= Remember the statement

Integer Optimization
Problem Set 1

February 19, 2024

1. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. A vector $v \in \Lambda$ is called *primitive* if Λ has a basis including v.

   Show the following. A lattice vector $v \in \Lambda \setminus \{0\}$ is primitive if and only if there is no lattice point of the form $\mu \cdot v$ with $0 < \mu < 1$.

2. Show that the set $\{x + y\sqrt{2} \colon x, y \in \mathbb{Z}\} \subseteq \mathbb{R}$ is not a lattice.

3. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice, let $u_1, \ldots, u_m \in \Lambda$ be lattice points and let $L = \operatorname{span}\{u_1, \ldots, u_m\}$.

   Let us consider the orthogonal projection

   $$\begin{array}{rccc} \pi\colon & \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ & x & \mapsto & x - l \end{array}$$

   where $l \in L$ such that $x - l \perp u_i$ for each i. This is called the projection onto the orthogonal complement $L^{\perp}$ of L.

   Prove that the image $\Lambda_1 = \pi(\Lambda)$ is a lattice.

4. Let $\Lambda \subset \mathbb{R}^d$ be a lattice, let $b_1, \ldots, b_k \in \Lambda$, $k < d+1$, be lattice points and let A be the affine hull of $\{b_1, \ldots, b_k\}$. Prove that there is a lattice point with the minimum possible positive distance to A.

5. Let $u_1, \ldots, u_d$ be a basis of a lattice $\Lambda \subset \mathbb{R}^d$, let $L_k = \operatorname{span}(u_1, \ldots, u_k)$ for $k = 1, \ldots, d$ and let $L_0 = \{0\}$. Prove that

   $$\| v \| \geqslant \min \operatorname{dist}(u_k, L_{k-1}) \qquad k = 1, \ldots, d$$

   for every vector $v \in \Lambda \setminus \{0\}$.

6. Let $u_1, \ldots, u_d$ and $v_1, \ldots, v_d$ be two bases of a lattice Λ. Suppose that $u_i = \sum_{j=1}^{d} \alpha_{ij} v_j$ and $v_i = \sum_{j=1}^{d} \beta_{ij} u_j$. Let $A = (\alpha_{ij})$ and $B = (\beta_{ij})$ be the $d \times d$ matrices composed of α_{ij}'s and β_{ij}'s correspondingly. Prove that A and B are integer matrices and that $AB = I$ is the identity matrix. Deduce that $|detA| = |detB| = 1$.

1. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. A vector $v \in \Lambda$ is called *primitive* if Λ has a basis including v.

   Show the following. A lattice vector $v \in \Lambda \setminus \{0\}$ is primitive if and only if there is no lattice point of the form $\mu \cdot v$ with $0 < \mu < 1$.

↗ the coefficient must be in $\mathbb{Z}$

$\Rightarrow$ By contradiction, let μv a lattice point with $\mu \in (0,1)$. Let $\{v, v_2, \dots, v_k\}$ a basis of the lattice. But, $\mu v \in \Lambda$ and so:

$$\mu v = \alpha_1 v + \dots + \alpha_k v_k \qquad \alpha_1, \dots, \alpha_k \in \mathbb{Z}$$

$$\Rightarrow (\alpha_1 - \mu) v + \dots + \alpha_k v_k = 0 \overset{v, \dots, v_k \text{ indipendent as vector in } \mathbb{R}^n}{\Longrightarrow} \alpha_1 - \mu = 0 \Rightarrow \alpha_1 = \mu \ \lightning.$$

$\Leftarrow$ By induction on the dimension of Λ:

- $k=1$: v must be a shortest vector of the lattice because, otherwise, $\exists \mu \in (0,1)$ s.t. $\mu v \in \Lambda$ but it's an absurd. So we conclude as in the proof of the theorem.
- $k \to k+1$: we use the same argument used in the existence of a basis, in fact in the proof we have only used that v is the shortest vector in its span (along his direction), that is exactly the hipothesis we have. □

2. Show that the set $\underbrace{\{x + y\sqrt{2} : x, y \in \mathbb{Z}\}}_{\text{!! I}} \subseteq \mathbb{R}$ is not a lattice.

If it was a lattice $\sqrt{2} - 1 \in I$. Furthermore we show by induction that $(\sqrt{2}-1)^n \in I$:

$n = 1$: ok;

$n \to n+1$: $(\sqrt{2}-1)^{n+1} = (\sqrt{2}-1)^n (\sqrt{2}-1) =$ ← induction hypothesis: $\exists x, y \in \mathbb{Z}$ s.t. $(\sqrt{2}-1)^n = (x + y\sqrt{2})$

$$= (x + \sqrt{2}y)(\sqrt{2} - 1) = x\sqrt{2} + 2y - x - \sqrt{2}y =$$

$$= (2y - x) + \sqrt{2}(x - y) \in I$$

But, $0 < \sqrt{2} - 1 < 1$ and so $(\sqrt{2}-1)^n \xrightarrow[n \to +\infty]{} 0$. So, $\forall \varepsilon > 0 \quad I \cap B(0, \varepsilon) \neq \{0\}$; $\lightning$. □

3. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice, let $u_1, \dots, u_m \in \Lambda$ be lattice points and let $L = \operatorname{span}\{u_1, \dots, u_m\}$.

   Let us consider the orthogonal projection

$$\begin{aligned} \pi : \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ x &\mapsto x - l_x \quad (\text{dipende da } x) \end{aligned}$$

   where $l \in L$ such that $x - l \perp u_i$ for each i. This is called the projection onto the orthogonal complement $L^\perp$ of L.

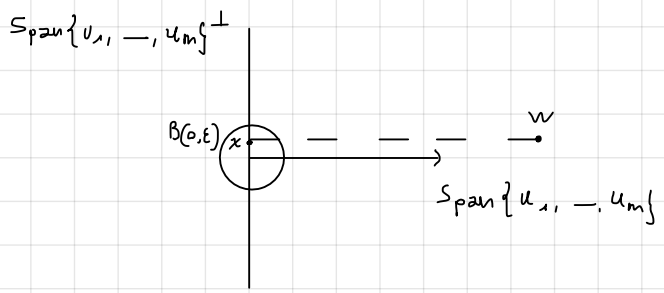
   Prove that the image $\Lambda_1 = \pi(\Lambda)$ is a lattice.

- Subgroup: $\pi(u_i) = 0 \quad \forall i \Rightarrow 0 \in \Lambda_1$.

If $x', y' \in \pi(\Lambda) \Rightarrow \exists\, x, y \in \Lambda$ s.t. $\pi(x) = x'$, $\pi(y) = y' \Rightarrow$:

$$x' - y' = \pi(x) - \pi(y) \underset{\text{linearity}}{=} \pi(x-y) \in \pi(\Lambda)$$

- Discrete: by contraddiction suppose $\exists \varepsilon$ s.t. $B(0,\varepsilon) \cap \pi(\Lambda)$ is infinite. Let $x \in B(0,\varepsilon) \cap \Lambda'$, then $\exists\, w \in \Lambda$ s.t. $\pi(w) = x \iff w - l = x \iff w = l + x$



Now, $l \in \text{Span}\{u_1, \dots, u_m\}$ ($\pi : \mathbb{R}^n \longrightarrow \mathbb{R}^n \cong \text{Span}\{u_1, \dots, u_m\} \oplus \text{Span}\{u_1, \dots, u_m\}^\perp$ $\pi(w) = l + x$). So, $l = \sum_{i=1}^{m} \lambda_i u_i$ and considering $w := \sum_{i=1}^{m} \lfloor \lambda_i \rfloor u_i \in \Lambda$ ($u_i \in \Lambda$ and $\lfloor \lambda_i \rfloor \in \mathbb{Z}$) we have $w - w' = x + \sum_{i=1}^{m} \{\lambda_i\} u_i \in I$ and $\| w - w' \|_2 \le \varepsilon + m \cdot \max_{i=0,\dots,m} |u_i|$.

Hence, $\Lambda \cap B(0, \varepsilon + m \cdot \max_{i=0,\dots,m} |u_i|)$ would be infinite. $\lightning$.

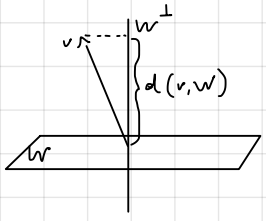
□

4. Let $\Lambda \subset \mathbb{R}^d$ be a lattice, let $b_1, \dots, b_k \in \Lambda, k < d+1$, be lattice points and let A be the affine hull of $\{b_1, \dots, b_k\}$. Prove that there is a lattice point with the minimum possible positive distance to A.

$$A = \left\{ \sum_{i=1}^{k} \alpha_i b_i \;\middle|\; \alpha_i \in \mathbb{R} \text{ (not } \in \mathbb{R}_0^+), \; \sum_{i=1}^{k} \alpha_i = 1 \right\}.$$

Now, an affine hull is an affine space so it can be seen as $b_1 + W$ where W is a vectorial space. If we had the thesis for vectorial space we would have $w \in \Lambda$ that has a point with the minimum possible positive distance to W, so $w + b_1 \in \Lambda$ and has the minum possible positive distance to $b_1 + W = A$.

So, we can suppose A linear. Now, the distance between a vector and a linear space is the projection onto the orthogonal of the linear space:



Hence, we do the projection $\pi(\Lambda)$ onto $W^{\perp}$, we know $\pi(\Lambda)$ is a lattice so has a "shortest vector", call it z. Now, $\overline{z} \in \pi^{-1}(z)$ will be the vector we were looking for.

5. Let $u_1,\dots,u_d$ be a basis of a lattice $\Lambda \subset \mathbb{R}^d$, let $L_k = \text{span}(u_1,\dots,u_k)$ for $k = 1,\dots,d$ and let $L_0 = \{0\}$. Prove that

$$\| v \| \geqslant \min \text{dist}(u_k, L_{k-1}) \qquad k = 1,\dots,d$$

for every vector $v \in \Lambda \backslash \{0\}$.

Consider $u_1^*, \_, u_d^*$ the G.S. basis associated. We know that for all K $\text{Span}(u_1,\_,u_K) =$

$= \text{Span}(u_1^*, \_, u_K^*)$. So, the thesis is to prove:

$$\|v\| \geq \min \text{dist}\left(u_K, \text{Span}(u_1^*, \_, u_{K-1}^*)\right) \qquad K = 1,\_,d, \; v \in \Lambda \backslash \{0\}$$

$$\| u_K - \underbrace{\sum_{i=1}^{K-1} \alpha_i u_i^*}_{\text{generic element in } \text{Span}(u_1^*,\_,u_{K-1}^*)} \|^2 = \quad \text{Gram-Schmidt theorem}$$

$$= \| u_K^* + \sum_{i=1}^{K-1} \mu_i u_i^* - \sum_{i=1}^{K-1} \alpha_i u_i^* \|^2 =$$

$$= \| u_K^* + \sum_{i=1}^{K-1} (\mu_i - \alpha_i) u_i^* \|^2 =$$

$$= \| u_K^* \|^2 + \sum_{i=1}^{K-1} (\mu_i - \alpha_i)^2 \| u_i^* \|^2$$

So if I choose $\alpha_i = \mu_i$ we have $\text{dist}(u_K, \text{Span}(u_1^*, \_, u_{K-1}^*)) = \| u_K^* \|$ so

$\min_{K=1,\_,n} \text{dist}(u_K, \text{Span}(u_1^*, \_, u_{K-1}^*)) \leq \min_{K=1,\_,n} \| u_K^* \| \leq \|v\|$ where the last inequality comes from the corollary. □

6. Let $u_1,\dots,u_d$ and $v_1,\dots,v_d$ be two bases of a lattice Λ. Suppose that $u_i = \sum_{j=1}^d \alpha_{ij} v_j$ and $v_i = \sum_{j=1}^d \beta_{ij} u_j$. Let $A = (\alpha_{ij})$ and $B = (\beta_{ij})$ be the $d \times d$ matrices composed of α_{ij}'s and β_{ij}'s correspondingly. Prove that A and B are integer matrices and that $AB = I$ is the identity matrix. Deduce that $|detA| = |detB| = 1$.

By definition, since $\{v_i\}_i$ is a basis for Λ and $u_i \in \Lambda \; \forall i$ we can write $u_i = \sum_j \alpha'_{ij} v_j$ where $\alpha'_{ij} \in \mathbb{Z} \; \forall ij$ and by uniqueness of the basis scripture we have $\alpha'_{ij} = \alpha_{ij} \; \forall i,j$. Viceversa for β_{ij}. So, A and B are integer matrices.

Also: $A = M_U^V$ and $B = M_V^U$ are the matrix for changing from basis U to basis V and viceversa. So, for linear algebra knowledge, $AB = BA = Id$.

By induction, the determinant of an integer matrix is an integer and so, since $\det(A) = \frac{1}{\det(B)}$, the only possibility is that $|\det(A)| = |\det(B)| = 1$.

□

= Remember the statement

Integer Optimization
Problem Set 2

February 26, 2024

1. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $v \in \Lambda \setminus \{0\}$ be a shortest vector, i.e., a nonzero lattice vector of minimum norm $\|\cdot\|_2$. We have seen in class that $\Lambda' = \{\pi(v) : v \in \Lambda\} \subseteq \mathbb{R}^n$ is a lattice and therefore has a basis $b'_1, \ldots, b'_k$. Recall that $\pi(u) = u - \lambda v$ where $\lambda \in \mathbb{R}$ satisfies $(u - \lambda v) \perp v$.

   Let $b_1, \ldots, b_k \in \Lambda$ such that $\pi(b_i) = b'_i$ for each i. Show the following:

   i) $b_1, \ldots, b_k, v$ are linearly independent.

   ii) The vectors $b_1, \ldots, b_k, v$ generate Λ.

   Give an example of a lattice $\Lambda \subseteq \mathbb{R}^2$ where 1ii cannot be concluded if v is not a shortest vector in the lattice.

2. Let $\Lambda(A) \subseteq \mathbb{R}^n$ be a lattice, where $A \in \mathbb{R}^{n \times n}$ is non-singular. Define the set

$$\Lambda^* = \left\{ y \in \mathbb{R}^n : y^T v \in \mathbb{Z} \text{ for each } v \in \Lambda \right\}.$$

   Show that Λ^* is a lattice. Determine a basis of Λ^*. What is $det(\Lambda^*)$?
   Λ^* *is called the dual lattice of* Λ.

3. Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice. Assume $b_1, \ldots, b_n \in \Lambda$ are linearly independent and that minimize $|\det(b_1, \ldots, b_n)|$ over all n linearly independent lattice vectors. Prove that $b_1, \ldots, b_n$ is a basis of Λ.

4. Let $B \in \mathbb{Q}^{n \times n}$ be a lattice basis that consists of pairwise orthogonal vectors. Prove that the shortest vector of $\Lambda(B)$ is the shortest column vector of B.

5. Given a lattice Λ, we denote by $\lambda_k(\Lambda) \in \mathbb{R}_{>0}$ the minimal number so that $B(0, \lambda_k)$ contains k linearly independent lattice vectors. Show that for any lattice $\Lambda \subseteq \mathbb{R}^n, \lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \geqslant 1$.

6. Let $\Lambda \subset \mathbb{R}^d$ be a full-dimensional lattice and let $u_1, \ldots, u_d$ be a set of vectors from Λ such that the volume of the parallelepiped

$$\{\alpha_1 u_1 + \ldots + \alpha_d u_d, \quad 0 \leqslant \alpha_i \leqslant 1 \quad \text{for } i = 1, \ldots, d\}$$

   is equal to $\det \Lambda$. Prove that $u_1, \ldots, u_d$ is a basis of Λ.

1. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $v \in \Lambda \setminus \{0\}$ be a shortest vector, i.e., a nonzero lattice vector of minimum norm $\|\cdot\|_2$. We have seen in class that $\Lambda' = \{\pi(v) : v \in \Lambda\} \subseteq \mathbb{R}^n$ is a lattice and therefore has a basis $b'_1, \ldots, b'_k$. Recall that $\pi(u) = u - \lambda v$ where $\lambda \in \mathbb{R}$ satisfies $(u - \lambda v) \perp v$.

Let $b_1, \ldots, b_k \in \Lambda$ such that $\pi(b_i) = b'_i$ for each i. Show the following:

i) $b_1, \ldots, b_k, v$ are linearly independent.

ii) The vectors $b_1, \ldots, b_k, v$ generate Λ.

iii) Give an example of a lattice $\Lambda \subseteq \mathbb{R}^2$ where 1ii cannot be concluded if v is not a shortest vector in the lattice.

(i) $\alpha_1 b_1 + \cdots + \alpha_K b_K + \alpha v = 0 \Rightarrow \pi(\cdot) = 0 \overset{\pi(v)=0}{\Rightarrow} \alpha_1 b'_1 + \cdots + \alpha_K b'_K = 0$ but $b'_1, \ldots, b'_K$ is a basis for Λ' so are independent and so $\alpha_1 = \cdots = \alpha_K = 0$. Hence, $\alpha v = 0 \Rightarrow \alpha = 0$.

(ii) $w = (w - \lambda v) + \lambda v$ and $w - \lambda v = \pi(w) \in \Lambda'$ so can be written as $z_1 b'_1 + \cdots + z_K b'_K$ $z_1, \ldots, z_K \in \mathbb{Z}$

$$\Rightarrow w = \sum_{i=1}^{K} z_i b'_i + \lambda v = \sum_{i=1}^{K} z_i \left(b_i - \lambda_{b_i} v\right) + \lambda v = \sum_{i=1}^{K} z_i b_i + \left(\lambda - \sum_{i=1}^{K} \lambda_{b_i}\right) v.$$

Now, if $\lambda - \sum_{i=1}^{K} \lambda_{b_i} \notin \mathbb{Z}$ so I can take $\left\| \left(\lambda - \sum_{i=1}^{K} \lambda_{b_i}\right) v - \left\lfloor \lambda - \sum_{i=1}^{K} \lambda_{b_i} \right\rfloor v \right\|_2 < \|v\|_2$, $\lightning$.

($\in \Lambda$ because is $w - \sum_{i=1}^{K} K_i b_i$ $K_i \in \mathbb{Z}$; $w \in \Lambda$, $\sum K_i b_i \in \Lambda$)

(iii) Consider $\mathbb{Z}^n \subseteq \mathbb{R}^n$. $v = 2e_n$ and $b_1 = e_1, \ldots, b_{n-1} = e_{n-1}$. So let's see e_n can't be generated by $b_1, \ldots, b_{n-1}, v$: $\mathbb{R}^n = \mathrm{Span}\{2e_n\} \oplus \mathrm{Span}^{\perp}\{2e_n\} = \mathrm{Span}\{e_n\} \oplus \mathrm{Span}\{b_1, \ldots, b_{n-1}\}$

so the only possibility is $e_n = K \, 2 e_n \Leftrightarrow K = \frac{1}{2} \notin \mathbb{Z}$.

2. Let $\Lambda(A) \subseteq \mathbb{R}^n$ be a lattice, where $A \in \mathbb{R}^{n \times n}$ is non-singular. Define the set

$$\Lambda^* = \{y \in \mathbb{R}^n : y^T v \in \mathbb{Z} \text{ for each } v \in \Lambda\}.$$

1 Show that Λ^* is a lattice. 2 Determine a basis of Λ^*. 3 What is $det(\Lambda^*)$?
Λ^* is called the dual lattice of Λ.

(1) $0 \in \Lambda^*$: $0 \in \mathbb{R}^n$ $0 \cdot v = 0 \in \mathbb{Z}$ $\forall v \in \Lambda$

$x, y \in \Lambda^* \Rightarrow x - y \in \Lambda^*$: $(x - y)^T v = \underset{\in \mathbb{Z}}{x^T v} - \underset{\in \mathbb{Z}}{y^T v} \in \mathbb{Z}$ $\forall v \in \Lambda$

Discrete: By contradiction $\forall \varepsilon > 0$ $\exists\, y_\varepsilon \in \Lambda^* \cap B(0, \varepsilon) \setminus \{0\}$, $\{b_1, \ldots, b_n\}$ basis of the lattice Λ

take $\varepsilon < \frac{1}{\|b_i\|_2}$

$\mathbb{Z} \ni |\langle y_\varepsilon, b_i \rangle| \leq \|y_\varepsilon\|_2 \|b_i\|_2 \leq \varepsilon \|b_i\|_2 < 1$. I take $\overline{\varepsilon} = \min_{i=1,\ldots,n} \frac{1}{\|b_i\|_2}$

so $|\langle y_\varepsilon, b_i \rangle| = 0$ $\forall i \Rightarrow y_\varepsilon = 0$ $\lightning$.

(2) We can see $\Lambda^* = \{y \in \mathbb{R}^n : y^T b^i \in \mathbb{Z}\ \forall b_i = 1, \ldots, n\}$ where $\{b^1, \ldots, b^n\}$ basis of Λ.

So, we have that $y \in \Lambda^* \iff \begin{cases} y_1 b_1^1 + \dots + y_n b_n^1 = K_1 \in \mathbb{Z} \\ \vdots \\ y_1 b_1^n + \dots + y_n b_n^n = K_n \in \mathbb{Z} \end{cases}$ (*)

where $y_1, \dots, y_n, K_1, \dots, K_n$ are variables so we have a system in $2n$ variables and n equations.

Since A is not singular it has always solution so the $\dim(\Lambda^*) = 2n - n = n$. Furthermore:

$$(*) \iff \underbrace{\begin{pmatrix} b_1^1 & \dots & b_n^1 \\ \vdots & & \vdots \\ b_1^n & \dots & b_n^n \end{pmatrix}}_{A^T} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{Z}^n \iff A^T y \in \mathbb{Z}^n \iff y \in (A^T)^{-1}\mathbb{Z}^n$$

$$\iff y = (A^T)^{-1}\begin{pmatrix} K_1 \\ \vdots \\ K_n \end{pmatrix} = (A^T)^{-1}(K_1 e_1 + \dots + K_n e_n) = K_1((A^T)^{-1}e_1) + \dots + K_n((A^T)^{-1}e_n)$$

(Faster: $y^T b_i = K_i \in \mathbb{Z}\ \forall b_i \iff \begin{pmatrix} b_1^T \\ \vdots \\ b_n^T \end{pmatrix} y = \begin{pmatrix} K_1 \\ \vdots \\ K_n \end{pmatrix} \in \mathbb{Z}^n \iff B^T y \in \mathbb{Z}^n \iff y \in B^{-T}\mathbb{Z}^n$)

So a basis for Λ^* will be $\{(A^T)^{-1}e_i\}_{i=1,\dots,n}$.

