# MIDO Space-Time Codes from Associative and Nonassociative Cyclic Algebras

Andrew Steele and Susanne Pumplün
School of Mathematical Sciences
University of Nottingham, University Park
Nottingham NG7 2RD,United Kingdom
Email:{pmxas4,Susanne.Pumpluen}@nottingham.ac.uk

Frédérique Oggier
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University, Singapore
Email:frederique@ntu.edu.sg

***Abstract*—Nonassociative division algebras have been recently proposed as an alternative way to design fully-diverse space-time codes. In particular, nonassociative cyclic algebras provide division algebras more easily than their associative counter-part. In this paper, we propose a few space-time code constructions coming from both associative and nonassociative cyclic algebras of degree 4, suitable for 4 transmit and 2 receive antennas, which furthermore exhibit good fast-decodability.**

## I. Introduction

Following the seminal work by Sethuraman et al. [1], division algebras, or to be more precise, associative division algebras have been adopted as a tool to construct fully-diverse space-time codes. Many good space-time codes coming from division algebras are by now available in the literature, though their main drawback stays their decoding complexity: these codes possess a lattice structure, and maximum likelihood (ML) decoding of a lattice code via sphere decoding remains costly. In [2], Biglieri et al. introduced the notion of fast-decodable space-time codes, that is space-time codes whose code design takes into account not only the performance of the code, but also its decoding complexing via sphere decoding. This triggered an already rich line of research, looking for fast-decodable codes. The particular case of MIDO (standing for multiple input double output) space-time codes has attracted a particular amount of attention, due to its potential application to digital broadcasting, for scenarios where the end user is carrying a portable device, whose number of antennas is less than that of the transmitter. From a coding perspective, a full rate space-time code for a MIDO channel carries 16 real information symbols instead of 32, offering several degrees of freedom that can be used to derive fast-decodable codes from division algebras. This has been already exploited for example in [3] where fast-decodable codes were derived by puncturing codewords coming from cyclic division algebras over a big center, in [4] where crossed product algebras over $\mathbb{Q}$ were considered, or in [5] through an iterated quaternion algebra construction. Using division algebras is of course not the only way to get fast-decodable codes, see for example [6], [7], [8].

Recently, nonassociative quaternion division algebras have been proposed as an alternative way to obtain fully-diverse space-time codes [9]. It is well understood that nonassociative finite-dimensional real division algebras can only have dimension 1, 2, 4 or 8 [12], and in fact, the best known finite-dimensional real division algebras are $\mathbb{R}$, $\mathbb{C}$, Hamilton's quaternions $\mathbb{H}$ and Cayley's octonions $\mathbb{O}$. Real nonassociative division algebras in general are however far from being classified. The situation becomes even more difficult when looking at other base fields like number fields, which is the case typically of interest in the context of space-time coding, or finite fields, where there are no restrictions on the possible dimensions of division algebras any more.

In [10], new nonassociative algebras have been found. Their construction is similar to the one of associative cyclic algebras, however they turn out to be highly nonassociative. These algebras were called nonassociative cyclic algebras. They exist over any base field possessing a cyclic field extension of degree $n$. They are unital and of dimension $n^n$. In particular, we will consider nonassociative cyclic algebras of dimension 16. They contain a cyclic field extension of degree four as a subalgebra and when division, can be used to design fully diverse $4 \times 4$-STBCs, similarly to the associative case.

In this paper, we address the design of MIDO space-time codes coming from cyclic algebras, both associative and nonassociative, of dimension 16. After recalling how to design space-time codes from associative algebras briefly in Section II, and more in detail for the less familiar case of nonassociative algebras in Section III, we discuss both their encoding in Section IV. We will present a few code constructions in Section V, which exhibit good fast-decodability properties. Advantages of codes constructed from associative and nonassociative cyclic algebras will be discussed, though we already emphasize here that nonassociative cyclic algebras provide division algebras much more easily than their associative counterpart, which in itself make them interesting to study in the context of space-time coding.

