III. Commutativity of Duality Operator and Propagation Operator

We will denote by $D^{\perp}$ the dual code of D. We have that $\mathcal{P}_{(C,s)}(D)^{\perp}$ is a linear $[h\cdot n, h\cdot n - s\cdot k - (r-s)]$ code with a parity-check matrix $\mathcal{P}_{(C,s)}(G)$. We are interested in knowing when the dual of a propagation code of D is a propagation code of $D^{\perp}$.

From now on let C_1, C_2 be linear codes with parameters $[h_1, r_1, d_1]$ and $[h_2, r_2, d_2]$. All the propagations will be made according to generator matrices G_{C_1}, G_{C_2} of C_1, C_2, respectively. We have the following characterization of commutativity.

Proposition 2: Let $0 \le s_1 \le r_1$ and $0 \le s_2 \le r_2$. The equality

$$\mathcal{P}_{(C_1,s_1)}(D^{\perp}) = \mathcal{P}_{(C_2,s_2)}(D)^{\perp} \tag{4}$$

holds if and only if the following conditions hold:

1) $h_1 = h_2$;
2) $nh_2 - ks_2 - (r_2 - s_2) = (n-k)s_1 + (r_1 - s_1)$;
3)

$$\sum_{l=1}^{r_1}\sum_{m=s_2+1}^{r_2}(G_{C_1}\cdot G_{C_2}^T)_{lm}\, c_l^T d_m + \sum_{l=s_1+1}^{r_1}\sum_{m=1}^{s_2}(G_{C_1}\cdot G_{C_2}^T)_{lm}\, c_l^T d_m = 0 \ \forall c_l, d_m$$

where

$$c_l \in \begin{cases} D, & \text{if } l \le s_1 \\ R_n, & \text{if } l > s_1 \end{cases} \qquad d_m \in \begin{cases} D^{\perp}, & \text{if } m \le s_2 \\ R_n, & \text{if } m > s_2. \end{cases} \tag{5}$$

Proof: Properties 1) and 2) arise directly if we compare the length, respectively, the dimension, of the codes in the right-hand side and the left-hand side of (4).

Suppose $\mathcal{P}_{(C_1,s_1)}(D^{\perp})$ and $\mathcal{P}_{(C_2,s_2)}(D)$ are orthogonal. Let

$$G_{C_1} = (\alpha_{ij}), G_{C_2} = (\beta_{ij}).$$

If we write down the orthogonality relation we have

$$\sum_{i=1}^{n}\sum_{j=1}^{h}\left(\sum_{l=1}^{r_1} c_{il}\alpha_{lj}\right)\cdot\left(\sum_{m=1}^{r_2} d_{im}\beta_{mj}\right) = 0 \tag{6}$$

where $c_l = (c_{1l}, \ldots, c_{nl})^T$ and $d_m = (d_{1m}, \ldots, d_{nm})^T$ fulfill the conditions in (5). The left-hand side of (6) is

$$\sum_{l=1}^{r_1}\sum_{m=1}^{r_2}\sum_{j=1}^{h}\alpha_{lj}\beta_{mj}\sum_{i=1}^{n}c_{il}d_{im} = \sum_{l=1}^{r_1}\sum_{m=1}^{r_2}\sum_{j=1}^{h}\alpha_{lj}\beta_{mj}c_l^T d_m = \sum_{l=1}^{r_1}\sum_{m=1}^{r_2}\left(G_{C_1}\cdot G_{C_2}^T\right)_{lm} c_l^T d_m. \tag{7}$$

Since for $l \le s_1$, $m \le s_2$ we have $c_l^T d_m = 0$, condition 3) in the proposition follows. □

Finally, the following proposition generalizes the result in [4].

Proposition 3: If $\overline{1} \notin D, \overline{1} \notin D^{\perp}$, and the characteristic of F_q does not divide n, then condition 3) in Proposition 2 is equivalent to

$$G_{C_1}\cdot G_{C_2}^T = \left(\begin{array}{c|c} *_{s_1\times s_2} & 0_{s_1\times(r_2-s_2)} \\ \hline 0_{(r_1-s_1)\times s_2} & 0_{(r_1-s_1)\times(r_2-s_2)} \end{array}\right)$$

where $*_{s_1\times s_2}$ is an arbitrary $s_1 \times s_2$ matrix in F_q and $0_{i\times j}$ is the $i \times j$ zero matrix.

Proof: Suppose $\mathcal{P}_{(C_1,s_1)}(D^{\perp}) = \mathcal{P}_{(C_2,s_2)}(D)^{\perp}$, thus, we have

$$\mathcal{P}_{(C_1,s_1)}(G_{D^{\perp}})\cdot\left(\mathcal{P}_{(C_2,s_2)}(G_D)\right)^T = 0$$

and the result follows. □

IV. Conclusion

In this correspondence, we have studied a generalization of Niederreiter–Xing's propagation rule for linear codes. We have seen that the classical Niederreiter–Xing's propagation rule is a particular case of our construction when we use a close nested family of MDS codes. We have also studied the commutativity of the propagation rule with duality. The necessary and sufficient conditions for this commutativity generalized those in [4] and reduces their proofs.

References

[1] T. Blackmore and G. H. Norton, "Matrix product codes over F_q," *Applicable Algebra in Eng., Commun. and Comput.*, vol. 12, pp. 477–500, 2001.

[2] F. Özbudak and H. Stichtenoth, "Note on Niederreiter–Xing's propagation rule for linear codes," *Applicable Algebra in Eng., Commun. and Comput.*, vol. 13, pp. 53–56, 2002.

[3] H. Niederreiter and C. Xing, "A propagation rule for linear codes," *Applicable Algebra in Eng., Commun. and Comput.*, vol. 10, pp. 424–432, 2000.

[4] L. M. Cheng, L. L. Cheng, and W. Sun, "On commutativity of duality operator and propagation operator of linear codes generated from algebraic curves," *IEEE Trans. Inform. Theory*, vol. 49, pp. 258–261, Jan. 2003.

New Algebraic Constructions of Rotated $\mathbb{Z}^n$-Lattice Constellations for the Rayleigh Fading Channel

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

***Abstract*—In this correspondence, we present various families of full diversity rotated $\mathbb{Z}^n$-lattice constellations based on algebraic number theory constructions. We are able to give closed-form expressions of their minimum product distance using the corresponding algebraic properties.**

***Index Terms*—Algebraic number theory, cyclic fields, cyclotomic fields, modulation diversity, rotated constellations.**

I. Introduction

Multidimensional $\mathbb{Z}^n$-lattice signal constellations with specified *modulation diversity* have been proposed for transmission over the fading channel [3]. Given a $\mathbb{Z}^n$-lattice constellation, the desired modulation diversity is obtained by applying a suitable rotation using algebraic number-theoretical tools [11], [5]. The Chernoff bound on the pairwise error probability shows that the two relevant design parameters are modulation diversity and minimum product distance, $d_{\mathrm{p,min}}$ [3], [4]. Good performance may be obtained by selecting rotations that maximize these parameters.

Manuscript received January 9, 2003; revised July 22, 2003. The material in this correspondence was presented in part at the IEEE Information Theory Workshop, Paris, France, March/April 2003.

E. Bayer-Fluckiger and F. Oggier are with the Institut de Mathématiques Bernoulli, Swiss Federal Institute of Technology, Lausanne, 1015 Lausanne, Switzerland (e-mail: eva.bayer@epfl.ch; 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 R. Koetter, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.825045

In [4], it is shown that lattices constructed by the canonical embedding of an algebraic number field K of signature (r_1, r_2) have diversity $L = r_1 + r_2$. Hence, totally real algebraic number fields result in the maximum diversity $L = n$, equal to the dimension of the lattice constellation (or the degree of K). This motivates the investigation on $\boldsymbol{Z}^n$-lattices over totally real number fields.

In this work, we consider algebraic constructions of rotated $\boldsymbol{Z}^n$-lattices using the theory of *ideal lattices* [1]. In particular, we analyze two families of totally real number fields:

1) the maximal real subfield of a cyclotomic field;
2) cyclic fields of odd prime degree.

We then provide a technique to combine these constructions in order to build rotated $\boldsymbol{Z}^n$-lattices in higher dimensions. A few *ad hoc* constructions over totally real number fields were previously proposed in [5], [2], [7]. This correspondence gives new systematic constructions of a large family of such constellations and presents explicit expressions for the corresponding $d_{\mathrm{p,min}}$.

The next section introduces basic definitions and facts of algebraic number theory. Section III discusses the lattice construction from an algebraic number field in the context of ideal lattices and shows how to evaluate $d_{\mathrm{p,min}}$.

In Sections IV–VI, we give an explicit construction of the lattices for each family and compute their minimum product distance. Section VII compares the performance of the new constructions, through simulation. Section VIII concludes the correspondence addressing topics for future work.

II. Basic Definitions and Facts in Algebraic Number Theory

We introduce some definitions and facts about algebraic number theory that will be used in the correspondence, though we assume basic knowledge about fields and rings. The interested reader may refer to [12] for an introduction to algebraic number theory and to [6] for lattice theory.

Recall first some basic definitions about field extensions. 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 of field automorphisms

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

is a group and is called the *Galois group* of K over $\boldsymbol{Q}$. If a Galois group is cylic, the extension is said to be a *cyclic extension*, or *cyclic field*. Here we will restrict our attention to Galois extensions.

Definition 1: 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

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

Definition 2: Let

$$O_K = \{x \in K \mid \exists \text{ a monic polynomial } f \in \boldsymbol{Z}[X] \text{ such that } f(x) = 0\}.$$

The set O_K is a ring called the *ring of integers* of K. Furthermore, it possesses a $\boldsymbol{Z}$-basis $\{\omega_1, \ldots, \omega_n\}$, i.e., $\forall x \in O_K$, $x = \sum_{i=1}^n a_i \omega_i$, with $a_i \in \boldsymbol{Z}$, $i = 1 \ldots n$ and n is the degree of K.

Definition 3: A $\boldsymbol{Z}$-basis of O_K is called an *integral basis* of K (or of O_K).

$$\begin{array}{ccccc} pO_K & \subseteq & O_K & \subseteq & K \\ & & & & | \\ p\mathbf{Z} & \subseteq & \mathbf{Z} & \subseteq & \mathbf{Q} \end{array}$$

Fig. 1. Ideal above $\boldsymbol{p}$.

Definition 4: Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis of O_K. The number

$$d_K = D(\omega_1, .., \omega_n) = \det(\mathrm{Tr}_{K/\boldsymbol{Q}}(\omega_i \omega_j))$$

is called the *discriminant* of K.

Note that the discriminant is independent of the choice of the basis.

We now recall some definitions about ideals, before introducing some ideas and facts related to the ramification of primes.

Definition 5: An *ideal* $\mathcal{I}$ of a commutative ring R is an additive subgroup of R which is stable under multiplication by R, i.e., $a\mathcal{I} \subseteq \mathcal{I}$ for all $a \in R$.

Definition 6: An ideal $\mathcal{I}$ is *principal* if it is of the form

$$\mathcal{I} = (x) = xR = \{xy,\ y \in R\}, \qquad x \in I.$$

Example 1: If $R = \boldsymbol{Z}$, we have that $n\boldsymbol{Z}$ is a principal ideal of $\boldsymbol{Z}$ for all n.

Definition 7: We say that an ideal $\mathcal{I}$ is *prime* if it satisfies the following property: if $xy \in \mathcal{I}$, then $x \in \mathcal{I}$ or $y \in \mathcal{I}$.

The notion of ideal can be extended as follows.

Definition 8: A fractional ideal $\mathcal{I}$ is a sub-O_K-module of K such that there exists $d \in O_K \setminus \{0\}$ with $\mathcal{I} \subseteq d^{-1}O_K$.

