Families of Lattices from Subfields of $\mathbb{Q}(\zeta_{pq})$ and Their Applications to Rayleigh Fading Channels

Trajano Pires da Nóbrega Neto, André Luiz Flores, and J. Carmelo Interlando
E-mail: (trajano, carmelo)@mat.ibilce.unesp.br
Departamento de Matemática
IBILCE - UNESP
Rua Cristóvão Colombo, 2265
15054-000, São José do Rio Preto, SP, BRAZIL

Abstract— **We provide a new method to evaluate the center density of ideals in the ring of algebraic integers of subfields of $\mathbb{Q}(\zeta_{pq})$, where p and q are distinct prime numbers. This method allows us to reproduce rotated versions of known dense lattices in some dimensions. For example, we obtain lattice E_8 from several fields $\mathbb{Q}(\zeta_{pq})$. Because of their high diversity, signal constellations constructed from these dense lattices perform well on both Gaussian and Rayleigh fading channels. One application of these constellations is in mobile communications, where one single modulation/demodulation device can be used to communicate over both terrestrial and satellite links.**

Keywords—**Number fields, quadratic forms, cyclotomic fields, algebraic lattices, signal sets, Gaussian and fading channels, diversity.**

I. Introduction

The theory of algebraic lattices has shown to be extremely useful in Information Theory. Signal sets from dense lattices perform well over an additive white Gaussian channel (AWGN). In fact, Conway and Sloane [4] have shown that lattices satisfying the Minkowski bound are equivalent to codes which attain channel capacity. This establishes a link between sphere-packing and Information Theory.

In [7], Giraud and Belfiori proposed a technique for constructing signal sets suitable for the Rayleigh fading channel. The basic idea was to use lattice rotations to increase diversity, that is, the number of different values in the components of any two distinct points of the constellation. In [3], Boutros *et al.* constructed rotated versions of lattices D_4, K_{12}, and Λ_6 via ideals of $\mathbb{Q}(\zeta_n)$, for $n = 8, 21$ and 40, respectively. The principal purpose of the work was to obtain constellations having good performance in both AWGN and Rayleigh fading channels.

In this paper, starting from suitable ideals in subfields of $\mathbb{Q}(\zeta_{pq})$, we construct new rotated versions of dense lattices, for example, Λ_{24}, K_{12}, and E_8. We conjecture the existence of a lattice in dimension 28 with center density equal to 1. As in [3], the lattices presented here perform well over Gaussian and fading channels. This is particularly useful when transmitting information over terrestrial and satellite links. The same modulation/demodulation device can be used to communicate over them both.

II. Preliminaries

Let K be a number field of degree m, and let $\sigma_1, \ldots, \sigma_m$ be the $\mathbb{Q}$-monomorphisms of K into $\mathbb{C}$, ordered in such a way that σ_i is real for $1 \leq i \leq r_1$ and σ_{j+r_2} is the complex conjugate of σ_j for $r_1 + 1 \leq j \leq r_1 + r_2$. Denoting by $\Re(z)$ and $\Im(z)$, the real and imaginary part of the complex number z, respectively, the canonical homomorphism $\sigma : K \to \mathbb{R}^m$ is the group homomorphism given by

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

Let $\mathcal{O}_K$ be the ring of algebraic integers of K, and let M be a submodule of $\mathcal{O}_K$ of index t. The set $\sigma(M)$ is a rank-m lattice in $\mathbb{R}^m$ whose volume is

$$v(\sigma(M)) = t \cdot 2^{-r_2} |\Delta_K|^{1/2}, \tag{1}$$

where Δ_K is the discriminant of K. Lattice $\sigma(M)$ is the geometrical representation of M. Given $x \in M$, we can compute distances in $\sigma(M) \subseteq \mathbb{R}^m$ by

$$|\sigma(x)|^2 = c_K \operatorname{Tr}_{K/\mathbb{Q}}(x\overline{x}), \tag{2}$$

where $c_K = 1$ if K is totally real, $c_K = 1/2$ if K is totally complex, and $\overline{x}$ is the complex conjugate of x. The parameter $\rho = \frac{1}{2} \min\{|\sigma(x)| \; ; \; x \in M, \; x \neq 0\}$ is the packing radius of $\sigma(M)$.

