



**HAL**  
open science

## On theta series vanishing at infinity and related lattices

Christine Bachoc, Riccardo Salvati Manni

► **To cite this version:**

Christine Bachoc, Riccardo Salvati Manni. On theta series vanishing at infinity and related lattices. Acta Arithmetica, 2006, 124 (1), pp.59-71. hal-00196181

**HAL Id: hal-00196181**

**<https://hal.science/hal-00196181>**

Submitted on 12 Dec 2007

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# ON THETA SERIES VANISHING AT $\infty$ AND RELATED LATTICES

CHRISTINE BACHOC AND RICCARDO SALVATI MANNI

ABSTRACT. In this paper we consider theta series with the highest order of vanishing at the cusp  $\infty$ . When the level is a power of 2, these theta series are the  $m$ -th powers of a certain theta function with characteristic, related to the lattice  $\sqrt{2^k}\mathbb{Z}^m$ . Instead if the level is a power of 3, these theta series are the  $m/2$ -th powers of a theta series associated to the 2-dimensional root lattice  $A_2$  with characteristic. These modular forms have also many representations as theta series related to different lattices; we prove that the lattices of level a power of 2, respectively a power of 3, that afford these theta series, are lattices constructed from binary, respectively ternary codes.

## 1. INTRODUCTION

In a recent paper [8], Imamoglu and Kohnen have studied the  $m$ -th power of the Riemann theta function  $\vartheta$  in relation with the number  $r_m(n)$  of representations of a positive integer  $n$  as a sum of  $m$  integral squares. Their result is interesting, since, for each  $m$ , the computation of  $r_m(n)$  does not require any pre-knowledge of  $r_m(n')$  for  $n' < n$ . One of the main tool used in this proof was that  $\vartheta^m$  has highest order of vanishing at one cusp or, better, that a translate of  $\vartheta$  has highest order of vanishing at the cusp  $\infty$ ; subsequently Kohnen and the second author extended the result to the integral representations of the lattice  $D_m^+$ , [9].

In this paper we want to treat the problem of theta series with the highest order of vanishing at the cusp  $\infty$ . When the level is a power of 2, these theta series are the  $m$ -th powers of a certain theta function with characteristic, related to the quadratic form  $2^k 1_m$  or, in the language of lattices, to the lattice  $\sqrt{2^k}\mathbb{Z}^m$ . Instead if the level is a power of 3, these theta series are the  $m/2$ -th powers of a theta series associated to the 2-dimensional root lattice  $A_2$  with characteristic. These modular forms have also many representations as theta series related to different lattices.

---

*Date:* March 24, 2006.

*2000 Mathematics Subject Classification.* 11H06, 11F11, 11F27.

*Key words and phrases.* theta series, lattices, codes.

Let  $L$  be an integral lattice of rank  $m$ . We denote by  $(\cdot, \cdot)$  its associated scalar product, and we say as usual that  $L$  is even if  $(x, x) \equiv 0 \pmod{2}$ . We define the dual lattice by

$$L' = \{x \in L \otimes \mathbb{Q} \mid (x, y) \in \mathbb{Z}, \text{ for all } y \in L\}.$$

If  $L$  is even, we define the level of  $L$  as the minimal positive integer  $l$  such that the lattice  $\sqrt{l}L'$  is an even lattice.

It is a standard method to exploit the properties of the thetas series that can be attached to a lattice to derive some interesting arithmetic properties of this lattice. For example one can derive bounds for the minimum, which turn out to be tight for small levels and dimension. Also the consideration of the shadow of odd lattices and of its theta series has lead to interesting results, and the property that a lattice contains designs is controlled by theta series with spherical coefficients.

In this paper, we shall consider cosets of  $L/2L$ ,  $L/3L$  and their theta series. In the case of unimodular lattices, among the cosets of  $L/2L$ , there is a fundamental one, the so called canonical class, cf [11], that is characterised by the property that all vectors  $w$  in this coset satisfy  $(v, w) \equiv (v, v) \pmod{2}$ , for all  $v \in L$ . In this paper we shall consider more general cosets.

For any coset  $2L + w$ , we set

$$m(w) := \min_{x \in 2L+w} (x, x)$$

and for any coset  $3L + v$ , we set

$$n(v) := \min_{x \in 3L+v} (x, x).$$

We shall prove that for even lattices of level  $2^k$ ,

$$m(w) \leq m2^{k-1}.$$

Similarly for even lattice of level  $3^k$ , we will get

$$n(v) \leq 3^k m.$$

Both these estimates are sharp. Moreover, we shall characterise the lattices that have a coset reaching these bounds to be the lattices obtained from binary and ternary codes. For a fixed level, the theta series associated to this coset is the same for all these lattices, while their homogeneous theta series may of course vary.

Of special interest is the case of odd unimodular lattices; in this case we get  $m(w) \leq m$  and this coset exists if and only if the lattice is isometric to  $\mathbb{Z}^m$  and  $2L + w$  is the canonical class. This extends the results of [E11] and [E12].

## 2. SOME BASIC FACTS ABOUT MODULAR FORMS

Let  $\mathcal{H}$  be the upper half complex plane. The group  $\Gamma(1) := SL(2, \mathbb{Z})$  acts on it by fractional linear transformations:

$$z \rightarrow \sigma \cdot z := \frac{az + b}{cz + d} \quad \sigma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1).$$

For any positive integer  $N$ , we denote by  $\Gamma(N)$  the subgroup of  $\Gamma(1)$  defined by  $\sigma \equiv 1_2 \pmod{N}$ . We have that the index of  $\Gamma(N)$  in  $\Gamma(1)$  is

$$i(N) := N^3 \prod_{p|N} (1 - p^{-2}).$$

We shall use also the intermediate subgroup  $\Gamma_0(N)$  defined in  $\Gamma(1)$  by the condition  $c \equiv 0 \pmod{N}$  and its subgroup  $\Gamma_1(N)$  defined in  $\Gamma_0(N)$  by the conditions  $a \equiv d \equiv 1 \pmod{N}$ .

