International Journal of Applied Mathematics

Volume 33 No. 6 2020, 1009-1015
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v33i6.4

FULLY-DIVERSE LATTICES FROM RAMIFIED CYCLIC EXTENSIONS OF PRIME DEGREE

J. Carmelo Interlando[1], Antonio A. Andrade[2 §],
Begoña García Malaxechebarría[3],
Agnaldo J. Ferrari[4], Robson R. de Araújo[5]

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

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

[3] University of Murcia
30100 Murcia, SPAIN

[4] Department of Mathematics
São Paulo State University
Bauru, SP 17033-360, BRAZIL

[5] Federal University of São Paulo
Cubatão, SP 11533-360, BRAZIL

Abstract: Let p be an odd prime. Algebraic lattices of full diversity in dimension p are obtained from ramified cyclic extensions of degree p. The 3, 5, and 7-dimensional lattices are optimal with respect to sphere packing density and therefore are isometric to laminated lattices in those dimensions.

AMS Subject Classification: 11H31, 11R18, 11H50, 94B75
Key Words: cyclotomic fields; lattices; modulation diversity; packing density

Received: April 6, 2020

[§]Correspondence author

1. Introduction

In this work lattices mean discrete subgroups of n-dimensional Euclidean space. They have been considered in different applied areas, in particular, in coding/modulation theory and more recently in cryptography. They have been studied in several papers from different points of view [1, 3, 2, 7, 11, 12]. In digital communications, two lattice parameters of interest are the sphere packing density and the minimum product distance. This paper presents a construction method of algebraic lattices of optimal packing density and full diversity via totally real number fields of prime degree.

2. Lattices and number fields

This section briefly reviews the concepts from lattices and number fields that are required for the rest of the work. Readers interested in further details are referred to [5]. Let Λ be a full lattice in $\mathbb{R}^n$, that is, Λ is the set of all integral linear combinations of some basis of the vector space $\mathbb{R}^n$. Λ is said to be of full diversity [3] if for any $\mathbf{0} \neq (x_1, \ldots, x_n) \in \Lambda$, one has $x_i \neq 0$ for $i = 1, \ldots, n$.

Let $\mathfrak{r}$ denote half the minimal distance between (distinct) lattice points. By centering an n-dimensional sphere with radius $\mathfrak{r}$ at each lattice point, the sphere packing associated to Λ is obtained. The proportion of the space that is occupied by the spheres is called the sphere packing density of Λ and is denoted by $\Delta(\Lambda)$. For comparison purposes, a more used parameter is the center density of the packing, denoted by $\delta(\Lambda)$, which in turn equals $\Delta(\Lambda)$ divided by V_n, the volume of an n-dimensional sphere of radius 1.

Let $\mathbb{K}$ be a number field of degree n and signature $[r_1, r_2]$. The $\mathbb{Q}$-monomorphisms (or embeddings) of $\mathbb{K}$ into $\mathbb{C}$ whose images are contained in $\mathbb{R}$ are denoted by $\sigma_1, \ldots, \sigma_{r_1}$, and those whose images are not contained in $\mathbb{R}$ are denoted by $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$.

Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be any $\mathbb{Z}$-basis for $\mathcal{O}_\mathbb{K}$, the ring of integers of $\mathbb{K}$. The integer $d_\mathbb{K} = (\det(\sigma_j(\alpha_i))_{i,j=1}^n)^2$ is called the discriminant of $\mathbb{K}$. The trace of any element $x \in \mathcal{O}_\mathbb{K}$ is defined by $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x) = \sum_{i=1}^n \sigma_i(x)$. For any complex number z, let $\Re(z)$ and $\Im(z)$ denote, respectively, its real and imaginary parts. The canonical homomorphism $\sigma : \mathbb{K} \to \mathbb{R}^n$ is defined by

