New algebraic constructions of rotated cubic lattice constellations for the Rayleigh fading channel

F. Oggier†, E. Bayer-Fluckiger†, E. Viterbo‡

Abstract—**In this paper we present new algebraic constructions of rotated cubic lattice constellations of prime dimension based on cyclic fields. The resulting constellations have full diversity and can be ranked according to the minimum product distance, a relevant performance parameter for transmission over the Rayleigh fading channel.**

I. Introduction

ROTATED cubic lattice signal constellations with specified *modulation diversity* have been proposed for transmission over the fading channel [3]. Given a cubic lattice constellation the desired modulation diversity is obtained by applying a suitable rotation. In [2] 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 full diversity ($L = n$) equal to the dimension of the lattice constellation (or the degree of K). Another relevant parameter is given by minimum product distance $d_{p,min}$ of the lattice constellation. In particular, it is also important to maximize $d_{p,min}$ when chosing a lattice constellation for transmission over the Rayleigh fading channel.

In [3] a few examples of rotated cubic lattice constellations from totally real fields were found by an exhaustive search. In this work, we consider the construction of a family of rotated cubic lattice constellations for all prime dimensions using cyclic fields.

A. Basic definitions

We introduce some definitions and facts that will be used in this work, though we assume basic knowledge about fields and ideals. The interested reader may refer to [5] for an introduction to algebraic number theory.

Let $K = \mathbf{Q}(\theta)$ be an extension of $\mathbf{Q}$ of degree n. If the minimal polynomial of θ over $\mathbf{Q}$ has all its roots in K, we say that K is a *Galois extension* of $\mathbf{Q}$. The set $\mathrm{Gal}(K/\mathbf{Q}) = \{\sigma : K \to K \mid \sigma(x) = x,\ \forall x \in \mathbf{Q}\}$ is a group and is called the *Galois group* of K over $\mathbf{Q}$. 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 I.1: Let $x \in K$ and $\mathrm{Gal}(K/\mathbf{Q}) = \{\sigma_i\}_{i=1}^n$. The *trace* of x over $\mathbf{Q}$ is defined as $\mathrm{Tr}_{K/\mathbf{Q}}(x) = \sum_{i=1}^n \sigma_i(x)$, while the *norm* of x is $N_{K/\mathbf{Q}}(x) = \prod_{i=1}^n \sigma_i(x)$.

Definition I.2: Let $O_K = \{x \in K \mid \exists$ monic polynomial $f \in \mathbf{Z}[X]$ such that $f(x) = 0\}$. Then O_K is a ring called the *ring of integers* of K.

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

Definition I.4: Let $\{x_1, ..., x_n\}$ be a $\mathbf{Z}$-basis of O_K. The number $d_K = D(x_1, .., x_n) = \det(\mathrm{Tr}_{K/\mathbf{Q}}(x_i x_j))$ is called the *discriminant* of K. We call the *discriminant ideal*, and denote by $d_K\mathbf{Z}$, the principal ideal of $\mathbf{Z}$ generated by the discriminant (the ideal is independent of the choice of a basis).

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

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

One of the key notions of algebraic number theory is the ramification property of an extension. Let $p \in \mathbf{Z}$. Consider $\mathfrak{p} = p\mathbf{Z}$, a prime ideal of $\mathbf{Z}$. 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 language) ramifies in O_K. If $pO_k = \mathfrak{P}^n$, we say that $\mathfrak{p}$ is *totally ramified* in O_K.

Fact I.2: A prime ideal $\mathfrak{p}$ of $\mathbf{Z}$ ramifies in O_K if and only if it contains the discriminant ideal.
We also introduce a useful definition for the analysis of the product distance.

Definition I.5: 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 $\mathfrak{a}$ is principal, then $N(\mathfrak{a}) = N(a)$.

Definition I.6: The set $D^{-1}_{K/\mathbf{Q}} = \{x \in K \mid \forall \alpha \in O_K,$ $\mathrm{Tr}_{K/\mathbf{Q}}(x\alpha) \in \mathbf{Z}\}$ is a fractional ideal of O_K called the *codifferent*. Its inverse ideal $D_{K/\mathbf{Q}}$ is an integral ideal of O_K called the *different*.

Fact I.3: $N(\mathcal{D}_{K/\mathbf{Q}}) = |d_K|$.

II. The cyclic constructions

We present a construction of rotated cubic lattice constellations using cyclic number fields.
Let K be a cyclic extension of $\mathbf{Q}$ of prime degree $n > 2$.

† Chaire d'algèbre et de géométrie, EPFL 1015 Lausanne, Switzerland, e-mail: `frederique.oggier@epfl.ch, eva.bayer@epfl.ch`.
‡ Dip. Elettronica, Politecnico di Torino, C.so Duca degli Abruzzi 24, 10129 Torino, Italy, e-mail: `viterbo@polito.it`.