It is well known that for all $n \in \boldsymbol{Z}$, there is a unique factorization into prime numbers (times ± 1). This notion of factorization fails to be true in general rings of integers, but is replaced by an analogous for ideals.

Fact 1: [12] Every ideal $\mathcal{I}$ of O_K can be written in a unique way as a product of powers of prime ideals

$$\mathcal{I} = \prod_{i=1}^{m} \mathfrak{P}_i^{e_i}.$$

For fractional ideals the powers e_i appearing in the above factorization may be negative. Ramification theory investigates how prime ideals of $\boldsymbol{Z}$ behave when considered as ideals of O_K (see Fig. 1).

Definition 9: Let $p \in \boldsymbol{Z}$. Consider $\mathfrak{p} = p\boldsymbol{Z}$, a prime ideal of $\boldsymbol{Z}$. Using the previous fact, $pO_K = \prod_{i=1}^m \mathfrak{P}_i^{e_i}$. The integer e_i is called the *ramification index* of $\mathfrak{P}_i$. If one $e_i \geq 2$, we say that $\mathfrak{p}$ (or p, by abuse of notation) ramifies in O_K. If $pO_K = \mathfrak{P}^n$, we say that $\mathfrak{p}$ is *totally ramified* in O_K. In the special case where $K/\boldsymbol{Q}$ is a Galois extension, $e_i = e$ for all i.

Example 2: Let $K = \boldsymbol{Q}(\zeta)$, where $\zeta = \zeta_p$, with p an odd prime and ζ a pth root of unity. The minimal polynomial of K is given by

$$\Phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Since we also have that $\Phi(x) = \prod_{k=1}^{p-1}(x - \zeta^k)$, evaluating the polynomial in $x = 1$, one obtains that $p = \prod_{k=1}^{p-1}(1 - \zeta^k)$. Recall that $O_K = \boldsymbol{Z}[\zeta]$ [12], [13]. Thus,

$$p\boldsymbol{Z}[\zeta] = \prod_{k=1}^{p-1}(1 - \zeta^k)$$

where $(1-\zeta^k)$ is here an ideal of $\boldsymbol{Z}[\zeta]$. Because $1-\zeta^k|1-\zeta$ and, conversely, $1-\zeta|1-\zeta^k$, the ideals equality $(1-\zeta^k)=(1-\zeta)$ holds for all k, so that one deduces the factorization of $p\boldsymbol{Z}[\zeta]$

$$p\boldsymbol{Z}[\zeta]=(1-\zeta)^{p-1}.$$

Here p is thus totally ramified. One can show that p is actually the only prime which ramifies.

The ramification of a number field K is closely linked to its discriminant and to the so-called *different*.

Definition 10: The set

$$D_{K/\boldsymbol{Q}}^{-1}=\{x\in K\mid \forall\alpha\in O_K,\ \mathrm{Tr}_{K/\boldsymbol{Q}}(x\alpha)\in\boldsymbol{Z}\}$$

is a fractional ideal of O_K called the *codifferent*. Its inverse ideal $D_{K/\boldsymbol{Q}}$ is an integral ideal of O_K called the *different*.

Fact 2: [13] A prime ideal $\mathfrak{P}$ of O_K is ramified in $K/\boldsymbol{Q}$ if and only if it divides the different, i.e., it appears with a positive exponent in its factorization into prime ideals.

Definition 11: Let $\mathfrak{a}$ be an ideal of O_K. Its *norm* is defined by $N(\mathfrak{a})=|O_K/\mathfrak{a}|$. It directly follows that if $\mathfrak{a}=aO_K$ is principal, then $N(\mathfrak{a})=|N_{K/\boldsymbol{Q}}(a)|$.

Fact 3: [1] $N(D_{K/\boldsymbol{Q}})=|d_K|$.

The primes in the factorization of the discriminant of K are thus exactly the ones that ramify.

Example 3: Let $K=\boldsymbol{Q}(\zeta)$. The discriminant of K is $(-1)^{(p-1)/2}p^{p-2}$. There is only the prime factor p in the factorization of the discriminant, which corresponds to the fact that only p ramifies.

III. Ideal Lattices

We start by introducing the notion of ideal lattice and derive a formula for its minimum product distance. Throughout the correspondence, we consider totally real number fields resulting in full diversity lattice constellations [4]. We then consider as a special case the $\boldsymbol{Z}^n$-lattice.

Definition 12: Let K be a totally real number field of degree n. An *ideal lattice* is a lattice $(\mathcal{I},q_\alpha)$, where $\mathcal{I}$ is an O_K-ideal (which may be fractional) and

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

where $\mathrm{Tr}=\mathrm{Tr}_{K/\boldsymbol{Q}}$ is the trace and $\alpha\in K$ is totally positive (i.e., $\sigma_i(\alpha)>0\ \forall i$).

In the following, we will use the term lattice to denote either the quadratic form defining the Gram matrix or the particular embedding defined by the lattice generator matrix M.

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

$$M=\begin{pmatrix}\sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_2}\sigma_2(\omega_1) & \dots & \sqrt{\alpha_n}\sigma_n(\omega_1)\\ \vdots & \vdots & \dots & \vdots\\ \sqrt{\alpha_1}\sigma_1(\omega_n) & \sqrt{\alpha_2}\sigma_2(\omega_n) & \dots & \sqrt{\alpha_n}\sigma_n(\omega_n)\end{pmatrix}\qquad(1)$$

where $\alpha_j=\sigma_j(\alpha),\ \forall j$. One easily verifies that

$$MM^t=\{\mathrm{Tr}(\alpha\,\omega_i\omega_j)\}_{i,j=1}^n.$$

This choice of a generator matrix uniquely identifies a lattice Λ from $(\mathcal{I},q_\alpha)$.

A. The Minimum Product Distance of an Ideal Lattice

We study the problem of computing the minimum product distance for general ideal lattices.

Definition 13: Given an n-dimensional lattice Λ with full diversity $L=n$, we define the minimum product distance of $\boldsymbol{x}=(x_1,\dots,x_n)$ from the origin as

$$d_{\mathrm{p,min}}=\min_{x\in\Lambda}d_p(\boldsymbol{x})$$

where

$$d_p(\boldsymbol{x})=\prod_{i=1}^n|x_i|.$$

We are interested in relating $d_{\mathrm{p,min}}$ to the algebraic properties of the fields and ideals used to construct the lattice. Recall first the following.

Lemma 1: If $\mathcal{I}$ is a principal ideal of O_K, then

$$\min_{x\neq0\in\mathcal{I}}N(x)=N(\mathcal{I}).$$

Proof: Since $\mathcal{I}$ is principal, $\mathcal{I}=(a)$ and $N(\mathcal{I})=|N(a)|$. Let $x\neq0\in\mathcal{I}$ and $x=ay$ for $y\in O_K$. Thus,

$$|N(x)|=|N(a)||N(y)|\geq N(\mathcal{I})$$

and equality holds iff $N(y)=\pm1$. The minimum is reached for $x=au$, where u is a unit. □

In the case where $\mathcal{I}$ is principal, we can give the exact value of the minimum product distance of an ideal lattice $(\mathcal{I},q_\alpha)$.

Theorem 1: Let $\mathcal{I}$ be a principal ideal of O_K. The minimum product distance of an ideal lattice of determinant $D=\det(\Lambda)$ defined over $\mathcal{I}$ is

$$d_{\mathrm{p,min}}(\Lambda)=\sqrt{\frac{D}{d_K}}.$$

Proof: Let $\{\omega_1,\dots,\omega_n\}$ be a basis of $\mathcal{I}$ and $x=\sum_{i=1}^n\lambda_i\omega_i$ for $\lambda_i\in\boldsymbol{Z}\ \forall i$. We have from (1)

$$\begin{aligned}d_p(\boldsymbol{x})&=\prod_{j=1}^n\left|\sum_{i=1}^n\lambda_i\sqrt{\alpha_j}\sigma_j(\omega_i)\right|\\&=\prod_{j=1}^n\left|\sqrt{\alpha_j}\sigma_j\left(\sum_{i=1}^n\lambda_i\omega_i\right)\right|\\&=\prod_{j=1}^n|\sqrt{\alpha_j}|\prod_{j=1}^n\left|\sigma_j\left(\sum_{i=1}^n\lambda_i\omega_i\right)\right|\\&=\sqrt{N(\alpha)}\left|N\left(\sum_{i=1}^n\lambda_i\omega_i\right)\right|.\end{aligned}$$

Since $\det(\Lambda)=N(\alpha)\,d_K\,N(\mathcal{I})^2$ (see [1]), we find that $N(\alpha)=D/N(\mathcal{I})^2d_K$, so that we conclude, using Lemma 1, that

$$\begin{aligned}d_{\mathrm{p,min}}(\Lambda)&=\sqrt{N(\alpha)}\min_{x\in\mathcal{I}}N(x)\\&=\sqrt{\frac{D}{d_K}}\frac{\min_{x\in\mathcal{I}}N(x)}{N(\mathcal{I})}=\sqrt{\frac{D}{d_K}}.\end{aligned}$$

□

Remark 1: In order to compare different lattices, we normalize the determinant D to be 1, so that $d_{\mathrm{p,min}}=1/\sqrt{d_K}$. It is also useful to consider $d_{\mathrm{p,min}}^{1/n}$ in order to compare lattices of different dimensions.

B. The Rotated Square Lattice as Ideal Lattice

We say that the $\boldsymbol{Z}^n$-lattice is realized if the matrix of the trace form gives the identity matrix. Equivalently, we say that the trace form is

isomorphic to the unit form. The corresponding generator matrix given in (1) becomes an orthogonal matrix ($M^{-1} = M^t$).

Let us consider here as a simple example, the case of quadratic fields realizing rotated square lattices. Let $K = \boldsymbol{Q}(\sqrt{d})$ with a square-free positive d. Let $\{1, \omega\}$ be an integral basis of O_K, then the corresponding lattice generator matrix is

$$M = \begin{pmatrix} 1 & 1 \\ \omega & \sigma(\omega) \end{pmatrix}.$$

It can be easily verified that $|\det(M)| = \sqrt{d_K}$. If there exists a totally positive element α such that $N(\alpha) = 1/\det(M)^2$, we obtain the rotated square lattice generator matrix

$$R = M \operatorname{diag}(\sqrt{\alpha}, \sqrt{\sigma(\alpha)})$$

since there is only one unimodular lattice in dimension two [6]. A sufficient condition for the existence of the above α is given by the following.

Lemma 2: Let m be an algebraic norm in K. If there exists a unit u such that $N(u) = -1$, then there exists a totally positive element α with algebraic norm m.

Proof: Let β be an element of given norm m. If $\sigma_i(\beta) > 0$ for $i = 1, 2$, we are done with $\alpha = \beta$. If $\sigma_1(\beta) > 0$ and $\sigma_2(\beta) < 0$, we take $\alpha = \beta/u$. In the other cases, we take $\alpha = -\beta$ or $\alpha = -\beta/u$, respectively. □

A family of quadratic fields with the desired property is given by $K = \boldsymbol{Q}(\sqrt{p})$ for all primes p such that $p \equiv 1 (\mathrm{mod}\ 4)$, [10, Corollary 2, p. 182]. For example, we obtain the square lattice for $\boldsymbol{Q}(\sqrt{5})$ with $\alpha = 1/(\sqrt{5}u)$, where $u = (1 + \sqrt{5})/2$. Note that the square lattice may also be obtained from other quadratic fields, e.g., $\boldsymbol{Q}(\sqrt{2})$, with $\alpha = 1/(2\sqrt{2}u)$, where $u = \omega = 1 + \sqrt{2}$.

