Corollary 4.3: For each possible value δ, there exists a unique additive dual code H of the extended 1-perfect additive non-$\mathbb{Z}_4$-linear code and all these codes H are pairwise nonequivalent, except for $\delta = 0$ and $\delta = 1$, where the codes H coincide with the binary dual of the extended Hamming code.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their work in reviewing this manuscript. Their comments have enabled us to improve the presentation of this paper.

REFERENCES

[1] H. Bauer, B. Ganter, and F. Hergert, "Algebraic techniques for nonlinear codes," *Combinatorica*, vol. 3, pp. 21–33, 1983.

[2] J. Borges and J. Rifà, "A characterization of 1-perfect additive codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1688–1697, Aug. 1999.

[3] J. Borges, K. T. Phelps, and J. Rifà, "The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear codes and additive non-$\mathbb{Z}_4$-linear codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 2028–2034, Aug. 2003.

[4] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance Regular Graphs*. Berlin, Germany: Springer-Verlag, 1989.

[5] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The Z4-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. Mar., pp. 301–319, 1994.

[6] D. S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes," in *Procs. Int. Workshop on Coding and Cryptography*, Paris, France, Jan. 2001, pp. 329–334.

[7] F. I. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*. New York: North-Holland, 1977.

[8] K. T. Phelps, J. Rifà, and M. Villanueva, "Rank and Kernel of additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes," in *Proc. ACCT'04 Conf.*, Kranevo, Bulgaria, Jun. 2004.

[9] K. T. Phelps and J. Rifà, "On binary 1-perfect additive codes: some structural properties," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2587–2592, Sep. 2002.

[10] J. Rifà and J. Pujol, "Translation invariant propelinear codes," *IEEE Trans. Inf. Theory*, vol. 43, no. 2, pp. 590–598, Mar. 1997.

[11] J. Rifà, "Well-ordered Steiner triple systems and 1-perfect partitions of the n-cube," *SIAM Discr. Math.*, vol. 12, no. 1, pp. 35–47, 1999.

[12] J. Rifà, J. M. Basart, and L. Huguet, "On completely regular propelinear codes," in *Proc. 6th Int. AAECC-6 Conf. (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1989, vol. 357, pp. 341–355.

Algebraic Lattice Constellations: Bounds on Performance

Eva Bayer-Fluckiger, Frédérique Oggier, and Emanuele Viterbo, *Member, IEEE*

***Abstract*—In this work, we give a bound on performance of any full-diversity lattice constellation constructed from algebraic number fields. We show that most of the already available constructions are almost optimal in the sense that any further improvement of the minimum product distance would lead to a negligible coding gain. Furthermore, we discuss constructions, minimum product distance, and bounds for full-diversity complex rotated $\boldsymbol{Z}[i]^n$-lattices for any dimension n, which avoid the need of component interleaving.**

***Index Terms*—Algebraic number theory, cyclotomic fields, modulation diversity, Odlyzko bound, rotated lattice constellations.**

I. INTRODUCTION

Lattice constellations with high modulation diversity have been extensively studied as an alternative approach for transmission over the single-antenna Rayleigh-fading channel. The original idea was to introduce bandwidth-efficient modulations with intrinsic diversity order and good minimum product distance to achieve substantial coding gains.

In [3], [4], [1], [2], it is shown that lattice constellations constructed using algebraic number theory provide the desired properties. The first examples using totally real algebraic number fields were given in [3], while complex algebraic number fields were used in [4], [9]. Initially, no restriction on the shape of the lattice constellation was imposed, which resulted in either a complex bit labeling procedure or loss in the average energy. Further investigations were addressed to finding rotated $\boldsymbol{Z}^n$-lattices to avoid the above problems [9], [5]. In [2], several families of full-diversity rotated $\boldsymbol{Z}^n$-lattices from totally real algebraic number fields were given and analyzed for all dimensions (see also [16]). Some full-diversity complex $\boldsymbol{Z}[i]^n$-lattices are known for $n = 2^r$ [9]. A comprehensive review of this topic can be found in [15].

The main contribution of this work is to give a bound on the minimum product distance of any lattice constellation constructed from algebraic number fields, and to compare this bound to known constructions. We show that most of the already available constructions, built from totally real number fields, are within a few tenths of a decibel from the lower bound. Moreover, we discuss constructions, minimum product distance and bounds for full-diversity complex $\boldsymbol{Z}[i]^n$-lattices for any n.

The correspondence is organized as follows: elementary definitions of algebraic number theory are provided in Section II. In Section III, we recall the notion of *ideal lattices* and in Section IV, we compute a bound on the minimum product distance of signal constellations carved from such lattices. With the aid of this bound, we are able to establish the ultimate coding gains achievable by such constellations. In Section

Manuscript received April 6, 2004; revised February 26, 2005.

E. Bayer-Fluckiger is with the Chaire de Structures Algébriques et Géométriques, Swiss Federal Institute of Technology, Lausanne (EPFL), 1015 Lausanne, Switzerland (e-mail: eva.bayer@epfl.ch).

F. Oggier was with the Chaire de Structures Algébriques et Géométriques, Swiss Federal Institute of Technology, Lausanne (EPFL), 1015 Lausanne, Switzerland. She is now with the California Institute of Technology, Pasadena, CA 91125 USA (e-mail: frederique.oggier@epfl.ch).

E. Viterbo is with the Dipartimento di Elettronica, Politecnico di Torino, 10129, Torino, Italy (e-mail: viterbo@polito.it).

Communicated by M. P. Fossorier, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2005.860452

V, we generalize our framework to *complex ideal lattices*, and compute the minimum product distance of complex constructions. Explicit constructions are given in Section VI. We finally discuss the performance of complex $\boldsymbol{Z}[i]^n$-lattices in Section VII.

II. Preliminary Definitions on Number Fields

Let K be a *number field*, i.e., an extension of finite degree of $\boldsymbol{Q}$. Let n be the degree of K.

Definition 2.1: We call the *embeddings* of K the set of field homomorphisms $\{\sigma_i : K \to \boldsymbol{C}, i = 1, \ldots, n | \sigma(x) = x, \forall x \in \boldsymbol{Q}\}$. The *signature* (r_1, r_2) of K is defined by the number of real (r_1) and complex $(2r_2)$ embeddings such that $n = r_1 + 2r_2$. If all the embeddings of K are real (resp., complex), we say that K is *totally real* (resp., *totally complex*).

Definition 2.2: Let $K = \boldsymbol{Q}(\theta)$ be an extension of $\boldsymbol{Q}$ of degree n. If the minimal polynomial of θ over $\boldsymbol{Q}$ has all its roots in K, we say that K is a *Galois extension* of $\boldsymbol{Q}$. The set

$$\mathrm{Gal}(K/\boldsymbol{Q}) = \{\sigma : K \to K | \sigma(x) = x, \forall x \in \boldsymbol{Q}\}$$

of field automorphisms fixing $\boldsymbol{Q}$, is a group under composition, called the *Galois group* of K over $\boldsymbol{Q}$.

Note that when K is a Galois extension, the set of its embeddings coincides with its Galois group. In the following, we will restrict ourselves to Galois extensions, so that we will use interchangeably the terms "embeddings" or "Galois group."

Definition 2.3: Let $x \in K$ and $\mathrm{Gal}(K/\boldsymbol{Q}) = \{\sigma_i\}_{i=1}^n$. The *trace* of x over $\boldsymbol{Q}$ is defined as

$$\mathrm{Tr}_{K/\boldsymbol{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

while the *norm* of x is

$$N_{K/\boldsymbol{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x).$$

If the field extension is clear from the context, we may write, respectively, $\mathrm{Tr}(x)$ and $N(x)$.

Definition 2.4: Let $O_K = \{x \in K \,|\, \exists$ a monic polynomial $f \in \boldsymbol{Z}[X]$ such that $f(x) = 0\}$. The set O_K is called *the ring of integers* of K.

It can be shown that O_K has a basis $\{\omega_1, \ldots, \omega_n\}$ over $\boldsymbol{Z}$, where n is the degree of K. In other words, every element $x \in O_K$ can be uniquely written as $x = \sum_{i=1}^n \lambda_i \omega_i, \lambda_i \in \boldsymbol{Z}$.

