Math 272y: Rational Lattices and their Theta Functions

13, 18, and 20 November 2019: Lattices of level 2 and their theta functions

Let $L \subset \mathbf{R}^n$ be a lattice of level 2, that is, an even lattice such that $L' := (L^*)\langle 2 \rangle$ is also even. (We may allow either L or L' to be self-dual, and thus of level 1, though we have dealt with such lattices already.) As a special case of what we showed last time, the discriminant groups — call them

$$\mathrm{D}(L) = L^*/L, \quad \mathrm{D}(L') = L'^*/L'$$

— are elementary abelian 2-groups with $|\mathrm{D}(L)|\,|\mathrm{D}(L')| = 2^n$. Also, by the part of last lecture's "Theorem 2" that we proved, the weighted theta functions $\theta_{L,P}$ and $\theta_{L',P}$ are modular forms of weight $(n/2) + \deg(P)$ and level 2 for any harmonic polynomial P, and are cusp forms if P is nonconstant. In this installment we show that $\dim_{\mathbf{Z}/2\mathbf{Z}} \mathrm{D}(L)$ and $\dim_{\mathbf{Z}/2\mathbf{Z}} \mathrm{D}(L')$ are even and that $4|n$, determine the discriminant forms on $\mathrm{D}(L)$ and $\mathrm{D}(L')$, construct the ring of modular forms for $\Gamma_1(2)$, and obtain some consequences for the structure of L.

First we analyze the discriminant groups. Recall that $\mathrm{D}(L)$ carries a symmetric pairing $(\cdot, \cdot)$ taking values in $\mathbf{Q}/\mathbf{Z}$. Since L^*/L has exponent 2, this pairing takes values in $\frac{1}{2}\mathbf{Z}/\mathbf{Z}$, so it is more convenient to consider the $(\mathbf{Z}/2\mathbf{Z})$-valued pairing $2(\cdot, \cdot)$. This pairing is alternating: for any $v \in L^*$, let $[v]$ be its coset mod L, and observe that $2([v], [v]) \equiv 2\langle v, v \rangle \bmod 2$, which is zero because L has level 2. Since the pairing is perfect, it follows that $\dim_{\mathbf{Z}/2\mathbf{Z}} \mathrm{D}(L)$ is even, as claimed. The same argument applies to $\dim_{\mathbf{Z}/2\mathbf{Z}} \mathrm{D}(L')$. The sum of these dimensions is n, so we have shown $2|n$; we next prove that in fact $4|n$.

The quadratic form $Q : [v] \mapsto \langle v, v \rangle \bmod 2$ refines the pairing $2(\cdot, \cdot)$. It is known[1] that if V is a $\mathbf{Z}/2\mathbf{Z}$-vector space of dimension $2k > 0$ with a quadratic form $Q : V \to \mathbf{Z}/2\mathbf{Z}$ whose associated alternating form is nondegenerate, then V is isomorphic with one of

$$Q_0 : (x_1, \ldots, x_{2k}) \mapsto \sum_{j=1}^{k} x_{2j-1} x_{2j}, \tag{1}$$

$$Q_1 : (x_1, \ldots, x_{2k}) \mapsto x_1^2 + x_1 x_2 + x_2^2 + \sum_{j=2}^{k} x_{2j-1} x_{2j}. \tag{2}$$

Moreover, $Q_0(x) = 0$ has $2^{2k-1} + 2^{k-1}$ solutions, and Q_0 has isotropic spaces of dimension k (such as the linear combinations of the unit vectors e_{2j} $(1 \leq j \leq k)$ in the coordinates of (1)); while $Q_1(x) = 0$ has $2^{2k-1} - 2^{k-1}$ solutions, and the maximal dimension of an isotropic space of Q_1 is $k - 1$. It soon follows that the direct sum of quadratic forms of the same type (either both Q_0 or both Q_1) is of type Q_0, while the direct sum of a Q_0 and a Q_1 form has type Q_1.

Now a maximal isotropic subspace W for the pairing $2(\cdot, \cdot)$ on $\mathrm{D}(L)$ lifts to a self-dual lattice between L and L^*, which is even if and only if W is isotropic for Q. Thus Q has type Q_0 then the rank of L

---

[1] This comes from the theory of the Arf invariant of quadratic forms in characteristic 2. For vector spaces of dimension $2k > 0$ over finite fields of odd characteristic, there are again two kinds of nondegenerate quadratic form, distinguished by whether their maximal isotropic subspaces have dimension k or $k - 1$; but in that setting there is no associated alternating form.

is a multiple of 8. But the quadratic form on $D(L) \oplus D(L)$ always has type Q_0. Thus $8|2n$, so $4|n$ as claimed. Moreover, if $n \equiv 4 \bmod 8$ then the quadratic form must have type Q_1. We claim that if $8|n$ then the quadratic form on $D(L)$ must have type Q_0. Indeed $L \oplus D_4$ is a level 2 lattice in $\mathbf{R}^{8n+4}$, so the quadratic form on $D(L \oplus D_4)$ must have type Q_1. But this is the direct sum of the forms on $D(L)$ and $D(D_4)$, and $D(D_4)$ has type Q_1 (either by direct computation or because 4 is not 0 mod 8). Hence the form on $D(L)$ must have type Q_0, and we are done. (We could also have used the forms on $D(L)$ and $D(L \oplus D_4)$, instead of $D(L \oplus L)$, to prove that $4|n$. We shall soon see that $4|n$ also follows from the modularity of θ_L in much the same way that we obtained $8|n$ for a self-dual even lattice in $\mathbf{R}^n$.)

To summarize:

Proposition. *Let $L \subset \mathbf{R}^n$ be a lattice of level 2. Then:*
i) $\operatorname{disc} L$ is an even power of 2;
ii) n is a multiple of 4; and
iii) The quadratic form on $D(L)$ has type Q_0 or Q_1 according as n is congruent to 0 or 4 mod 8.

The same results then hold for $L' = (L^*)\langle 2 \rangle$, because L' also has level 2.

Now to the modular forms.

