

BOOK REVIEW

Sphere packings, lattices and groups, second ed., by J. H. Conway and N. J. A. Sloane. Grundlehren der Mathematischen Wissenschaften, bd. 290, Springer-Verlag, New York and Berlin, 1993, xliii+679 pp., \$69.00. ISBN 0-387-97912-3 and ISBN 3-540-97912-3

In 1611 Johann Kepler published an essay “On the Six-Cornered Snowflake”; see [10]. He explains how equal rhomboid dodecahedra will fit together to fill space. He goes on to explain how the loculi of pomegranates obtain their rhombohedral shapes, arguing that a fixed number of initially round loculi swell within the tough skin, first to form a densest possible arrangement of spheres with each sphere touching twelve others, and then swell further, pressing against each other to take the shape of rhomboid dodecahedra. The sphere packing that he claims to be densest is just the familiar arrangement used to pile cannon balls or oranges. A similar claim to have found the densest arrangement of spheres was apparently made by Thomas Harriot in 1599; see [10, p. 52]. After much discussion Kepler admits that he cannot explain why a typical snowflake is a flat flake with hexagonal symmetry, saying that chemists should consider the question. For a modern discussion of the problem see the article by B. J. Mason included in [10, pp. 47–63]. In fact, the water molecules in ice are not packed as closely as they could be—if they were, ice would not float on water.

History is never simple (and seldom completely correct). The next results were consequences of work on the arithmetical theory of quadratic forms. Let M be a symmetric positive definite $n \times n$ matrix with integral elements and determinant D . Then

$$Q(\mathbf{x}) = \mathbf{x}M\mathbf{x}^T$$

with $\mathbf{x} = (x_1, x_2, \dots, x_n)$ is a positive definite quadratic form, taking only non-negative integral values when x_1, x_2, \dots, x_n are integers, not all zero. The least nonzero value $m(Q)$ of Q under these restrictions is called the arithmetical minimum of Q . One important question in the theory of numbers is to find the largest possible value for the ratio $m(Q)/D^{1/n}$. The exact largest value was determined by Lagrange (1773) for $n = 2$, by Seeber and Gauss (1831) for $n = 3$, by Korkine and Zolotareff (1872, 1877) for $n = 4, 5$, and by Blichfeldt (1925, 1926, 1934) for $n = 6, 7, 8$. For larger values of n the largest value of the ratio remains unknown. Gauss (1831) explained the very simple connection of this problem with the problem of finding the densest lattice packing of spheres. Since M is symmetric and Q is positive definite, one can write

$$M = NN^T$$

(in many ways) with N an $n \times n$ matrix (whose entries need no longer be rational). Then

$$Q(\mathbf{x}) = \mathbf{y}\mathbf{y}^T = \|\mathbf{y}\|^2,$$

with $\mathbf{y} = \mathbf{x}N$. As \mathbf{x} runs over all integer lattice points, \mathbf{y} runs over all points of a general lattice Λ with determinant $d(\Lambda) = \sqrt{D}$. Further, the largest radius $r(\Lambda)$ for a sphere S such that the translates of S by the vectors of Λ form a nonoverlapping system is precisely $\frac{1}{2}\sqrt{m(Q)}$. Thus, if V_n is the volume of the unit sphere in \mathbb{R}^n , the problem of finding the minimum value for

$$m(Q)/D^{1/n} = (2r(\Lambda)/d(\Lambda)^{1/n})^2$$

is equivalent to finding the largest density

$$V_n(r(\Lambda))^n/d(\Lambda)$$

for a packing of spheres by the lattice Λ . Thus the density of the densest lattice packings of spheres in \mathbb{R}^n is known only for $n \leq 8$.

Meanwhile, Minkowski in 1893 initiated his study (see [11–13]) of “Geometrie der Zahlen”, i.e., the use of geometric methods to prove results in the theory of numbers. In particular, in 1905 he asserted that, if K is any convex body in \mathbb{R}^n symmetrical in the origin, then there is a lattice Λ such that the translates of K by the vectors of Λ form a lattice packing of K with density at least $2^{-n+1}\zeta(n)$ with

$$\zeta(n) = \sum_{k=1}^{\infty} k^{-n} = 1 + O(2^{-n})$$

as $n \rightarrow \infty$. He proved the result only in the case when K is a sphere by using his theory of the arithmetical reduction of positive definite quadratic forms. It was only in 1944 that Hlawka [8] published a proof of Minkowski’s full statement. In 1945 Siegel [16] published a proof that might be a very concise version of Minkowski’s unpublished ideas.

