Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Uma nota sobre o raio de empacotamento de reticulados algébricos aplicados à Teoria da Informação

Agnaldo José Ferrari[1]

Departamento de Matemática, UNESP, Bauru, SP

Antonio Aparecido de Andrade[2]

Departamento de Matemática, UNESP, São José do Rio Preto, SP

Resumo. Neste trabalho apresentamos uma forma traço associada ao subcorpo maximal real de $\mathbb{Q}(\zeta_m)$. A forma traço é de suma importância para a obtenção de reticulados com alta densidade de empacotamento esférico, uma vez que a minimização desta forma, a qual é uma forma quadrática, fornece o raio de empacotamento do reticulado e isto tem um aplicação direta na teoria da informação. Com relação à corpos ciclotômicos e seus subcorpos, a única forma traço conhecida refere-se à extensão $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ [3].

Palavras-chave. Forma traço, Reticulados, Corpos ciclotômicos, Raio de empacotamento, Densidade de empacotamento.

1 Introdução

A teoria dos reticulados vem sendo bastante utilizada na área das telecomunicações, mais especificamente em teoria da informação, uma vez que constelações de sinais tendo a estrutura de reticulados tem sido estudadas como um meio eficiente de transmissão que minimizam a probabilidade de erros em canais de comunicação. Usualmente, o problema de encontrar boas constelações de sinais para o canal do tipo AWGN - Additive White Gaussian Noise está associado à busca por reticulados com alta densidade de empacotamento [2]. Os reticulados obtidos via teoria algébrica de números vem apresentando um impacto positivo na construção de códigos reticulados [1, 3].

2 Exposição do problema

Se $\mathbb{K}$ é um corpo de números de grau n, então existem n $\mathbb{Q}$-homomorfismos distintos $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ do corpo $\mathbb{K}$ no corpo $\mathbb{C}$ (complexos). O homomorfismo $\sigma : \mathbb{K} \to \mathbb{R}^n$ definido por $\sigma(x) = (\sigma_1(x), \cdots, \sigma_n(x))$ é chamado *homomorfismo de Minkowski*, onde n é o grau da extensão $\mathbb{Q} \subseteq \mathbb{K}$, e se $\mathcal{A} \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre, então $\sigma(\mathcal{A})$ é um

[1]ferrari@fc.unesp.br / Processos FAPESP n^{o}s. 2013/25977-7 e 2014/14449-2.
[2]andrade@ibilce.unesp.br / Processo FAPESP n^o. 2013/25977-7.

reticulado. Neste trabalho, $\mathbb{K} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ ($m = 5$ ou $m \geq 7$) é o subcorpo maximal real do corpo ciclotômico $\mathbb{Q}(\zeta_m)$, em que ζ_m é uma raiz primitiva m-ésima da unidade e $n = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$, com φ a função de Euler. Neste caso, se $\mathcal{O}_\mathbb{K}$ é o anel dos inteiros algébricos do corpo $\mathbb{K}$, então $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$. Nosso objetivo é apresentar uma expressão fechada para a forma traço $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \sum_{j=1}^{\frac{n}{2}} \sigma_j(x\overline{x})$, em que $x \in \mathcal{A} \subseteq \mathcal{O}_\mathbb{K}$, $\mathcal{A}$ é um ideal de $\mathcal{O}_\mathbb{K}$ e $\overline{x}$ é o conjugado complexo de x. Dados $m = p_1^{a_1} \cdots p_s^{a_s}$, a decomposição de m em fatores primos, $P = p_1 \cdots p_s$, $x = a_0 + \sum_{j=1}^{\frac{n}{2}-1} a_j \alpha_j \in \mathcal{A} \subseteq \mathcal{O}_\mathbb{K}$, em que $\alpha_j = \zeta_m^j + \zeta_m^{-j}$, segue que $\overline{x} = x$. Para $j = 0, 1, \cdots, \frac{n}{2} - 1$, se definirmos $A_j = a_1 a_{j+1} + a_2 a_{j+2} + \cdots + a_{\frac{n}{2}-1-j} a_{\frac{n}{2}-1}$ e $B_j = \sum_{k \in I} a_k a_{j-k}$, em que $I = \{k \in \mathbb{N};\ 1 \leq k < j - k \leq \frac{n}{2} - 1\}$, temos que

