JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Mark GAULTER

Characteristic vectors of unimodular lattices which represent two

Tome 19, n° 2 (2007), p. 405-414.

<http://jtnb.cedram.org/item?id=JTNB_2007__19_2_405_0>

Journal de Théorie des Nombres
de Bordeaux **19** (2007), 405-414

Characteristic vectors of unimodular lattices which represent two

par Mark GAULTER

Résumé. On améliore un majorant connu pour la dimension n d'un réseau unimodulaire indécomposable dont la longuer de l'ombre prend la troisième plus grande valeur possible, $n-16$.

Abstract. We improve the known upper bound of the dimension n of an indecomposable unimodular lattice whose shadow has the third largest possible length, $n-16$.

1. Introduction

Throughout, we will consider only unimodular $\mathbb{Z}$-lattices in $\mathbb{R}^n$. We denote the (squared) norm of a vector x in a lattice L by $|x|^2$. We use $x \cdot y$ to represent the inner product of two vectors $x, y \in \mathbb{R}^n$.

The vector w is called a *characteristic vector* of a lattice L if the congruence $x \cdot w \equiv |x|^2 \pmod 2$ holds for every $x \in L$.

The symbol χ will represent the set of characteristic vectors of a lattice. Occasionally, we will use $\chi(L)$ to emphasize that the set under discussion is the set of characteristic vectors of the specific lattice, L. Our focus here will be on the minimal norm of the elements of χ, and accordingly we define s, or for emphasis $s(L)$, to be the norm of the shortest characteristic vectors of L. The quantity s is sometimes called the length of the shadow of L.

Since L is self-dual, it is a simple exercise to show that χ constitutes a coset of $L/2L$. The relationship $s \equiv n \pmod 8$ can be proved in one of several ways, for example by using modular forms, or by using the explicit formula for the characteristic vectors of a lattice given by Gerstein in [7].

Elkies showed in [2] that $s \leq n$. He enumerated the lattices with $s = n$ and those with $s = n-8$, in [2] and [3]. Such lattices which do not represent 1 have dimension $n \leq 23$. Elkies asked whether, for any given value of k, a similar bound was available for lattices with $s = n - 8k$.

We will be interested here in the case $s = n - 16$. We may assume that L does not represent 1, as the following argument shows. Any unimodular lattice can be written as $L = L_0 \perp \mathbb{Z}^r$ for some lattice L_0 that does not represent 1. The lattice L_0 has shortest characteristic vectors of norm $s(L)-r$, and rank $\mathrm{rk}(L_0) = n - r$. Therefore, the difference between the length of

the shadow and the dimension of the lattice is the same for the lattices L and L_0.

If we make the additional assumption that L does not represent 2, then an exact bound on the dimension of L is available. Nebe and Venkov proved in [9] that if L has no roots and $s = n - 16$, then $\mathrm{rk}(L) \leq 46$. This bound is attained by $L = O_{23} \perp O_{23}$, where O_{23} is the shorter Leech lattice.

If L is permitted to represent 2 then the situation is less well understood. It is known from [6] that unimodular lattices with $s = n - 16$ and minimum ≥ 2 do not exist in dimensions above 2907; it follows (see for example, [1]) that the number of isometry classes of such lattices is finite. Before any serious effort is made to enumerate such lattices, it is essential to reduce the bound 2907. In this article, we achieve this by proving the theorem stated below. This result forms one part of Theorem 4.1, a theorem that also indicates restrictions on the possible root systems of a lattice with $s = n - 16$ and $n \geq 57$.

Theorem 1.1. *Let L be a unimodular lattice in $\mathbb{R}^n$ which does not represent 1. If the shortest characteristic vectors of L have norm $s = n - 16$, then $n \leq 89$.*

2. Notation

Throughout, L will denote a unimodular $\mathbb{Z}$-lattice in $\mathbb{R}^n$. Define

$$L_i := \{x \in L : |x|^2 = i\}$$
$$\chi_i := \{w \in \chi : |w|^2 = i\}.$$

We denote the cardinality of L_i in one of two ways: either as $|L_i|$, or as $a_i := |L_i|$. Define $b_i := |\chi_i|$. The symbol s or $s(L)$ will continue to represent the (squared) norm of the shortest characteristic vectors of L. In general, we prefer to use the terminology of characteristic vectors rather than shadows in the proofs of the various results in this article; readers who prefer the terminology of shadows will recognize that $w \in L$ is a characteristic vector precisely when $\frac{w}{2}$ is an element of the shadow of L.

