Strongly modular lattices with long shadow

par Gabriele NEBE

RÉSUMÉ. Cet article donne une classification des réseaux fortement modulaires dont la longueur de l'ombre prend les deux plus grandes valeurs possibles.

ABSTRACT. This article classifies the strongly modular lattices with longest and second longest possible shadow.

1. Introduction

To an integral lattice L in the euclidean space $(\mathbb{R}^n, (,))$, one associates the set of characteristic vectors $v \in \mathbb{R}^n$ with $(v, x) \equiv (x, x) \mod 2\mathbb{Z}$ for all $x \in L$. They form a coset modulo $2L^*$, where

$$L^* = \{ v \in \mathbb{R}^n \mid (v, x) \in \mathbb{Z} \ \forall x \in L \}$$

is the dual lattice of L. Recall that L is called integral, if $L \subset L^*$ and unimodular, if $L = L^*$. For a unimodular lattice, the square length of a characteristic vector is congruent to n modulo 8 and there is always a characteristic vector of square length $\leq n$. In [1] Elkies characterized the standard lattice \mathbb{Z}^n as the unique unimodular lattice of dimension n, for which all characteristic vectors have square length $\geq n$. [2] gives the short list of unimodular lattices L with $\min(L) \geq 2$ such that all characteristic vectors of L have length $\geq n - 8$. The largest dimension n is 23 and in dimension 23 this lattice is the shorter Leech lattice O_{23} of minimum 3. In this paper, these theorems are generalized to certain strongly modular lattices. Following [7] and [8], an integral lattice L is called N-modular, if L is isometric to its rescaled dual lattice $\sqrt{N}L^*$. A N-modular lattice L is called strongly N-modular, if L is isometric to all rescaled partial dual lattices $\sqrt{m}L^{*,m}$, for all exact divisors m of N, where

$$L^{*,m} := L^* \cap \frac{1}{m}L.$$

The simplest strongly N-modular lattice is

$$C_N := \perp_{d|N} \sqrt{d}\mathbb{Z}$$

Manuscrit reçu le 10 septembre 2002.

of dimension $\sigma_0(N) := \sum_{d|N} 1$ the number of divisors of N. The lattice C_N plays the role of $\mathbb{Z} = C_1$ for square free N > 1.

With the help of modular forms Quebbemann [8] shows that for

$$N \in \mathcal{L} := \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$$

(which is the set of all positive integers N such that the sum of divisors

$$\sigma_1(N) := \sum_{d|N} d$$

divides 24), the minimum of an even strongly N-modular lattice L of dimension n satisfies

$$\min(L) \le 2 + 2 \left\lfloor \frac{n \ \sigma_1(N)}{24 \ \sigma_0(N)} \right\rfloor.$$

Strongly modular lattices meeting this bound are called extremal. Whereas Quebbemann restricts to even lattices, [9] shows that the same bound also holds for odd strongly modular lattices, where there is one exceptional dimension $n = \sigma_0(N)(\frac{24}{\sigma_1(N)} - 1)$, where the bound on the minimum is 3 (and not 2). In this dimension, there is a unique lattice $S^{(N)}$ of minimum 3. For N = 1, this is again the shorter Leech lattice O_{23} . The main tool to get the bound for odd lattices is the shadow

$$S(L) := \left\{ \frac{v}{2} \mid v \text{ is a characteristic vector of } L \right\}.$$

If L is even, then $S(L) = L^*$ and if L is odd, $S(L) = L_0^* - L^*$, where

$$L_0 := \{ v \in L \mid (v, v) \in 2\mathbb{Z} \}$$

is the even sublattice of L.

