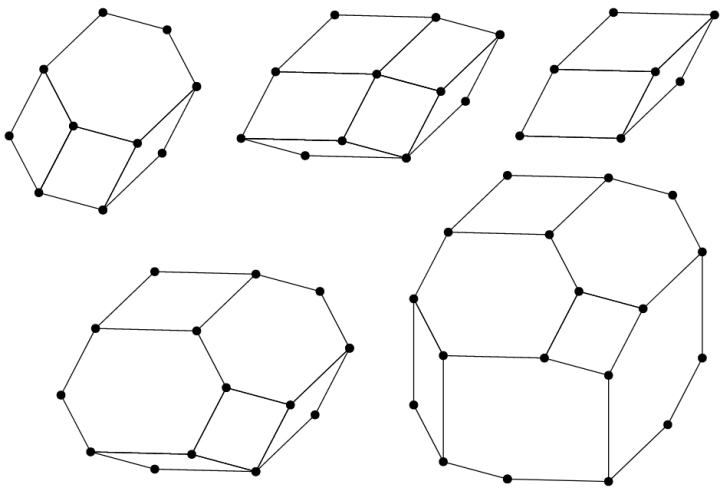


FIGURE 1. Five three-dimensional parallelohedra: hexagonal prism, rhombic dodecahedron, parallelepiped, elongated dodecahedron, and truncated octahedron.

Geometry of Numbers lecture 2

Q (from previous lecture). A polytope in $\mathbb{R}^n$ is the convex hull of a finite set.

(i.e. $P = \text{conv}(F) = \left\{ \sum_{f \in F} a_f f : \sum a_f = 1, a_f \geq 0 \ \forall f \right\}$

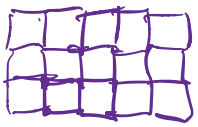
where $F \subset \mathbb{R}^n$ is finite).

Say that P tiles by translations if $\exists L_0 \subset \mathbb{R}^n$ s.t. $\mathbb{R}^n = \bigcup_{\ell \in L_0} (\ell + P)$, and $\{\ell + P : \ell \in L_0\}$ have disjoint interiors.

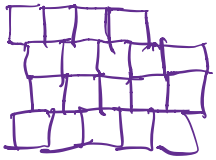
Suppose P tiles by translations, does it follow that P lattice tiles by translations

ie. can take L_0 to be a lattice?

Example $n=2$ $\quad P=[0,1]^2=\text{conv}(\text{vertices})$



part of a lattice tiling



part of a tiling which is not a lattice tiling

Answer Yes. proved ind. by Venkov '54 and P. McMullen in '80.

Voronoi conjecture If P is a polytope which tiles $\mathbb{R}^n$ (and hence lattice tiles $\mathbb{R}^n$), does it follow that P is an affine image of a Voronoi cell? I.e., is there a lattice L and $A\in GL_n(\mathbb{R})$, $x_0\in\mathbb{R}^n$, s.t.

$P=A(P_0)+x_0$, where P_0 is the Voronoi cell of L?

$P_0 = \{x \in \mathbb{R}^n : \|x\| \leq \|x - \ell\| \ \forall \ell \in L\}$.

Voronoi 1868-1908

solved for $n = 2, 3, 4, 5$. Along with the solution, in all cases, a list of all possible types of Voronoi cells was obtained.

n	# Voronoi cell types	
2	2 (square and hexagon)	
3	5 (picture)	
4	52 (list completed in '73)	Voronoi conj. was proved in '29 by Delone Delaunay
5	110,244 (list completed in '16, conj. proved in '20 by Garber and Magazinov)	

Characterization of lattices.

We defined a lattice to be $\mathrm{span}_{\mathbb{Z}}(v_1,\dots,v_n)$ $v_1,\dots,v_n$ a basis of $\mathbb{R}^n$.

Def $L \subset \mathbb{R}^n$ is called an additive subgroup if $v_1, v_2 \in L \Rightarrow v_1 \pm v_2 \in L$.

$L \subset \mathbb{R}^n$ is called discrete if $\forall \ell \in L$ $\exists r > 0$ s.t. $B(\ell, r) \cap L = \{\ell\}$.