Definition 2.5: A $\boldsymbol{Z}$-basis of O_K is called an *integral basis* of K (or O_K).

Definition 2.6: Let $\{\omega_1, \ldots, \omega_n\}$ be a $\boldsymbol{Z}$-basis of O_K. The integer $d_K = \det(\mathrm{Tr}_{K/\boldsymbol{Q}}(\omega_i \omega_j)_{i,j=1}^n)$ is called the *discriminant* of K.

Definition 2.7: An *ideal* $\mathcal{I}$ of a commutative ring R is an additive subgroup of R which is stable under multiplication by R, i.e., $x\mathcal{I} \subseteq \mathcal{I}$ for all $x \in R$. An ideal $\mathcal{I}$ is *principal* if it is of the form $\mathcal{I} = (a) = \{ax, x \in R\}$ for some $a \in \mathcal{I}$.

When R is not clear from the context we write $\mathcal{I} = (a)R$.

If an ideal $\mathcal{I}$ is not principal, then it is generated by several elements of the ring R. If $\mathcal{I}$ is generated by two elements a and b, we use the notation $\mathcal{I} = (a, b) = \{ax + by : x, y \in R\}$.

Definition 2.8: Let $\mathcal{I}$ be an ideal of O_K. Its *norm* is defined by $N(\mathcal{I}) = |O_K/\mathcal{I}|$. It directly follows that if $\mathcal{I} = (a)O_K$ is principal, then $N(\mathcal{I}) = |N(a)|$.

III. $\boldsymbol{Z}^n$-Ideal Lattices and Product Distance

The theory of ideal lattices gives a general framework for algebraic lattice constructions. We first start by recalling this notion in the case of totally real algebraic number fields. Totally complex number fields will be discussed in Section V.

Definition 3.1: Let K be a totally real number field of degree n. An *ideal lattice* is a lattice $\Lambda = (\mathcal{I}, q_\alpha)$, where $\mathcal{I}$ is an ideal of O_K and

$$q_\alpha : \mathcal{I} \times \mathcal{I} \to \boldsymbol{Z}, \quad q_\alpha(x, y) = \mathrm{Tr}_{K/\boldsymbol{Q}}(\alpha xy), \qquad \forall x, y \in \mathcal{I} \quad (1)$$

where $\alpha \in K$ is totally positive (i.e., $\sigma_i(\alpha) > 0, \forall i$).

We recall that the *diversity* L of a lattice in $\boldsymbol{R}^n$ is the minimum Hamming distance between any two distinct points of the lattice. In the case of algebraic lattices, L is related to the signature of the number field K by the formula $L = r_1 + r_2$ [4]. A lattice built over a totally real number field as in Definition 3.1 has thus maximal diversity order $L = n$. The constructions in [3], [4], [9], [5] fall in the case of ideal lattices with $\alpha = 1$. The general case was extensively applied in [2] to construct new full-diversity constellations with good minimum product distance.

If $\{\omega_1, \ldots, \omega_n\}$ is a $\boldsymbol{Z}$-basis of $\mathcal{I}$, the generator matrix R of an ideal lattice $\Lambda = \{\boldsymbol{x} = \boldsymbol{\lambda} R \,|\, \boldsymbol{\lambda} \in \boldsymbol{Z}^n\}$ is given by

$$R = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_2}\sigma_2(\omega_1) & \ldots & \sqrt{\alpha_n}\sigma_n(\omega_1) \\ \vdots & \vdots & \ldots & \vdots \\ \sqrt{\alpha_1}\sigma_1(\omega_n) & \sqrt{\alpha_2}\sigma_2(\omega_n) & \ldots & \sqrt{\alpha_n}\sigma_n(\omega_n) \end{pmatrix} \quad (2)$$

where $\alpha_i = \sigma_i(\alpha), i = 1, \ldots, n$ (see Definition 2.1). One easily verifies that the Gram matrix RR^T coincides with the trace form $(\mathrm{Tr}(\alpha\, \omega_i \omega_j))_{i,j=1}^n$, where T denotes the transposition. For the $\boldsymbol{Z}^n$-lattice, the corresponding lattice generator matrix given in (2) becomes an orthogonal matrix $(R^{-1} = R^T)$ and we talk about "rotated" $\boldsymbol{Z}^n$-lattices.

The following proposition, whose proof can be found in [1], will be useful in the following.

Proposition 3.1: Let $\mathcal{I}$ be an ideal of O_K, and $\Lambda = (\mathcal{I}, q_\alpha)$ be an ideal lattice. Then

$$|\det(\Lambda)| = N(\alpha) N(\mathcal{I})^2 |d_K|. \quad (3)$$

Once diversity of the signal constellation is fixed, the asymptotic coding gain is determined by the minimum product distance [4].

Definition 3.2: The *minimum product distance* of a lattice constellation Λ is given by

$$d_{p,\min}(\Lambda) = \min_{\boldsymbol{x} \neq \boldsymbol{y} \in \Lambda} \prod_{i=1}^{n} |x_i - y_i| = \min_{0 \neq x \in \Lambda} \prod_{i=1}^{n} |x_i|. \quad (4)$$

The minimum product distance of an ideal lattice can be computed explicitly.

Theorem 3.1: Let $\mathcal{I}$ be an ideal of O_K. The minimum product distance of a lattice constellation carved from an ideal lattice $\Lambda = (\mathcal{I}, q_\alpha)$, with normalized determinant $\det(\Lambda) = 1$, is

$$d_{p,\min}(\Lambda) = \sqrt{\frac{1}{d_K}} \min(\mathcal{I}), \qquad \text{where } \min(\mathcal{I}) = \min_{0 \neq x \in \mathcal{I}} \frac{N(x)}{N(\mathcal{I})}. \quad (5)$$

In the case where $\mathcal{I}$ is principal [2], this simplifies to

$$d_{p,\min}(\Lambda) = \sqrt{\frac{1}{d_K}}. \tag{6}$$

Proof: Let

$$\boldsymbol{x} = \left(\sum_{i=1}^{n} \lambda_i \sqrt{\alpha_1}\sigma_1(\omega_i), \ldots, \sum_{i=1}^{n} \lambda_i \sqrt{\alpha_n}\sigma_n(\omega_i) \right), \qquad \lambda_i \in \boldsymbol{Z}$$

be a lattice point and $x = \sum_{i=1}^{n} \lambda_i \omega_i \in \mathcal{I}$. We have

$$\begin{aligned} d_{p,\min}(\Lambda) &= \min_{0 \neq \boldsymbol{x} \in \Lambda} \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i \sqrt{\alpha_j}\sigma_j(\omega_i) \right| \\ &= \sqrt{N(\alpha)} \min_{0 \neq x \in \mathcal{I}} |N(x)|. \end{aligned} \tag{7}$$

We conclude using Proposition 3.1 that

$$d_{p,\min}(\Lambda) = \frac{\sqrt{\det(\Lambda)}}{N(\mathcal{I})\sqrt{d_K}} \min_{0 \neq x \in \mathcal{I}} |N(x)| = \sqrt{\frac{1}{d_K}} \min(\mathcal{I}). \tag{8}$$

□

When considering nonprincipal rings of integers (i.e., where not all ideals are principal), the $d_{p,\min}$ gives rise to the quantity $\min(\mathcal{I})$ which is hard to evaluate in general. However, the following heuristic can be suggested. When dealing with nonprincipal ideals, it is interesting to compare the proportion of these with respect to the principal ideals. This is measured by a quantity called the *class number* [18], denoted by $h(K)$. For example, if $h(K) = 1$, that means the ring of integers of K is principal. What is known (from an argument coming from class field theory [12]) is that the discriminant of the number field K increases with its class number $h(K)$. This would suggest that

$$d_{p,\min}(\Lambda(\mathcal{I}_K)) = \sqrt{\frac{1}{d_K}} \min(\mathcal{I}) < \sqrt{\frac{1}{d_{K'}}} = d_{p,\min}(\Lambda(\mathcal{I}_{K'}))$$

where K and K' are two totally real number fields of same degree, and K' is principal while K is not. Though one may argue that $\min(\mathcal{I})$ may increase as well as the discriminant, numerical computations show that $\min(\mathcal{I})$ seems to increase much less than the discriminant, at least in the case where the $\boldsymbol{Z}^n$-lattice is built. Here is an illustration in dimension 2 (the examples have been computed with the algorithm described in [13], [12]).

