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 $(v, v + w) \equiv 0 \mod 2$ 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 $L \not\sim \mathbb{Z}^n$ has characteristic vectors of norm $\leq n - 8$, 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 $n \leq 23$), 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 $\Gamma$ be the group $\text{PSL}_2(\mathbb{Z}) = \text{SL}_2(\mathbb{Z})/\{\pm 1\}$, acting on $H$ by the fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : t \mapsto \frac{at + b}{ct + d}.$$
It is known that \( \Gamma \) is generated by \( S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \) and \( T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \), acting on \( H \) by

\[
S(t) = -\frac{1}{t}, \quad T(t) = t + 1.
\]

Let \( \Gamma(2) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : b, c \text{ even} \} \); this is a normal subgroup of \( \Gamma \), and reduction mod 2 yields the quotient map \( \Gamma \to \Gamma/\Gamma(2) = \text{PSL}_2(\mathbb{Z}/2) \cong S_3 \). Finally, let \( \Gamma_+ \subset \Gamma \) be the subgroup generated by \( S \) and \( T^2 \). Then \( \Gamma_+ \) has index 3 in \( \Gamma \), contains \( \Gamma(2) \) with index 2, and consists of the matrices congruent mod 2 to either \( 1 \) or \( S \). Indeed, it is clear that \( \Gamma_+ \) consists of matrices of this form; that all such matrices are in \( \Gamma_+ \) is perhaps most readily seen by proving as in [Se, Ch.VII, Thm.1.2] that

\[
D_+ := \{ t = x + iy \in H : |x| \leq 1, |t| \geq 1 \}
\]

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

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 \( \theta_L \) of \( L \) is a generating function encoding the norms \( |v|^2 = (v, v) \) of lattice vectors:

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

For instance, for \( n = 1 \), we have

\[
\theta_{\mathbb{Z}}(t) := 1 + 2 \left( e^{\pi it} + e^{4\pi it} + e^{9\pi it} + \cdots \right).
\]

This sum converges uniformly in compact subsets of \( H \) (if \( t = x + iy \) then \( |e^{\pi |v|^2 t}| = e^{-\pi |v|^2 y} \) 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

\[
\theta_{L_1 \oplus L_2}(t) = \theta_{L_1}(t) \cdot \theta_{L_2}(t).
\]

Since each \(|v|^2\) is an integer, we have

\[
\theta_L(t) = \theta_L(t + 2) = \theta_L(T^2(t)).
\]

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

\[
(t/i)^{n/2} \theta_L(t) = \theta_L(-1/t) = \theta_L(S(t)),
\]
A CHARACTERIZATION OF THE \( z^n \) LATTICE

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

\[
\theta_\Gamma(g(t)) = \epsilon_n(c, d) \cdot (ct + d)^{n/2} \theta_\Gamma(t),
\]

where again \((ct+d)^{n/2}\) is the \( n \)th 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

\[
\epsilon_n(c, d) = (\epsilon_1(c, d))^n.
\]

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 \( n \equiv 0 \mod 8 \) for such lattices, whence the \( \epsilon_n \) 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 \( \equiv n \mod 8 \).

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

\[
\theta_\Gamma(T(t)) = \theta_\Gamma(t + 1) = \sum_{v \in L} e^{\pi i |v|^2(t+1)} = \sum_{v \in L} (-1)^{|v|^2} e^{\pi i |v|^2 t}.
\]

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

\[
|v + v'|^2 = |v|^2 + |v'|^2 + 2(v, v') \equiv |v|^2 + |v'|^2 \mod 2
\]

for all \( v, v' \in L \). Since \( L \) is unimodular, there is a bijection between characters \( L \to \{±1\} \) 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

\[
|v|^2 \equiv (v, w) \mod 2 \quad \text{for all } v \in L,
\]

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

\[
\theta_L(t + 1) = \sum_{v \in L} e^{\pi i |v|^2 t + (v, w)}.
\]  

Applying Poisson inversion to this sum, we find

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

where

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

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

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

To recover the result

\[
|w|^2 \equiv n \pmod{8},
\]

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

\[
\left( \frac{t + 1}{i} \right)^{n/2} \theta'_L(t + 1) = \theta_L(TST(t)) = \theta_L(ST^{-1}S(t))
\]

\[
= (T^{-1}S(t)/i)^{n/2} \theta_L(T^{-1}S(t)) = \left( \frac{i(t + 1)}{t} \right)^{n/2} \theta_L(TS(t))
\]

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

\[
\theta'_L(t + 1) = e^{\pi in/4} \theta'_L(t).
\]

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

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

\[
\theta'_Z(t) = 2 \sum_{m=0}^{\infty} e^{\pi i (m + \frac{1}{2})^2 t} = 2e^{\pi it/4} \left( 1 + e^{2\pi it} + e^{6\pi it} + e^{12\pi it} + \ldots \right).
\]
Thus $\theta_Z(t) \sim 2e^{\pi it/4} \to 0$ as $t \to i\infty$. From (17) it follows that $\theta_Z$ tends to zero as $t \in D_+$ approaches the “cusp” $\pm 1$. It will be crucial to us that $\theta_Z$ has no zeros in $H$. This can be seen either from explicit product formulas such as

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

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

$$R(t) := \frac{\theta_L(t)}{\theta_{\mathbb{Z}^n}(t)} = \frac{\theta_L(t)}{\theta_{\mathbb{Z}^n}(t)}.$$

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

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 $L$. \qed
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 \( \theta_L \) and \( \theta'_L \), 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 \( L_0 \subset \mathbb{R}^r \) is a unimodular integral lattice with no vectors of norm 1 and exactly \( 2n(23 - n) \) vectors of norm 2. In particular, \( n \leq 23 \), 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:

<table>
<thead>
<tr>
<th>( r )</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
</tr>
<tr>
<td>( E_8 )</td>
</tr>
</tbody>
</table>

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


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