Parâmetros de reticulados e criptografia

Fábio C. C. Meneghetti

IMECC — Unicamp

5 de abril de 2022

Noções de criptografia

Objetivos da criptografia:

- **confidencialidade**
- integridade
- autenticação
- não-repúdio

Chaves

- **criptografia simétrica:** uma única chave, que encripta e decripta as mensagens

Chaves

- **criptografia simétrica:** uma única chave, que encripta e decripta as mensagens
  - é necessário um método seguro para que Alice e Bob combinem previamente esta chave

Chaves

- **criptografia simétrica:** uma única chave, que encripta e decripta as mensagens
  - é necessário um método seguro para que Alice e Bob combinem previamente esta chave
- **criptografia assimétrica:** duas chaves

Chaves

- **criptografia simétrica:** uma única chave, que encripta e decripta as mensagens
  - é necessário um método seguro para que Alice e Bob combinem previamente esta chave
- **criptografia assimétrica:** duas chaves
  - chave pública, encripta mensagens

Chaves

- **criptografia simétrica:** uma única chave, que encripta e decripta as mensagens
  - é necessário um método seguro para que Alice e Bob combinem previamente esta chave
- **criptografia assimétrica:** duas chaves
  - chave pública, encripta mensagens
  - chave secreta, decripta mensagens

Problemas

- o objetivo dos algoritmos de encriptação é garantir que um atacante (Eva) precise de muito tempo (décadas/séculos) para desvendar a mensagem, mesmo com as máquinas mais potentes conhecidas

Problemas

- o objetivo dos algoritmos de encriptação é garantir que um atacante (Eva) precise de muito tempo (décadas/séculos) para desvendar a mensagem, mesmo com as máquinas mais potentes conhecidas
- para garantir essa dificuldade, precisamos garantir que para quebrar o esquema, Eva precisaria resolver um problema matemático difícil

Problemas

- o objetivo dos algoritmos de encriptação é garantir que um atacante (Eva) precise de muito tempo (décadas/séculos) para desvendar a mensagem, mesmo com as máquinas mais potentes conhecidas
- para garantir essa dificuldade, precisamos garantir que para quebrar o esquema, Eva precisaria resolver um problema matemático difícil
- "difícil" pode ter dois sentidos:

Problemas

- o objetivo dos algoritmos de encriptação é garantir que um atacante (Eva) precise de muito tempo (décadas/séculos) para desvendar a mensagem, mesmo com as máquinas mais potentes conhecidas
- para garantir essa dificuldade, precisamos garantir que para quebrar o esquema, Eva precisaria resolver um problema matemático difícil
- "difícil" pode ter dois sentidos:
  - um problema que tentou-se atacar por muito tempo, sem sucesso (ex: fatoração em primos, criptografia RSA)

Problemas

- o objetivo dos algoritmos de encriptação é garantir que um atacante (Eva) precise de muito tempo (décadas/séculos) para desvendar a mensagem, mesmo com as máquinas mais potentes conhecidas
- para garantir essa dificuldade, precisamos garantir que para quebrar o esquema, Eva precisaria resolver um problema matemático difícil
- "difícil" pode ter dois sentidos:
  - um problema que tentou-se atacar por muito tempo, sem sucesso (ex: fatoração em primos, criptografia RSA)
  - um problema NP-difícil ou NP-completo (ex: caixeiro viajante)

Complexidade

- **P:** pode ser resolvido em tempo polinomial por uma máquina de Turing determinística

Complexidade

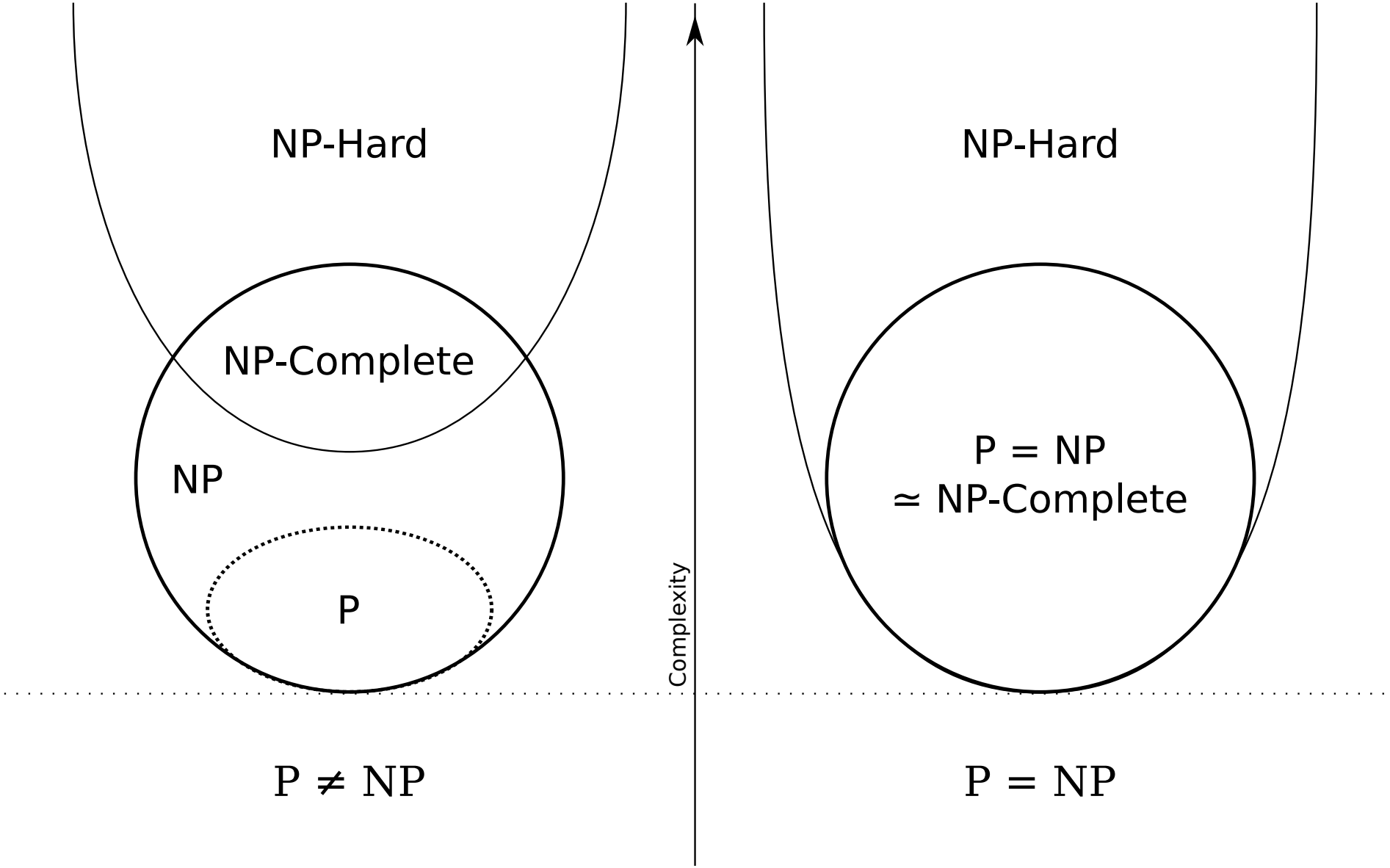
- **P:** pode ser resolvido em tempo polinomial por uma máquina de Turing determinística
- **NP:** pode ser resolvido em tempo polinomial por uma máquina de Turing não-determinística

