International Journal of Applied Mathematics

Volume 30 No. 5 2017, 401-408
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v30i5.4

FOUR-DIMENSIONAL LATTICES FROM $\mathbb{Q}(\sqrt{2}, \sqrt{5})$

J. Carmelo Interlando[1 §], Trajano Pires da Nóbrega Neto[2]
José Valter Lopes Nunes[3], José Othon Dantas Lopes[4]

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

[4]Department of Mathematics
Federal University of Ceará
Fortaleza, CE 60455-900, BRAZIL

Abstract: Four-dimensional lattices with block circulant generator matrices are constructed from submodules of the ring of integers of the totally real number field $\mathbb{Q}(\sqrt{2}, \sqrt{5})$. The obtained lattices are of full diversity and their sphere packing densities are the highest known for the given relative minimum product distances.

AMS Subject Classification: 11H06, 11H31, 11R16, 94A14
Key Words: lattices, number fields, sphere packings, modulation, minimum product distance

1. Introduction

Lattices occupy a prominent position in both pure and applied mathematics: On the theory side, they are the central entities in the geometry of numbers; on

Received: August 21, 2017

§Correspondence author

the application side, they have been instrumental in the design of signal sets for efficient data transmission [4]. For a given positive integer n, an n-dimensional lattice Λ is a discrete subgroup of $\mathbb{R}^n$ of rank n; alternatively, Λ can be described as the set of all integral linear combinations of a set of n linearly independent vectors in $\mathbb{R}^n$ (in passing, that set is referred to as a basis of the lattice).

By regarding the points of Λ as the centers of identical spheres of radii equal to half the minimum Euclidean distance between those points, one obtains an arrangement of spheres known as the sphere packing associated to Λ. The density of the packing, that is, the fraction of space occupied by the spheres, is one of the most important parameters associated to Λ. Finding dense lattice packings is a famous problem which remains open except in dimensions $n = 1, 2, \ldots, 8$, and 24, see [4] for its rich history, and [3] and [9] for recent developments.

Lattices of high packing density are suitable for data transmission over a Gaussian channel, whereas lattices with a high minimum product distance[1] are suitable for data transmission over the Rayleigh fading channel, see [2] and [4]. Lattices possessing both of those features are of interest because they allow the associated signal sets to be used at the same time over both channels [2]. Number fields have proved to be a useful tool in obtaining lattices with those properties, see [1], [2], and [4]. In particular, totally real number fields can be used to produce lattices of high minimum product distance [1].

Having the above in mind, the focus of the present work is on the number field $F = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. The motivation for its choice, which will become clear in the sections, is that among all totally real biquadratic number fields, F possesses the smallest discriminant in absolute value [5]. Four-dimensional lattices featuring high relative minimum product distances and packing densities will be obtained from submodules of $\mathfrak{O}_F$, the ring of integers of F.

2. Background on Algebraic Lattices

In this section the definitions and properties of lattices needed for this work will be briefly reviewed. For further details, the reader is referred to either [4] or [8]. Let Λ be an n-dimensional lattice. The minimum of Λ, $\min \Lambda$, is the minimum of the squared Euclidean norms of the nonzero vectors of Λ. The minimum distance of Λ, $d_{\min}(\Lambda)$, is the square root of $\min \Lambda$. The packing radius of Λ is

[1]The product distance of a nonzero lattice point is defined as the absolute value of the product of the point coordinates.

the real number

$$\rho = \frac{d_{\min}(\Lambda)}{2}.$$

The volume of Λ, denoted by $\operatorname{vol}\Lambda$, is defined as the volume of the parallelotope determined by any basis of the lattice. The center density of Λ is defined as $\delta(\Lambda) = \rho^n/\operatorname{vol}\Lambda$, see [4, Chap. 1].

For the purposes of this work, let K be a totally real number field of degree n whose embeddings ($\mathbb{Q}$-monomorphisms of K into $\mathbb{C}$) are $\sigma_1, \sigma_2, \ldots, \sigma_n$. If $\mathfrak{O}_K$ is the ring of integers of K, then $\sigma_K : \mathfrak{O}_K \to \mathbb{R}^n$, given by $\sigma_K(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x))$, is the canonical embedding of K into $\mathbb{R}^n$. If $\mathcal{M}$ is a submodule of $\mathfrak{O}_K$ of rank n, then $\sigma_K(\mathcal{M})$ is an n-dimensional algebraic lattice whose minimum and volume are given, respectively, by

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

where $\operatorname{Tr}_{K/\mathbb{Q}}(\cdot)$ denotes the field trace and $\operatorname{Disc}(K)$ denotes the discriminant of K. Therefore, the center density of Λ is given by

