Def. (Additive group): $\Lambda \subseteq \mathbb{R}^n$ is an additive subgroup of $\mathbb{R}^n$ if:

① $0 \in \Lambda$ ② $\forall x, y \in \Lambda$: $x - y \in \Lambda$

→ in general discrete: $\exists \varepsilon$ s.t. $\forall x \in \Lambda$ $B(x, \varepsilon) \cap \Lambda = \{x\}$. It is equivalent for an additive sub.

Def. (Discrete): $\Lambda \subseteq \mathbb{R}^n$ (additive) is discrete if $\exists \varepsilon > 0$ s.t. $B(0, \varepsilon) := \{x \in \mathbb{R}^n : \|x\| < \varepsilon\} \cap \Lambda = \{0\}$.

Def. (Lattice): Λ is a lattice if it is discrete additive subgroup of $\mathbb{R}^n$.

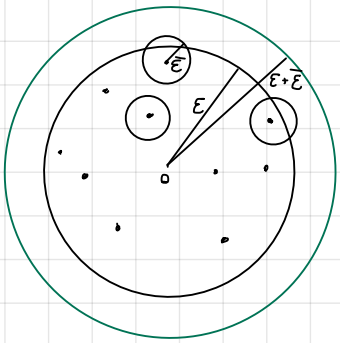
↓

N.B. The books we use require also: $\mathrm{Span}(\Lambda) = \mathbb{R}^n$. Instead, we can have lattice of dimension $k < n$.

Lemma: Λ lattice $\Rightarrow \forall \varepsilon > 0 \ |B(0, \varepsilon) \cap \Lambda| < +\infty$. If RHS holds (hp: additive) $\Rightarrow \Lambda$ is discrete.

Proof: $\Rightarrow$ Let's take the $\bar{\varepsilon}$ given by hypothesis. So $B(0, \bar{\varepsilon}) \cap \Lambda = \{0\}$. In particular, if $x \in \Lambda$ $B(x, \bar{\varepsilon}) \cap \Lambda = \{x\}$ in fact if $y \in B(x, \bar{\varepsilon}) \cap \Lambda \Rightarrow |y - x| \leq \bar{\varepsilon} \Rightarrow$ $y - x \in B(0, \bar{\varepsilon}) \cap \Lambda$ ($y - x \in \Lambda$ for subgroup hypothetis) $\Rightarrow y - x = 0 \Rightarrow y = x$.

So:



$B(x, \bar{\varepsilon})$ are disjoint changing x and so:

$$|\Lambda \cap B(0, \varepsilon)| \cdot \mathrm{Vol}\left(B(0, \bar{\varepsilon})\right) \overset{\text{Vol}(B(0,\bar{\varepsilon})) = \text{Vol}(B(x,\bar{\varepsilon}))\ \forall x \in \mathbb{R}^n}{=} \sum_{x \in \Lambda \cap B(0, \varepsilon)} \mathrm{Vol}\left(B(x, \bar{\varepsilon})\right) \overset{\text{disjoint}}{=} \mathrm{Vol}\left(\bigcup_{x \in \Lambda \cap B(0, \varepsilon)} B(x, \bar{\varepsilon})\right) \leq \mathrm{Vol}\left(B(0, \varepsilon + \bar{\varepsilon})\right)$$

But the quantities $\mathrm{Vol}(B(0, \bar{\varepsilon}))$ and $\mathrm{Vol}(B(0, \varepsilon + \bar{\varepsilon}))$ are finite so $|\Lambda \cap B(0, \varepsilon)|$ too.

$\Leftarrow$ Let's take an $\varepsilon > 0$. take $\bar{\varepsilon} := \min_{x \in B(0, \varepsilon) \cap \Lambda \setminus \{0\}} |x|$ (it is a minimum > 0 because $B(0, \varepsilon) \cap \Lambda$ is finite)

we take an ε:

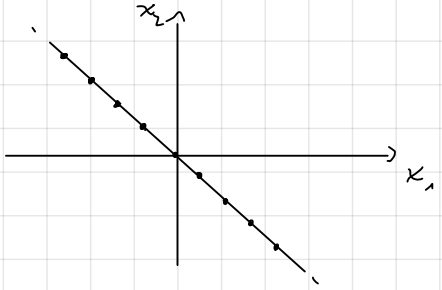
So $B\left(0, \frac{\bar{\varepsilon}}{2}\right) \cap \Lambda = \{0\}$. □

Corollary: Λ lattice $\Rightarrow \exists x \in \Lambda \setminus \{0\}$ of minimal norm ($|x| \leq |y| \ \forall y \in \Lambda \setminus \{0\}$). Also called "shortest vector"

Proof: as in $\Leftarrow$ of the previous proof. □

Example: ① $\Lambda = \mathbb{Z}^n \subseteq \mathbb{R}^n$ is a lattice. ($\varepsilon < 1$)

② $H = \{x \in \mathbb{R}^{n+1} : \sum_{i=1}^{n} x_i = 0\}$ $\Lambda := (H \cap \mathbb{Z}^{n+1}) \subseteq \mathbb{Z}^{n+1}$



③ $L = \{ x \cdot \alpha + y \cdot \beta : x, y \in \mathbb{Z} \} \subseteq \mathbb{R}$, $\alpha, \beta \in \mathbb{R}$ to be specified!

$L \subseteq \mathbb{R}$: obvious

For example if $\alpha = 1$, $\beta = \sqrt{2}$ L is not discrete ← Exercise 2

④ $M = \{ x \in \mathbb{R}^n , \sum_{i=1}^{n} x_i = 1 \pmod{\mathbb{Z}} \}$ no lattice $(0 \notin M)$

Theorem Let $b_1, \dots, b_K \in \mathbb{R}^n$ linear independent. ($\mathrm{Span}\{b_1, \dots, b_K\} = \mathbb{R}^n$) $(n \geq 1)$. So:

$$\Lambda(b) = \left\{ \sum_{i=1}^{K} x_i b_i : x_i \in \mathbb{Z}, i = 1, \dots, K \right\} = \{ B \cdot x : x \in \mathbb{Z}^n , B = (b_1, \dots, b_K) \in \mathbb{R}^{n \times K} \text{ full rank} \}$$

Proof. Subgroup: obvious.

Discrete:

Gram-Schimdt : Let $b_1, \dots, b_K \in \mathbb{R}^n$ lin. ind. ; so $\exists\, b_1^*, \dots, b_K^*$ s.t. pairwise are orthogonal $\left((b_i^*)^T \cdot b_j^* = 0 \quad \forall i \neq j \right)$ and $\mathrm{Span}\{b_1, \dots, b_K\} = \mathrm{Span}\{b_1^*, \dots, b_K^*\}$.

Proof. $\forall j$ we define b_j^* s.t. $\mathrm{Span}\{b_1, \dots, b_j\} = \mathrm{Span}\{b_1^*, \dots, b_j^*\}$ and $b_1^*, \dots, b_j^*$ are orthogonal:

$b_{j+1}^* := b_{j+1} - \sum_{i=1}^{j} \mu_i b_i^*$. We have to find μ_i s.t. we have orthogonality

$$\langle b_{j+1} - \sum_{i=1}^{j} \mu_i b_i^* , b_s^* \rangle = 0 \quad \forall 1 \leq s \leq j \iff \text{(inductive hp.)} \quad \langle b_{j+1}, b_j^* \rangle - \mu_s \langle b_s^*, b_s^* \rangle = 0$$

$$\iff \mu_s = \frac{\langle b_{j+1}, b_s^* \rangle}{\langle b_s^*, b_s^* \rangle} \iff \underbrace{(b_1, \dots, b_n)}_{\in M(n,K)} = \underbrace{(b_1^*, \dots, b_n^*)}_{\in M(n,K)} \cdot \begin{pmatrix} 1 & \mu_1 & \cdots & \mu_1 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mu_{K-1} \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in M(K,K) \quad \square$$

Now, $\varepsilon := \frac{\min \|b_i^*\|}{2}$, we see $B(0,\varepsilon) \cap \Lambda \setminus \{0\} = \emptyset$:

$v \in \Lambda(B) = \{ B \cdot x : x \in \mathbb{Z}^n \} \setminus \{0\}$. This means $\exists\, x \in \mathbb{Z}^n \setminus \{0\}$ s.t. $v = B \cdot x$. Suppose

x_t is the last component of x that is not zero i.e. $x = \begin{pmatrix} x_1 \\ \vdots \\ x_t \\ 0 \end{pmatrix}$. So:

$$\|v\|^2 = \|B \cdot x\|^2 = \| B^* \cdot \underbrace{\begin{pmatrix} 1 & & & \mu \\ & \ddots & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \cdot x}_{\begin{pmatrix} y_0 \\ \vdots \\ y_{t-1} \\ x_t \\ 0 \\ \vdots \\ 0 \end{pmatrix}} \|^2 = \sum_{i=1}^{t-1} (y_i)^2 \|b_i^*\|^2 + \underbrace{x_t^2}_{\geq 1} \|b_t^*\|^2 \geq \|b_t^*\|^2 \geq \min_i \|b_i^*\|^2$$

(Pythagoras : b_i^* are orthogonal; $x \in \mathbb{Z}^n$)

This proves $\Lambda(B)$ is discrete and also the following Corollary. $\square$

Corollary: Let $B \in \mathbb{R}^n \times \mathbb{R}^k$ full rank and $B = B^* \cdot \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ Gram Schmidt orth. of B.

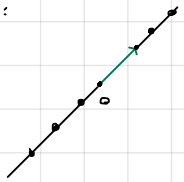
Then $\forall v \in \Lambda(B) \setminus \{0\}$: $\|v\| \geq \min_{i=1,\dots,k} \|b_i^*\|$ (and so the $sv(\Lambda) \geq \min_{i=1,\dots,k} \|b_i^*\|$

Theorem: $\Lambda \subseteq \mathbb{R}^n$ is a lattice $\Leftrightarrow \exists\, b_1, \dots, b_k \in \mathbb{R}^n$ indip. s.t. $\Lambda = \left\{ \sum_{i=1}^{k} x_i b_i : x_i \in \mathbb{Z},\ i = 1, \dots, n \right\}$

Proof: $\boxed{\Leftarrow}$ Previous theorem.

$\boxed{\Rightarrow}$ Induction on $\dim(\Lambda) := \dim(\text{Span}(\Lambda))$.

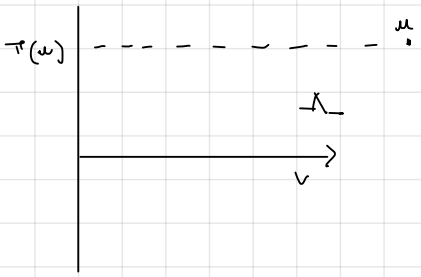
$n = 1$:



$b \in \Lambda$ of minimal norm. Suppose $\exists\, v \in \Lambda$ s.t. $v = \lambda \cdot b$, $\lambda \notin \mathbb{Z}$

but $v - \lfloor \lambda \rfloor \cdot b \in \Lambda$ and $\|v - \lfloor \lambda \rfloor \cdot b\| < \|b\|$. ↯

$n-1 \longrightarrow n$: Let v in the lattice ($v \neq 0$) of minimum norm. Now:



where $\pi(u) = u - \lambda \cdot v$, $\lambda \in \mathbb{R}$ s.t. $(u - \lambda v) \perp v$

↑ varia al variare di u

Now, $\pi(\Lambda)$ is a lattice. ← Exercise 3

So for inductive hypothesis $\pi(\Lambda)$ has a basis $b_1', \dots, b_{k-1}' \in \mathbb{R}^n$.

Let $b_1, \dots, b_{k-1} \in \Lambda$ s.t. $\pi(b_i) = b_i'$ $i = 1, \dots, k-1$, then $\Lambda = \left\{ \sum_{i=1}^{k-1} x_i b_i + x_k v \mid x_1, \dots, x_k \in \mathbb{Z} \right\}$.

Infact, suppose $w \in \Lambda$, $\pi(w) = \sum_{i=1}^{k-1} x_i b_i'$ but $\pi(w) = w - \lambda_v v$ and $b_i' = b_i - \lambda_i v$

$w = \sum_{i=1}^{k-1} x_i b_i' + \lambda_v v = \sum_{i=1}^{k-1} x_i b_i + \left(\lambda_v - \sum_{i=1}^{k-1} \lambda_i \right) v$. If $\lambda_v - \sum_{i=1}^{k-1} \lambda_i \notin \mathbb{Z}$, we consider

$w - \left(\sum_{i=1}^{k-1} x_i b_i + \lfloor \lambda_v - \sum_{i=1}^{k-1} \lambda_i \rfloor v \right) \in \Lambda$ and has norm $\leq \|v\|$, ↯.

□

Corollary: Every lattice has a basis.

Notation: If $b_1, \dots, b_K$ basis of Λ, we let: $B = (b_1, \dots, b_K) \in \mathbb{R}^{n \times K}$

and we write $\Lambda(B) = \{ B \cdot x : x \in \mathbb{Z}^K \}$.

Question: When $B \in \mathbb{R}^{n \times K_1}$, $C \in \mathbb{R}^{n \times K_2}$ of full column rank, generate the same lattice?

- A first necessary condition is that $K_1 = K_2$ ($\dim \operatorname{Span}(\Lambda(B)) = \dim \operatorname{Span}(\Lambda(C))$, remember $\dim(\Lambda) := \dim \operatorname{span}(\Lambda)$ as subspace of $\mathbb{R}^n$).

Theorem: Let $B, C \in \mathbb{R}^{m \times K}$ of rank K. One has:

$$\Lambda(B) = \Lambda(C) \iff \underbrace{\exists\, u \in \mathbb{Z}^{K \times K} \text{ with } \det(u) = \pm 1}_{\text{unimodular}} \text{ with } B = C \cdot u$$

[**Recall the matrix inversion formula**:

$A \in \mathbb{K}^{n \times n}$, $\mathbb{K}$ field with $\det(A) \neq 0$: $A^{-1} = \frac{1}{\det(A)} \cdot \underbrace{\operatorname{adj}(A)}_{n \times n}$

- Take $A = (a_{ij})$
- Define $B = (b_{ij})$ where $b_{ij} = (-1)^{i+j} \det M_{ij}$ where M_{ij} is the minor of A obtained eliminating the i^{th}-row and j^{th}-column
- $(\operatorname{adj}(A))_{ij} = b_{ji}$ (transpose of B)]

Proof.

$\boxed{\Leftarrow}$: Let $B = C \cdot u$ with $u \in \mathbb{Z}^{K \times K}$ unimodular. So each column of B is an element of $\Lambda(C)$, so $\Lambda(B) \subseteq \Lambda(C)$. But $u^{-1} = \frac{1}{\det(u)} \cdot \operatorname{adj}(u)$ and in general $\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$

$\Rightarrow u^{-1} \in \mathbb{Z}^{n \times n}$ ($\det(u) = \pm 1$) $\Rightarrow \Lambda(C) \subseteq \Lambda(B)$.

$\boxed{\Rightarrow}$ $\forall$ col. $b_i \in B$ $\exists\, x_i \in \mathbb{Z}^K$ s.th. $b_i = C x_i$, $i = 1, \dots, K$. So $B = C \cdot x$ with $x \in \mathbb{Z}^{K \times K}$.