Complexidade

- **P:** pode ser resolvido em tempo polinomial por uma máquina de Turing determinística
- **NP:** pode ser resolvido em tempo polinomial por uma máquina de Turing não-determinística
- **NP-difícil:** todo problema NP pode ser reduzido em tempo polinomial a um problema NP-difícil

Complexidade

- **P:** pode ser resolvido em tempo polinomial por uma máquina de Turing determinística
- **NP:** pode ser resolvido em tempo polinomial por uma máquina de Turing não-determinística
- **NP-difícil:** todo problema NP pode ser reduzido em tempo polinomial a um problema NP-difícil
- **NP-completo:** NP $\cap$ NP-difícil


NP-Hard
NP-Complete
NP
P
Complexity
NP-Hard
P = NP
≃ NP-Complete
P ≠ NP
P = NP

Computadores quânticos

- Computadores quânticos são uma ameaça à criptografia tradicional, pois já foram encontrados algoritmos polinomiais para computadores quânticos que resolvem problemas clássicos em tempo polinomial

Computadores quânticos

- Computadores quânticos são uma ameaça à criptografia tradicional, pois já foram encontrados algoritmos polinomiais para computadores quânticos que resolvem problemas clássicos em tempo polinomial
  - ex: algoritmo de Shor, resolve fatoração em primos (quebra RSA)

Computadores quânticos

- Computadores quânticos são uma ameaça à criptografia tradicional, pois já foram encontrados algoritmos polinomiais para computadores quânticos que resolvem problemas clássicos em tempo polinomial
  - ex: algoritmo de Shor, resolve fatoração em primos (quebra RSA)
- o concurso NIST Post-Quantum Cryptography Standardization é a tentativa de construir um padrão para criptografia resistente a computadores quânticos

Computadores quânticos

- Computadores quânticos são uma ameaça à criptografia tradicional, pois já foram encontrados algoritmos polinomiais para computadores quânticos que resolvem problemas clássicos em tempo polinomial
  - ex: algoritmo de Shor, resolve fatoração em primos (quebra RSA)
- o concurso NIST Post-Quantum Cryptography Standardization é a tentativa de construir um padrão para criptografia resistente a computadores quânticos
- Finalistas do Round 3:

Computadores quânticos

- Computadores quânticos são uma ameaça à criptografia tradicional, pois já foram encontrados algoritmos polinomiais para computadores quânticos que resolvem problemas clássicos em tempo polinomial
  - ex: algoritmo de Shor, resolve fatoração em primos (quebra RSA)
- o concurso NIST Post-Quantum Cryptography Standardization é a tentativa de construir um padrão para criptografia resistente a computadores quânticos
- Finalistas do Round 3:
  - baseados em reticulados: 3 de encriptação, 2 de assinatura

Computadores quânticos

- Computadores quânticos são uma ameaça à criptografia tradicional, pois já foram encontrados algoritmos polinomiais para computadores quânticos que resolvem problemas clássicos em tempo polinomial
  - ex: algoritmo de Shor, resolve fatoração em primos (quebra RSA)
- o concurso NIST Post-Quantum Cryptography Standardization é a tentativa de construir um padrão para criptografia resistente a computadores quânticos
- Finalistas do Round 3:
  - baseados em reticulados: 3 de encriptação, 2 de assinatura
  - baseados em códigos: 1 de encriptação

Computadores quânticos

- Computadores quânticos são uma ameaça à criptografia tradicional, pois já foram encontrados algoritmos polinomiais para computadores quânticos que resolvem problemas clássicos em tempo polinomial
  - ex: algoritmo de Shor, resolve fatoração em primos (quebra RSA)
- o concurso NIST Post-Quantum Cryptography Standardization é a tentativa de construir um padrão para criptografia resistente a computadores quânticos
- Finalistas do Round 3:
  - baseados em reticulados: 3 de encriptação, 2 de assinatura
  - baseados em códigos: 1 de encriptação
  - baseados polinômios multivariados: 1 de assinatura

Criptografia baseada em reticulados

Os algoritmos de criptografia em reticulados, a grosso modo, podem ser divididos em dois conjuntos:

- aqueles que utilizam diretamente reticulados em sua formulação (GGH)

Criptografia baseada em reticulados

Os algoritmos de criptografia em reticulados, a grosso modo, podem ser divididos em dois conjuntos:

- aqueles que utilizam diretamente reticulados em sua formulação (GGH)
- aqueles que podem ser reduzidos em tempo polinomial a problemas em reticulados (ex: NTRU, LWE, SIS, Ring-LWE, Ring-SIS)

Distâncias mínimas generalizadas

Seja $\Lambda \subset \mathbb{R}^n$ reticulado k-dimensional.

- a (1ª) distância mínima é

$$\lambda_1 = \min_{v \in \Lambda \setminus \{0\}} \|v\|_2$$

Distâncias mínimas generalizadas

Seja $\Lambda \subset \mathbb{R}^n$ reticulado k-dimensional.

- a (1^{a}) distância mínima é

$$\lambda_1 = \min_{v \in \Lambda \setminus \{0\}} \|v\|_2$$

- a j-ésima distância mínima ($j \in \{1, \ldots, k\}$) é

$$\lambda_j = \min \left\{ \max \left\{ \|v_1\|, \ldots, \|v_j\| \right\} \;\middle|\; v_1, \ldots, v_j \text{ é conjunto LI em } \Lambda \right\}$$

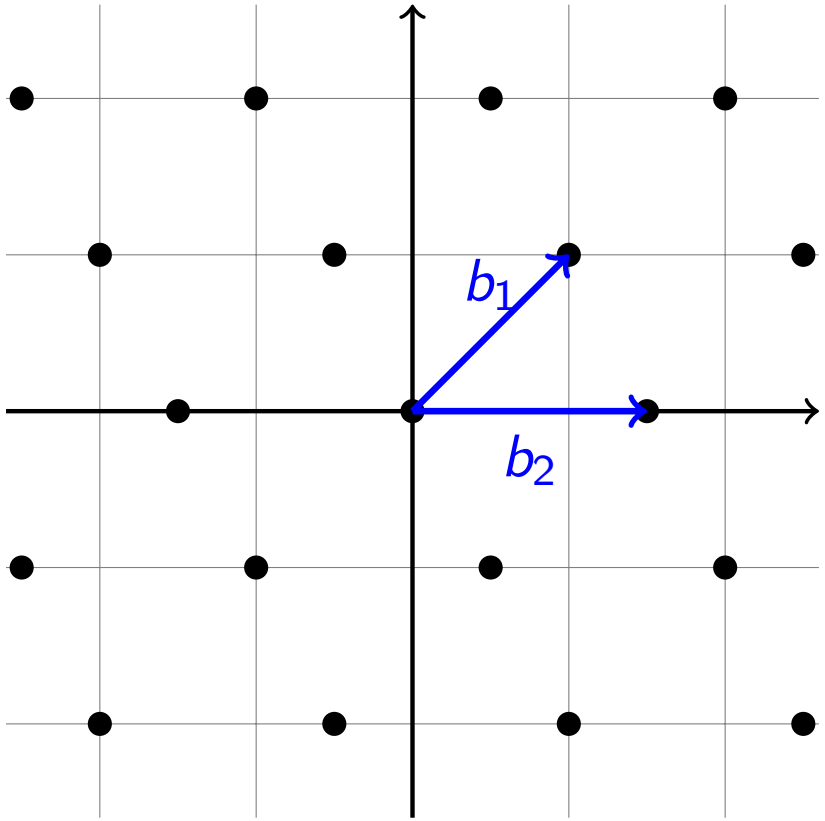


Figure: $\Lambda = \langle (1,1), (1.5,0) \rangle_{\mathbb{Z}} \subset \mathbb{R}^2$.