3. Information from theta series, and theta series with spherical coefficients

Throughout this section, L will be a unimodular $\mathbb{Z}$-lattice in $\mathbb{R}^n$ with shortest characteristic vectors of norm $n - 16$ that does not represent 1.

Following [3], we may write

$$\theta_L = \lambda_0 \theta_{\mathbb{Z}}^n + \lambda_1 \theta_{\mathbb{Z}}^{n-8} \theta_{E_8} + \lambda_2 \theta_{\mathbb{Z}}^{n-16} \theta_{E_8}^2. \tag{3.1}$$

Recall that $a_i := |L_i|$. Exactly as in the proof of Lemma 4.2 of [6], we use the information that $a_0 = 1$ and $a_1 = 0$ to solve for λ_i in terms of a_2, the number of vectors of norm 2. This enables us to find the number of

vectors of any given norm in terms of a_2. Indeed, the calculation of a_3 is performed in [9], equation (U3).

$$a_3 = \frac{4}{3}n(n^2 - 69n + 1208) + 2(n-24)a_2. \tag{3.2}$$

Elkies demonstrated in [2] that there is an analogous equation to equation (3.1) for the *shadow* of a lattice. Define

$$\theta'(L) := \sum_{w \in \chi} q^{|w/2|^2}.$$

We have

$$\theta'_L = \lambda_0 \theta'_{\mathbb{Z}^n} + \lambda_1 \theta'_{\mathbb{Z}^{n-8}} \theta_{E_8} + \lambda_2 \theta'_{\mathbb{Z}^{n-16}} \theta_{E_8^2}. \tag{3.3}$$

For any i, we are thus able to deduce b_i, the number of characteristic vectors of norm i, in terms of a_2. We will be most interested in the values of $b_s = b_{n-16}$ and $b_{s+16} = b_n$. These values are

$$b_{n-16} = 2^{n-24}(2n^2 - 46n + a_2), \tag{3.4}$$

$$\begin{aligned} b_n &= 2^n\lambda_0 + 2^{n-8}(n+232)\lambda_1 + 2^{n-17}(n^2+927n+108752)\lambda_2 \\ &= 2^{n-25}(2n^4 - 240n^3 + 25358n^2 - 496992n + 33554432 \\ &\qquad + a_2(n^2 - 97n + 2256)). \end{aligned} \tag{3.5}$$

Finally in this section, we will need a means of calculating the inner product of various elements of L_2 and L_3 with elements of χ_s. We will use the theta series of L with spherical coefficients. Nebe and Venkov have already completed the relevant calculation to produce equation (C2) of [9]; if L has shortest characteristic vectors of norm $s = n - 16$, then for any fixed $w \in \chi$, we have

$$\sum_{l \in L_3} (l \cdot w)^2 - 2(n-36) \sum_{r \in L_2} (r \cdot w)^2 = (4(n^2 - 69n + 1208) + 2a_2)|w|^2. \tag{3.6}$$

Indeed, this equation holds even if w is replaced by an arbitrary element of the underlying space $\mathbb{R}^n$.

4. Translation of elements of χ by short vectors

In this section, we prove some elementary relations between elements of χ and elements of L_2 and L_3. We combine these observations with those obtained using theta series arguments to prove the main result.

Proposition 4.1. *Given a lattice L and $w \in \chi_s$ we have for every $l \in L$, $|w \cdot l| \leq |l|^2$*

Proof. The vectors $w \pm 2l$ are both characteristic. Therefore, $|w \pm 2l|^2 \geq s$; expanding this equation enables us to bound $w \cdot l$. □

Before introducing the next lemma, we recall that the set of *roots* of L is defined to be the set of vectors of norm 1 or 2. Since L has no vectors of norm 1, the set of roots of L is precisely L_2.

