Lattices: Mathematical Background

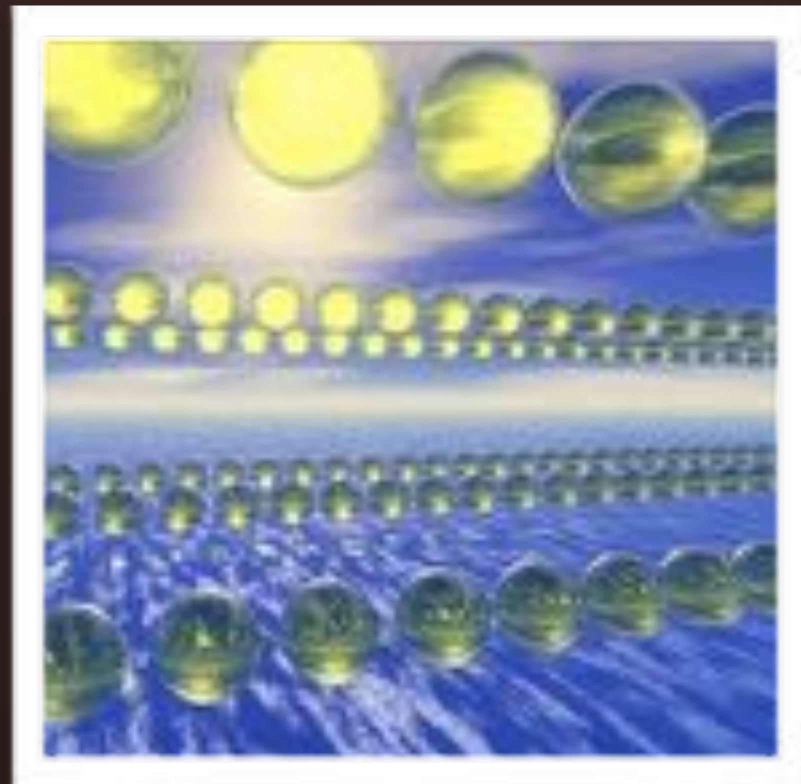
Phong Nguyễn

Duality

- Let L be a lattice.
- The dual lattice of L is $L^{\times}=\{y \in \mathrm{span}(L) \text{ s.t. } \langle x,y\rangle \in \mathbf{Z} \text{ for all } x \in L\}$
  - Show that it is a lattice.
  - Show that $\mathrm{rank}(L) = \mathrm{rank}(L^{\times})$

Ex: Kernel Lattices

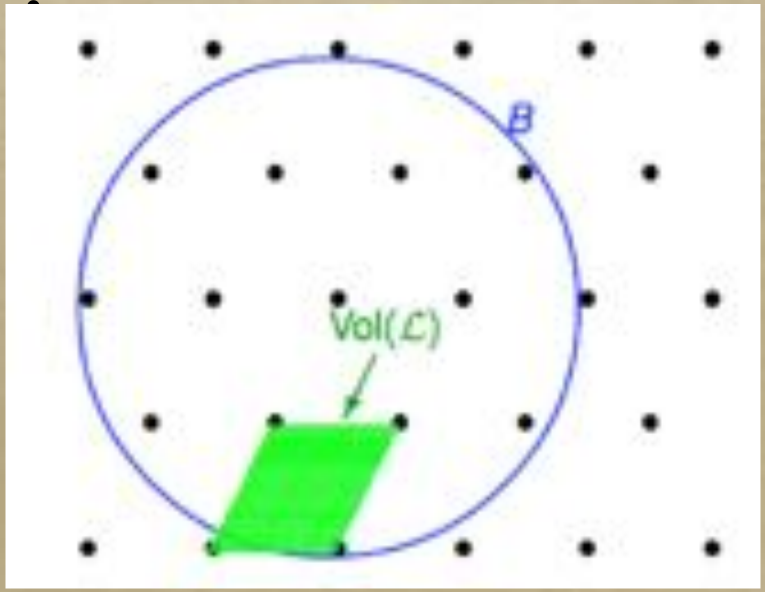
- Let $n,m,q \in \mathbf{N}$.
- Let A be an mxn matrix over $\mathbf{Z}$.
- The kernel $L_A=\{x \in \mathbf{Z}^m$ s.t. $xA \equiv 0 \bmod q\}$ is a full-rank lattice in $\mathbf{Z}^m$ s.t. $vol(L_A) \mid q^n$.
- Its dual lattice is $(1/q)L'_A$ where L'_A is the «image» i.e. $L'_A=\{y \in \mathbf{Z}^m$ s.t. $y \equiv zA^t \bmod q$ for some $z \in \mathbf{Z}^n\}$