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1}(x)), \ldots, \Im(\sigma_{r_1+r_2}(x))),$$

for every $x \in \mathbb{K}$. If $\mathcal{M}$ is a $\mathbb{Z}$-submodule of $\mathbb{K}$ of rank n, then $\sigma(\mathcal{M})$ is an n-dimensional lattice in $\mathbb{R}^n$. If either $r_1 = 0$ or $r_2 = 0$, then the center density of $\sigma(\mathcal{M})$ is given by

$$\delta(\sigma(\mathcal{M})) = \frac{t^{n/2}}{2^n \cdot \sqrt{|d_{\mathbb{K}}|} \cdot [\mathcal{O}_{\mathbb{K}} : \mathcal{M}]}, \tag{1}$$

where $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$ denotes the index of $\mathcal{M}$ in $\mathcal{O}_{\mathbb{K}}$, and

$$t = c_k \min\left\{\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) \ : \ x \in \mathcal{M}, x \neq 0\right\} \tag{2}$$

with $c_k = 1$ or $\frac{1}{2}$ according to whether $r_2 = 0$ or $r_1 = 0$, respectively. The quantity $2^{-r_2} \cdot \sqrt{|d_{\mathbb{K}}|} \cdot [\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$ represents the volume of $\sigma(\mathcal{M})$.

3. Trace form of cyclic fields of odd prime degree

This section presents a construction of algebraic lattices using cyclic fields of degree p, where $p > 2$ is prime and ramified. Let $\mathbb{K}/\mathbb{Q}$ be a cyclic extension of degree p. From the Kronecker-Weber Theorem [10], there is a smallest positive integer n such that $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$; that integer is the conductor of $\mathbb{K}$. In this case, the discriminant of $\mathbb{K}$ is given by $d_{\mathbb{K}} = n^{p-1}$ [4, p.186].

Since p is ramified in $\mathbb{K}$, then $n = p^2 p_1 p_2 \cdots p_r$ for some $r \geq 0$, where the p_i are distinct prime numbers such that $p_i \equiv 1 \pmod{p}$, see [9], for example. From [8], if $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$, then

1. $\mathbb{K} = \mathbb{Q}(t)$.
2. $\mathcal{B} = \{1, \sigma(t), \cdots, \sigma^{p-1}(t)\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_{\mathbb{K}}$.

Theorem 1 ([6]). *Let $\mathbb{K}$ be a cyclic field of prime degree $p > 2$ and conductor n as above. If $x = a_0 + \sum_{i=1}^{p-1} a_i \sigma^i(t) \in \mathcal{O}_{\mathbb{K}}$, where $a_i \in \mathbb{Z}$, for $i = 0, 1, \ldots, p-1$, then*

$$\begin{aligned} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x^2) &= p a_0^2 + p p_1 \cdots p_r \left(-2 \sum_{1 \leq i < j \leq p-1} a_i a_j + (p-1) \sum_{i=1}^{p-1} a_i^2 \right) \\ &= p a_0^2 + p p_1 \cdots p_r \left(\sum_{i=1}^{p-1} a_i^2 + \sum_{1 \leq i < j \leq p-1} (a_i - a_j)^2 \right). \end{aligned}$$

4. Construction of algebraic lattices

Let $\mathbb{K}/\mathbb{Q}$ be a cyclic number field of odd prime degree p and conductor n as in Section 3. This section will present a lattice construction whose main ingredient is a suitably chosen $\mathbb{Z}$-submodule $\mathcal{M}$ of $\mathcal{O}_K$ of rank n. Since $\mathbb{K}$ is totally real, all the obtained lattices will be of full diversity. Their center densities will be calculated by the formula in (1). Recall that the parameter t therein is equal to the nonzero minimum of the trace form of $\mathbb{K}$ restricted to $\mathcal{M}$, see (2).

4.1. The laminated lattice Λ_3

In this section, let $\mathbb{K}$ be the cyclic field of degree $p = 3$ and conductor $n = 3^2$. The Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle$ is cyclic of order 3, $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_{3^2})/\mathbb{K}}(\zeta_{3^2})$, and $d_{\mathbb{K}} = 3^4$. Let $\mathcal{M}$ be the submodule of $\mathcal{O}_{\mathbb{K}}$ of rank 3 and index 6 given by

$$\begin{aligned}\mathcal{M} \;=\; &\{a_0 + a_1\sigma(t) + a_2\sigma^2(t) \in \mathcal{O}_{\mathbb{K}} : a_0, a_1, a_2 \in \mathbb{Z} \text{ and} \\ &\; a_0 + 2a_1 + 2a_2 \equiv 0 \pmod 6\}.\end{aligned}$$