We have seen that the translation $T : z \mapsto z + 1$ and the involution $w_2 : z \mapsto -1/(2z)$ generate a hyperbolic triangle group, with a cusp at $i\infty$ (fixed by T) and elliptic points at $i/\sqrt{2}$ (fixed by w_2) and $(i - 1)/2$ (fixed by $w_2 T$, which has order 4). The index-2 subgroup $\Gamma_1(2)$ is also a triangle group, generated by T and $w_2 T w_2 : z \mapsto z/(1 - 2z)$, with cusps at 0 (fixed by $w_2 T w_2$) and $i\infty$, and an elliptic point at $(1 - i)/2$ fixed by $(w_2 T)^2 : z \mapsto -(z + 1)/(2z + 1)$. For $N = 2$ the congruence subgroup $\Gamma_1(N)$ still contains $-I_2$, so we might worry that the transformation formula

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z) \tag{3}$$

could hold for only one of each pair $\pm \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(2)$. But $(w_2 T)^2$ is represented by $\pm \left(\begin{smallmatrix} -1 & -1 \\ 2 & 1 \end{smallmatrix}\right)$; whichever sign is correct, if we iterate $f((w_2 T)^2 z) = (\pm(2z + 1))^k f(z)$ we find $f(z) = (-1)^k f(z)$ because $\left(\begin{smallmatrix} -1 & -1 \\ 2 & 1 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. It follows that $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and either $\left(\begin{smallmatrix} -1 & -1 \\ 2 & 1 \end{smallmatrix}\right)$ or $-\left(\begin{smallmatrix} -1 & -1 \\ 2 & 1 \end{smallmatrix}\right)$ generate all of $\Gamma_1(2)$, and not just some index-2 subgroup isomorphic with $\Gamma_1(2)/\{\pm 1\}$. Therefore, as was true for $\Gamma(1)$, *every nonzero modular form for $\Gamma_1(2)$ has even weight.*

For $k \in 2\mathbf{Z}$, let $M_k(\Gamma_1(2))$ be the vector space of modular forms of weight k for $\Gamma_1(2)$, and $S_k(\Gamma_1(2))$ its subspace of cusp forms. The involution w_2 acts on these spaces by

$$(w_2 f)(z) = (-2z^2)^{-k/2} f(-1/2z); \tag{4}$$

we choose $-2z^2$ rather than $2z^2$ so that the factor is positive on the imaginary axis.

We shall prove:

Theorem. *For any even integer k,*
i) $M_k(\Gamma_1(2))$ has dimension $\max(\lfloor (k + 4)/4 \rfloor, 0)$;

ii) $S_k(\Gamma_1(2))$ *has dimension* $\dim M_{k-8}(\Gamma_1(2)) = \max(\lfloor (k+4)/4 \rfloor - 2,\ 0)$;

iii) If $M_k(\Gamma_1(2))$ *or* $\dim S_k(\Gamma_1(2))$ *has dimension* d *then the* w_2*-invariant subspace has dimension* $d/2$ *or* $(d+1)/2$ *according as* d *is even or odd.*

That is:

k	<0	0	2	4	6	8	10	12	14	16	18	20	22	24	$\cdots$
$\dim M_k(\Gamma_1(2))$	0	1	1	2	2	3	3	4	4	5	5	6	6	7	$\cdots$
$\dim M_k(\Gamma_1(2))^{w_2}$	0	1	1	1	1	2	2	2	2	3	3	3	3	4	$\cdots$
$\dim S_k(\Gamma_1(2))$	0	0	0	0	0	1	1	2	2	3	3	4	4	5	$\cdots$
$\dim S_k(\Gamma_1(2))^{w_2}$	0	0	0	0	0	1	1	1	1	2	2	2	2	3	$\cdots$

Our proof will use what we already know for $M_k(\Gamma(1))$ and $S_k(\Gamma(1))$, and will also parallel some of Serre's treatment of modular forms for $\Gamma(1)$ (see Chapter VII, Theorem 4 of *A Course in Arithmetic*).

We begin by showing for each k that all nonzero $f \in M_k(\Gamma_1(2))$ have the same number of zeros in a fundamental domain $\mathcal{F}_2$ for $\Gamma_1(2)$, counted with multiplicity. This is entirely analogous to Serre's calculation in Theorem 3;[2] the final answer is $k/4$ instead of $k/12$, coming from an integral over a contour integral over the quarter-circle $\{z \in \mathcal{H} : |z| = 1/\sqrt{2},\ |\mathrm{Re}(z)| \le 1/2\}$ rather than the $1/12$-circle $\{z \in \mathcal{H} : |z| = 1,\ 0 \le \mathrm{Re}(z) \le 1/2\}$. (Check: if f is actually in $M_k(\Gamma(1))$ then it has $k/12$ roots in $\mathcal{F}_1$, and $[\Gamma(1) : \Gamma_1(2)] = 3$ so $\mathcal{F}_2$ can be dissected into three copies of $\mathcal{F}_1$ and there are $3(k/12) = k/4$ roots in $\mathcal{F}_2$.) As with $\Gamma(1)$, we must specify how to count zeros at cusps and elliptic points for $\Gamma_1(2)$. The cusp at $i\infty$ is counted as for Γ_1: if $f = a_n q^n + O(q^{n+1})$ at $i\infty$ for some $n \in \mathbf{Z}$ and $a_n \ne 0$, then we assign f valuation n at infinity. An n-th order zero at an elliptic point in the orbit of $(1-i)/2$ are counted with multiplicity $n/2$. Finally, at $z = 0$ the valuation of f is the valuation of $w_2 f$ at $z = i\infty$.

At this point we already know that there are no nonzero modular forms of negative weight, nor any nonzero cusp forms of weight $k < 8$ (because there are now two cusps, $k/4 \ge 2$). It also soon follows that $\dim M_k(\Gamma_1(2))$ and $\dim S_k(\Gamma_1(2))$ can be no larger than $\lfloor (k+4)/4 \rfloor$ and $\lfloor (k+4)/4 \rfloor - 2$ respectively, for instance by considering the largest possible order of a zero at $i\infty$. So it remains to construct enough modular forms of each weight.

We noted already that if $f \in M_k(\Gamma(1))$ then *a fortiori* $f \in M_k(\Gamma_1(2))$. But then $w_2 f \in M_k(\Gamma_1(2))$ also, and

$$(w_2 f)(z) = (-2z^2)^{-k/2} f(-1/2z) = (-2z^2)^{-k/2}(-2z)^k f(2z) = (-2)^{k/2} f(2z). \qquad (5)$$

So for each even $k \ge 4$ we have two linearly independent modular forms for $\Gamma_1(2)$, namely $\mathsf{E}_k(z)$ and $\mathsf{E}_k(2z)$. This proves our theorem for $k = 4$ and $k = 6$.