In 1914 Blichfeldt [1] discussed the more difficult problem of the densest packing of spheres in \mathbb{R}^n , without the restriction that the spheres form a lattice, and proved that the density Δ could not exceed

$$\frac{1}{2}(n+2)2^{-(1/2)n}.$$

This leaves a very large gap between Blichfeldt’s upper bound for the density of the closest packing of spheres in \mathbb{R}^n and Minkowski’s lower bound for the density of the closest lattice packing of spheres in \mathbb{R}^n . This gap has been reduced very considerably first by Levenshtein and then by Kubatianski and Levenshtein [9], who obtained $\Delta \leq 2^{-(0.5990\dots)n}$ for large n . The gap remains a challenge.

Results for the covering of \mathbb{R}^n by spheres have only been studied more recently. The best estimates for large n seem to be the proof [3] of Coxeter, Few, and Rogers in 1959 that the density of a covering of space by spheres cannot be less than a certain number $\tau_n \sim ne^{-3/2}$ ($n \rightarrow \infty$) and the results of Rogers [15] proving the existence of lattice coverings of space by spheres with densities no more than

$$c_1 n (\log_e n)^{(1/2) \log_2 2\pi e}$$

and by any symmetrical convex body with densities no more than

$$n^{\log_2 \log_e n + c_2}$$

for some constants c_1 and c_2 .

Leaving aside many special and especially interesting results on packing and covering in two and three dimensions and a few in four dimensions (see [2–7]), we have given an outline of the developments up to (and in one respect beyond) the publication of my modest book on the subject [15] in 1964.

So far I have been giving some of the background for the book under review. Most of this work is also surveyed in the book, but knowledge of the proofs is not necessary to follow it. Rather, a considerable appetite for combinatorics and group theory and a lot of persistence will be needed to progress beyond the first three chapters. While the results described above were more or less satisfactory from a theoretical point of view, once there were problems demanding practical solutions the nonconstructive methods that had been used were unsatisfactory—constructive methods became essential.

The authors are ably assisted by contributions from E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen, and B. B. Venkov. They confine their attention to the study of spheres, discarding the study of general convex bodies. They are largely motivated by the theory of error-correcting codes for the storage and transmission of information, a theory created by Shannon in 1948. Consider, for example, the problem of transmitting a string of n binary digits along a telegraph line that is noisy so that there is a probability $p < \frac{1}{2}$ that each digit will be incorrectly received. One needs to transform the string of n binary digits into a code of m binary digits with $m > n$, to transmit the longer string, and to uncode the true message of n digits from the corrupted string of m digits with high probability. This can be done with near certainty, when m is sufficiently large, if the 2^n code words of m digits are scattered among the 2^m corners of the cube,

$$0 \leq x_i \leq 1, \quad 1 \leq i \leq m,$$

so that the minimum distance between two code words is as large as possible. The corrupted message is regarded as one of the vertices of the cube and is replaced by the nearest (or one of the nearest) available code words. Shannon proved a remarkable existence theorem showing that for fixed $p < \frac{1}{2}$, the probability of incorrect decoding of a long message of length n could be made as small as one liked by taking m larger, but only modestly larger, than n . Shannon's ideas relate the problem of finding good codes, to the Packing Problem of finding dense packings of spheres. This works both ways: good lattice packings lead to good codes, and good codes lead back to good lattice packings.

The Kissing Problem asks, How many spheres of radius 1 can touch a sphere of radius 1 without overlapping each other? A more general version asks the same question of spheres of radius r touching a sphere of radius 1 and corresponds to the problem of constructing a special type of error-correcting codes called spherical codes.

