ADAPTANDO O LLL PARA CÓDIGOS BINÁRIOS

Resumo do artigo "An algorithm reduction theory for binary codes: LLL and more", T. Debris-Alazar et al.

Sumário

(I) RETICULADOS

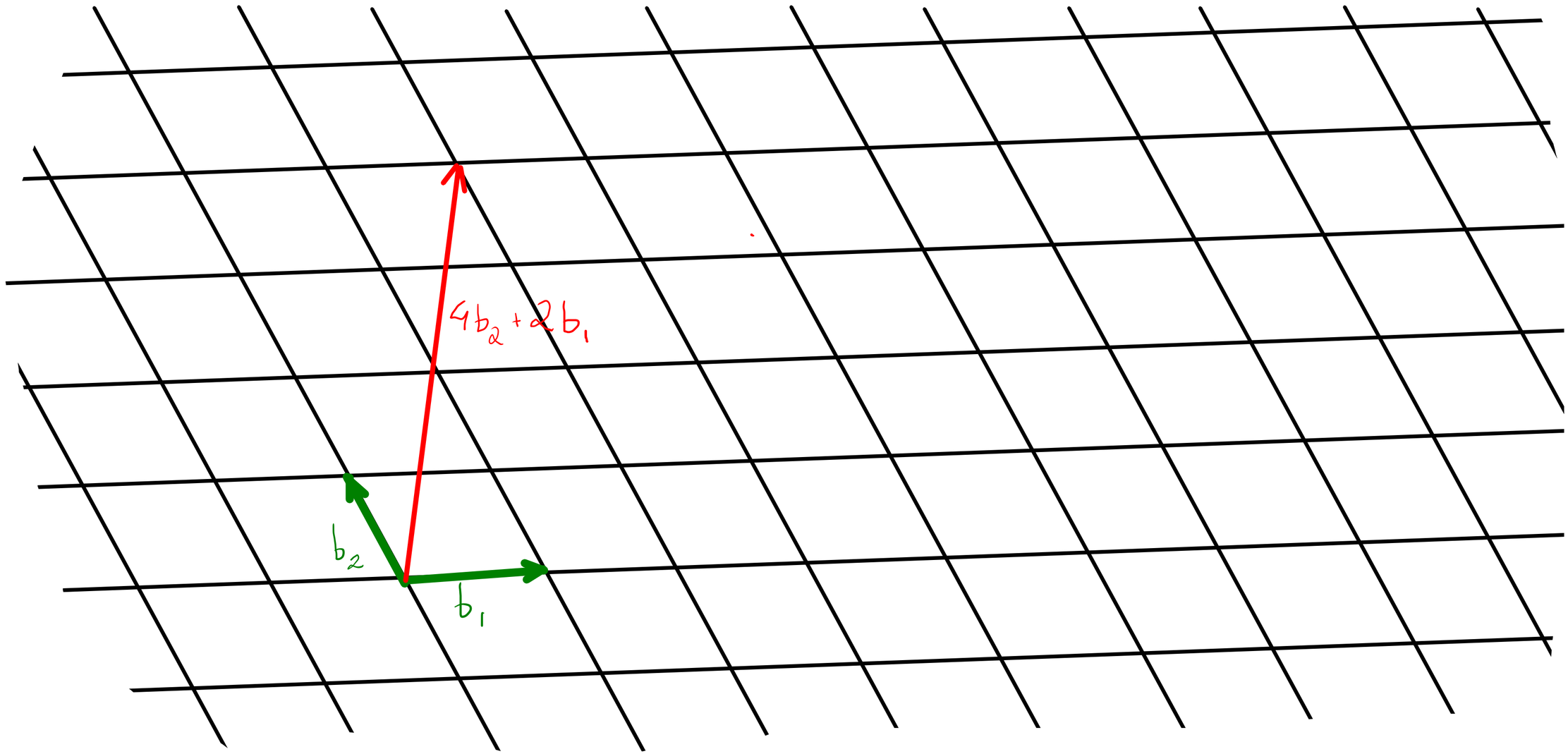
DEF Sejam $b_1, b_2, \dots, b_n \in \mathbb{R}^n$, e matriz $B \in \mathbb{R}^{n \times n}$.
Então o reticulado gerado por B é o conjunto

$$\mathcal{L}(B) = \{ Bx : x \in \mathbb{Z}^n \}$$

$$= \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}$$

Ou seja, $\mathcal{L}(B)$ é o conjunto de combinações lineares inteiras dos vetores da base.