(3) $\det(\Lambda^*) = |\det((A^T)^{-1})| = \dfrac{1}{|\det(A^T)|} = \dfrac{1}{|\det(A)|} = \dfrac{1}{\det(\Lambda)}$

3. Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice. Assume $b_1, \dots, b_n \in \Lambda$ are linearly independent and that minimize $|\det(b_1, \dots, b_n)|$ over all n linearly independent lattice vectors. Prove that $b_1, \dots, b_n$ is a basis of Λ.

Suppose $b_1, \dots, b_n$ is not a basis. So $\exists v \in \Lambda$ s.t. $v = \sum_{i=1}^n \lambda_i b_i$ where at least one $\lambda_i \notin \mathbb{Z}$ ($b_1, \dots, b_n$ is a basis of $\mathbb{R}^n$). w.l.o.g. $\lambda_1, \dots, \lambda_K \in \mathbb{Z}$; $\lambda_{K+1}, \dots, \lambda_n \notin \mathbb{Z}$. Now:

$$v - \underbrace{\sum_{i=1}^{K} \lambda_i b_i}_{\in \Lambda} = \sum_{i=K+1}^{n} \lambda_i b_i \implies \in \Lambda. \quad \text{So,} \quad \sum_{i=K+1}^{n} \lambda_i b_i - \sum_{i=K+1}^{n} \lfloor \lambda_i \rfloor b_i = \sum_{i=K+1}^{n} \{\lambda_i\} b_i \in \Lambda$$

Now $\{b_1, \dots, b_K, b_{K+1}, \dots, b_{n-1}, \sum_{i=K+1}^{n} \{\lambda_i\} b_i\}$ is always a set of n indipendent lattice vector but:

$$\left|\det\left(b_1, \dots, \sum_{K+1}^{n} \{\lambda_i\} b_i\right)\right| = \left|\sum_{i=K+1}^{n} \{\lambda_i\} \det(b_1, \dots, b_{n-1}, b_i)\right| = |\{\lambda_n\}|\,|\det(b_1, \dots, b_n)| <$$

$$< |\det(b_1, \dots, b_n)|. \quad \lightning$$

4. Let $B \in \mathbb{Q}^{n \times n}$ be a lattice basis that consists of pairwise orthogonal vectors. Prove that the shortest vector of $\Lambda(B)$ is the shortest column vector of B.

$$\Lambda(B) = \{a_1 B^1 + \dots + a_n B^n \mid a_1, \dots, a_n \in \mathbb{Z}\}.$$

$$\|a_1 B^1 + \dots + a_n B^n\|_2^2 \overset{\text{orthogonal}}{=} \sum_{i=1}^{n} a_i^2 \|B^i\|_2^2 \overset{a_i \in \mathbb{Z}}{\geq} \|B^i\|_2^2 \geq \min_{i=1,\dots,n} \|B^i\|_2^2.$$

5. Given a lattice Λ, we denote by $\lambda_k(\Lambda) \in \mathbb{R}_{>0}$ the minimal number so that $B(0, \lambda_k)$ contains k linearly independent lattice vectors. Show that for any lattice $\Lambda \subseteq \mathbb{R}^n, \lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \geqslant 1$.

In $B(0, \lambda_1(\Lambda))$ there is only one vector of Λ that is not 0, let's call it v.

In $B(0, \lambda_K(\Lambda))$ there are K vectors linearly indipendent of Λ^* $w_1, \dots, w_n$ (in particular they're a basis). Now by definition $\langle v, w_i \rangle \in \mathbb{Z}$ and, since $v \neq 0$ and $\{w_1, \dots, w_n\}$ is a basis, exists $i \in \{1, \dots, n\}$ s.th. $\langle v, w_i \rangle \neq 0$. Now,:

$$1 \leq |\langle v, w_i \rangle| \leq \|v\|_2 \cdot \|w_i\|_2 \leq \lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*)$$

$\uparrow$

$\langle v, w_i \rangle \neq 0$ and in $\mathbb{Z}$

6. Let $\Lambda \subset \mathbb{R}^d$ be a full-dimensional lattice and let $u_1, \dots, u_d$ be a set of vectors from Λ such that the volume of the parallelepiped

$$V(U) = \{\alpha_1 u_1 + \dots + \alpha_d u_d\} \quad 0 \leqslant \alpha_i \leqslant 1 \quad \text{for } i = 1, \dots, d\}$$

is equal to $\det \Lambda$. Prove that $u_1, \dots, u_d$ is a basis of Λ.

$V(U) = |\det(U)|$ where $U = (u_1, \dots, u_d)$.

Now, $\det(\Lambda) = |\det(B)|$ where B is a basis. So $|\det(U)| = |\det(B)| \neq 0$.

In particular, U is full rank and so $u_1, \dots, u_n$ are linearly indipendents.

If we say that $|\det(U)|$ minimizes the quantity $|\det(a_1, \dots, a_d)|$ with $a_1, \dots, a_d$ linearly indipendent lattice vectors, we obtain the thesis for Ex. 3. So, in general, we want to say that if $\{b_1, \dots, b_d\}$ is a basis, $|\det(b_1, \dots, b_d)|$ is the minimum of the previous quantity.

Let's take $a_1, \dots, a_d$ linearly indipendent lattice vectors so there is an integer matrix M s.t. $A = BM$ (B is a basis so by definition M is integer). So:

$|\det(A)| = |\det(B)| |\det(M)|$ but M is integer $\Rightarrow |\det(M)| \in \mathbb{Z} \setminus \{0\} \Rightarrow$

$|\det(A)| \geq |\det(B)|$.

Integer Optimization
Problem Set 3

March 4, 2024

1. Let $\Lambda \subseteq \mathbb{R}^2$ be a lattice and $b_1, b_2 \in \Lambda \setminus \{0\}$ be a basis of Λ, ordered such that $\|b_1\|_2 \leqslant \|b_2\|_2$.

   i) Show that $b_1, b_2 - x b_1$, $x \in \mathbb{Z}$ is also a basis of Λ.

   ii) Let $b_2^* = b_2 - \mu b_1$ with $\mu = <b_2, b_1> / <b_1, b_1>$ be the *projection* of b_2 into the *orthogonal complement of* b_1.
   Prove that, if $|\mu| > 1/2$, then $b_2 - \lfloor \mu \rceil \cdot b_1$ is strictly shorter than b_2, w.r.t. $\|\cdot\|_2$. Here $\lfloor \mu \rceil$ is the closest integer to μ.

   iii) Show that the following algorithm terminates in $O(\log(\|b_2\|)$ many steps: While $\|b_2^*\| \leqslant \frac{1}{4}\|b_1\|$: Replace b_2 by $b_2 - \lfloor \mu \rceil \cdot b_1$. Swap b_1 and b_2.
   Hint: $b_2 - \lfloor \mu \rceil \cdot b_1$ is much shorter than b_2.

   iv) We call b_1, b_2 *partially reduced* if $\|b_2\| \geqslant \|b_1\|$ and $\|b_2^*\| \geqslant \frac{1}{4}\|b_1\|$ holds. Show how to compute a shortest nonzero lattice vector in constant time, given a partially reduced basis.
   Hint: The length of $x b_1 + y b_2$ is at least $|y| \, \|b_2^*\| \geqslant |y| \|b_2\|/4$.

   v) Conclude the following. Given a non-singular $B \in \mathbb{Z}^{2\times 2}$ the shortest vector of $\Lambda(B)$ can be computed in time polynomial in the binary encoding length of the matrix $B \in \mathbb{Z}^{2\times 2}$ (number of bits needed to encode B).

2. Let $\Lambda \subseteq \mathbb{Z}^n$ be a full-dimensional integer lattice. Show that $\det(\Lambda) \cdot \mathbb{Z}^n \subseteq \Lambda$.

3. Use Minkowski's theorem to show the following result of Dirichlet:
   Let $Q \geqslant 1$ be a real number and let $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. There exists an integer q and integers $p_1, \ldots, p_n$ with

   (a) $1 \leqslant q \leqslant Q^n$

   (b) $|q \cdot \alpha_i - p_i| \leqslant \frac{1}{Q}$ for $i = 1, \ldots, n$.

4. Let $\Lambda := \Lambda(B) \subseteq \mathbb{R}^n$ be a full rank lattice for the basis B. Let $v_1, \ldots, v_n \in \Lambda \setminus \{0\}$ be linear independent vectors. Then $\max\{\| v_1 \|_2, \ldots, \| v_n \|_2\} \geqslant \| b_n^* \|_2$ where b_n^* is the "last" vector in the Gram-Schmidt orthogonalization of $B = (b_1, \ldots, b_n)$.

5. Let $B \in \mathbb{R}^{n\times n}$ be a regular matrix and let $\Lambda := \Lambda(B)$ be the lattice spanned by B. The *orthogonality defect* of the basis B is given by

$$\gamma(B) := \frac{\prod_{i=1}^n \|b_i\|_2}{\prod_{i=1}^n \|b_i^*\|_2}.$$

   Let $v \in \Lambda(B) \setminus \{0\}$ be a shortest vector of Λ w.r.t. the ℓ_2-norm. Show that one has

$$v = B x, \; x \in \mathbb{Z}^n \text{ with } \|x\|_\infty \leqslant \gamma(B).$$

1. Let $\Lambda \subseteq \mathbb{R}^2$ be a lattice and $b_1, b_2 \in \Lambda \setminus \{0\}$ be a basis of Λ, ordered such that $\|b_1\|_2 \leqslant \|b_2\|_2$.

   i) Show that $b_1, b_2 - x b_1$, $x \in \mathbb{Z}$ is also a basis of Λ.

   ii) Let $b_2^* = b_2 - \mu b_1$ with $\mu = <b_2, b_1>/<b_1, b_1>$ be the *projection* of b_2 into the *orthogonal complement of* b_1.
   Prove that, if $|\mu| > 1/2$, then $b_2 - \lfloor \mu \rceil \cdot b_1$ is strictly shorter than b_2, w.r.t. $\|\cdot\|_2$. Here $\lfloor \mu \rceil$ is the closest integer to μ.

   iii) Show that the following algorithm terminates in $O(\log(\|b_2\|))$ many steps: While $\|b_2^*\| \leqslant \frac{1}{4}\|b_1\|$: Replace b_2 by $b_2 - \lfloor \mu \rceil \cdot b_1$. Swap b_1 and b_2.
   Hint: $b_2 - \lfloor \mu \rceil \cdot b_1$ is much shorter than b_2.

   iv) We call b_1, b_2 *partially reduced* if $\|b_2\| \geqslant \|b_1\|$ and $\|b_2^*\| \geqslant \frac{1}{4}\|b_1\|$ holds. Show how to compute a shortest nonzero lattice vector in constant time, given a partially reduced basis.
   Hint: The length of $x b_1 + y b_2$ is at least $|y| \|b_2^*\| \geqslant |y| \|b_2\|/4$.

   v) Conclude the following. Given a non-singular $B \in \mathbb{Z}^{2\times 2}$ the shortest vector of $\Lambda(B)$ can be computed in time polynomial in the binary encoding length of the matrix $B \in \mathbb{Z}^{2\times 2}$ (number of bits needed to encode B).

(i) $v \in \Lambda$, so $v = a_1 b_1 + a_2 b_2$ with $a_1, a_2 \in \mathbb{Z}$. So $v = a_1 b_1 + a_2 b_2 = a_1 b_1 + a_2 b_2 + a_2 x b_1 - a_2 x b_1 =$

$= (a_1 + a_2 x) b_1 + a_2 (b_2 - x b_1)$ where $a_1 + a_2 x \in \mathbb{Z}$.

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

$$\|b_2 - \lfloor \mu \rceil b_1\|^2 = \|b_2^*\|^2 + \tfrac{1}{4}\|b_1\|^2 < \|b_2\|^2 - \tfrac{1}{4}\|b_1\| + \tfrac{1}{4}\|b_1\| = \|b_2\|^2$$

$$b_2 = b_2^* + \mu b_1 \Rightarrow \|b_2\|^2 = \|b_2^*\|^2 + |\mu|^2\|b_1\|^2 \Rightarrow \|b_2^*\|^2 = \|b_2\|^2 - |\mu|^2\|b_1\|^2 < \|b_2\|^2 - \tfrac{1}{4}\|b_1\|$$

(b_2^* orthogonal)

(iii) $(b_1, b_2) \overset{\text{replace}}{\rightsquigarrow} (b_1, b_2 - \lfloor \mu \rceil b_1) \overset{\text{swap}}{\rightsquigarrow} (b_2 - \lfloor \mu \rceil b_1, b_1) =: (b_1^{NEW}, b_2^{NEW})$

$$sv(\Lambda)^4 \leq \|b_1^{NEW}\|^2 \|b_2^{NEW}\|^2 \leq \left(\tfrac{5}{16}\right)^i \|b_2\|^2 \cdot \|b_1\|^2 \leq \left(\tfrac{5}{16}\right)^i \|b_2\|^4 \Rightarrow \left(\tfrac{16}{5}\right)^i \leq \left(\frac{\|b_2\|}{sv(\Lambda)}\right)^4$$

$$\|b_2 - \lfloor \mu \rceil b_1\|^2 = \|b_2^* + \lambda b_1\|^2 \leq$$

$$\leq \|b_2^*\|^2 + \tfrac{1}{4}\|b_1\|^2 \leq \tfrac{1}{16}\|b_1\|^2 + \tfrac{1}{4}\|b_1\|^2 =$$

$$= \tfrac{5}{16}\|b_1\|^2 \leq \tfrac{5}{16}\|b_2\|^2$$

$$\Rightarrow i \leq 4 \log_{\frac{16}{5}}\left(\frac{\|b_2\|}{sv(\Lambda)}\right) =$$

$$= 4 \frac{\log_{10}\|b_2\|}{\log_{10}\frac{16}{5}} =$$

$$= O(\log\|b_2\|)$$

(iv) We want to write the shortest vector v in the basis (b_1, b_2^*) as

$v = x_1 b_1 + x_2 b_2^*$. So $\|v\|^2 = x_1^2\|b_1\|^2 + x_2^2\|b_2^*\|^2 \geq x_2^2\|b_2^*\|^2 \geq x_2^2 \frac{1}{16}\|b_1\|^2 \geq x_2^2 \frac{1}{16}\|v\|^2$ (v is the sv)

$\Rightarrow x_2^2 \leq 16 \Rightarrow |x_2| \leq 4$ (9 cases).

On the other hand $\|b_1^*\|\|b_2\| = \det(\Lambda) = \|b_1\|\|b_2^*\| \geq \frac{1}{4}\|b_1\|^2 \Rightarrow \|b_2^*\| \geq \|b_1^*\|$

$$\|b_1^*\| \geq \tfrac{1}{4}\|b_2\|$$

$$(b_2^1)^2 + (b_2^2)^2 \leq 2\max\left((b_2^1)^2, (b_2^2)^2\right) \leq$$

$$\leq 2\max\left(b_2^1, b_2^2, b_1^1, b_1^2\right)^2$$

(v) $4 \cdot \operatorname{argmax}_N \{2^N < \text{numero}\}$ = binary enc. lenght

2. Let $\Lambda \subseteq \mathbb{Z}^n$ be a full-dimensional integer lattice. Show that $\det(\Lambda) \cdot \mathbb{Z}^n \subseteq \Lambda$.

Note that if $\Lambda = \Lambda(B) \Rightarrow B^{-1} = \frac{1}{\det(B)} \operatorname{adj}(B) \Rightarrow \det(B)\, Id = B \cdot \operatorname{adj}(B)$ where $\operatorname{adj}(B) \in \mathbb{Z}^{n \times n}$

$$\det(\Lambda)\mathbb{Z}^n = |\det(B)|\mathbb{Z}^n = \begin{cases} \det(B)\mathbb{Z}^n = \det(B)\, Id \cdot \mathbb{Z}^n = B \overbrace{\operatorname{adj}(B)\mathbb{Z}^n}^{\subseteq \mathbb{Z}^n} \subseteq \Lambda, & \det(B) > 0 \\ -\det(B)\mathbb{Z}^n = -\det(B)\, Id \cdot \mathbb{Z}^n = -B \underbrace{\operatorname{adj}(B)\mathbb{Z}^n}_{\subseteq \mathbb{Z}^n} \subseteq \Lambda, & \det(B) < 0 \end{cases}$$

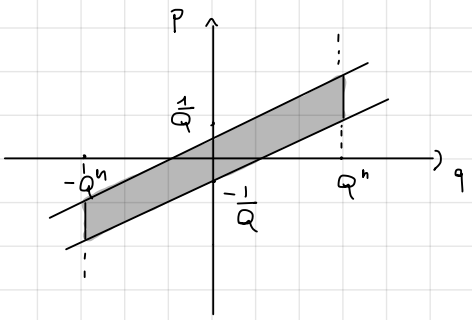
3. Use Minkowski's theorem to show the following result of Dirichlet:
Let $Q \geqslant 1$ be a real number and let $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. There exists an integer q and integers $p_1, \ldots, p_n$ with

(a) $1 \leqslant q \leqslant Q^n$

(b) $|q \cdot \alpha_i - p_i| \leqslant \frac{1}{Q}$ for $i = 1, \ldots, n$.

we put the module so K is symmetric

$$K = \left\{ (p_1, \ldots, p_n, q) \in \mathbb{R}^{n+1} \;\middle|\; |q\alpha_i - p_i| \leq \frac{1}{Q} \quad i = 1, \ldots, n \;;\; |q| \leq Q^n \right\}$$



$q\alpha - p \leq \frac{1}{Q} \quad p \geq q\alpha - \frac{1}{Q} \quad p = q\alpha - \frac{1}{Q}$

$q\alpha - p \geq -\frac{1}{Q} \quad p \leq q\alpha + \frac{1}{Q} \quad p = q\alpha + \frac{1}{Q}$

So K is centrally simmetric, convex, bounded and $\operatorname{Vol}(K) = 2Q^n \left(2 \cdot \frac{1}{Q}\right)^n = 2^{n+1}$

So, from Minkowski theorem we know $(q, p_1, \ldots, p_n) \in \mathbb{Z}^n \cap K$ (hoj greater than 2^{n+1}). Now $q \neq 0$ because otherwise $p_1 = \ldots = p_n = 0$ $(Q > 1)$ and if $q < 0$ i choose $(-q, -p_1, \ldots, -p_n) \in \mathbb{Z}^n \cap K$

4. Let $\Lambda := \Lambda(B) \subseteq \mathbb{R}^n$ be a full rank lattice for the basis B. Let $v_1, \ldots, v_n \in \Lambda \setminus \{0\}$ be linear independent vectors. Then $\max\{\| v_1 \|_2, \ldots, \| v_n \|_2\} \geqslant \| b_n^* \|_2$ where b_n^* is the "last" vector in the Gram-Schmidt orthogonalization of $B = (b_1, \ldots, b_n)$.

Consider $u \in \mathbb{Z}^{n \times n}$ the matrix such that $(v_1, \ldots, v_n) = Bu$. Since u is nonsingular ($(v_1, \ldots, v_n)$ and B are nonsingular) $\exists$ column K of u such that $u_{n,K} \neq 0$. It means

$$v_K = \sum_{i=1}^{n} \lambda_i b_i \quad \text{with } \lambda_n \neq 0,\ \lambda_n \in \mathbb{Z}.$$

$$\| v_K \|_2^2 = \| B \cdot \begin{pmatrix} \lambda_1 \\ | \\ \lambda_n \end{pmatrix} \|_2^2 = \| B^* \underbrace{\begin{pmatrix} 1 & & \mu \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ | \\ \lambda_n \end{pmatrix}}_{\text{orthogonal}} \|_2^2 = \| B^* \begin{pmatrix} y_1 \\ | \\ y_{n-1} \\ \lambda_n \end{pmatrix} \|_2^2 =$$

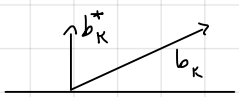
$$= \sum_{i=1}^{n-1} (y_i)^2 \| b_i^* \|_2^2 + \underbrace{\lambda_n^2}_{\geq 1} \| b_n^* \|_2^2 \geq \| b_n^* \|_2^2.$$

5. Let $B \in \mathbb{R}^{n\times n}$ be a regular matrix and let $\Lambda := \Lambda(B)$ be the lattice spanned by B. The *orthogonality defect* of the basis B is given by

$$\gamma(B) := \frac{\prod_{i=1}^{n} \|b_i\|_2}{\prod_{i=1}^{n} \|b_i^*\|_2}.$$

Let $v \in \Lambda(B) \setminus \{0\}$ be a shortest vector of Λ w.r.t. the ℓ_2-norm. Show that one has

$$v = Bx,\ x \in \mathbb{Z}^n \text{ with } \|x\|_\infty \leqslant \gamma(B).$$



$\longrightarrow$ So $\|b_K^*\| \leq \|b_K\|$ $\Rightarrow$ $\|b_i^*\| \cdot \gamma(B) = \dfrac{\prod_{K=1}^{n} \|b_K\|}{\prod_{K=1, K\neq i}^{n} \|b_K^*\|} \geq \|b_i\|$.

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

we can suppose is the n-th up to swap columns

Therefore if $v = Bx$ $x \in \mathbb{Z}^n$ $\forall$ s.t. $x_n \neq 0$, we have:

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

↑ 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.

Integer Optimization
Problem Set 4

March 11, 2024

1) Let $A \in \mathbb{R}^{n\times n}$ be a non-singular matrix. Show that the Gram-Schmidt orthogonalization is unique, i.e., show that there exists only one factorization

$$A = Q \cdot R$$

with $Q \in \mathbb{R}^{n\times n}$ having pairwise orthogonal columns and and $R \in \mathbb{R}^{n\times n}$ being upper triangular with all diagonal elements being 1.