The Gaussian Probability Problem asks, Given $\sigma > 0$, for what lattices Λ of determinant 1 in \mathbb{R}^n does the integral

$$\frac{1}{(\sigma\sqrt{2\pi})^n} \int_V e^{-\|\mathbf{x}\|^2/2\sigma^2} d\mathbf{x},$$

FIGURE 1

where V is the Voronoi polyhedron of all points of \mathbb{R}^n that are closer to the origin than to any other lattice point, attain its largest value? In a certain error-correcting problem the integral represents the probability that a code word subjected to a gaussian disturbance will be correctly decoded; hence, the demand for its maximization.

The Covering Problem, already discussed, is an informal dual of the Packing Problem and is discussed in detail for this reason. Although it does correspond to a coding problem, this correspondence is not very important and is merely mentioned in this book.

The Quantizer Problem is of a rather different nature. When one wishes to transmit or store information, one often starts with an analogue signal from a microphone, a television camera, or some other measuring instrument. One needs to convert this signal to digital form. The standard procedure is to first sample the signal at close intervals and then to split the sample into longish blocks of n values each, each block being represented by a point in \mathbb{R}^n . Since the original signal is of limited power, the points will lie in a bounded region in \mathbb{R}^n . The next step is to choose a number, say, m , of “code” points in this bounded region, each with its own code word, and to associate with each block of sample the code word of the code point nearest to the point representing the block. The idea is well illustrated by Figure 1 reproduced from the book (with $n = 2$ and $m = 11$). The Quantization Problem is to choose the best arrangement of the coding points. Usually the points representing the blocks are assumed to be uniformly distributed throughout a large sphere, and the code points are taken to be those points of a lattice that lie within the sphere (but the code points are not chosen in this way in the example illustrated).

These Problems (with a capital P) are mathematical problems, abstracted from communication engineering problems that have many other considerations demand-

ing compromise solutions. The book quite fairly treats them as mathematical problems. The solutions provided have led to many practical applications, and they will probably continue to do so for many years.

After the best possible lattice packings were determined up to dimension 8, good lattice packings in 9, 10, 11 dimensions were provided by Chaundy, and the Coxeter-Todd lattice was found in \mathbb{R}^{12} . A real breakthrough was made when Leech found his lattice in \mathbb{R}^{24} , and its automorphism group was analyzed by Conway, leading to his discovery of three new simple groups. By 1973 Fisher and Griess had independently concluded that there might well be a monstrous simple group of order

$$2^{46}3^{20}5^97^611^213^317 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

and found many of its properties on the postulate that it existed. Only in 1980 did Griess construct this Fisher-Griess group using amongst other things the Leech lattice. The Leech lattice provided an unexpectedly good packing of spheres in \mathbb{R}^{24} , and its sublattices and superlattices led to good packings up to about 48 dimensions. Combinations of coding theory results and of geometrical constructions by many authors have led to the construction of many lattices, which have been compared with each other to find the best-known lattices for the five problems discussed above. The book gives extensive tables of the lattices providing the best of the known solutions—tables that are complete up to 24 dimensions but that contain sporadic entries up to dimension 1,048,584.

Rather than list the many topics discussed in the book, it may be more helpful to say something about the methods that are employed.

Many methods of constructing lattices are employed. One of the simplest is the process of lamination. Suppose that \wedge is known to be a good lattice for packing spheres of radius 1 in \mathbb{R}^n . We can regard this packing as a packing of n -dimensional “discs” in the plane $x_{n+1} = 0$ in \mathbb{R}^{n+1} . One then forms a “lamina” L in \mathbb{R}^{n+1} by replacing each disc in $x_{n+1} = 0$ by a sphere of radius 1 in \mathbb{R}^{n+1} having the same centre. One then translates the lamina L by a vector

$$\mathbf{c} = (c_1, c_2, \dots, c_n, c_{n+1})$$

with $c_{n+2} > 0$ to form a lamina $L + \mathbf{c}$. One adjusts the parameters c_1, c_2, \dots, c_n to allow c_{n+1} to take its smallest possible value, subject to the condition that the laminae L and $L + \mathbf{c}$ should not overlap. Provided the laminae L and $L + k\mathbf{c}$ do not overlap when $1 \leq k \leq 2/c_{n+1}$, the lattice generated by \mathbf{c} and a basis for \wedge in $x_{n+1} = 0$ provides a “laminated” lattice in \mathbb{R}^{n+1} , yielding a good lattice packing for spheres of radius 1 in \mathbb{R}^{n+1} . However, this packing may not be the best-possible packing in \mathbb{R}^{n+1} even when \wedge is the best-possible packing in \mathbb{R}^n .

