# Plan for today

- Minkowski's theorem & applications
- Shortest vector problem and orthogonality defect

**Recall:** GIVEN A LATTICE $\Lambda \subseteq \mathbb{R}^n$, FIND $v \in \Lambda \setminus \{0\}$ OF MINIMUM $\|\cdot\|$.

# The geometry of numbers: Minkowski's theorem

## Theorem

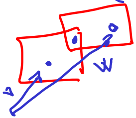
*Let $K \subseteq \mathbb{R}^n$ be a convex body which is* centrally symmetric *around the origin ($x \in K$ implies $-x \in K$). If $\underline{\mathrm{Vol}(K) \geq 2^n}$, then $K$ contains a nonzero integral vector $v \in \mathbb{Z}^n \setminus \{0\}$.*

$\underline{\text{PF.}}$ Let $K$ AS ABOVE AND SUPPOSE BY CONTRADICTION $K \cap \mathbb{Z}^n \setminus \{0\} = \emptyset$.

(1) WE CAN ASSUME WLOG $\mathrm{vol}(K) > 2^n$ (IF $\mathrm{vol} = 2^n$ THEN $\exists\, \delta > 0$: $(1+\delta)K \cap \mathbb{Z}^n \setminus \{0\} = \emptyset$)

$\forall v \in \mathbb{Z}^n$, consider $v + \frac{1}{2}K = S$ $\quad x \in S \Leftrightarrow 2x \in K$

$\underline{\text{CLAIM:}}$ $(v+S) \cap (w+S) = \emptyset$ FOR $\boxed{v \neq w} \in \mathbb{Z}^n$



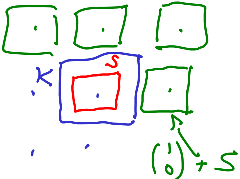
$\exists\, x = \boxed{v + \overset{S}{p} = \overline{w + q}^{\,\in S}}$

$p \in S \Leftrightarrow 2p \in K$

$q \in S \Leftrightarrow 2q \in K \Leftrightarrow -2q \in K$ (centrally symmetric)

$\Rightarrow \frac{1}{2}(2p - 2q) = p - q = w - v$ (convexity; $\in K$)

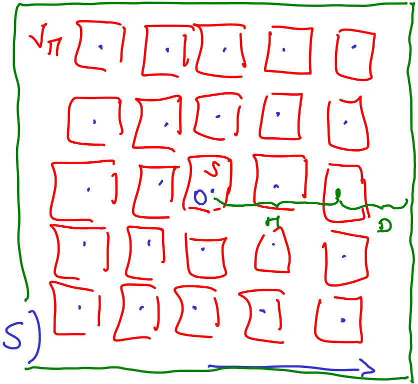
$K \cap \mathbb{Z}^n \setminus \{0\}$ ■



(I) $\boxed{\mathrm{vol}(K) > 2^n}$

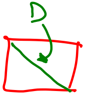
(II) $\forall\, v \neq w \in \mathbb{Z}^n,\ (v+S) \cap (w+S) = \emptyset$

$$M \in \mathbb{R}_+ \qquad V_M = \bigcup_{\substack{v \in \mathbb{Z}^n \\ \|v\|_\infty \le M}} v + S \qquad T_M$$



$$\mathrm{vol}(\boxed{V_M}) = \sum_{\substack{v \in \mathbb{Z}^n \\ \|v\|_\infty \le M}} \mathrm{vol}(S) = (2M+1)^n \mathrm{vol}(S)$$

D DIAMETER OF S



$$T_M = \{ x \in \mathbb{R}^n : \|x\|_\infty \le M + D \}$$

$$V_M \subseteq \boxed{T_M} \qquad \mathrm{vol}(V_M) \le \mathrm{vol}(T_M) = (2M + 2D)^n$$

[BOTH IN THE NUMERATOR AND DENOMINATOR, THE LEADING TERM IS $(2M)^n$]

$$1 \le \frac{\mathrm{vol}(T_M)}{\mathrm{vol}(V_M)} = \frac{1}{\mathrm{vol}(S)} \boxed{\frac{(2M+2D)^n}{(2M+1)^n}} \xrightarrow[M \to +\infty]{} \frac{1}{\mathrm{vol}(S)} \Rightarrow \mathrm{vol}(S) \le 1 \Rightarrow \mathrm{vol}(K) \le 2^n$$

$\frac{(2M+2D)^n}{(2M+1)^n} \xrightarrow[M \to +\infty]{} 1$

↯ ∎

# Lattice basis and lattice determinant

### Definition

A *basis* of a lattice $\Lambda$ is a matrix $B \in \mathbb{Z}^{m \times m}$ such that $\Lambda = \Lambda(B)$.