An ideal $\mathfrak{a} \neq \{0\}$ of $\mathcal{O}_K$ is a submodule of $\mathcal{O}_K$ of index $N(\mathfrak{a}) = \operatorname{card}(\mathcal{O}_K/\mathfrak{a})$, the norm of $\mathfrak{a}$. Thus, the center density of $\sigma(\mathfrak{a})$ is given by

$$\delta(\sigma(\mathfrak{a})) = \frac{2^{r_2} \rho^n}{|\Delta_K|^{1/2} N(\mathfrak{a})}. \tag{3}$$

III. The Quadratic Form

For each positive integer n, let Q_n be the the quadratic form given by

$$Q_n(X_1, \ldots, X_n) = \sum_{i=1}^{n} X_i^2 + \sum_{1 \leq i < j \leq n} (X_i - X_j)^2.$$

Q_p is the quadratic form associated to $\mathbb{Q}(\zeta_p)$ where p is a prime. This can be seen as follows: Given an element $x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathbb{Z}[\zeta_p]$, we can write

$$x\overline{x} = A_0 + \sum_{i=1}^{p-2} A_i \alpha_i,$$

where $\alpha_i = \zeta_p^i + \zeta_p^{-i}, \; i = 1, \ldots, p-2$, and $A_j = \sum_{i=0}^{p-2-j} a_i a_{i+j}, \; j = 0, \ldots, p-2$. The minimal polynomial of ζ_p over $\mathbb{Q}$ is $X^{p-1} + X^{p-2} + \cdots + X + 1$. Hence,

$\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = -1$ and for $i > 0$, $\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha_i) = -2$. Therefore,

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(x\overline{x}) = \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(A_0 + \sum_{i=1}^{p-2} A_i\alpha_i) =$$

$$(p-1)A_0 + \sum_{i=1}^{p-2} A_i \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha_i) = (p-1)A_0 - 2\sum_{i=1}^{p-2} A_i =$$

$$\sum_{i=0}^{p-2} a_i^2 + \sum_{0\le i<j\le p-2} (a_i - a_j)^2.$$

By identifying the element x with the corresponding $(p-1)$-tuple $\underline{x} = (a_0, \ldots, a_{p-2})$, we get

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(x\overline{x}) = Q_{p-1}(\underline{x}).$$

Let $K \subseteq L$ be number fields with $t = [L : K]$ and σ_K and σ_L the canonical homomorphisms of K and L, respectively. Further, let $x \in K$ and c_K and c_L be quantities taking values in the set $\{1/2, 1\}$, as the field under question is real or complex. Then

$$|\sigma_L(x)|^2 = c_L \mathrm{Tr}_{L/\mathbb{Q}}(x\overline{x}) = t c_L \mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}),$$

which implies

$$|\sigma_K(x)|^2 = \frac{c_K}{t c_L} \mid \sigma_L(x) \mid^2 .$$

Let K be a subfield of $\mathbb{Q}(\zeta_p)$ of index t and H, the group of the K-automorphisms of $\mathbb{Q}(\zeta_p)$. Then $K = \mathbb{Q}(\alpha)$, where $\alpha = \sum_{\sigma\in H} \sigma(\zeta_p)$.

