A NEW NUMBER FIELD CONSTRUCTION OF THE
 D_4 -LATTICE

J. Carmelo Interlando¹ §, José Othon Dantas Lopes²,
Trajano Pires da Nóbrega Neto³

¹Department of Mathematics and Statistics
San Diego State University
San Diego, CA 92182-7720, USA

²Department of Mathematics
Federal University of Ceará
Fortaleza, CE 60455-900, BRAZIL

³Department of Mathematics
São Paulo State University
São José do Rio Preto, SP 15054-000, BRAZIL

Abstract: A classical problem in lattice theory is to determine whether a given lattice can be realized as $\mathfrak{D}_K$ -lattice, where $\mathfrak{D}_K$ is the ring of integers of some number field K . In this work we show that the lattice D_4 can be realized as an $\mathfrak{D}_F$ -lattice for infinitely many totally real biquadratic fields F .

AMS Subject Classification: 11H06, 11H31, 11R16

Key Words: lattices, number fields, sphere packings

1. Introduction

In this work an n -dimensional lattice means a discrete subgroup of $\mathbb{R}^n$ of rank n . Given a number field K of degree n over the rationals and its ring of integers $\mathfrak{D}_K$, n -dimensional lattices can be obtained as geometric representations of submodules of rank n of $\mathfrak{D}_F$ via the Minkowski homomorphism (canonical

Received: March 6, 2018

© 2018 Academic Publications

§Correspondence author

embedding) [2, 11], and more generally via the twisted homomorphism [1]. A lattice Λ obtained from a number field K via one of the above mappings is an $\mathfrak{O}_K$ -lattice; alternatively, we also say that Λ can be realized as an $\mathfrak{O}_K$ -lattice.

One important feature of a lattice Λ is the sphere packing associated to it, namely, the arrangement of identical spheres centered at the points of Λ and of radii equal to half the minimum distance of Λ . The latter quantity is defined as the minimum Euclidean distance between any two distinct lattice points or equivalently, the minimum ℓ^2 -norm of any nonzero lattice vector. The packing density of Λ is equal to the fraction of the space filled by the spheres described above. Determining a lattice with the highest packing density in a given dimension n is a classical problem in geometry of numbers, which also has important applications in data transmission [2, 10].

An important open problem stated in [1] is: Given a lattice Λ , is there a number field K such that Λ is an $\mathfrak{O}_K$ -lattice? If so, what are the number fields having this property? Using the above algebraic construction and cyclotomic fields, M. Craig reproduced the Leech lattice [3] and the lattice E_6 [4]. He has also obtained a family lattices in dimensions $p - 1$, for p prime, denoted by $A_{p-1}^{(m)}$, such that the associated sphere packings have record density in several dimensions [2, pp. 222-227]. The lattice E_8 has been reproduced in [1] and [5] using cyclotomic fields.

The focus of this paper is on the checkerboard lattice D_4 , which is defined as the set of all points (x_1, x_2, x_3, x_4) in $\mathbb{Z}^4$ such that $x_1 + x_2 + x_3 + x_4$ is even. The sphere packing associated to D_4 is the densest lattice packing in four dimensions, with density equal to $\pi^2/16$. This result was proved by Korkine and Zolotareff [8]. In [7] the authors showed that D_4 is the image, under the twisted homomorphism, of a $\mathbb{Z}$ -submodule I in the ring of integers of $\mathbb{Q}(\zeta + \zeta^{-1})$, where $\zeta \in \mathbb{C}$ is a primitive 16th root of unity.

The contribution of the present paper, which is contained in Section 3, is a new number field construction for D_4 : We show that the lattice can be obtained from an infinite family of totally real biquadratic fields via the Minkowski homomorphism. A brief review of notation and the required background will be presented in Section 2.

2. Background

This section reviews the standard definitions and results that will be used in Section 3. The reader interested in further details is referred to [2, Chap. 1]. The volume of an n -dimensional lattice Λ , denoted by $\text{vol } \Lambda$, is defined as the

volume of the parallelotope determined by any basis of Λ . The center density of Λ is defined as $\delta(\Lambda) = \rho^n / \text{vol } \Lambda$.