For $N \in \mathcal{L}$ let

$$s(N) := \frac{24}{\sigma_1(N)}.$$

The main result of this paper is Theorem 3. It is shown that for a strongly N-modular lattice L that is rationally equivalent to C_N^k , the minimum

$$\min_0(S(L)) := \min\{(v,v) \mid v \in S(L)\}$$

equals

$$M^{(N)}(m,k) := \begin{cases} \frac{1}{N} (k \frac{\sigma_1(N)}{4} - 2m) & \text{if } N \text{ is odd} \\ \frac{1}{N} (k \frac{\sigma_1(N/2)}{2} - m) & \text{if } N \text{ is even} \end{cases}$$

for some $m \in \mathbb{Z}_{\geq 0}$. If $\min_0(S(L)) = M^{(N)}(0,k)$, then $L \cong C_N^k$. For the next smaller possible minimum $\min_0(S(L)) = M^{(N)}(1,k)$ one gets that $L \cong C_N^l \perp L'$, where $\min(L') > 1$ and $\dim(L') \leq \sigma_0(N)(s(N)-1)$ for odd N resp. $\dim(L') \leq \sigma_0(N)s(N)$ for even N. The lattices L' of maximal possible dimensions have minimum 3 and are uniquely determined: $L' = S^{(N)}$, if N

is odd and $L' = O^{(N)}$ (the "odd analogue" of the unique extremal strongly N-modular lattice of dimension $\sigma_0(N)s(N)$) if N is even (see [9, Table 1]).

The main tool to prove this theorem are the formulas for the theta series of a strongly N-modular lattice L and of its shadow S(L) developed in [9]. Therefore we briefly repeat these formulas in the next section.

2. Theta series

For a subset $S \subset \mathbb{R}^n$, which is a finite union of cosets of an integral lattice we put its theta series

$$\Theta_S(z) := \sum_{v \in S} q^{(v,v)}, \quad q = \exp(\pi i z).$$

The theta series of strongly N-modular lattices are modular forms for a certain discrete subgroup Γ_N of $SL_2(\mathbb{R})$ (see [9]). Fix $N \in \mathcal{L}$ and put

$$g_1^{(N)}(z) := \Theta_{C_N}(z) = 1 + 2q + 2\operatorname{ev}(N)q^2 + \dots$$

where

$$\operatorname{ev}(N) := \left\{ \begin{array}{ll} 1 & \text{if } N \text{ is even} \\ 0 & \text{if } N \text{ is odd} \end{array} \right..$$

Let η be the Dedekind eta-function

$$\eta(z) := q^{\frac{1}{12}} \prod_{m=1}^{\infty} (1 - q^{2m}), \quad q = \exp(\pi i z).$$

and put

$$\eta^{(N)}(z) := \prod_{d|N} \eta(dz).$$

If N is odd define

$$g_2^{(N)}(z) := \left(\frac{\eta^{(N)}(z/2)\eta^{(N)}(2z)}{\eta^{(N)}(z)^2}\right)^{s(N)}$$

and if N is even then

$$g_2^{(N)}(z) := \Big(rac{\eta^{(N/2)}(z/2)\eta^{(N/2)}(4z)}{\eta^{(N/2)}(z)\eta^{(N/2)}(2z)}\Big)^{s(N)}.$$

Then $g_2^{(N)}$ generates the field of modular functions of Γ_N . It is a power series in q starting with

$$g_2^{(N)}(z) = q - s(N)q^2 + \dots$$

Theorem 1. ([9, Theorem 9, Corollary 3]) Let $N \in \mathcal{L}$ and L be a strongly N-modular lattice that is rational equivalent to C_N^k . Define $l_N := \frac{1}{8}\sigma_1(N)$, if N is odd and $l_N := \frac{1}{6}\sigma_1(N)$, if N is even. Then

$$\Theta_L(z) = g_1^{(N)}(z)^k \sum_{i=0}^{\lfloor kl_N \rfloor} c_i g_2^{(N)}(z)^i$$

for $c_i \in \mathbb{R}$. The theta series of the rescaled shadow $S := \sqrt{N}S(L)$ of L is

$$\Theta_S(z) = s_1^{(N)}(z)^k \sum_{i=0}^{\lfloor kl_N \rfloor} c_i s_2^{(N)}(z)^i$$

where $s_1^{(N)}$ and $s_2^{(N)}$ are the corresponding "shadows" of $g_1^{(N)}$ and $g_2^{(N)}$.

