LATTICES WITHOUT SHORT CHARACTERISTIC VECTORS

MARK GAULTER

ABSTRACT. All the lattices here under discussion here are understood to be integral unimodular \( \mathbb{Z} \)-lattices in \( \mathbb{R}^n \). A characteristic vector of a lattice \( L \) is a vector \( w \in L \) such that \( v \cdot w \equiv |v|^2 \pmod{2} \) for every \( v \in L \). Elkies has considered the minimal (squared) norm of the characteristic vectors in a unimodular lattice. He showed that any unimodular \( \mathbb{Z} \)-lattice in \( \mathbb{R}^n \) has characteristic vectors of norm \( \leq n \); he also proved that of all such lattices, only the standard lattice \( \mathbb{Z}^n \) has no characteristic vectors of norm \( < n \) (Math Research Letters 2, 321-326). He then asked “For any \( k > 0 \), is there \( N_k \) such that every integral unimodular lattice all of whose characteristic vectors have norm \( \geq n - 8k \) is of the form \( L_0 \perp \mathbb{Z}^r \) for some lattice \( L_0 \) of rank at most \( N_k \)?” (Math Research Letters 2, 643-651). He solved this question in the case \( k = 1 \), showing that \( N_1 = 23 \) suffices; here I determine values for \( N_2 \) and \( N_3 \).

1. Introduction

A \( \mathbb{Z} \)-lattice is a free module of finite rank over \( \mathbb{Z} \). Given a \( \mathbb{Z} \)-lattice \( L \), let \( B : L \times L \to \mathbb{Z} \) be a symmetric bilinear form and \( q : L \to \mathbb{Z} \) given by \( q(x) = B(x,x) \) the corresponding quadratic form. Throughout this paper we will assume that \( q \) is positive definite. This enables us to embed \( L \) in \( \mathbb{R}^n \), with \( B(\cdot,\cdot) \) the standard inner product and \( q(\cdot) \) the corresponding (squared) norm. A characteristic vector of \( L \) is an element \( w \) such that \( B(v,w) \equiv q(v) \pmod{2} \) for every \( v \in L \). Characteristic vectors are known to exist in any unimodular \( \mathbb{Z} \)-lattice \( L \), and in this case they constitute a coset of \( 2L \) in \( L \). If \( L \) has rank \( n \), all the characteristic elements have norm congruent to \( n \) (mod 8) (see [B]; or see Chapter V of [S]).

Noam Elkies has considered the minimal norm of the characteristic vectors in a unimodular lattice. In [E1], Elkies shows that any positive definite unimodular \( \mathbb{Z} \)-lattice of rank \( n \) has characteristic vectors of norm \( \leq n \); he also proves that of all such lattices, only the standard lattice \( \mathbb{Z}^n \) has no characteristic vectors of norm strictly less than \( n \). Then in [E2], he begins a programme of showing that a positive definite unimodular lattice whose minimal characteristic vectors have norm close to \( n \) are in some sense close to \( \mathbb{Z}^n \). More precisely, he shows that every such lattice whose characteristic vectors all have norm \( \geq n - 8 \) is of the form \( L_0 \perp \mathbb{Z}^r \) for some \( L_0 \) of rank \( \leq 23 \). He then asks: “For any \( k > 0 \), is there \( N_k \) such that every integral [positive definite] unimodular lattice all of whose characteristic vectors have norm \( \geq n - 8k \) is of the form \( L_0 \perp \mathbb{Z}^r \) for
some lattice $L_0$ of rank at most $N_k$?” Elkies goes on to comment: “Even the case $k = 2$ appears difficult.”

In this paper, we first obtain upper bounds on the number of characteristic vectors of minimal norm $s$ and on the number of characteristic vectors of norm $s + 8$; then we apply a theorem of Hecke to settle the cases $k = 2$ and $k = 3$ of Elkies’ problem.

2. Notation

We will largely follow the notation of [O’M]. Also, for a given lattice $L$, we define:

\[ \chi_L := \{ v \in L : B(x,v) \equiv q(x) \pmod{2}, \forall x \in L \} \]
\[ \chi_t(L) := \{ v \in \chi_L : q(v) = t \} \]
\[ s(L) := \min_{v \in \chi_L} \{ q(v) \}. \]

Thus $\chi_s$ denotes the set of shortest characteristic vectors of the lattice $L$ under discussion. Finally, for any set $A$, define $|A|$ to be the cardinality of $A$.