If we let $u = (p-1)/t$, then from the symmetry of Q it follows that

$$|\sigma_K(x)|^2 = c_K \mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}) = \frac{c_K}{t}\mathrm{Tr}_{L/\mathbb{Q}}(x\overline{x}) =$$

$$\frac{c_K}{t} Q_{p-1,1}(a_0, \ldots, a_0, \ldots, a_u, \ldots, a_u),$$

where each a_i appears repeated t times. Hence,

$$|\sigma_K(x)|^2 = c_K(a_0^2 + \cdots + a_{u-1}^2 + t \cdot \sum_{0\le i<j\le u-1} (a_i - a_j)^2) =$$

$$Q_{u,t}(a_0, \ldots, a_{u-1}).$$

Let $K_1 \subset \mathbb{Q}(\zeta_p)$, $K_2 \subset \mathbb{Q}(\zeta_q)$, $u = [K_1 : \mathbb{Q}]$, $v = [K_2 : \mathbb{Q}]$, $t_1 = (p-1)/u$, and $t_2 = (q-1)/v$. Further, let $\{\alpha_1, \ldots, \alpha_u\}$ and $\{\beta_1, \ldots, \beta_v\}$ be integral bases for $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$, respectively, and

$$x = \sum_{j=1}^{v}\sum_{i=1}^{u} a_{ij}\alpha_i\beta_j = \sum_{j=1}^{v} x_j\beta_j \ \in K_1K_2,$$

where $x_j = \sum_{i=1}^{u} a_{ij}\alpha_i$. Then the quadratic form associated to K_1K_2 can be written as:

$$\mathrm{Tr}_{K_1K_2/\mathbb{Q}}(x\overline{x}) = Q_{v,t2}(Q_{u,t1}(x_1), Q_{u,t1}(x_2), \ldots, Q_{u,t1}(x_v)).$$

IV. Decomposition in $\mathbb{Q}(\zeta_{pq})$

Let $L = \mathbb{Q}(\zeta_{pq})$ and $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_L$ above $q\mathbb{Z}$. As we saw in Section III, its decomposition group depends only on $\mathfrak{q}$. In this way, given a subfield K of L, we denote the decomposition group of a prime ideal of $\mathcal{O}_L$ over $\mathfrak{q}$ by $\mathcal{D}_K(q)$.

When complex conjugation does not belong to the decomposition group $\mathcal{D}_L(q)$, there exists an ideal $\mathfrak{I}$ of $\mathcal{O}_L$ such that the factorization of $\mathfrak{q}\mathcal{O}_L$ in ideals have the form

$$\mathfrak{q}\mathcal{O}_L = (\mathfrak{I}\overline{\mathfrak{I}})^{q-1}.$$

Such property has consequences which will be described shortly. However, first we need the following two results:

Theorem 1: If θ is the complex conjugation, then $\theta \in \mathcal{D}_L(q)$ if and only if $\theta \in \mathcal{D}_K(q)$.

Proof: Let $\sigma_s \in \mathcal{D}_K(q)$ be defined by $\sigma_s(\zeta_p) = \zeta_p^s$. For each $\sigma_s \in \mathcal{D}_K(q)$, there are $q-1$ extensions $\sigma_{s,i}$ of $\mathcal{D}_L(q)$. Each $\sigma_{s,i}$ is defined by its value in ζ_{pq} . Let u and v be such that $1 = pu + qv$. Hence,

$$\sigma_{s,i}(\zeta_{pq}) = \sigma_{s,i}(\zeta_{pq}^{pu+qv}) = \sigma_{s,i}(\zeta_{pq}^{pu}) \cdot \sigma_{s,i}(\zeta_{pq}^{qv}) =$$

$$\sigma_{s,i}(\zeta_q^u) \cdot \sigma_{s,i}(\zeta_p^v) = \zeta_q^{ui} \cdot \zeta_p^{sv} = \zeta_{pq}^{pui+qsv}.$$

Then $\theta \in \mathcal{D}_L(q)$ if and only if there exist i and s such that $pui + qsv \equiv -1 \pmod{pq}$, which is equivalent to

$$\begin{cases} pui + qsv \equiv -1 \pmod{p} \\ pui + qsv \equiv -1 \pmod{q}. \end{cases}$$

The second condition always holds true since i can assume any nonzero value modulo q. The first one is equivalent to $\theta \in \mathcal{D}_K(p)$, which concludes the proof. □

Corollary 1: $\theta \in \mathcal{D}_L(q)$ if and only if $\mathrm{Ord}_p(q) \equiv 0 \pmod 2$, where $\mathrm{Ord}_m(n)$ is the order of n modulo m, when $(m, n) = 1$.

Proof: Recall that $\mathrm{card}(\mathcal{D}_K(q)) = \mathrm{Ord}_p(q)$. Then if $\theta \in \mathcal{D}_K(q)$,

$$2 \mid \mathrm{card}(\mathcal{D}_K(q)) = \mathrm{Ord}_p(q).$$

For the converse, suppose $\mathrm{Ord}_p(q) \equiv 0 \pmod 2$. Since $\mathcal{D}_K(q)$ is cyclic of an even order, it follows that $\{-1, 1\}$ is the only subgroup of order 2 of these groups. □

When p and q satisfy the condition $\mathrm{Ord}_p(q) \equiv \mathrm{Ord}_q(p) \equiv 1 \pmod 2$, the following decompositions in prime ideals

$$p\mathcal{O}_L = (\mathfrak{p}_1 \ldots \mathfrak{p}_r \overline{\mathfrak{p}_1 \ldots \mathfrak{p}_r})^{p-1} \quad \text{and}$$

$$q\mathcal{O}_L = (\mathfrak{q}_1 \ldots \mathfrak{q}_s \overline{\mathfrak{q}_1 \ldots \mathfrak{q}_s})^{q-1} \tag{4}$$

hold true in $\mathbb{Z}[\zeta_{pq}]$. We will be particularly interested in the ideal

$$\mathfrak{I} = \mathfrak{p}_1 \ldots \mathfrak{p}_r \mathfrak{q}_1 \ldots \mathfrak{q}_s. \tag{5}$$

V. Algebraic Constructions

A. Construction A - Dimension 24

Here we present a technique to obtain lattice Λ_{24} which is simpler than the one presented in [5]. In $\mathbb{Z}[\zeta_{39}]$, there are four prime ideals above 3 and two prime ideals above 13, and therefore the decompositions in prime ideals are

$$3\mathbb{Z}[\zeta_{39}] = (\mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_1\mathfrak{p}_2})^2 \text{ and } 13\mathbb{Z}[\zeta_{39}] = (\mathfrak{q}\overline{\mathfrak{q}})^6.$$

Proposition 1: Considering the decomposition above, let $\mathfrak{I} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}$ be an ideal in $\mathbb{Z}[\zeta_{39}]$. Then

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x}) \geq 4 \times 39, \;\; \forall x \in \mathfrak{I}.$$

Proof: Let $x \in \mathfrak{I}$ and $x_0, x_1 \in \mathbb{Z}[\zeta_{13}]$ be such that $x = x_0 + x_1\zeta_3$. We know that for $\forall x \in \mathfrak{I}$, $\mathrm{Tr}_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x})$ is even and a multiple of 39. The value 2×39 is not attained. This can be seen as follows:

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x}) = \mathrm{Tr}_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_0\overline{x_0}) +$$

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_1\overline{x_1}) + \mathrm{Tr}_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}((x_0 - x_1)\overline{(x_0 - x_1)}).$$

To attain the value 2×39, the only possibilities are, up to order,

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_0\overline{x_0}) = 12, \mathrm{Tr}_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_1\overline{x_1}) = 30 \;\text{ and}$$

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}((x_0 - x_1)\overline{(x_0 - x_1)}) = 36.$$

The possible values for x_0 are $\pm\zeta_{13}^{i_0}, \;\; i_0 = 0, \ldots, 12$, and for x_1 they are $\pm(\zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3})$, where the i_r are distinct. Let $x_0 = -\zeta_{13}^{i_0}$ and $x_1 = \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}$. If we suppose $i_0 \neq i_k$, $k = 1, 2, 3$, then $\mathrm{Tr}_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}((x_0 - x_1)\overline{(x_0 - x_1)}) = 36$. If $x \in \mathfrak{I}$, then

