The E_8 Root Lattice and Conway's Ovoids

G. Eric Moorhouse, March 1991

These lecture notes were prepared for my audience at a UW departmental seminar given in March, 1991 as relevant background when introducing my generalization [6] of Conway's ovoids.

0. Introduction

Conway [1] has constructed four new infinite families of ovoids in $O_8^+(p)$ for p prime, and these in turn produce large numbers of ovoids in $O_6^+(p)$ by the process of 'slicing' described last term; these 6-dimensional ovoids correspond, via the Klein correspondence, to translation planes. A couple of previously known 8-dimensional ovoids, previously thought to be sporadic, actually belong to Conway's lists.

Let V be a finite orthogonal space of type $O_8^+(q)$. A k-cap in V is a set of singular points of V, no two of which are orthogonal. Any cap is of size $\leq q^3+1$, and a (q^3+1)-cap is known as an **ovoid**. If $\mathcal{O}$ is an ovoid in V, then for any singular point $x \notin \mathcal{O}$, the space $x^\perp/x$ is of type $O_6^+(q)$, and the 'slice' $(\mathcal{O} \cap x^\perp)/x$ is a (q^2+1)-cap, i.e. an ovoid, in $x^\perp/x$. In general this ovoid (and the resulting translation plane) depend on the choice of x. However if x and x' are singular points of V outside $\mathcal{O}$, and if x and x' are equivalent under the group of $\mathcal{O}$, then x and x' give equivalent 6-dimensional slices and hence isomorphic translation planes. Since most known ovoids have very large (and often two-transitive!) groups, they tend to yield only small numbers of translation planes. Perhaps the most unique feature of Conway's ovoids is that they have groups of bounded order (in fact, subgroups of the Weyl group of type E_8), and so as $q \to \infty$, the number of orbits of singular points under the group of the ovoid, grows without bound. Thus Conway's ovoids yield large numbers of new translation planes; indeed Conway has privately conjectured that 'most' of the known finite projective planes are his, in the sense that

$$\lim_{n\to\infty} \frac{\text{no. of iso. classes of planes of order } \leq n \text{ obtained from Conway's ovoids}}{\text{total no. of known proj. planes of order } \leq n} = 1\,,$$

and this seems a reasonable conjecture. Verifying this conjecture would depend on showing that inequivalent choices of singular point $x \notin \mathcal{O}$ very often yield non-isomorphic translation planes, and Conway has already designed an invariant of projective planes for this purpose, and has set C. Charnes, one of his students, to work to investigate non-isomorphisms.

The constructions of these families require some knowledge of the E_8 root lattice, in particular the number of vectors of a given norm in the lattice, and we have tried to include some of theis background in this presentation. In particular we describe the Theta-function of a lattice, which embodies the number of vectors of a given norm in the lattice, in the same way as the weight-enumerator of a code lists the number of codewords

of a given weight. Analogous to the MacWilliams relations for codes, we have the Jacobi Theta-function identity, derived in Section 2 using the Poisson Summation Formula; these place strong constraints on the possiblities for self-dual codes and lattices, respectively.

1. Lattices

For $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, we denote the standard inner product by $\mathbf{u} \cdot \mathbf{v}$. A **lattice** in $\mathbb{R}^n$ is the $\mathbb{Z}$-span of a basis of $\mathbb{R}^n$, i.e. a $\mathbb{Z}$-submodule of $\mathbb{R}^n$ of rank n. Suppose that L is such a lattice. The **dual** of L is defined by $L' = \{\mathbf{v} \in \mathbb{R}^n : \mathbf{u} \cdot \mathbf{v} \in \mathbb{Z} \text{ for all } \mathbf{u} \in L\}$; clearly L' is also a lattice of $\mathbb{R}^n$. In case $L' = L$, we call L **self-dual**. Suppose that $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ is a base for L, and let $A = \big(\mathbf{e}_i \cdot \mathbf{e}_j\big)_{1 \le i,j \le n}$, the **Gram matrix** of this base. The **discriminant** of L is defined to be

$$\operatorname{disc}(L) = \det A = \Big(\det\Big(\mathbf{e}_1\, \mathbf{e}_2 \ldots \mathbf{e}_n\Big)\Big)^2,$$

which is independent of the choice of base for L. Observe that the n-volume of the 'parallelepiped' cell with sides $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ is $\sqrt{\operatorname{disc}(L)}$, and so the density of points of the lattice L per unit volume in $\mathbb{R}^n$ is $\big(\operatorname{disc}(L)\big)^{-1/2}$. Then $L \subseteq L'$ if and only if the entries of A are integers, and in this case, equality holds if and only if $\operatorname{disc}(L) = 1$.

The **norm** of a vector $\mathbf{v} \in L$ is $\mathbf{v} \cdot \mathbf{v}$. (Unfortunately perhaps, this is *not* a norm in the usual analytic sense, as is $\sqrt{\mathbf{v} \cdot \mathbf{v}}$; however, this is standard usage for lattice theory, and is consistent with the common algebraic usage.) Let $N_{_L}(\alpha)$ be the number of vectors $\mathbf{v} \in L$ of norm α. The **Theta-function** of the lattice L is the power series

$$\Theta_{_L}(z) = \sum_{\mathbf{v} \in L} q^{(\mathbf{v} \cdot \mathbf{v})} = \sum_{\mathbf{v} \in L} e^{\pi i (\mathbf{v} \cdot \mathbf{v}) z} = \sum_{\alpha \ge 0} N_{_L}(\alpha) e^{\pi i \alpha\, z}, \quad q = e^{\pi i z}.$$

Often we are interested in considering this purely as a formal power series; for other purposes, however, we consider this a holomorphic function in $z \in \mathbb{C}$, convergent for $\operatorname{Im} z > 0$ (i.e. $|q| < 1$). (This follows easily from the fact that $|\{\mathbf{v} \in L : \mathbf{v} \cdot \mathbf{v} = m\}| = O(m^{n/2})$.) It is clear from the above Fourier expansion for $\Theta_{_L}(z)$ that $\Theta_{_L}(z)$ is periodic with period 2. Another important functional relationship for the Theta-functions of self-dual lattices will be obtained in Section 2.

