Journal of Algebra 429 (2015) 218–235

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Algebraic constructions of densest lattices ☆

Grasiele C. Jorge [a,*], Antonio A. de Andrade [b,*], Sueli I.R. Costa [c,*], João E. Strapasson [d,*]

[a] *UNIFESP – Federal University of São Paulo, 12247-014, São José dos Campos, SP, Brazil*
[b] *UNESP – São Paulo State University, 15054-000, São José do Rio Preto, SP, Brazil*
[c] *UNICAMP – University of Campinas, 13083-859, Campinas, SP, Brazil*
[d] *UNICAMP – University of Campinas, 13484-350, Limeira, SP, Brazil*

ARTICLE INFO

Article history:
Received 7 March 2014
Available online 18 February 2015
Communicated by Eva Bayer-Fluckiger

Keywords:
Algebraic number theory
Lattices
Packing density
Diversity
Minimum product distance
Coding theory

ABSTRACT

The aim of this paper is to investigate rotated versions of the densest known lattices in dimensions 2, 3, 4, 5, 6, 7, 8, 12 and 24 constructed via ideals and free $\mathbb{Z}$-modules that are not ideals in subfields of cyclotomic fields. The focus is on totally real number fields and the associated full diversity lattices which may be suitable for signal transmission over both Gaussian and Rayleigh fading channels. We also discuss on the existence of a number field $\mathbb{K}$ such that it is possible to obtain the lattices A_2, E_6 and E_7 via a twisted embedding applied to a fractional ideal of $\mathcal{O}_{\mathbb{K}}$.

☆ This work was partially supported by CNPq 150802/2012-9 and 312926/2013-8 and FAPESP 2013/25977-7.

* Corresponding author.
E-mail addresses: grasiele.jorge@unifesp.br (G.C. Jorge), andrade@ibilce.unesp.br (A.A. Andrade), sueli@ime.unicamp.br (S.I.R. Costa), joao.strapasson@fca.unicamp.br (J.E. Strapasson).

http://dx.doi.org/10.1016/j.jalgebra.2014.12.044
0021-8693/© 2015 Elsevier Inc. All rights reserved.

1. Introduction

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 $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbb{R}^n$ such that $\Lambda = \{\sum_{i=1}^m a_i \boldsymbol{v}_i;\ a_i \in \mathbb{Z},\ i = 1, \ldots, m\}$.

Lattices have been considered in different areas, especially in coding theory and more recently in cryptography. In this paper, we attempt to construct lattices with full rank, i.e., $m = n$, which may be suitable for signal transmission over both Gaussian and Rayleigh fading channels (see [9, Section I]). For this purpose the lattice parameters we consider here are packing density, diversity and minimum product distance.

The classical sphere packing problem is to find out how densely a large number of identical spheres can be packed together in the Euclidean space. The *packing density* of a lattice Λ is the proportion of the space $\mathbb{R}^n$ covered by the non-overlapping spheres of maximum radius centered at the points of Λ. The densest possible lattice packings have only been determined in dimensions 1 to 8 and 24 (see [12, p. 12] for $n = 1, 2, \ldots, 8$ and [13] for $n = 24$). It is also known that these densest lattice packings are unique.

A lattice Λ has *diversity* $k \leq n$ if k is the maximum number such that any non-zero vector $\boldsymbol{y} \in \Lambda$ has at least k non-zero coordinates. Given a full rank lattice with full diversity $\Lambda \subseteq \mathbb{R}^n$, i.e., $k = n$, the *minimum product distance* of Λ is defined as $d_{p,min}(\Lambda) = \min\{\prod_{i=1}^n |y_i|;\ \boldsymbol{y} \in \Lambda,\ \boldsymbol{y} \neq \boldsymbol{0}\}$.

Usually the problem of finding good signal constellations for a Gaussian channel is associated with the search for lattices with high packing density (see [12, Chapter 3]). On the other hand, 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 (see [9, Section III]).

In this paper, we make use of algebraic number theory for constructing rotated lattices via subfields of cyclotomic fields. 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 positive real element. In [3,4] it was introduced a twisted embedding $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ such that if $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n, then $\sigma_\alpha(\mathcal{I})$ is a lattice in $\mathbb{R}^n$. These lattices are called here *algebraic lattices*. Special algebraic lattice constructions can be used to obtain certain lattice parameters such as packing density and minimum product distance, which are usually difficult to calculate for general lattices in $\mathbb{R}^n$. Some constructions and properties of algebraic lattices can be found in [1–18]. We quote particularly the paper [8], where full diversity rotated versions of the lattices A_2, E_6, E_8, K_{12} and Λ_{24} are constructed.

Let $\mathbb{K}$ be a totally real number field. When an algebraic lattice can be obtained via a free $\mathbb{Z}$-module $\mathcal{I}$ contained in $\mathcal{O}_{\mathbb{K}}$, its minimum product distance depends on the discriminant $d_{\mathbb{K}}$ of the number field considered (see [6, Section III]). In order to get greater minimum product distances, we consider number fields with small discriminants. Results on the existence of number fields $\mathbb{K}$ such that it is possible to obtain rotated A_2, E_6 and E_7-lattices via twisted embeddings applied to fractional ideals of $\mathcal{O}_{\mathbb{K}}$ are presented in Propositions 4.1, 4.7 and 4.10. Using some constructions of rotated $\mathbb{Z}^n$-lattices, we also