## II. Codes from Associative Algebras

Let $K/F$ be a cyclic Galois extension of degree 4 with Galois group $G = \mathrm{Gal}(K/F) = \langle\sigma\rangle$, and let $\gamma$ be a nonzero element of $F$. An associative cyclic algebra $A$ is a 4-dimensional $K$-vector space with $\{1, e, e^2, e^3\}$ as a $K$-basis, namely

$$A := K \oplus Ke \oplus Ke^2 \oplus Ke^3,$$

where multiplication is given by

$$e^4 = \gamma,\ el = \sigma(l)e, \tag{1}$$

for every $l$ in $K$. It is denoted $A = (K/F, \sigma, \gamma)$. Since the case of associative algebras is well-known (e.g. [1]), we will just recall here that codewords coming from this algebra are obtained by considering multiplication matrices of the form

$$\begin{bmatrix} y_0 & \sigma(y_3)\gamma & \sigma^2(y_2)\gamma & \sigma^3(y_1)\gamma \\ y_1 & \sigma(y_0) & \sigma^2(y_3)\gamma & \sigma^3(y_2)\gamma \\ y_2 & \sigma(y_1) & \sigma^2(y_0) & \sigma^3(y_3)\gamma \\ y_3 & \sigma(y_2) & \sigma^2(y_1) & \sigma^3(y_0) \end{bmatrix} \tag{2}$$

where $y_0, \dots, y_3 \in K$ and that this matrix corresponds to multiplication by $y = y_0 + y_1 e + y_2 e^2 + y_3 e^3$. To get fully-diverse codewords, it is enough for this algebra to be division, which is guaranteed if $\gamma \in F$ is chosen such that the smallest integer $t \geq 0$ with $\gamma^t \in N_{K/F}(K^\times)$ is $t = 4$.

## III. Codes from Non-Associative Algebras

Let us first recall a few basic properties of nonassociative algebras.

### A. Nonassociative cyclic algebras

Let $A$ be a finite-dimensional $F$-vector space. We assume there is an $F$-bilinear map $A \times A \to A$, $(x, y) \to x \cdot y$, also denoted simply by juxtaposition $xy$, called a *multiplication* on $A$. Every vector space $A$ together with a multiplication $A \times A \to A$ is called an *algebra* over $F$. This definition does not mean the algebra is associative, we only have $c(xy) = (cx)y = x(cy)$ for all $c \in F$, $x, y \in A$. Hence we also call such an algebra a *nonassociative algebra*. A nonassociative algebra $A$ is called *unital* if there is an element in $A$ (which can be shown to be uniquely determined), denoted by 1, such that $1x = x1 = x$ for all $x \in A$. The associator of $x, y, z \in A$ is defined to be

$$[x, y, z] := (xy)z - x(yz).$$

The *nucleus* of $A$ is then defined as

$$N(A) := \{x \in A \mid [x, A, A] = [A, x, A] = [A, A, x] = 0\}.$$

It is an associative subalgebra of $A$ (it may be zero), and $x(yz) = (xy)z$ whenever one of the elements $x, y, z$ is in $N(A)$. The nucleus of the algebra $A$ contains all the elements of $A$ which associate with every other two elements in $A$.

A nonassociative $F$-algebra $A$ is called a *division algebra* if for any $a \in A$, $a \neq 0$, the left multiplication with $a$, $L_a(x) = ax$, and the right multiplication with $a$, $R_a(x) = xa$, are bijective. Since we are working with finite-dimensional vector spaces, $A$ is a division algebra if and only if $A$ has no zero divisors [11].

Let $K/F$ be a cyclic Galois extension of degree 4, with Galois group $G = \mathrm{Gal}(K/F) = \langle \sigma \rangle$, and pick a nonzero element $\gamma \in K \backslash F$. A nonassociative algebra $A$ can be formed as follows. Let $A$ be the 4-dimensional $K$-vector space with $K$-basis given by $\{1, e, e^2, e^3\}$, such that

$$A := K \oplus Ke \oplus Ke^2 \oplus Ke^3.$$

Define a multiplication on $A$ via the following rules for all $l, m \in K$, which then are extended linearly to all elements of $A$:

$$\begin{array}{ll} l(me^j) = (lm)e^j,\ j = 1, 2, 3 & \\ (le)m = (l\sigma(m))e, & (le)(me) = (l\sigma(m))e^2 \\ (le)(me^2) = (l\sigma(m))e^3, & (le)(me^3) = (l\sigma(m))\gamma \\ (le^2)m = (l\sigma^2(m))e^2, & (le^2)(me) = (l\sigma^2(m))e^3 \\ (le^2)me^2 = (l\sigma^2(m))\gamma, & (le^2)(me^3) = (l\sigma^2(m))\gamma e, \\ (le^3)m = (l\sigma^3(m))e^3, & (le^3)(me) = (l\sigma^3(m)))\gamma, \\ (le^3)me^2 = (l\sigma^3(m))\gamma e, & (le^3)(me^3) = (l\sigma^3(m))\gamma e^2. \end{array}$$

We observe that the way to build the algebra $A$ is similar to the associative case (1): we again obtain that $el = \sigma(l)e$ and also that $e^i e^j = \gamma$ for all integers $i, j$ such that $i + j = 4$, so that the expression $e^4$ is well-defined and, indeed, $e^4 = \gamma$. Thus we again use the notation $A = (K/F, \sigma, \gamma)$. It can be shown that the nucleus of $A$ is $K$, while its center is $F$. These algebras are new unital nonassociative division algebras [10]. We call $A$ a *nonassociative cyclic algebra of dimension* 16.

### B. Codes from nonassociative cyclic algebras

Let $K/F$ be a cyclic field extension of degree four. Let $A = (K/F, \sigma, \gamma)$ be an associative or nonassociative cyclic $F$-algebra (i.e., $\gamma \in F^\times$ or $\gamma \in K \setminus F$).

In order to design space-time codes, cyclic associative division algebras are considered as a vector space over their subfield $K$, yielding fully diverse $4 \times 4$ codes. Given a nonassociative $F$-algebra with a subfield $K$, this method is usually not possible because of the nonexistence of the associative law. However, the nonassociative algebras $A$ presented above are special in that the subfield $K$ of the nonassociative cyclic algebra is such that $K = N(A)$.

Consider $A$ as a right $K$-vector space of dimension 4. After a choice of a $K$-basis for $A$, we can embed the right $K$-vector space $\mathrm{End}_K(A)$ into the vector space $\mathrm{Mat}_4(K)$. This way we get an embedding

$$\lambda : A \to \mathrm{Mat}_4(K)$$

of vector spaces. Obviously, we have $X \pm Y \in \lambda(A)$ for all $X, Y \in \lambda(A)$. Thus if we choose a subset $\mathcal{C}$ of $\lambda(A)$, the difference of two distinct elements of $\mathcal{C}$ will also lie in $\lambda(A)$, and $\mathcal{C}$ can be chosen for a codebook.

Similarly to the associative case, a matrix is associated to an element of the algebra via the regular representation. More precisely, the right regular representation, i.e., the matrix of right multiplication by an element $y = y_0 + y_1 e + y_2 e^2 + y_3 e^3$ in the basis $\{1, e, e^2, e^3\}$ can be computed to be

$$\begin{bmatrix} y_0 & \sigma(y_3)\gamma & \sigma^2(y_2)\gamma & \sigma^3(y_1)\gamma \\ y_1 & \sigma(y_0) & \sigma^2(y_3)\gamma & \sigma^3(y_2)\gamma \\ y_2 & \sigma(y_1) & \sigma^2(y_0) & \sigma^3(y_3)\gamma \\ y_3 & \sigma(y_2) & \sigma^2(y_1) & \sigma^3(y_0) \end{bmatrix}. \tag{3}$$

We note that codewords obtained from nonassociative cyclic algebras are actually very similar to those obtained from associative cyclic algebras, apart from the choice of the element $\gamma$.

We would like to point out here that the codewords obtained above cannot be obtained from a representation of an associative algebra: would this be the case, we would be able to take any two non-zero matrices in $\lambda(A)$, multiply them and again obtain an element in $\lambda(A)$. This, however, is not the case due to our choice of $\gamma \in K \setminus F$. Since this means that $\sigma(\gamma) \neq \gamma$, a straightforward computation shows this immediately.