Counting Lattice Points

The Gaussian Heuristic

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



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

Volume of the Ball

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

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

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

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

Validity of the Gaussian Heuristic

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

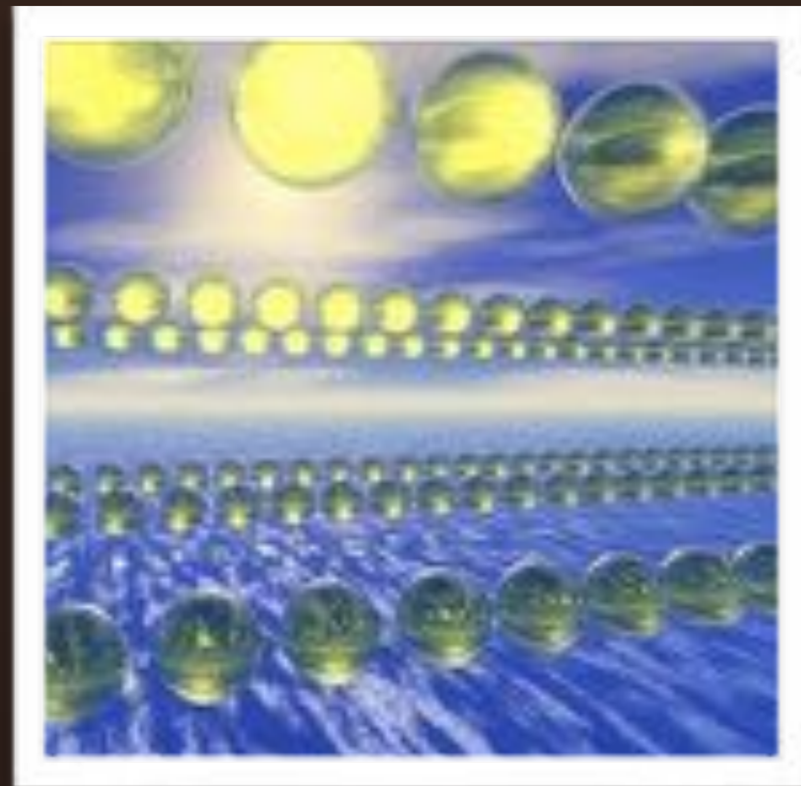
Short Lattice Vectors

- Th: Any d-dim lattice L has exponentially many vectors of norm ≤

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

- Th: In a random d-dim lattice L, all non-zero vectors have norm ≥

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



Short Lattice Vectors

Lattices and Quadratic Forms

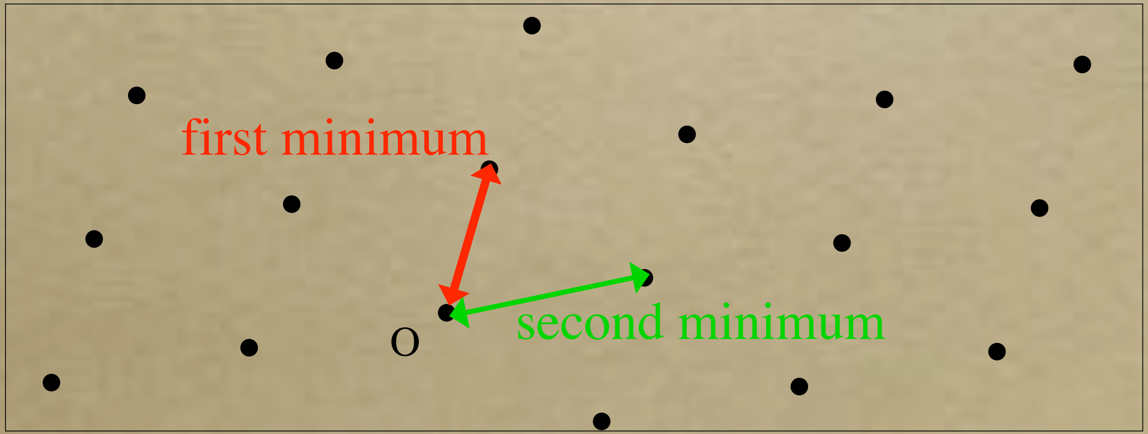
- Every lattice basis defines a positive definite quadratic form:

$$q(x_1, \ldots, x_d) = \left\| \sum_{i=1}^{d} x_i \vec{b}_i \right\|^2$$

- Reciprocally: Cholesky factorization.
- The squared volume is the discriminant of the form.

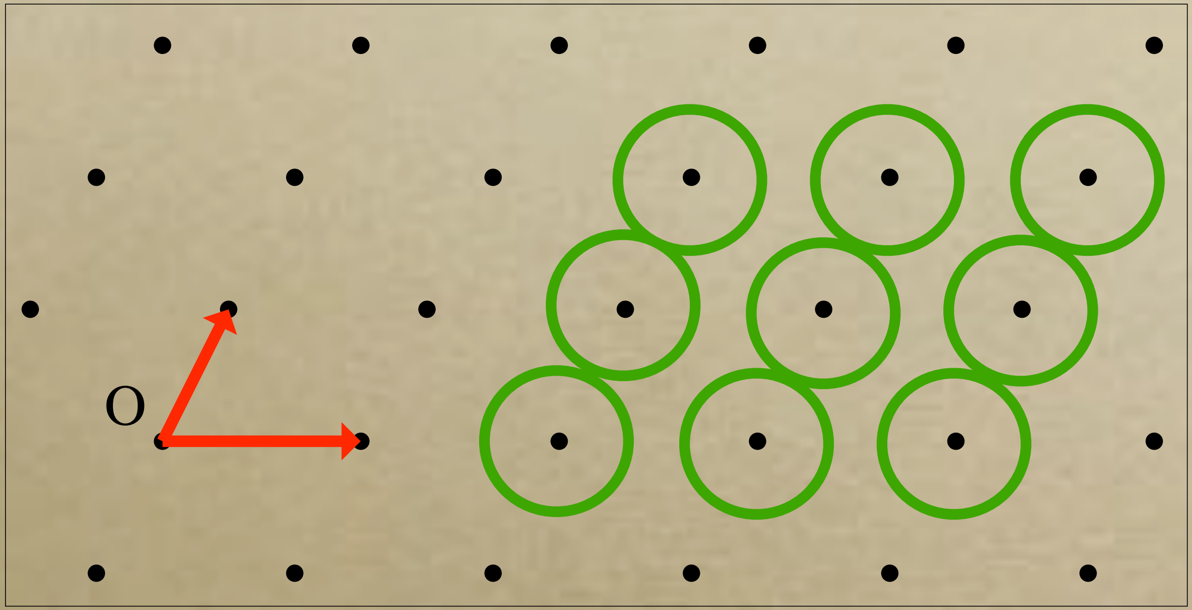
The First Minimum

- 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.