To illustrate the method of constructing lattices from error-correcting codes, we consider a very special type of code. Let p be a prime, and identify the finite field \mathbb{F}_p of order p with the integers $0, 1, \dots, p-1$, the operations being the usual addition and multiplication mod p . For fixed n we regard the product \mathbb{F}_p^n as an n -dimensional vector space over \mathbb{F}_p . Let C be a k -dimensional linear subspace of \mathbb{F}_p^n . We take the p^k points of C as our code words. We suppose that each code word, other than $(0, 0, \dots, 0)$, has at least d nonzero elements. Let \wedge be the set of all points of \mathbb{R}^n with integer coordinates that are congruent mod p to some codeword of C . It is easy to verify that \wedge is a lattice of determinant p^{n-k} and that the spheres of radius

$\frac{1}{2}\sqrt{d}$ centred on the lattice points are nonoverlapping. It seems that in practice one is able to construct good packings only when $p = 2$ or 3 . However, the first simple proof of the Minkowski-Hlawka theorem [14] used precisely this method, taking p to be a large prime and proving the existence of a suitable code C with $k = 1$ by an averaging method.

A third construction method uses the theory of algebraic number fields. Suppose that ζ is a complex algebraic integer of degree $n = 2s$, all of whose conjugates are complex. Let \mathcal{O} be an ideal in the ring of integers in the algebraic number field $Q(\zeta)$. Let

$$\xi_1^{(1)}, \xi_2^{(1)}, \dots, \xi_n^{(1)}$$

be a basis for \mathcal{O} over the rational integers, and let

$$\xi_i^{(1)}, \dots, \xi_i^{(s)}, \bar{\xi}_i^{(1)}, \dots, \bar{\xi}_i^{(s)}$$

be the conjugates of $\xi_i^{(1)}$, for $1 \leq i \leq n$. Then the set of all points

$$\boldsymbol{\eta} = u_1 \boldsymbol{\xi}_1 + \dots + u_n \boldsymbol{\xi}_n,$$

with

$$\boldsymbol{\xi}_i = (\xi_i^{(1)}, \dots, \xi_i^{(s)}), \quad 1 \leq i \leq n,$$

and u_1, u_2, \dots, u_n all rational integers, forms a lattice \wedge in \mathbb{R}^n , identified in the natural way with \mathbb{C}^s . Writing

$$\boldsymbol{\eta} = (\eta^{(1)}, \eta^{(2)}, \dots, \eta^{(s)})$$

in \mathbb{C}^s , we have

$$\begin{aligned} \left(\frac{1}{s}\right)^s \|\boldsymbol{\eta}\|^n &= \left(\frac{1}{s}\right)^s (|\eta^{(1)}|^2 + \dots + |\eta^{(s)}|^2)^s \\ &\geq |\eta^{(1)} \eta^{(2)} \dots \eta^{(s)}|^2 = |\text{norm} \eta^{(1)}|, \end{aligned}$$

which is a nonzero integer provided u_1, u_2, \dots, u_n are not all zero. Hence \wedge provides a lattice packing of spheres in \mathbb{R}^n of radius $(\frac{1}{2}n)^{1/2}$. By suitable choice of the ideal \mathcal{O} one can make the least value of $\|\boldsymbol{\eta}\|$, with $\boldsymbol{\eta} \neq 0$, as large as one pleases but at the expense of making the determinant of \wedge large as well. In particular, Craig studies the special case when $\zeta = e^{2\pi i/p}$ with $p = 2s + 1$ a prime and when \mathcal{O} is a principal ideal of the form $((1 - \zeta)^{m+1})$ and obtains some of the densest packings known so far when $148 \leq n \leq 3000$.

