Reticulados: um estudo de parâmetros relevantes para aplicações em criptografia

Fábio Campos Castro Meneghetti
Orientadora: Sueli Irene Rodrigues Costa

Instituto de Matemática, Estatística e Computação Científica
Universidade Estadual de Campinas

9 de março de 2020

Sumário

Reticulados: Introdução

Definição 1.1

Seja $\beta = \{b_1, \ldots, b_k\}$ um conjunto de vetores linearmente independentes em $\mathbb{R}^n$. O *reticulado* com base β é o conjunto de todas as combinações lineares inteiras de β:

$$\Lambda(\beta) = \langle \beta \rangle_{\mathbb{Z}} = \{\alpha_1 b_1 + \cdots + \alpha_k b_k \mid \alpha_1, \ldots, \alpha_k \in \mathbb{Z}\}.$$

Dizemos que k é a *dimensão* ou *posto* do reticulado. Se $k = n$, dizemos que o reticulado tem *posto completo*.

Teorema 1.2

$\Lambda \subset \mathbb{R}^n$ é reticulado sse Λ é subgrupo aditivo discreto de $\mathbb{R}^n$.

Reticulados: Introdução

Definição 1.1

Seja $\beta = \{b_1, \ldots, b_k\}$ um conjunto de vetores linearmente independentes em $\mathbb{R}^n$. O *reticulado* com base β é o conjunto de todas as combinações lineares inteiras de β:

$$\Lambda(\beta) = \langle \beta \rangle_{\mathbb{Z}} = \{\alpha_1 b_1 + \cdots + \alpha_k b_k \mid \alpha_1, \ldots, \alpha_k \in \mathbb{Z}\}.$$

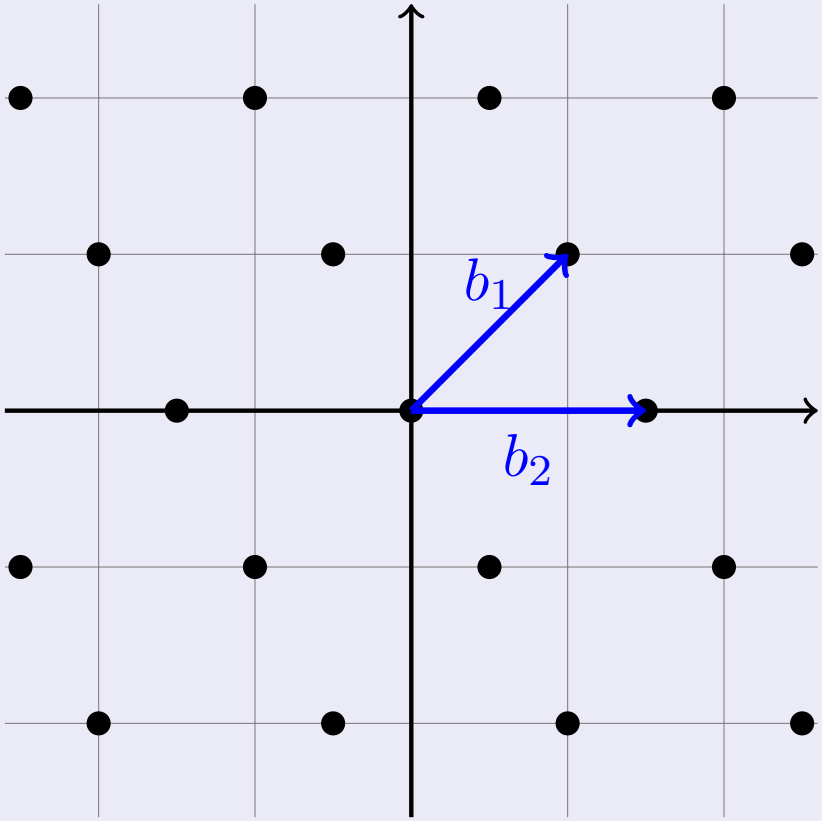
Dizemos que k é a *dimensão* ou *posto* do reticulado. Se $k = n$, dizemos que o reticulado tem *posto completo*.

Teorema 1.2

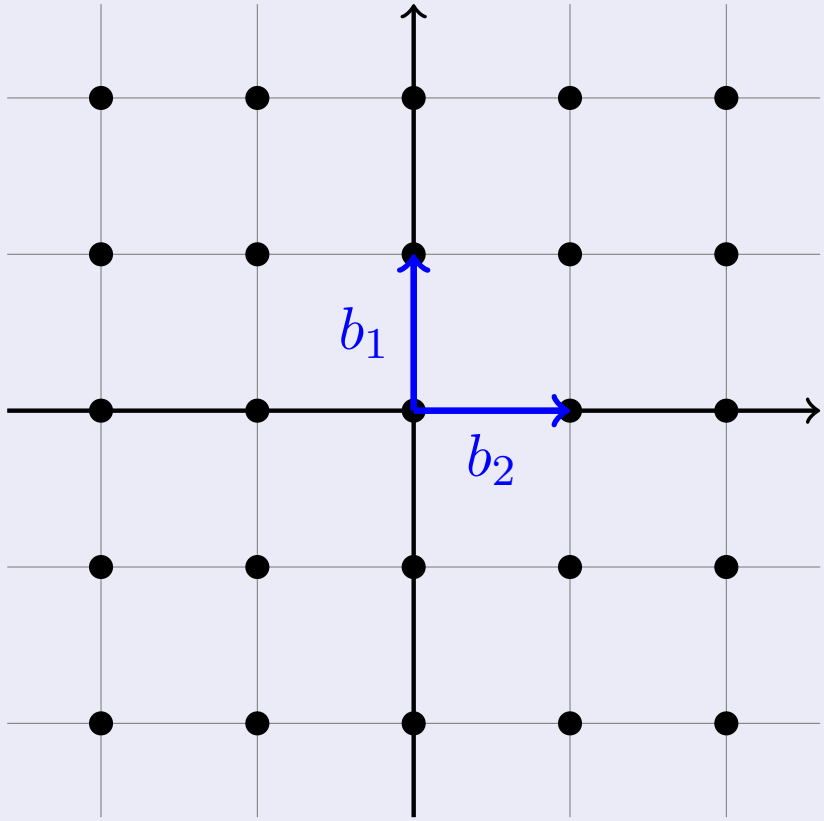
$\Lambda \subset \mathbb{R}^n$ é reticulado sse Λ é subgrupo aditivo discreto de $\mathbb{R}^n$.

Exemplo 1.3

Ilustramos aqui dois exemplos de reticulados de posto completo em $\mathbb{R}^2$.



(a) $\Lambda = \langle (1,1), (3/2, 0) \rangle_{\mathbb{Z}} \subset \mathbb{R}^2$.



(b) $\Lambda = \langle (0,1), (1,0) \rangle_{\mathbb{Z}} = \mathbb{Z}^2$.

Definição 1.4

Dado um reticulado Λ e uma base $\beta = \{b_1, \ldots, b_k\}$ deste reticulado, definimos a *matriz geradora* de Λ como

$$B = \begin{bmatrix} b_1 \cdots b_k \end{bmatrix}.$$

- Uma *matriz de Gram* é uma matriz simétrica $G = B^\top B$, onde B é matriz geradora de Λ.
- O determinante de Λ é dada por $\det \Lambda := \det G$, para qualquer matriz de Gram G. Um reticulado com determinante 1 é dito *unimodular*.
- O volume de Λ é $V(\Lambda) := \sqrt{\det \Lambda}$, e corresponde ao volume de um paralelotopo definido por uma base do reticulado.

Definição 1.4

Dado um reticulado Λ e uma base $\beta = \{b_1, \ldots, b_k\}$ deste reticulado, definimos a *matriz geradora* de Λ como

$$B = \begin{bmatrix} b_1 \cdots b_k \end{bmatrix}.$$

- Uma *matriz de Gram* é uma matriz simétrica $G = B^\top B$, onde B é matriz geradora de Λ.
- O determinante de Λ é dada por $\det \Lambda := \det G$, para qualquer matriz de Gram G. Um reticulado com determinante 1 é dito *unimodular*.
- O volume de Λ é $V(\Lambda) := \sqrt{\det \Lambda}$, e corresponde ao volume de um paralelotopo definido por uma base do reticulado.

Definição 1.4

Dado um reticulado Λ e uma base $\beta = \{b_1, \ldots, b_k\}$ deste reticulado, definimos a *matriz geradora* de Λ como

$$B = \begin{bmatrix} b_1 \cdots b_k \end{bmatrix}.$$

- Uma *matriz de Gram* é uma matriz simétrica $G = B^\top B$, onde B é matriz geradora de Λ.
- O determinante de Λ é dada por $\det \Lambda := \det G$, para qualquer matriz de Gram G. Um reticulado com determinante 1 é dito *unimodular*.
- O volume de Λ é $V(\Lambda) := \sqrt{\det \Lambda}$, e corresponde ao volume de um paralelotopo definido por uma base do reticulado.

Definição 1.4

Dado um reticulado Λ e uma base $\beta = \{b_1, \ldots, b_k\}$ deste reticulado, definimos a *matriz geradora* de Λ como

$$B = \begin{bmatrix} b_1 \cdots b_k \end{bmatrix}.$$

- Uma *matriz de Gram* é uma matriz simétrica $G = B^\top B$, onde B é matriz geradora de Λ.
- O determinante de Λ é dada por $\det \Lambda := \det G$, para qualquer matriz de Gram G. Um reticulado com determinante 1 é dito *unimodular*.
- O volume de Λ é $V(\Lambda) := \sqrt{\det \Lambda}$, e corresponde ao volume de um paralelotopo definido por uma base do reticulado.