For $k = 0$, the space M_k consists of the constant functions. For $k = 2$, the Eisenstein series

$$\mathsf{E}_2(z) = \frac{1}{2\pi i} \frac{\frac{d}{dz}\Delta(z)}{\Delta(z)} = \frac{q\frac{d}{dq}\Delta(z)}{\Delta(z)} = 1 - 24 \sum_{m=1}^{\infty} \frac{mq^m}{1-q^m} \qquad (6)$$

---

[2]Warning: formula (19) in Serre gives the answer as $k/6$, not $k/12$, but that is because he computes it for a form of weight $2k$, not k.

does not give a modular form for $\Gamma(1)$, but (as suggested by (5))

$$\mathrm{E}_2(z) = 2\mathrm{E}_2(2z) - \mathrm{E}_2(z) = 1 + 24 \sum_{m=1}^{\infty} \left(\frac{mq^m}{1-q^m} - \frac{2mq^{2m}}{1-q^{2m}} \right) = 1 + 24 \sum_{m=1}^{\infty} \frac{mq^m}{1+q^m} \qquad (7)$$

is a modular form for $\Gamma_1(2)$: it is $-1/(2\pi i)$ times the logarithmic derivative of the $\Gamma_1(2)$-invariant modular function

$$h_2(z) := \Delta(z)/\Delta(2z) = q^{-1} - 24 + 276q - 2048q^2 + 11202q^3 - 49152q^4 + 184024q^5 - + \cdots , \quad (8)$$

from which we soon see that $E_2(-1/2z) = -2z^2 E_2(z)$; since clearly $E_2(z+1) = E_2(z)$ we conclude that E_2 generates $M_2(\Gamma_1(2))$ and is invariant under the action (4) of w_2.

For $n > 0$ the q^n coefficient of E_2 is 24 times the sum of the *odd* factors of n, which we can also write as $24(\sigma_1(n) - 2\sigma_1(n/2))$ with the convention that $\sigma_k(n) = \sum_{d|n} d^k$ is zero if n is not a positive integer. [Numerical check: a modular form of weight 2 for $\Gamma_1(2)$ must vanish at $(i-1)/2$, where $q = -e^{-\pi}$. For $1 + 24(q + q^2 + \cdots)$ to vanish we should have $q/(1-q) \doteq -1/24$, so $q \doteq -1/23$, and indeed $e^{\pi} = 23.14+$; high-precision numerical calculation of $\sum_{m=1}^{\infty} mq^m/(1+q^m)$ for $q = -e^{-\pi}$ is also consistent with the expected value of $-1/24$.]

We pause briefly to note that since E_2 generates $M_2(\Gamma_1(2))$ and has constant coefficient 1 it must be equal to θ_{D_4}. Therefore $24(\sigma_1(n) - 2\sigma_1(n/2))$ is also the number vectors of norm $2n$ in D_4, and thus the number of vectors of norm n in D_4^*, because $D_4^* \cong D_4\langle 1/2 \rangle$. This is equivalent with Jacobi's four-square theorem: if n is even then all the norm-n vectors in D_4^* are in D_4, and thus in $\mathbf{Z}^4$; while if n is odd then $1/3$ of the norm-n vectors in D_4^* have integer coordinates, so the number of such vectors is $8(\sigma_1(n) - 2\sigma_1(n/2))$.

We next construct a nonzero cusp form $\Delta_{(2)}$ of weight 8. This form is analogous to the cusp form Δ of weight 12 for $\Gamma(1)$: it must have simple zeros at the cusps $z = i\infty$ and $z = 0$, and no zeros in $\mathcal{H}$; thus once we have constructed $\Delta_{(2)}$ we will have an isomorphism $f \mapsto \Delta_{(2)}f$ from each $M_k(\Gamma_1(2))$ to $S_{k+8}(\Gamma_1(2))$. We form $\Delta_{(2)}$ as the product of two forms of weight 4, one vanishing at $i\infty$, the other at 0. The first is

$$\frac{1}{240}(\mathsf{E}_4(z) - \mathsf{E}_4(2z)) = q + 8q^2 + 28q^3 + 64q^4 + 126q^5 + 224q^6 + \cdots ; \qquad (9)$$

the second is

$$\frac{1}{15}(16\mathsf{E}_4(2z) - \mathsf{E}_4(z)) = 1 - 16q + 112q^2 - 448q^3 + 1136q^4 - 2016q^5 + - \cdots , \qquad (10)$$

which vanishes at $z = 0$ because it is the proportional to the image of (9) under the action (4) of w_2. Then

$$\begin{aligned} \Delta_{(2)} &= \frac{1}{3600}(\mathsf{E}_4(z) - \mathsf{E}_4(2z))(16\mathsf{E}_4(2z) - \mathsf{E}_4(z)) \\ &= q - 8q^2 + 12q^3 + 64q^4 - 210q^5 - 96q^6 + 1016q^7 - 512q^8 \cdots . \end{aligned} \qquad (11)$$

[As with Δ, these modular forms have product formulas in terms of $\eta = q^{1/24} \prod_{m=1}^{\infty}(1 - q^m)$: the forms (9,10) are $\eta(2z)^{16}/\eta(z)^8$ and $\eta(z)^{16}/\eta(2z)^8$ respectively, whence $\Delta_{(2)}$ is $(\eta(z)\eta(2z))^8 = (\Delta(z)\Delta(2z))^{1/3}$.]

Next we show that $S_k(\Gamma_1(2))$ has codimension 2 in $M_k(\Gamma_1(2))$ for each $k \geq 8$; this will complete the proof of parts (i) and (ii) of our theorem by induction on $\lfloor k/8 \rfloor$, since we have already checked it for $k = 0, 2, 4, 6$ and shown that $\dim S_k(\Gamma_1(2)) = \dim M_{k-8}(\Gamma_1(2))$ for $k \geq 8$. It is enough to construct modular forms of weight k that vanish on just one of the cusps. We do this by generalizing (9,10): the form $\mathsf{E}_k(z) - \mathsf{E}_k(2z)$ vanishes at $z = i\infty$, while $2^k \mathsf{E}_k(2z) - \mathsf{E}_k(z)$ is a multiple of $w_2(\mathsf{E}_k(z) - \mathsf{E}_k(2z))$ and thus vanishes at $z = 0$; moreover $2^k \mathsf{E}_k(2z) - \mathsf{E}_k(z)$ plainly does not vanish at $z = i\infty$, whence the former is nonzero at $z = 0$. Therefore the $S_k(\Gamma_1(2))$ cosets of $\mathsf{E}_k(z)$ and $\mathsf{E}_k(2z)$ are a basis for the quotient space $M_k(\Gamma_1(2))/S_k(\Gamma_1(2))$.

Finally part (iii) of the theorem can also be obtained by induction on $\lfloor k/8 \rfloor$, keeping track of the action of w_2 on E_2, $\mathsf{E}_k(z)$, $\mathsf{E}_k(2z)$, and $\Delta_{(2)}$; the w_2-invariant forms are the polynomials in E_2 and $\Delta_{(2)}$.

Now suppose $L \in \mathbf{R}^n$ is a lattice of level 2 with discriminant 2^{2r}. Then $\theta_L \in M_{n/2}(\Gamma_1(2))$, and this theta function must satisfy two linear conditions: the q-expansion of θ_L must have constant term 1, but moreover

$$\theta_L(z) = 2^{-r}(z/i)^{-n/2}\theta_{L'}(-1/2z) = 2^{(n/4)-r}(w_2\theta_L)(z), \tag{12}$$

so the q-expansion of $w_2\theta_L$ must have constant term $2^{(n/4)-r}$. Once $n \geq 8$ these conditions are independent, and determine $\theta_L \bmod S_{n/2}(\Gamma_1(2))$. If P is a nonconstant harmonic polynomial then $\theta_{L,P} \in S_{(n/2)+\deg P}(\Gamma_1(2))$, and if $N_{\min}(L)$ or $N_{\min}(L')$ exceed 2 then $\theta_{L,P}$ must vanish to higher order at the cusp $z = i\infty$ or $z = 0$ respectively.

