Lattices

SUMS lecture, October 19, 2009; Winter School lecture, January 8, 2010.

Eyal Z. Goren, McGill University

• **Lattices**

A *lattice* $\mathscr{L}$ in $\mathbb{R}^n$ is

$$\mathscr{L} = \{a_1 v_1 + \cdots + a_n v_n : a_1, \ldots, a_n \in \mathbb{Z}\},$$

where the v_i are linearly independent, or, equivalently $\mathscr{L}$ is *discrete*: there is an $\epsilon > 0$ such that any two distinct elements of $\mathscr{L}$ are at least ϵ apart.

Example. $\mathbb{Z}^n \subset \mathbb{R}^n$. For $n = 2$, viewing $\mathbb{R}^2$ as $\mathbb{C}$, we can view $\mathbb{Z}^2$ as $\{a + bi : a, b \in \mathbb{Z}\}$.

Example. $n = 2$. The hexagonal lattice $\{a + b\omega : a, b \in \mathbb{Z}\}$, where $\omega = (1 + \sqrt{-3})/2$.

• **Sphere packing**

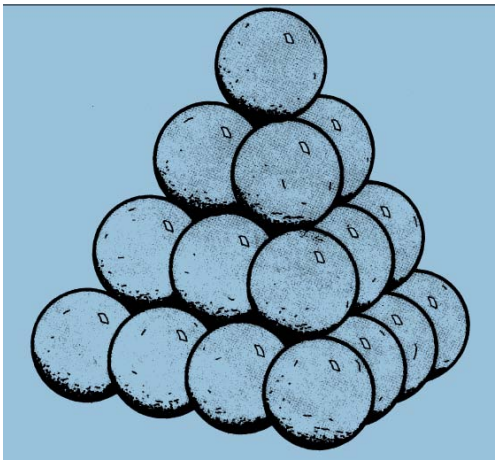
The problem of sphere packing:

What is the best way to pack solid spheres of radius 1 *in* $\mathbb{R}^n$*?*

▷ $n = 1$. Place each sphere on an even integer. (TRIVIAL)

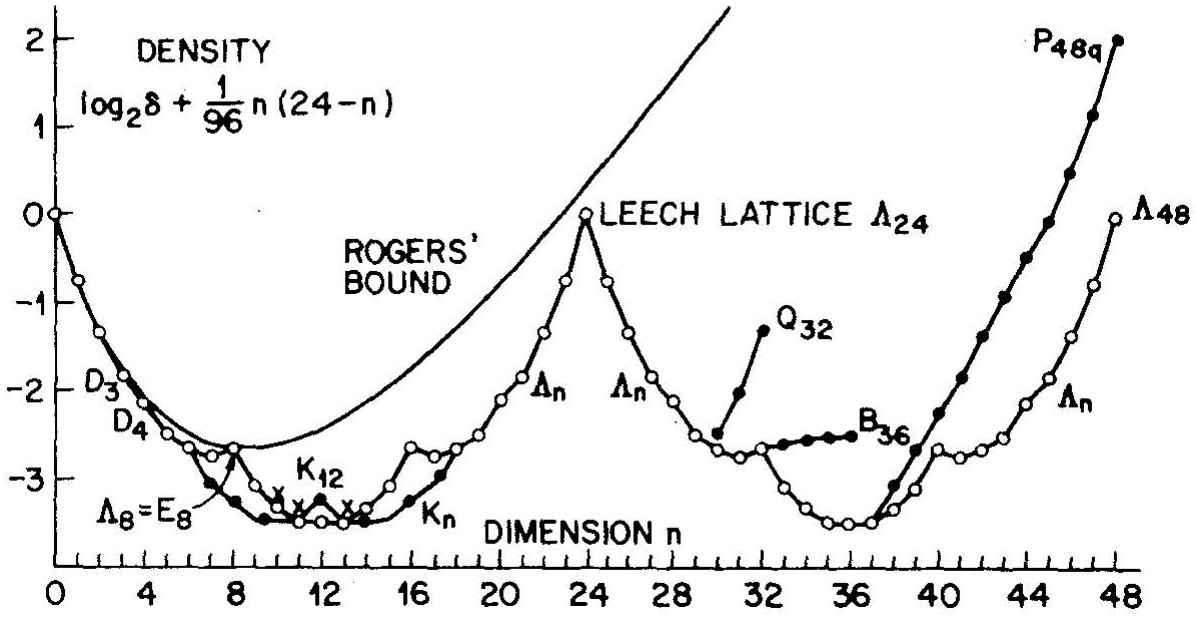
▷ $n = 2$. Place each sphere (rescaled) on a point of the hexagonal lattice. (GAUSS 1831, THUE 1890)

▷ $n = 3$. Stack as market vendors stack oranges. (FCC lattice). (KEPLER's conjecture, HALES 1998)



▷ $n \geq 4$. Totally out of reach.