Based on [4] we consider lattices constructed using the ideal $\mathcal{A}$ of O_K such that its square is the codifferent:

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

In [4], it is shown that there exists an element $x \in \mathcal{A}$ such that $\mathrm{Tr}_{K/\mathbf{Q}}(x\sigma^t(x)) = \delta_{0,t}p^2$, $t = 0, \ldots, n-1$. This results in the construction of rotated cubic lattices with full diversity $L = n$, since K is a totally real field (recall that K is a Galois field of odd degree).

The aim is to explicitly construct these lattices and analyze their product distance.

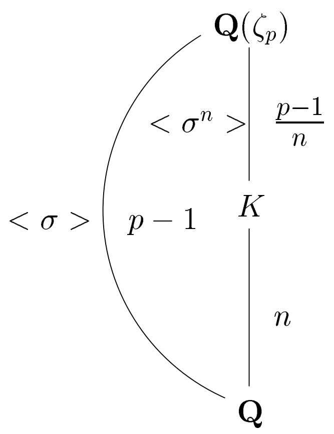
Let K be a cyclic extension of $\mathbf{Q}$ of prime degree $n > 2$ and let p be an odd prime. Depending on the ramification of $\mathfrak{p} = p\mathbf{Z}$ in O_K, we derive three different classes of lattices.

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

Here, due to space limitations, we present in detail only the first one. We emphasize the fact that we do not need an 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. Thus the knowledge of p and n is sufficient to construct the lattice. Concretely, this allows us to give construction algorithms that take as input any prime dimension n and any one of the primes p satisfying the existence hypotheses and gives as output the lattice generator matrix. Note that the implementation of these algorithms require the support of a computational algebra package such as KANT ([7]) or PARI([8]).

A. Construction where only $p \neq n$ ramifies

When only the prime $p \neq n$ ramifies in K, we can embed K in the cyclotomic field $\mathbf{Q}(\zeta)$, where $\zeta = \zeta_p$ is a primitive pth root of unity. Denote G =Gal($\mathbf{Q}(\zeta)/\mathbf{Q}$) the Galois group of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$. Then G is cyclic of order $p-1$. Let σ be a generator of G. Because $[\mathbf{Q}(\zeta) : K] = \frac{p-1}{n}$, note that σ^n is a generator of the cyclic group Gal($\mathbf{Q}(\zeta)/K$).



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

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

By definition of r, we may define σ by:

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

and the $p-1$ successive powers of σ form Gal($\mathbf{Q}(\zeta)/\mathbf{Q}$). By direct calculation, we can prove the following:

Lemma II.1: The following equalities hold:
(a) $\sigma(\alpha) = -\zeta^{p-1}\alpha$.
(b) $\sigma(\zeta^\lambda\alpha) = -\zeta^\lambda\alpha$.

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

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

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

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

$$\begin{aligned}
\mathrm{Tr}_{K/\mathbf{Q}}(x\sigma^t(x)) &= \sum_{a=0}^{n-1} \sigma^a\{x\sigma^t(x)\} \\
&= \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{a+cn}(z)\sigma^{a+t+jn}(z) \\
&= (-1)^t(-1)^m p \sum_c (-1)^c \sum_a \Bigg(\sum_j (-1)^j (1-\zeta^{r^{a+cn}}) \\
&\quad - \sum_j (-1)^j (\zeta^{r^{a+t+jn}} - \zeta^{r^{a+cn}+r^{a+t+jn}}) \Bigg)
\end{aligned} \tag{2}$$

We notice that the first term in parenthesis is 0 because there are as many 1s as -1s 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 (2) becomes:

$$(-1)^{t+m} p \sum_c (-1)^c \sum_{a,j} (-1)^j \zeta^{r^{a+cn}+r^{a+t+jn}} \tag{3}$$

The following identity can be proved by letting all the indexes run through all summation terms to verify that they cover the same set of exponents of ζ modulo p.

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

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

$$\sum_d (-1)^d \sum_{a,k} \zeta^{(r^{nd}+r^t)r^{nk+a}} = \sum_d (-1)^d \sum_{s=1}^{p-1} \omega_{d,t}^s \quad (4)$$

where

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

In order to evaluate (4), we distinguish two different cases. The case when $\omega_{d,t} = 1$ appears when

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

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

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

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:

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

and in the other case $t = 0$:

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

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

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

This proves that

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

■

n	p	r	λ
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

TABLE I
(*) MEANS THAT $K = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$

B. Application

The previous result gives a concrete method to construct x such that

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

is isomorphic to the identity matrix.