Let  $\Gamma$ ,  $k$  and  $\chi$  be respectively a subgroup of finite index of  $\Gamma(1)$ , a positive integer and a character of  $\Gamma$ , then a modular form relative to  $\Gamma$  of weight  $k$  and character  $\chi$  is a holomorphic function  $f : \mathcal{H} \rightarrow \mathbb{C}$  such that for all  $\sigma \in \Gamma$

$$f(\sigma \cdot z) = \chi(\sigma)(cz + d)^k f(z)$$

and  $f$  is holomorphic at the cusps. They form a finite dimensional vector space that we denote by  $[\Gamma, k, \chi]$ . The graded ring of modular forms

$$A(\Gamma, \chi) := \bigoplus_{k=0}^{\infty} [\Gamma, k, (\chi)^k]$$

is finitely generated and normal. We shall omit the character if it is trivial.

The projective variety associated to the ring of modular forms is the Satake compactification of  $\mathcal{H}/\Gamma$ . Set theoretically this is the union of  $\mathcal{H}/\Gamma$  and a finite number of cusps, which set we denote by  $\mathcal{C}$ . In the  $\Gamma(N)$ - case, we have that the number of cusps is equal to the index of  $\pm\Gamma_1(N)$  in  $\Gamma(1)$ . This is 1, 3 and  $c(N) := \frac{i(N)}{2N}$ , according as  $N$  is 1, 2 or  $> 2$ .

For  $N = 1, 2, 4$ , the ring  $A(\Gamma(N))$  is generated by suitable polynomials in the theta functions with half integral characteristics  $\vartheta_{(a,b)}$  defined by

$$\vartheta_{(a,b)}(z) := \sum_{n \in \mathbb{Z}} e^{\pi i((n+a)^2 z + 2b(n+a))} \quad (z \in \mathcal{H} \quad a, b = 0, \frac{1}{2}).$$

The theta function  $\vartheta_{(1/2, 1/2)}$  is identically zero. Only the theta function  $\vartheta_{(1/2, 0)}(z)$  vanishes at the cusp  $\infty$ , in fact it has the following expansion

$$\vartheta_{(1/2, 0)}(z) = 2e^{\pi iz/4} \sum_{n \geq 0} e^{2\pi i \frac{n(n+1)}{2} z} \quad (z \in \mathcal{H}).$$

On the theta functions with half integral characteristics acts the group  $\Gamma(1)$ . The action can be described on the generators by

$$(1) \quad \vartheta_{(a,b)}\left(-\frac{1}{z}\right) = \sqrt{\frac{z}{i}} \vartheta_{(b,-a)}(z)$$

where the square root is chosen to be positive on the positive imaginary axis. Moreover we have

$$\begin{cases} \vartheta_{(0,0)}(z+1) = \vartheta_{(0,1/2)}(z) \\ \vartheta_{(0,1/2)}(z+1) = \vartheta_{(0,0)}(z) \\ \vartheta_{(1/2,0)}(z+1) = e^{\pi i/4} \vartheta_{(1/2,0)}(z). \end{cases}$$

From these transformation formulae, it follows that  $\vartheta_{(a,b)}(z)^4$  belong to  $[\Gamma(2), 2]$ , see [7].

Any modular form  $f$  of weight  $k$  relative to  $\Gamma(N)$  has a Fourier expansion of the form:

$$f(z) = \sum_{n \geq 0} a(n) e^{2\pi i n z / N} \quad (z \in \mathcal{H}).$$

For such modular forms we will define the vanishing order at infinity  $v_\infty(f)$  putting

$$v_\infty(f) := \min_{a(n) \neq 0} (n/N).$$

Moreover we define the slope  $sl(f)$  setting

$$sl(f) := k/v_\infty(f).$$

The following result is rather well known, but we repeat it for sake of completeness:

**Proposition 2.1.** *Let  $f \in [\Gamma(N), k, \chi]$ , assume  $\chi$  has finite order, then  $f$  vanishes identically*

- (1) if  $N = 1$  and  $sl(f) < 12$ ,
- (2) if  $N = 2$  and  $sl(f) < 4$ ,
- (3) if  $N > 2$  and  $sl(f) < \frac{12}{c(N)}$ .

*Proof.* It follows easily from the classical formula computing the degree of the divisor associated to  $f$ . With the notations of [10], if  $f \in [\Gamma(N), k]$  with  $k$  even is non-zero, ([10][Theorem 2.3.3, Theorem 4.2.11]):

$$(2) \quad \sum_{a \in \mathcal{H}/\Gamma(N) \cup \mathcal{C}} \nu_a(f) = \frac{kN}{12} |\mathcal{C}|$$

(with the definition of [10],  $\nu_\infty(f) = Nv_\infty(f)$ ), and from the fact that  $\mathcal{H}/\Gamma(2)$  and  $\mathcal{H}/\Gamma(N)$  have respectively 3 and  $c(N)$  cusps. In case the character  $\chi$  is non trivial (in our situations it is quadratic) or the weight is odd, we replace  $f$  by  $f^2$  or by a suitable power of  $f$ .  $\square$

If  $N = 1, 2, 4$ , we have simple examples showing that these estimates are sharp: the modular form

$$\Delta(z) = (\vartheta_{(1/2,0)}(z)\vartheta_{(0,1/2)}(z)\vartheta_{(0,0)}(z))^8$$

is in  $[\Gamma(1), 12]$  and  $sl(\Delta) = 12$ , the modular form  $\vartheta_{(1/2,0)}(z)^4$  is in  $[\Gamma(2), 2]$  and has slope 4 and the modular form  $\vartheta_{(1/2,0)}(2z)^2$  is in  $[\Gamma(4), 1]$  and has slope 2. We could exhibit examples also for other few cases. In general these examples are not so easy to obtain; in fact theta functions or more generally theta series will not reach the sharp bound, since, geometrically speaking, they do not separate cusps. For example  $\vartheta_{(1/2,0)}(4z)^2$  is in  $[\Gamma(8), 1]$  and has slope 1 (instead of  $1/2$ ). However, as we shall see in next section we can give a sharp bound for theta series.