When all the vectors of a lattice \wedge have squared lengths that are integers, a theta function

$$\theta_{\wedge}(z) = \sum_{\mathbf{x} \in \wedge} q^{\|\mathbf{x}\|^2} = \sum_{m=0}^{\infty} N(m) q^m, \quad q = e^{\pi i z},$$

with $N(m)$ the number of lattice vectors with squared length m , can be associated with \wedge . Such theta series, originally defined for quadratic forms with integral coefficients, have been studied since they were introduced by Jacobi. Intricate calculations using theta series identities enable the authors to find the theta series

for many of the special lattices they study. In particular, the series for Blichfeldt's lattice in \mathbb{R}^8 is

$$\begin{aligned} & \theta_2(2z)^8 + 14\theta_2(2z)^4\theta_3(2z)^4 + \theta_3(2z)^8 \\ & = 1 + 240q^2 + 2160q^4 + \dots, \end{aligned}$$

and the series for Leech's lattice is

$$\begin{aligned} & \frac{1}{2}[\theta_2(z)^{24} + \theta_3(z)^{24} + \theta_4(z)^{24}] - \frac{69}{16}[\theta_2(z)\theta_3(z)\theta_4(z)]^8 \\ & = 1 + 196560q^4 + 16773120q^6 + \dots, \end{aligned}$$

where $\theta_2, \theta_3, \theta_4$ are elementary Jacobi theta series. Thus, in Blichfeldt's lattice each sphere touches 240 others, and in Leech's lattice each sphere (having radius 2) touches 196,560 others.

The improvements on Blichfeldt's upper bound for the density of packings of spheres in \mathbb{R}^n , due to Kabatianski and Levenshtein, depend on a remarkable new method that also yields upper bounds for the kissing numbers for spheres and bounds for the efficiency of error-correcting codes of various types. We give a brief outline of the method used for the study of spheres; the results for codes are equally striking, but they involve even more elaborate techniques. The first stage is to construct for each $k \geq 1$, from the spherical harmonics of degree k , a special ultraspherical polynomial $\Phi_k(t)$ with the property that, for any vectors $\mathbf{x}_1, \dots, \mathbf{x}_m$ in \mathbb{R}^n , all of length 1, and any complex numbers a_1, \dots, a_m ,

$$\sum_{i=1}^m \sum_{j=1}^m \Phi_k(\langle \mathbf{x}_i, \mathbf{x}_j \rangle) a_i \bar{a}_j \geq 0.$$

These polynomials are all normalized so that $\Phi_k(1) = 1$ and $\Phi_0(t)$ is taken to be 1. Let $A(n, \theta)$ denote the maximum number of points or codewords \mathbf{x}_i in \mathbb{R}^n with $\|\mathbf{x}_i\| = 1$ and

$$\langle \mathbf{x}_i, \mathbf{x}_j \rangle \leq \cos \theta, \quad \text{for } i \neq j.$$

If C is such a spherical code, let

$$t(0) = 1, t(1), \dots, t(s),$$

with

$$-1 \leq t(r) \leq \cos \theta, \quad 1 \leq r \leq s,$$

be the values taken by the scalar products $\langle \mathbf{x}_i, \mathbf{x}_j \rangle$. For $0 \leq r \leq s$ define $\alpha_{t(r)}$ to be the ratio to $|C|$ of the number of pairs $(\mathbf{x}_i, \mathbf{x}_j)$ in $C \times C$ with $\langle \mathbf{x}_i, \mathbf{x}_j \rangle = t(r)$. Then

$$\alpha_{t(0)} = 1; \quad \alpha_{t(r)} \geq 0, \quad 1 \leq r \leq s; \quad \sum_{r=0}^s \alpha_{t(r)} = |C|.$$

Further,

$$\begin{aligned} 1 + \sum_{r=1}^s \alpha_{t(r)} \Phi_k(t(r)) &= \sum_{r=0}^s \alpha_{t(r)} \Phi_k(t(r)) \\ &= |C|^{-1} \sum_{\mathbf{x}_m, \mathbf{y}_m \in C} \Phi_k(\langle \mathbf{x}_m, \mathbf{y}_m \rangle) \geq 0. \end{aligned}$$

