Constructions of unimodular lattices via subfields of cyclotomic fields[1]

Grasiele C. Jorge[a], João E. Strapasson[b], Agnaldo J. Ferrari[c], Sueli I. R. Costa[d]

[a] Federal University of São Paulo - São José dos Campos

[b] University of Campinas - Limeira

[c] São Paulo State University - Bauru

[d] University of Campinas - Campinas

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$. Equivalently, $\Lambda \subseteq \mathbb{R}^n$ is a lattice iff there are linearly independent vectors $v_1, \ldots, v_m \in \mathbb{R}^n$ such that $\Lambda = \{\sum_{i=1}^{m} a_i v_i;\ a_i \in \mathbb{Z},\ \forall i\}$.

Lattices have been studied for meaningful applications in coding theory and cryptography. Usually the problem of finding good signal constellations for a Gaussian channel is associated with the search for lattices with high packing density. For a Rayleigh fading channel the efficiency, measured by lower error probability in the transmission, is strongly related to the lattice diversity and high minimum product distance. On the other hand, for MIMO and SISO wiretap channels, the lattices that have been considered are well-rounded lattices.

Let $\mathbb{K}$ be a number field of degree n, $\mathcal{O}_{\mathbb{K}}$ its ring of integers and $\alpha \in \mathcal{O}_{\mathbb{K}}$ a totally real and totally positive element. In [1, 2] it was introduced a twisted embedding $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ such that if $\mathcal{I} \subseteq \mathcal{O}_{\mathcal{K}}$ is a free -module of rank m, $1 \leq m \leq n$, then $\sigma_\alpha(\mathcal{I})$ is a lattice in $\mathbb{R}^n$ of rank m, called here an algebraic lattice. Special algebraic lattice constructions can be used to obtain certain lattice parameters which are usually difficult to calculate for general lattices in $\mathbb{R}^n$.

In this talk we will approach constructions of full diversity unimodular lattices in dimension $n = 8k$ using the twisted embedding and the number fields $\mathbb{Q}(\zeta_{2^r q} + \zeta_{2^r q}^{-1})$ for $q > 1$ odd. The lattices obtained are equivalent to $\mathbb{Z}^8 \times E_8^{k-1}$, E_8^k and the Leech lattice Λ_{24}.

[1] This work was supported by Fapesp 2019/14390-1, 2020/09838-0 and 2013/25977-7 and CNPq 432735/2016-0 and 429346/2018-2

The lattices E_8 and Λ_{24} are the densest lattices in dimension 8 and 24, respectivelly, and both are well-rounded.

References

[1] E. Bayer-Fluckiger, *Lattices and number fields*, Contemporary Mathematics, v. 241, pp. 69-84, 1999.

[2] E. Bayer-Fluckiger, *Ideal lattices,* Proceedings of the conference Number theory and Diophantine Geometry, Zurich, 1999, Cambridge Univ. Press, pp. 168-184, 2002.

[3] J. E. Strapasson, A. J. Ferrari, G. C. Jorge, S. I. R. Costa, *Algebraic constructions of rotated unimodular lattices and direct sum of Barnes–Wall lattices*, Journal of Algebra and Its Applications, v. 20, n. 03, 2150029, 2021.