Finally, we note that using the above technique we find all the previous two-dimensional rotations given by [3], [5].

The two constructions that we present in the following sections are particular realizations of $\boldsymbol{Z}^n$-lattices as ideal lattices in higher dimensions. In the cyclotomic case, $\mathcal{I} = O_K$ and $\alpha = (1 - \zeta)(1 - \zeta^{-1})$, where ζ is a primitive root of unity. In the cyclic case, $\mathcal{I} = \mathcal{A}$ such that $\mathcal{A}^2 = \mathcal{D}_{K/\boldsymbol{Q}}^{-1}$ and $\alpha = 1$.

IV. The Cyclotomic Construction in Dimension $n = (p-1)/2$

We consider the construction of rotated $\boldsymbol{Z}^n$-lattices on the ring of integers of the maximal real subfield of a cyclotomic field.

Let $p \geq 5$ be a prime, $n = (p-1)/2$, and $\zeta = \zeta_p = e^{-2i\pi/p}$ be a pth root of unity. The lattices are built via the ring of integers of $K = \boldsymbol{Q}(\zeta + \zeta^{-1})$, the maximal real subfield of $\boldsymbol{Q}(\zeta)$, whose integral basis is given by $\{e_j = \zeta^j + \zeta^{-j}\}_{j=1}^n$. These notations will be used throughout the correspondence.

Proposition 1: Let $\alpha = (1 - \zeta)(1 - \zeta^{-1})$ then

$$\frac{1}{p} \operatorname{Tr}(\alpha x y)$$

is isomorphic to the unit form $\langle 1, \ldots, 1 \rangle$ of degree n.

Proof: The proof is a direct computation. We compute $\operatorname{Tr}(\alpha x y)$ in the usual integral basis of $\boldsymbol{Q}(\zeta + \zeta^{-1})$. From the matrix that we obtain, we find a new basis where $\frac{1}{p} \operatorname{Tr}(\alpha x y)$ is exactly the identity matrix. Let

$$\alpha = (1 - \zeta)(1 - \zeta^{-1}) = 2 - (\zeta + \zeta^{-1}) \tag{2}$$

and denote $\sigma_j(\zeta)$ and $\alpha_j = \sigma_j(\alpha)$ for $j = 1, \ldots, n$ the conjugates of ζ and α, respectively. Finally, define $q(x, y) = \operatorname{Tr}(\alpha x y)$.

Note that

$$\operatorname{Tr}(\zeta^k + \zeta^{-k}) = \sum_{j=1}^{n} \sigma_j(\zeta^k + \zeta^{-k}) = -1, \qquad \forall\, k = 1, \ldots, n. \tag{3}$$

Using (3) we have

$$\begin{aligned} \sum_{j=1}^{n} \alpha_j \sigma_j(\zeta^k + \zeta^{-k}) &= \sum_{j=1}^{n} (2 - \sigma_j(\zeta + \zeta^{-1}))\sigma_j(\zeta^k + \zeta^{-k}) \\ &= -2 - \sum_{j=1}^{n} \sigma_j(\zeta^{k+1} + \zeta^{-k-1} + \zeta^{-k+1} + \zeta^{k-1}) \\ &= \begin{cases} -2 + 1 - 2n = -p, & \text{if } k \equiv \pm 1 (\mathrm{mod}\ p) \\ -2 + 1 + 1 = 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{4}$$

We now compute $q(e_i, e_j)$ for $i = j$ and $i \neq j$ using (4) and (3)

$$\begin{aligned} q(e_k, e_k) &= \sum_{j=1}^{n} \alpha_j \sigma_j(\zeta^{2k} + \zeta^{-2k} + 2) \\ &= \sum_{j=1}^{n} \alpha_j \sigma_j(\zeta^{2k} + \zeta^{-2k}) + 2 \sum_{j=1}^{n} (2 - \sigma_j(\zeta + \zeta^{-1})) \\ &= \begin{cases} p, & \text{if } k = n, \text{ i.e, } 2k \equiv -1 (\mathrm{mod}\ p) \\ 2p, & \text{otherwise.} \end{cases} \\ q(e_k, e_j) &= \sum_{h=1}^{n} \alpha_h \sigma_h(\zeta^{k+j} + \zeta^{-(k+j)}) + \sum_{h=1}^{n} \alpha_h \sigma_h(\zeta^{k-j} + \zeta^{-(k-j)}) \\ &= \begin{cases} -p, & \text{if } |k - j| = 1 \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Let $Q(x, y) = \frac{1}{p} \operatorname{Tr}(\alpha x y)$. Then the matrix of Q in the basis $\{e_1, \ldots, e_n\}$ is given by

$$\begin{pmatrix} 2 & -1 & 0 & & \cdots & 0 \\ -1 & 2 & -1 & & & \\ 0 & -1 & 2 & & & \\ & & & \ddots & -1 & 0 \\ & & & & -1 & 2 & -1 \\ 0 & \cdots & & & 0 & -1 & 1 \end{pmatrix}.$$

This matrix is isomorphic to the identity matrix. In fact, it is enough to choose a new basis $\{e'_1, \ldots, e'_n\}$ where $e'_n = e_n$ and $e'_j = e_j + e'_{j+1}$, $j = 1, \ldots, n-1$. □

The corresponding rotated $\boldsymbol{Z}^n$-lattice is obtained as follows. Consider the n field embeddings defined by

$$\sigma_k(e_j) = \zeta^{kj} + \zeta^{-kj} = 2 \cos\left(\frac{2\pi k j}{p}\right)$$

then the lattice generated by the ring of integers has the $n \times n$ generator matrix M with elements $M_{k,j} = 2 \cos\left(\frac{2\pi k j}{p}\right)$. The twisting element can be represented by the diagonal matrix

$$A = \operatorname{diag}\left(\sqrt{\sigma_k(\alpha)}\right).$$

The basis transformation matrix from $\{e_j\}$ to $\{e'_j\}$ is given by

$$T = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 \\ \vdots & & \ddots & & \vdots \\ 0 & \cdots & 0 & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Finally, the rotated $\boldsymbol{Z}^n$-lattice generator matrix is given by

$$R = \frac{1}{\sqrt{p}} TMA.$$

Following the above recipe we constructed rotated $\boldsymbol{Z}^n$-lattices for $n = 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, 21, 23, 26, 29, 30, \ldots$.

By Theorem 1, the minimum product distance is given by $d_{\mathrm{p,min}} = 1/\sqrt{d_K} = p^{-\frac{n-1}{2}}$, since $d_K = p^{\frac{p-3}{2}} = p^{n-1}$[13].

V. The Cyclic Constructions

Let K be a cyclic extension of $\boldsymbol{Q}$ of prime degree $n > 2$. Based on [8], we consider lattices constructed using the ideal $\mathcal{A}$ of O_K such that its square is the codifferent, i.e.,

$$\mathcal{A}^2 = \mathcal{D}_{K/\boldsymbol{Q}}^{-1}. \tag{5}$$

Since a Galois extension of odd degree is totally real, we construct rotated $\boldsymbol{Z}^n$-lattices with full diversity $L = n$. The construction in [8] shows there exists a trace form over $\mathcal{A}$ which is isomorphic to the unit form up to a scaling factor. Let p be an odd prime. Depending on the ramification of p in O_K, we derive three different classes of lattices.

1) Case I: $p > n$ is the only prime which ramifies.
2) Case II: $p = n$ is the only prime which ramifies.
3) Case III: there are at least two primes p_1 and p_2 that ramify.

We present and illustrate these three constructions which result in prime dimensional lattices not available from the cyclotomic constructions.

For a given odd prime dimension n we prove that one can always select an odd prime p satisfying some conditions such that we fall into either Case I or Case II or two odd primes p_1 and p_2 such that we fall into Case III. Thus, the knowledge of p (or of p_1 and p_2) and n is sufficient to construct the desired lattice. We emphasize the fact that we do not need explicit knowledge of K. More precisely, we prove that given n and p two odd primes, there always exists a cyclic field K of degree n where only p ramifies. Note that the implementation of the construction algorithms requires the support of a computational algebra package such as KANT ([15]) or PARI ([16]).

The ultimate goal is to select for each dimension a construction giving the largest $d_{\mathrm{p,min}}$.

A. Case I: Only $p > n$ ramifies

If only the prime $p > n$ ramifies in K, we can embed K into the cyclotomic field $\boldsymbol{Q}(\zeta)$, where $\zeta = \zeta_p$ is a primitive pth root of unity. Denote $G = \mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$ the Galois group of $\boldsymbol{Q}(\zeta)$ over $\boldsymbol{Q}$. Then G is cyclic of order $p-1$. Let σ be a generator of G. Since $[\boldsymbol{Q}(\zeta) : K] = \frac{p-1}{n}$, the element σ^n is a generator of the cyclic group $\mathrm{Gal}(\boldsymbol{Q}(\zeta)/K)$ (see Fig. 2).

Let r be a primitive element $(\mathrm{mod}\ p)$ (i.e., $r^{p-1} \equiv 1(\mathrm{mod}\ p)$ and $p-1$ is the smallest integer having this property), $\alpha = \prod_{k=0}^{m-1}(1-\zeta^{r^k})$, $m = \frac{p-1}{2}$, and let λ be such that $\lambda(r-1) \equiv 1(\mathrm{mod}\ p)$.

Note that

$$r^m \equiv -1(\mathrm{mod}\ p).$$

According to the definition of r, we may take σ as

$$\sigma : \zeta \mapsto \zeta^r.$$

Lemma 3: The following equalities hold:

a) $\sigma(\alpha) = -\zeta^{p-1}\alpha$.
b) $\sigma(\zeta^\lambda\alpha) = -\zeta^\lambda\alpha$.

Proof of a):

$$\begin{aligned}\sigma(\alpha) &= \prod_{k=0}^{m-1}(1-\zeta^{r^{k+1}}) \\ &= (1-\zeta)^{-1}(1-\zeta)\prod_{k=0}^{m-2}(1-\zeta^{r^{k+1}})(1-\zeta^{r^m}) \\ &= (1-\zeta)^{-1}(1-\zeta^{-1})\alpha = -\zeta^{p-1}\alpha.\end{aligned}$$

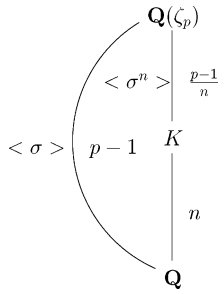

Fig. 2. Extension tower for Case I.

The last equality derives from

$$(1-\zeta)^{-1}(1-\zeta^{-1}) = \frac{1-\zeta^{p-1}}{1-\zeta} = \zeta^{p-2} + \cdots + \zeta + 1.$$

Proof of b): Using the previous equality and the definition of λ, we have

$$\sigma(\zeta^\lambda\alpha) = \zeta^{\lambda+1}(-\zeta^{p-1}\alpha) = -\zeta^\lambda\alpha. \qquad \square$$

Lemma 4: $(\zeta^\lambda\alpha)^2 = (-1)^m p$.

Proof: Recall that the cyclotomic polynomial of degree $p-1$ is given by

$$\begin{aligned}\Phi(x) &= x^{p-1} + x^{p-2} + \cdots + x + 1 \\ &= \prod_{k=0}^{p-2}(x - \sigma^k(\zeta)).\end{aligned}$$

Evaluating for $x = 1$, we obtain

$$\begin{aligned}p &= \prod_{k=0}^{p-2}(1-\zeta^{r^k}) = \prod_{k=0}^{m-1}(1-\zeta^{r^k})\prod_{j=0}^{m-1}(1-\zeta^{-r^j}) \\ &= (-1)^m\alpha^2\prod_{j=0}^{m-1}\zeta^{-r^j} = (-1)^m\alpha^2\zeta^{2\lambda}.\end{aligned}$$

The last equality holds since

$$\zeta^{-1-r\cdots-r^{m-1}} = \zeta^{\frac{1-r^m}{r-1}}$$

and λ is the inverse of $r-1\ (\mathrm{mod}\ p)$. $\square$

The construction is given by the following.