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}(\zeta_{13})}(x\overline{x}) =$$

$$3(x_0\overline{x_0} + x_1\overline{x_1}) - (x_0 + x_1)\overline{(x_0 + x_1)} \in 3\mathbb{Z}[\zeta_{13}],$$

and therefore,

$$(x_0 + x_1)\overline{(x_0 + x_1)} \equiv 0 \pmod{\mathbb{Z}[\zeta_{13}]}.$$

Let $\gamma : \mathbb{Z}[\zeta_{13}] \to \mathbb{Z}$ be the ring homomorphism defined by $\gamma(\sum_{i=0}^{11} a_i\zeta_{13}^i) = \sum_{i=0}^{11} a_i$. Since $(x_0 + x_1)\overline{(x_0 + x_1)} \in 3\mathbb{Z}[\zeta_{13}]$, then $\gamma((x_0 + x_1)\overline{(x_0 + x_1)}) \equiv 0 \pmod 3$. Rewriting, we get

$$(x_0 + x_1)\overline{(x_0 + x_1)} =$$

$$(-\zeta_{13}^{i_0} + \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3})(-\zeta_{13}^{-i_0} + \zeta_{13}^{-i_1} + \zeta_{13}^{-i_2} + \zeta_{13}^{-i_3}) =$$

$$4 - A + B \equiv 0 \pmod{3\mathbb{Z}[\zeta_{13}]},$$

where

$$A = \sum_{s=1}^{3}(\zeta_{13}^{i_0 - i_s} + \zeta_{13}^{i_s - i_0}) \text{ and } B = \sum_{r,s=1}^{3} \zeta_{13}^{i_r - i_s}.$$

Let n_A (respectively, n_B) the number of exponents such that $i_0 - i_s = -1$ or $i_s - i_0 = -1$ (respectively, $i_r - i_s = -1$). The possible values for n_A are 0 and 1 since the i_j are distinct. On the other hand, n_B can assume the values $0, 1$, or 2.

Note that $\gamma(\zeta_{13}^{-1}) = \gamma(-1 - \zeta_{13} - \cdots - \zeta_{13}^{11}) = -12 \equiv 0 \pmod 3$. Hence,

$$\gamma(A) = 6 - n_A \text{ and } \gamma(B) = 6 - n_B,$$

which implies

$$\gamma((x_0 + x_1)\overline{(x_0 + x_1)}) =$$

$$4 - (6 - n_A) + (6 - n_B) \equiv 1 + n_A - n_B \equiv 0 \pmod 3.$$

Therefore, the only possible solutions are $(n_A, n_B) = (0, 1)$ and $(n_A, n_B) = (1, 2)$. Suppose $n_A = 0$ and $n_B = 1$. By hypothesis, given that $0 < a \leq 11$, the coefficient of ζ_{13}^a is a multiple of 3. We have

$$B = \zeta_{13}^{-1} + \sum_{\substack{r,s=1 \\ i_r - i_s \neq -1}}^{3} \zeta_{13}^{i_r - i_s}.$$

If there are r and s such that $i_r - i_s = a$, then the coefficient of ζ_{13}^a in the equation above will vanish, since $\zeta_{13}^{-1} = -1 - \zeta_{13} - \cdots - \zeta_{13}^{11}$. In this way, ζ_{13}^a will also appear with a zero coefficient in the expansion of A in the $\mathbb{Z}$-basis $\{1, \ldots, \zeta_{13}^{11}\}$. If there are no r and s such that $i_r - i_s = a$, ζ_{13}^a will again appear with a zero coefficient in the decomposition of $(x_0 + x_1)\overline{(x_0 + x_1)}$. Therefore, the only possibility is $a = 0$ and $(x_0 + x_1)\overline{(x_0 + x_1)} = 3$. Then,

