We are going to consider sphere packing, identical sphere packing: trivial problem.

We are going to consider arbitrary dimensions $\mathbb{R}^n$.

**INTRODUCTION**

Problem: maximize density of spheres that can be tangent but are not allowed to overlap.

- Problem: $\frac{2d}{d^2}$ (fraction of space covered).
- Problem: optimal packing, proved by Thue 1932.
- Problem: not very well understood because in 3d there is no geometrical frustration (local vs. global way to behave in competition).

As boundary conditions are not so important, think of torus which we would go to infinity, infinite space...

$\mathbb{R}^3$: Kepler conjecture (pile of oranges) → stack 2d hexagonal layers.
- Problem: to distort how to position a layer above another.
- Problem: many packings of identical density corresponding to ($n, \pi, \alpha$) choices of positioning.

So what do we know: solutions for $n = 2, 3, 8, 24$.

For arbitrary dimension: upper bound grows exponentially with the dimension.

and this is because any layer, a $\mathbb{R}^d$ change in distance $\rightarrow 10^n$ change in volume $\rightarrow$ density $\rightarrow$ scaling problem.

Surprisingly, each dimension behaves a bit differently — even at the non-geometrical 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 $\rightarrow$ communication channel $\rightarrow n \in \mathbb{R}^n$ received.
- Many measurements $\rightarrow$ many $n \in \mathbb{R}^n$. Received.
- Average error.
- Error ball surrounding each possible signal.
- We see that we wish for these not too overlap so that we do not make mistakes in interpreting it.
1948 → consider a finite set of signals, which can be balls, don’t consider
unambiguous decoding → still want to maximize the density. I.e. maximize communication rate.

**A Proof**

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

**Theorem:** Maximum density in n-dimension $\leq 2^{-n}.$

**Proof:** Take any saturated packing (impossible to add a sphere).

1. Multiplying the radius results in complete coverage → multiply volume covered by $2^n$ balls.
2. $V_x$ density $\leq 2^{-n}$ → $V_x.$
3. $V$ density $\leq 2^{-n}$ → $\frac{\sqrt{m}}{2}.$

Pl. The square packing is not saturated in high dimension.

- Hole of $(\frac{\sqrt{m}}{2}, \frac{\sqrt{m}}{2}, \ldots, \frac{\sqrt{m}}{2}).$
- Distance from $(0, 0) \geq \sqrt{\left(\frac{\sqrt{m}}{2}\right)^2 + \ldots + \left(\frac{\sqrt{m}}{2}\right)^2} = \frac{\sqrt{m}}{2}.$

- Not saturated for $\frac{\sqrt{m}}{2} \geq 2 \rightarrow m \geq 4.$

**Lower bounds:**
- density $\geq \frac{1}{\log n}$ (sometimes loglog). (saturated in 2d)
- density $\leq 2^{-0.5 \sqrt{n}}$

We don’t know if optimal packings should be perfect crystals, or if they should random. Improvement is possible?

**How can we describe packings?**

- [Maths, Lattices, Periodic Packings]
- [Physics, Bravais Lattices]

- Bravais lattice: basis $v_1, \ldots, v_n$ for $\mathbb{R}^n.$

- Centers of the spheres at $\alpha v_1 + \ldots + \alpha v_n,$ $\alpha \in \mathbb{Z}^n.$

- What is the density of Bravais’s lattice?

- Packing radius = half minimum vector length → density = volume sphere / volume fundamental cell.

The basis given need not be $v_i = (1, 0, 0, \ldots)$ etc. In practice for the skew we... lattice it is very hard to make.

Finding the minimum vector lengths for a given basis is NP hard problem.

- Are lattices optimal?

- Well, they are incredibly constrained: many parameters to adjust the lattice, and exponential number of holes that you might want to try to fill.

**Conjecture:** in sufficiently large dimension, there is no saturated Bravais’s lattice.
If they are not solvable, they must be at least a factor of 2 suboptimal.

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

Periodic packing: union of translates of a Bravais lattice
= translation of fundamental cell.

come arbitrarily close to optimal density, anything can be approximated
numerically.

Big enough box of original packing
= slope spans on the edge
= repeat
= approximation of the density will
be better and better, the bigger the
box gets.

In the limit → ∞, we loose periodicity.

but do periodic packings achieve exactly the optimal density?

