Reticoli

Due Definizioni equivalenti:

Def 1 Dati $b_1, \dots, b_n \in \mathbb{R}^m$ vettori lin. ind. definiamo reticolo generato da $\mathcal{B} = \{b_1, \dots, b_n\}$ l'insieme

$$\mathcal{L}(\mathcal{B}) = \left\{ \sum_i^n a_i b_i \in \mathbb{R}^m \;\middle|\; a_i \in \mathbb{Z} \right\}.$$

se chiamiamo $B = \begin{pmatrix} b_1 & b_2 & \dots & b_n \end{pmatrix}$ la matrice $m \times n$ le cui colonne sono i vettori $b_i \in \mathcal{B}$

$$\mathcal{L}(\mathcal{B}) = \{ B \cdot \underline{a} \mid \underline{a} \in \mathbb{Z}^n \}$$

B si chiama la matrice del reticolo.
$\mathcal{B}$ si chiama la base del reticolo

Def. 2 Un reticolo $\mathcal{L}$ è un s.g. discreto di $\mathbb{R}^m$, ossia $\mathcal{L}$ è un s.g. tale che $\forall r \in \mathbb{R}_+$

$$\# \{ v \in \mathcal{L} \mid \|v\| < r \} \text{ è \underline{finita}}$$

Es. Provare che le due definizioni sono equivalenti.

OSS. Per le nostre applicazioni $\mathcal{B} \subset \mathbb{Z}^m$

Alcuni problemi che vogliamo risolvere:

se $\mathcal{B} \subset \mathbb{Z}^m$

Hermite

1. appartenenza: Dato $\mathcal{L}(\mathcal{B})$ decidere se $v \in \mathbb{Z}^m$ è t.c. $v \in \mathcal{L}$
2. Dati $b_1, \ldots, b_n \in \mathbb{Z}^m$ trovare una base per il reticolo che generano.
3. Data M matrice $m \times n$ trovare una base per il reticolo $\ker M = \{ \underline{x} \in \mathbb{R}^n \mid A\underline{x} = 0 \}$.

(4) * SVP (shortest vector problem)
dato $\mathcal{B}$ base per $\mathcal{L}(\mathcal{B})$ trovare $\underline{v} \in \mathcal{L}(\mathcal{B})$, $\underline{v} \neq 0$
t.c. $\|v\|$ è minimale.

(5) * (CVP) (closest vector problem) dato $w \in \mathbb{Q}^m$
calcolare $v \in \mathcal{L}$ t.c. $\|w - v\|$ minimale

(6) SVP_A (shortest v.p. approssimato)
Se $\gamma > 1$ trovare $v \in \mathcal{L}, v \neq 0$, t.c. $\|v\| \leq \gamma \cdot$ mi

(7) CVP_A (closest-vector problem - approssimato)
se $\gamma > 1$ e $w \in \mathbb{Q}^m$, calcolare $v \in \mathcal{L}$ t.c.
$\|w - v\| \leq \gamma \, \|w - B \cdot \underline{a}\| \quad \forall a \in \mathbb{Z}^n$

* sono molto difficili se $n >> 0$, per reticoli "generali"

Oss. se la matrice B di $\mathcal{L}$ è

$$B = \begin{pmatrix} 213 & 0 \\ 0 & 1151 \end{pmatrix}$$

allora $v \in \mathcal{L}$ $v = (a_1 213 + a_2 1151)$

$\Rightarrow$ vettori più corti $(213, 0)$ e $(-213, 0)$

e se $w = (476, 2371)$ $\rightarrow$ $v = (425, 2302)$

è t.c. $\|w - v\|$ è minimo.

Vantaggio: i vettori di B sono ortogonali

Cercheremo di vedere allora se dato $\mathcal{L}$ esiste e in caso come trovare una sua base ortogonale o almeno il "più possibile" ortogonale.

