Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 10, n. 1, 2023.

Trabalho apresentado no XLII CNMAC, Universidade Federal de Mato Grosso do Sul - Bonito - MS, 2023

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Reticulados bem arredondados como imagens de anéis de inteiros através de mergulhos torcidos

Robson Ricardo de Araujo[1]
IFSP, Catanduva, SP

Reticulados são subgrupos aditivos discretos no $\mathbb{R}^n$, os quais têm sido amplamente requisitados pelas teorias de códigos e criptografia. Recentemente tem-se ampliado a pesquisa sobre reticulados bem arredondados, que são os reticulados de posto máximo em $\mathbb{R}^n$ que possuem um conjunto com n vetores linearmente independentes de normas coincidentes à norma mínima do reticulado. Tais estruturas geométricas têm sido propostas para transmissão de sinais em canais *SISO do tipo Rayleigh com desvanecimento* e em canais *MIMO wiretap* [1, 2].

Uma maneira significativa de obter reticulados é via mergulhos algébricos em $\mathbb{R}^n$ de $\mathbb{Z}$-módulos (em particular, de ideais) de anéis de inteiros de corpos de números. Reticulados obtidos dessa forma podem ser chamados de **reticulados algébricos**. Os mergulhos mais usados são o canônico, também chamado de mergulho de Minkowski, e os mergulhos torcidos. Estes últimos são variações do mergulho canônico causadas por um elemento totalmente positivo do corpo. Precisamente, sejam $\mathbb{K}$ um corpo de números de grau n, $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros e M um $\mathbb{Z}$-módulo livre de posto completo em $\mathcal{O}_{\mathbb{K}}$. Considere $\sigma_1, \ldots, \sigma_n$ os n monomorfismos existentes de $\mathbb{K}$ em $\mathbb{C}$, enumerados de modo que σ_i é totalmente real se $i \in \{1, 2, \ldots, r_1\}$, σ_i é totalmente complexo se $i \in \{r_1+1, \ldots, n\}$ e $\sigma_{i+r_2} = \overline{\sigma_i}$ se $i \in \{r_1+1, \ldots, r_2\}$, onde $r_2 = (n-r_1)/2$. O **mergulho canônico** associado a $\mathbb{K}$ é o monomorfismo $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ definido, para todo $x \in \mathbb{K}$, por

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \mathfrak{Re}(\sigma_{r_1+1}(x)), \mathfrak{Im}(\sigma_{r_1+1}(x)), \ldots, \mathfrak{Re}(\sigma_{r_2}(x)), \mathfrak{Im}(\sigma_{r_2}(x))) \,. \tag{1}$$

Por sua vez, seja $\alpha \in \mathbb{K}$ tal que $\sigma_i(\alpha) > 0$ para todo $i \in \{1, \ldots, n\}$, ao qual chamamos elemento totalmente positivo em $\mathbb{K}$. Fazendo o produto escalar da expressão de $\sigma(x)$ por

$$\left(\sqrt{\sigma_1(\alpha)}, \ldots, \sqrt{\sigma_{r_1}(\alpha)}, \sqrt{2\sigma_{r_1+1}(\alpha)}, \sqrt{2\sigma_{r_1+1}(\alpha)}, \ldots \sqrt{2\sigma_{r_2}(\alpha)}, \sqrt{2\sigma_{r_2}(\alpha)}\right) \tag{2}$$

obtemos a lei de formação do $\boldsymbol{\alpha}$**-mergulho torcido** (ou somente mergulho torcido) $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$. O fato importante que vincula esses mergulhos algébricos com a teoria de reticulados é que $\sigma(M)$ e $\sigma_\alpha(M)$ são reticulados de posto completo em $\mathbb{R}^n$ (ou seja, têm $\mathbb{Z}$-base com n vetores de $\mathbb{R}^n$).

Em [3] os autores analisam determinadas situações em que reticulados algébricos obtidos pelo mergulho canônico são bem arredondados. Em particular, nesse artigo é provado que há uma condição necessária e suficiente para que a imagem do anel de inteiros $\mathcal{O}_{\mathbb{K}}$ através do mergulho canônico seja um reticulado bem arrendondado. Tal condição consiste em $\mathbb{K}$ ser um corpo ciclotômico. Desde então, construir reticulados algébricos bem arredondados tem dado campo a diversas pesquisas científicas. Por exemplo, em [4] apresenta-se uma família de $\mathbb{Z}$-módulos de anéis de inteiros de corpos de números abelianos de grau primo ímpar p que gera infinitas classes de reticulados bem arredondados através do mergulho canônico. Além disso, é possível encontrar na literatura da última década diversos artigos que têm se debruçado a construir ou estudar reticulados bem arredondados bidimensionais via o mergulho canônico ou via mergulhos torcidos (em corpos quadráticos).