Example 3.1: Consider the number field

$$K_1 = \boldsymbol{Q}[X]/(X^2 - X - 3292)$$

with discriminant $d_{K_1} = 13169$ and class number $h(K_1) = 4$. Let θ denote a root of $X^2 - X - 3292$. The $\boldsymbol{Z}^2$-lattice can be built over the nonprincipal ideal $\mathcal{I} = (13 - \theta, -56)$, with $\alpha = 1643/10324496 + (25/41297984)\theta$. We compute $N(\mathcal{I}) = 56$, while for $x = a(13 - \theta) - 56b \in \mathcal{I}$, we have $N(x) = 3136b^2 - 1400ab - 3136a^2$. The norm reaches its minimum for $a = -1$ and $b = 1$. We get

$$\min(\mathcal{I}) = 1400/56 = 25.$$

The minimum product distance is $d_{p,\min} = 25/\sqrt{13169} = 0.217853$.

Example 3.2: Consider the number field $K_2 = \boldsymbol{Q}[X]/(X^2 - X - 9870)$, with discriminant $d_{K_2} = 39481$ and class number $h(K_2) = 2$. Let θ denote a root of $X^2 - X - 9870$. The $\boldsymbol{Z}^2$-lattice can be built over the nonprincipal ideal $\mathcal{I} = (71 - \theta, 70)$, with

$$\alpha = 281/2763670 + (141/193456900)\theta.$$

TABLE I
VALUES OF $d_{p,\min}$ WITH RESPECT TO $h(K)$

Construction	$h(K)$	$d_{p,min}$
$\mathbf{Q}(\sqrt{5})$	1	0.447213
Example 3.2	2	0.352292
Example 3.1	4	0.217853

$$\begin{array}{c} \mathbf{Q}(\zeta_p) \\ \big| \frac{p-1}{n} \\ K \\ \big| n \\ \mathbf{Q} \end{array}$$

Fig. 1. Number fields in Construction II.

We compute $N(\mathcal{I}) = 70$, while for $x = a(71 - \theta) + 70b \in \mathcal{I}$, we have $N(x) = 4900b^2 + 9870ab - 4900a^2$. The norm reaches its minimum for $a = 0$ and $b = 1$. We get

$$\min(\mathcal{I}) = 4900/70 = 70.$$

The minimum product distance is $d_{p,\min} = 70/\sqrt{39481} = 0.352292$.

In Table I, we compare the values of $d_{p,\min}$ obtained in the preceding examples to the best one obtained over a principal ring of integers [2], namely, considering the quadratic field $\boldsymbol{Q}(\sqrt{5})$. It is clear that the latter construction yields a much better $d_{p,\min}$. This discussion leads us to the conjecture that the nonprincipal case is actually not bringing any improvement. In the following, we will thus focus our attention to the case when Λ is built over a principal ideal $\mathcal{I}$.

IV. BOUNDS ON PERFORMANCE

For high signal-to-noise ratio (SNR) and a given dimension n, optimal lattice constellations Λ achieve the maximum minimum product distance. As $d_{p,\min}(\Lambda) = 1/\sqrt{d_K}$ (by Theorem 3.1), maximizing $d_{p,\min}$ is obviously equivalent to minimizing the field discriminant. This has already been observed in [3], [4], though rotated $\boldsymbol{Z}^n$-lattice codes were not obtained on totally real number fields with minimal discriminant. The corresponding $\boldsymbol{Z}^n$-lattice codes were found later in [13] for dimensions up to 7. For $n \geq 8$, several families of rotated $\boldsymbol{Z}^n$-lattice codes [2] result in the best known performance. But no proof of optimality was given. The reason is that for dimensions $n \geq 8$, finding totally real fields with minimal, or only "small" discriminant is a hard question (see, for example, [6]). Fortunately, a lower bound on number field discriminants (due to Odlyzko [11]) is available. We use it here to find an upper bound on the minimum product distance. Asymptotically for $n \to \infty$, we have the following bound:

$$\begin{aligned} d_K^{1/n} &= (4\pi^{1+C})^{r_1/n} (4\pi e^C)^{2r_2/n} - O(n^{-2/3}) \\ &\geq (60.8395\ldots)^{r_1/n} (22.3816\ldots)^{2r_2/n} - O(n^{-2/3}) = C_n \end{aligned} \tag{9}$$

where $C = 0.577215\ldots$ is Euler's constant. The asymptotic behavior is only reached for very large values of n. The explicit computation of Odlyzko's lower bound for small values of n is rather involved, however, numerical tables for $n \leq 100$ are readily available, for example in PARI [17].

We can see that the *normalized minimum product distance* is upper-bounded by

$$d_{p,\min}{}^{1/n}(\Lambda) = \sqrt{\frac{1}{d_K}}^{1/n} \leq \frac{1}{\sqrt{C_n}}$$

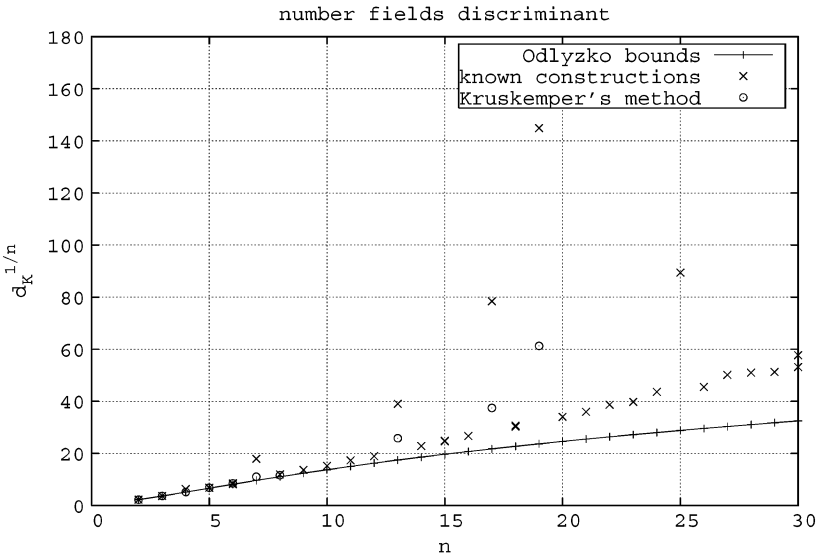

Fig. 2. Comparison of discriminants among the known constructions (Constructions I–III), the most recent one, Krüskemper's construction (Construction IV), and Odlyzko's bounds.

where we consider the normalized minimum product distance ${d_{p,\min}}^{1/n}$ in order to compare lattice constellations of different dimensions. Note that ${d_{p,\min}}^{1/n}$ may be interpreted as the geometric mean distance of the difference between the components of two codewords at the minimum product distance.

It is important to notice that Odlyzko's bounds are not tight, that is, they do not imply that there exists a number field whose discriminant would reach the bound. Furthermore, even if such a number field would exist, that does not imply that the $\boldsymbol{Z}^n$-lattice can be obtained. Thus, we are considering a worst case analysis.

A. Known Constructions of $\boldsymbol{Z}^n$-Lattices Are Good Enough

We compare here the $d_{p,\min}$ obtained in the constructions given in [2], [14], [13] with Odlyzko's bound.

- **Construction I: The cyclotomic case for dimensions $n = (p-1)/2$ with p prime** [2].

  Let p be an odd prime, and ζ_p be a primitive pth root of unity. The $\boldsymbol{Z}^n$-lattice is built over the ring of integers of $K = \boldsymbol{Q}(\zeta_p + \zeta_p^{-1})$, with $\alpha = (1-\zeta_p)(1-\zeta_p^{-1})$. The minimum product distance is given by $d_{p,\min} = p^{-(p-1)/6}$.

- **Construction II: The cyclic case for prime dimensions** [14], [2].

  We consider K a cyclic extension of $\boldsymbol{Q}$ of odd prime degree n. K is embedded into a cyclotomic field $\boldsymbol{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity (see Fig. 1).