I.e. the topology on L (as a subset of $\mathbb{R}^n$ is discrete).

Example $\{1, \frac{1}{2}, \frac{1}{3}, \dots\} \subset \mathbb{R}$ is discrete. (around $\frac{1}{n}$, let $r = \frac{1}{10n^3}$).

Remark In some books, discrete in $\mathbb{R}^n$ means "contains finitely many pts in any ball". In our terminology, equivalent to being discrete and closed.

Prop If L is an additive subgroup then TFAE: (i) L is discrete

(ii) $\exists r$ s.t. $\forall \ell \in L \quad B(\ell, r) \cap L = \{\ell\}$.

(iii) $\exists r$ s.t. $B(0, r) \cap L = \{0\}$.

Pf: (i) $\Rightarrow$ (iii) immediate.

(iii) $\Rightarrow$ (ii) Let $\ell \in L$, and let $\ell_1 \in L \cap B(\ell, r)$

$\Rightarrow \ell_1 - \ell \in L \cap B(0, r)$ (metric is translation inv. and L is an additive subgp).

$\Rightarrow$ by (iii) $\ell_1 - \ell = 0 \Rightarrow \ell = \ell_1$.

(ii) $\Rightarrow$ (i) immediate.

Prop: Let $L \subset \mathbb{R}^n$. L is a lattice $\Leftrightarrow$ the following three statements hold: (i) L is an additive subgp.

(ii) L contains a basis for $\mathbb{R}^n$ (as a vect. space)

(iii) L is discrete.

Pf: Assume L is a lattice.

(i) and (ii) immediate.

For (iii), recall $\exists A \in GL_n(\mathbb{R})$ s.t. $L = A(\mathbb{Z}^n)$. $\mathbb{Z}^n$ is discrete (use $r=1$). A is a bilipschitz map $\mathbb{R}^n \to \mathbb{R}^n$, i.e. $\exists c > 1$ s.t. $\forall x_1, x_2 \in \mathbb{R}^n$,

$$\frac{1}{c}\|x_1 - x_2\| \leq \|Ax_1 - Ax_2\| \leq c\|x_1 - x_2\|$$

bilipschitz maps send discrete sets to discrete sets. This proves (iii).

Now assume (i), (ii), (iii), and want to show $L = \text{span}_{\mathbb{Z}}(v_1, \ldots, v_n)$ for some basis $v_1, \ldots, v_n$ of $\mathbb{R}^n$.

By (ii), let $v_1, \ldots, v_n$ a basis of $\mathbb{R}^n$ contained in L, and let $L' = \text{span}_{\mathbb{Z}}(v_1, \ldots, v_n)$. L' a lattice, $L' \subset L$. If $L' = L$ we are

done. Let Ω be a bounded fundamental domain for L' (for example, a fund. parallelepiped). Let $x_1, x_2, \dots$ be coset representatives for L/L' contained in Ω. For any $i \neq j$, $\|x_i - x_j\| \geq r$ for some $r > 0$ (ind. of i, j), by the previous prop. and (iii). This means $x_1, \dots, x_D$ is finite, where $D = [L : L']$.

By induction on D, suffices to find a lattice L'', $L' \subsetneq L'' \subset L$.

Let v be the shortest nonzero element of $\{x_1, \dots, x_D\}$. Let m be the smallest natural number so that $v' \stackrel{\text{def}}{=} mv \in L'$.

Claim: v' can be completed to a basis (over $\mathbb{Z}$) of L', i.e. v' is primitive.

Assuming the claim, let

$v' = v_1', v_2', \ldots, v_n'$ are a basis of L'.

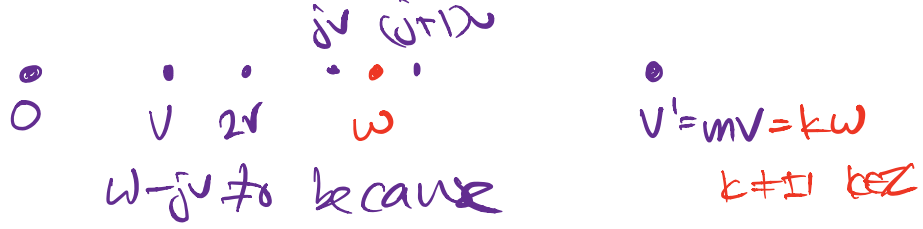
Define $L'' = \mathrm{span}_{\mathbb{Z}}(v, v_2', \ldots, v_n')$.