Proposition 2: Define $z = \zeta^\lambda\alpha(1-\zeta)$ and

$$x = \mathrm{Tr}_{\boldsymbol{Q}(\zeta)/K}(z) = \sum_{j=1}^{\frac{p-1}{n}}\sigma^{jn}(z).$$

Then we have $\mathrm{Tr}_{K/\boldsymbol{Q}}(x\sigma^t(x)) = \delta_{0,t}\,p^2$, $t = 0, \ldots, n-1$.

Proof:

$$\begin{aligned}&\mathrm{Tr}_{K/\boldsymbol{Q}}(x\sigma^t(x)) \\ &= \sum_{a=0}^{n-1}\sigma^a\{x\sigma^t(x)\} = \sum_{a=0}^{n-1}\sum_{c,j=1}^{\frac{p-1}{n}}\sigma^{a+cn}(z)\sigma^{a+t+jn}(z) \\ &\text{(Lemma 3)} \\ &= \sum_a\sum_{c,j}(-1)^{a+cn}\zeta^\lambda\alpha(1-\zeta^{r^{a+cn}})(-1)^{a+t+jn}\zeta^\lambda\alpha(1-\zeta^{r^{a+t+jn}}) \\ &= (-1)^t\sum_c(-1)^c\sum_{a,j}(-1)^j(\zeta^\lambda\alpha)^2(1-\zeta^{r^{a+cn}})(1-\zeta^{r^{a+t+jn}}) \\ &\text{(Lemma 4)} \\ &= (-1)^t(-1)^m p\sum_c(-1)^c\sum_a\left(\sum_j(-1)^j(1-\zeta^{r^{a+cn}})\right. \\ &\qquad \left. -\sum_j(-1)^j(\zeta^{r^{a+t+jn}} - \zeta^{r^{a+cn}+r^{a+t+jn}})\right).\end{aligned}$$

We notice that the first term in parenthesis is 0 because there are as many 1's as -1's in the sum over j. Using the same principle, the term $\zeta^{r^{a+t+jn}}$ also disappears because of the sum over c, so that we have

$$\mathrm{Tr}_{K/\boldsymbol{Q}}(x\sigma^t(x)) = (-1)^{t+m} p \sum_c (-1)^c \sum_{a,j} (-1)^j \zeta^{r^{a+cn}+r^{a+t+jn}}. \tag{6}$$

The following identity holds:

$$\sum_{c=1}^{\frac{p-1}{n}} (-1)^c \sum_{a,j} (-1)^j \zeta^{r^{a+cn}+r^{a+t+jn}} = \sum_{d=1}^{\frac{p-1}{n}} (-1)^d \sum_{a,k} \zeta^{r^{a+nd+nk}+r^{a+t+nk}} = \sum_d (-1)^d \sum_{a,k} \zeta^{(r^{nd}+r^t)r^{a+kn}}$$

and can be proved by letting all the indexes run through all summation terms to verify that they cover the same set of exponents of $\zeta \pmod p$.

We note that r^{a+kn} for $a = 0, \ldots, n-1$, $k = 1, \ldots, \frac{p-1}{n}$ takes on the values $s = 1, \ldots, p-1$, so that denoting $\omega_{d,t} = \zeta^{(r^{nd}+r^t)}$, we have

$$\sum_d (-1)^d \sum_{a,k} \zeta^{(r^{nd}+r^t)r^{nk+a}} = \sum_d (-1)^d \sum_{s=1}^{p-1} \omega_{d,t}^s \tag{7}$$

where

$$\sum_{s=1}^{p-1} \omega_{d,t}^s = \begin{cases} p-1, & \text{if } \omega_{d,t} = 1 \\ -1, & \text{otherwise.} \end{cases}$$

In order to evaluate (7), we distinguish the two different cases. The case $\omega_{d,t} = 1$ appears when

$$r^{nd} + r^t \equiv 0 \pmod p \Leftrightarrow r^{nd} \equiv r^{m+t} \pmod p \Leftrightarrow t = nd - m + k_1(p-1).$$

As n divides the term on the right, t needs to be a multiple of n which belongs to $\{0, \ldots, n-1\}$ and we conclude that we must have $t = 0$. The case $\omega_{d,t} = 1$ is then reduced to

$$\zeta^{r^{nd}+1} = 1 \Leftrightarrow r^{nd} \equiv -1 \pmod p \Leftrightarrow d = k_2 \left(\frac{p-1}{2n}\right), \quad k_2 \text{ odd}$$

implying that $k_2 = 1$ and $d = \frac{p-1}{2n}$. We conclude that this case appears if and only if $t = 0$ and $d = \frac{p-1}{2n}$.

Thus, the second case appears when $t \neq 0$ and we obtain

$$(-1)^{t+m} p \sum_d (-1)^d \sum_{s=1}^{p-1} \omega_{d,t}^s = (-1)^{t+m} p \sum_{d=1}^{\frac{p-1}{n}} (-1)^d (-1) = 0$$

while for $t = 0$ we have

$$\begin{aligned}(-1)^{t+m} p \sum_d (-1)^d \sum_{s=1}^{p-1} \omega_{d,t}^s &= (-1)^m p \sum_{d=1, d \neq \frac{p-1}{2n}}^{\frac{p-1}{n}} (-1)^d (-1) + (-1)^m p (-1)^{\frac{p-1}{2n}} (p-1) \\ &= p + p(p-1) = p^2.\end{aligned}$$

TABLE I
EXAMPLES OF PARAMETERS FOR CASE I: THE $*$ MEANS THAT $\boldsymbol{K} = \boldsymbol{Q}(\zeta_p + \zeta_p^{-1})$

n	p	r	λ
3*	7	3	4
3	13	2	1
5*	11	2	1
5	31	3	16
7	29	2	1
11*	23	5	6
11	67	2	1
13	53	2	1
17	103	5	26
19	191	19	138
23*	47	5	12
29*	59	2	1

For the last equality, note that $(-1)^{m+\frac{p-1}{2n}} = 1$ since the exponent is always even, and that

$$(-1)^m \sum_{d=1, d \neq \frac{p-1}{2n}}^{\frac{p-1}{n}} (-1)^d (-1) = \begin{cases} (-1)^{m+1}(-1) = 1, & \text{if } p \equiv 1 \pmod 4 \quad (m \text{ even}) \\ (-1)^{m+1}(1) = 1, & \text{if } p \equiv 3 \pmod 4 \quad (m \text{ odd}). \end{cases}$$

This proves that

$$(-1)^{t+m} p \sum_d (-1)^d \sum_{a,k} \zeta^{(r^{nd}+r^t)r^{nk+a}} = \begin{cases} 0, & \text{if } \omega_{d,t} = 1, \text{ i.e, if } t \neq 0 \\ p^2, & \text{else, i.e, if } t = 0. \end{cases}$$

□

1) Construction Algorithm: The previous result gives a concrete method to construct x such that

$$\frac{1}{p^2} \mathrm{Tr}_{K/\boldsymbol{Q}}(x\sigma^t(x))$$

is isomorphic to the unit form. The lattice matrix can be constructed as follows.

1) Choose a prime dimension n.
2) Compute p such that $p \equiv 1 \pmod n$.
3) Compute r and λ as given in the definition.
4) Compute α and z in the basis $\{1, \zeta, \ldots, \zeta^{p-2}\}$ of the cyclotomic field.
5) Compute x and its conjugates in the basis of the cyclotomic field. This can be done using $\sigma : \zeta \mapsto \zeta^r$ and $\sigma^n : \zeta \mapsto \zeta^{r^n}$.
6) Compute M the matrix of the lattice, which contains as first column $\sigma^i(x)$, $i = 0, \ldots, n-1$ and as other columns a cyclic shift of the first column. In order to have the numerical values of the matrix, we need to replace ζ by $e^{2i\pi/p}$. Note that M is a circulant matrix.
7) As a final step, we need to normalize the matrix to get the determinant equal to 1.

Examples of parameters are given in Table I. The lattices in dimensions marked with a $*$ coincide for certain p with the ones built in Section IV from $K = \boldsymbol{Q}(\zeta_p + \zeta_p^{-1})$.

Note that the value of p is not unique and that any choice of p satisfying $p \equiv 1 \pmod n$ will give a well-defined cyclic field K. More precisely, we get the following.

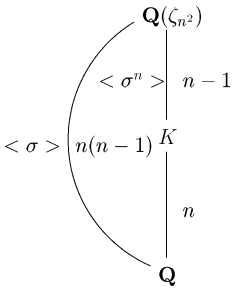

Fig. 3. Extension tower for Case II.

Lemma 5: Let n be an odd prime. If p is an odd prime satisfying $p \equiv 1 \pmod n$, then there exists a cyclic field K of degree n such that p is exactly the only prime which ramifies in K.

Proof: Let G be the cyclic subgroup of $\mathrm{Gal}(\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q})$ generated by σ^n of order $(p-1)/n$, which is an integer since $p \equiv 1 \pmod n$. Let $K = K^G$ be the subfield fixed by G. The extension $K/\boldsymbol{Q}$ is a Galois extension because $\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}$ is cyclic. Furthermore, K inherits the property that p is exactly the only prime which ramifies from $\boldsymbol{Q}(\zeta_p)$ (see [13]). □

2) Example: We give a complete example to illustrate the method.

1) We choose the dimension $n = 3$.
2) We compute a p such that $p \equiv 1 \pmod 3$ and choose $p = 13$. These two parameters determine the field K in which we will work. Note that we do not need to know it explicitly, but in this case $K = \boldsymbol{Q}(\boldsymbol{\theta})$ where $\theta^3 - \theta^2 - 4\theta - 1 = 0$. It has discriminant 13^2 which shows that actually only $p = 13$ ramifies in K.
3) We compute $r = 2$ and $\lambda = 1$.
4) In the basis $\{1, \zeta, \ldots, \zeta^{11}\}$ of $\boldsymbol{Q}(\zeta)$, where $\zeta = \zeta_{13}$, we get $z = (3, 1, 4, 0, 2, 4, 2, 2, 2, 0, 2, 4)$.
5) We compute

$$x = \sigma^0(z) + \sigma^n(z) + \sigma^{2n}(z) + \sigma^{3n}(z)$$

where $\sigma^n : \zeta \mapsto \zeta^{r^n} = \zeta^8$. Then we get

$$x = (5, 0, 3, 3, -1, 0, -1, -1, 0, -1, 3, 3).$$

Using the fact that $\sigma : \zeta \mapsto \zeta^2$, we have

$$\sigma(x) = (6, 0, 1, 1, 4, 0, 4, 4, 0, 4, 1, 1)$$

and

$$\sigma^2(x) = (2, 0, -4, -4, -3, 0, -3, -3, 0, -3, -4, -4).$$

6) Replacing $\zeta = e^{2i\pi/13}$, we compute

$$M = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) \\ \sigma(x) & \sigma^2(x) & x \\ \sigma^2(x) & x & \sigma(x) \end{pmatrix}.$$

7) Normalize by $1/p$

$$R = \frac{1}{13}M = \begin{pmatrix} 0.90636 & -0.24824 & 0.34188 \\ -0.24824 & 0.34188 & 0.90636 \\ 0.34188 & 0.90636 & -0.24824 \end{pmatrix}.$$

B. Case II: Only $p = n$ ramifies

If only the odd prime $p = n$ ramifies in K, we can embed K into $\boldsymbol{Q}(\zeta_{n^2})$, where $\mu = \zeta_{n^2}$ is a primitive n^2th root of unity. Denote by σ the generator of $\mathrm{Gal}(\boldsymbol{Q}(\mu)/\boldsymbol{Q})$. If r is an element such that $r^{n(n-1)} \equiv 1 \pmod{n^2}$, where $n(n-1)$ is the smallest integer having that property, then σ may be defined as $\sigma : \mu \mapsto \mu^r$ (see Fig. 3).