Similarly: $\exists\, Y \in \mathbb{Z}^{K \times K}$ with $C = B \cdot Y$. Combining this: $B = B \cdot Y \cdot X$. Since the columns of B are linearly independent $\Rightarrow Y \cdot X = \mathrm{Id}_K \Rightarrow 1 = \det(I_K) = \det(Y) \det(X) \Rightarrow$

$\det(Y) = \pm 1$, $\det(X) = \pm 1$ ($\det(Y), \det(X) \in \mathbb{Z}$) $\Rightarrow$ both X and Y are unimodular.

So $B = C \cdot X$ with $X \in \mathbb{Z}^{K \times K}$ unimod.

□

Achtung: $\varphi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$, $x \longmapsto A \cdot x$ is an isomorphism $\iff A \in \mathbb{Z}^{n \times n}$ unimodular.

Observation: Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $B, C \in \mathbb{R}^{n \times K}$ two bases of Λ. Let $u \in \mathbb{Z}^{K \times K}$ unimod. with $B = C \cdot u$. Now:

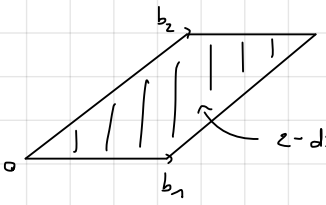
$$\det(\underbrace{B^T \cdot B}_{\mathbb{Z}^{K \times K}}) = \det(u^T C^T C u) = \underbrace{\det(u^T)}_{\det(u)} \cdot \det(C^T C) \cdot \det(u) \overset{\det^2(u) = 1}{=} \det(C^T C)$$

So $\det(B^T \cdot B)$ is invariant of Λ.

Def.: Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $B \in \mathbb{R}^{n \times K}$ be a basis of Λ. We call

$\det(\Lambda) := \sqrt{\det(B^T \cdot B)}$ the determinant of the basis (well defined for the previous observation).

Picture:



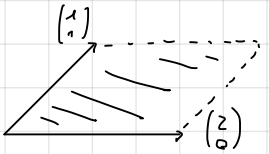
$b_1, b_2 \in \mathbb{R}^3$ basis of Λ

2-dim Volume $\sqrt{\det(B^T \cdot B)}$ with $B = (b_1, b_2) \in \mathbb{R}^{3\times 2}$

Def.: $P(B) = \left\{ \sum_{i=1}^{n} \lambda_i b_i : 0 \le \lambda_i < 1 \right\}$ is called fundamental parallelepiped of lattice B.

From the previous observation we can claim $\mathrm{Vol}(P(B))$ is invariant.

Example: $\Lambda = \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} : x_1, x_2 \in \mathbb{Z} \right\}$



Now, $(v_1 - v_2, v_2)$ is a basis for Λ too $\left((v_1 - v_2, v_2) = (v_1, v_2) \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \right)$

So, $P((v_1 - v_2), v_2) = P(v_1, v_2)$.

Observation: From now, unless explicity stated, **we assume $\dim(\Lambda) = n$**. (full-dimensional lattices).

So if $B \in \mathbb{R}^{n\times n}$ lattice basis of $\Lambda \subseteq \mathbb{R}^{n\times n}$: $\det(\Lambda) = \sqrt{\det(B^T B)} = |\det(B)|$

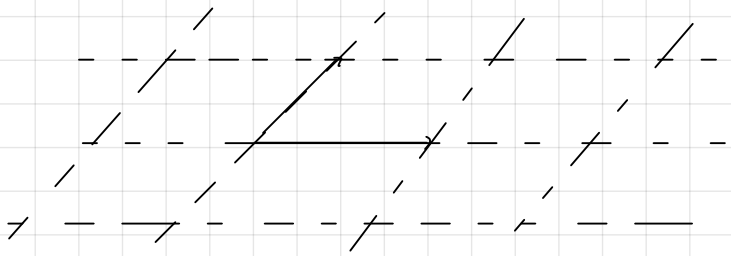
Another proof that $\mathrm{Vol}(P(B))$ is invariant

Obs.: For $x \in \mathbb{R}^n$ $\exists!$ $\lambda \in \mathbb{R}^n$ with $x = B \cdot \lambda = \sum_{i=1}^{n} \lambda_i \cdot b_i = \sum_{i=1}^{n} \left[\lfloor \lambda_i \rfloor \cdot b_i + (\lambda_i - \lfloor \lambda_i \rfloor) \cdot b_i \right] =$

$= \underbrace{\sum_{i=1}^{n} \lfloor \lambda_i \rfloor \cdot b_i}_{\in \Lambda(B)} + \underbrace{\sum_{i=1}^{n} (\overbrace{\lambda_i - \lfloor \lambda_i \rfloor}^{\in [0,1)}) \cdot b_i}_{P(B)}$.

So **$x = v + u$, $v \in \Lambda$ and $u \in P(B)$**. This decomposition is unique.

So **$\mathbb{R}^n = \bigcup_{v \in \Lambda} (\{v\} \oplus P(B))$**, in picture:



if $x = v + u = v' + u' \Rightarrow$

$\Lambda \ni v - v' = u' - u \in \Lambda \cap P(B)$

So $u' - u = \sum_i \lambda_i b_i$ with $\lambda_i \in \mathbb{Z}$ but

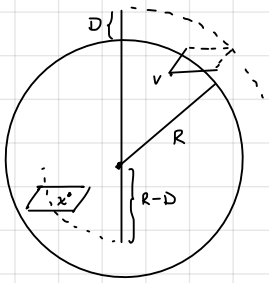
$\{b_i\}$ is a basis and $u' - u \in P(B) \Rightarrow$

$\lambda_i = 0 \ \forall i$.

Thm.: Let $B \in \mathbb{R}^{n\times n}$ be basis of lattice $\Lambda \subseteq \mathbb{R}^n$ $|\det(B)|$ is an invariant of Λ.

different proof:

$B' = B \cdot u$, So:



$v \in (B(0,R) \cap \Lambda)$

$v + P(B) \subseteq B(0, R+D)$ ← this D not dipend on v beause $|B(0,R) \cap \Lambda| < +\infty$ and we take the max

↓ also to satisfy this condition

$x \in B(0, R-D)$

Fundamental parallelipiped containing $x \subseteq B(0, R)$

for the previous obs.

$$\mathrm{Vol}\left(B(0,R-D)\right) \leq |B(0,R) \cap \Lambda| \quad \mathrm{Vol}(P(B)) \leq \mathrm{Vol}\left(B(0,R+D)\right)$$

↓ divide by $\mathrm{Vol}(B(0,R))$

$$\left(\frac{R-D}{R}\right)^n \leq \frac{|B(0,R) \cap \Lambda|}{\mathrm{Vol}(B(0,R))} \mathrm{Vol}(P(B)) \leq \left(\frac{R+D}{R}\right)^n$$

density of Λ (is invariant by definition)

When $R \to +\infty$ $\quad 1 \leq |B(0,R) \cap \Lambda| \dfrac{\mathrm{Vol}(P(B))}{\mathrm{Vol}(B(0,R))} \leq 1$, so $\mathrm{Vol}(P(B)) = \lim_{R \to +\infty} \dfrac{\mathrm{vol}(B(0,R))}{|B(0,R) \cap \Lambda|}$.

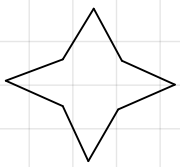
□

Def.: $K \subseteq \mathbb{R}^n$ is convex if $\forall x, y \in K$ and $\lambda \in [0,1]$, $\lambda x + (1-\lambda) y \in K$.

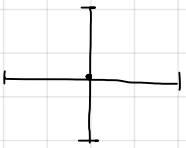
Question: $K \subseteq \mathbb{R}^n$ is convex and $K \cap \mathbb{Z}^n = \emptyset$. We can say something about $\mathrm{Vol}(K)$? No

I can make K as long as I want

Def.: $K \subseteq \mathbb{R}^n$ is centrally symmetric if $\forall x \in K \Rightarrow -x \in K$.



(Star-Shape)

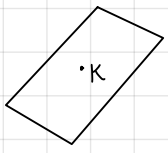


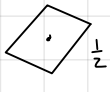
Observation: If $K \neq \emptyset$ is centrally simmetric and convex, then $K \cap \mathbb{Z}^n \supseteq \{0\}$.

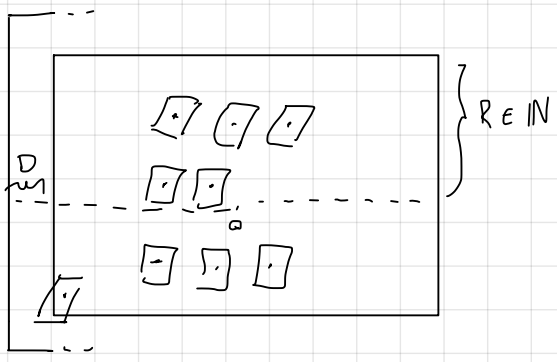
Indeed if $x \in K \overset{sym}{\Rightarrow} -x \in K$ and $0 = \frac{1}{2} x + \frac{1}{2}(-x) \in K$.

Thm. (Minkoski): Let $K \subseteq \mathbb{R}^n$ be centrally symmetric, convex, bounded and of volume $\mathrm{vol}(K) > 2^n$, then $\exists\, v \in (\mathbb{Z}^n \setminus \{0\} \cap K)$. (**Obs.** if K is closed it is sufficient $\mathrm{vol}(K) \geq 2^n$)

Proof $K' = \frac{1}{2} \cdot K = \left\{ \frac{1}{2} x : x \in K \right\}$. Take $x \in \mathbb{Z}^n$, $\|x\|_\infty \leq R$ and consider the translates $x + \frac{1}{2} K$.







If two translcts intersects: $\exists\, x_1 \neq x_2 \in \mathbb{Z}^n$ and $v_1, v_2 \in \frac{1}{2}K$: $x_1 + v_1 = x_2 + v_2$ but

$v_1 = \frac{1}{2}K_1$ $K_1 \in K$ $v_2 = \frac{1}{2}K_2$ $K_2 \in K$ $\Rightarrow$ $x_1 - x_2 = v_2 - v_1 = \frac{1}{2}K_2 - \frac{1}{2}K_1$ $\Rightarrow$ we have the thesis.

($x_1 - x_2 \in \mathbb{Z}^n \setminus \{0\}$; $\frac{1}{2}K_2 - \frac{1}{2}K_1 \in K$)

($-K_1 \in K$ because symm. so $\frac{1}{2}K_2 + \frac{1}{2}(-K_1) \in K$ because of convexity)

Suppose these translates $x + \frac{1}{2}\cdot K$ $x \in \mathbb{Z}^n$ don't intersect:

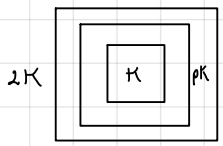
$$\left[2(R+D)\right]^n \geq \text{Vol}\left(\bigcup_{\substack{x \in \mathbb{Z}^n \\ \|x\|_\infty \leq R}} \left(x + \tfrac{1}{2}K\right) \right) = \sum_{\substack{x \in \mathbb{Z}^n \\ \|x\|_\infty \leq R}} \text{Vol}\left(x + \tfrac{1}{2}K\right) \geq (2R+1)^n (1+\varepsilon)$$

(we use that K is bounded; $\geq (1+\varepsilon)$ because $\text{Vol}(K) > 2^n$)

So $1 \geq \left(\frac{2R+1}{2R+2D}\right)^n (1+\varepsilon)$ and for $R \to +\infty$ $1 \geq 1+\varepsilon$, $\lightning$

□

Proof of the observation: Suppose K is closed and $\text{vol}\, A = 2^d \det \Lambda$. We consider the rescaled K : ρK with $1 < \rho < 2$:



Now, $\text{vol}(\rho K) = \rho^d \text{vol}(K) > 2^d \det \Lambda$, so there is a non-zero point in $\mathbb{Z}^n$ $u_\rho \in \rho K$.

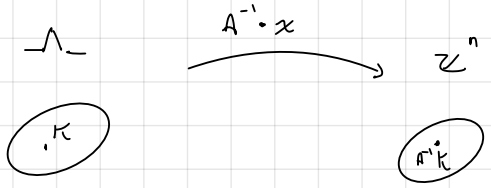
So, $\lim_{\rho \to 1^+} d(u_\rho, K) = 0$ but K is compact so $\exists$ a limit point (punto di accumulazione) in K of the sequence

But we also know that $\mathbb{Z}^n$ is discrete so the sequence $\{u_\rho\}$ has to stabilize and so the limit point is also in $\mathbb{Z}^n$.

□

Let's assume $\Lambda \subseteq \mathbb{R}^n$ full-dim. lattice. $\Lambda = \Lambda(A)$, $A \in \mathbb{R}^{n\times n}$ nonsingular.

$v \in \Lambda(A) \iff \exists x \in \mathbb{Z}^n : v = Ax$. We define $v \longmapsto A^{-1}v = x \in \mathbb{Z}^n$.



if $V = vol\left(A^{-1}K\right) > z^n$, then $\exists x \in \left(\mathbb{Z}^n \setminus \{0\} \cap A^{-1}K\right)$ (Minkowski), but $vol\left(A^{-1}K\right) = |\det(A^{-1})|\, vol(K) = \frac{vol(K)}{|\det(A)|}$

and $\exists x \in \left(\mathbb{Z}^n \setminus \{0\} \cap A^{-1}K\right) \iff \exists v \in \left(\Lambda(A) \setminus \{0\} \cap K\right)$.

Thm. Let $\Lambda \subseteq \mathbb{R}^n$ be a full-dimensional lattice, $K \subseteq \mathbb{R}^n$ bounded, centrally symmetric and convex with $vol(K) > z^n |\det(\Lambda)| \Rightarrow (\Lambda \setminus \{0\}) \cap K \neq \emptyset$.

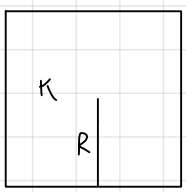
Def. : Let $\Lambda \subseteq \mathbb{R}^n$ be a full dimensional lattice, $i \in \{1, \dots, n\}$. $\lambda_i := \min\{r > 0 : B(0,r) \cap \Lambda$ is of dimension $\geq i\} = \min\{r > 0 : B(0,r) \cap \Lambda$ contains i linearly indipendent lattice points$\}$. λ_i is called the *i-th successive minimum of* Λ. λ_1 is also denoted by $SV_2(\Lambda)$ (lenght of the shortest non zero lattice vector with respect to l_2-norm). $SV_\infty(\Lambda)$ = the same with l_∞.

Theorem : Let $\Lambda \subseteq \mathbb{R}^n$ be a full-dimensional lattice :

① $SV_\infty \leq \sqrt[n]{\det(\Lambda)}$ ② $SV_2 \leq \sqrt{n} \cdot \sqrt[n]{\det(\Lambda)}$

Proof ② : follows immediatly from ① because $\|\cdot\|_2 \leq \sqrt{n}\, \|\cdot\|_\infty$

① :



$\{x \in \mathbb{R}^n : \|x\|_\infty \leq R\}$

$Vol(K) = 2^n R^n$; if $2^n R^n \geq z^n \cdot \det(\Lambda)$ ($\det(\Lambda)$ compact so $\exists R$) $\Rightarrow (\Lambda \setminus \{0\}) \cap K \neq \emptyset$

Thus, if $R = \sqrt[n]{\det(\Lambda)}$ then $\exists v \in \Lambda \setminus \{0\}$ of $\|v\|_\infty \leq R$.