From what we proved during last lectures, we deduce:

- each lattice has a basis;
- if $B$ is a basis of a lattice $\Lambda$, then $\boxed{\det(\Lambda)} = |\det(B)|$ is well-defined.

$\Lambda = \Lambda(A) = \Lambda(H)$, where $(\overset{\mathbb{Z}^{m\times m}}{H} \mid 0)$ IS THE HNF OF $A$

IN PARTICULAR, $H$ IS A BASIS

FOR DET$(\Lambda)$ TO BE WELL-DEFINED EACH BASIS OF A LATTICE MUST HAVE THE SAME DETERMINANT (IN ABSOLUTE VALUE)

SHOWN LAST TIME

$B, B'$ BASIS OF $\Lambda \Rightarrow$ THEY HAVE THE SAME HNF $H$

UNIMODULAR

$B \cdot U = H = B' \cdot U' \Rightarrow B = B' \underbrace{U' \cdot U^{-1}}_{\text{DET} = \pm 1}$

$\Rightarrow |\det(B)| = |\det(B')|$

# Minkowski's theorem: Lattice version

**Theorem**

*Let* $\Lambda \subseteq \mathbb{R}^n$ *be a lattice and let* $K \subseteq \mathbb{R}^n$ *be a convex body of volume* $\boxed{\mathrm{Vol}(K) \geqslant 2^n \det(\Lambda)}$ *that is symmetric about the origin. Then* $K$ *contains a nonzero lattice point.*

PF.

$B$ BASIS OF $\Lambda$

$$B^{-1}\Lambda = \mathbb{Z}^n$$

$$\Lambda = \{y \in \mathbb{R}^n : y = Bx \text{ FOR SOME } x \in \mathbb{Z}^n\}$$

$$\phi(K) = B^{-1}K$$

$$K \cap \Lambda \setminus \{0\} \neq \emptyset \iff B^{-1}K \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset$$

$$\Leftarrow \boxed{\mathrm{vol}(B^{-1}K)} \geq 2^n$$

$$\mathrm{vol}(B^{-1}K) = \mathrm{vol}(K) \cdot |\det(B^{-1})| = \mathrm{vol}(K)\, |\det(B)|^{-1}$$

$$\det(\Lambda) = |\det(B)|$$

$$= \mathrm{vol}(K) \det(\Lambda)^{-1} = \frac{\mathrm{vol}(K)}{\det(\Lambda)}$$

$$\boxed{\geq 2^n}$$

∎

# First application: short vectors in lattices

**Theorem**

*A lattice $\Lambda \subseteq \mathbb{R}^n$ has a nonzero lattice point of length at most* $2 \cdot \sqrt[n]{\det(\Lambda)/V_n}$.

VOLUME OF THE UNIT BALL IN $\mathbb{R}^n$

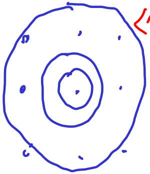
PF. APPLY MINKOWSKI WITH $K = B_n^R$ (BALL OF $\mathbb{R}^n$ OF RADIUS $R$)

