Uma breve introdução à Teoria de Reticulados e suas aplicações

Franciele do Carmo Silva
francielecs@ime.unicamp.br

6 de fevereiro de 2023

Um reticulado 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 $\beta = \{\mathbf{b_1}, \ldots, \mathbf{b_m}\}$ em $\mathbb{R}^n$ tal que Λ é o conjunto de todas combinações lineares de tais vetores com coeficientes inteiros [1, 2]. Reticulados têm sido estudados devido às suas aplicações em comunicações, particularmente na codificação para transmissão confiável e segura de informações, na chamada *Criptografia Pós-Quântica* [3]. Despertam também um grande interesse do ponto de vista teórico. Recentemente, isso foi evidenciado, por exemplo, pela premiação de Maryna Viazovska com a Medalha Fields devido aos seus trabalhosrelacionados a reticulados [4, 5]. Nessa palestra, apresentaremos os principais conceitos e propriedades na Teoria de reticulados. Além disso, destacaremos brevemente como tais propriedades se relacionam às suas utilizações na área de comunicações e criptografia. Encerraremos mencionando algumas das construções de reticulados com as quais temos trabalhado.

Referências

[1] J. H. Conway; N. J. A. Sloane. Sphere packings, lattices and groups. Springer Science & Business Media, 2013.

[2] S. I. R. Costa , F. Oggier, A. Campello, J.C. Belfiore, E, Viterbo; Lattices Applied to Codiging for Reliable and Secure Communications, Springer, 2017.

[3] C. Peikert. A decade of lattice cryptography. Cryptology ePrint Archive, 2015.

[4] Viazovska, M. S. The sphere packing problem in dimension 8. Annals of Mathematics, 991-1015, 2017.

[5] Cohn, H., Kumar, A., Miller, S., Radchenko, D., Viazovska, M. The sphere packing problem in dimension 24. Annals of Mathematics, 185(3), 1017-1033, 2017