UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

Fábio Campos Castro Meneghetti

Reticulados: um estudo de alguns parâmetros relevantes para aplicações em criptografia

Campinas
2020

Fábio Campos Castro Meneghetti

Reticulados: um estudo de alguns parâmetros relevantes para aplicações em criptografia

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática.

Orientadora: Sueli Irene Rodrigues Costa

Este exemplar corresponde à versão final da Dissertação defendida pelo aluno Fábio Campos Castro Meneghetti e orientada pela Profa. Dra. Sueli Irene Rodrigues Costa.

Campinas
2020

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

M524r

Meneghetti, Fábio Campos Castro, 1996-
Reticulados : um estudo de alguns parâmetros relevantes para aplicações em criptografia / Fábio Campos Castro Meneghetti. – Campinas, SP : [s.n.], 2020.

Orientador: Sueli Irene Rodrigues Costa.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos reticulados. 2. Criptografia pós-quântica. 3. Distribuição gaussiana. I. Costa, Sueli Irene Rodrigues. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Lattices : a study of some relevant parameters for applications in criptography
Palavras-chave em inglês:
Lattice theory
Post-quantum cryptography
Gaussian distribution
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Sueli Irene Rodrigues Costa [Orientador]
Grasiele Cristiane Jorge
Ricardo Dahab
Data de defesa: 09-03-2020
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0001-8323-1282
- Currículo Lattes do autor: http://lattes.cnpq.br/5029099102514492

Dissertação de Mestrado defendida em 09 de março de 2020 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof(a). Dr(a). RICARDO DAHAB

Prof(a). Dr(a). GRASIELE CRISTIANE JORGE

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Agradecimentos

Agradeço à Sueli Costa pela orientação, ajuda e todo o apoio que foi muito importante para mim. Agradeço também aos meus orientadores durante a graduação, Marcelo Firer e Sara Cardell, que foram muito importantes para a minha formação.

Agradeço também aos professores do IMECC pelo aprendizado nos excelentes cursos do programa, e aos funcionários do IMECC que são essenciais para o funcionamento da instituição. Agradeço principalmente à dona Zefa, cujos cafés, sempre feitos com muito amor, foram essenciais para minha graduação e meu mestrado.

Agradeço aos meus colegas pelas discussões profundas, estudos em grupo e amizade: Pedro Mattos, Caio Laurenti, Vinícius Vasconcelos, Renato Leme, Bianca Dornelas, Aline D'Oliveira, Leonardo Schultz, Flávio Kajiwara, Alejandro Otero, Isabel Triviño, Fernando Sônego. E agradeço aos meus pais, Suzana e Marcelo, que sempre me incentivaram a estudar o que eu gostasse, e me deram todo o apoio e carinho necessário para isso.

Agradeço também aos desenvolvedores do TEX e de todos os pacotes da distribuição TEX Live por trabalharem para a construção dessas ferramentas livres e gratuitas que são extremamente necessárias na elaboração de textos científicos.

Por fim, agradeço ao CNPq pela bolsa de pesquisa (processo 131290/2018-5), que foi um verdadeiro privilégio nestes tempos de desvalorização da pesquisa e da ciência no Brasil.

Resumo

Neste trabalho estudamos parâmetros de reticulados que são relevantes para aplicações na chamada criptografia pós-quântica, em sistemas importantes como LWE e SIS. São analisados o parâmetro de suavização, particularmente nos reticulados mais densos conhecidos em baixas dimensões, bem como reticulados ideais e reticulados q-ários.

Palavras chave: reticulados, criptografia pós-quântica, parâmetro de suavização

Abstract

In this work we study lattice parameters which are relevant for applications to the so called post-quantum cryptography, in important systems such as LWE and SIS. We analyze the smoothing parameter, particularly for the densest known lattices in lower dimensions, as well as ideal lattices and q-ary lattices.

Keywords: lattices, post-quantum cryptography, smoothing parameter

Notações e Símbolos

$\mathbb{N}$	O conjunto dos números naturais sem o 0.
$\mathbb{Z}$	O conjunto dos números inteiros.
$\mathbb{Z}_q$	O anel dos inteiros módulo q.
$\mathbb{Q}$	O conjunto dos números racionais.
$\mathbb{R}$	O conjunto dos números reais.
$\mathbb{R}_{>0}$	O conjunto dos números reais estritamente positivos.
$\mathbb{R}_{\geq 0}$	O conjunto dos números reais maiores ou iguais a zero.
$\mathbb{C}$	O conjunto dos números complexos.
$\mathbb{R}^n$	O espaço euclidiano n-dimensional.
$\mathbb{H}$	O hiperplano superior complexo, isto é, o conjunto dos números complexos com parte imaginária estritamente positiva.
$A^{m\times n}$	O conjunto de matrizes $m \times n$ com entradas no anel A.
I_n	A matriz identidade $n \times n$.
$M^\top$	A transposta da matriz M.
$B_r(x)$	A bola aberta de centro x e raio r, em $\mathbb{R}^n$.
$A[X]$	O anel de polinômios sobre o anel A.
$\subset$	Denota continência de conjuntos não-estrita.
$\langle \cdot, \cdot \rangle$	Produto interno de vetores em $\mathbb{R}^n$, dado por $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$.
$\|\cdot\|$	Quando não especificado refere-se à norma 2 em $\mathbb{R}^n$, dada por $\|x\| = \sqrt{\langle x, x \rangle}$.
$\delta_{i,j}$	A função delta de Dirac, que vale 1 se $i = j$, e 0 se $i \neq j$.
$\Pr[\cdot]$	Denota a função "probabilidade".

Sumário

Capítulo 1

Introdução

Neste trabalho apresentamos um estudo de reticulados em $\mathbb{R}^n$, isto é, conjuntos formados por combinações inteiras de vetores independentes, dando particular ênfase aos aspectos relevantes destes para segurança e confiabilidade da informação. Procuramos definir e caracterizar propriedades sobre parâmetros de reticulados que são úteis para criptografia e explicar como esses parâmetros são utilizados.

O estudo de reticulados e suas propriedades teve grande ampliação com a publicação do livro "Sphere Packings, Lattices and Groups" de J. H. Conway e N. J. A. Sloane [CS99], uma das principais referências desta subárea. Entre os temas do livro, são apresentadas diversas análises do ponto de vista matemático, principalmente para problemas relacionados ao empacotamento e cobertura de esferas no espaço. O problema do empacotamento de esferas consiste em determinar qual arranjo de esferas de mesmo tamanho, no espaço n-dimensional, é capaz de preenchê-lo com maior densidade média. Por exemplo, em dimensão 2, o melhor empacotamento é dado por um arranjo hexagonal, como é encontrado nas colmeias de abelhas, ou na forma como bolhas de mesmo tamanho se organizam sobre a superfície da água. Este é um exemplo de *arranjo em reticulado*, pois o conjunto dos centros das bolas forma um reticulado (no caso, o *reticulado hexagonal*).

Já na dimensão 3, o problema foi estudado em profundidade pelo astrônomo e matemático Johannes Kepler. Em 1611, Kepler publicou o folheto *Strena seu de Nive Sexangula*, onde questiona o motivo dos flocos de neve sempre parecerem ter um formato hexagonal. No escrito, Kepler formula pela primeira vez o que viria a ser chamado de *conjectura de Kepler*: a afirmação de que nenhum arranjo de esferas preenche mais densamente o espaço tridimensional do que o empacotamento cúbico centrado nas faces (FCC), e o empacotamento hexagonal próximo (HCP) [Kep10]. Kepler não provou sua afirmação, mas o próximo passo foi tomado por Carl Friedrich Gauss, que provou em um artigo de 1831 que a conjectura de Kepler vale quando restrita a arranjos em reticulados [Gau31]. A versão geral permaneceu em aberto, e fez parte da famosa lista dos 23 problemas de Hilbert, publicada em 1900. Em 1998 Thomas Hales anunciou a descoberta de uma prova por exaustão que envolvia a verificação de muitos casos individuais, computacionalmente. A prova foi publicada apenas em 2017 [Hal+17], e foram utilizados os

softwares provadores de teoremas Isabelle e HOL Light.

Outro problema relevante relacionado é o do *kissing number*, que pergunta qual é o número de esferas unitárias que podem ser colocadas tocando uma esfera comum fixada, também unitária. O problema se tornou famoso com a conhecida disputa entre o físico Isaac Newton e o astrônomo David Gregory, em 1694. Newton afirmava que a resposta na dimensão 3 era 12, dada pelo reticulado A_3, enquanto Gregory acreditava que seria possível adicionar ainda mais uma bola [Slo84]. A prova definitiva que esse número é 12 foi dada apenas em 1953, e até hoje o kissing number é conhecido apenas nas dimensões 1, 2, 3, 4, 8 e 24 [BV08].

Os reticulados começaram a ganhar maior destaque a partir do surgimento da teoria da informação de Shannon, que tem como um marco a publicação do artigo "A Mathematical Theory of Communication" em 1948 [Sha48]. Os reticulados têm diversas aplicações nessa área, dentre as quais quantização para sinais com ruído aditivo branco gaussiano (*additive white Gaussian noise* — AWNG) [Zam09], bem como no uso de codificação por classes laterais (*coset coding*) para canais do tipo *wiretap* [Wyn75][OSB16][BO10].

Mais recentemente, tem surgido um interesse por reticulados dentro da área de criptografia, que consiste no estudo e prática de técnicas para comunicação segura na presença de adversários. Dentre as características desejadas para essa comunicação destacam-se quatro: *confidencialidade*, a garantia de que indivíduos não autorizados não lerão a informação; *integridade*, a garantia de que a informação não seja perdida; *autenticação*, a verificação da identidade de um indivíduo, e *não-repúdio*, a certeza da autoria de uma mensagem [Riv90].

Um esquema criptográfico é a descrição de um método para comunicação, que preferencialmente tenha essas quatro características. A garantia da segurança é em geral baseada em problemas matemáticos para os quais haja evidência de que são difíceis (computacionalmente falando). Esta evidência pode ser tanto uma prova teórica (por exemplo NP-completude), quanto prática (problemas que foram atacados por muito tempo, sem sucesso)[Riv90]. Porém, alguns dos problemas mais utilizados atualmente, como o problema de fatoração em primos ou o problema do logaritmo discreto foram abalados com a descoberta de algoritmos quânticos que os resolvem de forma eficiente [Sho94]. Ainda não existem computadores quânticos poderosos o suficiente para rodar esses algoritmos; mas essa área tem tido intensa pesquisa e rápidos avanços com máquinas cada vez mais eficientes. A Google, por exemplo, anunciou que demonstrou a *quantum supremacy* no final de 2019 [Aru+19].

A perspectiva desses algoritmos quânticos incentivou a busca por esquemas e problemas criptográficos alternativos aos mais convencionais, que sejam resistentes a computadores quânticos. Esse estudo é denominado *criptografia pós-quântica*, e envolve métodos baseados em diferentes áreas da matemática, como códigos, reticulados, equações multivariadas, funções *hash*, entre outros [Ber09]. Os esquemas criptográficos baseados em reticulados destacam-se por provas seguras de dificuldade em pior-caso, implementações simples e eficientes [MR09].

Em 2016 o NIST (*National Institute for Standards and Technology*) anunciou um concurso para formulação de padrões da criptografia, chamado *Post-Quantum Cryptography Standardi-*

zation. Das 82 submissões originais, 28 eram baseadas em reticulados; já na segunda etapa do concurso, em 2019, 12 das 26 submissões restantes são baseadas em reticulados [Ala+19]. Isso mostra como a criptografia baseada em reticulados vem sendo amplamente estudada e considerada uma alternativa promissora aos esquemas tradicionais.

Os esquemas mais utilizados são baseados no problema chamado LWE (*learning with errors*) e sua generalização para anéis de polinômios sobre corpos finitos, chamada Ring-LWE (*ring learning with errors*) [Reg05][LPR12]. Eles são baseados em um problema que é originalmente da área de *machine learning*, chamado *parity learning*. O problema LWE consiste em, basicamente, dadas amostras $(x_i, y_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, onde $y_i = f(x_i) + \varepsilon_i$ para f linear e ε_i um erro gaussiano, descobrir f (ou uma aproximação) com alta probabilidade.

Em particular, estudamos nesta dissertação um parâmetro de reticulados que é amplamente utilizado nos problemas LWE, chamado *parâmetro de suavização* [Ajt96][Reg09]. Este parâmetro pode ser visto, intuitivamente, como a menor quantidade de erro gaussiano necessária para suavizar uma gaussiana discreta. Ele é utilizado na redução de pior-caso para caso-médio para vários problemas em construções criptográficas baseadas em reticulados (dentre as quais a LWE) e na dedução de alguns resultados de transferência para certas constantes [Pei+13]. Além das aplicações em criptografia pós-quântica, esse parâmetro tem relação com sistemas de codificação *wiretap* gaussianos, onde é utilizado um fator equivalente, chamado fator de achatamento (*flatness factor*). Esse fator foi introduzido em 2011 [Bel11]. No artigo [LLB12] é provada a equivalência entre o fator de achatamento e o parâmetro de suavização.

Esses fatos denotam o interesse no estudo do parâmetro de suavização em relação com parâmetros clássicos de reticulados, tais como: densidade de empacotamento, densidade de cobertura, distância mínima, entre outros [Pei+13]. Essa relação com os parâmetros de reticulados é enfatizada pelo fato de ser possível definir o parâmetro de suavização usando a série teta de reticulados.

O objetivo deste trabalho é fazer um estudo do parâmetro de suavização e sua relação com outros parâmetros de reticulados, e analisar as aplicações em criptografia e codificação de informações. Enfatizamos uma formulação mais precisa e adaptada ao rigor matemático de conceitos que são mais frequentemente publicados do ponto de vista de engenharia e computação; e por fim a análise de algumas simulações computacionais para melhor compreensão e comparação dos parâmetros. No Capítulo 2, fazemos uma introdução sobre reticulados, seus exemplos, e suas propriedades clássicas. No Capítulo 3 estudamos o parâmetro de suavização e suas propriedades, bem como algumas noções relacionadas a gaussianas sobre reticulados. Fazemos também algumas simulações computacionais para propósitos de comparação dos parâmetros. No Capítulo 4, apresentamos conceitos relevantes sobre criptografia, bem como alguns dos principais esquemas da criptografia baseada em reticulados.

Capítulo 2

Reticulados

Neste capítulo, fazemos uma introdução a conceitos e propriedades de reticulados. As principais referências utilizadas foram [CS99], [Cos+17], [Zam+14] e [Ebe12].

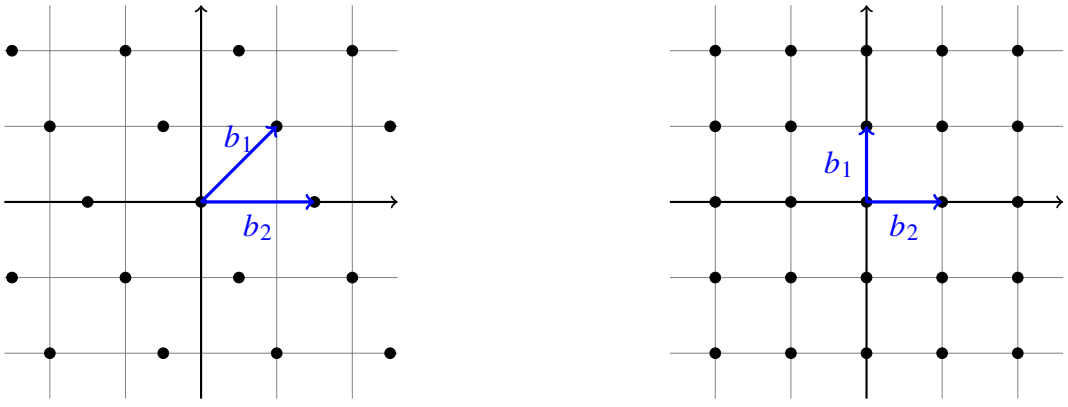
2.1 Definição e propriedades

Definição 2.1.1. [CS99] 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*.

Exemplo 2.1.2. 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) $\Lambda = \langle (0,1), (1,0) \rangle_{\mathbb{Z}} = \mathbb{Z}^2$.

Figura 2.1: Exemplos de reticulados de posto completo em $\mathbb{R}^2$.

Uma caracterização equivalente de reticulados é a destes serem *subgrupos aditivos discretos* de $\mathbb{R}^n$. Demonstramos aqui um dos sentidos, isto é, que todo reticulado é subgrupo aditivo discreto de $\mathbb{R}^n$ (Teorema 2.1.4).

Definição 2.1.3 (Ortogonalização de Gram-Schmidt)**.** Seja $\beta = \{b_1, \ldots, b_k\}$ conjunto L. I. de vetores em $\mathbb{R}^n$. A ortogonalização de Gram-Schmidt de β é um conjunto de vetores ortogonais $\beta' = \{b'_1, \ldots, b'_k\}$ em $\mathbb{R}^n$, definido recursivamente da seguinte forma:

- $b'_1 = b_1$,
- $b'_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b'_j$, onde $\mu_{i,j} = \frac{\langle b_i, b'_j \rangle}{\langle b'_j, b'_j \rangle}$, para $1 \leq j < i \leq k$.

Note que pela definição, a ortogonalização de Gram-Schmidt satisfaz as propriedades $\langle b'_i, b'_j \rangle = \delta_{i,j}$ e $\langle b'_j, b'_j \rangle = \langle b_j, b'_j \rangle$

Teorema 2.1.4. Se $\Lambda \subset \mathbb{R}^n$ é reticulado então Λ é subgrupo aditivo discreto de $\mathbb{R}^n$.

Demonstração. Tome $\Lambda = \langle b_1, \ldots, b_k \rangle_{\mathbb{Z}}$ reticulado. Claramente Λ é subgrupo, pois se $v, w \in \Lambda$ então $v - w \in \Lambda$. Para provar que Λ é discreto, considere a ortogonalização de Gram-Schmidt $\{b'_1, \ldots, b'_k\}$. Dado $v = x_1 b_1 + \cdots + x_k b_k \in \Lambda \setminus \{0\}$, seja i o maior índice tal que $x_i \neq 0$. Então pela ortogonalização de Gram-Schmidt temos que

$$\langle x_1 b_1 + \cdots + x_k b_k, b'_i \rangle = x_i \langle b_i, b'_i \rangle = x_i \left\| b'_i \right\|^2 . \tag{2.1}$$

Por outro lado, a desigualdade de Cauchy-Schwarz nos diz que

$$\left| \langle x_1 b_1 + \cdots + x_k b_k, b'_i \rangle \right| \leq \| x_1 b_1 + \cdots + x_k b_k \| \cdot \| b'_i \| . \tag{2.2}$$

Unindo 2.1 e 2.2 obtemos que $\| x_1 b_1 + \cdots + x_k b_k \| \geq |x_i| \| b'_i \| \geq \| b'_i \|$ (pois $x_i \neq 0$) e portanto $\| v \| \geq \min_{1 \leq i \leq k} b'_i$.

Assim, dado $v \in \Lambda$, tome $\varepsilon = \min_{1 \leq i \leq n} \left(\| b'_i \| / 2 \right)$. Então $B_\varepsilon(v) \cap \Lambda = \{v\}$, pois $\| v - w \| \geq \min_{1 \leq i \leq k} b'_i$ para todo $w \neq v$, $w \in \Lambda$. Demonstramos, assim que o conjunto Λ é discreto. □

Note que é demonstrável que a caracterização é equivalente, isto é, Λ é reticulado sse é subgrupo aditivo discreto de $\mathbb{R}^n$ (ver [Cas97, Teorema VI, p. 78]).

Definição 2.1.5. Dado um reticulado Λ e uma base $\beta = \{b_1, \ldots, b_k\}$ deste reticulado, definimos a *matriz geradora* de Λ relativa a esta base como

$$B = \left[b_1 \cdots b_k \right],$$

onde os vetores da base são colocados como colunas da matriz. Dessa forma podemos também representar os vetores de um reticulado como o conjunto dos vetores Bx para $x \in \mathbb{Z}^k$.

A *matriz de Gram* do reticulado relativa à base β é a matriz simétrica dada por $G = B^\top B$, com entradas da forma $g_{ij} = \langle b_i, b_j \rangle$. Ela é relevante pois nos permite definir o *determinante* de um reticulado mesmo quando o posto não for completo. Definimos o determinante de um reticulado Λ como

$$\det \Lambda := \det G. \tag{2.3}$$

para qualquer matriz de Gram G de Λ. Este valor independe da matriz de Gram escolhida. O volume de um reticulado, dado por $V(\Lambda) = \sqrt{\det \Lambda}$, de fato corresponde ao volume de um paralelotopo definido por uma base do reticulado [Cos+17]. Um reticulado com determinante ± 1 é dito *unimodular*.

Para determinar se duas matrizes geram o mesmo reticulado, consideramos o grupo das matrizes inteiras invertíveis

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

também chamadas de *matrizes unimodulares*.

Proposição 2.1.6. [Cos+17] As matrizes $B_1, B_2 \in \mathbb{R}^{n\times k}$ geram o mesmo reticulado se, e somente se, $B_1 = B_2 U$, onde $U \in \mathrm{GL}_k(\mathbb{Z})$.