EXEMPLOS



BASES

- Um reticulado (não nulo) tem infinitas bases.

Em particular, para qualquer matriz unimodular U,

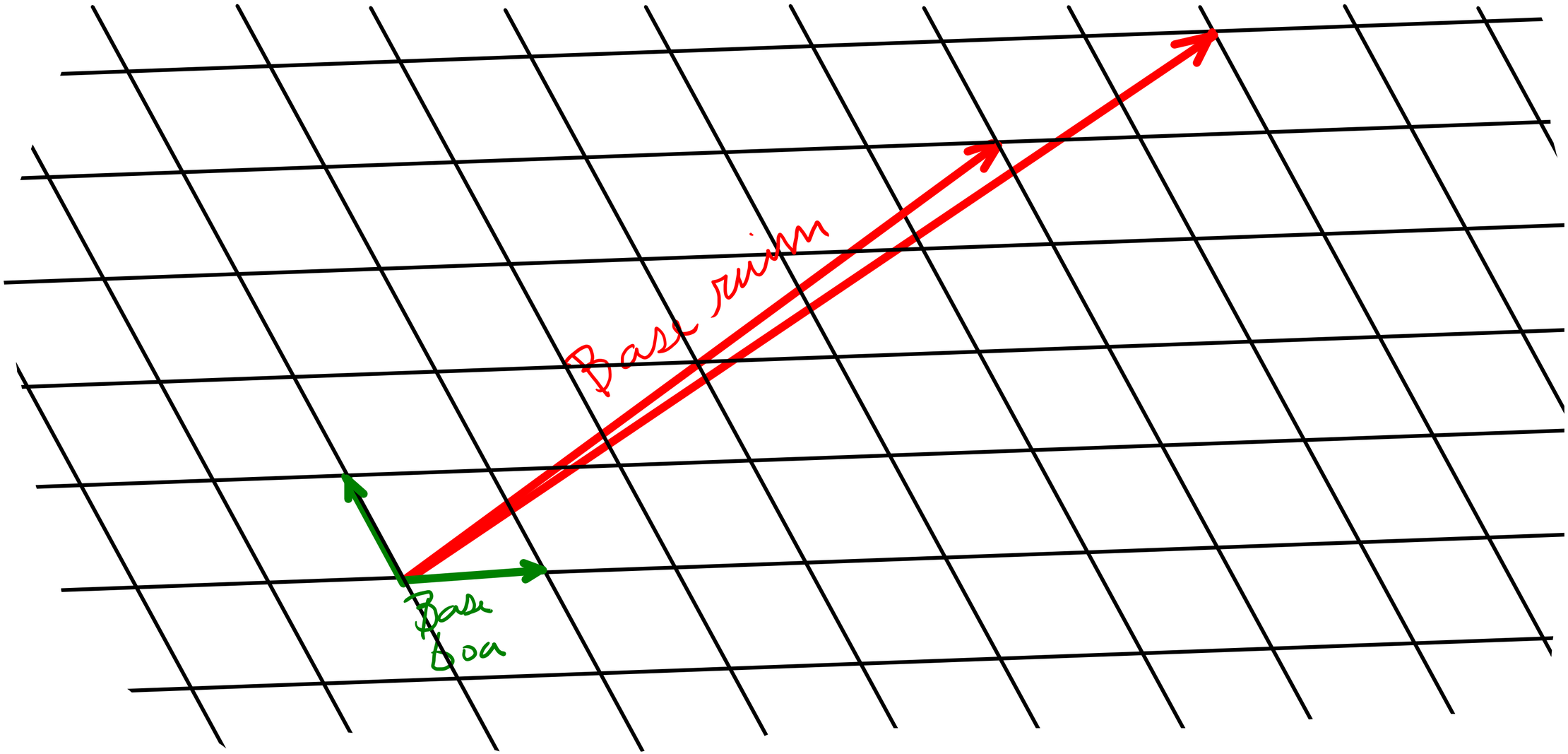
$$\mathcal{L}(B) = \mathcal{L}(UB),$$

portanto UB é uma base de $\mathcal{L}(B)$.