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) &= \tfrac{n}{2} a_0^2 + n \sum_{j=1}^{\frac{n}{2}-1} a_j^2 + \tfrac{2m}{P} a_0 \mu(P) \sum_{k=1}^{\frac{\varphi(P)}{2}-1} a_{\frac{mk}{P}} . \varphi((k,P)) . \mu((k,P)) \\ &\quad + \tfrac{2m}{P} \mu(P) \sum_{k=1}^{\frac{\varphi(P)}{2}-1} A_{\frac{mk}{P}} . \varphi((k,P)) . \mu((k,P)) \\ &\quad + \tfrac{2m}{P} \mu(P) \sum_{k \in J} B_{\frac{mk}{P}} . \varphi((k,P)) . \mu((k,P)) \\ &\quad + \tfrac{m}{P} \mu(P) \sum_{k \in L} a^2_{\frac{mk}{2P}} . \varphi((k,P)) . \mu((k,P)), \end{aligned}$$

em que $(k, P) = mdc(k, P)$, $J = \{k \in \mathbb{N};\ \text{máx}\{1, \frac{3P}{m}\} \leq k \leq \varphi(P) - 1\}$, $L = \{k \in \mathbb{N};\ 1 \leq k \leq \varphi(P)$ e $\frac{mk}{2P} \in \mathbb{Z}\}$ e μ é a função de Möbius. Como $\mathbb{K}$ é um corpo totalmente real, dado $x \in \mathcal{A} \subseteq \mathcal{O}_\mathbb{K}$ temos que $||\sigma(x)||^2 = Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$ [2] e, consequentemente, o raio de empacotamento do reticulado $\sigma(\mathcal{A})$ é dado por $\rho(\sigma(\mathcal{A})) = \frac{1}{2}\sqrt{min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}), x \in \mathcal{A}, x \neq 0\}}$. Associado a isto, a densidade de empacotamento do reticulado depende da minimização da forma traço, uma vez que a densidade de centro é dada por $\delta(\sigma(\mathcal{A})) = \frac{1}{2^n \sqrt{|d_\mathbb{K}|}} \frac{t^{n/2}}{|N(\mathcal{A})|}$, em que $d_\mathbb{K}$ é o discriminante do corpo $\mathbb{K}$, $N(\mathcal{A})$ é a norma do ideal $\mathcal{A}$ e $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}), x \in \mathcal{A}, x \neq 0\}$. Assim, dispomos de uma importante ferramenta para a construção de reticulados com altas densidades de empacotamento representando assim constelações de sinais que são eficientes para o canal do tipo AWGN - Additive White Gaussian Noise. A pesquisa referente ao tema está em andamento e o resultado obtido é parcial, uma vez que pretendemos usar o resultado para construir reticulados densos, além disso pretendemos também generalizar o resultado para outros subcorpos de corpos ciclotômicos.

Referências

[1] J. Boutros, E. Viterbo, C. Rastello and J. C. Belfiore, Good lattice constellations for both Rayleigh fading and Gaussian channels, IEEE Trans Inform Theory, Vol 42(2), 502-517, (1996).

[2] J. H. Conway and N. J. A. Sloane, Sphere Packings Lattices and Groups, Springer-Verlag, (1998).

[3] T. P. N. Neto, T. M. Rodrigues, J. C. Interlando and J. O. D. Lopes, A note on the Integral Trace Form in Cyclotomic Fields, Journal of Algebra and Its Applications, Vol 14, N.4, (2015).