In particular, for $n = 4, 8, 12$ the rank n and discriminant 2^{2r} determine θ_L uniquely. We warn that it does *not* follow automatically that L is determined up to isomorphism. Recall that for self-dual L of rank $n < 8$ we showed that $\theta_L = \theta_{\mathbf{Z}}^n$, and deduced that $L \cong \mathbf{Z}^n$ but this required an additional argument. We cannot do this for lattices of level 2; it happens that L is unique for each (n, r) with $n = 4$ or $n = 8$, but for $n = 12$ there is more than one L for each choice of r.

The case of $r = n/4$ is of particular interest: then $\operatorname{disc} L = \operatorname{disc} L'$, so it may happen that $L \cong L'$. This occurs for $L = D_4^r$, and for some but not all other lattices of discriminant $2^{n/2}$. If $L \cong L'$ then $\theta_L = \theta_{L'}$; it then follows from (12) that θ_L is in the w_2-invariant subspace of $M_{n/2}(\Gamma_1(2))$, and is therefore a polynomial in E_2 and $\Delta_{(2)}$. This situation is quite similar to what we saw for self-dual even lattices: $N_{\min}(L) \leq 2\lfloor n/16 \rfloor + 2$, with equality if and only if θ_L is the "extremal" modular form in $M_{n/2}(\Gamma_1(2))^{w_2}$ (whose $q^{\lfloor n/16 \rfloor + 1}$ coefficient is positive by the same argument we gave for E_4 and Δ, since E_2 and $1/\Delta_{(2)}$ have positive q-expansions). Moreover, if equality is attained then each shell of L is a spherical d-design where $d = 7, 5, 3, 1$ for $n \equiv 0, 4, 8, 12 \bmod 16$. It is not known for which n such lattices exist, though n is bounded above because eventually the $q^{\lfloor n/16 \rfloor + 2}$ coefficient is negative. Known examples include several lattices for which L yields the record lattice packing in $\mathbf{R}^n$, notably $n = 4, 16, 32$. For $n = 4$ this is the D_4 lattice, and for $n = 16$ the Barnes–Wall lattice BW_{16}, which is also the laminated lattice Λ_{16}, and to which we devote the last section of this chapter of the notes. For $n = 32$ several such lattices are known, the first of which was found by H.-G. Quebbemann.[3] As

---

[3] The OEIS entry (A002272) for the theta series cites his papers "Lattices with theta-functions for $G(\sqrt{2})$ and linear codes" (*J. Alg.* **105**, 443–450 (1987)) and "Modular lattices in Euclidean spaces" (*J. Number Theory* **54**, 190–202 (1995)). Another level-2 lattice L with the same theta function but *not* isomorphic with L' is described in my paper "Mordell–Weil lattices in characteristic 2: I. Construction and first properties" (*International Math. Research Notices* **1994** #8, 343–361); since $L \not\cong L'$, the lattice L' is another example. Several more are listed online in the Nebe-Sloane catalogue of lattices.

with the $n = 48$ case of extremal self-dual lattices, it is anybody's guess how many more such lattices there might be, if any.

We next list and describe the level-2 lattices in $\mathbf{R}^n$ for $n = 4, 8, 12$, and report on what is known for $n = 16$ and $n = 20$.

$\underline{n = 4}$: We noted already that the only possibility is $L = D_4$, with $\theta_L = E_2$. The shells of D_4 form spherical 5-designs: there are no cusp forms of weight less than 8, so $\theta_{D_4, P} = 0$ for all nonconstant harmonic P of degree less than $8 - (n/2) = 6$. Here, as was true of E_8 and the Leech lattices, the design property can also be deduced from the automorphism group, which for D_4 is $W(D_4) : S_3 = W(F_4)$ with invariant degrees $2, 6, 8, 12$, so every invariant of degree < 6 is a polynomial in the norm.

As we did for E_8, Λ_{24}, etc., we can now fix a vector $v_0 \in D_4$ and obtain conditions on the numbers $N_k(v_0)$ of D_4 roots v such that $\langle v, v_0 \rangle = k$. For example, if v_0 is itself a root then $N_{\pm 2}(v_0) = 1$, $N_{\pm 1}(v_0) = 8$, and $N_0(v_0) = 6$. A new feature is that we can do this also for $v_0 \in D_4^*$, when (v, v_0) is still constrained to be integral. For example, if $\langle v_0, v_0 \rangle = 1$ then $|\langle v, v_0 \rangle| \le 1$ by Cauchy-Schwarz, and we compute that $N_{\pm 1}(v_0) = 6$ and $N_{\pm 0}(v_0) = 12$ (check: the orthogonal complement of v_0 is A_3, which indeed has kissing number 12). If $\langle v_0, v_0 \rangle = 2$ then we are again in the case of a D_4 root; for $\langle v_0, v_0 \rangle = 3$ we compute $N_{\pm 2}(v_0) = 3$ and $N_{\pm 1}(v_0) = N_0(v_0) = 6$. (All such v_0 are still equivalent under $\mathrm{Aut}(D_4)$.)

$\underline{n = 8}$: There are three possible discriminants, $\mathrm{disc}(L) = 2^{2r}$ with $r = 1, 2, 3$, each realized by a unique lattice. The theta function is completely determined by by the condition that θ_L and $\theta_{L'}$ both have constant term 1; in particular the root number $N_2(L)$ is $16(2^{4-r} - 1)$. We tabulate the theta functions, root numbers, and lattices:

$D = 2^{2r}$	θ_L	$N_2(L)$	L
2^2	$\frac{1}{15}(8\mathsf{E}_4(2z) + 7\mathsf{E}_4(z))$	$16 \cdot 7 = 112$	D_8
2^4	$E_2^2 = \frac{1}{5}(4\mathsf{E}_4(2z) + \mathsf{E}_4(z))$	$16 \cdot 3 = 48$	D_4^2
2^6	$\frac{1}{15}(14\mathsf{E}_4(2z) + \mathsf{E}_4(z))$	$16 \cdot 1 = 16$	$D_8' = (D_8^*)\langle 2 \rangle = (A_1^8)^+$

We have already shown that D_8 is unique (for instance, by gluing to D_8 to get one of the two even unimodulars in $\mathbf{R}^{16}$, which must be $(D_{16})^+$ because E_8^2 does not contain D_8 as a saturated sublattice). We can now also deduce its uniqueness from the root number: since 112 roots is too few for E_7 or E_8, the only available simple factor with a Coxeter number as large as $112/8 = 14$ is D_8. By duality it follows that the lattice of discriminant 2^6 is unique too; this lattice $(D_8^*)\langle 2 \rangle = (A_1^8)^+$ is often called the "Nikulin lattice" in the context of intersection pairings in algebraic geometry. For the remaining case, with discriminant 2^4, we can again use the classification of root lattices now that we know θ_L and thus $N_2(L)$; here the count of 48 can be attained by two other root systems of rank at most 8, but these others are $A_1 A_2 D_5$ and $A_2 A_6$, which are impossible because each has rank 8 and non-square discriminant (namely 24 and 21).