DEF $\underline{U \in \mathbb{Z}^{n \times n}}$ é unimodular se $\det(U) = \pm 1$.

$$\Rightarrow \{Uz : z \in \mathbb{Z}^n\} = \mathbb{Z}^n$$

Bases Boas e Bases Ruins



Bases Boas e Bases Ruins

· Embora todas as bases gerem o mesmo reticulado, elas não são "algoritmicamente" equivalentes

· Bases mais ortogonais podem ser usadas para resolver problemas importantes de reticulados, como o Closest Vector Problem (CVP)

· Além disso, é computacionalmente difícil achar uma base boa a partir de uma ruim

→ Esta assimetria é muito usada em cripto

Mínimos Sucessivos

DEF: O i-ésimo mínimo é o real

$$\lambda_i(\mathcal{L}) = \inf\{r : \dim(\mathrm{span}(\mathcal{L} \cap \mathrm{Ball}(0,r))) \geq i\}$$

(min)

Ou seja, é o menor raio r tal que $\mathrm{Ball}(0,r)$ contém i pontos do reticulado linearmente independentes

(II) Redução de Bases

Problema: Dada uma base $\hat{B}$ de um reticulado

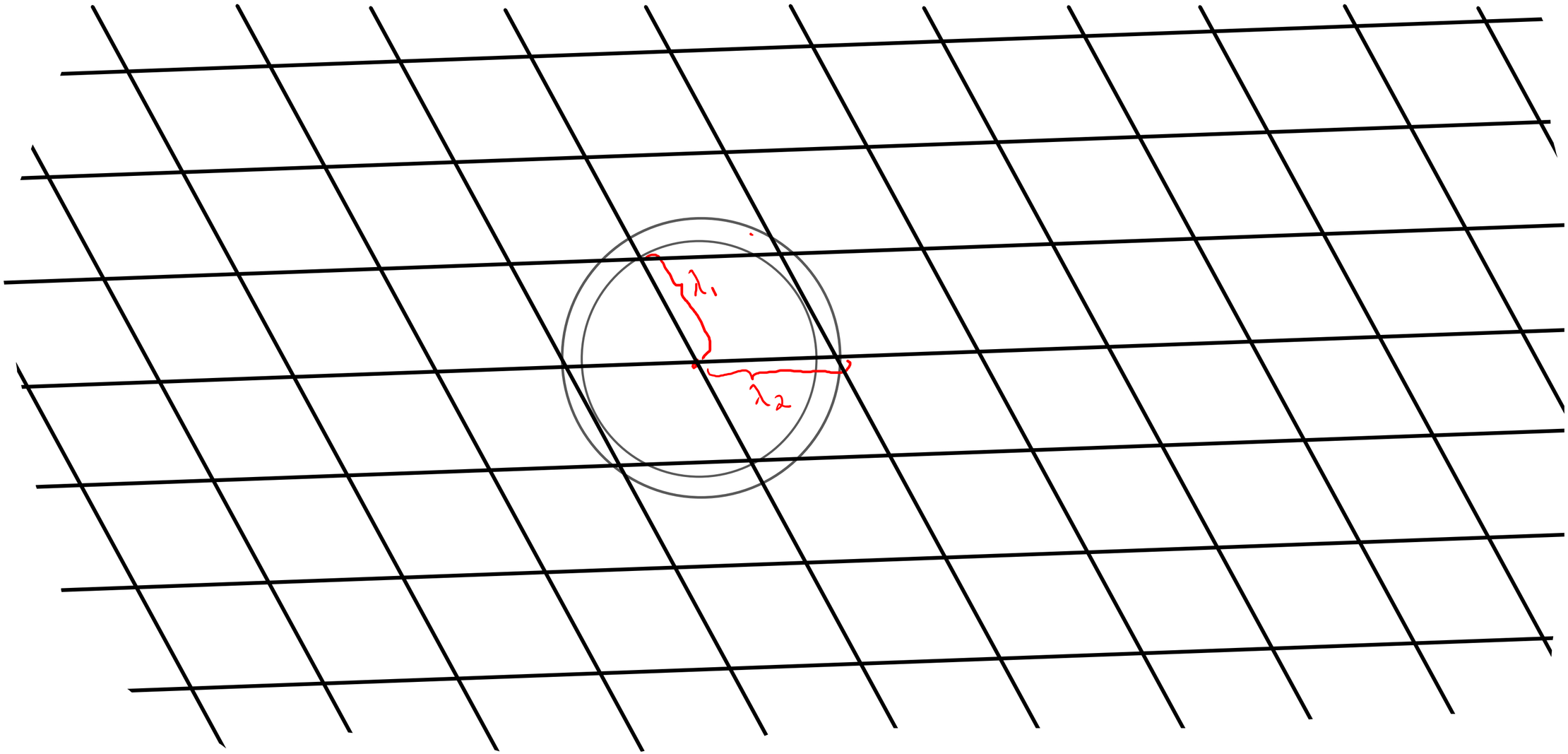
Encontrar uma base $B = [b_1, b_2, \cdots, b_m]$ tal que