Demonstração. Sejam Λ_1 reticulado gerado por B_1, e Λ_2 o gerado por B_2. Para que $\Lambda_1 \supset \Lambda_2$ é necessário e suficiente que $B_1 = B_2 U$, com $U \in \mathbb{Z}^{k\times k}$. Analogamente, a inclusão $\Lambda_2 \supset \Lambda_1$ é equivalente a pedir que $B_2 = B_1 V$ para alguma $V \in \mathbb{Z}^{k\times k}$. Daí tiramos que U é invertível, com inversa $U^{-1} = V \in \mathbb{Z}^{k\times k}$. Mas $U^{-1} \in \mathbb{Z}^{k\times k} \iff \det U = \pm 1$. □

Dois reticulados Λ_1 e Λ_2 são ditos *equivalentes* se existirem uma constante $\lambda \in \mathbb{R}$ e uma transformação ortogonal O (i.e. $O^\top O = I$), tais que $\lambda O(\Lambda_1) = \Lambda_2$. Se G_1 e G_2 são matrizes de Gram de Λ_1 e Λ_2, respectivamente, então $G_2 = \lambda^2 G_1$.

2.2 Distância mínima e empacotamento

Um parâmetro importante em reticulados é a *distância mínima* λ, que é a menor distância possível entre dois pontos distintos de Λ, ou equivalentemente, a menor norma de um vetor não-nulo de Λ:

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

Uma generalização da distância mínima de reticulados é dada pelos *mínimos sucessivos* λ_i, para $1 \le i \le \dim(\Lambda)$, definidos por

$$\lambda_i(\Lambda) \coloneqq \inf \left\{ \max_{v\in\mathcal{B}} \|v\| \;\middle|\; \mathcal{B} \text{ é conjunto L. I., } |\mathcal{B}| = i \right\}, \tag{2.4}$$

onde λ_1 equivale à distância mínima.

Exemplo 2.2.1. Seja $\Lambda = \langle (1,1), (3/2, 0) \rangle$ como no Exemplo 2.1.2 (a). Como pode-se observar na Figura 2.1, um vetor de norma mínima é $(-1/2, 1)$ e portanto $\lambda_1 = \|(-1/2, 1)\| = \sqrt{5}/2$.

Um vetor que tem a segunda menor norma possível é $(1, 1)$, com norma $\sqrt{2}$. Como o conjunto $\{(-1/2, 1), (1, 1)\}$ é L.I., então esse é um exemplo de conjunto de 2 elementos que tem a menor norma possível. Assim, $\lambda_2 = \sqrt{2}$.

Os reticulados também podem ser analisados no problema de encaixar esferas de mesmo raio em $\mathbb{R}^n$ de forma a preencher o maior espaço possível. A forma de fazer um empacotamento de esferas utilizando reticulados é centrar cada esfera em um ponto do reticulado e utilizar o maior raio possível tal que quaisquer duas esferas tenham interseção vazia ou no bordo. Este raio é chamado de *raio de empacotamento*, e ele coincide com a metade da distância mínima.

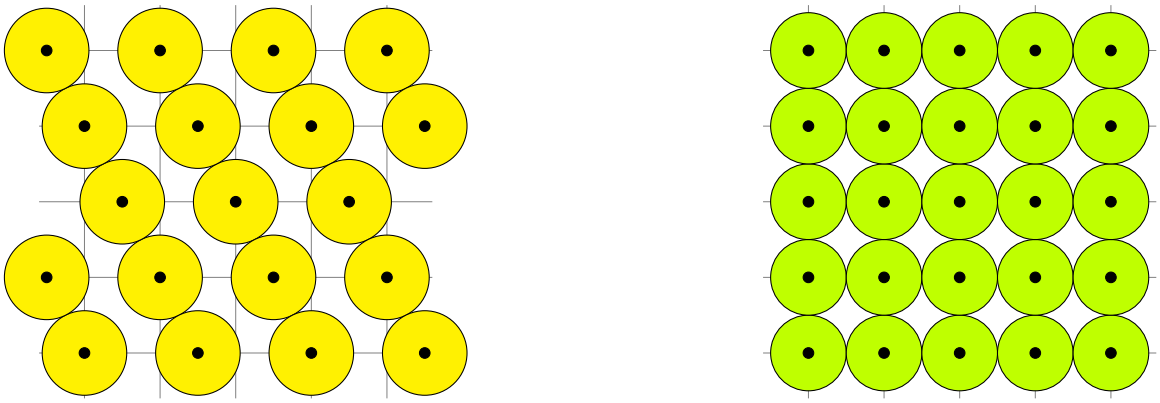


Figura 2.2: Empacotamento dos reticulados dos Exemplo 2.1.2 por esferas de raio $\lambda/2$.

A proporção do volume do espaço n-dimensional que é ocupada pelo empacotamento de um reticulado pode ser calculada pela razão entre o volume da bola de empacotamento, e o volume da *região de Voronoi* do reticulado. A região de Voronoi $\mathcal{V}$ de um reticulado Λ é o conjunto de pontos de $\mathbb{R}^n$ que estão mais perto da origem do que de qualquer outro vetor do reticulado:

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

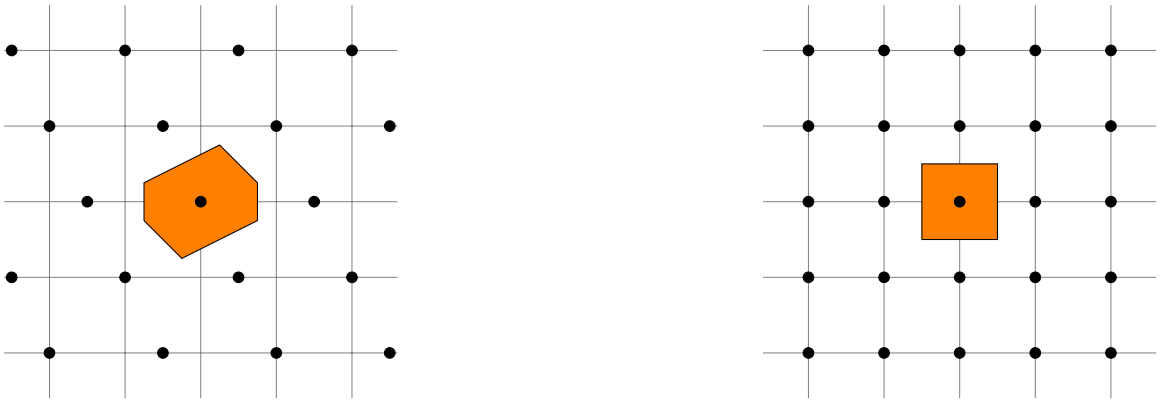


Figura 2.3: Regiões de Voronoi dos reticulados do Exemplo 2.1.2.

Definição 2.2.2. Sejam Λ reticulado de posto completo em $\mathbb{R}^n$, e $A \subset \mathbb{R}^n$ mensurável. Dizemos que A *ladrilha* o espaço por Λ, se satisfaz duas propriedades:

1. Se $v, w \in \Lambda$, $v \neq w$, então $(v + A) \cap (w + A)$ tem volume zero.

2. $\bigcup_{v\in\Lambda}(v + A) = \mathbb{R}^n$.

Uma propriedade interessante da região de Voronoi é que podemos construir um ladrilhamento do espaço por $\mathcal{V}$, considerando para cada $v \in \Lambda$, o ladrilho $(v + \mathcal{V})$.

Analogamente à região de Voronoi, podemos também ladrilhar perfeitamente $\mathbb{R}^n$ através do *paralelotopo fundamental*, que é o paralelotopo apoiado em uma base do reticulado:

$$P(\beta) = \left\{\alpha_1 b_1 + \cdots + \alpha_k b_k \;\middle|\; \alpha_1, \ldots, \alpha_k \in [0, 1]\right\}.$$

Figura 2.4: Paralelotopo fundamental dos reticulados do Exemplo 2.1.2.

Teorema 2.2.3. [HW00] Se dois conjuntos mensuráveis ladrilham o plano por Λ, então eles têm o mesmo volume.

Demonstração. Sejam A, B mensuráveis que ladrilham $\mathbb{R}^n$ por Λ. Pela segunda propriedade do ladrilhamento,

$$B = B \cap \left(\bigcup_{v\in\Lambda}(v + A)\right) = \bigcup_{v\in\Lambda} B \cap (v + A).$$

Assim, como os termos da união têm interseção com volume zero, e como volume é invariante por translação, temos que

$$\operatorname{Vol} B = \sum_{v\in\Lambda} \operatorname{Vol}\left((B \cap (v + A)) - v\right) = \sum_{v\in\Lambda} \operatorname{Vol}\left(A \cap (-v + B)\right) = \operatorname{Vol} A. \qquad \square$$

Corolário 2.2.4. Seja β base de um reticulado de posto completo Λ. Então

$$\operatorname{Vol}\mathcal{V} = \operatorname{Vol} P(\beta) = V(\Lambda).$$

Assim, faz sentido definir a densidade do empacotamento de Λ como a razão entre o volume de uma bola do empacotamento, pelo volume de uma região que ladrilha o plano, pois esta é a proporção do espaço ocupada pelas bolas.

Definição 2.2.5. Seja $\Lambda \subset \mathbb{R}^n$ reticulado de posto completo. Definimos a *densidade de empacotamento* de Λ como

$$\Delta(\Lambda) = \frac{\text{Vol}\left(B_{\lambda/2}(0)\right)}{V(\Lambda)}.$$

Reticulados equivalentes possuem a mesma densidade de empacotamento. É interessante notar que os reticulados com melhor densidade de empacotamento são conhecidos apenas nas dimensões de 1 a 8 e 24 [Coh+17] (para dimensão 24 a prova foi publicada em 2017).

Um parâmetro de reticulados semelhante, e em algum sentido dual ao raio de empacotamento é o raio de cobertura, que é o menor raio necessário para cobrir o espaço com bolas centradas nos pontos de um reticulado.

Definição 2.2.6. Seja $\Lambda \subset \mathbb{R}^n$ reticulado de posto completo. O *raio de cobertura* de Λ é dado por

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

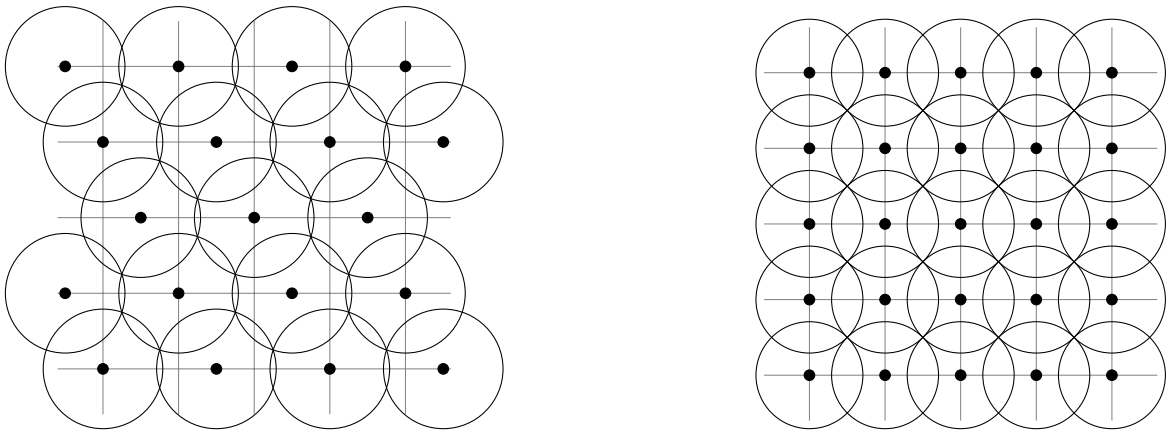


Figura 2.5: Cobertura dos reticulados do Exemplo 2.1.2.

A densidade de cobertura é definida de forma semelhante à densidade de empacotamento.

Definição 2.2.7. Seja $\Lambda \subset \mathbb{R}^n$ reticulado de posto completo com raio de empacotamento μ. A *densidade de empacotamento* de Λ é dada por

$$\Theta(\Lambda) \coloneqq \frac{\text{Vol}\, B_\mu(0)}{V(\Lambda)}.$$

2.3 Reticulados importantes

As descrições seguintes dos reticulados mais relevantes foram extraídas de [CS99, Cap. 4]. A razão para muitos dos nomes (como A_n, D_n, E_n, etc) é que estes reticulados são gerados por *sistemas de raízes*, que são um conceito fundamental na teoria de álgebras de Lie e grupos de Lie [Hal15].

Definição 2.3.1. Um sistema de raízes Φ em $\mathbb{R}^n$ é um conjunto finito de vetores não-nulos satisfazendo:

1. Φ gera $\mathbb{R}^n$;
2. Dado $\alpha \in \Phi$, os únicos múltiplos escalares de α que pertencem a Φ são α e $-\alpha$;
3. Para cada $\alpha \in \Phi$, o conjunto Φ é fechado por reflexão com relação ao hiperplano perpendicular a α;
4. Se $\alpha, \beta \in \Phi$, então a projeção ortogonal de β em α é um múltiplo inteiro ou meio-inteiro de α.

Tendo um sistema de raízes Φ, definimos o reticulado gerado por Φ como $\Lambda(\Phi) \coloneqq \langle \Phi \rangle_{\mathbb{Z}}$, isto é, o conjunto das combinações lineares inteiras de vetores de Φ. Um reticulado que é gerado por um sistema de raízes é chamado de *reticulado raiz* [Hal15].

Exemplo 2.3.2. Considere o conjunto $\Phi = \{(\pm 1, 0), (0, \pm 1)\}$. Vemos ver que Φ é sistema de raiz.

1. Φ gera $\mathbb{R}^2$ por $\{(1, 0), (0, 1)\}$ é base.
2. Claramente, os únicos múltiplos escalares de $\alpha \in \Phi$ são α e $-\alpha$.
3. Note que a reflexão de $(1, 0)$ com relação a $(0, 1)$ é $(-1, 0)$, e vice versa. Analogamente para a reflexão com relação a $(1, 0)$.
4. Basta notar que a projeção sobre qualquer vetor ortogonal resulta em $(0, 0)$.

   Assim, Φ é um sistema de raízes, e o reticulado gerado é $\mathbb{Z}^2$.

2.3.1 A_n

O reticulado $\mathrm{A}_n \subset \mathbb{R}^{n+1}$ é um reticulado raiz n-dimensional, formado pelos vetores inteiros cujas coordenadas somam 0:

$$\mathrm{A}_n = \left\{ (v_1, \ldots, v_{n+1}) \in \mathbb{Z}^{n+1} \;\middle|\; v_1 + \cdots + v_{n+1} = 0 \right\}.$$

Este reticulado pode ser gerado pelo sistema de raízes composto pelos vetores da forma $e_j - e_k$, com $j \neq k$ (onde e_i é o i-ésimo vetor da base canônica de $\mathbb{R}^{n+1}$). Também pode ser construído com a base de vetores $\alpha_i = e_i - e_{i+1}$, com $1 \leq i \leq n + 1$.

Exemplo 2.3.3. A_2 é o reticulado gerado pelos vetores $(1, -1, 0)$ e $(0, 1, -1)$.

2.3.2 Reticulados q-ários

Os reticulados q-ários têm grande relação com códigos lineares sobre o anel $\mathbb{Z}_q$. [Cos+17]

Definição 2.3.4. Um *código linear* sobre $\mathbb{Z}_q$ ($q \in \mathbb{N}$) é um submódulo de $\mathbb{Z}_q^n$. Dizemos que n é o *comprimento* do código.

Um reticulado q-ário é um reticulado inteiro $\Lambda \subset \mathbb{Z}^n$ tal que $\Lambda \supset q\mathbb{Z}^n$ para algum $q \in \mathbb{N}$. Dada uma matriz $A \in \mathbb{Z}_q^{k\times n}$ podemos construir os reticulados q-ários

$$\Lambda_q(A) \coloneqq \left\{ v \in \mathbb{Z}^n \;\middle|\; v \equiv A^\top x \mod q, \text{ para algum } x \in \mathbb{Z}^k \right\},$$
$$\Lambda_q^\perp(A) \coloneqq \left\{ v \in \mathbb{Z}^n \;\middle|\; Av = 0 \mod q \right\}.$$

Essas construções estabelecem uma relação entre reticulados e códigos lineares. Dado um código linear $C \subset \mathbb{Z}_q^n$, podemos definir a *construção A* de C como o reticulado $\phi^{-1}(C)$, onde $\phi(x) = x \mod q$ é a projeção canônica de $\mathbb{Z}^n$ em $\mathbb{Z}_q^n$.

Observe que o primeiro reticulado é a construção A do código linear gerado pelas linhas de A, enquanto o segundo é a construção A do código linear que tem matriz de paridade A. Se a matriz A estiver na forma sistemática, isto é, $A = \left[-B|I_k\right]$ então ela estará associada ao código $\begin{bmatrix} I_{n-k} \\ B \end{bmatrix}$ e a matriz geradora do reticulado $\Lambda_q^\perp(A)$ será [Cos+17]

$$\begin{bmatrix} I_{n-k} & 0 \\ B & I_k \end{bmatrix}.$$

Teorema 2.3.5. [Cos+17] Todo reticulado inteiro de posto completo é q-ário, para $q = \det \Lambda$.

2.3.3 Reticulado hexagonal

O reticulado hexagonal é um reticulado de dimensão 2 em $\mathbb{R}^2$, gerado pelos vetores $(1, 0)$ e $(1/2, \sqrt{3}/2)$ (que corresponde à rotação do primeiro vetor por $\pi/3$ radianos). Ele é equivalente ao reticulado A_2 definido na seção 2.3.1. Este reticulado possui esse nome por conta do fato de os vetores mais próximos da origem formarem um hexágono.

É também o reticulado 2-dimensional que possui melhor densidade de empacotamento: $\Delta = \pi/\sqrt{12} \approx 0.9069$.

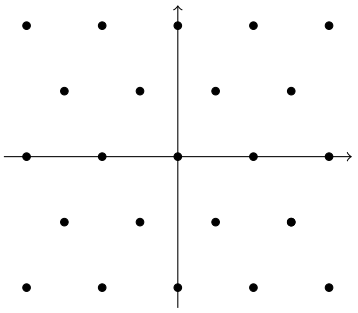


Figura 2.6: Reticulado hexagonal.

2.3.4 BCC e FCC

Os reticulados BCC (*body-centered cubic*) e FCC (*face-centered cubic*), chamados também de reticulados de Bravais, são amplamente utilizados em cristalografia, por descreverem uma organização encontrada em diversas estruturas cristalinas[AMW04].

O reticulado BCC pode ser descrito como o reticulado gerado pelos vértices de um cubo de lado 1 centrado na origem (Figura 2.7a), e portanto uma base é $\beta_{\text{BCC}} = \{(1,0,0),(0,1,0),(1/2,1/2,1/2)\}$. O reticulado FCC é gerado pelos vértices, e pelos centros das faces, deste mesmo cubo (Figura 2.7b), e portante tem como uma base $\beta_{\text{FCC}} = \{(1,1,0),(1,-1,0),(1,0,-1)\}$.

(a) BCC (b) FCC

Figura 2.7: 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 ($\Delta \approx 0.7405$).

2.3.5 $\mathbf{D}_n$

O reticulado D_n é um reticulado raiz em $\mathbb{R}^n$. Ele pode ser gerado pelo sistema de raízes composto por vetores da forma $\pm e_j \pm e_k$, com $j < k$. Como base, podemos tomar os vetores da forma $e_i - e_{i+1}$ com $1 \leq i \leq n$, mais o vetor $e_{n-1} + e_n$.

2.3.6 $\mathbf{E}_8$

O reticulado E_8 é um reticulado raiz definido como o conjunto de pontos em $\mathbb{R}^8$ com todas as coordenadas inteiras ou todas as coordenadas meio-inteiras, e cuja soma de todas as

coordenadas é par:

$$\mathrm{E}_8 = \left\{ x \in \mathbb{Z}^8 \cup (\mathbb{Z} + 1/2)^8 \;\middle|\; \sum_{i=1}^{8} x_i \equiv 0 \pmod 2 \right\}$$

Um exemplo de matriz geradora para E_8 é

$$B = \begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2 \end{bmatrix}.$$

O reticulado E_8 atinge os melhores valores de densidade de empacotamento e kissing number em sua dimensão [CS99].

2.4 Kissing number

O *kissing number* é uma constate importante relacionada ao empacotamento de esferas n-dimensionais. Ela pode ser definida como o maior número de esferas unitárias que é possível de se arranjar tocando uma esfera unitária fixa, em apenas um ponto.

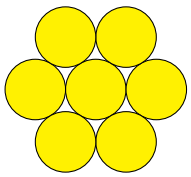


Figura 2.8: O *kissing number* tridimensional é 6.

Por mais que seja uma formulação simples, descobrir o *kissing number* para dimensões maiores que 4 tem se mostrado uma tarefa difícil. O *kissing number*, atualmente, é conhecido apenas para dimensões 1, 2, 3, 4, 8 e 24, como mostrado na Tabela 2.1 [Coh+17].

A relação entre o *kissing number* e reticulados está relacionada com o empacotamento de esferas de determinado reticulado. Dado um reticulado, podemos considerar o *kissing number de* Λ como o número de esferas de raio $\lambda/2$ que tocam a esfera deste mesmo raio centrada na origem. Mais formalmente, podemos definir da seguinte forma:

Definição 2.4.1. Dado um reticulado Λ com distância mínima λ, o kissing number de Λ é

$$k(\Lambda) := \left| \left\{ v \in \Lambda \;\middle|\; \|v\| = \lambda \right\} \right|.$$

Estudar o *kissing number* de reticulados é interessante pois muitos dos melhores valores de *kissing numbers* são de fato atingidos por reticulados, como pode ser visto na tabela 2.1.