$L' = \mathrm{span}_{\mathbb{Z}}(v_1', v_2', \ldots, v_n') \subset L''$ (with $\neq$)

This completes the proof, modulo the claim.

To prove claim, recall that v' is primitive $\Leftrightarrow$ it is not a multiple, by an integer $\neq \pm 1$, of an element of L'.

Picture proving claim.



$w - jv \neq 0$ because $w \notin L'$

m is the smallest integer s.t. $mv \in L'$

Then $w - jv$ is shorter than v contradiction.

Examples. (1) $L = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_8 \end{pmatrix} \in \mathbb{R}^8 : x_i \in \mathbb{Z},\ x_1 \equiv \cdots \equiv x_8 \pmod 2,\ \sum x_i \equiv 0 \pmod 4 \right\}$

This is the E_8 lattice.

It's a lattice by prop. (contains $4e_1, \dots, 4e_8$) discrete as a subset of $\mathbb{R}^8$, subgp

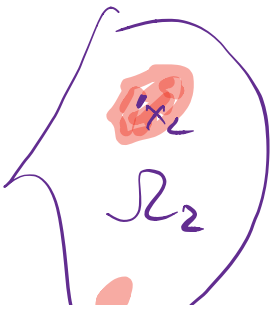
(2) In $\mathbb{R}^4$: $\mathrm{span}_{\mathbb{Z}}(2e_1, 2e_2, 2e_3, 2e_4, e_1+e_2+e_3+e_4)$.

Minkowski's first theorem

Recall: We proved in the previous lecture that any two fundamental domain for L have the same volume.

(A fundamental domain: a Borel set, and a collection of equivalence class representatives for the relation $x_1 \sim x_2 \iff x_1 - x_2 = \ell \in L$).

Idea of proof:



$x_1 - x_2 \in \ell$

$A_\ell = \{x_2 \in \Omega_2 : \text{s.t. } x_1 + x_2 = \ell\}$

$B_\ell = A_\ell + \ell$

Prop (Blichfeldt Lemma): Let L be a lattice and let $\Omega \subset \mathbb{R}^n$ be a Borel set intersecting every equiv. class at most once. Then there is a fund. domain containing Ω, and $\mathrm{Vol}(\Omega) \leq \mathrm{covol}(L)$.

Equivalently: If Ω is Borel, $\mathrm{Vol}(\Omega) > \mathrm{covol}(L)$ then $\exists x_1, x_2 \in \Omega$ and $\ell \in L \setminus \{0\}$ s.t. $x_1 - x_2 = \ell$.

Pf: Fix Ω_1, a fund. domain for L.

For each $\ell \in L$ define

$$A_\ell = \{x \in \Omega : \exists x_1 \in \Omega_1 \text{ s.t. } x_1 - x = \ell\}$$

Since each equiv. class intersects Ω at most once, if such an x_1 exists, it is unique and so for $\ell_1 \neq \ell_2$, $A_{\ell_1} \cap A_{\ell_2} = \emptyset$.

$\Omega' = \Omega \cup \left(\Omega_1 \setminus \bigcup_{\ell \in L} A_\ell + \ell\right)$, is a fund. domain containing Ω.

Let $K \subset \mathbb{R}^n$ be convex. K is called centrally symmetric if $K = -K = \{-x : x \in K\}$.

Minkowski's first theorem: Let K is convex and centrally symmetric, $L \subset \mathbb{R}^n$ is a lattice, $\mathrm{Vol}(K) > 2^n \mathrm{covol}(L)$. Then $K \cap L \neq \{0\}$, i.e. K contains an element of $L \setminus \{0\}$.

Pf: Let $K_0 = \frac{1}{2}K = \{\frac{1}{2}x : x \in K\}$.

