Arch. Math. 89 (2007), 143–151
© 2007 Birkhäuser Verlag Basel/Switzerland
0003/889X/020143-9, *published online* 2007-04-04
DOI 10.1007/s00013-006-1164-5

Archiv der Mathematik

A bound for certain s-extremal lattices and codes

Philippe Gaborit

Abstract. In this paper we introduce the notion of s-extremal lattice for unimodular Type I lattices. We give a bound on the existence of certain such s-extremal lattices: an s-extremal lattice of dimension n and minimal even norm μ must satisfy $n < 12\mu$. This result implies that such lattices are also extremal and that there are a finite number of them. We also give an equivalent bound for s-extremal self-dual codes: an s-extremal code with doubly-even minimum distance d and length n must satisfy $n < 6d$, moreover such codes are extremal.

Mathematics Subject Classification (2000). 20J05.

Keywords. Unimodular lattices, self-dual codes, modular forms, classification, shadow.

1. Introduction. The class of unimodular lattices has been studied for a long time and contains many interesting lattices. In particular it is possible to give a bound on the minimum norm of such lattices. If L is a unimodular lattice with theta series

$$\theta_L(\tau) := \sum_{x \in L} q^{(x \cdot x)}, \tag{1}$$

where $\tau \in \mathfrak{h}$, the upper half complex plane, and $q := e^{\pi i \tau}$; its theta series satisfies an invariance property under the transformation $\tau \to -1/\tau$. If the lattice is moreover even, then its theta series is invariant under the action of the full modular group $SL(2, \mathbb{Z})$, this result permits to show that the minimum norm μ of an even unimodular lattice satisfies:

$$\mu \leq 2[n/24] + 2, \tag{2}$$

where n is the dimension of the lattice. The first case where this bound is not known to be tight is $n = 72$.

In the case of odd unimodular lattices no satisfactory bound was known until the introduction of the shadow theory by Conway and Sloane in [4].

Let L be a unimodular lattice. The shadow S of L is $S := (L_0)^* \setminus L$, where L_0 denotes the even sublattice of L. If L is an odd lattice, its theta series has the following expression:

$$\theta_L(\tau) = \sum_{j=0}^{[n/8]} c_j \Delta_8(q)^j \theta_3(q)^{n-8j}, \tag{3}$$

and the theta series of the shadow S is

$$\theta_S(\tau) = \sum_{j=0}^{[n/8]} \frac{(-1)^j}{16^j} c_j \theta_4(q^2)^{8j} \theta_2(q)^{n-8j}, \tag{4}$$

where $q := e^{\pi i \tau}$, $\Delta_8(q) = q\prod_{m=1}^{\infty}(1-q^{2m-1})^8(1-q^{4m})^8$, and θ_2, θ_3, θ_4 are the usual Jacobi theta series (see [3, Chap. 4, § 4]).

This notion was used to prove new bounds for odd unimodular lattices, the most efficient is the bound by Rains and Sloane [16] which states that except for the short Leech lattice in dimension 23 all odd unimodular lattices also satisfy the bound (2) for even lattices.

Another point of view on the shadow was proposed by Elkies who studies in [6] the minimum norm of the shadow. If we denote, as usual, by μ the minimum norm of L and by σ, four times the minimum norm of its shadow, Elkies shows that $\sigma \leq n$ and that the only lattice with $\sigma = n$ is $\mathbb{Z}^n$. He also considers the case where $\sigma = n-8$ for which he gives the short list of such lattices from the classification of unimodular lattices up to dimension 24. The next cases $\sigma = n-16$ and $\sigma = n-24$ are first considered by Gaulter in [8] who gives two large upper bounds for the existence of such lattices. Then Nebe and Venkov consider in [13] more precisely the case $\sigma = n-16$ and $\mu \geq 3$ for which they give a tight upper bound of $n \leq 46$ for the existence of such lattice.