Let K be a totally real number field of degree n whose embeddings ($\mathbb{Q}$ -monomorphisms of K into $\mathbb{C}$) are $\sigma_1, \dots, \sigma_n$. If $\mathfrak{O}_K$ is the ring of integers of K , then $\sigma_K : \mathfrak{O}_K \rightarrow \mathbb{R}^n$, given by $\sigma_K(x) = (\sigma_1(x), \dots, \sigma_n(x))$, is the canonical embedding or Minkowski homomorphism of K into $\mathbb{R}^n$. Now regard $\mathfrak{O}_F$ as a $\mathbb{Z}$ -module. If $\mathcal{M}$ is a submodule of $\mathfrak{O}_F$ of rank n , then $\sigma_K(\mathcal{M})$ is an n -dimensional lattice whose minimum distance and volume are given, respectively, by

$$\min_{\substack{x \in \mathcal{M} \\ x \neq 0}} \sqrt{\text{Tr}_{K/\mathbb{Q}}(x^2)} \quad \text{and} \quad \sqrt{\text{Disc}(K)} \cdot [\mathfrak{O}_K : \mathcal{M}],$$

where $\text{Tr}_{K/\mathbb{Q}}(\cdot)$ denotes the field trace and $\text{Disc}(K)$ denotes the discriminant of K , see [2, Ch. 8] and [11, Ch. 4]. Therefore, the center density of Λ is given by

$$\delta(\sigma_K(\mathcal{M})) = \frac{\left(\min_{\substack{x \in \mathcal{M} \\ x \neq 0}} \text{Tr}_{K/\mathbb{Q}}(x^2) \right)^{n/2}}{\sqrt{\text{Disc}(K)} \cdot [\mathfrak{O}_K : \mathcal{M}]} . \quad (1)$$

3. Lattices from $\mathbb{Q}(\sqrt{2}, \sqrt{m})$

Let F be the totally real biquadratic field $\mathbb{Q}(\sqrt{2}, \sqrt{m})$ where m is a positive square-free integer congruent to 3 modulo 4. An integral basis for F is $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, where

$$\alpha_1 = 1, \alpha_2 = \sqrt{2}, \alpha_3 = \sqrt{m}, \alpha_4 = \frac{\sqrt{2} + \sqrt{2m}}{2},$$

and

$$\text{Disc}(F) = 256m^2, \quad (2)$$

see [9, pp. 51–52]. The automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{m})$ are:

$$\begin{aligned} \text{id} : \begin{cases} \sqrt{2} & \mapsto \sqrt{2} \\ \sqrt{m} & \mapsto \sqrt{m} \end{cases} & \quad \sigma : \begin{cases} \sqrt{2} & \mapsto -\sqrt{2} \\ \sqrt{m} & \mapsto \sqrt{m} \end{cases} \\ \tau : \begin{cases} \sqrt{2} & \mapsto \sqrt{2} \\ \sqrt{m} & \mapsto -\sqrt{m} \end{cases} & \quad \sigma\tau : \begin{cases} \sqrt{2} & \mapsto -\sqrt{2} \\ \sqrt{m} & \mapsto -\sqrt{m} \end{cases} . \end{aligned}$$

Let $x = x_1 \cdot \alpha_1 + x_2 \cdot \alpha_2 + x_3 \cdot \alpha_3 + x_4 \cdot \alpha_4$ be an arbitrary element in $\mathfrak{D}_F$ where $x_1, \dots, x_4$ are rational integers. Observing that

$$\mathrm{Tr}_{F/\mathbb{Q}}(\alpha_1) = 4, \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_2) = \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_3) = \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_4) = 0,$$

$$\mathrm{Tr}_{F/\mathbb{Q}}(\alpha_2^2) = 8, \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_3^2) = 4m, \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_4^2) = 2m + 2,$$

$$\mathrm{Tr}_{F/\mathbb{Q}}(\alpha_2\alpha_3) = 0, \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_2\alpha_4) = 4, \mathrm{Tr}_{F/\mathbb{Q}}(\alpha_3\alpha_4) = 0,$$

we obtain

$$\mathrm{Tr}_{F/\mathbb{Q}}(x^2) = 4x_1^2 + 2 \cdot (2x_2 + x_4)^2 + 2m \cdot (2x_3^2 + x_4^2). \quad (3)$$

Now let j be a fixed rational integer and define

$$\mathcal{M}_{j,m} := \left\{ \begin{array}{l} x_1 \cdot \alpha_1 + x_2 \cdot \alpha_2 + x_3 \cdot \alpha_3 \\ + x_4 \cdot \alpha_4 \in \mathfrak{D}_F \end{array} \left| \begin{array}{l} x_3 \equiv x_1 \pmod{2}, \\ x_4 \equiv jx_1 - 2x_2 \pmod{m} \end{array} \right. \right\}$$

Clearly, $\mathcal{M}_{j,m}$ is a submodule of $\mathfrak{D}_F$ of rank 4 and index $2m$.

