Mathematical Research Letters **2**, 321–326 (1995)

A CHARACTERIZATION OF THE $\mathbb{Z}^n$ LATTICE

Noam D. Elkies

1. Introduction

In this note we prove that $\mathbb{Z}^n$ is the only integral unimodular lattice $L \subset \mathbb{R}^n$ which does not contain a vector w such that $|w|^2 < n$ and $(v, v + w) \equiv 0 \bmod 2$ for all $v \in L$. By the work of Kronheimer and others on the Seiberg-Witten equation, this yields an alternative proof of a theorem of Donaldson [D1,D2] on the geometry of 4-manifolds.

The proof uses the theory of theta series and modular forms; since this technique is not yet in the standard-issue arsenal of the 4-manifold community, I begin with an abbreviated exposition of this theory to make this note reasonably self-contained. This develops only the barest minimum, even to the point of never using the phrase "modular form"; for a more substantial exposition, refer to [Se, Ch.VII], and note the concluding remarks (6.7, "Complements").

Knowing that any $L \not\cong \mathbb{Z}^n$ has characteristic vectors of norm $\leqslant n - 8$, one might ask for which lattices is $n-8$ the minimum. It turns out that the same technique also yields a complete answer to this question. Since the answer may be of some interest (for instance there are 14 such lattices in each dimension $n \leqslant 23$), but its proof requires a somewhat more extensive use of modular forms, we announce the result at the end of this note but defer its proof and further discussion to a later paper.

2. Fractional linear transformations and theta series

Let H be the Poincaré upper half-plane $\{t = x + iy : y > 0\}$, and let Γ be the group $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$, acting on H by the fractional linear transformations:

(1) $$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ t \mapsto \frac{at+b}{ct+d}\ .$$

Received February 14, 1995.
Partially supported by the NSF and the Packard Foundation.

It is known that Γ is generated by $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, acting on H by

$$S(t) = -\frac{1}{t}, \quad T(t) = t + 1. \tag{2}$$

Let $\Gamma(2) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma : b, c \text{ even}\}$; this is a normal subgroup of Γ, and reduction mod 2 yields the quotient map $\Gamma \to \Gamma/\Gamma(2) = \mathrm{PSL}_2(\mathbb{Z}/2) \cong \mathrm{S}_3$. Finally, let $\Gamma_+ \subset \Gamma$ be the subgroup generated by S and T^2. Then Γ_+ has index 3 in Γ, contains $\Gamma(2)$ with index 2, and consists of the matrices congruent mod 2 to either $\mathbf{1}$ or S. Indeed, it is clear that Γ_+ consists of matrices of this form; that all such matrices are in Γ_+ is perhaps most readily seen by proving as in [Se, Ch.VII, Thm.1,2] that

$$D_+ := \{t = x + iy \in H : |x| \le 1, |t| \ge 1\} \tag{3}$$

(the ideal hyperbolic triangle in H with vertices $-1, 1, i\infty$) is a fundamental domain for the action of Γ_+ on H, and noting that D_+ is 3 times as large as the standard fundamental domain for Γ.

Now let L be a unimodular integral lattice in $\mathbb{R}^n$, i.e., a lattice of discriminant 1 such that $(v, v') \in \mathbb{Z}$ for all $v, v' \in L$. The *theta series* θ_L of L is a generating function encoding the norms $|v|^2 = (v, v)$ of lattice vectors:

$$\theta_L(t) := \sum_{v \in L} e^{\pi i |v|^2 t} \quad (t \in H). \tag{4}$$

For instance, for $n = 1$, we have

$$\theta_{\mathbf{Z}}(t) := 1 + 2\left(e^{\pi i t} + e^{4\pi i t} + e^{9\pi i t} + \cdots\right) . \tag{5}$$