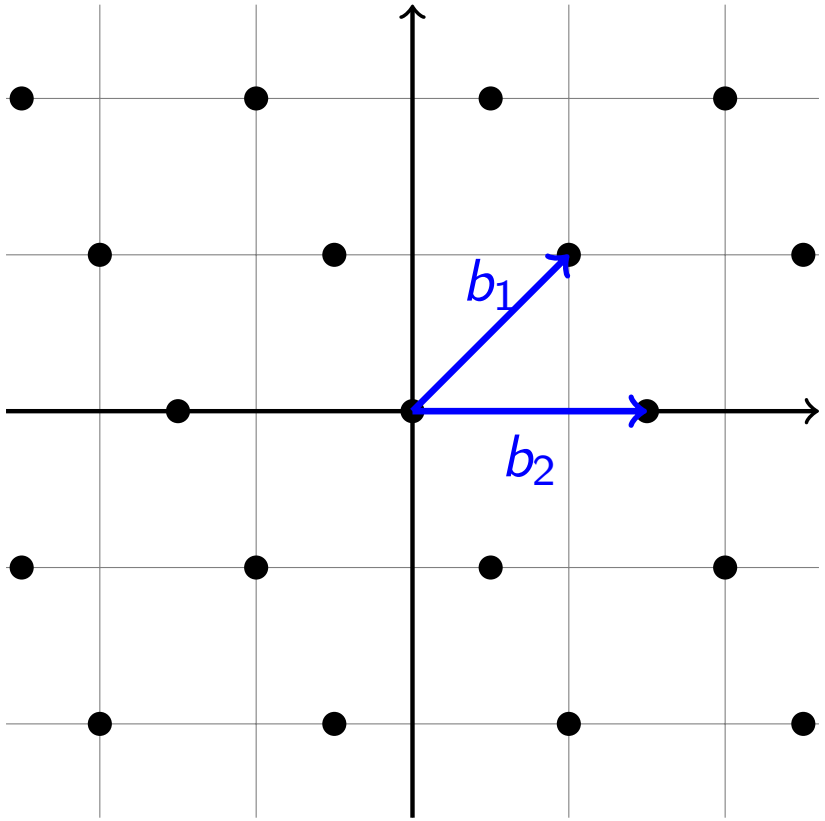


Figure: $\Lambda = \langle (1,1), (1.5,0) \rangle_{\mathbb{Z}} \subset \mathbb{R}^2$.

- temos: $\lambda_1 = \|b_1 - b_2\| = \|(-0.5,1)\| = \frac{\sqrt{5}}{2}$, e $\lambda_2 = \|b_1\| = \sqrt{2}$

Principais problemas

Seja Λ reticulado com distância mínima λ_1

Principais problemas

Seja Λ reticulado com distância mínima λ_1

- **SVP (problema do vetor mais curto):** dada uma matriz geradora B de Λ, encontrar $v \in \Lambda$ tal que $\|v\|_2 = \lambda_1$.

Principais problemas

Seja Λ reticulado com distância mínima λ_1

- **SVP (problema do vetor mais curto):** dada uma matriz geradora B de Λ, encontrar $v \in \Lambda$ tal que $\|v\|_2 = \lambda_1$.
- **CVP (problema do vetor mais próximo):** dada uma matriz geradora B de Λ, e $x \in \mathbb{R}^n$, encontrar $v \in \Lambda$ que minimize $\|x - v\|_2$.

Principais problemas

Seja Λ reticulado com distância mínima λ_1

- **SVP (problema do vetor mais curto):** dada uma matriz geradora B de Λ, encontrar $v \in \Lambda$ tal que $\|v\|_2 = \lambda_1$.
- **CVP (problema do vetor mais próximo):** dada uma matriz geradora B de Λ, e $x \in \mathbb{R}^n$, encontrar $v \in \Lambda$ que minimize $\|x - v\|_2$.
- **SIVP (problema dos vetores independentes mais curtos):** dada uma matriz geradora B de Λ, encontrar um conjunto LI $\{v_1, \ldots, v_k\}$ tal que $\max_{i \in \{1,\ldots,k\}} \|v_i\|_2 = \lambda_k$.

Principais problemas

Seja Λ reticulado com distância mínima λ_1

- **SVP (problema do vetor mais curto):** dada uma matriz geradora B de Λ, encontrar $v \in \Lambda$ tal que $\|v\|_2 = \lambda_1$.
- **CVP (problema do vetor mais próximo):** dada uma matriz geradora B de Λ, e $x \in \mathbb{R}^n$, encontrar $v \in \Lambda$ que minimize $\|x - v\|_2$.
- **SIVP (problema dos vetores independentes mais curtos):** dada uma matriz geradora B de Λ, encontrar um conjunto LI $\{v_1, \ldots, v_k\}$ tal que $\max_{i \in \{1,\ldots,k\}} \|v_i\|_2 = \lambda_k$.
- suas diversas variações: GapSVP, GapCVP, BDD etc.

Complexidade destes problemas

- SVP: é demonstrado NP-difícil para reduções aleatórias, e para a versão do problema na norma $\|\cdot\|_\infty$

Complexidade destes problemas

- SVP: é demonstrado NP-difícil para reduções aleatórias, e para a versão do problema na norma $\|\cdot\|_\infty$
- CVP: é NP-completo

Complexidade destes problemas

- SVP: é demonstrado NP-difícil para reduções aleatórias, e para a versão do problema na norma $\|\cdot\|_\infty$
- CVP: é NP-completo
- SIVP: é NP-completo

No caso de termos uma base ortogonal, são fáceis!

Seja $b_1, \ldots, b_n$ base ortogonal de Λ.

- SVP: $\|v\|^2 = \alpha_1^2\|b_1\|^2 + \cdots + \alpha_n^2\|b_n\|^2$
  (basta tomar $\min_i \alpha_i = 1$ e o resto 0)

No caso de termos uma base ortogonal, são fáceis!

Seja $b_1, \ldots, b_n$ base ortogonal de Λ.

- SVP: $\|v\|^2 = \alpha_1^2\|b_1\|^2 + \cdots + \alpha_n^2\|b_n\|^2$
  (basta tomar $\min_i \alpha_i = 1$ e o resto 0)
- CVP: $\|v - x\|^2 = (\alpha_1 - \beta_1)^2\|b_1\|^2 + \cdots + (\alpha_n - \beta_n)^2\|b_n\|^2$
  (basta tomar $\alpha_i = \lfloor \beta_i \rceil$)

Gaussianas

- definiremos a *função gaussiana* com parâmetros $\mu \in \mathbb{R}^n$, $s > 0$ como a função $\rho_{\mu,s} \colon \mathbb{R}^n \to \mathbb{R}_+$,

$$\rho_{\mu,s}(x) = \exp\left(-\pi \cdot \frac{\|x-\mu\|^2}{s^2}\right)$$

e $\rho_s \coloneqq \rho_{0,s}$.

Gaussianas

- definiremos a *função gaussiana* com parâmetros $\mu \in \mathbb{R}^n$, $s > 0$ como a função $\rho_{\mu,s} \colon \mathbb{R}^n \to \mathbb{R}_+$,

$$\rho_{\mu,s}(x) = \exp\left(-\pi \cdot \frac{\|x-\mu\|^2}{s^2}\right)$$

  e $\rho_s \coloneqq \rho_{0,s}$.