We can now use the formulas for θ_{D_8} and $\theta_{D_8'}$ to prove the Jacobi-Eisenstein formula

$$r_8(n) = 16(-1)^n \sum_{d|n} (-1)^d d^3 \tag{13}$$

6

for the number of representations of a positive integer n as a sum of 8 squares. If n is odd then $r_8(n)$ is the number of representations of n by D_8^*, which is the coefficient of q^n in the theta function $(14\mathsf{E}_4(2z) + \mathsf{E}_4(z))/15$ of D_8'; the $\mathsf{E}_4(2z)$ term does not contribute because n is odd, and $\mathsf{E}_4(z)/15$ contributes $(240/15)\sigma_3(n)$, which is the same as (13). When n is even, $r_8(n)$ is the $q^{n/2}$ coefficient of θ_{D_8}, which is $112\sigma_3(n/2) + 128\sigma_3(n/4)$; we leave the identification of this with (13) as an elementary exercise.

$\underline{n = 12}$: Here there are five possible discriminants; again the theta function is completely determined in each case, but L is no longer unique: there are three possible L with disc $L = 2^6$, and two for each of the other discriminants 2^{2r} with $r = 1, 2, 4, 5$. Thus we have several examples of isospectral tori $\mathbf{R}^{12}/L$ of dimension 12. In particular for $r = 1$ we find two *root lattices* D_{12} and D_4E_8 with the same theta function; this might be the only such example (up to taking powers, or direct sums with some other root lattice). The lattices can also be distinguished by the configuration of minimal vectors of L^*: both D_{12}^* and $(D_4E_8)^*$ have 24 vectors of minimal norm 1, but for D_{12}^* they form an orthogonal frame, while for $(D_4E_8)^*$ they span the 4-dimensional D_4 subspace.

For each r the root number is $N_2(L) = 8(2^{6-r} + 1)$. We tabulate the five theta functions and the $2 + 2 + 3 + 2 + 2$ lattices:

$D = 2^{2r}$	θ_L	$N_2(L)$	L
2^2	$\frac{1}{21}(32\mathsf{E}_6(2z) - 11\mathsf{E}_6(z))$	$8 \cdot 33 = 264$	D_{12}, D_4E_8
2^4	$\frac{1}{63}(80\mathsf{E}_6(2z) - 17\mathsf{E}_6(z))$	$8 \cdot 17 = 136$	$D_4D_8, (A_1^5E_7)^+$
2^6	$\mathsf{E}_2^3 = \frac{1}{7}(8\mathsf{E}_6(2z) - \mathsf{E}_6(z))$	$8 \cdot 9 = 72$	$D_4^3, (A_1^6D_6)^+, (E_6 \oplus (E_6\langle 2\rangle))^{+3}$
2^8	$\frac{1}{63}(68\mathsf{E}_6(2z) - 5\mathsf{E}_6(z))$	$8 \cdot 5 = 40$	$(A_1^8)^+D_4, (D_5 \oplus (E_7\langle 2\rangle))^+$
2^{10}	$\frac{1}{21}(22\mathsf{E}_6(2z) - \mathsf{E}_6(z))$	$8 \cdot 3 = 24$	$(A_1^{12})^+, D_4 \oplus (E_8\langle 2\rangle)$

The lattices with $\mathrm{disc}(L) = 2^2$ are the D_4 complements in the even unimodular lattices D_{16}^+ and E_8^2 in $\mathbf{R}^{16}$. This also gives the level-2 lattices L' of discriminant 2^{10}. The formula for $\theta_{D_{12}}$ yields the twelve-square theorem for even integers:

$$r_{12}(2n) = 264\sigma_5(n) - 768\sigma_5(n/2). \tag{14}$$

The formula for $r_{12}(n)$ is not so simple when n is odd: the σ_5 terms give only an approximation, with an error term $O(n^{\frac{5}{2}+o(1)})$ that is a coefficient of a cusp form of weight 6.

For $r = 2, 3, 4$ one could also classify the lattices L using the gluing method, or as sublattices of index 2^{r-1} in D_{12} or D_4E_8; but this is not so easy because neither the gluing map nor the superlattice is uniquely determined, so one gets each L several times and must check for isomorphisms among them. Instead we computed the $r = 2$ and $r = 3$ lists using the 2-neighbor method, and then recovered the $r = 4$ list as $\{L' : \mathrm{disc}(L) = 2^4\}$. In the $\mathrm{disc}(L) = 2^6$ row, all three lattices satisfy $L \cong L'$.

We also used the 2-neighbor method to check the lists for $(n, r) = (12, 1)$ and $n < 12$, and to check or generate the data reported below for $n = 16$ and $n = 20$.

$\underline{n = 16}$: Here for the first time disc L does not determine θ_L uniquely, because $\dim M_8(\Gamma_1(2)) > 2$. Still θ_L is a linear combination of $\mathsf{E}_8(z)$, $\mathsf{E}_8(2z)$, and $\Delta_{(2)}(z)$; the first two coefficients are determined

by disc L, and then the coefficient of $\Delta_{(2)}(z)$ is determined by the number $N_2(L)$ of roots of L (which thus also determines $N_2(L')$). For example, the theta functions of D_{16} and D'_{16} are

$$\frac{1}{255}\left(127\mathsf{E}_8(z) + 128\mathsf{E}_8(2z) + 61440\Delta_{(2)}(z)\right) = 1 + 480q + 29152q^2 + 525952q^3 + \cdots, \quad (15)$$

$$\frac{1}{255}\left(\mathsf{E}_8(z) + 254\mathsf{E}_8(2z) + 7680\Delta_{(2)}(z)\right) = 1 + 32q + 480q^2 + 4480q^3 + \cdots. \quad (16)$$

Thus the number of representations of a positive even integer as a sum of 16 squares is

$$r_{16}(2n) = \frac{32}{17}\left(127\sigma_7(n) + 128\sigma_7(n/2) + 128\tau_2(n/2)\right), \quad (17)$$

while $r_{16}(n) = (32\sigma_7(n) + 512\tau_2(n))/17$ for n odd, where $\tau_2(n/2)$ is the $q^{n/2}$ coefficient of $\Delta_{(2)}$; so for example if p is an odd prime then

$$r_{16}(p) = \frac{32}{17}\left(p^7 + 1 + 16\tau_2(p)\right), \quad r_{16}(2p) = \frac{32}{17}\left(127(p^7+1) + 128\tau_2(p)\right), \quad (18)$$

with $|\tau_2(p)| \leq 2p^{7/2}$.

