Recent results on signal constellation designs for transmission over Rayleigh fading channels

Emanuele VITERBO

Politecnico di Torino
C. Duca degli Abruzzi 24, 10129 Torino, Italy
viterbo@polito.it

Abstract – In this talk we review some recent algebraic constructions of rotated cubic lattice constellations for the Rayleigh fading channels.

1 Introduction[1]

Multidimensional cubic lattice signal constellations with specified modulation diversity have been recently proposed for transmission over the fading channel. Given a cubic lattice constellation the desired modulation diversity is obtained by applying a suitable rotation. Boutros et al. [2, 3] have 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 cubic lattices over totally real number fields.

In this paper, we give an overview of the new constructions of rotated cubic lattices using ideal lattices [1]. In particular, we analyze two families of totally real number fields: (i) the maximal real subfield of a cyclotomic field (ii) cyclic fields of odd prime degree. Then we provide a technique to combine these constructions to build rotated cubic lattices in higher dimensions.

2 Ideal lattices

Definition 1 *Let K be a totally real number field of degree n. An* ideal lattice *is an integral lattice $(\mathcal{I}, q_\alpha)$, where $\mathcal{I}$ is an O_K-ideal (which may be fractional) and*

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

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

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

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

where $\alpha_j = \sigma_j(\alpha),\ \forall j$. One easily verifies that the Gram matrix of this lattice is

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

When $\mathbf{G}$ is the $n \times n$ identity matrix we have an n-dimensional cubic lattice.

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

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

In order to compare among different lattices, we normalize the determinant D to be 1, so that

$$d_{p,min} = 1/\sqrt{d_K}$$

It is also useful to consider $d_{p,min}^{1/n}$ in order to compare among lattices of different dimensions.

3 Cyclotomic construction for $n = (p-1)/2$

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 rotated cubic n-dimensional lattices are built via the ring of integers of $K = \mathbf{Q}(\zeta + \zeta^{-1})$, the maximal real subfield of $\mathbf{Q}(\zeta)$, whose integral basis is given by $\{e_j = \zeta^j + \zeta^{-j}\}_{j=1}^n$.

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

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

is isomorphic to the unit form $< 1, \ldots, 1 >$ of degree n.

Using the above proposition, we construct rotated cubic lattices for $n = 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, 21, 23, 26, 29, 30, \ldots$. The lattice generated by the ring of integers has the $n \times n$ generator matrix $\mathbf{M}$ 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

$$\mathbf{A} = \mathrm{diag}\left(\sqrt{\sigma_k(\alpha)}\right)$$

The basis transformation matrix is given by

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

[1] This work was partly supported by CERCOM

Finally the rotated cubic lattice generator matrix is given by

$$\mathbf{R} = \frac{1}{\sqrt{p}}\,\mathbf{TMA}$$

By Theorem 1, the minimum product distance is given by $d_{p,min} = 1/\sqrt{d_K} = p^{-\frac{n-1}{2}}$, since $d_K = p^{\frac{p-3}{2}} = p^{n-1}$ (see Table below).

n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$
2	$1/\sqrt{5}$	0.66874030
3	$1/7$	0.52275795
5	$1/11^2$	0.38321537
6	$1/\sqrt{13^5}$	0.34344479
8	$1/\sqrt{17^7}$	0.28952001
9	$1/19^4$	0.27018738
11	$1/23^5$	0.24045444
14	$1/\sqrt{29^{13}}$	0.20942547
15	$1/31^7$	0.20138689
18	$1/\sqrt{37^{17}}$	0.18174408
20	$1/\sqrt{41^{19}}$	0.17136718
21	$1/43^{10}$	0.16678534
23	$1/47^{11}$	0.15859921
26	$1/\sqrt{53^{25}}$	0.14825905
29	$1/59^{14}$	0.13967089
30	$1/\sqrt{61^{29}}$	0.13711677

4 Cyclic construction in prime dimensions

Let K be a cyclic extension of $\mathbf{Q}$ of prime degree $n > 2$. Based on the work of Erez [4] we consider lattices constructed using the ideal $\mathcal{A}$ of O_K such that its square is the codifferent, i.e.,

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

Since a Galois extension of odd degree is totally real, we construct rotated cubic lattices with full diversity $L = n$. The construction is based on the existence of 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:

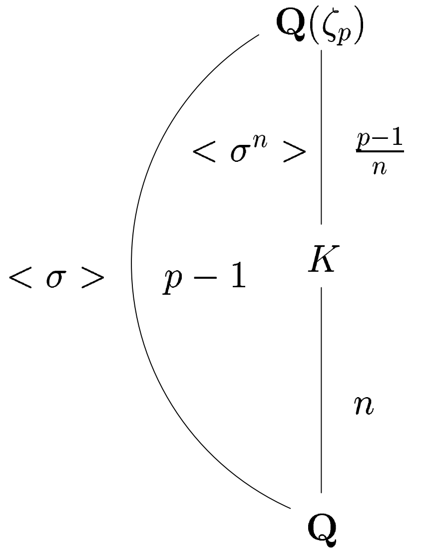
1. Case I: $p > n$ is the only prime which ramifies.
2. Case II: $p = n$ is the only prime which ramifies.
3. Case III: there are at least two primes p_1 and p_2 that ramify.

