TENSOR PRODUCTS OF CENTRAL SIMPLE ALGEBRAS AND FAST-DECODABLE SPACE-TIME BLOCK CODES

S. PUMPLÜN

Abstract. We use the representation matrices of the left multiplication in the tensor products of two cyclic (associative or nonassociative) algebras, or subsets of them, to obtain asymmetric space-time block codes, building asymmetric full rate multiple input double output (MIDO) codes which are fully diverse. Some of these codes appear in the iterated code constructions of multiple input double output (MIDO) codes by Markin and Oggier [1]. With the right choice of algebras they are full rate and fast-decodable. We also demonstrate how to obtain fully diverse, rate-2 (transmitting two complex symbols per channel use) codes presented with non-vanishing determinant (NVD).

1. Introduction

Central simple division algebras over number fields have been successfully used in the past to systematically design full rate, fully diverse space-time block codes (STBCs) for an arbitrary number of antennas. They are generally used for a symmetric transmission, where the number of transmit antennas equals the number of receive antennas. However, as soon as they are used in scenarios with less receive than transmit antennas, their decoding complexity is very high.

Space-time block codes used in settings where the number of receive antennas is less than the number of transmit antennas are called asymmetric space-time block codes. Among these, multiple-input double output (MIDO) codes stand out, where there are n antennas transmitting and 2 antennas receiving the data (a so-called $n \times 2$ system). In particular, the case of 4 transmit and 2 receive antennas has potential applications to digital video broadcasting used for example for portable TV devices, or for transmitting data to mobile phones.

The goal is to construct space-time codes which are fast-decodable in the sense of [8], [9], [10], also when there are less receive than transmit antennas, which support higher rates and have the potential to be systematically built for given numbers of transmit/receive antennas.

Fast-decodable codes are treated by Biglieri, Hong and Viterbo [3], Vehkalahti, Hollanti and Oggier [4], [5], Luzzi and Oggier [6], Markin and Oggier [7], Natarajan and Rajan [9], [10] and Steele, Oggier et al. [11], to name just a few.

In [1], Markin and Oggier propose a general iterated code construction to build $2n \times 2n$ asymmetric space-time block codes out of $n \times n$ algebraic space-time block codes (i.e. out of a family $\mathcal{D}$ of $n \times n$ complex matrices) coming from a cyclic division algebra D of degree n over a number field F, and investigate when these new codes are fully diverse and when they

Date: 1.7.2013.

inherit fast-decodability from the code $\mathcal{D}$. This way they design, in particular, iterated space-time codes for the asymmetric channel with 4 transmit and 2 receive antennas starting with the Golden and the Silver code. The case of 6 transmit and 3 receive antennas is considered as well.

Independently, a different approach is presented by Srinath and Rajan in [2], who build fully diverse, rate-2 STBCs which are full-rate for MIDO systems and are fast ML-decodable, have large coding gain and non-vanishing determinant (NVD). Their approach generalizes Vehkalahti, Hollanti, Oggier [5] which treat the case of 4 transmit and 2 receive antennas, as well as the iterative method from [1].

Markin and Oggier's iterated construction [1] starts with a cyclic division algebra D over a number field F of degree n and a $\mathbb{Q}$-automorphism τ of K, where K is a maximal subfield of the F-algebra D. It employs a map

$$\alpha_\theta : \mathrm{Mat}_n(K) \times \mathrm{Mat}_n(K) \to \mathrm{Mat}_{2n}(K),$$

$$\alpha_\theta : (X, Y) \to \begin{bmatrix} X & \Theta\tau(Y) \\ Y & \tau(X) \end{bmatrix}, \tag{1}$$

with a matrix $\Theta \in \mathcal{D}$, where $\mathcal{D} = \lambda(D) \subset \mathrm{Mat}_n(K)$ is the well-known canonical embedding of elements of the algebra D into the n by n matrices via left regular representation and $\Theta = \lambda(\theta)$ for $\theta \in D$. Under certain conditions on τ and θ, the matrices in $\mathcal{A}$ are invertible, thus making up a fully diverse space-time block code.

With the right choice of $\tau \in \mathrm{Gal}(K/F)$ and $\theta \in \mathrm{Fix}(\tau) \cap F$, the matrices in $\mathcal{A} = \alpha_\theta(\mathcal{D}, \mathcal{D})$ form an associative $\mathbb{Q}$-algebra of finite dimension $2n^2[F : \mathbb{Q}]$.