The lattices of discriminant 2^2 are the complements of D_8 in the six Niemeier lattices N whose root lattices $R(N)$ contain D_r for some $r \geq 8$:

$R(N)$	D_{24}	$D_{16}E_8$	$D_{10}E_7^2$	D_{12}^2	D_8^3	$A_{15}D_9$
L	D_{16}	D_8E_8	$(A_1^2E_7^2)^+$	$(D_4D_{12})^+$	$(D_8^2)^+$	$(A_{15}^+ \oplus \mathbf{Z}\langle 4\rangle)^+$
$N_2(L)$	480	352	256	288	224	240
$N_2(L')$	32	16	4	8	0	2

The linear relation between $N_2(L)$ and $N_2(L')$ is $N_2(L) - 8N_2(L') = 224$.

The lattices of discriminant 2^4 are Niemeier complements of D_4^2; there are 11, with root numbers

$$96,\ 128,\ 2*144,\ 160,\ 2*192,\ 224,\ 2*288; \quad (19)$$

the last pair is $D_4^2E_8$ and D_4D_{12}, but the other two isospectral pairs are new. Here the root numbers of L and L' are related by $N_2(L) - 4N_2(L') = 96$. For discriminant 2^6, there are 17 lattices, with root numbers

$$32,\ 48,\ 2*64,\ 2*80,\ 3*96,\ 112,\ 2*128,\ 144,\ 2*160,\ 192,\ 256 \quad (20)$$

including an isospectral triple; the maximal root number 256 is achieved by $L = (A_1^8)^+E_8$. In each casel $N_2(L) - 2N_2(L') = 32$.

The case of discriminant 2^8 is the most interesting. Here necessarily $\theta_L = \theta_{L'}$, though again it does not follow that $L \cong L'$. There are 24 lattices, first determined by Scharlau and Venkov in 1994;[4] nowadays

---

[4]Rudolf Scharlau and Boris B. Venkov: The genus of the Barnes–Wall lattice, *Comment. Math. Helv.* **69** (2), 322–333 (1994). NB in this paper a "root" means either a root of L or a vector of norm 4 in L that corresponds to a root of L'; either kind of "root" yields a reflection acting on L and L'. For the uniqueness of the Barnes–Wall lattice, Scharlau and Venkov cite Quebbemann's 1995 paper "Modular lattices in Euclidean spaces" cited in an earlier footnote, which at the time was still a preprint ("Universität Bielefeld, Sonderforschungsbereich 343, Preprint 93-031").

this calculation is routine (the 2-neighbor verification took about 5 minutes), but the result is still of interest, being analogous to Venkov's proof of the Niemeier classification — and not just because of the coincidence of 24 lattices in each case: it follows from the computation of $M_{10}(\Gamma_1(2))$ that the root lattices of L and L' taken together form a spherical 3-design, and must thus satisfy a Coxeter-number constraint; and each candidate pair $(R(L), R(L'))$ that is consistent with $\mathrm{disc}(L) = 2^8$ arises for a unique (L, L'). (This time it is not quite true that the square-discriminant condition is satisfied automatically; here this condition excludes one of the possible $(R(L), R(L'))$ that passes the Coxeter-number test.) Also, in each case $R(L)$ and $R(L')\langle 2\rangle$ span a finite-index sublattice of L, except for the case that L and L' have no roots, in which case an additional argument is needed as was the case for Λ_{24}.

Of the 24 lattices L, there are 8 with $L \not\cong L'$, in four isospectral pairs with $N_2(L) = N_2(L') = 48$, 64, 80, 144. The root numbers for the other 16 are

$$0, \ 16, \ 24, \ 2*32, \ 40, \ 2*48, \ 64, \ 72, \ 3*96, \ 112, \ 128, \ 240, \tag{21}$$

so there are in total two isospectral triples (with $N_2 = 64$ and 96), and a quadruple at $N_2 = 48$.

The case of $N_2(L) = N_2(L') = 0$ is of particular interest. Here

$$\theta_L = E_2^4 - 96\Delta_{(2)} = 1 + 4320q^2 + 61440q^3 + 522720q^4 + 2211840q^5 + \cdots, \tag{22}$$

or in terms of Eisenstein series of weight 8

$$\theta_L = \frac{1}{17}\left(\mathsf{E}_8(z) + 16\mathsf{E}_8(2z) - 480\Delta_{(2)}(z)\right). \tag{23}$$

This theta series characterizes the Barnes–Wall lattice $BW_{16} = \Lambda_{16}$, as Λ_{24} was characterized in $\mathbf{R}^{24}$ by the condition of being even and self-dual with no roots. It turns out that Λ_{16} can be found in Λ_{24} as the orthogonal complement of a sublattice $E_8\langle 2\rangle$. One can also construct Λ_{16} directly, analogous to Leech's construction of the index-2 sublattice of Λ_{24} (here no norm-doubling translate is possible). Start with the lattice

$$L_1 = \{x \in \mathbf{Z}^{16}\langle 1/2\rangle : x \bmod 2 \in H\}, \tag{24}$$

where H is the *Hadamard code* of length 16, generated by the columns of

$$\begin{pmatrix} 0000000011111111 \\ 0000111100001111 \\ 0011001100110011 \\ 0101010101010101 \\ 1111111111111111 \end{pmatrix}^{\mathsf{T}} \tag{25}$$

(note the transpose). We claim that L_1 is an even lattice with $R(L_1) = (2\mathbf{Z}^{16})\langle 1/2\rangle \cong A_1^{16}$, and that $\sum_{j=1}^{16} x_j \equiv 0 \bmod 2$ for all $x \in L_1$. Then Λ_{16} is the index-2 sublattice $\{x \in L_1 : \sum_{j=1}^{16} x_j \equiv 0 \bmod 4\}$.

In general, For any $m \geq 0$ the *Hadamard code* of length 2^m is the binary code $C \subset (\mathbf{Z}/2\mathbf{Z})^{2^m}$ defined as follows: the 2^m coordinates are identified with a vector space U of dimension m over $\mathbf{Z}/2\mathbf{Z}$, and

C consists of affine-linear maps $U \to \mathbf{Z}/2\mathbf{Z}$. This code has dimension $m + 1$, and consists of the all-zero and all-one words together with the $2^{m+1} - 2$ words of weight $2^{m/2}$ that are the characteristic functions of either a hyperplane in U or its complement. Thus C is a $[2^m, m+1, 2^{m-1}]$ code. For $m = 1$ this is the full Hamming space $(\mathbf{Z}/2\mathbf{Z})^U$; for $m = 2$, the $[4, 3, 2]$ parity check code; and for $m = 3$, the $[8, 4, 4]$ extended Hamming code. In general the code is generated by the all-ones vector together with the columns of a matrix whose rows are all 2^m binary vectors of length m.