- essa gaussiana não é normalizada: $\int_{\mathbb{R}^n} \rho_{\mu,s}(x)\,\mathrm{d}x = s^n$. Assim, dividimos por s^n para encontrar a função densidade de probabilidade.

Gaussianas

- definiremos a *função gaussiana* com parâmetros $\mu \in \mathbb{R}^n$, $s > 0$ como a função $\rho_{\mu,s} \colon \mathbb{R}^n \to \mathbb{R}_+$,

$$\rho_{\mu,s}(x) = \exp\left(-\pi \cdot \frac{\|x-\mu\|^2}{s^2}\right)$$

  e $\rho_s := \rho_{0,s}$.

- essa gaussiana não é normalizada: $\int_{\mathbb{R}^n} \rho_{\mu,s}(x)\,\mathrm{d}x = s^n$. Assim, dividimos por s^n para encontrar a função densidade de probabilidade.

- após normalizar, a substituição $s = \sqrt{2\pi}\sigma$ retorna aos parâmetros (μ, σ) usuais de gaussianas

Seja Λ reticulado de posto completo ($\dim \Lambda = n$)

- para qualquer conjunto da forma $x + \Lambda$, definimos

$$\mathcal{P}_{\mu,s}(x+\Lambda) := \frac{1}{s^n}\rho_{\mu,s}(x+\Lambda) = \sum_{v\in\Lambda}\frac{1}{s^n}\rho_{\mu,s}(x+v)$$

Seja Λ reticulado de posto completo ($\dim \Lambda = n$)

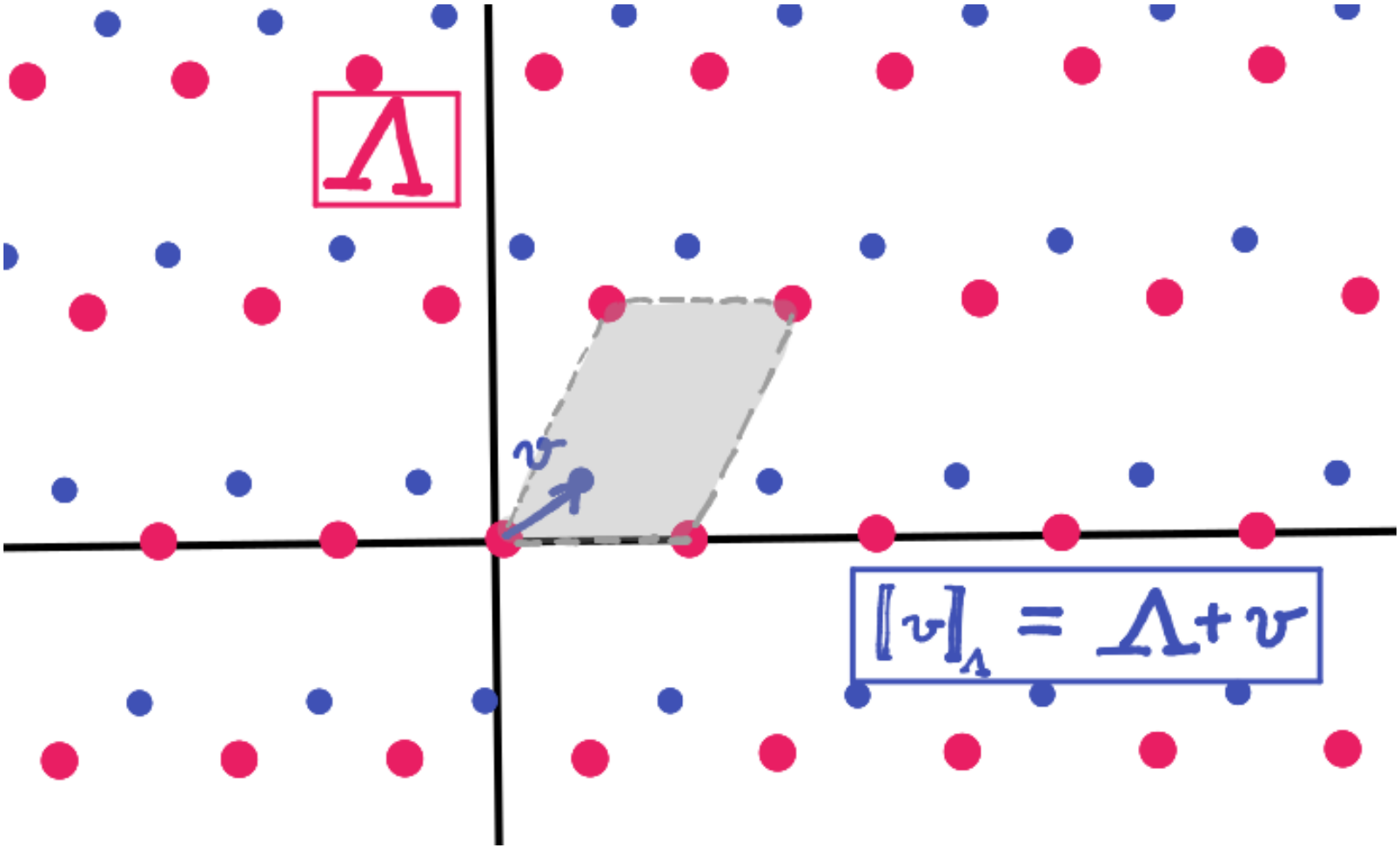
- para qualquer conjunto da forma $x + \Lambda$, definimos

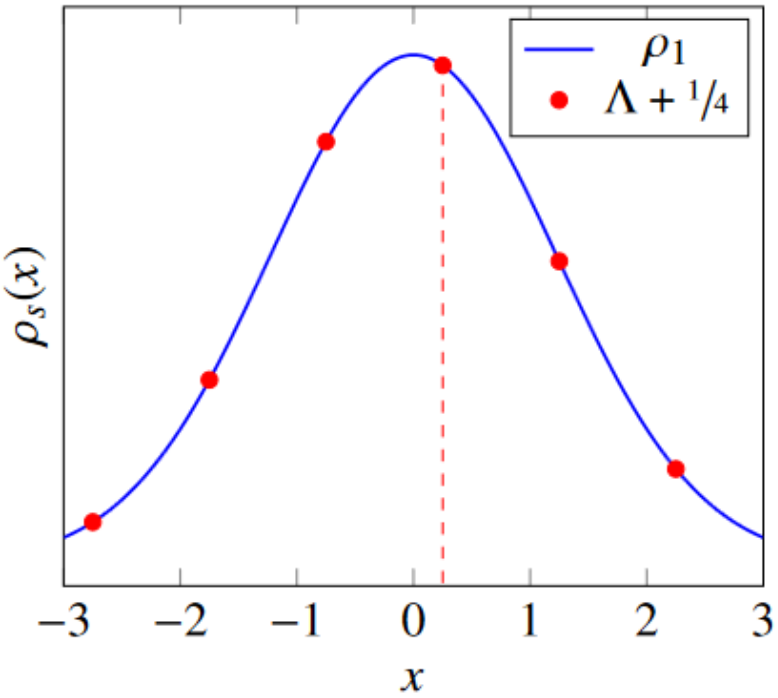
$$\mathcal{P}_{\mu,s}(x+\Lambda) := \frac{1}{s^n}\rho_{\mu,s}(x+\Lambda) = \sum_{v\in\Lambda}\frac{1}{s^n}\rho_{\mu,s}(x+v)$$

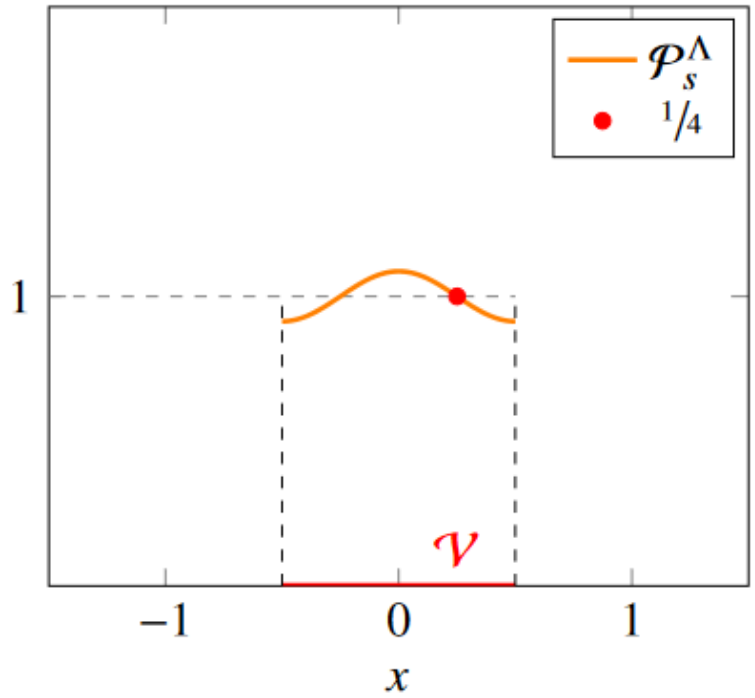
- isto define uma distribuição de probabilidade sobre

$$\mathbb{R}^n/\Lambda = \{x+\Lambda : x \in \mathbb{R}^n\},$$

que é topologicamente equivalente ao toro n-dimensional.


Λ
v
$[v]_\Lambda = \Lambda + v$





- vemos que a distribuição $\mathcal{P}_s(x + \Lambda)$ é aproximadamente uniforme

Identificação com região fundamental

- uma região fundamental de Λ é um conjunto $\mathcal{D} \subset \mathbb{R}^n$ mensurável, tal que

Identificação com região fundamental

- uma região fundamental de Λ é um conjunto $\mathcal{D} \subset \mathbb{R}^n$ mensurável, tal que
  1. $\bigcup_{v \in \Lambda}(v + \mathcal{D}) = \mathbb{R}^n$,

Identificação com região fundamental

- uma região fundamental de Λ é um conjunto $\mathcal{D} \subset \mathbb{R}^n$ mensurável, tal que
  1. $\bigcup_{v \in \Lambda}(v + \mathcal{D}) = \mathbb{R}^n$,
  2. $(v + \Lambda) \cap (w + \Lambda) = \emptyset$ para $v \neq w$ em Λ.

Identificação com região fundamental

- uma região fundamental de Λ é um conjunto $\mathcal{D} \subset \mathbb{R}^n$ mensurável, tal que
  1. $\bigcup_{v \in \Lambda}(v + \mathcal{D}) = \mathbb{R}^n$,
  2. $(v + \Lambda) \cap (w + \Lambda) = \emptyset$ para $v \neq w$ em Λ.
- existe uma bijeção $\mathcal{D} \to \mathbb{R}^n/\Lambda$ dada por $x \mapsto (x + \Lambda)$

Identificação com região fundamental

- uma região fundamental de Λ é um conjunto $\mathcal{D} \subset \mathbb{R}^n$ mensurável, tal que
  1. $\bigcup_{v \in \Lambda}(v + \mathcal{D}) = \mathbb{R}^n$,
  2. $(v + \Lambda) \cap (w + \Lambda) = \emptyset$ para $v \neq w$ em Λ.
- existe uma bijeção $\mathcal{D} \to \mathbb{R}^n/\Lambda$ dada por $x \mapsto (x + \Lambda)$
  - isso significa que podemos fixar uma região fundamental $\mathcal{D}$ e olhar para a distribuição $\rho_{\mu,s}(x + \Lambda)$ definida sobre $\mathcal{D}$.

Identificação com região fundamental

- uma região fundamental de Λ é um conjunto $\mathcal{D} \subset \mathbb{R}^n$ mensurável, tal que
  1. $\bigcup_{v \in \Lambda}(v + \mathcal{D}) = \mathbb{R}^n$,
  2. $(v + \Lambda) \cap (w + \Lambda) = \emptyset$ para $v \neq w$ em Λ.
- existe uma bijeção $\mathcal{D} \to \mathbb{R}^n/\Lambda$ dada por $x \mapsto (x + \Lambda)$
  - isso significa que podemos fixar uma região fundamental $\mathcal{D}$ e olhar para a distribuição $\rho_{\mu,s}(x + \Lambda)$ definida sobre $\mathcal{D}$.
- a distribuição uniforme sobre $\mathcal{D} \simeq \mathbb{R}^n/\Lambda$ é dada por $u(x) = \frac{1}{\det \Lambda} = \frac{1}{\operatorname{vol} \mathcal{D}}$

Soma de Poisson

- A *fórmula da soma de Poisson* é uma (inesperada) relação entre o reticulado dual

$$\Lambda^* = \left\{ w \in \mathbb{R}^n \;\middle|\; \langle w, v \rangle \in \mathbb{Z} \; \forall v \in \Lambda \right\} \simeq \mathsf{Hom}(\Lambda, \mathbb{Z})$$

e transformadas de Fourier!

Soma de Poisson

- A *fórmula da soma de Poisson* é uma (inesperada) relação entre o reticulado dual

$$\Lambda^* = \left\{ w \in \mathbb{R}^n \;\middle|\; \langle w, v \rangle \in \mathbb{Z} \; \forall v \in \Lambda \right\} \simeq \mathrm{Hom}(\Lambda, \mathbb{Z})$$

  e transformadas de Fourier!

- A transformada de Fourier de uma função $f : \mathbb{R}^n \to \mathbb{C}$ é dada por:

$$\hat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi i \langle x, y \rangle} f(x) \, \mathrm{d}x$$

Soma de Poisson

- A *fórmula da soma de Poisson* é uma (inesperada) relação entre o reticulado dual

$$\Lambda^* = \left\{ w \in \mathbb{R}^n \;\middle|\; \langle w, v \rangle \in \mathbb{Z} \; \forall v \in \Lambda \right\} \simeq \mathrm{Hom}(\Lambda, \mathbb{Z})$$

  e transformadas de Fourier!

- A transformada de Fourier de uma função $f : \mathbb{R}^n \to \mathbb{C}$ é dada por:

$$\hat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi i \langle x, y \rangle} f(x) \, \mathrm{d}x$$

- em particular, a transformada de fourier de ρ_s é $s^n \rho_{1/s}$

Colocamos as seguinte condições de regularidade sobre $f : \mathbb{R}^n \to \mathbb{C}$:

Colocamos as seguinte condições de regularidade sobre $f : \mathbb{R}^n \to \mathbb{C}$:

1. (R1) $\int_{\mathbb{R}^n} \left|f(x)\right| \mathrm{d}x < \infty$,
2. (R2) $\sum_{v \in \Lambda} \left|f(v+u)\right|$ converge uniformemente para u dentro de um compacto de $\mathbb{R}^n$
3. (R3) a transformada de Fourier $\hat{f}$ satisfaz: $\sum_{w \in \Lambda^*} \hat{f}(w)$ é absolutamente convergente

Colocamos as seguinte condições de regularidade sobre $f : \mathbb{R}^n \to \mathbb{C}$:

1. (R1) $\int_{\mathbb{R}^n} \left|f(x)\right| \mathrm{d}x < \infty$,
2. (R2) $\sum_{v\in\Lambda} \left|f(v+u)\right|$ converge uniformemente para u dentro de um compacto de $\mathbb{R}^n$
3. (R3) a transformada de Fourier $\hat{f}$ satisfaz: $\sum_{w\in\Lambda^*} \hat{f}(w)$ é absolutamente convergente

Theorem (Soma de Poisson)

Se $f : \mathbb{R}^n \to \mathbb{C}$ satisfaz (C1), (C2) e (C3),

$$\sum_{v\in\Lambda} f(v) = \frac{1}{\det\Lambda} \cdot \sum_{w\in\Lambda^*} \hat{f}(w)$$

Parâmetro de suavidade

O parâmetro de suavidade de um reticulado Λ é definido como

$$\eta_\varepsilon(\Lambda) := \inf\left\{ s > 0 \;\middle|\; \rho_{1/s}(\Lambda^* \setminus \{0\}) \leq \varepsilon \right\}$$

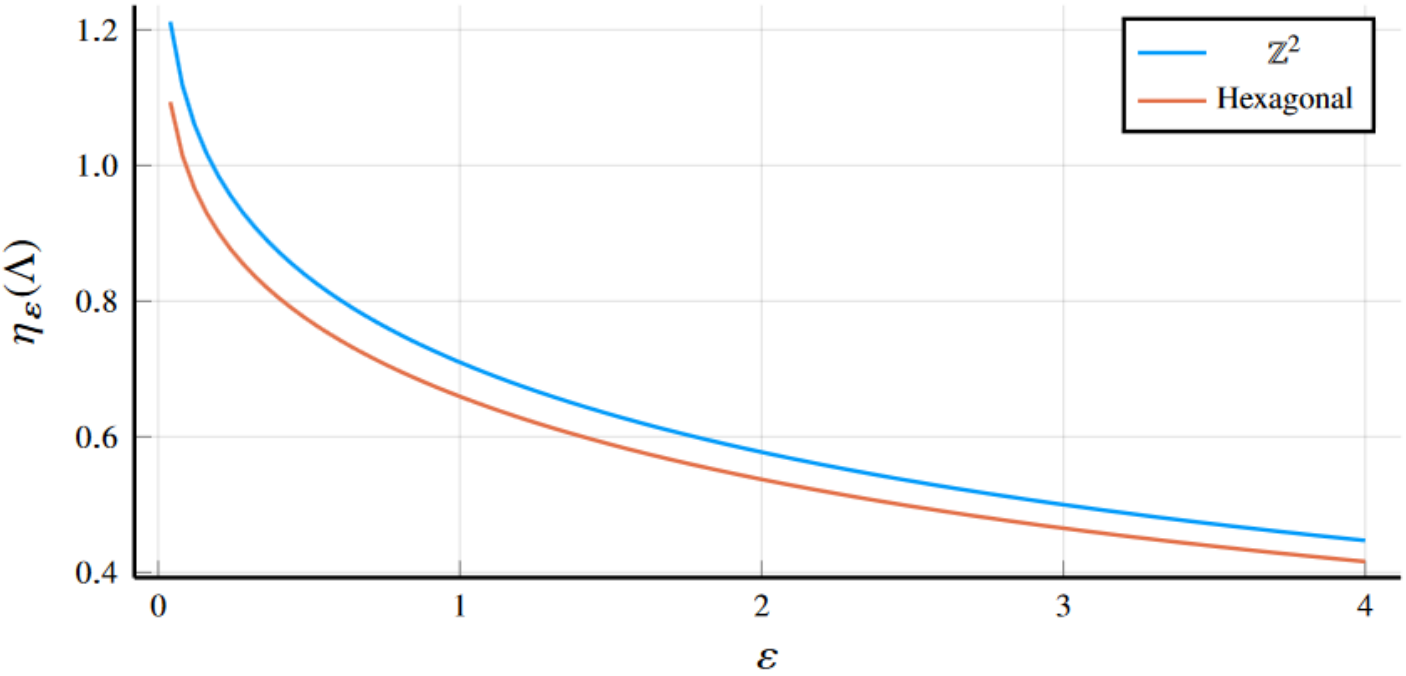


Figura 3.8: Parâmetro de suavização dos reticulados $\mathbb{Z}^2$ e hexagonal.

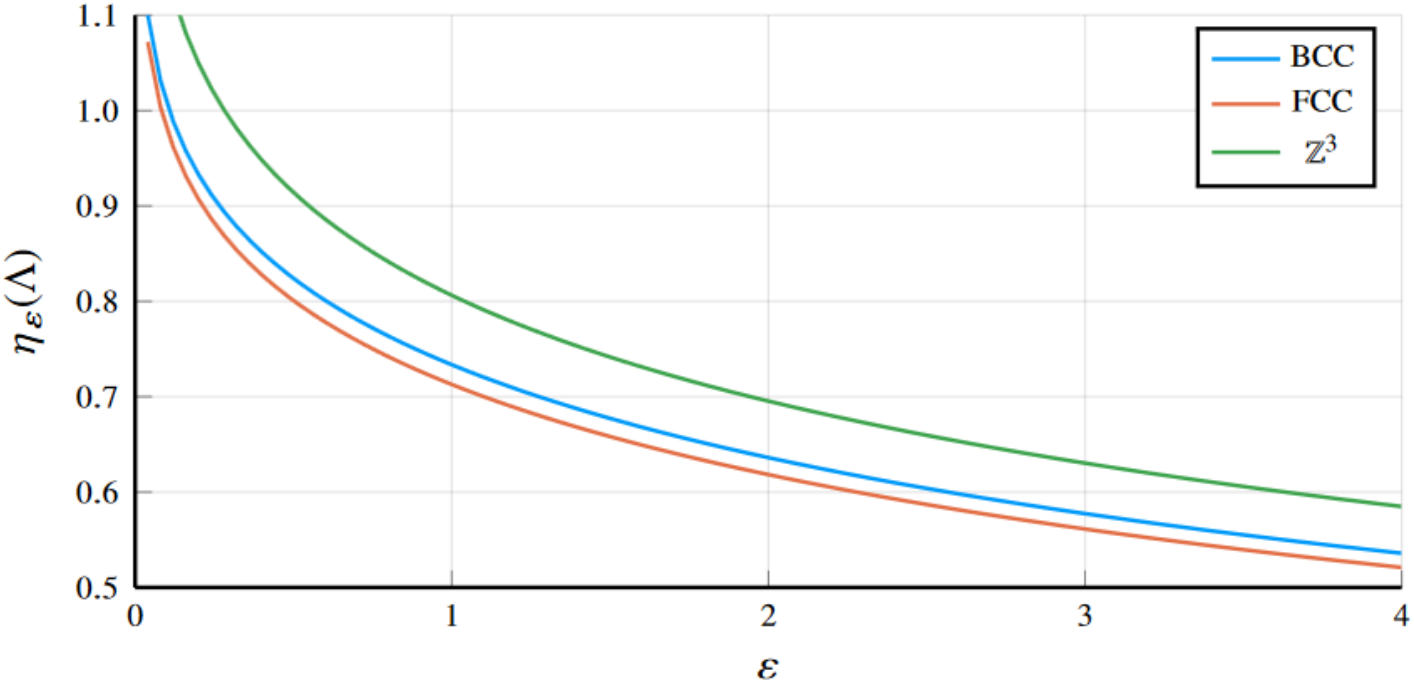


Figura 3.9: Parâmetro de suavização dos reticulados BCC, FCC e $\mathbb{Z}^3$.

- o parâmero de suavização nos diz que se $s \geq \eta_\varepsilon(\Lambda)$ é o parâmetro de ρ_s, então a distribuição $\mathcal{P}_s(x + \Lambda)$ está ε-próxima da distribuição uniforme!

- o parâmero de suavização nos diz que se $s \geq \eta_\varepsilon(\Lambda)$ é o parâmetro de ρ_s, então a distribuição $\mathcal{P}_s(x + \Lambda)$ está ε-próxima da distribuição uniforme!
- Porque? Pela soma de Poisson:

$$\mathcal{P}_s(x + \Lambda) = \frac{1}{s^n}\rho_s(x + \Lambda) = \frac{1}{\det \Lambda} \sum_{w \in \Lambda^*} e^{2\pi i \langle x, w \rangle} \rho_{1/s}(w)$$

- o parâmero de suavização nos diz que se $s \geq \eta_\varepsilon(\Lambda)$ é o parâmetro de ρ_s, então a distribuição $\mathcal{P}_s(x+\Lambda)$ está ε-próxima da distribuição uniforme!
- Porque? Pela soma de Poisson:

$$\mathcal{P}_s(x+\Lambda) = \frac{1}{s^n}\rho_s(x+\Lambda) = \frac{1}{\det\Lambda}\sum_{w\in\Lambda^*} e^{2\pi i\langle x,w\rangle}\rho_{1/s}(w)$$

- do fato que $\left\| e^{2\pi i\langle x,w\rangle} \right\| = 1$, temos que

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

- em outras palavras, $\eta_\varepsilon(\Lambda)$ é o menor $s > 0$ tal que

$$\det \Lambda \cdot \|\mathcal{P}_s - u\|_\infty < \varepsilon$$

- em outras palavras, $\eta_\varepsilon(\Lambda)$ é o menor $s > 0$ tal que

$$\det \Lambda \cdot \|\mathcal{P}_s - u\|_\infty < \varepsilon$$

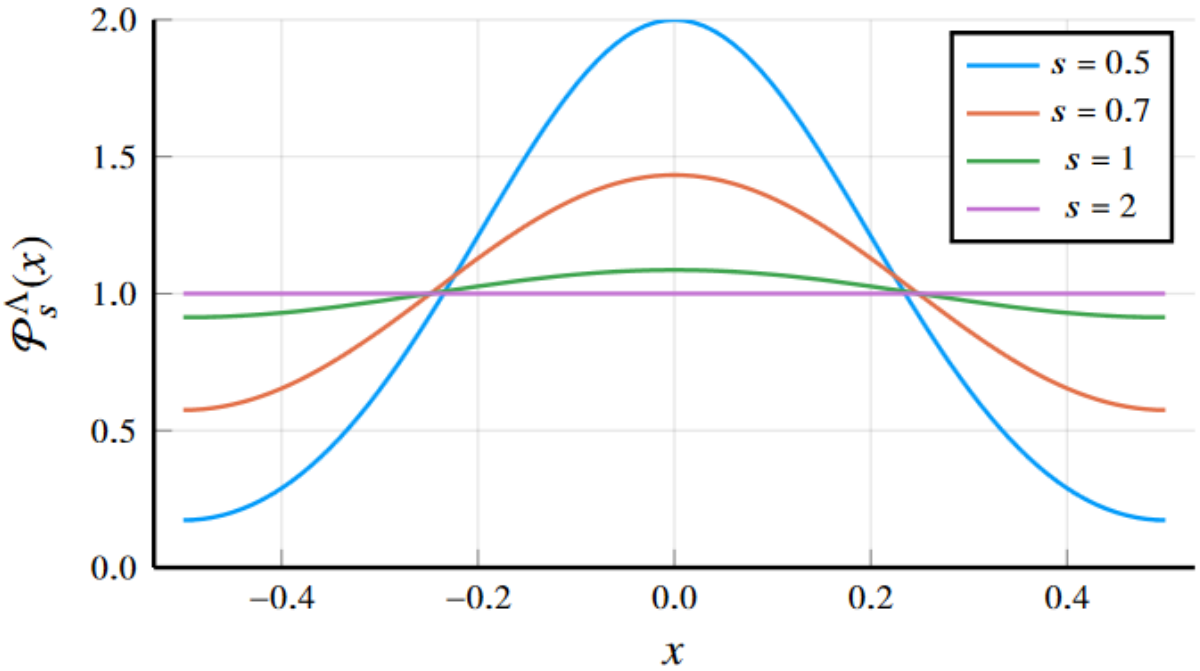


Figura 3.10: Gráfico de $\mathcal{P}_s^\Lambda(x)$ em função de x, para $s \in \{0.5, 0.7, 1, 2\}$.

Gaussianas discretas

- a discretização de uma gaussiana sobre um reticulado Λ é a distribuição de probabilidade

$$D_{\Lambda,s}(v) = \frac{\rho_s(v)}{\rho_s(\Lambda)}, \qquad v \in \Lambda.$$

Gaussianas discretas

- a discretização de uma gaussiana sobre um reticulado Λ é a distribuição de probabilidade

$$D_{\Lambda,s}(v) = \frac{\rho_s(v)}{\rho_s(\Lambda)}, \qquad v \in \Lambda.$$

- porém, se s é muito pequeno, $D_{\Lambda,s}$ não terá "cara" de gaussiana

Gaussianas discretas

- a discretização de uma gaussiana sobre um reticulado Λ é a distribuição de probabilidade

$$D_{\Lambda,s}(v) = \frac{\rho_s(v)}{\rho_s(\Lambda)}, \qquad v \in \Lambda.$$

- porém, se s é muito pequeno, $D_{\Lambda,s}$ não terá "cara" de gaussiana
- o parâmetro de suavidade tem a ver com o quão "suave" é a gaussiana discretizada, no sentido de ter formato de gaussiana

Problema DGS

- as gaussianas discretas são base para o problema DGS (amostragem gaussiana discreta)

Problema DGS

- as gaussianas discretas são base para o problema DGS (amostragem gaussiana discreta)
- este problema é relevante pois alguns dos mais modernos esquemas criptográficos baseados em reticulados (LWE, SIS) são baseados nele

Problema DGS

- as gaussianas discretas são base para o problema DGS (amostragem gaussiana discreta)
- este problema é relevante pois alguns dos mais modernos esquemas criptográficos baseados em reticulados (LWE, SIS) são baseados nele
- **Problema DGS$_\varphi$:** Dado um reticulado Λ e um número $s > \varphi(\Lambda)$, obtenha uma amostra de $D_{\Lambda,s}$

Problema DGS

- as gaussianas discretas são base para o problema DGS (amostragem gaussiana discreta)
- este problema é relevante pois alguns dos mais modernos esquemas criptográficos baseados em reticulados (LWE, SIS) são baseados nele
- **Problema DGS$_\varphi$:** Dado um reticulado Λ e um número $s > \varphi(\Lambda)$, obtenha uma amostra de $D_{\Lambda,s}$
- Porque este é um problema difícil?

Problema DGS

- as gaussianas discretas são base para o problema DGS (amostragem gaussiana discreta)
- este problema é relevante pois alguns dos mais modernos esquemas criptográficos baseados em reticulados (LWE, SIS) são baseados nele
- **Problema DGS$_\varphi$:** Dado um reticulado Λ e um número $s > \varphi(\Lambda)$, obtenha uma amostra de $D_{\Lambda,s}$
- Porque este é um problema difícil?
  - se os parâmetros (φ) forem escolhidos apropriadamente, então com alta probabilidade são amostrados vetores curtos. Isso equivale a, com alta probabilidade, resolver uma versão aproximada do SVP

Problema DGS

- as gaussianas discretas são base para o problema DGS (amostragem gaussiana discreta)
- este problema é relevante pois alguns dos mais modernos esquemas criptográficos baseados em reticulados (LWE, SIS) são baseados nele
- **Problema DGS$_\varphi$:** Dado um reticulado Λ e um número $s > \varphi(\Lambda)$, obtenha uma amostra de $D_{\Lambda,s}$
- Porque este é um problema difícil?
  - se os parâmetros (φ) forem escolhidos apropriadamente, então com alta probabilidade são amostrados vetores curtos. Isso equivale a, com alta probabilidade, resolver uma versão aproximada do SVP
  - mais formalmente: se $s > \sqrt{2n}\eta_\varepsilon(\Lambda)$, então com alta probabilidade são amostrados vetores de norma $\leq \sqrt{n}s$

- **A poly-time algorithm to solve LWE_{p,Ψ_α} implies in a poly-time quantum algorithm to $GapSVP$.**

  In [REGEV09], lemma 3.20 reduces $DGS_{\sqrt{n}\gamma(n)/\lambda_1(L^*)}$ to $GapSVP_{100\sqrt{n}\gamma(n)}$ and theorem 3.1 (quantum) reduces $DGS_{\sqrt{2n}\eta_\epsilon(L)/\alpha}$ to LWE_{p,Ψ_α} for $0 < \alpha < 1$ and $\alpha \cdot p < 2\sqrt{n}$

- **A poly-time algorithm to solve LWE_{p,Ψ_α} implies in a poly-time quantum algorithm to $SIVP$**

  In [REGEV09], lemma 3.17 reduces $DGS_{\gamma(n)}$ to $GIVP_{2\sqrt{n}\phi(L)}$ (GIVP is a generalization of SIVP) and theorem 3.1 (quantum) reduces $DGS_{\sqrt{2n}\eta_\epsilon(L)/\alpha}$ to LWE_{p,Ψ_α} for $0 < \alpha < 1$ and $\alpha \cdot p < 2\sqrt{n}$

- Fonte: Regev – *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. (2009)*

Problema GapSPP

O próprio problema de determinar o parâmetro de suavização constitui um problema criptográfico com parâmetros $\varepsilon > 0$, $\gamma > 1$, dado a seguir.

Problema GapSPP

O próprio problema de determinar o parâmetro de suavização constitui um problema criptográfico com parâmetros $\varepsilon > 0$, $\gamma > 1$, dado a seguir.

- **Problema γ-GapSPP$_\varepsilon$:** dada uma base B de um reticulado Λ, determinar se:
  - $\eta_\varepsilon(\Lambda) \leq 1$
  - $\eta_\varepsilon(\Lambda) \geq \gamma$

Problema GapSPP

O próprio problema de determinar o parâmetro de suavização constitui um problema criptográfico com parâmetros $\varepsilon > 0$, $\gamma > 1$, dado a seguir.

- **Problema γ-GapSPP$_\varepsilon$:** dada uma base B de um reticulado Λ, determinar se:
  - $\eta_\varepsilon(\Lambda) \leq 1$
  - $\eta_\varepsilon(\Lambda) \geq \gamma$

É mostrado que este problema está nas classes de complexidade AM e SZK.

Fator de achatamento

- concluiremos comentando que o parâmetro de suavidade é equivalente a uma outra quantidade chamada de *fator de achatamento*, muito usada na área de codificação para canais Wiretap e AWGN

Fator de achatamento

- concluiremos comentando que o parâmetro de suavidade é equivalente a uma outra quantidade chamada de *fator de achatamento*, muito usada na área de codificação para canais Wiretap e AWGN
- o fator de achatamento é o valor $\epsilon_\Lambda(\sigma)$ tal que que $\eta_{\epsilon_\Lambda(\sigma)}(\Lambda) = \sqrt{2\pi}\sigma$

Fator de achatamento

- concluiremos comentando que o parâmetro de suavidade é equivalente a uma outra quantidade chamada de *fator de achatamento*, muito usada na área de codificação para canais Wiretap e AWGN
- o fator de achatamento é o valor $\epsilon_\Lambda(\sigma)$ tal que que $\eta_{\epsilon_\Lambda(\sigma)}(\Lambda) = \sqrt{2\pi}\sigma$
  - o parâmetro de suavização é o parâmetro s que produz um achatamento ε

Fator de achatamento

- concluiremos comentando que o parâmetro de suavidade é equivalente a uma outra quantidade chamada de *fator de achatamento*, muito usada na área de codificação para canais Wiretap e AWGN
- o fator de achatamento é o valor $\epsilon_\Lambda(\sigma)$ tal que que $\eta_{\epsilon_\Lambda(\sigma)}(\Lambda) = \sqrt{2\pi}\sigma$
  - o parâmetro de suavização é o parâmetro s que produz um achatamento ε
  - o fator de achatamento é o achatamento ε produzido por um parâmetro $\sigma = \frac{s}{\sqrt{2\pi}}$

Fator de achatamento

- concluiremos comentando que o parâmetro de suavidade é equivalente a uma outra quantidade chamada de *fator de achatamento*, muito usada na área de codificação para canais Wiretap e AWGN
- o fator de achatamento é o valor $\epsilon_\Lambda(\sigma)$ tal que que $\eta_{\epsilon_\Lambda(\sigma)}(\Lambda) = \sqrt{2\pi}\sigma$
  - o parâmetro de suavização é o parâmetro s que produz um achatamento ε
  - o fator de achatamento é o achatamento ε produzido por um parâmetro $\sigma = \frac{s}{\sqrt{2\pi}}$
  - em outras palavras, um é a função inversa do outro, a menos da constante $\sqrt{2\pi}$

o fator de achatamento é usado para

- construir códigos que atingem a capacidade no canal AWGN (com ruído aditivo gaussiano branco)

o fator de achatamento é usado para

- construir códigos que atingem a capacidade no canal AWGN (com ruído aditivo gaussiano branco)
- obter sigilo no canal Wiretap (fator de achatamento pequeno $\Longrightarrow$ ganho de sigilo grande)

o fator de achatamento é usado para

- construir códigos que atingem a capacidade no canal AWGN (com ruído aditivo gaussiano branco)
- obter sigilo no canal Wiretap (fator de achatamento pequeno $\Longrightarrow$ ganho de sigilo grande)
- outras aplicações na área de teoria da informação

Para ler mais

- Regev – *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography.* (2009)
- Peikert – *A decade of lattice cryptography* (2016)
- Dissertação: `https://fabiom.net/docs/dissertacao.pdf`
- Esta apresentação: `https://fabiom.net/docs/crypto-lattice-2022.pdf`