For odd N

$$s_1^{(N)}(z) = 2^{\sigma_0(N)} \frac{\eta^{(N)}(2z)^2}{\eta^{(N)}(z)}$$

and

$$s_2^{(N)}(z) = -2^{-s(N)\sigma_0(N)/2} \left(\frac{\eta^{(N)}(z)}{\eta^{(N)}(2z)}\right)^{s(N)}$$

For N=2 one has

$$s_1^{(2)}(z) = \frac{2\eta(z)^5 \eta(4z)^2}{\eta(z/2)^2 \eta(2z)^3}$$

and

$$s_2^{(2)}(z) = -\frac{1}{16} \left(\frac{\eta(z/2)\eta(2z)^2}{\eta(z)^2\eta(4z)} \right)^8$$

which yields $s_1^{(N)}$ and $s_2^{(N)}$ for N = 6, 14 as

$$s_1^{(N)} = s_1^{(2)}(z)s_1^{(2)}\left(\frac{N}{2}z\right)$$

and

$$s_2^{(N)} = (s_2^{(2)}(z)s_2^{(2)}\Big(\frac{N}{2}z\Big))^{s(N)/s(2)}.$$

If N is odd, then $s_1^{(N)}$ starts with $q^{\sigma_1(N)/4}$ and $s_2^{(N)}$ starts with q^{-2} . If N is even, then $s_1^{(N)}$ starts with $q^{\sigma_1(\frac{N}{2})/2}$ and $s_2^{(N)}$ starts with q^{-1} .

3. Strongly modular lattices with long shadow.

Proposition 2. Let $N \in \mathbb{N}$ be square free and let L be a strongly N-modular lattice. If L contains a vector of length 1, then L has an orthogonal summand C_N .

<u>Proof.</u> Since L is an integral lattice that contains a vector of length 1, the unimodular lattice \mathbb{Z} is an orthogonal summand of L. Hence $L = \mathbb{Z} \perp L'$. If d is a divisor of N, then

$$L \cong \sqrt{d}L^{*,d} = \sqrt{d}\mathbb{Z} \perp \sqrt{d}(L')^{*,d}$$

by assumption. Hence L contains an orthogonal summand $\sqrt{d}\mathbb{Z}$ for all divisors d of N and therefore C_N is an orthogonal summand of L.

Theorem 3. (see [2] for N = 1) Let $N \in \mathcal{L}$ and L be a strongly N-modular lattice that is rational equivalent to C_N^k . Let $M^{(N)}(m,k)$ be as defined in the introduction.

- (i) $\min_0(S(L)) = M^{(N)}(m, k)$ for some $m \in \mathbb{Z}_{>0}$.
- (ii) If $\min_0(S(L)) = M^{(N)}(0, k)$ then $L \cong C_N^k$.
- (iii) If $\min_0(S(L)) = M^{(N)}(m,k)$ then $L \cong C_N^a \perp L'$, where L' is a strongly N-modular lattice rational equivalent to C_N^{k-a} with $\min(L') \geq 2$ and $\min_0(S(L')) = M^{(N)}(m,k-a)$.
- (iv) If $\min_0(S(L)) = M^{(N)}(m,1)$ and $\min(L) \geq 2$, then the number of vectors of length 2 in L is

$$2k(s(N) + ev(N) - (k+1)).$$

In particular $k \leq k_{max}(N)$ with

$$k_{max}(N) = s(N) - 1 + \operatorname{ev}(N)$$

and if $k = k_{max}(N)$, then $\min(L) \geq 3$.

Proof. (i) Follows immediately from Theorem 1.

- (ii) In this case the theta series of L is g_1^k . In particular L contains 2k vectors of norm 1. Applying Proposition 2 one finds that $L \cong C_N$.
- (iii) Follows from Proposition 2 and Theorem 1.
- (iv) Since $\min(L) > 1$, $\Theta_L = g_1^k 2kg_1^kg_2$. Explicit calculations give the number of norm-2-vectors in L.

The following table gives the maximal dimension $n_{max}(N) = \sigma_0(N)k_{max}(N)$ of a lattice in Theorem 3 (iv).

N	1	2	3	5	6	7	11	14	15	23
$\sigma_1(N)$	1	3	4	6	12	8	12	24	24	24
$k_{max}(N)$	23	8	5	3	2	2	1	1	0	0
$n_{max}(N)$	23	16	10	6	8	4	2	4	0	0

The lattices L with $\min_0(S(L)) = M^{(N)}(1,k)$ are listed in an appendix. These are only finitely many since k is bounded by k_{max} . In general it is an open problem whether for all m, there are only finitely many strongly N-modular lattices L rational equivalent to C_N^k for some k and of minimum

 $\min(L) > 1$ such that $\min_0(S(L)) = M^{(N)}(m, k)$. For N = 1, Gaulter [3] proved that $k \leq 2907$ for m = 2 and $k \leq 8388630$ for m = 3.

Theorem 4. (cf. [2] for N = 1) Let $N \in \mathcal{L}$ be odd and $k \in \mathbb{N}$ such that

$$\frac{8}{\sigma_1(N)} \le k \le k_{max}(N) = \frac{24}{\sigma_1(N)} - 1.$$

Then there is a unique strongly N-modular lattice $L := L_k(N)$ that is rational equivalent to C_N^k such that $\min(L) > 1$ and $\min_0(S(L)) = M^{(N)}(1,k)$, except for N = 1, where there is no such lattice in dimension 9, 10, 11, 13 and there are two lattices in dimension 18 and 20 (see [2]). If $k = k_{max}(N)$, then L is the shorter lattice $L = S^{(N)}$ described in [9, Table 1] and $\min(L) = 3$.

<u>Proof.</u> For N=15 and N=23 there is nothing to show since $k_{max}(N)=0$. The case N=1 is already shown in [2]. It remains to consider $N \in \{3,5,7,11\}$. Since N is a prime, there are only 2 genera of strongly modular lattices, one consisting of even lattices and one of odd lattices. With a short MAGMA program using Kneser's neighboring method, one obtains a list of all lattices in the relevant genus. In all cases there is a unique lattice with the right number of vectors of length 2. Gram matrices of these lattices are given in the appendix.

Remark 5. For N = 1 and dimension n = 9, 10, 11 the theta series of the hypothetical shadow has non integral resp. odd coefficients, so there is no lattice $L_n(1)$.

Theorem 6. Let $N \in \mathcal{L}$ be even and $k \in \mathbb{N}$ such that

$$\frac{2}{\sigma_1(N/2)} \le k \le k_{max}(N) = \frac{24}{\sigma_1(N)}.$$

If $(k, N) \neq (3, 2)$ then there are strongly N-modular lattices $L := L_k(N)$ that are rational equivalent to C_N^k such that $\min(L) > 1$ and $\min_0(S(L)) = M^{(N)}(1, k)$. If $k = k_{max}(N)$, then $L_k(N)$ is unique. It is the odd lattice $L = O^{(N)}$ described in [9, Table 1] and $\min(L) = 3$.

Remark 7. For N = 2 and k = 3 the corresponding shadow modular form has non integral coefficients, so there is no lattice $L_3(2)$.

Remark 8. All odd lattices $L_k(N)$ in Theorem 6 lie in the genus of C_N^k .

4. Appendix: The lattices $L_k(N)$.

The lattices $L_k(1)$:

The lattices $L_k(1)$ are already listed in [2]. They are uniquely determined by their root-sublattices R_k and given in the following table:

k	8	12	14	15	16	17	18	19	20	21	22	23
R_k	E_8	D_{12}	E_7^2	A_{15}	D_8^2	$A_{11}E_{6}$	D_6^3, A_9^2	$A_7^2D_5$	D_4^5, A_5^4	A_3^7	A_1^{22}	0

The lattices $L_k(N)$ for N > 1 odd:

$$L_2(3)$$
: $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \cong A_2 \perp A_2$.
Automorphism group: $D_{12} \wr C_2$.

Automorphism group: order 1152.

Automorphism group: order 6144.

Automorphism group: $\pm U_4(2).2$ of order 103680.

$$L_2(5)$$
: $\begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} \perp \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$.

Automorphism group: $(\pm C_2) \wr C_2$ of order 32.