### 3. LATTICES AND THEIR ASSOCIATED THETA SERIES

For any lattice  $L$  we define the theta series

$$\vartheta_L(z) = \sum_{x \in L} e^{\pi i(x \cdot x)z} \quad (z \in \mathcal{H}).$$

We shall consider also theta series with rational characteristic. We proceed as it follows: for any  $w \in L$ , we set

$$\vartheta_{L,w/q}(z) = \sum_{x \in L+w/q} e^{\pi i(x \cdot x)z} \quad (z \in \mathcal{H}).$$

Obviously this definition depends only on cosets  $qL+w$ , and clearly,  $\vartheta_{\mathbb{Z},1}(z) = \vartheta_{(1/2,0)}(z)$ . We will be mainly interested in the cases  $q = 2, 3$ . In the first case we will speak of theta series with half characteristic

$$\vartheta_{L,w/2}(z) = \sum_{x \in L+w/2} e^{\pi i(x \cdot x)z} \quad (z \in \mathcal{H}).$$

In the second case we will speak of theta series with one third integral characteristic

$$\vartheta_{L,v/3}(z) = \sum_{x \in L+v/3} e^{\pi i(x \cdot x)z} \quad (z \in \mathcal{H}).$$

Let  $A_2$  denote the 2-dimensional root lattice with Gram matrix  $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$  in the basis  $(e_1, e_2)$  and let  $e := e_1 + e_2$ . We have

$$(3) \quad \vartheta_{A_2, e/3}(z) = e^{\pi i \frac{2}{3}z} (3 + 3e^{\pi i 2z} + 6e^{\pi i 4z} + 6e^{\pi i 8z} + \dots).$$

From the inversion formula, cf.[1], page 24, we can calculate that

$$(4) \quad \vartheta_{A_2, e/3}\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right) \frac{1}{\sqrt{3}} \sum_{y \in A'_2} e^{2\pi i(y, e)} e^{\pi i(y, y)z}$$

$$(5) \quad = \left(\frac{z}{i}\right) \frac{1}{\sqrt{3}} (1 - 3e^{\pi i \frac{2}{3}z} + 6e^{\pi i 2z} + \dots).$$

We now state our main theorems:

**Theorem 3.1.** *Let  $L$  be an even lattice of rank  $m$ , of level  $2^k$ ,  $k \geq 0$ , then  $m(w) \leq 2^{k-1}m$ . Moreover, if for some  $w \in L$ ,  $m(w) = 2^{k-1}m$ , then  $\vartheta_{L, w/2}(z) = \lambda \vartheta_{(1/2, 0)}(2^{k-1}z)^m$  for some  $\lambda \in \mathbb{R}^*$ .*

**Theorem 3.2.** *Let  $L$  be an even lattice of rank  $m$ , of level  $3^k$ ,  $k \geq 0$ , then  $n(v) \leq 3^k m$ . Moreover, if for some  $v \in L$ ,  $n(v) = 3^k m$ , then  $m$  is even, and  $\vartheta_{L, v/3}(z) = \lambda \vartheta_{A_2, e/3}(3^{k-1}z)^{m/2}$  for some  $\lambda \in \mathbb{R}^*$ .*

*Proof.* The proofs of the two theorems are very similar. We shall give all details for theorem 3.1. For theorem 3.2 the same proof can be easily adapted. We can assume that the rank  $m$  is even, otherwise we replace  $L$  by  $L \oplus L$ . According to Theorem 1.3.13 in Andrianov's book [1, page 23], when  $L$  is unimodular, we have that  $\vartheta_{L, w/2}(2z)$  is in  $[\Gamma(2), m/2]$ . Similarly if  $L$  is even of level  $N$ ,  $\vartheta_{L, w}(z)$  belongs to  $[\Gamma(N), m/2, \chi]$  for some quadratic character  $\chi$ .

Let us assume that  $L$  is unimodular. Then,  $\vartheta_{L, w/2}(2z)$  has weight  $m/2$  and vanishing at  $\infty$  of  $m(w)/4$ , so we have from Proposition 2.1 (1)

$$sl(\vartheta_{L, w/2}(2z)) = \frac{2m}{m(w)} \geq 4.$$

Hence  $m(w) \leq m/2$ .

Now we assume that for some  $w \in L$ ,  $m(w) = m/2$ . Then  $\vartheta_{L, w/2}(z)$  and  $\vartheta_{(1/2, 0)}(z/2)^m$  have the same weight and vanishing order at  $\infty$ . Moreover  $\vartheta_{(1/2, 0)}^m$  does not have other zeros, so  $\vartheta_{L, w/2}(z)/\vartheta_{(1/2, 0)}(z/2)^m$  is a holomorphic modular function, also at the cusps, hence it is a constant.

