

PARTE 2

17/12/2020
T.P.

③ ALGORITMO LLL

④ ADAPTANDO O LLL PARA CÓDIGOS

RECAPITULAÇÃO DO SEMINÁRIO PASSADO

- DEFINIMOS RETICULADOS $\mathcal{L}(B) = \{B \cdot v : v \in \mathbb{Z}^n\}$
- PARA QUALQUER MATRIZ UNIMODULAR U : $\mathcal{L}(B) = \mathcal{L}(BU)$
- VIMOS QUE HÁ BASES Boas e Ruins
+ ortogonais
- DEFINIMOS OS MÍNIMOS SUCESSIVOS $\lambda_1(\mathcal{L}), \dots, \lambda_n(\mathcal{L})$
- DEFINIMOS BASE LAGRANGE-REDUZIDA EM DIM. 2
- VIMOS QUE É FÁCIL ENCONTRAR BASE BOA EM DIM 2
ALG. DE LAGRANGE

③ ALGORITMO LLL DE LENSTRA-LENSTRA-LOVÁSZ

- É um algoritmo que encontra uma base reduzida
- Não encontra a melhor base possível, apenas aprox.
- Se LLL devolver base $\{b_1, \dots, b_n\}$ de $\mathcal{L}$, então

$$\|b_1\| \leq \underbrace{2^{(n-1)/2}}_{\text{fator de aprox. exponencial}} \cdot \lambda_1(\mathcal{L})$$

$$\|b_j\| \leq 2^{(n-1)/2} \cdot \lambda_i \text{ para } 1 \leq j \leq i \leq n$$

PROPRIEDADES DO GSO (GRAM-SCHMIDT ORTHOGONALIZATION)

LEMA (17.2.2 GALBRAITH) Sejam $\{b_1, \dots, b_n\}$ l.i. em $\mathbb{R}^m$ e $\{b_1^*, \dots, b_n^*\}$ o resultado de GSO($b_1, \dots, b_n$). Então

$$\textcircled{i} \quad \|b_i^*\| \leq \|b_i\| \quad \text{para } 1 \leq i \leq n.$$

$$\textcircled{ii} \quad \langle b_i, b_i^* \rangle = \langle b_i^*, b_i^* \rangle \quad \text{para } 1 \leq i \leq n$$

① $\|b_i^*\| \leq \|b_i\|$ para $1 \leq i \leq n$.

DEM CASO $i=1 \Rightarrow b_i^* = b_i = b_1 = b_i \Rightarrow \|b_i^*\| = \|b_i\|$

CASO $i > 1$. $b_k^* = b_k - \sum_{j < k} \frac{\langle b_k, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} b_j^*$ S

$$\|b_k^*\|^2 = \langle b_k^*, b_k^* \rangle = \langle b_k - S, b_k - S \rangle$$

$$= \langle b_k - S, b_k \rangle - \langle b_k - S, S \rangle$$

b_k^*, S são $\perp$

$$= \langle b_k - S, b_k \rangle - 0$$

$$= \langle b_k, b_k \rangle - \langle S, b_k \rangle$$

Mas S é proj. de b_k , então $\langle S, b_k \rangle = \langle b_k, S \rangle \geq 0$.

Formalmente ... $\rightarrow$

Formalmente:

$$\langle b_k, S \rangle = \left\langle b_k, \sum_{j < k} \frac{\langle b_k, b_j^* \rangle}{\|b_j^*\|^2} \cdot b_j^* \right\rangle$$

Assoc.

$$= \sum_{j < k} \left\langle b_k, \frac{\langle b_k, b_j^* \rangle}{\|b_j^*\|^2} \cdot b_j^* \right\rangle$$

$$= \sum_{j < k} \left(\frac{\langle b_k, b_j^* \rangle}{\|b_j^*\|^2} \right) \langle b_k, b_j^* \rangle$$

$$= \sum_{j < k} \underbrace{\frac{\langle b_k, b_j^* \rangle^2}{\|b_j^*\|^2}}_{\geq 0} \geq 0$$

□

$$\textcircled{ii} \quad \langle b_i, b_i^* \rangle = \langle b_i^*, b_i^* \rangle \text{ para } 1 \leq i \leq n$$

$$\begin{aligned} \langle b_i^*, b_i^* \rangle &= \langle b_i - s, b_i - s \rangle = \underbrace{\langle b_i, b_i - s \rangle} - \underbrace{\langle s, b_i - s \rangle} \\ &= \langle b_i, b_i^* \rangle - \underbrace{0}_{\text{?}} \end{aligned}$$