$$\|b_1\| \approx \lambda_1(\mathcal{L})$$

$$\vdots$$

$$\|b_m\| \approx \lambda_m(\mathcal{L})$$

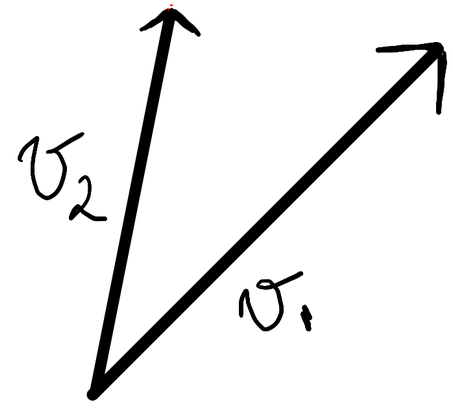
Exemplo

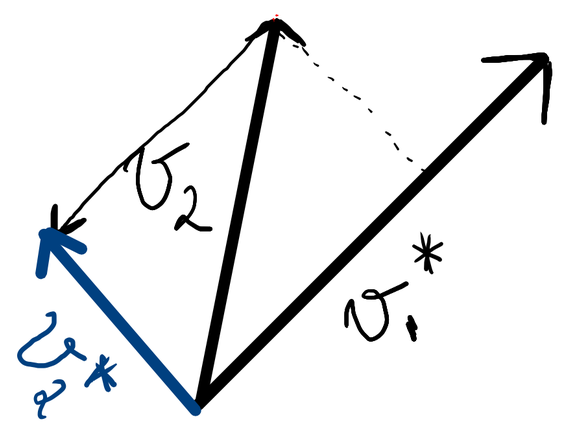


IDEIA BÁSICA: GRAM-Schmidt

Dada uma base $B = [b_1, b_2, \dots, b_n]$,

$$\begin{cases} b_1^* = b_1 \\ b_i^* = b_i - \sum_{j<i} \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|} b_j^* \end{cases}$$





PROBLEMA os b_i^* podem não fazer parte do reticulado

De certa forma, b_i^* dão o menor tamanho que podemos esperar de uma base. Formalmente

$$\lambda_1(\mathcal{L}) \geq \min_i \|b_i^*\|, \text{ para a ortogonalização de qualquer base } B.$$