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

An n-dimensional lattice Λ is said to have full diversity [1] if for every $y = (y_1, \ldots, y_n)$ in Λ with $y \neq 0$, one has $y_i \neq 0$ for $i = 1, \ldots, n$. In that case, the minimum product distance of Λ is defined as

$$d_{p,\min}(\Lambda) = \min_{\substack{y\in\Lambda\\ y\neq 0}} \prod_{i=1}^{n} |y_i|.$$

Finally, let K be a totally real number field of degree n and $\mathcal{M}$ a submodule of $\mathfrak{O}_K$ of rank n. Then $\Lambda = \sigma_K(\mathcal{M})$ has full diversity and its minimum product distance equals

$$d_{p,\min}(\Lambda) = \min_{\substack{y\in\Lambda\\ y\neq 0}} |\mathrm{N}_{K/\mathbb{Q}}(y)|,$$

where $\mathrm{N}_{K/\mathbb{Q}}(\cdot)$ denotes the field norm, see [6, Proposition 3.2]. Finally, the relative minimum product distance of Λ, viz.,

$$d_{p,\mathrm{rel}}(\Lambda) = \left(\frac{d_{p,\min}(\Lambda)}{d_{\min}(\Lambda)}\right)^{1/n},$$

is the standard parameter used for comparison purposes.

3. Lattices from $\mathbb{Q}(\sqrt{2},\sqrt{5})$

With the objective of maximizing the center density, in view of (1), we will work with fields of small discriminant. Among all totally real biquadratic fields, the one with smallest discriminant in absolute value is $F=\mathbb{Q}(\sqrt{2},\sqrt{5})$. In particular, $\mathrm{Disc}(F)=2^6\cdot 5^2$. An integral basis for F is $\{1,\alpha_1,\alpha_2,\alpha_3\}=\{1,\sqrt{2},\frac{1+\sqrt{5}}{2},\frac{\sqrt{2}+\sqrt{10}}{2}\}$, see [7, Exercise 42, pp. 51–52]. The automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{5})$ are:

$$\mathrm{id}:\left\{\begin{array}{ccc}\sqrt{2}&\mapsto&\sqrt{2}\\ \sqrt{5}&\mapsto&\sqrt{5}\end{array}\right. \quad \sigma:\left\{\begin{array}{ccc}\sqrt{2}&\mapsto&-\sqrt{2}\\ \sqrt{5}&\mapsto&\sqrt{5}\end{array}\right.,$$

$$\tau:\left\{\begin{array}{ccc}\sqrt{2}&\mapsto&\sqrt{2}\\ \sqrt{5}&\mapsto&-\sqrt{5}\end{array}\right. \quad \sigma\tau:\left\{\begin{array}{ccc}\sqrt{2}&\mapsto&-\sqrt{2}\\ \sqrt{5}&\mapsto&-\sqrt{5}\end{array}\right..$$

Let $u=u_0+u_1\cdot\alpha_1+u_2\cdot\alpha_2+u_3\cdot\alpha_3$ be a given arbitrary element of $\mathfrak{O}_F$, where u_0,u_1,u_2,u_3 are rational integers, and let $\mathcal{M}$ be the submodule of $\mathfrak{O}_F$ with basis $\{u,\sigma(u),\tau(u),\sigma\tau(u)\}$, where:

$$\begin{aligned}\sigma(u)&=u_0-u_1\cdot\alpha_1+u_2\cdot\alpha_2-u_3\cdot\alpha_3,\\ \tau(u)&=(u_0+u_2)+(u_1+u_3)\cdot\alpha_1-u_2\cdot\alpha_2-u_3\cdot\alpha_3,\\ \sigma\tau(u)&=(u_0+u_2)-(u_1+u_3)\cdot\alpha_1-u_2\cdot\alpha_2+u_3\cdot\alpha_3.\end{aligned}$$

Let $\sigma_F:F\to\mathbb{R}^4$ be the canonical embedding of F. The lattice $\Lambda=\sigma_F(\mathcal{M})$ is generated by the rows of

$$G=\begin{bmatrix}u&\sigma(u)&\tau(u)&\sigma\tau(u)\\ \sigma(u)&u&\sigma\tau(u)&\tau(u)\\ \tau(u)&\sigma\tau(u)&u&\sigma(u)\\ \sigma\tau(u)&\tau(u)&\sigma(u)&u\end{bmatrix}. \tag{2}$$

