Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 12, n. 1, 2026.

Trabalho apresentado no XLIV CNMAC, Fundação Getulio Vargas - Rio de Janeiro - RJ, 2025.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Reticulados Bem-arredondados via Corpos de Números

Cleber L. de O. Santos[1]
IBILCE/UNESP, São José do Rio Preto, SP
Robson R. de Araujo[2]
IFSP, Catanduva, SP

Dizemos que Λ é um reticulado se é um subgrupo aditivo discreto de $\mathbb{R}^n$. Equivalentemente, um reticulado Λ é um conjunto dado por todas as combinações lineares com coeficientes inteiros de um conjunto fixado de $m \leq n$ vetores reais linearmente independentes. Se $m = n$, dizemos que o reticulado é de posto completo. Além de sua reconhecida utilidade à otimização, pois reticulados são úteis na busca por soluções do problema do empacotamento esférico, da cobertura esférica, entre outros, nas últimas décadas os reticulados têm sido bastante requisitados para aplicações à teoria de códigos e à criptografia pós-quântica [1–3, 8].

Seja Λ um reticulado de posto completo em $\mathbb{R}^n$. Um vetor $\mathbf{v} \in \Lambda$ é dito ser de **norma mínima** se $\|\mathbf{v}\| = \min\{\|\mathbf{u}\| \in \Lambda \ : \ \mathbf{u} \in \Lambda \setminus \{\mathbf{0}\}\}$. Dizemos que Λ é um **reticulado bem-arredondado** se ele possui uma base formada exclusivamente por vetores de norma mínima. Recentemente, reticulados bem-arredondados têm se mostrado úteis para transmissão de sinais em canais *SISO do tipo Rayleigh com desvanecimento* e em canais *wiretap MIMO* [6, 7].

Uma das maneiras bastante exploradas para a construção de reticulados é utilizando recursos da teoria algébrica dos números. Seja M um $\mathbb{Z}$-módulo no anel de inteiros de um corpo de números $\mathbb{K}$ de grau n. Chama-se de **mergulho canônico** associado a $\mathbb{K}$ à aplicação $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ definida por

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

em que $\sigma_i : \mathbb{K} \longrightarrow \mathbb{C}$, $i = 1, \ldots, r_2$, denotam os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ tais que $\sigma_1, \ldots, \sigma_{r_1}$ são aqueles que têm imagem real e $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ são os que têm imagem não contida em $\mathbb{R}$ de modo que $\sigma_{r_1+i} \neq \overline{\sigma_{r_1+j}}$ para todo $i \neq j$ em $\{1, \ldots, r_2\}$. É fato que $n = r_1 + 2r_2$. O conjunto $\sigma(M)$ é um reticulado de posto completo em $\mathbb{R}^n$, chamado de **reticulado algébrico**. Se M é o anel de inteiros de $\mathbb{K}$ ou um de seus ideais, podemos chamar $\sigma(M)$ de **reticulado ideal**.

Em [5], os autores introduzem o estudo sobre a relação entre reticulados bem-arredondados e reticulados algébricos. Se $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ denota o mergulho canônico com domínio em um corpo de números $\mathbb{K}$ de grau n e $\mathcal{O}_\mathbb{K}$ denota o anel de inteiros desse corpo de números, em [5] prova-se o notável resultado que diz que $\sigma(\mathcal{O}_\mathbb{K})$ é um reticulado bem-arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico. Também nesse trabalho apresentam-se condições para que um reticulado de posto completo em $\mathbb{R}^2$ seja bem arredondado e para que ele seja equivalente ao reticulado hexagonal.

Na mesma linha de [5], em [4] mostra-se que é possível obter reticulados bem-arredondados através de uma determinada família de $\mathbb{Z}$-módulos de anéis de inteiros de corpos de números abelianos de grau primo p ímpar via o mergulho canônico, mesmo que esses corpos não sejam ciclotômicos. Precisamente, seja $\mathbb{K}$ um corpo de números abeliano de grau primo ímpar p contido

[1]cleber.luiz@unesp.br
[2]robson.ricardo@ifsp.edu.br

em um corpo ciclotômico $\mathbb{Q}(\zeta_n)$, em que n não é divisível por p (neste caso, dizemos que $\mathbb{K}$ é não-ramificado). Em [4] é mostrada uma maneira de obter uma infinidade de $\mathbb{Z}$-módulos M tais que os reticulados $\sigma(M)$ são bem-arredondados. Consequentemente, observa-se que é possível obter sub-reticulados bem arredondados de $\sigma(\mathcal{O}_{\mathbb{K}})$, mesmo que este último não seja bem arredondado. Além disso, mostra-se que, para cada corpo de números abeliano de grau p, existe um reticulado bem-arredondado construído pelo seu mergulho canônico.

Neste trabalho, fruto dos estudos iniciais da preparação da dissertação de mestrado do autor principal, pretendemos apresentar os resultados supramencionados com algumas de suas demonstrações, bem como citar alguns resultados recentes sobre novas pesquisas envolvendo reticulados algébricos bem-arredondados. Como pesquisa futura, nos interessamos por encontrar condições para garantir a existência de reticulados algébricos bem-arredondados de dimensão dois utilizando uma versão torcida do mergulho canônico.

Agradecimentos

Agradecemos à Comissão Organizadora do CNMAC 2025 pela oportunidade de apresentação deste trabalho. Também agradecemos à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e ao Programa de Pós-Graduação em Matemática do Ibilce/Unesp pela possibilidade e pelo financiamento desta pesquisa. Por fim, agradecemos ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), que através do Projeto Universal 405842/2023-6 fomentou o trabalho do segundo autor.

Referências

[1] J. Boutros, E. Viterbo, C. Rastello e J.-C. Belfiore. "Good lattice constellations for both Rayleigh fading and Gaussian channels". Em: **IEEE Transactions on Information Theory** 42.2 (1996), pp. 502–518. DOI: 10.1109/18.485720.

[2] J. H. Conway e N. J. A. Sloane. **Sphere packings, lattices and groups**. New York, NY, USA: Spring-Verlag, 1998.

[3] S. I. R. Costa, F. Oggier, A. Campello, J. Belfiore e E. Viterbo. **Lattices applied to coding for reliable and secure communications**. Springer, 2017.

[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.

[5] 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.

[6] O. W. Gnilke, A. Barreal, A. Karrila, H. T. N. Tran, D. A. Karpuk e C. Hollanti. "Well-rounded lattices for coset coding in MIMO wiretap channels". Em: **2016 26th International Telecommunication Networks and Applications Conference (ITNAC)**. 2016, pp. 289–294. DOI: 10.1109/ATNAC.2016.7878824.

[7] O. W. Gnilke, A. Karrila, H. T. N. Tran e C. Hollanti. "Well-rounded lattices for reliability and security in Rayleigh fading SISO channels". Em: **2016 IEEE Information Theory Workshop (ITW)**. 2016, pp. 359–363. DOI: 10.1109/ITW.2016.7606856.

[8] D. Micciancio e O. Regev. "Lattice-based cryptography". Em: **Post-quantum cryptography**. Springer, 2009, pp. 147–191.