If $\alpha \in \mathbb{K}$, then

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^2) = 3a_0^2 + 6a_1^2 - 6a_1a_2 + 6a_2^2.$$

It follows that $\min\{\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^2) : \alpha \in \mathcal{M}, \alpha \neq 0\} = 18$ is attained when $(a_0, a_1, a_2) = (2, -1, 0)$. Since the volume of $\sigma(\mathcal{M})$ equals $\sqrt{|d_{\mathbb{K}}|} \cdot [\mathcal{M} : \mathcal{O}_{\mathbb{K}}] = 3^2 \cdot 6 = 54$, one has

$$\delta(\sigma(\mathcal{M})) = \frac{(\sqrt{18}/2)^3}{54} = \frac{1}{4\sqrt{2}},$$

i.e., the center density of $\sigma(\mathcal{M})$ equals that of lattice Λ_3 [5, p. 15].

4.2. The laminated lattice Λ_5

In this section, let $\mathbb{K}$ be the number field of degree $p = 5$ and conductor $n = 5^2$. The Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle$ is cyclic of order 5, $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_{5^2})/\mathbb{K}}(\zeta_{5^2})$, and $d_{\mathbb{K}} = 5^8$. Let $\mathcal{M}$ be the submodule of $\mathcal{O}_{\mathbb{K}}$ of rank 5 and index 10 given by

$$\begin{aligned}\mathcal{M} \;=\; &\{a_0 + a_1\sigma(t) + a_2\sigma^2(t) + a_3\sigma^3(t) + a_4\sigma^4(t) \in \mathcal{O}_{\mathbb{K}} : a_0, \ldots, \\ &\; a_4 \in \mathbb{Z} \text{ and } a_0 + 4a_1 + 4a_2 + 4a_3 + 4a_4 \equiv 0 \pmod{10}\}.\end{aligned}$$

If $\alpha \in \mathbb{K}$, then

$$\begin{aligned}\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^2) \;=\; & 5 \cdot (a_0^2 + 4a_1^2 - 2a_1a_2 - 2a_1a_3 - 2a_1a_4 + 4a_2^2 \\ & -2a_2a_3 - 2a_2a_4 + 4a_3^2 - 2a_3a_4 + 4a_4^2).\end{aligned}$$

It follows that $\min\{\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^2) : \alpha \in \mathcal{M}\} = 50$ is attained when $a_0 = a_1 = a_2 = 0$, $a_3 = -1$ and $a_4 = 1$. Since the volume of $\sigma(\mathcal{M})$ equals $\sqrt{|d_{\mathbb{K}}|} \cdot [\mathcal{M} : \mathcal{O}_{\mathbb{K}}] = 5^4 \cdot 10 = 5^5 \cdot 2$, one has

$$\delta(\sigma(\mathcal{M})) = \frac{(\sqrt{50}/2)^5}{5^5 \cdot 2} = \frac{1}{8\sqrt{2}},$$

i.e., the center density of $\sigma(\mathcal{M})$ equals that of lattice Λ_5 [5, p.15].

4.3. The laminated lattice Λ_7

In this section, let $\mathbb{K}$ be the number field of degree $p = 7$ and conductor $n = 7^2$. The Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle \sigma \rangle$ is cyclic of order 7, $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_{7^2})/\mathbb{K}}(\zeta_{7^2})$, and $d_{\mathbb{K}} = 7^{12}$. Let $\mathcal{M}$ be the submodule of $\mathcal{O}_{\mathbb{K}}$ of rank 7 and index 112 given by

$$\mathcal{M} = \begin{cases} a_0 + a_1\sigma(t) + a_2\sigma^2(t) + \cdots + a_6\sigma^6(t) \in \mathcal{O}_{\mathbb{K}} : \\ a_0, a_1, a_2, \ldots, a_6 \in \mathbb{Z}, \\ a_0 + 6a_1 + 6a_2 + 6a_3 + 6a_4 + 6a_5 + 6a_6 \equiv 0 \pmod{14}, \\ a_1 + a_5 + a_6 \equiv 0 \pmod{2}, \\ a_2 + a_4 + a_6 \equiv 0 \pmod{2}, \text{ and} \\ a_3 + a_4 + a_5 + a_6 \equiv 0 \pmod{2}. \end{cases}$$