We can write the latter matrix as $G=A\cdot B$ where

$$A=\begin{bmatrix}u_0&u_1&u_2&u_3\\ u_0&-u_1&u_2&-u_3\\ u_0+u_2&u_1+u_3&-u_2&-u_3\\ u_0+u_2&-u_1-u_3&-u_2&u_3\end{bmatrix}$$

and

$$B=\begin{bmatrix}\alpha_1&\alpha_1&\alpha_1&\alpha_1\\ \alpha_2&\sigma(\alpha_2)&\tau(\alpha_2)&\sigma\tau(\alpha_2)\\ \alpha_3&\sigma(\alpha_3)&\tau(\alpha_3)&\sigma\tau(\alpha_3)\\ \alpha_4&\sigma(\alpha_4)&\tau(\alpha_4)&\sigma\tau(\alpha_4)\end{bmatrix}.$$

Since $\det A = 4\cdot(2u_0+u_2)\cdot(2u_1+u_3)\cdot u_2\cdot u_3$, it follows that the volume of Λ equals

$$\operatorname{vol}\Lambda = |\det G| = |\det A\cdot\sqrt{\operatorname{Disc}(F)}| = 2^5\cdot 5\cdot|(2u_0+u_2)\cdot(2u_1+u_3)\cdot u_2\cdot u_3|.$$

Therefore, Λ is of full rank if and only if $u_2\neq 0, u_2\neq -2u_0, u_3\neq 0$, and $u_3\neq -2u_1$.

Now we turn to the trace form, i.e., $\operatorname{Tr}_{F/\mathbb{Q}}(x^2)|_{\mathcal{M}}$ where

$$x = x_0\cdot u + x_1\cdot\sigma(u) + x_2\cdot\tau(u) + x_3\sigma\tau(u)$$

is an arbitrary element of $\mathcal{M}$ with x_0,x_1,x_2,x_3 in $\mathbb{Z}$. We have

$$\begin{aligned}\operatorname{Tr}_{F/\mathbb{Q}}(x^2) &= t_0\cdot(x_0^2+x_1^2+x_2^2+x_3^2)+2\cdot t_1\cdot(x_0x_1+x_2x_3)\\ &\quad +2\cdot t_2\cdot(x_0x_2+x_1x_3)+2\cdot t_3\cdot(x_0x_3+x_1x_2),\end{aligned}\tag{3}$$

where:

$$\begin{aligned}t_0=\operatorname{Tr}_{F/\mathbb{Q}}(u^2) &= 4u_0^2+4u_0u_2+6u_2^2+8u_1^2+8u_1u_3+12u_3^2\\ &= (2u_0+u_2)^2+2\cdot(2u_1+u_3)^2+5u_2^2+10u_3^2,\\ t_1=\operatorname{Tr}_{F/\mathbb{Q}}(u\cdot\sigma(u)) &= 4u_0^2+4u_0u_2+6u_2^2-8u_1^2-8u_1u_3-12u_3^2\\ &= (2u_0+u_2)^2-2\cdot(2u_1+u_3)^2+5u_2^2-10u_3^2,\\ t_2=\operatorname{Tr}_{F/\mathbb{Q}}(u\cdot\tau(u)) &= 4u_0^2+4u_0u_2-4u_2^2+8u_1^2+8u_1u_3-8u_3^2\\ &= (2u_0+u_2)^2+2\cdot(2u_1+u_3)^2-5u_2^2-10u_3^2,\\ t_3=\operatorname{Tr}_{F/\mathbb{Q}}(u\cdot\sigma\tau(u)) &= 4u_0^2+4u_0u_2-4u_2^2-8u_1^2-8u_1u_3+8u_3^2\\ &= (2u_0+u_2)^2-2\cdot(2u_1+u_3)^2-5u_2^2+10u_3^2.\end{aligned}$$

Alternatively,

$$\begin{aligned}\operatorname{Tr}_{F/\mathbb{Q}}(x^2) &= y_1^2(z_1+z_2)^2+5y_2^2(z_1-z_2)^2+\\ &\quad 2y_3^2(w_1+w_2)^2+10y_4^2(w_1-w_2)^2,\end{aligned}$$

where

$$\begin{cases} z_1 = x_0+x_1\\ z_2 = x_2+x_3\\ w_1 = x_0-x_1\\ w_2 = x_2-x_3\end{cases}\qquad\text{and}\qquad\begin{cases} y_1 = 2u_0+u_2\\ y_2 = u_2\\ y_3 = 2u_1+u_3\\ y_4 = u_3\end{cases}.$$

With this notation, it follows that

$$\operatorname{vol}\Lambda = 2^5\cdot 5\cdot|y_1y_2y_3y_4|.$$

3.1. New Four-Dimensional Lattices

The generator matrix in (2) has the form

$$M = \left[\begin{array}{cc|cc} a & b & c & d \\ b & a & d & c \\ \hline c & d & a & b \\ d & c & b & a \end{array}\right],$$

with a, b, c, d in $\mathbb{R}$, which characterizes it as a block circulant matrix with circulant blocks. For M of full rank, a lower bound on the center density of four-dimensional lattices generated by M equals $\delta^* = \frac{1}{4\sqrt{5}} = 0.111803$, and this is attained when $a = b = c = 1$ and $d = 2 - \sqrt{5}$. It seems that δ^* is an upper bound as well, however we have not been able to prove this so far. Nonetheless, we can still construct lattices with better parameters (center density and relative minimum product distance) than what is presently known as follows.