Lattice Packings

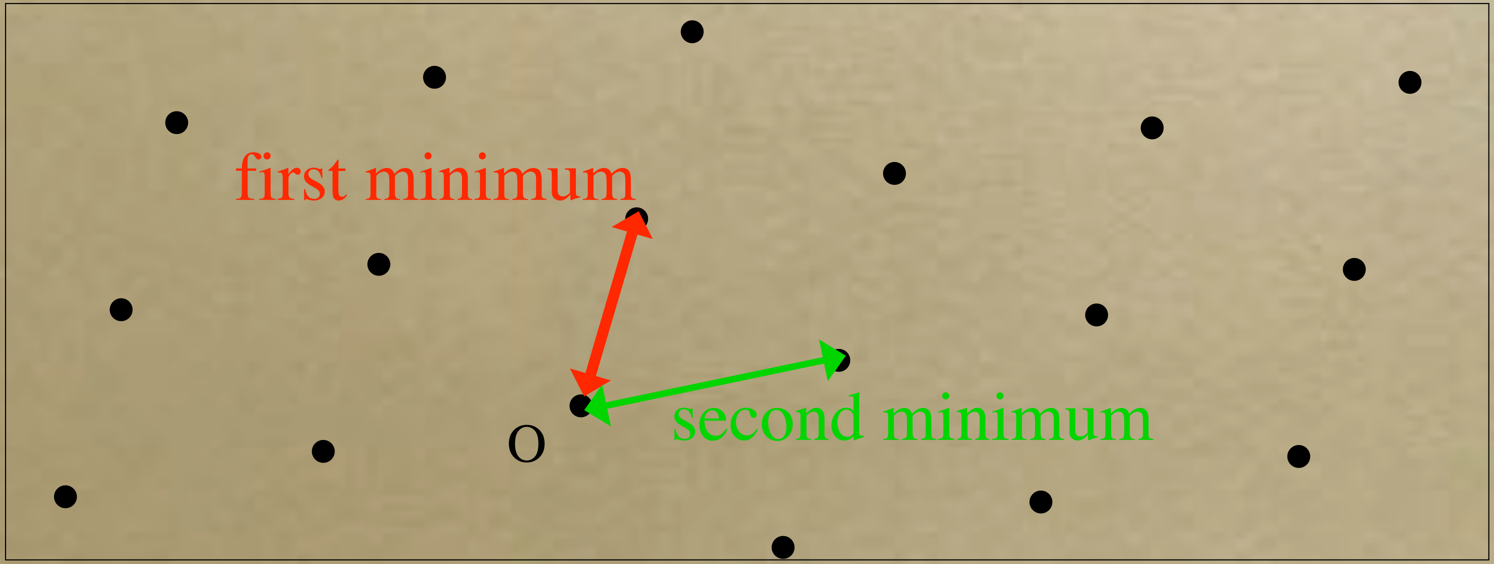
- Every lattice defines a sphere packing:



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



Note

- There exist linearly independent lattice vectors $c_1,\ldots,c_d$ such that $||c_i||= \lambda_i(L)$ for each $1 \leq i \leq d$.

Hermite's Constant (1850)

Hermite's Constant (1850)

- This is the "worst-case" for short lattice vectors.
- Hermite showed the existence of this constant:

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

- Here, $\lambda_1(L)$ is the minimal norm of a non-zero lattice vector.

Facts on Hermite's Constant

- 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, and in dim 24 [2004].

dim n	2	3	4	5	6	7	8	24
γ_n	$2/\sqrt{3}$	$2^{1/3}$	$\sqrt{2}$	$8^{1/5}$	$(64/3)^{1/6}$	$64^{1/7}$	2	4
approx	1.16	1.26	1.41	1.52	1.67	1.81	2	4

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

Minkowski's Theorem (1896)

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

Remarks

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

Application to a ball

- We obtain Minkowski's linear bound on Hermite's constant:

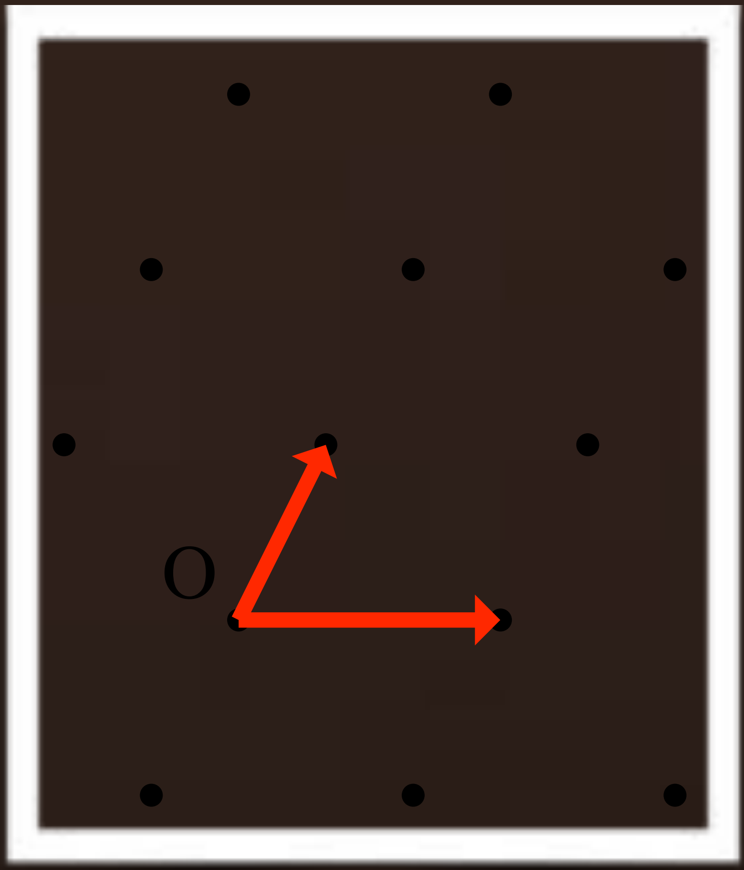
$$\sqrt{\gamma_n} \leq \frac{2}{(v_n)^{\frac{1}{n}}} = 2\,\frac{\Gamma\left(1+\frac{n}{2}\right)^{\frac{1}{n}}}{\sqrt{\pi}} \sim 2\sqrt{\frac{n}{2\pi e}}$$

