Sphere Packing, Lattices, and Groups

— Notes —

1. Sphere Packings and Kissing Numbers

1.1 The Sphere Packing Problem

1.1.4. n-Dimensional Packings

Definition. The **fcc** lattice is the face-centered cubic lattice.

Definition. A lattice Λ has a **dual** lattice Λ^* given by

$$\Lambda^* := \{x : \forall u \in \Lambda, x \cdot u \in \mathbb{Z}\} .$$

For example, the dual of the fcc lattice is the **body-centered cubic** lattice (bcc lattice). If A is a Gram matrix for Λ, then Λ^* has Gram matrix A^{-1}.

Why is is finding dense packings in n-dimensions interesting?

1. Interesting problem in pure geometry. Hilbert mentioned it in 1900 in his ist of open problems [Hil1], [Mil5].

2. Has (sometimes unexpected) connections to other branches of mathematics. For example, the densest lattice packings in up to 8 dimensions belong to the families A_n, D_n, E_n and the corresponding Coxeter-Dynkin diagrams turn in several seemingly unrelated areas.

3. The Leech lattice in 24 dimensions, Λ_{24}, has mysterious connections with hyperbolic geometry, Lie algebras, and the Monster simple group.

4. There are direct applications of lattice packings to number theory e.g. solving Diophantic equations and the "geometry of numbers." [Cas2], [Gru1], [Gru1a], [Han3], [Hla1], [Hla3], [Kel1], [Min4], [Min6]. (See subsection 2.3.)

5. There are practical applications of sphere packings to digital communications (see section 3).

6. 2- and 3-dimensional spheres have many practical applications in general e.g. positioning optical fibers in the cross-subsection of a cable [Kin1], chemistry, physics, antenna design, X-ray tomography, and statistical analysis (on spheres).

7. n-dimensional packings may be used in the numerical evaluation of integrals, either on the surface of a sphere in $\mathbb{R}^n$ or its interior. (See subsection 3.2.)

8. Dual theory and superstring theory in physics have made use of E_8 and Λ_{24} lattices and their related Lorentzian lattices in dimensions 10 and 26 discussed in sections 26 and 27.

1.1.5. Summary of Results in Sphere Packing

1.2. The Kissing Number Problem

1.2.1. The Problem of the Thirteen Spheres

The **kissing problem** is the question of how many equally-sized spheres can touch one central sphere. Leech proved that in three dimensions the answer is 12 [Lee2]. (See also [Boe1], [Was1]). The problem is so difficult because the 12-arrangement is not unique - in fact there are infinitely many ways to arrange 12 billiard balls around one central one. For example, the 12 balls can be placed at positions corresponding to the vertices of regular icosahedron concentric with the central ball, where the twelve out balls do not touch each other and may all be moved freely.

1.2.2. Kissing Numbers in Other Dimensions

The **kissing numer**, denoted τ, of a sphere packing in any dimension is the number of spheres that touch a given sphere. For a lattice packing, τ is the same for each sphere. For an arbitrary packing, τ may vary from sphere to sphere.

1.2.4. The Construction of Spherical Codes from Sphere Packings

Let Λ be a sphere packing in $\mathbb{R}^n$ and let the origin be convenient point P (usually the center of a sphere). Suppose there are N spheres in Λ with centers at distance u from P. Then these centers, when rescaled by dividing them by u, form an n-dimensional spherical code of size N. In other words, we take a *shell* of points around P as the spherical code [Slo12].

The distance between the centers of the spheres is at least 2ρ (where ρ is the radius of a sphere), so hte minimal angle in this code is at least $2\sin^{-1}(\rho/u)$. The number of points in this code is given by the theta series of the packing with respect to P (see subsection 2.3).

Example. Consider the lattice D_4, with the origin point P at a lattice point and $\rho = 1/\sqrt{2}$. The first shell has $u = \sqrt{2}$ and contains 23 centers (the kissing number), and the corresponding spherical code consists of the points $2^{-1/2}(\pm 1, \pm 1, 0, 0)$ with the minimal angle $2\sin^{-1}(1/2) = 60°$. The second shell has $u = 2$ and also contains 24 points, and the spherical code is $60°$, so in this case (53) does not given the exact value of ϕ. In fact this second code is a rotation of the first. Both examples show that $A(4, 60°) \geq 24$.