4.1 Case I

Proposition 2 *Let p such that $p \equiv 1$ (mod n). Let r be a primitive element (mod p), $\alpha = \prod_{i=0}^{m-1}(1-\zeta^{r^i})$, $m = \frac{p-1}{2}$ and let λ be such that $\lambda(r-1) \equiv 1$(mod p). Define $z = \zeta^{\lambda}\alpha(1-\zeta)$ and*

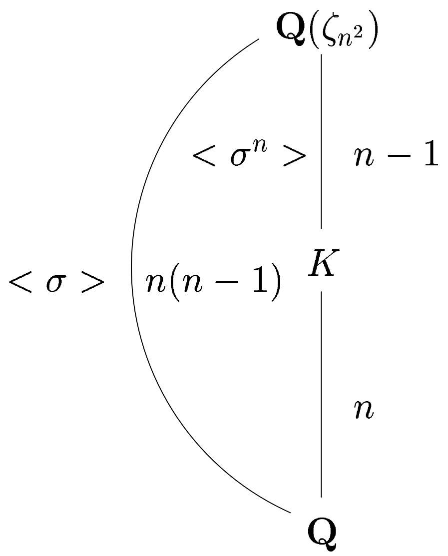
$$x = \mathrm{Tr}_{\,\mathbf{Q}(\zeta)/K}(z) = \sum_{j=1}^{\frac{p-1}{n}} \sigma^{jn}(z).$$

Then we have $Tr_{K/\mathbf{Q}}(x\sigma^t(x)) = \delta_{0,t}\,p^2$, $t = 0,\ldots,n-1$ (see diagram below).



4.2 Case II

If only the odd prime $p = n$ ramifies in K, we can embed K in $\mathbf{Q}(\zeta_{n^2})$, where $\mu = \zeta_{n^2}$ is a primitive n^2th root of unity (see diagram below).



Proposition 3 *Let $T = Tr_{\mathbf{Q}(\mu)/K}(\mu) = \sum_{j=1}^{n-1}\sigma^{nj}(\mu)$. Then*

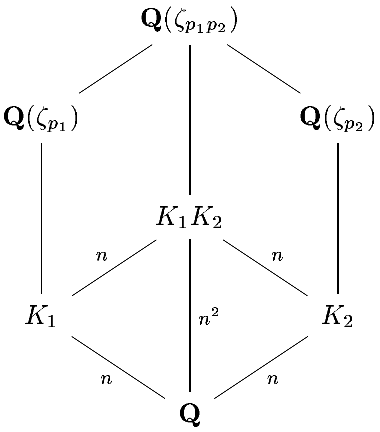
$$Tr_{K/\mathbf{Q}}((1+T)\sigma^t(1+T)) = \delta_{0,t}n^2, \quad t = 0,\ldots,n-1.$$

4.3 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 1 *Let n be an odd prime. Take two distinct odd primes p_1, p_2 such that $p_i \equiv 1$ (mod n), but $p_i \not\equiv 1$ (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, $i = 1,2$.*

The corresponding extension tower is shown below.



Proposition 4 *Let K_1, K_2 be two disjoint Galois extensions of $\mathbf{Q}$, whose discriminants are relatively prime.*
Let G_i =Gal$(K_i/\mathbf{Q})$ for $i = 1, 2$ and $G_1 =< \sigma >$, $G_2 =< \tau >$ 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

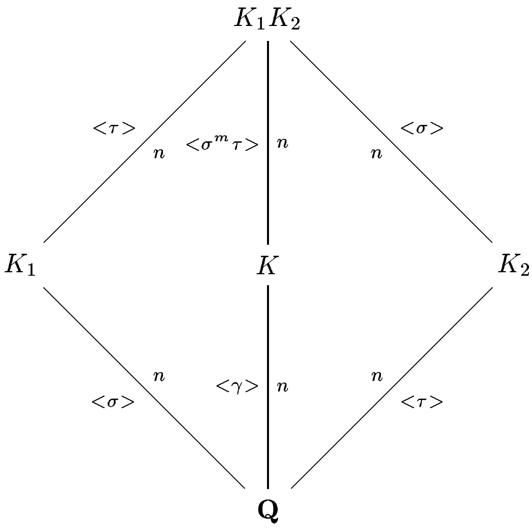
1. *Tr$_{K_1/\mathbf{Q}}(x_1\sigma^t(x_1)) = \delta_{0,t}p_1^2$, $t = 0, \ldots, n-1$*
2. *Tr$_{K_2/\mathbf{Q}}((x_2\tau^t(x_2)) = \delta_{0,t}p_2^2$, $t = 0, \ldots, n-1$*

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

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

where $<\gamma>= Gal(K/\mathbf{Q})$.