Thus we obtain a bound for $A(n, \theta)$ if we maximize $\sum_{r=0}^s \alpha_{t(r)}$ subject to

$$\begin{aligned} \alpha_{t(0)} &= 1; & \alpha_{t(r)} &\geq 0, & 1 \leq r \leq s; \\ \sum_{r=1}^s \alpha_{t(r)} \Phi_k(t(r)) &\geq -1, & k &= 0, 1, \dots, \end{aligned}$$

where $-1 \leq t(r) \leq \cos \theta$, $1 \leq r \leq s$. This is a linear programming problem. Hence, an upper bound for the maximum is provided by a feasible solution to the dual problem. It follows from this theory that

$$A(n, \theta) \leq 1 + f_1 + \dots + f_N$$

if f_1, \dots, f_N are real numbers satisfying

$$\begin{aligned} f_k &\geq 0, & k &= 1, 2, \dots, N; \\ \sum_{k=1}^N f_k \Phi_k(t) &\leq -1 & \text{for } -1 \leq t \leq \cos \theta. \end{aligned}$$

Now $A(n, \pi/3)$ is just the kissing number in \mathbb{R}^n . Using explicit formulae for the Φ_k and obtaining numerical solutions to the dual programming problem, the kissing number in \mathbb{R}^8 is shown to be no more than 240 and in \mathbb{R}^{24} is shown to be no more than 196,560. Thus the kissing numbers in \mathbb{R}^8 and \mathbb{R}^{24} are precisely determined, providing one of the most striking results in the book. A simple geometrical argument shows that the packing density Δ_n in \mathbb{R}^n satisfies

$$\Delta_n \leq (\sin \frac{1}{2}\theta)^n A(n+1, \theta),$$

for all θ with $0 < \theta < \pi$. By choosing a suitable θ and making a good estimate for $A(n+1, \theta)$ when n is large, Kabatianski and Levenshtein obtain their results that $\Delta_n \leq 2^{-0.599n}$, when n is sufficiently large.

As the title suggests, much space is devoted to the theory of groups. I shall not give an extensive review of this section, however, for sake of space and because I do not feel competent to do this. A few words will have to suffice. The main objective is to give a survey of the sporadic simple groups with details of their constructions. Particular attention is demanded by and given to the Conway groups and to the Fischer-Griess Monster group.

The second edition differs from the first by the inclusion of a survey of a surprisingly large body of work that has been completed since the first edition appeared and the addition of a supplementary bibliography of seventeen pages. The authors say that numerous small corrections and improvements have been made to the text.

REFERENCES

1. H. F. Blichfeldt, *A new principle in the geometry of numbers*, Trans. Amer. Math. Soc. **15** (1914), 227–235.
2. J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer-Verlag, New York, 1971.
3. H. S. M. Coxeter, L. Few, and C. A. Rogers, *Covering space with equal spheres*, *Mathematika* **6** (1959), 147–157.

4. L. Fejes Toth, *Lagerungen in der Ebene, auf der Kugel und in Raum*, Grundlehren Math. Wiss., bd. 65, Springer, Berlin, 1953.
5. ———, *Regular figures*, Pergamon, Oxford, 1964.
6. ———, *On the densest packing of convex discs*, *Mathematika* **30** (1983), 1–3.
7. P. M. Gruber and C. G. Lekkerkerker, *Geometry of numbers*, 2nd ed., North-Holland, Amsterdam, 1987.
8. E. Hlawka, *Zur Geometrie der Zahlen*, *Math. Z.* **49** (1944), 285–312.
9. G. A. Kabatiansky and V. I. Levenshtein, *Bounds for packings on a sphere and in space*, *Problems of Information Transmission* **14** (1978), 1–17.
10. J. Kepler, *The six-cornered snowflake*, Translated from the Latin booklet of 1611 by Colin Hardie, Clarendon Press, Oxford, 1966.
11. H. Minkowski, *Diphantische approximationen*, Teubner, Leipzig, 1907.
12. ———, *Geometrie der Zahlen*, Teubner, Leipzig, 1910.
13. ———, *Gesammelte abhandlungen*, Teubner, Berlin, 1911.
14. C. A. Rogers, *Existence theorems in the geometry of numbers*, *Ann. of Math. (2)* **48** (1947), 994–1002.
15. ———, *Packing and covering*, Cambridge Univ. Press, London and New York, 1964.
16. C. L. Siegel, *A mean value theorem in the geometry of numbers*, *Ann. of Math. (2)* **46** (1945), 340–347.

C. A. ROGERS
UNIVERSITY COLLEGE LONDON