In this paper we are primarily interested in the E_8 **root lattice**, defined as the set E of all vectors in $\mathbb{R}^8$ of the form $\frac{1}{2}(a_1, a_2, \ldots, a_n)$ such that $a_i \in \mathbb{Z}$, $a_1 \equiv a_2 \equiv \ldots \equiv a_n \mod 2$ and $\sum a_i \equiv 0 \mod 4$. Clearly the shortest nonzero vectors in E are the 240 vectors

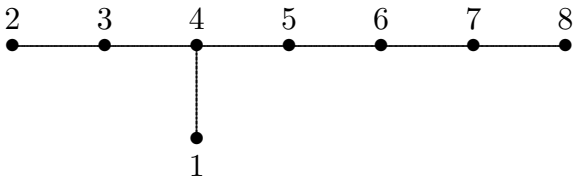
$$\begin{aligned} &\tfrac{1}{2}(\pm 1, \pm 1, \ldots, \pm 1) \quad (\text{an } \textit{even} \text{ number of } - \text{ signs}) \quad (128 \text{ of these}), \\ &(\pm 1, \pm 1, 0, 0, 0, 0, 0, 0) \quad \text{and permutations thereof} \quad (112 \text{ of these}) \end{aligned}$$

of 'norm' 2, known as the **root vectors** of the lattice, and we may have alternatively defined E as the $\mathbb{Z}$-span of these 240 root vectors. Thus $\Theta_{_E}(z) = 1 + 240q^2 + \cdots$. A popular choice for a base for E is the set of **fundamental roots** given by $\big\{\frac{1}{2}(11111111),$

(–1000000), (0–100000), (00––0000), (0001–000), (00001–00), (000001–0), (0000001–)$\big\}$ (here '–' abbreviates -1). The Gram matrix for this base of E (also known as the Cartan matrix of the E_8 root system) is

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

which is an integral matrix of determinant 1, and so E is self-dual. Furthermore it is apparent from the diagonal 2's that every vector in E has even norm, i.e. $N_{_E}(m)=0$ whenever m is odd. We remark that this Cartan matrix is equivalent to the usual E_8 Coxeter-Dynkin diagram, with vertices labelled according to the rows of the matrix as follows:



(More will be said concerning this diagram in Section 5.) Conway's ovoid constructions hang on an explicit determination of $N_{_E}(m)$, the number of vectors $\mathbf{v}\in E$ of norm $m\in\mathbb{Z}$. This will be accomplished in the next three Sections using analytic methods to determine $\Theta_{_E}(z)$. Actually, with very little work we can arrive at the formula

$$\Theta_{_E}(z)=\tfrac{1}{2}\big[\theta_2(z)^8+\theta_3(z)^8+\theta_4(z)^8\big]=1+240q^2+2160q^4+\dots$$

where

$$\begin{cases} \theta_2(z)=\displaystyle\sum_{m=-\infty}^{\infty} q^{(m+\frac{1}{2})^2}=2q^{1/4}+2q^{9/4}+2q^{25/4}+\dots, \\ \theta_3(z)=\displaystyle\sum_{m=-\infty}^{\infty} q^{m^2}=1+2q+2q^4+2q^9+2q^{16}+\dots, \\ \theta_4(z)=\theta_3(z+1)=\displaystyle\sum_{m=-\infty}^{\infty}(-q)^{m^2}=1-2q+2q^4-2q^9+2q^{16}-\dots\ . \end{cases}$$

However, this expression for $\Theta_{_E}(z)$ is of little value for us, since it does not explicitly give $N_{_E}(m)$. To illustrate the difficulty in a more familiar setting, let $\Lambda=\mathbb{Z}^8$, considered as a lattice in $\mathbb{R}^8$. Clearly Λ is self-dual, and since the Theta-function for the lattice $\mathbb{Z}\subset\mathbb{R}$ is given by $\theta_3(z)$ above, it is not hard to see that

$$\Theta_{_\Lambda}(z)=\theta_3(z)^8=\big(1+2q+2q^4+2q^9+\dots\big)^8=1+16q+112q^2+\dots\ .$$

However, this is very far from an explicit determination of the coefficient $N_\Lambda(m)$ of q^m in the above expansion. Actually, $N_\Lambda(m)$ is the number of ways m may be expressed as a sum of eight integer squares (using positive and negative integers, and counting different orders separately), and this is difficult to evaluate in closed form!

Note that the points of Λ may be taken as centres of spheres of radius $\frac{1}{2}$ in a 'rectangular' sphere-packing of $\mathbb{R}^8$, where each sphere 'kisses' exactly 16 other spheres. The lattice E does much better: we may use spheres of radius $1/\sqrt{2}$, and so the resulting sphere-packing is 16 times as dense as the rectangular packing, and each sphere kisses exactly 240 others. In fact, E determines the densest possible *lattice* sphere packing in eight dimensions*.