$([b_1^*, \dots, b_n^*] \leftarrow GSO(B))$

VER DEMONSTRAÇÃO NO LIVRO DO MICCIANCIO (THEO 1.1)

Para achar vetores curtos EM $\mathcal{L}$, precisamos ser um pouco mais espertos

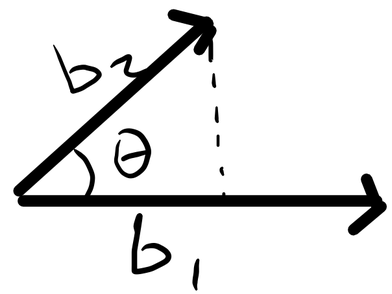
Caso $n = 2$

- Neste caso, é fácil encontrar uma base (b_1, b_2) tal que $\|b_1\| = \lambda_1$ e $\|b_2\| = \lambda_2$
- Usamos o algoritmo de Lagrange, que é uma generalização do alg. de Euclides para duas dimensões

DEF: Seja L um reticulado. Uma base (b_1, b_2) de L é dita ser Lagrange reduzida sse $\begin{cases} \|b_1\| \leq \|b_2\|, \text{ e} \\ |\langle b_1, b_2 \rangle| \leq \frac{\|b_1\|^2}{2} \end{cases}$

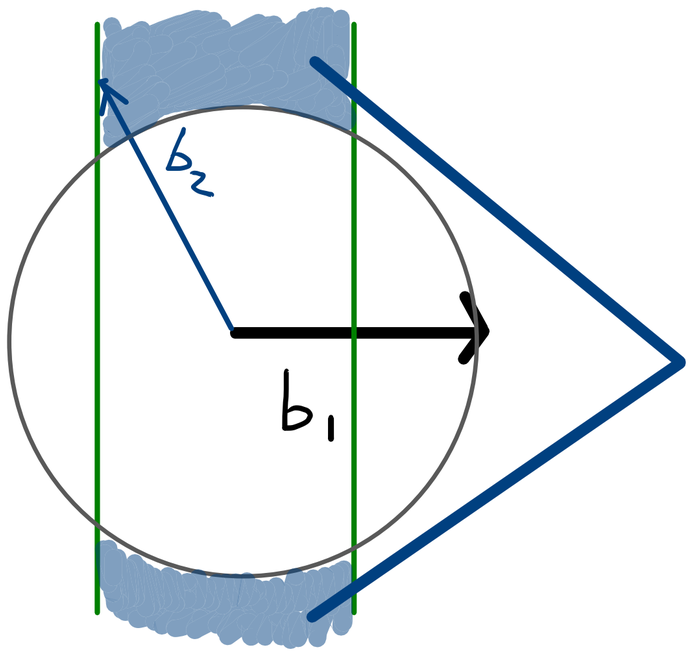
INTERPRETAÇÃO GEOMÉTRICA

$$\langle b_1, b_2 \rangle = \|b_1\| \, \|b_2\| \cos\theta$$



$$\Rightarrow \frac{\langle b_1, b_2 \rangle}{\|b_1\|} = \|b_2\| \cos\theta = \text{tamanho da projeção de } b_2 \text{ em } b_1$$

Assim, $\mathcal{L}$-reduzida se e somente se $\begin{cases} \|b_1\| \leq \|b_2\| \\ |\|b_2\| \cos\theta| \leq \dfrac{\|b_1\|}{2} \end{cases}$



Áreas em que b_2 deve estar

(ângulo entre 60° e 120°)

CARACTERIZAÇÃO ALTERNATIVA

TEO: (b_1, b_2) é $\mathcal{L}$-reduzida sse $\|b_1\| \leq \|b_2\| \leq \|b_2 + kb_1\|$, $\forall k \in \mathbb{Z}$

DEM: Pela Lei dos cossenos, sabemos que

$$\|b_2 + kb_1\| = \sqrt{\|b_2\|^2 + |k|\|b_1\|^2 - 2k\langle b_1, b_2\rangle}$$

$\Rightarrow$ Sup que (b_1, b_2) é $\mathcal{L}$-reduzida. Então $\begin{cases} \|b_1\| \leq \|b_2\| \\ |\langle b_1, b_2\rangle| \leq \frac{\|b_1\|^2}{2} \end{cases}$

