Cyclic Algebras for Noncoherent Differential Space-Time Coding

Frédérique Oggier
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA 91125
frederique@systems.caltech.edu

Abstract

We start the study of cyclic algebras for coding over the differential noncoherent channel. Cyclic algebras are an algebraic object that became popular for coherent space-time coding, since it naturally yields linear families of matrices with full-diversity. Coding for the differential noncoherent channel has a similar flavour in the sense that it asks for matrices that achieve full-diversity, except that these matrices furthermore have to be unitary. In this work, we give a systematic way to find infinitely many unitary matrices inside cyclic algebras, which yields for all dimensions. We show how cyclic algebras generalize previous families of unitary matrices obtained using the representation of fixed-point-free groups. As an application of our technique, we present families of codes for 3 and 4 antennas that achieve high diversity.

This work was supported by the Swiss National Science Foundation grant PBEL2-110209, and was started while the author was still with Laboratoire de mathématiques algorithmiques, Ecole Polytechnique Fédérale de Lausanne, 1015-Lausanne, Switzerland.

Cyclic Algebras for Noncoherent Differential Space-Time Coding

I. PRELIMINARY

Reliable mobile wireless transmission of high data rate is an important goal for telecommunications systems. It is now well understood that considering multiple antennas at the transmitter and/or receiver increases the data rate, while the use of space-time coding protects from the effect of fading. Two scenarios are traditionally distinguished: the *coherent case*, where the receiver is assumed to know the channel [20], and the *noncoherent case* , where we assume no channel information at the receiver. The noncoherent case is often a valid assumption for practical purposes, since detecting the channel requires training sequences, which is not always feasible (for example if one receiver is mobile). A popular approach to code without knowledge of the channel is to use differential unitary modulation [4], [5]. This strategy requires, as it will be recalled below, the design of unitary matrices that are *fully-diverse*, that is, that satisfy that the determinant of the difference of any two matrices is nonzero.

This problem has already been extensively studied. For example, in [8], a systematic parametrization has been done for the 2 antennas case, in order to get the highest possible diversity. In [3], Cayley codes have been proposed. These codes are based on the Cayley transform that maps the space of Hermitian matrices to the manifold of unitary matrices. There, the goal is not focused on maximizing the diversity, but on maximizing a mutual information criterion, in order to achieve high rate. Among the different other approaches investigated so far, let us emphasize the following algebraic ones. The representation of fixed point free groups has been studied in [18]. Fixed point free groups are groups with a unitary representation with no eigenvalue at 1, which yield fully diverse codes. The work in [18] gives a complete classification of finite groups that are fixed point free. Finite groups however do not allow high data rate, which led to consider infinite groups, and the representation of Lie groups. In [6], codes for 3 antennas have been built on the Special Unitary group $SU(3)$, while in [7], the Symplectic group $Sp(2)$ is used for 4 antennas codes.

For the sake of completeness, let us first recall the idea behind differential unitary modulation.

A. Differential unitary space-time modulation

Consider a Rayleigh flat fading channel with M transmit antennas and N receive antennas, with *unknown channel information*. The channel is used in blocks of M channel uses, so that the transmitted signal can be represented as an $M \times M$ matrix $\mathbf{S}_t$, where $t = 0, 1 \ldots$ represents the block channel use. If we assume that the channel is constant over M channel uses, we may write it as

$$\mathbf{Y}_t = \sqrt{\rho}\mathbf{S}_t\mathbf{H}_t + \mathbf{W}_t, \ t = 0, 1, \ldots \tag{1}$$

Here $\mathbf{H}_t$, the channel matrix, and $\mathbf{W}_t$, the noise matrix, are two $M \times N$ matrices with independent complex normal coefficients, and ρ is the expected SNR at each receiver antenna.

We use *differential unitary space-time modulation* [4], [5]. The transmitted signal $\mathbf{S}_t$ is encoded using differential modulation, that is (assuming $\mathbf{S}_0 = \mathbf{I}$)

$$\mathbf{S}_t = \mathbf{X}_{z_t}\mathbf{S}_{t-1}, \ t = 1, 2, \ldots, \tag{2}$$

where $z_t \in \{0, \ldots, L-1\}$ is the data to be transmitted, and $\mathcal{C} = \{\mathbf{X}_0, \ldots, \mathbf{X}_{L-1}\}$ the constellation to be designed. It can be seen from the above equation that the codebook has to contain *unitary* matrices, to prevent $\mathbf{S}_t$ to tend either to zero or infinity.

Note that since the channel is used M times, the transmission rate is

$$R = \frac{1}{M}\log_2 L. \tag{3}$$

The size $|\mathcal{C}|$ of the constellation is thus $L = 2^{MR}$.

If we further assume the channel constant for $2M$ consecutive uses, we get from Equations (1) and (2) that

$$\begin{aligned} \mathbf{Y}_t &= \sqrt{\rho}\mathbf{X}_{z_t}\mathbf{S}_{t-1}\mathbf{H} + \mathbf{W}_t \\ &= \mathbf{X}_{z_t}(\mathbf{Y}_{t-1} - \mathbf{W}_{t-1}) + \mathbf{W}_t \\ &= \mathbf{X}_{z_t}\mathbf{Y}_{t-1} + \mathbf{W}'_t, \end{aligned}$$

where $\mathbf{W}'_t = \mathbf{W}_t - \mathbf{X}_{z_t}\mathbf{W}_t$ is statistically independent of $\mathbf{X}_{z_t}$, since $\mathbf{X}_{z_t}$ is unitary. Since the matrix $\mathbf{H}$ does not appear in the last equation, this means that differential modulation allows decoding without knowledge of the channel.

The maximum likelihood decoder is thus given by

$$\hat{z}_t = \arg \min_{l=0,\dots,|\mathcal{C}|-1} \|\mathbf{Y}_t - \mathbf{X}_l \mathbf{Y}_{t-1}\|.$$

At high SNR, the pairwise block probability of error P_e can be upper bounded by [4], [5]

$$P_e \leq \left(\frac{1}{2}\right)\left(\frac{8}{\rho}\right)^{MN} \frac{1}{|\det(\mathbf{X}_i - \mathbf{X}_j)|^{2N}}.$$

Clearly, the bigger $\det(\mathbf{X}_i - \mathbf{X}_j)$, $i \neq j$, is, the better the code will perform. Thus the *diversity product*, given by,

$$\zeta(\mathcal{C}) = \frac{1}{2} \min_{\mathbf{X}_i \neq \mathbf{X}_j} |\det(\mathbf{X}_i - \mathbf{X}_j)|^{1/M} \qquad \forall\ \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C} \tag{4}$$

has been defined as a measure of the quality of the code. We say that *full diversity* is achieved when

$$\det(\mathbf{X}_i - \mathbf{X}_j) \neq 0 \qquad \forall\ \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}.$$

A design criterion can be summarized as follow: find a code constellation $\mathcal{C}$ of $L = 2^{MR}$ unitary matrices such that $\zeta(\mathcal{C})$ is maximized. Actually, a more realistic goal is first to guarantee that $\zeta(\mathcal{C}) > 0$. Note that among the previous works cited, all [8], [18], [6], [7] but [3] focused on maximizing the diversity product.

B. Organization and contribution of this work

The purpose of this work is to investigate the possible applications of cyclic algebras to noncoherent differential MIMO coding. Our motivation comes from the following observation: differential unitary space-time coding has this in common with coherent space-time coding that it requires fully-diverse matrices. In the coherent scenario, cyclic algebras have been proven to be an efficient tools [17], [9], exactly by providing linear families of fully-diverse matrices. It is thus natural to wonder whether such algebras are a suitable tool for our problem. This mainly reduces to the question of how to find unitary matrices inside a cyclic algebra. Furthermore, though a lot of research has been done on this problem, there is not so far a scheme that appears to be *the* solution. The representation of fixed point free groups [18] offers a nice systematic method for n number of antennas, however, fails to yield high rate. Cayley codes [3] offer an easy encoding, a decoding algorithm based on the Sphere Decoder [19], [2], and high rate, however, an heavy optimization is required for each number of transmit antennas and rate. The Lie groups based codes [6], [7] are optimized respectively for 3 and 4 antennas, while one may wonder about a general method that would perform reasonably well for different numbers of antennas.

The contribution of this work aims at showing that cyclic algebras are indeed a suitable tool for noncoherent differential space-time coding design. In particular, we explain in Subsection II-B how cyclic algebras generalize a wide family of codes obtained via fixed point free groups [18]. We then give in Section III a systematic method to build infinitely many unitary matrices in a cyclic algebra, and thus for all dimensions n, which will be illustrated in Section IV with a worked out example. As an application of our technique, we give in Section V new code constructions for the 3 and 4 antennas case that reach high diversity (for example comparable to the one reached by Lie groups based codes [6], [7]). We start by introducing cyclic algebras.