2. The Poisson Summation Formula

We shall need

$$\int_{-\infty}^{\infty} e^{-at^2}\,dt = \sqrt{\pi/a}. \tag{2.1}$$

This integral I is is evaluated by the well-known trick

$$\begin{aligned} I^2 &= \int\!\!\int_{\mathbb{R}^2} e^{-a(x^2+y^2)}dx\,dy = \int_0^{2\pi}\!\!\int_0^{\infty} e^{-ar^2} r dr\,d\theta \\ &= \int_0^{2\pi} d\theta \;\cdot \int_0^{\infty} re^{-ar^2}dr = \big(2\pi\big)\cdot\Big(\frac{1}{2a}\Big) = \frac{\pi}{a}. \end{aligned}$$

Recall that the **Fourier transform** of a function of one variable, $f(x)$, is defined by

$$\widehat{f}(y) = \int_{-\infty}^{\infty} e^{-2\pi i x y} f(x) dx. \tag{2.2}$$

We need in particular

(2.3) the Fourier transform of $f(x) = e^{-ax^2}$ is given by $\widehat{f}(y) = \sqrt{\frac{\pi}{a}}\, e^{-\pi^2 y^2/a}$, for $a > 0$.

To prove (2.3) we employ another couple tricks, differentiating under the integral sign, and then integrating by parts:

$$\begin{aligned} (\widehat{f})'(y) &= -2\pi i \int_{-\infty}^{\infty} x e^{-2\pi i x y} e^{-ax^2} dx = \frac{i\pi}{a}\int_{x=-\infty}^{x=\infty} e^{-2\pi i x y} d(e^{-ax^2}) \\ &= \frac{i\pi}{a} e^{-2\pi i x y} e^{-ax^2}\Big|_{-\infty}^{\infty} - \frac{i\pi}{a}\int_{x=-\infty}^{x=\infty} e^{-ax^2} d(e^{-2\pi i x y}) = -\frac{2\pi^2}{a} y\widehat{f}(y), \end{aligned}$$

* Note added in 2017: As we now know (after 2016), this is in fact the densest possible sphere packing in eight dimensions, lattice packing or otherwise [7].

which may be regarded as a differential equation for $\widehat{f}(y)$. Using the initial condition $\widehat{f}(0) = \sqrt{\pi/a}$, this gives the unique solution for $\widehat{f}(y)$ stated in (2.3).

Generalizing (2.2), the **Fourier transform** of a function $f(\mathbf{x})$ defined on $\mathbb{R}^n$, is defined by

$$\widehat{f}(\mathbf{y}) = \int_{\mathbb{R}^n} e^{-2\pi i\,\mathbf{x}\cdot\mathbf{y}} f(\mathbf{x}) d\mathbf{x}\,. \tag{2.4}$$

We require

(2.5) the Fourier transform of $f(\mathbf{x}) = e^{-a\,\mathbf{x}\cdot\mathbf{x}}$ is given by $\widehat{f}(\mathbf{y}) = \left(\frac{\pi}{a}\right)^{n/2} e^{-\pi^2\,\mathbf{y}\cdot\mathbf{y}/a}$.

To prove this, write $\mathbf{x} = \dfrac{s}{y}\mathbf{y} + \mathbf{v}$ where $y = \sqrt{\mathbf{y}\cdot\mathbf{y}}$ and $\mathbf{v} \in \mathbf{y}^{\perp}$. Then $d\mathbf{x} = ds\, d\mathbf{v}$ and using (2.1) and (2.3) we obtain

$$\begin{aligned}
\widehat{f}(\mathbf{y}) &= \int_{\mathbb{R}^{n-1}} \int_{-\infty}^{\infty} e^{-2\pi i y s} e^{-as^2 - a\mathbf{v}\cdot\mathbf{v}} ds\, d\mathbf{v} \\
&= \left(\prod_{j=1}^{n-1} \int_{-\infty}^{\infty} e^{-av_j^2} dv_j \right) \left(\int_{-\infty}^{\infty} e^{-2\pi i y s} e^{-as^2} ds \right) \\
&= \left(\frac{\pi}{a}\right)^{\frac{n-1}{2}} \left(\frac{\pi}{a}\right)^{\frac{1}{2}} e^{-\pi^2 y^2/a}\,,
\end{aligned}$$

which proves (2.5).

The most important functional identity for theta-functions of lattices is derived from the following theorem, which relates sums of values of a function over a lattice, to the sum of values of the Fourier transform over the dual lattice:

2.6 Theorem (Possion Summation Formula). $\displaystyle\sum_{\mathbf{x}\in L} f(\mathbf{x}) = \frac{1}{\sqrt{\operatorname{disc} L}} \sum_{\mathbf{y}\in L'} \widehat{f}(\mathbf{y}).$

For a proof, see [3], [5].

The Poisson Summation Formula determines the Theta-function of a dual lattice in terms of that of the original lattice:

2.7 Theorem (Jacobi Theta-Function Identity).

$$\Theta_{L'}(z) = \sqrt{\operatorname{disc} L}\left(\frac{i}{z}\right)^{n/2} \Theta_L\big(-1/z\big).$$

To prove the Jacobi identity, since both sides are holomorphic in $\operatorname{Im} z > 0$, it suffices to consider $z = it,\ t > 0$. Then $\Theta_L(it) = \sum_{\mathbf{x}\in L} e^{-\pi t\,\mathbf{x}\cdot\mathbf{x}}$ and $\Theta_{L'}\big(-1/it\big) = \sum_{\mathbf{y}\in L'} e^{-\pi\,\mathbf{y}\cdot\mathbf{y}/t}$, and so (2.7) follows from (2.5) and (2.6).