Alternatively, we can consider a **deep hole** $P = (1, 0, 0, 0)$ which yields a different sequence of spherical codes. The first shell contains 8 points at distance 1 from P, forming a code of minimal angle 90° (the vertices of a regular 4D generalized octahedron). Thus $A(4, 90°) \geq 8$. The number of points in these two families of spherical codes are the coefficients of the theta series $(1/2)(\theta_3(2z)^4 + \theta_4(2z)^4)$ and $(1/2)\theta_2(2z)^4$ respectively (see subsection 4.7).

1.2.5. The Construction of Spherical Codes from Binary Codes

Let C be a binary error-correcting code (see subsection 3.2) of length n, and minimal distance d. A spherical code is obtained by changing the 1s to -1s and the 0s to $+1$s in every codeword, and dividing by $\sqrt{n}$. The resulting points lie on Ω_n and the minimal angle is given by

$$\phi = \cos^{-1}\left(1 - \frac{2d}{n}\right)$$
$$\frac{d}{n} = \sin^2\frac{\phi}{2}$$

Example. The code containing all 2^n binary vectors of length n produces the spherical code consisting of all vertices $n^{-1/2}(\pm 1, \ldots, \pm 1)$ of an n-dimensional cube. Any other spherical code obtained by the construction is a subset of this. Importantly the **Golay code**, $\mathcal{C}_{24}$, with $n = 24$,

$d = 8$ produces a spherical code containing 4096 points of Ω_{24} with $\phi = \cos^{-1}(1/3) \approx 70.529°$. Thus $A(24, \cos^{-1}(1/3)) \geq 4096$ (see subsection 3.2.8.2).

5. Sphere Packing and Error-Correcting Codes

Definition. The **coordinate array of a point** $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ is obtained by writing the binary expansion of the coordinates x_i in column, beginning with the least significant digit [Lee5, Section 1.42]. The nth row corresponds to the 2^{n-1}th place. For examples, the coordinate array of $(4, 3, 2, 1, 0, -1, -2, -3)$ is

see display (1)

2.2. Construction A

Let C be an (n, M, d) binary code. The following construction specifies a set of centers for a sphere packing in $\mathbb{R}^n$.

Definition. **Construction A**: $x = (x_1, \ldots, x_n)$ is a center if and only if the 1s row of the coorinate array of x is in C. A lattice packing is obtained only if C is a linear code.

On the unit cube at the origin,

$$\{0 \leq x_i \leq 1 : i \in \{1, \ldots, n\}\},$$

the centers are exactly the M codewords. All other centers are obtainedby adding even integers to any of hte coordinates of a codeword. This corresponds to shifting the unit cube by two in any direction. Thus all centers are obtainedby repeating a building block consisting of a $Q_2 := 2 \times \cdots \times 2$ cube with codewords marked on teh vertices of the $Q_1 := 1 \times \cdots \times 1$ cube in one corner.

Each copy of Q_2 constributes M spheres of radius ρ (say), so the center density obtained from construction A is

$$\delta = M\rho^n 2^{-n}$$

If two distinct centers are congruent to the same codeword their distance is a least 2. If they are conguent to different codewords, then their distance is at least 1 in at least d places, so are at least $\sqrt{d}$ apart. Thus the radius of the spheres are

$$\rho = (1/2) \min \left\{2, \sqrt{d}\right\}.$$

2.2.3. Kissing Numbers

Let S be a sphere with center x, where x is congruent to the codeword c. Candidates for centers closest to x are as follows:

(a) There are $2n$ centers of the type $x + ((\pm 2)0^{n-1})$ at a distance 2 from x.