$\mathrm{Vol}(K_0) = (\frac{1}{2})^n \mathrm{Vol}(K) > \mathrm{covol}(L) = \mathrm{Vol}(\mathcal{L})$

where $\mathcal{L}$ is a fund. domain for L.

By Blichfeldt, there are $x_1, x_2 \in K_0$ s.t. $x_1 - x_2 \in L \setminus \{0\}$. $x_i = \frac{1}{2}y_i$, for $y_i \in K$, $i = 1, 2$.

$$L \setminus \{0\} \ni x_1 - x_2 = \frac{1}{2}y_1 - \frac{1}{2}y_2 = \frac{1}{2}y_1 + \frac{1}{2}(-y_2) \in K.$$

($y_1 \in K$, $-y_2 \in K$)

Example $L=\mathbb{Z}^n$, $K=(-1,1)^n$

Then $\mathrm{Vol}(K)=2^n$ $\mathrm{covol}(L)=1$

and so theorem is sharp (2^n can't be made smaller).

Prop: If K is compact, and $\mathrm{Vol}(K)=2^n\mathrm{covol}(L)$ then K contains a nonzero point of L.

Pf For each $j\in\mathbb{N}$, by Minkowski's thm, there is $\ell_j\neq 0$ in $L\cap(1+\frac{1}{j})K$.

ℓ_j is a bounded sequence (contained $2K$) and has a convergent subsequence.

$\ell_{j_i}\longrightarrow \ell_0$. By discreteness, $\ell_{j_i}\in L$ for $i\gg 0$.

$\ell_{j_i}\in(1+\frac{1}{j_i})K_{j_i}$. So $\ell_0\in\bigcap_{j=1}^{\infty}(1+\frac{1}{j})K=K$ (compactness).

Minkowski successive minima

L is a lattice. For $i=1,\dots,n$

$$\lambda_i(L) = \inf\{ r>0 : L \cap B(0,r) \text{ contains } i \text{ lin. independent vectors} \}$$

$B(0,r)$: ℓ_2 ball

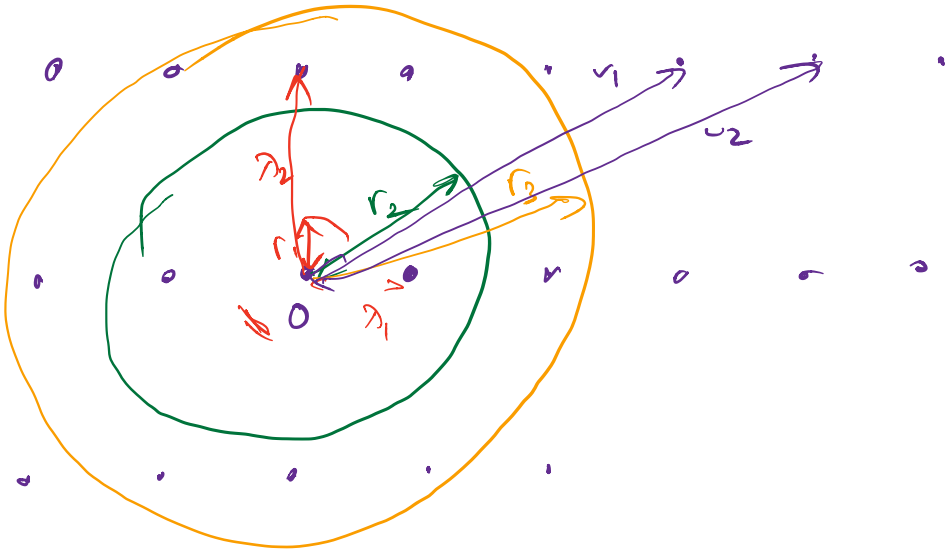
$$= \inf\{ r>0 : L \cap \bar{B}(0,r) \text{ contains } i \text{ lin. ind. vectors} \}$$

$\bar{B}(0,r)$: closed ℓ_2 ball

ex.

$$= \min\{ r>0 : L \cap \bar{B}(0,r) \text{ " " " " } \}.$$

$\lambda_1(L)$ is shortest nonzero vector of L.



Q1 Given L, what are $\lambda_1(L), \dots, \lambda_n(L)$.

Q2 What is a "good basis" for L.

Ex There is a basis for $\mathbb{R}^n$, $v_1, \dots, v_n$, as an $\mathbb{R}$-vector space

contained in L_1 s.t. $\lambda_i(L) = \|v_i\|$.

Idea "greedy algorithm": Take shortest vector, take shortest ind. of the first, given $v_1, \dots, v_i$, choose v_{i+1} to be shortest so that $v_1, \dots, v_{i+1}$ are lin. ind.

Example: $L_1 = \operatorname{span}_{\mathbb{Z}}(2e_1, 2e_2, 2e_3, 2e_4, e_1+e_2+e_3+e_4)$

$L_2 = \operatorname{span}_{\mathbb{Z}}(2e_1, 2e_2, \dots, 2e_5, e_1+\dots+e_5)$.

Note: in L_1, $\operatorname{span}_{\mathbb{Z}}\{2e_1, 2e_2, 2e_3, 2e_4\} \subsetneq L_1$

(does not contain $e_1+\dots+e_4$).

So greedy algorithm just mentioned doesn't necessarily give a basis of L.

Note: There are no shorter vectors in L_1.

Any vector in L_1, $v = (x_1, \dots, x_4)$, either has all x_i even, or all x_i odd.

If all x_i odd then length $\geq \sqrt{1^2+1^2+1^2+1^2} = 2$

" " even, and $v \neq 0$ ≥ 2.

Two more interesting examples.

The E_8 lattice has 240 vectors which realize λ_1 (shortest)

note $\mathbb{Z}^8$ has 16.

Voronoi cell has 17,280 7-dim faces.

The Leech lattice (famous lattice in $\mathbb{R}^{24}$)

$\lambda_1 = \cdots = \lambda_{24}$ realized by 196,560 vectors

Voronoi cell has 16,969,680 23-dim faces.

Proposal for a revised greedy algorithm.

Choose v_1 - shortest vector in L ($\|v_1\| = \lambda_1$)

Choose v_2 - shortest among v_2 s.t. v_1, v_2 is primitive.

(Last week we saw: $v_1, \ldots, v_k$ is a primitive k-tuple

$\Leftrightarrow$ $\mathrm{span}_{\mathbb{Z}}(v_1, \ldots, v_k) = L \cap \mathrm{span}_{\mathbb{R}}(v_1, \ldots, v_k)$

(A) and v_i are lin. ind.

Successively given $v_1, \ldots, v_i$ primitive,

choose v_{i+1} shortest possible s.t. $v_1, \dots, v_{i+1}$ primitive.

Korkine–Zolotarev reduction 1873

Given a lattice L, gives a basis for L (which is "economical").

First let v_1 be shortest nonzero vector in L.

Now successively, suppose $v_1, \dots, v_i$ have been chosen. Let $V = \text{span}(v_1, \dots, v_i) \subset \mathbb{R}^n$

Let $\pi : \mathbb{R}^n \to V^\perp$ be orthogonal projection.

Let u_{i+1} be shortest nonzero vector in $\pi(L)$. (We will see soon that $\pi(L)$ is discrete).

Take v_{i+1} to be shortest vector in $L \cap \pi^{-1}(u_{i+1})$.

Prop This is well-defined (at each step $\pi(L)$ discrete), and $v_1, \dots, v_n$ are a basis for L (over $\mathbb{Z}$).

Pf. We will prove by induction that $v_1, \dots, v_i$ are a primitive i-tuple for each i.

v_1 is primitive by (A).

Suppose $v_1, \dots, v_i$ already chosen, primitive (by induction hypothesis), let $w_{i+1}, \dots, w_n \in L$

s.t. $v_1, \dots, v_i, w_{i+1}, \dots, w_n$ is a $\mathbb{Z}$-basis of L. $\pi(L) = \operatorname{span}_{\mathbb{Z}}(\underbrace{\pi(v_1)}_{0}, \dots, \underbrace{\pi(v_i)}_{0}, \pi(w_{i+1}), \dots, \pi(w_n))$

$= \operatorname{span}_{\mathbb{Z}}(\pi(w_{i+1}), \dots, \pi(w_n))$

$n-i$ lin. ind. vectors in V, $\dim V = n-i$.