The case of level 2 is exactly the same. For the levels  $N = 2^k$  with  $k > 1$ , we need a sharper estimate for the slope of theta series. In the already cited theorem in [1], the transformation formula shows that the

theta series  $\vartheta_{L,w/2}$  vanishes not only at the cusp  $\infty$ , but also at all its  $\Gamma_0(N)$ -conjugates. Indeed, a matrix  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$  transforms  $L + w/2$  into  $L + aw/2 = L + w/2$  because  $ad \equiv 1 \pmod{2}$  hence  $a \equiv 1 \pmod{2}$  (in the case of level 3 we have  $L + aw/2 = L \pm w/2$ ). So the vanishing order is equal at all these cusps. The cardinality of the orbit of the cusp  $\infty$  under the action of  $\Gamma_0(N)$  is equal to the index of  $\pm\Gamma_1(N)$  in  $\Gamma_0(N)$ , that is  $\phi(N)/2 = 2^{k-2}$ . Here  $\phi$  is the Euler function.

Because of this result for theta series and again from (2) we have:

**Proposition 3.1.** *Let  $L$  be an even lattice of level  $2^k$  and rank  $m$ , and let  $f \in [\Gamma(2^k), m/2, \chi]$  be a theta series of the form  $\vartheta_{L,w/2}(z)$ . Then it vanishes identically if*

$$sl(f) < \frac{6\phi(2^k)}{c(2^k)} = 2^{3-k}.$$

From this fact the proof of the theorem easily follows. □

**Remark 3.1.** *As we wrote the proof of theorem 3.2 is similar. Also in this case a proposition similar to proposition 3.1 holds. Obviously for the slope we get the bound*

$$\frac{6\phi(3^k)}{c(3^k)} = 3^{2-k}.$$

**Remark 3.2.** *These precise estimates can be obtained, since, in both cases the theta series  $\vartheta_{L,w/2}(z)$  and  $\vartheta_{L,w/3}(z)$  have equal vanishing at all cusps  $\Gamma_0(q^k)$ -conjugate to the cusp  $\infty$ ,  $q = 2, 3$ . In all other cases, this is false since we would have different vanishing, since the characteristics will change by a factor  $a \in (\mathbb{Z}/q\mathbb{Z})^*$ . This is one of the main obstructions to further generalisations of the results of this paper.*

Of special interest is the case of odd unimodular lattices. Replacing  $L$  by  $\sqrt{2}L$ , an odd unimodular lattice becomes an even lattice of level 4, so we have:

**Corollary 3.1.** *Let  $L$  be an odd unimodular lattice of rank  $m$ , we have  $m(w) \leq m$ . Moreover, if for some  $w \in L$ ,  $m(w) = m$ , then  $\vartheta_{L,w/2}(z) = \lambda\vartheta_{(1/2,0)}(z)^m$  for some  $\lambda \in \mathbb{R}^*$ .*

There are well-known lattices for which the estimate is sharp, namely  $E_8, D_4, \mathbb{Z}^m, A_2$ . They are special cases of a more general family of lattices described in next sections.



Moreover, the natural question is to characterise the cases when this estimate is sharp. This is done in sections 5 and 8.

#### 4. LATTICES FROM BINARY CODES

We describe some lattices for which there exists elements  $w$  with the maximal value for  $m(w)$  according to Theorem 3.1.

We recall what is usually meant by “a lattice constructed from a binary code”. Let  $C \subset \mathbb{F}_2^n$  be a linear binary code of length  $m$ . We denote  $\mathbf{1}$  the all-one word. We define

$$L_C := \{(x_1, \dots, x_m) \in \mathbb{Z}^m \mid (x_1, \dots, x_m) \bmod 2 \in C\}.$$

We have the following result:

**Theorem 4.1.** *Let  $C$  be a binary code with  $\mathbf{1} \in C$ . Let  $w := (1, 1, \dots, 1) \in L_C$ . We have  $m(w) = m$  and:*

$$\vartheta_{L_C, w/2}(z) = \frac{|C|}{2^m} \vartheta_{(1/2, 0)}(z)^m.$$

Proof: Sending  $0 \in \mathbb{F}_2$  to  $0 \in \mathbb{Z}$  and  $1 \in \mathbb{F}_2$  to  $-1 \in \mathbb{Z}$ , we define a lifting map  $c \rightarrow \tilde{c}$  from  $\mathbb{F}_2^m$  to  $\mathbb{Z}^m$ . We have

$$L_C + w/2 = \cup_{c \in C} (2\mathbb{Z})^m + \tilde{c} + w/2.$$

The vectors  $\tilde{c} + w/2$  have their coordinates equal to  $\pm 1/2$ . Hence, for every  $c$ , a suitable isometry  $\sigma$  of the form  $(x_1, \dots, x_m) \rightarrow (\epsilon_1 x_1, \dots, \epsilon_m x_m)$  with  $\epsilon_i = \pm 1$  sends  $(2\mathbb{Z})^m + \tilde{c} + w/2$  to  $(2\mathbb{Z})^m + w/2$ . We derive

$$\vartheta_{L_C, w/2} = |C| \vartheta_{(2\mathbb{Z})^m, w/2}.$$

It is immediate that

$$\sum_{x \in 2\mathbb{Z}^m + w/2} e^{\pi i(x, x)z} = \left( \sum_{n \in \mathbb{Z}} e^{\pi i(2n+1/2)^2} \right)^m = 1/2^m \vartheta_{(1/2, 0)}(z)^m$$

hence the formula. □

**Remark 4.1.** *In the case  $L = \mathbb{Z}^n$ ,  $w = (1, 1, \dots, 1)$  defines the only coset of norm  $m$ ; this is not true for the other lattices. For example, when  $L = D_m$ ,  $w' = (-1, 1, \dots, 1)$  satisfies  $m(w') = m$  but  $w' \neq w \bmod 2L$ .*

From the previous theorem, an easy way to construct a lattice  $L$  containing an element  $w$  with  $m(w) = 2^{k-1}m$  is the following: take  $L = \sqrt{2^{k-1}}L_C$  with  $C$  a binary code.