- Duas matrizes $B_1, B_2 \in \mathbb{R}^{n\times k}$ geram o mesmo reticulado sse

$$B_1 = B_2 U$$

para alguma U *unimodular*, isto é,

$$U \in \mathrm{GL}_n(\mathbb{Z}) = \left\{ M \in \mathbb{Z}^{k\times k} \;\middle|\; \det M = \pm 1 \right\}.$$

- Dizemos que dois reticulados Λ_1, Λ_2 são *equivalentes* se existem $\lambda \in \mathbb{R}$ e O ortogonal $(O^\top O = I)$ tais que

$$\lambda O \Lambda_1 = \Lambda_2.$$

- Duas matrizes $B_1, B_2 \in \mathbb{R}^{n\times k}$ geram o mesmo reticulado sse

$$B_1 = B_2 U$$

para alguma U *unimodular*, isto é,

$$U \in \mathrm{GL}_n(\mathbb{Z}) = \left\{ M \in \mathbb{Z}^{k\times k} \;\middle|\; \det M = \pm 1 \right\}.$$

- Dizemos que dois reticulados Λ_1, Λ_2 são *equivalentes* se existem $\lambda \in \mathbb{R}$ e O ortogonal $(O^\top O = I)$ tais que

$$\lambda O \Lambda_1 = \Lambda_2.$$

Distância mínima

- Distância mínima:

$$\lambda(\Lambda) := \min_{\substack{x,y\in\Lambda \\ x\neq y}} \|x-y\| = \min_{v\in\Lambda\setminus\{0\}} \|v\| .$$

- Mínimos sucessivos:

$$\lambda_i(\Lambda) := \inf\left\{ \max_{v\in\mathcal{B}} \|v\| \;\middle|\; \mathcal{B} \text{ é conjunto L. I., } |\mathcal{B}| = i \right\}.$$

Distância mínima

- Distância mínima:

$$\lambda(\Lambda) := \min_{\substack{x,y\in\Lambda \\ x\neq y}} \|x-y\| = \min_{v\in\Lambda\setminus\{0\}} \|v\| .$$

- Mínimos sucessivos:

$$\lambda_i(\Lambda) := \inf\left\{ \max_{v\in\mathcal{B}} \|v\| \;\middle|\; \mathcal{B} \text{ é conjunto L. I., } |\mathcal{B}| = i \right\}.$$

Empacotamento

- O empacotamento do reticulado é feito colocando uma bola de raio $\lambda/2$ em cada ponto do reticulado.

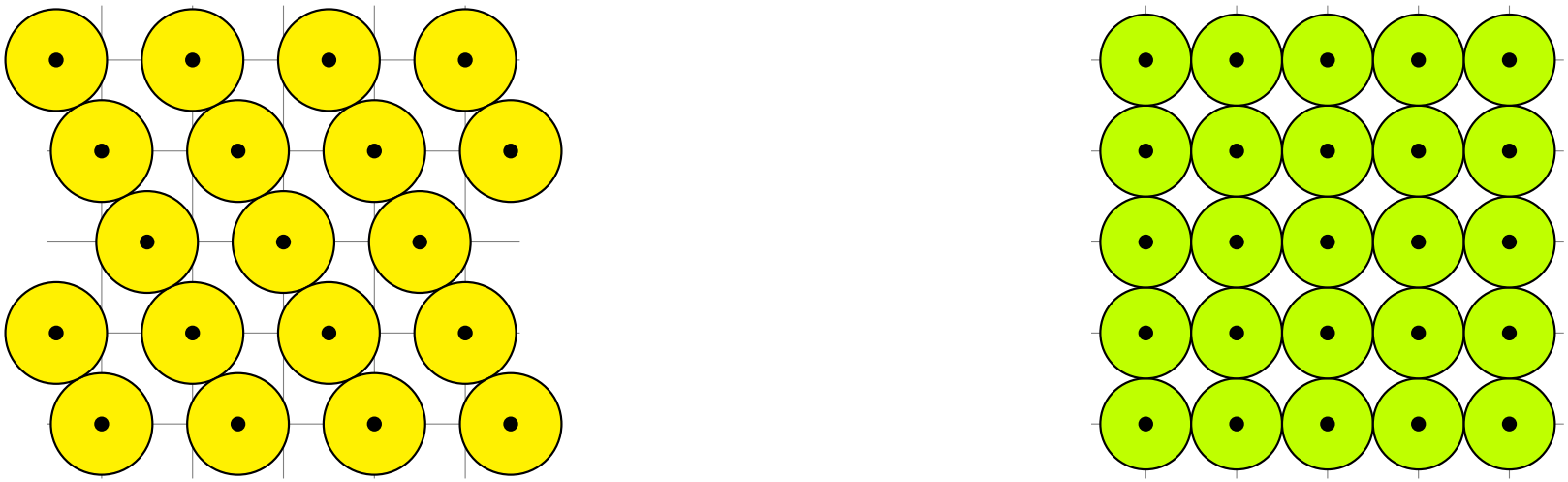


Figura: Empacotamento dos reticulados dos Exemplo 1.3.

- A proporção do espaço que é preenchida por esse empacotamento é dada pela densidade $\Delta(\Lambda) := \frac{\operatorname{Vol} B_{\lambda/2}(0)}{V(\Lambda)} \in [0, 1]$.

Empacotamento

- O empacotamento do reticulado é feito colocando uma bola de raio $\lambda/2$ em cada ponto do reticulado.

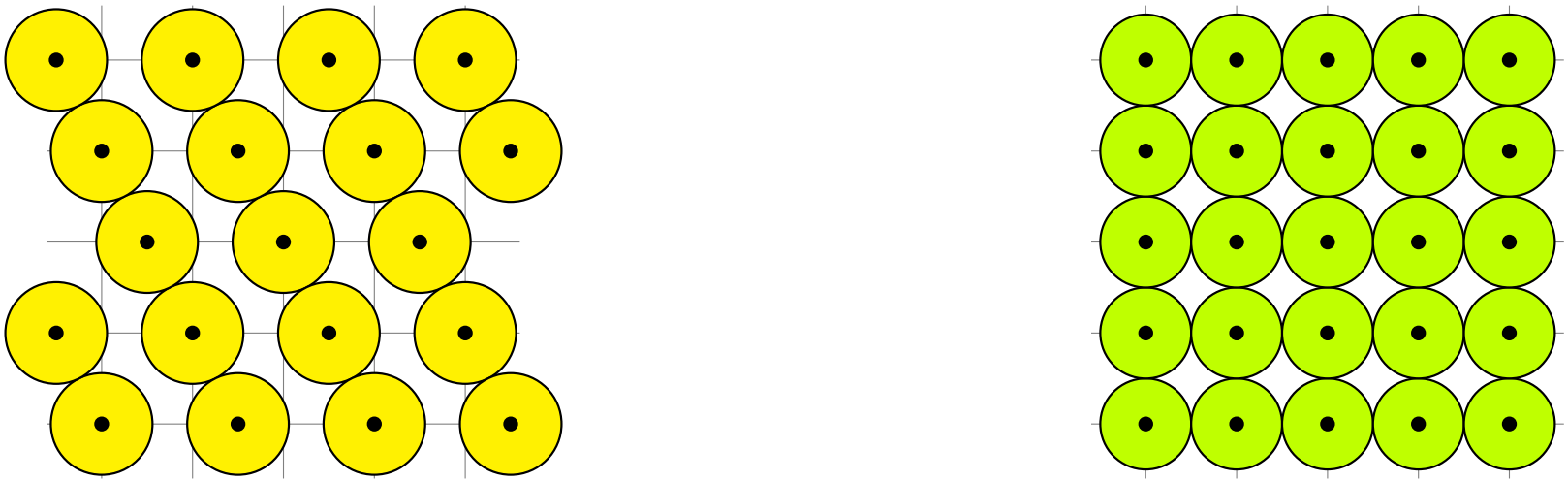


Figura: Empacotamento dos reticulados dos Exemplo 1.3.

- A proporção do espaço que é preenchida por esse empacotamento é dada pela densidade $\Delta(\Lambda) := \frac{\mathrm{Vol}\, B_{\lambda/2}(0)}{V(\Lambda)} \in [0,1]$.

Ladrilhamentos

- O volume de um reticulado também pode ser obtido através de conjuntos que ladrilham o espaço, isto é, conjuntos $A \subset \mathbb{R}^n$ mensuráveis, que satisfazem:
  1. se $v, w \in \Lambda$, $v \neq w$, então $(v + A) \cap (w + A)$ tem volume zero,
  2. $\bigcup_{v \in \Lambda} (v + A) = \mathbb{R}^n$.

Teorema 1.5

Se dois conjuntos mensuráveis ladrilham o plano por Λ, então eles têm o mesmo volume.

- Os dois principais ladrilhos são a **região de Voronói** e o **paralelotopo fundamental**.

Ladrilhamentos

- O volume de um reticulado também pode ser obtido através de conjuntos que ladrilham o espaço, isto é, conjuntos $A \subset \mathbb{R}^n$ mensuráveis, que satisfazem:
  1. se $v, w \in \Lambda$, $v \neq w$, então $(v + A) \cap (w + A)$ tem volume zero,
  2. $\bigcup_{v \in \Lambda}(v + A) = \mathbb{R}^n$.

Teorema 1.5

Se dois conjuntos mensuráveis ladrilham o plano por Λ, então eles têm o mesmo volume.

- Os dois principais ladrilhos são a **região de Voronói** e o **paralelotopo fundamental**.

Ladrilhamentos

- O volume de um reticulado também pode ser obtido através de conjuntos que ladrilham o espaço, isto é, conjuntos $A \subset \mathbb{R}^n$ mensuráveis, que satisfazem:
  1. se $v, w \in \Lambda$, $v \neq w$, então $(v + A) \cap (w + A)$ tem volume zero,
  2. $\bigcup_{v \in \Lambda}(v + A) = \mathbb{R}^n$.

Teorema 1.5

Se dois conjuntos mensuráveis ladrilham o plano por Λ, então eles têm o mesmo volume.

- Os dois principais ladrilhos são a **região de Voronói** e o **paralelotopo fundamental**.

Região de Voronói

É dada por

$$\mathcal{V}(\Lambda) = \{x \in \mathbb{R}^n \,|\, \|x\| \leq \|x - w\|\,,\ \forall\, w \in \Lambda \setminus \{0\}\}\,.$$

Figura: Regiões de Voronoi dos reticulados do Exemplo 1.3.