Definizioni. $\mathcal{B} = \{b_1, \dots, b_n\}$ l.i, $\mathcal{L}(\mathcal{B})$ e B. indichiamo $< \mathcal{B} >$ = SSV di $\mathbb{R}^m$ generato da $\mathcal{B}$.

- rango $\mathcal{L} = n = \dim < \mathcal{B} >$
- $\dim \mathcal{L} = m$
- $n = m$ $\mathcal{L}$ reticolo full rank.

(Nota $\mathcal{L}$ full rank $\Leftrightarrow$ $< \mathcal{B} > = \mathbb{R}^m$)

Se $\mathcal{L}' \subseteq \mathcal{L}$ è un reticolo allora $\mathcal{L}'$ sottoreticolo di $\mathcal{L}$.

Oss. Se $\mathcal{L}'(\mathcal{B}') = \mathcal{L}(\mathcal{B}) \Rightarrow \langle \mathcal{B}' \rangle = \langle \mathcal{B} \rangle$

ma se $\mathcal{B}' \subset \mathcal{L}(\mathcal{B})$ è un insieme l.i in generale anche se $\langle \mathcal{B}' \rangle = \langle \mathcal{B} \rangle$

$\mathcal{L}(\mathcal{B}') \neq \mathcal{L}(\mathcal{B})$.

Come scegliere una nuova base per $\mathcal{L}(\mathcal{B})$.

Una prima caratterizzazione:

se $\mathcal{B}' \subset \mathcal{L}(\mathcal{B})$ l.i allora

$$\mathcal{L}(\mathcal{B}') = \mathcal{L}(\mathcal{B}) \Longleftrightarrow \mathcal{P}(\mathcal{B}') = \{B'\underline{a} \mid 0 \leq \underline{a} < 1\} \cap \mathcal{L}(\mathcal{B}) = \{0\}.$$

parallelepipedo fondamentale

algebricamente

Proposizione 1. $\mathcal{B}$ e $\mathcal{B}' \subseteq \mathbb{R}^m$ di rango n sono t.c.

$\mathcal{L}(\mathcal{B}) = \mathcal{L}(\mathcal{B}')$ se e solo se

$\exists\, U$ matrice $n \times n$ a coefficienti interi

t.c. $\det U = \pm 1$ e $B' = BU$

Per provare la prop. 1 definiamo la proiezione di un reticolo.

Prop 2 Sia $\mathcal{L}(\mathcal{B})$ un reticolo di rango n e dimensione m e sia B la sua matrice.
Se $m > n$ esiste $\pi : \mathbb{R}^m \to \mathbb{R}^n$ lineare t.c.

1. $\pi(\mathcal{L})$ reticolo di full rank n
2. $\|\pi(v)\| = \|v\| \quad \forall v \in \mathcal{L}(\mathcal{B})$ (conserva la $\|\,\|$)
3. $(\pi(b_i), \pi(b_j)) = (b_i, b_j) \quad \forall b_i, b_j \in \mathcal{B} \; i \neq j$

Dim. Basta considerare $v_1, \dots, v_n$ base ortonormale di $V = \langle \mathcal{B} \rangle$ e definire
$\pi(v_i) = e_i$ e $\pi(w) = 0$ se $w \in V^\perp$.
È immediato che se Π è la matrice $n \times m$ che rappresenta π (risp basi canoniche), allora
$B' = \Pi B$ è una matrice $n \times n$ invertibile
e quindi $\mathcal{L}(\mathcal{B}')$ è un reticolo full-rank.

Dim (Prop 1) - Se $\mathcal{L}(\mathcal{B}) = \mathcal{L}(\mathcal{B}')$ $\forall b_i' \in \mathcal{B}'$ $b_i' = \sum_j u_{ji} b_j$
con $u_{ji} \in \mathbb{Z}$, così se $U = (u_{ij})$ $B' = BU$
Da $b_i = \sum u'_{ji} b'_i$ vale anche $B = B'U' = BUU'$
Applicano Π della prop precedente $\underbrace{\Pi B}_{\text{invertibili}} = \Pi B UU'$

Da cui $U \cdot U' = I_n$ $\Rightarrow$ dato che U e U' sono a coeff. interi $\det U = \pm 1$

$\Leftarrow$ $U\mathbb{Z}^n = \mathbb{Z}^n$, da cui $\{B\underline{a} \mid a \in \mathbb{Z}^n\} = \{\underbrace{B(U\underline{a})}_{B'} \mid a$

Determinante

Definiamo il determinante di un reticolo come il <u>volume</u> del parallelepipedo fondamentale

$$\mathcal{P}(\mathcal{B}) = \{ B\underline{x} \mid 0 \leq x < 1 \}.$$

<u>oss.</u> chiaro se $n = m$ che $\det \mathcal{L} = |\det B|$

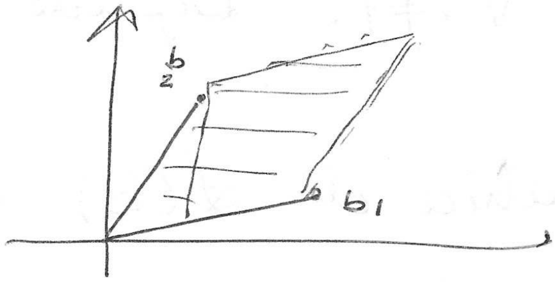
ma se $n < m$?

usiamo la matrice proiezione:

$$\det \mathcal{L}(\mathcal{B}) = |\det(\Pi B)|$$

<u>OSS</u>-<u>ES</u> Provare che la definizione non dipende dalla base scelta né dalla proiezione scelta

$n=2$. $\det(\mathcal{L}) = \|b_1\| \|b_2\| \cdot |\sin\theta|$



Fra le (infinite) basi di un reticolo ne vogliamo calcolare una con vettori relativamente corti e ortogonali

per $n=2$ $\|b_1\| \cdot \|b_2\|$ piccolo $\longleftrightarrow$ ~~sin~~ $\vartheta = \pm \frac{\pi}{2}$

Vogliamo trovare un altro modo per calcolare il $\det(\mathcal{L})$.

<u>Ricordiamo</u>: ORTOGONALIZZAZIONE di Gram-Schmidt

Siano $b_1, \dots, b_n$ vettori definiamo

$$b_1^* = b_1$$

$$b_i^* = b_i - \sum_{j<i} \mu_{ij} b_j^* \quad , \quad \mu_{ij} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)}$$

dove (x, y) è il prodotto scalare $\sum_i x_i y_i$ in $\mathbb{R}^m$

<u>Nota</u> $\forall i$ b_i^* è la componente di b_i ortogonale a $b_1, \dots, b_{i-1}$

Si ha anche: $\forall i\ \langle b_1, \dots, b_i \rangle = \langle b_1^*, \dots, b_i^* \rangle$
e $(b_i^*, b_j^*) = 0 \quad \forall i \neq j$. Dipende dall'ordine!

<u>Oss</u> Se B matrice di $\mathcal{L}(B)$ allora si ha che la matrice
$n \times n$ $\underline{B^T \cdot B = ((b_i, b_j))}$

<u>Proposizione</u> Sia $\mathcal{L}(\mathcal{B}) \subset \mathbb{Z}^m$ di rango n
$\mathcal{B} = \{b_1, \dots, b_n\}$ (ordinata) si ha

1. $\det(\mathcal{L}(\mathcal{B})) = \sqrt{\det(B^T B)}$
2. Se $\{b_1^*, \dots, b_n^*\}$ è l'ortogonalizzazione di $\mathcal{B}$

$$\det(\mathcal{L}(\mathcal{B})) = \prod \|b_i^*\|.$$

<u>Dim</u>. 1. Se $m = n$ $\quad \det(\mathcal{L}) = |\det B| = \sqrt{\det(B^T B)}$
$= \sqrt{(\det B)^2}$

se $m > n$. Sia Π una proiezione e consideriamo
$B' = \Pi B$ $(n \times n)$ allora