Note que $\langle s, b_i - s \rangle = \langle s, b_i \rangle - \langle s, s \rangle$

$$\langle s, s \rangle = \|s\|^2 = \left\| \sum_{j < i} \underbrace{\frac{\langle b_i, b_j^* \rangle}{\|b_j\|}}_{\substack{\|\cdot\|=1 \\ \text{orthonormal}}} \frac{b_j^*}{\|b_j^*\|} \right\|^2 = \sum_{j < i} \left(\frac{\langle b_i, b_j^* \rangle}{\|b_j\|} \right)^2$$

Mas, do slide anterior:

$$\langle s, b_i \rangle = \sum_{j < i} \frac{\langle b_i, b_j^* \rangle^2}{\|b_j^*\|^2} \Rightarrow \langle s, b_i \rangle - \langle s, s \rangle = 0 \quad \square$$

BASE LLL-REDUZIDA

DEF Seja $(b_1, \dots, b_n)$ base de $\mathcal{L}$ e $(b_1^*, \dots, b_n^*)$ sua ortogonalização por Gram-Schmidt. Sejam
 $\mu_{i,j} = \langle b_i, b_j^* \rangle / \langle b_j^*, b_j^* \rangle$ os coeficientes de GS.

FIXE um valor δ tal que $\frac{1}{4} < \delta < 1$.

ENTÃO $(b_1, b_2, \dots, b_n)$ é LLL-Reduzida se valem

(i) Tamanho Reduzido

$$|\mu_{i,j}| \leq \frac{1}{2} \quad \forall 1 \leq j < i \leq n.$$

(ii) Condição de Lovász

$$\|b_i^*\|^2 \geq (\delta - \mu_{i,i-1}^2) \|b_{i-1}^*\|^2 \quad \forall 2 \leq i \leq n$$

Tipicamente se usa $\delta = 3/4$.

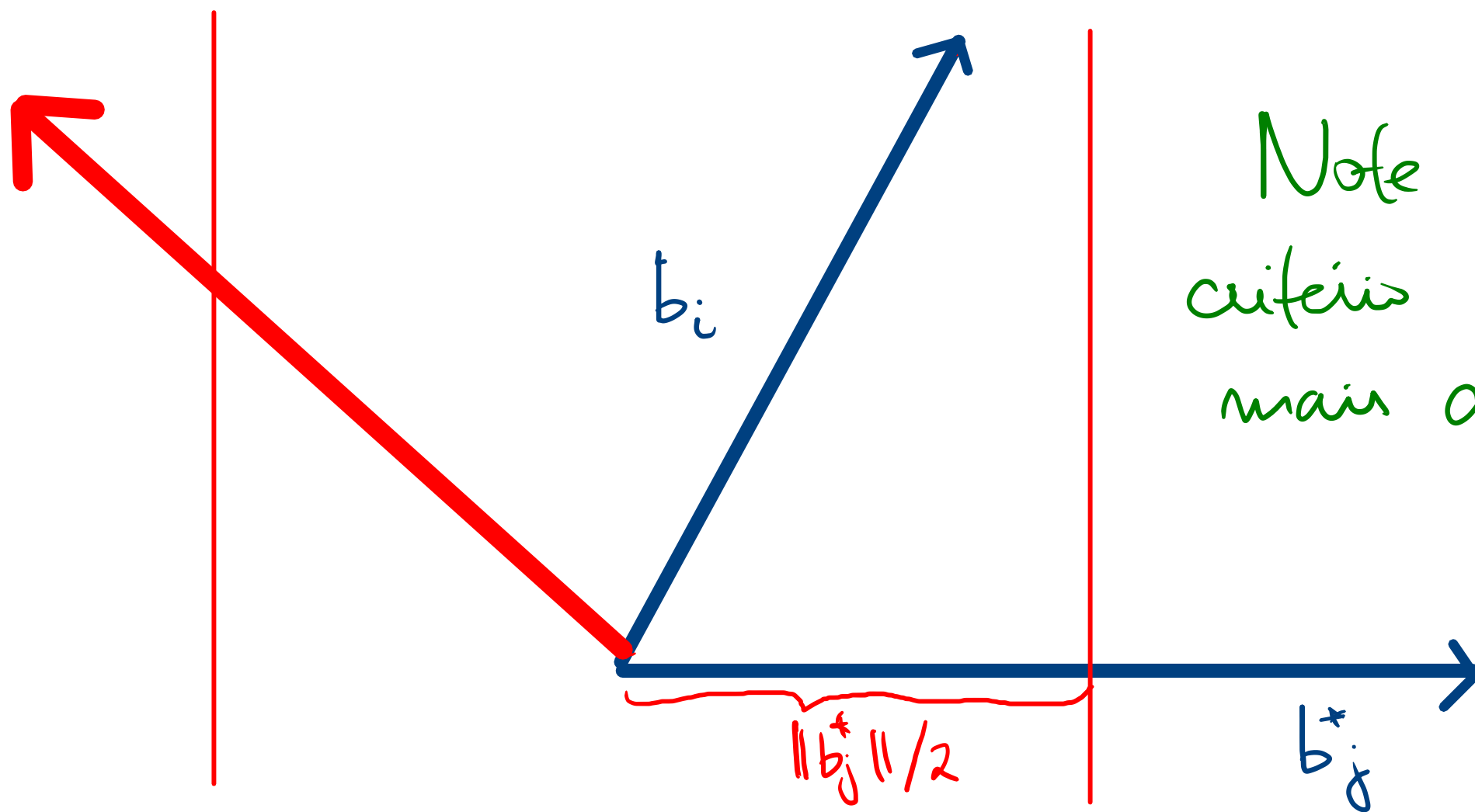
TAMANHO REDUZIDO $|M_{ij}| \leq 1/2 \quad \forall 1 \leq j < i \leq n.$

