

LATTICES: MATHEMATICAL BACKGROUND

PHONG NGUYEN

<http://www.di.ens.fr/~pnguyen>

September 2026

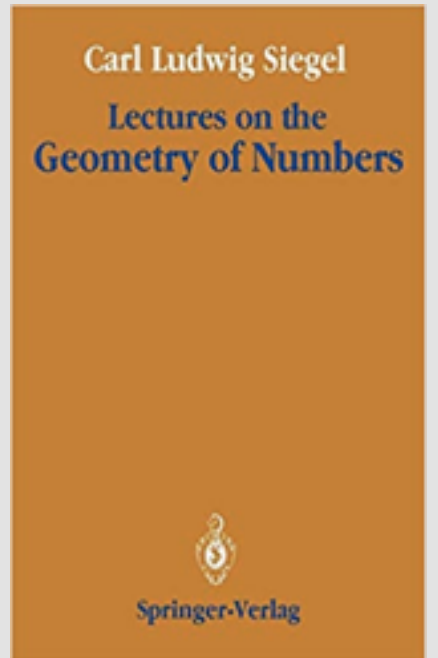


ADVICES

- **Interaction:** please ask questions during my talks; interruptions are welcome.
- **Implementation:** to understand an algorithm, it is helpful to implement it: sage, NTL, fplll, etc.

MATH REFERENCES

- Siegel's Lectures on the Geometry of Numbers (Springer).