Each root generates a reflective symmetry of L. This observation led to the classification of all possible root systems (see [1], Chapter 4) for an arbitrary integral lattice.

One possible subset of L_2 is A_i. Given a copy of A_i, one can choose a basis $\{x_1, \cdots, x_i\}$ such that the Gram matrix of the subset of L generated by this basis is

$$A_i = \begin{pmatrix} 2 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 1 & \cdots & 1 \\ 1 & 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 2 \end{pmatrix}. \tag{4.1}$$

It is possible for L_2 to contain many different copies of A_i; we will be most interested in the copy of A_r with largest rank. Define

$$r := \max\{i : \exists A_i \subset L\}. \tag{4.2}$$

Clearly, $r \leq n$.

Lemma 4.1. *Let L be a lattice with minimum ≥ 2. As in equation (4.2), define r to be the rank of the largest copy of A_i contained in L. Given a set $\{l_i : 1 \leq i \leq m\} \subset L_3$ with the property that $l_i \cdot l_j = 2$ whenever $i \neq j$, we can conclude that $m \leq r + 1$.*

Proof. Consider the set $T := \{l_1 - l_j : 1 < j \leq m\}$. First, note that T is a subset of L_2. Further, $(l_1 - l_i) \cdot (l_1 - l_j) = 1$ whenever $i \neq j$. Therefore the vectors $l_1 - l_i$ generate a copy of A_{m-1} contained in L; this ensures that $m - 1 \leq r$. □

Lemma 4.2. *Suppose that L is a lattice with $s = n - 16$ that does not represent 1. Define r as in equation (4.2). Then*

$$\frac{b_n}{b_{n-16}} \geq \frac{\min_{w \in \chi_s} |\{l \in L_3 : w \cdot l = 1\}|}{r + 1}.$$

Proof. Given $w \in \chi_s$ and $l \in L_3$, it is easy to show that $w \cdot l = 1$ if and only if $|w + 2l|^2 = s + 16 = n$. Therefore

$$T := \{w + 2l : w \in \chi_{n-16}, l \in L_3, w \cdot l = 1\} \subset \chi_n.$$

To bound from below the number of elements in T, we must bound from above the number of different ways of expressing a given element of χ_n in the form $w + 2l$ with $w \in \chi_{n-16}$ and $l \in L_3$.

To this end, fix $w \in \chi_n$ and write $w = w_i + 2l_i$ in as many different ways as possible with $w_i \in \chi_{n-16}$ and $|l_i|^2 = 3$. Index the list $1 \leq i \leq m$.

Given two expressions from the list

$$w_i + 2l_i = w_j + 2l_j$$

we have

$$|w_i + 2l_i - 2l_j|^2 = s.$$

Expanding, we obtain

$$4w_i \cdot l_i - 4w_i \cdot l_j - 8l_i \cdot l_j + 4|l_i|^2 + 4|l_j|^2 = 0.$$

Substituting known values, we obtain

$$4 - 4w_i \cdot l_j - 8l_i \cdot l_j + 12 + 12 = 0.$$

Dividing by 4,

$$w_i \cdot l_j + 2l_i \cdot l_j = 7. \tag{4.3}$$

Proposition 4.1 bounds the first term of equation (4.3). Since $l_i, l_j \in L_3$, the possible solutions to equation (4.3) are :

$$w_i \cdot l_j = 1,\ l_i \cdot l_j = 3,$$

$$w_i \cdot l_j = 3,\ l_i \cdot l_j = 2.$$

The first solution happens only if $i = j$. Applying Lemma 4.1 tells us that $m \leq r + 1$.

To conclude the proof, we bound the number of elements in

$$T := \{w + 2l : w \in \chi_{n-16}, l \in L_3, w \cdot l = 1\}.$$

The full list of expressions $w_i + 2l_i$ with $w_i \in \chi_{n-16}$ and $w_i \cdot l_i = 1$ has at least $b_{n-16} \min_{w \in \chi_s} |\{l \in L_3, w \cdot l = 1\}|$ items. Each element of χ_n that appears on this list appears at most $r + 1$ times. Therefore

$$|T| \geq b_{n-16} \frac{\min_{w \in \chi_s} |\{l \in L_3, w \cdot l = 1\}|}{r+1}.$$

Since $T \subset \chi_n$, we have $|T| \leq b_n$. This gives the required result. □

The final ingredient in the proof of the main result is an understanding of the number of elements $l \in L_3$ with $w \cdot l = 1$.