$$\mathrm{vol}(B_n^R) = V_n \cdot R^n \overset{(1)}{\geq} 2^n \det(\Lambda)$$

FOR $R = 2\left(\frac{\det(\Lambda)}{V_n}\right)^{1/n}$ (1) IS SATISFIED

$$\Rightarrow \Lambda \cap B_n^R \setminus \{0\} \neq \emptyset$$

$$\Rightarrow \exists\, v \in \Lambda \setminus \{0\} : \|v\|_2 \leq R$$



R BIG ENOUGH SO THAT THE VOLUME SATISFIES $\geq 2^n \det(\Lambda)$

$\Downarrow$

BALL CONTAINS A LATTICE POINT $v \neq 0$

$\Downarrow$

$\|v\| \leq$ RADIUS

∎

# Exercise

Show that the bound given in the previous slide is asymptotically equivalent to

$$\boxed{\sqrt{\frac{2n}{\pi\, e}}}\,\boxed{\det(\Lambda)^{1/n}}(n\pi)^{1/2n}.$$

IMPORTANT TERMS

# Second application: simultaneous approximation

### Theorem (Dirichlet)

*Given reals* $Q > 1$ *and* $\alpha$, *there exists* $p, q \in \mathbb{Z}$ *with* $1 \leq q \leq Q$ *such that* $|\alpha - \frac{p}{q}| \leq \frac{1}{qQ}$.

### Theorem (Dirichlet, simultaneous approximation of reals)

*Given real numbers* $Q > 1$, $\alpha_1, \ldots, \alpha_n$, *there exists* $p_1, \ldots, p_n, q \in \mathbb{Z}$ *such that:*

SAME DENOMINATOR IN THE APPROXIMATION

- $1 \leq q \leq Q^n$;
- $|\alpha_j - \frac{p_j}{q}| \leq \frac{1}{qQ}$.

PF.

$$\underset{\mathbb{R}^{n+1}}{\underset{\cap}{\Lambda}} = \Lambda(B)$$

$$B = \left(\begin{array}{cc} \begin{matrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{matrix} & \begin{matrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{matrix} \\ \underbrace{\begin{matrix}0 & \cdots & 0\end{matrix}}_{n} & \frac{1}{Q^{n+1}} \end{array}\right) \begin{matrix} \left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\} n \\ \vphantom{\frac{1}{Q}} \end{matrix}$$

$$\det \Lambda = |\det(B)| = \frac{1}{Q^{n+1}}$$

$$C = \left\{ x \in \mathbb{R}^{n+1} : \quad \|x\|_\infty \leq \frac{1}{Q} \right\}$$

$(n+1)$ DIM. CUBE WITH SIDE LENGTH $\frac{2}{Q}$

$$\operatorname{vol}(C) = \frac{2^{n+1}}{Q^{n+1}} = 2^{n+1} \cdot \det(\Lambda)$$

$\Rightarrow$ BY MINKOWSKI, $C \cap \Lambda \setminus \{0\} \supseteq \{v\}$

BY DEFINITION OF LATTICE

$$v = \overbrace{\begin{bmatrix} 1 & & & \alpha_1 \\ & \ddots & 0 & \vdots \\ 0 & & \ddots & \vdots \\ & & 1 & \alpha_n \\ 0 & \cdots & 0 & Q^{-(n+1)} \end{bmatrix}}^{B} \overbrace{\begin{bmatrix} -p_1 \\ \vdots \\ -p_n \\ \boxed{q} \end{bmatrix}}^{x \in \mathbb{Z}^{n+1}}$$

$q \geq 0$

(BY SWITCHING TO $-v$ IF NECESSARY)

$$\exists\, v \in \Lambda$$

$$v \neq 0$$

$$v \in \left\{ x \in \mathbb{R}^{n+1} : \|x\|_\infty \leq \frac{1}{Q} \right\} = C$$

$$v = \begin{bmatrix} -p_1 + q\alpha_1 \\ -p_2 + q\alpha_2 \\ \vdots \\ -p_n + q\alpha_n \\ \dfrac{q}{Q^{n+1}} \end{bmatrix} \in C$$

$$\left.\begin{aligned} |-p_1 + q\alpha_1| &\leq \frac{1}{Q} \\ &\vdots \\ |-p_n + q\alpha_n| &\leq \frac{1}{Q} \end{aligned}\right\} \iff \left| -\frac{p_j}{q} + \alpha_j \right| \leq \frac{1}{Qq} \quad \checkmark$$

$$\forall j$$

$$\frac{q}{Q^{n+1}} \leq \frac{1}{Q} \iff \overset{?}{\boxed{1 \leq}}\, q \overset{\checkmark}{\leq} Q^n$$

IF $q = 0 \implies v \notin C$

$$v = \begin{bmatrix} -p_1 \\ \vdots \\ -p_n \\ 0 \end{bmatrix} \in \mathbb{Z}^n$$