In this paper we propose to study simultaneously the parameters σ and μ as it was proposed for codes by Bachoc and the author in [1]. We show that $8\mu+\sigma \leq n+8$ except in the case $n = 23$ and $\mu = 3$ for which $\sigma = 15$. The lattices which satisfy equality in the bound are called s-extremal. We show that for even μ, s-extremal lattices exist only if $n < 12\mu$. We also give an equivalent bound for s-extremal codes: if an s-extremal code of length n has a minimum distance d divisible by four then $n < 6d$.

2. S-extremal lattices.

2.1. Definition of s-extremal lattices. We give in the following a theorem and a definition for s-extremal lattices.

Theorem 2.1. *Let L be a unimodular lattice, assumed not to be of Type II, of minimum norm μ, and let S be its shadow, of minimum norm σ. Then, $8\mu + \sigma \leq 8 + n$, unless $n = 23$ and $\mu = 3$, for which $\sigma = 15$ and the only possible lattice is the short Leech lattice O_{23}.*

Definition 2.2. *A lattice which parameters (μ, σ) satisfy equality in the previous bounds is said to be s-extremal.*

Remark: For an s-extremal lattice L the theta series θ_L and θ_S are uniquely determined.

Proof of Theorem 2.1**:** From (4), the norms in S are congruent to $\frac{n}{4}$ mod 2. Let us denote a_i the number of vectors of norm i in L and b_i the number of vectors of norm $\frac{i}{4}$ in S. Let us define σ' by $\sigma = n - 8\sigma'$. From (3) and (4), the conditions

$$\left\{\begin{array}{l} a_0 = 1 \\ a_i = 0 \text{ for } 1 \leq i \leq \mu - 1 \\ b_{n-8j} = 0 \text{ for } \sigma' + 1 \leq j \leq [n/8] \end{array}\right. \tag{5}$$

are linear and independent conditions on the $[n/8]+1$ coefficients c_i. Their number is $\mu + [n/8] - \sigma'$, which is greater or equal to $[n/8]+1$ if and only if $8\mu + \sigma \geq 8 + n$.

We now assume that the inequality $8\mu + \sigma \geq 8 + n$ holds. From the previous discussion, the theta series of L and S are uniquely determined. Let $t := 8 + n - 8\mu$. We have:

$$\left\{\begin{array}{l} \theta_L = 1 + a_\mu q^\mu + a_{\mu+1} q^{\mu+1} + \dots \\ \theta_S = b_t q^t + b_{t+8} q^{t+8} + \dots \end{array}\right. \tag{6}$$

where b_t is not assumed to be non-zero.

In the following we discuss the possibility that $b_t = 0$.

From (4), $b_t = \frac{(-1)^{\mu-1}}{16^{\mu-1}} c_{\mu-1}$ and $c_i = 0$ for all $i > \mu - 1$. Dividing (3) by θ_3^n one then gets:

$$\sum_{j=0}^{\mu-1} c_j \left(\frac{\Delta_8}{\theta_3^8}\right)^j = \frac{1}{\theta_3^n} + \frac{1}{\theta_3^n}\{a_\mu q^\mu + \cdots\} \tag{7}$$

Hence the coefficients $c_0, \cdots, c_{\mu-1}, -a_\mu$ are the coefficients of $\frac{1}{\theta_3^n}$ developed on $\left(\frac{\Delta_8}{\theta_3^8}\right)^j$. In the following in order to simplify the notation, we denote $m = \mu - 1$.