Define

$$n_{i,j}(w) = \{l \in L_i : w \cdot l = j\}.$$

Now fix w; this will enable us to suppress reference to w from our notation. Proposition 4.1 tells us that $n_{i,j} = 0$ whenever $i < j$. Since w is characteristic, we know that $n_{i,j} = 0$ whenever $i \neq j \pmod 2$. Finally, symmetry of the lattice assures us that $n_{i,j} = n_{i,-j}$. To use Lemma 4.2, we need to bound $n_{3,1}$ from below.

Lemma 4.3. *Suppose L is a lattice with $s = n - 16$. Fix $w \in \chi_s$. Define :*

$$n_{i,j} = \{l \in L_i : w \cdot l = j\}.$$

Then

$$n_{3,1} = \frac{1}{2}(9664 + 656n - 61n^2 + n^3 + 2(n-25)a_2 - 2(n-36)n_{2,2}).$$

Proof. Since $n_{3,j} \neq 0$ only for $j \in \{-3, -1, 1, 3\}$, we have

$$a_3 = 2n_{3,1} + 2n_{3,3}. \tag{4.4}$$

The earlier discussion of theta series yielded equation (3.2), which may now be written:

$$2n_{3,1} + 2n_{3,3} = \frac{4}{3}n(n^2 - 69n + 1208) + 2(n-24)a_2. \tag{4.5}$$

Equation (3.6) reduces to

$$18n_{3,3} + 2n_{3,1} - 16(n-36)n_{2,2} = (4(n^2 - 69n + 1208) + 2a_2)(n-16). \tag{4.6}$$

Solving equations (4.5) and (4.6) yields :

$$n_{3,1} = \frac{1}{2}(9664 + 656n - 61n^2 + n^3 + 2(n-25)a_2 - 2(n-36)n_{2,2}).$$

□

Lemma 4.4. *Let L be a lattice with $s = n - 16$. Suppose that L does not represent 1, and define*

$$r := \max\{i : \exists A_i \subset L\}.$$

Now define a to be the number of roots that are not elements of this largest A_i; that is,

$$a := |L_2| - |A_r|.$$

Then for any $w \in \chi_{n-16}$,

$$n_{2,2}(w) \leq \frac{(1+r)^2}{4} + \frac{a}{2}\,.$$

Proof. We will use the construction of A_r illustrated on page 108 of [1]; choose an orthonormal basis $\{e_1, \cdots, e_{r+1}\}$ for $\mathbb{R}^{r+1}$. Then take A_r to be the set of vectors $\{e_i - e_j : i \neq j\}$. The basis $\{e_1 - e_j\}$ yields the Gram matrix for A_r displayed in equation (4.1).

Define the map π_0 to be the projection from L onto its copy of A_r, and define ϕ to be an isometry from the copy of A_r embedded in L to the copy of A_r embedded in $\mathbb{R}^{r+1}$. Define π to be the composition:

$$\pi := \phi \circ \pi_0\,.$$

The inner product $(e_i - e_j) \cdot \pi(w) \in \{\pm 2, 0\}$. It follows that, as i varies, $e_i \cdot \pi(w)$ assumes at most two values. Therefore the equation $(e_i - e_j) \cdot \pi(w) = 0$ is satisfied at least

$$\min_{0 \le k \le r+1} k(k-1) + (r+1-k)(r-k) \ge \frac{r^2-1}{2}$$

times. Each solution to $(e_i - e_j) \cdot \pi(w) = 0$ corresponds to exactly one element of the set $\{x \in L_2 : x \cdot w = 0\}$. Since A_r contains $r(r+1)$ elements of norm 2, we deduce that

$$n_{2,2}(w) \le \frac{(1+r)^2}{4} + \frac{a}{2}\,.$$

□

Theorem 4.1. *Let L be a lattice with $s = n - 16$ that does not represent 1. Suppose further that $n > 23$. Define*

$$r := \max\{i : \exists A_i \subset L\}.$$

Then the following inequality is satisfied.