It remains to check when a codebook formed by such matrices is fully diverse. This is indeed the case for any choice of $\gamma$ in $K$ but not in $F$, such that $1, \gamma, \gamma^2, \gamma^3$ are linearly independent over $F$ [10]. Observe to that effect that the highest power of $\gamma$ in the determinant of (3) is $\gamma^3$, and comes from the term

$$N_{K/F}(y_3)\gamma^3$$

where $N_{K/F}$ denotes the algebraic norm (not to be mistaken for $N$ which stands for the nucleus). There is also a term without $\gamma$, which is the one coming from the main diagonal:

$$N_{K/F}(y_0).$$

Suppose that the elements $1, \gamma, \gamma^2, \gamma^3$ are linearly independent over $F$ and that the determinant of (3) is zero, then $N_{K/F}(y_0) = N_{K/F}(y_3) = 0$. Since the map $N_{K/F}$ is non-degenerate, this implies that $y_0 = y_3 = 0$, and (3) becomes

$$\begin{bmatrix} 0 & 0 & \sigma^2(y_2)\gamma & \sigma^3(y_1)\gamma \\ y_1 & 0 & 0 & \sigma^3(y_2)\gamma \\ y_2 & \sigma(y_1) & 0 & 0 \\ 0 & \sigma(y_2) & \sigma^2(y_1) & 0 \end{bmatrix}.$$

The highest power of $\gamma$ in this determinant is now $\gamma^2$, with coefficient $N_{K/F}(y_2)$, showing that $y_2 = 0$, and similarly $y_1$ must be zero. This shows that right multiplication by $y$ is an invertible endomorphism for all nonzero $y$ and thus $A$ is a division algebra, inducing a fully-diverse codebook.

## IV. Encoding and Fast Decodability

Let $K/F$ be a cyclic Galois extension of degree 4, with Galois group $G = \mathrm{Gal}(K/F) = \langle \sigma \rangle$.

Suppose that $\gamma$ is of the form $-\gamma'$ where $\gamma'$ is a positive real number (in what follows we will use by abuse of notation $-\gamma$ where $\gamma$ is a positive real number to avoid introducing more notation). Then (3) becomes

$$\begin{bmatrix} y_0 & -\gamma\sigma(y_3) & -\gamma\sigma^2(y_2) & -\gamma\sigma^3(y_1) \\ y_1 & \sigma(y_0) & -\gamma\sigma^2(y_3) & -\gamma\sigma^3(y_2) \\ y_2 & \sigma(y_1) & \sigma^2(y_0) & -\gamma\sigma^3(y_3) \\ y_3 & \sigma(c) & \sigma^2(y_1) & \sigma^3(y_0) \end{bmatrix}$$

where $y_0, y_1, y_2, y_3 \in K$. By exchanging the second and third row and the second and third column of the above matrix, we obtain

$$\begin{bmatrix} y_0 & -\gamma\sigma^2(y_2) & -\gamma\sigma(y_3) & -\gamma\sigma^3(y_1) \\ y_2 & \sigma^2(y_0) & \sigma(y_1) & -\gamma\sigma^3(y_3) \\ y_1 & -\gamma\sigma^2(y_3) & \sigma(y_0) & -\gamma\sigma^3(y_2) \\ y_3 & \sigma^2(y_1) & \sigma(y_2) & \sigma^3(y_0) \end{bmatrix}.$$

Notice that the determinant of the $4 \times 4$ matrix is not changed when we multiply the second and fourth column by $1/\sqrt{\gamma}$ and the second and fourth row by $\sqrt{\gamma}$. Renaming the variables $a, b, c, d$ we obtain the code $\mathcal{C}$ given by codewords of the form

$$\begin{bmatrix} a & -\sqrt{\gamma}\sigma^2(b) & -\gamma\sigma(d) & -\sqrt{\gamma}\sigma^3(c) \\ \sqrt{\gamma}b & \sigma^2(a) & \sqrt{\gamma}\sigma(c) & -\gamma\sigma^3(d) \\ c & -\sqrt{\gamma}\sigma^2(d) & \sigma(a) & -\sqrt{\gamma}\sigma^3(b) \\ \sqrt{\gamma}d & \sigma^2(c) & \sqrt{\gamma}\sigma(b) & \sigma^3(a) \end{bmatrix}. \qquad (4)$$

This code can be seen as a vector space of dimension 16 over $F$, with $F$-basis $B_1, \ldots, B_{16}$. Let $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ be an $F$-basis of $K$, so that

$$a = \sum_{j=1}^{4} a_j\theta_j,\ b = \sum_{j=1}^{4} b_j\theta_j,\ c = \sum_{j=1}^{4} c_j\theta_j,\ d = \sum_{j=1}^{4} d_j\theta_j.$$

Then $B_1, B_2, B_3, B_4$ are given by

$$\begin{bmatrix} \theta_j & & & \\ & \sigma^2(\theta_j) & & \\ & & \sigma(\theta_j) & \\ & & & \sigma^3(\theta_j) \end{bmatrix},\ j = 1, \ldots, 4,$$

$B_5, B_6, B_7, B_8$ by

$$\sqrt{\gamma}\begin{bmatrix} & -\sigma^2(\theta_j) & & \\ \theta_j & & & \\ & & & -\sigma^3(\theta_j) \\ & & \sigma(\theta_j) & \end{bmatrix},\ j = 1, \ldots, 4,$$

$B_9, B_{10}, B_{11}, B_{12}$ by

$$\begin{bmatrix} & & & -\sqrt{\gamma}\sigma^3(\theta_j) \\ & & \sqrt{\gamma}\sigma(\theta_j) & \\ \theta_j & & & \\ & \sigma^2(\theta_j) & & \end{bmatrix},\ j = 1, \ldots, 4$$

and finally $B_{13}, B_{14}, B_{15}, B_{16}$ by

$$\begin{bmatrix} & & -\gamma\sigma(\theta_j) & \\ & & & -\gamma\sigma^3(\theta_j) \\ & -\sqrt{\gamma}\sigma^2(\theta_j) & & \\ \sqrt{\gamma}\theta_j & & & \end{bmatrix},\ j = 1, \ldots, 4.$$

It was shown in [8] that the decoding complexity of the space-time code with $F$-basis $B_1, \ldots, B_{16}$ can be read from the matrix $M$ whose coefficients $m_{jk}$ are given by

$$m_{jk} = ||B_j B_k^* + B_k B_j^*||_F,$$

where $F$ refers to the Frobenius norm of matrices and $()^*$ means the Hermitian transpose. More precisely, the zero structure of $M$ is the same as that of $R$, the upper right triangular matrix used in the sphere decoder. Let $S$ be the real constellation in use (say PAM symbols). Then the worst case complexity is that of exhaustive search, which is of $O(|S|^{16})$ and corresponds to a full upper right triangular matrix $R$. If the zero structure of $M$ (or equivalently of $R$) is such that groups of real symbols can be decoded independently, then the complexity order might drop.

## V. Code Examples

We now propose a few code constructions and compute their decoding complexity order via sphere decoding.

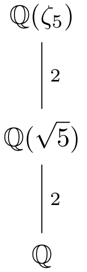

Fig. 1. The cyclotomic field $\mathbb{Q}(\zeta_5)$ and its subfield.

### A. A code from $\mathbb{Q}(\zeta_5)$

Let $\zeta_5$ be a primitive 5th root of unity, and consider the cyclotomic field extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ (see Figure 1), with cyclic Galois group generated by $\sigma : \zeta_5 \mapsto \zeta_5^2$. We have that $\sigma^2 : \zeta_5 \mapsto \zeta_5^2$ generates a subgroup of order 2, with corresponding fixed field $\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$.