II. Introducing Cyclic Algebras

As recalled in the introduction, the main design criterion for noncoherent differential coding is the diversity product

$$\zeta(\mathcal{C}) = \frac{1}{2}\min_{\mathbf{X}_i \neq \mathbf{X}_j} |\det(\mathbf{X}_i - \mathbf{X}_j)|^{1/M} \qquad \forall\ \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}.$$

The main difficulty in evaluating this quantity clearly comes from the non-linearity of the determinant. It is easy to find two matrices with determinant nonzero such that their difference has zero as determinant. The first important idea behind considering algebras of matrices is that if $\mathbf{X}_i, \mathbf{X}_j$ are in an algebra $\mathcal{A}$, then $\mathbf{X}_i - \mathbf{X}_j = \mathbf{X}_k$, another matrix in $\mathcal{A}$. We thus get rid of the non-linearity difficulty. The second idea is that since $\det(\mathbf{X}) \neq 0$ means the matrix $\mathbf{X}$ is invertible, if the matrix algebra we consider contains only invertible elements (namely, the algebra is a field, called a *division algebra*), then we guarantee full diversity, simply by starting with the right object. This idea has already been exploited successfully for the coherent case [9], [17], where the full diversity criterion is the same [20]. The aim here is to look for unitary matrices inside division algebras. We focus on the so-called cyclic algebras, defined in the next section. Note that the next section does assume some algebraic background. We let the reader refer to [9], which already contains a short tutorial with the useful background for that topic. Other references are, for example, [11], [16] for an introduction to algebraic number theory, [15] for basics about Galois theory, [13] for learning more about central simple algebras and cyclic algebras in particular).

A. Basic definitions

Let L/K be a Galois extension of degree n such that its Galois group $G = \mathrm{Gal}(L/K)$ is cyclic, with generator σ. Denote by K^* (resp. L^*) the non-zero elements of K (resp. L), and choose an element $\gamma \in K^*$. We construct a non-commutative algebra, denoted by $\mathcal{A} = (L/K, \sigma, \gamma)$, as follows:

$$\mathcal{A} = L \oplus eL \oplus \ldots \oplus e^{n-1}L$$

such that e satisfies

$$e^n = \gamma \quad \text{and} \quad \lambda e = e\sigma(\lambda) \text{ for } \lambda \in L.$$

Such an algebra is called a *cyclic algebra*. It is a right vector space over L, and as such has dimension $(\mathcal{A} : L) = n$.

Cyclic algebras naturally provide families of matrices thanks to an explicit isomorphism h between the algebras $\mathcal{A} \otimes_K L$ and $\mathcal{M}_n(L)$, the n-dimensional matrices with coefficients in L. Since each $x \in \mathcal{A}$ is expressible as

$$x = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1}, \; x_i \in L \text{ for all } i,$$

it is enough to give $h(x_i \otimes 1)$ and $h(e \otimes 1)$. We have that

$$h : \mathcal{A} \otimes_K L \cong \mathcal{M}_n(L) \tag{5}$$

is given by

$$x_i \otimes 1 \mapsto \begin{pmatrix} x_i & 0 & & 0 \\ 0 & \sigma(x_i) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \sigma^{n-1}(x_i) \end{pmatrix} \text{ for all } i, \; e \otimes 1 \mapsto \begin{pmatrix} 0 & 0 & 0 & & \gamma \\ 1 & 0 & 0 & & 0 \\ 0 & 1 & \ddots & & \vdots \\ 0 & & \ddots & & \\ 0 & & & 1 & 0 \end{pmatrix}.$$

Thus the matrix of $h(x \otimes 1)$ is easily checked to be

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \dots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \dots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \dots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \dots & \sigma^{n-1}(x_0) \end{pmatrix}. \tag{6}$$

Remark 1: Notice that (6) is also the matrix of multiplication by x.

We thus start with the family of matrices

$$\mathcal{C} = \left\{ \mathbf{X} = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \dots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \dots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \dots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \dots & \sigma^{n-1}(x_0) \end{pmatrix} \mid x_i \in L \text{ for all } i \right\}, \tag{7}$$

which is clearly linear (since σ is). Thus

$$\det(\mathbf{X}_1 - \mathbf{X}_2) = \det(\mathbf{X}),\ \mathbf{0} \neq \mathbf{X} \in \mathcal{C},\ \text{for all } \mathbf{X}_1 \neq \mathbf{X}_2 \in \mathcal{C},$$

so that the diversity (defined in (4)) simplifies to

$$\zeta(\mathcal{C}) = \frac{1}{2} \min_{\mathbf{X} \neq \mathbf{0}} |\det(\mathbf{X})|^{1/n},\ \mathbf{X} \in \mathcal{C}.$$

It is thus enough to consider cyclic division algebras to get $\zeta(\mathcal{C}) > 0$.

To decide whether a cyclic algebra is a division algebra, the following criterion is useful:

Proposition 1: [13, p. 279] Let L/K be a cyclic extension of degree n with Galois group $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. If the order of $\gamma \in K^*$ modulo $N_{L/K}(L^*)$ is n, then $(L/K, \sigma, \gamma)$ is a division algebra.

We are now interested in finding unitary matrices in $\mathcal{A} = (L/K, \sigma, \gamma)$. We first notice that there are natural candidates.

$$\begin{tikzcd}[row sep=large] \mathbb{Q}(\zeta_m) \arrow[d, dash, "n"] \\ K \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

Fig. 1. The cyclotomic field $\mathbb{Q}(\zeta_m)$ and its subfield K such that $\mathbb{Q}(\zeta_m)/K$ is cyclic of order n.

Consider the matrices

$$E = \begin{pmatrix} 0 & 0 & 0 & & \gamma \\ 1 & 0 & 0 & & 0 \\ 0 & 1 & \ddots & & \vdots \\ 0 & & \ddots & & \\ 0 & & & 1 & 0 \end{pmatrix} \text{ and } D = \begin{pmatrix} x & 0 & & 0 \\ 0 & \sigma(x) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \sigma^{n-1}(x) \end{pmatrix}, \ x \in L,$$

and their powers. The matrix E corresponds to e, via the isomorphism h. It is easy to check that $e^n = \gamma$ corresponds to $E^n = \gamma \mathbf{I}_n$. If γ satisfies $\gamma\bar{\gamma} = 1$, it is clear that E^k, $k = 0, \ldots, n-1$, is unitary. Similarly D corresponds to an element of L. We have that $DD^\dagger = \mathbf{I}_n \iff |\sigma(x)^i|^2 = 1$, $i = 0, \ldots, n-1$. If we assume that σ commutes with the complex conjugation, then an element x that satisfies $x\bar{x} = 1$ will imply that D and its powers are unitary.

Before going further, let us use these matrices to build the first families of unitary matrices [12].

B. Cyclic algebras versus fixed point free groups: the group $G_{m,r}$

Let r, m be two positive integers, and define n to be the order of r (mod m), i.e., n is the smallest positive integer such that $r^n \equiv 1$ (mod m). Set $t = m/\gcd(r-1, m)$.

Consider the cyclotomic field $L = \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive mth root of unity. It is of degree $\varphi(m)$ over $\mathbb{Q}$ (φ is the Euler totient function). Consider the extension described in Fig.1. Note first that this extension is well-defined, since $n|\varphi(m)$. This is a consequence of both the assumption that $r^n \equiv 1$

(mod m) and Lagrange's Theorem.

Proposition 2: Let $\sigma : \zeta_m \mapsto \zeta_m^r$. The cyclic algebra $\mathcal{A} = (\mathbb{Q}(\zeta_m)/K, \sigma, \zeta_m^t)$ is well-defined.

Proof: Since $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$, $r^n \equiv 1 \pmod{m}$ implies that there is a cyclic subgroup of order n in $(\mathbb{Z}/m\mathbb{Z})^*$, which means that $\mathbb{Q}(\zeta_m)/K$ is cyclic of order n. This subgroup of order n is generated by $\sigma : \zeta_m \mapsto \zeta_m^r$.

What is left to prove is that $\zeta_m^t \in K$, i.e., that ζ_m^t is fixed by σ. But

$$\sigma(\zeta_m^t) = \zeta_m^t \iff t(r-1) \equiv 0 \pmod{m},$$

which is satisfied since $t(r-1) = m(r-1)/\gcd(r-1,m)$ and clearly $\gcd(r-1,m) \mid r-1$. ■

The matrix representation of the element e of $\mathcal{A}$ such that $e^n = \zeta_m^t$ is thus

$$E = \begin{pmatrix} 0 & 0 & 0 & & \zeta_m^t \\ 1 & 0 & 0 & & 0 \\ 0 & 1 & \ddots & & \vdots \\ 0 & & \ddots & & \\ 0 & & & 1 & 0 \end{pmatrix},$$

while the one of $\zeta_m \in L$ is given by

$$D = \begin{pmatrix} \zeta_m & 0 & & 0 \\ 0 & \zeta_m^r & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \zeta_m^{r^{n-1}} \end{pmatrix}.$$

Since $\zeta_m^k \overline{\zeta_m^k} = 1$ for any integer k, the matrices E^i, $i = 0, \ldots, n-1$ and D^j, $j = 0, \ldots, m-1$ are unitary (as explained above). Thus the set $E^i D^j$ yields a family of $nm - 1$ unitary matrices.