Proposition 3: Let

$$T = \mathrm{Tr}_{\boldsymbol{Q}(\mu)/K}(\mu) = \sum_{j=1}^{n-1} \sigma^{nj}(\mu).$$

Then

$$\mathrm{Tr}_{K/\boldsymbol{Q}}((1+T)\sigma^t(1+T)) = \delta_{0,t}n^2, \qquad t = 0, \ldots, n-1.$$

Proof:

$$\begin{aligned}
&\mathrm{Tr}_{K/\boldsymbol{Q}}((1+T)\sigma^t(1+T)) \\
&= \sum_{a=0}^{n-1} \sigma^a((1+T)\sigma^t(1+T)) \\
&= \sum_{a=0}^{n-1} [1 + \sigma^{a+t}(T) + \sigma^a(T) + \sigma^a(T)\sigma^{a+t}(T)] \\
&= n + \sum_a \sum_{j=1}^{n-1} \sigma^{a+t+nj}(\mu) + \sum_a \sum_{j=1}^{n-1} \sigma^{a+nj}(\mu) \\
&\quad + \sum_a \sum_{j,k=1}^{n-1} \sigma^{a+nj}(\mu)\sigma^{a+t+kn}(\mu) \\
&= n + \sum_a \sum_{j=1}^{n-1} \mu^{r^{a+t+nj}} + \sum_a \sum_{j=1}^{n-1} \mu^{r^{a+nj}} + \sum_a \sum_{j,k=1}^{n-1} \mu^{r^{a+nj}+r^{a+t+kn}} \\
&= n + \sum_{s=0}^{n(n-1)-1} \mu^{r^{s+t}} + \sum_{s=0}^{n(n-1)-1} \mu^{r^s} + \sum_a \sum_{d,c=1}^{n-1} \mu^{r^{a+nd+nc}+r^{a+t+cn}}.
\end{aligned}$$

The last equality is true because the set of values $a + nj$ for $a = 0, \ldots, n-1, j = 1, \ldots, n-1$ is the same as $s = 0, \ldots, n(n-1)-1$. The change of variables in the triple sum can be verified by enumerating the values taken on by the different powers as in the previous section. Since

$$\mathrm{Tr}_{\boldsymbol{Q}(\mu)/\boldsymbol{Q}}(\mu) = \sum_{s=0}^{n(n-1)-1} \sigma^s(\mu) = \sum_{s=0}^{n(n-1)-1} \mu^{r^s} = \sum_{s=0}^{n(n-1)-1} \mu^{r^{s+t}} = 0$$

we obtain

$$\begin{aligned}
\mathrm{Tr}_{K/\boldsymbol{Q}}((1+T)\sigma^t(1+T)) &= n + \sum_{d=1}^{n-1} \sum_{s=0}^{n(n-1)-1} \mu^{(r^{nd}+r^t)r^s} \\
&= n + \sum_{d=1}^{n-1} \mathrm{Tr}_{\boldsymbol{Q}(\mu)/\boldsymbol{Q}}(\omega_{d,t}) \qquad (8)
\end{aligned}$$

where $\omega_{d,t} = \mu^{r^{nd}+r^t}$. The expression $\mathrm{Tr}_{\boldsymbol{Q}(\mu)/\boldsymbol{Q}}(\omega_{d,t})$ in (8) can take on three different values depending on $\omega_{d,t}$

1) $\omega_{d,t} = 1 \Rightarrow \mathrm{Tr}_{\boldsymbol{Q}(\mu)/\boldsymbol{Q}}(\omega_{d,t}) = n(n-1)$.
2) $\omega_{d,t}$ is an n^2th primitive root of unity $\Rightarrow \mathrm{Tr}_{\boldsymbol{Q}(\mu)/\boldsymbol{Q}}(\omega_{d,t}) = 0$.
3) $\omega_{d,t}$ is a root of unity which is not primitive: $\omega_{d,t}$ is of the form $\mu^{k_1 n}$, $k_1 = 1, \ldots, n-1$, which is an nth root of unity $\Rightarrow \mathrm{Tr}_{\boldsymbol{Q}(\mu)/\boldsymbol{Q}}(\omega_{d,t}) = -n$.

To prove the proposition we distiguish the two cases $t = 0$ and $t \neq 0$. In each case, we determine whether $\omega_{d,t}$ is primitive or not.

- *First case:* $t = 0$.

  We have that $\omega_{d,t} = 1$ only in this case. In fact

$$r^{nd} + r^t \equiv 0 \pmod{n^2}$$
$$\iff t = nd - \frac{n(n-1)}{2} + k_2 n(n-1) \iff t = 0$$

  and it occurs for $d = (n-1)/2$

$$r^{nd} \equiv -1 \pmod{n^2} \Rightarrow d = \frac{n-1}{2}.$$

We now verify that when $d \neq \frac{n-1}{2}$, $\omega_{d,t}$ is a primitive root of unity. Suppose it is not primitive, then

$$r^{nd}+1 \equiv 0 (\mathrm{mod}\ n^2) \Rightarrow r^{nd}+1 \equiv 0 (\mathrm{mod}\ n) \Rightarrow d = \frac{n-1}{2} + k_3 \frac{n-1}{n}.$$

Since $d \geq n-1$, we must have $k_3 = 0$, which gives the case $\omega_{d,t} = 1$. Putting all together, we obtain

$$n + \sum_{d=1}^{n-1} \sum_{s=0}^{n(n-1)-1} \mu^{(r^{nd}+r^t)r^s} = n + n(n-1) = n^2, \quad \text{for } t = 0.$$

- *Second case:* $t \neq 0$.
  We determine the primitive roots of unity

$$r^{nd} + r^t \equiv 0 \ (\mathrm{mod}\ n) \Rightarrow d = \frac{t-k_4}{n} + \frac{n-1}{2} + k_4.$$

We need to take $k_4 = t$ (since $d \geq n-1$, we cannot take $k_4 = t + k_5 n$). Thus, there is only one d such that $\omega_{d,t}$ is not primitive. Putting all together, we obtain

$$n + \sum_{d=1}^{n-1} \sum_{s=0}^{n(n-1)-1} \mu^{(r^{nd}+r^t)r^s} = n - n = 0. \qquad \square$$

1) Construction Algorithm: We give a construction procedure as in the previous case.

1) Choose a prime dimension n.
2) Compute r such that $r^{n(n-1)} \equiv 1 \ (\mathrm{mod}\ n^2)$ and that $n(n-1)$ is the smallest integer k such that $r^k \equiv 1 \ (\mathrm{mod}\ n^2)$.
3) Compute $1+T$ and its conjugates in the basis of the cyclotomic field. This can be done using $\sigma : \mu \mapsto \mu^r$ and $\sigma^n : \mu \mapsto \mu^{r^n}$.
4) Compute the lattice generator matrix M and the normalized lattice generator matrix R.

2) Example:

1) Take $n = 3$. This corresponds in fact to the field $K = \boldsymbol{Q}(\boldsymbol{\theta})$ where $\theta^3 - 3\theta - 1 = 0$, whose discriminant is 3^4.
2) $r = 2$.
3) In the basis of $\boldsymbol{Q}(\zeta_9)$, we compute $1+T$ and its conjugates

$$1+T = (1,1,-1,0,0,-1)$$
$$\sigma(1+T) = (1,-1,1,0,-1,0)$$
$$\sigma^2(1+T) = (1,0,0,0,1,1).$$

4) Finally

$$R = \frac{1}{3}M = \begin{pmatrix} 0.84402 & -0.29312 & 0.44909 \\ 0.44909 & 0.84402 & -0.29312 \\ -0.29312 & 0.44909 & 0.84402 \end{pmatrix}.$$

C. Case III: At Least Two Primes Ramify

Suppose now that K contains at least two primes that ramify. We will use two fields where only one prime ramifies as bulding blocks to construct K.

Lemma 6: Let n be an odd prime. Take two distinct odd primes p_1, p_2 such that $p_i \equiv 1 \ (\mathrm{mod}\ n)$, but $p_i \not\equiv 1 \ (\mathrm{mod}\ n^2)$, $i = 1,2$. Let K be a cyclic field of degree n such that p_1 and p_2 ramify. Then K is contained in the compositum K_1K_2 of two fields such that K_i is the cyclic field of degree n where only p_i ramifies, $i = 1,2$.

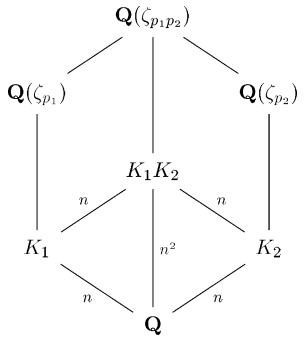

Fig. 4. Extension tower for Case III.

Proof: Since $p_i \equiv 1 \ (\mathrm{mod}\ n)$, $i = 1,2$, we have the extension tower of Fig. 4. It is clear that K is a subextension of $\boldsymbol{Q}(\zeta_{p_1p_2})$. What is left to prove is that $K \subseteq K_1K_2$. Let $G = \mathrm{Gal}(\boldsymbol{Q}(\zeta_{p_1p_2})/\boldsymbol{Q})$.

$$G \cong \boldsymbol{Z}/(p_1-1)\boldsymbol{Z} \times \boldsymbol{Z}/(p_2-1)\boldsymbol{Z} \cong C_n \times C_n \times \boldsymbol{Z}/\left(\frac{p_1-1}{n}\right)\boldsymbol{Z} \times \boldsymbol{Z}/\left(\frac{p_2-1}{n}\right)\boldsymbol{Z}.$$

Recall that an Abelian group has a unique decomposition into its Sylow subgroups. G is thus the direct product of a Sylow n-subgroup and of Sylow p_i-subgroups where $(p_i, n) = 1$.

Let $H = \mathrm{Gal}(\boldsymbol{Q}(\zeta_{p_1p_2})/K_1K_2)$. H is a subgroup of G of order $\frac{p_1-1}{n}\frac{p_2-1}{n}$. Because $(|H|, n) = 1$, we deduce that H corresponds to the direct product of the Sylow p_i-subgroups of G where $(p_i, n) = 1$. Let $I = \mathrm{Gal}(\boldsymbol{Q}(\zeta_{p_1p_2})/K)$ a subgroup of G. As I is of order

$$\frac{(p_1-1)(p_2-1)}{n} = n\frac{p_1-1}{n}\frac{p_2-1}{n}$$

this implies that I contains a subgroup J of order $\frac{p_1-1}{n}\frac{p_2-1}{n}$. We use the same technique as before to obtain that J is also the direct product of the p_i Sylow of G where $(p_i, n) = 1$, so that $H \subseteq I$, implying that $K \subseteq K_1K_2$. $\square$

Remark 2: We do not prove the case when p_1 or p_2 is equal to n, which can be handled in a similar way by replacing $\boldsymbol{Q}(\zeta_{p_1p_2})$ with $\boldsymbol{Q}(\zeta_{p_1n^2})$.

Proposition 4: Let K_1, K_2 be two disjoint Galois extensions of $\boldsymbol{Q}$, whose discriminants are relatively prime.