As in [16] the Bürman-Lagrange formula [17] allows us to calculate:

$$\begin{aligned} c_m &= \frac{1}{m!}\frac{\partial^{m-1}}{\partial q^{m-1}}\left(\frac{\partial}{\partial q}\left(\theta_3^{-n}\right)\left(\frac{q\theta_3^8}{\Delta_8}\right)^m\right)_{q=0} \\ &= \frac{1}{m!}\frac{\partial^{m-1}}{\partial q^{m-1}}\left(-n\frac{\theta_3'}{\theta_3^{n-8m+1}}\left(\frac{q}{\Delta_8}\right)^m\right)_{q=0} \\ &= \frac{-n}{m}\left\{\text{coeff. of } q^{m-1} \text{ in: } \frac{\theta_3'/\theta_3}{\theta_3^n(\frac{\Delta_8}{q\theta_3^8})^m}\right\} \end{aligned}$$

Following Rains and Sloane [16], we denote $g_1 = \theta_3$ and $g_2 = \Delta_8/\theta_3^8$, with $(q^{-1}g_2)^m = \prod_{j=1}^\infty(1+q^{2j-1})^{24m}$ and $g_1^n = \prod_{j=1}^\infty(1-q^{2j})^n(1+q^{2j-1})^{2n}$, so that:

$$c_m = \frac{-n}{m}\{\text{coeff. of } q^{m-1} \text{ in: } \frac{\theta_3'/\theta_3}{g_1^n(q^{-1}g_2)^m}\}$$

By considering the product form of θ_3 we remark that the q-expansion of the series θ_3'/θ_3 is an alternating series with all coefficients non null and positive for even powers of q. Moreover the series $1/(g_1^n(q^{-1}g_2)^m)$ is an alternating series if and only if $2n-24m>0$. Hence since the product of an alternating series with a series with only positive terms for even powers of q is still an alternating series, the sign of a_μ is related to $2n-24m$. Three cases occur:

If $2n-24m \geq 0$ the series $1/(g_1^n(q^{-1}g_2)^m)$ is either an alternating series or a series with only even powers and positive coefficients, hence since θ_3'/θ_3 is an alternating series and has only non null coefficients, we deduce that $c_{\mu-1} \neq 0$ (and therefore $b_t \neq 0$).

If $2n-24m \leq -4$ then one gets:

$$c_m = \frac{-n}{m}\left\{\text{coeff. of } q^{m-1} \text{ in: } \frac{\theta_3'\prod_{j=1}^\infty(1+q^{2j-1})^{-(2n-24m+2)}}{\prod_{m=1}^\infty(1-q^{2j})^{n+1}}\right\}$$

since $-(2n-24m+2) \geq 2$, $c_{\mu-1} \neq 0$.

If $2n-24m=-2$: from the bound of [16] this last possibility may only happen for $n = 24k+11, \mu = 2k+2$ or $n = 23, \mu = 3$. We then have:

$$c_m = \frac{-n}{m}\left\{\text{coeff. of } q^{m-1} \text{ in: } \frac{\theta_3'}{\prod_{m=1}^\infty(1-q^{2j})^{n+1}}\right\}$$

In the case where $n = 24k+11$ and $\mu = 2k+2$ since μ is even we deduce from the q-expansion of the series that $c_{\mu-1}$ is non null. The second case corresponds to the short Leech lattice for which $b_7 = 0$ but $b_{15} \neq 0$ (see [6]). This concludes the proof. □

2.2. A bound for certain s-extremal lattices. The following theorem gives a bound on the existence of s-extremal lattices in the case of even minimum norms. Note that as we will see in the next section for $\mu = 4$, this bound is tight.

Theorem 2.3. *Let L be an s-extremal lattice with parameters (μ, σ) of dimension n, if μ is even then $n < 12\mu$.*

Proof. The proof is similar to the proof of the previous theorem. From (7) we deduce that the coefficients $c_0, \cdots c_{\mu-1}, -a_\mu$ are the coefficients of $\frac{1}{\theta_3^n}$ developed on $\left(\frac{\Delta_8}{\theta_3^8}\right)^j$. The Bürman-Lagrange formula allows us then to calculate:

$$\begin{aligned}-a_\mu &= -\frac{n}{\mu}\left\{\text{coeff. of } q^{\mu-1} \text{ in: } \frac{\theta_3'/\theta_3}{\prod_{j=1}^\infty [(1-q^{2j})(1+q^{2j-1})]^{n-8\mu}[(1-q^{2j-1})(1-q^{4j})]^{8\mu}}\right\}\\ &= -\frac{n}{\mu}\left\{\text{coeff. of } q^{\mu-1} \text{ in: } \frac{\theta_3'/\theta_3}{\prod_{j=1}^\infty (1-q^{2j})^{n-8\mu}(1-q^{4j-2})^{8\mu}(1-q^{4j})^{8\mu}(1+q^{2j-1})^{2n-24\mu}}\right\}\end{aligned}$$

and eventually after simplification:

$$a_\mu = \frac{n}{\mu}\left\{\text{coeff. of } q^{\mu-1} \text{ in: } \frac{\theta_3'/\theta_3}{\prod_{j=1}^\infty (1-q^{2j})^n(1+q^{2j-1})^{2n-24\mu}}\right\}$$

Hence if $2n - 24\mu \geq 0$ the series $\frac{1}{(1+q^{2j-1})^{2n-24\mu}}$ are alternating series and therefore since θ_3'/θ_3 is an alternating series with non null coefficients, the term a_μ is non null and its sign is $(-1)^{\mu-1}$. This implies that s-extremal lattices for even μ and $n \geq 12\mu$ cannot exist since a_μ has to be positive or null. □

Corollary 2.4. *S-extremal lattices with even minimum norm are extremal and there are only finitely many such lattices.*

Proof. From the result by Rains and Sloane [16] the minimum norm of a Type I lattice of dimension n with even norm μ, satisfies: $\mu \leq 2[n/24] + 2$. The previous bound implies: $2[n/24] \leq n/12 < \mu \leq 2[n/24]+2$ and the extremality of s-extremal lattices with even norm. The finite number of such lattice is a consequence of Rains results of [15, Theorem 5.2]. □

Remark: The notion of s-extremal lattice and the previous bound have been generalized to strongly unimodular lattices by Nebe and Schindelar in [11].

2.3. Examples of s-extremal lattices.

• $\mu = 2$

Such lattices exist up to dimension 23, this case has been completely classified by Elkies in [6] from the classification of unimodular lattices up to dimension 24.

• $\mu = 3$

This case has been considered in [13], such lattices exist up to dimension 46. A questionmark in the table means that no lattice is known at present.

n	num	ref	n	num	ref
23	1	[13]	35	≥ 1	[13]
24	1	[13]	36	?	
25	0		37	?	
26	1	[13]	38	?	
27	2	[13]	39	?	
28	36	[13]	40	≥ 1	[1]
29	≥ 1	[13]	41	?	
30	≥ 1	[13]	42	?	
31	≥ 1	[13]	43	?	
32	≥ 1	[13]	44	0	[13]
33	≥ 1	[13]	45	0	[13]
34	≥ 1	[13]	46	1	[13]

- $\mu = 4$

In that case, such lattices exist up to dimension 47. We list known lattices for $\mu = 4$:

n	32	36	37	38	39	40	41	42	43	44	45	46	47
num	5	≥ 2	?	≥ 1	≥ 1	≥ 1	?	≥ 1	?	?	?	≥ 1	≥ 1
ref	[5]	[12],[7]		[7]	[9]	[7]		[12],[7]				[10]	[10]

- $\mu = 5$

In that case, it is not known up to which dimension such lattices do exist. The only known lattice is for dimension 54 in [7].

- $\mu \geq 6$

For $\mu = 6$, such lattices may only exist for dimensions 56 to 71 ([16, 12, 7]). No s-extremal lattice is known for $\mu \geq 6$.