This sum converges uniformly in compact subsets of H (if $t = x + iy$ then $|e^{\pi i |v|^2 t}| = e^{-\pi |v|^2 y}$) and thus defines a holomorphic function on H. If L_1, L_2 are unimodular integral lattices in $\mathbb{R}^{n_1}, \mathbb{R}^{n_2}$, then $L_1 \oplus L_2$ is a unimodular integral lattice in $\mathbb{R}^{n_1+n_2}$ whose theta series is given by

$$\theta_{L_1 \oplus L_2}(t) = \theta_{L_1}(t) \cdot \theta_{L_2}(t). \tag{6}$$

Since each $|v|^2$ is an integer, we have

$$\theta_L(t) = \theta_L(t + 2) = \theta_L(T^2(t)). \tag{7}$$

Since L is its own dual lattice, we obtain a more interesting functional equation by applying Poisson inversion to (4):

$$(t/i)^{n/2} \theta_L(t) = \theta_L(-1/t) = \theta_L(S(t)), \tag{8}$$

where $(t/i)^{n/2}$ is the nth power of the principal branch of $\sqrt{t/i}$. By iterating (7,8) we find that for every $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\langle S, T^2 \rangle = \Gamma_+$ there is a functional equation

$$\theta_L(g(t)) = \epsilon_n(c,d) \cdot (ct+d)^{n/2}\theta_L(t), \tag{9}$$

where again $(ct+d)^{n/2}$ is the nth power of the principal branch of $\sqrt{ct+d}$, and $\epsilon_n(c,d)$ is an eighth root of unity which does not depend on the choice of unimodular integral lattice L. (It does not depend on a, b, because c, d determine g up to a power of T^2.) By choosing $L = \mathbb{Z}^n$ and using (6) we find

$$\epsilon_n(c,d) = \big(\epsilon_1(c,d)\big)^n. \tag{10}$$

Note that [Se, Ch.VII] assumes that L is an *even* lattice, i.e., $|v|^2 \in 2\mathbb{Z}$ for all $v \in L$. Such L have theta series invariant under T, and thus satisfy (9) for all $g \in \langle S, T \rangle = \Gamma$. It is known from the arithmetic theory [Se, Ch.V] that $n \equiv 0 \bmod 8$ for such lattices, whence the ϵ_n factors all equal 1 in that case; this could also be proved analytically using (8) and the identity $(ST)^3 = 1$. We shall soon observe, en route to our estimate on the norm of characteristic vectors of odd lattices, that this method also yields an analytic proof of the fact [Se, Ch.V, Thm.2] that these vectors all have norm $\equiv n \bmod 8$.

How do fractional linear transformations $g \in \Gamma - \Gamma_+$ act on θ_L? We need only consider one representative of each of the two nontrivial cosets of Γ_+ in Γ, for instance $g = T$ and $g = TS$. For the first we find simply

$$\theta_L(T(t)) = \theta_L(t+1) = \sum_{v \in L} e^{\pi i |v|^2 (t+1)} = \sum_{v \in L} (-1)^{|v|^2} e^{\pi i |v|^2 t}. \tag{11}$$

Now recall that the sign $v \mapsto (-1)^{|v|^2}$ is a group homomorphism from L to $\{\pm 1\}$ (because

$$|v+v'|^2 = |v|^2 + |v'|^2 + 2(v,v') \equiv |v|^2 + |v'|^2 \bmod 2 \tag{12}$$

for all $v, v' \in L$). Since L is unimodular, there is a bijection between characters $L \to \{\pm 1\}$ and cosets of $2L$ in L which associates to the coset of any $w \in L$ the character $v \mapsto (-1)^{(v,w)}$. In particular, there is a coset associated with $v \mapsto (-1)^{|v|^2}$; vectors in that coset, characterized by

$$|v|^2 \equiv (v,w) \bmod 2 \text{ for all } v \in L, \tag{13}$$

are known as *characteristic vectors* of L. (In [Se, Ch.V] this coset is called the "canonical class" in $L/2L$; in [CS2] this coset, scaled by $1/2$ to obtain a translate of L by $w/2$, is called the "shadow" of L, and our key formula