□

Lattice basis reduction : How to change the basis, such that the shortest lattice vector can be "easily" determined ($\nearrow 2^{O(n)}$)? Let's star very simple : given $\Lambda \subseteq \mathbb{Z}$, $\Lambda = \{a \cdot x + b \cdot y : x, y \in \mathbb{Z}$ $a, b \in \mathbb{Z} \setminus \{0\}$ given$\} =$

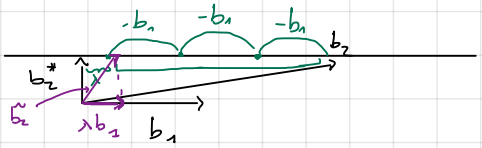
$= \{gcd(a,b)\, x : x \in \mathbb{Z}\} \Rightarrow SV_2(\Lambda) = gcd(a,b)$ and so we can use euclidian algorithm.

the 2-d case : $\Lambda \subseteq \mathbb{R}^2$ $\Lambda = \{x b_1 + y b_2 : x, y \in \mathbb{Z}\}$

Assume $\|b_2\| \geq \|b_1\|$ (*). So, let's describe Algorithm of Lagrange & Gauss:

Suppose $\|b_2^*\| \leq \frac{1}{4}\|b_2\|$ Analogue of Divisor with remainder in Euclid. We want

$(b_1, b_2) \longrightarrow (b_1, \tilde{b_2})$ other basis of the lattice in which $\tilde{b_2}$ is shorter than b_2.



$$b_2^* = b_2 - \boxed{\frac{\langle b_1, b_2\rangle}{\langle b_1, b_1\rangle}} b_1 \quad \left(\text{then } \langle b_2^*, b_1\rangle = 0\right), \qquad \mu = \frac{\langle b_1, b_2\rangle}{\langle b_1, b_1\rangle}$$

μ = the nearest integer

$\tilde{b_2} = b_2 - \lfloor \mu \rceil b_1 = b_2^* + \lambda b_1$ where $|\lambda| \leq \frac{1}{2}$. So:

$$\|\tilde{b_2}\| = \|b_2^* + \lambda b_1\| \leq \|b_2^*\| + \frac{1}{2}\|b_1\| \leq \frac{3}{4}\|b_2\|$$

$\|b_2^*\| \leq \frac{1}{4}\|b_2\|$, $\|b_1\| \leq \|b_2\|$

Suppose at the beginning: $b_1, b_2 \in \mathbb{Z}^2$, meaning $\Lambda \subseteq \mathbb{Z}^2$.

(*) Every time I change the basis I have to control if $\|b_1\| \geq \|b_2\|$ or $\|b_2\| \geq \|b_1\|$ so I have to put b_2 and b_1

Process: while $\|b_2^*\| \leq \frac{1}{4}\|b_2\|$ replace b_2 by $\tilde{b_2}$. After i iterations:

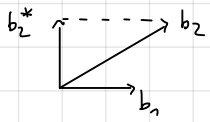
if is a general lattice we can use (SV_2)

$$1 \leq \|b_{1\,NEW}\|^2 \cdot \|b_{2\,NEW}\|^2 \leq \|b_{1\,BEG.}\|^2 \cdot \|b_{2\,BEG.}\|^2 \cdot \left(\frac{3}{4}\right)^{2i}$$

(b_1, b_2 BEG.; $\Lambda \subseteq \mathbb{Z}^2$; see exercise 1 for the computation)

$\Rightarrow$ total number of iterations is $O\left(\log\left(\|b_2\|^2\right)\right)$ polynomial in input encoding of basis b_1, b_2.

Suppose again: $\|b_2\| \geq \|b_1\|$ and furthermore $\|b_2^*\| \geq \frac{1}{4}\|b_2\|$. Shortest vector can quickly be retrieved:



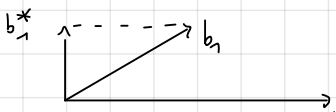
$$v = x_1 b_1 + x_2 b_2 = x_1 b_1 + x_2\left(b_2^* + \lambda b_1\right)$$

$$\|v\| \geq |x_2|\,\|b_2^*\| \geq |x_2| \cdot \frac{\|b_2\|}{4} \geq \frac{|x_2|}{4}\|v\| \quad \Rightarrow |x_2| \leq 4$$

($\|v\| \geq$ Pythagoras; $\geq \frac{\|b_2\|}{4}$ shortest vector)

If v is shortest vector, then $\|v\| \leq \|b_2\|$ and therefore $|x_2| \leq 4$ (9 candidates for x_2).

On the other hand:



(b_2, b_1^*) and (b_1, b_2^*) are cso basis

$$\|b_2\| \cdot \|b_1^*\| = \det(\Lambda) = \|b_1\|\,\|b_2^*\| = \|b_1\| \cdot \|b_2\|\,\gamma$$

$\|b_2^*\| = \gamma\|b_2\|$ $\gamma \geq \frac{1}{4}$

$$\|b_1^*\| = \gamma\|b_1\| \geq \frac{\|b_1\|}{4} \quad \overset{\text{same argument}}{\Rightarrow} \quad |x_1| \leq 4$$

Scheme of the algorithm:

$(b_1, b_2) = (b_1, \tilde{b})$ or $(b_1, b_2) = (\tilde{b}, b_2)$ $\rightarrow (b_1, b_2)$ basis, take the maximum in norm, $\overline{b}$

if $\|\overline{b}^*\| \leq \frac{1}{4}\|\overline{b}\|$: do the reduction algorithm obtaining $\tilde{b}$

if $\|\overline{b}^*\| \geq \frac{1}{4}\|\overline{b}\|$: we find the two coordinates x_1, x_2 of the shortest vector

Def. : (Orthogonality defect): Let $B \in \mathbb{R}^{n \times n}$ non-singular. $\gamma(B)$ is the orthogonality defect and is defined as $\gamma(B) = \frac{\prod_i \|b_i\|}{\prod_i \|b_i^*\|} = \frac{\prod_i \|b_i\|}{|\det(B)|}$ $\left(B = B^* \begin{bmatrix} \ddots & \mu \\ 0 & \ddots \end{bmatrix} \quad |\det(B)| = \prod_i \|b_i^*\| \right)$

Exercises : Let $\Lambda(B) \subseteq \mathbb{R}^n$ be full dim. lattice and B have orthogonality defect $\gamma(B)$. Let $v = B \cdot x \quad x \in \mathbb{Z}^n \setminus \{0\}$ be a shortest vector of $\Lambda(B)$. Then $\|x\|_\infty \leq \gamma(B)$. ← See Ex. 5

This shows that the shortest vector can be retrieved in time $(2\gamma(B)+1)^n \rightarrow \left(\begin{array}{l} \gamma = 5 \quad \#x \in \mathbb{Z}^n : \|x\|_\infty \leq 5 \\ \leq (11)^n \end{array} \right)$

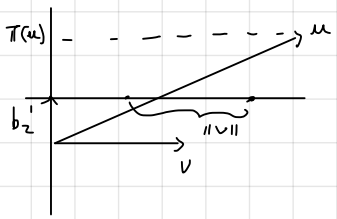
Meta thm. : Let $\Lambda \subseteq \mathbb{R}^n$ full-dim lattice. Λ has a basis $B \in \mathbb{R}^{n \times n}$ with $\gamma(B) \leq f(n)$ with f function depending only on n.

Let's go back to the 2-dim. case: $\Lambda \subseteq \mathbb{R}^n$ has basis (b_1, b_2) such that:

$\|b_2^*\| \geq \frac{1}{4}\|b_2\|$, $\gamma(b_1, b_2) = \frac{\|b_1\|\|b_2\|}{\|b_1\|\|b_2^*\|} \leq 4 \Rightarrow f(2) \leq 4$.

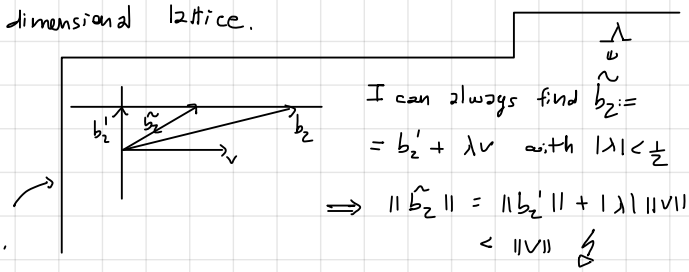
Thm. : Let $\Lambda \subseteq \mathbb{R}^n$ be full-dimensional lattice. Then Λ has a basis $B \in \mathbb{R}^{n \times n}$ with $\gamma(B) \leq 2^{\frac{(n-1)n}{2}}$

Proof **2-D case** : Let $\Lambda \subseteq \mathbb{R}^2$ be full-dim lattice and $v \in \Lambda \setminus \{0\}$ be shortest vector w.r.t. l_2-norm.



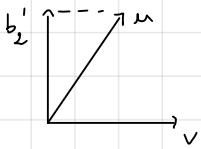
$\Lambda' = \pi(\Lambda)$ is one dimensional lattice.

$\Lambda' = \{b_2' x : x \in \mathbb{Z}\}$



If $\|b_2'\| < \frac{1}{2}\|v\|$ ↯ to v being the shortest vector.

But: $u \in \Lambda$ with $\pi(u) = b_2'$ makes (v, u) basis of Λ. Picking $u \in \Lambda$: $\|u\| \leq \frac{1}{2}\|v\| + \|b_2'\|$ has orthogonality defect ≤ 2, indeed:



I have to show $\|u\|\|v\| \leq 2\|v\|\|b_2'\|$, so we have to show

$\|u\| \leq 2\|b_2'\|$ but $\|u\| = \|b_2'\| + \frac{1}{2}\|v\| \leq 2\|b_2'\|$.

□

Rothvoss: pp. 13-18 LLL-Algorithm

Lezione 11 Marzo (4)

Recap: Given $\Lambda \subseteq \mathbb{R}^n$ full-dimensional, there exists a basis $B \in \mathbb{R}^{n \times n}$ of Λ s.t

$$\gamma(B) = \frac{\prod_{i=1}^{n} \|b_i\|}{|\det(B)|} \leq 2^{\frac{n(n-1)}{2}} \quad \text{(Exercise \#2)}$$

LLL-Algorithm: Efficient algorithm that compute a basis with similar orthogonality defect.

Relevence of $\gamma(B)$: $B \in \mathbb{R}^{n \times n}$ non singular, for Gram-Schimdt $B = B^* \begin{bmatrix} 1 & & \mu \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$

Recap: $\boxed{SV_2(\Lambda(B)) \geq \min_i \|b_i^*\|}$: $B^* = (b_1^*, \dots, b_n^*)$, $v \in \Lambda(B) \setminus \{0\}$ $v = B \cdot x$ $x \in \mathbb{Z}^n$

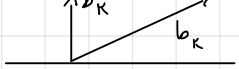
$$x = \begin{bmatrix} x_1 \\ \vdots \\ x_k \\ 0 \end{bmatrix} \neq 0, \quad v = B^* \begin{bmatrix} 1 & & \mu \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = B^* \begin{bmatrix} y_1 \\ \vdots \\ y_{k-1} \\ x_k \\ 0 \end{bmatrix} \in \mathbb{Z} \setminus \{0\}. \text{ So:}$$

$$\|v\|^2 = \left\| \sum_{i=1}^{k-1} b_i^* y_i + x_k b_k^* \right\|^2 \overset{\text{Pyth.}}{\geq} (x_k)^2 \|b_k^*\|^2 \geq \|b_k^*\|^2$$

[A shortest vector $\Lambda(B)$ is of the form $v = Bx$ $x \in \mathbb{Z}^n$ where $\|x\|_\infty \leq \gamma(B)$.

$\Rightarrow$ shortest vector can be found in time $\left(2 \cdot \gamma(B) + 1\right)^n$.

With LLL-Reduced basis: $2^{O(n^2)}$

→ Proof: 

→ So $\|b_k^*\| \leq \|b_k\|$ $\Rightarrow$ $\|b_i^*\| \cdot \gamma(B) = \frac{\prod_{k=1}^{n} \|b_k\|}{\prod_{\substack{k=1 \\ k \neq i}}^{n} \|b_k^*\|} \geq \|b_i\|$.

Also $\gamma(B) = \frac{\prod_{i=1}^{n} \|b_i\|_2}{|\det(B)|}$ so if I swap two columns, $\gamma(B)$ is invariant.

Therefore if $v = Bx$ $x \in \mathbb{Z}^n \setminus \{0\}$ s.t. $x_n \neq 0$, we have: (we can suppose is the n-th op to swap columns)

$$\|v\| \geq |x_n| \|b_n^*\| \geq |x_n| \frac{\|b_n\|}{\gamma(B)}$$

(↑ same trick as always)

So if $|x_n| > \gamma(B)$ (and so $\|x\|_\infty > \gamma(B)$)

then $\|v\| > \|b_n\|$ and so v is not the shortest vector. □

Definition (LLL-reduced): Let $B \in \mathbb{R}^{n \times n}$ non singular. Let $B = B^* \begin{bmatrix} 1 & & u_{ij} \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$ be the GSO of B.

B is LLL-reduced if:

(i) $|u_{ij}| \leq \frac{1}{2}$ $1 \leq i < j \leq n$ (ii) $\|b_i^*\|^2 \leq 2 \|b_{i+1}^*\|^2$ $i = 1, \dots, n-1$

Remember that $\Lambda(BM) = \Lambda(B)$ if $M \in \mathbb{Z}^{n \times n}$ unimodular.

LLL-algorithm finds, on input $B \in \mathbb{R}^{n \times n}$ non singular, a unimodular $M \in \mathbb{Z}^{n \times n}$ s.t. $B \cdot M$ is LLL-reduced.

Lemma: Let $B \in \mathbb{R}^{n\times n}$ non singular and LLL-reduced. Then $\|b_1\| \le 2^{\frac{n-1}{2}} \cdot sv(\Lambda(B))$ ← exponential approximation factor

Proof $\|b_1\|^2 = \|b_1^*\|^2 \le 2\cdot\|b_2^*\| \le 2^2\|b_3^*\|^2 \le 2^{n-1}\|b_n^*\|^2$

$\Rightarrow \|b_1\|^2 \le 2^{n-1} \min \|b_i^*\|^2$ $\Rightarrow$ $\|b_1\| \le 2^{\frac{n-1}{2}} sv(\Lambda(B))$.

$\min \|b_i^*\|^2 \le sv(\Lambda(B))^2$

□

Remarks: Up to today, there is no polynomial-time alg. that finds a vector $v \in \Lambda(B)\setminus\{0\}$ s.th. $\|v\| \le 2^{\sqrt{n}} \cdot sv(\Lambda(B))$. We will see: if it is hard to approximate sv in polynomial time, with an approximation factor of n^2, then NP = co-NP.

