# Construção de Reticulados via Corpos de Funções


## Franciele do Carmo Silva & Beatriz Motta (Orientadora)

Universidade Federal de Juiz de Fora

francieledocarmo@hotmail.com



**Resumo**

O objetivo principal deste trabalho é apresentar construções de reticulados utilizando corpos de funções elípticas e Hermitiano. Tais reticulados são gerados por seus vetores minimais, isto é, são reticulados bem arredondados. Estabelecemos correspondências entre o conjunto de lugares racionais e o conjunto de pontos do reticulado, obtendo estimativas do número total de vetores minimais e a densidade de empacotamento dos mesmos. Seguimos [3] e [7].


## 1.Reticulados: Noções Básicas

**Definições:** Seja $\{v_1, \ldots, v_m\} \subset \mathbb{R}^n$ um conjunto de vetores LI tal que $m \leq n$. O reticulado com relação a este conjunto é dado por:

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_i v_i : \lambda_i \in \mathbb{Z} \text{ para todo } i = 1, \ldots, m \right\}$$

Dado um reticulado $\Lambda$, definimos ainda:

- **Matriz geradora:** matriz cujas linhas são vetores de uma base de $\Lambda$.
- **Matriz de Gram:** matriz da forma $G = MM^T$, em que $M$ é uma matriz geradora de $\Lambda$.
- **Determinante** de $\Lambda$: o det de uma de suas matrizes de Gram.
- **Volume** de $\Lambda$: corresponde a $\sqrt{\det(\Lambda)}$.

## 2.Reticulados via Corpos de Funções

Seja $F/\mathbb{F}_q$ um corpo de funções cujo conjunto de lugares racionais é $\mathcal{P} := \{P_0, P_1, \ldots, P_{n-1}\} \subseteq \mathbb{P}_F$. A valorização associada ao lugar $P_i$ é denotada por $v_i$ $(i = 0, \ldots, n-1)$.

**Definições:** Consideraremos:

$$O^*_{\mathcal{P}} := \{f \in F/\mathbb{F}_q : f \neq 0 \text{ e } supp(f) \subseteq \mathcal{P}\}$$

Definimos o homomorfismo $\phi_{\mathcal{P}}$ e fazemos $L_{\mathcal{P}} := \mathrm{Im}(\phi_{\mathcal{P}})$.

$$\begin{aligned} \phi_{\mathcal{P}} : O^*_{\mathcal{P}} &\to \mathbb{Z}^n \\ f &\mapsto (v_0(f), v_1(f), \ldots, v_{n-1}(f)) \end{aligned}$$

**Proposição 2.1:** $L_{\mathcal{P}}$ é um sub-reticulado do reticulado $\mathcal{A}_{n-1}$:

$$\mathcal{A}_{n-1} := \left\{ x = (x_0, \ldots, x_{n-1}) \in \mathbb{Z}^n : \sum_{i=0}^{n-1} x_i = 0 \right\}$$

Além disso: $Div(\mathcal{P}) \cong \mathbb{Z}^n$, $Div^0(\mathcal{P}) \cong \mathcal{A}_{n-1}$ e $L_{\mathcal{P}} \cong Princ(\mathcal{P})$

**Teorema 2.1:** A distância mínima e o volume de $L_{\mathcal{P}}$ satisfazem:

$$d(L_{\mathcal{P}}) \geq min\left\{ \sqrt{2 \deg f} : f \in O^*_{\mathcal{P}} \setminus \mathbb{F}_q \right\}$$

$$vol(L_{\mathcal{P}}) \leq \sqrt{n}(\#Cl^0(F)) \leq \sqrt{n}\left(1 + q + \frac{n-q-1}{g}\right)^g$$

**Definições:** Seja $S(\Lambda) := \{x \in \Lambda : \|x\| = d(\Lambda)\}$ o conjunto de vetores minimais de $\Lambda$. Dizemos que $\Lambda \subseteq \mathbb{R}^m$ é **gerado por seus vetores minimais** se $\Lambda = span_{\mathbb{Z}}(S(\Lambda))$. Dizemos que $\Lambda$ de posto $m$ é **bem arredondado** se contém $m$ vetores minimais LI, i.e., se $span_{\mathbb{R}}(S(\Lambda)) = \mathbb{R}^m$.

## 3. Reticulados via Corpos de Funções Elípticas

Seja $F/\mathbb{F}_q$ um corpo funções elípticas, isto é, um corpo de funções de gênero 1 no qual existe $D \in Div(F)$ com $\deg D = 1$.