(17) below is also a key ingredient of [CS2].) Choose some characteristic vector w, and rewrite (11) as

$$\theta_L(t+1) = \sum_{v\in L} e^{\pi i\left(|v|^2 t + (v,w)\right)}. \tag{14}$$

Applying Poisson inversion to this sum, we find

$$(t/i)^{n/2}\theta_L(t+1) = \sum_{v\in L} e^{\pi i |v+\frac{w}{2}|^2(\frac{-1}{t})} = \theta'_L(S(t)), \tag{15}$$

where

$$\theta'_L(t) := \sum_{v\in L+\frac{w}{2}} e^{\pi i |v|^2 t} \tag{16}$$

is a generating function encoding the norms of characteristic vectors. Replacing t by $St = -1/t$ in (16), we conclude that

$$\theta_L(TS(t)) = \theta_L(\frac{-1}{t}+1) = (t/i)^{n/2}\theta'_L(t). \tag{17}$$

To recover the result

$$|w|^2 \equiv n \bmod 8, \tag{18}$$

we may now regard (17) as a formula for $\theta'_L(t)$ and compare it with

$$\begin{aligned} \left(\frac{t+1}{i}\right)^{n/2}\theta'_L(t+1) &= \theta_L(TST(t)) = \theta_L(ST^{-1}S(t)) \\ &= (T^{-1}S(t)/i)^{n/2}\theta_L(T^{-1}S(t)) = \left(\frac{i(t+1)}{t}\right)^{n/2}\theta_L(TS(t)) \end{aligned} \tag{19}$$

(in which we used $S^2 = (ST)^3 = 1$ and the invariance of θ_L under T^2, and again use $n/2$ power to mean the nth power of the principal square root). This yields

$$\theta'_L(t+1) = e^{\pi i n/4}\theta'_L(t). \tag{20}$$

Thus $\theta'_L(t)$ is a linear combination of terms $e^{\pi i m t/4}$ with $m \equiv n \bmod 8$, from which it follows that all the characteristic vectors have norm congruent to $n \bmod 8$ as claimed.

The characteristic vectors of $\mathbb{Z}$ are the odd integers, so

$$\theta'_{\mathbf{Z}}(t) = 2\sum_{m=0}^{\infty} e^{\pi i (m+\frac{1}{2})^2 t} = 2e^{\pi i t/4}\left(1 + e^{2\pi i t} + e^{6\pi i t} + e^{12\pi i t} + \cdots\right). \tag{21}$$

Thus $\theta'_{\mathbf{Z}}(t) \sim 2e^{\pi i t/4} \to 0$ as $t \to i\infty$. From (17) it follows that $\theta_{\mathbf{Z}}$ tends to zero as $t \in D_+$ approaches the "cusp" ± 1. It will be crucial to us that $\theta_{\mathbf{Z}}$ **has no zeros in** H. This can be seen either from explicit product formulas such as

$$\sum_{m=0}^{\infty} q^{(m+\frac{1}{2})^2} = q^{1/4} \prod_{j=1}^{\infty} (1+q^{2j})(1-q^{4j}) \tag{22}$$

(a special case of the Jacobi triple product), or by using contour integrals as in [Se, Ch.VII, Thm.3] to show that ± 1 is the only zero of $\theta_{\mathbf{Z}}$ in $D_+ \cup \{$ cusps$\}$. Also $\theta_{\mathbf{Z}}(i\infty) = 1$ so $\theta_{\mathbf{Z}}$ is bounded away from zero as $t \to i\infty$.