One asks instead about *Lattice packing*. Much more is known ($n \leq 8$). There is a bound (the Rogers' bound) on how good a lattice packing can be; in general there is a huge gap between the bound and construction of lattices coming close to the bound, but in dimension 24 something singular happens: *The Leech lattice*.



The usual *density* of the packing Δ is defined to be the proportion of space that is occupied by the spheres (which is a volume of one sphere divided by the volume of the fundamental parallelotope). The *center density* is defined as

$$\delta = \Delta / V_n,$$

where V_n is the volume of the unit ball in $\mathbb{R}^n$.

Key Problem: How to construct interesting lattices??

• **Codes**

Let $\mathbb{F}_2 = \{0, 1\}$ be the field of 2 elements. A (linear) *code* $\mathbf{C}$ of length n is a subset of

$$\mathbb{F}_2^n = \{\underline{a} = (a_1, \ldots, a_n) : a_i = 0, 1\},$$

which is non-empty and closed under addition; one adds vectors by adding their respective components modulo 2,

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1 \pmod 2, \ldots, a_n + b_n \pmod 2).$$

Given a code $\mathbf{C}$ in $\mathbb{F}_2^n$ we can extend it to $\mathbf{C}^e$ in $\mathbb{F}_2^{n+1}$ by adding a check-sum digit

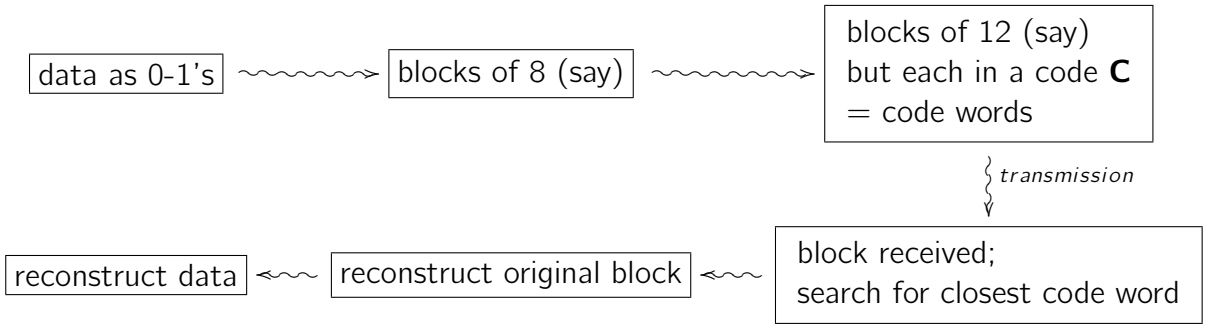
$$\mathbf{C}^e = \{(\underline{a}, a_1 + \cdots + a_n \pmod 2) : \underline{a} \in \mathbf{C}\}.$$

For example, taking $\mathbf{C} = \mathbb{F}_2^2$ we get a code $\mathbf{C}^e$, called the parity check code, in $\mathbb{F}_2^3$,

$$\{(0, 0, 0), (1, 0, 1), (0, 1, 0), (1, 1, 0)\}.$$

(This code is still used in everyday applications.)

A code is used to detect and repair mistakes in data sent over noisy channel. Here is a schematics:



For example, in the case of the parity check code, we chop to blocks of size two, add a check sum digit and get block of size 3. If we get after the transmission (a, b, c) such that $c \neq a + b$ then we know an error had occurred.

