Unimodular lattices via $\mathbb{Q}(\zeta_{2^r p} + \zeta_{2^r p}^{-1})$ for $p = 3$ and $p = 5$

Grasiele Jorge
Federal University of Sao Paulo, Brazil
grajorge@gmail.com

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$. Lattices have a range of applications in different areas, especially in information theory and more recently in cryptography. Special algebraic lattice constructions can be used to derive certain parameters which are usually difficult to calculate for general lattices such as diversity and minimum product distance, which are important parameters related to the signal transmission error probability over Rayleigh fading channels [3]. In this work we approach algebraic constructions of full diversity unimodular lattices via the twisted embedding, introduced in [1,2], applied to the ring of the integers of $\mathbb{Q}(\zeta_{2^r p} + \zeta_{2^r p}^{-1})$ for $p = 3$ and $p = 5$ and calculate their minimum product distances. The lattices obtained here are direct sums of rotated versions of the lattices $\mathbb{Z}^8$ and E_8.

References

[1] E. Bayer-Fluckiger, Lattices and number fields, Contemporary Mathematics, vol. 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] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, New Algebraic Constructions of Rotated $\mathbb{Z}^n$-Lattice Constellations for the Rayleigh Fading Channel, IEEE Transactions on Information Theory, vol. 50, no. 4, pp. 702-714, 2004.

Joint work with Agnaldo José Ferrari (Sao Paulo State University, Brazil).