3. A bound on the number of shortest characteristic vectors

Throughout this section, $L$ denotes a positive definite unimodular $\mathbb{Z}$-lattice of rank $n$. We will find bounds on $|\chi_s|$ and $|\chi_{s+8}|$. The characteristic elements of $L$ constitute a coset of $2L$ in $L$, so if $v_1, v_2 \in \chi_L$ then $v_1 + v_2 \in 2L$. If $v_1, v_2$ have the same norm, we can say more:

**Lemma 3.1.** Let $v_1, v_2$ be characteristic elements of $L$ with $q(v_1) = q(v_2) = t$. Then
\[ q \left( \frac{v_1 + v_2}{2} \right) \leq t \]
with equality if and only if $v_1 = v_2$.

*Proof.* This is because a ball in Euclidean space is strictly convex. \qed

**Lemma 3.2.** Fix $w \in \chi_s$. Define the map $\phi_w : \chi_s \to L/2L$ by
\[ \phi_w(v) := \frac{v - w}{2} + 2L. \]
Then $\phi_w$ is injective.

*Proof.* Suppose $\phi_w(v_1) = \phi_w(v_2)$. Then $\frac{v_1 - v_2}{2} \in 2L$, from which we see
\[ \frac{v_1 + v_2}{2} = v_2 + \frac{v_1 - v_2}{2} \in \chi_L. \]
Therefore
\[ q \left( \frac{v_1 + v_2}{2} \right) \geq s. \]
But $v_1, v_2 \in \chi_s$, so by Lemma 3.1 we have $q(\frac{v_1 + v_2}{2}) \leq s$. Thus we have equality, and by applying Lemma 3.1 again we see $v_1 = v_2$, as required. \qed
Lemma 3.2 gives us an injective function from $\chi_s$ into a group of order $2^n$. This proves the following:

**Corollary 3.3.** The number of shortest characteristic vectors of a positive definite unimodular $\mathbb{Z}$-lattice of dimension $n$ is at most $2^n$.

This result is the best possible, as the following example shows. Let \(\{e_1, e_2, \ldots, e_n\}\) be an orthonormal basis for $\mathbb{Z}^n$. Then the characteristic vectors are those of the form $\sum_{j=1}^n \lambda_j e_j$ with all the $\lambda_j$ odd. In particular, the shortest characteristic vectors are the vectors of the form $\sum_{j=1}^n \lambda_j e_j$ with each $\lambda_j \in \{\pm 1\}$; there are $2^n$ such vectors.

Now we shall find an upper bound on the number of characteristic vectors of norm $s + 8$. This bound must be at least $n^2$, for the lattice $\mathbb{Z}^n$ has $n^2$ such vectors. (These are the vectors $\sum_{j=1}^n \lambda_j e_j$ with one $\lambda_j = \pm 3$ and all other $\lambda_j \in \{\pm 1\}$.)

**Lemma 3.4.** Suppose $w \in \chi_{s+8}$. Define

\[
\mathcal{C}_w := \{v \in \chi_{s+8} : w - v \in 4L\}.
\]

If $n \neq 15$ then $|\mathcal{C}_w| \leq n$; if $n = 15$ then $|\mathcal{C}_w| \leq 16$.

**Proof.** It is enough to show that $|\mathcal{C}_w| \leq n + 1$, and then to show that equality can hold only when $n = 15$.

(a) **Proof of the inequality** $|\mathcal{C}_w| \leq n + 1$.

Write

\[
\begin{align*}
    w &= x_1 + 2l_1 \\
    w &= x_2 + 2l_2 \\
    \vdots \\
    w &= x_{m+1} + 2l_{m+1}
\end{align*}
\]

in as many different ways as possible with $x_i \in \chi$ and $B(x_i, l_i) = 0$ for each $i$.

The list is finite because $q$ is positive definite.

