Journal of Number Theory **72**, 357–362 (1998)
Article No. NT982257

A Note on Optimal Unimodular Lattices

J. H. Conway

Department of Mathematics, Princeton University, Princeton, New Jersey 08544

and

N. J. A. Sloane

Information Sciences Research, AT&T Labs-Research, Florham Park, New Jersey 07932-0971

Communicated by M. Pohst

Received February 10, 1998

The highest possible minimal norm of a unimodular lattice is determined in dimensions $n \leqslant 33$. There are precisely five odd 32-dimensional lattices with the highest possible minimal norm (compared with more than 8.10^{20} in dimension 33). Unimodular lattices with no roots exist if and only if $n \geqslant 23$, $n \neq 25$.

1. INTRODUCTION

The results stated in the abstract were announced in 1989 [7]. For their proof we define the *shadow* S (cf. [7, 8]) of an integral lattice Λ as follows. If Λ is odd, $S = (\Lambda_0)^* \backslash \Lambda^*$, where the subscript 0 denotes "even sublattice" and $*$ denotes "dual"; if Λ is even, $S = \Lambda$. It is immediate that the theta series Θ_S of the shadow of an n-dimensional odd lattice is related to theta series Θ_Λ of the lattice by

$$\Theta_S(z) = \sqrt{\det \Lambda} \left(\frac{\eta}{\sqrt{z}}\right)^n \Theta_\Lambda\left(1 - \frac{1}{z}\right), \tag{1}$$

where $\eta = e^{\pi i/4}$.

If Λ is an odd unimodular lattice then we can write

$$\Theta_\Lambda(z) = \sum_{j=0}^{[n/8]} a_j \Delta_8(q)^j \theta_3(q)^{n-8j}, \tag{2}$$

0022-314X/98 $25.00

where $q = e^{\pi i z}$,

$$\Delta_8(q) = q \prod_{m=1}^{\infty} (1-q^{2m-1})^8 (1-q^{4m})^8,$$

and θ_2, θ_3, θ_4 are the usual Jacobi theta series [6, p. 102]. From (1) and (2) we have

$$\Theta_S(z) = \sum_{j=0}^{[n/8]} \frac{(-1)^j}{16^j} a_j \theta_4(q^2)^{8j} \theta_2(q)^{n-8j} = \sum \beta_n q^n \qquad \text{(say)}. \tag{3}$$

2. BOUNDS

Suppose Λ is an odd unimodular lattice with the highest possible minimal norm μ_n. Then $a_0, ..., a_{\mu_n - 1}$ are determined by (2). Most of the bounds in Table I now follow from the following conditions: Θ_Λ and Θ_S must have nonnegative integer coefficients; $\Theta_\Lambda \equiv \Theta_S \equiv 1 \pmod 2$; there is at most one nonzero β_r for $r < (\mu_n + 2)/2$; $\beta_r = 0$ for $r < \mu_n/4$; and $\beta_r \leqslant 2$ for $r < \mu_n/2$. (The last three conditions follow from the fact if the four cosets of Λ_0 in Λ_0^* are $\Lambda_0^{(0)}$, $\Lambda_0^{(1)}$, $\Lambda_0^{(2)}$, $\Lambda_0^{(3)}$, with $\Lambda_0 = \Lambda_0^{(0)}$, $\Lambda = \Lambda_0^{(0)} \cup \Lambda_0^{(2)}$, $S = \Lambda_0^{(1)} \cup \Lambda_0^{(3)}$, then $u, v \in S$ implies $u \pm v \in \Lambda$.)

We give two examples. For dimension $n = 9$, if minimal norm 2 were possible, (2) would imply $a_0 = 1$, $a_1 = -18$, hence $\Theta_\Lambda = 1 + 252q^2 + \cdots$, $\Theta_S = (9/4)\, q^{1/4} + \cdots$ Since the coefficients of Θ_S are not integers, we conclude that $\mu_9 \leqslant 1$.

For dimension $n = 33$, if minimal norm 4 were possible, (2) would imply $a_0 = 1$, $a_1 = -66$, $a_2 = 660$, $a_3 = -880$, hence $\Theta_\Lambda = 1 + (70290 + a_4)\, q^4 + \cdots$, $\Theta_S = (a_4/32768)\, q^{1/4} + (110 - 63a_4/32768)\, q^{9/4} + \cdots$ From the initial term of Θ_S we see that $a_4 = 0$ or 2^{16}, but if $a_4 = 2^{16}$ the second term of Θ_S is negative; so $a_4 = 0$ and $\Theta_S = 110q^{9/4} + \cdots$

The following additional argument is needed to eliminate this case (and also for $n = 13$). At least one of $\Lambda_0^{(1)}$ and $\Lambda_0^{(3)}$ must contain 55 vectors of norm 9/4. Suppose $u, v \in \Lambda_0^{(1)}$ with $u \cdot u = v \cdot v = 9/4$, $u \neq \pm v$. Then $v \cdot v \in \{\pm 1/4, \pm 3/4\}$. But since $u \pm v \in \Lambda$, $u - v \in \Lambda_0$, the only possibility is $u \cdot v = 1/4$. The inner product matrix of these 55 vectors is therefore $8I + J/4$, where J is an all-1's matrix, which has rank 55, impossible in a 33-dimensional space. Therefore $\mu_{33} \leqslant 3$.