The Jacobi identity gives strong constraints for self-dual lattices. In particular for the E_8 root lattice E defined in Section 1, we have

$$\Theta_E(z+2) = \Theta_E(z), \qquad \Theta_E\big(-1/z\big) = z^4\Theta_E(z). \tag{2.8}$$

3. Eisenstein Series

We begin with the series

$$\sum_{m=-\infty}^{\infty} \frac{1}{(m+z)^2} = \frac{\pi^2}{\sin^2 \pi z}. \tag{3.1}$$

To prove this, both sides have a double pole at $z = 0$ with the same residue, and no other poles; hence the difference $f(z) = \sum_{m=-\infty}^{\infty} \frac{1}{(m+z)^2} - \frac{\pi^2}{\sin^2 \pi z}$ is an entire function of z. We wish to show that $f(z) = 0$. Since $f(it) \to 0$ as $t \to \infty$ $(t \in \mathbb{R})$, it suffices to show that $f(z)$ is constant. Since any nonconstant entire function assumes arbitrarily large values outside any compact subset of $\mathbb{C}$, and since $f(z+1) = f(z)$, it suffices to show that $f(z)$ is bounded on each region $0 < \operatorname{Re} z < 1,\ |\operatorname{Im} z| > 1$. This we leave as an exercise.

Rewriting (3.1) as

$$\pi^2 \csc^2 \pi z = \frac{1}{z^2} + \sum_{m=1}^{\infty} \left[\frac{1}{(z+m)^2} + \frac{1}{(z-m)^2}\right]$$

and integrating both sides with respect to z, gives

$$\pi \cot \pi z = \frac{1}{z} + \sum_{m=1}^{\infty} \left[\frac{1}{z+m} + \frac{1}{z-m}\right] = \frac{1}{z} + \sum_{m=1}^{\infty} \frac{2z}{z^2 - m^2}.$$

(That the constant of integration is 0, follows from the fact that the left side is an odd function of z.) Thus

$$\begin{aligned} z \cot z &= 1 - 2\sum_{m=1}^{\infty} \frac{z^2}{m^2\pi^2\big(1 - (z/m\pi)^2\big)} \\ &= 1 - 2\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} \frac{z^{2n}}{m^{2n}\pi^{2n}} = 1 - 2\sum_{n=1}^{\infty} \zeta(2n) \left(\frac{z}{\pi}\right)^{2n} \end{aligned}$$

where $\zeta(s) = \sum_{k=1}^{\infty} k^{-s}$ is the Riemann zeta-function. However, even some first-year calculus students can give the first few terms in the Taylor series

$$z \cot z = 1 - \tfrac{1}{3}z^2 - \tfrac{1}{45}z^4 - \tfrac{2}{945}z^6 - \dots .$$

(Actually the coefficient of z^{2n} is $(-4)^n B_{2n}/(2n)!$ in terms of the Bernoulli numbers B_{2n}; however this is not relevant to our present study, which requires only the first few terms.) Thus

$$\zeta(2) = \frac{\pi^2}{6},\ \zeta(4) = \frac{\pi^4}{90},\ \zeta(6) = \frac{\pi^6}{945},\ \text{etc.} \tag{3.2}$$

(In view of the previeous remark, we have $\zeta(2k) = (-1)^{k+1}(2\pi)^{2k} B_{2k}/2(2k)!$.)

Now writing $q = e^{\pi i z}$, we have $\sin \pi z = (q^2 - 1)/2iq$, and so (3.1) may be rewritten as

$$\sum_{m=-\infty}^{\infty} \frac{1}{(m+z)^2} = \frac{(2\pi i)^2 q^2}{\left(1-q^2\right)^2} = (2\pi i)^2 \sum_{r=1}^{\infty} r q^{2r}.$$

Differentiating both sides $k-2$ times with respect to z, where $k \in \{2, 4, 6, 8, \dots\}$, and using $\dfrac{dq^{2r}}{dz} = 2\pi r i q$, we obtain

$$\sum_{m=-\infty}^{\infty} \frac{(-1)^k (k-1)!}{(m+z)^k} = (2\pi i)^k \sum_{r=1}^{\infty} r^{k-1} q^{2r}.$$

Replacing z by nz and summing over $n \geq 0$ gives

$$\sum_{n=1}^{\infty} \sum_{m=-\infty}^{\infty} \frac{1}{(m+nz)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sum_{r=1}^{\infty} r^{k-1} q^{2nr} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sigma_{k-1}(m) q^{2m},$$

in terms of the multiplicative number-theoretic function $\sigma_s(m) = \sum d^s$, summing over all positive divisors $d \,\big|\, m$. Now we are ready to introduce the **Eisenstein series** $G_k(z)$ and the **normalized Eisenstein series** $E_k(z)$, defined by

$$\begin{cases} G_k(z) = \displaystyle\sum_{(m,n)\neq(0,0)} \frac{1}{(m+nz)^k}\,, \\[2ex] E_k(z) = \dfrac{G_k(z)}{2\zeta(k)} = 1 + \dfrac{(-1)^{k/2}(2\pi)^k}{(k-1)!\zeta(k)} \displaystyle\sum_{m=1}^{\infty} \sigma_{k-1}(m) e^{2\pi m i z}, \quad k = 2, 4, 6, 8, \dots, \end{cases} \tag{3.3}$$

holomorphic in $\operatorname{Im} z > 0$, i.e. $|q| < 1$. (In view of (3.2) and the remarks thereafter, the ugly coefficient in front of the latter sum reduces to $-2k/B_k$.) It is clear that these functions both satisfy the functional identities $F(z+1) = F(z),\ F(-z^{-1}) = z^k F(z)$, which we shall pursue in the next section. We are especially interested in

$$(3.4)\qquad \begin{cases} G_4(z) = \displaystyle\sum_{(m,n)\neq(0,0)} \frac{1}{(m+nz)^4}, \\ E_4(z) = \dfrac{45}{\pi^4} G_4(z) = 1 + 240 \displaystyle\sum_{m=1}^{\infty} \sigma_3(m) q^{2m}, \quad q = e^{\pi i z}. \end{cases}$$