**Claim:** $|\mathcal{C}_w| = m + 1$. Given $v \in \mathcal{C}_w$, let $x = \frac{w+v}{2}$ and $l = \frac{w-v}{4}$ (So $w = x + 2l$ and $v = x - 2l$.) Then

\[
x = w + \frac{v-w}{2} \in w + 2L = \chi.
\]

But the equality $q(v) = q(w)$ then yields $q(x - 2l) = q(x + 2l)$, from which $B(x, l) = 0$. This gives an injective map from $\mathcal{C}_w$ to rows of the list (1). Thus $|\mathcal{C}_w| \leq m + 1$.

On the other hand, if $w = x_i + 2l_i$, then we assert that $x_i - 2l_i \in \mathcal{C}_w$; this vector is characteristic and in the same coset of $L/4L$ as $w$, and $q(w) = q(x_i - 2l_i)$. If $x_i - 2l_i = x_j - 2l_j$ then $w - 4l_i = w - 4l_j$ and so each expression for $w$ yields a different element of $\mathcal{C}_w$. Thus $|\mathcal{C}_w| = m + 1$ as claimed.
Having established this claim, to prove part (a) we need only show that \( m \leq n \). One of our expressions for \( w \) in (1) will be \( w + 0 \). So without loss of generality, suppose \( l_{m+1} = 0 \). The proof will proceed by showing \( l_1, \ldots, l_m \) are linearly independent.

For \( 1 \leq i \leq m \) we have \( q(x_i) + 4q(l_i) = s + 8 \). Since \( x_i \) is characteristic, it follows that \( q(l_i) = 2 \) and \( q(x_i) = s \). Suppose \( 1 \leq i < j \leq m \). Because \( x_i - 2l_j \in \chi \) we know \( q(x_i - 2l_j) \geq s \). Hence, because \( q(x_i) = s \), we have

\[
B(x_i, l_j) \leq q(l_j) = 2.
\]

We also know \( l_i \neq l_j \), since the expressions in (1) are different. So \( q(l_i - l_j) > 0 \) and therefore \( B(l_i, l_j) \leq 1 \). But

\[
B(x_i, l_j) + 2B(l_i, l_j) = B(w, l_j) = B(x_j + 2l_j, l_j) = 4.
\]

Thus \( B(x_i, l_j) = 2 \) and \( B(l_i, l_j) = 1 \) whenever \( 1 \leq i < j \leq m \).

We are now ready to prove that \( l_1, l_2, \ldots, l_m \) are linearly independent. For suppose

\[
\sum_{i=1}^{m} \mu_i l_i = 0
\]

with \( \mu_1 \cdots \mu_m \in \mathbb{Q} \). Then for each \( k \leq m \) we have \( B(\sum_{i=1}^{m} \mu_i l_i, l_k) = 0 \), and hence

\[
A_m \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_m \end{pmatrix} = 0
\]

where \( A_m \) is the \( m \times m \) matrix

\[
\begin{pmatrix}
2 & 1 & \ldots & 1 \\
1 & 2 & \ddots & \vdots \\
\vdots & \ddots & \ddots & 1 \\
1 & \ldots & 1 & 2
\end{pmatrix}.
\]

But \( \det A_m = m + 1 \), and hence \( A_m \) is invertible over \( \mathbb{Q} \). Therefore \( \mu_1 = \mu_2 = \cdots = \mu_m = 0 \), which proves the claim.

Therefore \( m \leq \dim \mathbb{Q}L = n \) and so \( |C_w| \leq n + 1 \) as required.

(b) Suppose \( |C_w| = n + 1 \); we will show that \( n = 15 \).