$$\det \mathcal{L} = |\det(\Pi B)| = \sqrt{\det((B')^t \cdot B')}$$

ma per costruzione e prop 1 si ha che
l'elemento (i,j) in $(B')^T \cdot B$ è $(\pi(b_i), \pi(b_j)) = (b_i, b_j)$

$$\Rightarrow \det \mathcal{L} = \sqrt{\det(B^T \cdot B)}.$$

2. Osserviamo che dalle relazioni

$$b_i = b_i^* + \sum_{j<i} \mu_{ij}\, b_j^*$$

otteniamo che esiste una matrice (triangolare) U, con $\det(U) = 1$

t.c. $\quad B = B^* U.$

Se $m = n$ allora $|\det B| = |\det B^*| = \prod \|b_i^*\| = \det$

Se $m > n$ $\quad \det \mathcal{L} = |\det(\Pi B)| = |\det(\Pi B^* U)|$

$$= |\det(\Pi B^*)| = \sqrt{\det((B^*)^t \cdot B^*)}$$

$$= \prod \|b_i^*\| .$$

<u>Oss.</u> Dato che $\forall i \quad \|b_i\| \geq \|b_i^*\|$ (provare)

$$\det(\mathcal{L}) \leq \prod \|b_i\|$$

<u>Oss.</u> Se $m > n$ $\quad \det(\mathcal{L})$ può <u>non</u> essere intero.

<u>Es.</u> $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \Rightarrow \det \mathcal{L} = \sqrt{B^t \cdot B} = \sqrt{2}$

Vogliamo trovare un modo per "misurare" la lunghezza dei vettori di $\mathcal{L}$

Consideriamo $B_n(0,r) = \{x \in \mathbb{R}^n \mid \|x\| < r\}$

Dato $\mathcal{L}$ definiamo l'i-esimo minimo λ_i di $\mathcal{L}$ come il raggio della più piccola sfera che contiene i vettori $v_i \in \mathcal{L}$ linearmente indipendenti.

$$\lambda_i = \inf\{r \in \mathbb{R} \mid \dim(<\mathcal{L} \cap B(0,r)>) \geq i\}.$$

ossia esistono in $\mathcal{L}$ i vettori $v_1 .. v_i$ linearmente indipendenti t.c. $\|v_i\| \leq \lambda_i$

Nota $0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$.

In generale NON esiste una base $\mathcal{B}$ per cui la norma $\|b_i\| = \lambda_i \ \forall i$

<u>Esempio</u> $\mathcal{L} = \{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid x_i \equiv x_j\ (2), \forall i,j\}$

esistono in $\mathcal{L}$

- $2e_i = v_i$, $\|v_i\| = 2$. e $v_1, \dots, v_n$ sono lin. ind.
- se in $w \in \mathcal{L}$ esiste una coordinata dispari allora <u>tutte</u> le coordinate sono $\neq 0$ ossia $\|w\| \geq \sqrt{n}$

Quindi se $n=2$ $\quad \lambda_1 = \lambda_2 = \sqrt{2}$ $\quad$ base $(1,1)\ (1,-1)$ ok

$n=3$ $\quad \lambda_1 = \lambda_2 = \lambda_3 = \sqrt{3}$ $\quad$ base $(1,1,1)\ (1,-1,-1)\ (-1,-1,1)$

$n \geq 4$ $\quad \lambda_1 = \lambda_2 = \dots = \lambda_n = 2$.

non esiste una base con vettori di norma 2.

Però esistono <u>sempre</u> n vettori linearmente indipendenti $v_1 \dots v_n \in \mathcal{L}$ t.c.

$$\|v_i\| = \lambda_i \quad \forall i$$

<u>Teorema</u> Sia $\mathcal{L}$ di rango n con base $\mathcal{B}$ e minimi $\lambda_1, \dots, \lambda_n$ allora esistono $v_1 \dots v_n \in \mathcal{L}$ lin. ind. t.c. $\|v_i\| = \lambda_i \ \forall i$

<u>Dim.</u> Proviamo che $\lambda_1 > 0$.