Let $G_i = \mathrm{Gal}(K_i/\boldsymbol{Q})$ for $i = 1,2$ and $G_1 = \langle\sigma\rangle$, $G_2 = \langle\tau\rangle$ be cyclic of order n. Let $K \subseteq K_1K_2$ be another cyclic extension of order n. If there exist $x_i \in K_i$, $i = 1,2$ which satisfy

1) $\mathrm{Tr}_{K_1/\boldsymbol{Q}}(x_1\sigma^t(x_1)) = \delta_{0,t}p_1^2, \ t = 0, \ldots, n-1$
2) $\mathrm{Tr}_{K_2/\boldsymbol{Q}}(x_2\tau^t(x_2)) = \delta_{0,t}p_2^2, \ t = 0, \ldots, n-1$

then there exists $x \in K$, given by $x = \mathrm{Tr}_{K_1K_2/K}(x_1x_2)$, such that

$$\mathrm{Tr}_{K/\boldsymbol{Q}}(x\gamma^t(x)) = \delta_{0,t}p_1^2p_2^2, \qquad t = 0, \ldots, n-1$$

where $\langle\gamma\rangle = Gal(K/\boldsymbol{Q})$.

Proof: We will use the fact that

$$\mathrm{Tr}_{K_1K_2/\boldsymbol{Q}}(x_1x_2) = \sum_{k=1}^{n}\sum_{j=1}^{n}\sigma^k\tau^j(x_1x_2) = \sum_{k=1}^{n}\sigma^k(x_1)\sum_{j=1}^{n}\tau^j(x_2) = \mathrm{Tr}_{K_1/\boldsymbol{Q}}(x_1)\mathrm{Tr}_{K_2/\boldsymbol{Q}}(x_2).$$

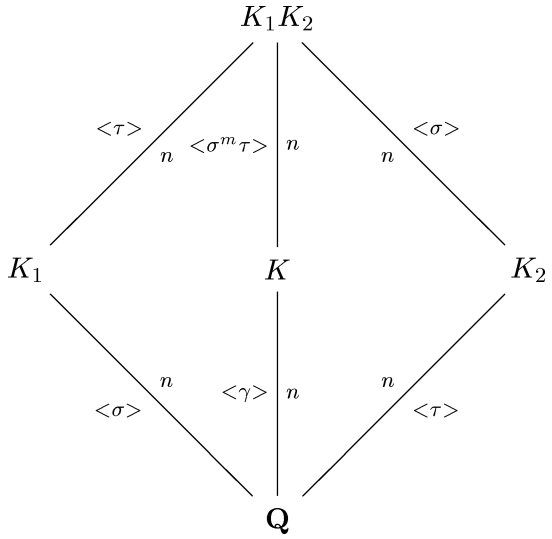

Fig. 5. Detail of the extension tower for Case III.

Let $1 \leq m \leq n-1$ be such that $\langle \sigma^m \tau \rangle = \mathrm{Gal}(K_1K_2/K)$ (see Fig. 5). Choose $\gamma = \sigma^{-m}\tau$ as generator of $\mathrm{Gal}(K/\boldsymbol{Q})$. So

$$\begin{aligned} x &= \sum_{b=0}^{n-1} (\sigma^m \tau)^b (x_1 x_2) \\ x\gamma^t(x) &= \sum_{b,c=0}^{n-1} \sigma^{mb}(x_1)\tau^b(x_2)\sigma^{-mt}\tau^t\sigma^{mc}(x_1)\sigma^{-mt}\tau^t\tau^c(x_2) \\ &= \sum_{b,c=0}^{n-1} \sigma^{mb}(x_1\sigma^{m(c-t-b)}(x_1))\tau^b(x_2\tau^{t+c-b}(x_2)) \end{aligned}$$

and

$$\begin{aligned} & n\mathrm{Tr}_{K/\boldsymbol{Q}}(x\gamma^t(x)) \\ &\quad = \mathrm{Tr}_{K_1K_2/\boldsymbol{Q}}(x\gamma^t(x)) \\ &\quad = \sum_{b,c=0}^{n-1} \mathrm{Tr}_{K_1K_2/\boldsymbol{Q}}(\sigma^{mb}\tau^b[(x_1\sigma^{m(c-t-b)}(x_1))(x_2\tau^{c+t-b}(x_2))]) \\ &\quad = \sum_{b,c} \mathrm{Tr}_{K_1/\boldsymbol{Q}}(x_1\sigma^{m(c-t-b)}(x_1))\mathrm{Tr}_{K_2/\boldsymbol{Q}}(x_2\tau^{c+t-b}(x_2)). \quad (9) \end{aligned}$$

Finally, the terms in the sum of (9) are different from zero only when $m(c-b-t) = 0$ and $c+t-b = 0$, which is equivalent to ask that $t = 0$ and $c = b$. This means that (9) is nonzero if and only if $t = 0$, and it is equal to $np_1^2p_2^2$. □

1) Construction Algorithm: If we know that two primes p_1 and p_2 ramify in a cyclic field K of prime degree n, we know how to find an element $x \in K$ which gives the unit form. Note that no explicit knowledge of K is required to construct the lattice.

1) Choose a prime dimension n.
2) Choose p_1 and p_2 that satisfy the hypotheses.
3) Compute x_1, x_2, and their conjugates using the previous techniques, and embed them into $\boldsymbol{Q}(\zeta_{p_1p_2})$ if $p_2 > n$ or into $\boldsymbol{Q}(\zeta_{p_1n^2})$ if $p_2 = n$.
4) Compute x using the knowledge of $\sigma^t(x_1)$ and $\tau^t(x_2)$, $t = 0, \ldots, n-1$.
5) Compute the conjugates in K of x using $\mathrm{Gal}(K/\boldsymbol{Q})$. The cyclic group $\mathrm{Gal}(K/\boldsymbol{Q})$ of order n must be carefully selected among the subgroups of order n of $\mathrm{Gal}(K_1K_2/\boldsymbol{Q})$.
6) Compute the matrix R.

2) Example: As an example, we use the two cases computed previously.

1) Choose the prime dimension $n = 3$.
2) Choose $p_1 = 13$ and $p_2 = 3$.
3) Let $\zeta = \zeta_{117}$. In the basis of $\boldsymbol{Q}(\zeta)$ of degree 72, we have for example that

$$\begin{aligned} x_1 = (&5,0,0,1,0,0,0,0,0,0,0,0,-3,0,0,0,0,0,0,3,0,0,\\ &-3,0,0,0,0,0,3,0,0,0,0,0,0,0,0,-1,0,0,0,0,0,0,\\ &1,0,0,0,0,0,0,0,0,0,-3,0,0,-1,0,0,0,0,0,-3,\\ &0,0,-1,0,0,0,0,0,0,0,0). \end{aligned}$$

Similarly, we embed x_2 into $\boldsymbol{Q}(\zeta)$.
4) We compute $x = x_1x_2 + \sigma(x_1)\tau(x_2) + \sigma^2(x_1)\tau^2(x_2)$, which gives

$$\begin{aligned} x = (&13,5,-9,0,-2,7,0,2,0,0,7,-9,0,-3,7,0,0,2,0,0,\\ &-2,0,-2,2,0,-5,3,0,7,-9,0,0,0,0,-5,2,0,7,\\ &-7,0,5,-7,0,0,7,0,2,-7,0,0,-7,0,-4,7,0,7,0,0,\\ &-2,-2,0,0,9,0,0,-3,0,0,-7,0,-5,2). \end{aligned}$$

5) Using the generator $\gamma : \zeta \mapsto \zeta^{40}$ of $\mathrm{Gal}(K/\boldsymbol{Q})$, we compute the conjugates of x.
6) Finally

$$R = \begin{pmatrix} 0.55329 & 0.76837 & -0.32166 \\ -0.32166 & 0.55329 & 0.76837 \\ 0.76837 & -0.32166 & 0.55329 \end{pmatrix}.$$

D. The Minimum Product Distance

Since the ideal $\mathcal{A}$ given in (5) is principal in all the cases and dimensions that we consider, we can give the minimum product distance using Theorem 1, namely, $d_{\mathrm{p,min}} = \frac{1}{\sqrt{d_K}}$. Some numerical values of $d_{\mathrm{p,min}}$ for the Cases I and II are reported in Table II.

We have seen that for each prime dimension n, several constructions of lattices are avilable, all yielding maximum diversity. The minimum product distance gives us a way to rank them. For example, for $n = 5$, we can build the following lattices depending on the choice of the primes p:

1) only 11 ramifies, with $d_p = 1/121$ (Case I);
2) only 31 ramifies, with $d_p = 1/961$ (Case I);
3) only 5 ramifies, with $d_p = 1/625$ (Case II);
4) 11 and 31 ramify, with $d_p = 1/(121 \times 961)$ (Case III);
5) 11 and 5 ramify, with $d_p = 1/(121 \times 625)$ (Case III).

Since our aim is to maximize the $d_{\mathrm{p,min}}$, in this example, the best choice is to take the first construction in the preceding list, i.e., when only one prime ramifies, this prime being the smallest possible. This appears to be true in general.

Proposition 5: For a given prime dimension $n > 2$, the construction of Case I, with the smallest possible p maximizes the minimum product distance.

Proof:

1) We first show that the discriminant of K in Case I is $d_K = p^{n-1}$. Since p is totally ramified in K, $pO_k = \mathfrak{p}^n$. This implies, since $p \nmid n$, that $\mathfrak{p}^{n-1} | \mathcal{D}_{K/\boldsymbol{Q}}$ but $\mathfrak{p}^n \nmid \mathcal{D}_{K/\boldsymbol{Q}}$[13]. Thus, from Fact 3, we have $N(\mathcal{D}_{K/\boldsymbol{Q}}) = d_K = p^{n-1}$, since $\mathcal{D}_{K/\boldsymbol{Q}} = \mathfrak{p}^{n-1}$. In order to maximize $d_{\mathrm{p,min}}$, one has to take the smallest $p > n$ that ramifies. This also shows that Case III is always worse than Case I as $d_K = (p_1p_2)^{n-1}$.

TABLE II
SOME MINIMUM PRODUCT DISTANCES FOR CASES I AND II, N IS SUCH THAT $K \subseteq \mathbb{Q}(\zeta_N)$

n	N	d_K	$d_{\mathrm{p,min}}$	$\sqrt[n]{d_{\mathrm{p,min}}}$
3	7	7^2	$1/7$	0.522757958
3	13	13^2	$1/13$	0.425290370
5	11	11^4	$1/11^2$	0.383215375
5	31	31^4	$1/31^2$	0.253195115
7	29	29^6	$1/29^3$	0.236188093
11	23	23^{10}	$1/23^5$	0.240454440
11	67	67^{10}	$1/67^5$	0.147899259
13	53	53^{12}	$1/53^6$	0.160022248
17	103	103^{16}	$1/103^8$	0.112923019
19	191	191^{18}	$1/191^9$	0.083082682
23	47	47^{22}	$1/47^{11}$	0.158599211
29	59	59^{28}	$1/59^{14}$	0.139670898
3	9	9^2	$1/9$	0.480749856
5	25	5^8	$1/5^4$	0.275945932
7	49	7^{12}	$1/7^6$	0.188638463

2) Using the same technique as in the previous case, we find $\mathfrak{p}^n | \mathcal{D}_{K/\mathbb{Q}}$, but now we can have $\mathfrak{p}^k | \mathcal{D}_{K/\mathbb{Q}}$, for $k > n$. Consider the transitivity formula for the different [13]

$$\mathcal{D}_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \mathcal{D}_{\mathbb{Q}(\zeta)/K}\mathcal{D}_{K/\mathbb{Q}}. \tag{10}$$

Denote $\mathfrak{p} = (1-\zeta)O_{\mathbb{Q}(\zeta)}$, $\mathfrak{p}_K = \mathfrak{p} \cap O_K$ and note that

$$\mathfrak{p}_K O_{\mathbb{Q}(\zeta)} = \mathfrak{p}^{n-1}$$

as p is totally ramified. It is known that $\mathcal{D}_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \mathfrak{p}^{n(2n-3)}$ and that $\mathcal{D}_{\mathbb{Q}(\zeta)/K} = \mathfrak{p}^{n-2}$[13]. From (10) we then obtain that

$$\mathcal{D}_{K/\mathbb{Q}} = \mathfrak{p}^{2(n-1)^2} = (\mathfrak{p}^{n-1})^{2(n-1)} = \mathfrak{p}_K^{2(n-1)}.$$

From Fact 3, we have

$$d_K = N_{K/\mathbb{Q}}(\mathfrak{p}_K^{2(n-1)}) = p^{2(n-1)}.$$

It follows that as long as $n^2 > p$ (true for $n > 2$), the minimum distance is smaller than in the case where $p > n$. □

VI. MIXED CONSTRUCTIONS

Here, we present a technique to combine the previous constructions to build rotated $\mathbb{Z}^n$-lattices in higher dimensions.