NP: Decision problems for which all-mighty can convince you of "yes". (P → Yes, No)

Example LLL:

$$B = \begin{bmatrix} 1 & 4 & 6 \\ 2 & 5 & 8 \\ 3 & 9 & 10 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & \frac{3}{2} & -\frac{4}{35} \\ 2 & 0 & \frac{4}{7} \\ 3 & -\frac{1}{2} & -\frac{12}{35} \end{bmatrix}}_{B^*} \cdot \begin{bmatrix} 1 & 5/2 & 26/7 \\ 0 & 1 & 8/5 \\ 0 & 0 & 1 \end{bmatrix}$$

$\cdot(-2)$

same operations

$$? = = // \cdot \begin{bmatrix} 1 & \frac{5}{2} & \frac{9}{7} \\ 0 & 1 & -\frac{2}{5} \\ 0 & 0 & 1 \end{bmatrix} \to |-\tfrac{2}{5}| \le \tfrac{1}{2}$$

$\cdot 2$ $\quad +$

$$B' = \begin{bmatrix} 1 & 2 & -1 \\ 2 & 1 & 0 \\ 3 & 1 & -1 \end{bmatrix} = // \cdot \begin{bmatrix} 1 & \frac{1}{2} & -\frac{2}{7} \\ 0 & 1 & -\frac{2}{5} \\ 0 & 0 & 1 \end{bmatrix}$$

(*) $B' = BU$ where

$$U = \begin{pmatrix} 1 & -2 & +1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

it is the same, U brings B in B'

Also, $U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -2 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ with $B' = BU$

This step is called normalization:

Input: $B \in \mathbb{R}^{n\times n}$ with GSO $B = B^* \begin{bmatrix} 1 & & \mu \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$

Output: $B' \in \mathbb{R}^{n\times n}$ " $B' = B^* \begin{bmatrix} 1 & & \mu' \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$ where $|\mu'_{ij}| \le \frac{1}{2}$ $\forall 1 \le i < j \le n$.

It takes $O(n^3)$ operations.

: to fix the K-th (from the bottom) row I have to do:

$K\ (n-K)\ o(1)$ (every time I change the coeff. ↑ multiplication ↑ subtraction)

$\Rightarrow$ for fixing all the matrix: $\sum_{K=1}^{n-1} K(n-K)\,o(1) = \sum_{K=1}^{n-1}(Kn-K^2) = o(n^3)$

LLL-Algorithm:

↳ **Input:** $B \in \mathbb{R}^{n\times n}$ non-singular.

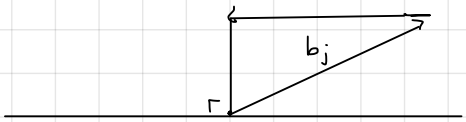
↳ Upon termination: B is LLL-reduced.

$B := \text{Normalize}(B)$. (it is true the first condition).

While (ii) not satisfied:

- Let $i \in \{1, \dots, n-1\}$ be index with $\|b_i^*\|^2 > 2\|b_{i+1}^*\|^2$ (the minimum)
- Swap columns i and $i+1$ in B
- $B := \text{Normalize}(B)$

Remember g.s.-orthogonalization:



$$\text{Span}\{b_1, \dots, b_{j-1}\} = \text{Span}\{b_1^*, \dots, b_{j-1}^*\}$$

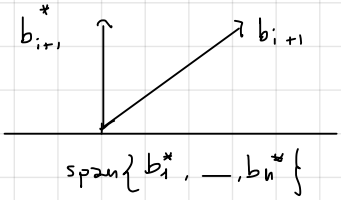
$$B = (b_1, \dots, b_{i-1}, b_i, b_{i+1}, b_{i+2}, \dots, b_n)$$

$$B' = (b_1, \dots, b_{i-1}, b_{i+1}, b_i, b_{i+2}, \dots, b_n)$$

GSO's:

$$B^* = (b_1^*, \dots, b_{i-1}^*, b_i^*, b_{i+1}^*, b_{i+2}^*, \dots, b_n^*)$$

$$(B')^* = (b_1^*, \dots, b_{i-1}^*, b_i'^*, b_{i+1}'^*, b_{i+2}^*, \dots, b_n^*)$$



$$b_{i+1}^* = b_{i+1} - \sum_{j=1}^{i} \mu_{i+1,j} b_j^*, \qquad \boxed{b_i'^* = b_{i+1}^* + \mu_{i+1,i} b_i^*}$$

Lemma: After the swap $\|b_i'^*\|^2 = \|b_{i+1}^* + \mu_{i+1,i} b_i^*\|^2 \leq \|b_{i+1}^*\|^2 + \frac{1}{4}\|b_i^*\|^2 \leq$ (not (ii) (we are in this hyp.))

$\leq \frac{1}{2}\|b_i^*\|^2 + \frac{1}{4}\|b_i^*\|^2 = \frac{3}{4}\|b_i^*\|^2$.

(Pythagoras + $|\mu_{i,j}| \leq \frac{1}{2}$)

Now: $\|b_i^*\| \cdot \|b_{i+1}^*\| = \|b_i'^*\| \|b_{i+1}'^*\|$ ($|\det(B)| = |\det(B')|$ lattice invariant; product of the terms; product of the terms; and the first $i-1$ and the last $n-i-1$ terms of B and B' are the same)

Effect: $\frac{\|b_i'^*\|}{\|b_i^*\|} \leq \sqrt{\frac{3}{4}}$ $\qquad \frac{\|b_{i+1}'^*\|}{\|b_{i+1}^*\|} \geq \sqrt{\frac{3}{4}}$ (they have to compensate each other since the product is the same).

Def.: Let $B \in \mathbb{R}^{n \times n}$ non singular and $B = B^* \cdot R$ of the GSO of B.

$$\Phi(B) = \|b_1^*\|^{2n} \cdot \|b_2^*\|^{2(n-1)} \cdot \dots \cdot \|b_n^*\|^2.$$

Definition: Let $B \in \mathbb{R}^{n \times n}$ non singular, the potential of B is

$$\Phi(B) := \prod_{i=1}^{n} \|b_i^*\|^{2(n-i+1)}$$

Exercise: $\Phi(B) = \prod_{i=1}^{n} \underbrace{\det(B_i^T B_i)}_{\prod_{j=1}^{i} \|b_j^*\|^2}$, where $B_i = (b_1, \dots, b_i) \in \mathbb{R}^{n \times i}$

$B_i = B^* \begin{bmatrix} 1 & \mu \\ & \ddots \\ 0 & & 1 \end{bmatrix} = B_i^* \begin{bmatrix} 1 & \mu \\ & \ddots \\ 0 & & 1 \end{bmatrix}$

Corollary: If $B \in \mathbb{Z}^{n \times n}$ then $\phi(B) \in \mathbb{N}^+$, in particular $\Phi(B) \geq 1$.

Lemma: Let B^j be the basis immediately after a swap operation on B of LLL-algorithm. Then:

$$\frac{\phi(B')}{\phi(B)} \leq \frac{3}{4}$$

Proof:

$$\frac{\phi(B')}{\phi(B)} = \frac{\|b_i'^*\|^{2(n-i+1)} \cdot \|b_{i+1}'^*\|^{2(n-i)}}{\|b_i^*\|^{2(n-i+1)} \cdot \|b_{i+1}^*\|^{2(n-i)}} = \frac{\|b_i'^*\|^2}{\|b_i^*\|^2} \leq \frac{3}{4}.$$

□

Corollary: Let $B \in \mathbb{Z}^{n \times n}$ be non singular and $M = \max_{i,j} |b_{i,j}|$. The number of iterations of LLL algorithm on input B is bounded by $O(n^2 \log_2(nM))$.

Remark: the binary incoding lenght of $B \in \mathbb{Z}^{n \times n}$ is $\Omega(n^2 + \log_2 M)$

Therefore number of iterations of LLL-algorithm is polynomial in input encoding. To show that LLL is in fact a polynomial-time alg., we need to show that encoding lenght of B in course of LLL-algorithm stays polynomial in the input as well. We do not do here.

Proof (Corollary): After i iterations: $\phi(B^{i,j}) \leq \left(\frac{3}{4}\right)^i \phi(B)$ *. Now $\|b_i\| \leq \sqrt{n} \cdot M \Rightarrow \|b_i^*\|^2 \leq nM^2$

and so $* \left(\frac{3}{4}\right)^i \phi(B) \leq \frac{3}{4} \prod_{i=1}^{n} (nM^2)^i = \frac{3}{4} (nM^2)^{\frac{n(n+1)}{2}} \Rightarrow \left(\frac{4}{3}\right)^i \leq (n \cdot M^2)^{n^2} \Rightarrow$

$\log_2\left(\frac{4}{3}\right) i \leq n^2 \log_2(nM^2) \Rightarrow i = O(n^2 + \log(n \cdot M))$.

□

Theorem: Let $B \in \mathbb{Z}^{n \times n}$ non singular, there exists a polynomial time algorithm (LLL alg.) that finds $v \in \Lambda(B) \setminus \{0\}$ s.th. $\|v\| \leq 2^{\frac{n-1}{2}} \cdot sv(\Lambda)$.

Proof: LLL: $\|b_1\|^2 \leq 2^{n-1} \cdot \min_i \|b_i^*\|^2 \leq 2^{n-1} \cdot sv(\Lambda)^2$.

□

Recall: $\gamma(B) = \frac{\prod \|b_i\|}{\underbrace{\prod \|b_i^*\|}_{= \det(\Lambda)}}$ orthogonal defect of B.

$v \in \Lambda(B)$ the shortest vector, then $v = Bx$, $x \in \mathbb{Z}^n$, $\|x\|_\infty \le \gamma(B)$.

Enumerate all: $(2\gamma(B)+1)^n$ vectors $\in \mathbb{Z}^n$, $\|x\|_\infty \le \gamma(B)$ gives candidates $v = B \cdot x$. In this set there is the shortest vector. SV can be computed in $(\gamma(B))^{O(n)}$ time.

Question: B LLL-reduced, $\gamma(B) \le ?$

$$\gamma(B)^2 = \frac{\prod \|b_i\|^2}{\prod \|b_i^*\|^2}, \quad b_i = b_i^* + \sum_{j=1}^{i-1} \underbrace{\mu_{ij}}_{|\cdot| \le \frac{1}{2}} b_j^* \overset{\text{Pythagoras}}{\Rightarrow} \|b_i\|^2 \le \|b_i^*\|^2 + \frac{1}{4}\sum_{j=1}^{i-1} \|b_j^*\|^2 \le$$

$$\le \|b_i^*\|^2 + \frac{1}{4}\sum_{j=1}^{i-1} 2^{i-j}\|b_i^*\|^2 \le \|b_i^*\|^2 + 2^{i-2}\|b_i^*\|^2 \le 2^i \|b_i^*\|^2$$

$\|b_i^*\|^2 2^{i-j} \ge \|b_j\|^2$

Therefore: $\gamma(B)^2 \le \prod_{i=1}^{n} 2^i = 2^{O(n^2)} \Rightarrow \gamma(B) \le 2^{n^2}$

Theorem: There exists an algorithm that, on input $B \in \mathbb{Z}^{n\times n}$ non-singular, computes a shortest non zero vector $v \in \Lambda(B)$ in time $2^{O(n^3)} + \text{poly}(\log \|B\|_\infty + n)$. The algorithm runs in polynomial space.

Theorem: If $B \in \mathbb{Z}^{n\times n}$ in LLL-reduced, then one can compute $v \in \Lambda(B) \setminus \{0\}$ of shortest vector of Λ in time $2^{O(n^2)}$

Exercise: Let $R = \begin{pmatrix} 1 & & \mu_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathbb{R}^{n\times n}$ and $M \in \mathbb{R}_{\ge 1}$. The number of vectors $v \in \Lambda(R) = \{Rx : x \in \mathbb{Z}^n\}$ with $\|v\|_\infty \le M$ is bounded by $(2M+1)^n$.

Proof (thm): $v \in \Lambda(B)$, $\exists x \in \mathbb{Z}^n$ with $v = Bx = B^* \overbrace{\begin{pmatrix} 1 & & \mu \\ & \ddots & \\ 0 & & 1 \end{pmatrix}}^{y} x$.

$$\|v\|^2 = \sum_{i=1}^{n} (y_i)^2 \|b_i^*\|^2 \ge \|y\|_\infty \min_i \|b_i^*\|^2 \overset{\|b_i^*\| \ge \frac{1}{2^i}\|v\| \ge \frac{1}{2^i} SV(\Lambda)}{\ge} \frac{\|y\|_\infty}{2^n} \cdot SV(\Lambda)^2$$

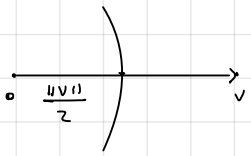
If v is a shortest vector then $\|y\|_\infty \le 2^n$

Exercise: The $x \in \mathbb{Z}^n$ s.th. $\|Rx\|_\infty \le 2^n$ can be enumerated in time $2^{O(n^2)}$ and polynomial space. □

Thm.: Let $B \in \mathbb{Z}^{n\times n}$ non singular. A shortest non zero vector $v \in \Lambda(B)$ can be computed in time $2^{O(n^2)} + \text{poly}(n, \log_2 |B|_\infty)$ and space polynomial in n and $\log_2 |B|_\infty$.

Def.: Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. The packing radius $\rho(\Lambda)$ is the largest radius $R > 0$ s.t. no two open balls of radius R, centered at two different lattice points intersect.

Remark: $v \in \Lambda \setminus \{0\}$ of shortest vector w.r.t. ℓ_2. Now:



Exercise: $\rho(\Lambda) = \frac{\lambda_1(\Lambda)}{2} = \frac{sv(\Lambda)}{2}$

Def.: Let $\Lambda \subseteq \mathbb{R}^n$ full-dimensional lattice. The packing density is.

$$\sigma(\Lambda) := \lim_{\tilde{r} \to +\infty} \frac{Vol\left(X \cap B(0,\tilde{r})\right)}{Vol\left(B(0,\tilde{r})\right)} \quad \text{where} \quad X = \bigcup_{v \in \Lambda \cap B(0,\tilde{r})} B\left(v, \rho(\Lambda)\right)$$

Remark: $\sigma(\Lambda) \leq 1 \quad \left(X \cap B(0,\tilde{r}) \subseteq B(0,\tilde{r})\right)$.

Remark: How many lattice points (roughly) are contained in $B(0,\tilde{r})$? $\approx \frac{\tilde{r}^n \cdot \sqrt{n}}{\det(\Lambda)}$

Theorem: (Viazowska): For $n = 8$, the density $\leq \frac{\pi^4}{384}$ and tight example E_8.

Def.: (Covering radius): Let $\Lambda \subseteq \mathbb{R}^n$ be full-dimensional lattice. Let $\mu(\Lambda) := \max_{x \in \mathbb{R}^n} dist(x, \Lambda)$ where $dist(x,\Lambda) = \min_{v \in \Lambda} \|x - v\|$ (this is a minimum because there are only many finite elements of Λ in a ball). This is the covering radius.

Remark: $\rho(\Lambda) \leq \mu(\Lambda)$: let v the shortest vector $\Rightarrow d\left(\frac{v}{2}, \Lambda\right) = \frac{\|v\|}{2} = \frac{\lambda_1(\Lambda)}{2} = \rho(\Lambda)$

Exercise: Let $B = (b_1, \dots, b_n) \in \mathbb{R}^{n \times n}$ be non-singular. Then, $\mu\left(\Lambda(B)\right) \leq \frac{1}{2}\sqrt{\sum_{i=1}^n \|b_i\|^2}$.

Proof: $x \in \mathbb{R}^n$ arbitrary. $x = B \cdot \lambda$, $\lambda \in \mathbb{R}^n$. Let $y \in \mathbb{Z}^n$ s.t. $\|y_i - \lambda_i\| \leq \frac{1}{2}\ \forall i$ (the nearest integer in every coordinate). Then $\|x - By\|^2 = \|B(\lambda - y)\|^2 \leq \frac{1}{4}\sum_{i=1}^n \|b_i\|^2$.