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}(\zeta_{13})}(x\overline{x}) = 3(x_0\overline{x_0} + x_1\overline{x_1}) - (x_0 + x_1)\overline{(x_0 + x_1)},$$

and in this case, $\mathrm{Tr}_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x}) = 90$, which contradicts the hypothesis on x. The case $n_A = 1$ and $n_B = 2$ is handled similarly. $\square$

B. Construction B - Dimension 12

Using computational methods, K_{12} was obtained in [3] via the geometrical representation of a prime ideal in $\mathcal{O}_K$ above 7, where $K = \mathbb{Q}(\zeta_{21})$. Here, instead, we give a formal proof, based on a more general result:

Theorem 2: Let p and q be primes such that $\mathrm{Ord}_p(q) \equiv 1 \pmod 2$ and $q > 2p - 3$. Furthermore, suppose

$$q\mathbb{Z}[\zeta_{pq}] = (\mathfrak{I}\overline{\mathfrak{I}})^{q-1}$$

is the decomposition of q in $\mathbb{Q}[\zeta_{pq}]$. Then,

$$\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}) \geq (p - 1) \cdot 2q, \;\; \forall x \in \mathfrak{I}.$$

Proof: Let $x_0, \ldots, x_{p-2} \in \mathbb{Z}[\zeta_q]$ be such that $x = \sum_{i=0}^{p-2} x_i\zeta_p^i \in \mathfrak{I}$. After doing a little algebra,

$$\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}) = \sum_{i=0}^{p-2} Q_{p-1}(x_i) + \sum_{i<j} Q_{p-1}(x_i - x_j).$$

If $x_0 = \cdots = x_{p-2}$, then $x = x_0(1 + \zeta_p + \cdots + \zeta_p^{p-2})$, and therefore $x_0 \in \mathfrak{I} \cap \mathbb{Z}[\zeta_q]$. Hence,

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_i\overline{x_i}) \geq 2q, \; i = 0, \ldots, p - 2,$$

which implies that

$$\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}) = \sum_{i=0}^{p-2} Q_{p-1}(x_0) \geq (p - 1)2q.$$

$\square$

If there are at least two distinct values for the x_j, and since $Q_{p-1}(x_i) \geq p - 1$, the number of nonzero $x_i - x_j$ is at least $p - 2$, and so

$$\sum_{i<j} Q_{p-1}(x_i - x_j) \geq (p - 2)(p - 1).$$

Hence,

$$\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}) \geq (2p-3)(q-1).$$

Being that $q > 2p-3$,

$$\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}) > (p-2)2q.$$

Since the quadratic form is even and a multiple of q, $\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}) \geq (p-1)2q$. The norm of $\mathfrak{I}$ is equal to $q^{n_1/2}$. $\square$

Ad hoc calculations show that the center density of $\sigma(\mathfrak{I})$ is

$$\delta(\sigma(\mathfrak{I})) \geq \frac{((p-1)\cdot 2q)^{n_1 n_2/2}}{p^{n_2(n_1-1)/2}\cdot q^{n_1(n_2-1)/2} q^{n_1/2}\cdot 2^{n_1 n_2}} =$$

$$\frac{(\frac{p-1}{2})^{n_1 n_2/2}}{p^{n_2(n_1-1)/2}}. \tag{6}$$

In particular, for $p=3$, the smallest prime satisfying the conditions $q > 2p-3$ and $\mathrm{Ord}_p(q) \equiv 1 \pmod 2$ is $q=7$. For these primes, we have a lattice $\sigma(\mathfrak{I})$ in dimension 12 whose center density is $\delta = \frac{1}{3^3}$, which is exactly the center density of K_{12}.