Example 1: Take $n = 3$, $r = 4$ and $m = 21$. We thus have the cyclic algebra $\mathcal{A} = (\mathbb{Q}(\zeta_{21})/K, \sigma, \zeta_{21}^7)$, where $\sigma : \zeta_{21} \mapsto \zeta_{21}^4$. We get the family of 63 unitary matrices $E^i D^j$, where

$$D = \begin{pmatrix} \zeta_{21} & 0 & 0 \\ 0 & \zeta_{21}^4 & 0 \\ 0 & 0 & \zeta_{21}^{16} \end{pmatrix}, \quad E = \begin{pmatrix} 0 & 0 & \zeta_{21}^7 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

It is interesting to notice that these families of unitary matrices are exactly the ones obtained using fixed point free groups representation in [18]. In the latter work, it is shown that the n-dimensional representation of the group

$$G_{m,r} = \langle \sigma, \tau \mid \sigma^m,\ \tau^n = \sigma^t, \sigma^\tau = \sigma^r \rangle,$$

where r, m and t are as defined here, is given by

$$\Delta(G_{m,r}) = \{\Delta(\sigma)^l \Delta(\tau)^k \mid l = 0, \ldots, m-1,\ k = 0, \ldots, n-1\},$$

where

$$\Delta(\tau) = \begin{pmatrix} 0 & 0 & 0 & & \zeta_m^t \\ 1 & 0 & 0 & & 0 \\ 0 & 1 & \ddots & & \vdots \\ 0 & & \ddots & & \\ 0 & & & 1 & 0 \end{pmatrix}^T,\ \Delta(\sigma) = \begin{pmatrix} \zeta_m & 0 & & 0 \\ 0 & \zeta_m^r & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \zeta_m^{r^{n-1}} \end{pmatrix}.$$

A first immediate result of the application of cyclic algebras thus yields a generalization of this well known family of unitary matrices. Furthermore, unlike finite groups, cyclic algebras offer infinitely many elements, which makes very likely the existence of other unitary matrices. In the next section, we will give a systematic way of finding such matrices.

III. The General Machinery

This section gives step by step a general procedure to find unitary matrices in a cyclic algebra [10].

Roughly speaking, the main idea is to exploit the isomorphism (5)

$$h : \mathcal{A} \otimes_K L \cong \mathcal{M}_n(L)$$

between the matrices algebra $\mathcal{M}_n(L)$ and the algebra $\mathcal{A} \otimes_K L$, so as to translate the hermitian conjugation of a matrix into an involution on the cyclic algebra $\mathcal{A}$. As shown in Subsection III-A, this reformulates the condition of being unitary for a matrix into an equivalent condition for an element of the algebra . The second main step, explained in Subsection III-B, is to consider the latter condition in commutative subfields of the algebra, where it will be shown to be a norm condition. Recall that much of the work focuses on finding unitary matrices, since the diversity will follow immediately by considering cyclic division algebras.

A. The unitary constraint in the algebra

With the notations of Section II, let $\mathcal{A} = (L/K, \sigma, \gamma)$ be a cyclic division algebra. We now have a linear family $\mathcal{C}$ of invertible matrices (as described in (7)) among which we are looking for unitary matrices, i.e., $\mathbf{X} \in \mathcal{C}$ such $\mathbf{X}\mathbf{X}^\dagger = \mathbf{I}_n$, where † denotes the conjugate transpose. We take advantage of the matrices coming from the algebra $\mathcal{A}$ and translate the condition of "being unitary" into the algebra. More precisely, we will show that $\mathcal{A}$ can be endowed with an involution α, and that

$$\mathbf{X}\mathbf{X}^\dagger = \mathbf{I}_n \iff h(x \otimes 1)h(x \otimes 1)^\dagger = 1 \iff x\alpha(x) = 1.$$

Let us first define an involution on $\mathcal{A}$.

Proposition 3: Let $\alpha_L : L \to L$ be a (non-trivial) involution on L such that α_L commutes with all elements of Gal(L/K). Let $\alpha : \mathcal{A} \to \mathcal{A}$ such that

$$\alpha(x_0 + ex_1 + \ldots + e^{n-1}x_{n-1}) = \alpha_L(x_0) + e^{-1}\sigma^{-1}(\alpha_L(x_1)) + \ldots + e^{-(n-1)}\sigma^{-(n-1)}(\alpha_L(x_{n-1})).$$

Then α defines an involution on $\mathcal{A}$ if and only if $\gamma\alpha_L(\gamma) = 1$.

Remark 2: Note that the condition that α_L commutes with all elements of Gal(L/K) implies that $\alpha_L(K) = K$. Indeed,

$$\sigma(\alpha_L(k)) = \alpha_L(\sigma(k)) = \alpha_L(k), \text{ for any } k \in K,$$

showing that $\alpha_L(k)$ is fixed by σ.

Proof: Check that

1) $\alpha(x + y) = \alpha(x) + \alpha(y)$ for all $x, y \in \mathcal{A}$.

   This is clear.

2) $\alpha(e^j y_j e^i x_i) = \alpha(e^i x_i)\alpha(e^j y_j)$ for all $x_i, y_j \in L$.

   For checking this equality, it is useful to remember that $le = e\sigma(l)$, for all $l \in L$, and thus, $le^j = e^j\sigma^j(l)$, $j = 1, \ldots, n-1$.

   If $i + j < n$, we have

$$\begin{aligned}\alpha(e^j y_j e^i x_i) &= \alpha(e^{i+j}\sigma^i(y_j)x_i)\\ &= e^{-(i+j)}\sigma^{-(i+j)}(\alpha_L(x_i)\alpha_L(\sigma^i(y_j)))\end{aligned}$$

$$= e^{-(i+j)}\sigma^{-(i+j)}(\alpha_L(x_i))\sigma^{-j}(\alpha_L(y_j)).$$

Now the right handside term is given by

$$\begin{aligned}\alpha(e^i x_i)\alpha(e^j y_j) &= e^{-i}\sigma^{-i}(\alpha_L(x_i))e^{-j}\sigma^{-j}(\alpha_L(y_j)) \\ &= e^{-(i+j)}\sigma^{-(i+j)}(\alpha_L(x_i))\sigma^{-j}(\alpha_L(y_j)),\end{aligned}$$

which concludes the case $i+j<n$.

If $i+j \geq n$, then $i+j = n+k$, $0 \leq k < n$, and we have with similar computations

$$\begin{aligned}\alpha(e^j y_j e^i x_i) &= \alpha(e^k \gamma \sigma^i(y_j) x_i) \\ &= e^{-k}\sigma^{-k}(\alpha_L(\gamma)\alpha_L(x_i)\alpha_L(\sigma^i(y_j))) \\ &= e^{-k}\alpha_L(\gamma)\sigma^{-k}(\alpha_L(x_i))\sigma^{-j}(\alpha_L(y_j)).\end{aligned}$$

As above, the right handside term is given by

$$\begin{aligned}\alpha(e^i x_i)\alpha(e^j y_j) &= e^{-(i+j)}\sigma^{-(i+j)}(\alpha_L(x_i))\sigma^{-j}(\alpha_L(y_j)) \\ &= e^{-k}\gamma^{-1}\sigma^{-k}(\alpha_L(x_i))\sigma^{-j}(\alpha_L(y_j)).\end{aligned}$$

We have equality if and only if $\alpha_L(\gamma) = \gamma^{-1}$.

3) $\alpha(\alpha(x)) = x$ for all $x \in \mathcal{A}$. By linearity, it is enough to check that $\alpha(\alpha(e^i x_i)) = e^i x_i$ for all $x_i \in L$. We have

$$\begin{aligned}\alpha(\alpha(e^i x_i)) &= \alpha(e^{-i}\sigma^{-i}(\alpha_L(x_i))) \\ &= \alpha_L(\sigma^{-i}(\alpha_L(x_i)))\alpha(e^{-i}) \\ &= \sigma^{-i}(x_i)e^i \\ &= e^i x_i.\end{aligned}$$

■

This involution can be extended to the algebra $\mathcal{A} \otimes_K L \cong \mathcal{M}_n(L)$ as follows.

$$\alpha \otimes \alpha_L : \mathcal{A} \otimes_K L \to \mathcal{A} \otimes_K L.$$

It is used to define an involution α_h on $\mathcal{M}_n(L)$ via the isomorphism h:

$$h \circ (\alpha \otimes \alpha_L) = \alpha_h \circ h. \tag{8}$$

Proposition 4: Let $\mathbf{X} = h(x \otimes 1)$. If α_L is the complex conjugation, then $\alpha_h(\mathbf{X}) = \mathbf{X}^\dagger$.

Proof: Recall first that

$$\mathbf{X} = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \dots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \dots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \dots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

We have

$$\begin{aligned} \alpha_h(\mathbf{X}) &= \alpha_h(h(x \otimes 1)) \\ &= h \circ (\alpha \otimes \alpha_L)(x \otimes 1) \\ &= h(\alpha(x) \otimes \alpha_L(1)) \\ &= h(\alpha(x) \otimes 1)\alpha_L(1). \end{aligned}$$

Recall that $e^{-1} = \gamma^{-1}e^{n-1}$, $\gamma^{-1} = \alpha_L(\gamma)$ and that $h(\alpha(x) \otimes 1)$ is the matrix of multiplication by $\alpha(x)$ (see Remark 1). Since

$$\begin{aligned} \alpha(x) &= \alpha_L(x_0) + e^{-1}\sigma^{-1}(\alpha_L(x_1)) + \ldots + e^{-(n-1)}\sigma^{-(n-1)}(\alpha_L(x_{n-1})) \\ &= \alpha_L(x_0) + e\gamma^{-1}\sigma(\alpha_L(x_{n-1})) + \ldots + e^{n-1}\gamma^{-1}\sigma^{n-1}(\alpha_L(x_1)), \end{aligned}$$

we have

$$h(\alpha(x) \otimes 1) = \begin{pmatrix} \alpha_L(x_0) & \alpha_L(x_1) & \dots & \alpha_L(x_{n-1}) \\ \alpha_L(\gamma)\sigma(\alpha_L(x_{n-1})) & \sigma(\alpha_L(x_0)) & \dots & \sigma(\alpha_L(x_1)) \\ \vdots & & & \vdots \\ \alpha_L(\gamma)\sigma^{n-1}(\alpha_L(x_1)) & \alpha_L(\gamma)\sigma^{n-1}(\alpha_L(x_{n-1})) & \dots & \sigma^{n-1}(\alpha_L(x_0)) \end{pmatrix}.$$

Since α_L and σ commute, and α_L is multiplicative, we get the desired result. ■

It is clear from the above matrix of $h(\alpha(x)\otimes 1)$ that α_L being the complex conjugation is the only choice.