Let us discuss in which cases such a lattice  $L$  is even of level  $2^k$ .

- (1)  $k = 0$ . Then  $L = \frac{1}{\sqrt{2}}L_C$  is even unimodular if and only if  $C = C^\perp$  and  $C$  is doubly even.
- (2)  $k = 1$ . Then  $L = L_C$  is even if and only if  $C$  is even.
- (3)  $k > 1$ . Then  $L = \sqrt{2^{k-1}}L_C$  is always even.

Moreover, we need that  $2^k(x, x) \in 2\mathbb{Z}$  for all  $x \in L'$ . Since  $L' = \frac{1}{\sqrt{2^{k-1}}}L_C'$  and since  $L_C' = \frac{1}{2}L_{C^\perp}$ , we need  $(x, x) \in 4\mathbb{Z}$  for all  $x \in L_{C^\perp}$ . This leads to the condition that  $C^\perp$  is doubly even.

Let  $\{e_1, \dots, e_m\}$  denote the canonical basis of  $\mathbb{Z}^m$ . If an even lattice  $L$  has the form  $L = \frac{1}{\sqrt{2}}L_C$ , the elements  $\{\sqrt{2}e_1, \dots, \sqrt{2}e_m\}$  provide pairwise orthogonal elements of norm 2 in  $L$ , also called roots.

Conversely, an even lattice  $L$  containing  $m$  pairwise orthogonal roots is easily seen to be isometric to a lattice of the form  $L = \frac{1}{\sqrt{2}}L_C$ .

Standard examples are the following:  $C = \mathbb{F}_2(1, 1, \dots, 1)$  leads to  $L = L_C = D_m$ . The lattice  $E_8$  arises from the extended Hamming code; the Golay code of length 24 leads to the even unimodular lattice in dimension 24 with root system  $A_1^{24}$ .

## 5. THE LATTICES WITH THE LARGEST $m(w)$

Here we characterise all lattices that reach the bounds of Theorem 3.1.

**Theorem 5.1.** *Let  $L$  be an even lattice of rank  $m$  and level  $2^k$ ,  $k \geq 0$ , such that there exists  $w \in L$  with  $m(w) = 2^{k-1}m$ . Then  $L = \sqrt{2^{k-1}}M$ , and there exists a binary code  $C$  such that  $M = L_C$ . Moreover,  $C$  has the following properties:*

- (1) If  $k = 0$ ,  $C = C^\perp$  and  $C$  is doubly even.
- (2) If  $k = 1$ ,  $C^\perp$  is doubly even and  $\mathbf{1} \in C^\perp$ .
- (3) If  $k > 1$ ,  $C^\perp$  is doubly even.

In all cases,  $w := \sqrt{2^{k-1}}(1, 1, \dots, 1) \in L$  and satisfies  $m(w) = 2^{k-1}m$ .

*Proof.* From Theorem 3.1, we have  $\vartheta_{L, w/2}(z) = \lambda \vartheta_{(1/2, 0)}(2^{k-1}z)^m$  for some  $\lambda \in \mathbb{R}^*$ . We recall the inversion formula for  $\vartheta_{L, w/2}(z)$  ([3, Prop 3.1]):

$$(6) \quad \vartheta_{L, w/2}\left(-\frac{1}{z}\right) = \left(\sqrt{\frac{z}{i}}\right)^m \frac{1}{\sqrt{\det(L)}} \sum_{x \in L'} e^{2\pi i(x, w/2)} e^{\pi i z(x, x)}.$$

Taking account of the inversion formula (1) for  $\vartheta_{(1/2, 0)}$  we obtain:

$$(7) \quad \frac{1}{\sqrt{\det(L)}} \sum_{x \in L'} e^{2\pi i(x, w/2)} e^{\pi i z(x, x)} = \frac{\lambda}{2^{(k-1)m/2}} \vartheta_{(0, 1/2)}\left(\frac{z}{2^{k-1}}\right)^m.$$

Since the constant coefficients of the left and right hand side must be equal, we have in fact:

$$(8) \quad \sum_{x \in L'} e^{2\pi i(x, w/2)} e^{\pi i z(x, x)} = \vartheta_{(0, 1/2)} \left( \frac{z}{2^{k-1}} \right)^m.$$

It is worth noticing that this argument in fact calculates the value of  $\lambda$ . We have:

$$\vartheta_{(0, 1/2)}(z)^m = (1 + 2 \sum_{n \geq 1} (-1)^n e^{\pi i n^2 z})^m = 1 - 2m e^{\pi i z} + \dots$$

Now we compare the second coefficient in (8). The notation  $L_i$  stands for  $L_i := \{x \in L \mid (x, x) = i\}$ , and we set  $S := L'_{1/2^{k-1}}$ . We obtain:

$$(9) \quad \sum_{x \in S} e^{\pi i(x, w)} = -2m.$$

The first easy consequence of (9) is that  $S$  is non empty, but we need more: we want to prove that  $S$  contains  $m$  pairwise orthogonal elements. We first notice that, if  $x$  belongs to  $S$ ,  $(x, w)$  can take only the values  $0, \pm 1, \pm 2$ . Indeed, since  $L$  has level  $2^k$ ,  $2^k x \in L$  and hence,  $(w \pm 2^{k+1}x)^2 \geq w^2$  which leads to  $|(x, w)| \leq 2$ . We partition  $S$  into two subsets:  $S_0 := \{x \in S \mid (x, w) = 0, \pm 2\}$  and  $S_1 := \{x \in S \mid (x, w) = \pm 1\}$ . The first set contributes to (9) by  $+1$  and the second by  $-1$ . Obviously, vectors go by pairs  $\pm x$ . So (9) tells us that  $S_1$  contains at least  $2m$  pairs of elements. Moreover, let us prove that, if  $x \neq \pm x' \in S$ , we have  $(x, x') = 0, \pm 1/2^k$ . Since  $L$  has level  $2^k$ , for any  $y \in L'$ ,  $2^{k-1}(y, y) \in \mathbb{Z}$ . Hence, if  $x \neq \pm x'$ ,  $(x \pm x')^2 \geq 1/2^{k-1}$ , and therefore  $|(x, x')| \leq 1/2^k$ . Finally,  $2^k x \in L$  implies  $(x, x') \in 1/2^k \mathbb{Z}$ .