4. Modular Forms

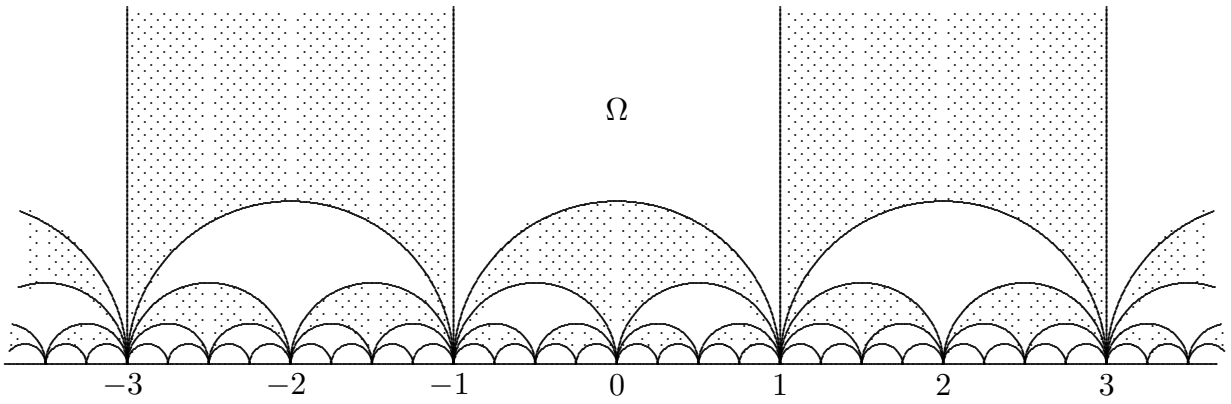
The full **modular group** is the group $\Gamma \cong \mathrm{PSL}(2,\mathbb{Z})$ consisting of transformations of the form

$$z \mapsto \frac{az+b}{cz+d}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

acting on the upper half-plane $\mathrm{Im}\, z > 0$. Then Γ is generated by the two transformations $z \mapsto z+1$ and $z \mapsto -1/z$. Let $G(2)$ denote the subgroup of Γ generated by the two transformations $z \mapsto z+2$ and $z \mapsto -1/z$. Then $G(2)$ consists of precisely those transformations in Γ such that a, b, c, d are either odd-even-even-odd or even-odd-odd-even. Since $G(2)$ is the pre-image of $\left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \right\}$ under the epimorphism $\Gamma \to \mathrm{SL}(2,2) \cong \mathrm{S}_3$, we have $[\Gamma : G(2)] = 3$. A fundamental domain for $G(2)$ is the region

$$\Omega = \{ z \in \mathbb{C} \,:\, \mathrm{Im}\, z > 0,\ |z| > 1,\ -1 < \mathrm{Re}\, z < 1 \}.$$

We illustrate Ω and its images under $G(2)$:



Let $k \in \{2, 4, 6, \ldots\}$. A **modular form of weight k for $G(2)$** is a $\mathbb{C}$-valued function $f(z)$ defined and holomorphic on the upper half-plane $\mathrm{Im}\, z > 0$, such that

(i) $f\Big(\dfrac{az+b}{cz+d}\Big) = (cz+d)^{-k} f(z)$ for every transformation $z \mapsto \frac{az+b}{cz+d}$ in $G(2)$, and

(ii) the Laurent expansion of $f(z)$ in $q = e^{\pi i z}$ has no negative powers of q, i.e. $f(z) = \sum_{n=0}^{\infty} a_n q^n$.

Clearly condition (i) is equivalent to

(i') $f(z+2) = f(z),\ f\big(-1/z\big) = z^k f(z)$.

The values of $f(z)$ on Ω determine the values of $f(z)$ everywhere on the upper half-plane. Also, the set of modular forms for $G(2)$ of a given weight k, constitute a vector space. It is known (see [4]) that the space of modular forms of weight 4 for $G(2)$, is 2-dimensional. We have already encountered certain functions in this space:

$$\begin{aligned}\Theta_{E}(z) &= 1 + 240q^2 + 2160q^4 + \dots,\\ \Theta_{\Lambda}(z) &= 1 + 16q + 112q^2 + \dots,\\ E_4(z) &= 1 + 240q^2 + 2160q^4 + \dots\ .\end{aligned}$$

Therefore $\Theta_{E}(z)$ is a $\mathbb{C}$-linear combination of $\Theta_{\Lambda}(z)$ and $E_4(z)$, and comparing the first few coefficients gives

$$\Theta_{E}(z) = E_4(z) = 1 + 240\sum_{m=1}^{\infty}\sigma_3(m)q^{2m}.$$

This finally answers our question regarding the number of vectors $\mathbf{v} \in E$ such that $\mathbf{v}\cdot\mathbf{v} = m$:

$$N_{E}(m) = \begin{cases} 1, & m = 0;\\ 240\sigma_3(m/2), & m = 2,4,6,\dots;\\ 0, & m \text{ odd.}\end{cases}$$