Corollary 1: We have the following equivalence:

$$\mathbf{X}\mathbf{X}^\dagger = \mathbf{I}_n \iff x\alpha(x) = 1.$$

Proof: This comes from

$$\begin{aligned}
\mathbf{X}\mathbf{X}^\dagger &= h(x\otimes 1)\alpha_h(h(x\otimes 1)) \text{ by the above proposition}\\
&= h(x\otimes 1)h(\alpha\otimes\alpha_L)(x\otimes 1), \text{ using (8)}\\
&= h(x\alpha(x)\otimes 1).
\end{aligned}$$

■

Example 2: Take $n=3$. Let $K=\mathbb{Q}(\zeta_3)$ be a cyclotomic field, where ζ_3 is a primitive third root of unity, and let $L=K\mathbb{Q}(\theta)$ be the compositum of K and a totally real cubic number field $\mathbb{Q}(\theta)$, with discriminant coprime to d_K and cyclic Galois group $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}) = \langle\sigma\rangle$ (see Figure 2). We consider the algebra $\mathcal{A}=(L/K,\sigma,\gamma)$, where $\gamma=\zeta_3$.

The involution on L is given by

$$\begin{aligned}
\alpha_L :\ & L & \to\ & L\\
& a_0+a_1\theta+a_2\theta^2 & \mapsto\ & \tau(a_0)+\tau(a_1)\theta+\tau(a_2)\theta^2
\end{aligned}$$

where τ is the generator of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$. Namely, $\tau(b_0+b_1\zeta_3)=b_0+b_1\zeta_3^2$ and $\zeta_3^2=-\zeta_3-1$. Since α_L commutes with σ, the involution

$$\begin{aligned}
\alpha :\ & \mathcal{A} & \to\ & \mathcal{A}\\
& x_0+ex_1+e^2x_2 & \mapsto\ & \alpha_L(x_0)+e\zeta_3^2\sigma(\alpha_L(x_2))+e^2\zeta_3^2\sigma^2(\alpha_L(x_1))
\end{aligned}$$

is well defined by Proposition 3.

Note that the involution α_L is indeed the complex conjugation. We have

$$\begin{pmatrix} 0 & 0 & \gamma\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}\begin{pmatrix} 0 & 1 & 0\\ 0 & 0 & 1\\ \bar\gamma & 0 & 0\end{pmatrix} = \begin{pmatrix} 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} \iff \gamma\bar\gamma = 1 \iff e\alpha(e)=1.$$

$$
\begin{tikzcd}[arrows=dash]
 & \mathcal{A} \arrow[d] & \\
 & L \arrow[dl, "2"'] \arrow[dr, "3"] & \\
\mathbb{Q}(\theta) \arrow[dr, "3"'] & & \mathbb{Q}(\zeta_3) \arrow[dl, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Fig. 2. The cyclic algebra $\mathcal{A} = (L/K, \sigma, \gamma)$.

At this point, note that we started our construction by taking L/K any cyclic extension of number fields. In Proposition 3, a first condition on L was given: L has to be endowed with an involution α_L such that α_L commutes with all elements of $Gal(L/K)$. Furthermore, it was shown in Proposition 4 that α_L has to be the complex conjugation. These are the only conditions on the field extension L/K to apply the construction presented here.

B. The unitary constraint in commutative subfields

We now show how the problem of finding unitary elements in the algebra $\mathcal{A}$ can be reduced to find elements of norm 1 in commutative subfields of $\mathcal{A}$.

Proposition 5: Let $\mathcal{A} = (L/K, \sigma, \gamma)$ be a cyclic division algebra. Let $x \in \mathcal{A}^*$ such that $x\alpha(x) = 1$, $x \notin K$. Then there exists $u \in \mathcal{A}^*$ such that $u\alpha(u) = \alpha(u)u$ and $x = u\alpha(u)^{-1} = \alpha(u)^{-1}u$.

Proof: Let $x \in \mathcal{A}^*$ such that $x\alpha(x) = 1$. Let M denote the subfield of $\mathcal{A}$ generated by K and x (which is well-defined since $x \notin K$). It is commutative and satisfies that $\alpha(M) = M$, since $\alpha(K) = K$ and $\alpha(x) = x^{-1}$. Thus

$$M^\alpha = \{y \in M \mid \alpha(y) = y\},$$

the subfield fixed by α is well-defined. Since $M^\alpha \neq M$ ($x \neq \pm 1$), M/M^α is a quadratic extension with Galois group Gal$(M/M^\alpha) = \{Id_M, \alpha|_M\}$. The condition $x\alpha(x) = 1$ is here translated into $N_{M/M^\alpha}(x) = 1$. By the corollary of Hilbert 90 Theorem that exactly characterizes elements of norm 1 in cyclic extension, there exists $u \in M^*$ such that $x = u/\alpha(u)$. ∎

Remark 3: If $x \in K$, then $M = K$ and $x\alpha(x) = |x|^2$.

The above proof gives a way of building unitary elements of the algebra $\mathcal{A}$. Take a commutative subfield $M \neq K$ of $\mathcal{A}$ such that $\alpha(M) = M$ but with $y \in M$ such that $\alpha(y) \neq y$, so that M^α is not M itself. Take $u \in M^*$ and compute $x = u/\alpha(u)$. The element $x \in \mathcal{A}$ will satisfy $x\alpha(x) = 1$.

Finally, we give a way of describing commutative subfields of $\mathcal{A}$.

Definition 1: [14, p. 113] Let $\mathcal{A}$ be a cyclic algebra. For $x \in \mathcal{A}$, define its *reduced characteristic polynomial* χ_x as the characteristic polynomial of $h(x \otimes 1)$.

Let $x \in \mathcal{A} = (L/K, \sigma, \gamma)$. Its reduced characteristic polynomial is given by

$$\chi_x(X) = \det \begin{pmatrix} x_0 - X & \gamma\sigma(x_{n-1}) & \dots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) - X & \dots & \gamma\sigma^{n-1}(x_{n-1}) \\ \vdots & & & \vdots \\ x_{n-1} & \sigma(x_1) & & \sigma^{n-1}(x_0) - X \end{pmatrix}.$$

It has been shown that for each $x \in \mathcal{A}$, its reduced characteristic polynomial lies in $K[X]$ [14, p. 113]. If the polynomial χ_x is irreducible over K, since it is monic and in $K[X]$, it is the minimal polynomial of an extension of degree n of K. Thus, $K[X]/(\chi_x(X))$ is a commutative subfield of $\mathcal{A}$.

Example 3: Let $\mathcal{A} = (L/K, \sigma, \gamma)$ and $\mathcal{A} = L \oplus eL \oplus e^2L$. Let χ_e be the reduced characteristic polynomial of e, given by

$$\begin{aligned} \chi_e(X) &= \det \begin{pmatrix} -X & 0 & \gamma \\ 1 & -X & 0 \\ 0 & 1 & -X \end{pmatrix} \\ &= -X^3 + \gamma. \end{aligned}$$

As long as γ is not a cube in K, χ_e is irreducible and $K[X]/\chi_e(X) \cong K(e)$ is a commutative subfield of $\mathcal{A}$ of degree 3 over K.

IV. A WORKED OUT EXAMPLE

In this section, we consider a particular cyclic division algebra and show how to use it to build families of fully-diverse unitary matrices.

Let $K = \mathbb{Q}(\zeta_3)$ and $L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_3)$ be the compositum of $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_7)$ (see Figure 2, with $\theta = \zeta_7 + \zeta_7^{-1}$).
We have $\mathrm{Gal}(L/\mathbb{Q}(\zeta_3)) = \langle \sigma \rangle$, with $\sigma : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}$.

Let $\mathcal{A} = (\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_3)/\mathbb{Q}(\zeta_3), \sigma, \zeta_3)$ be the corresponding cyclic algebra. This is a division algebra [9]. As already explained in Example 2, the involution α on $\mathcal{A}$ is given by

$$\begin{array}{rlcl} \alpha : & \mathcal{A} & \rightarrow & \mathcal{A} \\ & x_0 + ex_1 + e^2 x_2 & \mapsto & \alpha_L(x_0) + e\zeta_3^2 \sigma(\alpha_L(x_2)) + e^2 \zeta_3^2 \sigma^2(\alpha_L(x_1)), \end{array}$$

where $\alpha_L(b_0 + b_1\zeta_3) = b_0 + b_1\zeta_3^2$.

A. *Commutative subfields of $\mathcal{A}$*

Following the method explained in Subsection III-B, we look for subfields M of $\mathcal{A}$, which possess a quadratic subfield M/M^α fixed by α.