2) Consider the integer matrix

$$A = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 10 \end{pmatrix}$$

and its Gram-Schmidt orthogonalization

$$A = \begin{pmatrix} 1 & \frac{12}{7} & \frac{1}{6} \\ 2 & \frac{3}{7} & -\frac{1}{3} \\ 3 & -\frac{6}{7} & \frac{1}{6} \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{16}{7} & \frac{53}{14} \\ 0 & 1 & \frac{16}{9} \\ 0 & 0 & 1 \end{pmatrix}$$

i) What is the matrix in $\mathbb{Z}^{3\times 3}$ that is the result of the *normalization step* of the LLL-algorithm?

ii) Is this result LLL-reduced? If not, which columns should be swapped?

iii) Carry on LLL-reduction with your favorite computer algebra system.

I have created this example with sage. It is slightly annoying that Gram-Schmidt is row-wise instead of column-wise. All matrices need to be transposed. You can find the code in the Github-Repository `https://github.com/EisenIn/IntegerOptimization` *under the directory* `Sage/Exercises-2024/Exercise-04`

3) Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of dimension $k \leqslant n$. In this exercise, you are to construct a orthogonal matrix $U \in \mathbb{R}^{n\times n}$ ($U^T \cdot U = I_n$) such that the first $n-k$ components of $U \cdot v$ are zero, for each $v \in \Lambda$. This means that we can identify Λ as a full-dimensional lattice in $\mathbb{R}^k$ when it comes to ℓ_2-related problems.

i) Explain how to use Gram-Schmidt orthogonalization to find an orthonormal basis $v_1, \ldots, v_{n-k} \in \mathbb{R}^n$ of the orthogonal complement of Λ.

ii) Let $b_1, \ldots, b_k$ be a basis of Λ. Explain how Gram-Schmidt on $v_1, \ldots, v_{n-k}, b_1, \ldots, b_k$ (in this order and with normalization) constructs a orthogonal matrix $U \in \mathbb{R}^{n\times n}$ that rotates v_i into e_i respectively, for $i = 1, \ldots, n-k$.

iii) Show that the image of $\{U \cdot v \colon v \in \Lambda\}$ is a k-dimensional lattice such that the first $n-k$ components of each lattice vector are zero.

iv) Let $\Lambda' \subseteq \mathbb{R}^k$ be the lattice that is obtained from $\{Uv \colon v \in \Lambda\}$ after deleting the first $n-k$ components. Show that Λ' is full-dimensional and that $\det(\Lambda') = \det(\Lambda)$ holds.

4) Let $\Lambda \subseteq \mathbb{R}^n$ be a full-dimensional lattice. In this exercise, we will prove that Λ has a basis $B \in \mathbb{R}^{n \times n}$ that is reduced in the following sense:

$$\prod_i^n \|b_i\| \leqslant 2^{n(n-1)/2} |\det(B)|.$$

We refer to the notation used in Exercise 1) of Problem Set 2, i.e., let $v \in \Lambda \setminus \{0\}$ be a shortest vector of Λ and Λ' the projection of Λ into the orthogonal complement of v.

i) Show that $\dim(\Lambda') = n-1$.

ii) Moreover

$$\det(\Lambda') = \det(\Lambda)/\|v\|.$$

iii) Let $b'_1, \ldots, b'_{n-1}$ be a basis of Λ'. One has

$$\|b'_i\|^2 + (1/4)\|v\|^2 \geqslant \|v\|^2$$

and therefore

$$\|b'_i\| \geqslant \sqrt{3/4}\|v\| \geqslant 1/2\|v\|.$$

Hint: Pythagoras!

iv) Show that there exists a basis $\{v, b_1, \ldots, b_n\}$ of Λ such that

$$b_i = b'_i + \lambda_i v,\ i = 1, \ldots, n-1,$$

where $|\lambda_i| \leqslant 1/2$ for each i and therefore each b_i satisfies

$$\|b_i\| \leqslant 2\|b'_i\|,\ i = 1, \ldots, n-1.$$

v) Using induction on the dimension of the lattice, we assume the inequality

$$\begin{aligned} \prod_{i=1}^{n-1} \|b'_i\| &\leqslant 2^{(n-1)(n-2)/2} \det(\Lambda') \\ &= 2^{(n-1)(n-2)/2} \det(\Lambda)/\|v\|. \end{aligned}$$

Conclude

$$\prod_i^n \|b_i\| \leqslant 2^{n(n-1)/2} |\det(B)|.$$

1) Let $A \in \mathbb{R}^{n\times n}$ be a non-singular matrix. Show that the Gram-Schmidt orthogonalization is unique, i.e., show that there exists only one factorization

$$A = Q \cdot R$$

with $Q \in \mathbb{R}^{n\times n}$ having pairwise orthogonal columns and and $R \in \mathbb{R}^{n\times n}$ being upper triangular with all diagonal elements being 1.

Suppose $A = Q_1 R_1 = Q_2 R_2$. So: $Q_2^{-1} Q_1 = R_2 R_1^{-1}$. Now inverse and product of upper triangular with all diagonal element being 1 is upper triangular with all diagonal element being 1 too. So:

$$R_2 R_1^{-1} = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

In particular, $Q_1 = Q_2 R_2 R_1^{-1}$:

$$(Q_1)^1 = Q_1 e_1 = Q_2 R_2 R_1^{-1} e_1 = (Q_2)^1 \quad \text{(they have the same column)}$$

$$(Q_1)^2 = Q_1 e_2 = Q_2 R_2 R_1^{-1} e_2 = Q_2 \begin{pmatrix} y_1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = y_1 (Q_2)^1 + (Q_2)^2 = y_1 (Q_1)^1 + (Q_2)^2$$

But $0 = \langle (Q_1)^1, (Q_1)^2 \rangle = \langle (Q_1)^1, y(Q_1)^1 + (Q_2)^2 \rangle = y \langle (Q_1)^1, (Q_1)^1 \rangle +$

$$+ \underbrace{\langle (Q_1)^1, (Q_2)^2 \rangle}_{\langle (Q_2)^1, (Q_2)^2 \rangle = 0} \Rightarrow y \, \|(Q_1)^1\|_2^2 = 0 \Rightarrow y = 0$$

By induction we conclude.

2) Consider the integer matrix

$$A = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 10 \end{pmatrix}$$

and its Gram-Schmidt orthogonalization $A = \overbrace{\begin{pmatrix} 1 & \frac{12}{7} & \frac{1}{6} \\ 2 & \frac{3}{7} & -\frac{1}{3} \\ 3 & -\frac{6}{7} & \frac{1}{6} \end{pmatrix}}^{B^*} \cdot \overbrace{\begin{pmatrix} 1 & \frac{16}{7} & \frac{53}{14} \\ 0 & 1 & \frac{16}{9} \\ 0 & 0 & 1 \end{pmatrix}}^{C}$

i) What is the matrix in $\mathbb{Z}^{3\times 3}$ that is the result of the *normalization step* of the LLL-algorithm?

ii) Is this result LLL-reduced? If not, which columns should be swapped?

iii) Carry on LLL-reduction with your favorite computer algebra system.

I have created this example with sage. It is slightly annoying that Gram-Schmidt is row-wise instead of column-wise. All matrices need to be transposed. You can find the code in the Github-Repository `https://github.com/EisenIn/IntegerOptimization` *under the directory* `Sage/Exercises-2024/Exercise-04`

i)

$$\begin{pmatrix} 1 & \frac{16}{7} & \frac{53}{14} \\ 0 & 1 & \frac{16}{9} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{\sim} \begin{pmatrix} 1 & \frac{16}{7} & \frac{21}{14} \\ 0 & 1 & -\frac{2}{9} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{\sim} \begin{pmatrix} 1 & -\frac{2}{7} & \frac{21}{14} \\ 0 & 1 & -\frac{2}{9} \\ 0 & 0 & 1 \end{pmatrix}$$

$\times 2$ $-$ $\times 2$ $-$ $-$

$$\rightsquigarrow \begin{pmatrix} 1 & -\frac{2}{7} & \frac{1}{2} \\ 0 & 1 & -\frac{2}{3} \\ 0 & 0 & 1 \end{pmatrix}$$

Hence:

$A = B \cdot C \quad \Rightarrow \quad AU = B^* \cdot CU$ where U is the matrix of "moves" i do:

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

In general, if I do $A^i + \alpha A^j$ I have to put in (j,i) α.

So:

$$A' = AU = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 10 \end{pmatrix} \begin{pmatrix} 1 & -2 & -1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -2 \\ 2 & 1 & -4 \\ 3 & 0 & -5 \end{pmatrix}$$

(ii) $b_1^* = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ $\quad \|b_1^*\|^2 = 14$ $\quad b_2^* = \begin{pmatrix} \frac{12}{7} \\ \frac{3}{7} \\ \frac{-6}{7} \end{pmatrix}$ $\quad \|b_2^*\|^2 = \frac{189}{49} = \frac{27}{7}$

$b_3^* = \begin{pmatrix} \frac{1}{6} \\ -\frac{1}{3} \\ \frac{1}{6} \end{pmatrix}$ $\quad \|b_3^*\|^2 = \frac{1}{6}$

$\|b_1^*\|^2 \leq 2\|b_2^*\|^2$? No, so I have to swap column 1 and 2.

$$A_{NEW} = \begin{pmatrix} 2 & 1 & -2 \\ 1 & 2 & -4 \\ 0 & 3 & -5 \end{pmatrix} =$$

3) Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of dimension $k \leqslant n$. In this exercise, you are to construct a orthogonal matrix $U \in \mathbb{R}^{n \times n}$ ($U^T \cdot U = I_n$) such that the first $n-k$ components of $U \cdot v$ are zero, for each $v \in \Lambda$. This means that we can identify Λ as a full-dimensional lattice in $\mathbb{R}^k$ when it comes to ℓ_2-related problems.

i) Explain how to use Gram-Schmidt orthogonalization to find an orthonormal basis $v_1, \ldots, v_{n-k} \in \mathbb{R}^n$ of the orthogonal complement of Λ.

ii) Let $b_1, \ldots, b_k$ be a basis of Λ. Explain how Gram-Schmidt on $v_1, \ldots, v_{n-k}, b_1, \ldots, b_k$ (in this order and with normalization) constructs a orthogonal matrix $U \in \mathbb{R}^{n \times n}$ that rotates v_i into e_i respectively, for $i = 1, \ldots, n-k$.

iii) Show that the image of $\{U \cdot v \colon v \in \Lambda\}$ is a k-dimensional lattice such that the first $n-k$ components of each lattice vector are zero.

iv) Let $\Lambda' \subseteq \mathbb{R}^k$ be the lattice that is obtained from $\{Uv \colon v \in \Lambda\}$ after deleting the first $n-k$ components. Show that Λ' is full-dimensional and that $\det(\Lambda') = \det(\Lambda)$ holds.

(3) (i) If $b_1, \dots, b_K$ is a basis of Λ. We know $\mathbb{R}^n = \text{Span}\{b_1, \dots, b_K\} \oplus \text{Span}\{b_1, \dots, b_K\}^\perp$.

So I take a basis of $\text{Span}\{b_1, \dots, b_n\}^\perp$ let's call it $\{\overline{v_1}, \dots, \overline{v_n}\}$. Now:

$$\begin{cases} v_1^* := \overline{v_1} \\ v_i^* = \overline{v_i} - \sum_{K=1}^{i-1} \frac{\langle \overline{v_i}, v_K \rangle}{\langle v_K, v_K \rangle} v_K \quad , \quad i = 2, \dots, n \end{cases}$$

Furthermore I have to normalize so I take $v_i := \frac{v_i^*}{\|v_i^*\|}$ $\forall i = 1, \dots, n$.

Since $\text{Span}\{v_1^*, \dots, v_i^*\} = \text{Span}\{\overline{v_1}, \dots, \overline{v_i}\}$ $\forall i = 1, \dots, n$ so $\text{Span}\{v_1, \dots, v_n\} = \text{Span}\{\overline{v_1}, \dots, \overline{v_n}\} =$

$= \text{Span}\{b_1, \dots, b_2\}^\perp$.

(ii) $v_1, \dots, v_{n-K}$ are already orthonormal so $v_i^* = v_i$ $\forall i = 1, \dots, n-K$.

Now, let $b_1^*, \dots, b_K^*$ the vectors obtained by GSO such that

$\{v_1, \dots, v_{n-K}, b_1^*, \dots, b_K^*\}$ is an orthonormal basis of $\mathbb{R}^n$.

Let U the matrix we are looking for. So, if such a matrix exists we have:

$$Uv_i = e_i \quad \forall i \in \{1, \dots, n-K\} \text{ and since } U \text{ has to be orthogonal}$$

$$v_i = U^T e_i = (U^T)^i \Rightarrow (U)_i = v_i \text{. So we can consider the matrix:}$$

$$U = \begin{pmatrix} \leftarrow v_1 \rightarrow \\ | \\ \leftarrow v_{n-K} \rightarrow \\ \leftarrow b_1^* \rightarrow \\ | \\ \leftarrow b_K^* \rightarrow \end{pmatrix} \quad \text{(rows seen as row-vectors)}$$

; U is orthogonal because U^T has a orthonormal basis as columns and in fact:

$$Uv_i = \begin{pmatrix} \langle v_1, v_i \rangle \\ | \\ \langle v_i, v_i \rangle \\ | \\ \langle v_{n-K}, v_i \rangle \\ \langle b_1^*, v_i \rangle \\ | \\ \langle b_K^*, v_i \rangle \end{pmatrix} = \begin{pmatrix} 0 \\ | \\ 0 \\ \|v_i\|^2 \\ 0 \\ | \\ 0 \end{pmatrix} = e_i$$

(iii) Lattice: • subgroup: $Uv_1 - Uv_2 = U(\overset{\Lambda}{v_1 - v_2}) \in \mathcal{Y}$

• discrete: suppose $\forall \varepsilon > 0 \ \exists x_\varepsilon \in B(0, \varepsilon) \cap \mathcal{Y} \setminus \{0\}$. So:

$x_\varepsilon = Uv_\varepsilon$ with $v_\varepsilon \in \Lambda \Rightarrow v_\varepsilon = U^T x_\varepsilon$ but U^T is orthogonal

so $\|v_\varepsilon\|_2 = \|x_\varepsilon\|_2 \Rightarrow \forall \varepsilon > 0 \ B(0, \varepsilon) \cap \Lambda \setminus \{0\} \neq \emptyset \Rightarrow$ ↯.

Now, let's see the first $n-K$ components: $v = \sum_{i=1}^{K} b_i$:

$$U\left(\sum_{i=1}^{K} b_i\right) = \sum_{i=1}^{K} U b_i \overset{\text{def. } U}{=} \sum_{i=1}^{K} \begin{pmatrix} \langle v_1, b_i \rangle \\ \vdots \\ \langle v_{n-K}, b_i \rangle \\ * \\ \vdots \\ * \end{pmatrix} \overset{v_1,\dots,v_{n-K} \in \mathrm{Span}\{b_1,\dots,b_K\}^{\perp}}{=} \sum_{i=1}^{K} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ * \\ \vdots \\ * \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ * \\ \vdots \\ * \end{pmatrix} \Big\}^{n-K}$$

(iv) U is invertible, so send basis in basis, in particular the basis $\{v_1,\dots,v_{n-K}, b_1,\dots,b_K\}$ goes into $\left\{e_1,\dots,e_{n-K}, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ w_1 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ w_K \end{pmatrix}\right\}$. Since the first $n-K$ components of the last K vectors are zero $\Rightarrow$ $\mathrm{Span}\{w_1,\dots,w_K\} \simeq \mathbb{R}^K$ and so the lattice $\Lambda' \subseteq \mathbb{R}^K$ is full-dimension. (they are a basis of Λ' by def.)

And: $\det(\Lambda) = \sqrt{\det\left((b_1,\dots,b_K)^T (b_1,\dots,b_K)\right)}$ ($K \times K$) $= \sqrt{\det\left((b_1,\dots,b_K)^T U^T U (b_1,\dots,b_K)\right)}$ ($K \times n$, $n \times K$) $= \sqrt{\det\left(\left(\begin{pmatrix} 0 & -w_1 \\ & \\ 0 & -w_K \end{pmatrix}\begin{pmatrix} 0 & 0 \\ w_1 & \\ & w_K \end{pmatrix}\right)\right)} =$

$1 = \det(UU^T) = \det(U)\cdot\det(U^T)$

$$= \sqrt{\det\left(\begin{pmatrix} w_1 \\ \vdots \\ w_K \end{pmatrix}(w_1,\dots,w_K)\right)} = \det(\Lambda')$$

4) Let $\Lambda \subseteq \mathbb{R}^n$ be a full-dimensional lattice. In this exercise, we will prove that Λ has a basis $B \in \mathbb{R}^{n\times n}$ that is reduced in the following sense:

$$\prod_i^n \|b_i\| \leqslant 2^{n(n-1)/2} |\det(B)|.$$

We refer to the notation used in Exercise 1) of Problem Set 2, i.e., let $v \in \Lambda \setminus \{0\}$ be a shortest vector of Λ and Λ' the projection of Λ into the orthogonal complement of v.

i) Show that $\dim(\Lambda') = n-1$.

ii) Moreover

$$\det(\Lambda') = \det(\Lambda)/\|v\|.$$

iii) Let $b'_1,\dots,b'_{n-1}$ be a basis of Λ'. One has

$$\|b'_i\|^2 + (1/4)\|v\|^2 \geqslant \|v\|^2$$

and therefore

$$\|b'_i\| \geqslant \sqrt{3/4}\,\|v\| \geqslant 1/2\|v\|.$$

(obvious from the above disequality; $\sqrt{\frac{3}{4}} > \frac{1}{2}$)

Hint: Pythagoras!

iv) Show that there exists a basis $\{v, b_1,\dots,b_{n-1}\}$ of Λ such that

$$b_i = b'_i + \lambda_i v,\ i = 1,\dots,n-1,$$

where $|\lambda_i| \leqslant 1/2$ for each i and therefore each b_i satisfies

$$\|b_i\| \leqslant 2\|b'_i\|,\ i = 1,\dots,n-1.$$

(follows from the above inequality: $\|b_i\| = \|b'_i + \lambda_i v\| \leq \|b'_i\| + |\lambda_i|\|v\| \leq \|b'_i\| + \frac{1}{2}\|b_i\|$; Δ ineq.; $|\lambda_i| \leq \frac{1}{2}$; $\|v\| \leq \|b_i\|$)

v) Using induction on the dimension of the lattice, we assume the inequality

$$\prod_{i=1}^{n-1} \|b'_i\| \leqslant 2^{(n-1)(n-2)/2} \det(\Lambda') = 2^{(n-1)(n-2)/2} \det(\Lambda)/\|v\|.$$

Conclude

$$\prod_i^n \|b_i\| \leqslant 2^{n(n-1)/2} |\det(B)|.$$

(they are all the vectors of the basis (v too))

(i) For Exercise 1 sheet 2, we have that if $b'_1,\dots,b'_K$ is a basis of $\Lambda' \Rightarrow b_1,\dots,b_K, v$ is a basis of Λ. Since Λ has dimension $n \Rightarrow K = n-1 \Rightarrow \dim\Lambda' = n-1$.

(ii) Let $\{v, b_1, \dots, b_{n-1}\}$ be a base of Λ. We know $\{b_i - \mu_{i,v} v =: b_i'\}_{i=1,\dots,n-1}$ is a basis of Λ'. Now, if I do GSO's of $\{v, b_1, \dots, b_{n-1}\}$ we have:

$$\begin{cases} v^* = v \\ b_1^* = b_1 - \mu_{1,v} v = b_1' \\ b_j^* = b_j - \mu_{j,v} v - \sum_{i=1}^{j-1} \mu_{i,j} b_i^* = b_j' - \sum_{i=1}^{j-1} \mu_{ij} b_i^* \end{cases} \qquad \left(\mu_{ij} = \frac{\langle b_i, b_i^* \rangle}{\langle b_i^*, b_i^* \rangle}\right)$$

If I do GSO's of $\{b_1', \dots, b_K'\}$ as subspace of $v^\perp$ we have:

$$\begin{cases} b_1'^* = b_1' \\ b_j'^* = b_j' - \sum_{i=1}^{j-1} \mu_{ij}' b_i'^* \end{cases} \qquad \left(\mu_{ij} = \frac{\langle b_j', b_i'^* \rangle}{\langle b_i'^*, b_i'^* \rangle}\right)$$

So, by induction, we have $b_i^* = b_i'^*$ and $\mu_{ij} = \mu_{ij}'$.

In particular we know $\det(\Lambda) = \prod_{i=1}^{n-1} \|b_i^*\| \cdot \|v\|$. And:

$$\underbrace{(b_1', \dots, b_{n-1}')}_{n \times n-1} = \underbrace{(b_1'^*, \dots, b_{n-1}'^*)}_{n \times n-1} \underbrace{\begin{pmatrix} 1 & & \mu_{ij}' \\ & \ddots & \\ 0 & & 1 \end{pmatrix}}_{n-1 \times n-1} = (b_1^*, \dots, b_{n-1}^*) \begin{pmatrix} 1 & & \mu_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

And so:

$$\det(\Lambda') = \sqrt{\det\left((b_1', \dots, b_{n-1}')^T (b_1', \dots, b_{n-1}')\right)} =$$

$$= \sqrt{\det\left(\underbrace{\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ \mu_{ij} & & 1 \end{pmatrix}}_{n-1 \times n-1} \underbrace{\begin{pmatrix} b_1^{*T} \\ \vdots \\ b_{n-1}^{*T} \end{pmatrix}}_{n-1 \times n} \underbrace{(b_1^*, \dots, b_{n-1}^*)}_{n \times n-1} \underbrace{\begin{pmatrix} 1 & & \mu_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}}_{n-1 \times n-1}\right)} =$$

$$= \sqrt{1 \cdot \prod_{i=1}^{n-1} \|b_i^*\|^2 \cdot 1} = \prod_{i=1}^{n-1} \|b_i^*\|$$

Binet since they are all $n-1 \times n-1$

(iii) We know that $\forall b_i'$ $\exists b_i$ s.t. $b_i' = b_i - \lambda_i v$ with $b_i \in \Lambda$. In particular $\Lambda \ni b_i - \lfloor \lambda_i \rfloor v =$

$= b_i' + \lambda_i v - \lfloor \lambda_i \rfloor v = b_i' + \{\lambda_i\} v$ with $|\{\lambda_i\}| \le \frac{1}{2}$. Now:

$$\|b_i'\| + \frac{1}{4}\|v\|^2 \ge \|b_i'\| + \{\lambda_i\}^2 \|v\|^2 = \|b_i' + \{\lambda_i\} v\|^2 \ge \|v\|$$

$\uparrow$ $|\{\lambda_i\}| \le \frac{1}{2}$ — $\uparrow$ Pyt. — $\uparrow$ $b_i' + \{\lambda_i\} v \in \Lambda$ and v is the s.v.