If $\alpha \in \mathbb{K}$, then

$$\begin{aligned} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^2) = \; & 7 \cdot (a_0^2 + 6a_1^2 - 2a_1a_2 - 2a_1a_3 - 2a_1a_4 - 2a_1a_5 \\ & -2a_1a_6 + 6a_2^2 - 2a_2a_3 - 2a_2a_4 - 2a_2a_5 - 2a_2a_6 \\ & +6a_3^2 - 2a_3a_4 - 2a_3a_5 - 2a_3a_6 + 6a_4^2 - 2a_4a_5 \\ & -2a_4a_6 + 6a_5^2 - 2a_5a_6 + 6a_6^2). \end{aligned}$$

It follows that $\min\{\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^2) : \alpha \in \mathcal{M}\} = 196$ is attained when $a_0 = a_6 = 2$ and $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Since the volume of $\sigma(\mathcal{M})$ equals $\sqrt{|d_{\mathbb{K}}|} \cdot [\mathcal{M} : \mathcal{O}_{\mathbb{K}}] = 7^6 \cdot 112 = 2^4 \cdot 7^7$, one has

$$\delta(\sigma(\mathcal{M})) = \frac{(\sqrt{196}/2)^7}{2^4 \cdot 7^7} = \frac{1}{16},$$

i.e., the center density of $\sigma(\mathcal{M})$ equals that of lattice Λ_7 [5, p. 15].

5. Conclusion

A method for constructing laminated lattices Λ_p from cyclic fields of odd prime degree p and conductor p^2, where p is ramified, was presented. Explicit numerical examples were given for $p = 3, 5$, and 7. All the obtained lattices have maximal diversity; however, the determination of their exact minimum product distances is left for future research.

6. Acknowledgment

This work was supported by CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico), Brazil, 429346/2018-2 and FAPESP (São Paulo Research Foundation) 2013/25977-7.

References

[1] A. A. Andrade, C. Alves and T. B. Carlos, Rotated lattices via the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$, *Int. J. Appl. Math.*, **19** (2006), 321–331.

[2] A. A. Andrade and J. C. Interlando, Construction of even-dimensional lattices of full diversity, *Int. J. Appl. Math.*, **32**, No 2 (2019), 325–332; doi: 10.12732/ijam.v32i2.12.

[3] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, Algebraic lattice constellations: Bounds on performance, *IEEE Trans. Inform. Theory*, **52** (2006), 319–327.

[4] P. E. Conner and R. Perlis, *A Survey of Trace Forms of Algebraic Number Fields*, World Scientific Publishing Co Pte Ltd., Singapore (1984).

[5] J. H. Conway, N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*, 3rd Ed., Springer-Verlag, New York (1999).

[6] R. R. de Araujo, A. C. M. M. Chagas, A. A. Andrade and T. P. Nóbrega Neto, Trace form associated to cyclic number fields of ramified odd prime degree, *J. Algebra App.*, (2019), Art. 2050080.

[7] J. C. Interlando, J. O. D. Lopes and T. P. N. Neto, A new number field construction of the D_4-lattice, *Int. J. Appl. Math.*, **31**, No 2 (2018), 299–305; doi: 10.12732/ijam.v31i2.11.

[8] G. Lettl, The ring of integers of an Abelian number field, *J. Reine Angew. Math.*, **404** (1990), 162–170.

[9] B. K. Spearman and K. S. Wiliams, The discriminant of a cyclic field of odd prime degree, *Rocky Mountain J. Math*, **33** (2003), 1001–1122.

[10] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd Ed., Springer-Verlag, New York (1997).

[11] C. C. T. Watanabe, J. C. Belfiore, E. D. Carvalho and J. V. Filho, E_8-lattice via the cyclotomic field $\mathbb{Q}(\zeta_{24})$, *Int. J. Appl. Math.*, **31**, No 1 (2018), 63–71; doi: 10.12732/ijam.v31i1.6.

[12] C. C. T. Watanabe, J. C. Belfiore, E. D. Carvalho and J. V. Filho, Construction of nested real ideal lattices for interference channel coding, *Int. J. Appl. Math.*, **32**, No 2 (2019), 295–323; doi: 10.12732/ijam.v32i2.11.