As in the proof of part (a), write \( w = x_i + 2l_i \) for each \( 1 \leq i \leq n \), with the \( x_i \) distinct elements of \( \chi_s \), and \( B(x_i, l_i) = 0 \) for each \( i \). Then the set \( \{l_1, l_2, \cdots, l_n\} \) is a basis for \( \mathbb{Q}L \), and \( q(l_i) = 2 \) for each \( i \).
Write \( x_1 = \sum_{i=1}^{n} \nu_i l_i \) with \( \nu_i \in \mathbb{Q} \). Recall that \( B(x_1, l_1) = 0 \) and \( B(x_1, l_i) = 2 \) for \( 2 \leq i \leq n \). Thus
\[
A_n \begin{pmatrix} \nu_1 \\ \nu_2 \\ \vdots \\ \nu_n \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ \vdots \\ 2 \end{pmatrix}.
\]
Solving this for \( \nu_1, \ldots, \nu_n \) yields \( \nu_1 = -2(\frac{n-1}{n+1}) \) and \( \nu_2 = \cdots = \nu_n = \frac{4}{n+1} \) and hence
\[
x_1 = \frac{2}{n+1} \left[ - (n-1) l_1 + 2(l_2 + \cdots + l_n) \right]
\]
from which we find
\[
q(x_1) = 8 \left( \frac{n-1}{n+1} \right) \in \mathbb{Z}.
\]
Since \( (n-1, n+1) \leq 2 \), it follows that \( (n+1) | 16 \). So \( n \in \{1, 3, 7, 15\} \). But \( x_1 \) was characteristic, so \( q(x_1) \equiv n \) (mod 8). This happens only for \( n = 15 \). \( \square \)

**Corollary 3.5.** Let \( L \) be a positive definite unimodular \( \mathbb{Z} \)-lattice of rank \( n \). If \( n \neq 15 \) then \( L \) has at most \( n2^n \) characteristic elements of length \( s+8 \). If \( L \) has rank 15 then there are at most \( 2^{19} \) such elements.

**Proof.** Regardless of the rank of \( L \), the elements of \( \chi \) form a coset of \( L/2L \). Therefore \( \chi \) consists of precisely \( 2^n \) cosets of \( L/4L \). Pick an element \( w_k \) of norm \( s+8 \) from each coset of \( L/4L \) that contains such an element. Then
\[
\chi_{s+8} = \bigcup_k C_{w_k}.
\]
If \( n \neq 15 \), Lemma 3.4 tells us there are no more than \( n \) elements in each \( C_{w_k} \).
Thus there can be no more than \( n2^n \) elements of \( \chi_{s+8} \).
If \( n = 15 \), Lemma 3.4 tells us there are no more than 16 elements of \( \chi_{s+8} \) in each \( C_{w_k} \). Thus there can be no more than \( 16 \cdot 2^{15} = 2^{19} \) elements of \( \chi_{s+8} \). \( \square \)

**Remark.** In fact if \( n = 15 \), calculations involving theta series show that there are at most \( 15 \times 2^{15} \) characteristic elements of length \( s+8 \).

4. **The main result**

In the first part this section, we largely follow the notation of [E2]. Let \( H \) be the complex upper half plane: the set of complex numbers with strictly positive imaginary part. Define the theta series of the lattice \( L \) to be
\[
\theta_L(t) := \sum_{v \in L} e^{\pi i q(v) t}
\]
for any \( t \in H \). Then
\[
\theta_L(t) = \sum_{k=0}^{\infty} N_k e^{\pi i k t},
\]
where \( N_k \) is the number of times \( L \) represents \( k \). Now let \( w \) be any characteristic vector of \( L \) and define
\[
\theta'_L(t) := \sum_{v \in L + \frac{w}{2}} e^{\pi i q(v) t} = \sum_{k=0}^{\infty} N'_k e^{\pi i k t / 4},
\]
where \( N'_k \) is the number of characteristic vectors of norm \( k \). In [E1], Elkies relates these series by the identity
\[
\theta_L \left( - \frac{1}{t} + 1 \right) = \left( \frac{t}{i} \right)^{n/2} \theta'_L(t).
\]
The \( n/2 \) power refers to the \( n \)th power of the principal square root.