Dimensão	1	2	3	4	8	24
Kissing number	2	6	12	24	240	196560
Reticulado	$\mathbb{Z}$	Hexagonal	A_3	D_4	E_8	Λ_{24}

Tabela 2.1: *Kissing numbers* conhecidos, suas respectivas dimensões, e reticulados que realizam esse kissing number.

2.5 Reticulado Dual

Uma noção importante é a noção de dualidade, para reticulados de posto completo [Cos+17].

Definição 2.5.1. O dual de um reticulado de posto completo $\Lambda \subset \mathbb{R}^n$ é o reticulado

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

Proposição 2.5.2. [Cos+17] Se B é matriz geradora de Λ, então $\left(B^{-1}\right)^\top$ é matriz geradora de Λ^*.

Exemplo 2.5.3. Considere $\Lambda = \langle (1,1), (3/2, 0) \rangle_{\mathbb{Z}}$ reticulado do Exemplo 2.1.2. Então, uma vez que

$$\begin{bmatrix} 1 & 0 \\ 1 & 3/2 \end{bmatrix}^{-\top} = \begin{bmatrix} 1 & 2/3 \\ 0 & -2/3) \end{bmatrix},$$

temos que o dual é dado por $\langle (0,1), (2/3, -2/3) \rangle_{\mathbb{Z}}$, como ilustrado na Figura 2.9.

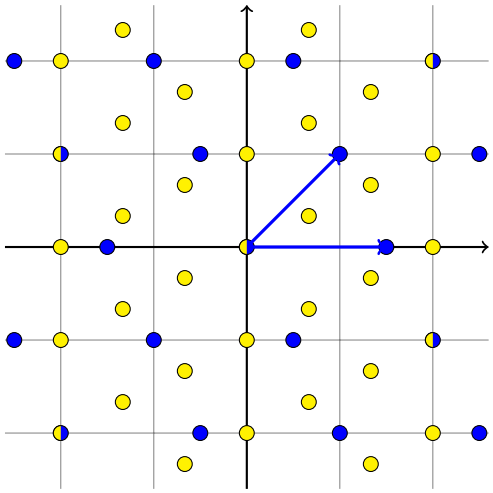


Figura 2.9: $\Lambda = \langle (1,1), (3/2, 0) \rangle_{\mathbb{Z}}$ em azul, e $\Lambda^* = \langle (0,1), (2/3, -2/3) \rangle_{\mathbb{Z}}$ em amarelo.

A partir da Proposição 2.5.2 podemos concluir algumas propriedades do dual:

- 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 que são equivalentes a seus duais são chamados de *reticulados autoduais*. Exemplos de reticulados autoduais são: E_8, o $\mathbb{Z}^n$, e o hexagonal. Ainda analisando os reticulados importantes, temos que o dual do BCC é equivalente ao FCC, e o dual do FCC é equivalente ao BCC [CS99].

2.6 Funções Teta

Seja $\mathbb{H}$ o hiperplano superior complexo, formado pelos números complexos com parte imaginária estritamente positiva (isto é, $\Im(\tau) > 0$). Para $\tau \in \mathbb{H}$, denotamos $q = q(\tau) = e^{2\pi i \tau}$.

Definição 2.6.1. [Ebe12] A *função teta* de um reticulado $\Lambda \subset \mathbb{R}^n$ é a função $\vartheta_\Lambda \colon \mathbb{H} \to \mathbb{C}$ dada por

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

O seguinte resultado mostra que a função teta está bem definida, e que é uma função holomorfa em $\mathbb{H}$.

Proposição 2.6.2. [Ebe12] Seja $\Lambda \subset \mathbb{R}^n$ reticulado. Então a série da função teta

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

converge absolutamente e uniformemente para todo τ que satisfaz $\Im(\tau) \geq v_0 > 0$.

Demonstração. Sejam B matriz geradora de Λ, e $\epsilon := \min\left\{ \|Bx\|^2 \;\middle|\; x \in \mathbb{R}^n, \|x\|^2 = 1 \right\}$, que existe B é operador linear sobre um espaço de dimensão finita. Então temos que $\epsilon \|x\|^2 \leq \|Bx\|^2$ para todo $x \in \mathbb{R}^n$. Assim,

$$\sum_{v \in \Lambda} \left| e^{\pi i \tau \langle v, v\rangle} \right| = \sum_{x \in \mathbb{Z}^n} \left| e^{\pi i \tau \langle Bx, Bx\rangle} \right| \leq \sum_{x \in \mathbb{Z}^n} e^{-\pi v_0 \epsilon \langle x, x\rangle} = \left(\sum_{r=-\infty}^{\infty} e^{-\pi v_0 \varepsilon r^2} \right)^n.$$

É um fato conhecido que para $k > 0$, a série $\sum_{n=1}^{\infty} e^{-kx^2}$ converge. Tomando $k = \pi v_0 \varepsilon > 0$, concluímos que a série $\sum_{r=-\infty}^{\infty} e^{-\pi v_0 \varepsilon r^2}$ converge e portanto $\sum_{v \in \Lambda} \left| e^{\pi i \tau \langle v, v\rangle} \right|$ converge. □

Por [SS10, Teorema 5.2, p. 53], se uma sequência de funções holomorfas converge uniformemente em todo compacto para uma função f, então f é holomorfa. Mostramos que uma série de funções holomorfas converge uniformemente para ϑ_Λ em qualquer semiplano $\Im(\tau) \geq v_0 > 0$, então ϑ_Λ é holomorfa.

O coeficiente $N(m)$ de q^m na série da função teta nos diz qual é o número de pontos do reticulado que têm distância $\sqrt{m}$ da origem. Por conta disso, a função teta fornece informações importantes sobre o reticulado, como o kissing number k e a distância mínima λ:

$$\vartheta_\Lambda(\tau) = 1 + kq^{\lambda^2} + \cdots$$

A densidade de empacotamento também pode ser calculada por

$$\Delta(\Lambda) = \lim_{r\to\infty} \left(\frac{\lambda}{2r}\right)^n \sum_{m\leq r^2} N(m),$$

e a série teta do reticulado dual a Λ é [Ebe12]

$$\vartheta_{\Lambda^*}(\tau) = V(\Lambda)\left(\frac{i}{\tau}\right)^{n/2} \vartheta_\Lambda\left(-\frac{1}{\tau}\right). \tag{2.5}$$

Uma das motivações para se estudar funções teta está relacionada ao teorema dos quadrados de Lagrange, que diz que todo inteiro positivo pode ser escrito como soma de quatro quadrados. Se tomarmos a função teta do reticulado $\mathbb{Z}^4$, o coeficiente $N(m)$ de cada termo q^m é exatamente o número de formas de escrever m como soma de quatro quadrados.

No caso de $\mathbb{Z}^n$, conseguimos escrever $\vartheta_{\mathbb{Z}^n}$ em termos de $\vartheta_\mathbb{Z}$, da seguinte forma:

$$\vartheta_{\mathbb{Z}^n}(\tau) = \sum_{x\in\mathbb{Z}^n} q^{\langle x,x\rangle} = \left(\sum_{x_1\in\mathbb{Z}} q^{\langle x_1,x_1\rangle} \cdots \sum_{x_n\in\mathbb{Z}} q^{\langle x_n,x_n\rangle}\right) = \left(\sum_{m\in\mathbb{Z}} q^{\langle m,m\rangle}\right)^n = \vartheta_\mathbb{Z}(\tau)^n.$$

$\mathbb{Z}^2$	m	0	1	2	4	5	8	9	10	13
	$N(m)$	1	4	4	4	8	4	4	8	8
$\mathbb{Z}^3$	m	0	1	2	3	4	5	6	8	9
	$N(m)$	1	6	12	8	5	24	24	12	30
FCC	m	0	2	4	6	8	10	12	14	16
	$N(m)$	1	12	6	24	12	24	8	28	6
BCC	m	0	3	4	8	11	12	16	18	19
	$N(m)$	1	8	6	12	24	8	6	24	24
E_8	m	0	2	4	6	8	10	12	14	16
	$N(m)$	1	240	2160	6720	17520	30240	60480	82560	140400

Tabela 2.2: Coeficientes da função teta de alguns reticulados importantes.

2.7 Reticulados Ideais

Uma importante construção de reticulados é a que chamamos de *reticulados ideais*. São reticulados inteiros (isto é, $\Lambda \subset \mathbb{Z}^n$) construídos a partir de homomorfismos com anéis de polinômios. A principal vantagem de construções algébricas como esta é a possibilidade de se

usar propriedades algébricas do anel para obter informações sobre o reticulado. São também utilizadas em problemas criptográficos, como o anel-SIS e o anel-LWE (Seção 4.8).

Nesta seção utilizaremos anéis de polinômios da forma $R = \mathbb{Z}[X]/\langle f \rangle$, onde

$$\langle f \rangle \coloneqq \left\{ g \cdot f \;\middle|\; g \in \mathbb{Z}[X] \right\}$$

é o ideal gerado por f.

Definição 2.7.1. Sejam $f \in \mathbb{Z}[X]$ polinômio inteiro, mônico, de grau n, e $R = \mathbb{Z}[X]/\langle f \rangle$ o anel associado a f. Seja ainda $\varphi\colon R \to \mathbb{Z}^n$ um isomorfismo de grupos aditivos. Um reticulado ideal é um reticulado da forma $\varphi(I)$, onde $I \lhd R$ é um ideal.

Um exemplo de isomorfismo $\varphi\colon R \to \mathbb{Z}^n$ é o *mergulho geométrico*, dado por

$$\varphi\left(\overline{a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}}\right) = (a_0, a_1, \ldots, a_{n-1}).$$

Uma propriedade interessante que surge no contexto de reticulados ideais é a de reticulados *cíclicos*. Um reticulado $\Lambda \subset \mathbb{R}^n$ é dito cíclico se, dado $(v_1, v_2, \ldots, v_n) \in \Lambda$, temos que $(v_n, v_1, \ldots, v_{n-1}) \in \Lambda$.

Proposição 2.7.2. [Pei16] Sejam $R = \mathbb{Z}[X]/\langle X^n - 1 \rangle$ e $\varphi\colon R \to \mathbb{Z}^n$ o mergulho geométrico. O reticulado $\Lambda \subset \mathbb{Z}^n$ é cíclico se, e somente se, $\Lambda = \varphi(I)$ é reticulado ideal para algum $I \lhd R$.

Demonstração. ($\Rightarrow$) Defina o conjunto de polinômios

$$I = \left\{ \overline{\textstyle\sum_{i=0}^{n-1} v_i X^i} \;\middle|\; (v_0, \ldots, v_{n-1}) \in \Lambda \right\} \subset R.$$

- Como Λ é subgrupo aditivo de $\mathbb{Z}^n$, temos que I é subgrupo aditivo de R.
- Seja $\overline{g} \in I$. Como Λ é reticulado, $\overline{vg} \in I$ para todo $v \in \mathbb{Z}$, e como Λ é cíclico, temos que $\overline{v_i g} \cdot \overline{X}^i \in I$ para todo $\overline{g} \in I$ $v_i \in \mathbb{Z}$. Assim, $\overline{g} \cdot \overline{v_i X^i} \in I$ para todo $i \in \mathbb{N}$. Logo, $\overline{g} \cdot \overline{v_0 + v_1 X + \cdots + v_n X^n} \in I$ para qualquer $\overline{v_0 + v_1 X + \cdots + v_n X^n} \in R$.

Assim, I é ideal de R e temos que $\Lambda = \varphi(I)$.

($\Leftarrow$) Seja $g = \overline{a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}} \in I$. Então $\varphi(g) = (a_0, \ldots, a_{n-1})$. Como I é ideal, temos que $\overline{X}g \in I$. Mas

$$\begin{aligned} \overline{X}g = \overline{X(a_0 + a_1 X + \cdots + a_{n-1}X^{n-1})} &= \overline{a_0 X + a_1 X^2 + \cdots + a_{n-1}X^n} \\ &= \overline{a_{n-1} + a_0 X + \cdots + a_{n-2}X^{n-1}} \end{aligned}$$

Assim, $(a_{n-1}, a_0, \ldots, a_{n-2}) = \varphi(\overline{X}g) \in \varphi(I)$ e portanto Λ é cíclico. □

Exemplo 2.7.3. Seja $f = X^2 - 1$, e $I = \langle \overline{2 + X} \rangle$. Então

$$I = \left\{ \overline{(a + bX)(2 + X)} \;\middle|\; a, b \in \mathbb{Z} \right\} = \left\{ \overline{(2a + b) + X(a + 2b)} \;\middle|\; a, b \in \mathbb{Z} \right\}.$$

Assim, $\varphi(I) = \{(2a + b, a + 2b) \mid a, b \in \mathbb{Z}\} = \{a(2, 1) + b(1, 2) \mid a, b \in \mathbb{Z}\}$ (ver Figura 2.10). Note que o reticulado obtido é de fato um reticulado cíclico.

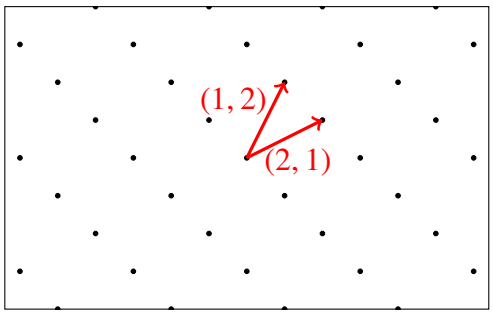


Figura 2.10: Reticulado ideal $\varphi(I)$.

Para se estudar a geometria de anéis de polinômios e de reticulados ideais, é útil ter uma noção de norma dentro do anel $R = \mathbb{Z}[X]/\langle f \rangle$. Entre as possíveis normas, duas em particular se destacam: [LPR12]

1. **Norma p dos coeficientes**: É a norma p induzida pelo mergulho geométrico, isto é,

$$\left\| \overline{a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}} \right\|_p := \|(a_0, \ldots, a_{n-1})\|_p,$$

onde escolhemos os coeficientes $a_0, \ldots, a_{n-1}$ do representante canônico.

Apesar de ser a forma aparentemente mais simples de se definir a norma em R, ela possui duas grandes desvantagens: primeiro que a norma depende da escolha do representante; segundo que a norma de $g \cdot h$ não precisa estar relacionada com as normas de g e de h;

2. **Norma p do mergulho canônico**: Sejam $\alpha_1, \ldots, \alpha_n$ as n raízes complexas de f. Essas raízes nos permitem definir o *mergulho canônico* $\sigma \colon R \to \mathbb{C}^n$, dado por $\sigma(\overline{g}) := (g(\alpha_1), \ldots, g(\alpha_n))$. Note que σ está bem definido uma vez que a imagem não depende da escolha de representante: se $h = g + zf$, então

$$\begin{aligned} \sigma(\overline{h}) = (h(\alpha_1), \ldots, h(\alpha_n)) &= \big((g + zf)(\alpha_1), \ldots, (g + zf)(\alpha_n)\big) \\ &= \big(g(\alpha_1), \ldots, g(\alpha_n)\big) = \sigma\left(\overline{g}\right) \end{aligned}$$

Assim, conseguimos definir um norma, usando a norma p do mergulho canônico complexo, isto é,

$$\left\|\overline{g}\right\|_p := \left\|\sigma(\overline{g})\right\|_p = \left(\sum_{i=1}^{n} \left|g(\alpha_i)\right|^p \right)^{1/p},$$

e $\left\|\overline{g}\right\|_\infty := \max_{1\leq i\leq n}\left|g(\alpha_i)\right|$.

Uma das vantagens desta norma é que temos boas desigualdades sobre a norma do produto, como por exemplo $\|\overline{g}\cdot\overline{h}\|_p \leq \left\|\overline{g}\right\|_\infty \cdot \|\overline{h}\|_p$.

Capítulo 3

O parâmetro de suavização

Neste capítulo apresentamos o parâmetro de suavização, e alguns outros conceitos relacionados a gaussianas sobre reticulados, detalhando os conceitos e resultados. Mostramos, também, algumas simulações computacionais que fazemos, para calcular o parâmetro de suavização. As principais referências foram: [MR07], [Mic07], [Reg09], [Pei+13] e [LPR12].

3.1 Introdução

Definição 3.1.1. A *função gaussiana* com fator $s \in \mathbb{R}_{>0}$ 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

$$\int_{\mathbb{R}^n} \rho_s(x)\,\mathrm{d}x = \int_{\mathbb{R}^n} e^{-\pi\|x\|^2/s^2}\,\mathrm{d}x = \prod_{i=1}^{n} \int_{\mathbb{R}} e^{-\pi x_i^2/s^2}\,\mathrm{d}x_i = s^n.$$

Definição 3.1.2. Seja $\Lambda \subset \mathbb{R}^n$ reticulado de posto completo, e $c \in \mathbb{R}^n$. Definimos a *massa gaussiana* com fator $s > 0$ de $(\Lambda + c)$ por

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

É interessante notar que a massa gaussiana de um reticulado pode ser escrita em termos de sua série teta (Definição 2.6.1) da seguinte forma:

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

Como $\tau = \frac{1}{s^2} i \in \mathbb{H}$ para todo $s > 0$ a Proposição 2.6.2 garante que a massa gaussiana está bem definida, e que é contínua em s. Além disso, como ϑ_Λ é holomorfa em $\mathbb{H}$, temos que $\vartheta_\Lambda(i/s^2)$ é diferenciável em s; portanto $\rho_s(\Lambda)$ é diferenciável em s.

Os dois resultados seguintes são mencionados nos textos [Pei16] e [Reg09] sem as demonstrações, que colocamos a seguir.

Lema 3.1.3. A massa gaussiana de um reticulado Λ, em função de s, é crescente e injetiva.

Demonstração. Se $s_1 > s_2$, então $-1/s_1 > -1/s_2$, e temos que $e^{-\pi\|v\|^2/s_1^2} > e^{-\pi\|v\|^2/s_2^2}$ para todo $v \in \Lambda \setminus \{0\}$ por e^x ser crescente. Assim, $\sum_{v\in\Lambda} e^{-\pi\|v\|^2/s_1^2} > \sum_{v\in\Lambda} e^{-\pi\|v\|^2/s_2^2}$. Note que a injetividade também segue daqui. □

Lema 3.1.4. Seja $\Lambda \subset \mathbb{R}^n$ reticulado. Então

$$\lim_{s\to 0^+} \left(\rho_s(\Lambda \setminus \{0\})\right) = 0, \qquad \lim_{s\to+\infty} \left(\rho_s(\Lambda \setminus \{0\})\right) = +\infty.$$

Demonstração. Tome B matriz geradora de Λ, e $w = \min\left\{\|Bx\|^2 \;\middle|\; \|x\|^2 = 1\right\}$. Então temos que $w\|x\|^2 \le \|Bx\|^2$ para todo $x \in \mathbb{R}^n$. Assim,

$$\rho_s\left(\Lambda \setminus 0\right) = \sum_{v\in\Lambda\setminus\{0\}} e^{-\pi\|v\|^2/s^2} = \sum_{x\in\mathbb{Z}^n\setminus\{0\}} e^{-\pi\|Bx\|^2/s^2} \le \sum_{x\in\mathbb{Z}^n\setminus\{0\}} e^{-\pi w\|x\|^2/s^2}.$$

Para o primeiro limite, basta ver que

$$\sum_{x\in\mathbb{Z}^n\setminus\{0\}} e^{-\pi w\|x\|^2/s^2} = \underbrace{\sum_{\substack{x\in\mathbb{Z}^n\setminus\{0\}\\ \|x\|\le k}} e^{-\pi w\|x\|^2/s^2}}_{I_1} + \underbrace{\sum_{\substack{x\in\mathbb{Z}^n\setminus\{0\}\\ \|x\|> k}} e^{-\pi w\|x\|^2/s^2}}_{I_2}.$$

Tome $\varepsilon > 0$. Fixando $s = 1$, tome $k \in \mathbb{R}$ tal que $I_2 < \varepsilon/2$, que existe pois a série converge. Em particular, temos que para todo $s \le 1$ vale que $I_2 < \varepsilon/2$. Com isso, resta I_1, que consiste em finitos termos $e^{-\pi w\,\|x\|^2/s^2}$. Como cada um desses termos converge para zero quando $s \to 0^+$, então existe $s < 1$ tal que $I_1 < \varepsilon/2$. Assim, $I_1 + I_2 < \varepsilon$.