  The $\boldsymbol{Z}^n$-lattice is constructed using $\alpha = 1$ and the ideal $\mathcal{A}$ of K such that its square is the inverse different, i.e.,

$$\mathcal{A}^2 = \mathcal{D}_{K/\boldsymbol{Q}}^{-1}. \tag{10}$$

  The minimum product distance of these lattices is $d_{p,\min} = p^{-(n-1)/2}$.

- **Construction III: The mixed case** [2].

  Constellations in other dimensions are derived from the compositum of two (or more) fields involved in Constructions I and II. In terms of lattice generator matrices, we consider the tensor product of matrices from Constructions I and II. The expression of $d_{p,\min}$ in this case can be found in [2].

TABLE II
SOME VALUES OF γ, IN DECIBELS, RELATIVE TO THE BOUND

n	γ (dB)
7	0.03
13	0.09
17	0.12
19	0.21
25	0.25

- **Construction IV: Krüskemper's method** [13].

  Using Krüskemper's method, we obtain the optimal rotated $\boldsymbol{Z}^n$-lattice over the number field with minimum discriminant in all dimensions from 2 up to 7. We also use Krüskemper's method to build lattices over number fields with small (though not minimal) discriminant in dimensions $7, 13, 17$, and 19, where the other available constructions appeared to yield a poor $d_{p,\min}$.

We recall from [4] that the asymptotic coding gain between two rotated lattice constellations with the same dimension and maximal diversity is given by

$$\gamma = 10\log_{10}\left(\frac{d_{p,\min}(1)}{d_{p,\min}(2)}\right)^{1/n} \text{[dB]} \tag{11}$$

where $d_{p,\min}(i), i = 1, 2$ is the minimum product distance of each constellation.

In Fig. 2, we compare the discriminants found in [2], [14], [13] to Odlyzko's bounds. We observe that they are close to the bounds, except for dimensions $7, 13, 17, 19$, and 25. Though the discriminants are notin the continuity of the others, we show that even in the worst cases they are good enough in the sense that any improvement would bring a negligeable coding gain. We compute the achievable coding gain obtained by using a number field whose discriminant would reach Odlyzko's bound, relatively to the given constructions. We observe in Table II that the maximal gain would be at most 0.25 dB in the worst case when a full diversity $\boldsymbol{Z}^n$-lattice could be constructed from a number field achieving Odlyzko's bound.

V. Framework for Complex Lattice Constructions

Following [7], we call *complex lattice* a $\boldsymbol{Z}[i]$-lattice

$$\Lambda^c = \{\boldsymbol{x} = \boldsymbol{\lambda} M : \boldsymbol{\lambda} \in \boldsymbol{Z}[i]^n\} \tag{12}$$

where M is the *lattice generator matrix* and MM^H is the *Gram matrix*, where H denotes the transpose conjugate. We are interested in the case where M is a complex unitary matrix yielding "rotated" versions of the $\boldsymbol{Z}[i]^n$-lattice.

Complex algebraic lattices can be obtained using the relative canonical embedding of a number field and may be applied to the case where the complex Rayleigh-fading channel is considered [9]. This framework enables to precisely describe the design parameters in terms of the algebraic structure, similarly to the case of real algebraic lattices.

Let L be a Galois extension of degree n over $\boldsymbol{Q}(i)$. We denote by $\mathrm{Gal}(L/\boldsymbol{Q}(i)) = \{\sigma_1, \ldots, \sigma_n\}$ the Galois group of L over $\boldsymbol{Q}(i)$ and define the *relative canonical embedding* of L into $\boldsymbol{C}^n$ as

$$\begin{aligned} \sigma : L &\to \boldsymbol{C}^n \\ \sigma(x) &= (\sigma_1(x), \ldots, \sigma_n(x)). \end{aligned} \tag{13}$$

Let O_L be the ring of integers of L. Since $\boldsymbol{Z}[i]$ is principal, there exists a $\boldsymbol{Z}[i]$-basis $\mathcal{B}_L = \{\omega_1, \ldots, \omega_n\}$. Similarly to the real case, the generator matrix of the complex algebraic lattice $\Lambda^c(O_L)$ is obtained by applying the relative canonical embedding to the basis of O_L

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_n(\omega_1) \\ \vdots & & \vdots \\ \sigma_1(\omega_n) & \ldots & \sigma_n(\omega_n) \end{pmatrix}. \tag{14}$$

The *complex diversity* of such lattices is still the minimum Hamming distance between any two complex vectors, i.e., by linearity

$$\min_{0 \neq \boldsymbol{x} \in \Lambda^c} \#\{x_i \neq 0\}$$

with $x = (x_1, \ldots, x_n), x_i \in \boldsymbol{C}$.

Proposition 5.1: The *complex diversity* of $\Lambda^c(O_L)$ is equal to n and we say the lattice has full complex diversity.

Proof: Let $\boldsymbol{x} = (x_1, \ldots, x_n), x_i \in \boldsymbol{C}$, be a lattice point different from the origin. Suppose there exists an $x_j = 0$ for some $j = 1, \ldots, n$ then we get

$$0 = x_j = \sum_{i=1}^{n} \lambda_i \sigma_j(\omega_i) = \sigma_j\left(\sum_{i=1}^{n} \lambda_i \omega_i\right), \qquad \lambda_i \in \boldsymbol{Z}[i]. \tag{15}$$

This implies $\sum_{i=1}^{n} \lambda_i \omega_i = 0$, a contradiction since $\{\omega_j\}_{j=1}^{n}$ is a basis of O_L. □

We now generalize the definition of ideal lattices to the complex case.

Definition 5.1: Let $L/\boldsymbol{Q}(i)$ be a Galois extension of degree n over $\boldsymbol{Q}(i)$. A *complex ideal lattice* is a $\boldsymbol{Z}[i]$-lattice $\Lambda^c = (\mathcal{I}, q)$, where $\mathcal{I}$ is an O_L-ideal and

$$q : \mathcal{I} \times \mathcal{I} \to \boldsymbol{Z}[i], \quad q(x, y) = \mathrm{Tr}_{L/\boldsymbol{Q}(i)}(x\bar{y}), \qquad \forall x, y \in \mathcal{I} \tag{16}$$

where $\bar{}$ denotes the complex conjugation.

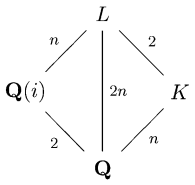

Fig. 3. The compositum of a totally real field K and $\boldsymbol{Q}(i)$: relative degrees are shown on the branches.

When considering complex ideal lattices, the Gram matrix MM^H must be an Hermitian trace form.

Lemma 5.1: The matrix M defined, as in (14), by embedding the basis $\mathcal{B}_{\mathcal{I}} = (\nu_1, \ldots, \nu_n)$ of the ideal $\mathcal{I} \subseteq O_L$

$$M = \begin{pmatrix} \sigma_1(\nu_1) & \ldots & \sigma_n(\nu_1) \\ \vdots & & \vdots \\ \sigma_1(\nu_n) & \ldots & \sigma_n(\nu_n) \end{pmatrix} \tag{17}$$

is the generator matrix of a complex ideal lattice if and only if the complex conjugation commutes with all the other embeddings.

Proof: We have

$$\begin{aligned} MM^H &= \begin{pmatrix} \sigma_1(\nu_1) & \ldots & \sigma_n(\nu_1) \\ \vdots & & \vdots \\ \sigma_1(\nu_n) & \ldots & \sigma_n(\nu_n) \end{pmatrix} \begin{pmatrix} \overline{\sigma_1(\nu_1)} & \ldots & \overline{\sigma_1(\nu_n)} \\ \vdots & & \vdots \\ \overline{\sigma_n(\nu_1)} & \ldots & \overline{\sigma_n(\nu_n)} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i=1}^{n} \sigma_i(\nu_1)\overline{\sigma_i(\nu_1)} & \ldots & \sum_{i=1}^{n} \sigma_i(\nu_1)\overline{\sigma_i(\nu_n)} \\ \vdots & & \vdots \\ \sum_{i=1}^{n} \sigma_i(\nu_n)\overline{\sigma_i(\nu_1)} & \ldots & \sum_{i=1}^{n} \sigma_i(\nu_n)\overline{\sigma_i(\nu_n)} \end{pmatrix} \end{aligned} \tag{18}$$

while the matrix of an Hermitian trace form is given by

$$\begin{pmatrix} \sum_{i=1}^{n} \sigma_i(\nu_1\overline{\nu_1}) & \ldots & \sum_{i=1}^{n} \sigma_i(\nu_1\overline{\nu_n}) \\ \vdots & & \vdots \\ \sum_{i=1}^{n} \sigma_i(\nu_n\overline{\nu_1}) & \ldots & \sum_{i=1}^{n} \sigma_i(\nu_n\overline{\nu_n}) \end{pmatrix} \tag{19}$$

so (18) and (19) coincide if and only if the complex conjugation commutes with all σ_i. □

If L is a totally complex field containing a totally real field K such that $[L : K] = 2$ (we say that L is a *complex multiplication field—CM field*), then it can be shown that the complex conjugation commutes with all σ_i (see, for example, [10, Ch. 1]).