Hecke has proved that if \( L \) is a unimodular \( \mathbb{Z} \)-lattice, then \( \theta_L \) is a modular form of weight \( \frac{n}{2} \) and can be expressed as a weighted-homogeneous polynomial \( P_L(\theta_Z, \theta_{E_8}) \) in the modular forms \( \theta_Z \) and \( \theta_{E_8} \) of weight \( \frac{1}{2} \) and 4 respectively (see Theorem 7, Chapter 7 of [CS] and the remark that follows it). Here, \( \theta_Z \) and \( \theta_{E_8} \) are the theta series of the lattices \( \mathbb{Z} \) and \( E_8 \). Specifically
\[
\theta_Z = 1 + 2(e^{\pi it} + e^{4\pi it} + e^{9\pi it} + \ldots)
\]
and
\[
\theta_{E_8} = 1 + 240 \sum_{k=0}^{\infty} \frac{k^3 e^{2\pi itk}}{1 - e^{2\pi itk}} = 1 + 240e^{2\pi it} + 2160e^{4\pi it} + \ldots.
\]
We can express
\[
P_L(X, Y) = \sum_{k=0}^{l} \lambda_k X^{n-8k} Y^k
\]
with \( \lambda_i \in \mathbb{R} \), \( l \leq \lfloor \frac{n}{8} \rfloor \) and \( \lambda_l \neq 0 \) and so we may write
\[
(3) \quad \theta_L(t) = \sum_{k=0}^{l} \lambda_k \theta_{Z}^{n-8k}(t) \theta_{E_8}^{k}(t)
\]
with \( \lambda_i \in \mathbb{R} \), \( l \leq \lfloor \frac{n}{8} \rfloor \) and \( \lambda_l \neq 0 \). Combining this with equation (2), we have
\[
\theta'_L(t) = \left( \frac{i}{\ell} \right)^{n/2} \theta_L \left( - \frac{1}{t} + 1 \right)
\]
\[
= \sum_{k=0}^{l} \lambda_k \left[ \left( \frac{i}{\ell} \right)^{(n-8k)/2} \theta_{Z}^{n-8k} \left( - \frac{1}{t} + 1 \right) \right] \left[ \left( \frac{i}{\ell} \right)^4 \theta_{E_8}^{k} \left( - \frac{1}{t} + 1 \right) \right]
\]
\[
= \sum_{k=0}^{l} \lambda_k \theta_{Z}^{n-8k}(t) \theta_{E_8}^{k}(t)
\]
\[
= P_L(\theta'_Z, \theta'_E).
\]
But $E_8$ is an even lattice, hence 0 is one of its characteristic vectors. Thus $\theta_{E_8} = \theta'_{E_8}$. So we have

\[ \theta'_{L} = P_L(\theta'_Z, \theta_{E_8}). \tag{4} \]

Because the characteristic vectors of $\mathbb{Z}$ (viewed as a lattice of rank one) are the odd integers, we have

\[ \theta'_Z = 2(e^{\pi it/4} + e^{3\pi it/4} + \cdots). \]

Expanding the polynomial in equation (4) now gives

\[ \theta'_{L}(t) = \lambda_l 2^{n-8l}e^{(n-8l)\pi it/4} + (2^n \lambda_{l-1} + (n + 232l)\lambda_l)2^{n-8l}e^{(n-8l+8)\pi it/4} + \cdots, \]

where $\lambda_l$ and $\lambda_{l-1}$ are as in equation (3). Since $\theta'_{L}$ encodes the number of characteristic vectors of each norm, we can deduce that if $\theta_{L}$ is expressed as in equation (3) then

\[ \begin{cases}
  s = n - 8l \\
  |\chi_s| = \lambda_l 2^{n-8l} \\
  |\chi_{s+8}| = (2^n \lambda_{l-1} + (n + 232l)\lambda_l)2^{n-8l}.
\end{cases} \tag{5} \]

**Theorem 4.1.** Let $L$ be a positive definite unimodular $\mathbb{Z}$-lattice. Then its theta series $\theta_{L}(t)$ is a modular form of weight $\frac{n}{2}$ and can be expressed as a weighted-homogeneous polynomial $P_L(\theta_Z, \theta_{E_8})$ in the modular forms $\theta_Z$ and $\theta_{E_8}$ of weight $\frac{1}{2}$ and 4 respectively. Here $\theta_Z$ and $\theta_{E_8}$ are the theta series of the lattices $\mathbb{Z}$ and $E_8$. Further, if we write

\[ P_L(X,Y) = \sum_{k=0}^l \lambda_k X^{n-8k}Y^k \tag{6} \]

then $\lambda_l \leq 2^{8l}$.