By considering as $\mathbb{Q}$-basis the canonical basis $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$, and $-\gamma$ for any positive real $\gamma$ in $\mathbb{Q}(\zeta_5)$, we observe that the four blocks of (4) are in fact of the form of a generalized Alamouti block code, that is

$$\begin{bmatrix} a & -\sqrt{\gamma}\sigma^2(b) \\ \sqrt{\gamma}b & \sigma^2(a) \end{bmatrix}, \begin{bmatrix} \sigma(a) & -\sqrt{\gamma}\gamma\sigma^3(b) \\ \sqrt{\gamma}\sigma(b) & \sigma^3(a) \end{bmatrix}$$

and

$$\begin{bmatrix} c & -\sqrt{\gamma}\sigma^2(d) \\ \sqrt{\gamma}d & \sigma^2(c) \end{bmatrix}, \begin{bmatrix} -\gamma\sigma(d) & \zeta\sqrt{\gamma}\sigma^3(c) \\ \sqrt{\gamma}\sigma(b) & \sigma^3(a) \end{bmatrix},$$

since $\sigma^2$ fixes the maximal real subfield of $\mathbb{Q}(\zeta_5)$, and thus plays the role of the complex conjugation. Note that by generalized Alamouti code, we mean a slightly more general definition than in [2]. An Alamouti codeword has the form

$$\begin{bmatrix} u & -v^* \\ v & u^* \end{bmatrix}$$

with the property that the two columns are orthonormal (we use $()^*$ to denote the complex conjugation). In our case, each block similarly has the property that both columns are orthogonal. As a result, we have that

$$m_{jk} = ||B_j B_k^* + B_k B_j^*||_F = 0$$

for $j = 1,2,3,4$ and $k = 5,6,7,8$, $j = 5,6,7,8$ and $k = 1,2,3,4$, and symmetrically, for $j = 13,14,15,16$ and $k = 9,10,11,12$ as well as $j = 9,10,11,12$ and $k = 13,14,15,16$, which gives a matrix $M$ of the form

$$M = \begin{bmatrix} * & \mathbf{0}_{4\times4} & * & * \\ \mathbf{0}_{4\times4} & * & * & * \\ * & * & * & \mathbf{0}_{4\times4} \\ * & * & \mathbf{0}_{4\times4} & * \end{bmatrix}, \qquad (5)$$

where $*$ are $4 \times 4$ full matrices, for a decoding complexity of $O(M^{12})$. Indeed, 8 symbols have to be decoded first, for a complexity of $O(M^8)$, after which two groups of 4 symbols each can be decoded, for a cost of $O(2M^4)$, and thus a total of $O(M^{12})$.

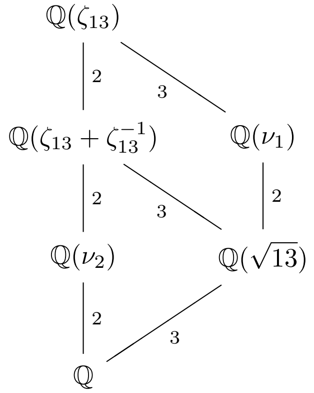

Fig. 2. The cyclotomic field $\mathbb{Q}(\zeta_{13})$ and its subfields: $\nu_1 = \zeta_{13} + \zeta_{13}^3 + \zeta_{13}^5$ and $\nu_2 = \zeta_{13}^2 + \zeta_{13}^3 + \zeta_{13}^{10} + \zeta_{13}^{11}$.