Paralelotopo fundamental

Dada uma base β, o paralelotopo fundamental associado é dado por

$$P(\beta) = \{\alpha_1 b_1 + \cdots + \alpha_k b_k \mid \alpha_1, \ldots, \alpha_k \in [0,1]\}.$$

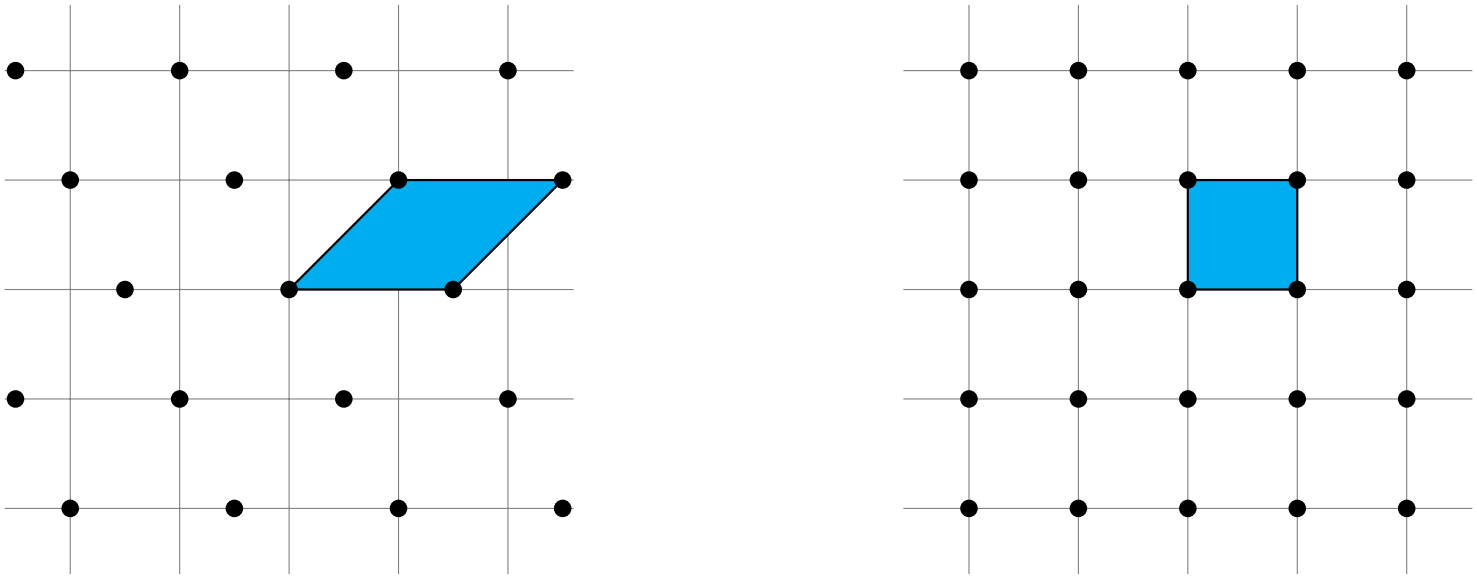


Figura: Paralelotopo fundamental dos reticulados do Exemplo 1.3.

Cobertura

- O *raio de cobertura* de Λ é dado por

$$\mu(\Lambda) = \inf\left\{r > 0 \,\middle|\, \bigcup_{v\in\Lambda} B_r(v) = \mathbb{R}^n\right\}.$$

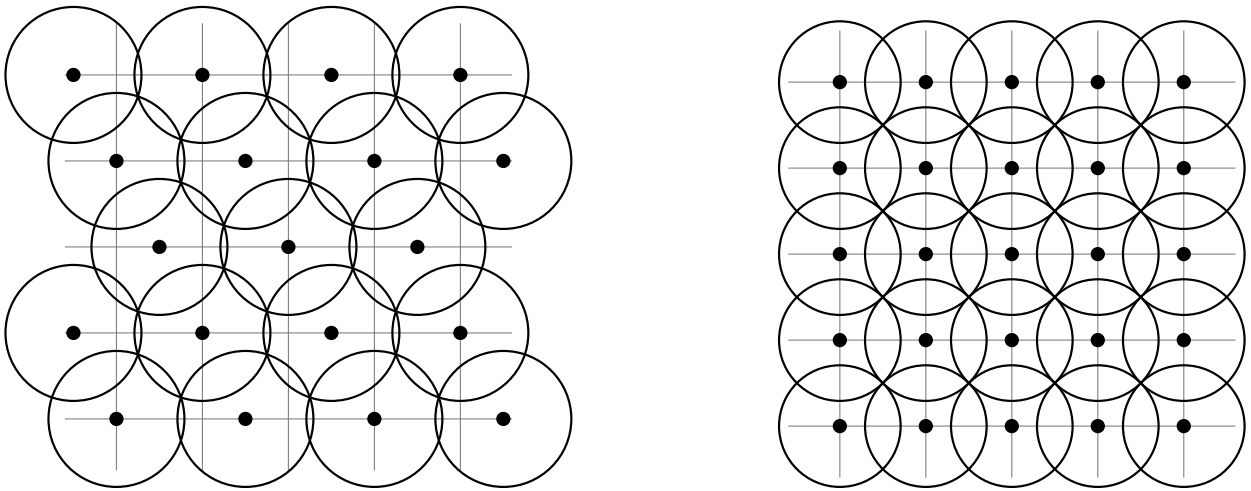


Figura: Cobertura dos reticulados do Exemplo 1.3.

- A *densidade de cobertura* de Λ é dada por $\Theta(\Lambda) := \frac{\operatorname{Vol} B_\mu(0)}{V(\Lambda)} \geq 1.$

Cobertura

- O *raio de cobertura* de Λ é dado por

$$\mu(\Lambda) = \inf\left\{r > 0 \,\middle|\, \bigcup_{v\in\Lambda} B_r(v) = \mathbb{R}^n\right\}.$$

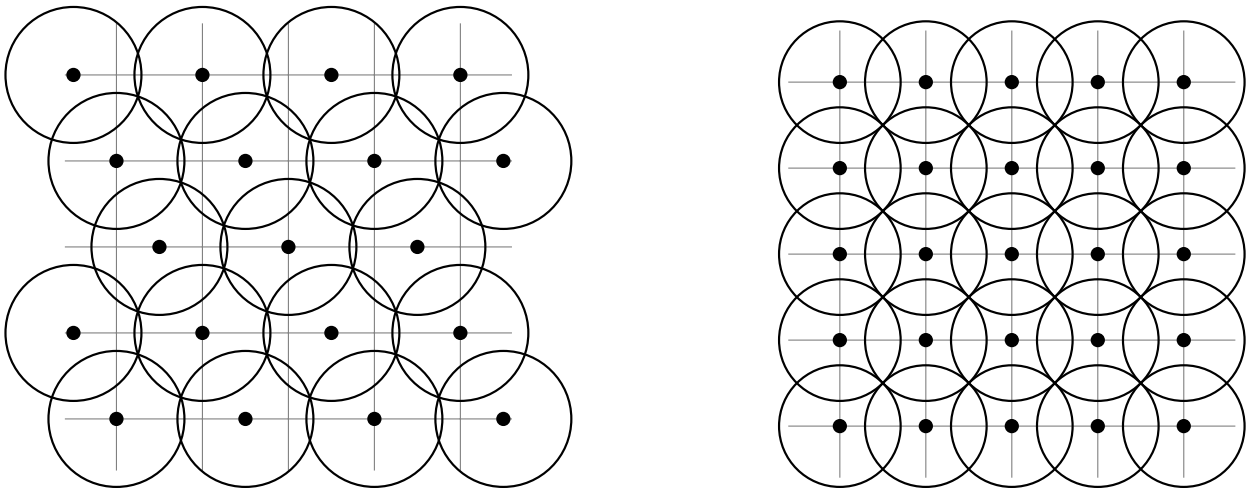


Figura: Cobertura dos reticulados do Exemplo 1.3.

- A *densidade de cobertura* de Λ é dada por $\Theta(\Lambda) := \dfrac{\operatorname{Vol} B_\mu(0)}{V(\Lambda)} \geq 1.$

Reticulados duais

O dual de um reticulado de posto completo $\Lambda \subset \mathbb{R}^n$ é o reticulado

$$\Lambda^* := \left\{ x \in \mathbb{R}^n \;\middle|\; \langle x, y \rangle \in \mathbb{Z},\ \forall\, y \in \Lambda \right\}.$$

- Se B é matriz geradora de Λ, então $(B^{-1})^\top$ é matriz geradora de Λ^*.
- Se rotacionamos um reticulado por um ângulo θ, o reticulado dual é igualmente rotacionado por θ.
- Se multiplicarmos um reticulado por uma constante $k > 0$, o reticulado dual é multiplicado por $\frac{1}{k}$.

Reticulados duais

O dual de um reticulado de posto completo $\Lambda \subset \mathbb{R}^n$ é o reticulado

$$\Lambda^* := \left\{ x \in \mathbb{R}^n \;\middle|\; \langle x, y \rangle \in \mathbb{Z},\ \forall\, y \in \Lambda \right\}.$$

- Se B é matriz geradora de Λ, então $\left(B^{-1}\right)^\top$ é matriz geradora de Λ^*.
- Se rotacionamos um reticulado por um ângulo θ, o reticulado dual é igualmente rotacionado por θ.
- Se multiplicarmos um reticulado por uma constante $k > 0$, o reticulado dual é multiplicado por $\frac{1}{k}$.

Reticulados duais

O dual de um reticulado de posto completo $\Lambda \subset \mathbb{R}^n$ é o reticulado

$$\Lambda^* := \left\{ x \in \mathbb{R}^n \;\middle|\; \langle x, y \rangle \in \mathbb{Z},\ \forall\, y \in \Lambda \right\}.$$

- Se B é matriz geradora de Λ, então $\left(B^{-1}\right)^\top$ é matriz geradora de Λ^*.
- Se rotacionamos um reticulado por um ângulo θ, o reticulado dual é igualmente rotacionado por θ.
- Se multiplicarmos um reticulado por uma constante $k > 0$, o reticulado dual é multiplicado por $\frac{1}{k}$.