□

Example:
- $\mu(\mathbb{Z}^n) = \frac{1}{2}\sqrt{n}$ ← half of the diagonal of cubic n-cube
- $B = (b_1, \dots, b_n)$ $b_i^T \cdot b_j = 0$, B non singular $\Lambda(B) = \Lambda$. So, $\mu(\Lambda)^2 = \frac{1}{4}\sum_{i=1}^n \|b_i\|^2$. (it makes sense because given a basis $\{b_i\}$ if b_i are the s.v. in their span) ↘ ↙ look at Ex. 4 Sheet 6

Def.: Let $\Lambda \subseteq \mathbb{R}^n$ be a full dimensional lattice and $\Lambda^* = \{y \in \mathbb{R}^n : y^T \cdot v \in \mathbb{Z}\ \forall v \in \Lambda\}$ is the dual lattice.

Theorem: Suppose $B \in \mathbb{R}^{n \times n}$ is non singular and $\Lambda = \Lambda(B)$. We have that $\Lambda^* = \Lambda\left((B^{-1})^T\right)$.

Proof ⊇ Let $y = (B^{-1})^T \cdot x$, $x \in \mathbb{Z}^n$. Let $v = B \cdot z$, $z \in \mathbb{Z}^n$ be an arbitrary element of Λ.

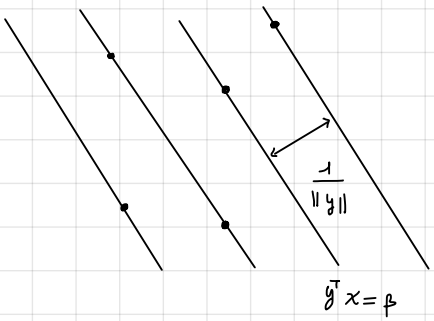
Then $y^T v = x^T B^{-1} B z = x^T z \in \mathbb{Z}$.

⊆ Suppose $y \notin \Lambda((B^{-1})^T)$. Then $y = (B^{-1})^T \cdot x$, where $x_i \notin \mathbb{Z}$ for some i. Let $v = B \cdot e_i$

$\Rightarrow y^T v \notin \mathbb{Z}$.

□

Observation: $\Lambda \subseteq \bigcup_{\beta \in \mathbb{Z}} (y^T x = \beta)$ $\quad (\Lambda^* = \{ y \in \mathbb{R}^n : y^T v \in \mathbb{Z} \ \forall v \in \Lambda \})$

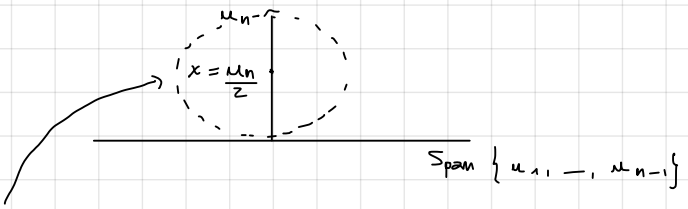


All lattice points lie in the union of translated hyperplanes $y^T x = \beta \in \mathbb{Z}$.

Theorem (Lagarias, Lenstra & Schnorr 1990): Let $\Lambda \subseteq \mathbb{R}^n$ be a full dimensional lattice. Then:

$$\frac{1}{4} \le \mu(\Lambda)\, \rho(\Lambda^*) \le c(n) \quad \text{where} \quad c(n) = \frac{\sqrt{\sum_{i=1}^{n} i^2}}{4} = \Theta(n^{\frac{3}{2}})$$

Proof Let $u_1, \dots, u_n \in \Lambda$ be the vectors where the successive minima are attained, i.e. $\|u_i\| = \lambda_i(\Lambda)$ where $\lambda_i(\Lambda)$ is the smallest radius of a ball around 0 containing i linearly independent lattice points. Obviously $\|u_1\| \le \dots \le \|u_n\|$. Now:



$\text{dist}(x, \Lambda) = \frac{\|u_n\|}{2}$ $\quad$ (use $\|u_n\| = \lambda_n$).

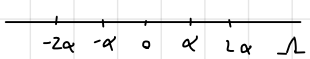
[**Exercise**: $v \in \Lambda$, $u_1, \dots, u_n \in \Lambda^*$ linearly independent. $\max_{i=1,\dots,n} \|v\| \cdot \|u_i\| \ge 1$ (Cauchy-Schwarz).

Let $v \in \Lambda^* \setminus \{0\}$ s.t. $\|v\| = \rho(\Lambda^*) \cdot 2$. Then $\max_i \|v\| \|u_i\| = \underbrace{\|v\|}_{= \rho(\Lambda^*) \cdot 2} \underbrace{\|u_n\|}_{\le 2\mu(\Lambda)} \ge 1 \quad \Rightarrow 2\rho(\Lambda^*)\, 2\rho(\Lambda) \ge 1$

$\Leftrightarrow \rho(\Lambda^*)\, \mu(\Lambda) \ge \frac{1}{4}$.

Now, the upper bound. We prove by induction on n:

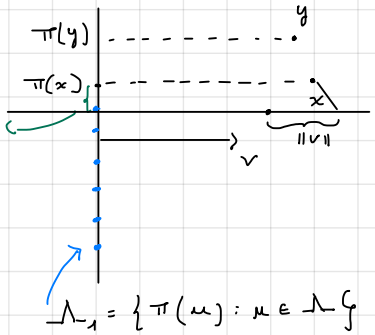
- $n = 1$: $\Lambda = \{ \alpha x : x \in \mathbb{Z} \}$



$\Lambda^* = \{ \frac{1}{\alpha} \cdot x : x \in \mathbb{Z} \}$

$\mu(\Lambda) = \frac{\alpha}{2}$ $\quad \rho(\Lambda^*) = \frac{1}{L}\frac{1}{\alpha}$ $\quad \rho(\Lambda^*)\mu(\Lambda) = \frac{1}{4} = C(1)$.

· $n-1 \to n$:



$I \le \mu(\Lambda_1)$

$\Lambda_1 = \{\pi(u) : u \in \Lambda\}$

Let $v \in \Lambda \setminus \{0\}$ be shortest vector.

$\operatorname{dist}(x, \Lambda)^2 \overset{\text{Pyt.}}{\le} \left(\frac{\|v\|}{2}\right)^2 + \mu(\Lambda_1)^2$ (*)

Now $\Lambda_1^* \subseteq \Lambda^*$ ($d \in \Lambda_1^*$ $d \perp v$, $d^T(\underbrace{\pi(u)}_{\in \Lambda_1}) \in \mathbb{Z}$

$\forall u \in \Lambda$. $\Rightarrow d^T u \in \mathbb{Z}$ $d^T(\pi(u) + dv) \in \mathbb{Z}$).

So, $\rho(\Lambda^*) \le \rho(\Lambda_1^*)$. Now (*) $\Rightarrow \mu(\Lambda)^2 \le \rho(\Lambda)^2 + \mu_1(\Lambda_1)^2 \Rightarrow$

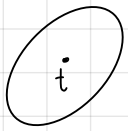
$$\rho(\Lambda^*)^2 \mu(\Lambda)^2 \le \underbrace{\rho(\Lambda^*)^2}_{\le \frac{1}{2}\sqrt{n}\sqrt[n]{\det(\Lambda)}} \underbrace{\rho(\Lambda)^2}_{\le \frac{1}{2}\sqrt{n}\sqrt[n]{\frac{1}{\det(\Lambda)}}} + \rho(\Lambda^*)^2 \mu_1(\Lambda_1)^2 \le \frac{1}{16}n^2 + \frac{1}{16}\sum_{i=1}^{n-1} i^2 =: c(n)^2.$$

$$= \frac{1}{16}\sum_{i=1}^{n} i^2 \left(= \frac{1}{16}\frac{n(n+1)(2n+1)}{6}\right)$$

□

Lecture 8 April (4)

Def.: Ellipsoid is a set $\mathcal{E} = \{x \in \mathbb{R}^n : \|A^{-1}(x-t)\|_2 \leq 1\}$. ($A$: invertible matrix)



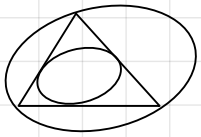
Exercise: $\mathcal{E}$ is image of $B(0,1) = \{x \in \mathbb{R}^n : \|x\| \leq 1\}$ under $T: \mathbb{R}^n \to \mathbb{R}^n$

$x \mapsto Ax + t$.

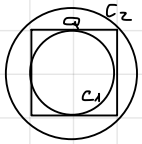
Remark: $\text{vol}(\mathcal{E}) = |\det(A)|$, $\text{vol}(B(0,1)) =: V_n$

Theorem (John ellipsoids): Let $K \subseteq \mathbb{R}^n$ a convex body (convex, compact and full-dimensional), there exists an ellipsoid $\mathcal{E}$ centered at 0 and $t \in \mathbb{R}^n$ s.t.:

$$t + \mathcal{E} \subseteq K \subseteq \underbrace{C_n}_{\text{scaling factor}} \mathcal{E} + t.$$ (n: the dimension)



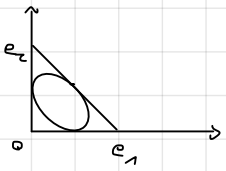
Exercise:



$Q = \{x \in \mathbb{R} : \|x\|_\infty \leq 1\}$ $C_1 = B(0,1)$ $C_2 = B(0,\sqrt{n})$

If K is centrally symmetric, then the scaling factor can be improved to $\sqrt{n}$.

Example: $\Sigma = \text{convex\_hull}\{0, e_1, \dots, e_n\}$.



Exercise: Show that scaling factor n is needed here

Heart of proof

There exist a universal constant C such that convex hull of $B(0,1)$ and $\{C_n e_1\}$ contains an ellipsoid $\mathcal{E}'$ with $\text{vol}(\mathcal{E}') > \text{vol}(B(0,1))$. Let's do the construction of $\mathcal{E}'$:

$$\mathcal{E}' = \{x \in \mathbb{R}^n : \sum_{i=1}^{n} \frac{1}{\alpha_i^2}(x_i - t_i)^2 \leq 1\} \quad \text{where} \quad t = e_1, \ \alpha_1 = 2, \ \alpha_2 = \dots = \alpha_n = \sqrt{\frac{n}{n+\frac{1}{10}}}.$$

$\mathcal{E}'$ is in fact an ellipsoid because $A^{-1} = \begin{pmatrix} \alpha_1^{-1} & & 0 \\ & \ddots & \\ 0 & & \alpha_n^{-1} \end{pmatrix}$, $\left(A = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}\right)$. And:

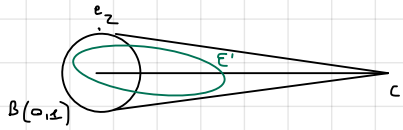
$$\text{Vol}(\mathcal{E}') = 2\left(\frac{n}{n+\frac{1}{10}}\right)^{\frac{n-1}{2}} \cdot V_n. \quad \text{But:} \quad 2\left(\frac{n}{n+\frac{1}{10}}\right)^{\frac{n-1}{2}} = 2\left(\frac{1}{1+\frac{1}{10n}}\right)^{\frac{n-1}{2}} \geq$$

($\geq$: $1+x \leq e^x$)

$$= 2\left(\frac{1}{e^{\frac{1}{10n}}}\right)^{\frac{n-1}{2}} \geq \frac{1}{e^{\frac{1}{20}}} \cdot 2 > 1. \quad \text{So} \quad \text{Vol}(\mathcal{E}') > \text{Vol}(B(0,1)).$$

($\geq$: drop the "−1" at the exponent)

It reminds to show that $\mathcal{E}' \subseteq \text{convex\_hull}\{B(0,1) \cup \{C_n e_1\}\}$.



Idea: show that line-segment spanned by $c \cdot n e_1$ and $y \in \mathbb{R}^n$ s.t. $y_1 = 0$, $\|y\|_2 = 1$ does not intersect the boundary of $\mathcal{E}'$. For simmetry reason we assume that $y = e_2$.

A point on line-segment is $x_\lambda = \lambda e_2 + (1-\lambda)(cne_1)$ $\lambda \in [0,1]$. We have to show:

$$f(\lambda) := \sum_{i=1}^{n} \frac{1}{a_i^2} (x_\lambda - t)_i^2 > 1$$

$$f(\lambda) = \frac{1}{4}\left((1-\lambda) cn - 1 \right)^2 + \left(1 + \frac{1}{10n} \right) \lambda^2 \quad (*)$$

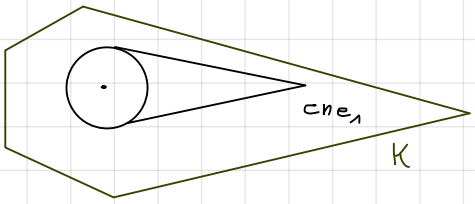
Observation: if $\lambda \geq 1 - \frac{1}{30n}$ then $\left(1 + \frac{1}{10n}\right)\left(1 - \frac{1}{30n}\right)^2 > 1$, if $0 \leq \lambda \leq 1 - \frac{1}{30n}$ first term in $(*)$ $\geq \frac{1}{4}\left(\frac{1}{30n} cn - 1 \right)^2 > 1$ for c large enough.

It remains to show that if $x_1 \leq 0$ and $x \in \mathcal{E}'$, then $\|x\| < 1$ (exercise). □

Proof (John's theorem):

Let $\mathcal{E} + t \subseteq K$ such that $\mathrm{vol}(\mathcal{E})$ is maximal. We argue that $K \subseteq c \cdot n\, \mathcal{E} + t$. By linear trasformation $\tau : x \longmapsto A^{-1}x - t$ where $\mathcal{E}$ is image of $B(0,1)$ under A x, we can assume that $t = 0$, $\mathcal{E} = B(0,1)$.

If $cn\mathcal{E} \not\subseteq K$, then $\exists x \in K$ s.th. $\|x\| = cn\mathcal{E}$. By notation: this point is cne_1:

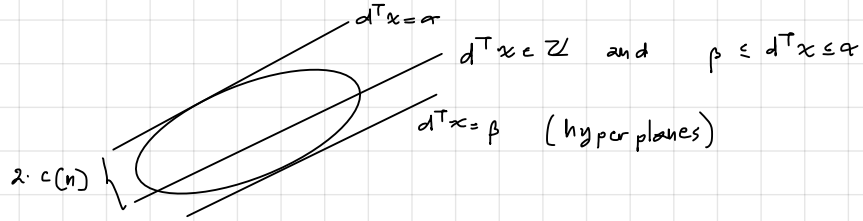


"Heart of proof" tells us that $\exists \mathcal{E}'$ of larger volume than $B(0,1)$ with $\mathcal{E}' \subseteq K$, $\lightning$. □

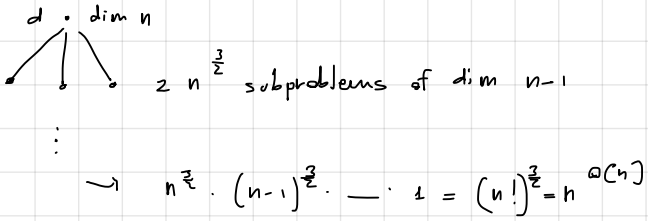
Flatness theorem for ellipsoids: Let $\mathcal{E} \subseteq \mathbb{R}^n$ an ellipsoid. If $\mathcal{E} \cap \mathbb{Z}^n = \emptyset$ then there exists $d \in \mathbb{Z}^n \setminus \{0\}$ s.t. $\max_{x \in \mathcal{E}} d^T x - \min_{x \in \mathcal{E}} d^T x \left(= \max_{x,y \in \mathcal{E}} d^T(x-y) \right) \leq \frac{c(n)}{2}$ with $c(n) = \frac{1}{4}\sqrt{\sum_{k=1}^{n^2} k^2} \leq \frac{1}{4} n^{\frac{3}{2}}$

Furthermore, if $v = A^T x$, $x \in \mathbb{Z}^n \setminus \{0\}$ is shortest vector of $\Lambda(A^T)$, then $d := x$ satifies the previous inequality.