(iv) We know that exists a basis of the form $\{v, b_1, \dots, b_n\}$ where $b_i' = b_i - \lambda_i v \ \forall i$.

Now if $\exists i$ s.t. $|\lambda_i| > \frac{1}{2}$ I substitute b_i with $b_i - \lfloor \lambda_i \rceil v$.

Now $\{v, b_1 - \lfloor \lambda_1 \rceil v, \dots, b_n - \lfloor \lambda_n \rceil v\}$ is still a basis and:

$$b_i - \lfloor \lambda_i \rceil v = b_i' + \lambda_i v - \lfloor \lambda_i \rceil v = b_i' + (\lambda_i - \lfloor \lambda_i \rceil) v \quad \text{with} \quad |\lambda_i - \lfloor \lambda_i \rceil| \leq \frac{1}{2}.$$

(v) $$\prod_{i=1}^{n} \|b_i\| = \|v\| \cdot \prod_{i=1}^{n-1} \|b_i\| \underset{(iv)}{\leq} \|v\| \, 2^{n-1} \prod_{i=1}^{n-1} \|b_i'\| \underset{hp}{\leq} \|v\| \cdot 2^{n-1} \cdot 2^{(n-1)(n-2)/2} \frac{\det(\Lambda)}{\|v\|} =$$

$$= 2^{(n-1)(2+n-2)} \det(\Lambda) = 2^{(n-1)n} \det(\Lambda)$$

Integer Optimization
Problem Set 5

March 18, 2024

1. Using Minkowski's theorem, show that for prime $p \equiv 1 \pmod 4$, we can always find some $a, b \in \mathbb{Z}$, such that $p = a^2 + b^2$. Explain how to use the LLL algorithm to find the numbers a, b that satisfy $p = a^2 + b^2$.

2. Let GapSVP$_\gamma$ be defined as the following problem: given a basis B and a positive real d, determine if $\lambda_1(\Lambda(B)) \leqslant d$ or $\lambda_1(\Lambda(B)) > \gamma \cdot d$.
Show that the problem of approximating $\lambda_1(\Lambda(B))$ within a factor γ can be efficiently reduced to GapSVP$_\gamma$.

3. The Hermite factor of an n-dimensional lattice Λ is the quantity $\gamma(\Lambda) = \left(\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{1/n}}\right)^2$. The Hermite constant in dimension n is the supremum $\gamma_n = \sup_\Lambda \gamma(\Lambda)$, where Λ ranges over all n-dimensional lattices.

   (a) Show that $\gamma_n \leqslant n$ for every n.
   (b) Find a lattice $\Lambda \subset \mathbb{R}^2$ such that $\gamma(\Lambda) = 2/\sqrt{3}$.
   (c) For any lattice Λ, $(\prod_{i=1}^n \lambda_i)^{1/n} \leqslant \sqrt{\gamma}_n \cdot \det(\Lambda)^{1/n}$.
   (d) Prove that any lattice achieving Hermite's constant γ_n must have $\lambda_1 = \lambda_2 = \ldots = \lambda_n$.

4. For the LLL algorithm on a basis A, we discussed the potential function

$$\phi(A) := \|b_1^*\|^{2n} \|b_2^*\|^{2(n-1)} \ldots \|b_n^*\|^2.$$

   Let $A_i = (b_1, \ldots, b_i)$ be the truncated matrix with the first i column vectors of A. Show that

$$\phi(A) = \prod_{i=1}^n \det(A_i^T A_i).$$

5. Find a basis $b_1, \ldots, b_n$ such that after we apply one reduction step of the LLL algorithm to it, the maximum length of a vector in it increases (even by as much as $\Omega(\sqrt{n})$).

6. Let $R \in \mathbb{R}^{n \times n}$ be an upper triangular matrix with all diagonal elements equal to 1. Show that the number of vectors

$$Rx,\ x \in \mathbb{Z}^m,\ \|Rx\|_\infty \leqslant M$$

   is bounded by $(2M+1)^n$.

1. Using Minkowski's theorem, show that for prime $p \equiv 1 \pmod 4$, we can always find some $a, b \in \mathbb{Z}$, such that $p = a^2 + b^2$. Explain how to use the LLL algorithm to find the numbers a, b that satisfy $p = a^2 + b^2$.

$p \equiv 1 \ (4) \Rightarrow \exists\, a \in \mathbb{Z}$ s.t. $p \mid a^2 + 1$. We define the lattice

$\Lambda = \left\{ m \begin{pmatrix} a \\ 1 \end{pmatrix} + n \begin{pmatrix} p \\ 0 \end{pmatrix} \mid m, n \in \mathbb{Z} \right\} \subseteq \mathbb{R}^2$. Now:

$$\det(\Lambda) = \left| \det \begin{pmatrix} a & p \\ 1 & 0 \end{pmatrix} \right| = p$$

We choose $C = \{ (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 < 2p \} \Rightarrow A(C) = 2p\pi > 2^2 \cdot p = 2^2 \det(\Lambda) \Rightarrow$

$\exists\, (x, y) \neq 0 \in C \cap \Lambda$; in particular:

$$(x, y) \in \Lambda \iff \exists\, m, n \in \mathbb{Z} : \quad (x, y) = m(a, 1) + n(p, 0) = (ma + np, m)$$

$$\Rightarrow x^2 + y^2 = m^2 a^2 + n^2 p^2 + 2mnp + m^2 = m^2(a^2 + 1) + 2mnp + n^2 p^2 = 0 \pmod p.$$

So, $\exists K \in \mathbb{Z}$ s.t. $x^2 + y^2 = Kp$. But $(x, y) \in C \Rightarrow x^2 + y^2 < 2p$ and is also positive

$\Rightarrow K = 1 \Rightarrow x^2 + y^2 = p$.

2. Let GapSVP_γ be defined as the following problem: given a basis B and a positive real d, determine if $\lambda_1(\Lambda(B)) \leqslant d$ or $\lambda_1(\Lambda(B)) > \gamma \cdot d$.
Show that the problem of approximating $\lambda_1(\Lambda(B))$ within a factor γ can be efficiently reduced to GapSVP_γ.
↳ we want something in $[\lambda_1, \gamma\lambda_1)$ for every input

If $B = \{ b_1, \dots, b_n \}$, we have $\lambda_1(\Lambda(B)) \in \left(0, \min_{i=1,\dots,n} \|b_i\|_2 = : \xi \right)$.

So, if $\gamma \geq \xi$ we have finished. If $\gamma < \xi$ we start a bynary research in $(0, \xi)$: I choose as $d = \frac{\xi}{2}$; if $\lambda_1 \leq d = \frac{\xi}{2}$ we consider the interval $\left(0, \frac{\xi}{2}\right)$ and $d = \frac{\xi}{4}$; if $\lambda_1 > \gamma d = \gamma \frac{\xi}{2}$ we consider the interval $\left(\frac{\xi}{2}, \gamma \frac{\xi}{2} \right)$ and we have finished; if $d \leq \lambda_1 \leq \gamma d$ we have finished. And so on.

3. The Hermite factor of an n-dimensional lattice Λ is the quantity $\gamma(\Lambda) = \left(\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{1/n}}\right)^2$. The Hermite constant in dimension n is the supremum $\gamma_n = \sup_\Lambda \gamma(\Lambda)$, where Λ ranges over all n-dimensional lattices.

(a) Show that $\gamma_n \leqslant n$ for every n.

(b) Find a lattice $\Lambda \subset \mathbb{R}^2$ such that $\gamma(\Lambda) = 2/\sqrt{3}$.

(c) For any lattice Λ, $(\prod_{i=1}^n \lambda_i)^{1/n} \leqslant \sqrt{\gamma}_n \cdot \det(\Lambda)^{1/n}$.

(d) Prove that any lattice achieving Hermite's constant γ_n must have $\lambda_1 = \lambda_2 = \ldots = \lambda_n$.

(a) $\gamma(\Lambda) = \left(\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{\frac{1}{n}}}\right)^2 = \left(\frac{SV_2}{\det(\Lambda)^{\frac{1}{n}}}\right)^2 \leq \frac{n \cdot \det(\Lambda)^{\frac{2}{n}}}{\det(\Lambda)^{\frac{2}{n}}} = n \Rightarrow \gamma_n \leq n$.

$\lambda_1(\Lambda) = SV_2$ seen in class $SV_2 \leq \sqrt{n} \cdot \sqrt[n]{\det(\Lambda)}$

(b) $\gamma(\Lambda) = \frac{\lambda_1(\Lambda)^2}{\det(\Lambda)}$. $\Lambda = \left\{ \underbrace{\begin{pmatrix}1\\0\end{pmatrix}}_{b_1} x + \underbrace{\begin{pmatrix}1/2\\\sqrt{3}/2\end{pmatrix}}_{b_2} y \mid x, y \in \mathbb{Z} \right\}$.

Now, $\|b_2\| = \|b_1\|$. $b_2^* = \begin{pmatrix}\frac{1}{2}\\\frac{\sqrt{3}}{2}\end{pmatrix} - \frac{\left\langle \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1/2\\\sqrt{3}/2\end{pmatrix} \right\rangle}{\|b_1\|^2} \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{2} & -\frac{1}{2}\\\sqrt{3}/2 & 0\end{pmatrix} = \begin{pmatrix}0\\\frac{\sqrt{3}}{2}\end{pmatrix}$

$\|b_2^*\| = \frac{\sqrt{3}}{2} > \frac{1}{4} 1 \Rightarrow$ the shortest vector v :

$v = x_1 \begin{pmatrix}1\\0\end{pmatrix} + x_2 \begin{pmatrix}\frac{1}{2}\\\frac{\sqrt{3}}{2}\end{pmatrix}$, we know from theory that $|x_2| \leq 4$ and $|x_1| \leq 4$ so:

it's easy to compute that $v = \begin{pmatrix}1\\0\end{pmatrix}$. And so:

$$\gamma(\Lambda) = \frac{1^2}{1 \cdot \frac{\sqrt{3}}{2}} = \frac{2}{\sqrt{3}}$$

(c) Suppose $\{x_1, \ldots, x_n\}$ basis of the lattice s.t. $\|x_i\|_2 = \lambda_i$ (exists by definition of λ_i) $\forall i$. Suppose $\{x_1^*, \ldots, x_n^*\}$ the GSO. Now, if $T: \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is a linear function and Λ is a lattice $T(\Lambda)$ is a lattice. In particular if it is an isomorphism $T(\Lambda)$ has the same rank of Λ. So we set $T: \mathbb{R}^n \longrightarrow \mathbb{R}^n$ $T(x_i^*) = \frac{x_i^*}{\lambda_i}$. Now:

if $\{x_1, \ldots, x_n\}$ is a basis of $\Lambda \Rightarrow \{T(x_1), \ldots, T(x_n)\}$ is a basis of $T(\Lambda)$, since

$x_i^* = x_i - \sum_{j=1}^{i-1} \mu_{ij} x_j^* \Rightarrow x_i = x_i^* + \sum_{j=1}^{i-1} \mu_{ij} x_j^* \Rightarrow T(x_i) = \frac{x_i^*}{\lambda_i} + \sum_{j=1}^{i-1} \mu_{ij} \frac{x_j^*}{\lambda_j}$. Now:

$$\det(T(\Lambda)) = |\det(T(x_1), \ldots, T(x_n))| = \left|\det\left(\frac{x_1^*}{\lambda_1}, \ldots, x_n^* + \sum_{j=1}^{n-1} \mu_{ij} \frac{x_j^*}{\lambda_j}\right)\right| =$$

$$= \left|\det\left(\frac{x_1^*}{\lambda_1}, \frac{x_2^*}{\lambda_2}, \ldots, \frac{x_n^*}{\lambda_n}\right)\right| = \prod_{i=1}^n \frac{1}{\lambda_i} |\det(x_1^*, \ldots, x_n^*)| = \prod_{i=1}^n \frac{1}{\lambda_i} \det(\Lambda)$$

($\lambda_i > 0$)

So: $\sqrt{\gamma_n}\left(\frac{\det(\Lambda)}{\prod_{i=1}^{n}\lambda_i}\right)^{\frac{1}{n}} = \sqrt{\gamma_n}\,\det(T(\Lambda))^{\frac{1}{n}} \geq \frac{\lambda_1(T(\Lambda))}{\det(T(\Lambda))^{\frac{1}{n}}}\cdot \det(T(\Lambda))^{\frac{1}{n}} = \lambda_1(T(\Lambda))$.

$T(\Lambda)$ has full rank

Now, if we show that $\lambda_1(T(\Lambda)) \geq 1$, we have done.

Let $v \in T(\Lambda) \Rightarrow \exists w \in \Lambda$ s.t. $T(w) = v$, if $w = \sum_{i=1}^{n} c_i x_i^*$ (not integers!) $\Rightarrow v = \sum_{i=1}^{n} \frac{c_i}{\lambda_i} x_i^*$.

Let K be the largest index s.t. $c_K \neq 0$, so $w \in \text{Span}\{x_1^*, \dots, x_K^*\} = \text{Span}\{x_1, \dots, x_K\}$

$\Rightarrow$ by definition of λ_K, $\lambda_K \leq \|w\|_2$. So:

$$\|v\|_2^2 = \left\|\sum_{i=0}^{n} c_i \frac{x_i^*}{\lambda_i}\right\|_2^2 = \left\|\sum_{i=0}^{K} c_i \frac{x_i^*}{\lambda_i}\right\|_2^2 \overset{\text{Pyt.}}{=} \sum_{i=0}^{K} |c_i|^2 \frac{\|x_i^*\|^2}{|\lambda_i|^2} \geq \frac{1}{|\lambda_K|^2}\sum_{i=0}^{K} |c_i|^2 \|x_i^*\|^2 = \frac{1}{|\lambda_K|^2}\cdot\|w\|_2^2 \geq 1.$$

($|\lambda_K| > \dots > |\lambda_1| > 0$)

(d) $\lambda_1(\Lambda) \leq \left(\prod_{i=1}^{n}\lambda_i(\Lambda)\right)^{\frac{1}{n}} \leq \frac{\lambda_1(\Lambda)}{\det(\Lambda)^{\frac{1}{n}}}\cdot \det(\Lambda)^{\frac{1}{n}} = \lambda_1(\Lambda)$

definition: $\lambda_i \Rightarrow \lambda_1 \leq \lambda_i$

previous result

$$\Rightarrow \left(\prod_{i=1}^{n}\lambda_i(\Lambda)\right)^{\frac{1}{n}} = \lambda_1(\Lambda) \quad \text{but} \quad \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n \Rightarrow$$

$$\lambda_i(\Lambda) = \lambda_1(\Lambda) \quad \forall i = 1, \dots, n.$$

4. For the LLL algorithm on a basis A, we discussed the potential function

$$\phi(A) := \|b_1^*\|^{2n}\|b_2^*\|^{2(n-1)}\dots\|b_n^*\|^2.$$

Let $A_i = \underbrace{(b_1, \dots, b_i)}_{n \times i}$ be the truncated matrix with the first i column vectors of A. Show that

$$\phi(A) = \prod_{i=1}^{n} \det(A_i^T A_i).$$

$$\underbrace{A_i}_{n\times i} = \underbrace{(b_1, \dots, b_i, b_{i+1}, \dots, b_n)}_{n\times n}\underbrace{\begin{pmatrix} Id_{i\times i} \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{n\times i} = B\begin{pmatrix} Id_{i\times i} \\ 0 \end{pmatrix}$$

$$\Rightarrow A_i^T A_i = \begin{pmatrix} Id_{i\times i} & 0 \end{pmatrix} B^T B \begin{pmatrix} Id_{i\times i} \\ 0 \end{pmatrix} \quad \leftarrow B = B^* \begin{pmatrix} 1 & & \mu \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

$$= \overbrace{\begin{pmatrix} Id_{i\times i} & 0 \end{pmatrix}}^{i\times n}\overbrace{\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ \mu & & 1 \end{pmatrix}}^{n\times n} B^{*T} B^* \begin{pmatrix} 1 & & \mu \\ & \ddots & \\ 0 & & 1 \end{pmatrix}\begin{pmatrix} Id_{i\times i} \\ 0 \end{pmatrix} = \overbrace{\begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ & \ddots & & & \\ \mu & & 1 & 0 & \cdots & 0 \end{pmatrix}}^{i\times n} \overbrace{B^{*T}}^{n\times n} B^* \begin{pmatrix} 1 & & \mu \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = *$$

$\mu_{i\times i}$ $\quad 0_{i\times(n-i)}$

(block with first i columns)

So if $B^* = \begin{pmatrix} B^*_{n\times i} & B^*_{n\times(n-i)} \end{pmatrix}$ we have:

(block with first i columns)

$$* = \begin{pmatrix} \mu_{i\times i} & 0_{i\times(n-i)} \end{pmatrix} \begin{pmatrix} B^*_{i\times n} \\ B^*_{(n-i)\times n} \end{pmatrix} \begin{pmatrix} B^*_{n\times i} & B^*_{n\times(n-i)} \end{pmatrix} \begin{pmatrix} \mu_{i\times i} \\ 0_{(n-i)\times i} \end{pmatrix} =$$

$$= \begin{pmatrix} \underbrace{\mu_{i\times i} \cdot B^*_{i\times n}}_{i\times n} + 0_{i\times(n-i)} \cdot B^*_{(n-i)\times n} \end{pmatrix} \begin{pmatrix} B^*_{n\times i}\,\mu_{i\times i} + B^*_{n\times(n-i)} \cdot 0_{(n-i)\times i} \end{pmatrix} =$$

$$= \left(\mu_{i\times i} \cdot B^*_{i\times n}\right)\left(B^*_{n\times i}\,\mu_{i\times i}\right) = \mu_{i\times i}\left(B^*_{i\times n} \cdot B^*_{n\times i}\right)\mu_{i\times i}$$

$$\Rightarrow \det\left(A_i^T A_i\right) = \det\left(\mu_{i\times i}\right)\det\left(B^*_{i\times n} \cdot B^*_{n\times i}\right)\det\left(\mu_{i\times i}\right) = \prod_{j=1}^{i} \|b_j^*\|_2^2$$

(the two $\det(\mu_{i\times i})$ factors are $\det(I_{i\times i}) = 1$)

So $\prod_{i=1}^{n} \det\left(A_i^T A_i\right) = \prod_{i=1}^{n}\prod_{j=1}^{i} \|b_j^*\|_2^2 = \|b_1^*\|_2^{2n} \cdot \|b_2^*\|_2^{2(n-1)} \cdot \ldots \cdot \|b_{n-1}^*\|_2^4 \|b_n^*\|_2^2$.

5. Find a basis $b_1, \ldots, b_n$ such that after we apply one reduction step of the LLL algorithm to it, the maximum length of a vector in it increases (even by as much as $\Omega(\sqrt{n})$).

6. Let $R \in \mathbb{R}^{n\times n}$ be an upper triangular matrix with all diagonal elements equal to 1. Show that the number of vectors

$$Rx,\ x \in \mathbb{Z}^n,\ \|Rx\|_\infty \leqslant M$$

is bounded by $(2M+1)^n$.

$$\begin{pmatrix} 1 & & r_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 + \sum_{i=2}^{n} r_{1i}\, x_i \\ \vdots \\ x_{n-1} + r_{n-1,n}\, x_n \\ x_n \end{pmatrix}$$

So
$$\begin{cases} \left| x_1 + \sum_{i=2}^{n} r_{1i}\, x_i \right| \leq M \\ \vdots \\ |x_{n-1} + r_{n-1,n} x_n| \leq M \\ |x_n| \leq M \longrightarrow x_n \in \{-M, \dots, M\} \Rightarrow \text{there are } 2M+1 \text{ possibilities for } x_n \end{cases}$$

I go up to $|x_{n-1} + r_{n-1} x_n| \leq M$. We have chosen x_n and so since

$x_{n-1} + r_{n-1} x_n \in \{-M, \dots, M\}$, $x_{n-1} \in \{-M - r_{n-1} x_n, \dots, M - r_{n-1} x_n\}$

$\Rightarrow$ there are $2M+1$ possibilities for x_{n-1} and so on $\Rightarrow$ there are $(2M+1)^n$ possibilities for x.