$$M_{ij} = \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}$$

$$\Rightarrow |\langle b_i, b_j^* \rangle| \leq \frac{\|b_j^*\|^2}{2}$$

$$\Rightarrow \|b_i\| \|b_j^*\| |\cos \theta| \leq \frac{\|b_j^*\|^2}{2}$$

$$\Rightarrow \|b_i\| |\cos \theta| \leq \frac{\|b_j^*\|}{2}$$



Note como parece o
critério de Lagrange em
mais dimensões

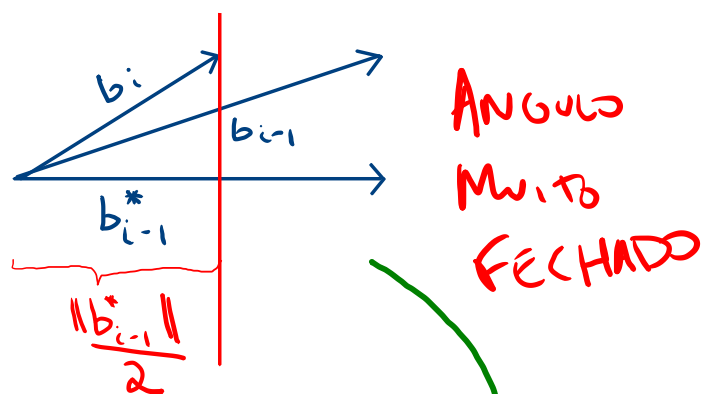
CONDICÃO DE LOVÁSZ

$$\|b_i^*\|^2 \geq (\delta - \mu_{i,i-1}^2) \|b_{i-1}^*\|^2 \quad \forall 2 \leq i \leq n$$

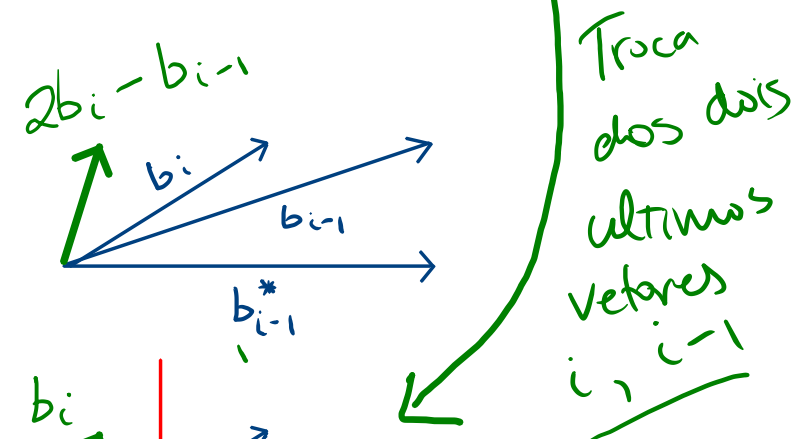
$$\mu_{i,i-1} = \frac{\|b_i\| \cos \theta}{\|b_{i-1}^*\|} \text{ mede o ângulo entre } b_i \text{ e } b_{i-1}^*$$