**Proof.** In light of Hecke’s theorem, the only new information here is the bound on $\lambda_l$. Express $P_L(X,Y)$ as in equation (6). Then there are $\lambda_l 2^{n-8l}$ shortest characteristic vectors. But Corollary 3.3 states that there are at most $2^n$ such vectors. Thus $\lambda_l \leq 2^{8l}$.

**Lemma 4.2.** Let $L$ be an $n$-dimensional positive definite unimodular $\mathbb{Z}$-lattice that does not represent 1. Suppose further that the shortest characteristic vectors of $L$ have norm $n - 16$. Then

\[ |\chi_s| = 2^{n-24}(2n^2 - 46n + N_2) \]

(Recall that $N_2$ is the number of times $L$ represents 2.)
Proof. The shortest characteristic vectors of \( L \) have norm \( n - 16 \); thus
\[
\theta_L(t) = \lambda_0 \theta^n_Z(t) + \lambda_1 \theta^{n-8}_Z(t) \theta_{E_8}(t) + \lambda_2 \theta^{n-16}_Z(t) \theta_{E_8}^2(t) \\
= \lambda_0 \theta^n_Z(t) + \lambda_1 \theta^{n-8} Z_{E_8}(t) + \lambda_2 \theta^{n-16} Z_{E_8} E_8(t).
\]

We know how many times each of the numbers 0, 1 and 2 are represented by
the lattices \( Z^n, Z^{n-8} \perp E_8 \) and \( Z^{n-16} \perp E_8 \perp E_8 \).
So we have that
\[
\theta_L(t) = 1 + 0 e^{\pi i t} + N_2 e^{2\pi i t} + \ldots \\
= \lambda_0 \left( 1 + 2 \left( \frac{n}{1} \right) e^{\pi i t} + 2 \left( \frac{n}{2} \right) e^{2\pi i t} + \ldots \right) \\
+ \lambda_1 \left( 1 + 2 \left( \frac{n-8}{1} \right) e^{\pi i t} + \left( 2 \left( \frac{n-8}{2} \right) + 240 \right) e^{2\pi i t} + \ldots \right) \\
+ \lambda_2 \left( 1 + 2 \left( \frac{n-16}{1} \right) e^{\pi i t} + \left( 2 \left( \frac{n-16}{2} \right) + 480 \right) e^{2\pi i t} + \ldots \right).
\]

This yields the simultaneous equations
\[
\lambda_0 + \lambda_1 + \lambda_2 = 1 \\
2n\lambda_0 + 2(n-8)\lambda_1 + 2(n-16)\lambda_2 = 0 \\
2n(n-1)\lambda_0 + (2(n-8)(n-9) + 240)\lambda_1 + (2(n-16)(n-17) + 480)\lambda_2 = N_2.
\]

Upon solving these equations, we find
\[
\lambda_2 = \frac{2n^2 - 46n + N_2}{256}.
\]

The observations (5) now tell us
\[
|\chi_s| = 2^{n-24}(2n^2 - 46n + N_2)
\]
as claimed.

Theorem 4.3. Let \( L \) be a positive definite unimodular \( Z \)-lattice of rank \( n \). Suppose further that the shortest characteristic vectors of \( L \) have norm \( n - 16 \). Then \( L = L_0 \perp Z^r \) for some sublattice \( L_0 \) of rank \( \leq 2907 \).

Proof. We may assume \( L \) does not represent 1 and prove that \( n \leq 2907 \). By Corollary 3.3, we know there are at most \( 2^n \) shortest characteristic vectors. But Lemma 4.2 tells us \( L \) has exactly \( 2^{n-24}(2n^2 - 46n + N_2) \) shortest characteristic vectors. So
\[
2^{n-24}(2n^2 - 46n + N_2) \leq 2^n.
\]

Hence
\[
2n^2 - 46n + N_2 \leq 2^{24}.
\]