Proposition 6: Let K be the compositum of N Galois extensions K_j of degree n_j (i.e., the smallest field containing all K_j) with coprime discriminant i.e., $(d_{K_i}, d_{K_j}) = 1, \forall i \neq j$. Assume there exists an α_j such that the trace form over K_j, $\mathrm{Tr}(\alpha_j xy)$, is isomorphic to the unit form $\langle 1, \ldots, 1\rangle$ of degree n_j for $j = 1, \ldots, N$. Then the form over K

$$\mathrm{Tr}(\alpha_1 xy) \otimes \cdots \otimes \mathrm{Tr}(\alpha_N xy)$$

is isomorphic to the unit form $\langle 1, \ldots, 1\rangle$ of degree $n = \prod_{j=1}^{N} n_j$.

Proof: Let us consider the case $K = K_1K_2$. Denote by $\{\omega_1, \ldots, \omega_{n_1}\}$ and $\{\omega'_1, \ldots, \omega'_{n_2}\}$ the integral bases of K_1 and K_2, respectively. Since K_1 and K_2 are Galois extension over $\mathbb{Q}$ with coprime discriminants, we have that $\{\omega_j\omega'_k \mid j = 1, \ldots, n_1,\ k = 1, \ldots, n_2\}$ defines a basis for O_K[13]. We conclude using the fact that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1\omega_i\omega_j\alpha_2\omega'_k\omega'_l) = \mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha_1\omega_i\omega_j)\mathrm{Tr}_{K_2/\mathbb{Q}}(\alpha_2\omega'_k\omega'_l).$$

□

TABLE III
MINIMUM PRODUCT DISTANCES FOR THE MIXED CONSTRUCTIONS

n	$d_{\mathrm{p,min}}$	$\sqrt[n]{d_{\mathrm{p,min}}}$	n	$d_{\mathrm{p,min}}$	$\sqrt[n]{d_{\mathrm{p,min}}}$
4	$1/(5\cdot 8)$	0.39763536	22	$1/\sqrt{5^{11}23^{20}}$	0.16080157
6	$1/\sqrt{5^3 7^4}$	0.34958931	24	$1/\sqrt{7^{16}17^{21}}$	0.15134889
10	$1/\sqrt{5^5 11^8}$	0.25627156	25	$1/(5^{20}11^{10})$	0.10574672
12	$1/\sqrt{5^6 13^{10}}$	0.22967537	27	$1/\sqrt{7^{18}19^{24}}$	0.14124260
15	$1/\sqrt{7^{10}11^{12}}$	0.20032888	28	$1/\sqrt{5^{14}29^{26}}$	0.14005125
16	$1/\sqrt{5^8 17^{14}}$	0.19361370	30	$1/\sqrt{11^{24}13^{25}}$	0.13161332
18	$1/\sqrt{5^9 19^{16}}$	0.18068519			

The lattice generator matrix can be immediatly obtained as the tensor product of the generator matrices $R^{(j)}$ corresponding to the forms $\mathrm{Tr}(\alpha_j xy)$, for $j = 1, \ldots, N$

$$R = R^{(1)} \otimes \cdots \otimes R^{(N)}.$$

In the particular case of the cyclotomic construction, Proposition 6 yields.

Corollary 1: Let $m = p_1 \cdots p_N$ be the product of N distinct primes, $\zeta_j = e^{-i2\pi/p_j}$ for $j = 1, \ldots, N$ and K be the compositum of

$$K_j = \mathbb{Q}(\zeta_j + \zeta_j^{-1}), \qquad j = 1, \ldots, N$$

(i.e., the smallest field containing all K_j). Let $\alpha_j = (1-\zeta_j)(1-\zeta_j^{-1})$ then

$$\frac{1}{p_1}\,\mathrm{Tr}(\alpha_1 xy) \otimes \cdots \otimes \frac{1}{p_N}\,\mathrm{Tr}(\alpha_N xy)$$

is isomorphic to the unit form $\langle 1, \ldots, 1\rangle$ of degree

$$n = \prod_{j=1}^{N}(p_j - 1)/2.$$

Corollary 1 generalizes the cyclotomic construction to $\mathbb{Q}(\zeta_m)$, where m is a square-free product of primes. We are now able to construct rotated $\mathbb{Z}^n$-lattices in other dimensions such as $n = 10, 12, 16, 22, 24, 27, 28, \ldots$.

The only missing dimensions below 30 are 4 and 25 and can be completed with the aid of Proposition 6.

1) The case $n = 4$ can be obtained combining the two rotated square lattices constructed in Section III-C.
2) The case $n = 25$ can be obtained combining the two rotated $\mathbb{Z}^n$-lattices of dimension 5 constructed using Case I and Case II of the cyclic constructions.

A. The Minimum Product Distance

For the mixed construction, we have the following.

Proposition 7: Let $K = K_1K_2$ be the compositum of two Galois extensions of degree n_1 and n_2, with coprime discriminant. The discriminant of K is $d_K = d_{K_1}^{m_1} d_{K_2}^{m_2}$, where $m_j = [K : K_j] = n/n_j$, $j = 1, 2$.

Proof: Since $D_{K/\mathbb{Q}} = D_{K_1/\mathbb{Q}}D_{K_2/\mathbb{Q}}$ (see [13]), we directly deduce that

$$\begin{aligned} N_{K/\mathbb{Q}}(D_{K/\mathbb{Q}}) &= N_{K/\mathbb{Q}}(D_{K_1/\mathbb{Q}})N_{K/\mathbb{Q}}(D_{K_2/\mathbb{Q}}) \\ &= N_{K_1/\mathbb{Q}}(D_{K_1/\mathbb{Q}})^{m_1}N_{K_2/\mathbb{Q}}(D_{K_2/\mathbb{Q}})^{m_2} \end{aligned}$$

which proves the result, recalling that $N_{K/\mathbb{Q}}(D_{K/\mathbb{Q}}) = d_K$. □

TABLE IV
COMPARISON OF THE VALUES OF $\sqrt[n]{d_{\mathrm{p,min}}}$ FOR CYCLOTOMIC, CYCLIC, AND MIXED CONSTRUCTIONS

n	Cyclotomic constructions	Cyclic constructions	Mixed constructions
2	0.66874030	-	-
3	0.52275795	0.52275795	-
4	-	-	0.39763536
5	0.38321537	0.38321537	-
6	0.34344479	-	0.34958931
7	-	0.23618809	-
8	0.28952001	-	-
9	0.27018738	-	-
10	-	-	0.25627156
11	0.24045444	0.24045444	-
12	-	-	0.22967537
13	-	0.16002224	-
14	0.20942547	-	-
15	0.20138689	-	0.20032888
16	-	-	0.19361370
17	-	0.11292301	-
18	0.18174408	-	0.18068519
19	-	0.08308268	-
20	0.17136718	-	-
21	0.16678534	-	-
22	-	-	0.16080157
23	0.15859921	0.15859921	-
24	-	-	0.15134889
25	-		0.10574672
26	0.14825905	-	-
27	-	-	0.14124260
28	-	-	0.14005125
29	0.13967089	0.13967089	-
30	0.13711677	-	0.13161332

As a direct consequence, we have that for the mixed construction

$$d_{\mathrm{p,min}} = \frac{1}{\sqrt{d_{K_1}^{m_1} d_{K_2}^{m_2}}}.$$

The numerical values for $d_{\mathrm{p,min}}$ are given in Table III. We note that the lattices in dimensions $n = 4$ and 25 have minimum product distance $1/40$ and $1/(5^{20}11^{10})$ given by Proposition 7.

VII. PERFORMANCE

A rotated $\boldsymbol{Z}^n$-lattice with diversity L is obtained by applying the rotation matrix R to the integer grid $\boldsymbol{Z}^n$, i.e.,

$$Z_{n,L} = \{\boldsymbol{x} = \boldsymbol{u}R,\ \boldsymbol{u} \in \boldsymbol{Z}^n\}.$$

The finite signal constellation is carved from this lattice by restricting the elements of $\boldsymbol{u}$ to a finite set of integers such as $\{\pm 1, \pm 3, \ldots, \pm(2^{\eta/2} - 1)\}$, where η is the spectral efficiency measured in bits per two dimensions.

The newly constructed rotated $\boldsymbol{Z}^n$-lattice constellations have been simulated over an independent Rayleigh fading channel of the form

$$\boldsymbol{r} = \boldsymbol{g} \odot \boldsymbol{x} + \boldsymbol{n}$$

where $\boldsymbol{r} = (r_1, r_2, \ldots r_n) \in \boldsymbol{R}^n$ is the received vector, $\boldsymbol{n} = (n_1, n_2, \ldots n_n) \in \boldsymbol{R}^n$ is a noise vector, whose real components n_i are zero mean, $N_0/2$ variance Gaussian distributed independent random variables, $\boldsymbol{g} = (g_1, g_2, \ldots g_n) \in \boldsymbol{R}^n$ are the Rayleigh distributed random fading coefficients with $E[g_i^2] = 1$, and $\odot$ represents the component-wise product.

Performance of $Z_{n,L}$ depends on its modulation diversity L and its minimum product distance $d_{\mathrm{p,min}}$. Best minimum product distance lattices among the families we considered are summarized in Table IV. A few observations are appropriate at this point. When both cyclotomic and cyclic constructions are available in the same dimension we find the same values for $d_{\mathrm{p,min}}$, suggesting that the same field is used. The mixed construction yields a higher $d_{\mathrm{p,min}}$, only for $n = 6$.

For $n = 3, 5, 9, 11, 15$ *ad hoc* constructions were given in [5] without the values of $d_{\mathrm{p,min}}$. Since they are based on the field $\boldsymbol{Q}(\zeta_p + \zeta_p^{-1})$, they have the same $d_{\mathrm{p,min}}$ as our cyclotomic construction (see Theorem 1). For the case $n = 2^m$ given in [7], constructed from the field $\boldsymbol{Q}(\zeta_{8n} + \zeta_{8n}^{-1})$, our schemes result in higher $d_{\mathrm{p,min}}$, e.g., for $n = 8$ we find 0.28952001 against 0.26106844 and for $n = 16$ we find 0.19361370 against 0.18064760.