**Teorema 3.1:** A distância mínima de $L_{\mathcal{P}}$ é dada por:

$$d(L_{\mathcal{P}}) = \begin{cases} 2, \text{ se } n \geq 4 \\ \sqrt{6}, \text{ se } n = 3 \end{cases}$$

- Se $n \geq 4$, os vetores minimais são da forma $P + Q + R - S$, em que $P, Q, R, S \in \mathcal{P}$ são distintos e $\mathbf{P + Q = R + S}$.
- Se $n = 3$, são da forma $\pm(P + Q - 2Q_\infty)$, $\pm(P - 2Q + Q_\infty)$ e $\pm(-2P + Q + Q_\infty)$, em que $\mathcal{P} = \{P, Q, Q_\infty\}$.

**Teorema 3.2:** Suponhamos que $E$ possua, no mínimo, $5$ pontos. Então, o reticulado $L_{\mathcal{P}}$ é gerado por seus vetores minimais.

**Teorema 3.3:** Sejam $n \geq 4$ e $\epsilon$ o número de $2$-pontos de torsão de $E$. O número de vetores minimais de $L_{\mathcal{P}}$ é:

$$\frac{n}{\epsilon} \cdot \frac{(n-\epsilon)(n-\epsilon-2)}{4} + \left(n - \frac{n}{\epsilon}\right) \cdot \frac{n(n-2)}{4}$$

## 4. Reticulados via Corpo de Funções Hermitiano

Corpo de funções Hermitiano $H := \mathbb{F}_{q^2}(x, y)/\mathbb{F}_{q^2}$, onde $y^q + y = x^{q+1}$.

**Teorema 4.1:** A distância mínima de $L_{\mathcal{P}}$ é igual a $d(L_{\mathcal{P}}) = \sqrt{2q}$.

**Teorema 4.2:** Sejam $f_1$ e $f_2$ retas distintas. O divisor $(f_1/f_2)$ (ou $(f_2/f_1)$) é um vetor minimal de $L_{\mathcal{P}} \iff$ vale uma das seguintes condições:

- $f_1$ e $f_2$ são da forma $x - \alpha$;
- uma das retas $f_1$ ou $f_2$ é da forma $x - \alpha$ e a outra é não tangente (da forma $y - bx + c$) e as tem exatamente um ponto de interseção;
- $f_1$ e $f_2$ são não tangentes (da forma $y - bx + c$) com um ponto de interseção.

**Teorema 4.3:** O reticulado $L_{\mathcal{P}}$ é gerado por seus vetores minimais.

**Teorema 4.4:** $L_{\mathcal{P}}$ contém, no mínimo, $q^7 - q^5 + q^4 - q^2$ vetores minimais.

**Teorema 4.5:** O volume do reticulado $L_{\mathcal{P}}$ é igual a $\sqrt{q^3 + 1} \cdot (q+1)^{q^2-q}$.

## Referências


[1] BEARDON, A. F. *The geometry of discrete groups.* New York: Springer Verlag, 2012.

[2] ALVES, C. *Reticulados e Códigos.* Tese (Doutorado) - Unicamp, Campinas, 2008.

[3] BÖTCHER, A.; FUKSHANSKY, L.; GARCIA, S.; MAHARAJ, H. *Lattices from Hermitian Function Fields.* Journal of Algebra, v. 447, p. 560-579, Elsevier, 2016.

[4] CAMPELLO, A. *Reticulados, Projeções e Aplicações à Teoria da Informação.* Tese (Doutorado) - Unicamp, Campinas, 2014.

[5] CASTELLANOS, A. S.; TIZZIOTTI, G. C. *On the Automorphism Group of Generalized Hermitian Codes.* IEEE Transactions on Information Theory v. 59, p. 6642-6645, IEEE, 2013.

[6] CONWAY, J.H.; SLOANE, N. J.A. *Sphere packings, lattices and groups.* Springer Science & Business Media, v. 290, 2013.

[7] FUKSHANSKY, L.; MAHARAJ, H. *Lattices from Elliptic Curves over Finite Fields.* Finite Fields and Their Applications, v. 28, p. 67-78, Elsevier, 2014.

[8] HISS, G. *Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups.* Indagationes Mathematicae v. 15, p. 223-243, Elsevier, 2004.

[9] JORGE, G. C. *Reticulados q-ários e algébricos.* Tese (Doutorado) - Unicamp, Campinas, 2012.

[10] MARTINET, J. *Perfect Lattices in Euclidean Spaces.* Springer Science & Business Media, v. 327, 2013.

[11] ROGERS, C.A. *Packing and Covering.* Cambridge University Press, 1964.

[12] SILVERMAN, J. H. *The Arithmetic of Elliptic Curves.* Springer Science & Business Media, v. 106, 2009.

[13] STEWART, I.; TALL, D. *Algebraic Number Theory and Fermat's Last Theorem.* Massachussets: A K Peters, 2002.


## Agradecimentos


À UFJF e ao Departamento de Matemática pelas diversas oportunidades ofertadas.

Ao CNPq pelo apoio financeiro no PICME.

À CAPES pelo fundamental apoio no mestrado (Código de Financiamento 001).