WHAT IS . . .

the Leech Lattice?

Chuanming Zong

The *Leech lattice* is a magical structure in twenty-four-dimensional Euclidean space $\mathbb{E}^{24}$ that was inspired by Golay's error-correcting code $\mathcal{G}_{24}$. The magic of the Leech lattice led Conway to the discovery of the three *sporadic simple groups*: Co_1, Co_2, and Co_3. Also magically, the Leech lattice provides the optimal kissing configuration for the 24-dimensional unit ball as well as the densest *lattice ball packing* in $\mathbb{E}^{24}$.

Data in digital systems are typically stored, transmitted, and processed in binary codewords. If a single codeword is in error, the message is garbled or the computation spoiled. Starting in the 1940s, scientists searched for coding systems that could detect and even correct errors.

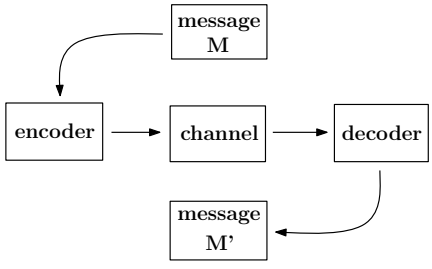

Figure 1. The data transmission process.

In 1947 R. Hamming discovered the first binary error-correcting code, $\mathcal{H}_7$, which is generated by four vectors, $(1,1,0,1,0,0,0)$, $(0,1,1,0,1,0,0)$, $(0,0,1,1,0,1,0)$ and $(0,0,0,1,1,0,1)$, over $\mathbb{Z}_2$. The *Hamming distance* between two codewords is the number of their different entries. The minimal Hamming distance of the code above is four, and therefore this code can detect and correct single-bit errors.

Let $\mathbf{w}_1$ denote the binary 23-tuple $(1,1,0,0,0,1,1,1,0,1,0,1,0,0,0,0,0,0,0,0,0,0,0)$. If we write the final entry, 0, first, followed by the other 22 entries, we get the first cyclic shift of $\mathbf{w}_1$: $(0,1,1,0,0,0,1,1,1,0,1,0,1,0,0,0,0,0,0,0,0,0,0,0)$. The next cyclic shift is $(0,0,1,1,0,0,0,1,1,1,0,1,0,1,0,0,0,0,0,0,0,0,0,0)$, and so on. Then $\mathbf{w}_1$ and its cyclic shifts generate a binary code, the *Golay code* $\mathcal{G}_{23}$, which was discovered by M. J. E. Golay in 1949. The minimal Hamming distance of this code is seven, and therefore it can detect and correct three-bit errors. This code has $2^{12} = 4096$ codewords. By adding a parity check to each codeword of $\mathcal{G}_{23}$, we get the *extended Golay code* $\mathcal{G}_{24}$. The minimal Hamming distance of $\mathcal{G}_{24}$ is eight.

The philosophy of error-correcting codes—to design codes with both large minimal Hamming distances and large numbers of codewords—is related to ball packings with large packing densities. In 1965 J. Leech constructed a twenty-four-dimensional lattice Λ by lifting the extended Golay code $\mathcal{G}_{24}$ from $\mathbb{Z}_2^{24}$ to $\mathbb{Z}^{24}$ and restricting the sum of the coordinates to zero modulo 4. Here an n-dimensional *lattice* is the set of all linear combinations of n linearly independent vectors over $\mathbb{Z}$. In 1967 Leech realized that there are big holes in Λ. Filling those holes doubles the density and produces a remarkable lattice, Λ_{24}, the Leech lattice. For convenience, we say a vector $(v_1, v_2, \ldots, v_n)$ has shape $(a^j, b^k, \ldots)$ if $v_i = a$ for j entries, $v_i = b$ for k entries, etc. In fact, the Leech lattice can be generated by all vectors of the shape

$$\tfrac{1}{\sqrt{8}}(\mp 3, \pm 1^{23}),$$

where the ∓ 3 can be in any position and the upper signs are taken on a set of coordinates where a codeword of $\mathcal{G}_{24}$ is one.

The Leech lattice has 196,560 shortest vectors of length two: 97,152 of them have shape $(0^{16}, \pm 2^8)$; 98,304 of them have shape $(\pm 1^{23}, \pm 3)$; and 1,104 of them have shape $(0^{22}, \pm 4^2)$. One might therefore conjecture that Λ_{24} has a large *symmetry group*. In 1968 J. H. Conway determined this group, Co_0. It is generated by six elements and has order

$$|Co_0| = 2^{22}3^9 5^4 7^2 11 \cdot 13 \cdot 23.$$

Chuanming Zong is professor of mathematics at Peking University. His email address is cmzong@math.pku.edu.cn.

DOI: http://dx.doi.org/10.1090/noti1045

More surprisingly, he discovered three new sporadic[1] simple groups, Co_1, Co_2, and Co_3, as subgroups of Co_0, where

$$|Co_1| = 2^{21}3^9 5^4 7^2 11 \cdot 13 \cdot 23,$$

$$|Co_2| = 2^{18}3^6 5^3 7 \cdot 11 \cdot 23,$$

and

$$|Co_3| = 2^{10}3^7 5^3 7 \cdot 11 \cdot 23.$$

Let B^n denote the n-dimensional unit ball centered at the origin, that is,

$$B^n = \{\mathbf{x} \in \mathbb{E}^n : \ |\mathbf{x}| \le 1\};$$

let $\tau(B^n)$ denote its *kissing number* (the maximal number of nonoverlapping unit balls that can simultaneously touch B^n at its boundary); and let $\tau^*(B^n)$ denote its *lattice kissing number*. Since the length of the shortest vectors in Λ_{24} is two, $B^{24}+\Lambda_{24}$ is a lattice ball packing. Therefore we have