(b) Let $\{A_i(c)\}$ be the weight distribution of C with respect to c (section 2.2 in chapter 3). Since there are $A_d(c)$ codewords at distance d from c, there are $2^d A_d(c)$ centers the type $x + ((\pm 1)^d 0^{n-d})$ at a distance $\sqrt{d}$ from x. Therefor the number of spheres touching S, the kissing number of S, is

$$\tau(S) = \begin{cases} 2^d A_d(c) & \text{if } d < 4 \\ 2n + 16A_4(c) & \text{if } d = 4 \\ 2n & \text{if } d > 4 \end{cases}$$

2.2.4. Dimensions 3 to 6

3. Codes, Designs and Groups

3.1. The Channel Coding Problem

THEOREM 1.1. **The Sampling Theorem**. If $f(t)$ is a signal containing no components of frequency greater than W cycles per second, then $f(t)$ is completely specified by its samples

$$\ldots, f\left(-\frac{1}{2W}\right), f(0), f\left(\frac{1}{2W}\right), f\left(\frac{2}{2W}\right), \ldots$$

which are taken every $1/(2W)$ seconds [Lee0]. The **cardinal series** describes $f(t)$ in terms of its sample values:

$$f(t) = \sum_{k=-\infty}^{\infty} f\left(\frac{k}{2W}\right) \frac{\sin 2\pi W(t - l/(2W))}{2\pi W(t - l/(2W))}$$

The **energy** in $f(t)$ is given by

$$\int_{-\infty}^{\infty} f(t)^2 dt = \frac{1}{2W} \sum_{-\infty}^{\infty} f\left(\frac{k}{2W}\right)^2$$

The sampling theorem is the basis for the digital transmission system **pulse code modulation (PCM)**. It is an alternative to **amplitude modulation (AM)** and **frequency modulation (PM)** and is good for medium distance telephone calls.

If the signal $f(t)$ lasts for T seconds, then there are $n = 2TW$ samples, e.g.

$$(f(0), f(1/(2W)), f(2/(2W)), \ldots, f((n-1)/(2W)))$$

These are coordinates of n-dimensional space. Thus the sampling theory yields that $f(t)$ can be represented by a single point $F \in \mathbb{R}^n$. Additionally, the norm of F is the energy in $f(t)$:

$$N(F) = F \cdot F = 2W \int_0^T f(t)^2 dt = 2WTP = nP$$

where

$$p = \frac{1}{T} \int_0^T f(t)^2 dt$$

is the **average power** in the signal.

3.1.2. Shannon's Theorem

Claude Shannon wrote a paper using all of this called *A Mathematical Theorem of Communication.*

DEFINITION. A **binary symmetric channel** is one in which only sequences of 0s and 1s are transmitted and received.

DEFINITION. A **Gaussian white noise channel** transmits continuous signals. The cutoff frequency of the channel, W is called the **bandwidth**. All frequencies above W are attenuated completely, all below W are passed without attenuation. In the course of transmitting the signal, the channel adds Gaussian white noise to it.

A transmitted signal $f(t)$ is represented by the point $F = (f_1, \ldots, f_n)$. During transmission the point is perturbed by the addition of a noise vector $Y = (y_1, \ldots, y_n)$ whose components are independent Gaussian random variables with mean 0 and variance σ^2. The received signal is represented by $F + Y$.

Definition. The **rate** of the code is defined to be

$$R := \frac{1}{T} \log_2 M \text{ bits per second}$$

The decoder find the closest point to the received vector and from that reconstructs the signal. If the noise is too large, then $F+Y$ may be closer to a different point than F, which results in a decoding error.

A way to reduce the chance of error is to place the code points further apart. However, this requires signals with greater energy and increases the cost of transmission.

Theorem. One of Shannon's basic theorems is that, it turns out, it is possible to construct a decoding scheme that results in negligible error and uses finite power, provided that the rate of the code does not exceed a threshold called the **capacity** of the channel. The statement of the theorem is the following: For any rate R less than the capacity $C = W \log_2 \left(1 + \frac{P}{\sigma^2}\right)$ i.e.

$$R < C = W \log_2 \left(1 + \frac{P}{\sigma^2}\right),$$

then by making T and hence $n = 2WT$ sufficiently large we can find a code of rate R and average power at most P for which the probability of a decoding error is arbitrary small. Conversely, such codes do not exist for $R \gg C$. For a rigorous proof see [Sha2, Sha6].