$$\begin{aligned} &(67108864 + 67094012r - 10312r^2 + 4604r^3 + 64r^4) \\ &+ (-103240 - 996777r - 4645r^2 - 199r^3 - 3r^4)n \\ &+ (72294 + 50988r + 392r^2 + 2r^3)n^2 + (-8714 - 486r - 8r^2)n^3 \\ &+ (340 + 4r)n^4 - 4n^5 \ge 0\,. \end{aligned} \tag{4.7}$$

It follows that $n \le 89$.

Proof. Lemma 4.2 tells us:

$$\frac{b_n}{b_{n-16}} \ge \frac{\min_{w \in \chi_s} |\{l \in L_3 : w \cdot l = 1\}|}{r+1}\,.$$

Lemma 4.3 and Lemma 4.4 bound the numerator of the right hand side.

$$\frac{b_n}{b_{n-16}} \ge \frac{\frac{1}{2}(9664 + 656n - 61n^2 + n^3 + 2(n-25)a_2 - 2(n-36)(\frac{(1+r)^2}{4} + \frac{a}{2}))}{r+1}.$$

The quantities b_n and b_{n-16} are given explicitly in terms of a_2 by equations (3.4) and (3.5). Substituting, we obtain

$$\begin{aligned} &\frac{2^{n-25}(2n^4 - 240n^3 + 25358n^2 - 496992n + 33554432 + a_2(n^2 - 97n + 2256))}{2^{n-24}(2n^2 - 46n + a_2)} \\ &\ge \frac{\frac{1}{2}(9664 + 656n - 61n^2 + n^3 + 2(n-25)a_2 - 2(n-36)(\frac{(1+r)^2}{4} + \frac{a}{2}))}{r+1} \end{aligned} \tag{4.8}$$

That is,

(4.9)

$$\frac{(2n^4 - 240n^3 + 25358n^2 - 496992n + 33554432 + a_2(n^2 - 97n + 2256))}{2(2n^2 - 46n + a_2)}$$
$$\geq \frac{9664 + 656n - 61n^2 + n^3 + (2(n-25)a_2 - 2(n-36)(\frac{(1+r)^2}{4} + \frac{a}{2}))}{2(r+1)}.$$

Note that $a_2 = r(r+1) + a$. Since $n > 23$, this inequality can be better understood by cross-multiplying, and observing that for fixed n and r, the terms involving a on the left hand side are smaller than those involving a on the right hand side. That is, the inequality can be true for a triple (n, r, a) only if it is true for $(n, r, 0)$.

Expanding and collecting like terms, we are left with the inequality (4.7). A little computer time is enough to demonstrate that our lattice must have $n \leq 89$. □

One can use inequality (4.7) to bound the rank r of the largest copy of $A_i \subset L$. We discover that for each possible dimension of L the rank $r \leq 74$. For each value of n, Table 1 records the possible values of r for that dimension. In dimensions between 47 and 56, calculations merely indicate that L must contain an A_1; that is, that L must represent 2. However, this has already been proved in [9].

5. The relationship between the minimum of a lattice and the norm of a shortest characteristic vector

It is possible slightly to strengthen the upper bound of Theorem 4.1 using an argument that includes examining each possible root system in turn. There are no known lattices with $s = n - 16$ and $n > 46$, but reducing the upper bound of Theorem 4.1 to an upper bound of 46 seems to be beyond the scope of this method.

In general, the question of proving that a lattice L in $\mathbb{R}^n$ has bounded dimension is easier if more assumptions are made about the minimum of the lattice. Table 2 describes what is known: each entry is justified after this descriptive paragraph. An asterisk means that the bound is known to be best possible, The symbol "-" means that no such lattices exist.

For lattices with minimum 2, the cases $s = n$ and $s = n - 8$ are included in [2] and [3] respectively. The case $s = n - 16$ is Theorem 4.1 of this paper; the case $s = n - 24$ is discussed in [6].

