Trabalho apresentado no XL CNMAC, Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS).

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Construção de Reticulados via Corpos de Funções Elípticas

Franciele do Carmo Silva[1]
IMECC, Unicamp, Campinas, SP
Beatriz Casulari da Motta Ribeiro[2]
Depto de Matemática, ICE, UFJF, Juiz de Fora, MG

1 Introdução

Este trabalho tem como objetivo apresentar a construção de reticulados utilizando corpos de funções elípticas. Tais reticulados são gerados por seus vetores minimais e, como consequência, são reticulados bem arredondados. Para a construção, estabelecemos correspondências entre o conjunto de lugares racionais e o conjunto de pontos do reticulado. Ao final, apresentamos estimativas do número total de vetores minimais. Seguimos [1] e [2].

2 Reticulados via Corpos de Funções Elípticas

Um reticulado $\Lambda \subseteq \mathbb{R}^n$ é um subgrupo aditivo discreto de $\mathbb{R}^n$. Equivalentemente, $\Lambda \subseteq \mathbb{R}^n$ é um reticulado se, e somente se, existe um conjunto de vetores linearmente independentes $\{\mathbf{v_1}, \ldots, \mathbf{v_m}\} \subset \mathbb{R}^n$, com $m \leq n$, tal que:

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

O conjunto $\{\mathbf{v_1}, \ldots, \mathbf{v_m}\} \subset \mathbb{R}^n$ é dito uma base de Λ e a matriz cujas linhas são os vetores $\mathbf{v_1}, \ldots, \mathbf{v_m}$ é uma matriz geradora de Λ. Os vetores em Λ que minimizam o valor de $d(\Lambda) := min\{||y|| : y \in \Lambda \text{ e } y \neq 0\}$ são chamados vetores minimais e dizemos que geram o reticulado se ele é o subespaço coberto pelo conjunto de seus vetores minimais

Para a construção, 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 $\deg D = 1$. De modo equivalente, um corpo de funções elípticas é um corpo de funções da forma $K(x; y) =: F$, em que x e y são as funções coordenadas associadas à chamada *curva elíptica*. Nesse sentido, lembramos que uma curva elíptica é um par $(E, \mathbf{O})$, em que E é uma curva não singular de gênero 1 e $\mathbf{O} \in E$.

Exemplo 2.1. Consideremos a curva $E : y^2 = x^3 - 3x + 3$ sobre $\mathbb{F}_9^2$ sendo x transcendente sobre $\mathbb{F}_9$. Tal curva é não singular, visto que suas derivadas parciais são nulas apenas nos pontos $(1, 0)$ e $(-1, 0)$, os quais não pertencem à curva. Ainda, o gênero associado a essa curva é 1 (veja [3]).

Assim, tomando o ponto $\mathbf{O}$ como sendo $(0 : 1 : 0)$ na homogeneização da equação, temos que $(E, \mathbf{O})$ é uma curva elíptica. O corpo de funções associado a $(E, \mathbf{O})$ corresponde a:

$$\mathbb{F}_9[x, y] = \frac{\mathbb{F}_9[X, Y]}{\langle y^2 - x^3 + 3x - 3 \rangle} = \left\{ \frac{g(x, y)}{h(x, y)} : \ g, h \in \mathbb{F}_9[X, Y] \ e \ y^2 - x^3 + 3x - 3 \nmid h \right\}.$$

[1] francieledocarmo@hotmail.com
[2] beatriz@ice.ufjf.br

Sabe-se que uma das motivações para o estudo de curvas elípticas deve-se ao fato de que os pontos de uma curva elíptica possuem a estrutura de um grupo abeliano. Estendemos essa estrutura de modo natural ao grupo de lugares racionais do corpo de funções elípticas [3].

Denotemos $\mathcal{P} := \{P_0, P_1, \ldots, P_{n-1}\} \subseteq \mathbb{P}_F$ os lugares racionais de $F/\mathbb{F}_q$ e υ_i a valorização associada ao lugar P_i para cada i. Cada lugar P de F corresponde um único ponto $\mathbf{P}$ sobre a curva elíptica em questão. Consideremos $\mathcal{O}^*_{\mathcal{P}} := \{f \in F/\mathbb{F}_q : \ f \neq 0 \text{ e } supp(f) \subseteq \mathcal{P}\}$.

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

$$\begin{array}{rcl} \phi_{\mathcal{P}} : \mathcal{O}^*_{\mathcal{P}} & \to & \mathbb{Z}^n \\ f & \mapsto & (\upsilon_0(f), \upsilon_1(f), \ldots, \upsilon_{n-1}(f)) \end{array}$$

Mostra-se que $L_{\mathcal{P}}$ é um sub-reticulado do reticulado raiz $\mathcal{A}_{n-1}$, isomorfo ao grupo de divisores principais das funções pertencentes a $\mathcal{O}^*_{\mathcal{P}}$ [1].

Teorema 2.1. *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 $\mathbf{P} + \mathbf{Q} = \mathbf{R} + \mathbf{S}$.*
- *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 2.2. *Suponhamos que a curva elíptica possua, no mínimo, 5 pontos. Então, o reticulado $L_{\mathcal{P}}$ é gerado por seus vetores minimais.*

Teorema 2.3. *Sejam $n \geq 4$ e ϵ o número de 2-pontos de torsão de E. O número de vetores minimais de $L_{\mathcal{P}}$ é:*

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

Agradecimentos

Ao Conselho Nacional de Pesquisa e Desencolvimento (CNPq) pelo apoio financeiro no Programa de Iniciação Científica e Mestrado (PICME). À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior-Brasil (CAPES) pelo apoio no mestrado (Código de Financiamento 001).

Referências

[1] Fukshansky, L.; Maharaj, H. Lattices from Elliptic Curves over Finite Fields, *Finite Fields and Their Applications*, 28:67-78, 2014. DOI:10.1016/j.ffa.2014.01.007.

[2] Silverman, J. H. The Arithmetic of Elliptic Curves. In *Graduate Texts in Mathematics*. Springer, 2009. ISSN: 0072-5285.

[3] Stichtenoth, H. Algebraic Function Fields and Codes. In *Graduate Texts in Mathematics*. Springer, 2009. ISSN 0072-5285.