Integer Optimization
Problem Set 6

March 25, 2024

1. Show that for any lattice Λ, the packing radius of a lattice equals $\frac{1}{2}\lambda_1(\Lambda)$.
2. Show that for any lattice Λ, the covering radius is at least $\mu(\Lambda) \geqslant \frac{1}{2}\lambda_n(\Lambda)$.
3. Show that for any n-dimensional lattice Λ, the covering radius is at most $\mu(\Lambda) \leqslant \frac{\sqrt{n}}{2}\lambda_n(\Lambda)$. Show that for any n, there exists an n-dimensional lattice Λ such that $\mu(\Lambda) = \frac{\sqrt{n}}{2}\lambda_n(\Lambda)$.
4. Show that for any real $c > \frac{1}{2}$ and any integer $n \geqslant 1$, there exists an n- dimensional lattice Λ such that $\mu(\Lambda) = c\lambda_n(\Lambda)$. → per l'fs. 3 se $c > \frac{\sqrt{n}}{2} \Rightarrow \mu(\Lambda) > \frac{\sqrt{n}}{2}\lambda_n(\Lambda)$ che è assurdo
5. Prove that for any n-dimensional lattice Λ, the covering radius is at least $\mu(\Lambda) \geqslant (det(\Lambda)/V_n)^{1/n}$, where V_n is the volume of the unit ball in $\mathbb{R}^n$.
6. Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice and $v \in \Lambda$ be a lattice vector.
   (a) Prove that $\Lambda' = \Lambda \cup (\Lambda + \frac{v}{2})$ is also a lattice. In particular, if $\frac{v}{2}$ is at distance at least $\lambda_1(\Lambda)$ from Λ, then Λ' is a lattice with minimum distance $\lambda_1(\Lambda') = \lambda_1(\Lambda)$ and determinant $\det(\Lambda') = \det(\Lambda)/2$.
   (b) Prove that for any full rank lattice Λ there is a lattice $\Lambda' \supseteq \Lambda$ such that $\mu(\Lambda') \leqslant 2\lambda_1(\Lambda) = 2\lambda_1(\Lambda')$.
   (c) Prove that for any n, there exists an n-dimensional lattice Λ such that $\mu(\Lambda) \leqslant 1.5 \cdot \lambda_1(\Lambda)$.

1. Show that for any lattice Λ, the packing radius of a lattice equals $\frac{1}{2}\lambda_1(\Lambda)$.

$\rho(\Lambda)$ = packing radius. If $v \in \Lambda \setminus \{0\}$ s.t. $\|v\| = \lambda_1(\Lambda) \Rightarrow$ consider v, $2v$ ($v \in \Lambda$, $2v \in \Lambda$)

$\Rightarrow v + \frac{1}{2}v \in \overline{B\left(v, \lambda_1(\Lambda)\right)}$ $\left(\|v + \frac{1}{2}v - v\| = \|\frac{1}{2}v\| = \frac{1}{2}\|v\| = \frac{1}{2}\lambda_1(\Lambda)\right)$ and

$2v - \frac{1}{2}v \in \overline{B\left(2v, \lambda_1(\Lambda)\right)}$ but $v + \frac{1}{2}v = \frac{3}{2}v = 2v - \frac{1}{2}v \Rightarrow$

$\overline{B(v, \lambda_1(\Lambda)} \cap \overline{B(2v, \lambda_1(\Lambda))} \neq \emptyset \Rightarrow$ if $r \geq \frac{1}{2}\lambda_1(\Lambda)$ we have intersection for the open balls. So, $\rho(\Lambda) \leq \frac{1}{2}\lambda_1(\Lambda)$.

Now, If two open balls $B\left(v, \frac{1}{2}\lambda_1(\Lambda)\right) \cap B(w, \lambda_1(\Lambda))$ for $v, w \in \Lambda$ have intersection not empty, let $z \in B\left(v, \frac{1}{2}\lambda_1(\Lambda)\right) \cap B(w, \lambda_1(\Lambda))$

$\Rightarrow \|v - w\| < \frac{1}{2}\lambda_1(\Lambda) + \frac{1}{2}\lambda_1(\Lambda) = \lambda_1(\Lambda)$ but $v - w \in \Lambda$, $\lightning$.

2. Show that for any lattice Λ, the covering radius is at least $\mu(\Lambda) \geqslant \frac{1}{2}\lambda_n(\Lambda)$.

Assume by contradiction $\mu(\Lambda) < \frac{1}{2}\lambda_n(\Lambda) \Rightarrow \varepsilon := \frac{1}{2}\lambda_n(\Lambda) - \mu(\Lambda) > 0$. Now, we want to construct $v_1, \dots, v_n$ linearly independent vectors of Λ s.t. $\|v_i\| \leq 2\mu(\Lambda) + \varepsilon =$

$= \lambda_n(\Lambda) - 2\varepsilon + \varepsilon = \lambda_n(\Lambda) - \varepsilon < \lambda_n(\Lambda)$ $\forall i = 1, \dots, n$, and it would be an absurd by definition of $\lambda_n(\Lambda)$. Construct them by induction:

- $n = 1$: consider a vector w s.t. $\|w\| = \mu + \varepsilon \Rightarrow$ by definition of $\mu(\Lambda)$ $\exists\, v \in \Lambda$ s.t. $\|v - w\| \leq \mu(\Lambda) \Rightarrow \|v\| = \|(v - w) + w\| \leq \|v - w\| + \|w\| \leq \mu(\Lambda) + \mu(\Lambda) + \varepsilon =$ $= 2\mu(\Lambda) + \varepsilon$;
- $n - 1 \longrightarrow n$: let $v_1, \dots, v_{n-1}$ given by induction hypothesis. Let $w \in \mathbb{R}^n$ a vector orthogonal to $v_1, \dots, v_{n-1}$ s.t. $\|w\| = \mu + \varepsilon$. By definition of $\mu(\Lambda)$ $\exists\, v_n \in \Lambda$ s.t. $\|v_n - w\| \leq \mu(\Lambda) \Rightarrow \|v_n\| = \|(v_n - w) + w\| \leq \|v_n - w\| + \|w\| = \mu(\Lambda) + \mu(\Lambda) + \varepsilon = 2\mu + \varepsilon$.

If $v_n \in \operatorname{Span}\{v_1, \dots, v_{n-1}\} \Rightarrow v_n = \sum_{i=1}^{n-1} \alpha_i v_i \Rightarrow \|w - v_n\| = \left\|w - \sum_{i=1}^{n-1} \alpha_i v_i\right\| =$

$= \sqrt{\langle w - \sum_{i=1}^{n-1} \alpha_i v_i \rangle + \langle w, -\sum_{i=1}^{n-1} \alpha_i v_i \rangle} = \sqrt{\|w\|^2 + \sum_{i=1}^{n-1} \alpha_i^2 \|v_i\|^2} \geq \|w\| = \mu + \varepsilon$, absurd.

($w \perp v_i$)

So v_n is independent from $v_1, \dots, v_{n-1}$. By induction hypothesis $\|v_i\| \leq 2\mu + \varepsilon$ $\forall i = 1, \dots, n-1$ as well.

3. Show that for any n-dimensional lattice Λ, the covering radius is at most $\mu(\Lambda) \leqslant \frac{\sqrt{n}}{2}\lambda_n(\Lambda)$. Show that for any n, there exists an n-dimensional lattice Λ such that $\mu(\Lambda) = \frac{\sqrt{n}}{2}\lambda_n(\Lambda)$.

- Consider a basis of Λ $b_1, \dots, b_n$ s.t. $\|b_i\| = \lambda_i \ \forall i = 1, \dots, n$. So for exercise in the lecture:

$$\mu(\Lambda) \leq \frac{1}{2}\sqrt{\sum_{i=1}^{n}\|b_i\|^2} \leq \frac{1}{2}\sqrt{n \cdot \lambda_n^2} = \frac{\sqrt{n}}{2}\lambda_n.$$

- Just consider $\mathbb{Z}^n$: we know $\mu(\mathbb{Z}^n) = \frac{1}{2}\sqrt{n}$ and $\lambda_n(\Lambda) = 1$ and so we get the equality

4. Show that for any real $c > \frac{1}{2}$ and any integer $n \geqslant 1$, there exists an n- dimensional lattice Λ such that $\mu(\Lambda) = c\lambda_n(\Lambda)$. $\quad \curvearrowright c \leq \frac{\sqrt{n}}{2}$

Consider the lattice generated by $b_1, \dots, b_n$ basis of $\mathbb{R}^n$ s.t. $\langle b_i, b_j \rangle = 0 \ i \neq j$. So,

$$\boxed{\mu(\Lambda) = \frac{1}{2}\sqrt{\sum_i \|b_i\|^2}}.$$ Proof:

Now we compute $\mu(\Lambda)$. Let $\sum_{i=1}^{n}\lambda_i b_i$ with $\lambda_i \in \mathbb{Z}$ a generic element in Λ. Let $x \in \mathbb{R}^n$ so $x = \sum_{i=1}^{n} k_i b_i$ with $k_i \in \mathbb{R}$. So:

$$d\left(\sum_{i=1}^{n} k_i b_i, \sum_{i=1}^{n}\lambda_i b_i\right)^2 = \left\|\sum_{i=1}^{n}(k_i - \lambda_i) b_i\right\|^2 \overset{\text{Pyt.}}{=} \sum_{i=1}^{n}|k_i - \lambda_i|^2\|b_i\|^2.$$

Hence, $\forall (k_1, \dots, k_n)$ we can consider $(\lfloor k_1 \rceil, \dots, \lfloor k_n \rceil)$ ($\lfloor k_i \rceil$ = nearest integer) $\Rightarrow \lambda_i := \lfloor k_i \rceil \Rightarrow$

$|k_i - \lambda_i| \leq \frac{1}{2} \Rightarrow \mu(\Lambda)^2 \leq \frac{1}{4}\sum_{i=1}^{n}\|b_i\|^2 \Rightarrow \mu(\Lambda) \leq \frac{1}{2}\sqrt{\sum_{i=1}^{n}\|b_i\|^2}$.

Since $\mu(\Lambda)$ is a max, to show that $\mu(\Lambda) \geq \frac{1}{2}\sqrt{\sum_{i=1}^{n}\|b_i\|^2}$ we just need $x = \sum_{i=1}^{n} k_i b_i \in \mathbb{R}^n$ s.t. $d(x, \Lambda) = \min_{(\lambda_1, \dots, \lambda_n) \in \mathbb{Z}} \sqrt{\sum_i |k_i - \lambda_i|^2\|b_i\|^2} \geq \frac{1}{2}\sqrt{\sum_{i=1}^{n}\|b_i\|^2}$. Take $k_i = \frac{1}{2}$ and so $\forall (\lambda_1, \dots, \lambda_n) \in \mathbb{Z}^n$ we have: $\sqrt{\sum_i |\frac{1}{2} - \lambda_i|^2\|b_i\|^2} \geq \frac{1}{2}\sqrt{\sum_{i=1}^{n}\|b_i\|^2}$.

$\uparrow$ since $|\frac{1}{2} - \lambda_i| \geq \frac{1}{2}$

So, given $c > \frac{1}{2}$ and $n \geq 1$, we can choose the basis for our lattice given by $(e_1, \dots, e_{n-1}, \beta e_n)$ with $\beta \geq 1$. So $\lambda_n(\Lambda) = \beta$ since in $B(0, \beta)$ we can only find elements of the lattice that are in $\text{Span}\{e_n\}^{\perp}$ and $\dim(\text{Span}\{e_n\}^{\perp}) = n-1$.

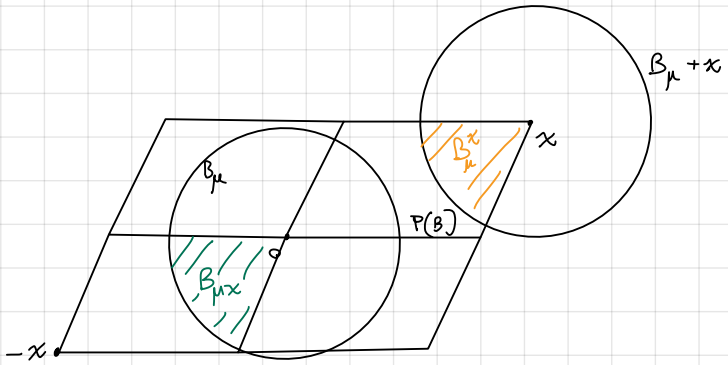
So I want $\frac{1}{2}\sqrt{n-1+\beta^2} = c\beta \iff \beta = \sqrt{\frac{n-1}{4c^2-1}}$ that makes sense iff $c > \frac{1}{2}$ and $\beta \geq 1$ iff $\frac{1}{2} < c \leq \frac{\sqrt{n}}{2}$ that is the hyp.

5. Prove that for any n-dimensional lattice Λ, the covering radius is at least $\mu(\Lambda) \geq (det(\Lambda)/V_n)^{1/n}$, where V_n is the volume of the unit ball in $\mathbb{R}^n$.

$\mu(\Lambda) \geq \left(\frac{\det(\Lambda)}{V_n}\right)^{\frac{1}{n}} \iff \underbrace{V_n \mu(\Lambda)^n}_{\text{Vol}(B_n(0, \mu(\Lambda)))} \geq \underbrace{\det(\Lambda)}_{\text{Vol}(P(B))}$. So we want to prove the last inequality. (if $\det(\Lambda) < 0$ it's obvious)

$B_n(0, \mu(\Lambda)) =: B_\mu$

Now we set $B_\mu^x := (B_\mu + x) \cap P$ with $x \in \Lambda$. We know that B_μ^x are a partition of B_μ. Also, $B_{\mu x} := B_\mu \cap (P - x)$ $\forall x \in \Lambda$. In particular we have $B_{\mu x} = B_\mu^x - x$ $\forall x \in \Lambda$.



$\forall y \in P(B)$ $\exists x \in \Lambda$ s.t. $y \in B_{\mu x}$ (μ is the covering radius) so:

$$P(B) \subseteq \bigcup_{x \in \Lambda} B_{\mu x} \Rightarrow \text{Vol}(P(B)) \leq \text{Vol}\left(\bigcup_{x \in \Lambda} B_{\mu x}\right) \leq \sum_{x \in \Lambda} \text{Vol}(B_{\mu x}) =$$

$$= \sum_{x \in \Lambda} \text{Vol}(B_\mu^x - x) = \sum_{x \in \Lambda} \text{Vol}(B_\mu^x) = \text{Vol}(B_\mu)$$

B_μ^x partition of B_μ

6. Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice and $v \in \Lambda$ be a lattice vector.

(a) Prove that $\Lambda' = \Lambda \cup (\Lambda + \frac{v}{2})$ is also a lattice. In particular, if $\frac{v}{2}$ is at distance at least $\lambda_1(\Lambda)$ from Λ, then Λ' is a lattice with minimum distance $\lambda_1(\Lambda') = \lambda_1(\Lambda)$ and determinant $\det(\Lambda') = \det(\Lambda)/2$.

(b) Prove that for any full rank lattice Λ there is a lattice $\Lambda' \supseteq \Lambda$ such that $\mu(\Lambda') \leqslant 2\lambda_1(\Lambda) = 2\lambda_1(\Lambda')$.

(c) Prove that for any n, there exists an n-dimensional lattice Λ such that $\mu(\Lambda) \leqslant 1.5 \cdot \lambda_1(\Lambda)$.

(2) 1. Λ' lattice: • subgroup: we have two types of elements in Λ': $x \in \Lambda$ or $y + \frac{v}{2}$ $y \in \Lambda$.

Now, if $x, y \in \Lambda \Rightarrow x - y \in \Lambda \subseteq \Lambda'$; if $x \in \Lambda$ and $y + \frac{v}{2} \in \Lambda \Rightarrow x - y - \frac{v}{2} =$

$= x - y - \frac{v}{2} + v - v = \underbrace{x - y - v}_{\in \Lambda} + \frac{v}{2} \in \Lambda + \frac{v}{2} \subseteq \Lambda'$; if $y + \frac{v}{2}, x + \frac{v}{2} \in \Lambda + \frac{v}{2} \Rightarrow$

$y + \frac{v}{2} - x - \frac{v}{2} = y - x \in \Lambda$.

- discrete: Let $\varepsilon > 0$ the radius s.t. $B(0,\varepsilon) \cap \Lambda = \{0\}$. Now $\Lambda + \frac{v}{2}$ is a discrete subset translated so is discrete (the distance between points of $\Lambda + \frac{v}{2}$ are the same of Λ and so in $\Lambda + \frac{v}{2}$ there are only isolated points). Finite union of discrete subgroup is discrete.

2 $\lambda_1(\Lambda') \leq \lambda_1(\Lambda)$ since $\Lambda \subseteq \Lambda'$. Now if $\lambda_1(\Lambda') < \lambda_1(\Lambda) \Rightarrow \exists \underbrace{x + \frac{v}{2}}_{\in \Lambda'} \in \Lambda$ s.t. $\| x + \frac{v}{2} \| < \| w \|$ where w is a $sv(\Lambda)$. But:

$$\| x + \frac{v}{2} \| = \| (x+v) - \frac{v}{2} \| = \text{dist}\left(\underset{\in \Lambda}{x+v}, \frac{v}{2} \right) \geq \text{dist}\left(\Lambda, \frac{v}{2} \right) \overset{\text{hp.}}{\geq} \| w \| \quad \lightning$$

3 Dalla dim. prec abbiamo mostrato che pi short. vector sono pi stessi (non possono essere della forma $x + \frac{v}{2}$) $\Rightarrow$ prendo w s.v di $\Lambda \in \Lambda'$ $\Rightarrow$ completo a base di Λ

$w, v_2, \dots, v_n \Rightarrow \frac{w}{2}, v_2, \dots, v_n$ base di $\Lambda' \Rightarrow \det\left(\frac{w}{2}, v_2, \dots, v_n\right) \leq \frac{1}{2} \det(w, v_2, \dots, v_n)$

(b)

Integer Optimization
Problem Set 7

April 8, 2024

1. Recall the transference bound that we showed in class:

$$\mu(\Lambda)\rho(\Lambda^*) \leqslant \frac{1}{4}\sqrt{\sum_{k=1}^{n} k^2} \leqslant \frac{n^{3/2}}{4}.$$

This bound only depends on the dimension. In this exercise, you will show a weaker bound which, nevertheless, is also only depending on the dimension n via the notion of LLL-reduction. Let $B = (b_1, \ldots, b_n) \in \mathbb{R}^{n\times n}$ be nonsingular and *LLL*-reduced with Gram-Schmidt orthogonalization $B = B^* \cdot R$ and let $\Lambda = \Lambda(B)$.

   (a) Show that $\frac{b_n^*}{\|b_n^*\|^2} \in \Lambda^*$

   (b) Use Exercise 3) from Problem set 6 and the LLL-reduction criterion to show that

$$\mu(\Lambda)\rho(\Lambda^*) \leqslant \sqrt{n} \cdot 2^{n-2}$$

2. An *ellipsoid* $\mathscr{E}$ is a set of the form

$$\mathscr{E} = \left\{x \in \mathbb{R}^n \colon \|A(x-t)\| \leqslant 1\right\}$$

where $A \in \mathbb{R}^{n\times n}$ is a non-singular matrix.

   (a) Show that $\mathscr{E}$ is the image of $B(0,1)$ under the map

$$\tau(x) = A^{-1}x + t$$

   (b) Show that, for any $d \in \mathbb{R}^n$, one has

$$\max_{x,y\in\mathscr{E}} d^T(x-y) = 2\|A^T d\|$$

   (c) Conclude the following: If $\mathscr{E} \cap \mathbb{Z}^n = \emptyset$, then there exists a $d \in \mathbb{Z}^n \setminus \{0\}$ such that

$$\max_{x,y\in\mathscr{E}} d^T(x-y) \leqslant n^{3/2}/2.$$

3. Show that there is a constant $c > 0$ such that the following algorithm, given a basis $B \in \mathbb{Z}^{m\times n}$ and a target vector $t \in \mathbb{Z}^m$, finds a lattice point $y \in \Lambda(B)$ where $\|y - t\| \leqslant 2^{cn} \cdot \operatorname{dist}(t, \Lambda(B))$:

   (a) Run the LLL-reduction algorithm on B to get an LLL-reduced basis B'.

   (b) Find $s = (s_1, \ldots, s_n) \in \mathbb{R}^n$ such that $B's = t$, say, by Gaussian Elimination.

   (c) Let $\hat{s} = (\lfloor s_1 \rceil, \ldots, \lfloor s_n \rceil)$ be the vector consisting of the entries of s rounded to the nearest integer.

(d) Output $y = B'\hat{s}$.

4. In this exercise, we want to show that SVP is not harder than CVP (Closest Vector Problem) in the sense that we can use an oracle for CVP to solve the SVP problem. We denote

$$\mathrm{CVP}(B', t) := \mathrm{argmin}\{\| x - t\|_2 : x \in \Lambda(B')\}.$$

Suppose that $B = (b_1, \ldots, b_n)$ is the input basis for our SVP problem. Show how an oracle that solves CVP can be used to solve SVP in polynomially many calls to the oracle.

5. Recall that for $X \subseteq \mathbb{R}^n$ the convex hull of X is

$$\mathrm{conv}(X) = \left\{ \sum_{i=1}^{t} \mu_i x_i : t \in \mathbb{N}_+, \mu_i \geqslant 0, x_i \in X, \sum_{i=1}^{t} \mu_i = 1 \right\}.$$

Show that, for $A, B \subseteq \mathbb{R}^n$, one has

$$\mathrm{conv}(A \cup B) = \mathrm{conv}(\mathrm{conv}(A) \cup \mathrm{conv}(B)).$$

1. Recall the transference bound that we showed in class:

$$\mu(\Lambda)\rho(\Lambda^*) \leqslant \frac{1}{4}\sqrt{\sum_{k=1}^{n} k^2} \leqslant \frac{n^{3/2}}{4}.$$

This bound only depends on the dimension. In this exercise, you will show a weaker bound which, nevertheless, is also only depending on the dimension n via the notion of LLL-reduction. Let $B = (b_1, \dots, b_n) \in \mathbb{R}^{n\times n}$ be nonsingular and *LLL*-reduced with Gram-Schmidt orthogonalization $B = B^* \cdot R$ and let $\Lambda = \Lambda(B)$.