Combinada com restrição (i), temos para $\delta=1$ que

$$\|b_i^*\|^2 \geq (1 - \mu_{i,i-1}^2) \|b_{i-1}^*\|^2$$



Ângulo
Muito
FECHADO



Troca
dos dois
ultimos
vetores
 $i, i-1$

Se angulo entre b_i e b_{i-1}^*

for muito pequeno ($\mu_{i,i-1} \approx 1$),

$\Rightarrow$ vai aceitar b_i se b_i^* for

NÃO FOR EXTREMAMENTE PEQUENO

$$\|b_i^*\|^2 \geq \epsilon \|b_{i-1}^*\|^2$$

LEMA Seja $(b_1, \dots, b_n)$ uma base de $\mathcal{L}$ LLL-reduzida com $\delta = 3/4$. Então

$$\textcircled{i} \quad \|b_j^*\| \leq 2^{i-j} \|b_i^*\| \quad \forall 1 \leq j \leq i \leq n$$

$$\|b_j^*\| \leq 2^{i-j} \|b_i^*\| \quad \forall 1 \leq j \leq i \leq n$$

DEM. Pela condição de Lovász, $\|b_i^*\|^2 \geq (\delta - \mu_{i,i-1}^2) \|b_{i-1}\|^2$

Mas a condição de base reduzida garante que $\mu_{i,j} \leq \frac{1}{2}$

$$\Rightarrow \|b_i^*\|^2 \geq \left(\frac{3}{4} - \frac{1}{4}\right) \|b_{i-1}\|^2$$

$$\Rightarrow \underbrace{\|b_i^*\|^2}_i \geq 2^{-1} \underbrace{\|b_{i-1}\|^2}_j$$

Por indução então, para $i > j$

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

□

LEMA Seja $(b_1, \dots, b_n)$ uma base qualquer de reticulado $\mathcal{L}$. Então $\lambda_1(\mathcal{L}) \geq \min_{1 \leq i \leq n} \|b_i^*\|$

DEM Tome um vetor qualquer $x \in \mathbb{Z}^n$, com $x \neq 0$.

Seja i a maior coordenada tq $x_i \neq 0$. Mostremos que $\|xB\| \geq \|b_i^*\|$.

$$\langle xB, b_i^* \rangle = \left\langle \sum_{j=1}^i x_j b_j, b_i^* \right\rangle = \sum_{j=1}^i x_j \underbrace{\langle b_j, b_i^* \rangle}_{0 \text{ para } j \neq i}$$

$$\text{Mas } b_i^* \perp \text{span}(b_1, \dots, b_{i-1}) \Rightarrow \langle xB, b_i^* \rangle = x_i \langle b_i, b_i^* \rangle$$

$$\langle xB, b_i^* \rangle \stackrel{\text{Lema}}{=} x_i \langle b_i^*, b_i^* \rangle = x_i \|b_i^*\|^2$$

$$\text{Mas } \|xB\| \leq \frac{\langle xB, b_i^* \rangle}{\|b_i^*\|} = x_i \|b_i^*\| \quad \square$$

TEOREMA. Seja $(b_1, b_2, \dots, b_n)$ uma base LLL-reduzida, com $\delta = 3/4$. Então $\|b_1\| \leq 2^{(n-1)/2} \lambda_1(\mathcal{L})$

DEM. Pelos LEMAS ANTERIORES $\|b_i^*\| \geq 2^{\delta^i} \|b_j^*\|$.

Para $i=1$, temos $\|b_i^*\| \geq 2^{\frac{1-i}{2}} \|b_j^*\|$

$$\begin{aligned} \lambda_1(\mathcal{L}) &\geq \min_{1 \leq i \leq n} \|b_i^*\| \\ &\geq \min_{1 \leq i \leq n} 2^{\frac{1-i}{2}} \|b_1^*\| = b_1 \\ &= 2^{\frac{(1-n)}{2}} \|b_1\| \end{aligned}$$

$$\Rightarrow \|b_1\| \leq 2^{\frac{(n-1)}{2}} \lambda_1(\mathcal{L}) \quad \square$$