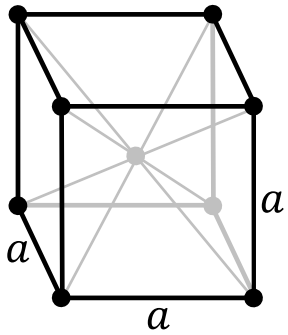
Reticulados duais

O dual de um reticulado de posto completo $\Lambda \subset \mathbb{R}^n$ é o reticulado

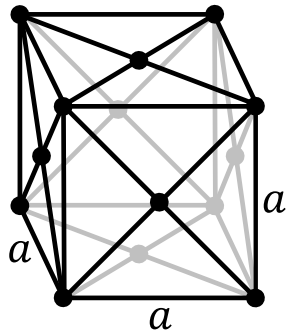
$$\Lambda^* := \left\{ x \in \mathbb{R}^n \;\middle|\; \langle x, y \rangle \in \mathbb{Z},\ \forall\, y \in \Lambda \right\}.$$

- Se B é matriz geradora de Λ, então $\left(B^{-1}\right)^\top$ é matriz geradora de Λ^*.
- Se rotacionamos um reticulado por um ângulo θ, o reticulado dual é igualmente rotacionado por θ.
- Se multiplicarmos um reticulado por uma constante $k > 0$, o reticulado dual é multiplicado por $\frac{1}{k}$.

BCC e FCC



(a) BCC



(b) FCC

Figura: Conjuntos geradores dos reticulados BCC e FCC.

Entre os reticulados de dimensão 3, o BCC é o que tem melhor densidade de cobertura ($\Theta = 1.4635$), enquanto o FCC é o que tem melhor densidade de empacotamento ($\Delta \approx 0.7405$).

Função teta

Seja $\mathbb{H} := \{\tau \in \mathbb{C} \mid \Im(\tau) > 0\}$ o hiperplano superior complexo. Para $\tau \in \mathbb{H}$, denotamos $q = q(\tau) = e^{2\pi i \tau}$.

Definição 1.6

A *função teta* de um reticulado $\Lambda \subset \mathbb{R}^n$ é a função $\vartheta_\Lambda \colon \mathbb{H} \to \mathbb{C}$ dada por [1]

$$\vartheta_\Lambda(\tau) = \sum_{v \in \Lambda} q^{\frac{1}{2}\langle v, v \rangle} = \sum_{v \in \Lambda} e^{\pi i \tau \langle v, v \rangle}.$$

A função teta do reticulado dual a Λ é dada por [1]

$$\vartheta_{\Lambda^*}(\tau) = V(\Lambda)\left(\frac{i}{\tau}\right)^{n/2}\vartheta_{\Lambda}\left(-\frac{1}{\tau}\right).$$

Exemplo 1.7

$$\vartheta_{\mathbb{Z}^2}(\tau) = 1 + 4q + 4q^2 + 8q^5 + 4q^8 + \dots$$
$$\vartheta_{\mathrm{FCC}}(\tau) = 1 + 12q^2 + 6q^4 + 24q^6 + 12q^8 + \dots$$
$$\vartheta_{\mathrm{BCC}}(\tau) = 1 + 8q^3 + 6q^4 + 12q^8 + 24q^{11} + \dots$$

A função teta do reticulado dual a Λ é dada por [1]

$$\vartheta_{\Lambda^*}(\tau) = V(\Lambda)\left(\frac{i}{\tau}\right)^{n/2}\vartheta_{\Lambda}\left(-\frac{1}{\tau}\right).$$

Exemplo 1.7

$$\vartheta_{\mathbb{Z}^2}(\tau) = 1 + 4q + 4q^2 + 8q^5 + 4q^8 + \dots$$
$$\vartheta_{\mathrm{FCC}}(\tau) = 1 + 12q^2 + 6q^4 + 24q^6 + 12q^8 + \dots$$
$$\vartheta_{\mathrm{BCC}}(\tau) = 1 + 8q^3 + 6q^4 + 12q^8 + 24q^{11} + \dots$$

Função gaussiana

Definição 2.1

A *função gaussiana* com fator $s > 0$ é a função $\rho_s \colon \mathbb{R}^n \to \mathbb{R}$ dada por

$$\rho_s(v) = \exp\left(-\pi \|v\|^2 / s^2\right).$$

- Observamos que $\int_{\mathbb{R}^n} \rho_s(x)\,\mathrm{d}x = s^n$.
- A gaussiana clássica é obtida fazendo $s = \sqrt{2\pi}\sigma$ e normalizando.

Função gaussiana

Definição 2.1

A *função gaussiana* com fator $s > 0$ é a função $\rho_s \colon \mathbb{R}^n \to \mathbb{R}$ dada por

$$\rho_s(v) = \exp\left(-\pi \|v\|^2 / s^2\right).$$

- Observamos que $\int_{\mathbb{R}^n} \rho_s(x)\,\mathrm{d}x = s^n$.
- A gaussiana clássica é obtida fazendo $s = \sqrt{2\pi}\sigma$ e normalizando.

Massa gaussiana

Definição 2.2

Sejam $\Lambda \subset \mathbb{R}^n$ de posto completo, e $c \in \mathbb{R}^n$. Definimos a *massa gaussiana* por

$$\rho_s(\Lambda + c) := \sum_{v \in (\Lambda + c)} \rho_s(v) = \sum_{v \in \Lambda} e^{-\pi \|v+c\|^2 / s^2}.$$

- Note que para calcular todas as massas gaussianas de um reticulado, basta tomarmos c em uma região fundamental do reticulado, como a região de Voronoi.
- Como detalhamos na dissertação, a massa gaussiana como função de $s > 0$ é contínua, diferenciável, crescente e injetiva.

Massa gaussiana

Definição 2.2

Sejam $\Lambda \subset \mathbb{R}^n$ de posto completo, e $c \in \mathbb{R}^n$. Definimos a *massa gaussiana* por

$$\rho_s(\Lambda + c) := \sum_{v \in (\Lambda + c)} \rho_s(v) = \sum_{v \in \Lambda} e^{-\pi \|v+c\|^2/s^2}.$$

- Note que para calcular todas as massas gaussianas de um reticulado, basta tomarmos c em uma região fundamental do reticulado, como a região de Voronoi.
- Como detalhamos na dissertação, a massa gaussiana como função de $s > 0$ é contínua, diferenciável, crescente e injetiva.

Massa gaussiana

Definição 2.2

Sejam $\Lambda \subset \mathbb{R}^n$ de posto completo, e $c \in \mathbb{R}^n$. Definimos a *massa gaussiana* por

$$\rho_s(\Lambda + c) := \sum_{v \in (\Lambda + c)} \rho_s(v) = \sum_{v \in \Lambda} e^{-\pi \|v+c\|^2 / s^2}.$$

- Note que para calcular todas as massas gaussianas de um reticulado, basta tomarmos c em uma região fundamental do reticulado, como a região de Voronoi.
- Como detalhamos na dissertação, a massa gaussiana como função de $s > 0$ é contínua, diferenciável, crescente e injetiva.

- A massa Gaussiana de Λ pode ser escrita em termos da função teta:

$$\rho_s(\Lambda) = \vartheta_\Lambda\left(\frac{1}{s^2}i\right).$$

- $\rho_s(\Lambda \setminus \{0\}) \xrightarrow{s\to+\infty} +\infty.$
- $\rho_s(\Lambda \setminus \{0\}) \xrightarrow{s\to 0^+} 0.$

- A massa Gaussiana de Λ pode ser escrita em termos da função teta:

$$\rho_s(\Lambda) = \vartheta_\Lambda\left(\frac{1}{s^2}i\right).$$

- $\rho_s(\Lambda \setminus \{0\}) \xrightarrow{s\to+\infty} +\infty.$
- $\rho_s(\Lambda \setminus \{0\}) \xrightarrow{s\to 0^+} 0.$

O parâmetro de suavização

Definição 2.3

Sejam Λ reticulado de posto completo e $\varepsilon > 0$. O parâmetro de suavização $\eta_\varepsilon(\Lambda)$ é o menor $s > 0$ tal que

$$\rho_{1/s}(\Lambda^* \setminus \{0\}) \leq \varepsilon.$$

Neste trabalho, observamos e demonstramos a seguinte propriedade:

Proposição 2.4

O parâmetro de suavização é invariante por rotação, e satisfaz

$$\eta_\varepsilon(k\Lambda) = k\eta_\varepsilon(\Lambda).$$

O parâmetro de suavização

Definição 2.3

Sejam Λ reticulado de posto completo e $\varepsilon > 0$. O parâmetro de suavização $\eta_\varepsilon(\Lambda)$ é o menor $s > 0$ tal que

$$\rho_{1/s}(\Lambda^* \setminus \{0\}) \leq \varepsilon.$$

Neste trabalho, observamos e demonstramos a seguinte propriedade:

Proposição 2.4

O parâmetro de suavização é invariante por rotação, e satisfaz

$$\eta_\varepsilon(k\Lambda) = k\eta_\varepsilon(\Lambda).$$

Dois exemplos de limitantes superiores para on parâmetro de suavização são mostradas em [2]:

- $\eta_{2^{-n}}(\Lambda) \leq \frac{\sqrt{n}}{\lambda(\Lambda^*)}$,
- $\eta_{\varepsilon}(\Lambda) \leq \lambda_n \sqrt{\frac{\ln\left(2n\left(1+{}^{1}/_{\varepsilon}\right)\right)}{\pi}}$.

- Definimos uma distribuição $\mathcal{P}_s^{\Lambda}$ sobre a região de Voronói $\mathcal{V}$ por:

$$\mathcal{P}_s^{\Lambda}(x) = \frac{1}{s^n}\rho_s(\Lambda + x) = \frac{1}{s^n}\sum_{v\in\Lambda}\rho_s(x+v)$$

Teorema 2.5 ([5])

Sejam Λ reticulado, $\varepsilon > 0$, $s \geq \eta_\varepsilon(\Lambda)$. Então

$$V(\Lambda)\cdot\mathcal{P}_s^{\Lambda}(x) \in [1-\varepsilon, 1+\varepsilon],$$

para todo $x \in \mathcal{V}$.