But \( N_2 \geq 0 \), hence \( 2n^2 - 46n \leq 2^{24} \) and so the integer \( n \) cannot exceed 2907.
Lemma 4.4. Let $L$ be an $n$-dimensional positive definite unimodular $\mathbb{Z}$-lattice that does not represent 1, and assume that the shortest characteristic vectors of $L$ have norm $n - 24$. Then

$$|\chi_{n-16}| = (2n^2 - 46n + N_2)2^{n-24} + (n - 72)|\chi_{n-24}|.$$ 

Proof. Since the shortest characteristic vectors of $L$ have norm $n - 24$, we may write

$$\theta_L(t) = \lambda_0 \theta_Z^n(t) + \lambda_1 \theta_Z^{n-8}(t)\theta_E(t) + \lambda_2 \theta_Z^{n-16}(t)\theta_E(t) + \lambda_3 \theta_Z^{n-24}(t)\theta_E^2(t) + \lambda_4 \theta_Z^{n-32}(t)\theta_E^3(t).$$

Forming three simultaneous equations exactly as in the proof of Lemma 3.1, we discover

$$\lambda_2 = \frac{3N_3 + 160N_2 - 5568n - 6N_2n + 308n^2 - 4n^3}{2^{12}},$$

$$\lambda_3 = \frac{-3N_3 - 144N_2 + 4832n + 6N_2n - 276n^2 + 4n^3}{3 \times 2^{12}}.$$ 

Therefore

$$\lambda_2 = -3\lambda_3 + \frac{2n^2 - 46n + N_2}{2^{28}}$$

and from the observations (5), we can express the number of characteristic vectors of length $n - 16$ in terms of the number of shortest characteristic vectors:

$$|\chi_{n-16}| = (2^8 \lambda_2 + (n + 696)\lambda_3)2^{n-24}$$

$$= (2n^2 - 46n + N_2)2^{n-24} + (n - 72)(\lambda_3 2^{n-24})$$

$$= (2n^2 - 46n + N_2)2^{n-24} + (n - 72)|\chi_{n-24}|$$

as claimed. $\square$

Theorem 4.5. Let $L$ be a positive definite unimodular $\mathbb{Z}$-lattice of rank $n$. Suppose further that the shortest characteristic vectors of $L$ have norm $n - 24$. Then $L = L_0 \perp \mathbb{Z}^r$ for some sublattice $L_0$ of rank $\leq 8388630$.

Proof. We may assume $L$ does not represent 1 and prove that the rank of $L$ is at most 8388630.

The hypotheses imply $n \neq 15$. So Corollary 3.5 (b) tells us there can be no more than $n2^n$ second shortest characteristic vectors. So by Lemma 4.4 ,

$$(2n^2 - 46n + N_2)2^{n-24} + (n - 72)|\chi_{n-24}| \leq n2^n.$$ 

We may assume that $n \geq 72$ and we know that the number of shortest characteristic vectors is positive. So

$$(2n^2 - 46n + N_2)2^{n-24} < n2^n.$$ 

Rearranging,

$$2n^2 - (46 + 2^{24})n + N_2 < 0.$$ 

(8)
Next notice that $N_2 \geq 0$. So inequality (8) implies $n$ can be no larger than $8\,388\,630$. \hfill \qed

5. Remarks

I do not claim to have found the best possible bounds for $N_2$ or $N_3$. However, if $N_k$ exists, we can see $N_k \geq 23k$ as follows. Consider the lattice

$$L_k := \bigoplus_{i=1}^{k} O_{23}$$

whose components are all copies of the 23-dimensional shorter Leech lattice $O_{23}$ (see, for example, [CS], 179). In [E2], Elkies notes that $O_{23}$ has shortest characteristic vectors of norm 15. From this it follows that $L_k$ is a $23k$-dimensional lattice with shortest characteristic vectors of norm $23k - 8k$.

It appears that my method of bounding the number of short characteristic vectors does not yield $N_k$ for $k \geq 4$. So Elkies’ question remains open for $k \geq 4$.

Finally, by Construction A of ([CS], 137), we notice that if $k \leq 3$, there is an $n_k$ such that every binary self-dual code whose shadow has minimal norm $\geq \frac{n - 8k}{2}$ is of the form $C_0 \oplus z^r$ for some code $C_0$ of length at most $n_k$.

Acknowledgement

I would like to thank my Ph.D. adviser, Larry Gerstein, for his continuing guidance and support.

References