For lattices with minimum 3, the cases $s \geq n - 8$ are included in [2] and [3]. The case $s = n - 16$ is examined in [9], and the case $s = n - 24$ is Theorem 4.5 of [6]; this theorem applies to any L that does not represent 1.

Dimension n	Smallest allowable r	Largest allowable r
57	2	57
58	2	58
59	2	59
60	2	60
61	3	61
62	3	62
63	4	63
64	4	64
65	4	65
66	5	66
67	5	67
68	6	68
69	7	69
70	7	70
71	8	71
72	9	72
73	9	73
74	10	74
75	11	74
76	12	73
77	13	71
78	14	70
79	15	69
80	16	68
81	17	66
82	19	65
83	21	63
84	22	61
85	24	59
86	27	57
87	29	54
88	33	51
89	39	44

TABLE 1. The largest copy of A_i contained in a lattice $L \in \mathbb{R}^n$ whose shortest characteristic vectors have norm $n - 16$

For lattices with minimum 4, the cases $s = n$ and $s = n - 8$ are covered in [2] and [3]. No lattices exist in the case $s = n - 16$; to see this, use equation (3.2) of this article, which originally appeared in [9]. Set $a_2 = 0$, and calculate a_3 for each $n \leq 46$. In no case does $a_3 = 0$.

Minimum	$s = n$	$s = n - 8$	$s = n - 16$	$s = n - 24$	$s = n - 32$
2	-	22*	89	8 388 630	unknown
3	-	23*	46*	8 388 630	unknown
4	-	-	-	47*	unknown

TABLE 2. Bounds on dimension of a unimodular lattice with given minimum and norm of shortest characteristic vector

The final bound, for lattices with minimum 4 and $s = n - 24$, is due to Gaborit. Lattices with minimum $k + 1$ and shortest characteristic vectors of norm $n - 8k$ were defined as k-extremal in Section 8 of [5]; it was shown that for any given k, the dimension of k-extremal lattices is bounded, but an explicit bound was not given. This notion was independently introduced and studied by Gaborit who, in [4], found that if k is odd, then there is an explicit upper bound of $12(k + 1)$ on the dimension of a k-extremal lattice. Gaborit showed that this bound is optimal in the case $k = 3$, by exhibiting a suitable lattice of rank 47. In the same paper, Gaborit proved that only when $k = 1$ does there exist a lattice with minimum $k + 2$ and shortest characteristic vectors of norm $n - 8k$; the only such lattice is the shorter Leech lattice, O_{23}. This fact has implications for the main diagonal of Table 2.

References

[1] J. H. CONWAY AND N. J. A. SLOANE, *Sphere Packings, Lattices and Groups*. Third Edition, Springer-Verlag New York, 1999.
[2] N. D. ELKIES, *A characterization of the $\mathbb{Z}^n$ lattice*. Math Res. Lett. **2** (1995), 321–326.
[3] N. D. ELKIES, *Lattices and codes with long shadows*. Math Res. Lett. **2** (1995), 643–651.
[4] P. GABORIT, *Bounds for certain s-extremal lattices and codes*. Preprint.
[5] M. GAULTER, *Characteristic Vectors of Unimodular Lattices over the Integers*. Ph.D. Thesis, University of California, Santa Barbara, 1998.
[6] M. GAULTER, *Lattices without short characteristic vectors*. Math Res. Lett. **5** (1998), 353–362.
[7] L. J. GERSTEIN, *Characteristic elements of unimodular lattices*. Linear and Multilinear Algebra **52** (2004), 381–383.
[8] J. MARTINET, *Réseaux Euclidiens Designs Sphériques et Formes Modulaires*. L'Enseignement Mathématique, Geneva, 2001.
[9] G. NEBE AND B. VENKOV, *Unimodular Lattices with Long Shadow*. J. Number Theory **99** (2003), 307–317.

Mark GAULTER
446 Nineteenth Avenue Northeast
Saint Petersburg, Florida 33704
États-Unis d'Amérique
E-mail: markgaulter@gmail.com