- The unit-ball contains the hypercube $[-1/\sqrt{n},1/\sqrt{n}]^n$, therefore $v_n \geq (2/\sqrt{n})^n$, hence the upper bound implies: $\gamma_n \leq n$.

Proving Minkowski

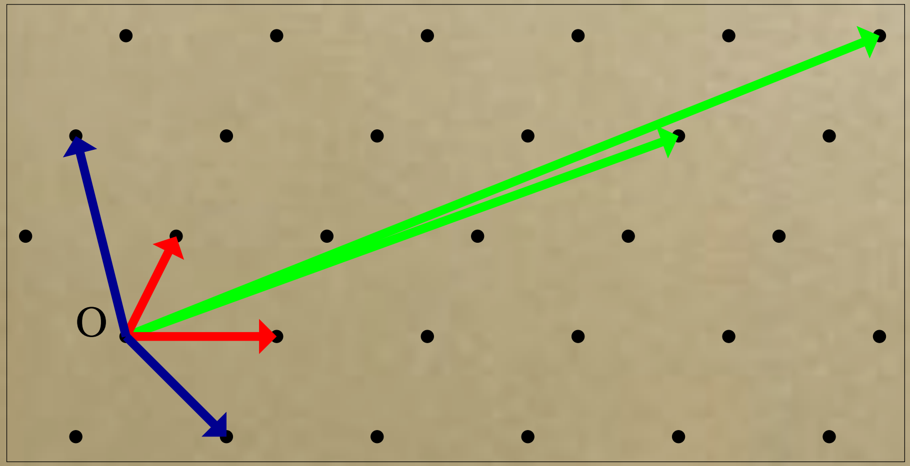
- Blichfeldt's lemma:
  - Let L be a full-rank lattice of R^n.
  - Let F be a measurable subset of R^n, of measure > vol(L).
- Then F contains at least two distinct vectors whose difference is in L.
- Take F=C/2 to prove Minkowski.

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

Bounding Minima

- Thanks to Hermite's constant, we can always upper bound the first minimum: $\lambda_1(L) \le \sqrt{\gamma_d}\, \mathrm{vol}(L)^{1/d}$.
- But the same bound does not apply in general for the other minima: they can be arbitrarily larger.
- Yet, the geometric mean can be bounded similarly.

Minkowski's second theorem

- Let L be a d-rank lattice.
  - Then: $[\lambda_1(L)\ \lambda_2(L)\ \ldots\ \lambda_k(L)]^{1/k} \leq \sqrt{\gamma_d}$ $vol(L)^{1/d}$ for $1 \leq k \leq d$.
- Corollary:
  - $vol(L) \leq [\lambda_1(L)\ \lambda_2(L)\ \ldots\ \lambda_d(L)] \leq d^{d/2}$ $vol(L)$

Minima ≠ Basis

- As soon as $d \geq 4$, a free family reaching the minima is not necessarily a basis.

  Ex: the sublattice of $\mathbf{Z}^4$ 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.