A simple way to construct a CM field is to consider the compositum of $\boldsymbol{Q}(i)$ and a totally real number field K as illustrated in Fig. 3. In the following we restrict ourselves to these CM fields.

The definition of minimum product distance can be derived from Definition 3.2 as follows.

Definition 5.2: Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in \Lambda^c, x_i \in \boldsymbol{C}$, we define the *complex minimum product distance* as

$$d_{p,\min}(\Lambda^c) = \min_{0 \neq \boldsymbol{x} \in \Lambda^c} \prod_{i=1}^{n} |x_i|. \tag{20}$$

We show now that the complex minimum product distance of complex ideal lattices is related to the relative discriminant. Let

$L = K\boldsymbol{Q}(i)$ (see Fig. 3) be the compositum of a totally real number field K and $\boldsymbol{Q}(i)$.

Proposition 5.2: Let $\Lambda^c = (\mathcal{I}, q)$ be a complex ideal lattice over $\boldsymbol{Z}[i]$, where $\mathcal{I} = (\alpha)O_L$ is a principal ideal of O_L,

$$\begin{aligned} q\colon \mathcal{I} \times \mathcal{I} &\to \boldsymbol{Z}[i] \\ (x, y) &\mapsto c\,\mathrm{Tr}_{L/\boldsymbol{Q}(i)}(x\bar{y}) \end{aligned} \tag{21}$$

and c is a normalization factor. Then

$$|\det(\Lambda^c)| = c^n \left|N_{L/\boldsymbol{Q}(i)}(\alpha)\right|^2 |d_{L/\boldsymbol{Q}(i)}| \tag{22}$$

where $d_{L/\boldsymbol{Q}(i)}$ denotes the relative discriminant of L over $\boldsymbol{Q}(i)$.

Proof: Let $\{\omega_j\}_{j=1}^n$ be a $\boldsymbol{Z}[i]$-basis of O_L and $\{\alpha\omega_j\}_{j=1}^n$ be a $\boldsymbol{Z}[i]$-basis of $\mathcal{I}$. By definition

$$|\det(\boldsymbol{\Lambda}^c)| = \left|\det\left(c\,\mathrm{Tr}_{L/\boldsymbol{Q}(i)}(\alpha\omega_j\bar{\alpha}\overline{\omega_k})\right)\right|.$$

Notice that $\mathrm{Tr}_{L/\boldsymbol{Q}(i)}(\alpha\omega_j\overline{\alpha\omega_k})_{j,k=1}^n$ is a matrix of the form MAA^HM^H where M is the matrix defined in (14) and

$$A = \mathrm{diag}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)).$$

Thus,

$$|\det(\Lambda^c)| = c^n |N_{L/\boldsymbol{Q}(i)}(\alpha)| \cdot |\det(\mathrm{Tr}_{L/\boldsymbol{Q}(i)}(\omega_j\overline{\omega_k})| \left|\overline{N_{L/\boldsymbol{Q}(i)}(\alpha)}\right|.$$

Since $\det(MM^H) = \det(M)\det(M^H) = \det(M)\overline{\det(M)}$, we have

$$\left|\det(\mathrm{Tr}_{L/\boldsymbol{Q}(i)}(\omega_j\overline{\omega_k}))\right| = \left|d_{L/\boldsymbol{Q}(i)}\right| \tag{23}$$

which concludes the proof. □

Theorem 5.1: Let Λ^c denote a complex ideal lattice as described in Proposition 5.2, with $|\det(\Lambda^c)| = 1$, we have

$$d_{p,\min}(\Lambda^c) = \frac{1}{\sqrt{\left|d_{L/\boldsymbol{Q}(i)}\right|}}. \tag{24}$$

Proof: Let $\{\omega_i\}_{i=1}^n$ be a $\boldsymbol{Z}$-basis of O_L, and

$$x = \sum_{i=1}^n \lambda_i\omega_i, \lambda_i \in \boldsymbol{Z}.$$

Then

$$\begin{aligned} d_{p,\min}(\Lambda^c) &= \min_{0\neq \boldsymbol{x}\in\Lambda^c} \prod_{j=1}^n \left|\sqrt{c}\sum_{i=1}^n \lambda_i\sigma_j(\alpha\omega_i)\right| \\ &= \sqrt{c^n} \min_{0\neq x\in O_L} \left|N_{L/\boldsymbol{Q}(i)}\left(\alpha\sum_{i=1}^n \lambda_i\omega_i\right)\right| \\ &= \sqrt{c^n}\left|N_{L/\boldsymbol{Q}(i)}(\alpha)\right|. \end{aligned}$$

We conclude using Proposition 5.2

$$d_{p,\min}(\Lambda^c) = \sqrt{c^n}\sqrt{\frac{|\det(\Lambda^c)|}{|d_{L/\boldsymbol{Q}(i)}|}}\frac{1}{\sqrt{c^n}} = \frac{1}{\sqrt{|d_{L/\boldsymbol{Q}(i)}|}}. \tag{25}$$

□

Corollary 5.1: If K has an odd discriminant d_K, then

$$d_{p,\min}(\Lambda^c) = \frac{1}{\sqrt{d_K}}.$$

Proof: If d_K is odd, it satisfies $(d_K, d_{\boldsymbol{Q}(i)}) = 1$, since $d_{\boldsymbol{Q}(i)} = -4$. Thus, a $\boldsymbol{Z}[i]$-basis of L is given by the $\boldsymbol{Z}$-basis of K [20, p. 48], and $d_{L/\boldsymbol{Q}(i)} = d_K$. □

VI. Complex Constructions

This section discusses various constructions of complex lattices. We first recall a known construction over cyclotomic fields, in order to compute its minimum product distance, before introducing two new types of constructions.

A. Cyclotomic Fields $\boldsymbol{Q}(\zeta_{2^r})$

Complex lattice constructions from cyclotomic fields were found in [9], [8]. Here, we show that these lattices may be seen as ideal lattices, which allows to evaluate the complex minimum product distance in terms of field discriminants.

It is well-known [20, p. 65] that $\boldsymbol{Z}[\zeta]$ is the ring of integers of $L = \boldsymbol{Q}(\zeta)$, where $\zeta = \zeta_{2^r}$ and that a $\boldsymbol{Z}$-basis is given by $\{1, \zeta, \zeta^2, \ldots, \zeta^{2^{r-1}-1}\}$.

Propositon 6.1: A $\boldsymbol{Z}[i]$-basis of $\boldsymbol{Z}[\zeta]$ is given by $\{1, \zeta, \zeta^2, \ldots, \zeta^{2^{r-2}-1}\}$.

Proof: Let x be in $\boldsymbol{Z}[\zeta]$. Since $\{1, \zeta, \zeta^2, \ldots, \zeta^{2^{r-1}-1}\}$ is a $\boldsymbol{Z}$-basis and $\zeta^{2^{r-2}} = i$, we have

$$\begin{aligned} x &= \sum_{k=0}^{2^{r-1}-1} a_k\zeta^k, \qquad a_k \in \boldsymbol{Z} \\ &= \sum_{k=0}^{2^{r-2}-1} a_k\zeta^k + \sum_{k=2^{r-2}}^{2^{r-1}-1} a_k\zeta^k \\ &= \sum_{k=0}^{2^{r-2}-1} a_k\zeta^k + \sum_{l=0}^{2^{r-2}-1} i\tilde{a}_l\zeta^l, \qquad \tilde{a}_l = a_{l+2^{r-2}} \in \boldsymbol{Z} \\ &= \sum_{k=0}^{2^{r-2}-1} (a_k + i\tilde{a}_k)\zeta^k. \end{aligned}$$

The set $\{1, \zeta, \zeta^2, \ldots, \zeta^{2^{r-2}-1}\}$ is a system of generators, and the coefficients $b_k = a_k + i\tilde{a}_k$ are in $\boldsymbol{Z}[i]$ for all $k = 0, \ldots, 2^{r-2} - 1$. What is left to prove is the unicity of the representation of x. Suppose there exists another way of writing x, then this will lead to two ways of writing x in a $\boldsymbol{Z}$-basis of $\boldsymbol{Z}[\zeta]$, which is a contradiction.