The first obvious subfield of $\mathcal{A}$ one can think of is L. The restriction of α on L is α_L, given by the complex conjugation. The totally real quadratic subfield of L given by $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ is thus fixed by α_L. Then, as explained in Example 3, we can consider $K(e)$, with minimal polynomial $\chi_e(X) = X^3 - \zeta_3$. Thus $K(e) = \mathbb{Q}(\zeta_9)$.
Since $\alpha(e) = e^{-1}$, we have that $\alpha(\zeta_9) = \zeta_9^{-1}$ and α is the complex conjugation on $K(e) = \mathbb{Q}(\zeta_9)$. Its maximal real subfield $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ is fixed by α (See Figure 3). Let us now try to determine more systematically which are the commutative subfields of $\mathcal{A}$ which contain a quadratic subfield fixed by α. Let M be a subfield of $\mathcal{A}$. We want to determine when M^α is non-trivial. Clearly $M^\alpha \subseteq \{x \in \mathcal{A} \mid \alpha(x) = x\}$. We thus look for conditions so as to satisfy $x = \alpha(x)$.

Lemma 1: Let $x = x_0 + ex_1 + e^2x_2$, with $x_i \in L$, that is $x_i = v_i + \zeta_3 w_i$, v_i, $w_i \in \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ for $i = 0, 1, 2$. We have

$$x = \alpha(x) \quad \Longleftrightarrow \quad \left\{ \begin{array}{rcl} x_0 & = & \alpha_L(x_0) \\ v_1 & = & -\sigma(v_2) \\ w_1 & = & \sigma(w_2) + v_1 \end{array} \right.$$

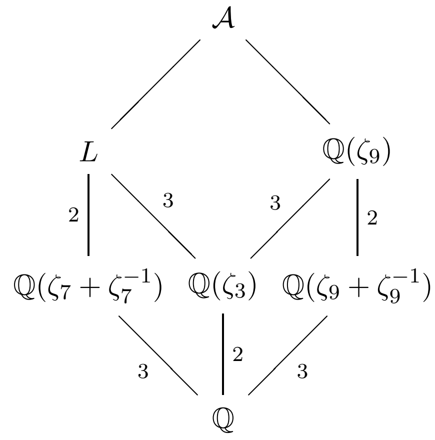

Fig. 3. The algebra $\mathcal{A}$ and some of its commutative subfields

Proof: This is a straightforward computation. Identify the coefficients of the power of e

$$\begin{cases} x_0 &= \alpha_L(x_0) \\ x_1 &= \alpha_L(\sigma(x_2))\gamma^{-1} \\ x_2 &= \alpha_L(\sigma^2(x-1))\gamma^{-1} \end{cases}$$

then develop and using that $\gamma = \zeta_3$, identify the constant term and the coefficient of ζ_3. ■

Example 4: Let $x = x_0 + ex_1 + e^2x_2 \in \mathcal{A}$, with $x_i = v_i + \zeta_3 w_i$, v_i, $w_i \in \mathbb{Q}$ for $i = 0, 1, 2$. The conditions of Lemma 1 are $v_1 = -v_2$ and $w_1 = w_2 + v_1$. Thus

$$x = x_0 + e[(w_1 - w_2) + \zeta_3 w_1] + e^2[(-w_1 + w_2) + \zeta_3 w_2].$$

This defines the number field $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_9)$. Indeed, we have that $y \in \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ can be written as follows

$$\begin{aligned} y &= y_0 + y_1(\zeta_9 + \zeta_9^{-1}) + y_2(\zeta_9 + \zeta_9^{-1})^2,\ y_i \in \mathbb{Q},\ i = 0, 1, 2 \\ &= y_0 + y_1(\zeta_9 - \zeta_9^2 - \zeta_9^5) + y_2(2 - \zeta_9 + \zeta_9^2 - \zeta_9^4) \\ &= (y_0 + 2y_2) + [(y_1 - y_2) - y_2\zeta_3]\zeta_9 + [(y_2 - y_1) - y_1\zeta_3]\zeta_9^2. \end{aligned}$$

Note that we already found this field extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$.

Other examples can be found in Table I. The fields are of the form $\mathbb{Q}(\zeta_3, \nu)$, where ν is fixed by the

$\mathbb{Q}(\zeta_3)(\nu)$	minimal polynomial of ν	discriminant
$\nu = \theta + (1+\zeta_3)e - e^2$	$X^3 + X^2 - 5X - 3$	$2^2 \cdot 3 \cdot 47$
$\nu = 2\theta + (1+\zeta_3)e - e^2$	$X^3 - X^2 - 12X + 1$	$11 \cdot 659$
$\nu = 3\theta + (1+\zeta_3)e - e^2$	$X^3 - 6X - 1$	$3^3 \cdot 31$
$\nu = 4\theta + (1+\zeta_3)e - e^2$	$X^3 - 11X + 9$	3137
$\nu = 5\theta + (1+\zeta_3)e - e^2$	$X^3 - X^2 - 61X - 13$	$2^2 \cdot 307 \cdot 727$

TABLE I

EXAMPLES OF COMMUTATIVE SUBFIELDS OF $\mathcal{A}$.

involution. The minimal polynomial of ν seen in $\mathbb{Z}[\zeta_3][X]$ generates an extension of degree 3 of $\mathbb{Q}(\zeta_3)$, which contains $\mathbb{Q}(\nu)$ as quadratic subextension fixed by α. The discriminant in the table is the one of $\mathbb{Q}(\nu)$.

B. Unitary matrices in $\mathcal{A}$

We now illustrate how to build unitary matrices in the commutative subfield $\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3)$ of $\mathcal{A}$ that we built in the previous subsection.

Take for example the element

$$\begin{aligned} y &= 1 + \zeta_9 + \zeta_9^3 + \zeta_9^5 \in \mathbb{Q}(\zeta_9) \\ &= (1+\zeta_3) + e + e^2\zeta_3 \in \mathcal{A} \end{aligned}$$

As a matrix, y can be represented as

$$\mathbf{Y} = \begin{pmatrix} 1+\zeta_3 & \zeta_3^2 & \zeta_3 \\ 1 & 1+\zeta_3 & \zeta_3^2 \\ \zeta_3 & 1 & 1+\zeta_3 \end{pmatrix}.$$

We have

$$\begin{aligned} \alpha(y) &= -\zeta_9^2 - \zeta_9^3 + \zeta_9^4 - \zeta_9^5 \in \mathbb{Q}(\zeta_9) \\ &= -\zeta_3 + e\zeta_3 + e^2\zeta_3^2 \in \mathcal{A} \end{aligned}$$

Again, as a matrix, $\alpha(y)$ can be represented as

$$\begin{pmatrix} -\zeta_3 & 1 & \zeta_3^2 \\ \zeta_3 & -\zeta_3 & 1 \\ \zeta_3^2 & \zeta_3 & -\zeta_3 \end{pmatrix}$$

which can be checked to be $\mathbf{Y}^*$. We have

$$x = y/\alpha(y) = \frac{1}{19}(-10 + 16\zeta_9 + \zeta_9^2 - 4\zeta_9^3 + 14\zeta_9^4 + 8\zeta_9^5),$$

which has norm 1. Clearly $x\alpha(x) = 1$ and by Corollary 1, the matrix $\mathbf{X} = \mathbf{Y}(\mathbf{Y}^*)^{-1}$ is unitary. This can be easily verified, since

$$\mathbf{X} = \mathbf{Y}(\mathbf{Y}^*)^{-1} = \begin{pmatrix} -0.421 - 0.182i & 0.473 + 0.638i & -0.157 + 0.36i \\ -0.236 - 0.319i & -0.421 - 0.182i & 0.473 + 0.638i \\ -0.789 + 0.09i & -0.236 - 0.319i & -0.421 - 0.182i \end{pmatrix}^T.$$

Notice that this procedure can be applied

- to any element of $\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3)$, and for each, it will give a unitary matrix. There may obviously be some redundancy. Typically, if the element x is invariant by α, the above procedure will yield the identity matrix.
- to any commutative subfield of $\mathcal{A}$, assuming that it has a quadratic subfield fixed by the involution.

V. New Code Constructions

As an application of the technique we described in the previous sections, we now give new code constructions for the 3 and 4 antennas case.

Let $\mathcal{A} = (L/K, \sigma, \gamma)$ be a cyclic division algebra. We have seen from Proposition 3 and 4 that any cyclic division algebra is suitable for our construction, as long as γ satisfies $|\gamma|^2 = 1$ and α_L is the complex conjugation, which commutes with $Gal(L/K)$. Furthermore, any commutative subfield M/M^α of $\mathcal{A}$ could be used. We will give a construction that exploits the two most natural subfields of $\mathcal{A}$ that are L and $K(e)$.

A. Extending the $G_{m,r}$ construction

We consider again the construction described in Subsection II-B. Given the algebra $\mathcal{A} = (\mathbb{Q}(\zeta_m), \sigma, \zeta_m^t)$, the code is built using the matrix representation of the elements e and ζ_m, and their powers. Recall that the rate of the code is defined by

$$R = \frac{\log_2(\#\mathcal{C})}{n} = \frac{\log_2(nm-1)}{n}.$$

Given the algebra $\mathcal{A} = (\mathbb{Q}(\zeta_m), \sigma, \zeta_m^t)$ which contains infinitely many elements, we are using only $mn-1$ of them. It is thus natural to look for other suitable elements in the algebra.

Using the technique explained in the previous sections, let us start by considering L/L^α. Here $L = \mathbb{Q}(\zeta_m)$ and α_L is the complex conjugation. Let $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ denote the maximal real subfield of $\mathbb{Q}(\zeta_m)$, which is L^α. It is of degree $\varphi(m)/2$ over $\mathbb{Q}$. We have that $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m + \zeta_m^{-1}))$ is of order 2, generated by the complex conjugation. We are now interested in finding elements of norm 1 in this quadratic extension.