5. The Weyl Group of Type E_8

For each of the 240 root vectors $\mathbf{e} \in E$ we consider the reflection of $\mathbb{R}^8$ in the hyperplane $\mathbf{e}^{\perp}$, i.e. $T_{\mathbf{e}}(\mathbf{v}) = \mathbf{v} - (\mathbf{v}\cdot\mathbf{e})\mathbf{e}$. (Recall that $\mathbf{e}\cdot\mathbf{e} = 2$.) The **Weyl group of type** E_8 is the group $W = W(E_8)$ generated by these 240 reflections. This is a subgroup of $O_8(\mathbb{R})$ of order $2^{14}3^5 5^2 7 = 696{,}729{,}600$ which leaves invariant the lattice E (this is a property of root systems). W has a normal subgroup W' of index 2 consisting of rotations, and W' has a centre $\langle -I\rangle$ of order two. The quotient group $W'/\langle -I\rangle$ is a simple group of order $2^{12}3^5 5^2 7 = 174{,}182{,}400$, usually denoted $\Omega_8^+(2)$, for reasons which will become apparent below.

Let $\mathbf{e}_1$, $\mathbf{e}_2$, …, $\mathbf{e}_8$ be the eight fundamental roots of E given in Section 1. The corresponding reflections $T_{\mathbf{e}_i}$, $i = 1,2,\dots,8$ suffice to generate W. Let $\theta_{ij} = \cos^{-1}\dfrac{\mathbf{e}_i\cdot\mathbf{e}_j}{2}$, which is the angle between $\mathbf{e}_i$ and $\mathbf{e}_j$, and let $m_{ij} = \pi/(\pi - \theta_{ij})$, which is the order of $T_{\mathbf{e}_i}T_{\mathbf{e}_j}$. Refering to the Coxeter-Dynkin diagram of type E_8 given in Section 1, with vertices labelled 1,2,…,8, we have

$$m_{ij} = \begin{cases} 1, & i = j,\\ 2, & \text{vertices } i \neq j \text{ unjoined},\\ 3, & \text{vertices } i \neq j \text{ joined}.\end{cases}$$

Then W is given by the presentation

$$W \cong \langle s_1, s_2, \ldots, s_8 \,:\, (s_i s_j)^{m_{ij}} = 1 \rangle,$$

where $T_{\mathbf{e}_i} \mapsto s_i$ determines the isomorphism.

Now let L be a lattice in $\mathbb{R}^n$, and let p be a prime. Then L/pL is a $\mathbb{Z}$-module of rank n which is annihilated by $p\mathbb{Z}$. Hence L/pL is a module of rank n for $\mathbb{Z}/p\mathbb{Z}$, i.e. an n-dimensional vector space over $\mathbb{F}_p$. Let $^-$ denote the reduction modulo p, so that $\overline{\mathbf{x}} \in \overline{L} = L/pL$ for $\mathbf{x} \in L$, and $\overline{a} \in \mathbb{F}_p$ for $a \in \mathbb{Z}$. Reducing $\frac{1}{2}\mathbf{x}\cdot\mathbf{x} \in \mathbb{Z}$ modulo p gives a quadratic form on $\overline{L}$, which is clearly well-defined:

$$Q : \overline{L} \to \mathbb{F}_p, \qquad Q(\overline{\mathbf{x}}) = \overline{\tfrac{1}{2}\mathbf{x}\cdot\mathbf{x}}\,.$$

The associated bilinear form,

$$(\overline{\mathbf{x}}, \overline{\mathbf{y}}) = Q(\overline{\mathbf{x}} + \overline{\mathbf{y}}) - Q(\overline{\mathbf{x}}) - Q(\overline{\mathbf{y}}) = \overline{\mathbf{x}\cdot\mathbf{y}}\,,$$

is nondegenerate if and only if $p \not| \operatorname{disc} L$. We shall consider only $L = E$, the self-dual E_8 root lattice, and so $\overline{E} = E/pE$ becomes an $O_8^+(p)$ orthogonal space with quadratic form $Q(\overline{\mathbf{x}}) = \overline{\frac{1}{2}\mathbf{x}\cdot\mathbf{x}}$. Since W preserves E, pE and the inner product $\mathbf{x}\cdot\mathbf{y}$, it acts on $\overline{E}$, preserving the quadratic form Q, and so W acts as an isometry group on the finite orthogonal space $\overline{E}$ of type $O_8^+(p)$. For p odd, this action is faithful (since $-I$ acts nontrivially and $W'/\langle -I\rangle$ is simple); hence $W \overset{\sim}{\subseteq} \mathcal{O}(\overline{E}) \cong GO_8^+(p)$. For $p=2$, $-I$ acts trivially and so $W/\langle -I\rangle$ acts faithfully on an $O_8^+(2)$ orthogonal space, so that $W/\langle -I\rangle \overset{\sim}{\subseteq} GO_8^+(2)$; but comparing orders, we find that equality holds.

6. Ovoid Constructions

Using counting arguments and mathematical induction on the dimension, one obtains the following (also mentioned last semester):

(7.1) An $O_8^+(q)$-space has exactly $q^7 + q^4 - q^3$ singular vectors ($\mathbf{v}$ such that $Q(\mathbf{v}) = 0$), and for each $\alpha \in \mathbb{F}_q \smallsetminus 0$, exactly $q^7 - q^3$ (nonsingular) vectors $\mathbf{v}$ such that $Q(\mathbf{v}) = 0$. (Total: q^8 vectors.)

