INFORMATION AND CONTROL 46, 270–272 (1980)

A Note on the Leech Lattice as a Code for the Gaussian Channel

N. J. A. SLOANE

Bell Laboratories, Murray Hill, New Jersey 07974

The Leech lattice Λ is a very dense packing of spheres in 24-dimensional Euclidean space, discovered by Leech (1967). Its automorphism group was determined by Conway (1969), and its usefulness as a source of codes for the Gaussian channel was studied by Blake (1971). The present note contains some comments on and corrections to the latter paper.

Both Leech (1967) and Conway (1969) use essentially the same definition of Λ. This can be stated succinctly using the binary Golay code g_{24} of length 24 and minimum Hamming distance 8: Λ consists of those points in real 24-dimensional space $\mathbb{R}^{24}$ with coordinates

$$\mathbf{0} + 2\mathbf{c} + 4\mathbf{x}$$

or

$$\mathbf{1} + 2\mathbf{c} + 4\mathbf{y},$$

where $\mathbf{0} = (00 \ldots 0)$, $\mathbf{1} = (11 \ldots 1)$, $\mathbf{c} \in g_{24}$, and $\mathbf{x} = (x_1 x_2 \ldots x_{24})$, $\mathbf{y} = (y_1 y_2 \ldots y_{24})$ have integer coordinates with Σx_i even, Σy_i odd (cf. Sloane (1979)).

Let u_n denote the number of points $\mathbf{v} \in \Lambda$ with $\mathbf{v} \cdot \mathbf{v} = 16n$, for $n = 0, 1, 2, \ldots$. In Table I on p. 67 of Blake (1971) the radius for $n = 6$ is 9.79796 ... (not 9.799), the correct values of u_7, u_9 are

$$u_7 = 187\ 489\ 935\ 360,$$
$$u_9 = 2\ 975\ 551\ 488\ 000,$$

and the values of

$$\sum_{i=1}^{n} u_i$$

for $n = 7, 8, 9, 10$ should be

$$226\ 951\ 976\ 160,$$
$$1\ 041\ 831\ 750\ 960,$$
$$4\ 017\ 383\ 238\ 960,$$
$$13\ 503\ 934\ 538\ 640,$$

respectively. Further values of u_n are given in Sloane (1981).

0019-9958/80/090270–03$02.00/0

On p. 68, Ramanujan's conjecture should read

$$|\tau(n)| \leqslant n^{11/2}\, d(n)$$

(rather than $n^{1/2}\, d(n)$). The conjecture has since been established by Deligne (see Katz (1976)). As for the lower bound, it is known that there are infinitely many values of n for which

$$|\tau(n)| \geqslant n^{11/2}$$

(again p. 68 has $n^{1/2}$).

In view of Deligne's result, or in fact from the much older result that

$$|\tau(n)| = O(n^6)$$

(see, for example, Hardy (1959, p. 170)), the approximation

$$u_n \approx \frac{65520}{691} \cdot \sigma_{11}(n)$$

is justified for all values of n. Furthermore as n increases the ratio of the two sides approaches 1, i.e.,

$$u_n \sim \frac{65520}{691} \cdot \sigma_{11}(n), \qquad \text{as } n \to \infty.$$

The approximation

$$\sum_{i=1}^{n} u_i \approx 7.9016\, n^{12}$$

given in Eq. (1) of Blake (1971) may be obtained directly, without appealing to Ramanujan's formula for $\Sigma\sigma_{11}(i)$, as follows. The number of points of Λ inside a sphere of radius $4n^{1/2}$ is very close to the volume of that sphere divided by the determinant of Λ (which is 2^{36}, from Leech (1967) or Sloane (1977)). Thus

$$\sum_{i=1}^{n} u_i \approx \frac{\pi^{12}(4n^{1/2})^{24}}{12! \cdot 2^{36}} = \frac{(2\pi n)^{12}}{12!} = 7.9016 \ldots n^{12}.$$

Furthermore using a theorem of Val'fiš (1924, Eq. (13)) this may be improved to give

$$\sum_{i=1}^{n} u_i = \frac{(2\pi n)^{12}}{12!} + O(n^{11}).$$

The fourth displayed equation on p. 70 should read

$$E_s \leqslant 24E_N = 16n.$$

Finally we mention that de Buda (1975) has given an upper bound on the error probability of the form

$$\text{constant} \cdot e^{-nE(R)},$$

thus answering the question raised on p. 72.

RECEIVED: March 12, 1980; REVISED, July 18, 1980

REFERENCES

BLAKE, I. F. (1971), The Leech lattice as a code for the Gaussian channel, Inform. Contr. **19**, 66–74.

DE BUDA, R. (1975), The upper error bound of a new near-optimal code, *IEEE Trans. Info. Theory* **IT-21**, 441–445.

CONWAY, J. H. (1969), A group of order 8,315,553,613,086,720,000, *Bull. London Math. Soc.* 1, 79–88.

HARDY, G. H. (1959), "Ramanujan," Chelsea, New York.

KATZ, N. M. (1976), An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields, *in* "Mathematical Developments Arising from Hilbert Problems," Proc. Sympos. Pure Math. XXVIII (F. E. Browder, Ed.), pp. 275–305, Amer. Math. Soc., Providence, R. I.

LEECH, J. (1967), Notes on sphere packings, *Canad. J. Math.* **19**, 251–267.

SLOANE, N. J. A. (1977), Binary codes, lattices, and sphere packings, *in* "Combinatorial Surveys: Proceedings, 6th British Combinatorial Conference" (P. J. Cameron, Ed.), pp. 117–164, Academic Press, London/New York.

SLOANE, N. J. A. (1979), Self-dual codes and lattices, *in* "Relations Between Combinatorics and Other Parts of Mathematics," Proc. Sympos. Pure Math. XXXIV (D. K. Ray-Chaudhuri, Ed.), pp. 273–308, Amer. Math. Soc., Providence, R. I.

SLOANE, N. J. A. (1981), Tables of sphere packings and spherical codes, *IEEE Trans. Information Theory* **IT-27**, in press.

WALFISZ, A. [= A. Z. Val'fiš] (1924), Über Gitterpunkte in mehrdimensionalen Ellipsoiden, *Math. Z.* **19**, 300–307.