Portanto

$$\|b_2\|^2 + |k|\|b_1\|^2 - 2k\langle b_1, b_2\rangle \geq \|b_2\|^2 + |k|\|b_1\|^2 - \frac{2|k|\|b_1\|^2}{2}$$

$$\Rightarrow \|b_2 + kb_1\| \geq \|b_2\| \quad \forall k \in \mathbb{Z}.$$

continua →

(⇐) Suponha agora que $\|b_1\| \leq \|b_2\| \leq \|b_2 + kb_1\| \ \forall k \in \mathbb{Z}$.

Caso (i) $\langle b_1, b_2 \rangle > 0$. Então, tomando $k = 1$

$\|b_2 + kb_1\| \geq \|b_2\| \Rightarrow \|b_2\|^2 + |k|\|b_1\|^2 - 2k\langle b_1, b_2 \rangle \geq \|b_2\|^2$

$\Rightarrow \|b_1\|^2 - 2\langle b_1, b_2 \rangle \geq 0 \Rightarrow |\langle b_1, b_2 \rangle| \leq \frac{\|b_1\|^2}{2}$

Caso (ii) $\langle b_1, b_2 \rangle < 0$. Então tomando $k = -1$

$\|b_2\|^2 + |k|\|b_1\|^2 - 2k\langle b_1, b_2 \rangle \geq \|b_2\|^2$

$\Rightarrow -\langle b_1, b_2 \rangle \leq \frac{\|b_1\|^2}{2} \Rightarrow |\langle b_1, b_2 \rangle| \leq \frac{\|b_1\|^2}{2}$ ∎

Teo (b_1, b_2) é $\mathcal{L}$-reduzida sse $\|b_1\| = \lambda_1(\mathcal{L})$ e $\|b_2\| = \lambda_2(\mathcal{L})$

DEM (b_1, b_2) é $\mathcal{L}$-reduzida, então $\|b_1\| \leq \|b_2\| \leq \|b_2 + k b_1\| \ \forall k \in \mathbb{Z}$

Seja $v = l_1 b_1 + l_2 b_2 \neq \mathbf{0}$ um ponto qualquer do reticulado

Se $l_2 = 0 \Rightarrow v = l_1 b_1 \Rightarrow \|v\| \geq \|b_1\|$

Se $l_2 \neq 0 \Rightarrow$ Podemos escrever $l_1 = q l_2 + r$ com $\begin{cases} q, r \in \mathbb{Z} \\ 0 \leq r < |l_2| \end{cases}$

$$\Rightarrow v = r b_1 + l_2 (q b_1 + b_2)$$

Lembre da desigualdade triangular

$\bar{a} = a - b$

$\|a\| + \|b\| \geq \|a + b\| \Rightarrow \|a\| \geq \|a+b\| - \|b\| \Rightarrow \|\bar{a} + b\| \geq \|\bar{a}\| - \|b\|$

continua

$$\Rightarrow \|v\| = \|\underbrace{r\hat{b}_1 + l_2(qb_1 + b_2)}_{=\lambda}\| \geq \|l_2(qb_1+b_2)\| - \|-rb_1\|$$

$$= |l_2|\,\|qb_1+b_2\| - r\|b_1\|$$

$$\Rightarrow \|v\| \geq (|l_2| - r)\,\|b_2 + qb_1\| + r(\|b_2 + qb_1\| - \|b_1\|)$$