The detail of the extension tower for Case III is shown below.



5 Mixed constructions

Proposition 5 *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, $\text{Tr}\,(\alpha_j xy)$, is isomorphic to the unit form $< 1, \ldots, 1 >$ of degree n_j for $j = 1, \ldots, N$. Then the form over K*

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

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

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

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

Using as components two cyclotomic constructions we are now able to construct rotated cubic lattices in other dimensions such as $n = 10, 12, 16, 22, 24, 27, 28, \ldots$. The case $n = 4$ can be obtained combining the two distinct rotated square lattices and the case $n = 25$ can be obtained combining the two rotated cubic lattices of dimension 5 constructed using Case I and Case II cyclic constructions.

Proposition 6 *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 $m_j = [K : K_j] = n/n_j$, $j = 1, 2$.*

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

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

n	Cyclotomic	Cyclic	Mixed
2	0.66874030	-	-
3	0.52275795	0.52275795	-
4	-	-	0.02500000
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

6 Conclusions and future research

We have presented some new algebraic constructions of full-diversity rotated cubic lattices using the theory of ideal lattices: one based on cyclotomic 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

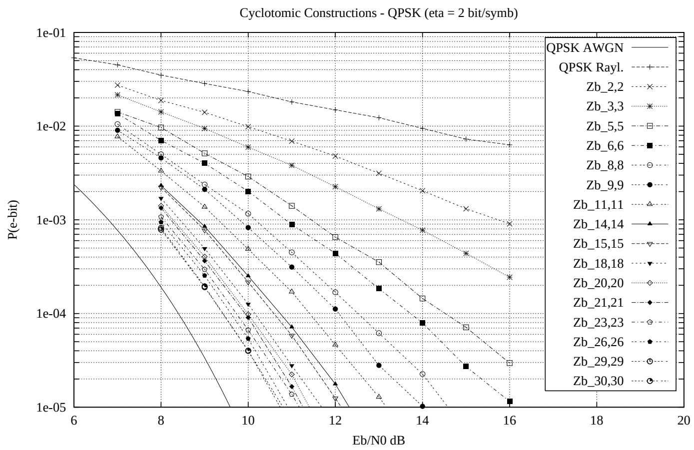


FIG. 1: BER for $L = n$, 2 bits/symbol

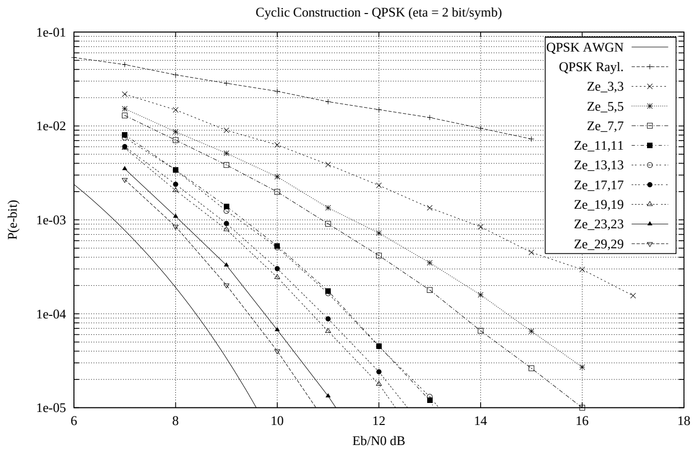


FIG. 2: BER for $L = n$, 2 bits/symbol

terms of minimum product distance is clearly given by means of explicit formulas related to the field discriminant. The cyclotomic constructions give better results in terms of $d_{p,min}$ when compared to the cyclic ones in the same dimension. The cyclotomic, cyclic and mixed constructions enable to build a rotated cubic lattice for all dimensions from 2 to 30.

Figures 1 and 2 show the bit error rate performance of the signal constellations with a spectral efficiency od 2bit/symbol obtained by simulation. Decoding is performed using the ML sphere decoder [5]. Future work will involve the search for maximal minimum product distance rotated cubic lattices in every dimension.

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] E. Viterbo and J. Boutros: "A Universal Lattice Code Decoder for Fading Channels," *IEEE Transactions on Information Theory*, vol. 45, n. 5, pp. 1639–1642, July 1999.