~~(a)~~ Show that $\frac{b_n^*}{\|b_n^*\|^2} \in \Lambda^*$

(b) Use Exercise 3) from Problem set 6 and the LLL-reduction criterion to show that

$$\mu(\Lambda)\rho(\Lambda^*) \leqslant \sqrt{n}\cdot 2^{n-2}$$

(a) $\Lambda^* = \{ y \in \mathbb{R}^n : y^T v \in \mathbb{Z} \quad \forall v \in \Lambda \}$, so $\forall v \in \Lambda \ \exists \lambda \in \mathbb{Z}^n$ s.t. $v = B\lambda$:

$$\left(\frac{b_n^*}{\|b_n^*\|^2}\right)^T v = \left(\frac{b_n^*}{\|b_n^*\|^2}\right)^T B\lambda = \left(\frac{b_n^*}{\|b_n^*\|^2}\right)^T B^* R \lambda = (0, \dots, 0, 1) R \lambda = (0, \dots, 0, 1) \begin{pmatrix} * \\ \vdots \\ \lambda_n \end{pmatrix} = \lambda_n \in \mathbb{Z}$$

$\Downarrow$ $\quad\uparrow$

$\langle b_n^*, b_i^* \rangle = 0 \ \forall i < n \qquad R = \begin{pmatrix} 1 & & \mu_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

$\left\langle \frac{b_n^*}{\|b_n^*\|}, b_n^* \right\rangle = 1$

(b) From Ex. 3 Sheet 6 we know that:

$$\mu(\Lambda) \leq \frac{\sqrt{n}}{2}\lambda_n(\Lambda)$$

So we need to prove:

$$\rho(\Lambda^*) \leq \frac{2^{n-1}}{\lambda_n(\Lambda)}$$

$$\rho(\Lambda^*) = \frac{\lambda_1(\Lambda^*)}{2} \leq \frac{\left\| \frac{b_n^*}{\|b_n^*\|^2} \right\|}{2} = \frac{1}{2\|b_n^*\|} \leq \frac{2^{n-2}}{\|b_1\|}$$

$\uparrow \quad \frac{b_n^*}{\|b_n^*\|^2} \in \Lambda^*$ $\qquad$ LLL: $\begin{cases} 2\|b_n^*\| \geq \|b_{n-1}\|^* \\ \dots \\ 2\|b_2^*\| \geq \|b_1^*\| \end{cases}$ and $b_1^* = b_1$

Now: $b_n = B^* \begin{pmatrix} \mu_{1n} \\ \vdots \\ \mu_{n-1,n} \\ 1 \end{pmatrix} = \sum_{i=1}^{n-1} b_i^* \mu_{in} + b_n^* \Rightarrow \|b_n\|^2 = \sum_{i=1}^{n-1} |\mu_{in}|^2 \|b_i^*\|^2 + \|b_n^*\|^2 \leq$

$$\leq \frac{1}{4}\sum_{i=1}^{n-1}\|b_i^*\|^2 + \|b_n^*\|^2 \leq \frac{1}{4}\|b_n^*\|^2 \sum_{i=1}^{n-1} 2^{n-i} + \|b_n^*\| = \frac{1}{4}\|b_n^*\|^2 (2^n - 2) + \|b_n^*\|^2 =$$

$$= \|b_n^*\|^2 \left(2^{n-2} + \frac{1}{2}\right) \Rightarrow \|b_n\| \leq \|b_n^*\| \left(2^{n-2} + \frac{1}{2}\right)^{\frac{1}{2}}$$

$$\rho(\Lambda^*) \leq \frac{1}{2\|b_n^*\|} \leq \frac{\left(2^{n-2} + \frac{1}{2}\right)^{\frac{1}{2}}}{2\|b_n\|} \leq$$

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

2. An *ellipsoid* $\mathcal{E}$ is a set of the form

$$\mathcal{E} = \{x \in \mathbb{R}^n : \|A(x-t)\| \leqslant 1\}$$

where $A \in \mathbb{R}^{n\times n}$ is a non-singular matrix.

(a) Show that $\mathcal{E}$ is the image of $B(0,1)$ under the map

$$\tau(x) = A^{-1}x + t$$

(b) Show that, for any $d \in \mathbb{R}^n$, one has

$$\max_{x,y\in\mathcal{E}} d^T(x-y) = 2\|A^T d\|$$

(c) Conclude the following: If $\mathcal{E} \cap \mathbb{Z}^n = \emptyset$, then there exists a $d \in \mathbb{Z}^n \setminus \{0\}$ such that

$$\max_{x,y\in\mathcal{E}} d^T(x-y) \leqslant n^{3/2}.$$ (2.) ← I don't have it

(a) $x \in B(0,1)$: $\tau(x) = A^{-1}x + t \Rightarrow \|A((A^{-1}x+t)-t)\| = \|A(A^{-1}x)\| = \|x\| \leq 1$

(b) $\max_{x,y\in\mathcal{E}} d^T(x-y) = \max_{x\in\mathcal{E}} d^T x - \min_{x\in\mathcal{E}} d^T y = \max_{x\in B(0,1)} d^T(A^{-1}x+t) - \min_{x\in B(0,1)} d^T(A^{-1}x+t) =$

$= \max_{x\in B(0,1)} (d^T A^{-1})x + d^T t - \min_{x\in B(0,1)} (d^T A^{-1})x - d^T t =$

$= (d^T A^{-1})\frac{(d^T A^{-1})^T}{\|(d^T A^{-1})^T\|} - (d^T A^{-1})\left(-\frac{d^T A^{-1}}{\|(d^T A^{-1})^T\|}\right)^T = 2\|A^{-T}d\|$

$K^T x = \langle K, x\rangle = \|K\|\|x\|\cos\theta$ so it is maximized when $\cos\theta = 1$ $(+ x \in B(0,1)) \Rightarrow x = \frac{K}{\|K\|}$,

for the minimum $\cos\theta = -1 \Rightarrow x = -\frac{K}{\|K\|}$

(c) $\mathcal{E} \cap \mathbb{Z}^n = \emptyset \iff \tau(B(0,1)) \cap \mathbb{Z}^n = \emptyset \iff$ (· A) $B(At, 1) \cap A\mathbb{Z}^n = \emptyset$ ($A\mathbb{Z}^n = \Lambda(A)$)

$\Rightarrow$ by definition $\mu(\Lambda(A)) \geq 1$ but we know by transference theorem:

$$\mu(\Lambda(A))\,\rho(\Lambda^*(A)) \leq \frac{n^{\frac{3}{2}}}{4} \Rightarrow \rho(\Lambda^*(A)) \leq \frac{n^{\frac{3}{2}}}{4}$$

but $\Lambda^*(A) = \Lambda(A^{-T}) \Rightarrow \rho(\Lambda(A^{-T})) \leq \frac{n^{\frac{3}{2}}}{4}$, by def. of ρ $\exists\, x, y \in \Lambda(A^{-T})$ s.t. d

$$\max_{x,y\in\mathcal{E}} d^T(x-y) = 2\|A^{-T}d\| \overset{\uparrow}{=} 2\cdot 2\rho(\Lambda(A^{-T})) \leq n^{\frac{3}{2}}.$$

d s.t. $A^{-T}d$ is $sv(\Lambda(A^{-T}))$

4. In this exercise, we want to show that SVP is not harder than CVP (Closest Vector Problem) in the sense that we can use an oracle for CVP to solve the SVP problem. We denote

$$\mathrm{CVP}(B', t) := \mathrm{argmin}\{\| x - t\|_2 : x \in \Lambda(B')\}.$$

Suppose that $B = (b_1, \ldots, b_n)$ is the input basis for our SVP problem. Show how an oracle that solves CVP can be used to solve SVP in polynomially many calls to the oracle. (CVP is hard at least as SVP)

This is the algorithm:

(1) We define n lattices: $\Lambda(B^i)$ where $B^i = \{b_1, \ldots, b_{i-1}, 2b_i, b_{i+1}, \ldots, b_n\}$ $\forall i \in \{1, \ldots, n\}$.

(2) $v_i :=$ output of $\mathrm{CVP}(B^i, b_i)$

(3) $w := \mathrm{argmin}\{\| v_i - b_i \|, i = 1, \ldots, n\}$

In fact $w = v_i - b_i$ for some i and so $w = \sum_{\substack{j=1 \\ j \neq i}}^{n} z_i b_i + 2z_i b_i - b_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} z_i b_i + (2z_i - 1) b_i$

with $z_i \in \mathbb{Z}$ $\forall i$ and $2z_i - 1$ odd integer. So $w \in \Lambda \setminus \{0\}$. Prove that is the shortest.

Now, suppose $v \in \Lambda \setminus \{0\}$ is a $\mathrm{sv}(\Lambda)$, so $v = \sum_{j=1}^{n} k_j b_j$ with $k_j \in \mathbb{Z}$. In particular $\exists s$ s.t. $k_s = 2t - 1$ ($t \in \mathbb{Z}$) otherwise $\frac{v}{2} \in \Lambda$ and v would not be the shortest.

So $v = \sum_{\substack{j=1 \\ j \neq s}}^{n} k_j b_j + (2t - 1) b_s \Rightarrow$ the vector $u := \sum_{\substack{j=1 \\ j \neq s}}^{n} k_j b_j + 2t b_s \in B^s$ and so:

$$\|w\| = \| v_i - w_i \| \leq \| v_s - b_s \| \leq \| u - b_s \| = \Big\| \sum_{\substack{j=1 \\ j \neq s}}^{n} k_j b_j + (2t-1) b_s \Big\| = \|v\|$$

(i is the minimum; v_s output of $\mathrm{cvp}(B^s, b_s)$)

5. Recall that for $X \subseteq \mathbb{R}^n$ the convex hull of X is

$$\mathrm{conv}(X) = \left\{ \sum_{i=1}^{t} \mu_i x_i : t \in \mathbb{N}_+, \mu_i \geqslant 0, x_i \in X, \sum_{i=1}^{t} \mu_i = 1 \right\}.$$

Show that, for $A, B \subseteq \mathbb{R}^n$, one has

$$\mathrm{conv}(A \cup B) = \mathrm{conv}(\mathrm{conv}(A) \cup \mathrm{conv}(B)).$$

C Let $x \in \mathrm{conv}(A \cup B) \Rightarrow x = \sum_{i \in I} \mu_i x_i$ with $\mu_i \geq 0$ $\sum_{i \in I} \mu_i = 1$ and $x_i \in A$ or $x_i \in B$.

Define $I_A := \{i : x_i \in A\}$ $I_B := \{i : x_i \in B\}$. So:

$$x = \sum_{i \in I} \mu_i x_i = \sum_{i \in I_A} \mu_i x_i + \sum_{i \in I_B} \mu_i x_i = R_A \sum_{i \in I_A} \frac{\mu_i}{R_A} x_i + R_B \sum_{i \in I_B} \frac{\mu_i}{R_B} x_i =$$

($I_A \sqcup I_B = I$; $R_A := \sum_{i \in I_A} \mu_i$; $R_B = \sum_{i \in I_B} \mu_i$)

Now $\sum_{i \in I_A} \frac{\mu_i}{R_A} x_i \in \mathrm{conv}\, A$ $\left(\sum_{i \in I_A} \frac{\mu_i}{R_A} = \frac{R_A}{R_A} = 1 \right)$ and in the same way $\sum_{i \in I_B} \frac{\mu_i}{R_B} x_i \in \mathrm{conv}(B)$,

To finish, notice that $R_A + R_B = 1$ $(R_A, R_B \geq 0) \Rightarrow x \in \text{Conv}\left(\text{Conv}(A) \cup \text{Conv}(B)\right)$.

$\boxed{\supseteq}$ $x \in \text{conv}\left(\text{conv}(A) \cup \text{conv}(B)\right) \Rightarrow x = \sum_{i \in I} \mu_i x_i$ where $\mu_i \geq 0$, $\sum_{i \in I} \mu_i = 1$

and $x_i \in \text{conv}(A)$ or $x_i \in \text{conv}(B)$. If $x_i \in \text{conv}(A) \Rightarrow x_i = \sum_{j \in I_A^i} \lambda_{ij}^A a_{ij}$ where

$\sum_{j \in I_A^i} \lambda_{ij}^A = 1$, if $x \in \text{conv}(B) \Rightarrow x_i = \sum_{j \in I_B^i} \lambda_{ij}^B b_{ij}$ with $\sum_{j \in I_B^i} \lambda_{ij}^B = 1$. So:

$$x = \sum_{i \in I} \mu_i x_i = \sum_{i \in J_A} \mu_i \left(\sum_{j \in I_A^i} \lambda_{ij}^A a_{ij} \right) + \sum_{i \in J_B} \mu_i \left(\sum_{j \in I_B^i} \lambda_{ij}^B b_{ij} \right) =$$

$$J_A = \{ i : x_i \in \text{conv}(A) \}$$

$$J_B = \{ i : x_i \in \text{conv}(B) \}$$

$$= \sum_{i \in J_A} \sum_{j \in I_A^i} \mu_i \lambda_{ij}^A \underbrace{a_{ij}}_{\in A} + \sum_{i \in J_B} \sum_{j \in I_B^i} \mu_i \lambda_{ij}^B \underbrace{b_{ij}}_{\in B}$$

and $\sum_{i \in J_A} \sum_{j \in I_A^i} \mu_i \lambda_{ij}^A + \sum_{i \in J_B} \sum_{j \in I_B^i} \mu_i \lambda_{ij}^B = \sum_{i \in J_A} \mu_i \underbrace{\left(\sum_{j \in J_A^i} \lambda_{ij}^A \right)}_{=1} + \sum_{i \in J_B} \mu_i \underbrace{\left(\sum_{j \in J_B^i} \lambda_{ij}^B \right)}_{=1} =$

$= \sum_{i \in J_A} \mu_i + \sum_{i \in J_B} \mu_i = \sum_{i \in I} \mu_i = 1$. So $x \in \text{Conv}(A \cup B)$.

Integer Optimization
Problem Set 8

April 15, 2024

1. This exercise finishes the argument of the *heart of the proof* of John's theorem. Let

$$\mathscr{E} = \{x \in \mathbb{R}^n : \sum_{i=1}^{n} \frac{1}{\alpha_i^2}(x_i - t_i)^2 \leqslant 1\},$$

where $t = e_1$, $\alpha_1 = 2$, $\alpha_2 = \cdots = \alpha_n = \sqrt{n/\left(n + \frac{1}{10}\right)}$. Show the following. If $x^* \in \mathscr{E}$ and $x_1^* \leqslant 0$, then $\|x^*\|_2 \leqslant 1$.

2. Consider the *simplex* $\Sigma = \text{conv}\{e_1, \ldots, e_n\} \subseteq \mathbb{R}^n$. We interpret Σ as *full-dimensional* in the hyperplane

$$\sum_i x_i = 1.$$

   a) Determine the center and radius of the largest euclidean ball contained in Σ.

   ~~b) Show that this ball is the largest volume ellipsoid that is contained in Σ.~~

3. Consider the *simplex* $\Sigma = \text{conv}\{0, n \cdot e_1, \ldots, n \cdot e_n\} \subseteq \mathbb{R}^n$.

   a) Show that the *interior* of Σ does not contain an integer point. (I.e. all points in $\Sigma \cap \mathbb{Z}^n$ are on the boundary of Σ.)

   b) Show that $w(\Sigma) = n$, where $w(K)$ denotes the *lattice width* of K

$$w(K) = \min_{d \in \mathbb{Z}^n \setminus \{0\}} \max_{x,y \in K} d^T(x - y).$$

4. Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body. Show that there is an ellipsoid E (with the origin as center) so that $E \subseteq K \subseteq C\sqrt{n} \cdot E$ for some (large) constant $C > 0$.

5. Let $\|\cdot\|_*$ be any norm in $\mathbb{R}^n$. Show that there is a matrix A so that $\|Ax\|_2 \leqslant \|x\|_* \leqslant \sqrt{n}\,\|Ax\|_2$. Find a norm for which the factor $\sqrt{n}$ is tight.

1. This exercise finishes the argument of the *heart of the proof* of John's theorem. Let

$$\mathcal{E} = \{x \in \mathbb{R}^n : \sum_{i=1}^{n} \frac{1}{\alpha_i^2}(x_i - t_i)^2 \leqslant 1\},$$

where $t = e_1$, $\alpha_1 = 2$, $\alpha_2 = \cdots = \alpha_n = \sqrt{n/\left(n+\frac{1}{10}\right)}$. Show the following. If $x^* \in \mathcal{E}$ and $x_1^* \leqslant 0$, then $\|x^*\|_2 \leqslant 1$.

$\sum_{i=1}^{n} \frac{1}{\alpha_i^2}(x_i - t_i)^2 \leq 1 \Rightarrow \frac{1}{\alpha_i^2}(x_i - t_i)^2 \leq 1 \quad \forall i = 1, \dots, n \Rightarrow$

$\begin{cases} (x_1 - 1)^2 \leq 4 \iff -1 \leq x_1 \leq 3 \\ \frac{n+\frac{1}{10}}{n} x_i^2 \leq 1 \iff x_i^2 \leq \frac{n}{n+\frac{1}{10}} \quad \forall i = 2, \dots n \end{cases}$

$\sum_{i=1}^{n} \frac{1}{\alpha_i^2}(x_i - t_i)^2 = \frac{1}{\alpha_1^2}(x_1 - t_1)^2 + \sum_{i=2}^{n} \frac{1}{\alpha_i^2}(x_i - t_i)^2 = \frac{1}{4}(x_1 - 1)^2 + \frac{n+\frac{1}{10}}{n} \sum_{i=2}^{n} x_i^2 =$

$= \frac{1}{4}x_1^2 - \frac{x_1}{2} + \frac{1}{4} + \frac{n+\frac{1}{10}}{n} \sum_{i=2}^{n} x_i^2 =$

$= \frac{1}{4}x_1^2 - \frac{x_1}{2} + \frac{1}{4} + \sum_{i=2}^{n} x_i^2 + \frac{1}{10n} \sum_{i=2}^{n} x_i^2 + (x_1^2 - x_1^2) =$

$= \|x\|_2^2 - \frac{x_1}{2} + \frac{1}{4} + \frac{1}{10n} \sum_{i=2}^{n} x_i^2 - \frac{3}{4}x_1^2.$

If $-\frac{x_1}{2} + \frac{1}{4} + \frac{1}{10n} \sum_{i=2}^{n} x_i^2 - \frac{3}{4}x_1^2 \geq 0 \quad \forall -1 \leq x_1 \leq 0$ we would have:

$1 \geq \sum_{i=1}^{n} \frac{1}{\alpha_i^2}(x_i - t_i)^2 \geq \|x\|_2^2.$

But $-\frac{3}{4}x_1^2 - \frac{x_1}{2} + \frac{1}{10n} \sum_{i=1}^{n} x_i^2 + \frac{1}{4} \geq -\frac{3}{4}x_1^2 - \frac{x_1}{2} + \frac{1}{4} \geq 0$ ← I want this

$-\frac{3}{4}x_1^2 - \frac{x_1}{2} + \frac{1}{4} \geq 0 \iff -3x_1^2 - 2x_1 + 1 \geq 0 \qquad (x_1)_{1,2} = \frac{1 \pm \sqrt{1^2+3}}{-3} = \frac{1 \pm 2}{-3} \searrow -1 \;\nearrow \frac{1}{3}$

$\iff -1 \leq x_1 \leq \frac{1}{3}$. So for $-1 \leq x_1 \leq 0$ we have the inequality

2. Consider the *simplex* $\Sigma = \operatorname{conv}\{e_1, \dots, e_n\} \subseteq \mathbb{R}^n$. We interpret Σ as *full-dimensional* in the hyperplane

$$\sum_i x_i = 1.$$

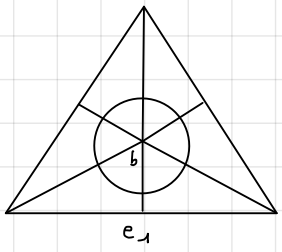
a) Determine the center and radius of the largest euclidean ball contained in Σ.

~~b)~~ Show that this ball is the largest volume ellipsoid that is contained in Σ. ← NOT IN THE EXAM

(2) We first prove that the largest euclidian ball contained in Σ is the inscribed one, i.e. the one which has the center in the barycenter and radius we compute after.

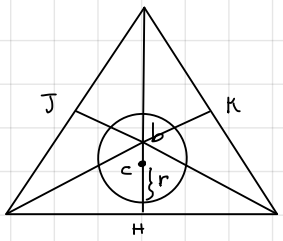
Infact, suppose there is a face of the simplex not touched by the sphere $B(c, r)$. WLOG the face is e_1. Now we can have:

1. The center of the ball is the barycenter: since the barycenter is equidistant from the face, the ball will not touch the others faces as well. So there is an $\varepsilon > 0$ s.t. $B(c, \varepsilon + r) \subseteq \Sigma$.

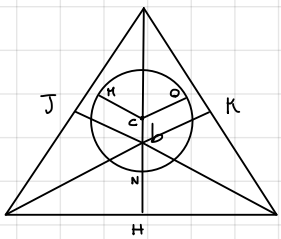


2. The center of the ball is along the median but $c \neq$ barycenter: we move the ball s.t. the center of the ball is the barycenter of the simplex. Now, if we prove that this ball does not touch e_1, e_2, e_3 (and is inside the simplex), we conclude as in point 1.

Now, if c is under b, it means that $r < \overline{bH}$, so when I move c up to b the ball is strictly contained in Σ since $\overline{bH} = \overline{bK} = \overline{bJ}$.



If c is over b the radius $\overline{cr}$, $\overline{co}$ and $\overline{cN}$ (the ones which are parallel with respect to the medians) are shorter than $\overline{bJ} = \overline{bK} = \overline{bH}$ and so when $c = b$ the sphere

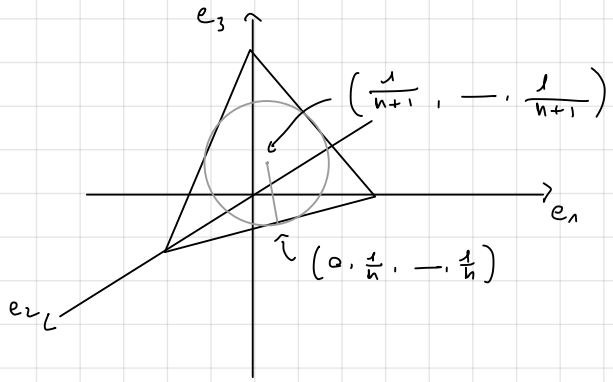


3. If the center is not on the median, we can always translate the sphere along the straight line parallel with respect to e_1 and passing through c.

This argument can be used in any dimension n.

So, the center is the baricenter of the simplex that is $\left(\frac{1}{n+1}, \dots, \frac{1}{n+1}\right)$.