- Definimos uma distribuição $\mathcal{P}_s^{\Lambda}$ sobre a região de Voronói $\mathcal{V}$ por:

$$\mathcal{P}_s^{\Lambda}(x) = \frac{1}{s^n}\rho_s(\Lambda + x) = \frac{1}{s^n}\sum_{v\in\Lambda}\rho_s(x+v)$$

Teorema 2.5 ([5])

Sejam Λ reticulado, $\varepsilon > 0$, $s \geq \eta_\varepsilon(\Lambda)$. Então

$$V(\Lambda)\cdot\mathcal{P}_s^{\Lambda}(x) \in [1-\varepsilon, 1+\varepsilon],$$

para todo $x \in \mathcal{V}$.

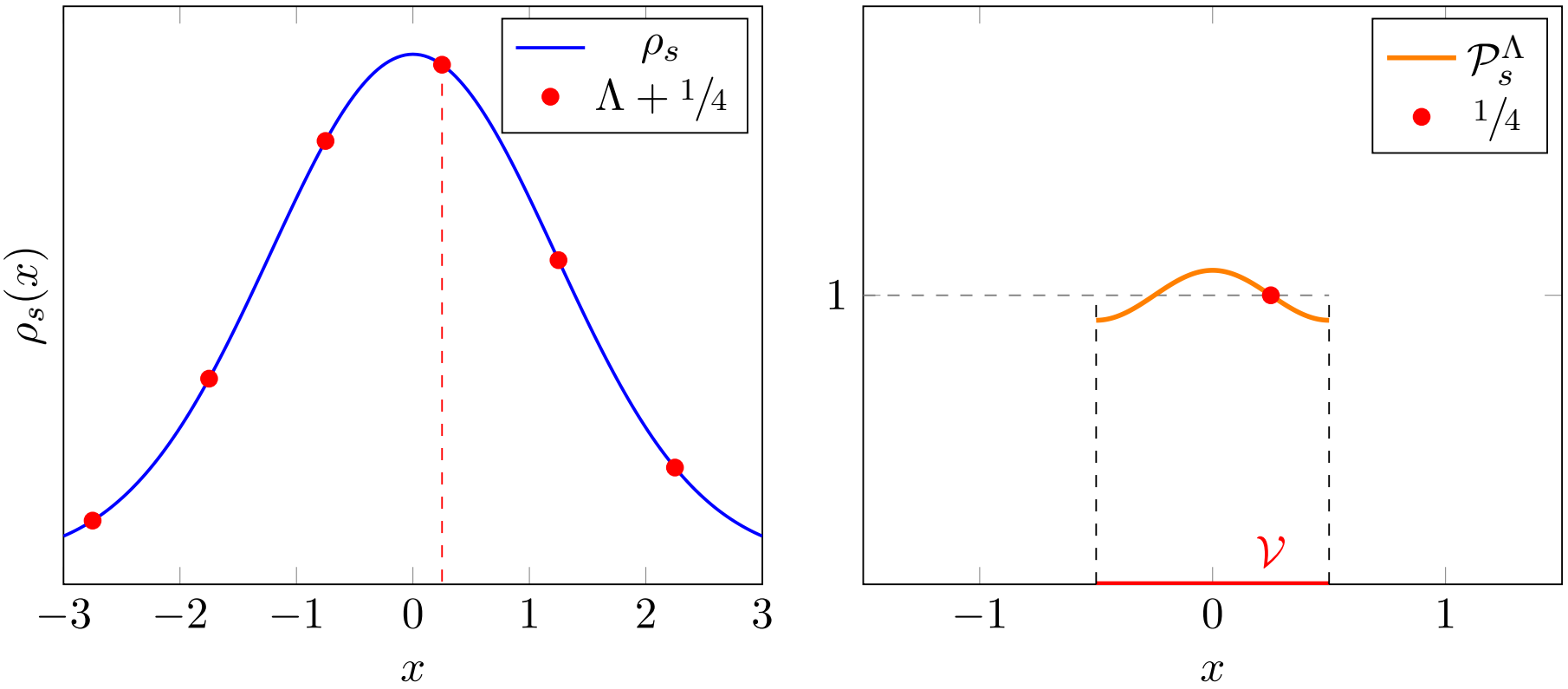


Figura: Representação de $\mathcal{P}_s^\Lambda$ para $\Lambda = \mathbb{Z}$, com $s = 1$.

Ideia da demonstração

- Para f que satisfaz certas condições (ρ_s satisfaz) temos

$$\sum_{x\in\Lambda} f(x) = \frac{1}{V(\Lambda)} \sum_{y\in\Lambda^*} \hat{f}(y),$$

  onde $\hat{f}$ é a transformada de Fourier de f.

- $\hat{\rho}_s = s^n \rho_{1/s}$.
- se $g(x) = f(x+c)$, então $\hat{g}(x) = e^{2\pi i\langle x,c\rangle}\hat{f}(x)$.

Ideia da demonstração

- Para f que satisfaz certas condições (ρ_s satisfaz) temos

$$\sum_{x\in\Lambda} f(x) = \frac{1}{V(\Lambda)} \sum_{y\in\Lambda^*} \hat{f}(y),$$

  onde $\hat{f}$ é a transformada de Fourier de f.
- $\hat{\rho}_s = s^n \rho_{1/s}$.
- se $g(x) = f(x+c)$, então $\hat{g}(x) = e^{2\pi i\langle x,c\rangle}\hat{f}(x)$.

Ideia da demonstração

- Para f que satisfaz certas condições (ρ_s satisfaz) temos

$$\sum_{x\in\Lambda} f(x) = \frac{1}{V(\Lambda)} \sum_{y\in\Lambda^*} \hat{f}(y),$$

  onde $\hat{f}$ é a transformada de Fourier de f.
- $\hat{\rho}_s = s^n \rho_{1/s}$.
- se $g(x) = f(x+c)$, então $\hat{g}(x) = e^{2\pi i\langle x,c\rangle}\hat{f}(x)$.

Demonstração.

$$\begin{aligned}\mathcal{P}_s^{\Lambda}(x) &= \frac{1}{s^n}\sum_{v\in\Lambda}\rho_s(x+v)\\ &= \frac{1}{s^n V(\Lambda)}\sum_{w\in\Lambda^*}\hat{\rho}_s(x+w)\\ &= \frac{\cancel{s^n}}{\cancel{s^n}V(\Lambda)}\sum_{w\in\Lambda^*}\left(e^{2\pi i\langle x,w\rangle}\rho_{1/s}(w)\right).\end{aligned}$$

Note que como $s \geq \eta_\varepsilon(\Lambda)$, e $\|e^{2\pi i\langle x,w\rangle}\| = 1$, temos que

$$\left|\sum_{w\in\Lambda^*\setminus\{0\}} e^{2\pi i\langle x,w\rangle}\rho_{1/s}(w)\right| \leq \varepsilon \implies V(\Lambda)\mathcal{P}_s^{\Lambda} \in [1-\varepsilon, 1+\varepsilon]. \qquad \square$$

Problemas difíceis em reticulados

Problema (SVP aproximado (SVP_γ))

Dado Λ um reticulado com base β, encontrar $v \in \Lambda$, $v \neq 0$, tal que $\|v\| \leq \gamma\, \lambda$.

Problema (CVP aproximado (CVP_γ))

Dados Λ um reticulado com base β e $w \in \mathbb{R}^n$, encontrar $v \in \Lambda$, $v \neq w$, tal que $\|w - v\| \leq \gamma \|w - x\|$ para todo $x \in \Lambda$, $x \neq w$.

Problema ($SIVP_\gamma$)

Dados uma base β para Λ e $\gamma > 1$, encontrar um conjunto $\{v_1, \ldots, v_k\} \subset \Lambda$ linearmente independente, tal que $\max_{1 \leq i \leq n} \|v_i\| \leq \gamma \lambda_k$.

Problemas difíceis em reticulados

Problema (SVP aproximado (SVP_γ))

Dado Λ um reticulado com base β, encontrar $v \in \Lambda$, $v \neq 0$, tal que $\|v\| \leq \gamma\, \lambda$.

Problema (CVP aproximado (CVP_γ))

Dados Λ um reticulado com base β e $w \in \mathbb{R}^n$, encontrar $v \in \Lambda$, $v \neq w$, tal que $\|w - v\| \leq \gamma \|w - x\|$ para todo $x \in \Lambda$, $x \neq w$.

Problema ($SIVP_\gamma$)

Dados uma base β para Λ e $\gamma > 1$, encontrar um conjunto $\{v_1, \ldots, v_k\} \subset \Lambda$ linearmente independente, tal que $\max_{1 \leq i \leq n} \|v_i\| \leq \gamma \lambda_k$.

Problemas difíceis em reticulados

Problema (SVP aproximado (SVP$_\gamma$))

Dado Λ um reticulado com base β, encontrar $v \in \Lambda$, $v \neq 0$, tal que $\|v\| \leq \gamma\, \lambda$.

Problema (CVP aproximado (CVP$_\gamma$))

Dados Λ um reticulado com base β e $w \in \mathbb{R}^n$, encontrar $v \in \Lambda$, $v \neq w$, tal que $\|w - v\| \leq \gamma \|w - x\|$ para todo $x \in \Lambda$, $x \neq w$.

Problema (SIVP$_\gamma$)

Dados uma base β para Λ e $\gamma > 1$, encontrar um conjunto $\{v_1, \ldots, v_k\} \subset \Lambda$ linearmente independente, tal que $\max\limits_{1 \leq i \leq n} \|v_i\| \leq \gamma \lambda_k$.

Gaussianas discretas

- Dado um conjunto discreto $A \subset \mathbb{R}^n$, a distribuição de probabilidade gaussiana discreta $D_{A,s}\colon A \to \mathbb{R}_{>0}$ é a normalização da função ρ_s sobre A:

$$D_{A,s}(x) = \frac{\rho_s(x)}{\rho_s(A)}.$$

- Seja φ função que associa a cada reticulado $\Lambda \subset \mathbb{R}^n$ um número real $\varphi(\Lambda) > 0$.

Problema (DGS_φ)

Dado um reticulado $\Lambda \subset \mathbb{R}^n$ e um número $r > \varphi(\Lambda)$, exibir uma amostra de $D_{\Lambda,r}$.

Gaussianas discretas

- Dado um conjunto discreto $A \subset \mathbb{R}^n$, a distribuição de probabilidade gaussiana discreta $D_{A,s}\colon A \to \mathbb{R}_{>0}$ é a normalização da função ρ_s sobre A:

$$D_{A,s}(x) = \frac{\rho_s(x)}{\rho_s(A)}.$$

- Seja φ função que associa a cada reticulado $\Lambda \subset \mathbb{R}^n$ um número real $\varphi(\Lambda) > 0$.

Problema (DGS_φ)

Dado um reticulado $\Lambda \subset \mathbb{R}^n$ e um número $r > \varphi(\Lambda)$, exibir uma amostra de $D_{\Lambda,r}$.

Gaussianas discretas

- Dado um conjunto discreto $A \subset \mathbb{R}^n$, a distribuição de probabilidade gaussiana discreta $D_{A,s}\colon A \to \mathbb{R}_{>0}$ é a normalização da função ρ_s sobre A:

$$D_{A,s}(x) = \frac{\rho_s(x)}{\rho_s(A)}.$$

- Seja φ função que associa a cada reticulado $\Lambda \subset \mathbb{R}^n$ um número real $\varphi(\Lambda) > 0$.

Problema (DGS_φ)

Dado um reticulado $\Lambda \subset \mathbb{R}^n$ e um número $r > \varphi(\Lambda)$, exibir uma amostra de $D_{\Lambda,r}$.

- Em geral o problema DGS é utilizado sobre um número polinomial de amostras em n (dimensão do reticulado).
- Se $r \geq \sqrt{2n} \cdot \eta_\varepsilon(\Lambda)$ então com alta probabilidade são amostrados vetores de norma $\leq \sqrt{n}r$.
- Assim, em uma gaussiana de fator r maior que $\sqrt{2n} \cdot \eta_\varepsilon(\Lambda)$, a dificuldade de DGS está relacionada a amostrar vetores curtos do reticulado (SVP).

- Em geral o problema DGS é utilizado sobre um número polinomial de amostras em n (dimensão do reticulado).
- Se $r \geq \sqrt{2n} \cdot \eta_\varepsilon(\Lambda)$ então com alta probabilidade são amostrados vetores de norma $\leq \sqrt{n}r$.
- Assim, em uma gaussiana de fator r maior que $\sqrt{2n} \cdot \eta_\varepsilon(\Lambda)$, a dificuldade de DGS está relacionada a amostrar vetores curtos do reticulado (SVP).

- Em geral o problema DGS é utilizado sobre um número polinomial de amostras em n (dimensão do reticulado).
- Se $r \geq \sqrt{2n} \cdot \eta_\varepsilon(\Lambda)$ então com alta probabilidade são amostrados vetores de norma $\leq \sqrt{n}r$.
- Assim, em uma gaussiana de fator r maior que $\sqrt{2n} \cdot \eta_\varepsilon(\Lambda)$, a dificuldade de DGS está relacionada a amostrar vetores curtos do reticulado (SVP).

LWE

- Seja χ uma distribuição de probabilidade sobre $\mathbb{Z}_q$ (geralmente uma gaussiana discreta).
- Uma *amostra* da **distribuição LWE** sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$ (denotada $A_{s,\chi}$) é um par (a, b) onde
  - a é escolhido uniformemente em $\mathbb{Z}_q^n$,
  - $b = \langle a, s \rangle + \varepsilon \pmod{q}$ para ε escolhido por χ.

Problema ($\mathrm{LWE}_{n,q,\chi,m}$)

Dadas m amostras independentes $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, escolhidas por $A_{s,\chi}$ para um $s \in \mathbb{Z}_q^n$ uniformemente aleatório, encontrar s. [3]

LWE

- Seja χ uma distribuição de probabilidade sobre $\mathbb{Z}_q$ (geralmente uma gaussiana discreta).
- Uma *amostra* da **distribuição LWE** sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$ (denotada $A_{s,\chi}$) é um par (a, b) onde
  - a é escolhido uniformemente em $\mathbb{Z}_q^n$,
  - $b = \langle a, s \rangle + \varepsilon \pmod{q}$ para ε escolhido por χ.

Problema ($\mathrm{LWE}_{n,q,\chi,m}$)

Dadas m amostras independentes $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, escolhidas por $A_{s,\chi}$ para um $s \in \mathbb{Z}_q^n$ uniformemente aleatório, encontrar s. [3]

LWE

- Seja χ uma distribuição de probabilidade sobre $\mathbb{Z}_q$ (geralmente uma gaussiana discreta).
- Uma *amostra* da **distribuição LWE** sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$ (denotada $A_{s,\chi}$) é um par (a, b) onde
  - a é escolhido uniformemente em $\mathbb{Z}_q^n$,
  - $b = \langle a, s \rangle + \varepsilon \pmod{q}$ para ε escolhido por χ.

Problema ($\mathrm{LWE}_{n,q,\chi,m}$)

Dadas m amostras independentes $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, escolhidas por $A_{s,\chi}$ para um $s \in \mathbb{Z}_q^n$ uniformemente aleatório, encontrar s. [3]

Dificuldade de LWE

- Sejam $p(n) \in \mathbb{Z}$ e $\alpha(n) \in (0,1)$ tais que $\alpha(n)p(n) > 2\sqrt{n}$.
- Se existir um algoritmo eficiente W que resolve $\mathrm{LWE}_{n,q,\bar{\Psi}_\alpha,m}$ polinomialmente em m, então existe um algoritmo quântico eficiente que resolve $\mathrm{DGS}_{\sqrt{2n}\cdot\eta_\varepsilon(\Lambda)/\alpha}$.

Problema do parâmetro de suavização

Problema (γ-GapSPP$_\varepsilon$ [4])

Sejam $\gamma > 1$, $\varepsilon > 0$. Cada instância de γ-GapSPP$_\varepsilon$ é uma base β de um reticulado n-dimensional $\Lambda \subset \mathbb{R}^n$.

- *As instâncias* SIM *são as bases β com $\eta_\varepsilon(\Lambda) \leq 1$.*
- *As instâncias* $\mathrm{NÃO}$ *são as bases β com $\eta_\varepsilon(\Lambda) \geq \gamma$.*

- A dificuldade vem através da prova que o problema é SZK e AM, que são classes de complexidade de problemas difíceis.

Problema do parâmetro de suavização

Problema (γ-GapSPP$_\varepsilon$ [4])

Sejam $\gamma > 1$, $\varepsilon > 0$. Cada instância de γ-GapSPP$_\varepsilon$ é uma base β de um reticulado n-dimensional $\Lambda \subset \mathbb{R}^n$.

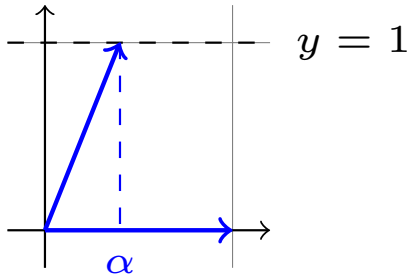
- *As instâncias* SIM *são as bases β com $\eta_\varepsilon(\Lambda) \leq 1$.*
- *As instâncias* NÃO *são as bases β com $\eta_\varepsilon(\Lambda) \geq \gamma$.*

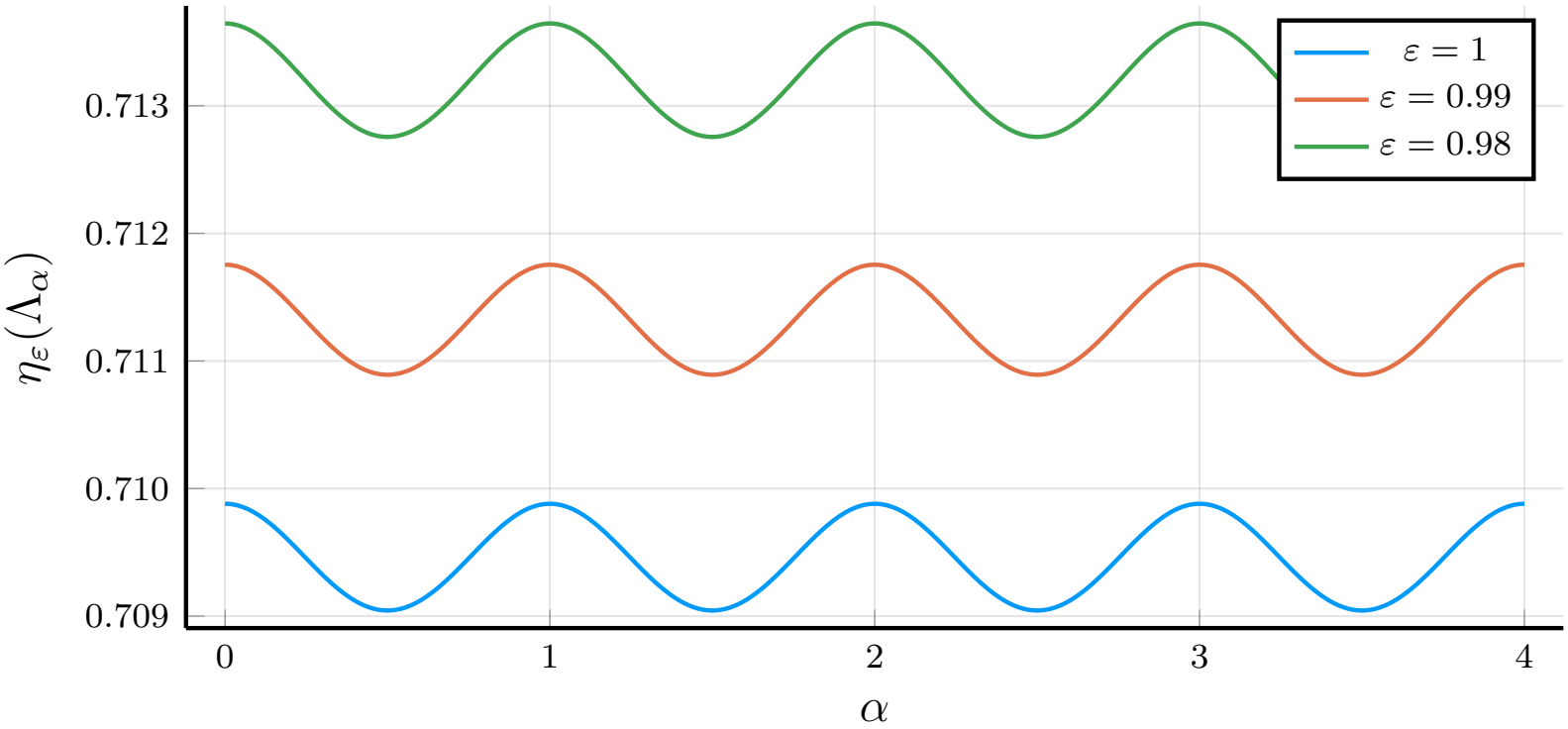
- A dificuldade vem através da prova que o problema é SZK e AM, que são classes de complexidade de problemas difíceis.

Simulações computacionais

- Fizemos simulações computacionais na linguagem Julia para calcular o parâmetro de suavização nas dimensões 2 e 3.
- Sempre normalizamos o reticulado com $\lambda = 1$ para fazer as comparações.

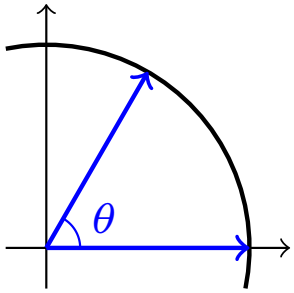
a) Reticulado $\Lambda_\alpha = \langle (1,0), (\alpha,1) \rangle_{\mathbb{Z}}$ para $\alpha \in \mathbb{R}$.
Neste caso, $\lambda = 1$ e $\Delta = \pi/4$.

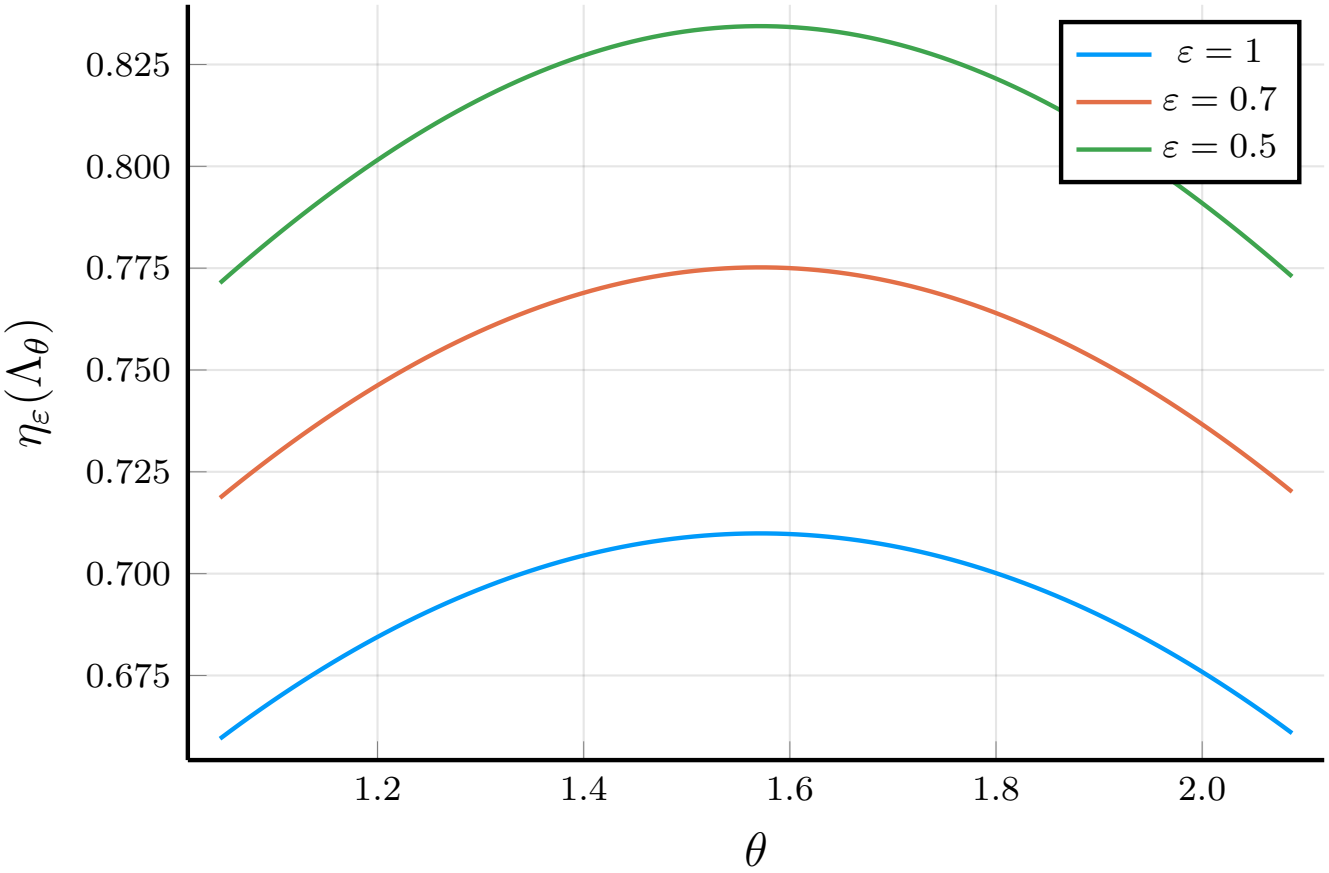




b) Reticulado $\Lambda_\theta = \langle (1,0), (\cos\theta, \sin\theta) \rangle_{\mathbb{Z}}$ para $\theta \in \left[\frac{\pi}{3}, \frac{2\pi}{3}\right]$.

Neste caso, $\lambda = 1$ e $\Delta = \frac{\pi}{4\sin\theta}$.





Dimensão 2

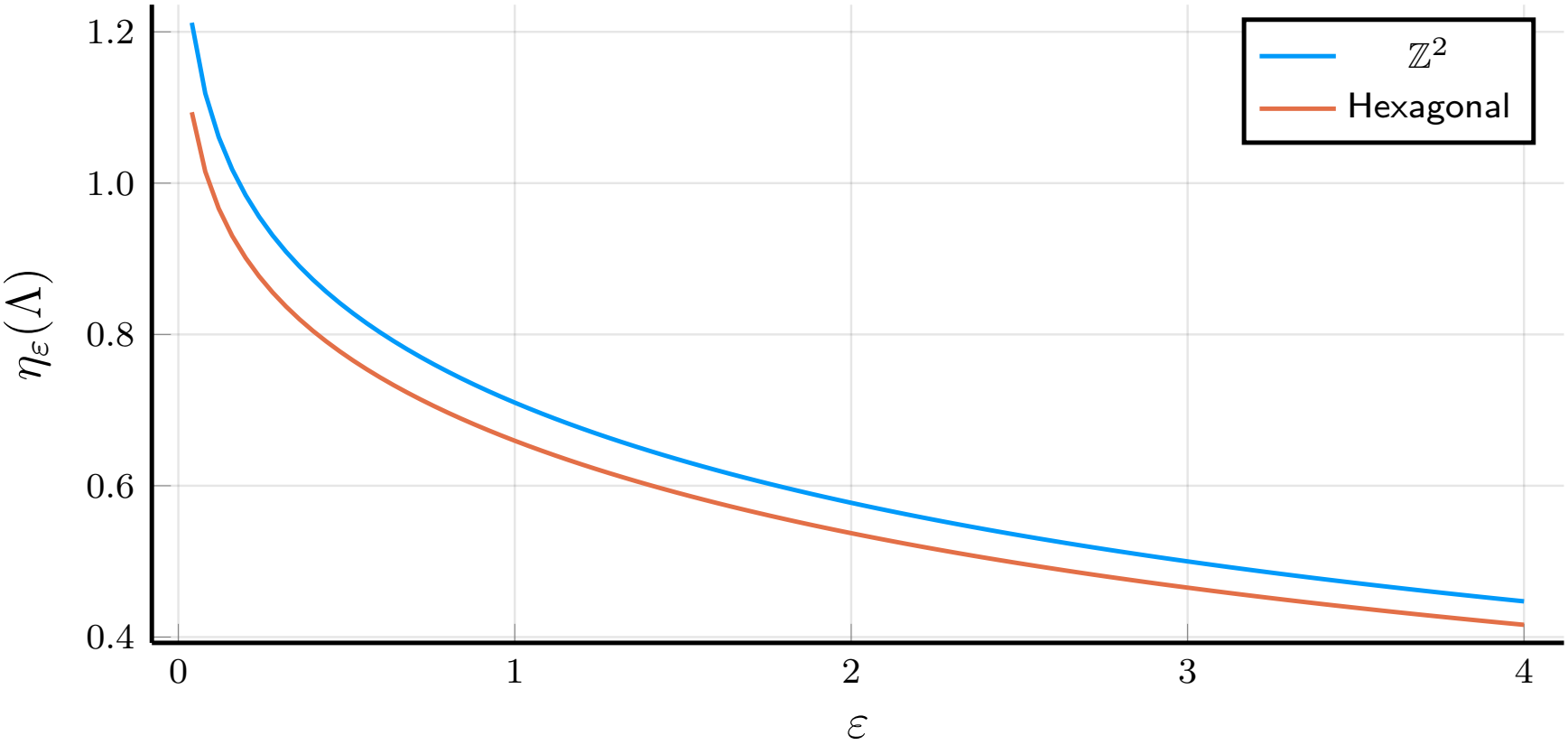


Figura: Parâmetro de suavização dos reticulados $\mathbb{Z}^2$ e hexagonal.