Relevance of the flatness theorem: given $\mathcal{E} \subseteq \mathbb{R}^n$. Decide $\mathcal{E} \cap \mathbb{Z}^n = \emptyset$. Certificate for no: find $\overline{x} \in \mathcal{E} \cap \mathbb{Z}^n$. Certificate for yes: $d \in \mathbb{Z}^n \setminus \{0\}$ given by flatness theorem



Continue our search in $2 \cdot c(n)$ lower-dimensional ellipsoids:

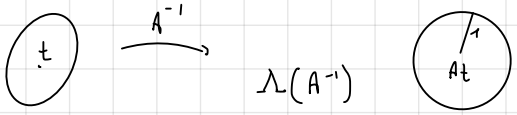


Proof Exercise: if $\mathcal{E}$ image of $Ax+t$ of $B(0,1)$ and $d \in \mathbb{R}^n$.

$$\max_{x \in \mathcal{E}} d^T x = \max_{x \in B(0,1)} d^T (Ax+t) = \max_{x \in B(0,1)} (d^T \cdot A)\, x + d^T t = \| A^T d \|_2 + d^T t$$

$\max_{x \in B(0,1)} d^T x$ is obtained at $\frac{d}{\|d\|}$

Now $\mu(\Lambda)\, \rho(\Lambda^*) \le \frac{c(n)}{4}$

↳ 

. So $\mathcal{E} \cap \mathbb{Z}^n = \emptyset \iff \Lambda(A^{-1}) \cap B(At, 1) = \emptyset \Rightarrow$

$\mu(\Lambda(A^{-1})) \ge 1$. for transference $\rho(\Lambda(A^T)) \le \frac{c(n)}{4}$.

↙ d is the d s.t. $A^T d$ is SV of $\Lambda(A^T)$

Exercise: $\max_{x,y \in \mathcal{E}} d^T(x-y) = 2 \cdot \| A^T d \|_2$. But since $\rho(\Lambda(A^T)) \le \frac{c(n)}{4} \Rightarrow \exists\, d \in \mathbb{Z}^n$:

$\max_{x,y \in \mathcal{E}} d^T(x-y) \le \frac{1}{2}\, c(n)$.

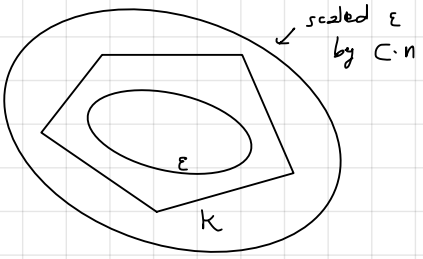
□

Theorem (Flatness theorem): Let $K \subseteq \mathbb{R}^n$ be a convex body. if $K \cap \mathbb{Z}^n = \emptyset$ 15 April (8)

then $\exists d \in \mathbb{Z}^n \setminus \{0\}$ s.t. $\max_{x,y \in K} d^T(x-y) \leq C \cdot n \cdot c(n) \leq C \cdot n^{\frac{5}{2}}$

Proof.

Let $\mathcal{E} \subseteq \mathbb{R}^n$ be the max volume ellipsoid in K. Since $K \cap \mathbb{Z}^n = \emptyset \Rightarrow \mathcal{E} \cap \mathbb{Z}^n = \emptyset$.



But this means that with $d \in \mathbb{Z}^n$ s.t. $A^T d$ shortest vector in $\Lambda(A^T)$, $\left[\mathcal{E} = \{Ax + t : x \in B(0,1)\} \subseteq \mathbb{R}^n\right]$ then

$\max_{x,y \in \mathcal{E}} d^T(x-y) \leq c(n)$. But $\max_{x,y \in K} d^T(x-y) \leq C \cdot n \cdot \max_{x,y \in \mathcal{E}} d^T(x,y) \leq$

$\leq C \cdot n \cdot c(n) \leq C \cdot n^{\frac{5}{2}}$.

□

An algorithm for integer programming

Input: $K \subseteq \mathbb{R}^n$ convex body **Task**: describe $K \cap \mathbb{Z}^n = \emptyset$

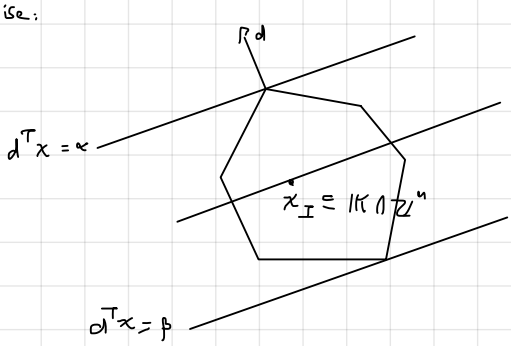
1: compute max volume ellipsoid $\mathcal{E} = \{Ax + t, x \in B \subseteq \mathbb{R}^n\}$ (not in this course)

2: compute shortest vector $v = A^T d$, $d \in \mathbb{Z}^n \setminus \{0\}$ of $\Lambda(A^T)$ ($2^{O(n)}$ with LLL)

3: if $\|v\| > \frac{C(n)}{2}$. Answer "No" because K contains an integer point.

↕

4: Otherwise:



$\alpha^T x = \alpha^T x_I$ ← convex optimization

$\beta = \min_{x \in K} \alpha^T x$

$\alpha \geq \alpha^T \cdot x_I \geq \beta$

For each $\gamma \in [\beta, \alpha] \cap \mathbb{Z}$ decide $[K \cap (\alpha^T x = \gamma)] \cap \mathbb{Z}^n$. So we have $C \cdot n^{\frac{5}{2}}$ lower-dimensional integer problems.

Lemma: wLOG $d = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $K' = \left\{ \begin{pmatrix} x_2 \\ \vdots \\ x_n \end{pmatrix} : \begin{pmatrix} \gamma \\ x_2 \\ \vdots \\ x_K \end{pmatrix} \in K \right\} \subseteq \mathbb{R}^{n-1}$ convex.

The hermite normal form (HNF)

Goal: Translate the problem $K \subseteq \mathbb{R}^n$, convex body $[K \cap (a^T x = \gamma)] \cap \mathbb{Z}^n = \emptyset$ into

$$[K' \cap (a'^T x = \gamma')] \cap \mathbb{Z}^{n-1} = \emptyset \quad K' \subseteq \mathbb{R}^{n-1}.$$

Then: Number of recursive calls $T(n)$ to decide $(K \cap \mathbb{Z}^n) = \emptyset$ can be bounded as

$$T(n) < C \cdot n^{\frac{5}{3}} \cdot T(n-1) \leq C^n \cdot (n!)^{\frac{5}{3}} = n^{O(n)}.$$

Unimodular matrices: $U \in \mathbb{Z}^{n \times n}$ with $\det(U) = \pm 1$ is called unimodular.

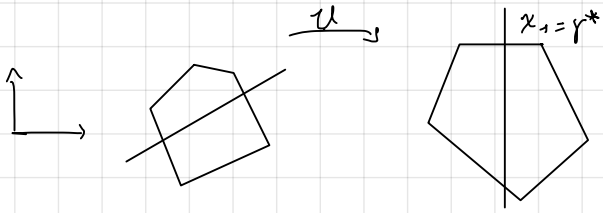
Remember that $\phi: \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$, $x \longmapsto Ux$ is bijection $\Leftrightarrow U \in \mathbb{Z}^{n \times n}$ is unimodular.

Consequence: $K \cap \mathbb{Z}^n = \phi \iff \underbrace{U \cdot K}_{= \{Ux : x \in K\}} \cap \mathbb{Z}^n = \emptyset$

Goal: Find $U \in \mathbb{Z}^{n \times n}$ unimodular s.t. $U \cdot \{x \in \mathbb{R}^n : a^T x = \gamma\} = \{x \in \mathbb{R}^n : x_1 = \gamma^*\}$

Then: $[K \cap (a^T x = \gamma)] \cap \mathbb{Z}^n = \emptyset \iff \underbrace{U \cdot K}_{\text{convex}} \cap (x_1 = \gamma^*) \cap \mathbb{Z}^n = \emptyset \iff K' \cap \mathbb{Z}^{n-1} = \emptyset$ where

$$K' = \left\{ \begin{pmatrix} x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^{n-1} : \begin{pmatrix} \gamma^* \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in U K \right\}$$



Warm up: $U \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} * \\ 0 \end{pmatrix}$ $U \in \mathbb{Z}^{2 \times 2}$ unimod. $a, b \in \mathbb{Z}$ not both 0 and $\gcd(a, b) = 1$.

Theorem. $\exists x, y \in \mathbb{Z}$ s.th. $xa + yb = \gcd(a, b) = 1$.

$$U = \begin{pmatrix} x & y \\ -b & a \end{pmatrix} \in \mathbb{Z}^{2 \times 2}$$ unimodular. In the following, we generalize this procedure.

Def. Let $A \in \mathbb{Z}^{m \times n}$ with $\operatorname{rank}(A) = m$ is in "Hermite normal form", if $A = [H \mid 0]$ where $H \in \mathbb{Z}^{m \times m}$ is lower triangular, $H \geq 0$ and for each row, unique max entry is on the diagonal.

Example: $A = \left[\begin{array}{cc|cc} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \end{array}\right]$ is in HNF. $[1 \ 0 \ \cdots \ 0]$ is in HNF.

$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 2 & 0 & 0 \end{bmatrix}$ not in HNF for "-1" $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 3 & 2 & 0 & 0 \end{bmatrix}$ not in HNF for "3"

Theorem: Let $A \in \mathbb{Z}^{m \times n}$, $\operatorname{rank}(A) = m$. Then, exists a unimodular matrix $U \in \mathbb{Z}^{n \times n}$ s.t. $A \cdot U = [H \mid 0]$ is in HNF.

Proof Step 1: find $U \in \mathbb{Z}^{n \times n}$ unimodular s.t. $AU = [L \mid 0]$, $L \in \mathbb{Z}^{m \times m}$ is lower triangular.

By induction: find $U \in \mathbb{Z}^{n \times n}$ unimod. s.th.

$$A\,U = \left(\begin{array}{c|ccc} d_1 & 0 & \cdots & 0 \\ \hline d_2 & & & \\ \vdots & & B \in \mathbb{Z}^{(m-1)\times(n-1)} & \\ d_m & & & \end{array}\right) \quad (2)$$

By induction $\exists\, U' \in \mathbb{Z}^{(m-1)\times(n-1)}$ unimodular s.t. $B \cdot U' = \left(\begin{array}{c|c} \triangle & 0 \end{array}\right) \Rightarrow \underbrace{A \cdot U \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & U' & \\ 0 & & & \end{pmatrix}}_{*}$

with $U \cdot \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & U' & \\ 0 & & & \end{pmatrix}$ unimodular and:

$$* = \left(\begin{array}{c|ccc} d_1 & 0 & \cdots & 0 \\ \hline d_2 & & & \\ \vdots & & \triangle & \\ d_m & & & \end{array}\right)$$

The shape (2) can be obtained using inductive argument: by multiplying columns with -1 (if necessary) we arrive at the stage where all components of the first row of A are elements in $\mathbb{N}_0$

If there are two non zero elements: $0 < a \le b$

$$\begin{array}{cc} a & b \\ \hline a & b-a \end{array}$$

and so step by step I get only "0" except at most one element.

$$A \underbrace{\begin{pmatrix} 1 & & \\ & -1 & \\ & & 1 \end{pmatrix}}_{\text{unimod}} \leftarrow i \quad \sim 0$$

Example:

$$\begin{pmatrix} 2 & -3 & 5 \\ 6 & 7 & 1 \end{pmatrix} \to \begin{pmatrix} 2 & 3 & 5 \\ 6 & -7 & 1 \end{pmatrix} \to \begin{pmatrix} 2 & 1 & 1 \\ 6 & -13 & -11 \end{pmatrix}$$

$A \cdot U$ with $U = \begin{pmatrix} 1 & -1 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (shortcut with -2)

$$\to \begin{pmatrix} 1 & 1 & 2 \\ -11 & -13 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ -11 & -2 & 28 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ -11 & 2 & 0 \end{pmatrix} \sim 0 \quad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \end{pmatrix}$$

I put the remainder of the division by the diagonal element "$-11 + 6 \cdot 2 = 1$"

So:

$$\begin{pmatrix} h_{11} > 0 & & 0 & 0 \\ & \ddots & & \\ 0 & & h_{m-1\,m-1} & 0 \\ 0 & \cdots\ 0 & h_{m\,m-1} & h_{m\,m} > 0 \end{pmatrix}$$

$h_{m\,m-1}$: remainder of div by

Theorem: Let $A \in \mathbb{Z}^{m \times n}$ be of rank n. The HNF $[H \mid 0]$ of A is unique.

Proof: $\Lambda(A) = \{ A \cdot x : x \in \mathbb{Z}^n \}$ full dimensional lattice $\subseteq \mathbb{Z}^n$. But, $\Lambda(A) = \Lambda(H)$ since $\{ A \cdot x : x \in \mathbb{Z}^n \} = \{ A U U^{-1} x : x \in \mathbb{Z}^n \} = \{ [H \mid 0] x : x \in \mathbb{Z}^n \} = \Lambda(H)$. If $\exists$ possesses diff. HNF $H_1 \neq H_2$, then $\Lambda(H_1) = \Lambda(H_2)$. We show that $\Lambda(H_1) \neq \Lambda(H_2)$.

$$H_1 = \begin{bmatrix} h_{11} & & 0 \\ \vdots & \ddots & \\ h_{m1} & \cdots & h_{nn} \end{bmatrix} \qquad H_2 = \begin{bmatrix} h'_{11} & & 0 \\ \vdots & \ddots & \\ h'_{m1} & \cdots & h'_{nn} \end{bmatrix}$$

h_{ii} is a generator of the sub-group of $\mathbb{Z}$ defined by the i-th components of vectors $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ * \\ \vdots \end{pmatrix} \leftarrow i$ of $\Lambda(H_1) = \Lambda(A) \Rightarrow h_{ii} = h'_{ii} \quad \forall i \in \{1, \dots, n\}$.

Let i be the minimal, such that $\text{row}_i(H_1) \neq \text{row}_i(H_2)$ ($i \geq 2$ for the previous obs.).

$$H_1 = \begin{bmatrix} h_{11} & & 0 \\ \vdots & \ddots & \\ h_{i1} & h_{ii} & \\ \vdots & & h_{nn} \end{bmatrix} \quad \neq \quad H_2 = \begin{bmatrix} h_{11} & & 0 \\ \vdots & \ddots & \\ h'_{i1} & h_{ii} & \\ \vdots & & h_{nn} \end{bmatrix}$$

Assume WLOG $h_{ij} > h'_{ij}$. Then $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ h_{ij} - h'_{ij} \\ \vdots \end{pmatrix} \in \Lambda(A)$. But $h_{ii} > h_{ij} \geq h_{ij} - h'_{ij} \geq 0$ & since $h_{ij} - h'_{ij} \in h_{ii}\mathbb{Z}$.