For the radios: we just need to compute the distance between the center and the baricenter of an hyperface that is, for example $\left(0, \frac{1}{n}, \dots, \frac{1}{n}\right)$



So $r = \sqrt{\left(\frac{1}{n+1}\right)^2 + n\left(\frac{1}{n+1} - \frac{1}{n}\right)^2} = \sqrt{\left(\frac{1}{n+1}\right)^2 + n\left(\frac{n-n-1}{(n+1)n}\right)^2} = \sqrt{\frac{n+1}{(n+1)^2 n}} = \frac{1}{\sqrt{(n+1)n}}$

3. Consider the *simplex* $\Sigma = \text{conv}\{0, n \cdot e_1, \dots, n \cdot e_n\} \subseteq \mathbb{R}^n$.

   a) Show that the *interior* of Σ does not contain an integer point. (I.e. all points in $\Sigma \cap \mathbb{Z}^n$ are on the boundary of Σ.)

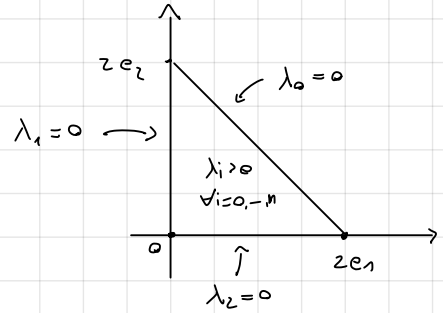
   b) Show that $w(\Sigma) = n$, where $w(K)$ denotes the *lattice width* of K

$$w(K) = \min_{d \in \mathbb{Z}^n \setminus \{0\}} \max_{x,y \in K} d^T(x - y).$$

(a) $\text{Conv}\{0, ne_1, \dots, ne_n\} = \left\{ \lambda_0 \cdot 0 + \sum_{i=1}^n \lambda_i ne_i : \lambda_i \geq 0 \ \forall i = 0, \dots, n \text{ and } \sum_{i=0}^n \lambda_i = 1 \right\} =$

$$= \left\{ n \sum_{i=1}^n \lambda_i e_i : \lambda_i \geq 0 \ \forall i = 0, \dots, n \text{ and } \sum_{i=0}^n \lambda_i = 1 \right\}$$

The interior part of Σ is $\overset{\circ}{\Sigma} = \left\{ n \sum_{i=1}^n \lambda_i e_i : \lambda_i > 0 \ \forall i = 0, \dots, n \text{ and } \sum_{i=0}^n \lambda_i = 1 \right\}$



Suppose $\exists (z_1, \dots, z_n)^T \in \mathbb{Z}^n \cap \overset{\circ}{\Sigma}$, so $\exists \lambda_0, \dots, \lambda_n > 0$ $\sum_{i=0}^n \lambda_i = 1$ s.t.:

$(z_1, \dots, z_n)^T = n \sum_{i=1}^{n} \lambda_i e_i \iff \begin{cases} z_1 = n\lambda_1 \\ \vdots \\ z_n = n\lambda_n \end{cases}$ so $0 \le z_i \left(< n\right)$ $\forall i = 1, \dots n$

$\lambda_i \ge 0 \quad \lambda_i < 1$

but at the same time if I sum up all the terms:

$\sum_{i=1}^{n} z_i = n\left(\sum_{i=1}^{n} \lambda_i\right) = n(1-\lambda_0) \Rightarrow \left(0 \le \sum_{i=1}^{n} z_i < n\right)$ but $\sum_{i=1}^{n} z_i \ge n \Rightarrow$ contraddiction.

$\lambda_0 < 1 \quad \lambda_0 > 0$

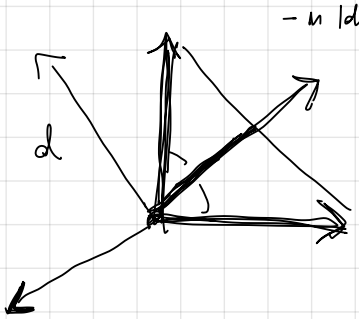
$z_i \ge 0$ and integers so ≥ 1

(b) $\min_{d \in \mathbb{Z}^n \setminus 0} \max_{x,y \in \Sigma} d^T(x-y) = \min_{d \in \mathbb{Z}^n \setminus 0} \left(\max_{x \in \Sigma} d^T x - \min_{x \in \Sigma} d^T x\right) =$

$= \min_{d \in \mathbb{Z}^n \setminus 0}$

$d = (1, \dots, 1)$

n



$-n|d| \le d^T x = |d|\,|x| \underbrace{\cos\theta}_{\le 1} \le |d| \cdot n$

$\min \max \le \min 2n|d|$ $\quad \min_y f(x) \le g(y)$

$\max_{x \in \Sigma} d^T x = \max_{\substack{(\lambda_1, \dots, \lambda_n) \\ \sum_{i=0}^{n} \lambda_i = 1,\ \lambda_i \ge 1}} d^T \left(\sum_{i=1}^{n} n\lambda_i e_i\right) = \max_{\substack{(\lambda_1, \dots, \lambda_n) \\ \sum_{i=0}^{n} \lambda_i = 1,\ \lambda_i \ge 0}} \sum_{i=1}^{n} d_i \lambda_i n,$ so to maximize this

same I set $\lambda_i = 0$ when $d_i < 0$,

2. An *ellipsoid* $\mathscr{E}$ is a set of the form

$$\mathscr{E} = \{x \in \mathbb{R}^n : \|A(x-t)\| \leqslant 1\}$$

where $A \in \mathbb{R}^{n \times n}$ is a non-singular matrix.

(a) Show that $\mathscr{E}$ is the image of $B(0,1)$ under the map

$$\tau(x) = A^{-1}x + t$$

(b) Show that, for any $d \in \mathbb{R}^n$, one has

$$\max_{x,y \in \mathscr{E}} d^T(x-y) = 2\|A^T d\|$$

(c) Conclude the following: If $\mathscr{E} \cap \mathbb{Z}^n = \emptyset$, then there exists a $d \in \mathbb{Z}^n \setminus \{0\}$ such that

$$\max_{x,y \in \mathscr{E}} d^T(x-y) \leqslant n^{3/2}/2.$$

4. Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body. Show that there is an ellipsoid E (with the origin as center) so that $E \subseteq K \subseteq C\sqrt{n} \cdot E$ for some (large) constant $C > 0$.

5. Let $\| \cdot \|_*$ be any norm in $\mathbb{R}^n$. Show that there is a matrix A so that $\| Ax \|_2 \leqslant \| x \|_* \leqslant \sqrt{n} \| Ax \|_2$. Find a norm for which the factor $\sqrt{n}$ is tight.

If it is true for x s.t. $\|x\|_* = 1$ than we obtain the thesis $\forall x \in \mathbb{R}^n$, in fact:

$$\left\| A \frac{x}{\|x\|_*} \right\|_2 \leq \left\| \frac{x}{\|x\|_*} \right\|_* \leq \sqrt{n} \left\| A \frac{x}{\|x\|_*} \right\|_2$$

Set $K := \{ x \in \mathbb{R}^n \text{ s.t. } \|x\|_* \leq 1 \}$. K is symmetric ($\|-x\|_* = \|x\|_*$) and is convex ($\|tx + (1-t)y\|_* \leq t\|x\|_* + (1-t)\|y\|_* \leq 1$ if $x, y \in K$). So there is an ellipsoid $E = \{ x \in \mathbb{R}^n : \|A^{-1}x\|_2 \leq 1 \}$ with the origin as center s.t. $E \subseteq K \subseteq \sqrt{n} E$ (I'm using John's theorem in the stronger version without C). In particular for x: $\|x\|_* = 1$ we have that $\sqrt{n} \|A^{-1}x\|_2 \leq 1 \Rightarrow$

Integer Optimization
Problem Set 9

April 22, 2024

1. Compute the Hermite Normal Form of

$$\begin{pmatrix} 5 & 18 & 2 \\ 11 & 40 & 22 \end{pmatrix}$$

via a sequence of elementary column operations. Give the final result, the sequence of operations performed, and the unimodular matrix corresponding to the sequence of operations.

2. Let $d \in \mathbb{Z}^n$, $d \neq 0$ and $\beta \in \mathbb{Z}$. Show that there exists $x \in \mathbb{Z}^n$ with

$$d^T x = \beta$$

if and only if $\gcd(d_1, \ldots, d_n)$ divides β.

3. Let $K \subseteq \mathbb{R}^n$ be convex, $d \in \mathbb{Z}^n \setminus \{0\}$ with $\gcd(\vec{d}) = 1$. We consider one *branch* of an integer program, where we have to decide whether

$$\left(K \cap \{x \in \mathbb{R}^n : d^T x = \gamma\}\right) \cap \mathbb{Z}^n = \emptyset. \tag{1}$$

   a) Show that there exists a unimodular matrix $U \in \mathbb{Z}^{n \times n}$ with $d^T \cdot U = (1, 0, \ldots, 0)$.

   b) Determine a convex set $K' \subseteq \mathbb{R}^{n-1}$ such that (1) holds if and only if

$$K' \cap \mathbb{Z}^{n-1} = \emptyset.$$

4. Let $A \in \mathbb{Z}^{m \times n}$ be of full row rank. Let $B \subseteq \{1, \ldots, n\}$ be a *basis* of A, i,e,. a set of m indices such that the corresponding columns of A are linearly independent.

   (a) Show that $\Lambda(A) = \Lambda([A|v])$, where $v \in \Lambda(A)$.

   (b) Show that $\Lambda(A) = \Lambda([A|DI_m])$, where $D = |\det(A_B)|$, where $A_B \in \mathbb{Z}^{m \times m}$ is the matrix with columns of A indexed by B.

5. Let $P \subset \mathbb{R}^d$ be a polyhedron defined by $m \geqslant 4$ linear inequalities, and let $Q = \pi(P) \subset \mathbb{R}^{d-1}$ be its projection onto the first $d-1$ coordinates. In other words, Q is the image of P under the map

$$\begin{array}{rccc} \pi: & \mathbb{R}^n & \longrightarrow & \mathbb{R}^{n-1} \\ & \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} & \longmapsto & \begin{pmatrix} x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} \end{array}$$

Prove that Q is a polyhedron that is defined by at most $m^2/4$ linear inequalities.

6. Let $v_1, \ldots, v_{d+1} \in \mathbb{R}^d$ be affinely independent points in $\mathbb{R}^d$. The polytope $\Delta = \text{conv}(v_1, \ldots, v_{d+1})$ is called a d-dimensional simplex. Prove that Δ has a non-empty interior. Describe the faces of the d-dimensional simplex.

7. Let $A \subset \mathbb{R}^d$ be a closed convex set. Prove that A has finitely many faces if and only if A is a polyhedron.

1. Compute the Hermite Normal Form of

$$\begin{pmatrix} 5 & 18 & 2 \\ 11 & 40 & 22 \end{pmatrix}$$

via a sequence of elementary column operations. Give the final result, the sequence of operations performed, and the unimodular matrix corresponding to the sequence of operations.

$$\begin{pmatrix} 5 & 18 & 2 \\ 11 & 40 & 22 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 2 \\ -33 & -158 & 22 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ -33 & -158 & 88 \end{pmatrix} \rightsquigarrow$$

use column 3 $\quad U_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & -9 & 1 \end{pmatrix}$

use column 1 $\quad U_2 = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ -33 & -70 & 88 \end{pmatrix} \leftarrow \begin{pmatrix} 1 & 0 & 0 \\ -33 & -70 & 18 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ -33 & 2 & 18 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ -33 & 2 & 0 \end{pmatrix}$$

$U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ $\quad U_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ $\quad U_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{pmatrix}$ $\quad U_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -9 \\ 0 & 0 & 1 \end{pmatrix}$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \end{pmatrix}$$

$U_7 = \begin{pmatrix} 1 & 0 & 0 \\ 19 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$U = U_1 \cdot \ldots \cdot U_7 = \begin{pmatrix} -305 & -18 & 158 \\ 85 & 5 & -44 \\ -2 & 0 & 1 \end{pmatrix}$$

2. Let $d \in \mathbb{Z}^n$, $d \neq 0$ and $\beta \in \mathbb{Z}$. Show that there exists $x \in \mathbb{Z}^n$ with

$$d^T x = \beta$$

if and only if $\gcd(d_1, \ldots, d_n)$ divides β.

$\Rightarrow$ Suppose $\exists\, x_1, \ldots, x_n \in \mathbb{Z}$ s.t. $\sum_{i=1}^n d_i x_i = \beta \in \mathbb{Z}$. Now $\gcd(d_1, \ldots, d_n) \mid d_i$ $\forall i \in \{1, \ldots, n\}$ so divides the LHS, and so has to divides β too.

$\Leftarrow$ First, we want to prove an extension of "Bezout Lemma": if $(a_1, \ldots, a_n) \in \mathbb{Z}^n$, $d = \gcd(a_1, \ldots, a_n) \Rightarrow \exists\, (x_1, \ldots, x_n) \in \mathbb{Z}^n$ s.t. $\sum_{i=1}^n a_i x_i = d$. By induction:

- $n = 2$: is the "classical" Bezout Lemma
- $n \to n+1$: by induction hypothesis $\exists (x_1, \ldots, x_n) \in \mathbb{Z}^n$ s.t. $\sum_{i=1}^n x_i a_i = \gcd(a_1, \ldots, a_n)$.

Now I apply the classical Bezout Lemma to $\gcd(a_1, \ldots, a_n)$ and a_{n+1}. So $\exists\, y_1, y_2 \in \mathbb{Z}$

s.t. : $y_1 \gcd(a_1,\dots,a_n) + y_2 a_{n+1} = \gcd\left(\gcd(a_1,\dots,a_n), a_{n+1}\right) = \gcd(a_1,\dots,a_{n+1})$

(property of gcd)

$\sum_{i=1}^{n} \underbrace{y_1 x_i}_{\in\mathbb{Z}} a_i + \underbrace{y_2}_{\in\mathbb{Z}} a_{n+1}$. So, it is proved.

Hence, we know $\exists\, x \in \mathbb{Z}^n$ s.t. $\sum_{i=1}^{n} d_i x_i = \gcd(d_1,\dots,d_n)$ but $\gcd(d_1,\dots,d_n) \mid \beta$

$\Rightarrow \gcd(b_1,\dots,b_n)K = \beta$ with $K \in \mathbb{Z} \Rightarrow \sum_{i=1}^{n} K d_i x_i = K\cdot\gcd(b_1,\dots,b_n) = \beta$ and $K d_i \in \mathbb{Z}\ \forall i$.

3. Let $K \subseteq \mathbb{R}^n$ be convex, $d \in \mathbb{Z}^n \setminus \{0\}$ with $\gcd(\vec{d}) = 1$. We consider one *branch* of an integer program, where we have to decide whether

$$\left(K \cap \{x \in \mathbb{R}^n : d^T x = \gamma\}\right) \cap \mathbb{Z}^n = \emptyset. \tag{1}$$

a) Show that there exists a unimodular matrix $U \in \mathbb{Z}^{n\times n}$ with $d^T \cdot U = (1,0,\dots,0)$.

b) Determine a convex set $K' \subseteq \mathbb{R}^{n-1}$ such that (1) holds if and only if

$$K' \cap \mathbb{Z}^{n-1} = \emptyset.$$

(a) $d^T := (d_1, \_, d_n)$. We know that the Hermite normal form of d^T is:

$(\alpha \ 0 \ \_\_ \ 0)$ with $\alpha > 0$.

We also know that we can obtain the Hermite normal form by using only 3 moves:

- swap of two columns
- multiply a column by ± 1
- add to one column a scalar multiple of another

Now: if I swap two numbers in $(d_1, \_, d_n)$ obviously the gcd doesn't change.

If I multiply by ± 1, the gcd doesn't change since gcd is defined as the "largest positive integer".

If I add to one d_i a scalar multiple of d_j $(i \neq j)$ the gcd doesn't change since $\gcd(a + mb, b) = \gcd(a,b)\ \forall a,b,m \in \mathbb{Z}$.

So $\gcd(\alpha, 0, \_\_, 0) = \gcd(d_1, \_, d_n) = 1 \Rightarrow \alpha = 1$ and so $\exists\, U$ unimodular s.t. $(d_1, \_, d_n)^T U = (1, 0, \_\_, 0)$.

(b) $\left(K \cap \{x \in \mathbb{R}^n : d^T x = \gamma\}\right) \cap \mathbb{Z}^n = \emptyset \iff \underbrace{U^{-1}K}_{\text{is a convex}} \cap \underbrace{U^{-1}\{x \in \mathbb{R}^n : d^T x = \gamma\}}_{=\{U^{-1}x \in \mathbb{R}^n : d^T x = \gamma\} = \{x \in \mathbb{R}^n : d^T U x = \gamma\} = \{x \in \mathbb{R}^n : x_1 = \gamma\}} \cap \underbrace{U^{-1}\mathbb{Z}^n}_{=\mathbb{Z}^n,\ U^{-1}\text{ unimodular}} = \emptyset$

(U is in the previous point)

$\Leftrightarrow \quad \mathcal{U}^{-1}K \cap \{x_1 = \gamma\} \cap \mathbb{Z}^n = \emptyset \iff K' \cap \mathbb{Z}^{n-1} = \emptyset$

$K' := \left\{ \begin{pmatrix} x_2 \\ | \\ x_n \end{pmatrix} \in \mathbb{R}^{n-1} \text{ s.t. } \begin{pmatrix} \gamma \\ x_2 \\ | \\ x_n \end{pmatrix} \in \mathcal{U}^{-1}K \right\}$

K' is a convex (follows immediatly by def. of convex). The last "$\Leftrightarrow$":

$\Rightarrow$: if $\begin{pmatrix} \gamma \\ x_2 \\ | \\ x_n \end{pmatrix} \in \mathcal{U}^{-1}K \cap \mathbb{Z}^n \Rightarrow \begin{pmatrix} x_2 \\ | \\ x_n \end{pmatrix} \in K' \cap \mathbb{Z}^{n-1}$.

$\Leftarrow$: if $\begin{pmatrix} x_2 \\ | \\ x_n \end{pmatrix} \in \mathbb{Z}^{n-1} \cap K' \Rightarrow \begin{pmatrix} \gamma \\ x_2 \\ | \\ x_n \end{pmatrix} \in \mathcal{U}^{-1}K$

~~4.~~ Let $A \in \mathbb{Z}^{m \times n}$ be of full row rank ($n \geq m$). Let $B \subseteq \{1, \dots, n\}$ be a *basis* of A, i,e,. a set of m indices such that the corresponding columns of A are linearly independent.

~~(a)~~ Show that $\Lambda(A) = \Lambda([A|v])$, where $v \in \Lambda(A)$.

~~(b)~~ Show that $\Lambda(A) = \Lambda([A|DI_m])$, where $D = |\det(A_B)|$, where $A_B \in \mathbb{Z}^{m \times m}$ is the matrix with columns of A indexed by B.

(a) $\Lambda(A) = \{Ax : x \in \mathbb{Z}^n\}$

$\Lambda([A|v]) = \{[A|v]y : \begin{bmatrix} x \\ \lambda \end{bmatrix} \in \mathbb{Z}^n \times \mathbb{Z}\} = \{Ax + \lambda v : x \in \mathbb{Z}^n \ \lambda \in \mathbb{Z}\} =$ ($v \in \Lambda(A)$)

$= \{Ax + yA\bar{x} : x \in \mathbb{Z}^n \ \lambda \in \mathbb{Z}\} = \{A(x + y\bar{x}) : x \in \mathbb{Z}^n \ \lambda \in \mathbb{Z}\} = \{Ax : x \in \mathbb{Z}^n\}$.

$\{x + y\bar{x} : x \in \mathbb{Z}^n \ \lambda \in \mathbb{Z}\} = \{x : x \in \mathbb{Z}^n\}$

(b) Remember that $A \, \mathrm{adj}(A) = \det(A) I$.

So, in this case, $A_B \, \mathrm{adj}(A_B) = \det(A_B) I = \pm |\det(A_B)| I = \pm D I_m$.

Remember also that, since $A_B \in \mathbb{Z}^{m \times m}$, so $\mathrm{adj}(A_B) \in \mathbb{Z}^{m \times m}$ as well.

In particular $\Lambda([A \mid D I_m]) = \Lambda([A \mid \pm A_B \, \mathrm{adj}(A_B)]) =$

$= \{[A \mid \pm A_B \, \mathrm{adj}(A_B)] \begin{pmatrix} x \\ y \end{pmatrix} : x \in \mathbb{Z}^m \ y \in \mathbb{Z}^m\} =$

$= \{[Ax \pm A_B \, \mathrm{adj}(A_B) y : x \in \mathbb{Z}^m \ y \in \mathbb{Z}^m]\} =$ ← column i: $(A_B \, \mathrm{adj}(A_B))^i = A_B (\mathrm{adj}(A_B))^i \in \Lambda(A)$ since A_B is the basis of $\Lambda(A)$ and $\mathrm{adj}(A_B)^i \in \mathbb{Z}^m$. So $\exists \lambda_i \in \mathbb{Z}^m$ s.t. $(A_B \, \mathrm{adj}(A_B))^i = A\lambda_i \ \forall i$

$= \{[Ax \pm \sum_{i=1}^m y_i A\lambda_i : x \in \mathbb{Z}^m, y_i \in \mathbb{Z}, \lambda_i \in \mathbb{Z}^m]\} =$

$= \{[A(x \pm \sum_{i=1}^m y_i \lambda_i) : x \in \mathbb{Z}^m, y_i \in \mathbb{Z}, \lambda_i \in \mathbb{Z}^m]\} =$

$= \{Ax : x \in \mathbb{Z}^m\} = \Lambda(A)$

$\{x \pm \sum_{i=1}^m y_i \lambda_i : x \in \mathbb{Z}^n, y_i \in \mathbb{Z}, \lambda_i \in \mathbb{Z}^m\} = \{x : x \in \mathbb{Z}^m\}$

5. Let $P \subset \mathbb{R}^d$ be a polyhedron defined by $m \geqslant 4$ linear inequalities, and let $Q = \pi(P) \subset \mathbb{R}^{d-1}$ be its projection onto the first $d-1$ coordinates. In other words, Q is the image of P under the map

$$\pi: \begin{array}{ccc} \mathbb{R}^d & \longrightarrow & \mathbb{R}^{d-1} \\ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} & \longmapsto & \begin{pmatrix} x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} \end{array}$$

Prove that Q is a polyhedron that is defined by at most $m^2/4$ linear inequalities.