[1] robson.ricardo@ifsp.edu.br

© 2023 SBMAC

Como destacado acima, foi provado em [3] que $\sigma(\mathcal{O}_\mathbb{K})$ é um reticulado bem arredondado somente quando $\mathbb{K}$ é um corpo ciclotômico. No entanto, há pouco estudo publicado sobre o que ocorre com a imagem do anel de inteiros via *mergulhos torcidos*. Somos levados a questionar, por exemplo, se para cada corpo de números existe um elemento totalmente real α tal que $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um reticulado bem arredondado. Caso a resposta seja negativa, podemos investigar se ao menos em cada dimensão conseguimos encontrar um corpo de números que possui tal propriedade.

Algumas simulações computacionais realizadas em busca de encontrar elementos totalmente positivos α tais que $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ seja um reticulado bem arredondado, com $\mathbb{K}$ fixo, tem indicado sucesso apesar da raridade de respostas positivas. Em dimensão três investigamos reticulados bem arredondados obtidos em corpos de números abelianos (e portanto cíclicos) através de mergulhos torcidos. Se $\mathbb{K}$ é um corpo de números abeliano de grau 3, então $\mathbb{K}$ é subcorpo de algum n-ésimo corpo ciclotômico $\mathbb{Q}(\zeta_n)$, em que $n = p_1 \dots p_\ell$ ou $n = 9p_1 \dots p_\ell$, sendo os p_i's números primos distintos tais que $p_i \equiv 1 \ (mod\ 3)$. O símbolo ζ_n denota a n-ésima raiz primitiva da unidade. Em dimensão três os casos mais simples ocorrem quando $n = 7$ e $n = 9$, onde os corpos $\mathbb{K}$ são subcorpos ciclotômicos maximais reais. A seguir resumimos os resultados obtidos nesses casos:

- Se $n = 7$, então $\mathbb{K} = \mathbb{Q}(\omega_7)$ é um corpo maximal de grau três, onde $\omega_7 = \zeta_7 + \zeta_7^{-1}$. Através de técnicas computacionais foram encontrados os valores $\alpha = 2 - \omega_7$ e $\alpha = \omega_7^2 + \omega + 1$ tais que $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ são reticulados bem arredondados (no entanto, pode haver outros α para quais essa mesma propriedade vale);
- Se $n = 9$, então $\mathbb{K} = \mathbb{Q}(\omega_9)$ é um corpo maximal de grau três, onde $\omega_9 = \zeta_9 + \zeta_9^{-1}$. Simulações computacionais mostraram que $\alpha = \omega_9^2 - \omega_9 + 1$, $\alpha = \omega_9^2 + 2\omega_9 + 1$ e $\alpha = \omega_9^2 - 4\omega_9 + 4$ são elementos totalmente positivos para os quais $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ são reticulados bem arredondados (novamente esses podem não ser únicos).

Em trabalhos futuros pretendemos estudar subcorpos maximais reais de corpos ciclotômicos em outras dimensões, a fim de buscar a existência de elementos totalmente positivos que produzem reticulados algébricos bem arredondados através de mergulhos torcidos como imagem de anéis de inteiros desses subcorpos.

Agradecimentos

Agradecimentos à FAPESP, Processos 2013/25977-7 e 2021/11311-3, e à Comissão Organizadora do CNMAC 2023 pela oportunidade de apresentação deste trabalho.

Referências

[1] O. W. Gnilke, H. T. N. Tran, A. Karilla e C. Hollanti. "Well-Rounded Lattices for Reliability and Security in Rayleigh Fading SISO Channels". Em: **IEEE Information Theory Workshop (ITW)** (2016), pp. 359–363. DOI: 10.1109/ITW.2016.7606856.

[2] O. W. Gnilke, A. Barreal, A. Karrila, H. T. N. Tran, D. Karpuk e C. Hollanti. "Well-Rounded Lattices for Coset Coding in MIMO Wiretap Channels". Em: **IEEE Int. Telecommunication Networks and Applications Conference (ITNAC)** (2016), pp. 289–294. DOI: 10.1109/ATNAC.2016.7878824.

[3] L. Fukshansky e K. Petersen. "On well-rounded ideal lattices". Em: **Int. J. Number Theory** 8 (1) (2012), pp. 189–206. DOI: 10.1142/S179304211250011X.

[4] R. R. de Araujo e S. I. R. Costa. "Well-rounded algebraic lattices in odd prime dimension". Em: **Arch. Math. 112** (2019), pp. 138–148. DOI: 10.1007/s00013-018-1232-7.

© 2023 SBMAC