### B. A code from $\mathbb{Q}(\zeta_{13})$

What gave us four generalized Alamouti blocks in the above code construction is the fact that the Galois group of $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\zeta_5 + \zeta_5^{-1})$ plays the role of the complex conjugation. This is true for every cyclotomic field $\mathbb{Q}(\zeta_n)$ for $\zeta_n$ a primitive $n$th root of unity, when looking at the quadratic extension it forms together with its maximal real subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. However, we further have here two constraints: we need a cyclic Galois group, and we need it to be of degree 4. An easy way to fullfil the former is to choose a $p$th root of unity, since then the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is cyclic, and a subgroup might be chosen to be of order 4. For example, take $p = 13$, and consider the cyclotomic field $\mathbb{Q}(\zeta_{13})$ which is of degree 12 over $\mathbb{Q}$ (see Figure 2). It has Galois group generated by $\sigma : \zeta_{13} \mapsto \zeta_{13}^2$. The subgroup $\langle\sigma^3\rangle$ has order 4, and since $\sigma^3 : \zeta_{13} \mapsto \zeta_{13}^8$, it can be computed that its fixed field is $\mathbb{Q}(\zeta_{13}^2 + \zeta_{13}^3 + \zeta_{13}^{10} + \zeta_{13}^{11})$. Similarly, the subgroup of order 3 generated by $\sigma : \zeta_{13} \mapsto \zeta_{13}^4$ has fixed field $\mathbb{Q}(\zeta_{13} + \zeta_{13}^3 + \zeta_{13}^5)$. The maximal real subfield $\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$ is fixed by $\langle\sigma^6\rangle$, which is a subgroup of $\langle\sigma^3\rangle$. The field extension $\mathbb{Q}(\zeta_{13})/\mathbb{Q}(\zeta_{13}^2 + \zeta_{13}^3 + \zeta_{13}^{10} + \zeta_{13}^{11})$ has degree 4 with cyclic Galois group generated by $\tau = \sigma^3$, where $\tau^2 = \sigma^6$ is acting as the complex conjugation.

By picking $-\gamma$, for $\gamma$ a positive real number in $\mathbb{Q}(\zeta_{13})$, a codeword of the form (4) will again contain four generalized Alamouti block codes. The corresponding matrix $M$ is again as in (5), for a complexity of $O(M^{12})$. Unlike in the case of $\mathbb{Q}(\zeta_5)$ where the code was naturally providing 16 real information symbols, in this case up to $4 \cdot 12$ real symbols are available, and thus there is a need to choose $4 \cdot 3$ symbols to be transmitted.

### C. A second code from $\mathbb{Q}(\zeta_5)$

In order to reduce the complexity further, the matrix $M$ in (5) should become sparser. In particular, the $4 \times 4$ upper left block should get some zeroes, that is

$$||B_j B_k^* + B_k B_j^*||_F = 0$$

for some indices $j, k \in \{1, 2, 3, 4\}$. The condition

$$B_j B_k^* = -B_k B_j^*$$

means that $B_j B_k^*$ is in fact a skew-Hermitian matrix. One way to obtain this is to pick as $F$-basis of $K$ elements which are either totally real or totally imaginary. While consider the number field $\mathbb{Q}(\zeta_5)/\mathbb{Q}$, the canonical $\mathbb{Q}$-basis $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$ does not satisfy this condition. However, a less natural basis can be chosen instead, by noticing that $\zeta_5 + \zeta_5^4$ and $\zeta_5^2 + \zeta_5^3$ are totally real, while $\zeta_5 - \zeta_5^{-1}$ is totally imaginary. For example, the choice of

$$1, \zeta_5 - \zeta_5^4, \zeta_5^2 + \zeta_5^3, (\zeta_5^2 + \zeta_5^3)(\zeta_5 - \zeta_5^4) = -1 - 2\zeta_5 - 2\zeta_5^2$$

yields a matrix $M$, this time of the form

$$\begin{bmatrix}
* & \mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} & * & * & * & * \\
\mathbf{0}_{2\times 2} & * & \mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} & * & * & * & * \\
\mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} & * & \mathbf{0}_{2\times 2} & * & * & * & * \\
\mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} & * & * & * & * & * \\
* & * & * & * & * & \mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} \\
* & * & * & * & \mathbf{0}_{2\times 2} & * & \mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} \\
* & * & * & * & \mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} & * & \mathbf{0}_{2\times 2} \\
* & * & * & * & \mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} & \mathbf{0}_{2\times 2} & *
\end{bmatrix} \tag{6}$$

where $*$ denotes $2 \times 2$ full matrices. It now means that 8 symbols have to be decoded first, for a complexity of $O(M^8)$, and then 4 groups of 2 symbols each are decoded, each with a complexity of $O(M^2)$ for a total of $O(M^{10})$.