Now assume  $(x_1, \dots, x_s)$  is a maximal chain of pairwise orthogonal elements in  $S_1$ . Of course  $s \leq m$  and we want to prove that  $s = m$ . To any  $x \in S_1$  not in this chain, we can associate an index  $i$  such that  $(x, x_i) = \pm 1/2^k$  (from the previous discussion) otherwise we could increase the chain. If, without loss of generality,  $(x, x_i) = -1/2^k$ , then  $x' = x - x_i$  is another element of  $S$  but this one belongs to  $S_0$ . So the pair  $(x, x')$  contributes to 0 in the sum (9). Since the chain itself contribute to  $-2s$ , this proves that we must have  $s = m$ .

We have found a sublattice of  $L'$  isometric to  $\left(\frac{1}{\sqrt{2^{k-1}}} \mathbb{Z}\right)^m$ . This proves that (up to isometry)  $L \subset \left(\sqrt{2^{k-1}} \mathbb{Z}\right)^m$ . In the case  $k = 0$ , i.e. the even unimodular lattices, we have found  $m$  pairwise orthogonal roots in  $L = L'$ , so we are in case (2) described in previous section.

Let us assume  $k > 0$ . Let  $M := \frac{1}{\sqrt{2^{k-1}}}L$ ;  $M$  is an integral lattice and  $M \subset \mathbb{Z}^m$ . Moreover, since  $2^k L' \subset L$  and  $\left(\frac{1}{\sqrt{2^{k-1}}}\mathbb{Z}\right)^m \subset L'$ , we also have  $(2\mathbb{Z})^m \subset M$ . This obviously means that  $M = L_C$  for some binary code  $C$ . The condition  $2^k(x, x) \in 2\mathbb{Z}$  for all  $x \in L'$  is equivalent to:  $2(x, x) \in 2\mathbb{Z}$  for all  $x \in M'$ . Since  $M' = (L_C)' = \frac{1}{2}L_{C^\perp}$ , it leads to the condition that  $C^\perp$  is doubly even. When  $k > 1$ ,  $L$  is automatically even; when  $k = 1$ ,  $L = L_C$  is even if and only if  $\mathbf{1} \in C^\perp$ .

In all the cases, the code  $C^\perp$  is doubly even, which guaranties that  $\mathbf{1} \in C$ , and hence  $w := \sqrt{2^{k-1}}(1, 1, \dots, 1) \in L$ . From Theorem 4.1,  $m(w) = 2^{k-1}m$ .  $\square$

As a consequence, we obtain in the case of unimodular lattices a strengthening of Elkies result ([4]):

**Corollary 5.1.** *The lattice  $\mathbb{Z}^m$  is the unimodular lattice of dimension  $m$  that contains a coset of minimal norm  $m$ . Moreover, this coset is the canonical class.*

*Proof.* Let  $U$  be such a unimodular lattice. From Theorem 3.1,  $U$  must be odd. Consider the lattice  $L := \sqrt{2}U$ , which is even of level 4. The assumption on  $U$  implies that  $L$  contains an element  $w$  with  $m(w) = 2m$ . From previous theorem,  $L = \sqrt{2}M$  with  $M \subset \mathbb{Z}^m$ . Hence  $M = U = \mathbb{Z}^m$ .  $\square$

## 6. LOWER BOUND

In some cases we can give a lower bound for the maximum of the possible  $m(w)$ . For this reason we need to introduce theta series with double characteristics. For  $w \in L$  and  $l \in L' \otimes \mathbb{Q}$ , we set

$$\vartheta_{L,w/2,l}(z) = \sum_{x \in L+w/2} e^{\pi i[(x \cdot x)z + 2(x \cdot l)]} \quad (z \in \mathcal{H}).$$

Now let  $L$  be an even unimodular lattice such that  $2L \subset \mathbb{Z}^m$  and one vector of the form  $(1, 1, \dots, 1) + 2\mathbb{Z}^m$  is in  $2L$ . We shall denote this vector by  $w_0$ . We remark that all even unimodular 24 dimensional lattices have these properties .

Let  $d$  be the order of  $(1/2)L'/\mathbb{Z}^m$ , then we have

$$\sum_{x \in (1/2)L'/\mathbb{Z}^m} e^{2\pi i(x \cdot (w_0/2))} \vartheta_{\mathbb{Z}^m, w_0, x}(z) = \sum_{x \in (1/2)L'/\mathbb{Z}^m} \sum_{y \in \mathbb{Z}^m} e^{\pi i[(y+w_0/2) \cdot (y+w_0/2)]z + 2(x \cdot y)}.$$

Using the orthogonality of the characters we get

$$d \sum_{y \in 2L} e^{\pi i((y+w_0/2) \cdot (y+w_0/2))z} = d \vartheta_{2L, w_0}(z) \quad (z \in \mathcal{H}).$$

We know that the theta series  $\vartheta_{\mathbb{Z}^m, w, x}(z)$  have vanishing at the cusp  $\infty$  equal to  $m/8$ . For a linear combination the vanishing order cannot decrease, thus for the above described lattices, we have that  $m(w_0/2) \geq m/4$ .

Unfortunately this estimate is not sharp, since we know that for even unimodular 24 dimensional lattices we have  $\max m(w) \geq 8$ . This is the case of the Leech lattice.

## 7. LATTICES FROM TERNARY CODES

We describe some lattices for which there exists elements  $v$  with the maximal value for  $n(v)$  according to Theorem 3.2.

Let  $C \subset \mathbb{F}_3^n$  be a linear ternary code of length  $n$ . Using the isomorphism  $A_2/3A'_2 \simeq \mathbb{Z}/3\mathbb{Z}$ , we can lift a ternary code to a sublattice of  $A_2^n$ :

$$L_C := \{(x_1, \dots, x_n) \in A_2^n \mid (x_1, \dots, x_n) \bmod (3A'_2)^n \in C\}.$$

The resulting lattice is of dimension  $m = 2n$ , and is even since it is a sublattice of  $A_2^n$ . It has level 3, 9 or 27; the case of level 3 corresponds to  $C^\perp \subset C$ .

It is worth noticing that  $e/3 \in A'_2$  and hence  $(e, e, \dots, e) \in L_C$ . We have the following result:

**Theorem 7.1.** *Let  $C$  be a ternary code. Let  $v := (e, e, \dots, e) \in L_C$ . We have  $n(v) = m$  and:*

$$\vartheta_{L_C, v/3}(z) = \frac{|C|}{3^{m/2}} \vartheta_{A_2, e/3}(z)^{m/2}.$$

Proof: We fix a preimage  $\tilde{a} \in A_2$  of each element  $a \in \mathbb{F}_3$  in the following way:  $[\tilde{0}, \tilde{1}, \tilde{2}] = [0, -e_1, -e_2]$ , and define in an obvious way  $\tilde{c}$  for all  $c \in \mathbb{F}_3^n$ . Then

$$L_C + v/3 = \cup_{c \in C} (v/3 + \tilde{c} + (3A'_2)^n).$$

The coordinates of  $v/3 + \tilde{c}$  belong to  $\{e/3, e/3 - e_1, e/3 - e_2\}$ . These three vectors have the same norm  $2/3$ , moreover they are transitively permuted

by the automorphism group of  $A_2$ . Let  $\sigma_i \in \text{Aut}(A_2)$  such that  $e/3 = \sigma_i(e/3 + \tilde{c}_i)$  and let  $\sigma := (\sigma_1, \dots, \sigma_n)$ . Obviously,  $\sigma \in \text{Aut}((3A'_2)^n)$ , and hence  $v/3 + \tilde{c} + (3A'_2)^n = \sigma(v/3 + (3A'_2)^n)$ . As a consequence, the classes  $v/3 + \tilde{c} + (3A'_2)^n$  and  $v/3 + (3A'_2)^n$  have the same theta series, and

$$\vartheta_{L_C, v/3}(z) = |C| \vartheta_{3A'_2, e}(z)^{m/2}.$$

Moreover, the decomposition  $A_2 = 3A'_2 \cup (3A'_2 - e_1) \cup (3A'_2 - e_2)$  and the transitive action of  $\text{Aut}(A_2)$  on  $\{e/3, e/3 - e_1, e/3 - e_2\}$  show that

$$\vartheta_{A_2, e/3}(z) = 3\vartheta_{3A'_2, e/3}(z)$$

hence the formula. □

## 8. THE LATTICES WITH THE LARGEST $n(v)$

Here we characterise all lattices that reach the bounds of Theorem 3.2.

**Theorem 8.1.** *Let  $L$  be an even lattice of rank  $m$  and level  $3^k$ ,  $k \geq 0$ , such that there exists  $v \in L$  with  $n(v) = 3^k m$ . Then  $L = \sqrt{3^k} M$ , and there exists a ternary code  $C$  such that  $M = L_C$ . Moreover,  $C$  has the following properties:*

- (1) If  $k = 0$ ,  $C = C^\perp$
- (2) If  $k > 0$ ,  $C^\perp \subset C$ .

*Proof.* From Theorem 3.2, we have  $\vartheta_{L, v/3}(z) = \lambda \vartheta_{A_2, e/3}(3^{k-1}z)^{m/2}$  for some  $\lambda \in \mathbb{R}^*$ .

We recall the inversion formula for  $\vartheta_{L, v/3}(z)$  ([3, Prop 3.1]):

$$\vartheta_{L, v/3}\left(-\frac{1}{z}\right) = \left(\sqrt{\frac{z}{i}}\right)^m \frac{1}{\sqrt{\det(L)}} \sum_{x \in L'} e^{2\pi i(x, v/3)} e^{\pi i z(x, x)}.$$

Taking account of the inversion formula (4) for  $\vartheta_{A_2, e}$  we obtain:

$$\frac{1}{\sqrt{\det(L)}} \sum_{x \in L'} e^{2\pi i(x, v/3)} e^{\pi i(x, x)z} = \frac{\lambda}{3^{m/2(k-1/2)}} \left(1 - \frac{3m}{2} e^{\pi i \frac{2}{3^k} z} + \dots\right)$$

from which we obtain

$$(10) \quad \sum_{x \in (L')_{\frac{2}{3^k}}} e^{2\pi i(x, v/3)} = -\frac{3m}{2}.$$

Let  $S := (L')_{\frac{2}{3^k}}$ . Similar arguments as in the case of level 2 show that  $|(v, x)| \leq 3$ . We set for  $i = 0, 1, 2$ ,

$$S_i := \{x \in S \mid (x, v) = i \pmod{3}\}.$$

If  $x \in S_0$ ,  $-x \in S_0$  and the pair  $(x, -x)$  contributes to (10) by 2; if  $x \in S_1$ ,  $-x \in S_2$  and the pair  $(x, -x)$  contributes to (10) by  $-1$  (and similarly if  $x \in S_2$ ).