1.1. **Contribution and organization of paper.** Although it is well-known that over number fields all central simple algebras are cyclic, it is well-known that the representation of an algebra plays an important role for code constructions, since two different representations of the same algebra may give codes which perform vastly differently.

In order to find a systematic way to build asymmetric STBCs which are fast-decodable, it seems therefore only natural to look for a way to use already known fast-decodable codes to obtain new fast-decodable codes but also to try to imitate already working methods used in systematic code design before.

In this paper, we compute the tensor products of two (associative or nonassociative) cyclic algebras and the representation matrices of the left multiplication in the resulting tensor product, after explaining some basic design criteria for space-time block codes in Section 2, introducing the nonassociative cyclic algebras we use in Section 3 and recalling the iterated construction in Section 4. In particular, we give a condition for the resulting code to be fully diverse, for any choice of invertible $\theta \in D$.

The representation of the tensor product of an associative cyclic division algebra and a quaternion algebra plays a role in the the iteration process presented in [1] and is treated in Sections 4 to 9: The representation matrix of the tensor product algebra A either already has the form $\alpha_\theta(\mathcal{D}, \mathcal{D})$, or obtains it after restricting the entries x_i of its matrices to a suitable subfield. Surprisingly, in the latter scenario, the matrices in $\alpha_\theta(\mathcal{D}, \mathcal{D})$, belong to a subset of

matrices in the matrix representation of a tensor product algebra A, which by construction has zero divisors. They hence arise from a division subalgebra inside A.

This implies that the methods to check for fast-decodabiliy etc. developed in [1] all can be applied to a certain set of codes obtained from tensor products and discussed in Sections 8 and 9. It also means that often it is easy to see that the determinant of any matrix in the resulting codebook must lie in a certain field and therefore if a code has the non-vanishing determinant property (NVD).

Our scheme can be applied to a wide range of MIMO configurations. In particular, we investigate the tensor product of a quaternion division algebra and a (perhaps nonassociative) quaternion algebra, which are either defined over the same field and share a maximal subfield, or where the quaternion algebra is defined over a subfield of F and actually splits over F. These two scenarios are the ones treated in the literature on iterative code constructions. The matrix representation of left multiplication in the resulting (perhaps nonassociative) algebra has its matrix entries in a unital commutative subring, but with the entries restricted to the proper subfield, equals codes obtained by the iterative constructions given in [1].

We then proceed and compare our codes with those in [1]. It turns out that they make up one family of full rate, iterated codes for $2n$ transmit and n receive antennas, where $\tau^2 = id$. By our construction, either $\theta \in F$, or $n = 2$ and θ lies in a quadratic field extension K_1 of F (which happens when we employ a nonassociative quaternion division algebra in the tensor product). In particular, we obtain fully diverse asymmetric codes for 6 transmit and 3 receive antennas, a case still rarely treated in the literature. Employing the tensor product of a cyclic division algebra of degree 3 over $\mathbb{Q}(\sqrt{-7})$ and the quaternion algebra used to build the Silver code, we obtain an example of a full rate STBC for 6 transmit and 3 receive antennas in Example 15 which is fully diverse and has non-vanishing determinant (NVD). Employing the Silver code, we obtain an example of a rate-2 STBC for 6 transmit antennas in Example 20 which is fully diverse and has non-vanishing determinant.

We give a general construction how to design full rate asymmetric space-time codes for mn transmit and m receive multiple input-multiple output (MIMO) channels in Section 10. This construction employs the tensor product of two cyclic (associative or nonassociative) algebras A and C of degree n, resp. m, over a number field F and its matrix representation.

Tensoring a quaternion division algebra over F of degree n with a cyclic division algebra over F also yields examples of fully diverse space-time block codes (STBCs) which are rate 2 for a $2n \times 2$ system of antennas and look similar in structure to the ones constructed in [2], but are not treated there.

In the last section, we look at the tensor product of a cyclic division algebra of degree n and a nonassociative quaternion algebra. The representation of this nonassociative algebra is not closed under multiplication and thus not an algebra itself, however when the tensor product is division, then the matrix representation is a fully diverse STBC which fits nicely into the iterated codes constructed in [1].