C. Construction C - Dimension 8

Lemma 1: Let L be a number field and K a subfield of L such that $[L:K]=h$ is odd. Futhermore, let q be a prime number and suppose the decomposition of $q\mathcal{O}_L$ in $\mathcal{O}_L$ has the form

$$q\mathcal{O}_L = \mathfrak{q}_1\ldots\mathfrak{q}_{s/2}\overline{\mathfrak{q}_1\ldots\mathfrak{q}_{s/2}},$$

for some $s \in \mathbb{N}$. Then the decomposition of $q\mathcal{O}_K$ in prime ideals is

$$q\mathcal{O}_K = \mathfrak{q}_1\ldots\mathfrak{q}_{t/2}\overline{\mathfrak{q}_1\ldots\mathfrak{q}_{t/2}},$$

for some $t \in \mathbb{N}$.

Proof: Let us consider a prime ideal $\mathfrak{q}$ in $\mathcal{O}_K$ dividing $q\mathcal{O}_K$. Let $\mathfrak{q}\mathcal{O}_L = \mathfrak{b}_1\ldots\mathfrak{b}_t$ where t divides h, that is, t is odd. On the other hand, suppose $\overline{\mathfrak{q}} = \mathfrak{q}$. Then $\mathfrak{b}_1\ldots\mathfrak{b}_t = \overline{\mathfrak{b}_1\ldots\mathfrak{b}_t}$, and for each ideal $\mathfrak{b}_i$, $i=1,\ldots,t$, there exists $j \neq i$ such that $\overline{\mathfrak{b}_i} = \mathfrak{b}_j$. This means that the ideals above $\mathfrak{q}$ appear in pairs, contradicting the hypothesis on the parity of t. Hence, $\overline{\mathfrak{q}} \neq \mathfrak{q}$, and therefore the stated result holds. $\square$.

Let p and q be primes satisfying the conditions $\mathrm{Ord}_p(q) \equiv \mathrm{Ord}_q(p) \equiv 1 \pmod 2$, and $K_1 \subseteq \mathbb{Q}(\zeta_p)$ and $K_2 \subseteq \mathbb{Q}(\zeta_q)$ be such that $h_p = [\mathbb{Q}(\zeta_p):K_1]$ and $h_q = [\mathbb{Q}(\zeta_q):K_2]$ are odd. Further, let $n_1 = [K_1:\mathbb{Q}]$ and $n_2 = [K_2:\mathbb{Q}]$.

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_{pq}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_p) \arrow[d, dash] & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \mathbb{Q}(\zeta_q) \arrow[d, dash] \\
K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

The field $K = K_1K_2$ has degree n_1n_2. Since K_1 and K_2 are linearly disjoint fields, that is, they have coprime discriminants and satisfy $K_1 \cap K_2 = \mathbb{Q}$, then the discriminant of K is given by

$$\Delta_K = p^{n_2(n_1-1)}\cdot q^{n_1(n_2-1)}.$$

In K, let r_p and r_q be the number of primes above p and q, respectively. Since h_p and h_q are odd, the following decompositions hold true:

$$p\mathcal{O}_K = (\mathfrak{p}_1\ldots\mathfrak{p}_{r_p/2}\cdot\overline{\mathfrak{p}_1\ldots\mathfrak{p}_{r_q/2}})^{n_2} \text{ and}$$

$$q\mathcal{O}_K = (\mathfrak{q}_1\ldots\mathfrak{q}_{r_q/2}\cdot\overline{\mathfrak{q}_1\ldots\mathfrak{q}_{r_q/2}})^{n_1}.$$

Let $\mathfrak{I} = \mathfrak{p}_1\ldots\mathfrak{p}_{r_p/2}\cdot\mathfrak{q}_1\ldots\mathfrak{q}_{r_q/2}$. Its norm is

$$N(\mathfrak{I}) = (p^{h_p})^{r_p/2}(q^{h_q})^{r_q/2} = p^{n_2/2}q^{n_1/2},$$

and for $x \in \mathfrak{I}$,

$$\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}) = \frac{1}{h_p h_q}\mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}).$$