• **The Hamming code $\mathscr{H}$**

This is the code generated by

$$(1, 1, 0, 1, 0, 0, 0), \ \ (0, 1, 1, 0, 1, 0, 0), \ \ (0, 0, 1, 1, 0, 1, 0), \ \ (0, 0, 0, 1, 1, 0, 1).$$

It has 2^4 elements and the minimal distance between two distinct code words is 3. It can therefore detect up to 2 errors and correct a single error. Consider $\mathscr{H}^e \subset \mathbb{F}_2^8$. Consider

all the vectors in $\mathbb{Z}^8$ that reduce to elements of $\mathscr{H}^e$ modulo 2 (one says that we apply "construction A" to the code $\mathscr{H}^e$). This is a lattice $\mathscr{L}$, which we rescale it to obtain a lattice

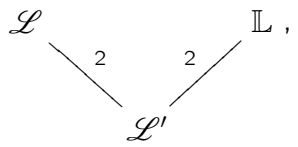
$$E_8 = \frac{1}{\sqrt{2}}\,\mathscr{L}.$$

The E_8 lattice is "famous". It appears for example in the theory of Lie groups and in many other places. It gives the best lattice packing in $\mathbb{R}^8$.

• **The Golay code $\mathscr{G}$**

Let $\underline{a} = (a_1, \ldots, a_{23})$, where $a_i = 1$ if i is a non-zero square modulo 23 and else is zero. Take all cyclic shifts of $\underline{a}$, such as $(a_{23}, a_1, a_2, \ldots, a_{22})$ and so on, and take the minimal code containing them. This is the Golay code $\mathscr{G}$. There are 2^{12} elements in this code and the minimal distance between code words is 7. Thus, if we put a sphere of radius 3 around each code word, the spheres are disjoint, each has 2^{11} elements and since $2^{23} = 2^{12} \times 2^{11} =$ the number of distinct points in the spheres, we find that this discrete lattice packing covers the space completely. As a result, *every* received transmission, if it has less than 3 errors, can be corrected. This remarkable code was used in the Voyager I (1979) and Voyager II (1980) missions to Jupiter and Saturn; it is used today in DVD readers. The rovers on Mars are actually using a complicated system involving two codes, one of them is a Reed-Solomon code.

Consider now $\mathscr{G}^e \subset \mathbb{F}_2^{24}$. We perform "construction A" of Sloane and get a lattice $\mathscr{L}$ in $\mathbb{R}^{24}$ by considering all the vectors in $\mathbb{Z}^{24}$ that reduce modulo 2 to the extended Golay code $\mathscr{G}^e$. The Leech lattice is a lattice $\mathbb{L}$ in $\mathbb{R}^{24}$ such that



where the 2 refers to index 2 (namely, $\mathscr{L} = \mathscr{L}' \cup (v + \mathscr{L}')$ for some $v \in \mathscr{L}$ and so on.) The precise description is a bit technical: $\mathscr{L}'$ consists of the vectors $v = (v_1, \ldots, v_{24})$ such that $\sum_i v_i \equiv 0 \pmod 4$. The Leech lattice is generated by $\mathscr{L}'$ and the vector $(-3/2, 1/2, 1/2, \ldots, 1/2)$. One rescales $\mathbb{L}$ by dividing all its vectors by $1/\sqrt{2}$.

• **Automorphism of lattices**

Let $\mathscr{L}$ be a lattice in $\mathbb{R}^n$. An automorphism of $\mathscr{L}$ is defined to be a distance preserving linear map taking $\mathscr{L}$ to itself. It is therefore an element of

$$\underbrace{M_n(\mathbb{Z})}_{discrete} \cap \underbrace{O_n(\mathbb{R})}_{bounded},$$

hence $\mathrm{Aut}(\mathscr{L})$ is a *finite* group.

A finite group is a non-empty finite set with an associative operation $(g, h) \mapsto gh$ such that there is a neutral element and there are inverses. A subgroup is a subset H of G such that if $g, h \in H$ also $gh \in H$. For example, the permutations σ of a set with n elements are a group, called the symmetric group S_n. It has $n!$ elements.

Every finite group is, up to some natural identification, a subgroup of S_n. As an example, A_n is the subgroup of permutations σ in S_n such that

$$\prod_{i<j}(x_i - x_j) = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}).$$

If H is a subgroup of G, a coset of H is a subset of G of the form $aH = \{ah : h \in H\}$. A subgroup is called *normal* if the cosets $aH, bH, cH, \ldots$ form a group in their own right under the definition

$$aH * bH = abH.$$

This group is denoted G/H. We can then say that G is simplified by $(H, G/H)$ (the number of elements of G/H is $\sharp\, G/\sharp\, H$ and so, if H is a proper subgroup, both groups $H, G/H$ have less elements than G does).