$(|l_2| - r) > 0$

$(\|b_2 + qb_1\| - \|b_1\|) \geq \|b_1\| \geq 0$

$$\geq \|b_2 + qb_1\| \geq \|b_2\| \geq \|b_1\|$$

Então $\|b_1\| \leq \|v\|\ \forall v \Rightarrow \|b_1\| = \lambda_1$

$\|b_2\| \leq \|v\|\ \forall v$ l.i. a $b_1 \Rightarrow \|b_2\| = \lambda_2$

∎

ALGORITMO DE LAGRANGE

ENTRADA: Base $(b_1, b_2) \in \mathbb{Z}^2$ de reticulado $\mathcal{L}$

SAÍDA: Base (b_1, b_2) tais que $\|b_1\| = \lambda_1$ e $\|b_2\| = \lambda_2$

$\mu \leftarrow \langle b_1, b_2 \rangle / \|b_1\|^2$

$b_2 \leftarrow b_2 - \lfloor \mu \rceil b_1$

while $\|b_2\|^2 < \|b_1\|^2$:

$b_1, b_2 \leftarrow b_2, b_1$

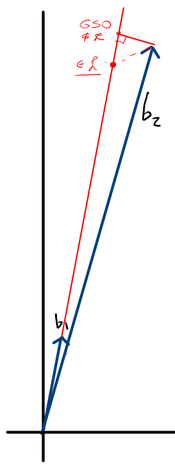
$\mu \leftarrow \langle b_1, b_2 \rangle / \|b_1\|^2$

$b_2 \leftarrow b_2 - \lfloor \mu \rceil b_1$

return (b_1, b_2)

EXEMPLO $b_1 = (1,5)$, $b_2 = (6,21)$

GALBRAITH CAP 17



$\mu = \frac{(1.6+5.21)}{(1+5^2)}$

$= \frac{111}{26} \approx 4.27$

$b_2 \leftarrow (6,21) - \lfloor 4.27 \rceil (1,5)$

$= (6,21) - (4,20)$

$= (2,1)$

$\|b_1\| = \sqrt{26}$

$\|b_2\| = \sqrt{5}$ $\Rightarrow \|b_2\| < \|b_1\|$

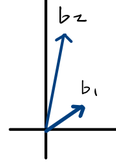
troca b_1 e b_2

$\mu = \frac{(2.1+1.5)}{5} = \frac{7}{5} = 1.4$

$b_2 = (1,5) - \lfloor 1.4 \rceil b_1$

$= (1,5) - (2,1)$

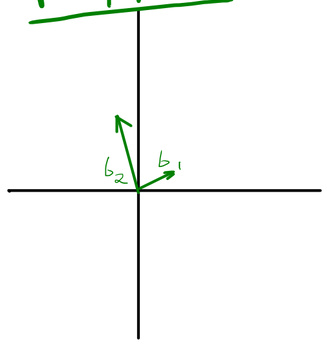
$= (-1,4)$



$\|b_1\| = \sqrt{5}$

$\|b_2\| = \sqrt{17}$

FIM



Por que o Algoritmo funciona?

- A cada iteração, $\mu = \frac{\langle b_1, b_2 \rangle}{\|b_1\|^2}$ minimiza

$$\|b_2 - \lceil \mu \rfloor b_1\|$$

Seja b_2^* o valor final e $\bar{b}_2$ o valor no início da última iteração, sabemos que

$$\|b_1\| \leq \|b_2^*\| \quad e \quad \|b_1\| \leq \|\bar{b}_2\|$$

$$b_2^* = \bar{b}_2 - \lfloor \mu \rceil b_1$$

$$\Rightarrow \|b_2^*\| \leq \|b_2^* + q b_1\| \quad \forall q \in \mathbb{Z}.$$

$\mu \leftarrow \langle b_1, b_2 \rangle / \|b_1\|^2$

$b_2 \leftarrow b_2 - \lfloor \mu \rceil b_1$

while $\|b_2\|^2 < \|b_1\|^2$:

$b_1, b_2 \leftarrow b_2, b_1$

$\mu \leftarrow \langle b_1, b_2 \rangle / \|b_1\|^2$

$b_2 \leftarrow b_2 - \lceil \mu \rfloor b_1$

return (b_1, b_2)

PRÓXIMO SEMINÁRIO:

- Generalizar para dimensão $n \to$ LLL
- Adaptar LLL para códigos binários