06/07/2017 COHN THE MATHEMATICAL PACKING PROBLEM. Lecture Notes PCMI 2014

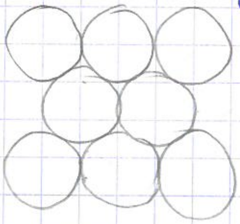
We are going to consider sphere packing, identical · perfect spheres → easiest non trivial problem.

We are going to consider arbitrary dimensions $\mathbb{R}^n$ – (rk: applications for information theory).

INTRODUCTION

→ Problem: maximize density of spheres, that can be tangent but are not allowed to overlap! (= fraction of space covered).

$2d/\mathbb{R}^2$:

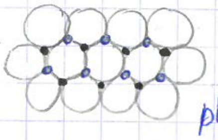


→ optimal packing, proof by Thue 1892
this pretty well understood because in 2d there is no geometrical frustration (local vs global way to behave in competition).

(hexagonal)

Rk: boundary conditions are not so important, think of torus which size would go to infinity, infinite space...

$\mathbb{R}^3$: Kepler conjecture (pile of oranges) → stack 2d hexagonal layers.
(2 ways to choose how to position a layer above another
↳ many ≠ packings of identical density corresponding to the ≠ choices of positioning successive layers.



place additional layer over { blue / black

→ Not at all obvious to prove, although done (Hales 1998, 2014).
Because there is here frustration, so not very understandable proof (eg: max 12 neighbors, although to obvious

So what do we know: solutions for $n = 1, 2, 3, 8, 24$
8 → 2016 Viazovska
24 → 2016 Kumar, Miller-Ro... , Viazovska, Cohn.

For arbitrary dimension: $\frac{\text{upper bound}}{\text{low bound}}$ grows exponentially with the dimension.
↓
and this is because any how, a 1% change in distance → 1.01^n change in volume → density → scaling problem.

Surprisingly, each dimension behaves a bit differently → even at the non rigorous level no intuition from one to the other...

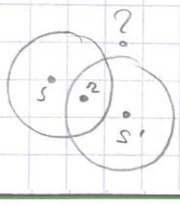
MOTIVATION

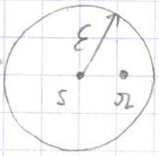
A Motivation to study sphere packing is that they can be seen as ERROR CORRECTING CODES.

n measurements (signal) $s \in \mathbb{R}^n$ → communication channel (noisy) → $r \in \mathbb{R}^n$ received.

↳ measure of the noise level $\|r - s\| < \varepsilon$

Pictorial view:





error ball surrounding each possible signal
↳ We see that we wish for these not too overlap so that we do not make mistaken in interpreting r.

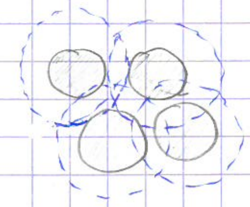
Shannon 1948 → consider a finite set of signals, which error balls don't overlap
↳ unambiguous decoding.
→ still we want to maximize the density. ↳ maximize communication rate -

A PROOF

Why does there exist good packings in high-dimension? A proof of a lower bound:

THEOREM: maximum density in n-dimension $\geq 2^{-n}$

PROOF: • Take any saturated packing (impossible to add a sphere)
• Doubling the radius results in a complete coverage → multiply volume covered by 2^n

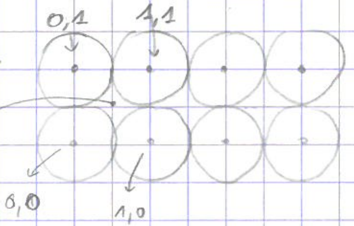


$\Rightarrow V \times \text{density} \times 2^n \geq V$

$\Rightarrow \text{density} \geq 2^{-n}$

▨

RK: The square packing is not saturated in high dimension.



(saturated in 2d).

hole at $(1/2, 1/2, \dots 1/2)$.

$\Rightarrow$ distance from $(0,0) \to \sqrt{(1/2)^2 + \dots + (1/2)^2} = \frac{\sqrt{n}}{2}$!!

$\Rightarrow$ not saturated for $\frac{\sqrt{n}}{2} \geq 1 \to n \geq 4$ -

$\mathbb{Z}^n$ density $= \frac{\pi^{n/2}}{(n/2)!} \frac{1}{2^n}$ ↳ volume of a sphere of $r = 1/2$

07/07/2017

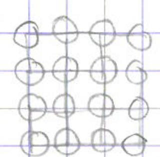
lower bounds: density $\geq c n 2^{-n}$
(sometimes $\log\log n$)

lower bounds: density $\leq 2^{-0{,}599n}$

↘ We don't know if optimal packings should be perfect cristals, or ~~look~~ more random..
We don't know if an exponential improvement is possible?

HOW CAN WE DESCRIBE PACKINGS?

maths	lattice	periodic packing
physics	Bravais lattice	lattice -



Bravais lattice: basis $v_1, \dots v_n$ for $\mathbb{R}^n$
center of the spheres at $a_1 v_1 + \dots + a_n v_n$, $a \in \mathbb{Z}^n$.

what is the density of Bravais lattice?
→ packing radius = half minimum vector length
→ volume of fundamental cell = |det(basis)|

$\Rightarrow \text{density} = \frac{\text{volume sphere}}{\text{volume fund. cell}}$

The basis given, need not be $v_1 = (1, 0, 0..)$ etc.. In practice for the skewed lattice, this is very hard to compute.
Finding the minimum vector length for the given basis is NP hard problem as $n \to +\infty$.

