A NEW UPPER BOUND FOR THE MINIMUM OF AN INTEGRAL LATTICE OF DETERMINANT 1

J. H. CONWAY AND N. J. A. SLOANE

ABSTRACT. Let \( \Lambda \) be an \( n \)-dimensional integral lattice of determinant 1. We show that, for all sufficiently large \( n \), the minimal nonzero squared length in \( \Lambda \) does not exceed \( \left\lceil (n + 6)/10 \right\rceil \). This bound is a consequence of some new conditions on the theta series of these lattices; these conditions also enable us to find the greatest possible minimal squared length in all dimensions \( n \leq 33 \). In particular, we settle the “no-roots” problem: There is a determinant 1 lattice containing no vectors of squared length 1 or 2 precisely when \( n \geq 23 \), \( n \neq 25 \). There are also analogues of all these results for codes.

1. INTRODUCTION

The problem of classifying \( n \)-dimensional integral lattices of determinant 1 has been studied by Magnus, Mordell, Ko, Witt, Kneser, Niemeier and others [4, Chapters 1, 16, and 17]. The lattices \( \Lambda \) of this type for which the minimal norm

\[
\min\{u \cdot u : u \in \Lambda, \ u \neq 0\}
\]

takes its highest possible value \( \mu \) are of the greatest interest. It was shown in [7] that for even lattices (those in which \( u \cdot u \) is always even), the minimal norm is at most \( 2[n/24] + 2 \), while for odd lattices (those in which \( u \cdot u \) is sometimes odd) the corresponding bound is \( [n/8] + 1 \) [7, 11]. These are the bounds one would expect from the dimension of the space of available theta series. In fact, it is known that \( \mu \) differs from these bounds by an amount that tends to infinity with \( n \), so that equality can hold for only finitely many lattices [7]. In the odd case, the bound holds with equality for precisely 12 lattices, the highest dimension of which is 23 [2, 4, Chapter 19]. As to lower bounds, it is known that both even and odd lattices exist in which the minimal norm is asymptotically at least \( n/2\pi e \) [4, Chapter 7; 10].

Received by the editors October 3, 1989 and, in revised form, April 10, 1990. 1980 Mathematics Subject Classification (1985 Revision). Primary 11E25, 11E41, 11H31, 52A45, 94B05.

©1990 American Mathematical Society 0273-0979/90 $1.00 + $.25 per page

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The purpose of this paper is to announce the following improved bound.

**Theorem 1.** For all sufficiently large \( n \), we have \( \mu \leq \frac{(n + 6)}{10} \).

(An upper bound asymptotic to \( n/9.793 \ldots \) is implied by the Kabatiansky–Levenshtein sphere-packing bound [4, Chapter 9; 5].) We believe that for odd lattices the bound of Theorem 1 in fact holds for all dimensions \( n \) except 1, 2, 3, 12, 23 and 32, where special circumstances permit \( \mu \) to exceed the bound by 1.

In particular cases we can often obtain additional information. For dimensions 1 through 33, we have been able to find the exact value of \( \mu \).

**Theorem 2.** \( \mu = 1 \) for \( n = 1 \) to 7, 9 to 11 and 13; \( \mu = 2 \) for \( n = 8, 12, 14 \) to 22 and 25; \( \mu = 3 \) for \( n = 23, 26 \) to 31 and 33; and \( \mu = 4 \) for \( n = 24 \) and 32.

We also have information about the optimal lattices (those whose minimal norm equals \( \mu \)). For example, there are precisely five odd optimal lattices in 32 dimensions, while there are more than \( 8 \times 10^{20} \) optimal lattices (which are necessarily odd) in 33 dimensions!

Vectors of norms 1 or 2 in a lattice of determinant 1 are called *roots* (the reflections in such vectors are symmetries of the lattice).

**Theorem 3.** Determinant 1 lattices with no roots exist precisely for \( n \geq 23, n \neq 25 \).

Most of these theorems have analogues for binary self-dual codes.