Consequently,

(7.2) $E/2E$ has $2^7 + 2^4 - 2^3 = 136$ congruence classes with $\frac{1}{2}\mathbf{v}\cdot\mathbf{v} \equiv 0 \mod 2$, and $2^7 - 2^3 = 120$ congruence classes with $\frac{1}{2}\mathbf{v}\cdot\mathbf{v} \equiv 1 \mod 2$ (total: $136 + 120 = 256 = 2^8$ congruence classes).

(7.3) $E/3E$ has $3^7+3^4-3^3 = 2241$ congruence classes with $\frac{1}{2}\mathbf{v}\cdot\mathbf{v} \equiv 0 \mod 3$, and for $k=1,2$, exactly $3^4-3^3 = 2160$ congruence classes with $\frac{1}{2}\mathbf{v}\cdot\mathbf{v} \equiv k \mod 3$ (total: $2241+2160+2160 = 6561 = 3^8$ classes).

The 'Binary' Construction

Let $V_{2m} = \{\mathbf{v} \in E : \mathbf{v}\cdot\mathbf{v} = 2m\}$, so that $|V_{2p}| = 240(p^3+1)$ where p is any *odd* prime. Partition V_{2p} into congruence classes modulo $2E$: for $\mathbf{x} \in V_{2p}$, define

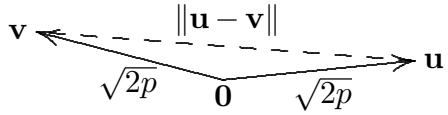
$$[\mathbf{x}] = \{\mathbf{v} \in V_{2p} : \mathbf{v} \equiv \mathbf{x} \mod 2E\}.$$

Now reduce the vectors $\mathbf{v} \in [\mathbf{x}]$ modulo pE to obtain

$$\mathcal{O}_2(\mathbf{x}) = \big\{\langle\overline{\mathbf{v}}\rangle : \mathbf{v} \in [\mathbf{x}]\big\}.$$

(Here $\langle\overline{\mathbf{v}}\rangle = \mathbb{F}_p\overline{\mathbf{v}}$ denotes the *point*, i.e. one-dimensional subspace of $\overline{E}$, spanned by $\overline{\mathbf{v}}$.) We claim that $\mathcal{O}_2(\mathbf{x})$ is an ovoid in $\overline{E}$, for every $\mathbf{x} \in V_{2p}$. Since $Q(\overline{\mathbf{v}}) = \overline{\frac{1}{2}\mathbf{v}\cdot\mathbf{v}} = \overline{p} = 0$ for every $\mathbf{v} \in V_{2p}$, $\mathcal{O}_2(\mathbf{x})$ consists of singular points of $\overline{E}$.

Suppose that $\langle\overline{\mathbf{u}}\rangle$, $\langle\overline{\mathbf{v}}\rangle \in \mathcal{O}_2(\mathbf{x})$ such that $(\overline{\mathbf{u}},\overline{\mathbf{v}}) = 0$, i.e. $\overline{\mathbf{u}}\cdot\overline{\mathbf{v}} \equiv 0 \mod p$. Then $\mathbf{u}\cdot\mathbf{u} = \mathbf{v}\cdot\mathbf{v} = 2p$ and so $(\mathbf{u}-\mathbf{v})\cdot(\mathbf{u}-\mathbf{v}) \equiv 0 \mod p$. But also $\mathbf{u}-\mathbf{v} \in 2E$ implies that $(\mathbf{u}-\mathbf{v})\cdot(\mathbf{u}-\mathbf{v}) \equiv 0 \mod 8$. Together this yields $\|\mathbf{u}-\mathbf{v}\|^2 \equiv 0 \mod 8p$. But $0 \le \|\mathbf{u}-\mathbf{v}\|^2 \le \big(\|\mathbf{u}\| + \|\mathbf{v}\|\big)^2 = \big(\sqrt{2p}+\sqrt{2p}\big)^2 = 8p$.



This allows only two cases: (i) $\mathbf{u}-\mathbf{v} = 0$, or (ii) $\mathbf{u} = -\mathbf{v}$. (We obtain (ii) from the case of equality in the triangle inequality.) But both cases yield the same point $\langle\overline{\mathbf{u}}\rangle = \langle\overline{\mathbf{v}}\rangle$. We conclude that pairs $\pm\mathbf{v} \in [\mathbf{x}]$ yield distinct points in $\mathcal{O}_2(\mathbf{x})$, and that $\mathcal{O}_2(\mathbf{x})$ is a cap of size $\frac{1}{2}\big|[\mathbf{x}]\big|$ in $\overline{E}$.

By the remarks in Section 0, we have $|\mathcal{O}_2(\mathbf{x})| \le p^3+1$, i.e. $\big|[\mathbf{x}]\big| \le 2(p^3+1)$. But we have a partition

$$V_{2p} = \bigcup_{\mathbf{x}\in V_{2p}} [\mathbf{x}]$$

with at most 120 classes by (7.2). Since $|V_{2p}| = 240(p^3+1)$, equality must hold: $\big|[\mathbf{x}]\big| = 2(p^3+1)$, $|\mathcal{O}_2(\mathbf{x})| = p^3+1$. Thus $\mathcal{O}_2(\mathbf{x})$ is an ovoid in $\overline{E}$.