Table I gives μ_n for $n \leqslant 40$ (for $34 \leqslant n \leqslant 39$ the value is either 3 or 4). All the upper bounds for $8 \leqslant n \leqslant 40$, $n \neq 25$, follow from the above arguments. In dimension 25 they give only $\mu_{25} \leqslant 3$. However, Borcherds has enumerated all 25-dimensional unimodular lattices, showing that $\mu_{25} = 2$ ([2]; the list is included in [14]).

TABLE I

Highest Minimal Norm μ_n of an n-Dimensional Unimodular Lattice

n	1	2	3	4	5	6	7	8
μ_n	1	1	1	1	1	1	1	2
n	9	10	11	12	13	14	15	16
μ_n	1	1	1	2	1	2	2	2
n	17	18	19	20	21	22	23	24
μ_n	2	2	2	2	2	2	3	4
n	25	26	27	28	29	30	31	32
μ_n	2	3	3	3	3	3	3	4
n	33	34	35	36	37	38	39	40
μ_n	3	3–4	3–4	4	3–4	3–4	3–4	4

Lattices achieving the bounds are well known for $n \leqslant 24$, 32, and 40 [6, Chap. 16]. Borcherds showed that there is a unique unimodular lattice in dimension 26 with minimal norm 3, and least one in dimension 27 ([2]; see also [6, 3rd ed.; 14]). Bacher and Venkov [1] showed that there are exactly three such lattices in dimension 27 and exactly 38 in dimension 28.

In dimension 30 a unimodular lattice L_{30} of minimal norm 3 may be obtained by gluing together two copies of $\sqrt{2}\,L$, where L is the unimodular lattice A_{15}^{+}. A 29-dimensional example can be obtained by taking an appropriate vector $v_4 \in L_{30}$ with $v_4 \cdot v_4 = 4$, and projecting $\{u \in L_{30}: u \cdot v_4 \equiv 0 \pmod 2\}$ onto $v_4^{\perp}$. Examples in dimensions 32 and 31 may be similarly obtained from the lattice $\sqrt{2}\,D_{16}^{+}$.

The Conway–Thompson theorem [10, p. 46] shows that unimodular lattices with minimal norm $\geqslant 3$ exist in all dimensions $n \geqslant 37$, and we have found explicit examples in dimensions 33–36 [14]. A 36-dimensional unimodular lattice with minimal norm 4 was recently constructed by G. Nebe (personal communication). This establishes all the lower bounds in the table, as well as the third result mentioned in the abstract.

The first gap in the table is at dimension 34, where the theta series of a putative lattice with minimal norm 4 is

$$1 + 60180q^4 + 2075904q^5 + \cdots;$$

its shadow would have theta series

$$204q^{5/2} + 758200q^{9/2} + \cdots.$$

We do not know if such a lattice exists.

In [7] it was also announced that (2) and (3) imply that for all sufficiently large n, $\mu_n \leqslant [(n+6)/10]$. In fact a more delicate analysis yields $\mu_n \leqslant 2[n/24]+2$, unless $n=23$ when $\mu_{23} \leqslant 3$—see [11].

3. DIMENSION 32

Suppose Λ is an odd unimodular lattice in dimension 32 having minimal norm 4. The argument of Section 2 shows that

$$\Theta_\Lambda(z) = 1 + 81344q^4 + \cdots,$$
$$\Theta_S(z) = 64q^2 + 144896q^4 + \cdots.$$

At least 32 vectors of S must be in (say) the coset $\Lambda_0^{(1)}$, but since their sum and difference is in Λ, such vectors must be orthogonal, and so both $\Lambda_0^{(1)}$ and $\Lambda_0^{(3)}$ must contain exactly 32. Suppose $u_1 = c(2, 0, ..., 0), ..., u_{32} = c(0, ..., 0, 2)$, $c = 1/\sqrt{8}$, are a set of 32 such vectors. Then Λ contains the sublattice spanned by all vectors of the form $c(\pm 4, \pm 4, 0^{30})$.

We may now apply the argument of [6, Chap. 12, p. 333] to construct a binary code $\mathscr{C}$ of length 32, which must be doubly even and self-dual. There are precisely five such codes [4, 5], so there are therefore five possibilities for Λ. If $\mathscr{C}$ is one of the five codes, the corresponding lattice Λ is constructed from it in the same way that the Leech lattice is constructed from the Golay code: Λ is spanned by the vectors $c(-3, 1^{31})$, $c(2u)$ for $u \in \mathscr{C}$, and $c(\pm 4^2, 0^{30})$. $\mathscr{C}$ has 620 minimal vectors, of weight 8, so Λ contains $2^7 \cdot 620 + 2^2\binom{32}{2} = 81344$ minimal vectors, of norm 4.