Consideriamo $\mathcal{B}^*$ l'ortogonalizzazione di $\mathcal{B}$.

e proviamo che $\lambda_1 \geq \min \|b_i^*\| > 0$

Sia $v = B\underline{x}$, $x \in \mathbb{Z}^n$, $x \neq 0$ un el. di $\mathcal{L}$

Sia $i = \max\{j \mid x_j \neq 0\}$ e proviamo che

$\|Bx\| \geq \|b_i^*\|$ così $\|Bx\| \geq \min_j \|b_j^*\|$

e $\lambda_1 = \inf \|Bx\| \geq \min_j \|b_j^*\| > 0$

Consideriamo:

$$(Bx, b_i^*) = \left(\sum_1^n (x_j b_j), b_i^*\right) = \sum_{j=1}^{i} x_j (b_j, b_i^*) =$$

$$= x_i (b_i, b_i^*) = x_i\left(b_i^* + \sum_{j<i} \mu_{ij} b_j^*, b_i^*\right) =$$

$$= x_i (b_i^*, b_i^*) = x_i \|b_i^*\|^2$$

Da cui

$$\|Bx\| \cdot \|b_i^*\| \geq |(Bx, b_i^*)| \geq |x_i| \cdot \|b_i^*\|^2 \geq \|b_i^*\|^2$$

Proviamo ora che esiste $v \in \mathcal{L}$ t.c $\|v\| = \lambda_1$

per definizione $\exists \{v_i\}$ t.c. $\lim_{i\to\infty} \|v_i\| = \lambda_1 > 0$

allora per $i >> 0$ $\|v_i\| \leq 2\lambda_1$ e quindi

$v_i \in B(0, 2\lambda_1)$ che è compatto quindi

esiste una sottosuccessione $\{v_{i_j}\}$ convergente

$w = \lim_{j\to\infty} v_{i_j}$ e $\|w\| = \lim_j \|v_{i_j}\| = \lambda_1$.

Per concludere dobbiamo provare che $w \in \mathcal{L}$

per $j >> 0$ $\|v_{i_j} - w\| < \lambda_1/2$ e quindi per $k > j >> 0$

$$\|v_{i_j} - v_{i_k}\| \leq \|v_{i_j} - w\| + \|v_{i_k} - w\| < \lambda_1$$

$\in \mathcal{L}$ $\Rightarrow$ $v_{i_j} - v_{i_k} = 0$ $\forall k > j$ $\Rightarrow \lim_k v_{i_k} = w = v_{i_j} \in \mathcal{L}$.

finire per esercizio per λ_i, $i > 1$.

—

Precisiamo ora il concetto di base "buona", ossia con vettori corti e quasi ortogonali e cerchiamo degli algoritmi per calcolarla.

Se $n=2$ vedremo che si può costruire (Gauss (Gauss-Legendre)) una base $\{b_1, b_2\}$ t.c. $\|b_1\| = \lambda_1$ e $\|b_2\| = \lambda_2$

se $n>2$ LLL - ma in questo caso non riusciremo a trovare $v \in \mathcal{L}$ t.c $\|v\| = \lambda_1$ ma solo una sua approssimazione

—

Sia $n=2$ e consideriamo $\mathcal{B}=\{b_1, b_2\}$ e $\mathcal{L}=\mathcal{L}(\mathcal{B})$.