Para o segundo limite, note que $\|Bx\| \le \|B\| \cdot \|x\|$ para todo $x \in \mathbb{Z}^n$. Então

$$\rho_s\left(\Lambda \setminus 0\right) \ge \sum_{x\in\mathbb{Z}^n\setminus\{0\}} e^{-\pi\|B\|^2\|x\|^2/s^2} = \underbrace{\sum_{\substack{x\in\mathbb{Z}^n\setminus\{0\}\\ \|x\|\le k}} e^{-\pi\|B\|^2\|x\|^2/s^2}}_{J_1} + \underbrace{\sum_{\substack{x\in\mathbb{Z}^n\setminus\{0\}\\ \|x\|> k}} e^{-\pi\|B\|^2\|x\|^2/s^2}}_{J_2}$$

Note que J_1 é uma soma finita. Para cada $x \neq 0$, temos que $e^{-\pi\|B\|^2\|x\|^2/s^2} \xrightarrow{s\to+\infty} 1$. Assim, existe $s > 0$ tal que $e^{-\pi\|B\|^2\|x\|^2/s^2} \ge 1/2$ para todo termo de J_1. Então, dado $k \in \mathbb{N}$, existe $s_0 > 0$ tal que

$$s > s_0 \implies \rho_s\left(\Lambda \setminus \{0\}\right) \ge J_1 \ge \sum_{\substack{x\in\mathbb{Z}^n\setminus\{0\}\\ \|x\|\le k}} 1/2 \ge \frac{2k}{2} - 1 = k - 1.$$

Como k é arbitrário, temos que $\rho_s(\Lambda \setminus 0) \xrightarrow{s\to+\infty} +\infty$. □

Definição 3.1.5 (Parâmetro de suavização)**.** Sejam $\Lambda \subset \mathbb{R}^n$ reticulado de posto completo com dual Λ^*, e $\varepsilon > 0$. Definimos o *parâmetro de suavização* $\eta_\varepsilon(\Lambda)$ como

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

O parâmetro de suavização está bem definido, uma vez que $\rho_{1/s}(\Lambda^* \setminus \{0\})$ é contínua, decrescente, e pelo Lema 3.1.4 satisfaz

$$\lim_{s\to 0^+}\left(\rho_{1/s}(\Lambda^* \setminus \{0\})\right) = \infty, \qquad \lim_{s\to +\infty}\left(\rho_{1/s}(\Lambda^* \setminus \{0\})\right) = 0.$$

Note que a massa gaussiana $\rho_{1/s}\left(\Lambda^* \setminus \{0\}\right)$ que define o parâmetro de suavização pode ser escrita como a série teta $\vartheta_{\Lambda^*}(is^2) - 1$. Assim, utilizamos a Equação 2.5 para obter uma relação entre as massas gaussianas $\rho_{1/s}(\Lambda^* \setminus \{0\})$ e $\rho_s(\Lambda)$:

$$\rho_{1/s}\left(\Lambda^* \setminus \{0\}\right) = \frac{V(\Lambda)}{s^n}\vartheta_\Lambda\left(\frac{i}{s^2}\right) - 1 = \frac{V(\Lambda)}{s^n}\rho_s\left(\Lambda\right) - 1$$

Achamos importante destacar o resultado a seguir, que analisa como o parâmetro de suavização se comporta em reticulados equivalentes:

Proposição 3.1.6. O parâmetro de suavização é invariante por rotação do reticulado, e satisfaz $\eta_\varepsilon(k\Lambda) = k\eta_\varepsilon(\Lambda)$, $k > 0$.

Demonstração. A invariância por rotação segue do fato de usarmos apenas a norma dos vetores de Λ na definição. Para a segunda parte, basta notar que se $s = \eta_\varepsilon(k\Lambda)$ então

$$\rho_{1/s}\left((k\Lambda)^* \setminus \{0\}\right) = \sum_{v\in(k\Lambda)^*\setminus\{0\}} e^{-\pi\|v\|^2 s^2} = \sum_{v\in\frac{1}{k}(\Lambda^*)\setminus\{0\}} e^{-\pi\|v\|^2 s^2} = \sum_{v\in(\Lambda^*)\setminus\{0\}} e^{-\pi\|v\|^2 (s/k)^2}.$$

Assim,

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

e portanto

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

Lema 3.1.7 (Lema 1.5, [Ban93])**.** Sejam $\Lambda \subset \mathbb{R}^n$ reticulado de posto completo, $c \geq 1/\sqrt{2\pi}$ e $v \in \mathbb{R}^n$. Então

1. $\rho_1\left(\Lambda \setminus B_{c\sqrt{n}}(0)\right) < C^n\rho_1(\Lambda)$,
2. $\rho_1\left(\Lambda + v \setminus B_{c\sqrt{n}}(0)\right) < 2C^n\rho_1(\Lambda)$,

onde $C = c\sqrt{2\pi e}\cdot e^{-\pi c^2} < 1$.

As duas próximas proposições apresentam limitantes superiores para o parâmetro de suavização, a primeira das quais demonstramos aqui.

Proposição 3.1.8 (Lema 3.2, [MR07])**.** Seja $\Lambda \subset \mathbb{R}^n$ reticulado de posto completo. Então $\eta_{2^{-n}}(\Lambda) \leq \frac{\sqrt{n}}{\lambda(\Lambda^*)}$.

Demonstração. Utilizamos a relação (1) do Lema 3.1.7, com $c = 1$ e $C = \sqrt{2\pi e} \cdot e^{-\pi} < 1/4$. Separando $\rho_1(\Lambda) = \rho_1\left(\Lambda \setminus B_{\sqrt{n}}(0)\right) + \rho_1\left(\Lambda \cap B_{\sqrt{n}}(0)\right)$, obtemos que

$$\rho_1\left(\Lambda \setminus \sqrt{n}B_1(0)\right) < \frac{C^n}{1-C^n} \cdot \rho_1\left(\Lambda \cap \sqrt{n}B_1(0)\right).$$

Tome $s > \sqrt{n}/\lambda_1(\Lambda^*)$. Então temos que

$$\begin{aligned}\rho_{1/s}\left(\Lambda^* \setminus \{0\}\right) &= \rho_1\left(s\Lambda^* \setminus \{0\}\right) = \rho_1\left(s\Lambda^* \setminus B_{\sqrt{n}}(0)\right) \\ &< \frac{C^n}{1-C^n} \cdot \underbrace{\rho_1\left(s\Lambda^* \cap B_{\sqrt{n}}(0)\right)}_{=1} = \frac{C^n}{1-C^n} < 2^{-n}.\end{aligned}$$ □

Proposição 3.1.9. [MR07, Lema 3.3] Sejam $\Lambda \subset \mathbb{R}^n$ reticulado de posto completo, $\varepsilon > 0$. Então

$$\eta_\varepsilon(\Lambda) \leq \lambda_n \sqrt{\frac{\ln(2n(1+{}^1/_\varepsilon))}{\pi}}.$$

A partir de ρ_s, podemos definir uma distribuição gaussiana $\mathcal{P}_s^\Lambda \colon \mathcal{V} \to \mathbb{R}_{\geq 0}$ sobre a região de Voronoi $\mathcal{V}$ do reticulado Λ, dada por

$$\mathcal{P}_s^\Lambda(x) \coloneqq \frac{1}{s^n} \sum_{v \in \Lambda} \rho_s(x+v). \tag{3.1}$$

Observamos que na definição da distribuição adicionamos um fator $\frac{1}{s^n}$ para fazer a normalização, pois

$$s^n = \int_{\mathbb{R}^n} \rho_s(x)\,\mathrm{d}x = \sum_{v \in \Lambda} \int_{\mathcal{V}} \rho_s(x+v)\,\mathrm{d}x = \int_{\mathcal{V}} \sum_{v \in \Lambda} \rho_s(x+v)\,\mathrm{d}x.$$

A Figura 3.1 ilustra a distribuição $\mathcal{P}_s^\Lambda$ para o reticulado $\mathbb{Z}$, com $s = 1$. Pode-se observar que $\mathcal{P}_s^\Lambda$ é próxima de uma distribuição uniforme $\mathcal{U}(x) = 1$. Veremos mais adiante que para valores grandes de s, a distribuição $\mathcal{P}_s^\Lambda$ tende a ser próxima de uma distribuição uniforme centrada em $\frac{1}{V(\Lambda)}$, e quem mede essa proximidade é o parâmetro de suavização. Em particular, o Teorema 3.1.13 demonstra que, dado um reticulado Λ, se $s > \eta_\varepsilon(\Lambda)$ então a distância máxima pontual entre essas duas distribuições não é maior que ε.

Para demonstrar isso, é necessário introduzir transformadas de Fourier.

Definição 3.1.10 (Transformada de Fourier)**.** Seja $f \colon \mathbb{R}^n \to \mathbb{C}$ uma função integrável. Definimos

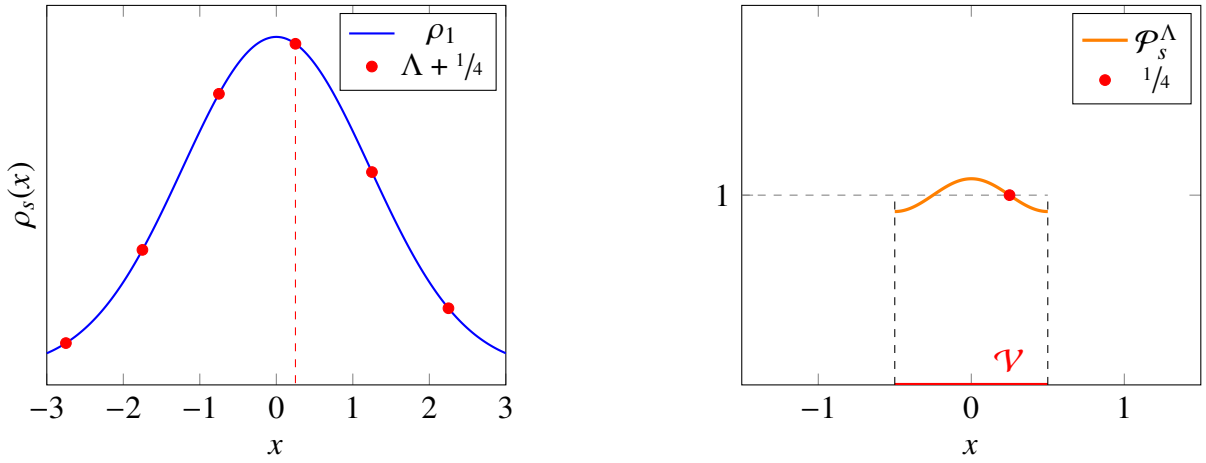


Figura 3.1: Ilustrações da função ρ_s sobre $\mathbb{R}$, e da função $\mathcal{P}_s^\Lambda$ associada, com $s = 1$ e $\Lambda = \mathbb{Z}$. O valor $\mathcal{P}_s^\Lambda(1/4)$ à direita é calculado somando os valores de ρ_s sobre $\Lambda + 1/4$, à esquerda.

a *transformada de Fourier* de f como a função $\hat{f}\colon \mathbb{R}^n \to \mathbb{C}$ dada por

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

Proposição 3.1.11. [Reg09] Temos que:

i) $\hat{\rho}_s = s^n \rho_{1/s}$;

ii) se $g(x) = f(x + c)$, então $\hat{g}(x) = e^{2\pi i\langle x,c\rangle}\hat{f}(x)$.

Teorema 3.1.12 (Soma de Poisson, [Ebe12])**.** Sejam Λ reticulado, e $f\colon \mathbb{R}^n \to \mathbb{C}$ uma função que satisfaz as três condições:

(1) $\displaystyle\int_{\mathbb{R}^n} \big|f(x)\big|\, \mathrm{d}x < \infty$;

(2) A série $\displaystyle\sum_{x\in\Lambda} \big|f(x+u)\big|$ converge uniformemente para u dentro de um compacto de $\mathbb{R}^n$;

Observação: O item (1) implica na existência da transformada de Fourier de f. O item (2) implica na continuidade da função $F(u) := \sum_{x\in\Lambda} f(x+u)$ em $\mathbb{R}^n$.

(3) A série $\displaystyle\sum_{y\in\Lambda^*} \hat{f}(y)$ é absolutamente convergente.

Então

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

Demonstração. Supomos primeiramente que $\Lambda = \mathbb{Z}^n$. Então a função $F(u) = \sum_{x\in\Lambda} f(x+u)$ é contínua (por (2)), e periódica, pois $F(u+y) = F(u)$ para todo $y \in \mathbb{Z}^n$. Portanto, podemos escrever sua série de Fourier

$$\sum_{y\in\mathbb{Z}^n} e^{2\pi i\langle u,y\rangle} a(y),$$

onde $a(y) = \int_{[0,1]^n} F(t)e^{-2\pi i\langle y,t\rangle}\,\mathrm{d}t$. Note que $a(y) = \hat{f}(y)$, pois

$$\begin{aligned} a(y) &= \int_{[0,1]^n} \sum_{x\in\mathbb{Z}^n} f(x+t)e^{-2\pi i\langle t,y\rangle}\,\mathrm{d}t \\ &= \sum_{x\in\mathbb{Z}^n} \int_{[0,1]^n} f(x+t)e^{-2\pi i\langle t+x,y\rangle}\,\mathrm{d}t \\ &= \sum_{x\in\mathbb{Z}^n} \int_{x+[0,1]^n} f(t')e^{-2\pi i\langle t',y\rangle}\,\mathrm{d}t' = \hat{f}(y) \end{aligned}$$

Assim, a condição (3) implica que a série de Fourier de F converge absolutamente e uniformemente, e portanto converge para F. Logo,

$$F(0) = \sum_{x\in\Lambda} f(x) = \sum_{y\in\mathbb{Z}^n} \hat{f}(y).$$

No caso geral, $\Lambda = B\cdot\mathbb{Z}^n$ e $\Lambda^* = \left(B^\top\right)^{-1}\cdot\mathbb{Z}^n$. Definindo $f_B(x) \coloneqq f(Bx)$, para $x\in\mathbb{Z}^n$ temos que

$$\sum_{v\in\Lambda} f(v) = \sum_{x\in\mathbb{Z}^n} f(Bx) = \sum_{x\in\mathbb{Z}^n} f_B(x) = \sum_{y\in\mathbb{Z}^n} \hat{f}_B(y),$$

onde

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

Fazendo a substituição $t' = Bt$:

$$\hat{f}_B(y) = \frac{1}{\det B}\int_{\mathbb{R}^n} f(t')\cdot e^{2\pi i\langle B^{-1}t',y\rangle}\,\mathrm{d}t'.$$

Utilizando a igualdade $\left\langle B^{-1}t', y\right\rangle = \left\langle t', \left(B^\top\right)^{-1} y\right\rangle$:

$$\hat{f}_B(y) = \frac{1}{V(\Lambda)}\,\hat{f}\left(\left(B^\top\right)^{-1} y\right).$$

Assim, concluímos que

$$\sum_{v\in\Lambda} f(v) = \frac{1}{V(\Lambda)}\sum_{y\in\Lambda^*}\hat{f}(y). \qquad \square$$

No teorema a seguir, mostramos que a distribuição $\mathcal{P}_s^\Lambda$ definida em 3.1 é aproximadamente uniforme, desde que $s > \eta_\varepsilon(\Lambda)$. Note que uma vez que $\int_{\mathcal{V}}\mathrm{d}x = V(\Lambda)$, a distribuição uniforme em $\mathcal{V}$ é dada por $\mathcal{U}(x) = \frac{1}{V(\Lambda)}, \forall x\in\mathcal{V}$.

Teorema 3.1.13. [Reg05, Claim 3.8] 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 $x \in \mathcal{V}$.

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

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

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

$$\left| \sum_{w \in \Lambda^* \setminus \{0\}} e^{2\pi i \langle x,w \rangle} \rho_{1/s}(w) \right| \leq \varepsilon.$$

Assim,

$$(1-\varepsilon) \ \leq \ \sum_{w \in \Lambda^*} e^{2\pi i \langle x,w \rangle} \rho_{1/s}(w) \ \leq \ (1+\varepsilon),$$

donde segue o resultado. □

Além disso observamos que a Equação 3.1 vista anteriormente pode ser reescrita como

$$\frac{V(\Lambda)}{s^n} \rho_s(\Lambda) \in [1-\varepsilon, 1+\varepsilon],$$

quando $s > \eta_\varepsilon(\Lambda)$, e coincide justamente com a afirmação exatamente de o Teorema 3.1.13 vale para $x = 0$.

Se denotarmos $d_\infty(f,g) = \sup_{x \in \mathcal{V}} \left| f(x) - g(x) \right|$, então o Teorema 3.1.13 afirma que, para todo $s > \eta_\varepsilon(\Lambda)$,

$$d_\infty \left(V(\Lambda) \cdot \mathcal{P}_s^{\Lambda}, 1 \right) < \varepsilon.$$

Nesse sentido, dizemos que a distribuição $\mathcal{P}_s(\Lambda)$ é aproximadamente uniforme para $s > \eta_\varepsilon(\Lambda)$.

Outra caracterização interessante do parâmetro de suavização é a chamada *caracterização por sobreposição de bolas* introduzida em [Pei+13]. Ela relaciona o parâmetro de suavização com a proporção de volume que bolas de raio r centradas em pontos de um reticulado interseccionam uma bola central.

Sejam $r > 0$ e $\Lambda \subset \mathbb{R}^n$ reticulado n-dimensional. Definimos

$$\text{Overlap}(\Lambda, r) := \frac{\text{Vol}\left(\bigcup_{v \in \Lambda \setminus \{0\}} \left(B_r(0) \cap B_r(v) \right) \right)}{\text{Vol}\, B_r(0)},$$

que denota a proporção de volume que as bolas de raio r centradas em pontos de $\Lambda \setminus \{0\}$ que

intersectam $B_r(0)$.

Teorema 3.1.14 (*Caracterização por sobreposição de bolas*)**.** [Pei+13, Lema 4.4] Sejam $\Lambda \subset \mathbb{R}^n$ reticulado n-dimensional, $\varepsilon \in (2^{o(-n)}, 1/3)$ e $r_\varepsilon = \sqrt{\frac{n}{2\pi}} \frac{1}{2\eta_\varepsilon(\Lambda^*)}$. Então

1. Para $0 \leq r \leq r_\varepsilon$ temos que $\text{Overlap}(\Lambda, r) \leq 2\varepsilon$.
2. Para todo $r \geq 2r_\varepsilon(1+\delta)$, onde $\delta = \sqrt{\frac{3}{2n} \ln \frac{4}{\varepsilon}}$, temos que $\text{Overlap}(\Lambda, r) \geq \varepsilon/2$.

3.2 Gaussianas discretas

Relacionado ao parâmetro de suavização está o estudo de gaussianas sobre conjuntos discretos. As definições a seguir são extraídas de [Reg05].

Definição 3.2.1. Dado um conjunto discreto $A \subset \mathbb{R}^n$, definimos a distribuição de probabilidade gaussiana discreta $D_{A,s}\colon A \to \mathbb{R}_{>0}$ como a normalização da função ρ_s, isto é,

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

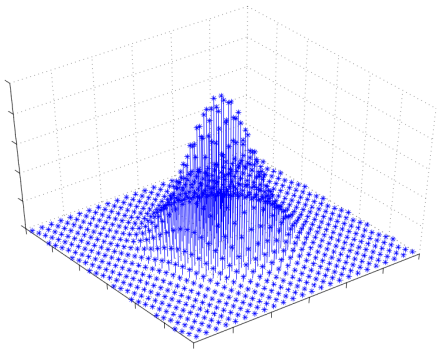


Figura 3.2: Uma gaussiana discreta sobre reticulado.

Para estudar distribuições de probabilidade definidas sobre corpos ou anéis finitos, é também útil definir gaussianas discretas em $\mathbb{Z}_q$ para $q \in \mathbb{N}$. Considere $\mathbb{T}$ a identificação do quociente $\mathbb{R}/\mathbb{Z}$ com o intervalo $[0, 1)$ (isto é, fazemos a soma módulo 1).

Definição 3.2.2. Dado $\alpha \in \mathbb{R}_{>0}$, a distribuição Ψ_α sobre $\mathbb{T}$ é definida por

$$\Psi_\alpha(r) \coloneqq \frac{1}{\alpha} \rho_\alpha(r + \mathbb{Z}) = \sum_{k=-\infty}^{\infty} \frac{1}{\alpha} e^{-\pi\left(\frac{r-k}{\alpha}\right)^2}. \tag{3.2}$$

Definição 3.2.3. Dada uma função de densidade de probabilidade $\phi\colon \mathbb{T} \to \mathbb{R}_{>0}$, definimos sua discretização $\bar{\phi}\colon \mathbb{Z}_q \to \mathbb{R}_{>0}$ por

$$\bar{\phi}(i) \coloneqq \int_{\frac{i-1}{2q}}^{\frac{i+1}{2q}} \phi(x)\, \mathrm{d}x.$$

A partir da função de discretização, definimos ter a distribuição gaussiana discreta $\bar{\Psi}_\alpha : \mathbb{Z}_q \to \mathbb{R}_{>0}$, ilustrada na Figura 3.3.

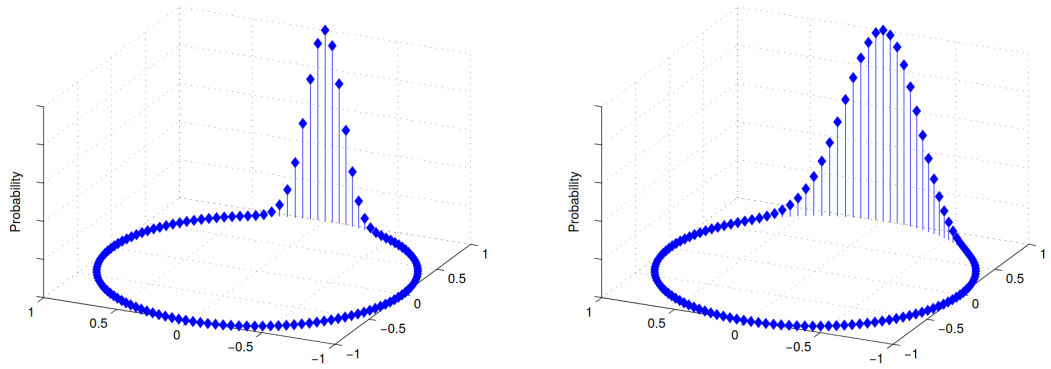


Figura 3.3: $\bar{\Psi}_\alpha$ com $q = 127$, para $\alpha = 0.05$ (esquerda) e $\alpha = 0.1$ (direita). Os elementos de $\mathbb{Z}_q$ estão arranjados num círculo (extraída de [Reg05]).

Essas distribuições são utilizadas em problemas de criptografia pós-quântica como o LWE, que depende de distribuições de probabilidade discretas.

3.3 Códigos wiretap e fator de achatamento

Nesta seção falaremos um pouco sobre uma subárea da teoria da informação, chamada codificação *wiretap*, introduzida por Wyner [Wyn75]. *Códigos wiretap* são esquemas de comunicação para canais sujeitos a ruídos, os quais definiremos aqui informalmente. Sejam Alice e Bob dois participantes que querem comunicar-se por um canal sujeito a ruídos. Suponha ainda que Eva é uma participante que quer interceptar a mensagem. O objetivo dos canais wiretap é utilizar a redundância do canal garantir a segurança da comunicação.

Para isso, duas propriedades são desejadas dos códigos wiretap: [LJO14]

1. Confiabilidade: Alice e Bob introduzem redundância às mensagens para que não haja perda de informação, e

2. Confidencialidade: Alice e Bob introduzem aleatoriedade para que um potencial interceptador não consiga decodificar a mensagem

O modelo original introduzido por Wyner, é baseado em *códigos de classe lateral*. A ideia consiste em associar a cada mensagem não apenas uma palavra-código, mas um conjunto de palavras-código, que formam uma classe lateral de determinado grupo. Uma forma de fazer isso é levando cada mensagem a uma classe lateral de um reticulado, isto é, em $v + \Lambda$ para algum $v \in \mathbb{R}^n$.

Se o ruído do canal for gaussiano, então uma das formas de verificar bons reticulados para a codificação wiretap é através do fator de achatamento (*flatness factor*) [LLB12][Lin+14], que

definiremos a seguir. O fator de achatamento é de fato equivalente ao parâmetro de suavização (ver Teorema 3.3.3).

Definição 3.3.1. [LLB12] Sejam $v \in \mathbb{R}^n$, $c > 0$. Definimos a distribuição gaussiana de variância σ, centrada em v, como a função $f_{\sigma,v}\colon \mathbb{R}^n \to \mathbb{R}_{>0}$ dada por

$$f_{\sigma,v}(x) = \frac{1}{\left(\sqrt{2\pi}\sigma\right)^n} e^{-\|x-v\|^2/2\sigma^2} = \frac{1}{\left(\sqrt{2\pi}\sigma\right)^n} \rho_{\sqrt{2\pi}\sigma}(x-v)$$

e a medida gaussiana em Λ como

$$f_{\sigma,\Lambda}(x) = \sum_{v\in\Lambda} f_{\sigma,v}(x)$$

Considerando a distribuição $f_{\sigma,\Lambda}$, podemos considerar a esperança, que é dada por [LLB12]

$$\mathrm{E}\left[f_{\sigma,\Lambda}\right] = \int_{\mathbb{R}^n} x f_{\sigma,\Lambda}(x)\,\mathrm{d}x = \frac{1}{V(\Lambda)}.$$

Definição 3.3.2. O fator de achatamento de um reticulado Λ é uma função $\epsilon_\Lambda\colon \mathbb{R}_{>0} \to \mathbb{R}_{\geq 0}$ dada por

$$\epsilon_\Lambda(\sigma) = \max_{x\in\mathcal{V}(\Lambda)} \frac{\left|f_{\sigma,\Lambda}(x) - \mathrm{E}\left[f_{\sigma,\Lambda}\right]\right|}{\mathrm{E}\left[f_{\sigma,\Lambda}\right]},$$

onde $\mathcal{V}(\Lambda)$ é a região de Voronoi do reticulado.

O teorema a seguir, provado em [LLB12], demonstra a equivalência com o parâmetro de suavização.

Teorema 3.3.3. [LLB12, Proposição 2] Se $\eta_\varepsilon(\Lambda) = \sqrt{2\pi}\sigma$, então $\epsilon_\Lambda(\sigma) = \varepsilon$.

O uso do fator de achatamento para escolher reticulados usados em codificação wiretap é decorrente de diversas propriedades boas que ocorrem quando o fator de achatamento é pequeno, tais como *ganho de sigilo* (ver [BO10] e [OSB16]) e resolvibilidade (ver [Blo11]).

3.4 Parâmetro de suavização generalizado

Definição 3.4.1. Seja X um conjunto. Uma *métrica* sobre X é uma função $d\colon X \times X \to \mathbb{R}_{\geq 0}$ que satisfaz, para todo $x, y, z \in X$ as propriedades:

1. $d(x, y) = 0$ se, e somente se, $x = y$ (identidade de indiscerníveis),
2. $d(x, y) = d(y, x)$ (simetria),
3. $d(x, z) \leq d(x, y) + d(y, z)$ (desigualdade triangular).

Podemos generalizar o parâmetro de suavização de forma natural, considerando métricas sobre o conjunto $X = \mathcal{F}(\mathcal{V}) = \left\{f : \mathcal{V} \to \mathbb{R}_{\geq 0}\right\}$.

Definição 3.4.2. Sejam Λ reticulado com região de Voronoi $\mathcal{V}$, e d uma métrica sobre $\mathcal{F}(\mathcal{V})$. Definimos o *parâmetro de suavização generalizado* $\eta_\varepsilon^d(\Lambda)$ como

$$\eta_\varepsilon^d(\Lambda) \coloneqq \inf\left\{s > 0 \;\middle|\; d\left(V(\Lambda)\cdot \mathcal{P}_s^\Lambda,\, 1\right) \leq \varepsilon\right\}.$$

Em particular podemos considerar as normas p, com $1 \leq p \leq \infty$, dadas por

- $\left\|f\right\|_p = \left(\int_{\mathcal{V}} |f(x)|^p \mathrm{d}x\right)^{1/p}$ se $p < \infty$,
- $\left\|f\right\|_\infty = \sup_{x\in\mathcal{V}} |f(x)|$.

Cada norma p induz uma distância definida por $d_p(f,g) = \|f-g\|_p$. Essa distância forma uma métrica sobre o espaço $L^p(\mathcal{V}) \subset \mathcal{F}(\mathcal{V})$, composto por classes de funções com norma p finita:

$$L^p(\mathcal{V}) \coloneqq \left\{f \in \mathcal{F}(\mathcal{V}) \;\middle|\; \|f\|_p < \infty\right\}_{/\sim},$$

onde $f \sim g$ se o conjunto dos pontos em que f difere de g tem medida nula.

Portanto o espaço L^p induz um parâmetro de suavização η_ε^p. É fácil notar que $\eta_\varepsilon^\infty = \eta_\varepsilon$. Um caso interessante é o parâmetro L^1, que parece ter relações com um problema criptográfico relevante chamado *problema da diferença estatística*, ou SD [Pei+13]. Uma possibilidade não muito explorada é a possibilidade de extender a definição para noções mais amplas de distância (como pseudométricas, ou divergências).

3.5 Simulações computacionais

No nosso estudo do parâmetro de suavização, escrevemos um programa na linguagem de computação numérica Julia [Bez+17] que calcula o valor aproximado parâmetro de suavização de reticulados nas dimensões 1, 2 e 3. Uma vez que o parâmetro de suavização satisfaz $\eta_\varepsilon(k\Lambda) = k\eta_\varepsilon(\Lambda)$, isto é, se altera com a dilatação de reticulados (mas não com rotação), precisamos desconsiderar a dilatação de um reticulado para tornar a comparação justa. Assim, tomamos como padrão para comparação justa a norma mínima fixa, e sempre que comparamos reticulados fazemos uma normalização. Escolhemos por nenhum motivo particular a norma mínima igual a 1.

3.5.1 Reticulados em dimensão 2

Assumimos $\Lambda = \langle v, w\rangle_{\mathbb{Z}} \subset \mathbb{R}^2$ reticulado de dimensão 2, com $v = (v_1, v_2)$, $w = (w_1, w_2)$ e matriz geradora dada por

$$M = \begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}.$$

Então o reticulado Λ^* tem matriz geradora

$$M^* = \left(M^{-1}\right)^\top = \frac{1}{\det M}\begin{bmatrix} w_2 & -v_2 \\ -w_1 & v_1 \end{bmatrix}.$$

Assim, podemos calcular a norma de um vetor genérico de Λ^*, que é dada por

$$\begin{aligned} \left\| M^* \begin{bmatrix} x \\ y \end{bmatrix} \right\|^2 &= \frac{1}{|\det M|^2} \left\| \begin{bmatrix} xw_2 - yv_2 \\ -xw_1 + yv_1 \end{bmatrix} \right\|^2 \\ &= \frac{1}{|\det M|^2}\left(x^2\|v\|^2 - 2xy\langle v, w\rangle + y^2\|w\|^2\right) \\ &= \frac{1}{|\det M|^2}\|xv - yw\|^2, \end{aligned}$$

o que facilita muito o cálculo do parâmetro nesta dimensão.

a) Primeiramente, a fim de comparar os parâmetros de suavização de reticulados com mesma norma mínima, fazemos o gráfico do parâmetro de suavização de $\Lambda_\alpha = \langle (1, 0), (\alpha, 1)\rangle_{\mathbb{Z}}$ em função de α, para alguns valores de ε.

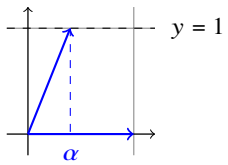


Figura 3.4: Ilustração das bases dos reticulados Λ_α.

Esta classe de reticulados é interessante, pois para todo $\alpha \in \mathbb{R}$, Λ_α tem distância mínima $\lambda = 1$ e densidade $\Delta = \frac{\pi}{4}$ (a base é de Minkowski [Cos+17, Cap. 2]). Além disso, uma vez que $\Lambda_\alpha = \Lambda_{\alpha+1}$, temos que a função é periódica com período 1.

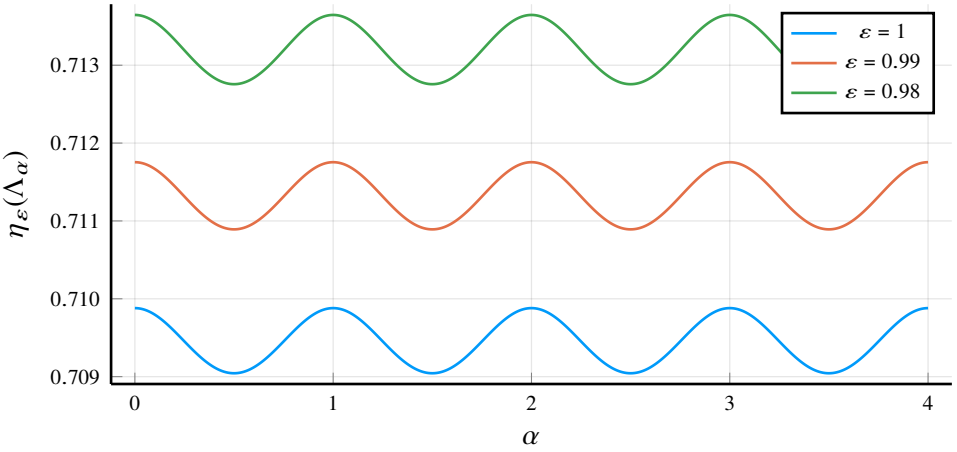


Figura 3.5: Parâmetro de suavização dos reticulados $\Lambda_\alpha = \langle (1,0), (\alpha, 1) \rangle_{\mathbb{Z}}$ em função de α.

Pode-se observar que a função obtida aparenta ter a forma de uma senoide em α. Fixando diferentes valores de $\varepsilon > 0$, obtemos senoides com diferentes centros. Notamos ainda que, para qualquer valor de ε, obtemos sempre o menor valor de parâmetro de suavização em $\alpha = 1/2$, e o maior valor em $\alpha = 0$ (que corresponde ao reticulado mais ortogonal e mais arredondado desta família).

b) A seguir, foram analisados os reticulados da forma

$$\Lambda_\theta = \langle (1,0), (\cos\theta, \sin\theta) \rangle_{\mathbb{Z}},$$

para $\frac{\pi}{3} \leq \theta \leq \frac{2\pi}{3}$. Apenas para valores de θ neste intervalo temos norma mínima igual a 1 (a base é de Minkowski), tornando a comparação justa.

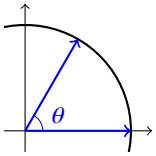


Figura 3.6: Ilustração das bases dos reticulados Λ_θ.

Ao computar o gráfico de $\eta_\varepsilon(\Lambda_\theta)$ para em função de θ para $\varepsilon \in \{0.5, 0.7, 1\}$, obtivemos, em todas os casos, gráficos semelhantes a parábolas (Figura 3.7).

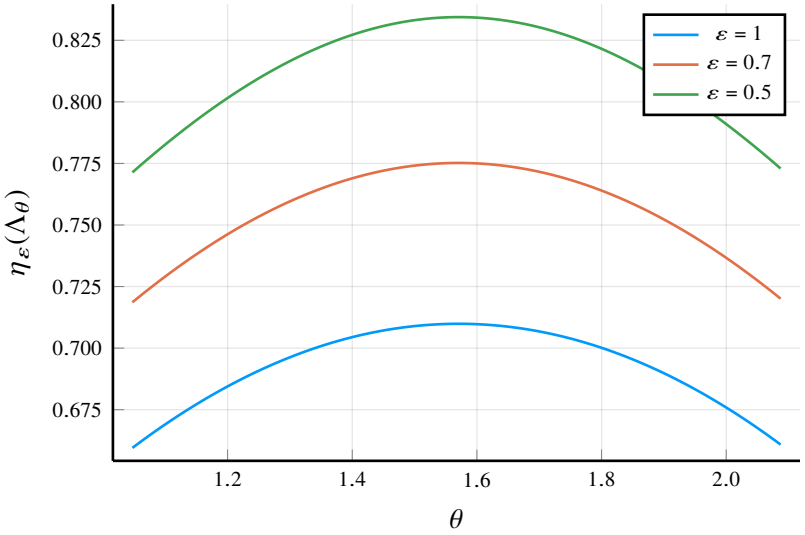


Figura 3.7: Parâmetro de suavização de $\Lambda_\theta = \langle (1,0), (\cos\theta, \sin\theta)\rangle_{\mathbb{Z}}$ em função de θ.

Observamos que a densidade $\Delta = \frac{\pi}{4\sin\theta}$ varia, sendo máxima em $\theta = \frac{\pi}{3}$ e $\theta = \frac{2\pi}{3}$ (reticulado hexagonal), e mínima em $\theta = \frac{\pi}{2}$. Enquanto isso,o parâmetro de suavização tem o efeito contrário, tendo seu menor valor em $\theta = \frac{\pi}{3}$ e $\theta = \frac{2\pi}{3}$ e seu maior valor em $\theta = \frac{\pi}{2}$.

c) Comparamos, ainda, o parâmetro de suavização de alguns reticulados importantes na dimensão 2: o reticulado $\mathbb{Z}^2$ e o reticulado hexagonal (Figure 3.8). O reticulado hexagonal parece ficar sempre abaixo do $\mathbb{Z}^2$.

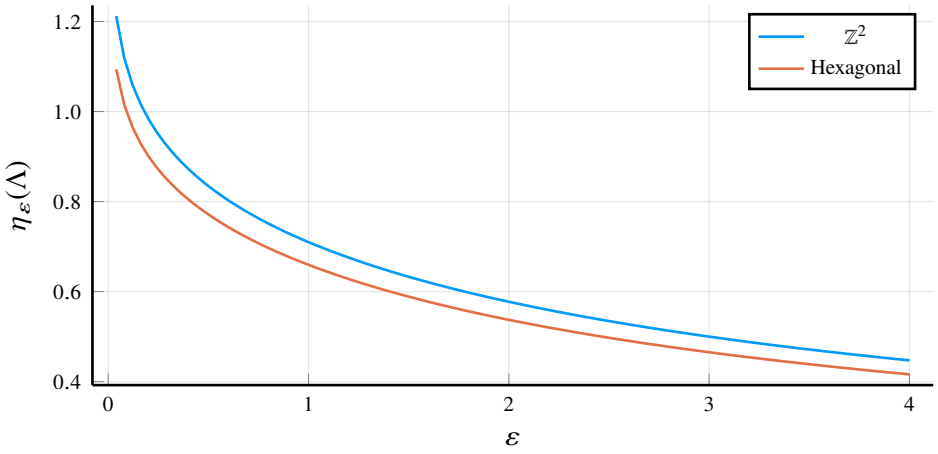


Figura 3.8: Parâmetro de suavização dos reticulados $\mathbb{Z}^2$ e hexagonal.

A princípio poderia-se suspeitar que para reticulados diferentes os gráficos dos parâmetros de suavização nunca se cruzam. Porém, não é este o caso; encontramos exemplos de dois reticulados, dos exemplos a) e b) acima, e cujos gráficos se cruzam. Na Tabela 3.1, temos valores dos parâmetros dos reticulados $\Lambda_1 = \left\langle (1,0), (1/2, 1)\right\rangle$, que tem densidade $\Delta = \pi/4 \approx 0.7854$ e $\Lambda_2 = \left\langle (1,0), (\cos(\pi/2.05), \sin(\pi/2.05))\right\rangle$, que tem densidade $\Delta = \frac{\pi}{4\sin(2.05)} \approx 0.8851$.

Λ	$\Lambda_1 = \langle (1,0), (1/2, 1) \rangle$	$\Lambda_2 = \langle (1,0), (\cos(\pi/2.05), \sin(\pi/2.05)) \rangle$
$\eta_{1/5}$	0.9727123208582191	0.9835658418363413
η_6	0.37796447311646797	0.3778257690216619

Tabela 3.1: Tabela de parâmetro de suavização de reticulados. Note que para $\varepsilon = 1/5$, Λ_1 é melhor, enquanto para $\varepsilon = 6$, Λ_2 é melhor.

Para valores bem pequenos de ε, o reticulado Λ_1 tem parâmetro de suavização menor, enquanto para valores grandes, é o Λ_2 que tem parâmetro de suavização menor. Na Tabela 3.1, isso é ilustrado para $\varepsilon = 1/5$ e $\varepsilon = 6$. Esse exemplo ilustra também que não basta ter melhor densidade para ter menor parâmetro de suavização.

3.5.2 Reticulados em dimensão 3

Comparamos aqui o parâmetro de suavização de alguns dos reticulados principais na dimensão 3: BCC e FCC (Seção 2.3.4), e $\mathbb{Z}^3$. Note que consideramos a versão normalizada de cada um deles, e para isso usamos as matrizes geradoras seguintes:

$$M_{\text{BCC}} = \frac{1}{\sqrt{3}} \begin{bmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \qquad M_{\text{FCC}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 \\ 1 & -1 & 1 \\ 0 & 0 & -1 \end{bmatrix}, \qquad M_{\mathbb{Z}^3} = I_3.$$

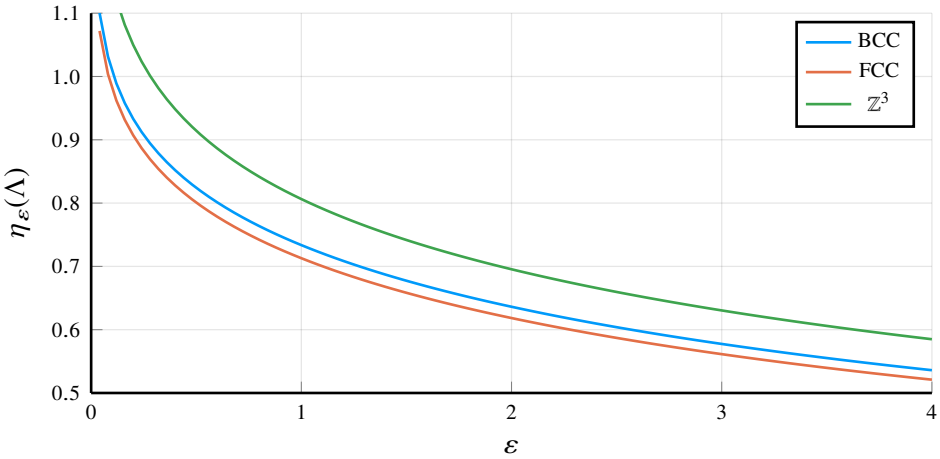


Figura 3.9: Parâmetro de suavização dos reticulados BCC, FCC e $\mathbb{Z}^3$.

Podemos observar nestes reticulados que quanto maior a densidade, menor o parâmetro de suavização, para diferentes parâmetros de ε. As densidades de empacotamento aproximadas dos reticulados $\mathbb{Z}^3$, BCC e FCC são respectivamente: 0.5236, 0.6802 e 0.7405.

Faz parte de nossas perspectivas futuras entender melhor qual a influência de parâmetros

como densidade de empacotamento, densidade de cobertura, razão de Hadamard e "arredondamento" dos reticulados no parâmetro de suavização.

3.5.3 Aproximação da distribuição uniforme

O Teorema 3.1.13 afirma que se $s > \eta_\varepsilon(\Lambda)$ então a distribuição $\mathcal{P}_s^\Lambda$ é aproximadamente uniforme em $1/V(\Lambda)$. Dessa forma, quanto maior for o s, mais perto de uniforme deve ser $\mathcal{P}_s^\Lambda$. Fazemos algumas simulações para visualizar melhor este fato. Nelas, consideramos o reticulado $\mathbb{Z} \subset \mathbb{R}$, e analisamos os gráficos de $\mathcal{P}_s^\Lambda$ para $s \in \{0.5, 0.7, 1, 2\}$ (ver Figura 3.10) note que de fato, quanto maior o s, mais a distribuição obtida aproxima-se de $1 = 1/V(\mathbb{Z})$.

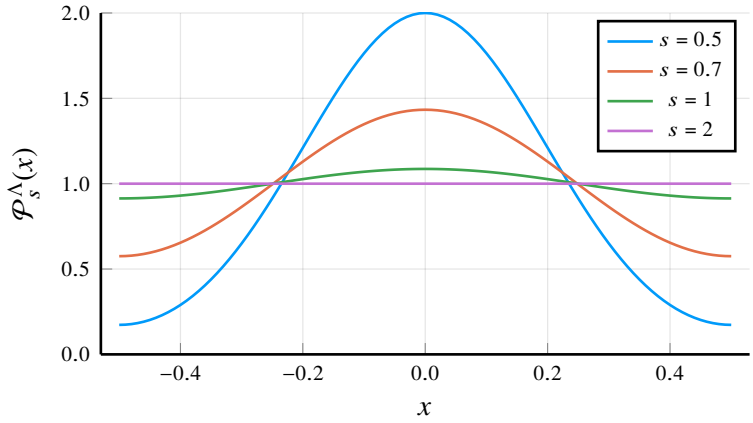


Figura 3.10: Gráfico de $\mathcal{P}_s^\Lambda(x)$ em função de x, para $s \in \{0.5, 0.7, 1, 2\}$.

Observamos assim que quanto menor for o parâmetro de suavização de um reticulado comparado com outros na mesma dimensão e com mesma distância mínima, menor é o s necessário para aproximar $\mathcal{P}_s^\Lambda$ da distribuição uniforme.

Capítulo 4

Criptografia baseada em reticulados

Neste capítulo, apresentamos alguns conceitos importantes de criptografia, e em seguida problemas que fundamentam alguns esquemas criptográficos baseados em reticulados. As principais referências foram: [MR07], [Mic07], [Reg09], [LPR12], [Pei16], [Pei+13] e [Gal12].

Utilizamos algumas vezes a notação assintótica para taxa de crescimento de funções, muito frequente em complexidade computacional. Por isso, introduzimos aqui as principais notações assintóticas.

Definição 4.0.1 (Notação Assintótica)**.** Sejam $f, g: \mathbb{N} \to \mathbb{N}$. Dizemos que:

i) $f = O(g)$ se existem $M > 0$, $n_0 \in \mathbb{N}$ tais que $n > n_0 \implies f(n) \leq Mg(n)$;

ii) $f = o(g)$ se, dado $M > 0$, existe $n_0 \in N$ tal que $n > n_0 \implies f(n) \leq Mg(n)$;

iii) $f = \Omega(g)$ se $g = O(f)$;

iv) $f = \theta(g)$ se $f = O(g)$ e $f = \Omega(g)$.

Utilizamos também a notação $\tilde{O}$ para omitir fatores logarítmicos na função, isto é, $f = \tilde{O}(g)$ se $f = O(g \cdot \log^k)$ para algum $k \in \mathbb{N}$.

4.1 Máquinas de Turing

Uma máquina de Turing é um modelo matemático de máquina que realiza computações. Informalmente, ela pode ser descrita com uma fita que se estende infinitamente para a esquerda e para a direita, com posições igualmente espaçadas onde podem ser inseridos símbolos. Uma "cabeça" da máquina avança por essas posições, substituindo símbolos e guardando a cada instante um estado.

Para cada símbolo e estado, a cabeça da máquina:

1. substitui o símbolo da posição que ela está;

2. muda o estado;

3. avança para a esquerda ou para a direita.

A forma como isso é feito é determinada pelo algoritmo da máquina. Se, para determinada posição e estado, não houver instrução, ou se a máquina chegar a um estado final, então a máquina termina a computação. Essa máquina pode ser definida mais formalmente da seguinte forma:

Definição 4.1.1 (Máquina de Turing)**.** [HMU13] Considere um conjunto finito não-vazio Q de estados, com um estado inicial $q_0 \in Q$ e um subconjunto de estados finais $F \subset Q$. Sejam ainda $\mathcal{L}$ um alfabeto finito não vazio, tal que existe um símbolo "branco" $b \in \mathcal{L}$ e um subconjunto de símbolos iniciais $\Sigma \subset \mathcal{L} \setminus \{b\}$. Uma *máquina de Turing* é uma 7-upla $\langle Q, \mathcal{L}, b, \Sigma, \delta, q_0, F \rangle$, onde

$$\delta : (Q \setminus F) \times \mathcal{L} \rightharpoonup Q \times \mathcal{L} \times \{\leftarrow, \rightarrow\}$$

é uma função parcial.

Supõe-se que a máquina recebe como entrada uma sequência finita não-vazia I de símbolos de Σ, e que a máquina começa com o estado q_0. A função parcial δ deve ser interpretada como a função que diz o comportamento da máquina ao se deparar com o par $(q, \alpha) \in (Q \setminus F) \times L$. Se $\delta(q, \alpha) = (\tilde{q}, \tilde{\alpha}, d)$, então a máquina deve trocar o símbolo α por $\tilde{\alpha}$, mudar para o estado $\tilde{q}$ e ir para a direção d. A máquina eventualmente para ao chegar em um estado de F ou ao não haver mais computações possíveis. A sequência de símbolos produzida é a saída da máquina.

Uma **máquina de Turing não-determinística** é uma máquina com definição semelhante; a única diferença é que basta que δ seja uma relação em $\big((Q \setminus F) \times \mathcal{L}\big) \times \big(Q \times \mathcal{L} \times \{\leftarrow, \rightarrow\}\big)$. Isto quer dizer que para um dado estado (q, α) podem haver várias instruções válidas em $Q \times \mathcal{L} \times \{\leftarrow, \rightarrow\}$, e qualquer sequência de instruções válidas de δ que chega num estado final de F é uma solução válida.

4.2 Problemas criptográficos

Criptografia é a prática e o estudo de técnicas para comunicação segura na presença de adversários [Riv90]. Isso geralmente é feito de tal forma que o adversário precise resolver um problema computacional difícil. Frequentemente o problema é caracterizado por um conjunto I de possíveis entradas, e um conjunto O de possíveis saídas. Chamaremos estes de *problemas instanciados*, e os elementos de I serão chamados de *instâncias*. Os dois tipos de problemas mais usados são:

- **Problema decisional:** é um problema tal que, para cada instância $x \in I$, existe uma única resposta $S(x) \in \{0, 1\}$ (que representam "não" e "sim"). Assim, podemos particionar $I = I_0 \cup I_1$, onde $I_0 = S^{-1}(0)$ e $I_1 = S^{-1}(1)$.

- **Problema de procura:** é um problema em que, dada uma instância $x \in I$ e uma relação $R \subset I \times O$, deve-se encontrar (se existir) y tal que xRy. Caso contrário, a entrada é rejeitada pelo problema.

Pela Tese de Church-Turing, supomos que cada problema computável que puder ser resolvido por métodos efetivos, pode ter sua solução descrita por uma máquina de Turing [Cop19]. Assim, para sermos mais formais, quando falamos *problema* estamos querendo dizer uma linguagem (um conjunto de palavras I num alfabeto Σ). E quando nos referirmos a um algoritmo ou à resolução de um problema, estaremos nos referindo a uma máquina de Turing que dá uma solução para cada palavra do problema.

Para construir técnicas de criptografia é natural procurar por problemas que sejam difíceis de resolver. De fato, a dificuldade do problema é o que dá a garantia da segurança. Assim, para construir métodos seguros de criptografia, precisamos ter uma definição de dificuldade.

Um problema difícil, do ponto de vista computacional, deveria ser um problema que precisa de k passos para ser resolvido, onde k é um número muito grande. Em particular, se o problema tivesse uma entrada de tamanho n, o problema deveria precisar de pelo menos $O(f(n))$ passos para ser resolvido, onde $f\colon \mathbb{N} \to \mathbb{N}$ é uma função que cresce muito rapidamente (ex: exponencial). No entanto, nenhum problema até hoje foi provado ser de tal forma.

Assim, dois critérios geralmente são utilizados para classificar problemas que provavelmente são difíceis na definição aqui colocada [Ajt96]:

1. Se um problema foi por muito tempo atacado por especialistas e cientistas, sem sucesso (por exemplo, o problema de fatoração de inteiros);

2. Se o problema é *NP-completo* (por exemplo, o problema da mochila).

Apesar do primeiro critério ser muito usado, o critério de NP-completude tem a vantagem de ser um argumento matemático (mesmo não sendo uma prova) para suspeitar da dificuldade. Vamos compreender o que significa um problema NP-completo.

Definição 4.2.1. Um problema decisional é dito NP se satisfaz uma das condições equivalentes:

i) o problema é solucionável em tempo polinomial por uma máquina de Turing não-determinística.

ii) cada entrada $x \in I_1$ (com resposta "sim") pode ser verificada em tempo polinomial;

Definição 4.2.2. Um problema L é NP-completo se L é NP, e cada problema NP pode ser reduzido a L em tempo polinomial.

Assim, se resolvermos um problema NP-completo em tempo polinomial, automaticamente resolvemos todos os problemas NP em tempo polinomial. Por isso NP-completude é uma boa forma de garantir dificuldade.

4.2.1 Análise de pior-caso e caso-médio

Para analisar a dificuldade de um problema, também é relevante fazer a diferenciação entre dificuldade no pior-caso, e dificuldade no caso-médio.

Definição 4.2.3. [Cor+09] Seja P um problema com instâncias em I. P é dito:

i) *difícil no caso-médio* se o problema $P(x)$ for difícil para instâncias aleatórias $x \in I$ tiradas a partir de certa distribuição pré-definida;

ii) *difícil no pior-caso* se existem instâncias difíceis.

Na criptografia é ideal que problemas sejam difíceis no caso-médio pois o problema será usado em instâncias aleatórias. Mas os problemas difíceis no pior-caso se tornam interessantes se houver uma **redução de pior-caso para médio-caso**, isto é, se tivermos P e Q problemas instanciados tais que se P for difícil no pior-caso então Q é difícil no caso médio. Dessa forma, para garantir que Q é um bom problema para criptografia basta garantir que não existem instâncias fáceis para P. É comum fazer esse tipo de redução para problemas em reticulados[Ajt96][MR07], como citamos em 4.4.

4.2.2 Sistemas de prova interativa

Definição 4.2.4 (Sistema de prova interativa)**.** [GMR89] Sejam Alice (ou verificador) e Bob (ou provador) dois participantes de um protocolo, tais que Alice é uma participante honesta com o poder computacional de uma máquina de Turing, e Bob é um participante não-confiável com poder computacional ilimitado. Dado um problema decisional instanciado P, um *sistema de prova interativa* de P é uma sequência de perguntas de Alice para Bob, que satisfaz duas propriedades:

1. **completude:** se a resposta de $P(x)$ é sim, então Alice é convencida deste fato através das respostas de Bob;

2. **correção:** se $P(x)$ é não, então a probabilidade de Bob conseguir convencer Alice do contrário é baixa.

Para maior formalidade, podemos descrever o protocolo através de uma distribuição de probabilidade $\mathfrak{K}_{A,B}: I \to \mathbb{R}_{\geq 0}$, onde I é o conjunto das instâncias de P. Então $\mathfrak{K}_{A,B}$ tem completude $c: I \to [0,1]$ e correção $s: I \to [0,1]$ se satisfaz [SV03]

1. se $x \in I_1$, então $\Pr\left[\mathfrak{K}_{A,B}(x) = 1\right] \geq 1 - c(x)$;

2. se $x \in I_0$, então $\Pr\left[\mathfrak{K}_{A,B}(x) = 0\right] \geq 1 - s(x)$.

Dois exemplos de sistemas de provas interativas são o protocolo de *Arthur-Merlin* e as provas de conhecimento-zero (*zero-knowledge proofs*).

Definição 4.2.5 (Protocolo de Arthur-Merlin)**.** [Bab85] Sejam Arthur um verificador, e Merlin um provador de um sistema de prova interativa. Suponha que Arthur está munido de um gerador probabilístico de números aleatórios. O sistema é dito *protocolo de Arthur-Merlin* se, dado um problema decisional instanciado P, o sistema satisfaz as propriedades:

- quando $x \in I_1$, existe uma sequência de respostas de Merlin tal que Arthur aceita a resposta pelo menos $2/3$ das vezes ($c(x) = 1/3$);
- quando $x \in I_0$, Arthur recusa o a resposta de Merlin em pelo menos $2/3$ das vezes ($s(x) = 1/3$).

Definição 4.2.6 (Problema AM)**.** Um problema decisional é dito AM se existe um protocolo de Arthur-Merlin com duas mensagens que decide este problema em tempo polinomial.

Uma *prova de conhecimento-zero* é um sistema de prova interativa que satisfaz a propriedade de *conhecimento-zero*, que pode ser definida informalmente da seguinte forma: dado um problema P a ser provado, Alice (a verificadora) consegue simular transcrição de possíveis interações válidas entre ela e um provador honesto. [Gol]

A propriedade de conhecimento-zero pode ter entendida como a propriedade de não revelar nada além da prova do problema. Suponhamos, por exemplo, que Bob quer provar para Alice que possui um segredo S, mas sem revelar para ela o segredo. Então é ideal que Alice e Bob usem um protocolo de conhecimento-zero, pois se Alice consegue produzir quaisquer transcritos de interações válidas, isso quer dizer que o protocolo não vaza nenhuma informação sobre S. Se houvesse transcrições de interações que Alice não é capaz de produzir, então isso significaria que em tal interação ela aprende algo.

Podemos definir provas de conhecimento-zero mais formalmente usando distribuições de probabilidade [Gol].

Definição 4.2.7 (Prova de conhecimento zero)**.** [Gol] Seja P um problema decisional com instâncias em I. Sejam Alice a verificadora, e Bob o provador de um sistema de prova interativa $\mathfrak{K}_{A,B}$. Sejam $\mathfrak{S}$ a distribuição de probabilidade de um simulador de interações entre Alice e Bob com entradas em I, e $\mathfrak{V}_{A,B}$ a distribuição de probabilidade relativa ao resultado das interações entre Alice e Bob. $\mathfrak{K}_{A,B}$ é dito *prova de conhecimento-zero estatística*, com parâmetro $\alpha\colon I \to \mathbb{R}_{\geq 0}$ se

$$\left\| \mathfrak{S}(x) - \mathfrak{V}_{A,B}(x) \right\| \leq \alpha(x),$$

onde $\|\cdot\|$ é a distância estatística, isto é, a distância induzida pela norma $\|\cdot\|_\infty$.

Se $\alpha = 0$ então $\mathfrak{K}_{A,B}$ é dita *prova de conhecimento-zero perfeita* (neste caso, Alice sempre consegue simular qualquer interação com Bob com perfeição).

Definição 4.2.8. [Gol] Um problema P é dito SZK se ele admite prova de conhecimento-zero estatística com um verificador honesto.

4.3 Problemas em reticulados

Dentro da criptografia, existe uma série de esquemas e métodos que depende de problemas em reticulados. Há tanto esquemas que são formulados em termos de reticulados, como o GGH, mostrado na seção 4.6, quando esquemas que não são formulados em termos de reticulados, mas para os quais existe uma redução a problemas em reticulados, como o SIS (Seção 4.4) e o LWE (Seção 4.7). Assim, a dificuldade, e consequentemente a segurança, de uma série de esquemas criptográficos é garantida pela dificuldade de problemas em reticulados.

Apresentamos aqui alguns dos mais clássicos e importantes problemas da criptografia baseada em reticulados. Primeiramente, definimos os problemas do vetor mais curto, e do vetor mais próximos, também conhecidos como SVP (*shortest vector problem*) e CVP (*closest vector problem*) [Pei16]. Lembre que $\lambda(\Lambda)$ é a menor norma de um vetor não-nulo de Λ.

Problema SVP. *Dado Λ um reticulado com base β, encontrar $v \in \Lambda \setminus \{0\}$, tal que $\|v\| = \lambda(\Lambda)$.*

Problema CVP. *Dados Λ um reticulado com base β e $w \in \mathbb{R}^n$, encontrar $v \in \Lambda$, $v \neq w$, que minimize $\|w - v\|$.*

É interessante notar que nas aplicações costuma-se utilizar as versões aproximadas dos problemas, por uma constante $\gamma \geq 1$ (onde para $\gamma = 1$ temos o problema original):

Problema SVP aproximado (SVP$_\gamma$). *Dado Λ um reticulado com base β, encontrar $v \in \Lambda$, $v \neq 0$, tal que $\|v\| \leq \gamma\, \lambda(\Lambda)$.*

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 $x \in \Lambda$, $x \neq w$.*

O problema SVP possui demonstrações de NP-dificuldade apenas para algumas reduções aleatórias [Ajt98] e para uma versão do problema na norma $\|\cdot\|_\infty$ [Emd81]. Já o problema CVP foi demonstrado NP-difícil na sua versão aproximada por uma constante $\gamma = 2^{(\log n)^{1-\varepsilon}}$, onde $\varepsilon = (\log\log n)^{-\alpha}$ para qualquer $\alpha < 1/2$ [DKS98].

Note que se o reticulado for suficientemente bom, ou se a base for ortogonal, os problemas SVP e CVP ficam fáceis, como mostra o exemplo a seguir.

Exemplo 4.3.1. Seja $\beta = \{b_1, \ldots, b_n\}$ é uma base ortogonal de Λ.

- SVP: O vetor mais curto de Λ é o vetor mais curto de β, pois se $v = \alpha_1 b_1 + \cdots + \alpha_n b_n \in \Lambda$, então
$$\|v\|^2 = \|\alpha_1 b_1 + \cdots + \alpha_n b_n\|^2 = \alpha_1^2\|b_1\|^2 + \cdots + \alpha_n^2\|b_n\|^2\,,\ \alpha_i \in \mathbb{Z}.$$
- CVP: Dado $w \in \mathbb{R}^n$, temos
$$\|v - w\|^2 = (\alpha_1 - \beta_1)^2\|b_1\|^2 + \cdots + (\alpha_n - \beta_n)^2\|b_n\|^2\,.$$

Assim, escolhendo $\alpha_i := \lfloor \beta_i \rceil$ (o inteiro mais próximo de β_i), vemos que $v = \alpha_1 b_1 + \cdots + \alpha_n b_n$ minimiza $\|v - w\|$.

É comum também a utilização de certas versões decisionais aproximadas destes problemas, conhecidas como GapSVP$_\gamma$ e GapCVP$_\gamma$ (onde $\gamma > 1$).

Problema GapSVP$_\gamma$. *Dados Λ um reticulado com base β, e $\gamma > 1$, tal que vale um dos dois casos: $\lambda \leq 1$ ou $\lambda \geq \gamma$. O problema consiste em descobrir qual dos casos vale.*

Problema GapCVP$_\gamma$. *Dados Λ um reticulado com base β, $\gamma > 1$ e $w \in \Lambda$, tal que vale um dos dois casos:*

i) existe $v \in \Lambda$ com $\|v - w\| \leq 1$, ou

ii) para todo $v \in \Lambda, \|v - w\| \geq \gamma$.

O problema consiste em descobrir qual dos casos vale.

O último dos problemas clássicos que enunciaremos é o problema dos vetores independentes mais curtos SIVP (*shortest independent vectors problem*), bem como sua versão aproximada por um $\gamma > 1$. Lembre (2.4) que λ_k denota a menor norma possível para um conjunto de k vetores independentes.

Problema SIVP. *Dada uma base β para Λ, encontrar um conjunto $\{v_1, \ldots, v_k\} \subset \Lambda$ linearmente independente, tal que $\max_{1 \leq i \leq n} \|v_i\| = \lambda_k$.*

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 $\max_{1 \leq i \leq n} \|v_i\| \leq \gamma \lambda_k$.*

4.4 Problema SIS

O problema SIS (*short integer solution*, isto é, solução inteira curta) foi introduzido por Ajtai em um trabalho de congresso ([Ajt96]). O interesse dele no trabalho era de mostrar uma família de funções resistentes a colisão (isto é, encontrar dois elementos do domínio com a mesma imagem é difícil). O problema SIS, como veremos, apesar de de não ser definido em termos de reticulados, pode ser reformulado em termos de reticulados, e tem sua demonstração de dificuldade baseada na redução a problemas em reticulados definidos na Seção 4.3.

Utilizaremos aqui a notação SIS$_\beta$ para denotar o problema SIS com parâmetro $\beta > 0$.

Problema SIS$_\beta$. *Sejam $a_1, \ldots, a_m \in \mathbb{Z}_q^n$ vetores uniformemente aleatórios, com $n, q \in \mathbb{N}$, e $\beta > 0$ um limitante. Encontre $z = (z_1, \ldots, z_m) \in \mathbb{Z}^m$ não-nulo, tal que*

$$a_1 z_1 + \cdots + a_m z_m = 0_{\mathbb{Z}_q^n} \qquad e \qquad \|z\| \leq \beta.$$

O problema SIS pode ser equivalentemente formulado em termos de reticulados. Note que a partir dos vetores $a_1, \ldots, a_m$ podemos construir uma matriz $A = [a_1 \ldots a_m] \in \mathbb{Z}_q^{n \times m}$. Então o problema SIS é equivalente a resolver o problema SVP_β no reticulado q-ário

$$\Lambda^\perp(A) = \left\{ z \in \mathbb{Z}^m \;\middle|\; Az = 0_{\mathbb{Z}_q^n} \right\},$$

definido na Seção 2.3.2.

Proposição 4.4.1. [Ajt96] Se $\sqrt{m} \leq \beta < q$ e $m > n \log_2 q$ então existem soluções não-triviais de SIS.

Demonstração. Se $m > n \log_2 q$ então $2^m > q^n$. Mas $2^m = |\{0,1\}^m|$ e $q^n \geq |\mathrm{Im}\, A|$. Logo, devem existir $x \neq x'$ em $\{0,1\}^m$ tais que $Ax = Ax'$. Portanto $(x - x') \in \{0, 1, -1\}^m$ é uma solução não-nula de $Az = 0_{\mathbb{Z}_q^n}$ com $\|x - x'\| \leq \sqrt{m} \leq \beta$. □

Uma consequência interessante da proposição acima é que a *função SIS* $f_A \colon \{0,1\}^n \to \mathbb{Z}_q^n$ definida por

$$f_A(z) = a_1 z_1 + \cdots + a_n z_n$$

é resistente a colisões, pois se obtivermos uma colisão de f_A (isto é, $z \neq z'$ com $f_A(z) = f_A(z')$) então obtemos automaticamente uma solução de SIS.

No trabalho [Ajt96] foi provado que se tivermos uma solução de SIS_β no médio-caso, então também temos soluções de $\mathrm{GapSVP}_{\beta\sqrt{n}}$ e de $\mathrm{SIVP}_{\beta\sqrt{n}}$ no pior-caso. Assim, se os problemas $\mathrm{GapSVP}_{\beta\sqrt{n}}$ ou $\mathrm{SIVP}_{\beta\sqrt{n}}$ forem difíceis no pior-caso, então o problema SIS_β é difícil no médio-caso.

4.5 Algoritmo LLL

Uma das importantes vertentes da criptografia baseada em reticulados é o estudo de algoritmos de redução de base. Uma vez que muitos criptossistemas baseiam-se na dificuldade de encontrar uma base de dado reticulado com vetores curtos e/ou próximos de ortogonal, o estudo de algoritmos de redução de base é uma forma de procurar ataques a criptossistemas.

O principal algoritmo conhecido de redução de base em tempo polinomial é o algoritmo LLL (1982) [LLL82], baseado da ortogonalização de Gram-Schmidt (ver a Definição 2.1.3), e que transforma uma base de reticulado em uma base LLL-reduzida (noção explicada na Definição 4.5.1).

Definição 4.5.1. [Gal12] Sejam $\beta = \{b_1, \ldots, b_k\}$ base de um reticulado em $\mathbb{R}^n$ e $\delta \in (1/4, 1)$. Dizemos que β é uma base LLL-reduzida com fator δ se satisfaz as seguintes condições:

- $|\mu_{i,j}| \leq 1/2$ para $1 \leq i < j \leq k$,
- $\|b_i'\|^2 \geq (\delta - \mu_{i,i-1}^2) \|b_{i-1}'\|^2$ para $2 \leq i \leq k$ (Condição de Lovász),

onde $b'_1, \ldots, b'_k$ é a ortogonalização de Gram-Schmidt de β e $\mu_{i,j}$ são os coeficientes.

Tipicamente é utilizado $\delta = 3/4$.

Proposição 4.5.2. [LLL82] Seja $\beta = \{b_1, \ldots, b_k\}$ base LLL-reduzida de um reticulado $\Lambda \subset \mathbb{R}^n$, com fator $\delta = 3/4$. Então $2^{1-i}\lambda_i \leq \|b_i\| \leq 2^{k-1}\lambda_i$ para todo $i \in \{1, \ldots, k\}$, onde os λ_i são os mínimos sucessivos, definidos na seção 2.2.

O algoritmo LLL, definido a seguir, é um algoritmo que, dada uma base de um reticulado, e um $\delta \in (1/4, 1)$, retorna uma base LLL-reduzida por fator δ do mesmo reticulado.

Algoritmo 1: (LLL com fator δ) [Gal12]

Entrada: Uma base de reticulado $\beta = \{b_1, \ldots, b_k\} \subset \mathbb{R}^n$.
Saída: Uma base $\beta = \{b_1, \ldots, b_k\}$ LLL-reduzida do mesmo reticulado.

Calcule a base de Gram-Schmidt β' e os coeficientes $\mu_{i,j}$ para $1 \leq j < i \leq k$;
$m = 2$;
enquanto $m \leq k$ **faça**
  para $j = m - 1$ *até* 1 **faça** (Reduz os vetores)
    Faça $b_m \leftarrow b_m - \lfloor \mu_{m,j} \rceil b_j$;
    Recalcule $\mu_{m,j}$ para $1 \leq j < m$;
  fim
  se $\|b'_m\|^2 \geq \left(\delta - \mu^2_{m,m-1}\right) \|b'_{m-1}\|^2$ **então** (Verifica condição de Lovász)
    $m \leftarrow m + 1$;
  senão
    Troque os valores de b_m e b_{m-1};
    Recalcule b'_m, b'_{m-1}, $\mu_{m-1,j}$, $\mu_{m,j}$ para $1 \leq j < m$ e $\mu_{i,m-1}$, $\mu_{i,m}$ para $m < i \leq k$;
    $m \leftarrow \max\{2, m - 1\}$;
  fim
fim

No livro [Gal12] é mostrado que se o algoritmo LLL termina, então a saída é uma base LLL-reduzida. Além disso, se $\delta \in (1/4, 1)$ então o algoritmo termina em $O(k^5 n^4 \log^3(B))$ operações, onde $B = \max\{\|b\| : b \in \beta\}$.

Exemplo 4.5.3. Sejam $b_1 = (1, 1)$, $b_2 = (2, 1)$. Então $\mu_{2,1} = 3/2$ e portanto a ortogonalização de Gram-Schmidt é $b'_1 = b_1$, $b'_2 = b_2 - \frac{3}{2}b'_1 = (1/2, -1/2)$.

Substituímos b_2 por $b_2 - \lfloor \mu_{2,1} \rceil b_1 = (2, 1) - 2 \cdot (1, 1) = (0, -1)$. Assim, $\mu_{2,1}$ será atualizado para $-1/2$, e b'_2 permanece $(1/2, -1/2)$. Assim, os novos vetores satisfazem a condição de Lovász:

$$\|b'_2\|^2 = 1/2 \geq 1 = \left(3/4 - \mu^2_{2,1}\right) \|b'_1\|^2.$$

Portanto o algoritmo acabou e a base LLL-reduzida é $b_1 = (1, 1)$, $b_2 = (0, -1)$.

4.6 Criptossistema GGH

Um dos primeiros algoritmos da criptografia baseada em reticulados é o algoritmo GGH (*Goldreich–Goldwasser–Halevi*), que ilustra bem como utilizar reticulados em esquemas criptográficos. Introduzido em 1997, ele é considerado ultrapassado, e hoje são consideradas viáveis apenas variantes do esquema [Pei16].

O esquema GGH é baseado na forma normal de Hermite, e sua segurança é baseada na dificuldade do problema CVP.

Teorema 4.6.1. Seja A matriz invertível com entradas inteiras. Então existe uma única matriz U unimodular tal que a matriz $H = AU$ (com entradas h_{ij}) satisfaz:

- $h_{ii} > 0$ para todo i;
- $h_{ij} = 0$ para $j > i$;
- $|h_{ij}| > h_{ii}$ para $j < i$.

A matriz H é chamada *forma normal de Hermite* de A.

Note que forma normal de Hermite pode ser computada de maneira eficiente, como mostrado em [SL96].

Exemplo 4.6.2. Se

$$A = \begin{bmatrix} 2 & 1 & 2 \\ 2 & 3 & 1 \\ 0 & 1 & 2 \end{bmatrix},$$

então temos que

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 7 & 8 & 10 \end{bmatrix}}_{H} = A \cdot \underbrace{\begin{bmatrix} -3 & -4 & -5 \\ 1 & 2 & 2 \\ 3 & 3 & 4 \end{bmatrix}}_{U}.$$

Definição 4.6.3 (Razão de Hadamard)**.** Dada uma matriz geradora $B = [b_1 \dots b_n]$ de um reticulado em $\mathbb{R}^n$, definimos a razão de Hadamard de B como

$$\mathcal{H}(B) = \left(\frac{\det(B)}{\|b_1\| \cdots \|b_n\|} \right)^{\frac{1}{n}}.$$

A razão de Hadamard é um valor dentro do intervalo $(0, 1)$. Quanto mais perto de 1 for a razão de Hadamard, mais próxima de ortogonal a base é, e ela vale 1 apenas no caso em que B é ortogonal. Assim, podemos usar esse valor para distinguir se uma base é "quase ortogonal", com uma razão próxima de 1.

Algoritmo 2: Geração de Chaves GGH

Entrada: Um parâmetro de segurança $n \in \mathbb{N}$ e um valor pequeno $b \in \mathbb{N}$.
Saída: Matrizes geradoras B (chave secreta) e H (chave pública) de um reticulado Λ.

1 Escolha vetores quase-ortogonais $b_1, \ldots, b_n \in \mathbb{Z}^n$ com $b_{ij} < b$;
2 Calcule a forma normal de Hermite H de $B = [b_1 \cdots b_n]$;
3 Retorne B e H.

Algoritmo 3: Encriptação GGH

Entrada: Uma matriz geradora de reticulado H e uma mensagem $m \in \mathbb{Z}^n$.
Saída: Um texto cifrado $c \in \mathbb{R}^n$.

1 Calcule $v = Hm$;
2 Escolha $r \in \mathbb{R}^n$ tal que o vetor mais próximo de $v + r$ seja v;
3 Retorne $c = v + r$.

Apresentamos aqui os esquemas de geração de chaves, e de encriptação do GGH. Este esquema é de criptografia assimétrica, isto é, existem duas chaves: a *chave pública*, responsável por encriptar mensagens, e a *chave secreta*, responsável por decriptá-las.

Definição 4.6.4. Dado $x \in \mathbb{R}$, definimos o arredondamento de x por $\lfloor x \rceil := \lfloor x + 1/2 \rfloor$. Para $v \in \mathbb{R}^n$, $\lfloor v \rceil := \big(\lfloor v_1 \rceil, \ldots, \lfloor v_n \rceil\big)$.

Definição 4.6.5 (Arredondamento de Babai)**.** Dada uma matriz geradora $B = [b_1 \cdots b_n]$ de um reticulado, e um vetor $y \in \mathbb{R}^n$, definimos o *arredondamento de Babai* [Bab86] de y com relação a B como o vetor

$$z = B\left\lfloor B^{-1} y \right\rceil$$

Se $y = \alpha_1 b_1 + \cdots + \alpha_n b_n$, o arredondamento de Babai pode ser escrito equivalentemente como $z = \lfloor \alpha_1 \rceil b_1 + \cdots + \lfloor \alpha_n \rceil b_n$.

A ideia para fazer a decriptação é utilizar o algoritmo de Babai para encontrar o vetor mais próximo de $(v + r)$. O algoritmo de arredondamento de Babai geralmente funciona bem quando temos uma base B suficientemente ortogonal (algo que pode ser medido através da razão de Hadamard). Em particular, o arredondamento de Babai resolve CVP_γ para $\gamma = \left(1 + 2n\left(9/2\right)^{n/2}\right)$ [Gal12].

Algoritmo 4: Decriptação GGH

Entrada: Um texto cifrado $c \in \mathbb{R}^n$ e a chave secreta B.
Saída: A mensagem decriptada $\tilde{m}$.

1 Calcule $U = B^{-1}H$;
2 Retorne $\tilde{m} = U^{-1}\left\lfloor B^{-1}c \right\rceil$, onde $H = BU$.

Teorema 4.6.6. [Pei16] Se B é matriz geradora, e r curto o suficiente para que o arredondamento de Babai funcione, então o esquema GGH funciona.

Demonstração. Como r é curto o suficiente para o arredondamento de Babai funcionar, temos que $\left\lfloor B^{-1}(v+r)\right\rceil = B^{-1}v$. Logo:

$$U^{-1}\left\lfloor B^{-1}c\right\rceil = U^{-1}\left\lfloor B^{-1}(v+r)\right\rceil = U^{-1}B^{-1}v = U^{-1}B^{-1}Hm = U^{-1}B^{-1}BUm = m. \qquad \square$$

4.7 Problema LWE

Um dos problemas mais estudados atualmente dentro da criptografia baseada em reticulados é o problema da aprendizagem com erros (*learning with errors*), abreviado por LWE. Este problema foi introduzido em 2005 por Oded Regev [Reg05], como uma generalização do problema de aprendizado de máquinas conhecido como *parity learning*.

O problema tem como parâmetros os inteiros n, q, e por uma distribuição de probabilidade $\chi : \mathbb{Z}_q \to \mathbb{R}_{>0}$.

Definição 4.7.1 (Distribuição LWE)**.** Seja $s \in \mathbb{Z}_q^n$ um vetor chamado "segredo". A *distribuição LWE* é uma distribuição de probabilidade $A_{s,\chi}$ sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$ amostrada por pares $\big(a, \langle a, s\rangle + \varepsilon \pmod q\big)$, onde a é escolhido uniformemente em $\mathbb{Z}_q^n$ e ε é escolhido usando a distribuição χ.

Note que a definição não explicita qual a probabilidade de cada par $(a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ ser escolhido, mas explicita como escolher um par (a, b) segundo a distribuição, o que será suficiente para nós.

O problema LWE é geralmente formulado como problema de procura, da seguinte forma:

Problema 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.*

No entanto existe também a formulação como problema de decisão, dada a seguir.

Problema DLWE$_{n,q,\chi,m}$**.** *Dadas m amostras independentes $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, escolhidas por uma das duas formas:*

1. *pela distribuição $A_{s,\chi}$ para um $s \in \mathbb{Z}_q^n$ uniformemente aleatório, ou*
2. *uniformemente em $\mathbb{Z}_q^n \times \mathbb{Z}_q$,*

distinguir qual das duas formas foi usada.

Sem os termos de erro de χ, ambos os problemas se tornam fáceis, pois para resolver o LWE-procura basta resolver o sistema linear

$$\begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix} s = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix},$$

e para resolver o LWE-decisão, basta ver se o sistema tem solução (no caso de as amostras serem escolhidas uniformemente, com grande probabilidade não haverá solução).

A noção formal de *resolver LWE* é dada pela definição seguinte.

Definição 4.7.2. Dado $q: \mathbb{N} \to \mathbb{Z}$, dizemos que um algoritmo W resolve $\mathrm{LWE}_{n,q,\chi,m}$ se, dadas m amostras de $A_{s,\chi}$ para um s arbitrário, W retorna s com probabilidade exponencialmente próxima a 1.

4.7.1 Dificuldade do problema LWE

A dificuldade do problema LWE é provada através de uma redução para um problema em reticulados: o problema da amostragem gaussiana discreta, abreviado por DGS (*discrete Gaussian sampling problem*). Informalmente, o objetivo do problema é em, dado um reticulado, encontrar uma amostra da distribuição gaussiana discreta $D_{\Lambda,r}$ para r suficientemente grande. No caso de LWE, a noção de "suficientemente grande" será dada pelo parâmetro de suavização.[Reg09]

O Teorema 4.7.3 reduz DGS a LWE, enquanto as Proposições 4.7.5 e 4.7.4 reduzem DGS aos problemas GapSVP e SIVP (ver Seção 4.3). Dessa forma, a segurança de LWE é garantida pela segurança de problemas em reticulados, utilizando o parâmetro de suavização.

Seja $\mathcal{L}^n$ o conjunto de todos os reticulados em $\mathbb{R}^n$. O problema DGS_φ tem como parâmetro uma função $\varphi: \mathcal{L}^n \to \mathbb{R}$.

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). Costuma-se utilizar o problema DGS com a uma função da forma $\varphi(\Lambda) = \sqrt{2n}\eta_\varepsilon(\Lambda)/\alpha$ para certos valores de $\alpha > 0$ e $\varepsilon > 0$, como mostrado nos teoremas a seguir. 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), e essa dificuldade é determinada pelo parâmetro de suavização.

Nos teoremas a seguir utilizaremos $\chi = \bar{\Psi}_\alpha$, como definido na seção 3.2, e como é mais comum na literatura[Pei16].

Teorema 4.7.3. [Reg09, Teo. 3.1] Sejam $\varepsilon: \mathbb{N} \to \mathbb{R}_{>0}$ função "erro", $p: \mathbb{N} \to \mathbb{Z}$ e $\alpha: \mathbb{N} \to (0, 1)$ funções tais que $\alpha(n) \cdot p(n) > 2\sqrt{n}$ para todo $n \in \mathbb{N}$. 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 $\mathrm{DGS}_{\sqrt{2n}\cdot\eta_\varepsilon(\Lambda)/\alpha}$.

Proposição 4.7.4. [Reg09] Dados $\varepsilon: \mathbb{N} \to (0, 1/10)$ e $\varphi(\Lambda) \geq \sqrt{2}\eta_{\varepsilon(n)}(\Lambda)$, existe uma redução polinomial de $\mathrm{SIVP}_{2\sqrt{n}\varphi}$ a DGS_φ.

Proposição 4.7.5. [Reg09] Dado $\gamma\colon \mathbb{N} \to \mathbb{R}_{\geq 1}$, existe uma redução polinomial de $\text{GapSVP}_{100\sqrt{n}\gamma(n)}$ a $\text{DGS}_{\sqrt{n}\gamma(n)/\lambda(\Lambda^*)}$.

4.7.2 Criptossistema LWE

A primeira utilização do problema LWE em um esquema criptográfico foi o *criptossistema LWE* apresentado primeiramente em [Reg05]. Notemos que este é um esquema de criptografia *assimétrica*, isto é, existem duas chaves: uma chave pública, que encripta mensagens; e uma chave secreta, que decripta mensagens cifradas.

- **Chave secreta:** $s \in \mathbb{Z}_q^n$ escolhido uniformemente;
- **Chave pública:** um conjunto de m pares ordenados $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ escolhidos por $A_{s,\chi}$.

Apresentamos aqui os algoritmos para encriptação de mensagens, e decriptação deste esquema.

Algoritmo 5: Encriptação LWE

Entrada: um bit $b \in \{0, 1\}$ e $S \subset \{1, \ldots, m\}$.
Saída: um bit cifrado $c \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

se $b = 0$ **então**
  $c = (\sum_{i\in S} a_i, \sum_{i\in S} b_i)$;
senão se $b = 1$ **então**
  $c = (\sum_{i\in S} a_i, \lfloor q/2 \rfloor + \sum_{i\in S} b_i)$;
fim
retorne c.

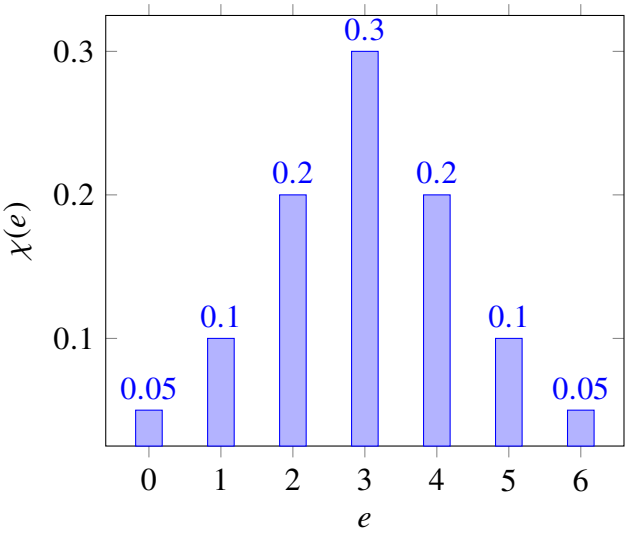
Algoritmo 6: Decriptação LWE

Entrada: um bit cifrado $c = (a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ e um segredo $s \in \mathbb{Z}_q^n$.
Saída: um bit descriptado $\tilde{b} \in \{0, 1\}$.

se $b - \langle a, s\rangle \mod q$ *está mais perto de* 0 *que de* $\lfloor q/2 \rfloor$ **então**
  $\tilde{b} = 0$;
senão
  $\tilde{b} = 1$;
fim
retorne $\tilde{b}$.

Para n, q e χ adequadamente escolhidos, a probabilidade de haver um erro no processo de decriptação fica pequena, e o criptossistema é fica seguro [Pei16].

Exemplo 4.7.6. Tome $n = 2$, $q = 7$ e χ dada por



Escolhemos $s = (1, 2) \in \mathbb{Z}_7^2$, e tomamos 5 amostras aleatórias:

$$
\begin{aligned}
(a_1, b_1) &= \big((3,1), \langle (3,1), (1,2)\rangle + 3 \mod 7\big) = ((3,1), 1)\,, \\
(a_2, b_2) &= \big((4,2), \langle (4,2), (1,2)\rangle + 3 \mod 7\big) = ((4,2), 4)\,, \\
(a_3, b_3) &= \big((4,1), \langle (4,1), (1,2)\rangle + 4 \mod 7\big) = ((4,1), 3)\,, \\
(a_4, b_4) &= \big((2,0), \langle (2,0), (1,2)\rangle + 2 \mod 7\big) = ((2,0), 4)\,, \\
(a_5, b_5) &= \big((1,5), \langle (1,5), (1,2)\rangle + 3 \mod 7\big) = ((1,5), 0)\,.
\end{aligned}
$$

Assim, tomando o conjunto $S = \{1, 2, 3, 4, 5\} \subset [5]$, encriptamos os bits 0 e 1:

$$
\begin{aligned}
c_0 &= (\textstyle\sum_{i\in S} a_i, \sum_{i\in S} b_i) = ((0,2), 5), \\
c_1 &= (\textstyle\sum_{i\in S} a_i, 3 + \sum_{i\in S} b_i) = ((0,2), 1).
\end{aligned}
$$

- No caso de c_0, temos que $b - \langle a, s\rangle = 5 - \langle (0,2), (1,2)\rangle = 1$, que está mais próximo de 0 que de 3, e portanto $\tilde{b_0} = 0$.
- No caso de c_1, temos que $b - \langle a, s\rangle = 1 - \langle (0,2), (1,2)\rangle = 4$, que está mais próximo de 3 que de 0, e portanto $\tilde{b_1} = 1$.