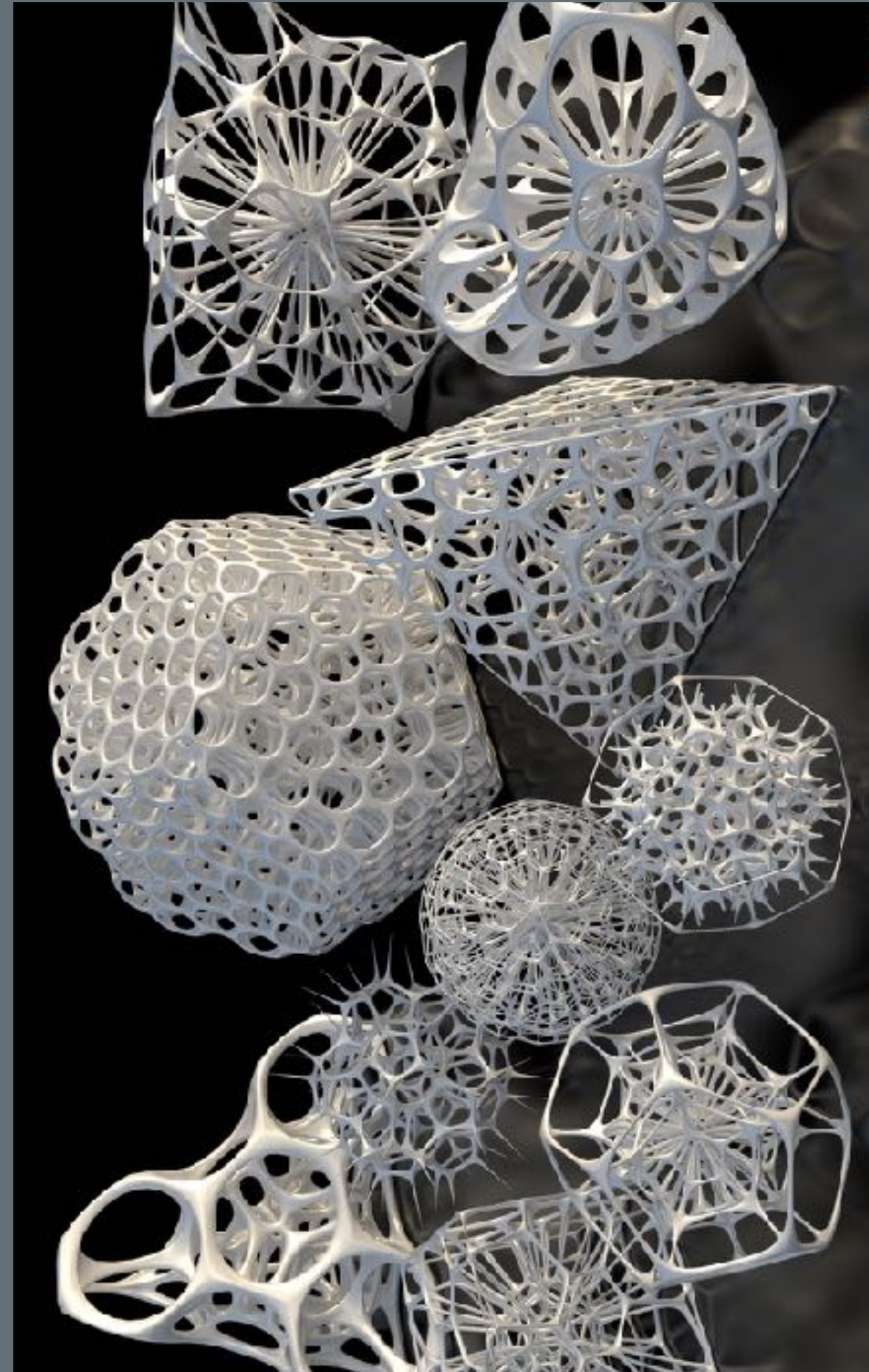


- Venkatesh's Stanford lecture notes on geometry of numbers

TODAY: LATTICES MATHEMATICAL BACKGROUND

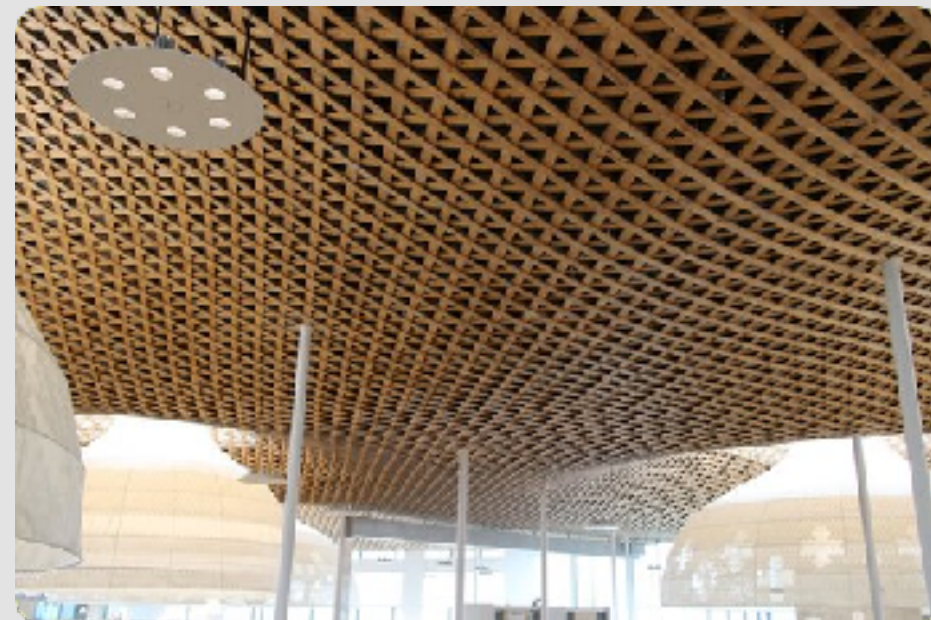
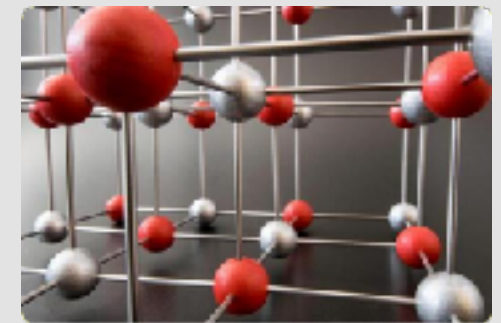
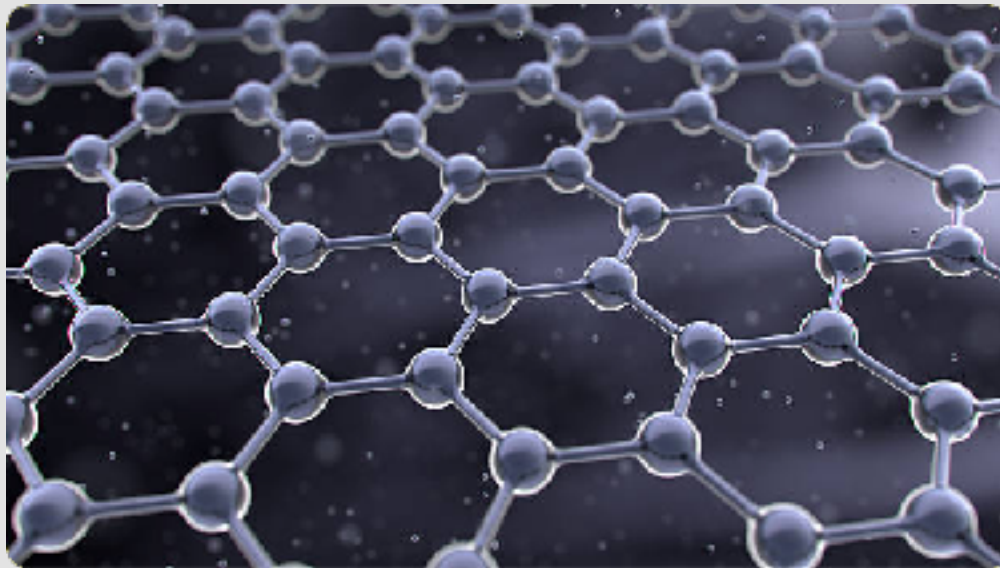
- **What is a lattice?**
- **Characterization of lattices**
- **Counting lattice points**

WHAT IS LATTICE?



WHAT IS A LATTICE?

- An **infinite** arrangement of “**regularly spaced**” points



WHAT IS A LATTICE?

- A linear deformation of $\mathbf{Z}^n$.
 - Let B be a non-singular $n \times n$ matrix.
 - The **lattice** spanned by the basis B is $L = \mathbf{Z}^n B$.

2	0	0	0	0
0	2	0	0	0
0	0	2	0	0
0	0	0	2	0
1	1	1	1	1

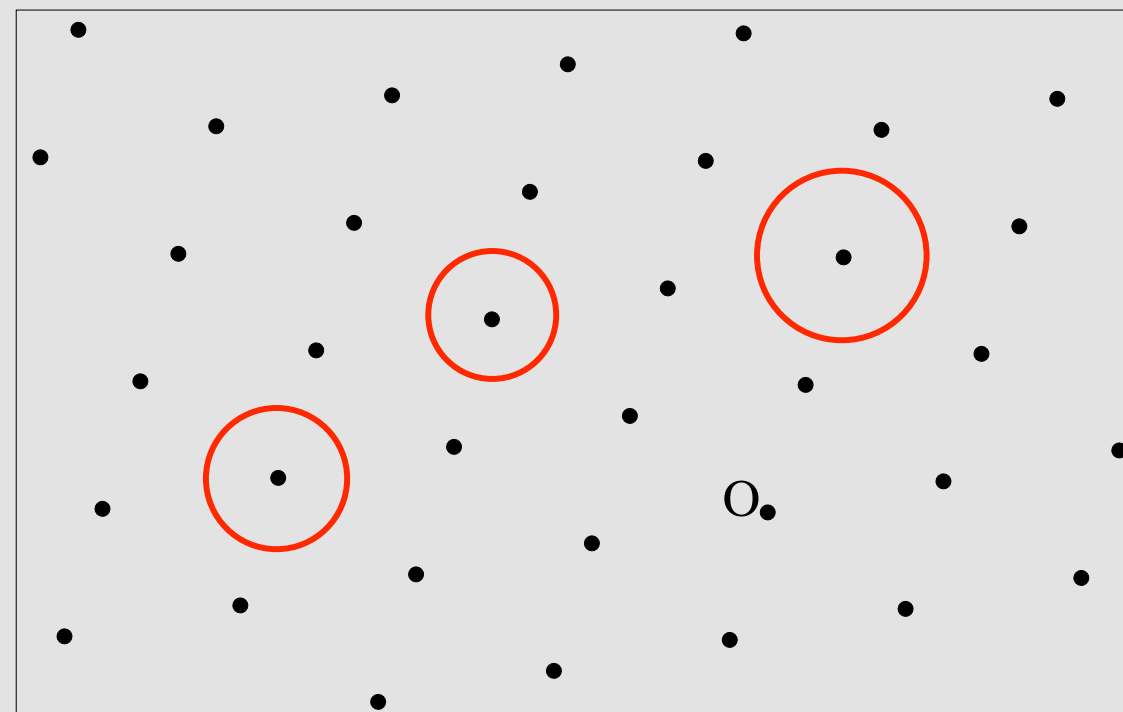
EUCLIDEAN LATTICES

- Consider $\mathbf{R}^n$ as a Euclidean space: let $\langle u, v \rangle$ be the dot product
 $\|\vec{w}\|$ be the norm.

- A **lattice** is a discrete subgroup L of $\mathbf{R}^n$:

$$\forall v \in L \exists r > 0 \text{ s.t. } L \cap \text{Ball}(v, r) = \{v\}$$

$$\dim(L) = \text{rank}(L) = \dim(\text{span}(L))$$



- Ex: $\mathbf{Z}^n$ and its subgroups.

EXERCISES

- Show that for any lattice L of $\mathbf{R}^n$:
 - $\exists r > 0$ s.t. $\forall v \in L, L \cap \text{Ball}(v, r) = \{v\}$.
 - L is closed: the limit of any convergent sequence stays in L .
 - $\forall r > 0$ and $x \in \mathbf{R}^n$, $L \cap \text{Ball}(x, r)$ is finite. In particular, L has **shortest non-zero vectors**.
 - L is countable.

EXAMPLES

- Let L and L' be lattices in $\mathbf{R}^n$.
- Let E be a subspace of $\mathbf{R}^n$.
 - Is $E \cap L$ a lattice?
 - Is $L \cap L'$ a lattice?
 - Is $L \cup L'$ a lattice?