Finally, we discuss odd unimodular 33-dimensional lattices. The total mass $M = \sum |\mathrm{Aut}\,\Lambda|^{-1}$ of this genus is $1.407\cdots \times 10^{21}$ [6, Chap. 16]. Let M_{2k} be the mass of the lattices with exactly $2k$ vectors of norm 1 or 2, $k = 0, 1, ...$, so that $M = M_0 + M_2 + M_4 + M_6 + \cdots$. Although for even n the average theta series

$$\frac{1}{M}\sum_\Lambda \frac{\Theta_\Lambda(q)}{|\mathrm{Aut}\,\Lambda|} \tag{4}$$

of the genus of odd unimodular lattices is given in [3, p. 386; 9, Chap. 12; 12, Sect. 7.4], no analogous formula seems to be known for odd n. However, Eric Rains has pointed out that the results of [13, p. 70] imply that for both even and odd $n > 4$ the average theta series is given by

$$\theta_3(z)^n \sum_{j=0}^{[n/4]} c_j(g_2(z)^j + h_2(z)^j), \tag{5}$$

where

$$g_2(z) = 16q \prod_{m=1}^{\infty} \left(\frac{1+q^{2m}}{1+q^{2m-1}} \right)^8,$$

$$h_2(z) = \prod_{m=1}^{\infty} \left(\frac{1-q^{2m-1}}{1+q^{2m-1}} \right)^8,$$

and the c_j are chosen so that the coefficients α_i in the q-expansion of

$$\theta_3(z)^n \sum_{j=0}^{[n/4]} c_j g_2(z)^j$$

satisfy $\alpha_{4i} = 2^{n-2}\alpha_i$ for all i, and the coefficient of q^0 in (5) is 1.

For $n = 33$ we find that (4) is

$$1 + \frac{15535133760578}{505245773078238529} q + \frac{719890853572979520}{505245773078238529} q^2 + \cdots,$$

$$= 1 + 0.0000307...q + 1.4248...q^2 + \cdots.$$

Therefore the total number of vectors of norms 1 and 2 in all lattices in the genus is $1.425\cdots \times M = 2M_2 + 4M_4 + 6M_6 + \cdots \geqslant 2(M - M_0)$. Hence $M_0 \geqslant 0.404\cdots \times 10^{21}$, and so the number of lattices with minimal norm 3 (the highest possible value) is $\geqslant 8 \times 10^{20}$.

ACKNOWLEDGMENT

We thank Eric Rains for helpful comments.

REFERENCES

1. R. Bacher and B. B. Venkov, Réseaux entiers unimodulaires sans racines en dimension 27 et 28, preprint No. 332 Inst. Fourier, Grenoble, 1996.
2. R. E. Borcherds, "The Leech Lattice and Other Lattices," Ph.D. Dissertation, Univ. of Cambridge, 1984.
3. J. W. S. Cassels, "Rational Quadratic Forms," Academic Press, New York, 1978.
4. J. H. Conway and V. Pless, On the enumeration of self-dual codes, *J. Combin. Theory Ser. A* **28** (1980), 26–53.
5. J. H. Conway, V. Pless, and N. J. A. Sloane, Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16, *IEEE Trans. Inform. Theory* **25** (1979), 312–322.
6. J. H. Conway and N. J. A. Sloane, "Sphere Packings, Lattices and groups," 3rd ed., Springer-Verlag, New York, 1998, in press.

7. J. H. Conway and N. J. A. Sloane, A new upper bound for the minimum of an integral lattice of determinant one, *Bull. Amer. Math. Soc.* **23** (1990), 383–387; Erratum, **24** (1991), 479.
8. J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.
9. E. Grosswald, "Representations of Integers as Sums of Squares," Springer-Verlag, New York, 1985.
10. J. Milnor and D. Husemoller, "Symmetric Bilinear Forms," Springer-Verlag, New York, 1973.
11. E M. Rains and N. J. A. Sloane, The shadow theory of modular and unimodular lattices, *J. Number Theory*, in press.
12. R. A. Rankin, "Modular Forms and Functions," Cambridge Univ. Press, Cambridge, UK, 1977.
13. G. Shimura, Modular forms of half integral weight, *in* "Modular Functions of One Variable" (W. Kuyk, Ed.), Lecture Notes in Math., Vol. 320, pp. 57–74, Springer-Verlag, New York, 1973.
14. N. J. A. Sloane and G. Nebe, "A Catalogue of Lattices," published electronically at http://www.research.att.com/~njas/lattices/.