Finite Fields and Their Applications 45 (2017) 217–236

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Dense packings from algebraic number fields and codes ☆

Shantian Cheng

Risk Management Institute, National University of Singapore, 21 Heng Mui Keng Terrace, 119613, Singapore

ARTICLE INFO

Article history:
Received 25 June 2016
Received in revised form 11 December 2016
Accepted 16 December 2016
Available online xxxx
Communicated by Chaoping Xing

MSC:
11H31
52C17
11H71
11H06
11R04

Keywords:
Dense packings
Number fields
Minkowski lattice
Codes

ABSTRACT

We introduce a new method from number fields and codes to construct dense packings in the Euclidean spaces. Via the canonical $\mathbb{Q}$-embedding of arbitrary number field K into $\mathbb{R}^{[K:\mathbb{Q}]}$, both the prime ideal $\mathfrak{p}$ and its residue field κ can be embedded as discrete subsets in $\mathbb{R}^{[K:\mathbb{Q}]}$. Thus we can concatenate the embedding image of the Cartesian product of n copies of $\mathfrak{p}$ together with the image of a length n code over κ. This concatenation leads to a packing in the Euclidean space $\mathbb{R}^{n[K:\mathbb{Q}]}$. Moreover, we extend the single concatenation to multiple concatenations to obtain dense packings and asymptotically good packing families. For instance, with the help of Magma, we construct a 256-dimensional packing denser than the Barnes–Wall lattice BW_{256}.

© 2017 Elsevier Inc. All rights reserved.

1. Introduction

The classical problem of packing non-overlapping equal spheres densely in an n-dimensional Euclidean space has attracted the interest of numerous mathematicians

☆ This research began when the author was a PhD candidate at Nanyang Technological University, Singapore.

E-mail addresses: rmicst@nus.edu.sg, chengshantian@gmail.com.

http://dx.doi.org/10.1016/j.ffa.2016.12.006
1071-5797/© 2017 Elsevier Inc. All rights reserved.

for centuries. Many methods and results from different disciplines, such as discrete geometry, combinatorics, number theory and coding theory, etc. have been involved in this problem, while some explicit fascinating dense constructions and asymptotically good packing families have been found. For a detailed survey on the development in this field, the reader may refer to the books of Cassels [6], Conway and Sloane [8], Zong [20]. If the centers of the packed spheres form a discrete additive subgroup of $\mathbb{R}^n$ (lattice), we call it a lattice packing.

Sphere packings are continuous analogues of error-correcting codes in the Hamming space [9]. The basic goal of error-correcting codes is to seek the maximum size of a code given a fixed length, alphabet size and minimal Hamming distance (that is, to achieve a dense packing of points in the Hamming space), such that each pair of distinct points is separated at least by the minimum Hamming distance. In the digital world, error-correcting codes are widely employed in information storage and transmission, for example, the blue ray storage format and the communication between space stations and the Earth. Based on the similarities between sphere packings and error-correcting codes, the results in sphere packings can potentially contribute to the development of error-correcting codes.

On the other hand, some constructions of dense lattice or non-lattice packings are inspired by constructions in coding theory. For example, similar to concatenated codes, Leech and Sloane's "Construction A" method concatenated certain binary codes together with $2 \cdot \mathbb{Z}^n$ to construct new lattice packings (see details in [8, Chapter 5]). Bachoc [2] generalized the method to construct modular lattices using codes over finite involution algebras. In Construction C [20, Chapter 5], the binary expansion of the coordinates in $\mathbb{Z}^n$ is considered. Specifically, a point is a packing center if and only if its first ℓ coordinate arrays are codewords in certain ℓ binary codes.

Let $\omega = \frac{-1+\sqrt{-3}}{2}$. Xing [19] further investigated the concatenating method. Instead of packings in $\mathbb{Z}^n$, he considered the packings in $\mathcal{O}_K^n$, where $\mathcal{O}_K = \mathbb{Z}[\omega]$ denotes the ring of integers in the number field $\mathbb{Q}(\sqrt{-3})$. In other words, for a non-zero prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$, the power of the prime ideal, denoted by $\mathfrak{P}^n$, can be embedded as a lattice L in $\mathbb{R}^{2n}$ via the canonical $\mathbb{Q}$-embedding of the special number field $\mathbb{Q}(\sqrt{-3})$ into $\mathbb{R}^2$. Hence any subset $\mathcal{P}$ of $\mathfrak{P}^n$ can be regarded as a packing in $\mathbb{R}^{2n}$. Then he replaced the binary expansion in Construction C by the $\mathfrak{P}$-adic expansion, and concatenated the lattice L with some special codes over $\mathcal{O}_K/\mathfrak{P}$. This method produces several dense packings in low dimensions attaining the best-known densities and also obtains an unconditional bound on the asymptotic density exponent $\lambda \geqslant -1.265$ (see [19]). Cheng [7] applied this concatenation to multiplicative lattices and improved the asymptotic density of packing families derived from multiplicative lattices. One natural question is whether we can use arbitrary number field instead of the special quadratic number field $\mathbb{Q}(\sqrt{-3})$ to generalize the constructing method.

In this paper, we extend Xing's method to a general level, i.e. we employ the ideals in $\mathcal{O}_K$ instead of $\mathbb{Z}[\omega]$, where $\mathcal{O}_K$ denotes the ring of integers in an arbitrary number field K. Suppose the extension degree of K over $\mathbb{Q}$ is m. Minkowski interpreted the

Download English Version:

https://daneshyari.com/en/article/5771593

Download Persian Version:

https://daneshyari.com/article/5771593

Daneshyari.com