1) Choose a prime 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 of the cyclotomic field given by the powers of ζ up to $p-2$.
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 $\sigma^i(x)$, $i = 0,\dots,n-1$ 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 the Table I

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:

Lemma II.3: 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 $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ 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 $K/\mathbf{Q}$ is a Galois extension because $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ is cyclic. Furthermore, K inherits the property that p is exactly the only prime which ramifies from $\mathbf{Q}(\zeta_p)$ (see [6]). ■

C. 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, altough in this case $K = \mathbf{Q}(\theta)$ 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 $\mathbf{Q}(\zeta)$, where $\zeta = \zeta_{13}$, we obtain that $z = (3, 1, 4, 0, 2, 4, 2, 2, 2, 0, 2, 4)$.
5) We compute $x = \sigma^0(z) + \sigma^n(z) + \sigma^{2n}(z) + \sigma^{3n}(z)$, where $\sigma^n : \zeta \mapsto \zeta^{r^n} = \zeta^8$. We obtain that $x = (5, 0, 3, 3, -1, 0, -1, -1, 0, -1, 3, 3)$. Using 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) Using that $\zeta = e^{2i\pi/13}$, we compute M:

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

7) Normalizing

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

D. Product distance

Given an n-dimensional lattice constellation Λ with full diversity $L = n$, we define the *minimum product distance* as

$$d_{p,min} = \min_{x,y \in \Lambda} \prod_{i=1}^{n} |x_i - y_i| = \min_{x \in \Lambda} \prod_{i=1}^{n} |x_i|,$$

due to the lattice properties.
In [2], it was shown that $d_{p,min} = 1/(\sqrt{d_K})^n$, for lattices constructed from the ring of integers O_K of the field K. Here, we are interested in relating $d_{p,min}$ to the algebraic properties of the fields and ideals used to construct the lattice. It has been shown [2] that large product distance improves the perfomance of the lattices. Hence, we look for the best choice of p to obtain the maximum $d_{p,min}$. For all the dimensions given in Table II, the ideal $\mathcal{A}$ given in (1) is principal, so that we can easily compute the product distance.

Proposition 1: For the ideal $\mathcal{A}$ given in (1) we have

$$d_{p,min} = \min_{x \in \mathcal{A}} N(x) \stackrel{(i)}{=} N(\mathcal{A}) \stackrel{(ii)}{=} \frac{1}{\sqrt{d_K}} = \frac{1}{p^{(n-1)/2}}. \quad (5)$$

Proof. (i) Since $\mathcal{A}$ is principal, $\mathcal{A} = (a)$ and $N(\mathcal{A}) = N(a)$. Let $x \in \mathcal{A}$, then $x = ay$ for $y \in O_K$. Thus $N(x) = N(a)N(y) \geq N(\mathcal{A})$ and equality holds if and only if $y = 1$, i.e., $x = a$. (ii) It is a direct consequence of Fact I.3: $N(\mathcal{D}_{K/\mathbf{Q}}) = d_K$. The last equality holds since the discriminant of K in the case where only $p \neq n$ ramifies is p^{n-1}. (see [6]). ■

n	N	d_K	d_p	$\sqrt[n]{d_p}$
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

TABLE II
p IS SUCH THAT $K \subseteq \mathbf{Q}(\zeta_p)$.

As a direct consequence, maximizing the minimum product distance consists in choosing the smallest prime that ramifies. We also proved that the other two constructions yield lower minimum product distance for all $n > 3$. Numerical values for $d_{p,min}$ are shown in Table II.

III. Conclusions

In this paper, we presented an algebraic construction of families of cubic lattices of odd prime dimension based on cyclic fields. We derived the exact expression for the minimum product distance and we were able to select the best construction as the one maximizing $d_{p,min}$.

References

[1] E. Bayer-Fluckiger, "Lattices and Number Fields," *Contemporary Mathematics*, vol. 241,pp. 69–84, 1999.
[2] J. Boutros, E. Viterbo, C. Rastello, and J.C. Belfiore: "Good Lattice Constellations for both Rayleigh Fading and Gaussian Channels," *IEEE Transactions on Information Theory*, vol. 42, n. 2, pp. 502-518, March 1996.
[3] J. Boutros and E. Viterbo, "Signal Space Diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE Transactions on Information Theory*, vol. 44, n. 4, pp. 1453–1467, July 1998.
[4] B. Erez, "The Galois Structure of the Trace form in Extensions of Odd Prime Degree", *J. of Algebra*, vol. 118, pp. 438–446, 1988.
[5] P. Samuel, "Théorie algébrique des nombres" (also available in English), *Hermann* , 1971.
[6] H.P.F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*, University Press of Cambridge, 2001.
[7] KASH/KANT-computer algebra system, Prof. M. Pohst, Technische Universität, Berlin.
[8] PARI/GP-a software package for computer-aided number theory, C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier.