Reticulados e Aplicações em Criptografia

Fábio Meneghetti
Orientadora: Sueli I. R. Costa
IMECC – UNICAMP

Introdução

Neste trabalho, apresentamos uma análise do parâmetro de suavização de reticulados, e alguns resultados obtidos através de simulações computacionais. Além disso, comentamos algumas aplicações deste parâmetro à criptografia baseada em reticulados, importante subárea da chamada criptografia pós-quântica.

Definição (Reticulado)

Dado um conjunto $\beta = \{b_1, \ldots, b_n\}$ de vetores linearmente independentes em $\mathbb{R}^n$, o **reticulado gerado** por β é o conjunto de todas as combinações lineares inteiras de β:

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

- Trabalhamos aqui apenas com reticulados de posto completo. Exemplos: $\mathbb{Z}^2$, $\langle (1,0), (1/2, \sqrt{3}/2) \rangle_{\mathbb{Z}}$ (hexagonal).
- A **distância mínima** de Λ é $\lambda(\Lambda) = \min\{\|v\| : v \in \Lambda \setminus \{0\}\}$.
- A **densidade** de $\Lambda = \Lambda(\{b_1, \ldots, b_n\})$ é

$$\Delta(\Lambda) = \frac{\operatorname{Vol} B_n(\lambda/2)}{|\det[b_1 \ldots b_n]|}.$$

Definição (Reticulado Dual)

Dado um reticulado $\Lambda \subset \mathbb{R}^n$, definimos seu dual como

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

- Se B é matriz geradora de Λ, então $(B^{-1})^\top$ é matriz geradora de Λ^*.

Parâmetro de suavização

- A *função Gaussiana* de parâmetro $s > 0$ em $\mathbb{R}^n$ é dada por

$$\rho_s(x) := e^{-\pi \|x\|^2 / s^2}.$$

- A função Gaussiana definida acima não é distribuição de probabilidade, mas podemos transformá-la em uma distribuição de probabilidade D_s dividindo por $s^n = \int_{\mathbb{R}^n} \rho_s(x)\, dx$.

Definição

Dado um reticulado Λ e $\varepsilon > 0$, definimos o **parâmetro de suavização** $\eta_\varepsilon(\Lambda)$ como o menor $s > 0$ tal que

$$\sum_{v \in \Lambda^* \setminus \{0\}} \rho_{1/s}(v) \leq \epsilon.$$

- η_ε é invariante por transformações ortogonais e $\eta_\varepsilon(k\Lambda) = k\eta_\varepsilon(\Lambda)$.
- O que torna esta definição interessante é o seguinte teorema:

Teorema

Sejam Λ reticulado, $c \in \mathbb{R}^n$, $\varepsilon > 0$, $s \geq \eta_\varepsilon(\Lambda)$. Então

$$s^n \det(\Lambda^*) \cdot (1 - \varepsilon) < \sum_{x \in \Lambda} \rho_s(x + c) < s^n \det(\Lambda^*) \cdot (1 + \varepsilon).$$

- Se definirmos $\mathbb{R}^n/\Lambda := \{c + \Lambda \mid c \in \mathbb{R}^n\}$, então podemos induzir uma distribuição $P_s \colon \mathbb{R}^n/\Lambda \to \mathbb{R}$ dada por

$$P_s(c + \Lambda) := \frac{1}{s^n} \sum_{v \in \Lambda} \rho_s(v + c).$$

- O teorema nos diz que o parâmetro de suavização é o menor $s > 0$ que torna a distribuição P_s aproximadamente uniforme em $\mathbb{R}^n/\Lambda$. Formalmente, podemos dizer a *distância estatística* entre P_s e a distribuição uniforme em $\mathbb{R}^n/\Lambda$ é no máximo ε.

Simulações

- Para construir exemplos, escrevemos um programa na linguagem Julia para calcular o parâmetro de suavização. Seguem alguns exemplos.

Reticulado	$\eta_{0.25}$	$\eta_{0.5}$	η_1	η_{10}
$\mathbb{Z}^2$	0.94914	0.83442	0.70988	0.30151
Hexagonal	0.87128	0.77136	0.65947	0.28059
$\langle (1,0), (0,5) \rangle$	4.06978	3.33915	2.50002	0.67488

- Observamos que reticulados que são melhores em aspectos diferentes, como o hexagonal (melhor em densidade e kissing number) em geral têm parâmetros de suavização menores.
- Porém, é possível que para ε diferentes tenhamos diferentes reticulados "melhores". Considerando, por exemplo,

$$\beta_1 = \left\langle (1,0,0), (0,1,{}^1\!/_{10}), (0,0,20) \right\rangle,$$
$$\beta_2 = \left\langle (1,0,0), (0,{}^1\!/_{10},3), (0,0,25) \right\rangle,$$

obtemos o seguinte gráfico de η_ε por ε:

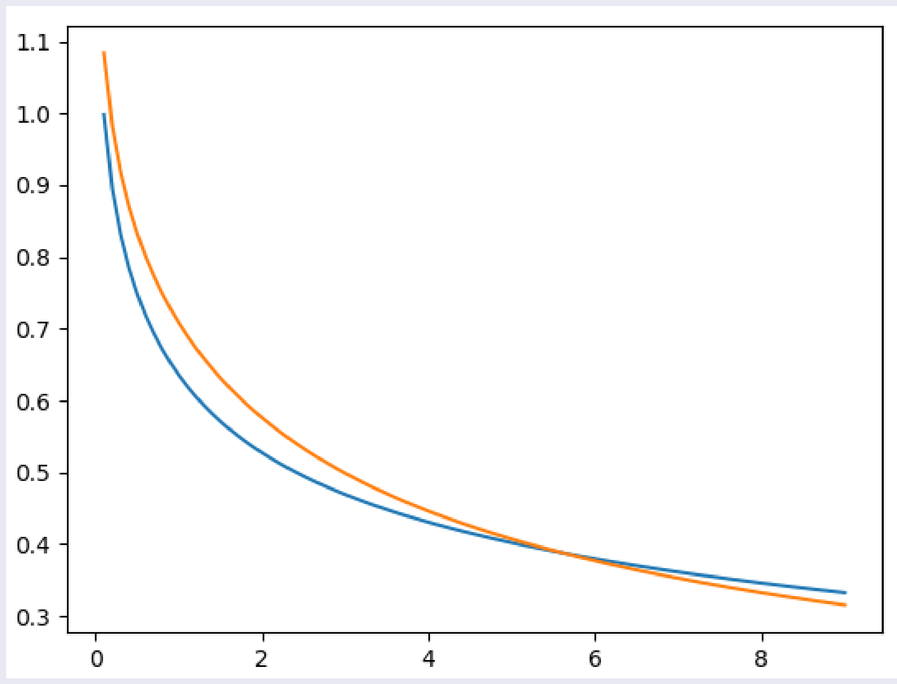

Figura: Azul: $\Lambda(\beta_1)$, Laranja: $\Lambda(\beta_2)$.

Criptografia

- O parâmetro de suavização tem diversas aplicações em criptografia. Ele é utilizado, por exemplo, na demonstração de dificuldade do problema LWE. Mas uma aplicação mais direta é o problema γ-GapSPP$_\varepsilon$:
- **γ-GapSPP$_\varepsilon$:** é o problema de promessa que consiste em decidir, dado um reticulado Λ, qual é o caso: se $\eta_\varepsilon(\Lambda) \leq 1$ ou se $\eta_\varepsilon(\Lambda) > \gamma$ (onde é prometido que um dos dois é o caso).
- O artigo [2] estuda a dificuldade deste problema e propõe dois protocolos criptográficos baseados nele.

Agradecimentos

Agradecemos ao CNPQ (313326/2017-7 e 131290/2018-5), à FAPESP (13/25977-7), e à pós-graduação do departamento de matemática do IMECC (UNICAMP).

Referências

C. Peikert. *A Decade of Lattice Cryptography*, 2016

C. Peikert et al. *On the Lattice Smoothing Parameter Problem*, 2013 IEEE Conference on Computational Complexity, 2013, DOI: 10.1109/CCC.2013.31

O. Regev. *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography*, J. ACM, 2009, DOI: 10.1145/1568318.1568324