Hereafter, we will assume that m is a prime congruent to 3 modulo 8. By Dirichlet's Theorem [6, Ch. II, Theorem 15], there are infinitely many such primes; furthermore, from [6, Ch. VI, Theorems 82 and 95], it follows that

$$\left(\frac{-2}{m} \right) = \left(\frac{-1}{m} \right) \cdot \left(\frac{2}{m} \right) = (-1) \cdot (-1) = 1,$$

that is, -2 is quadratic residue of m .

Lemma 1. *Notation as above, let j be such that $j^2 \equiv -2 \pmod{m}$. If x is a nonzero element of $\mathcal{M}_{j,m}$, then $\mathrm{Tr}_{F/\mathbb{Q}}(x^2) \geq 8m$.*

Proof. The assertion is clear if $|x_3|$ and $|x_4|$ are both greater than 1, so we will analyze the following cases:

1. $x_3 = x_4 = 0$.	4. $x_3 = x_4 = 1$.
2. $x_3 = 0, x_4 = 1$.	
3. $x_3 = 1, x_4 = 0$.	5. $x_3 = -1, x_4 = 0$.

The case $(x_3, x_4) = (0, -1)$ is analogous to Case 2 whereas the cases $(x_3, x_4) = (1, -1), (-1, 1)$, and $(-1, -1)$ are analogous to Case 4, so they will be omitted.

Case 1: We have $x_1 = 2y_1$ for some y_1 in $\mathbb{Z}$. The form in (3) becomes

$$\mathrm{Tr}_{F/\mathbb{Q}}(x^2) = 16y_1^2 + 2 \cdot (2x_2)^2 = 8(2y_1^2 + x_2^2).$$

If we show that $2y_1^2 + x_2^2 \geq m$, this case is concluded. Indeed, from $jx_1 - 2x_2 \equiv 0 \pmod{m}$, it follows that $j(2y_1) \equiv 2x_2 \pmod{m}$, whence $2y_1^2 + x_2^2 \equiv 0 \pmod{m}$. Since y_1 and x_2 cannot be both zero, the assertion follows.

Case 2: We have $x_1 = 2y_1$ for some y_1 in $\mathbb{Z}$. From $x_4 \equiv (jx_1 - 2x_2) \pmod{m}$, it follows that $jx_1 - 2x_2 \equiv 1 \pmod{m}$, whence $(2x_2 + 1)^2 \equiv -8y_1^2 \pmod{m}$. The form in (3) becomes

$$\begin{aligned} \mathrm{Tr}_{F/\mathbb{Q}}(x^2) &= 16y_1^2 + 2 \cdot (2x_2 + 1)^2 + 2m \\ &= 16y_1^2 + 2(-8y_1^2 + km) + 2m = 2(k + 1)m \end{aligned}$$

for some $k \in \mathbb{Z}$. Once we show that $k \geq 3$, this case is concluded. Indeed, if $k = 0$, then $(2x_2 + 1)^2 = -8y_1^2$, which is impossible. Similarly, if $k = 1$, then $(2x_2 + 1)^2 = -8y_1^2 + m$, which is impossible because $m \equiv 3 \pmod{8}$. Finally, if $k = 2$, then $(2x_2 + 1)^2 = -8y_1^2 + 2m$, which is impossible again. Hence, $k \geq 3$.

Case 3: We have $x_1 = 2y_1 + 1$ for some y_1 in $\mathbb{Z}$. From $x_4 \equiv (jx_1 - 2x_2) \pmod{m}$, it follows that $jx_1 - 2x_2 \equiv 0 \pmod{m}$, whence $2x_2^2 \equiv -x_1^2 \pmod{m}$. The form in (3) becomes

$$\begin{aligned} \mathrm{Tr}_{F/\mathbb{Q}}(x^2) &= 4x_1^2 + 8x_2^2 + 4m = 4x_1^2 + 4(-x_1^2 + km) + 4m \\ &= 4m(k + 1) \end{aligned}$$

for some $k \in \mathbb{Z}$. Once we show that $k \geq 1$, this case is concluded. Indeed, if $k = 0$, then $-x_1^2 = 2x_2^2$, which is impossible. Hence, $k \geq 1$.