What are the building blocks? the groups that cannot be simplified? That is, what are the groups that don't have proper normal subgroups? (such groups are called "simple"). The classification theorem, completed in 1980's and consisting of hundreds of papers totalling more than 10000 pages answers that (with certain gaps still being closed). There are some families of simple groups:

$\triangleright$ $\mathbb{Z}/p\mathbb{Z}$, where p is prime.

$\triangleright$ $A_n, n \geq 5$.

$\triangleright$ $\mathrm{SL}_n(\mathbb{F})/\pm I_n$ ($n \times n$ matrices of determinant 1 with entries in a finite field $\mathbb{F}$, under the identification $A \leftrightarrow -A$), except for $n = 2$ and $\mathbb{F} = \mathbb{F}_2, \mathbb{F}_3$.

$\triangleright$ Similar families arising from other matrix groups.

$\triangleright$ 26 *sporadic groups*. The really difficult part was to prove that there are finitely many groups not following into the previous systematic lists and to find them all, not knowing a priori their number.

At least 3 sporadic groups come from the Leech lattice; they are denoted Co_1, Co_2, Co_3 and are called the Conway groups. Inside the automorphism group of the Leech lattice - which is a group with 8,315,553,613,086,720,000 elements - one consider the subgroup Co_1 that fixes a vector of length 2, Co_2 that fixes a vector of length 4 and Co_3 that fixes a vector of length 6. They have orders $4157776806543360000, 42305421312000$ and 495766656000, respectively. In fact, $\mathrm{Aut}(\mathbb{L})$ has 12 sporadic subgroups as subquotients!

• Lattices and number theory

Let $\mathscr{L} \subset \mathbb{R}^n$ be an integral lattice - a lattice such that $\|x\|^2$ is an integer for every $x \in \mathscr{L}$. We can then create a theta function

$$\Theta_L(q) = \sum_{m=0}^{\infty} r(m) q^m,$$

where q is a free variable and

$$r(m) = \sharp\{x \in \mathscr{L} : \|x\| = m\}.$$

It turns out that Θ_L is a very special type of generating series. It is a *modular form* - one of the main objects of number theory. Modular forms are such generating series that have a huge amount of inner symmetries. One implication of that is that the knowledge of the first few coefficients of Θ_L allows determining the rest of the coefficients of Θ_L without actually calculating the numbers $r(n)$ and often in a closed form formula. How many coefficients are needed is a function of the volume of the fundamental parallelotop of $\mathscr{L}$ and of n, but in particular one finds that if two integral lattices (possibly of different dimension) have the same number of vectors of length m for $m = 1, \ldots, M$ (where M can be effectively calculated) then they have the name number of vectors of length m for any m.

• Lattices in higher dimensions

Are there more wonderful lattices, in higher dimensions?

The sum of it is that we know very little about lattices in higher dimensions. If one restricts attention to even unimodular lattices, i.e. to lattices of volume 1 in which every vector has even integral norm, and if one weighs the lattices with weights $\frac{1}{\sharp \mathrm{Aut}(\mathscr{L})}$ then we have:

Theorem (Siegel-Minkowski) *The weighted sum of isomorphism classes of even unimodular lattices in* $\mathbb{R}^{2k}$ *is*

$$\sum_{\mathscr{L}/\cong} \frac{1}{\mathrm{Aut}(\mathscr{L})} = \frac{|B_k|}{2k} \prod_{j=1}^{k-1} \frac{|B_{2j}|}{4j} = 2 * \zeta(1-k) * \prod_{j=1}^{k-1} \zeta(1-2j),$$

where ζ *is the Riemann zeta function.*

One knows that there is a unique even unimodular lattice of dimension 8 up to isomorphism, the E_8 lattice, and one finds:

$$\sharp\mathrm{Aut}(E_8) = 696729600,$$

Note that the l.h.s. in the theorem is less or equal to the number of lattices. Here is the growth of the l.h.s. - the Siegel-Minkowski constant.