Notation as before, by choosing $u \in \mathcal{M}$ such that three of the quantities $u, \sigma(u), \tau(u)$, and $\sigma\tau(u)$ are close to k and the other is close to $k(2-\sqrt{5})$ for k a nonzero constant, one can obtain lattices whose center densities are close to δ^*. With this in mind, let

$$u_0 = 34, u_1 = 0, u_2 = 55, u_3 = 87,$$

so $u = u_0 + u_1\alpha_2 + u_2\alpha_3 + u_3\alpha_4$. Let $\mathcal{M}$ be the submodule of $\mathfrak{O}_F$ generated by $u, \sigma(u), \tau(u)$, and $\sigma\tau(u)$. The parameters of $\sigma_F(\mathcal{M})$ are:

$$\begin{cases} \text{minimum} & = & 121016 = 2^3 \cdot 7 \cdot 2161, \\ & & \text{attained at } x^* = (1,1,0,0); \\ \text{volume} & = & 8192685600 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 11 \cdot 29^2 \cdot 41; \\ \text{center density} & = & \frac{7^2 \cdot 2161^2}{2^3 \cdot 3^3 \cdot 5^2 \cdot 11 \cdot 29^2 \cdot 41} = 0.111722. \end{cases}$$

The minimum product distance of $\sigma_F(\mathcal{M})$ is equal to

$$\mathrm{N}_{F/\mathbb{Q}}(u + \sigma(u)) = 16.$$

Thus,

$$d_{p,\mathrm{rel}}(\sigma_F(\mathcal{M})) = \left(\frac{16}{\sqrt{121016}}\right)^{1/4} = 0.463099.$$

For comparison purposes, the center density and relative minimum product distance of the lattice $\mathbb{Z}^4$ are equal to 0.0625 and 0.385553, respectively; the

center density and relative minimum product distance of the lattice D_4 are equal to 0.125 and 0.324210, respectively, see [6, Table 2, p. 2404].

As a second example, let

$$u_0 = -13551, u_1 = 1974, u_2 = 4517, u_3 = 3194,$$

and $\mathcal{M}$ the submodule of $\mathfrak{O}_F$ generated by $u, \sigma(u), \tau(u)$, and $\sigma\tau(u)$. The minimum of $\sigma_F(\mathcal{M})$ is equal to 816130752 and it occurs at $x^* = (1, -1, 0, 0)$. The volume of $\sigma_F(\mathcal{M})$ is equal to 372344485105097600, hence

$$\delta(\sigma_F(\mathcal{M})) = \frac{325229201347698}{2908941289883575} = 0.111803.$$

Finally, the minimum product distance of $\sigma_F(\mathcal{M})$ is equal to

$$\mathrm{N}_{F/\mathbb{Q}}(u - \sigma(u)) = 1024.$$

Thus,

$$d_{p,\mathrm{rel}}(\sigma_F(\mathcal{M})) = \left(\frac{1024}{\sqrt{816130752}}\right)^{1/4} = 0.435115,$$

which also compare favorably with previous results.

References

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

[2] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, Good lattice constellations for both the Rayleigh fading and Gaussian channels, *IEEE Trans. Inform. Theory*, **42** (1996), 502–518.

[3] H. Cohn, A. Kumar, S.D. Miller, D. Radchenko, and M. Viazovska, The sphere packing problem in dimension 24, *arXiv*:1603.06518.

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

[5] H.J. Godwin, Real quartic fields with small discriminant, *J. London Math. Soc.*, **31** (1956), 478–485.

[6] G.C. Jorge, A.J. Ferrari, and S.I.R. Costa, Rotated D_n lattices, *J. Number Theory*, **132** (2012), 2397–2406.

[7] D. Marcus, *Number Fields*, Springer-Verlag (1977).

[8] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 3rd Edition, AK Peters Ltd. (2002).

[9] M.S. Viazovska, The sphere packing problem in dimension 8, *Ann. of Math.*, **185** (2017), 991–1015.