More precise versions of this theorem show how the probability P_e of a decoding error drops as the dimension n increases, for a fixed rate R.

Additionally, a rigorous proof of the previous theorem shows that for small values of σ, finding an optimal code of maximal power P is closely related to finding the densest packing of spheres in $\mathbb{R}^n$.

3.1.3. Error Probability

Suppose the code consists of M more code points $C_1, \ldots, C_M$ in $\mathbb{R}^n$. Let $V(C_k)$ be the Voronoi cell for C_k. Given that C_k is transmitted, the decoder makes the correct decision if and only if hte noise vector Y is in $V(C_k)$, an even of probability

$$\frac{1}{(\sigma\sqrt{2\pi})^2} \int_{V(C_k)} e^{-x\cdot x/(2\sigma^2)} dx.$$

Assuming that all code points are equally likely to be used, the error probability for this code is

$$P_e = 1 - \frac{1}{M} \sum_{k=1}^{M} \frac{1}{(\sigma\sqrt{2\pi})^2} \int_{V(C_k)} e^{-x\cdot x/(2\sigma^2)} dx$$

If all the Voronoi cells are congruent, say to some polytope Π, this simplifies to

$$P_e = 1 - \frac{1}{(\sigma\sqrt{2\pi})^n} \int_{\Pi} e^{-x\cdot x/2\sigma^2} dx.$$

Then one version of the Gaussian channel coding problem can we stated as the following. Given the dimension n, the number of code points M, and a power constraint

$$N(C_K) \leq nP, k \in \{1, \ldots, M\},$$

find a code $(C_1, \ldots, C_M)$ satisfying the above inequality for which P_e is minimized.

Furthermore, the *constant energy problem* replaces the power constant with the requirement that

$$\forall k : N(C_k) = nP$$

The **lattice version** of the Gaussian channel coding problem is to find, given a value of σ, that n-dimension lattice of determinant 1 for which P_e is minimized, where Π is the Voronoi cell of the lattice with volume 1.

Overall, the lattice problems are described by the following. Let Λ be a lattice with Π of volume 1.

- For the packing problem we maximize the in-radius of Π.
- For the covering problem we minimize the circumradius.
- For the quantizing problem we minimize the escond moment $G(\Pi)$.
- For the channel coding problem we minimize P_e.

3.1.4. Lattice codes for the Gaussian channel

In one dimension, there is only one lattice. In two dimensions, the optimality of the hexagonal lattice for all σ follows by taking $f(x) = (\sigma\sqrt{2\pi})^{-1}\exp\left\{-x^2/(2\sigma^2)\right\}$ in the theorem on page 81 of [Fej101]. In higher dimensions, the problem depends on the value of σ.

Assume σ is small. From equation 20, can approximate P_e by

$$P_e^{-1} = \frac{\tau}{2}\text{erfc}\left(\frac{\rho}{\sigma\sqrt{2}}\right)$$

Let the code consist of all lattice points C with $N(C) \leq nP$. The number of points M is given by

$$M \cdot V_n \rho^n = \Delta \cdot V_n (nP)^{n/2}(1 + o(1))$$

where $o(1) \to 0$ as $M \to \infty$ and Δ is the **lattice density**. So,

$$\rho = \sqrt{nP}\left(\frac{\Delta}{M}\right)^{1/n}(1 + o(1))$$

The average norm of the code points is

$$\frac{n}{n+2} \cdot nP(1 + o(1))$$

Define the **rate** of the code to be

$$R := \frac{1}{n}\log_2 M \text{ bits per dimension}$$

rather than before with $1/T$ and bits per second. Then

$$\rho = \frac{\sqrt{nP}}{2^R}\Delta^{1/2}(1 + o(1))$$

Define also the **normalized signal-to-noise ration** of the code to be

$$S := \frac{P}{2^{2R}\sigma^2} = \frac{P}{M^2\sigma^2}$$

Then finally by combining the last few formulas we have the following estimate for the error of the probability of a Gaussian channel code with normalized signal-to-noise ratio S, obtained from an n-dimensional lattice of density Δ and kissing number τ.

$$P_e'' = \frac{\tau}{2}\left(\sqrt{\frac{nS}{2}}\Delta^{1/2}\right)$$

This estimate gains accuracy with increasing S. For large values of x,

$$\text{erfc}(x) \sim \frac{1}{x\sqrt{\pi}}e^{-x^2}$$

and therefor

$$\log P_e'' \sim \text{ constant } - \left(\frac{1}{2}n\Delta^{2/n}\log e\right)S$$

Figure 3.3: graph of smallest known noise ratio for various lattices as a function of S

Also shown some exact results for various low dimensional lattices using Monte Carlo integration (in section 3).