It turns out (see [1]) that different choices of $\mathbf{x} \in V_{2p}$ yield equivalent ovoids $\mathcal{O}_2(\mathbf{x})$ (i.e. equivalent under $GO_8^+(p)$). So fixing some particular choice $\mathbf{x} \in V_{2p}$, we have one 'Conway binary ovoid' in $O_8^+(p)$ for each odd prime p. The stabilizer of such an ovoid in $GO_8^+(p)$ is a subgroup of $W = W(E_8)$ given by $\langle -1\rangle \times W(E_7) \cong 2^2 \times S_6(2)$, of order $2^{11}\cdot 3^5\cdot 5\cdot 7 = 5{,}806{,}080$; here the central factor $\langle -1\rangle$ acts trivially on the ovoid.

The 'Ternary' Construction

For this construction we take p to be a prime ≥ 5, and $V_{4p} = \{\mathbf{v} \in E : \mathbf{v}\cdot\mathbf{v} = 4p\}$, so that $|V_{4p}| = 2160(p^3+1)$. This time we partition V_{4p} into classes modulo $3E$: for $\mathbf{x} \in V_{4p}$, define

$$[\mathbf{x}] = \{\mathbf{v} \in V_{4p} : \mathbf{v} \equiv \mathbf{x} \mod 3E\}.$$

Reduction of the vectors $\mathbf{v} \in [\mathbf{x}]$ modulo pE yields

$$\mathcal{O}_3(\mathbf{x}) = \big\{\langle\overline{\mathbf{v}}\rangle : \mathbf{v} \in [\mathbf{x}]\big\}.$$

Again, $\mathcal{O}_3(\mathbf{x})$ consists of singular points of $\overline{E}$. Suppose that $\langle\overline{\mathbf{u}}\rangle$, $\langle\overline{\mathbf{v}}\rangle \in \mathcal{O}_3(\mathbf{x})$ such that $(\overline{\mathbf{u}},\overline{\mathbf{v}}) = 0$, i.e. $\mathbf{u}\cdot\mathbf{v} \equiv 0 \mod p$. Since $\mathbf{u}\cdot\mathbf{u} = \mathbf{v}\cdot\mathbf{v} = 4p$, we have $(\mathbf{u}-\mathbf{v})\cdot(\mathbf{u}-\mathbf{v}) \equiv 0 \mod p$. Also $\mathbf{u}-\mathbf{v} \in 3E$ implies that $(\mathbf{u}-\mathbf{v})\cdot(\mathbf{u}-\mathbf{v}) \equiv 0 \mod 18$, so $\|\mathbf{u}-\mathbf{v}\|^2 \equiv 0 \mod 18p$. But $0 \leq \|\mathbf{u}-\mathbf{v}\|^2 \leq \big(\|\mathbf{u}\| + \|\mathbf{v}\|\big)^2 = \big(\sqrt{4p}+\sqrt{4p}\big)^2 = 16p$, so $\mathbf{u} = \mathbf{v}$, and so distinct vectors $\mathbf{v} \in [\mathbf{x}]$ yields distinct points $\langle\overline{\mathbf{v}}\rangle \in \mathcal{O}_3(\mathbf{x})$, and $\mathcal{O}_3(\mathbf{x})$ is a cap in $\overline{E}$, of size $|\mathcal{O}_3(\mathbf{x})| = \big|[\mathbf{x}]\big| \leq p^3+1$. But the partition

$$V_{4p} = \bigcup_{\mathbf{x}\in V_{4p}} [\mathbf{x}]$$

has at most 2160 classes by (7.3), each of size at most p^3+1. Since $|V_{4p}| = 2160(p^3+1)$, equality holds: $|\mathcal{O}_3(\mathbf{x})| = p^3+1$ for all $\mathbf{x} \in V_{4p}$, so $\mathcal{O}_3(\mathbf{x})$ is an ovoid.

For $p \equiv 1 \mod 3$, the resulting 'ternary ovoids' do not depend on the choice of $\mathbf{x} \in V_{4p}$, and the stabilizer of such an ovoid in $GO_8^+(p)$, is a subgroup of W given by $\langle -1\rangle \times W(D_7) \cong 2^7{:}S_7$ of order $2^{11}{\cdot}3^2{\cdot}5{\cdot}7 = 624{,}120$.

However, for $p \equiv 2 \mod 3$, depending on the choice of $\mathbf{x} \in V_{4p}$, we obtain either the 'first' or 'second' ternary ovoid. The first type has stabilizer $\langle -1\rangle \times W(E_7) \cong 2^2 \times S_6(2)$, of order $2^{11}{\cdot}3^5{\cdot}5{\cdot}7 = 5{,}806{,}080$; the second type has stabilizer $\langle -1\rangle \times W(A_8) \cong 2 \times \mathrm{S}_9$ of order $2^4{\cdot}3^4{\cdot}5{\cdot}7 = 725{,}760$. In each case $\langle -1\rangle$ acts trivially on the ovoid.

7. References

[1] J. H. Conway, P. B. Kleidman and R. A. Wilson, 'New families of ovoids in O_8^+', *Geom. Ded.* **26** (1988), 157–170.

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups,* Springer-Verlag, 1988.

[3] H. Dym and H. P. McKean, *Fourier Series and Integrals,* Acad. Press, 1972.

[4] A. Ogg, *Modular Forms and Dirichlet Series,* W. A. Benjamin, 1969.

[5] J.-P. Serre, *A Course in Arithmetic,* GTM #7, Springer-Verlag, 1973.

[6] G. Eric Moorhouse, 'Ovoids from the E_8 root lattice', *Geom. Ded.* **46** (1993), 287–297.

[7] M. S. Viazovska, 'The sphere packing problem in dimension 8', preprint, 2016, arXiv:1603.04246