**Theorem 4.** For all \( n \geq 50 \), the minimal distance \( d \) of a self-dual code of length \( n \) satisfies \( d \leq 2 \left( \frac{(n + 6)}{10} \right) \).

We can show that, for self-dual codes in which the weights are not all multiples of 4, the bound of Theorem 4 holds for all lengths \( n \) except 2, 12, 22 and 32. Here, however, the bound of McEliece et al. [6, Chapter 17; 9] is asymptotically stronger, yielding \( d \leq 0.182 \ n + o(n) \).

**Theorem 5.** The greatest minimal distance of any self-dual code of length \( n \) is 2 for \( n = 2, 4, 6 \) and 10; 4 for \( n = 8 \) and 12 to 20; 6 for \( n = 22, 26, 28, 30 \) and 34; 8 for \( n = 24, 32 \) and 36 to 44; 10 for \( n = 46, 50, 52, 54 \) and 58; and 12 for \( n = 48, 56 \) and 60.
**Theorem 6.** Self-dual codes with minimal distance

\[ d \geq 6 \] exist precisely for \( n \geq 22 \),

\[ d \geq 8 \] exist precisely for \( n = 24 \) and \( n \geq 32 \), and \( n \geq 36 \), and

\[ d \geq 10 \] exist precisely for \( n \geq 46 \).

There are precisely three self-dual codes with \( n = 32, d = 8 \) such that not all weights are multiples of 4. (In the case where the weights are multiples of 4, it was already known that there are precisely 5 codes [3].)

**2. Remarks on the proofs**

Theorem 2 follows from a detailed study of the theta series and by explicit constructions in dimensions \( n \leq 32 \), while Theorem 3 also uses an analytic argument (involving the average theta series) for \( n \geq 33 \). We now sketch the proof of Theorem 1. Complete details will appear elsewhere.

Let \( \Lambda \) be an \( n \)-dimensional integral lattice of determinant 1. If \( \Lambda \) is even, the result follows from [7], so we assume \( \Lambda \) is odd. The theta series \( \Theta_\Lambda(q) = \sum_{u \in \Lambda} q^{\langle u \rangle} \) can be written as

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

where

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

[4, page 187]. \((\theta_2, \theta_3 \text{ and } \theta_4 \) are the usual Jacobi theta series [4, page 102; 12, page 464]. If \( \Lambda \) has minimal norm at least \( \sigma \), then \( a_0, \ldots, a_{\sigma-1} \) are determined and can be found from the Bürmann–Lagrange theorem [7; 8; 12, page 128]. We obtain

\[
a_j = -\frac{n}{j!} \left[ \frac{d^{j-1}}{dq^{j-1}} \{ \theta_3(q)^{8j-n-1} h(q) \} \right]_{q=0},
\]

where \( h(q) = q \Delta_8(q)^{-1} \) (cf. [7, Equation (6); 8, page 191]).

Suppose, seeking a contradiction, that \( \sigma = [(n+6)/10] + 1 \).

Let \( n = 10k + \delta, -6 \leq \delta \leq 3 \), so \( \sigma = k + 1 \). We use (1) and the saddle point method (as in Lemma 1 of [7]) to obtain

\[
ak \sim -\frac{c_1}{\sqrt{k}} c_2^k, \quad \text{as } k \to \infty,
\]

where \( c_2 = 14.91050 \) and \( c_1 \) is a positive number (depending on \( \delta \)).
We now obtain a second estimate for \( a_k \), incompatible with (2). Let \( \Lambda_0 \) denote the even sublattice of \( \Lambda \), of index 2. The dual lattice \( \Lambda_0^* \) is the union of four cosets of \( \Lambda_0 \), say \( \Lambda_0^* = \bigcup_{i=0}^{3} \Lambda_0^{(i)} \), with \( \Lambda_0 = \Lambda_0^{(0)} \), \( \Lambda = \Lambda_0^{(0)} \cup \Lambda_0^{(2)} \). We set \( \Omega = \Lambda_0^{(1)} \cup \Lambda_0^{(3)} \). The theta series of \( \Omega \) is given by [4, page 440, Equations (5) and (6)]:

\[
\Theta_{\Omega}(q) = \sum_{j=0}^{[n/8]} \frac{(-1)^j}{16^j} a_j \theta_4(q^2)^{8j} \theta_2(q)^{n-8j} = \sum \beta_j q^r \quad \text{(say)}.
\]