So $\pi(L)$ is discrete.

To verify (A) for $v_1, \dots, v_i, v_{i+1}$, let

$w \in L \cap \operatorname{span}_{\mathbb{R}}(v_1, \dots, v_i, v_{i+1})$.

If $\pi(w) = 0$ then $w \in \operatorname{span}_{\mathbb{R}}(v_1, \dots, v_i)$

and (by primitivity of $v_1, \dots, v_i$), $w \in \operatorname{span}_{\mathbb{Z}}(v_1, \dots, v_i)$.

If $\pi(w) \neq 0$ then $\pi(w) \in \operatorname{span}_{\mathbb{R}}(\pi(v_{i+1}))$

$\pi(w)$ is a multiple of $\pi(v_{i+1}) = u_{i+1}$.

$\pi(w) = k u_{i+1}$ for some $k \in \mathbb{Z}$.

$w' = w - k v_{i+1}$ satisfies $\pi(w') = 0$

$\Rightarrow w' \in \operatorname{span}_{\mathbb{Z}}(v_1, \dots, v_i) \Rightarrow w \in \operatorname{span}_{\mathbb{Z}}(v_1, \dots, v_{i+1})$.

Minkowski's second theorem

For any lattice L

$$\operatorname{covol}(L) \leq \lambda_1(L) \cdots \lambda_n(L) \leq 2^n \operatorname{covol}(L).$$

(this is a special case).

(Obviously $\lambda_1 \leq \cdots \leq \lambda_n$).

We are going to generalize this to arbitrary norms on $\mathbb{R}^n$.

(A norm: $x \mapsto \|x\|$ $\mathbb{R}^n \to [0, \infty)$)

$\|u+v\| \leq \|u\| + \|v\|$

$\|cu\| = |c| \|u\|$

Given any norm $\|\cdot\|$, the set

$A = \{u \in \mathbb{R}^n : \|u\| \le 1\}$ is a centrally symmetric, closed convex set, with nonempty interior.

Conversely, given a centrally symmetric closed bounded convex set K with nonempty (a.k.a. convex body) there is a norm $\|\cdot\|$ for which $A = K$,

namely: $\|u\| = \begin{cases} 0 & u = 0 \\ \dfrac{1}{\max\{t \ge 0 : tu \in K\}} & u \neq 0 \end{cases}$

Generalizing the previous defn, for any fixed norm, we can define

$$\lambda_i(L) = \inf\{r > 0 : B(0,r) \cap L \text{ contains } i \text{ lin. ind. vectors}\}$$

w.r.t. the given norm.

If we care about the precise norm, we will write $\lambda_i^{\|\cdot\|}$ or λ_i^K where K is the corresponding

centrally symmetric convex body.

Minkowski's second theorem

For any lattice L and any norm on $\mathbb{R}^n$,

$$\frac{2^n}{n!}\frac{\mathrm{covol}(L)}{\mathrm{Vol}(B(0,1))} \le \lambda_1(L)\cdots\lambda_n(L) \le 2^n \frac{\mathrm{covol}(L)}{\mathrm{Vol}(B(0,1))}$$

$B(0,1)$: w.r.t. given norm.

In next lecture we will prove the special case of the Euclidean norm.

Remarks: For the ℓ_2 norm,

$$\mathrm{Vol}(B(0,1)) \sim \frac{1}{\sqrt{n\pi}}\left(\frac{2\pi e}{n}\right)^{\frac{n}{2}}$$

$B(0,1)$: ball in $\mathbb{R}^n$ w.r.t. ℓ_2 norm

So RHS of the inequality, for ℓ_2 norm, you get a bound of size roughly

$$\left(\frac{2}{\sqrt{2\pi e}}\right)^n n^{n/2} = (cn)^{n/2}$$

2. The theorem is optimal for general norms. Take $\|\cdot\| = \|\cdot\|_\infty$ $L = \mathbb{Z}^n$, RHS is tight.

Take $\|\cdot\| = \ell_1$-norm $L = \mathbb{Z}^n$, LHS is tight.

Q Fix your favorite norm. Find a tight version of Minkowski's second thm for that norm. Generally open.