□

Exercises: Given $A \in \mathbb{Z}^{m \times n}$ of full row-rank. Then:

(i) $v \in \Lambda(A)$, $\text{HNF}(A) = (H \mid 0) \Rightarrow \text{HNF}(A \mid v) = (H \mid 0)$

→ for $\mathbb{Z}_{\geq 4}$ $\Lambda(A \mid v) = \Lambda(A)$ ⇒ the Hermite Normal forms are the same

(ii) Let $A_B \in \mathbb{Z}^{m \times m}$ be a full rank submatrix of A and $D = |\det(A_B)|$. Then $\text{HNF}(A) = \text{HNF}[A \mid DI]$. If $\Delta = \|A\|_\infty$, then Hadamard $\Rightarrow D \leq (\sqrt{m} \cdot \Delta)^m \Rightarrow$

$|\det(A)| \leq \prod_{i=1}^{m} \|a_i\|_2 \leq \sqrt{m}^m \prod_{i=1}^{m} \|a_i\|_\infty \leq \sqrt{m}^m \|A\|_\infty^m$

$\log(D) = O(m \cdot \log(m + \Delta))$. $[A \mid DI] \rightsquigarrow [H \mid 0]$ (intermediate results are reduced mod 100).

↑ # bits encoding D ↑ polynomial in encoding lenght of A

I can do it in polynomial time using a specific algorithm but not if I do randomly

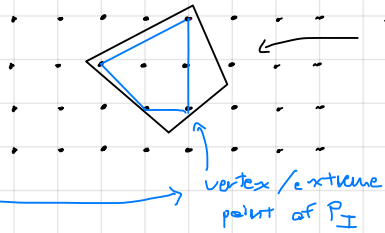
$$\left[A \;\middle|\; {}^{100}\diagdown_{100} \right] \rightsquigarrow \left[H \mid 0 \;\middle|\; {}^{100}\diagdown_{100} \right]$$

↑ reduced mod 100

$$\left[\begin{matrix} \cancel{8} & & \\ 8 & 10 & \\ 9 & 5 & 11 \end{matrix} \;\middle|\; {}^{100}\diagdown_{100} \right] \rightarrow$$

Integer hulls of polyhedra

Polytope: convex body described by a finite set of affine inequalities:



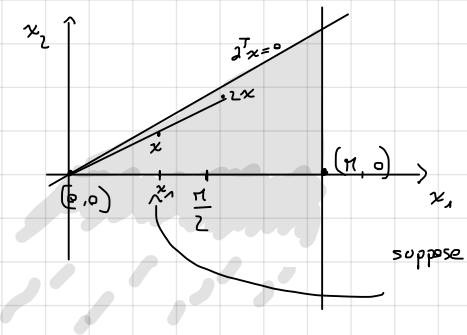
$P = \{x \in \mathbb{R}^n : Ax \le b\}$ $A \in \mathbb{R}^{m \times n}$ $b \in \mathbb{R}^n$

polyhedron / polytope (the difference is only that polyhedron are bounded)

P_I = conv_hull $\{x \in \mathbb{Z}^n : x \in P\}$

↑ the integer hull of $P = \{x \in \mathbb{R}^n \mid Ax \le b\}$

Example: $P \subseteq \mathbb{R}^n$ given by two inequalities $\begin{cases} a^T x \le 0 \\ x_1 \le M \end{cases}$ in $\mathbb{R}^2$



# of extreme points $\le \log_2(M)$

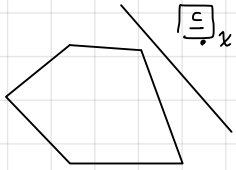
suppose $x \in P_I$ with $x_1 \le \frac{M}{2}$ $\Rightarrow 2x \in P$ because $a^T(2x) \le 0$ and $2x_1 \le M$, and $2x \in \mathbb{Z}^2$ $(x \in \mathbb{Z}^2)$ $\Rightarrow 2x \in P_I \Rightarrow x = (0,0)\frac{1}{2} + 2x \cdot \frac{1}{2} \Rightarrow$ x not a vertex

Def.: $P \subseteq \mathbb{R}^n$ is polyhedron, if $P = \{x \in \mathbb{R}^n : Ax \le b\}$ for some $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$ (right hand side vector). If P is bounded, then P is a polytope. An inequality $c^T \cdot x \le \delta$, $c \in \mathbb{R}^n$, $\delta \in \mathbb{R}$ is valid for P, if $\forall x \in P$, $c^T x \le \delta$. Let $c^T x \le \delta$ be valid, then $\mathcal{F} = P \cap (c^T x = \delta)$ is a face of P. The dimension of $P(F)$ is its affine dimension. So $\dim(P)$ = dim of subspace generated by $P - x$ for some $x \in P$. Face of P is a face of dimension $\dim(P) - 1$.

An extreme point / vertex of P is a face of dimension 0.

Obs: A polytope is the convex hull of its vertices: $P = \{Ax \le b\} \overset{?}{=} \text{Conv}(v_1, \dots, v_{n+1})$

$\subseteq$: obvious



x not in the convex hull of vertices, but the maximum of a linear function is obtained at the boundary...

Obs.: Let P be a polytope. $x \in P$ is an extreme point of $P \iff \nexists\, u, v \in P$ s.t. $\frac{1}{2}(u + v) = x$

(Exercise).

Theorem: Let $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$ s.t. $\|A\|_\infty \leq \Delta$ (a number), $\|b\|_\infty \leq \Delta$. Further, $P = \{x \in \mathbb{R}^n : Ax \leq b\} \subseteq [-\Delta, \Delta]^n$. then P_I has at most $O(\log(n\Delta)^m)$ extreme points.

Proof Idea: Partition space into cells such that:

(i) each integer points in P contained in a cell

(ii) each cell has at most one extreme point of P_I.

(iii) The number of cells is $O(\log(n\Delta)^m)$

For $\alpha \in \mathbb{N}_0$: $L(\alpha) = \begin{cases} 2^{\alpha-1}, & \text{if } \alpha \geq 1 \\ 0, & \text{if } \alpha = 0 \end{cases}$ $\quad u(\alpha) = \begin{cases} 2^\alpha & \text{if } \alpha \geq 1 \\ 0 & \text{if } \alpha = 0 \end{cases}$

For $\alpha \in \mathbb{N}_0^m$ $C(\alpha) = \{x \in \mathbb{R}^n : L(\alpha_i) \leq b_i - a_i^T x \leq u(\alpha_i)\}$ where $A = \begin{pmatrix} a_1^T \\ | \\ a_m^T \end{pmatrix}$

The conditions hold, in fact:

(i) Let $x_I \in \mathbb{Z}^n \cap P : (b_i - a_i^T x_I) \in \mathbb{N}_0$, $\alpha_i = \max\{K \in \mathbb{N}_0 : 2^{K-1} \leq b_i - a_i^T x_I\} \Rightarrow x_I \in C(\alpha)$ by def.

(ii) Let $x \neq y$ (vertex of P_I) be two points in $C(\alpha) \cap \mathbb{Z}^n$. We argue that $2y - x \in P \cap \mathbb{Z}^n$. Then, y is not a vertex. ($y = \frac{1}{2}x + \frac{1}{2}(2y - x)$ that is a contradiction by the previous obs.)

If $\alpha_i = 0$ $\quad b_i - a_i^T(2y - x) = 0$.

If $\alpha_i \neq 0$ $\quad b_i - a_i^T(2y - x) = (b_i - a_i^T y) - a_i^T y + a_i^T x = (b_i - a_i^T y) + (b_i - a_i^T y) - (b_i - a_i^T x) \geq$

$$\geq 2^{\alpha_i - 1} + (b_i - a_i^T y) - (b_i - a_i^T x) \geq 2^{\alpha_i - 1} + (2^{\alpha_i - 1} - 2^{\alpha_i}) \geq 0$$

(iii) How many cells: for $i \in \{1, \ldots, m\}$:

$$|b_i - a_i^T x| \leq \|b\|_\infty + n\|A\|_\infty \|x\|_\infty \leq \Delta + n\Delta^2 \Rightarrow \max_{x \in P \subseteq [-\Delta, \Delta]^n} (b_i - a_i^T x) \leq$$

$$\|\alpha\|_\infty \leq O(\log(n\Delta)) \Rightarrow \#\alpha \leq O(\log(n\Delta))^m.$$

(a cell is defined by an α and every entrance α_i of α can be chosen at most between $O(\log(n\Delta))$)

□

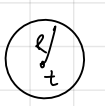
$2^{O(n)}$-time algorithm for Closest Vector Problem (CVP)

Lecture 29/04 (10)

Closest vector problem: given $t \in \mathbb{R}^n$ (target), $B \in \mathbb{Q}^{n\times n}$ (for reason complexity in $\mathbb{Q}^{n\times n}$) non singular. The $CVP(t, \Lambda(B)) := \underset{v\in\Lambda(B)}{\arg\min} \|v-t\|_2$.

$\updownarrow$

Decision version: The $CVP(t, \Lambda(B))$ is equivalent to decide if as $R>0$ varies:



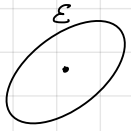
$B_R(t) \cap \Lambda(B) = \emptyset$ or not.

But $\Lambda(B) = \{Bx : x \in \mathbb{Z}^n\}$ and $B_R(t) = \{x \in \mathbb{R}^n : \|x-t\| < R\}$. So under the transformation B^{-1}, $B^{-1}(\Lambda(B)) = \mathbb{Z}^n$ and $B^{-1}(B_R(t)) = \{B^{-1}x : \|x-t\|^2 < R^2\} =$

$= \{y : \|\frac{B}{R^2}(y - B^{-1}t)\| < 1\} =: \mathcal{E}$ ellipsoid

$$\left[\begin{array}{l} y := B^{-1}x \\ \\ \\ \\ \end{array}\right. \begin{array}{l} \|x-t\|^2 < R^2 \iff \|BB^{-1}x - t\|^2 < R^2 \iff \\ \iff \|By - t\|^2 < R^2 \iff \|B(y - B^{-1}t)\|^2 < R^2 \\ \iff \|\frac{B}{R^2}(y - B^{-1}t)\|^2 < 1 \end{array}$$

So it's equivalent to decide if as $R>0$ varies:



$\cap\, \mathbb{Z}^n = \emptyset$ or not.

$\mathbb{Q}^{n\times n}$

Approximating CVP: Let $B = B^* \cdot R$, $B^* = (b_1^*, \dots, b_n^*) \in \mathbb{Q}^{n\times n}$ $R = \begin{pmatrix} 1 & & \mu_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathbb{Q}^{n\times n}$

GSO of B and suppose that B is LLL-reduced. (i.e. $|\mu_{ij}| \le \frac{1}{2}$ $\forall i,j$ and $\|b_i^*\|^2 \le 2\|b_{i+1}^*\|^2$ $i = 1, \dots, n$).

$\downarrow$

$2^{O(n)}$-Factor Approximation algorithm for CVP:

- polynomial time alg
- output: $v \in \Lambda$ s.t. $\|v-t\| \le 2^{\frac{n}{2}} \underbrace{\min_{v\in\Lambda} \|t-v\|}_{\text{constant}} \le 2^{O(n)}$

Steps: ① $t = B\cdot y^* = B^*\cdot R\cdot y^*$, $\exists y^* \in \mathbb{Q}^n$ (B non singular)

② Find $x \in \mathbb{Z}^n$ s.t. $\|R(x-y^*)\|_\infty \le \frac{1}{2}$: example:

$$R = \begin{pmatrix} 1 & 0.2 & 0.7 \\ 0 & 1 & 0.3 \\ 0 & 0 & 1 \end{pmatrix} \qquad y^* = \begin{pmatrix} 3.2 \\ 5.8 \\ 9.3 \end{pmatrix}$$

from the last one: $|x_3 - 7.3| \le \frac{1}{2}$; $\left|(x_2 - \underbrace{y_2^*}_{5.8}) + 0.3\underbrace{(x_3 - y_3^*)}_{0.3}\right| \le \frac{1}{2} \Rightarrow |x_2 - 5.8 + 0.09| \le \frac{1}{2} \Rightarrow x_2 = 6$

... it always works obviously. (Could be not unique because of $\le \frac{1}{2}$).

Theorem: Let $x \in \mathbb{Z}^n$ be determined as above, i.e. $\|R(x-y^*)\|_\infty \le \frac{1}{2}$ and let $v = Bx \in \Lambda(B)$. $\cap\, \mathbb{Z}^n$

Hence $\|v-t\|_2 \le 2^{\frac{n}{2}} \cdot \min_{u\in\Lambda} \|u-t\|_2$.

Proof $\|v-t\| = \|Bx - By^*\| = \|B^* R(x-y^*)\|$. So we want $\forall z \in \mathbb{Z}^n \ \|B^* R(x-y^*)\| \le 2^{\frac{n}{2}} \|B^* R(z-y^*)\|$.

Let $z \in \mathbb{Z}^n$, $z \neq x$. Suppose j is the last index s.t. $z_j \neq x_j$. If $|[R(y^*-z)]_j| < \frac{1}{2}$:

$$\left| \sum_{i=j}^{n} R_{ji}(y_i^* - z_i) \right| = \left| R_{jj}(y_j^* - z_j) + \sum_{i=j+1}^{n} R_{ji}(y_i^* - z_i) \right| = \begin{cases} R = (0 \nabla) \\ z_i = x_i \ \forall i \ge j+1 \end{cases}$$

$$= \left| R_{jj}(y_j^* - z_j) + \sum_{i=j+1}^{n} R_{ji}(y_i^* - x_i) \right| < \frac{1}{2} \quad \text{(hp.)}$$

but thinking z_j as a variable to find, we are exactly doing the j-th step to find x in the example above and since, now, we have $< \frac{1}{2}$, the only possibility is that $z_j = x_j$, i.e. $|[R(y^*-z)]_j| \ge \frac{1}{2}$. (@)

Now we set $s := R(x-y^*)$ and $r := R(y^*-z)$ and $u := \begin{bmatrix} 0 \\ \vdots \\ r_{j+1} = s_{j+1} \\ \vdots \\ r_n = s_n \end{bmatrix}$, we can write $r = \begin{bmatrix} r' \\ 0 \end{bmatrix} + u$ and $s = \begin{bmatrix} s' \\ 0 \end{bmatrix} + u$. Now:

$$\|B^* \begin{bmatrix} r' \\ 0 \end{bmatrix}\|^2 = \|\sum_{i=1}^{j} b_i^* r_i\|^2 \overset{\text{Pyt.}}{=} \sum_{i=1}^{j} \|b_i^*\|^2 |r_i|^2 \overset{(@)}{\ge} \frac{1}{4} \|b_j^*\|^2 \quad (*)$$

Furthermore: ($\|s\|_\infty \le \frac{1}{2}$ by def of x)

$$\|B^* \begin{bmatrix} s' \\ 0 \end{bmatrix}\|^2 = \|\sum_{i=1}^{j} b_i^* s_i\|_2^2 \overset{\text{Pyt.}}{=} \sum_{i=1}^{j} |s_i|^2 \|b_i^*\|_2^2 \le \frac{1}{4} \sum_{i=1}^{j} \|b_i^*\|_2^2 \quad (*)$$

So: $\|B^* s\|_2^2 = \|B^*\left(\begin{bmatrix} s' \\ 0 \end{bmatrix} + u\right)\|_2^2 = \|B^* \begin{bmatrix} s' \\ 0 \end{bmatrix} + B^* u\|_2^2 =$ ← $\begin{bmatrix} r' \\ 0 \end{bmatrix} \perp u$ and B^* "orthogonal" $\Rightarrow B^* \begin{bmatrix} r' \\ 0 \end{bmatrix} \perp B^* u$

$$= \|B^* \begin{bmatrix} s' \\ 0 \end{bmatrix}\|_2^2 + \|B^* u\|_2^2 \overset{(*)}{\le} \frac{1}{4} \sum_{i=1}^{j} \|b_i^*\|^2 + \|B^* u\|_2^2 \le$$

$$\le \frac{1}{4} \sum_{i=1}^{j} 2^{j-i} \|b_j^*\|_2^2 + \|B^* u\|_2^2 \le \frac{1}{4} 2^n \|b_j^*\|_2^2 + \|B^* u\|_2^2 \le \frac{1}{4} 2^n \cdot 4 \|B^* \begin{bmatrix} r' \\ 0 \end{bmatrix}\|_2^2 + \|B^* u\|_2^2 \quad (*)$$

↑ LLL reduction $\Rightarrow \|b_i^*\|^2 \le 2^{j-i} \|b_j^*\|_2^2$

↑ $2^0 + \dots + 2^{j-1} \le 2^j \le 2^n$

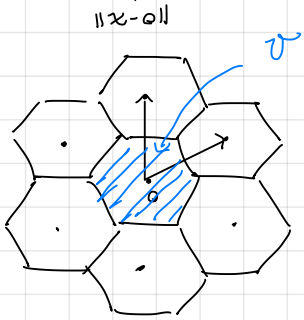
$$\le 2^n \left(\|B^* r'\|_2^2 + \|B^* u\|_2^2\right) = 2^n \|B^* r\|_2^2 \Rightarrow \|B^* s\|_2 \le 2^{\frac{n}{2}} \|B^* r\|_2.$$

↑ $\|B^* u\|_2^2 \le 2^n \|B^* u\|_2^2$ obviously

□

$2^{O(n)}$-time (and space) algorithm for CVP:

$\mathcal{V}(\Lambda) := \{ x \in \mathbb{R}^n : \|x\| \le \|x - v\| \ \forall v \in \Lambda \}$. (Voronoi cells)



Remark $\mathcal{V}(\Lambda)$ is a set of points in $\mathbb{R}^n$ that is closer to 0 than to any other lattice point.