NOTATION: LINEAR COMBINATIONS

- For any vectors $b_1, \dots, b_n \in \mathbf{R}^m$,
let $L(b_1, \dots, b_n)$ denote their $\mathbf{Z}$ -span.
- $L(b_1, \dots, b_n) = \mathbf{Z}b_1 + \dots + \mathbf{Z}b_n = \{ x_1b_1 + \dots + x_nb_n \text{ where each } x_i \in \mathbf{Z} \}$

QUESTION 1

- If $b_1, \dots, b_n \in \mathbb{Z}^m$, is $L(b_1, \dots, b_n)$ a lattice?

ANSWER 1

- If $b_1, \dots, b_n \in \mathbf{Z}^m$, is $L(b_1, \dots, b_n)$ a lattice?
- Yes, because it is a subgroup of $\mathbf{Z}^m$, therefore a discrete subgroup of $\mathbf{R}^m$.

QUESTION 2

- If $b_1, \dots, b_n \in \mathbb{Q}^m$, is $L(b_1, \dots, b_n)$ a lattice?

ANSWER 2

- If $b_1, \dots, b_n \in \mathbb{Q}^m$, is $L(b_1, \dots, b_n)$ a lattice?
- Yes, because it is can be reduced to the previous question.

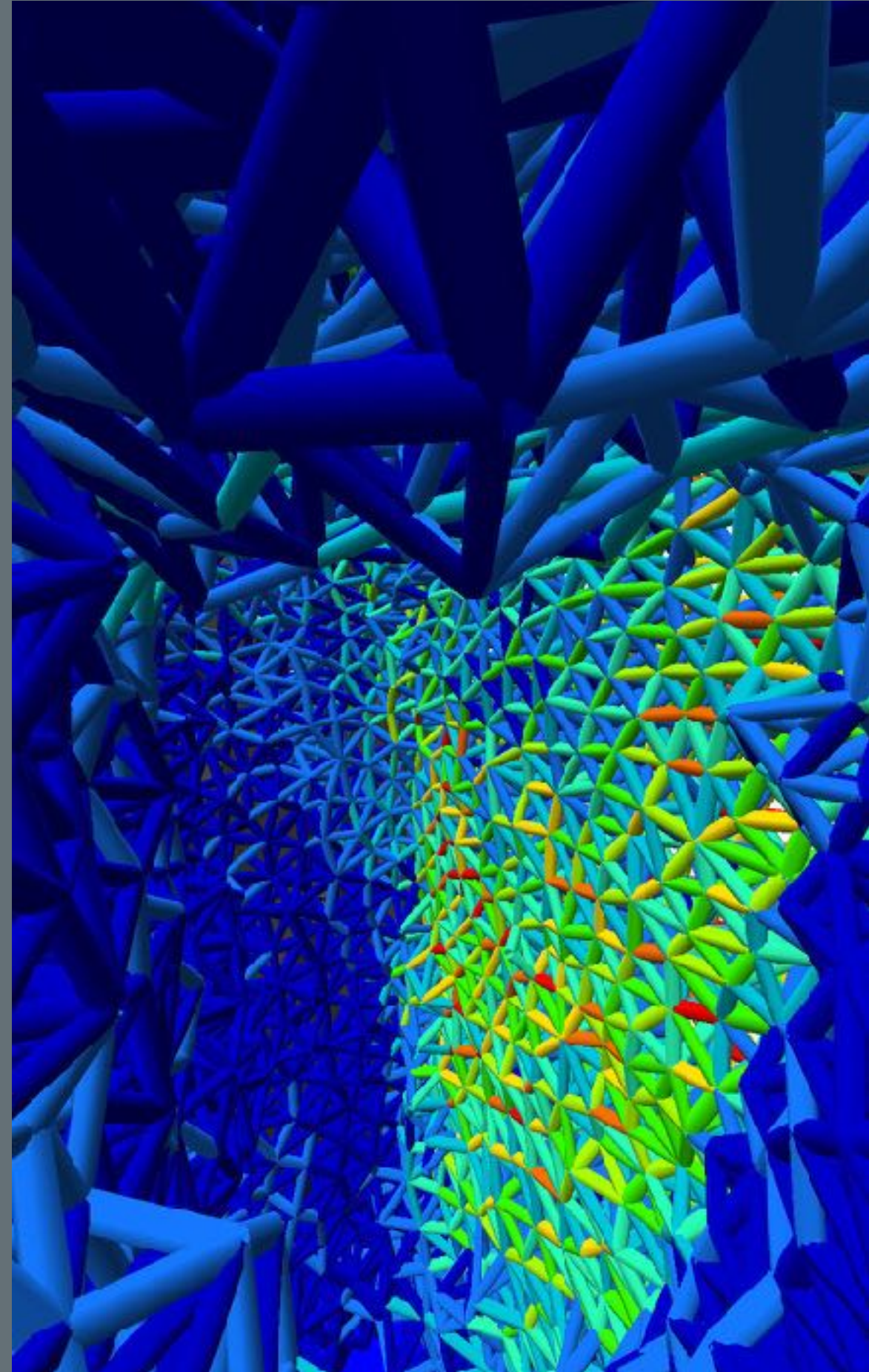
QUESTION 3

- If $b_1, \dots, b_n \in \mathbb{R}^m$, is $L(b_1, \dots, b_n)$ a lattice?

ANSWER 3

- If $b_1, \dots, b_n \in \mathbf{R}^m$, is $L(b_1, \dots, b_n)$ a lattice?
 - Not necessarily, even for $n=2$ and $m=1$: $L(1, \sqrt{2}) = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ is not a lattice because it is dense in $\mathbf{R}$.
 - Yet, $L(1, \sqrt{2})$ can also be "viewed" as a lattice: it is the ring of integers of $\mathbf{Q}(\sqrt{2})$.

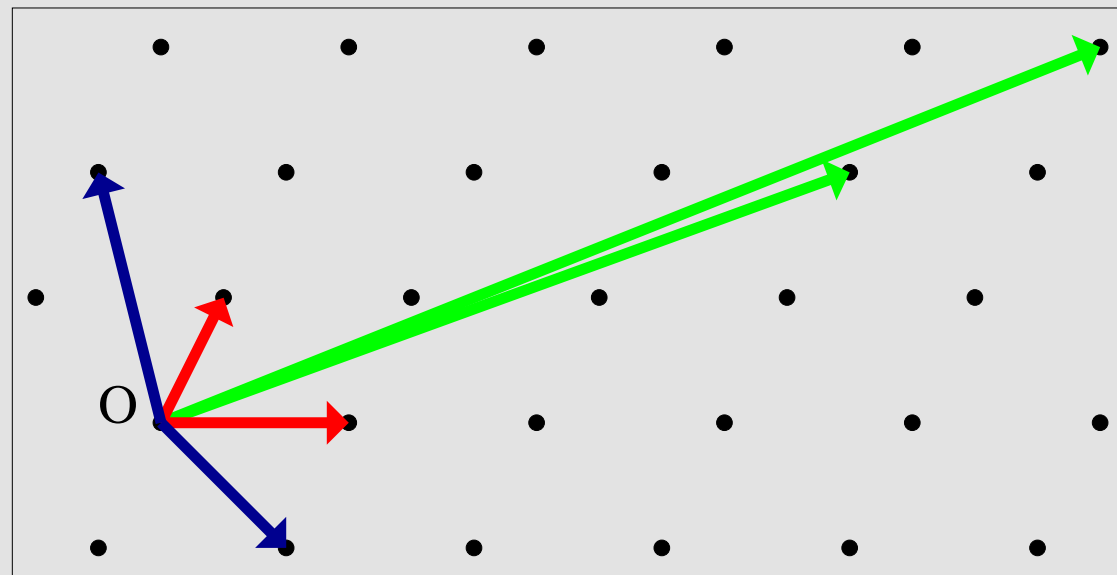
CHARACTERIZ ATION OF LATTICES



A NON-TRIVIAL LATTICE THEOREM

STATEMENT

- Th: Let $L \subseteq \mathbb{R}^m$ be non-empty. There is equivalence between:
 - L is a lattice.
 - $\exists b_1, \dots, b_n \in \mathbb{R}^m$ **linearly independent** s.t. $L = L(b_1, \dots, b_n)$: such $(b_1, \dots, b_n)$ is called a **basis** of L and **$\dim(L) := n$** .