Similar arguments as in the case of level 2 show that the set  $R := 3^{k/2}S$  satisfy  $(r, r') = 0, \pm 1, \pm 2$  for all  $r, r' \in R$  and hence is a root system. Defining  $R_0, R_1, R_2$  in an obvious way, we let  $s$  be the maximal integer such that a chain  $A_2^s$  is contained in  $R_1 \cup R_2$  (here  $A_2$  denotes the root system, not the root lattice). The contribution of this  $A_2^s$  in (10) equals  $-3s$ . Our goal is to prove that  $s = m/2$ .

Let  $x \in R_1 \cup R_2$ ,  $x \notin A_2^s$ . There are two possibilities:

- (1)  $x$  is orthogonal to all the elements of  $A_2^s$
- (2) There exists one component  $A_2$  and one root  $r$  in this component such that  $(x, r) = -1$ .

If several elements  $x$  are in case 1., they can only be pairwise orthogonal otherwise  $s$  would not be maximal. So this leads to a root system of type  $A_2^s \perp A_1^t$  and  $2s + t \leq m$ . The contribution in (10) is  $-3s - t$ . Since  $-3s - t = (-2s - t) - s \geq -m - m/2$ , it can reach  $-3m/2$  only if  $s = m/2$  and  $t = 0$ .

Now let us consider the case 2. The component  $A_2$  together with  $x$  generate a root lattice of dimension 3 which can only be isometric to  $A_3$ , and hence contains 12 roots. We need to discuss how many of these roots belong to  $R_0$  and how many to  $R_1 \cup R_2$ . It is easy to exhaust all possibilities since these roots are linear combinations of a given basis  $(r_1, r_2)$  of the component  $A_2$  and of  $x$ , with  $(x, r_1) = -1$  and  $(x, r_2) = 0$ . We have  $(v, x), (v, r_1), (w, r_2) \in [1, -1, 2, -2]$  and they uniquely determine the other values  $(v, r)$  when  $r$  is one of these 12 roots. We find by the computation of all possibilities, and after having eliminated irrelevant possibilities (e.g.  $|(v, r)| > 3$  for some  $r$ ), that the contribution of these 12 roots is either  $-3$  or 0. The conclusion is that there is no hope that such a root  $x$  can make the value of the summation decrease. In order to have (10), we must have  $s = m/2$ .

The end of the argument is essentially the same: we have found a sublattice of  $L'$  isometric to  $\left(\frac{1}{\sqrt{3^{k-1}}}A_2'\right)^{m/2}$ , which proves that up to isometry  $L \subset (\sqrt{3^{k-1}}A_2)^{m/2}$ . Let  $M := \frac{1}{\sqrt{3^{k-1}}}L$ . The lattice  $M$  is a sublattice of

$A_2^{m/2}$  hence is even. Moreover,  $(3A_2')^{m/2} \subset M \subset (A_2)^{m/2}$  which means that  $M$  arises from a ternary code.

When  $k = 0$ , we want  $L = \frac{1}{\sqrt{3}}L_C$  to be unimodular, which is equivalent to  $C = C^\perp$ . When  $k > 0$ ,  $L$  has level  $3^k$  if and only if  $M = L_C$  has level 3, which is equivalent to  $C^\perp \subset C$ .

□

## REFERENCES

- [1] A. Andrianov: Quadratic forms and Hecke operators. Grundlehren der Mathematischen Wissenschaften, 286. Berlin etc.: Springer-Verlag. XII,(1987).
- [2] J.H. Conway, N.J.A. Sloane, Sphere packings, lattices and groups, Grundlehren der Mathematischen Wissenschaften, no. 290, Springer, New York Berlin Heidelberg, 1988.
- [3] W. Ebeling, Lattices and Codes, Vieweg, Braunschweig, 1994.
- [4] N. Elkies, A characterization of the  $\mathbb{Z}^n$  lattice, Math. Res. Lett. 2, No.3, 321-326 (1995).
- [5] N. Elkies, Lattices and codes with long shadows, Math. Res. Lett. 2, No.5, 643-651 (1995)
- [6] E. Freitag, Singular modular forms and theta relations, Lecture Notes in Mathematics. 1487. Berlin etc., Springer-Verlag. vi, 172 p. (1991).
- [7] J. Igusa, Theta functions, Grundlehren der Mathematischen Wissenschaften, 194. Berlin etc., Springer-Verlag. XII, (1972).
- [8] O. Imamoglu, W. Kohnen, Representations of integers as sums of an even number of squares, to appear in Math. Ann.
- [9] W. Kohnen, R. Salvati Manni, On the Theta Series Attached to  $D_m^+$ -Lattices, to appear in Int. Journal of Number Theory.
- [10] T. Miyake, Modular Forms, Springer-Verlag (1989).
- [11] J.-P. Serre, A course in arithmetic (English), Graduate Texts in Mathematics. 7. New York-Heidelberg-Berlin, Springer-Verlag. VIII, (1973).

CHRISTINE BACHOC, LABORATOIRE A2X, UNIVERSITÉ BORDEAUX I, 351, COURS DE LA LIBÉRATION, 33405 TALENCE FRANCE

*E-mail address:* bachoc@math.u-bordeaux1.fr

RICCARDO SALVATI MANNI, DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI ROMA, PIAZZALE ALDO MORO, 2, I-00185 ROMA, ITALY

*E-mail address:* salvati@mat.uniroma1.it