Thus we are using the $m = 4$ code, which has parameters $[16, 5, 8]$. Since all words have weight $0 \bmod 8$, all $x \in L_1$ have even norm and satisfy $\sum_{j=1}^{16} x_j \equiv 0 \bmod 2$; moreover, $\langle x, x \rangle = 2$ if and only if x is one of the $2 \cdot 16$ doubled unit vectors $\pm 2e_j$. Therefore L is even, with $N_{\min}(L) \geq 4$ (and thus $N_{\min}(L) = 4$, attained by $\pm 2e_j$ and by preimages of the Hadamard words of weight 8). We compute

$$\operatorname{disc} L = [L_1 : L]^2 [L_1 : A_1^{16}]^{-2} \operatorname{disc} A_1^{16} = 2^2 \, 2^{-10} \, 2^{16} = 2^8. \tag{26}$$

It remains to show that L is of level 2. The dual of L_1 is the preimage in $\mathbf{Z}^{16}\langle \frac{1}{2} \rangle$ of the dual of H (and likewise for the dual of any lattice between $2\mathbf{Z}^{16}\langle \frac{1}{2} \rangle$ and $\mathbf{Z}^{16}\langle \frac{1}{2} \rangle$, so e.g. SPLAG on "Construction A"); since H contains the all-1 word, every word in the dual code has even weight, so all norms in L_1 are integral and L_1 is of level 1. (This L_1 is the level 2 lattice of rank 16 and discriminant 2^6 with the smallest root number listed in (20), namely 32; the lattice L_1' and its level-2 sublattices are the unique lattice of level 2 and discriminants 2^{10}, 2^{12}, 2^{14} that have no vectors of norm 2.) The dual of L is generated by L_1 and $\frac{1}{2} \sum_{j=1}^{16} e_j$, which again has integral norm. Thus $L' = L^*\langle 2 \rangle$ is an even lattice, so L has level 2 as claimed.

It is not obvious from our construction that $L' \cong L$. This isomorphism can be recovered from $\operatorname{Aut}(L)$ (which, as with $\operatorname{Aut}(\Lambda_{24})$, is not fully visible in our construction either).[5] Of course the isomorphism also follows from the fact that L is characterized among level 2 lattices by its rank, discriminant, and minimal norm.

For $\underline{n = 20}$, the level-2 lattices are known for all possible $\operatorname{disc} L$ except the one discriminant 2^{10} that makes $\operatorname{disc} L' = \operatorname{disc} L$. The discriminant 2^2 lattices are Niemeier complements of D_4; there are 18.[6] The numbers of level-2 lattices of rank 20 and discriminant 2^4, 2^6, and 2^8 are are 68, 211, and 410 respectively (and thus dually the same counts for discriminants 2^{16}, 2^{14}, and 2^{12}); as far as I know these counts were not known before February of this year, and the enumeration for discriminant 2^{10} is still not complete.

For $n > 20$, as far as I know the level-2 lattices are known only for $n = 24$ and discriminant 2^2 (and dually 2^{22}): the lattices L of discriminant 2^2 are in one-to-one correspondence with the 273 odd

---

[5]For more on this, including the symmetry groups of Barnes–Wall lattices of other power-of-2 dimensions, see Benedict H. Gross: Group representations and lattices, *J. Amer. Math. Soc.* **3** #4, 929–960 (October 1990).

[6]See for instance Table 1 in the paper

Noam D. Elkies and Matthias Schütt: Genus 1 Fibrations on the Supersingular K3 Surface in Characteristic 2 with Artin Invariant 1, *Asian J. Math.* **19** #3 (2015), 555–581. arXiv:1207.1239

The connection with elliptic fibrations of supersingular K3 surfaces also motivated the more recent enumerations of level-2 lattices of rank 20 and discriminant $\neq 2^2, 2^{18}$.

unimodular lattices in $\mathbf{R}^{24}$, and those of discriminant 2^{22} are the corresponding L'.

We conclude by proving[7] that the Barnes–Wall lattice Λ_{16} is the only level-2 lattice $L \subset \mathbf{R}^{16}$ with disc $L = 2^8$ and $N_{\min}(L) > 2$. We have seen that $\theta_{L'}$ is given by (22), so in particular L' contains $4320 = 2^5 \, 135$ vectors of norm 4. Consider their images in $L'/2L'^* \cong \mathrm{D}(L)$. The image of any $v \in L'$ in $\mathrm{D}(L)$ has $Q = 0$ or $Q = 1$ according as $\langle v, v \rangle \equiv 0$ or $2 \bmod 4$. Since $\mathrm{D}(L')$ has Arf invariant 0, it has $2^7 + 2^3 - 1 = 135$ nonzero elements on which $Q = 0$. If $\langle v, v \rangle = 4$ then its image in $\mathrm{D}(L')$ is one of these 135. Hence there are on average $2^5 = 32$ vectors of norm 4 in each of the nonzero cosets of L' in $2L'^*$ on which the norm is doubly even. But if v, v' are vectors in the same coset with $v' \neq \pm v$ then each of $v \pm v'$ is a nonzero vector in $2L'^* = L\langle 2 \rangle$, and thus has norm at least 8. As happened already for $E_8/2E_8$ and $\Lambda_{24}/2\Lambda_{24}$, it follows that $\langle v, v' \rangle = 0$, and thus that these vectors v form an orthogonal frame. Since $L' \subset \mathbf{R}^{16}$, there are at most 16 pairs of vectors in this frame — and, again as happened for E_8 and Λ_{24}, the theta-function coefficient is so large that each eligible coset must contain a full frame.

Choose one of these 135 cosets, and fix orthonormal coordinates on $\mathbf{R}^{16}$ so that the $2 \cdot 16$ minimal vectors in the coset are $\pm 2e_j$ $(1 \leq j \leq 16)$. Then the vectors $\pm e_j \pm e_{j'}$ are contained in L'^* and generate D_{16}. Comparing discriminants we find $[L'^* : D_{16}] = 2^5$. Moreover, since each $2e_j \in L'$, all vectors in L'^* have half-integer coordinates. So we need a suitable 32-element subgroup G of $\frac{1}{2}\mathbf{Z}^{16}/D_{16}$, and it remains to show that all such G are equivalent under $\mathrm{Aut}(D_{16})$ with the group we used to construct BW_{16}^*.