∴ Trovare una base $\mathcal{B}_{\text{rid.}}=\{b_1', b_2'\}$ t.c.

$$\|b_1'\| = \lambda_1 \quad e \quad \|b_2'\| = \lambda_2 . \quad (*)$$

<u>Oss.</u> In questo modo risolviamo <u>SVP</u>

Caratterizziamo le basi "buone":

<u>Def.</u> Una base $\{b_1, b_2\}$ ordinata è L-G ridotta se:

$$\|b_1\| \le \|b_2\| \le \|b_2 + q b_1\| \quad \forall q \in \mathbb{Z}$$

Si ha:

<u>Prop.</u> Una base è L-G ridotta $\Longleftrightarrow$

$$\|b_1\| \le \|b_2\| \le \|b_2 \pm b_1\|$$

<u>Dim.</u> $\Rightarrow$ ovvio $(q = \pm 1)$

$\Leftarrow$ supponiamo $\|b_2\| \le \|b_2 \pm b_1\|$

allora $\|b_2\|^2 \le \|b_2 \pm b_1\|^2 = \|b_1\|^2 + \|b_2\|^2 \pm 2(b_1, b_2)$

$$\Rightarrow \|b_1\|^2 \pm 2(b_1, b_2) \ge 0$$

Se consideriamo $F(x) = \|b_2 + x b_1\|^2$

$F(x)$ ha minimo per $x_0 = -\dfrac{(b_1, b_2)}{\|b_1\|^2}$

e quindi $-1 < x_0 < 1 \Rightarrow$

$$\|b_1\| \le \|b_2\| \le \|b_2 + q b_1\| \quad \forall q \in \mathbb{Z}$$

—

Proviamo ora che i vettori di una base L-G ridotta sono i più corti possibili

<u>Th</u> Siano λ_1, λ_2 i due minimi successivi di $\mathcal{L}$. $\mathcal{B} = \{b_1, b_2\}$ è una base (<u>ordinata</u>) G-L ridotta di $\mathcal{L}$ $\Rightarrow$ $\|b_1\| = \lambda_1$ e $\|b_2\| = \lambda_2$

<u>Dim.</u> Vale $\|b_1\| \le \|b_2\| \le \|b_2 + q b_1\| \quad \forall q \in \mathbb{Z}$

Sia $v \neq 0$, $v \in \mathcal{L}$, $v = a_1 b_1 + a_2 b_2$, $a_1, a_2 \in \mathbb{Z}$

1. Se $a_2 = 0 \Rightarrow \|v\| = |a_1| \cdot \|b_1\| \ge \|b_1\|$
2. Se $a_2 = 0$ dividiamo a_1 per a_2 $\quad a_1 = q a_2 + r$

   con $0 \le r < |a_2|$

   Allora $v = r b_1 + a_2 (b_2 + q b_1) \Rightarrow$

$$\|v\| \ge |a_2| \, \|b_2 + q b_1\| - r \|b_1\| = (|a_2| - r)\|b_2 + q b_1\| + r(\|b_2 + q b_1\| - \|b_1\|)$$

$$\ge \|b_2 + q b_1\| \ge \|b_2\| \ge \|b_1\| \quad \boxtimes$$

Oss. Dal momento che $F(x) = \|b_2 - q b_1\|^2$ ha minimo in $x_0 = \frac{(b_1, b_2)}{\|b_1\|^2}$

se sostituiamo:

$$b_2 \longrightarrow b_2 - \lfloor x_0 \rceil b_1 \quad \text{(parte intera)}$$

riduciamo la lunghezza di b_2.

Algoritmo

Input: $\mathcal{B} = \{b_1, b_2\} \subset \mathbb{Z}^2$ base per $\mathcal{L}$, $\|b_1\| \le \|b_2\|$

Output: Base ridotta L-G per $\mathcal{L}$

1. $\beta_1 := \|b_1\|^2$
2. $\mu := \frac{(b_1, b_2)}{\beta_1}$
3. $b_2 := b_2 - \lfloor \mu \rceil b_1$
4. $\beta_2 := \|b_2\|^2$
5. while $\beta_2 < \beta_1$ repeat
   - $(b_1, b_2) := (b_2, b_1)$ scambia
   - $\beta_1 := \beta_2$
   - $\mu := \frac{(b_1, b_2)}{\beta_1}$
   - $b_2 := b_2 - \lfloor \mu \rceil b_1$
   - $\beta_2 := \|b_2\|^2$

$\rightarrow (b_1, b_2)$