Properties ① $\bigcup_{v\in\Lambda}\left(\mathcal{V}(\Lambda)+v\right)=\mathbb{R}^n$: $\forall x\in\mathbb{R}^n\ \exists\, v\in\Lambda$ s.t. $d(x,v)=\min_{w\in\Lambda} d(x,w)$ (discrete hp.)

$\Rightarrow x\in\mathcal{V}(\Lambda)+v$. They're not disjoint obviously.

② $\mathcal{V}(\Lambda)$ is convex: $\|x\|^2\le\|x-v\|^2\iff x^Tx\le x^Tx+v^Tv-2x^Tv\iff x^Tv\le\frac{\|v\|^2}{2}$

$\Rightarrow \mathcal{V}(\Lambda)=\left\{x\in\mathbb{R}^n:\ x^Tv\le\frac{\|v\|^2}{2}\ \forall v\in\Lambda\right\}$ is convex.
($\tilde{\infty}$ linear inequalities)

③ $\mathcal{V}(\Lambda)$ is simmetric: $\|-x\|\le\|-x-v\|\ \forall v\in\Lambda\iff\|x\|\le\|-x+v\|\ \forall v\in\Lambda$ ($\forall v\in\Lambda\iff\forall -v\in\Lambda$)

$\iff\|x\|\le\|x-v\|\ \forall v\in\Lambda$.

④ $\mathcal{V}(\Lambda)$ is full-dimension (polyhedron) and when Λ is full-dimension so $\mathcal{V}(\Lambda)$ is a polytope: (we really don't say it cause we don't know if the ineq. are finite)

- full-dimension: we show $B(0,\frac{1}{2}\lambda_1)\subseteq\mathcal{V}(\Lambda)$: by contraddiction if $x\in B(0,\frac{1}{2}\lambda_1)$ and $x\notin\mathcal{V}(\lambda)$

$\Rightarrow\exists\, v\neq 0$ s.t. $\|v-x\|<\|x\|$ but $\|x\|\le\frac{1}{2}\lambda_1\Rightarrow\frac{1}{2}\lambda_1>\|v-x\|\ge\|v\|-\|x\|\ge$

$\ge\lambda_1-\frac{1}{2}\lambda_1=\frac{1}{2}\lambda_1$.

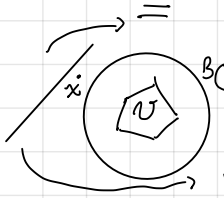
- Λ full dim. $\Rightarrow$ bounded: for point ② we can write $\mathcal{V}(\Lambda)\overset{\text{only }\subseteq}{\subseteq}\left\{x\in\mathbb{R}^n:\ x^T\left(\pm b_i\right)\le\frac{\|b_i\|^2}{2}\right.$

$\forall\, b_i$ vector of the basis$\Big\} = \bigcap_{v\in\{\pm b_i\}} H_v$ $\quad H_v:=\left\{x\in\mathbb{R}^n:\ x^Tv\le\frac{\|v\|^2}{2}\right\}$. They're $2n$ constraints

$\Rightarrow$ is bounded.

- Finite inequalities when bounded: Let's take R s.t. $\bigcap_{v\in\{\pm b_i\}} H_v\subseteq B(0,\sqrt{2R})$.

Obviously $\mathcal{V}(\Lambda)=\bigcap_{\substack{v\in\Lambda\\ \|v\|^2\le 2R}} H_v\ \cap\ \bigcap_{\substack{v\in\Lambda\\ \|v\|^2>2R}} H_v$ $=$ $\bigcap_{\substack{v\in\Lambda\\ \|v\|^2\le 2R}} H_v$ ← they're finite!!!



$\frac{\|v\|^2}{2}>R$ so there are x s.t.

$R<x^Tv<\frac{\|v\|^2}{2}\Rightarrow$ don't cut the ball $\Rightarrow$ don't cut $\mathcal{V}(\Lambda)\Rightarrow$ is redundant.

Exercises: if P is a full-dimensional polytope, then $\exists$ unique $A'x\le b'$ sub-syst. minimal, such that $P=\left\{x\in\mathbb{R}^n:\ A'x\le b'\right\}$. Also, if $a^Tx\le\beta$ can be obtained as a non negative linear combination of two other inequalities, than $a^Tx\le\beta$ is redundant.

Theorem: $\mathcal{V}(\Lambda)$ has at most $2\left(2^n-1\right)$ facets.

Proof Let $v\in\Lambda(B)$, $v=B\cdot x$ $x\in\mathbb{Z}^n$. If $x\equiv 0\pmod 2$ then $v^Tx\le\frac{\|v\|^2}{2}$ is redundant because is dominated by $\left(\frac{1}{2}v\right)^Tx\le\frac{\|\frac{1}{2}v\|^2}{2}$ $\left(\frac{1}{2}v\in\Lambda(B)\right)$. Let $u,v\in\Lambda$ $u=Bx$, $v=By$, $x\equiv y\pmod 2$

If: $\|u\| \geq \|v\|$, then $u^T x \leq \frac{\|u\|^2}{2}$ can be derived with weights '1' from two other inequalities that are valid for $\mathcal{V}$:

$u \neq \pm v$ →

(i) $\left(\frac{1}{2}(u-v)\right)^T x \leq \frac{\|\frac{1}{2}(u-v)\|^2}{2}$ ($\in \mathbb{Z}$ because $x \equiv y \pmod 2 \Rightarrow x - y \equiv 0 \pmod 2$)

(ii) $\left(\frac{1}{2}(u+v)\right)^T x \leq \frac{\|\frac{1}{2}(u+v)\|^2}{2}$ → same argument

Let's add the equations up $u^T x \leq \frac{\|u-v\|^2 + \|u+v\|^2}{8} \leq \frac{4}{8}\|u\|^2$, since $\|u\| \geq \|v\|$ and $u \neq \pm v$

So (i) + (ii) give $u^T x \leq \frac{\|u\|^2}{2}$ and so is not facet-defining.

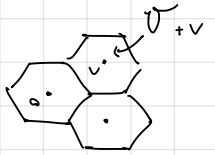
Parallelogram law:
$\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2$

So # facets $\leq 2 \cdot$ (string of 1's, 0's of lenght n that can't be $(0, -, 0)$ (first obs)) $= 2(2^n - 1)$.

↑ in the previous step we excluded $u \neq -v$

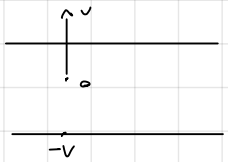
□

$\Lambda \subseteq \mathbb{R}^n$ $\mathcal{V} = \{ x \in \mathbb{R}^n : \|x\| \le \|v - x\| \ \forall v \in \Lambda \setminus \{0\} \}$.



$\mathcal{V} + v$, $v \in \Lambda$

Facets $\le 2(2^n - 1)$ $u, v \in \Lambda$, $u \equiv v \pmod 2$



$\Lambda = \{ Ax : x \in \mathbb{Z}^n \}$ $u = A x_u$ $v = A x_v$ $x_u, x_v \in \mathbb{Z}^n$

$u \equiv v \ (2)$ if $x_u \equiv x_v \ (2)$ (definition) $\leftarrow$

if $\|u\| \ge \|v\|$ and $u \ne v$, then $u^T x \le \frac{\|u\|}{2}$ is not facet-defining. In fact is implied by:

$$+ \begin{cases} \frac{1}{2}(u+v)^T x \le \frac{\|u+v\|^2}{8} = \|u\|^2 + 2u^T v + \|v\|^2 \\ \frac{1}{2}(u-v)^T x \le \frac{\|u-v\|^2}{8} = \frac{\|u\|^2 + 2u^T v + \|v\|^2}{8} \end{cases} \Rightarrow u^T x \le \frac{\|u\|^2 + \|v\|^2}{4} \le \frac{\|u\|^2}{4}$$

For each $p \in \{0,1\}^n \setminus \{0\}$ only "one" $v \in \Lambda$ s.th. $v = A \cdot x$, $x \equiv p \pmod 2$ can define facets

$v^T x \le \frac{\|v\|^2}{2}$, $v^T x \ge -\frac{\|v\|^2}{2}$ $\Rightarrow$ Facets $\le (2^n - 1)2$.

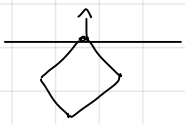
Remark Given a parity vector $p \in \{0,1\}^n - \{0\}$, candidate lattice vector $v \in \Lambda \setminus \{0\}$ for being facet-defining for $\mathcal{V}$: $v = A(2x + p)$, $\|v\|$ minimal. But we are looking for:

$$\min_{x \in \mathbb{Z}^n} \|A(2x+p)\| = \min_{x \in \mathbb{Z}^n} \|(2A)x - (-Ap)\|$$ and so is a closest vector problem

with target $t = -Ap$ in the lattice 2Λ.

The complexity of computing facets of $\mathcal{V}$:

$2^n - 1$ candidates $v_1, \dots, v_{2^n - 1} \in \Lambda$ computed with algorithm for cvp. But for example



$a^T x \le \beta$ is redundant. Note that $a^T x \le \beta$ is redundant $\Leftrightarrow \max_{Ax \le b} a^T x \le \beta$
$Ax \le b$

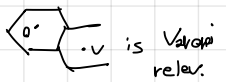
So with linear programming (is polynomial) retrain facets of $\mathcal{V}$ only. So the complexity is $2^{O(n)} \cdot \text{cvp}(n) \cdot \text{poly}(I)$ where I is lenght of input (A,t). Now we want to do a sort of inverse:
↑ it varies

Reducing cvp to Voronoi Cell computation:

Given: $\Lambda(A)$, $A \in \mathbb{Z}^{n \times n}$, $t \in \mathbb{R}^n$, $\mathcal{V}$ ← Facets of Voronoi cells

Task: compute $v \in \Lambda$ s.t. $\|v - t\|$ is minimal.

Def: $v \in \Lambda \setminus \{0\}$ is Voronoi relevant if $v^T x \le \frac{\|v\|^2}{2}$ defines a facet of $\mathcal{V}$.



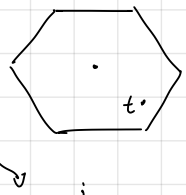
v is Voron. relev.

So a reinterpretation of the task is: find $v \in \Lambda$ s.t. $t \in \mathcal{V} + v$

Idea: Start with 2^j $j \in \mathbb{N}$ large enough s.th.:

$t \in 2^j \cdot \mathcal{V}$ ← Voronoi cell of $\Lambda(2^j A)$, for us $2^j > 2\|t\|_\infty$ is enough (exercise).

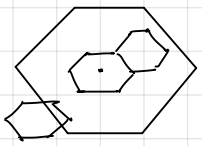
One iteration:



Know $t \in \mathcal{V}_{2\Lambda}$ Question: for which v $t \in (\mathcal{V}_\Lambda + v)$ (*)

(We start with $2^j \Lambda$ the closest vector to t is 0; I take $2^{j-1}\Lambda$ and the closest vector to t is v; but if $u = cvp(t)$ $u \in \Lambda \Rightarrow u - v = cvp(t-v)$ with $v \in \Lambda$).

How to solve (*):



Exercise: # of intersections of $(V_\Lambda + v) \cap V_{2\Lambda} \neq \emptyset$ $\le 4^n$

$\sum \text{vol}\left(\frac{1}{2}\text{ hex}\right) \le \text{vol}\left(2\text{ hex}\right)$

$\left(\frac{1}{2}\right)^n \sum \text{vol}(\text{hex}) \le 2^n \text{vol}(\text{hex}) \Rightarrow \# \le 2^{2n} = 4^n$

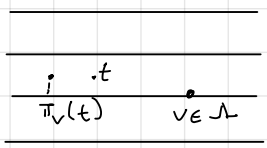
$cvp(n) \le \mathcal{V}(n) + 2^{O(n)} \cdot \text{poly}(I)$

↑ running time for the closest vector problem; ↑ running time for Voronoi-cell construction

The $2^{O(n)}$ time algorithm for cvp.

LLL-Algorithm: compute $\alpha \in \Lambda^*$ s.th. solution of cvp is one of the $2^{O(n)}$ hyperplane:

$\alpha^T x = \lfloor \alpha^T t \rceil + z$ $z \in \mathbb{Z}$, $|z| \le 2^{O(n)}$:



$\alpha^T x = \lfloor \alpha^T t \rceil$

$\alpha^T x = \lfloor \alpha^T t \rceil - 1$

$2^{O(n)}$ cvp's with different targets but the same lattice Λ'

but $(\alpha^T x = \beta) \cap \Lambda = (\alpha^T x = 0 \cap \Lambda) + v$ with $v \in \Lambda$ $\alpha^T x = \beta$ so

So, putting things together:

$V(n) \le 2^{O(n)} cvp(n) \le$ (on the same lattice 2Λ)

$\le 2^{O(n)} 2^{O(n)} cvp(n-1) \le$ ← on lattice

$\le V(n-1) + 2^{O(n)} 2^{O(n)} 2^{O(n)}$

and $cvp(n) \le 2^{O(n)} cvp(n-1) \le V(n-1) + 2^{O(n)} \cdot 2^{O(n)}$ ↑ on the same lattice

$= V(n-1) + 2^{O(n)}$

$(2\Lambda) \cap (\alpha^T x = 0) = 2^{O(n)}$