$$\tau(B^{24}) \ge \tau^*(B^{24}) \ge 196560. \tag{1}$$

Let $A(n, \theta)$ denote the maximal number of points on the surface of B^n with minimal spherical separation θ. Clearly we have

$$\tau(B^n) = A(n, \pi/3).$$

For $k = 0, 1, 2, \ldots$, let $P_k^{\alpha,\beta}(t)$ denote the *Jacobi polynomial* of degree k, where $\alpha > -1$ and $\beta > -1$ are two parameters. These polynomials form an orthogonal basis for the space of all polynomials. In the 1970s P. Delsarte et al. discovered the following criterion: *Write* $\alpha = (n-3)/2$. *If*

$$f(t) = \sum_{i=0}^{k} f_i P_i^{\alpha,\alpha}(t)$$

is a real polynomial such that $f_0 > 0$, $f_i \ge 0$ *for* $i = 1, 2, \ldots, k$, *and* $f(t) \le 0$ *for* $-1 \le t \le \cos\theta$, *then*

$$A(n, \theta) \le \frac{f(1)}{f_0}. \tag{2}$$

In 1978 V. I. Levenštein, A. M. Odlyzko, and N. J. A. Sloane constructed such a polynomial $f(t)$ for $n = 24$ and surprisingly obtained

$$\tau(B^{24}) = A(24, \pi/3) \le 196560. \tag{3}$$

Then (1) and (3) together yield

$$\tau(B^{24}) = \tau^*(B^{24}) = 196560.$$

Moreover, as was shown by E. Bannai and N. J. A. Sloane in 1981, the local kissing configuration of $B^{24} + \Lambda_{24}$ is the only optimal one for $\tau(B^{24})$, up to isometry.

The problem of optimizing the upper bound in (2) is unsolved in general and appears to be difficult. However, there are simple choices of $f(t)$ that exactly solve the kissing number problem in both $\mathbb{E}^8$ and $\mathbb{E}^{24}$. Perhaps the mystery lurking in the background is the uniqueness of the optimal configurations.

Let $\delta(B^n)$ and $\delta^*(B^n)$ denote the densities of the densest packings and the densest lattice packings of B^n respectively. It can be verified that the determinant of Λ_{24} is one and therefore the packing density of $B^{24} + \Lambda_{24}$ is $\pi^{12}/12!$. Thus we have

$$\delta(B^{24}) \ge \delta^*(B^{24}) \ge \frac{\pi^{12}}{12!}.$$

For a real function $f(\mathbf{x})$ defined on $\mathbb{E}^n$ we define

$$\hat{f}(\mathbf{y}) = \int_{\mathbb{E}^n} f(\mathbf{x}) e^{2\pi i \langle \mathbf{y}, \mathbf{x} \rangle} d\mathbf{x},$$

where $\langle \mathbf{y}, \mathbf{x} \rangle$ is the inner product of $\mathbf{y}$ and $\mathbf{x}$, and $i = \sqrt{-1}$. If there is a positive constant μ such that both $|f(\mathbf{x})|$ and $|\hat{f}(\mathbf{x})|$ are bounded above by a constant times $(1 + |\mathbf{x}|)^{-n-\mu}$, we say $f(\mathbf{x})$ is *admissible*.

In 2003 H. Cohn and N. D. Elkies proved the following criterion: *Suppose* $f(\mathbf{x})$ *is an admissible function defined on* $\mathbb{E}^n$ *that satisfies:*
1. $f(\mathbf{o}) = \hat{f}(\mathbf{o})$,
2. $f(\mathbf{x}) \le 0$ *whenever* $|\mathbf{x}| \ge r$, *and*
3. $\hat{f}(\mathbf{x}) \ge 0$ *for all* $\mathbf{x} \in \mathbb{E}^n$.

Then we have

$$\delta(B^n) \le \frac{\pi^{n/2}}{(n/2)!} \left(\frac{r}{2}\right)^n.$$

Actually, this is a Euclidean analog of (2). Based on this result, in 2009 H. Cohn and A. Kumar proved

$$\frac{\pi^{12}}{12!} \le \delta(B^{24}) \le \left(1 + 1.65 \cdot 10^{-30}\right) \cdot \frac{\pi^{12}}{12!} \tag{4}$$

and

$$\delta^*(B^{24}) = \frac{\pi^{12}}{12!}.$$

This time, up to symmetry, the Leech lattice again is the only optimal 24-dimensional lattice for $\delta^*(B^{24})$. Doubtless, given (4), everybody will bet on

$$\delta(B^{24}) = \frac{\pi^{12}}{12!}.$$

Acknowledgments

This work is supported by 973 Programs 2013CB834201 and 2011CB302401, the National Natural Science Foundation of China (grant No. 11071003), and the Chang Jiang Scholars Program of China. I am grateful to the referee for helpful comments.

References

1. H. Cohn and A. Kumar, Optimality and uniqueness of the Leech lattice among lattices, *Ann. Math. (2)* **170** (2009), 1003–1050.
2. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 1988; 3rd ed, 1999.
3. T. M. Thompson, *From Error Correcting Codes through Sphere Packings to Simple Groups*, Mathematical Association of America, 1983.
4. C. Zong, *Sphere Packings*, Springer-Verlag, New York, 1999.

[1] *There are twenty-six sporadic simple groups. The first was discovered in 1861 by E. Mathieu, and the last one, known as the friendly giant or the monster, was constructed by R. Griess in 1982 (see "What is the monster?", by Richard Borcherds,* Notices, *October 2002).*