3. The shortest characteristic vector

We are now ready to prove:

Theorem 1. *Let L be a unimodular integral lattice in $\mathbb{R}^n$ with no characteristic vector w such that $|w|^2 < n$. Then $L \cong \mathbb{Z}^n$.*

Proof. We first show that L and $\mathbb{Z}^n$ have the same theta function. To that end consider

$$R(t) := \theta_L(t)/\theta_{\mathbf{Z}^n}(t) = \theta_L(t)/\theta^n_{\mathbf{Z}}(t). \tag{23}$$

This is a holomorphic function because $\theta_{\mathbf{Z}}$ does not vanish in H. Since θ_L and $\theta_{\mathbf{Z}^n}$ both transform according to (9) under Γ_+, their quotient $R(t)$ is invariant under Γ_+. By the hypothesis on L we have $\theta'_L \ll e^{\pi i n t/4}$ as $t \to i\infty$. Thus $\theta'_L/\theta'_{\mathbf{Z}^n}$ is bounded as $t \to i\infty$, whence by (17), $R(t)$ is bounded as $t \in D_+$ approaches ± 1. Finally, $R(i\infty) = 1$. By the maximum principle we deduce that R is the constant function 1, i.e. $\theta_L = \theta^n_{\mathbf{Z}}$.

Thus for each m the lattices L and $\mathbb{Z}^n$ have the same number of vectors of norm m. Taking $m = 1$ we find that L has n pairs of unit vectors. Since L is integral these must be orthogonal to each other, and thus generate a copy of $\mathbb{Z}^n$ inside L. Using integrality again, we conclude that this copy is all of L. $\square$

Since the hypothesis is automatically satisfied if $n < 8$, we also recover the fact that $\mathbb{Z}^n$ is the only unimodular integral lattice for those n. With some more work, we can also use the relation between θ_L and θ'_L and the theory of modular forms to completely describe those $L \subset \mathbb{R}^n$ whose shortest characteristic vector has norm $n-8$; these are precisely the lattices of the form $\mathbb{Z}^{n-r} \oplus L_0$, where $L_0 \subseteq \mathbb{R}^r$ is a unimodular integral lattice with no vectors of norm 1 and exactly $2n(23-n)$ vectors of norm 2. In particular, $n \leqslant 23$, and there are only finitely many choices for L_0. Fortunately, the table of unimodular lattices in [CS1, pp.416–7] extends just far enough that we can list all possible L_0. These are tabulated below, indexed as in the table of [CS1] by the root system of norm-2 vectors:

r	8	12	14	15	16	17	18	18	19	20	20	21	22	23
	E_8	D_{12}	E_7^2	A_{15}	D_8^2	$A_{11}E_6$	D_6^3	A_9^2	$A_7^2 D_5$	D_4^5	A_5^4	A_3^7	A_1^{22}	O_{23}

Of these, the first is the E_8 lattice, and the last is the "shorter Leech lattice"—the unimodular integral lattices of minimal dimension having minimal norm 2 and 3, respectively. It also follows from the analysis that each of these lattices has exactly $2^{n-11}r$ characteristic vectors of norm $n-8$. We defer the proof of the $\mathbb{Z}^{n-r} \oplus L_0$ criterion, and an analogous condition for self-dual binary codes, to a subsequent paper.

4. Acknowledgements

Thanks to Tom Mrowka for bringing this problem to my attention and to John H. Conway for enlightening correspondence.

References

[Do1] S.K. Donaldson, *An application of gauge theory to the topology of 4-manifolds*, J. Diff. Geom. **18** (1983), 279–315.

[Do2] ———, *The orientation of Yang-Mills moduli spaces and 4-manifold topology*, J. Diff. Geom. **26** (1987), 397–428.

[CS1] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups,* Springer, New York, 1993.

[CS2] ———, ———, *A new upper bound on the minimal distance of self-dual codes*, IEEE Trans. Inform. Theory **36** (1990), 1319–1333.

[Se] J. P. Serre, *A Course in Arithmetic,* Springer, New York, 1973.

Department of Mathematics, Harvard University, Cambridge, MA 02138
E-mail address: elkies@zariski.harvard.edu