Figs. 6 and 7 show the bit-error rates of the rotated $\boldsymbol{Z}^n$ constellations for $\eta = 2$ and for the cyclotomic and cyclic constructions. For comparison, the performance of a standard component interleaved quaternary phase-shift keying (QPSK) over Gaussian and Rayleigh fading channels is reported in the figures. We can observe how the bit-error rate performance over Rayleigh fading channel approaches the one over the Gaussian channel as the diversity increases. Clearly, this gain is obtained at the expense of a higher decoding complexity due to the greater lattice dimension [9], [14], but no extra bandwidth is used.

VIII. CONCLUSION

In this correspondence, we constructed two families of full-diversity rotated $\boldsymbol{Z}^n$-lattices using the theory of ideal lattices: one based on cy-

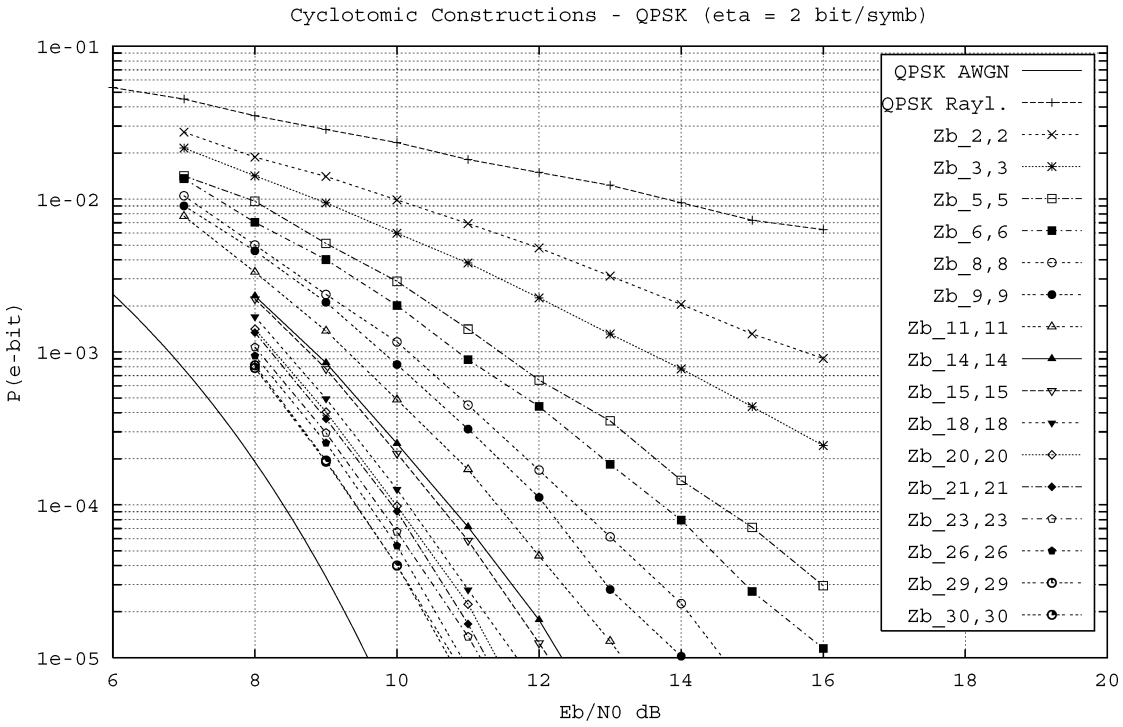

Fig. 6. Cyclotomic construction with QPSK.

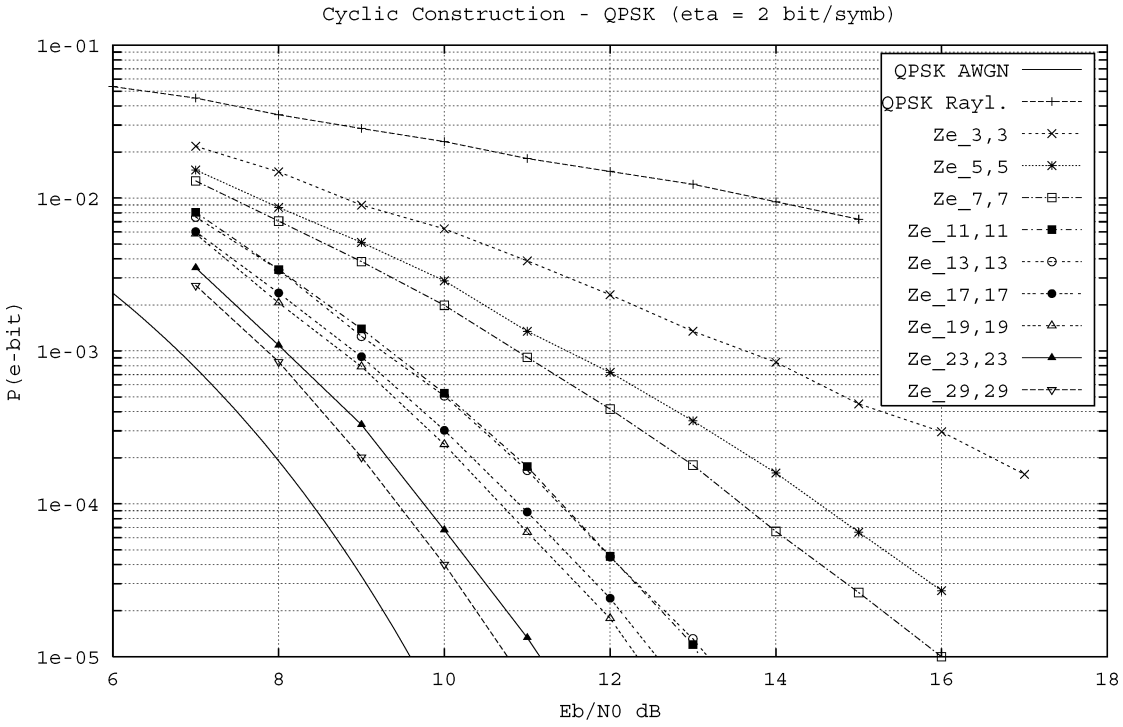

Fig. 7. Cyclic construction with QPSK.

clotomic fields, the other based on cyclic fields. We also provided a way of combining the constructions in order to obtain some missing dimensions.

The performance in terms of minimum product distance is clearly given by means of explicit formulas related to the field discriminant. The cyclotomic constructions give better results when compared to the cyclic ones in the same dimension. The cyclotomic $(n = (p-1)/2)$, cyclic $(n = p)$ and mixed constructions enable to build a rotated $\boldsymbol{Z}^n$-lattice for all dimensions. We gave explicit numerical values for dimensions from 2 to 30. Future work will involve the search for optimal rotated $\boldsymbol{Z}^n$-lattices in terms of maximal minimum product distance and constructions of maximum diversity complex $\boldsymbol{Z}[i]^n$-lattices.

ACKNOWLEDGMENT

The authors would like to thank Dr. Stéphane Vinatier for helpful discussions.

REFERENCES

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

[2] J. C. Belfiore, X. Giraud, and J. Rodriguez, "Optimal linear labeling for the minimization of both source and channel distortion," in *Proc. IEEE Int. Symp. Information Theory*, Sorrento, Italy, June 2000, p. 404.

[3] K. Boullé and J. C. Belfiore, "Modulation schemes designed for the Rayleigh channel," in *Proc. CISS'92*, 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. Inform. Theory*, vol. 42, 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. Inform. Theory*, vol. 44, pp. 1453–1467, July 1998.

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

[7] M. O. Damen, K. Abed-Meraim, and J. C. Belfiore, "Diagonal algebraic space–time block codes," *IEEE Trans. Inform. Theory*, vol. 48, pp. 628–636, Mar. 2002.

[8] B. Erez, "The Galois structure of the trace form in extensions of odd prime degree," *J. Algebra*, vol. 118, pp. 438–446, 1988.

[9] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comput.*, vol. 44, pp. 463–471, Apr. 1985.

[10] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*. Cambridge, U.K.: Cambridge Univ. Press, 1991.

[11] X. Giraud, E. Boutillon, and J. C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. Inform. Theory*, vol. 43, pp. 938–952, May 1997.

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

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

[14] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1639–1642, July 1999.

[15] M. Pohst, "KASH/KANT–Computer Algebra System," Tech. Univ. Berlin, Berlin, Germany. [Online] Available: http://www.math.tu-berlin.de/algebra/.

[16] 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/.

Generalized Self-Shrinking Generator

Yupu Hu and Guozhen Xiao

***Abstract*—In this correspondence, we present a simple bit-stream generator. It is a specialization of shrinking generator and a generalization of self-shrinking generator. We call it "generalized self-shrinking generator." The family of such generated sequences has a group structure. The correlation between the sequences is quite good and the sequences themselves are balanced. For each $k, 0 < k < n$, no more than $1/2^{n-k}$ of the sequences have least periods less than 2^k. No more than $1/4$ of the sequences have least periods less than 2^{n-1}. There are two sequences with least periods of 2. There is no sequence with a least period p such that $2 < p < n/2$.**

***Index Terms*—Least period, m-sequence, self-shrinking generator, shrinking generator, stream cipher.**

I. INTRODUCTION: DEFINITION AND SOME FACTS

Pseudorandom sequences have many applications in cryptography (for example, stream ciphers) and communication engineering (for example, code-division multiple access (CDMA)). The pseudorandomness of a periodic sequence includes many factors, such as its least period, its autocorrelation feature, its balance feature, its run distribution, etc. For stream cipher applications, another important factor for information security, called linear complexity, should be considered. In designing a periodic sequence for a stream cipher, an equally important component is the ease with which it can be generated. For the sake of pseudorandomness and simplicity, Coppersmith, Krawczyk, and Mansour [1] proposed a "shrinking generator." Later, Meier and Staffelbach [2] proposed a "self-shrinking generator," as a special case of the "shrinking generator." The definition of "self-shrinking generator" is as follows.

Definition 1: [2] Let $a = a_0a_1a_2\ldots$ be an m-sequence on GF(2), with the least period $2^n - 1$. Output a_k if $a_{k-1} = 1$, or no output if $a_{k-1} = 0$, $k = 1, 3, 5, \ldots$. The output sequence $b = b_0b_1b_2\ldots$ is called a *self-shrinking sequence*.

The self-shrinking sequence has many advantages in cryptography, such as its simplicity for generation, balance, and period of no less than $2^{[n/2]}$. It is known that the linear complexity of a periodic sequence is more than 2^{l-1} if its least period is 2^l. This means that the linear complexity of a self-shrinking sequence is more than $2^{[n/2]-1}$. Blackburn [3] gave concrete results about the self-shrinking sequence's linear complexity. Some cryptanalysis of self-shrinking sequence were given by Mihaljevic [4], Zenner, Krause, and Lucks [5], and Krause [6].

In this correspondence, we present the "generalized self-shrinking generator." This concept is a specialization of "shrinking generator" [1], and a generalization of "self-shrinking generator" [2]. The family of generalized self-shrinking sequences has a group structure and includes self-shrinking sequence as a special case. The correlation feature between the two sequences is quite good except that one is the complemented sequence of the other. All such sequences are balanced except sequences "$00\ldots$" and "$11\ldots$." For each $k, 0 < k < n$, no more than $1/2^{n-k}$ of the sequences have least periods less than 2^k. No more than

Manuscript received March 3, 2003; revised September 24, 2003. This work was supported in part by the Natural Science Foundation of China under Grant 60273084 and Doctoral Foundation under Grant 20020701013.

Y. Hu is with the ISN National Key Laboratory, Xidian University, Xi'an, China (e-mail: yphu8969@sohu.com).

G. Xiao is with the Information Security and Privacy Institute, Xidian University, Xi'an, China (e-mail: xiaogz@ xidian.edu.cn).

Communicated by K. G. Paterson, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2004.825256