Lemma 2: Let $x \in \mathbb{Q}(\zeta_m)$ such that $N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m+\zeta_m^{-1})}(x) = 1$. Then the matrix representation of x is unitary.

Proof: The element x is of norm 1, which means that $x\bar{x} = 1$. Since x is in $\mathbb{Q}(\zeta_m)$, its representation is a diagonal matrix F, whose diagonal coefficients verify $F_{ii}\overline{F_{ii}} = 1$. ∎

This lemma is an illustration in this particular case of the general machinery developed previously.

Example 5: We consider the same algebra as in Example 1, the cyclic algebra $\mathcal{A} = (\mathbb{Q}(\zeta_{21})/K, \sigma, \zeta_{21}^7)$, where $\sigma : \zeta_{21} \mapsto \zeta_{21}^4$. Take for example the following element x and its conjugates

$$\begin{aligned} x &= (-\zeta^3 - \zeta^5 + \zeta^8 - \zeta^{10} + \zeta^{11})/2 \\ \sigma(x) &= (-1 + 2\zeta^2 - \zeta^3 + 2\zeta^5 - \zeta^7 + \zeta^8 - \zeta^{10} + 2\zeta^{11})/2 \\ \sigma^2(x) &= (1 + 2\zeta^3 - \zeta^5 + \zeta^7 + 2\zeta^{10} - \zeta^{11})/2 \end{aligned}$$

whose matrix representation is given by

$$F = \begin{pmatrix} x & 0 & 0 \\ 0 & \sigma(x) & 0 \\ 0 & 0 & \sigma^2(x) \end{pmatrix} = \begin{pmatrix} -0.7156 - 0.6985i & 0 & 0 \\ 0 & -0.5217 + 0.8531i & 0 \\ 0 & 0 & 0.3417 + 0.9398i \end{pmatrix}.$$

It is a straightfoward computation to check that x has norm 1 and that F is unitary.

This simple result allows to construct codebooks of the form

$$\mathcal{C}_i = \{D^l E^k F^i \mid l = 0, \dots, m-1,\ k = 0, \dots, n-1\}$$

where i can be chosen to vary into a given range and F is a matrix constructed using the above lemma:

$$F = \begin{pmatrix} x & 0 & & 0 \\ 0 & \sigma(x) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \sigma^n(x) \end{pmatrix}. \tag{9}$$

Note that letting i grow yields infinitely many codewords, and that by bounding i, we loose the group structure. It still may be interesting to have F^i and its inverse F^{-i}, for example for evaluating the diversity (see Subsection V-B).

Of course, several matrices F_j and their powers could be added in order to increase the size of the codebook

$$\mathcal{C}(i_1, \dots, i_s) = \{D^l E^k F_1^{i_1} \cdots F_s^{i_1 s} \mid l = 0, \dots, m-1,\ k = 0, \dots, n-1\},$$

with $i_1, \dots, i_s$ varying into a given range.

B. Discussion on the diversity

Let us discuss the diversity of codebooks of the form

$$\mathcal{C}_i = \{D^l E^k F^i \mid l = 0, \dots, m-1,\ k = 0, 1, n-1,\ i = -I, \dots, I\}.$$

If the cyclic algebra we consider is a division algebra, we know that $\mathcal{C}_i$ will be fully-diverse. However, we are interested here in computing a better bound. Recall that by definition, the diversity product $\zeta(\mathcal{C})$ of a codebook $\mathcal{C}$ of cardinality M is given by

$$\zeta(\mathcal{C}) = \frac{1}{2} \min_{0 \le l < l' < M} |\det(\mathbf{X}_l - \mathbf{X}_{l'})|^{1/n}$$

where n is the dimension of the matrices.

Though we do not have a group structure, we still have the property that if $\mathbf{X} \in \mathcal{C}$, then $\mathbf{X}^{-1} \in \mathcal{C}$.

This allows us to say that

$$|\det(\mathbf{X}_l - \mathbf{X}_{l'})| = |\det(\mathbf{X}_l)\det(\mathbf{I} - \mathbf{X}_l^{-1}\mathbf{X}_{l'})| = |\det(\mathbf{I} - \mathbf{X}_l^{-1}\mathbf{X}_{l'})|$$

so that

$$\zeta(\mathcal{C}) = \frac{1}{2}\min_{\mathbf{0}\neq\mathbf{X}\in\mathcal{C}} |\det(\mathbf{I}-\mathbf{X})|^{1/n}.$$

By definition of $\mathcal{C}_i$, the matrix $\mathbf{I}-\mathbf{X}$ is doubly-banded for any $\mathbf{X}\in\mathcal{C}$. More precisely, if $\mathbf{X} = D^l E^k F^i$, then

$$\mathbf{I}-\mathbf{X}^T = \begin{pmatrix} 1 & & & -\zeta_m^l x^i & & 0 \\ 0 & 1 & & & -\zeta_m^{lr}\sigma(x^i) & 0 \\ \vdots & & \ddots & & \ddots & \\ 0 & & & & & \zeta_m^{lr^{n-k-1}}\sigma^{n-k-1}(x^i) \\ \zeta_m^t\zeta_m^{lr^{n-k}}\sigma^{n-k}(x^i) & & & & & \\ & \ddots & & & & \\ 0 & \zeta_m^t\zeta_m^{lr^{n-1}}\sigma^{n-1}(x^i) & & & & 1 \end{pmatrix},$$

where the upper band starts in column $k+1$. A formula for the determinant of doubly-banded matrices has been computed in [18, Lemma 6]. Using it and denoting $q = \gcd(n, n-k-1)$, we get

$$\det(\mathbf{I}-\mathbf{X}) = \begin{cases} 1-\zeta_m^{kt}\prod_{j=0}^{n-1}\zeta_m^{lr^j}\sigma^j(x^i) & \text{if } q=1 \\ \prod_{j=0}^{n-1}(1-\zeta_m^{lr^j}\sigma^j(x^i)) & \text{if } q=n \end{cases}.$$

Since $1+r+\ldots+r^{n-1} = \frac{r^n-1}{r-1}$ and $r^n = 1 \pmod m$, the case $q=1$ simplifies to

$$1-\zeta_m^{tk}N_{\mathbb{Q}(\zeta_m)/K}(x^i).$$

Summarizing the above computations, we get

Proposition 6: The diversity product of the codebook $\mathcal{C}_i$ is given by

$$\zeta(\mathcal{C}_i) = \frac{1}{2}\min\{|N_{\mathbb{Q}(\zeta_m)/K}(1-\zeta_m^l x^i)|, |1-\zeta_m^{tk}N_{\mathbb{Q}(\zeta_m)/K}(x^i)|\}^{1/n}.$$

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_{21}) \arrow[d, dash, "3"] & \\
& K = \mathbb{Q}(\zeta_3, \sqrt{-7}) \arrow[dl, dash] \arrow[d, dash, "2"] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_3) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{21}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{-7}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Fig. 4. The algebra $\mathcal{A} = (\mathbb{Q}(\zeta_{21})/K, \sigma, \zeta_{21}^7)$ and its subfields.

C. *Codes for 3 antennas*

In this section, we construct families of codes for 3 antennas and study their diversity [12], as a particular case of the construction extending $G_{m,r}$ explained above. We focus on families of matrices with common denominator, having in mind to maximize the diversity. Note that a suggestion using different techniques for extending the $G_{m,r}$ construction for the 3 antennas case has been proposed in [1].

A first construction. Consider the cyclic algebra $\mathcal{A} = (\mathbb{Q}(\zeta_{21})/K, \sigma, \zeta_{21}^7)$, where $\sigma : \zeta_{21} \mapsto \zeta_{21}^4$ (see Figure 4 where some subfields of $\mathcal{A}$ are described). Consider the following element x and its conjugates (we write $\zeta = \zeta_{21}$)

$$\begin{aligned}
x &= (4 - 2\zeta - \zeta^2 - 4\zeta^4 - 2\zeta^5 + 3\zeta^6 - 2\zeta^7 - 5\zeta^8 + 5\zeta^9 - \zeta^{10} - \zeta^{11})/7 \\
\sigma(x) &= (1 - 4\zeta + 5\zeta^2 - \zeta^4 + 3\zeta^5 - \zeta^6 - 4\zeta^7 - 3\zeta^8 + 3\zeta^9 - 2\zeta^{10} - 2\zeta^{11})/7 \\
\sigma^2(x) &= (2 - \zeta - 4\zeta^2 - 2\zeta^4 - \zeta^5 - 2\zeta^6 - \zeta^7 + \zeta^8 - \zeta^9 + 3\zeta^{10} - 4\zeta^{11})/7
\end{aligned}$$

whose matrix representation is given by

$$F = \begin{pmatrix} x & 0 & 0 \\ 0 & \sigma(x) & 0 \\ 0 & 0 & \sigma^2(x) \end{pmatrix} = \begin{pmatrix} 0.1603 - 0.98706i & 0 & 0 \\ 0 & 0.9774 - 0.2113i & 0 \\ 0 & 0 & -0.1377 - 0.9904i \end{pmatrix}.$$

We consider the following codebook

$$\mathcal{C} = \{(-1)^j D^l E^k F^i \mid j = 0,1,\ l = 0,\dots,20,\ k = 0,1,2,\ i = -6,\dots,6\},$$

where

$$D = \begin{pmatrix} \zeta_{21} & 0 & 0 \\ 0 & \zeta_{21}^4 & 0 \\ 0 & 0 & \zeta_{21}^{16} \end{pmatrix},\ E = \begin{pmatrix} 0 & 0 & \zeta_{21}^7 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

It has the property that if we write $\mathbf{X} = (x_{ij}) \in \mathcal{C}$ with coefficients $x_{ij} = \tilde{x}_{ij}/d$ with $\tilde{x}_{ij} \in \mathbb{Z}[\zeta_m]$ and $d \in \mathbb{Z}$, then d will be 1 or 7. This comes first from the element x to be in $\frac{1}{7}\mathbb{Z}[\zeta_m]$ and thus the associated matrix F to have coefficients in $\frac{1}{7}\mathbb{Z}[\zeta_m]$. But more importantly, it can be computed that the matrices F^i, $i = 1,\dots,6$ all have coefficients in $\frac{1}{7}\mathbb{Z}[\zeta_m]$, which is also true for the matrices F^{-i}, $i = 1,\dots,6$.