The best known packing in \( \mathbb{R}^3 \) is periodic with 40 parts/cell, E7 densest any boxed lattice.

**A COMPUTATIONAL PROBLEM: FINDING SHORT VECTORS**

1. Can we take advantage of the computational cryptography?

   A handful of mathematical problems 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 computer
   → quantum secure?

   Goldreich, Goldreich, Halevi (cont.)

   "How to encode messages using packings?"

   \[
   \begin{align*}
   \text{PUBLIC KEY (encryption)} & \quad \text{PRIVATE KEY (decryption)} \\
   \text{everybody can send me message} & \quad \text{only I can read it} \\
   \text{BRAVAIS LATTICE BASIS} & \quad \text{SECRET NEARLY ORTHOGONAL BASIS for same lattice} \\
   \text{(ugly basis)} & \quad \text{(ugly basis)}
   \end{align*}
   \]

And a message = lattice point \( \rightarrow \) 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: \( a = -7,8264609933547 \ldots \)?

   \[
   \begin{align*}
   \frac{19}{10} & = 1 + \frac{9990}{9990} \\
   \end{align*}
   \]
8. Mapping to sphere packing

- Consider a very big constant \( C = 400 \)
- Consider the basis: 
  \[
  \begin{pmatrix}
  4, 0, 0, 0, \ldots, C \\
  0, 1, 0, 0, \ldots, C \\
  0, 0, 1, 0, \ldots, C \\
  0, 0, 0, 1, \ldots, C
  \end{pmatrix}
  \]
  \( \vdots \)

- \( n \) Bravais lattice \( \Sigma = \{ \mathbf{a}_0, \mathbf{a}_1, \ldots, C \Sigma \mathbf{a}_0; \mathbf{c}_0; \mathbf{c}_1; \ldots \} \)

- Find \( \mathbf{a}_0, \mathbf{a}_1 \ldots \mathbf{a}_n \) that had \( \Sigma \mathbf{a}_i = 0 \) a approximate root = find sparse polynomial

- Find density of Bravais lattice

- In our example of 6 dimensional lattice embedded in 3 dimension:
  \[
  C_6(\mathbf{a}_{0}, \mathbf{a}_{1}, \ldots; \mathbf{a}_{0} + \mathbf{a}_{5} \mathbf{a}_{5}) = (37, -5, 12, 19, 18, 2, 0.00000004) .
  \]

**Elements of Bounds Computations**

1. Fourier transform: structure factor \( \neq 0 \) \rightarrow constraints on plausible pair correlation functions \( \rightarrow \) bounds by showing that could not be improved without structure factor going below zero.

- Argument working on \( 1, 2, 3, 8, 24 \).

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

- Poisson summation: Bravais Bravais lattice \( \Lambda \) in \( \mathbb{R}^n \), \( \sum_{x \in \Lambda} f(x) = \frac{1}{\text{Vol}(\mathbb{R}^n)} \sum_{t \in \mathbb{R}^n} \hat{f}(t) \).

**Theorem (John Eklas 2003):** Let \( f: \mathbb{R}^n \rightarrow \mathbb{R} \) (nice) s.t. \( \hat{f}(x) \leq 0 \) for \( \|x\| > 0 \).

- \( \| \hat{f}(t) \| \leq 0 \) \forall t and \( \hat{f}(0) = 0 \)

- Then the sphere packing density on \( \mathbb{R}^n \leq \frac{\mathbb{V}^{n/2}}{V} \frac{\mathbb{S}^{n/2}}{V} \).

**Proof for Bravais Lattices:** Bravais lattice \( \Lambda \subset \mathbb{R}^n \) with minimum vector length \( \delta \) (sphere).

\[
\frac{1}{V} \sum_{x \in \Lambda} f(x) \leq \frac{1}{V} \sum_{z \in \mathbb{Z}^n} \hat{f}(z) \rightarrow \frac{1}{V} \frac{\hat{f}(0)}{\mathbb{S}^{n/2}} \frac{\mathbb{V}^{n/2}}{V} \frac{\mathbb{S}^{n/2}}{V} \]

- \( f(x) \): Taking beautiful duality and throwing all the complicated:
- \( \delta \): Other choices, we don't know about all the nontrivial terms
- We might be lucky enough that actually these terms are decaying fast, and we are not losing much!