Proposition 6.2: Consider the ideal lattice $\Lambda^c = (O_L, q)$ where $L = \boldsymbol{Q}(\zeta)$ is of degree $n = 2^{r-2}$ over $\boldsymbol{Q}(i)$ and

$$q(x, y) = \frac{1}{2^{r-2}}\mathrm{Tr}_{L/\boldsymbol{Q}(i)}(x\bar{y}), \qquad \text{for all } x, y \in O_L.$$

Then Λ^c is isomorphic to the $\boldsymbol{Z}[i]^n$-lattice.

Proof: See [9]. □

Let us now consider the product distance. As

$$\boldsymbol{Q}(\zeta) = \boldsymbol{Q}(\zeta + \zeta^{-1})\boldsymbol{Q}(i)$$

we apply Theorem 5.1.

Proposition 6.3: The relative discriminant $d_{\boldsymbol{Q}(\zeta)/\boldsymbol{Q}(i)}$ satisfies

$$\left|d_{\boldsymbol{Q}(\zeta)/\boldsymbol{Q}(i)}\right| = (2^{r-2})^{2^{r-2}}. \tag{26}$$

Proof: The relative discriminant $|d_{\boldsymbol{Q}(\zeta)/\boldsymbol{Q}(i)}|$ is given by $|N_{\boldsymbol{Q}(\zeta)/\boldsymbol{Q}(i)}(f'(\zeta))|$ [18, p. 49], where f is the minimal polynomial of $\boldsymbol{Q}(\zeta)$ over $\boldsymbol{Q}(i)$ and $\zeta = \zeta_{2^r}$. As $f(x) = x^{2^{r-2}} + i$, $f'(\zeta) = 2^{r-2}i\zeta^{-1}$. Thus,

$$N_{\boldsymbol{Q}(\zeta)/\boldsymbol{Q}(i)}(f'(\zeta)) = (2^{r-2}i)^{2^{r-2}} N_{\boldsymbol{Q}(\zeta)/\boldsymbol{Q}(i)}(\zeta^{-1}), \tag{27}$$

and we conclude by taking the absolute value. □

The minimum product distance of the above ideal lattice is then given by Theorem 5.1

$$d_{p,\min}(\Lambda^c) = (2^{r-2})^{-2^{r-3}}. \tag{28}$$

B. Complex Constructions From Real Ones

We show a simple method to derive unitary complex matrices (i.e., rotated $\boldsymbol{Z}[i]^n$-lattices) from known constructions of rotated $\boldsymbol{Z}^n$-lattices from totally real number fields. Then we compute their minimum product distance.

Consider the extension tower as described in Fig. 3, where K is a totally real number field, and L denotes the compositum of K and $\boldsymbol{Q}(i)$. We are interested in the extension $L/\boldsymbol{Q}(i)$. A $\boldsymbol{Z}[i]$-basis is easily derived.

Lemma 6.1:

a) Suppose K has an odd discriminant (so that d_K and $d_{\boldsymbol{Q}(i)}$ are coprime). Let $\mathcal{B}_K = \{\nu_j\}_{j=1}^n$ be a $\boldsymbol{Z}$-basis of K. Then $\mathcal{B}_K$ is a $\boldsymbol{Z}[i]$-basis of L.

b) Let $\mathcal{B}_L = \{\omega_j\}_{j=1}^n$ be a $\boldsymbol{Z}[i]$-basis of L. Then $\{i\omega_j\}_{j=1}^n$ is a also a $\boldsymbol{Z}[i]$-basis of L.

Proof:

a) Let x be in L. Since $(d_K, d_{\boldsymbol{Q}(i)}) = 1$, a $\boldsymbol{Z}$-basis of L is given by $\{\nu_1, \ldots, \nu_n, i\nu_1, \ldots, i\nu_n\}$ [20, p. 48]. Thus,

$$\begin{aligned} x &= \sum_{j=1}^{n} a_j\nu_j + \sum_{j=1}^{n} ib_j\nu_j \quad a_j, b_j \in \boldsymbol{Z},\ \forall j \\ &= \sum_{j=1}^{n} (a_j + ib_j)\nu_j. \end{aligned}$$

b) This is trivial since i is a unit of $\boldsymbol{Z}[i]$. □

The preceding lemma clearly extends to a basis of any ideal of O_L, which may be used to construct an ideal lattice as explained in the following proposition.

Proposition 6.4: Let $B_{\mathcal{I}} = \{\omega_j = i\nu_j\}_{j=1}^n$ be a $\boldsymbol{Z}[i]$-basis of an ideal $\mathcal{I} \subseteq O_L$. We have

$$\mathrm{Tr}_{L/\boldsymbol{Q}(i)}(\omega_j\overline{\omega_k}) = \mathrm{Tr}_{K/\boldsymbol{Q}}(\nu_j\nu_k). \tag{29}$$

Proof: We have

$$\begin{aligned} \mathrm{Tr}_{L/\boldsymbol{Q}(i)}(\omega_j\overline{\omega_k}) &= \mathrm{Tr}_{L/\boldsymbol{Q}(i)}(i\nu_j\overline{i\nu_k}) \\ &= \mathrm{Tr}_{L/\boldsymbol{Q}(i)}(\nu_j\overline{\nu_k}) \\ &= \mathrm{Tr}_{K/\boldsymbol{Q}}(\nu_j\nu_k) \end{aligned}$$

where the last equality holds since $\mathrm{Gal}(L/\boldsymbol{Q}(i)) = \mathrm{Gal}(K/\boldsymbol{Q})$ [20, p. 47]. □

This construction always yields a purely imaginary lattice generator matrix. In practice, the same rotation may be obtained by directly applying the real generator matrix of Λ, obtained from the field K, to a complex vector in $\boldsymbol{Z}[i]^n$. However, our point of view enables to evaluate the complex minimum product distance from Corollary 5.1

$$d_{p,\min}(\Lambda^c) = d_{p,\min}(\Lambda). \tag{30}$$

The following example shows how to build a $\boldsymbol{Z}[i]^n$-lattice using a $\boldsymbol{Z}^n$-lattice.

Example 6.1: Let $K = \boldsymbol{Q}(\zeta_7 + \zeta_7^{-1})$ and $\alpha = 2 - (\zeta_7 + \zeta_7^{-1})$. A $\boldsymbol{Z}^3$-lattice is built using the ideal $\mathcal{I}_K = (\alpha)O_K$ of $\boldsymbol{Z}[\zeta_7 + \zeta_7^{-1}]$ as follows [2]. A $\boldsymbol{Z}$-basis of the ideal $\mathcal{I}_K$ is given by

$$\{\alpha(\zeta_7^3 + \zeta_7^{-3}), \alpha(\zeta_7^3 + \zeta_7^{-3} + \zeta_7^2 + \zeta_7^{-2}), -\alpha\} = \{\nu_i\}_{i=1}^3.$$

By direct computation we have

$$\frac{1}{7}\mathrm{Tr}_{K/\boldsymbol{Q}}(\nu_i\nu_j) = \delta_{ij}, \qquad i, j = 1, 2, 3.$$

The lattice generator matrix of $\Lambda(\mathcal{I}_K)$ can be used to define a $\boldsymbol{Z}[i]^3$-lattice $\Lambda^c(\mathcal{I}_L)$, where $L = \boldsymbol{Q}(\zeta_7 + \zeta_7^{-1}, i)$ and $\mathcal{I}_L = (\alpha)O_L$. Using Proposition 6.4, the lattice generator matrix of $\Lambda^c(\mathcal{I}_L)$ becomes

$$\begin{pmatrix} 0.327985277i & -0.736976229i & -0.591009048i \\ -0.736976229i & -0.591009048i & 0.327985277i \\ -0.591009048i & 0.327985277i & -0.736976229i \end{pmatrix}.$$

Since $d_K = 49$, the complex minimum product distance of this lattice is given by

$$d_{p,\min}(\Lambda^c) = 1/7.$$

C. Some Other Constructions

The previous method gives lattice generator matrices that are purely imaginary. One may ask if fully complex coefficients could be obtained. We discuss this question in some particular cases.