First we show that the map from G to $\frac{1}{2}\mathbf{Z}^{16}/\mathbf{Z}^{16}$ is an injection. If it weren't, then L'^* would contain $\mathbf{Z}^{16}$, but then $L = L''$ would contain vectors of norm 2, which contradicts $\theta_{L'} = \theta_L$. So we may regard G as a 2^5-element subgroup of $\frac{1}{2}\mathbf{Z}^{16}/\mathbf{Z}^{16}$, or equivalently, a binary linear code $C \subset (\mathbf{Z}/2\mathbf{Z})^{16}$ of dimension 5.

Next we claim that C is doubly even with no words of weight 4; that is, that for every $c \in C$, the number $\mathrm{wt}(c)$ of nonzero coordinates of c is a multiple of 4 and there is no $c \in C$ with $\mathrm{wt}(c) = 4$. The first claim follows from the observation that the square of a half-integer is $\frac{1}{4} \bmod 1$ while integers have integer squares. For the second claim, if $c_j = 1$ only for $j = j_1, j_2, j_3, j_4$ then L'^* contains either $(e_{j_1} + e_{j_2} + e_{j_3} + e_{j_4})/2$ or $(e_{j_1} + e_{j_2} + e_{j_3} - e_{j_4})/2$, either of which has norm 1.

Next we show that in fact $\mathrm{wt}(c) \equiv 0 \bmod 8$ for all $c \in C$. If not then there is some $c_0 \in C$ with $\mathrm{wt}(c) = 12$, so $c_j = 0$ only for $j = j_1, j_2, j_3, j_4$. Any $c \in C$ must satisfy $c_{j_1} + c_{j_2} + c_{j_3} + c_{j_4} = 0$, else c or $c_0 + c$ cannot both have weight $0 \bmod 4$. But then the linear map

$$C \to (\mathbf{Z}/2\mathbf{Z})^4, \quad c \mapsto (c_{j_1}, c_{j_2}, c_{j_3}, c_{j_4})$$

[7]This proof is outlined on page 199 of Quebbemann's 1995 paper, which notes the analogy with Conway's characterization of Λ_{24}. We give some more details here, especially concerning the Hadamard code. By carefully keeping track of the number of choices made at made at each step we could also recover the number of automorphisms of this lattice.

has image of dimension at most 3, and thus kernel of dimension at least $5 - 3 = 2$. So the kernel contains not just c_0 but some other nonzero vector c, and then either c or c_0 has weight at most $\frac{1}{2} \operatorname{wt}(c_0) = 6$, which is a contradiction.[8]

So it remains to prove that the Hamadard $[16, 5, 8]$ code is the only linear code of length 16 each of whose words has weight 0, 8, or 16. We prove more generally:

Proposition. *If C is a binary code of length 2^m and dimension $m+1$ such that $\operatorname{wt}(c) \in \{0, 2^{m-1}, 2^m\}$ for all $c \in C$, then C is isomorphic with the Hadamard $[2^m, m+1, 2^{m-1}]$ code.*

Proof: Consider the configuration of (± 1)-vectors $\{(-1)^c \in \mathbf{R}^{2^m} : c \in C\}$. There are 2^{m+1} of them, all of norm 2^m, and for any $c, c' \in C$ the vectors $(-1)^c$ and $(-1)^{c'}$ are orthogonal unless c and c' are equal or complementary in which case $(-1)^{c'} = \pm(-1)^c$. Hence they form a complete orthogonal frame; in particular C is closed under complementation, and thus contains the all-1 vector $\mathbf{1}$. Choose from each complementary pair in C the word with first coordinate 0; these 2^m vectors form a subcode, call it C_0, each of whose nonzero words has weight 2^{m-1}. The correspodnding 2^m vectors $(-1)^c$, each with first coordinate $+1$, form a Hadamard matrix. Since the transpose of a Hadamard matrix is again Hadamard, we deduce that for any j, j' with $1 \le j < j' \le 2^m$ exactly half the vectors $c \in C_0$ have $c_j = c_{j'}$. But this gives us 2^m *distinct* coordinate functionals $C_0 \to \mathbf{Z}/2\mathbf{Z}$, $c \mapsto c_j$, one for each j with $1 \le j \le 2^m$. Since $\operatorname{Hom}(C_0, \mathbf{Z}/2\mathbf{Z})$ has size 2^m, this means that each functional in $\operatorname{Hom}(C_0, \mathbf{Z}/2\mathbf{Z})$ occurs once. Thus in any matrix whose columns constitute a basis for C_0 the rows are all 2^m vectors of $(\mathbf{Z}/2\mathbf{Z})^m$, each occurring once. This makes $C = C_0 \cup (C_0 + \mathbf{1})$ a Hadamard $[2^m, m+1, 2^{m-1}]$ code. $\square$

Remark: The hypothesis that $\operatorname{wt}(c) \in \{0, 2^{m-1}, 2^m\}$ for all $c \in C$ can be weakened to $\operatorname{wt}(c) \ge 2^{m-1}$ for all nonzero $c \in C$, because it is known that if a set S of $2n$ unit vectors $v \in \mathbf{R}^n$ has $\langle v, v' \rangle \le 0$ for all distinct $v, v' \in S$ then $S = \{\pm e_m : 1 \le m \le n\}$ for some orthonormal basis $\{e_m\}$. But this is harder to prove than showing that $\operatorname{wt}(c)$ cannot equal 12 in our setting.

We can now finish Quebbemann's proof of the characterization of Λ_{16}. The conclusion is familiar. We have shown L'^* is contained with index 2 in a lattice isomorphic with $L_1\langle 1/2 \rangle$. Scaling by 2, this gives L as an index-2 sublattice of L_1. Hence L is the kernel of a homomorphism $f : L_1 \to \mathbf{Z}/2\mathbf{Z}$ that sends every root of L_1 to 1. This determines f on A_1^{16}, so there are $[L_1 : A_1^{16}] = 2^5$ such homomorphisms. Again we check that all are equivalent under coordinate reflections with our choice $x \mapsto (\frac{1}{2} \sum_{j=1}^{16} x_j) \bmod 2$. Hence $L \cong \Lambda_{16}$. $\square$

---

[8]Warning: it might seem that $8 | \operatorname{wt}(c)$ implies that all vectors in L'^* have even norm, because the square of a half-integer is always $\frac{1}{4} \bmod 2$. But the parity of the number of odd *integer* coordinates can vary. For example, if $C \ni (1111111100000000)$ then L'^* contains 2^7 of the vectors $e_9 + \frac{1}{2} \sum_{j=1}^8 \pm e_j$, and these have norm 3. Indeed all vectors of norm 3 in L'^* have one coordinate ± 1, eight coordinates $\pm 1/2$, and the remaining seven coordinates 0; each $c \in C$ with $\operatorname{wt}(c) = 8$ yields 2^{11} such vectors (2^7 sign choices for the $\pm 1/2$ coordinates, $2 \cdot 8$ choices for the index and sign of the ± 1), and we shall soon see that there are 30 choices for c, for a total of 61440 which happily agrees with the q^3 coefficient in (23).