### *D. Associative versus nonassociative cyclic algebras*

The above code constructions were about finding suitable cyclic extensions. They did not discuss the choice of the element $\gamma$ used in the codewords, apart from a restriction to negative real elements in order to facilitate fast decodability. The element $\gamma$ is typically deciding whether the chosen algebra is division, that is, whether the space-time code is fully diverse. In fact, $\gamma$ will also play a role in the overall performance of the code by influencing its shaping. In what follows, some terminology which is customary in the area of algebraic space-time coding will be used without much explanation, due to space constraints. Now,

- in the associative case, $\gamma$ is restricted to the base field, and for the algebra to be division, the non-norm condition is usually checked (see end of Section 2). The disadvantage is that checking the non-norm condition is actually not easy, and can be quite restrictive in the choices that $\gamma$ can actually take. On the other hand, it is necessary to satisfy the non-vanishing minimum determinant, a condition which is useful to ensure the performance of the code irrespectively of the size of the constellation.
- in the nonassociative case, $\gamma$ is on the contrary taken in the field extension. The advantage is that it is very easy to make sure the algebra is division, but on the negative side, a non-vanishing determinant cannot be achieved. However, for scenarios like the MIDO code design, it could be worth trading the non-vanishing determinant for fast-decodability.

## VI. Conclusion

We considered the problem of designing space-time codes for the asymmetric channel with 4 transmit and 2 receive antennas. We presented a few constructions all coming from cyclic algebras containing a cyclotomic field extension. We considered both associative and nonassociative cyclic algebras of dimension 16, and discussed the pros and cons of both types of algebras. All the codes presented enjoy the property of fast-decodability.

Obvious future work involves continuing the optimization of these codes and providing simulations to evaluate the actual code performance. In fact, it would be valuable to start with having a lower bound on the fast-decodability of lattice codes, to know what can be best achieved. It would also be interesting to address the question of designing space-time codes from nonassociative crossed product division algebras, which means that such algebras should first be defined/found somehow. Getting division algebras from associative crossed product algebras is already challenging. It would be relevant in the context of space-time coding to have an easier condition to test whether the algebra is division. This is particularly the case for fast-decodable codes, where having $\mathbb{Q}(i)$ as a subfield simplifies the design.

## Acknowledgment

The research of F. Oggier for this work is supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

## References

[1] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. on Information Theory*, vol. 49, no. 10, pp. 2596-2616, Oct. 2003.

[2] E. Biglieri, Y. Hong and E. Viterbo, "On fast-decodable space-time block codes", *IEEE Trans. Inform. Theory*, vol. 55, no. 2, Feb 2009.

[3] R. Vehkalahti, C. Hollanti, F. Oggier, "Fast-Decodable Asymmetric Space-Time Codes from Division Algebras", *IEEE Transactions on Information Theory*, vol. 58, no. 4, April 2012.

[4] L. Luzzi, F. Oggier, "A family of fast-decodable MIDO codes from crossed-product algebras over $\mathbb{Q}$", *ISIT 2011*.

[5] N. Markin, F. Oggier, " Iterated MIDO Space-Time Code Constructions," *Allerton Conference*, 2011.

[6] L. P. Natarajan, B. S. Rajan, "Fast group-decodable STBCs via codes over GF(4)," *Proc. IEEE Int. Symp. Inform. Theory*, Austin, TX, June 2010

[7] Lakshmi Prasad Natarajan and B. Sundar Rajan, "Fast-Group-Decodable STBCs via codes over GF(4): Further Results," *Proceedings of IEEE ICC 2011, (ICC'11)*, Kyoto, Japan, June 2011.

[8] G. R. Jithamitra, B. Sundar Rajan, "Minimizing the Complexity of Fast Sphere Decoding of STBCs," submitted, http://arxiv.org/abs/1004.2844

[9] S. Pumplün and T. Unger, "Space-time block codes from nonassociative division algebras", *Advances in Mathematics of Communications*, vol. 5, no. 3, pp. 449-471, 2011.

[10] A. Steele, "Nonassociative Cyclic Algebras", preprint, available at http://molle.fernuni-hagen.de/∼loos/jordan/archive/nonassoc_cyclic/index.html.

[11] R.D. Schafer, "An introduction to nonassociative algebras", Dover Publ., Inc., New York, 1995.

[12] Bott, R., Milnor, J., *On the parallelizability of the spheres*. Bull. Amer. Math. Soc. 64 (1958), 87 – 89.