As in the previous section, we work with the compositum field $L = K\boldsymbol{Q}(i)$ (see Fig. 3). Instead of starting from the real $\boldsymbol{Z}^n$-lattice from K, we attempt to directly construct the $\boldsymbol{Z}[i]^n$-lattice on a particular ideal $\mathcal{I}$ of O_L. Our approach is as follows.

- Consider the ramification in $L/\boldsymbol{Q}$. The prime factorization of the discriminant $d_{L/\boldsymbol{Q}} = \prod p_i^{r_i}$ contains the primes which ramify [18, p. 88], i.e., $(p_i)O_L = \prod_j \mathfrak{P}_{ij}^{e_i}$ where $e_i > 1$ [18, p. 86]. We recall that a prime ideal $\mathfrak{P}_{ij}$ is said to be *above* p_i.
- Considering real lattices, we know that

  $$\mathrm{vol}(\Lambda(O_L)) = \sqrt{|d_{L/\boldsymbol{Q}}|}.$$

  We look for a sublattice $\Lambda(\mathcal{I})$ of $\Lambda(O_L)$, which could be a scaled version of $\boldsymbol{Z}^{2n}$, i.e., $\Lambda(\mathcal{I}) = (\sqrt{c}\boldsymbol{Z})^{2n}$ for some integer c.
- Since $\Lambda(\mathcal{I})$ is a sublattice of $\Lambda(O_L)$

  $$\mathrm{vol}(\Lambda(O_L)) = \sqrt{|d_{L/\boldsymbol{Q}}|}$$

  must divide $\mathrm{vol}(\Lambda(\mathcal{I})) = c^n$, i.e., $\prod p_i^{r_i}$ divides c^{2n}.
- This gives a necessary condition for the choice of $\mathcal{I}$. In terms of norm of the ideal $\mathcal{I}$ [18, p. 69],we need

  $$N(\mathcal{I}) = |O_L/\mathcal{I}| = \frac{\mathrm{vol}(\Lambda(\mathcal{I}))}{\mathrm{vol}(\Lambda(O_L))} = \frac{c^n}{\sqrt{\prod p_i^{r_i}}}. \tag{31}$$

- In order to satisfy (31), we must find an ideal of the form

  $$\mathcal{I} = \prod \mathfrak{P}_{ij}^{s_{ij}} \tag{32}$$

  with norm $\prod p_i^{n-r_i/2}$.

From Corollary 5.1, the minimum product distance remains

$$d_{p,\min}(\Lambda^c) = \frac{1}{\sqrt{d_K}}. \tag{33}$$

1) Dimension 2: Let $\theta = \zeta_5 + \zeta_5^{-1}$ and $L = \boldsymbol{Q}(i,\theta)$. The Galois group $\mathrm{Gal}(L/\boldsymbol{Q}(i))$ is of order 2, generated by σ, that acts on θ as follows: $\sigma(\theta) = -1-\theta$. We have

$$(5)O_L = \mathfrak{P}_1^2\mathfrak{P}_2^2 = (1-i\theta)^2(1-i\sigma(\theta))^2$$

so that $N(\mathfrak{P}_1) = N(\mathfrak{P}_2) = 5$.

We take the principal ideal $\mathcal{I} = \mathfrak{P}_1 = (\alpha)O_L$ with $\alpha = 1-i\theta$, which satisfies (31). A $\boldsymbol{Z}[i]$-basis of $\mathcal{I}$ is $\{\alpha, \alpha\theta\}$. Using the change of basis given by the matrix

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

we get for $(\alpha)O_L$ the new $\boldsymbol{Z}[i]$-basis $\{\nu_i\}_{i=1}^2 = \{1-i\theta, 1-i+\theta\}$. Then it is a straightforward computation, to show that

$$\frac{1}{5}\mathrm{Tr}_{L/\boldsymbol{Q}}(\nu_i\bar{\nu_j}) = \delta_{ij}, \qquad i,j = 1,2.$$

For example

$$\begin{aligned}\mathrm{Tr}_{L/\boldsymbol{Q}(i)}((1-i\theta)\overline{(1-i\theta)}) &= \mathrm{Tr}_{L/\boldsymbol{Q}(i)}(1+\theta^2)\\ &= \mathrm{Tr}_{L/\boldsymbol{Q}(i)}(2-\theta)\\ &= \mathrm{Tr}_{\boldsymbol{Q}(\theta)/\boldsymbol{Q}}(2) - \mathrm{Tr}_{\boldsymbol{Q}(\theta)/\boldsymbol{Q}}(\theta) = 5.\end{aligned}$$

The generator matrix of the lattice is given by

$$\begin{aligned}\begin{pmatrix} \nu_1 & \sigma(\nu_1) \\ \nu_2 & \sigma(\nu_2) \end{pmatrix} &= \begin{pmatrix} 1-i\theta & (1+i)+i\theta \\ (1-i)+\theta & -i-\theta \end{pmatrix}\\ &= \begin{pmatrix} 0.44721-0.27639i & 0.44721+0.72360i \\ 0.72360-0.44721i & -0.27639-0.44721i \end{pmatrix}\end{aligned}$$

The lattice generator matrix is fully complex as opposed to the one obtained with the method of Section VI-B using $K = \boldsymbol{Q}(\theta)$ and $\alpha = 2-\theta$. Its minimum product distance is

$$d_{p,\min}(\Lambda^c) = \frac{1}{\sqrt{5}}.$$

2) Dimension 3: In Example 6.1 we found a purely imaginary generator matrix for dimension 3, using $K = \boldsymbol{Q}(\theta), \theta = \zeta_7 + \zeta_7^{-1}$. We have

$$(7)O_K = \mathfrak{P}^3 = (2-\theta)^3$$

so that $N_{K/\boldsymbol{Q}}(\mathfrak{P}) = 7$. The prime above 7 in $L = \boldsymbol{Q}(i,\theta)$ is $(2-\theta)$ and has norm 7. So if we consider $(2-\theta)$ as an element of L, it has norm 49. No other ideal with this norm can be found hence we can only find the $\boldsymbol{Z}[i]^n$-lattice with a purely imaginary matrix of Example 6.1.

3) Dimension 4: Let $\theta = \zeta_{15} + \zeta_{15}^{-1}$ and $L = \boldsymbol{Q}(\theta, i)$. Consider the ideal $(\alpha) = ((1-3i) + i\theta^2)$ of O_L. A $\boldsymbol{Z}[i]$-basis of (α) is given by $\{\alpha\theta^i\}_{i=0}^3$. Using the change of basis given by the following matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -3 & 0 & 1 \\ -1 & -3 & 1 & 1 \end{pmatrix}$$

TABLE III
COMPARISON OF $d_{p,\min}$ FOR CONSTRUCTIONS IN SECTION VI-A and VI-C

n	Section VI-A	Section VI-C
2	0.5	0.44721359
3	-	0.14285714
4	0.0625	0.02981423

one gets a new $\boldsymbol{Z}[i]$-basis $\{\nu_i\}_{i=1}^4 = \{(1-3i)+i\theta^2, (1-3i)\theta+i\theta^3, -i+(-3+4i)\theta+(1-i)\theta^3, (-1+i)-3\theta+\theta^2+\theta^3\}$. Then by straightforward computation we find

$$\frac{1}{15}\mathrm{Tr}_{L/\boldsymbol{Q}}(\nu_i\bar{\nu_j}) = \delta_{ij}, \qquad i,j = 1,2,3,4.$$

Using (17) and the basis $\{\nu_i\}_{i=1}^4$ we find the lattice generator matrix shown at the bottom of the page. Its minimum product distance is

$$d_{p,\min}(\Lambda^c) = \frac{1}{\sqrt{1125}}.$$

VII. PERFORMANCE OF COMPLEX LATTICES

Performance of ideal $\boldsymbol{Z}[i]$-lattices depends, as in the real case, on both diversity (which is already maximal) and minimum product distance, which has to be maximized.