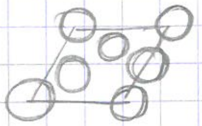
Are lattices optimal?
_ Well they are incredibly constrained { n^2 parameters to adjust the lattice
{ exponential number of holes that you might want to try to fill.

↳ CONJECTURE: In sufficiently large dimension, there is no saturated Bravais lattice -
↳ think 1000.
(e.g. 13-dim best known packing on a Bravais lattice).

If they are not satured, they must be at least by a factor of 2 suboptimal.

↳ Bravais lattice are not good, but easy for us to handle...

<u>Periodic packing</u> := union of translate of a Bravais lattice
= translation of fondamental cell.



↳ come arbitrarly close to optimal density ≡ anything can be approximated periodically

↳ big enough box of original packing
↳ share spheres on the edges
↳ repeat
⟹ approximation of the density will be better and better the bigger the box gets.
(in the limit → ∞, we loose periodicity)

↳ <u>but</u> do periodic packings achieve exactly the optimal density?

<u>e.g</u> Best known packing in $\mathbb{R}^{10}$ is periodic with 40 parts / cell, 8% denser than any bravais lattice.

A COMPUTATIONAL PROBLEM : FINDING SHORT VECTORS

1* Can we take advantage of the computational criptography?

↳ handfull of mathematical problem are really well-suited for public-key encryption (almost no chance of people breaking them by tomorrow).

↳ factoring, discrete logarithm.. → YET, could be broken by quantum computers
lattices → <u>quantum secure</u>?

Goldreich - Goldwasser - Halevi (Don't use :))
↳ How to encode messages using packings?

PUBLIC KEY (encryption)
everybody can send me a message ⟹ PRIVATE KEY (decryption)
only I can read it

= BRAVAIS LATTICE BASIS.
(ugly basis)

= SECRET <u>NEARLY</u> ORTHOGONAL BASIS for same lattice.

And a message ≡ lattice point $\xrightarrow{\text{encrypt.}}$ perturb point off the lattice

decrypt. what is the nearest lattice point? → very hard to solve straight away
→ much easier with a nearly orthogonal basis.

2* Embedding numbers recognition in the short vector problem:

do you recognize: $\alpha = -7,8264609923767...$? close rational?
eg: $0,1345345345345 \simeq \frac{1}{10} + \frac{345}{9990}$

→ in particular, recognize algebraic numbers ≡ roots of polynomial equations of integer coefficients

↳ Mapping to sphere packing

. consider a very big constant $C = 10^{20}$
. consider the basis: $(1, 0, 0, 0 \dots, C)$
$(0, 1, 0, 0 \dots, C\alpha)$
$(0, 0, 1, 0, \dots, C\alpha^2)$

↳ Bravais lattice: $\sum a_i v_i = (\underbrace{a_0, a_1, \dots}_{\text{pretty small}}, \underset{\text{huge}}{C} \underbrace{\sum_i a_i \alpha_i^i}_{\text{that we would wish to be tiny to have a short vector!}})$

⇒ find $\{a_i\}$ so that last ≈ 0, α approximate root ≡ find simplest polynom. find density of Bravais lattice.

in our example of 6 dimensional lattice embeded in 7-dimension:
$C_5(a_0, a_1, \dots; a_0 + \dots + a_5\alpha^5) = (71, -5, 12, -19, 132, 0.000004..)$

ELEMENTS OF BOUNDS COMPUTATIONS.

1 * pair correlation function = "number of times pairwise distances occur"

↳ Fourier transform: structure factor $\geqslant 0$ → constraints on plausible pair correlation functions → bounds by showing that could not be improved without structure factor going below zero.

↓ determines packing density

→ argument working in 1, 2 ? (can't prove it!), 8, 24.

2. Recall the Fourier transform: $f: \mathbb{R}^n \to \mathbb{R}$, $\hat{f}(t) = \int_{\mathbb{R}^n} f(x) e^{2\pi i \langle t, x\rangle} dx$.

Poisson summation: Consider Bravais lattice Λ in $\mathbb{R}^n$, $\sum_{x \in \Lambda} f(x) = \frac{1}{\underset{\text{fundamental cell lattice}}{\mathrm{Vol}(\mathbb{R}^n/\Lambda)}} \sum_{\underset{\text{dual lattice}}{\Lambda^*}} \hat{f}(t)$

Theorem (Cohn Elkies 2003): let $f: \mathbb{R}^n \to \mathbb{R}$ (nice) s.t. $\begin{cases} f(x) \leq 0 & \text{for } \|x\| \geqslant 2 \\ \hat{f}(t) \geqslant 0 & \forall t \text{ and } \hat{f}(0) = 0 \end{cases}$

then the sphere packing density in $\mathbb{R}^n \leqslant \frac{\pi^{n/2}}{(n/2)!} \frac{f(0)}{\hat{f}(0)}$.

PROOF FOR BRAVAIS LATTICES: Bravais lattice $\Lambda \subseteq \mathbb{R}^n$ with minimum vector length 2 (unit spheres).

$f(0) \geqslant \sum_{x \in \Lambda} f(x) = \frac{1}{V} \sum_{t \in \Lambda^*} \hat{f}(t) \geqslant \frac{\hat{f}(0)}{V}$ → $\frac{1}{V} \leqslant \frac{f(0)}{\hat{f}(0)}$ yet, density $= \frac{\pi^{n/2}}{(n/2)!} \frac{1}{V}$ ∎

Rk: taking beautiful duality and throwing all the complicated.
→ no other choice, we don't know about all the nontrivial terms
→ we might be lucky enough that actually those terms are decaying fast, and we are not loosing much!