$\square$

# Gram-Schmidt orthogonalization and orthogonality defect

Let $B \in \mathbb{Z}^{m \times m}$ be the basis of a lattice, and $B^*$ its GS orthogonalization. Then

BASIS OF SPAN(B)
BUT IN GENERAL
NOT OF $\Lambda(B)$

$$\boxed{B = B^* R}$$

HADAMARD BOUND

$$|\det(B)| \leq \Pi_i \, ||b_i||$$

for some upper triangular matrix $R = \begin{pmatrix} 1 & & & \mu \\ & 1 & & \\ & & \cdots & \\ 0 & & & 1 \end{pmatrix}.$

$$|\det(B)| = |\det(B^*)| \cdot |\underbrace{\det(R)}_{= 1}| = |\det(B^*)| = \Pi_i \, ||b_i^*|| \leq \Pi_i \, ||b_i||$$

### Definition

The *orthogonality defect* of $B$ is the value $\gamma = \frac{\prod_i ||b_i||}{|\det B|}$.

MEASURE OF "HOW FAR"
IS MY BASIS B FROM
AN ORTHOGONAL BASIS

# Small orthogonality defect [redacted] short non-zero vector

HELPS FOR FINDING

## Theorem

*Let $B \in \mathbb{Z}^{n\times n}$ be a basis of a lattice $\Lambda$ with orthogonal defect $\gamma$. Then a shortest non-zero vector of $\Lambda$ has the form*

$$v = \sum_i x_i b_i,$$

*with $x_i \in \mathbb{Z}$, $x_i \in [-\gamma, \gamma]$.*

BOTTOM LINE ⇒ # OF VECTORS TO BE CHECKED TO FIND THE SHORTEST NON-ZERO ARE $\leq (2\gamma+1)^n$

PF.

GM ORTH.

$$B = B^* \cdot R$$

$$\prod_i \|b_i\| = \gamma \cdot \prod_i \|b_i\|^* \iff \underset{\|b_1^*\|}{\underset{\rotatebox{90}{$\leq$}}{\|b_1\|}} \cdot \underset{\|b_2^*\|}{\underset{\rotatebox{90}{$\leq$}}{\|b_2\|}} \cdot \ldots \|b_n\| = \|b_1^*\| \cdot \|b_2^*\| \cdot \ldots \|b_n^*\| \cdot \gamma$$

$$\|b_n\| \leq \|b_n^*\| \cdot \gamma$$

TAKE ANY $v \in \Lambda$

$$v = \sum_i x_i b_i = B \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = B^* \cdot \begin{bmatrix} 1 & \ddots & \mu \\ 0 & & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ \boxed{x_n} \end{bmatrix} = B^* \begin{bmatrix} x_1' \\ x_2' \\ \vdots \\ x_{n-1}' \\ \boxed{x_n} \end{bmatrix}$$

THESE ARE THE SAME, FOR THE LAST ROW OF $R$ IS $(0 \ldots 0 1)$

$$v = \sum_i x_i b_i = B \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = B^* \cdot \begin{bmatrix} 1 & & \mu \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ \boxed{x_n} \end{bmatrix} = B^* \begin{bmatrix} x_1' \\ x_2' \\ \vdots \\ x_{n-1}' \\ \boxed{x_n} \end{bmatrix} = \sum_{i=1}^{n-1} x_i' b_i^* + x_n b_n^*$$

RECALL: THEY ARE THE SAME

$$\|v\| \geq |x_n| \, \|b_n^*\| \geq |x_n| \frac{\|b_n\|}{\gamma} \quad \text{IF} \quad |x_n| > \gamma \Rightarrow \|v\| > \|b_n\| \in \mathcal{L}$$

ALL $\|b_i^*\|$ ARE ORTHOGONAL

$\Rightarrow$ v IS NOT A SHORTEST VECTOR

FOR v TO BE A SHORTEST VECTOR WE MUST HAVE

$$|x_n| \leq \gamma$$

BY PERMUTING COLUMNS OF B
$\gamma$ DOES NOT CHANGE
(NOR DOES THE ARGUMENT OF THE PROOF)

$\Rightarrow |x_j| \leq \gamma \quad \forall j$