Note that the values of \( r \) in (3) are rational numbers congruent to \( n/4 \pmod{2} \).

For two distinct pairs \( \pm u, \pm v \in \Omega \) we cannot have \( N(u) + N(v) < \sigma \), since \( u \pm v \in \Lambda \). This principle implies that there is at most one nonzero \( \beta_r \) for \( r < (\sigma + 2)/2 \), that \( \beta_r = 0 \) for \( r < \sigma/4 \), \( \beta_r = 0 \) or 2 for \( r < \sigma/2 \) and (by consideration of inner products) that \( \beta_r \leq 2n \) for \( r < (\sigma + 1)/2 \), \( n \neq 3 \). (R. E. Borcherds [1] used similar ideas in studying lattices in dimensions 25 to 27.)

Thus the values of \( \beta_r \) for \( r < (\sigma + 1)/2 \) are small. A second application of the Bürmann–Lagrange theorem now enables us to determine \( a_{[n/8]}, a_{[n/8]-1}, \ldots, a_k \). Again applying Lemma 1 of [7], we obtain an upper bound for \( a_k \) which is asymptotic to

\[
a_k \sim \frac{c_3}{c_4} k^k \quad \text{as} \quad k \to \infty,
\]

where \( c_3 \) is positive and independent of \( k \), and \( c_4 = 7.10716 \ldots \). Comparison of (2) and (4) yields the desired contradiction.

REFERENCES

1. R. E. Borcherds, *The Leech lattice and other lattices*, Ph.D. dissertation, Univ. of Cambridge, 1984.
2. J. H. Conway, A. M. Odlyzko, and N. J. A. Sloane, *Extremal self-dual lattices exist only in dimensions 1 to 8, 12, 14, 15, 23 and 24*, Mathematika 25 (1978), 36–43.
3. J. H. Conway and V. Pless, *On the enumeration of self-dual codes*, J. Combin. Theory Ser. A 28 (1980), 26–53.
4. J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Springer-Verlag, New York, 1988.
5. G. A. Kabatiansky and V. I. Levenshtein, *Bounds for packings on a sphere and in space*, (in Russian), Problemy Peredachi Informatsii 14 (1) (1978), 3–25.
6. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.
7. C. L. Mallows, A. M. Odlyzko, and N. J. A. Sloane, *Upper bounds for modular forms, lattices, and codes*, J. Algebra 36 (1975), 68–76.
8. C. L. Mallows and N. J. A. Sloane, *An upper bound for self-dual codes*, Inform. and Control 22 (1973), 188–200.

9. R. J. McEliece, E. R. Rodemich, H. C. Rumsey, Jr., and L. R. Welch, *New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities*, IEEE Trans. Inform. Theory 23 (1977), 157–166.

10. J. Milnor and D. Husemoller, *Symmetric bilinear forms*, Springer-Verlag, New York, 1973.

11. C. L. Siegel, *Berechnung von Zetafunktionen an ganzzahligen Stellen*, Göttingen Nach. 10 (1969), 87–102. (Gesam. Abh. vol. IV, pp. 82–97.)

12. E. T. Whittaker and G. N. Watson, *A course of modern analysis*, 4th ed., Cambridge Univ. Press, 1963.

Mathematics Department, Princeton University, Princeton, New Jersey 08540

Mathematical Sciences Research Center, AT&T Bell Laboratories, Murray Hill, New Jersey 07974