Automorphism group: $\pm S_5$ of order 240.

$$L_1(7)$$
: $\begin{pmatrix} 2 & 1 \\ 1 & 4 \end{pmatrix}$.
Automorphism group: $\pm C_2$.

$$L_2(7): \left(\begin{array}{cccc} 3 & -1 & 1 & 0 \\ -1 & 3 & 0 & 1 \\ 1 & 0 & 3 & 1 \\ 0 & 1 & 1 & 3 \end{array}\right).$$

Automorphism group: order 16.

$$L_1(11)$$
: $\begin{pmatrix} 2 & 1 \\ 1 & 6 \end{pmatrix}$.

The lattices $L_k(N)$ for N even:

For N=2 there is only one genus of odd lattices to be considered. Also for N = 14 there is only one odd genus for each k, since 2 is a square modulo 7. For N=6, there are 2 such genera, since $L:=(\sqrt{2}\mathbb{Z})^2 \perp (\sqrt{3}\mathbb{Z})^2$ is not in the genus of C_6 . The genus of L contains no strongly modular lattices. The genus of $L \perp C_6$ contains 3 lattices with minimum 3, none of which is strongly modular.

 $L_2(2): L_2(2) = D_4$ with automorphism group $W(F_4)$ of order 1152.

$$L_4(2): \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & -1 & -1 & 1 \\ 0 & 2 & 0 & 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & 2 & -1 & 1 & 1 & 1 & -1 \\ 0 & 0 & -1 & 2 & -1 & -1 & 0 & 1 \\ 0 & 0 & 1 & -1 & 2 & 1 & 0 & -1 \\ -1 & 1 & 1 & -1 & 1 & 3 & 2 & -2 \\ -1 & 1 & 1 & 0 & 0 & 2 & 3 & -1 \\ 1 & -1 & -1 & 1 & -1 & -2 & -1 & 3 \end{pmatrix}. \text{ The root sublattice is } D_4 \perp A_1^4 \text{ and the automorphism group of } L_4(2) \text{ is } W(F_4) \times (C_2^4:D_8) \text{ of order } 147456.$$

The root sublattice is A_5 and the

$L_6(2)$: There are two such lattices:

with automorphism group of order $2^{15}3^4$ resp. $2^{21}3$.

Automorphism group of order 2752512.

 $L_8(2)$: $L_8(2)$ is the odd version of the Barnes–Wall lattice BW_{16} (see [6]). It is unique by [9, Theorem 8].

$$L_1(6)$$
: $\begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 3 & 0 & -1 \\ -1 & 0 & 3 & -1 \\ 0 & -1 & -1 & 4 \end{pmatrix}$.

Automorphism group C_2^4 .

Automorphism group $SL_2(3).2^2$ of order 96.

$$L_1(14)$$
: Gram matrix $\begin{pmatrix} 3 & 1 \\ 1 & 5 \end{pmatrix} \perp \begin{pmatrix} 3 & 1 \\ 1 & 5 \end{pmatrix}$.
Automorphism group D_8 .

References

- [1] N.D. ELKIES, A characterization of the \mathbb{Z}^n lattice. Math. Res. Lett. 2 no. 3 (1995), 321–326.
- [2] N.D. Elkies, Lattices and codes with long shadows. Math. Res. Lett. 2 no. 5 (1995), 643–651.
- [3] M. GAULTER, Lattices without short characteristic vectors. Math. Res. Lett. 5 no. 3 (1998), 353-362.
- [4] C. L. MALLOWS, A. M. ODLYSKO, N. J. A. SLOANE, Upper bounds for modular forms, lattices and codes. J. Alg. 36 (1975), 68-76.
- [5] T. MIYAKE, Modular Forms. Springer (1989).
- [6] G. NEBE, N.J.A. SLOANE, A database of lattices. http://www.research.att.com/ ~njas/lattices
- [7] H.-G. QUEBBEMANN, Modular lattices in euclidean spaces. J. Number Th. 54 (1995), 190– 202.
- [8] H.-G. QUEBBEMANN, Atkin-Lehner eigenforms and strongly modular lattices. L'Ens. Math. 43 (1997), 55-65.
- [9] E.M. RAINS, N.J.A. SLOANE, The shadow theory of modular and unimodular lattices. J. Number Th. 73 (1998), 359-389.

Gabriele Nebe

Abteilung Reine Mathematik

Universität Ulm

89069 Ulm, Germany

E-mail: nebe@mathematik.uni-ulm.de