Since $\{F^i,\ i = -6,\dots,6\}$ contains 13 differents matrices, the rate R of $\mathcal{C}$ is immediatly given by

$$R = \frac{\log_2(63 \cdot 13 \cdot j)}{3},$$

where $j = 1$ if we fix the sign and $j = 2$ if we alternate the sign.

We can get variations with different rates of this code, letting the parameters j,l,k,i vary. By Proposition 6, we have

$$\zeta(\mathcal{C}) = \frac{1}{2}\min\{|N_{\mathbb{Q}(\zeta_{21})/K}(1-\zeta_{21}^l x^i)|, |1-\zeta_3^k N_{\mathbb{Q}(\zeta_{21})/K}(x^i)|\}^{1/3}.$$

For example, if $\mathcal{C} = \{D^l E^k,\ l = 0,\dots 20, k = 0,1,2\}$, we have

$$N_{\mathbb{Q}(\zeta_{21})/K}(1-\zeta_{21}) = 0.4568502i,\ \text{ so that } \frac{1}{2}|N_{\mathbb{Q}(\zeta_{21})/K}(1-\zeta_{21})|^{1/3} = 0.385089.$$

Similarly,

$$\begin{aligned} N_{\mathbb{Q}(\zeta_{21})/K}(x) &= -0.9819 + 0.1889i, \\ 1-\zeta_3 N_{\mathbb{Q}(\zeta_{21})/K}(x) &= 0.6726 + 0.9449i,\ \text{ so that} \\ \tfrac{1}{2}|N_{\mathbb{Q}(\zeta_{21})/K}(1-\zeta_{21})|^{1/3} &= 0.525342. \end{aligned}$$

The minimum is thus

$$\zeta(\mathcal{C}) = 0.385089.$$

The diversity of this code at different rates is given below.

$\lvert\mathcal{C}\rvert$	R	diversity	family of matrices
63	1.9924	0.38508	$D^l E^k$, $l = 0, \dots 20, k = 0, 1, 2$
126	2.3258	0.29658	$\pm D^l E^k$, $l = 0, \dots 20, k = 0, 1, 2$
441	2.9282	0.18898	$D^l E^k F^n$, $l = 0, \dots 20, k = 0, 1, 2,\ n = 0, \dots, 6$
819	3.2259	0.06442	$D^l E^k F^n$, $l = 0, \dots 20, k = 0, 1, 2,\ n = 0, \dots, 12$

A second construction. We give a second construction, built in a similar manner. We consider now the cyclic algebra

$$\mathcal{A} = (\mathbb{Q}(\zeta_{39})/K, \sigma, \zeta_{39}^{13}),$$

where $\sigma : \zeta_{39} \mapsto \zeta_{39}^{16}$. Similarly as for the first construction, we look for a family of matrices of common denominator. This time, we take the element x such that

$$x = (-\zeta^2 + \zeta^3 + \zeta^9 - \zeta^{11} - \zeta^{14} + \zeta^{16} - \zeta^{17} - \zeta^{20})/2$$

(we write $\zeta = \zeta_{39}$). Its conjugates are given by

$$\begin{aligned} \sigma(x) &= (-1 - \zeta + \zeta^2 + \zeta^5 + \zeta^{11} - \zeta^{13} + \zeta^{17} + \zeta^{23})/2 \\ \sigma^2(x) &= (\zeta^3 - \zeta^5 - \zeta^8 + \zeta^9 - \zeta^{11} - \zeta^{14} + \zeta^{22} - \zeta^{23})/2 \end{aligned}$$

We use the following matrices:

$$D = \begin{pmatrix} \zeta_{39} & 0 & 0 \\ 0 & \zeta_{39}^{16} & 0 \\ 0 & 0 & \zeta_{39}^{22} \end{pmatrix},\ E = \begin{pmatrix} 0 & 0 & \zeta_{39}^{13} \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},\ F = \begin{pmatrix} x & 0 & 0 \\ 0 & \sigma(x) & 0 \\ 0 & 0 & \sigma^2(x) \end{pmatrix}.$$

Some values of the diversity product for this construction is reported below.

$\vert\mathcal{C}\vert$	R	diversity	family of matrices
117	2.2901	0.3227	D^lE^k, $l=0,\dots 38, k=0,1,2$
234	2.6235	0.2730	$\pm D^lE^k$, $l=0,\dots 38, k=0,1,2$
1638	3.5592	0.0723	$\pm D^lE^kF^n$, $l=0,\dots 38, k=0,1,2,\ n=0,\dots,6$

Performance of the new codes. We compare the two new constructions for 3 antennas given above with codes for 3 antennas given in [18] and [6].

We have simulated the codes over a noncoherent Rayleigh flat fading channel (as described in Subsection I-A),

$$\mathbf{Y}_t = \sqrt{\rho}\mathbf{S}_t\mathbf{H}_t + \mathbf{W}_t,\ \ t=0,1,\dots$$

with $M=3$ transmitter antennas and $N=1$ receiver antennas. Here $\mathbf{H}_t$ and $\mathbf{W}_t$ are two 3×1 matrices with independent complex normal coefficients, and ρ is the expected SNR at each receiver antenna. Symbols transmitted over 3 antennas are grouped in blocks of 3 channel uses (t indexes these blocks) over which the fading is assume to be constant. The transmitted signal $\mathbf{S}_t$ is encoded using differential modulation, that is

$$\mathbf{S}_t = \mathbf{X}_{z_t}\mathbf{S}_{t-1},\ \ t=1,2,\dots,$$

with $\mathbf{S}_0 = \mathbf{I}_3$. The maximum likelihood decoder is thus given by

$$\hat{z}_t = \arg\min_{l=0,\dots,|\mathcal{C}|-1} \|\mathbf{Y}_t - \mathbf{X}_l\mathbf{Y}_{t-1}\|.$$

We will use here for the simulations maximum likelihood through exhaustive search, since a decoding algorithm is beyhond the scope of this work. On Fig. 5, the block-error rate performance of the first construction at rate 2.93 (with diversity 0.189) is compared to the code obtained from the fixed point free group $G_{171,64}$ with rate 3 (and diversity 0.1353). The new code performs better. On Fig. 6, we compare the new code at rate 3.23 to codes based on the representation of the Lie group SU_3 [6]. The new code performs similarly. Notice here that the decodings are different, since the Lie group based codes are decoded using a modified version of the complex Sphere Decoder.

D. Codes for 4 antennas

We give an illustration of our technique for the case of 4 antennas. Let ζ_{20} be a primitive 20th root of unity. We consider the field extension $\mathbb{Q}(\zeta_{20})/\mathbb{Q}(i)$, which is cyclic of degree 4. Its Galois group is

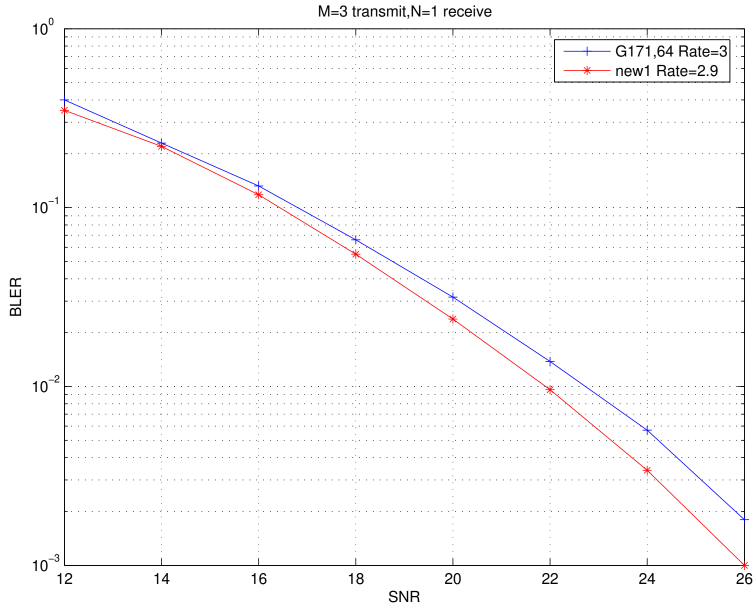

Fig. 5. Block-error rate for 3 transmit antennas and 1 receive antenna at rate 3.

