Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 11, n. 1, 2025.

Trabalho apresentado no XLIII CNMAC, Centro de Convenções do Armação Resort - Porto de Galinhas - PE, 2024

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Sobre Propriedades das Construção D e D' via Códigos q-ários

Franciele C. Silva[1], Ana Paula de Souza[2], Eleonesio Strey[3], Sueli I. R. Costa [4]
IMECC/Unicamp, Campinas, SP

Reticulados no espaço Euclidiano n-dimensional, i.e., subgrupos aditivos discretos de $\mathbb{R}^n$, têm recebido especial atenção visando aplicações em codificação para transmissão confiável e em Criptografia Pós-Quântica. Reticulados obtidos por meio de construções multicamadas, como as Construções D, D', C e C^*, em particular, destacam-se ainda por admitir uma decodificação multinível, a qual pode permitir complexidade de decodificação razoável. Soma-se a isso o fato de que alguns dos reticulados notáveis, como E_8, BW_{16} e Leech, por exemplo, são construtíveis por tais métodos. Sob essa perspectiva, o estudo de parâmetros como distância mínima sob a norma L_p e densidade de empacotamento, assim como esquemas de codificação e decodificação para essas construções podem-se mostrar úteis.

Para construções via códigos binários e p-ários, com p primo, e as distâncias euclidiana e de Lee, algumas dessas propriedades foram obtidas separadamente em trabalhos conhecidos [1, 2, 4, 5]. Neste trabalho, propomos a obtenção de limitantes para esses invariantes, assim como condições suficientes para atingi-los para as construções D e D' via códigos sobre $\mathbb{Z}_q$ (códigos q-ários). Métodos para a obtenção de uma matriz geradora também são apresentados. Os resultados a serem apresentados incluem parte de um artigo recém publicado [3]. Futuras direções nesta pesquisa em andamento e suas perspectivas incluem a análise de classes conhecidas de códigos, como LDPC (Low-Density-Parity-Check codes) e quase-cíclicos para a obtenção de reticulados com boas propriedades, assim como a obtenção de outros invariantes relevantes.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, do CNPq (32441/2021-2) e da FAPESP (2020/09838-0) e ao IMECC-Unicamp.

Referências

[1] M. F. Bollauf, R. Zamir e S. I. R. Costa. "Multilevel constructions: coding, packing and geometric uniformity". Em: **IEEE Transactions on Information Theory** 65.12 (2019), pp. 7669–7681.

[2] J. H. Conway e N. J. A. Sloane. **Sphere Packings, Lattices and Groups**. New York, NY, USA: Spring-Verlag, 1998. ISBN: 978-1-4757-6568-7.

[1] francielecs@ime.unicamp.br
[2] anasouza@ime.unicamp.br
[3] eleonesio.strey@ufes.br
[4] sueli@ime.unicamp.br

[3] F. C. Silva, A. P. Souza, E. Strey, e S. I. R. Costa. "On lattice constructions D and D' from q-ary linear codes". Em: **Communications in Mathematics** 31.(2) (2023), pp. 173–207. DOI: 10.46298/cm.11146.

[4] W. Kositwattanarerk e F. Oggier. "Connections between construction D and related constructions of lattices". Em: **Designs, codes and cryptography** 73.2 (2014), pp. 441–455. DOI: 10.1007/s10623-014-9939-3.

[5] E. Strey. "Construções de reticulados a partir de códigos q-ários". Tese de doutorado. Unicamp, 2017.