3. S-extremal codes. We now give for s-extremal codes a bound equivalent to the bound of Theorem 2.3. Let C be a self-dual binary code, which is assumed not to be doubly-even and let S be its shadow defined as $S := {C_0}^{\perp} \setminus C$, for C_0 the doubly-even subcode of C. We denote W_C and W_S the weight enumerators of C and S. From [4], there exists $c_0, \ldots, c_{[n/8]} \in \mathbb{R}$ such that:

$$\begin{cases} W_C(x,y) & = \sum_{i=0}^{[n/8]} c_i (x^2+y^2)^{\frac{n}{2}-4i} \{x^2y^2(x^2-y^2)^2\}^i \\ W_S(x,y) & = \sum_{i=0}^{[n/8]} c_i (-1)^i 2^{\frac{n}{2}-6i} (xy)^{\frac{n}{2}-4i} (x^4-y^4)^{2i} \end{cases} \tag{8}$$

We denote d the minimum weight of C and s the minimum weight of its shadow. The following theorem and definition are from [1]:

Theorem 3.1. *Let C be a self-dual binary code, assumed not to be doubly-even, of minimum weight d, and let S be its shadow, of minimum weight s. Then, $2d + s \leq 4 + \frac{n}{2}$, unless $n \equiv 22 \mod 24$ and $d = 4[n/24] + 6$, in which case $2d + s = 8 + \frac{n}{2}$.*

Definition 3.2. *A code which parameters (d, s) satisfy equality in the previous bounds is said to be s-extremal.*

Remark: The polynomials W_C and W_S of an s-extremal code are uniquely determined.

The following theorem gives a bound on the existence of such s-extremal codes. Note that as for lattices for $d = 8$, this bound is tight in the sense that such codes exist for $n = 44$, and $n = 46$ corresponds to the special case of a $[46, 23, 10]$ code with $s = 11$.

Theorem 3.3. *Let C be an s-extremal code with parameters (s, d) of length n, if $d \equiv 0 \pmod 4$ then $n < 6d$.*

Proof. Let C be an s-extremal codes with parameters (s, d) with $d \equiv 0 \pmod 4$ then one may assume that the equality $2d + s = 4 + \frac{n}{2}$ holds. The weight enumerators of C and S are uniquely determined. Bürman-Lagrange formula allows us to calculate the coefficients of these polynomials. Let $t := 4 + \frac{n}{2} - 2d$. We have:

$$\begin{cases} W_C(x, y) = 1 + a_d x^{n-d} y^d + a_{d+2} x^{n-d-2} y^{d+2} + \dots \\ W_S(x, y) = b_t x^{n-t} y^t + b_{t+4} x^{n-t-4} y^{t+4} + \dots \end{cases} \tag{9}$$

We now prove that if $d \equiv 0 \pmod 4$ and $n \geq 6d$ then then $a_d < 0$, which proves the theorem since all the coefficients have to be greater or equal to zero.

We have in (8) $c_i = 0$ for all $i > \frac{d}{2} - 1$. Setting $x = 1$ and dividing by $(1 + y^2)^{\frac{n}{2}}$ the first equation of (8) leads to:

$$\sum_{i=0}^{\frac{d}{2}-1} c_i \left\{ \frac{y(1 - y^2)}{(1 + y^2)^2} \right\}^{2i} = \frac{1}{(1 + y^2)^{\frac{n}{2}}} + \frac{1}{(1 + y^2)^{\frac{n}{2}}} \{a_d y^d + \dots\}$$

Let $g(y) := \frac{y(1-y^2)}{(1+y^2)^2}$. From this last expression, we see that $c_0, c_1, \dots, c_{\frac{d}{2}-1}, -a_d$ are the first coefficients of the development of $\frac{1}{(1+y^2)^{\frac{n}{2}}}$ as a series in $g(y)$. From the Bürman-Lagrange formula, we obtain:

$$-a_d = \frac{1}{d!} \frac{\partial^{d-1}}{\partial y^{d-1}} \left(\frac{\partial}{\partial y} \left(\frac{1}{(1 + y^2)^{\frac{n}{2}}} \right) \left(\frac{(1 + y^2)^2}{1 - y^2} \right)^d \right)_{y=0}$$

which, after simplification, becomes:

$$a_d = \frac{n}{d} \left\{ \text{coeff. of } y^{d-2} \text{ in: } \frac{1}{(1 + y^2)^{\frac{n}{2}-2d+1} (1 - y^2)^d} \right\}.$$

