

Construção do reticulado hexagonal via método de Krüskemper

Agnaldo José Ferrari ¹

Departamento de Matemática, FC - Unesp, Bauru - SP

Antonio Aparecido de Andrade ²

Departamento de Matemática, IBILCE - Unesp, São José do Rio Preto - SP ³

Resumo. O objetivo deste trabalho é a construção do reticulado hexagonal via ideais reticulados em alguma algebra $\mathbb{Z}[X]/(f(X))$, em que $f(X)$ é um polinômio mônico e irredutível. A construção é baseada no Método de Krüskemper [2], [4]. Os reticulados construídos, via este método, possuem diversidade máxima, representando assim constelações eficientes para transmissão sobre os canais com desvanecimento do tipo Rayleigh e através da distância produto mínima, um relevante parâmetro de performance, obtemos constelações mais eficientes do que as construídas anteriormente.

1 Resultados

Seja M um $\mathbb{Z}$ -módulo livre finitamente gerado de posto n e $b : M \times M \rightarrow \mathbb{Z}$ uma forma bilinear simétrica. Seja $f(X) \in \mathbb{Z}[X]$ um polinômio mônico irredutível de grau n e θ uma raiz de f . Então $\mathbb{Z}[X]/(f(X)) = \mathbb{Z}[\theta]$ com base $\{1, \theta, \dots, \theta^{n-1}\}$. Se $\mathcal{A}$ é um ideal de $\mathbb{Z}[\theta]$, definimos $\mathcal{A}^\# = \{c \in \mathbb{Q}(\theta) \mid \text{Tr}(c\mathcal{A}) \subseteq \mathbb{Z}\}$. Seja $B \in \mathcal{M}_n(\mathbb{Z})$ uma matriz simétrica não singular e $A \in \mathcal{M}_n(\mathbb{Z})$ tal que seu polinômio característico χ_A é irredutível e $B^{-1}AB = A^T$, então B é a matriz de um ideal reticulado [2]. Seja (M, b) um reticulado integral, então existe um inteiro algébrico θ , um ideal $\mathcal{A}$ de $\mathbb{Z}[\theta]$ e $\alpha \in (\mathcal{A}^\#)^\# \subseteq \mathbb{Q}(\theta)$ tal que b é isomorfo a $\varphi : \mathcal{A} \times \mathcal{A} \rightarrow \mathbb{Z}$ dado por $\varphi(x, y) = \text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha xy)$. Além disso, θ pode ser considerado totalmente real [4].

1.1 Reticulado hexagonal

Uma matriz geradora para o reticulado A_2 (hexagonal) é dada por $M = \{(-1, 1, 0), (0, -1, 1)\}$, em que a Matriz de Gram associada é $B = \{(2, -1), (-1, 2)\}$. Consideramos o Corpo de Números $\mathbb{K}$ dado por $X^2 - 3$. A matriz $A = \{(-1, 1), (2, 1)\}$ satisfaz $\mathcal{X}_A(X) = X^2 - 3$, onde $\mathcal{X}_A$ é irredutível sobre $\mathbb{Q}$, e $B^{-1}AB = A^T$. Agora, computamos as matrizes V e G do seguinte modo: $v_\theta = \{v_1, v_2\}$, onde $v_j = (-1)^{i+j} \Delta_{ij}(A - \theta I_n)$, seja $i = 1$, temos $v_\theta = \{(1 - \theta, -2)\}$. Seja $V = \{(v_{11}, v_{12}), (v_{21}, v_{22})\}$ e $\{(1, \theta)\}V = \{(v_1, v_2)\}$, então $V = \{(1, -2), (-1, 0)\}$ e consequentemente $(V^T)^{-1} = \{(\frac{1}{2}, 0), (0, \frac{1}{6})\}$. Agora, temos $G = (\text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1}\theta^{j-1}))_{i,j=1}^2 = \{(2, 0), (0, 6)\}$, uma vez que θ é uma raiz de $\mathcal{X}_A$, o conjunto das raízes de $\mathcal{X}_A$ é $\{-\sqrt{3}, \sqrt{3}\}$, isto significa que os homomorfismos reais de θ são $\sigma_1(\theta) = -\sqrt{3}$ e $\sigma_2(\theta) = \sqrt{3}$. Temos também que $d_{\mathbb{K}} = \det(G) =$

¹ferrari@fc.unesp.br

²andrade@ibilce.unesp.br

³Agradecimentos a Fapesp - Processo 2013/25977-7

12. Seja $v'_\theta = \{(v'_1, v'_2)\}$, em que $v'_1 = \sum_{i=1}^2 m_{i1} \theta^{i-1}$, $v'_2 = \sum_{i=1}^2 m_{i2} \theta^{i-1}$ e

$$(m_{ij})_{i,j=1}^2 = G^{-1}(V^T)^{-1} = \left\{ \left(0, -\frac{1}{4}\right), \left(-\frac{1}{6}, -\frac{1}{12}\right) \right\}.$$

Portanto, $v'_\theta = \{(v'_1, v'_2)\} = \{(-\frac{1}{6}\theta, -\frac{1}{4} - \frac{1}{12}\theta)\}$. O elemento α é dado por $\alpha v_\theta = Bv'_\theta$, i.e., $\alpha\{(1 - \theta, -2)\} = \{(2, -1), (-1, 2)\}\{(-\frac{1}{6}\theta, -\frac{1}{4} - \frac{1}{12}\theta)\}$. Usando, por exemplo, a última linha, computamos $\alpha = \frac{1}{4}$. Então, a matriz geradora do reticulado é dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) \end{pmatrix} = \begin{pmatrix} \frac{1+\sqrt{3}}{2} & \frac{1-\sqrt{3}}{2} \\ -1 & -1 \end{pmatrix}.$$

Assim, temos $\det(b_\alpha) = \det(B) = 3$, $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$ and $h(\mathbb{K}) = 1$. Como a norma mínima de A_2 é $\mu = 2$, segue que o reticulado construído sobre o anel $\mathcal{O}_{\mathbb{K}}$ terá distância produto mínima relativa dada por

$$\sqrt{d_{p,rel}(A_2)} = \left(\frac{1}{(\sqrt{\mu})^2} \sqrt{\frac{\det(b_\alpha)}{d_{\mathbb{K}}}} \frac{\min\{\mathcal{A}\}}{[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]} \right)^{1/2} = \left(\frac{1}{(\sqrt{2})^2} \sqrt{\frac{3}{12}} \right)^{1/2} = 0.5$$

Referências

- [1] Boutros, J., Viterbo, E., Rastello, C., Belfiore, J. C., *Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels. IEEE Transactions on Information Theory*, v. 42, n. 2, pp. 502-518, March 1996.
- [2] Conner, E. P., *A survey of trace forms of algebraic number fields*. 1984.
- [3] Conway, J. H., Sloane, N. J. A. *Sphere Packings, Lattices and Groups*, 3rd edition, Springer-Verlag, New York, 1999.
- [4] Krüskemper, M., *Algebraic construction of bilinear forms over $\mathbb{Z}$* . *Pub. Math. de Besancon, Théorie des nombres*, 1996/97 - 1997/98.
- [5] Oggier, F., *Algebraic Methods for Channel Coding. Tese de doutorado*, École Polytechnique fédérale de Lausanne, 2005.
- [6] Oggier, F., Fluckiger, E. B., *Best rotated cubic lattice constellations for Rayleigh fading channel. Proc. Int. Symposium of Information Theory - ISIT 2003*, Yokohama, Japan, July 2003.
- [7] Samuel, P. *Algebraic Theory of Numbers*, Hermann, Paris, 1967.