Case 4: We have $x_1 = 2y_1 + 1$ for some y_1 in $\mathbb{Z}$. From $x_4 \equiv (jx_1 - 2x_2) \pmod{m}$, it follows that $jx_1 - 2x_2 \equiv 1 \pmod{m}$, whence $(1 + 2x_2)^2 \equiv -2x_1^2 \pmod{m}$. The form in (3) becomes

$$\mathrm{Tr}_{F/\mathbb{Q}}(x^2) = 4x_1^2 + 2(-2x_1^2 + km) + 6m = 2m(k + 3)$$

for some $k \in \mathbb{Z}$. Once we show that $k \geq 1$, this case is concluded. Indeed, if $k = 0$, then $(1 + 2x_2)^2 = -2x_1^2$, which is impossible. Hence, $k \geq 1$.

Case 5: We have $x_1 = 2y_1 + 1$ for some y_1 in $\mathbb{Z}$. From $x_4 \equiv (jx_1 - 2x_2) \pmod{m}$, it follows that $jx_1 - 2x_2 \equiv -1 \pmod{m}$, whence $(1 + 2x_2)^2 \equiv -2x_1^2 \pmod{m}$. The form in (3) becomes

$$\mathrm{Tr}_{F/\mathbb{Q}}(x^2) = 4x_1^2 + 2(-2x_1^2 + km) + 6m = 2m(k + 3)$$

for some $k \in \mathbb{Z}$. Once we show that $k \geq 1$, this case is concluded. Indeed, if $k = 0$, then $(1 + 2x_2)^2 = -2x_1^2$, which is impossible. Hence, $k \geq 1$. □

Recalling that the densest 4-dimensional lattice packing is unique and has center density equal to $1/8$, see [2, pp. 13 and 15], we can now state the main result of the paper.

Theorem 2. *Let j and m be rational integers such that m is a prime congruent to 3 modulo 8 and $j^2 \equiv -2 \pmod{m}$. The center density of the four-dimensional lattice $\sigma_F(\mathcal{M}_{j,m})$ is equal to $1/8$. Thus, $\sigma_F(\mathcal{M}_{j,m})$ is the lattice D_4 up to scaling and isometries.*

Proof. From (1), (2), $[\mathfrak{D}_F : \mathcal{M}_{j,m}] = 2m$, and Lemma 1, one has

$$\delta(\sigma_F(\mathcal{M}_{j,m})) = \frac{(8m)^2}{2^4 \cdot 16m \cdot 2m} = \frac{1}{8}.$$
□

References

- [1] E. Bayer-Fluckiger, Lattices and number fields, In: *Contemp. Math.*, Amer. Math. Soc., Providence (1999), 69–84.
- [2] J.H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd Edition, Springer Verlag, New York (1999).
- [3] M. Craig, A cyclotomic construction for Leech’s lattice, *Mathematika*, **25** (1978), 236–241.
- [4] M. Craig, Extreme forms and cyclotomy, *Mathematika*, **25** (1978), 44–56.
- [5] A.L. Flores, J.C. Interlando, T.P. da Nóbrega Neto, and A.L. Contiero, A new number field construction of the lattice E_8 , *Beiträge zur Algebra und Geometrie/Contributions to Algebra and Geometry*, **54** (2013), 503–508.

- [6] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Sixth edition, Oxford University Press, Oxford (2008).
- [7] G.C. Jorge, A.J. Ferrari, and S.I.R. Costa, Rotated D_n lattices, *J. Number Theory*, **132** (2012), 2397–2406.
- [8] A. Korkine and G. Zolotareff, Sur les formes quadratique positive quaternaires, *Math. Ann.*, **5** (1872), 581–583.
- [9] D. Marcus, *Number Fields*, Springer Verlag, New York (1977).
- [10] M. Pischella and D. Le Ruyet, *Digital Communications 2: Digital Modulations*, Wiley (2015).
- [11] P. Samuel, *Algebraic Theory of Numbers*, Hermann, Paris (1970).