Let us write $n = 6d + 2\alpha$, with $\alpha \geq 0$ then the previous formula becomes:

$$a_d = \frac{n}{d}\left\{\text{coeff. of } y^{d-2} \text{ in: } \frac{1}{(1+y^2)^{1+\alpha}(1-y^4)^d}\right\},$$

and, finally, leads to :

$$\begin{aligned} a_d &= \frac{n}{d} \sum_{\substack{j,k\in\mathbb{N}\\ j+2k=\frac{d}{2}-1}} (-1)^j \binom{\alpha+j}{j}\binom{d+k+1}{k} \\ &= \frac{n}{d}(-1)^{\frac{d}{2}-1} \sum_{\substack{j,k\in\mathbb{N}\\ j+2k=\frac{d}{2}-1}} \binom{\alpha+j}{j}\binom{d+k+1}{k} \end{aligned}$$

which shows that a_d is negative for $d \equiv 0 \pmod 4$. □

Corollary 3.4. *All s-extremal codes with doubly-even minimum weight are extremal.*

Proof. From the extension by Rains [14] of the bound on Type II codes to Type I codes and from the previous bounds one gets: $4[n/24] \leq n/6 < d \leq 4[n/24] + 4$ and the result follows. □

Acknowledgement. We thank C. Bachoc and G. Nebe for helpful comments. All the computations were done with the MAGMA system [2].

References

[1] C. Bachoc and P. Gaborit, Designs and self-dual codes with long shadows. J. Combin. Theory Ser. A, **105**(1), 15–34 (2004).

[2] W. Bosma and J. Cannon, Handbook of Magma Functions. Sydney, 1995.

[3] J. Conway and N. J. A. Sloane, “Sphere packing mattices and groups”. (Third Edition) Springer-Verlag, New-York, 1988.

[4] J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes. IEEE Trans. Inf. Th., **36**, 1319–1333 (1990).

[5] J. H. Conway and N. J. A. Sloane, A Note on Optimal Unimodular Lattices. J. Number Theory, **72**, 357–362 (1998).

[6] N. Elkies, Lattices and codes with long shadows. Math. Res. Lett. **2**(5), 643–651 (1995).

[7] P. Gaborit, Construction of new unimodular lattices. Eur. J. Comb. **25**(4), 549–564 (2004).

[8] M. Gaulter, Lattices without short characteristic vectors. Math. Res. Lett. **5**(3), 353–362 (1998).

[9] T. A. Gulliver and M. Harada, An optimal unimodular lattice in dimension 39. J. Combin. Theory Ser. A **88**(1) 158–161 (1999).

[10] M. HARADA, Extremal odd unimodular lattices in dimensions 44, 46 and 47. Hokkaido Math. J. **32**(1) 153–159 (2003).

[11] G. NEBE AND K. SCHINDELAR, S-extremal strongly modular lattices. Preprint.

[12] G. NEBE AND N. J. A. SLOANE, A catalogue of lattices. http://www.research.att.com/~njas/lattices

[13] G. NEBE AND B. VENKOV, Unimodular lattices with long shadow. J. Number Theory, **99**(2), 307–317 (2003).

[14] E. M. RAINS, Shadow bounds for self-dual codes. IEEE Trans. Inform. Theory, **44**, 134–139 (2003).

[15] E. M. RAINS, New asymptotic bounds for self-dual codes and lattices. IEEE Trans. Inf. Th., **49**(5), 1261–1274 (2003).

[16] E. M. RAINS AND N. J. A. SLOANE, Self-dual codes: In Handbook of Coding Theory, ed. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 1998, 177–294.

[17] E. T. WHITTAKER AND G. N. WATSON, A course of Modern Analysis. 4th edition. New-York, Cambridge University Press, 1963.

PHILIPPE GABORIT, XLIM, Université de Limoges, 123, av. A. Thomas, 87000 Limoges, France
e-mail: gaborit@unilim.fr

Received: 25 July 2006