$\pi(P)$ is a polyhedron: Suppose $P = \left\{ x : \sum_{j=1}^{d} a_{ij} x_j \leq b_i \quad i = 1, \dots, m \right\}$.

So we define:

$$I_+ = \{ i : a_{i1} > 0 \} \qquad I_- = \{ i : a_{i1} < 0 \} \qquad I_0 = \{ i : a_{i1} = 0 \}.$$

$$\pi(P) = \left\{ \begin{pmatrix} x_2 \\ \vdots \\ x_n \end{pmatrix} : \exists x_1 : \sum_{j=1}^{d} a_{ij} x_j \leq \beta_i \ \ \forall i = 1, \dots, d \right\} =$$

$$= \left\{ \begin{pmatrix} x_2 \\ \vdots \\ x_n \end{pmatrix} : \sum_{j=2}^{d} a_{ij} x_j \leq \beta_i \ \ \forall i \in I_0 \text{ and } \exists x_1 \text{ s.t. } \sum_{j=1}^{d} a_{ij} x_j \leq \beta_i \ \ \forall i \in I_+ \cup I_- \right\} =$$

Now, the condition "$\exists x_1$ s.t. $\sum_{j=1}^{d} a_{ij} x_j \leq \beta_i \ \ \forall i \in I_+ \cup I_-$" can be written as:

$$\exists x_1 : \sum_{j=1}^{d} a_{ij} x_j \leq \beta_i \ \ \forall i \in I_+ \text{ and } \sum_{j=1}^{d} a_{ij} x_j \leq \beta_i \ \ \forall i \in I_- \iff$$

$$\exists x_1 : \left(x_1 \leq \frac{\beta_i - \sum_{j=2}^{d} a_{ij} x_j}{a_{i1}} \ \ \forall i \in I_+ \right) \text{ and } \left(x_1 \geq \frac{\beta_i - \sum_{j=2}^{d} a_{ij} x_j}{a_{i1}} \ \ \forall i \in I_- \right)$$

So such x_1 exists $\iff$ $\frac{\beta_i}{a_{i1}} - \sum_{j=2}^{d} \frac{a_{ij}}{a_{i1}} x_j \leq \frac{\beta_k}{a_{k1}} - \sum_{j=2}^{d} \frac{a_{kj}}{a_{k1}} x_j \quad \forall i \in I_- \ \forall k \in I_+$

($\exists x$ s.t. $x \geq a_1, \dots, a_n$ and $x \leq b_1, \dots, b_m \iff a_i \leq b_j \ \ \forall i, j$)

So, the linear inequalities for $\pi(P)$ are:

$$\begin{cases} \sum_{j=2}^{d} a_{ij} x_j \leq \beta_i \ \ \forall i \in I_0 \\ \sum_{j=2}^{d} \left(\frac{a_{kj}}{a_{k1}} - \frac{a_{ij}}{a_{i1}} \right) x_j \leq \frac{\beta_k}{a_{k1}} - \frac{\beta_i}{a_{i1}} \quad \forall i \in I_- \ \forall k \in I_+ \end{cases}$$

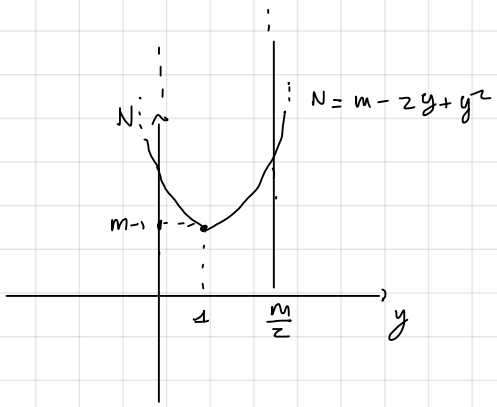
At most $\frac{m^2}{4}$ inequalities: We know that $|I_0| + |I_-| + |I_+| = m$.

So the number N of inequalities by the previous point is:

$$\begin{cases} |I_0| + |I_+| \cdot |I_-| = N \\ |I_0| + |I_-| + |I_+| = m \\ 0 \le |I_0|, |I_-|, |I_+| \le m \end{cases} \iff \begin{cases} |I_0| = x \\ |I_+| = y \\ |I_-| = z \end{cases} \quad \begin{cases} x + yz = N \\ x + y + z = m \\ 0 \le x, y, z \le m \end{cases}$$

Note that, for a fixed x $\begin{cases} yz = N - x \\ y + z = m - x \\ 0 \le x, y, z \le m \end{cases}$ is equivalent to maximize the area $N - x$ of a rectangle with perimeter $2(m-x)$ and we know that the solution is the square.

So, we obtain the equation $y = z$ and so $N = m - 2y + y^2$ but since $z = y \Rightarrow$ $0 \le y \le \frac{m}{2}$:



So the possible maximum are at $y = 0$ $(N = m)$ or $y = \frac{m}{2}$ $\left(N = \frac{m^2}{4}\right)$. Since $\frac{m^2}{4} > m$ for $m \ge 4$, we have that $N \le \frac{m^2}{4}$.

6. Let $v_1, \dots, v_{d+1} \in \mathbb{R}^d$ be affinely independent points in $\mathbb{R}^d$. The polytope $\Delta = \text{conv}(v_1, \dots, v_{d+1})$ is called a d-dimensional simplex. Prove that Δ has a non-empty interior. Describe the faces of the d-dimensional simplex.

Δ has no empty interior: consider $p = \frac{1}{d+1} v_1 + \dots + \frac{1}{d+1} v_{d+1} \in \Delta$.

Consider the $(n-1)$-faces $\Delta_i = \text{conv}\left(v_1, \dots, \hat{v_i}, \dots, v_{d+1}\right)$. A d-dimensional simplex is closed (is the preimage of a closed condition) and bounded (bounded condition) $\Rightarrow$ is compact.

In particular, Δ_i are compact so:

$$r := \min_{y \in \bigcup_{i=1}^{n+1} \Delta_i} d(p, y)$$; since $\bigcup_{i=1}^{n+1} \Delta_i$ is compact $\Rightarrow$ the minimum is well defined and $r > 0$ since $p \notin \bigcup_{i=1}^{n+1} \Delta_i$. Now $I_{p,y} := \{tp + (1-t)y \quad \forall t \in [0,1]\} \subseteq \Delta$

$\forall y \in \bigcup_{i=1}^{n+1} \Delta_i$ and since $I_{p,y}$ is a segment of lenght $d(p,y)$, we have that the segment starting from p, with direction $\overrightarrow{py}$ and lenght r is included in Δ, we call it r_{py}. In particular we have that $\bigcup_{y \in \bigcup_{i=1}^{n+1} \Delta_i} r_{py} = B(p,r)$, in fact:

$\subseteq$ by definition

$\supseteq$ we have to show that $\forall z \in B(p,r)$ the extension of r_{pz} intersects $\bigcup_{i=1}^{n+1} \Delta_i$ at some point. If this were not the case ... devo dire che

e non

<u>Δ has no empty interior</u>: $v \in \Delta \iff v = \begin{pmatrix} V_1 & \cdots & V_{d+1} \end{pmatrix} \begin{pmatrix} \gamma_1 \\ | \\ \gamma_{d+1} \end{pmatrix}$ with $\sum_{i=1}^{n} \gamma_n = 1$ and $\gamma_i \geq 0$.

In a compact way, $v \in \Delta \iff$:

$$\exists \begin{pmatrix} \gamma_1 \\ | \\ \gamma_n \end{pmatrix} \quad \begin{pmatrix} V_1 & \cdots & V_{d+1} \\ 1 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \gamma_1 \\ | \\ \gamma_n \end{pmatrix} = \begin{pmatrix} v \\ 1 \end{pmatrix} \quad \text{and} \quad \gamma_i \geq 0 \ \forall i \in \{1, \dots, d+1\}.$$

$$\det\left(\begin{pmatrix} V_1 & \cdots & V_{d+1} \\ 1 & \cdots & 1 \end{pmatrix}\right) = \det\left(\begin{pmatrix} V_1 & V_2 - V_1 & \cdots & V_{d+1} - V_1 \\ 1 & 0 & & 0 \end{pmatrix}\right) =$$

$$= \pm 1 \det\left(\begin{pmatrix} V_2 - V_1 & \cdots & V_{d+1} - V_1 \end{pmatrix}\right) \neq 0$$

(Laplace using last row)

(since $V_1, \dots, V_{d+1}$ affinely indipendent)

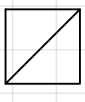
So $\forall v \ \exists! \begin{pmatrix} \gamma_1 \\ | \\ \gamma_n \end{pmatrix}$ s.t. the system is satisfied but we don't know if $\gamma_i \geq 0$.

For $p = \frac{1}{d+1} V_1 + \cdots + \frac{1}{d+1} V_{d+1}$, $\gamma_i = \frac{1}{d+1} > 0 \ \forall i$ and since the solution of the system is continuous with respect to v, there is a $\varepsilon > 0$ s.t.

$\forall w \in B(p, \varepsilon)$ the solution $\begin{pmatrix} \gamma_1^w \\ | \\ \gamma_{d+1}^w \end{pmatrix}$ is s.t. $\gamma_i^w > 0 \ \forall i \in \{1, \dots, d+1\}$. So, $B(p, \varepsilon) \subseteq \Delta$.

<u>Faces of the d-simplex</u>: the K-faces of a d-simplex ($K \leq d$) are K-simplex themselves and the number of K-faces is $\binom{d+1}{K+1} = \frac{(d+1)!}{(K+1)!\,(n-K)!}$

there is no "diagonal" in a simplex!



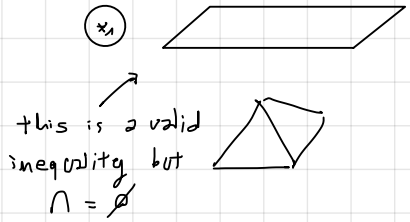
↩ is not a simplex in $\mathbb{R}^2$!

7. Let $A \subset \mathbb{R}^d$ be a closed convex set. Prove that A has finitely many faces if and only if A is a polyhedron.

$\Rightarrow$ If A has finitely many faces $\Rightarrow \exists$ a finite number m of valid inequality $c_i^T x \leq \delta_i$ $i \in \{1, \dots, m\}$ s.t. $A \cap \{c_i^T x = \delta_i\} \neq \emptyset$ and $A \cap \{c_i^T x = \delta_i\} \neq A \cap \{c_j^T x = \delta_j\}$. So A can be described by

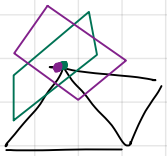
x_1

$$x \in A \iff \begin{pmatrix} c_1^T \\ | \\ c_m^T \end{pmatrix} x \leq \begin{pmatrix} \delta_1 \\ | \\ \delta_m \end{pmatrix}$$



this is a valid inequality but $\cap = \emptyset$

x_2



← two valid inequalities with $\cap \neq \emptyset$ but they are the same

$\Leftarrow$ A is a polyhedron so $A = \{ x \in \mathbb{R}^d : Mx \leq b \text{ with } M \in \mathbb{R}^{m \times d} \; b \in \mathbb{R}^m \}$.

So $x \in A \iff$

is valid for P, if $\forall x \in P$, $c^T x \leq j$. Let $c^T x \leq j$ be valid, then $y = P \cap (c^T x = \delta)$ is a face of P.

Integer Optimization
Problem Set 10

April 29, 2024

1. Is the Voronoi cell with respect to the l_∞ norm convex? If so, prove it and if not give a counterexample.

2. Prove that $\mathcal{V} \subseteq B(0, n \cdot \lambda_n(\Lambda))$ where $\mathcal{V}$ is the Voronoi cell of the full-dimensional lattice $\Lambda \subseteq \mathbb{R}^n$.

3. Let $P = \{p_1, p_2, p_3\} \subseteq \mathbb{R}^n$ be a finite set of three points. Show that the Voronoi cells $\mathcal{V}(p_1), \mathcal{V}(p_2)$ and $\mathcal{V}(p_3)$ intersect in one point. Show that this point is equidistant from all points p_1, p_2, p_3. Show that it is the center of the circle passing through these points, and this circle contains no other points in its interior.

4. Given any n points in $\mathbb{R}^2$, show that their Voronoi diagram has at most $2n-5$ vertices and $3n-6$ edges.

5. Given a set of points $S \subseteq \mathbb{R}^2$ and $p \in S$. Show that the region $\mathcal{V}(p)$ is unbounded if and only if p is an extreme point of $\text{conv}(S)$.

6. Show that the voronoi cell of the dual lattice satisfies

$$\mathcal{V}(\Lambda^*) = \text{conv}\left\{ \frac{2}{\|z\|_2^2} z \colon z \in \Lambda \setminus \{0\} \right\}.$$

7. Let $P = \{x \in \mathbb{R}^n : Ax \leqslant b\} \subseteq \mathbb{R}^n$ be a full-dimensional polytope. An inequality $a^T x \leqslant \beta$ of $Ax \leqslant b$ is *redundant* if the inequalities obtained by removing $a^T x \leqslant \beta$ from $Ax \leqslant b$ define the same polytope P. Let $A'x \leqslant b'$ be the result of the removal of $a^T x \leqslant \beta$ from $Ax \leqslant b$.

   i) Show that $a^T x \leqslant \beta$ is redundant if and only if

   $$\max\{a^T x \colon x \in \mathbb{R}^n, A'x \leqslant b'\} \leqslant \beta.$$

   ii) Show that $a^T x \leqslant \beta$ is redundant if and only if there exists $\lambda \in \mathbb{R}^{m-1}_{\geqslant 0}$ such that

   $$a^T = \lambda^T A' \text{ and } \lambda^T b' \leqslant \beta.$$

   Hint: Linear programming duality.

   iii) Show that $a^T x \leqslant \beta$ is redundant if and only if the affine dimension of the face $F = \{x \in P \colon a^T x = \beta\}$ is at most $n-2$, in other words, if and only if F is not a facet.

1. Is the Voronoi cell with respect to the l_∞ norm convex? If so, prove it and if not give a counterexample.

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

Consider $\Lambda \subseteq \mathbb{R}^4$ generated by $b_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$, $b_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$. Consider the points $x = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$ and $y = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$. $x \in \mathcal{V}_\infty(\Lambda)$ infact:

$\|x\|_\infty = 1$ and $\|x - (m(\text{col}_1) + n(\text{col}_2))\|_\infty = \left\| \begin{pmatrix} 1-m \\ -m-n \\ 1-m-n \\ 1-m-n \end{pmatrix} \right\|_\infty \ge 1$ ($m, n \in \mathbb{Z}$)

if $m \neq 1$ $|1-m| \ge 1$, so $m = 1$: if $n \neq -1$ $|-m-n| \ge 1$; but for $m = 1$ and $n = -1$ the third entrance ≥ 1 in module

With the same argument $y \in \mathcal{V}_\infty(\Lambda)$.

But $K := \frac{1}{2}\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1 \end{pmatrix} \notin \mathcal{V}_\infty(\Lambda)$, indeed

for $v = b_1$ $\|K - v\|_\infty = \left\| \begin{pmatrix} -1/2 \\ -1/2 \\ -1/2 \\ 0 \end{pmatrix} \right\|_\infty = \frac{1}{2} < 1 = \|K\|_\infty$.

2. Prove that $\mathcal{V} \subseteq B(0, n \cdot \lambda_n(\Lambda))$ where $\mathcal{V}$ is the Voronoi cell of the full-dimensional lattice $\Lambda \subseteq \mathbb{R}^n$.

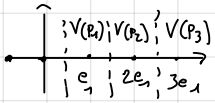
Suppose by contraddiction that exists $x \in \mathcal{V}(\Lambda)$ but $x \notin B(0, n\lambda_n(\Lambda))$.

So: $n\lambda_n(\Lambda) \le \|x\| \le \|x - v\| \ \forall v \in \Lambda$. But we knew that $\mu(\Lambda) \le \frac{\sqrt{n}}{2}\lambda_n$ so there

$\exists$ a lattice point $v \in \Lambda$ s.t. $\|v - x\| \le \frac{\sqrt{n}}{2}\lambda_n(\Lambda) < n\lambda_n(\Lambda) \le \|x - v\|$, $\lightning$.

3. Let $P = \{p_1, p_2, p_3\} \subseteq \mathbb{R}^n$ be a finite set of three points. Show that the Voronoi cells $\mathcal{V}(p_1), \mathcal{V}(p_2)$ and $\mathcal{V}(p_3)$ intersect in one point. Show that this point is equidistant from all points p_1, p_2, p_3. Show that it is the center of the circle passing through these points, and this circle contains no other points in its interior.

non collinear (it's not true if for example I choose $p_1 = e_1$ $p_2 = 2e_1$ $p_3 = 3e_1$ in $\mathbb{R}^2$



lattice points

Λ generated by p_1, p_2, p_3. $\mathcal{V}(p_i) = \mathcal{V} + p_i = \{ x \in \mathbb{R}^n : \|x\| \le \|x - v\| \ \forall v \in \Lambda \} + p_i =$

$= \{ x + p_i \in \mathbb{R}^n : \|x + p_i - p_i\| \le \|x + p_i - p_i - v\| \ \forall v \in \Lambda \} =$ ($x + p_i =: y$)

$= \{ y \in \mathbb{R}^n : \|y - p_i\| \le \|y - (p_i + v)\| \ \forall v \in \Lambda \} =$

$\Lambda = \Lambda + p_i$: $\subseteq$ $v = (\underbrace{v - p_i}_{\in \Lambda}) + p_i \in \Lambda + p_i$

$\supseteq$ $v + p_i \in \Lambda$ obviously

$= \{ y \in \mathbb{R}^n : \|y - p_i\| \le \|y - v\| \ \forall v \in \Lambda \}$ $\forall i = 1, 2, 3$.

(The vectors s.t. p_i is the nearest lattice point).

So, suppose $x \in \mathcal{V}(p_1) \cap \mathcal{V}(p_2) \cap \mathcal{V}(p_3) \Rightarrow \|x-p_1\| \leq \|x-p_2\| \leq \|x-p_1\|$

($x \in \mathcal{V}(p_1)$, $x \in \mathcal{V}(p_2)$)

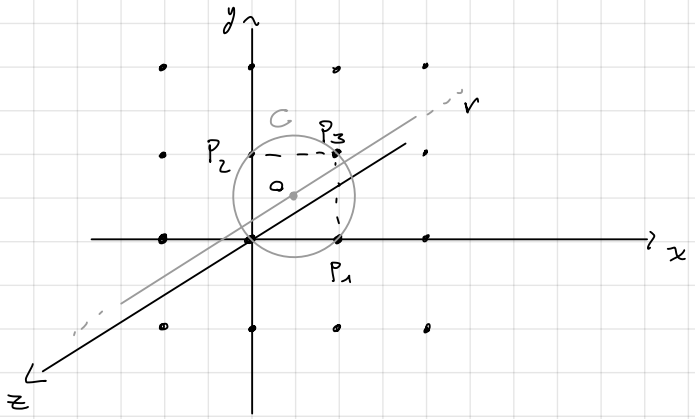
$\Rightarrow \|x-p_1\| = \|x-p_2\| = \|x-p_3\|$. (in the same way)

So, x is equidistant from p_1, p_2, p_3.

Let show x exist: p_1, p_2, p_3 are not collinear $\Rightarrow \exists!$ circle C s.t. $p_1, p_2, p_3 \in C$.

In particular the center of the circle o is equidistant from $p_1, p_2, p_3 \Rightarrow o \in \bigcap_{i=1}^{3} \mathcal{V}(p_i)$.

It is not unique, for example $\Lambda\left(p_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, p_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}\right) \subseteq \mathbb{R}^3$:



$p_3 := \begin{pmatrix}1\\1\\0\end{pmatrix}$

$o = \begin{pmatrix}\frac{1}{2}\\ \frac{1}{2}\\ 0\end{pmatrix}$

All the points in r are equidistant from p_1, p_2, p_3.

Now, by contraddiction, if $v \in \Lambda \cap B(o, \|o-p_1\| = \|o-p_2\| = \|o-p_3\|) \Rightarrow$ (letter "o", the center)

$\|o-v\| < \|o-p_1\|$ but $o \in \mathcal{V}(p_1) \Rightarrow$ since $v \in \Lambda$ $\|o-p_1\| \leq \|o-v\| < \|o-p_1\|$ ↯.

4. Given any n points in $\mathbb{R}^2$, show that their Voronoi diagram has at most $2n-5$ vertices and $3n-6$ edges.

The Voronoi diagram a set I (discrete) is what we expect: a partition of $\mathbb{R}^2$ s.t. to any element of the set p_i is associated a region of $\mathbb{R}^2$ $R(p_i)$ s.t. $R(p_i) := \{x \in \mathbb{R}^2 : \|x-p_i\| \leq \|x-p_j\| \ \forall p_j \in I\}$

In particular, by definition # faces $= |I| = n$.

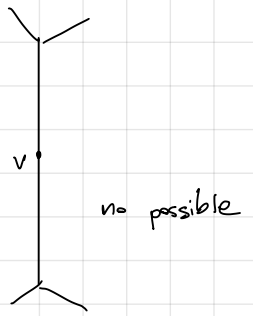
Now by Euler's formula for bounded simplex: $v - e + f = 2$. (# vertices, # edges, # faces)

In order to use this formula, we use the Alexandorf compactification where the unbounded edges are connected to p_∞. Now the numbers of faces and edges don't change; we have only one more point so:

$$(v+1) - e + n = 2 \Rightarrow \quad v - e = 1 - n$$

Furthermore, note that a vertex v is incident to at least three cells: by definition

it is intersection of two Voronoi cells. If there is no other cell intersecting $V \Rightarrow$ V is in the interior part of an edge shared by the cells $\Rightarrow$ is not a vertex:



no possible

possible

furthermore, we need two vertice to define an edge so:

$e \leq$