Dimensão 3

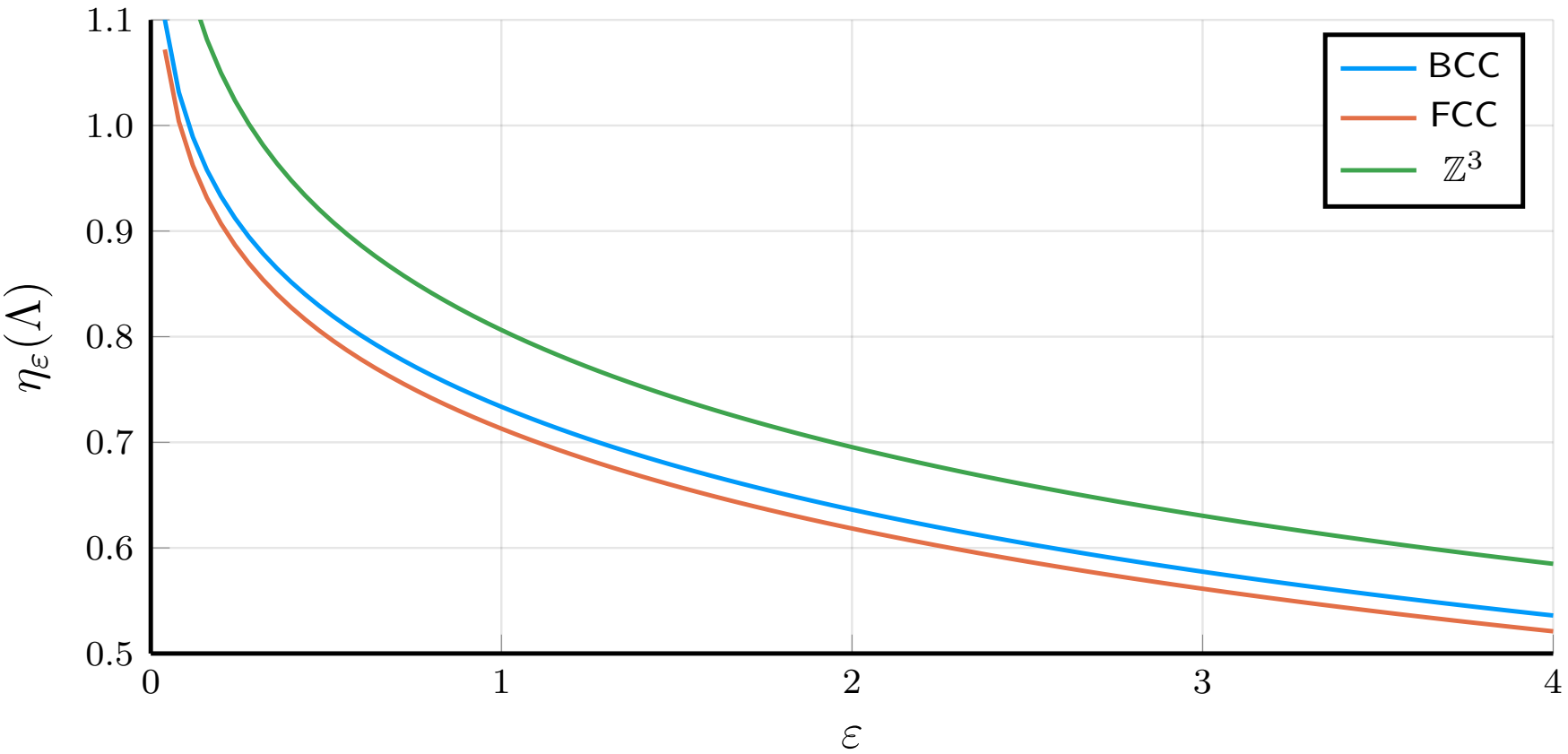


Figura: Parâmetro de suavização dos reticulados BCC, FCC e $\mathbb{Z}^3$.

Exemplos onde as curvas de η_ε se intersectam

Λ	$\Lambda_1 = \left\langle (1,0), \left(1/2, 1\right) \right\rangle$	$\Lambda_2 = \left\langle (1,0), \left(\cos\left(\pi/2.05\right), \sin\left(\pi/2.05\right)\right) \right\rangle$
$\eta_{1/5}$	0.972712320858219 1	0.983565841836341 3
η_6	0.377964473116467 97	0.377825769021661 9

Tabela: Tabela de parâmetros de suavização de reticulados. Note que para $\varepsilon \leq 1/5$, Λ_1 é tem um valor menor, enquanto para $\varepsilon \geq 6$, o valor menor é o de Λ_2.

Aproximação da distribuição uniforme

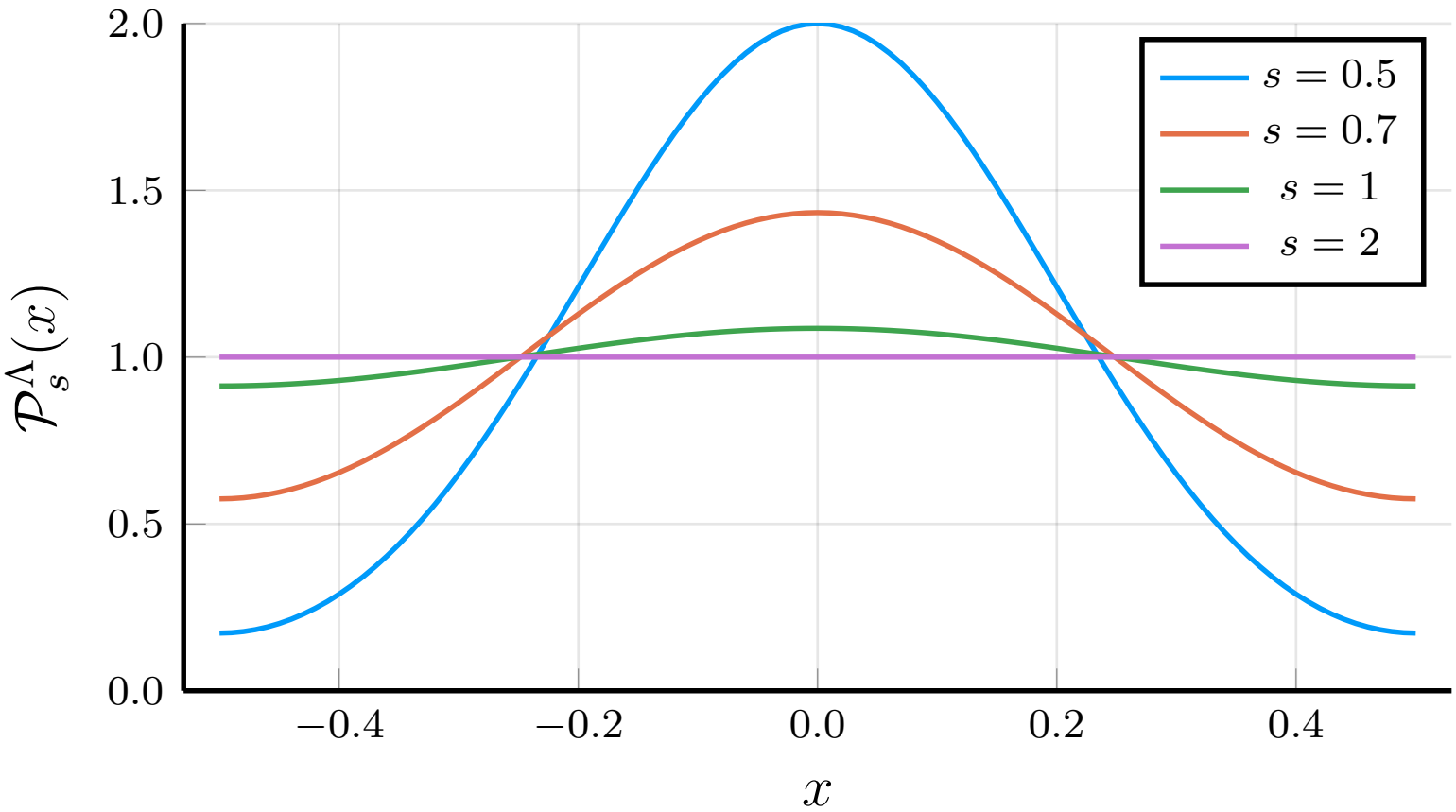


Figura: Gráfico de $\mathcal{P}_s^{\mathbb{Z}}(x)$ em função de x, para valores crescentes de s.

Perspectivas

- Procurar se é interessante estender a definição do parâmetro de suavização para gaussianas não-redondas (trocando $\langle v, v \rangle$ por $v^\top B v$ para B simétrica positivo-definida).
- Analisar melhor a relação entre o parâmetro de suavização com outros parâmetros de reticulados, como densidades de empacotamento e de cobertura, razão de Hadamard, arredondamento, entre outros.
- Estudar mais profundamente o parâmetro de suavização generalizado, para noções diferentes de distância, e possivelmente de divergência.

Bibliografia I

W. Ebeling. *Lattices and Codes: A Course Partially Based on Lectures by Friedrich Hirzebruch*. Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2012. ISBN: 9783658003593. DOI: 10.1007/978-3-658-00360-9.

D. Micciancio e O. Regev. "Worst-Case to Average-Case Reductions Based on Gaussian Measures". Em: *SIAM Journal on Computing* 37.1 (2007), pp. 267–302. DOI: 10.1137/S0097539705447360.

C. Peikert. *A Decade of Lattice Cryptography*. Fev. de 2016. URL: https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf.

Bibliografia II

 C. Peikert, K. Chung, D. Dadush e F. Liu. "On the Lattice Smoothing Parameter Problem". Em: *2013 IEEE Conference on Computational Complexity*. Jun. de 2013, pp. 230–241. DOI: 10.1109/CCC.2013.31.

 O. Regev. "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography". Em: *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*. STOC '05. ACM, 2005, pp. 84–93. ISBN: 1-58113-960-8. DOI: 10.1145/1060590.1060603.