As shown in Theorem 5.1, the minimum product distance of complex lattices depends on a relative discriminant $d_{L/\boldsymbol{Q}(i)}$. For example, some numerical values of the $d_{p,\min}$ for constructions given in the previous section are available in Table III.

In order to compute in general a relative discriminant, we use a transitivity formula [20]

$$d_{L/\boldsymbol{Q}} = d_{\boldsymbol{Q}(i)/\boldsymbol{Q}}^n N_{\boldsymbol{Q}(i)/\boldsymbol{Q}}\left(d_{L/\boldsymbol{Q}(i)}\right) \tag{34}$$

where n is the degree of L over $\boldsymbol{Q}(i)$. Since $N_{\boldsymbol{Q}(i)/\boldsymbol{Q}}(d_{L/\boldsymbol{Q}(i)}) = |d_{L/\boldsymbol{Q}(i)}|^2$, we get

$$\left|d_{L/\boldsymbol{Q}(i)}\right| = 2^{-n}\sqrt{|d_{L/\boldsymbol{Q}}|} \tag{35}$$

where L is a totally complex number field.

We already noticed in Corollary 5.1 that when d_K is odd, then the relative discriminant is nothing else than d_K itself, i.e., $d_{L/\boldsymbol{Q}(i)} = d_K$.

As in Section IV, we can use Odlyzko's bounds to give a lower bound on totally complex number field discriminants. Knowing that $|d_{L/\boldsymbol{Q}}|^{1/2n} \geq C_{2n}$, we consequently get a bound on the relative discriminant

$$|d_{L/\boldsymbol{Q}(i)}|^{1/n} \geq C_{2n}/2. \tag{36}$$

In Fig. 4, we compare Odlyzko's bound for $|d_{L/\boldsymbol{Q}(i)}|^{1/n}$ to known values of d_K and relative discriminants obtained from cyclotomic constructions. One easily notices that the bound for $|d_{L/\boldsymbol{Q}(i)}|^{1/n}$ grows very slowly. This can be explained by the fact that discriminants of totally complex number fields are much smaller than the ones of totally real number fields. The large gap from the bound can be explained by

$$\begin{pmatrix} 0.2582-0.3122i & 0.3455-0.4178i & -0.4178+0.5051i & -0.2136+0.2582i \\ 0.2582+0.0873i & 0.4718+0.1596i & 0.1596+0.054i & 0.7633+0.2582i \\ 0.2582+0.2136i & -0.5051-0.4178i & -0.4178-0.3455i & 0.3122+0.2582i \\ 0.2582-0.7633i & -0.054+0.1596i & 0.1596-0.4718i & -0.0873+0.2582i \end{pmatrix}.$$

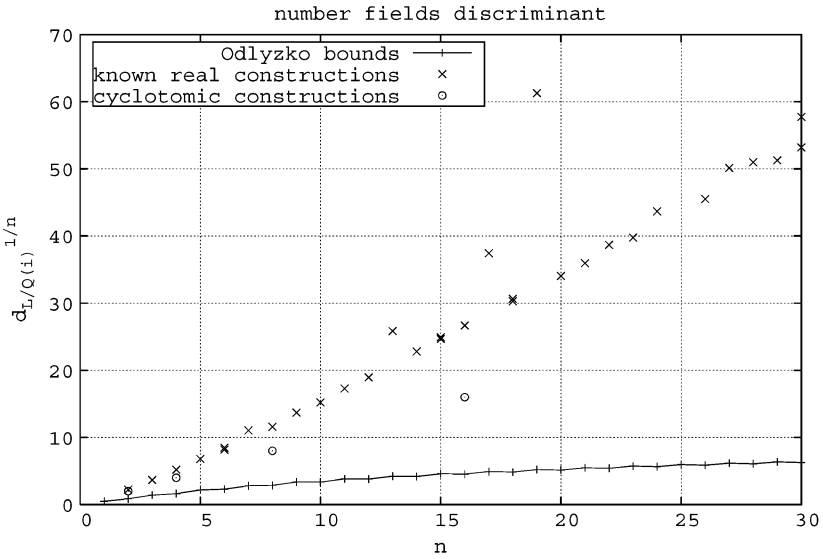

Fig. 4. Comparison of discriminants among the known constructions and Odlyzko's bounds.

the fact that the family of number fields L necessary to produce complex ideal lattices is limited to CM fields which have a high discriminant. On the other hand, Odlyzko's bound is valid for arbitrary number fields.

VIII. Conclusion

Previous work has exhibited several families of $\boldsymbol{Z}^n$-lattices built from totally real algebraic number fields. This correspondence has shown that the known constructions are indeed good enough, in the sense that no significant coding gain can be further achieved. The case of complex lattices was then considered and some full-diversity $\boldsymbol{Z}[i]^n$-lattices constructions were compared to Odlyzko's bound. In this case, the lower bound is not tight due to the important requirements imposed by the structure of ideal lattices which, nevertheless, enables to easily evaluate their complex minimum product distance.

As a final remark, we suggest that the use of totally real lattices should be preferred due to their greater design flexibility although it may require the use of I/Q component interleaving to split the complex fading coefficients.

References

[1] E. Bayer-Fluckiger, "Lattices and number fields," *Contemp. Math.*, vol. 241, pp. 69–84, 1999.

[2] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "New algebraic constructions of rotated $\boldsymbol{Z}^n$-lattice constellations for the Rayleigh fading channel," *IEEE Trans. Inf. Theory*, vol. 50, no. 4, pp. 702–714, Apr. 2004.

[3] K. Boullé and J. C. Belfiore, "Modulation schemes designed for the rayleigh channel," in *Proc. Conf. Information Science and Systems*, Princeton, NJ, Mar. 1992, pp. 288–293.

[4] J. Boutros, E. Viterbo, C. Rastello, and J. C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 502–518, Mar. 1996.

[5] J. Boutros and E. Viterbo, "Signal space diversity: A power and bandwidth efficient diversity technique for the rayleigh fading channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1453–1467, Jul. 1998.

[6] H. Cohen, *Advanced Topics in Computational Number Theory*. Berlin, Germany: Springer-Verlag, 1999.

[7] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. New York: Springer-Verlag, 1988.

[8] M. O. Damen, H. El Gamal, and N. C. Beaulieu, "Systematic construction of full diversity algebraic constellations," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3344–3349, Dec. 2003.

[9] X. Giraud, E. Boutillon, and J. C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 938–952, May 1997.

[10] S. Lang, *Complex Multiplication*. New York: Spring-Verlag, 1983.

[11] A. M. Odlyzko, "Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: A survey of recent results," in *Séminaire de Théorie des Nombres*, Bordeaux, France, 1989, pp. 1–15.

[12] F. Oggier, "Algebraic Methods for Channel Coding," Ph.D. dissertation, Ecole Polytechnique de Lausanne, Lausanne, Switzerland, 2005.

[13] F. Oggier and E. Bayer-Fluckiger, "Best rotated cubic lattice constellations for the rayleigh fading channel," in *Proc. IEEE Int. Symp. Information Theory*, Yokohama, Japan, Jun./Jul. 2003, p. 37.

[14] F. Oggier, E. Bayer-Fluckiger, and E. Viterbo, "New algebraic constructions of rotated cubic lattice constellations for the Rayleigh fading channel," in *Proc. IEEE Information Theory Workshop*, Paris, France, Mar./Apr. 2003, pp. 263–266.

[15] F. Oggier and E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels," *Foundations and Trends in Commun. and Inf. Theory*, vol. 1, pp. 333–415, 2004.

[16] ——, Full Diversity Rotations. [Online]. Available: www.tlc.polito.it/~viterbo/rotations/rotations.html

[17] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. PARI/GP-a Software Package for Computer-Aided Number Theory. [Online]. Available: http://www.math.u-psud.fr/ belabas/pari

[18] P. Samuel, *Théorie Algébrique des Nombres*. Paris, France: Hermann, 1971. Also available in English.

[19] L. C. Washington, *Introduction to Cyclotomic Fields*. New York: Springer-Verlag, 1982.

[20] H. P F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2001.