3.2. Error-correcting Codes

3.2.1. The error-correcting code problem

The other idealized model for a channel was the **binary symmetric channel**, where the input and output symbols are 0s and 1s, and there is some fixed probability $p < 1/2$ that when a 0 or 1 is transmitted, the other symbol is received. A **binary code** C of length n is a set of binary vectors (called **codewords**) with n coordinates, or in other words is a subset of $\mathbb{F}_2^n$ where $F_2 = \{0, 1\}$ is the Galois field of order 2.

Definition. A **q-ary** code is a subset of $\mathbb{F}_q^n$ where q is a prime or prime-power. Besides $\mathbb{F}_2$, $\mathbb{F}_3 = \{0, 1, -1\}$ and $\mathbb{F}_4 = \left\{0, 1, \omega, \omega^2\right\}$ are especially interesting.

Definition. The **Hamming distance** between two vectors $u, v \in \mathbb{F}_q^n$ is defined to be the number of coordinates where they differ, i.e.

$$d(u, v) := |\{i : u_i \neq v_i\}|$$

The **(Hamming) weight** $wt(u)$ of a vector u is the number of nonzero coordinates u_i; therefor

$$d(u, v) = wt(u - v)$$

The **minimal distance** d of a code is

$$d = \min\{d(u, v) : u, v \in C \wedge u \neq v\}$$

If a code has minimal distance d, the **Hamming spheres** of radius $\rho = [(1/2)(d-1)]$ around the codewords are disjoint and therefor the code can correct ρ errors. Note that ρ is the packing radius of the code. A code length n, containing M codewords and with minimal distance d is said to be a (n, M, d) code.

Definition. A **linear** (or **group**) code C is a linear subspace of $\mathbb{F}_q^n$: the set of codewords is closed under vector addition and coordinate-wise multiplication of this space, and there are q^k codewords. The rate of the code is

$$R = \frac{1}{n} \log_2 M = \frac{k}{n} \log_2 q \text{ bits per symbol.}$$

A linear code of length n, dimension k and minimal distance d is said to be a $[n, k, d]$ code. the minimal distance of a linear code is the minimal nonzero weight of any codeword:

$$d = \min\{wt(u) : u \in C \wedge u \neq 0\}$$

Definition. The **error-correcting code problem** is the following: given n and d, find the maximal number of of codewords in any (n, M, d) code, called $A(n, d)$. A good code has n small (reduces delays), M large (to make efficient use of the channel), and d large (to correct many errors). But these features trade off with each other. There is a similar problem for linear codes. The general problem is unsolved, but upper and lower bounds on $A(n, d)$ have been found.

Table 9.1 in Chapter 9 of the found $A(n, d)$

3.2.2. Further definitions from coding theory

More definitions and various specific constructions.

3.2.8. Quadratic Resudue Codes

Let p, n be primes such that p is a square mod n. For $p = 2$, n is a prime of the form $8m \pm 1$ i.e. $n \equiv_8 \pm 1$. The **quadratic residue** code of length n over F_p is the cyclic code whose generator polynomial has roots

$$\{\alpha^i : i \neq 0 \text{ is a square mod } n\}$$

References: [Lin11], [Mac6, Chapter 16], [Leo5, Leo6]. The dimension of this code is $(n+1)/2$. The extended quadratic residue code is obtained by appending a zero-sum check digit. If n is of the form $4a-1$, then the extended code is self-dual. In particular, extended binary quadratic residue odes of length $8m$ are self-dual Type II codes.

Examples. Some examples.

The Golay codes are studied in more detail in Chapters 10 and 11.