilizer in M_{24} is M_{23} of order $\frac{1}{24}|M_{24}| = 2^7.3^2.5.7.11.23$. It is the automorphism group of the Steiner system $S(4, 7, 23)$. The automorphism group of the perfect binary Golay code is $2^{12}.M_{23}$.

$\mathbf{M_{22}}$ A point stabilizer in M_{23} is M_{22} of order $\frac{1}{23}|M_{23}| = 2^7.3^2.5.7.11$. It is the automorphism group of the Steiner system $S(3, 6, 22)$. It is the group of automorphisms of a strongly regular graph on 77 points.

$\mathbf{M_{12}}$ The group M_{12} of order $12.11.10.9.8 = 2^6.3^3.5.11$ is sharply 5-transitive on 12 points. It is the stabilizer of a word of weight 12 in the action of M_{24} on the extended binary Golay code. It is the automorphism group of the Steiner system $S(5, 6, 12)$. The automorphism group of the extended ternary Golay code is $3^6.2.M_{12}$.

$\mathbf{M_{11}}$ A point stabilizer in M_{12} is M_{11} of order $\frac{1}{12}|M_{12}| = 2^4.3^2.5.11$. It is the automorphism group of the Steiner system $S(4, 5, 11)$.

The letters here abbreviate Co: Conway, McL: McLaughlin, HS or HiS: Higman-Sims, M: Mathieu.

3 Theta functions

Let us give some more detail for the sentence above that said 'Computing the coefficients one finds $N_4 = 196560$, $N_6 = 16773120$, $N_8 = 398034000$'.

The theta function for the E_8 lattice is

$$1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^m = 1 + 240(q + 9q^2 + 28q^3 + 73q^4 + \cdots).$$

The theta function for the two nonisomorphic even unimodular lattices in $\mathbf{R}^{16}$ is

$$1 + 480 \sum_{m=1}^{\infty} \sigma_7(m) q^m = 1 + 480(q + 129q^2 + 2188q^3 + 16513q^4 + \cdots).$$

Since one of these lattices is $E_8 \oplus E_8$ with theta function

$$(1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^m)^2,$$

we find the identity $1 + 480 \sum_{m=1}^{\infty} \sigma_7(m) q^m = (1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^m)^2$.

A basis for the 2-dimensional space M_6 of modular forms of weight 12 is given by $f = 1 + \frac{65520}{691} \sum_{m=1}^{\infty} \sigma_{11}(m) q^m$ and $g = q \prod_{m=1}^{\infty} (1 - q^m)^{24} = \sum_{m=1}^{\infty} \tau(m) q^m$. Since

$$f = 1 + \frac{65520}{691}(q + 2049q^2 + 177148q^3 + 4196353q^4 + \cdots)$$

and

$$g = q - 24q^2 + 252q^3 - 1472q^4 + \cdots,$$

a linear combination $af + bg = 1 + 0q + \cdots$ must have $a = 1$ and $b = -\frac{65520}{691}$. Therefore, the theta function of the Leech lattice is

$$\begin{aligned} \theta_\Lambda(z) &= 1 + \frac{65520}{691} \sum_{m=1}^{\infty} (\sigma_{11}(m) - \tau(m)) q^m \\ &= 1 + \frac{65520}{691}(2073q^2 + 176896q^3 + 4197825q^4 + \cdots) \\ &= 1 + 196560q^2 + 16773120q^3 + 398034000q^4 + \cdots \end{aligned}$$

as desired.