PROVING “ $\Leftarrow$ ”

- Let $b_1, b_2, \dots, b_n$ be linearly independent in $\mathbf{R}^m$.
- Consider an injective sequence (v_i) of $L=L(b_1, \dots, b_n)$ converging to 0.
 - $\exists! m_i \in \mathbf{Z}^n$ s.t. $v_i = m_i B$ where $B=(b_1, \dots, b_n)$.
 - Then $m_i = (v_i B^t) (B B^t)^{-1}$ converges to 0 but $\mathbf{Z}^n$ is discrete: the m_i 's must become 0.
- Thus L is discrete.

PROVING " $\Rightarrow$ " BY INDUCTION

- Induction over $n = \dim(\text{span}(L))$.
- If $n=1$:
 - Let $b \in L$ be a shortest non-zero vector of L .
 - Then $\text{span}(L) = \mathbf{R}b$ and $L = \mathbf{Z}b$.

PROVING " $\Rightarrow$ " BY INDUCTION

- Now, assume that $\dim(\text{span}(L))=n$.
- Let $b \in L$ non-zero.
 - Then $\text{span}(b) \cap L = \mathbb{Z}b_1$ because it is a 1-dim lattice.
- Let π be the projection over $b_1^\perp$.
 - Claim 1: $\pi(L)$ is a lattice whose dim is $n-1$.
 - Claim 2: If $(\pi(b_2), \dots, \pi(b_n))$ is a basis of $\pi(L)$, then $(b_1, \dots, b_n)$ is a basis of L .

PROOF OF CLAIM 1

- Note: the projection of a lattice may not be a lattice! Why?
- $\text{span}(b) \cap L = \mathbb{Z}b_1$ and π is the projection over $b_1^\perp$.
- Consider an injective sequence $\pi(v_i)$ converging to 0, where $v_i \in L$.
- $|\langle v_i, b_1 \rangle| \leq \|b_1\|^2/2$ by **lifting**: $v_i = v_i - \lfloor \langle v_i, b_1 \rangle / \langle b_1, b_1 \rangle \rfloor b_1$
- Then the v_i 's are bounded: contradiction! Why?

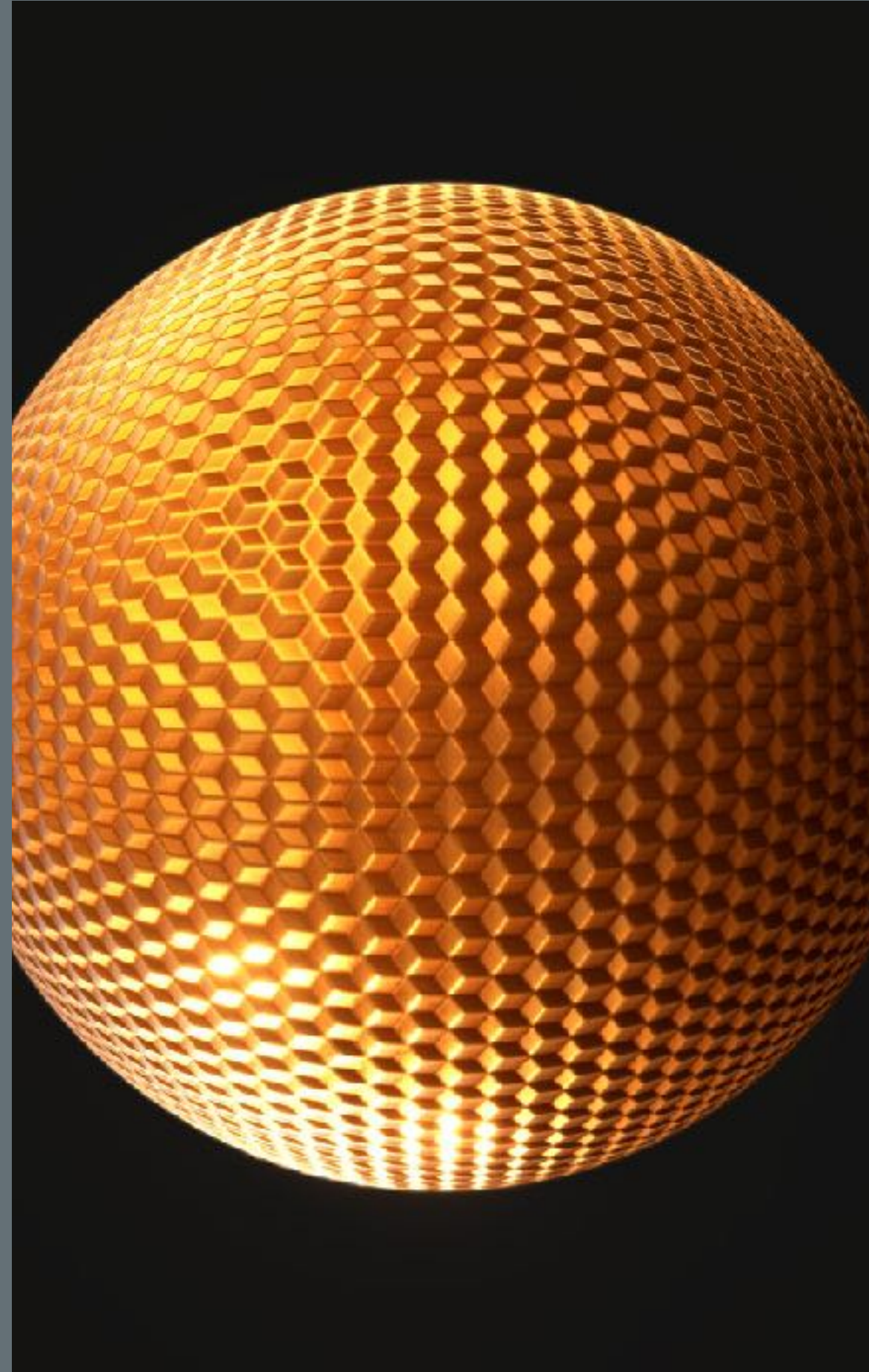
PROOF OF CLAIM 2

- Let $(\pi(b_2), \dots, \pi(b_n))$ is a basis of $\pi(L)$.
- Let $v \in L$.
 - Then $\pi(v) = x_2\pi(b_2) + \dots + x_n\pi(b_n)$ for some $x_i \in \mathbb{Z}$.
 - And $v - (x_2b_2 + \dots + x_nb_n) \in L \cap \text{span}(b_1) = \mathbb{Z}b_1$
 - So $v = x_1b_1 + \dots + x_nb_n$ where $x_i \in \mathbb{Z}$.
- Hence: $L = L(b_1, \dots, b_n)$.