Since h_p and h_q are odd and the quadratic form is even in $\mathbb{Z}[\zeta_{pq}]$, $\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}) \geq 2pq$. The expression for the center density is then

$$\delta = \frac{(2pq)^{n_1n_2/2}}{p^{n_2(n_1-1)/2}\cdot q^{n_1(n_2-1)/2}p^{n_2/2}q^{n_1/2}\cdot 2^{n_1n_2}} = \frac{1}{2^{n_1n_2/2}}. \tag{7}$$

For $n_1n_2 = 4$, $\delta = 1/4$, which is exactly the center density of D_4. Analogously, for $n_1n_2 = 8$, the center density will be $\delta = 1/8$, the center density of E_8.

By the same method, to obtain a lattice with the same center density as E_8's, we need to take suitable p, q, n_1 and n_2. We see that, in principle, there are infinitely many possibilities of construction.

Below is a list of the pairs (p,q) in the interval $p < 50$ and $q < 350$, for which we constructed lattice E_8 from a subfield of $\mathbb{Q}(\zeta_{pq})$:

(p,q)	(p,q)	(p,q)
(7,37)	(7,109)	(11,157)
(11,317)	(19,101)	(19,149)
(19,157)	(19,227)	(23,29)
(23,173)	(23,197)	(23,269)
(23,317)	(31,101)	(31,149)
(31,317)	(43,181)	(43,229)
(43,317)	(47,53)	(47,61)
(47,157)	(47,173)	(47,269)

Example 1: In particular, the conditions above for $n_1n_2 = 8$ are satisfied in the following cases:
i) $p=3$, $q=13$, $K_1 = \mathbb{Q}(\zeta_3)$, and K_2 the subfield of $\mathbb{Q}(\zeta_{13})$ of degree 4;
ii) $p=7$, $q=29$, $K_1 = \mathbb{Q}(\sqrt{-7})$ the quadratic extension contained in $\mathbb{Q}(\zeta_7)$, and K_2 the subfield of $\mathbb{Q}(\zeta_{29})$ of degree 4.
In both cases, the field $K = K_1K_2$ has degree 8 and satisfies the conditions above.

Example 2: Let $p=5$, $q=31$, $K_1 = \mathbb{Q}(\zeta_5)$, and K_2 the subfield of $\mathbb{Q}(\zeta_{31})$ of degree 6. If every $x \in \mathfrak{I}\cap K_1K_2$ satisfies

$$\mathrm{Tr}_{K_1K_2/\mathbb{Q}}(x\overline{x}) \geq 4pq,$$

then we have a rotated version of Λ_{24}. Another possibility is to set K_2 as the quadratic extension contained in $\mathbb{Q}(\zeta_{31})$. Again, this is the same as in Example 1.

Acknowledgments

This work was partially supported by FAPESP under grant No. 95/4720-8.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[2] J. Boutros and E. Viterbo, "Signal space diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. on Inform. Theory,* vol. 44, No. 4, pp. 1453-1467, July 1998.

[3] J. Boutros, E. Viterbo, C. Rastello, and J. C. Belfiori, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. on Inform. Theory,* vol. 42, No. 2, pp. 502-518, March 1996.

[4] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*, Springer-Verlag, New York, 1999.

[5] M. Craig, "A cyclotomic construction for Leech's lattice," *Mathematika* **25**, pp. 236-241, 1978.

[6] M. Craig, " Extreme forms and cyclotomy," *Mathematika* **25**, pp. 44-56, 1978.

[7] X. Giraud and J. C. Belfiori, "Constellations matched to the Rayleigh fading channel," *IEEE Trans. on Inform. Theory,* vol. 42, No. 1, pp. 106-115, Jan. 1996.

[8] D. A. Marcus, *Number Fields*, Springer-Verlag, 1977.

[9] P. Samuel, *Algebraic Theory of Numbers*, Hermann, 1970..

[10] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379-423 and 623-656, 1948.

[11] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.