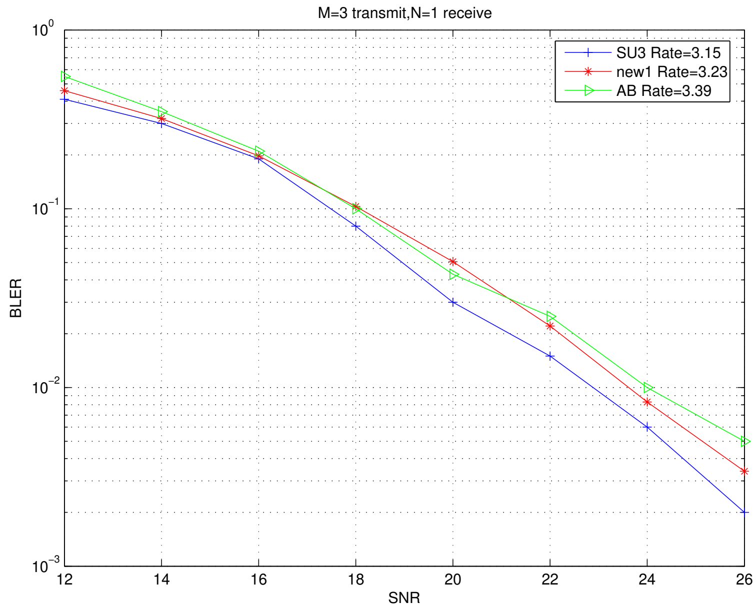

Fig. 6. Block-error rate for 3 transmit antennas and 1 receive antenna at rate greater than 3.

generated by $\langle\sigma\rangle$, with $\sigma : \zeta_{20} \mapsto \zeta_{20}^{13}$. We thus defined the cyclic algebra $\mathcal{A} = (\mathbb{Q}(\zeta_{20})/\mathbb{Q}(i), \sigma, i)$.

As previously, we consider the codebook

$$\mathcal{C} = \{D^l E^k F^i \mid l = 0, \ldots, 20,\ k = 0, 1, 2,\ i = 0, \ldots, 4\},$$

where

$$D = \begin{pmatrix} \zeta_{20} & 0 & 0 & 0 \\ 0 & \zeta_{20}^{13} & 0 & 0 \\ 0 & 0 & \zeta_{20}^{9} & 0 \\ 0 & 0 & 0 & \zeta_{20}^{17} \end{pmatrix},\ E = \begin{pmatrix} 0 & 0 & 0 & \zeta_{21}^{7} \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

and F is defined as follows. For short, we write $\zeta = \zeta_{20}$. Consider x given by

$$x = (-1 - 3\zeta + 2\zeta^2 + \zeta^3 + 2\zeta^4 + \zeta^5 - \zeta^6 + 2\zeta^7)/5.$$

Its conjugates are

$$\begin{aligned} \sigma(x) &= (-2 - \zeta - \zeta^2 + 2\zeta^3 - \zeta^4 + 2\zeta^5 + 3\zeta^6 - \zeta^7)/5 \\ \sigma^2(x) &= (1 + 3\zeta - 2\zeta^2 - \zeta^3 + 3\zeta^4 + 4\zeta^5 - 4\zeta^6 - 2\zeta^7)/5 \\ \sigma^3(x) &= (-3 + \zeta + \zeta^2 - 2\zeta^3 - 4\zeta^4 + 3\zeta^5 + 2\zeta^6 + \zeta^7)/5 \end{aligned}$$

The matrix F is

$$F = \begin{pmatrix} x & 0 & 0 & 0 \\ 0 & \sigma(x) & 0 & 0 \\ 0 & 0 & \sigma^2(x) & 0 \\ 0 & 0 & 0 & \sigma^3(x) \end{pmatrix}.$$

In Fig. 7, we compare the performance of this code to a code based on the Lie group Sp_2 [7]. The two codes behave similarly. Note again that the decoding algorithms are different.

VI. Conclusion and Perspective

In this work, we have presented a method to construct infinitely many unitary matrices in cyclic algebras, and thus in any dimension n, which is in itself of theoretical interest. Our motivation was the design of fully-diverse unitary matrices for the noncoherent differential channel. As an application of our

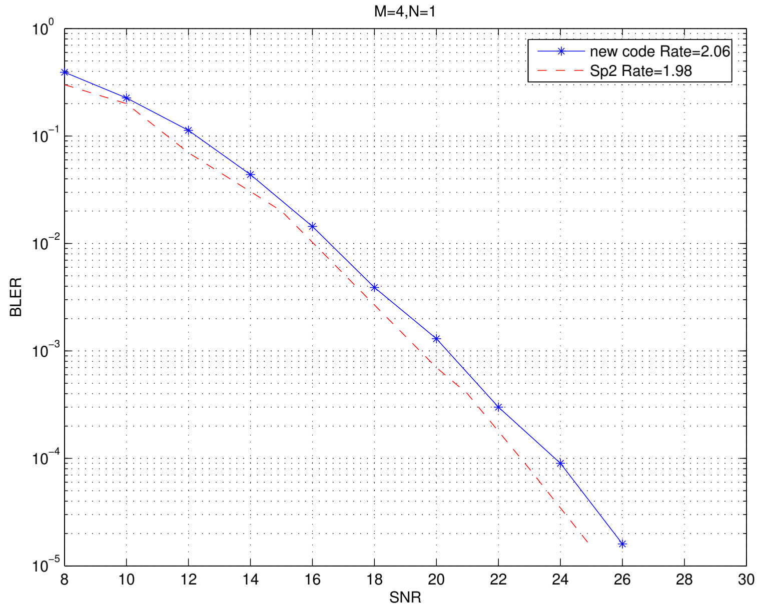

Fig. 7. Block-error rate for 4 transmit antennas and 1 receive antenna at rate 2.

technique, we present new families of codes for 3 and 4 antennas. The aim of this work is to point out the use of cyclic algebras for noncoherent space-time coding. We believe this is a promising tool, thanks to its generality, and the many degrees of freedom it offers. In any cyclic algebra based on a suitable field, one can take any quadratic extension M/M^{α} in which any element can be taken to create a unitary element.

There are a lot of perspectives using this method. To start with, one can use it for designing codes for other numbers of antennas, since the method is available for any dimension. A better bound on the diversity product would be of great interest for that purpose. High rate is also a goal. Since there are infinitely many matrices, high rate is of course possible. There is work to be done on how to choose carefully the matrices. One could try to compose several subfields inside a given algebra for example. The decoding is also an issue. One possible research direction is to look for a suitable decoder algorithm.

Acknowledgment

The author would like to thank Dr. E. Lequeu for useful discussions at the beginning of this work.

REFERENCES

[1] J. Abarbanel, A. Averbuch, S. Rosset, J. Zlotnick,“Unitary non-group STBC codes from cyclic algebras”, online at www.cs.tau.ac.il/ amir1/PS/mimo1.pdf.

[2] B. Hassibi and H. Vikalo, “On sphere decoding algorithm. I. Expected complexity”, *IEEE Transactions on Signal Processing*, vol. 53, no. 8, August 2005, pp. 2806 - 2818.

[3] B. Hassibi and B. Hochwald,“Cayley Differential Unitary Space-Time Codes”, *IEEE Trans. on Information Theory*, vol. 48, June 2002.

[4] B. Hochwald and W. Sweldens,“Differential unitary space time modulation”, *IEEE Trans. Commun.*, vol. 48, Dec. 2000.

[5] B. Hughes, “Differential space-time modulation,” *IEEE Trans. Inform. Theory*, vol 46, Nov. 2000.

[6] Y. Jing, B. Hassibi, “Three-Transmit-Antenna Space-Time Codes Based on SU(3)”, *IEEE Trans. Signal Processing*, vol. 53, no 10, Oct. 2005.

[7] Y. Jing, B. Hassibi, “Design of full-diverse multiple-antenna codes based on Sp(2)”, *IEEE Trans. on Information Theory*, vol. 50, no 11, Nov. 2004.

[8] Xue-Bin Liang and Xiang-Gen Xia, “Unitary Signal Constellations for Differential Space-Time Modulation With Two Transmit Antennas: Parametric Codes, Optimal Designs, and Bounds,” *IEEE Trans. on Inform. Theory*, vol. 48, no.8, August 2002.

[9] F. E. Oggier, G. Rekaya, J.-C. Belfiore and E. Viterbo, “Perfect Space-Time Block Codes”, to appear in *IEEE Trans. on Information Theory*, September 2006.

[10] F. Oggier, E. Lequeu,“Families of unitary matrices achieving full diversity”, *Proceedings of the International Symposium on Information Theory (ISIT)*, Adelaide, 2005.

[11] F. Oggier and E. Viterbo, “Algebraic number theory and code design for Rayleigh fading channels”, *Foundations and Trends in Communications and Information Theory*, vol. 1, pp. 333-415, 2004.

[12] F. Oggier,“First applications of cyclic algebras to noncoherent MIMO channels”, *Proceedings of the 43rd annual Allerton conference on communication, control, and computing*, 2005.

[13] R. S. Pierce, “Associative Algebras,” Springer-Verlag, New York, 1982.

[14] I. Reiner,”Maximal Orders”, Academic Press, 1975.

[15] I. Stewart, “Galois Theory”, Chapman and Hall, 1989.

[16] I. Steward and D. Tall,“Algebraic Number Theory”, Chapman and Hall, 1979.

[17] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, “Full-diversity, high-rate space-time block codes from division algebras,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 2596– 2616, October 2003.

[18] A. Shokrollahi, B. Hassibi, B. M. Hochwald, W. Sweldens, “Representation Theory for High-Rate Multiple-Antenna Code Design”, *IEEE Trans. Information Theory*, vol. 47, no 6, Sept. 2001.

[19] 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.

[20] V. Tarokh, N. Seshadri, and A. Calderbank, “Space-time codes for high data rate wireless communication : Performance criterion and code construction,” *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, March 1998.