TAKE AWAY

- Key ideas:
 - **Projecting** a lattice to decrease its dimension: quotient with a sublattice.
 - **Lifting** short projections into short lattice vectors.
 - $$\begin{array}{ccccc} v & = & \pi(v) & + & (v - \pi(v)) \\ \in \text{lattice} & & \text{Projection} \in \text{subspace}^\perp & & \text{Lift} \in \text{subspace} \\ & & \in \text{lattice} & & \end{array}$$

COUNTING LATTICE POINTS



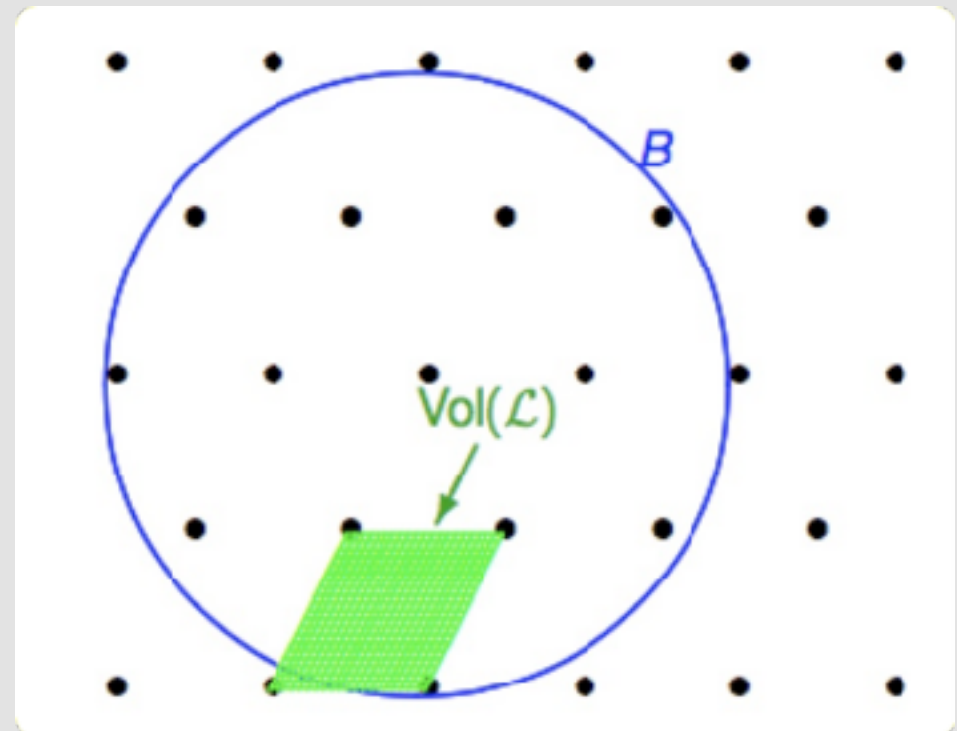
CO-VOLUMES

- $\text{Gram}(b_1, \dots, b_n) = \det(\langle b_i, b_j \rangle)_{1 \leq i, j \leq n} \geq 0$.
- Th: If B is a basis of a lattice L , then $\text{Gram}(B)$ only depends on L : $\sqrt{\text{Gram}(B)}$ is called the **(co-)volume of L** .
- Ex: $\text{vol}(\mathbf{Z}^n) = 1$.
 $\text{vol}(L)\text{vol}(L^\times) = 1$.

THE GAUSSIAN HEURISTIC

- The volume measures the **density** of lattice points.
- For “**nice**” full-rank lattices L , and “**nice**” measurable sets C of $\mathbf{R}^n$:

$$\text{Card}(L \cap C) \approx \frac{\text{vol}(C)}{\text{vol}(L)}$$



VOLUME OF THE BALL

The n -dimensional volume of a Euclidean ball of radius R in n -dimensional Euclidean space is

$$V_n(R) = \frac{\pi^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2} + 1\right)} R^n,$$

$$\Gamma(z) = \int_0^{\infty} x^{z-1} e^{-x} \, dx$$

The unit-volume ball has radius $\sim \sqrt{\frac{n}{2\pi e}}$

VALIDITY OF THE GAUSSIAN HEURISTIC

- Fails for $L=\mathbf{Z}^n$, and $C=\text{Ball}(0,\sqrt{(n/10)})$.
- Easy to prove for asymptotically large balls: $1/\text{vol}(L) = \lim_{r \rightarrow \infty} (\text{number of lattice points of norm} \leq r) / \text{vol}(\text{Ball}(0,r))$

SHORT LATTICE VECTORS

- Th: Any d -dim lattice L has **exponentially many** vectors of norm $\leq$

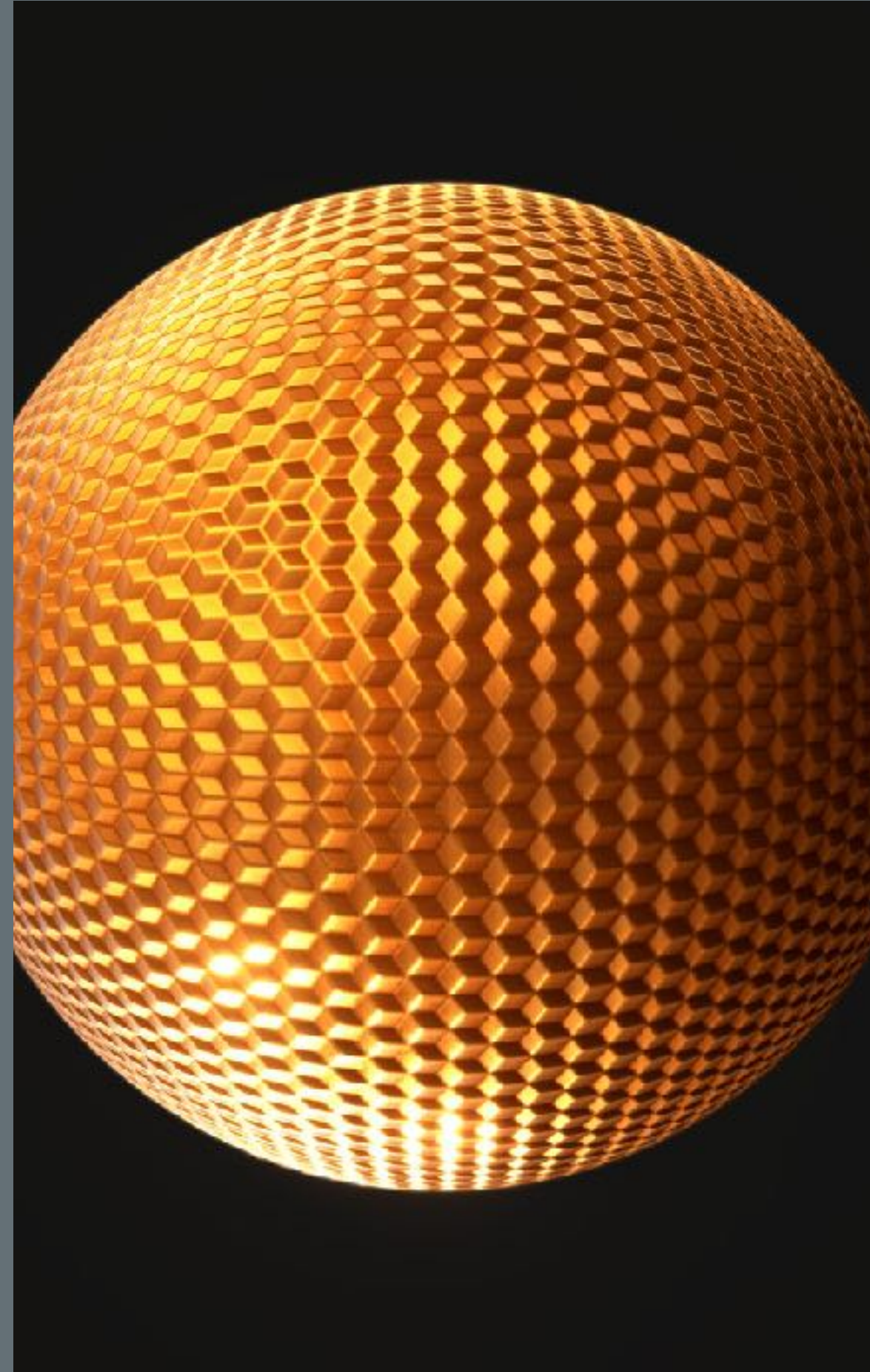
$$O\left(\sqrt{d}\right) \text{vol}(L)^{1/d}$$

- Th: In a **random** d -dim lattice L , all non-zero vectors have norm $\geq$

$$\Omega\left(\sqrt{d}\right) \text{vol}(L)^{1/d}$$

Check IHP's youtube talk by Maryna Viazovska at Serre-100

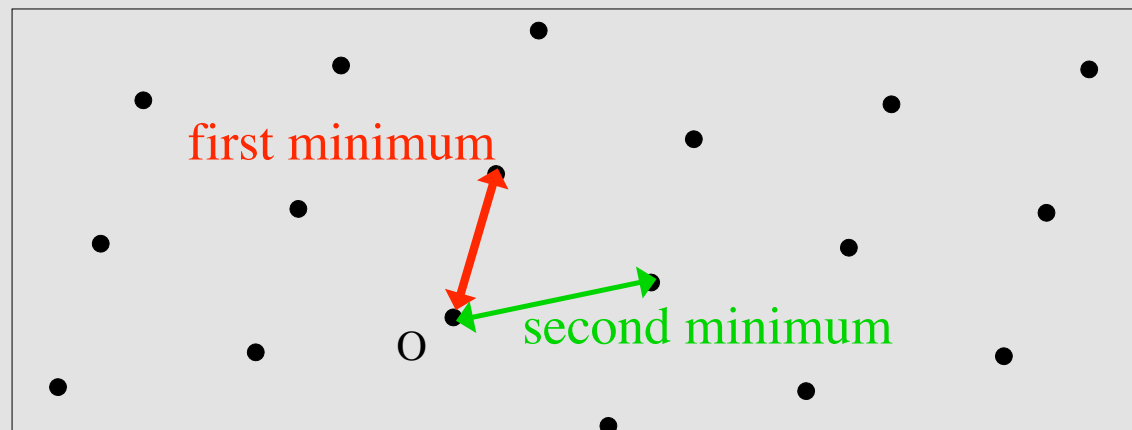
SHORT LATTICE VECTORS



THE FIRST MINIMUM

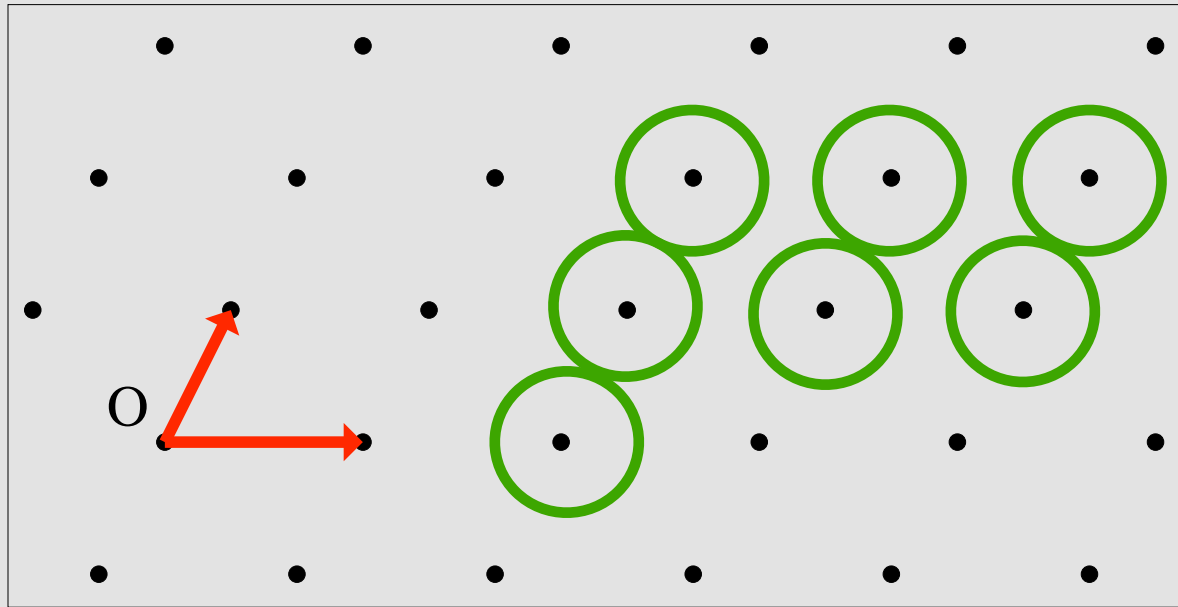
- The intersection of a lattice with any bounded set is **finite**.
- In a lattice L , there are non-zero vectors of minimal norm: this is the **first minimum** $\lambda_1(L)$ or the minimum distance..

• Ex: $\lambda_1(\mathbb{Z}^n)=1$.



LATTICE PACKINGS

- Every lattice defines a sphere packing:

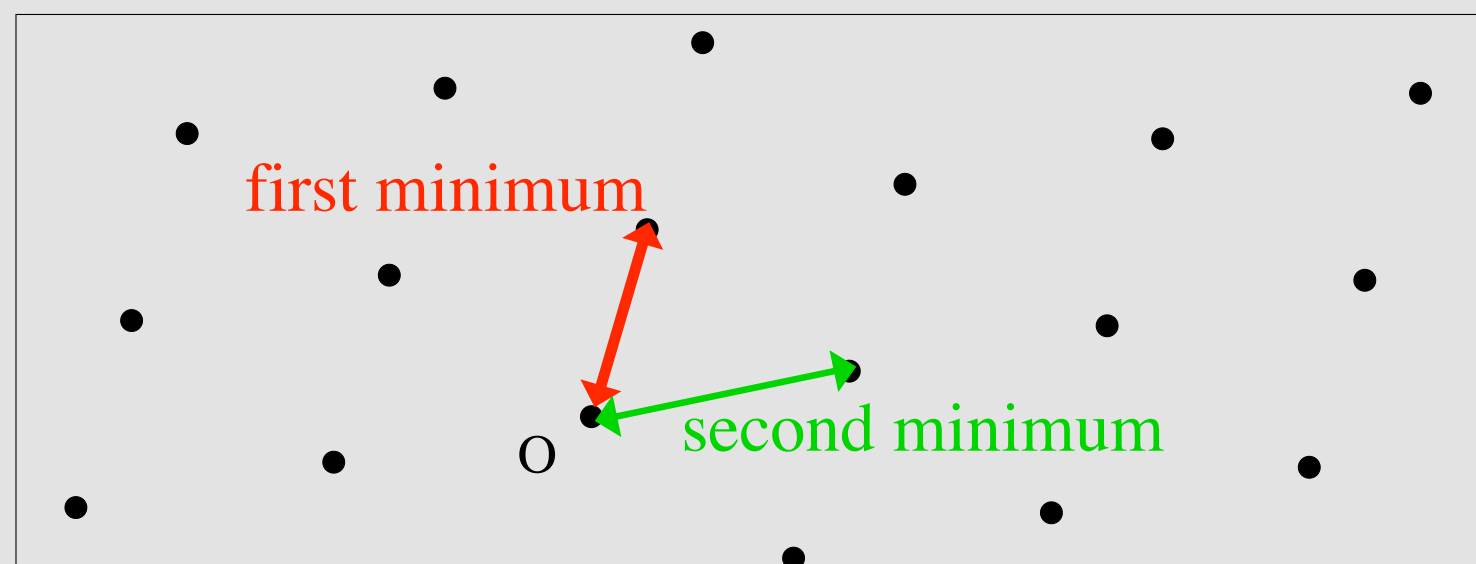


- The diameter of spheres is the **first minimum** of the lattice: the shortest norm of a non-zero lattice vector.

MINKOWSKI'S MINIMA



- Denoted by: $\lambda_1(L), \dots, \lambda_d(L)$
- The **k-th minimum** is the radius of the smallest (centered) ball containing k linearly independent lattice vectors.



- There exist linearly independent lattice vectors $c_1, \dots, c_d$ such that $\|\vec{c}_i\| = \lambda_i(L)$ for each $1 \leq i \leq d$.

HERMITE'S CONSTANT



HERMITE'S CONSTANT (1850)



- This is the “**worst-case**” for short lattice vectors.
- Hermite showed the existence of:

$$\sqrt{\gamma_d} = \max_L \frac{\lambda_1(L)}{\text{vol}(L)^{1/d}}$$

- Here, $\lambda_1(L)$ is the minimal norm of a non-zero lattice vector.
- Hermite’s constant is asymptotically **linear**:

$$\Omega(n) \leq \gamma_n \leq O(n)$$

- The exact value of the constant is only known up to dim 8, in dim 24, and very recently in dim 9.

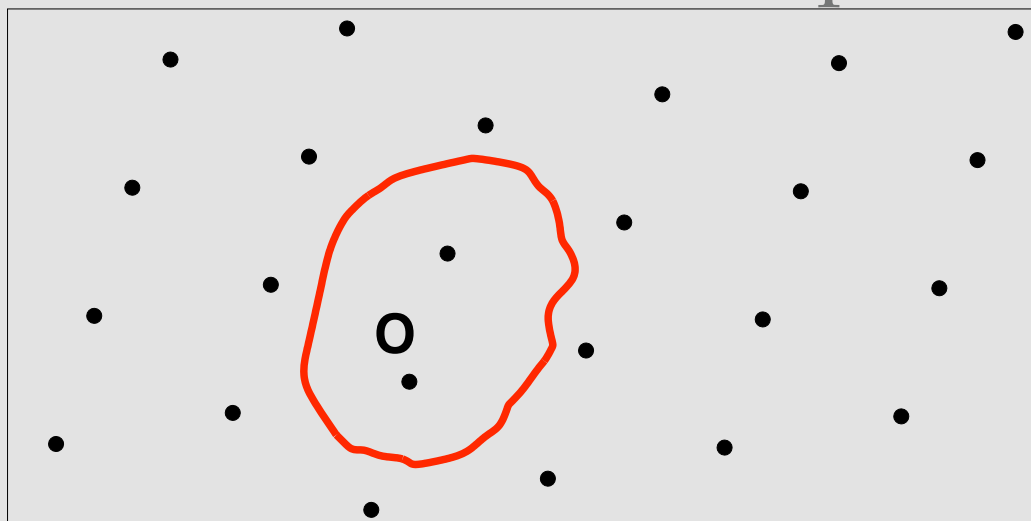
THE EXISTENCE OF SHORT LATTICE VECTORS

➤ Hermite proved in 1850:

$$\gamma_d \leq \left(\frac{4}{3}\right)^{(d-1)/2}$$

➤ Minkowski's theorem implies:

$$\gamma_d \leq d$$



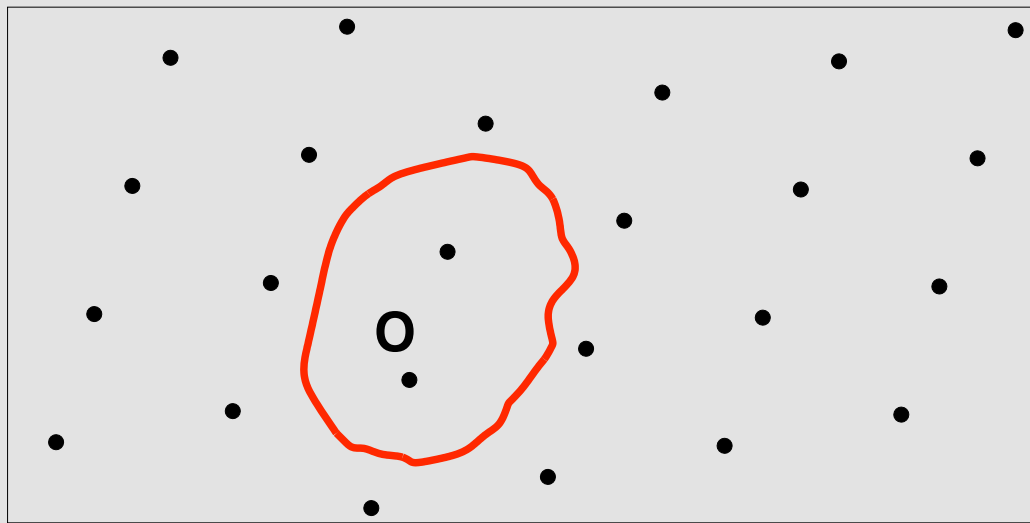
➤ Thus, any lattice contains a non-zero vector of norm

$$\leq \sqrt{d} \text{vol}(L)^{1/d}$$



MINKOWSKI'S CONVEX BODY THEOREM (1896)

- Let L be a full-rank lattice of $\mathbb{R}^n$. Let C be a measurable subset of $\mathbb{R}^n$, convex, symmetric, and of measure $> 2^n \text{vol}(L)$.
- Then C contains at least a non-zero point of L .



- The volume bound is optimal in the worst case.
- If C is furthermore compact, the $>$ can be replaced by $\geq$.

APPLICATION TO A BALL

- Let C be the n -dim ball of radius r . Then its volume is r^n multiplied by:

$$v_n = \frac{\pi^{\frac{n}{2}}}{\Gamma\left(1 + \frac{n}{2}\right)} \sim \left(\frac{2e\pi}{n}\right)^{\frac{n}{2}} \frac{1}{\sqrt{\pi n}}$$

- To apply Minkowski's theorem, one can take:

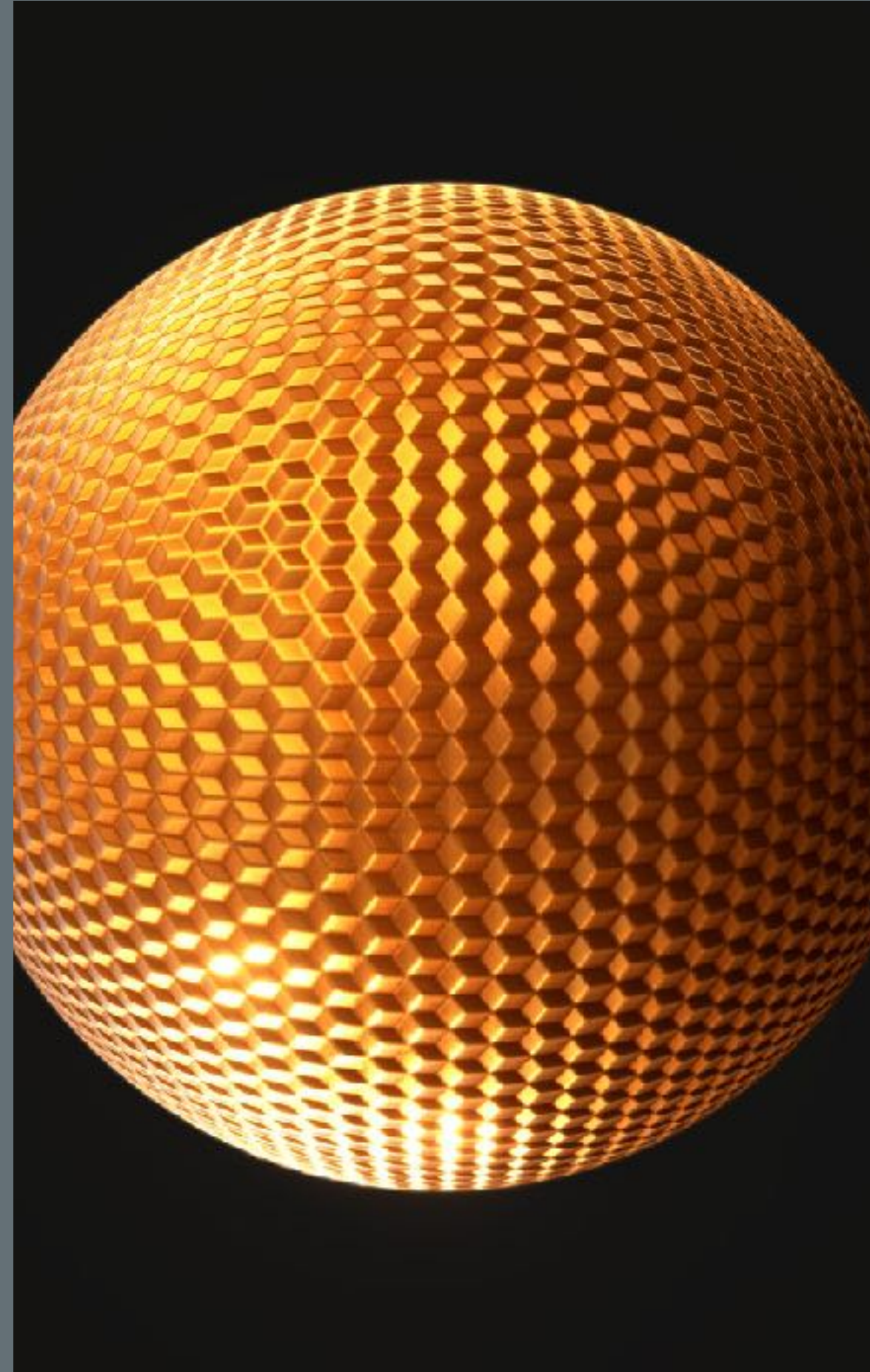
$$r = \frac{2}{(v_n)^{\frac{1}{n}}} \text{vol}(L)^{\frac{1}{n}}$$

PROVING MINKOWSKI'S THEOREM



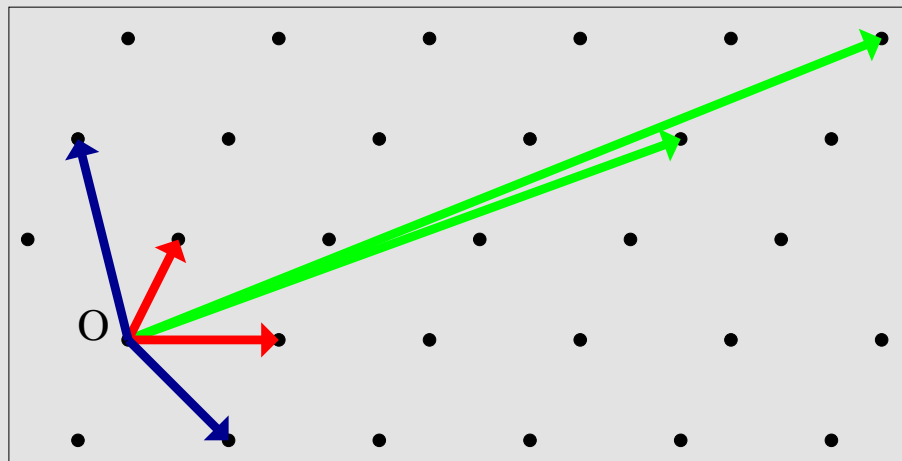
- Blichfeldt's lemma:
 - Let L be a full-rank lattice of $\mathbb{R}^n$.
 - Let F be a measurable subset of $\mathbb{R}^n$, of measure $> \text{vol}(L)$.
 - Then F contains at least two distinct vectors whose difference is in L .
- Take $F=C/2$ to prove Minkowski.

LATTICE REDUCTION



LATTICE REDUCTION

- Euclidean spaces have orthogonal bases.
- Lattices have **reduced bases** whose vectors are short and **nearly-orthogonal**.



non-reduced

35184372088891	0
8497214565171	1

reduced

-3219347	2033901
-5233012	-7622957

MINIMA AND BASES

- As soon as $d \geq 4$, a free family reaching the minima is not necessarily a basis. Ex: the sublattice of $\mathbb{Z}^4$ formed by all vectors whose sum of coordinates is even.

Basis

1	1	0	0
1	0	-1	0
0	0	1	1
0	0	1	-1

*Not a
basis*

1	1	0	0
1	-1	0	0
0	0	1	1
0	0	1	-1

MINIMAL BASES

- As soon as $d \geq 5$, there may not exist a basis reaching all the minima.
- Ex: this lattice whose minima are all equal to 2.

2	0	0	0	0
0	2	0	0	0
0	0	2	0	0
0	0	0	2	0
1	1	1	1	1

REDUCED BASES

- There is no basis which is “naturally” shorter than all others, as soon as $d \geq 5$.
- But the first minimum can always be extended to a basis.
- A **reduced basis** is a basis close to the minima. There are many notions of reduction.