Note que para o sucesso da decriptação, é ideal utilizar valores mais altos de n e q.

4.8 Generalizações sobre anéis

Em 2002, Micciancio [Mic07] introduz uma generalização do problema SIS para anéis da forma $R = \mathbb{Z}[X]/(f)$, já estudados na Seção 2.7. Nesta seção também foi definido o sentido de norma no anel R, que pode ser estendido para R^m pela formula $\|z^m\| = \sum_{i=1}^m \|z_i\|$. Usamos também o anel quociente $R_q := R/qR$, onde $q \in \mathbb{N}$.

Problema anel-SIS. *Dados $a_1, \ldots, a_m \in R_q$ e $\beta \in \mathbb{R}_{>0}$ limitante, encontrar $z = (z_1, \ldots, z_m) \in R^m$ tal que*

$$a_1 z_1 + \cdots + a_m z_m = 0_{R_q} \qquad e \qquad \|z\| \leq \beta.$$

Note que para cada $a = (a_1, \ldots, a_m) \in R_q^m$ podemos definir a *função SIS* $f_a \colon R^m \to R_q$ dada por

$$f_a(z_1, \ldots, z_m) = a_1 z_1 + \cdots + a_m z_m.$$

Assim, o problema anel-SIS se reduz a encontrar $z \in R^m, \|z\| \leq \beta$ tal que $f_a(z) = 0_{R_q}$.

Existe também uma generalização do problema LWE para anéis da forma $R = \mathbb{Z}[X]/(f)$, chamado de R-LWE. O problema foi introduzido em 2012 no artigo [LPR12], e tem sua segurança baseada em uma redução de pior-caso para médio-caso do problema SVP. Analogamente ao problema LWE original, definimos uma distribuição $A_{s,\chi}$ sobre $R_q \times R_q$, para algum segredo $s \in R_q$, definida por amostras. Suas amostras são pares (a, b), onde a é escolhido uniformemente em R_q, e $b = sa + e$ onde e é amostrado de χ [Pei16]. O problema R-LWE em sua versão decisional é definido a seguir.

Problema R-DLWE$_{q,\chi,m}$. *Dadas m amostras independentes $(a_i, b_i) \in R_q \times R_q$, escolhidas por uma das duas formas:*

1. *pela distribuição $A_{s,\chi}$ para um $s \in R_q$ uniformemente aleatório, ou*
2. *uniformemente em $R_q \times R_q$,*

distinguir qual das duas formas foi usada.

4.9 O problema do parâmetro de suavização

O problema do parâmetro de suavização (problema GapSPP) é um problema criptográfico relacionado à dificuldade de encontrar uma aproximação deste parâmetro. Foi apresentado pela primeira vez em 2013, no artigo [Pei+13].

Este é um *problema de promessa*, que é uma generalização de um problema de decisão. Em um problema de promessa, existem o conjunto de possíveis instâncias I, o subconjunto $I_{\mathrm{S}} \subset I$ das instâncias que retornam SIM, e o subconjunto $I_{\mathrm{N}} \subset I$ das instâncias que retornam NÃO. No entanto pode ser o caso que $I_{\mathrm{S}} \cup I_{\mathrm{N}} \neq I$, pois podem haver instâncias que não são aceitas pelo problema.

Problema γ-GapSPP$_{\varepsilon_{\mathrm{S}},\varepsilon_{\mathrm{N}}}$. *Sejam γ, ε_S e ε_N funções de $\mathbb{N}$ em $\mathbb{R}_{>0}$, com $\gamma > 1$ e $\varepsilon_S \leq \varepsilon_N$. Cada instância de γ-GapSPP$_{\varepsilon_S,\varepsilon_N}$ é uma base β de um reticulado n-dimensional $\Lambda \subset \mathbb{R}^n$.*

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

Escrevemos γ-GapSPP$_\varepsilon$ para a versão do problema quando $\varepsilon = \varepsilon_S = \varepsilon_N$.

As demonstrações de segurança do problema do parâmetro de suavização consistem nas classes de complexidade AM e SZK (ver Seção 4.2.2).

O artigo [Pei+13] demonstra que para $\gamma = (2 + o(1))$ e $\eta = 1/P(n)$, onde P é um polinômio em $\mathbb{Z}$, o problema γ-GapSPP$_\varepsilon$ é AM e SZK. O algoritmo de Arthur-Merlin que garante a propriedade AM é dado a seguir.

Algoritmo 7: Protocolo Goldreich-Goldwasser gaussiano (Arthur-Merlin).

Entrada: Uma matriz geradora B de reticulado $\Lambda \subset \mathbb{R}^n$.

1 Verificadora amostra $x \leftarrow D_{\Lambda^*,1}$ e envia $\overline{x} = x \mod B$ para o provador;
2 Provador escolhe $x' \in \mathbb{R}^n$;
3 Verificador aceita se $x' = x$;

A intuição é que o provador deve escolher o vetor $x' \in x + \Lambda$ mais provável de ter sido amostrada por $D_{\Lambda^*,1}$. Como esta distribuição é centrada na origem, ele deve escolher o vetor mais curto de $x + \Lambda$.

Teorema 4.9.1. [Pei+13] Sejam ε, δ com $0 < \varepsilon \leq \delta < 1/2$. O Algoritmo 7 satisfaz:

1. completude: se $\eta_\varepsilon(\Lambda) \leq 1/2$, então existe um provador tal que a verificadora aceita o resultado com probabilidade maior ou igual a $1 - \varepsilon$;

2. correção: se $\eta_{\delta/(1-\delta)}(\Lambda) \geq 1$ então a verificadora rejeita o resultado com probabilidade maior ou igual a δ.

A demonstração de que $(2 + o(1))$-GapSPP é SZK é dada através de passos intermediários, envolvendo protocolos de compromisso, e por isso não há a explicitação de um algoritmo de provas de conhecimento-zero. Um problema em aberto interessante é de verificar se $(2 + o(1))$-GapSPP é SZK-completo, no sentido de que cada problema SZK pode ser reduzido em tempo polinomial a $(2 + o(1))$-GapSPP. Uma razão para se acreditar que é o caso, é que não se sabe se $(2 + o(1))$-GapSPP é NP nem coNP, e os únicos problemas conhecidos com essas características são problemas SZK-completos [Pei+13].

Capítulo 5

Conclusões

Neste trabalho estudamos reticulados e suas propriedades, em particular nos aspectos mais relevantes para aplicações em segurança e confiabilidade da informação, bem como as aplicações particulares dessas propriedades em alguns problemas criptográficos importantes.

No Capítulo 2, apresentamos as definições básicas do estudo reticulados, e vimos alguns exemplos importantes. No capítulo 3, estudamos o parâmetro de suavização, importante parâmetro de reticulado para aplicações em criptografia, e estudamos como são usadas funções e distribuições gaussianas sobre reticulados. Fazemos também algumas simulações computacionais que comparam os parâmetros e ilustram os conceitos definidos. Por fim, no capítulo 4, apresentamos conceitos de criptografia, segurança e complexidade computacional e vimos como reticulados são utilizados em alguns sistemas criptográficos. Principalmente, vimos como o parâmetro de suavização é utilizado nesses sistemas.

Como colocado no Capítulo 3, uma perspectiva futura é a de analisar melhor como o parâmetro de suavização se relaciona com outros parâmetros importantes de reticulados, como densidade de empacotamento, densidade de cobertura, razão de Hadamard, arredondamento, entre outros.

Outras perspectivas são o aprofundamento do estudo de como gaussianas em reticulados, e o parâmetro de suavização são utilizados em codificação wiretap. Além disso, parece interessante estudar mais profundamente o parâmetro de suavização generalizado, para noções diferentes de distância, e possivelmente de divergência. Uma outra questão interessante é se no caso de termos uma estrutura algébrica nos reticulados, como por exemplo nos reticulados ideais, podemos ter mais informações sobre o parâmetro de suavização.

Referências

[Agg+15] D. Aggarwal, D. Dadush, O. Regev e N. Stephens-Davidowitz. "Solving the Shortest Vector Problem in 2^n Time Using Discrete Gaussian Sampling: Extended Abstract". Em: *Proceedings of the Forty-seventh Annual ACM Symposium on Theory of Computing*. STOC '15. ACM, 2015, pp. 733–742. ISBN: 978-1-4503-3536-2. DOI: 10.1145/2746539.2746606.

[Ajt96] M. Ajtai. "Generating Hard Instances of Lattice Problems (Extended Abstract)". Em: *In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*. ACM, 1996, pp. 99–108. DOI: 10.1145/237814.237838.

[Ajt98] Miklós Ajtai. "The Shortest Vector Problem in L2 is NP-Hard for Randomized Reductions (Extended Abstract)". Em: *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*. STOC '98. Association for Computing Machinery, 1998, pp. 10–19. ISBN: 0897919629. DOI: 10.1145/276698.276705.

[Ala+19] G. Alagic et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. National Institute of Standards and Technology. Jan. de 2019. DOI: 10.6028/NIST.IR.8240.

[AMW04] M. I. Aroyo, U. Müller e H. Wondratschek. "Historical introduction". Em: *International Tables for Crystallography*. Vol. A1. Springer, 2004, pp. 2–5. ISBN: 978-1-4020-2355-2. DOI: 10.1107/97809553602060000537.

[Aru+19] F. Arute et al. "Quantum supremacy using a programmable superconducting processor". Em: *Nature* 574.7779 (out. de 2019), pp. 505–510. DOI: 10.1038/s41586-019-1666-5.

[Bab85] L Babai. "Trading Group Theory for Randomness". Em: *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*. STOC '85. Association for Computing Machinery, 1985, pp. 421–429. ISBN: 0897911512. DOI: 10.1145/22145.22192.

[Bab86] L. Babai. "On Lovász' lattice reduction and the nearest lattice point problem". Em: *Combinatorica* 6.1 (1986), pp. 1–13. ISSN: 1439-6912. DOI: 10.1007/BF02579403.

[BV08] Christine Bachoc e Frank Vallentin. “New upper bounds for kissing numbers from semidefinite programming”. Em: *Journal of the American Mathematical Society* 21.3 (set. de 2008), pp. 909–909. ISSN: 1088-6834. DOI: 10.1090/s0894-0347-07-00589-9. URL: http://dx.doi.org/10.1090/S0894-0347-07-00589-9.

[Ban93] W. Banaszczyk. “New bounds in some transference theorems in the geometry of numbers”. Em: *Mathematische Annalen* 296 (1993), pp. 625–635. DOI: 10.1007/BF01445125.

[Bel11] J. Belfiore. “Lattice codes for the compute-and-forward protocol: The flatness factor”. Em: *2011 IEEE Information Theory Workshop*. Out. de 2011, pp. 1–4.

[BO10] J. Belfiore e F. Oggier. “Secrecy gain: A wiretap lattice code design”. Em: *2010 International Symposium On Information Theory Its Applications*. Out. de 2010, pp. 174–178. DOI: 10.1109/ISITA.2010.5650095.

[Ber09] Daniel J. Bernstein. “Introduction to post-quantum cryptography”. Em: *Post-Quantum Cryptography*. Springer Berlin Heidelberg, 2009, pp. 1–14. ISBN: 978-3-540-88702-7. DOI: 10.1007/978-3-540-88702-7_1.

[Bez+17] J. Bezanson, A. Edelman, S. Karpinski e V. B. Shah. “Julia: A fresh approach to numerical computing”. Em: *SIAM review* 59.1 (2017), pp. 65–98. DOI: 10.1137/141000671.

[Blo11] M. R. Bloch. “Achieving secrecy: Capacity vs. resolvability”. Em: *2011 IEEE International Symposium on Information Theory Proceedings*. Jul. de 2011, pp. 633–637.

[Cas97] J. W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer Berlin Heidelberg, 1997. ISBN: 978-3-642-62035-5. DOI: 10.1007/978-3-642-62035-5.

[Coh+17] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko e Ma. Viazovska. “The sphere packing problem in dimension 24”. Em: *Annals of Mathematics* 185.3 (2017), pp. 1017–1033. ISSN: 0003486X.

[CS99] J. H. Conway e N. J. A. Sloane. *Sphere Packings, Lattices and Groups*. Springer New York, 1999, pp. 94–135. ISBN: 978-1-4757-6568-7. DOI: 10.1007/978-1-4757-6568-7_4.

[Cop19] B. J. Copeland. “The Church-Turing Thesis”. Em: *The Stanford Encyclopedia of Philosophy*. Ed. por Edward N. Zalta. Spring 2019. Metaphysics Research Lab, Stanford University, 2019.

[Cor+09] T. H. Cormen, C. E. Leiserson, R. L. Rivest e C. Stein. *Introduction to Algorithms*. MIT press, 2009. ISBN: 9780262033848.

[Cos+17] S. I. R. Costa, F. Oggier, A. Campello, J. C. Belfiore e E. Viterbo. *Lattices Applied to Coding for Reliable and Secure Communications*. Springer International Publishing, 2017. ISBN: 978-3-319-67882-5. DOI: 10.1007/978-3-319-67882-5.

[DKS98] I. Dinur, G. Kindler e S. Safra. "Approximating-CVP to within almost-polynomial factors is NP-hard". Em: *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*. Nov. de 1998, pp. 99–109. DOI: 10.1109/SFCS.1998.743433.

[Ebe12] 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.

[Emd81] P. van Emde-Boas. *Another NP-complete partition problem and the complexity of computing short vectors in a lattice*. Report. Department of Mathematics. University of Amsterdam. Department, Univ., 1981. URL: http://staff.science.uva.nl/~peter/vectors/mi8104c.html.

[Gal12] S. D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012. DOI: 10.1017/CBO9781139012843.

[Gau31] C. F. Gauss. "Untersuchungen uber die Eigenschaften der positiven ternaren quadratishen Former von Ludwig August Seeber". Em: *Gottingische gelehrte Anzeigen* (1831).

[GPV07] C. Gentry, C. Peikert e V. Vaikuntanathan. *Trapdoors for Hard Lattices and New Cryptographic Constructions*. Cryptology ePrint Archive, Report 2007/432. 2007. URL: https://eprint.iacr.org/2007/432.

[Gol] O. Goldreich. *A Short Tutorial of Zero-Knowledge*. URL: http://www.wisdom.weizmann.ac.il/~oded/zk-tut02.html.

[GMR89] S. Goldwasser, S. Micali e C. Rackoff. "The Knowledge Complexity of Interactive Proof Systems". Em: *SIAM Journal on Computing* 18.1 (1989), pp. 186–208. DOI: 10.1137/0218012.

[Hal+17] T. Hales et al. "A formal proof of the Kepler conjecture". Em: *Forum of Mathematics, Pi* 5 (2017), e2. DOI: 10.1017/fmp.2017.1.

[Hal15] B. C. Hall. "Root Systems". Em: *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*. Springer International Publishing, 2015, pp. 197–240. ISBN: 978-3-319-13467-3. DOI: 10.1007/978-3-319-13467-3_8.

[HW00] D. Han e Y. Wang. *Lattice Tiling and the Weyl-Heisenberg Frames*. Set. de 2000. DOI: 10.1007/PL00001683. URL: https://www.math.ust.hk/~yangwang/Reprints/wh.pdf.

[HMU13] J. E. Hopcroft, R. Motwani e J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. 3ª ed. Pearson, 2013. ISBN: 1292039051.

[Kep10] J. Kepler. *The Six-Cornered Snowflake*. Paul Dry Books, 2010. ISBN: 9781589882850.

[LLL82] A. K. Lenstra, H. W. Lenstra e L. Lovász. "Factoring polynomials with rational coefficients". Em: *Mathematische Annalen* 261.4 (1982), pp. 515–534. ISSN: 1432-1807. DOI: 10.1007/BF01457454.

[LLB12] C. Ling, L. Luzzi e J. Belfiore. "Lattice codes achieving strong secrecy over the mod-Λ Gaussian Channel". Em: *2012 IEEE International Symposium on Information Theory Proceedings*. Jul. de 2012, pp. 2306–2310. DOI: 10.1109/ISIT.2012.6283924.

[Lin+14] C. Ling, L. Luzzi, J.-C. Belfiore e D. Stehle. "Semantically Secure Lattice Codes for the Gaussian Wiretap Channel". Em: *IEEE Transactions on Information Theory* 60.10 (out. de 2014), pp. 6399–6416. ISSN: 1557-9654. DOI: 10.1109/tit.2014.2343226.

[LJO14] J. Lu, H. Jagadeesh e F. Oggier. "On wiretap codes, what they are, and what they (promise to) do for you". Em: (dez. de 2014). URL: https://www.researchgate.net/publication/271589135_On_wiretap_codes_what_they_are_and_what_they_promise_to_do_for_you.

[LPR12] V. Lyubashevsky, C. Peikert e O. Regev. *On Ideal Lattices and Learning with Errors Over Rings*. Cryptology ePrint Archive, Report 2012/230. https://eprint.iacr.org/2012/230. 2012.

[Mic07] D. Micciancio. "Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions". Em: *Comput. Complex.* 16.4 (dez. de 2007), pp. 365–411. ISSN: 1016-3328. DOI: 10.1007/s00037-007-0234-9.

[MG02] D. Micciancio e S. Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*. Springer US, 2002. ISBN: 978-1-4615-0897-7. DOI: 10.1007/978-1-4615-0897-7_1.

[MR09] D. Micciancio e O. Regev. "Lattice-based Cryptography". Em: *Post-Quantum Cryptography*. Springer Berlin Heidelberg, 2009, pp. 147–191. ISBN: 978-3-540-88702-7. DOI: 10.1007/978-3-540-88702-7_5.

[MR07] 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.

[NS01] P. Q. Nguyen e J. Stern. "The Two Faces of Lattices in Cryptology". Em: *Cryptography and Lattices*. Springer Berlin Heidelberg, 2001, pp. 146–180. ISBN: 978-3-540-44670-5. DOI: 10.1007/3-540-44670-2_12.

[OSB16] F. Oggier, P. Solé e J. Belfiore. "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis". Em: *IEEE Transactions on Information Theory* 62.10 (out. de 2016), pp. 5690–5708. ISSN: 1557-9654. DOI: 10.1109/TIT.2015.2494594.

[Pei16] C. Peikert. *A Decade of Lattice Cryptography*. Fev. de 2016. URL: https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf.

[Pei+13] 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.

[Reg05] 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.

[Reg09] O. Regev. "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography". Em: *J. ACM* 56.6 (2009). ISSN: 0004-5411. DOI: 10.1145/1568318.1568324.

[Riv90] R. L. Rivest. "Cryptography". Em: *Algorithms and Complexity*. Handbook of Theoretical Computer Science. Elsevier, 1990. Cap. 13, pp. 717–755. ISBN: 978-0-444-88071-0. DOI: 10.1016/B978-0-444-88071-0.50018-7.

[SV03] A. Sahai e S. Vadhan. "A Complete Problem for Statistical Zero Knowledge". Em: *J. ACM* 50.2 (mar. de 2003), pp. 196–249. ISSN: 0004-5411. DOI: 10.1145/636865.636868.

[Sha48] C. E. Shannon. "A mathematical theory of communication". Em: *The Bell System Technical Journal* 27.3 (jul. de 1948), pp. 379–423. ISSN: 0005-8580. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[Sho94] P. W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". Em: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Nov. de 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[Slo84] N. J. A. Sloane. "The Packing of Spheres". Em: *Scientific American* 250.1 (1984), pp. 116–125. ISSN: 00368733, 19467087. URL: http://www.jstor.org/stable/24969283.

[SS10] E. M. Stein e R. Shakarchi. *Complex Analysis*. Princeton Lectures in Analysis. Princeton University Press, 2010. Cap. 10. ISBN: 9781400831159.

[SL96] A. Storjohann e G. Labahn. “Asymptotically Fast Computation of Hermite Normal Forms of Integer Matrices”. Em: *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*. ISSAC ’96. ACM, 1996, pp. 259–266. ISBN: 0-89791-796-0. DOI: 10.1145/236869.237083.

[Wyn75] A. D. Wyner. “The wire-tap channel”. Em: *The Bell System Technical Journal* 54.8 (out. de 1975), pp. 1355–1387. ISSN: 0005-8580. DOI: 10.1002/j.1538-7305.1975.tb02040.x.

[Zam09] R. Zamir. “Lattices are Everywhere”. Em: *2009 Information Theory and Applications Workshop*. Fev. de 2009, pp. 392–421. DOI: 10.1109/ITA.2009.5044976. URL: https://www.eng.tau.ac.il/~zamir/papers/LatticesEverywhere.pdf.

[Zam+14] R. Zamir, B. Nazer, Y. Kochman e I. Bistritz. *Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation and Multiuser Information Theory*. Cambridge University Press, 2014. DOI: 10.1017/CBO9781139045520.