We point out that due to the construction of our codes, the codes obtained as representations of tensor products of cyclic algebras will automatically have the NVD property even

for infinite constellations, if F is $\mathbb{Q}$ or quadratic imaginary and the cyclic division algebras $(K_i/F, \sigma_i, \gamma_i)$, $i = 1, 2$, chosen in the tensor product, have $\gamma_i, \theta_i \in \mathcal{O}_F$, cf. [15, Cor. 17.8].

To keep the paper within a reasonable length we focus on the algebraic aspect of the different tensor product constructions possible and used in the literature, and leave the optimization and actual code design to the experts.

2. Design criteria for space-time block codes

A space-time block code (STBC) for an n_t transmit antenna MIMO system is a set of complex $n_t \times T$ matrices, called codebook, that satisfies a number of properties which determine how well the code performs.

Most of the existing codes are built from cyclic division algebras over number fields F, in particular over $F = \mathbb{Q}(i)$ or $F = \mathbb{Q}(\omega)$ with $\omega = e^{2\pi i/3}$ a third root of unity, since these fields are used for the transmission of QAM or HEX constellations, respectively.

2.1. **STBC design criteria.** If a STBC has a rate of $min(n_t, n_r)$ complex symbols per channel use (with n_r the number of receive antennas) it is called *full-rate*.

One goal is to find *fully diverse* codebooks $\mathcal{A}$, where the difference of any two code words has full rank, i.e. with $\det(X - X') \neq 0$ for all matrices $X \neq X'$, $X, X' \in \mathcal{A}$.

If the minimum determinant of the code, defined as

$$\delta(\mathcal{A}) = \inf_{X' \neq X'' \in \mathcal{A}} |\det(X' - X'')|^2,$$

is bounded below by a constant, even if the codebook $\mathcal{A}$ is infinite, the code $\mathcal{A}$ has *non-vanishing determinant* (NVD). Since our codebooks $\mathcal{A}$ will be based on the representation matrix of a tensor product algebra, they are linear and thus their minimum determinant is given by

$$\delta(\mathcal{A}) = \inf_{0 \neq X \in \mathcal{A}} |\det(X)|^2.$$

If $\mathcal{A}$ is fully diverse, $\delta(\mathcal{A})$ defines the *coding gain* $\delta(\mathcal{A})^{\frac{1}{n_t}}$.

If A is a central simple division algebra over a number field F with matrix representation $\mathcal{A}$, it is well-known that

$$\delta(\mathcal{A}) \in F^\times \cap \mathbb{R}^+$$

(since A is a division algebra, $\delta(\mathcal{A}) \neq 0$). If the code $\mathcal{A}$ is finite, i.e. if the information symbols s_i belong to a finite constellation in F, then $\delta(\mathcal{A})$ is bounded below by a constant.

For associative division algebras over a number field F with maximal subfield K, infinite codes that satisfy the NVD property can often be obtained by restricting the entries in the codebook to the ring of integers $\mathcal{O}_K$. If $F = \mathbb{Q}$ or F is quadratic imaginary, then the resulting code will still be infinite, and its minimum determinant is guaranteed to be bounded away from zero, cf. [15, Cor. 17.8].

It follows that fully diverse codes based on division algebras A over a field F which are tensor products of associative cyclic algebras over F, as we will study in the following, satisfy the NVD property if $F = \mathbb{Q}$ or if F is a quadratic imaginary number field and we restrict matrix entries as above. For instance, assume we want to encode QAM symbols. These can

be seen as elements in $\mathbb{Z}[i] \subset \mathbb{Q}(i)$. Hence we use the field $F = \mathbb{Q}(i)$ which is quadratic imaginary and whose ring of integers $\mathcal{O}_F = \mathbb{Z}[i]$ is a unique factorization domain.

3. Linear codes obtained from associative or nonassociative cyclic algebras

Let F be a field and let A be a finite-dimensional F-vector space. We call A an *algebra* over F if there exists an F-bilinear map $A \times A \to A$, $(x, y) \mapsto x \cdot y$ (denoted simply by juxtaposition xy), called *multiplication*, on A. This definition does not imply that 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, denoted by 1, such that $1x = x1 = x$ for all $x \in A$. We will only consider unital nonassociative algebras.

A nonassociative algebra $A \neq 0$ 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. A is a division algebra if and only if A has no zero divisors [Sch, pp. 15, 16].

For an F-algebra A, associativity is measured by the *associator* $[x, y, z] = (xy)z - x(yz)$. The *nucleus* of A is given by $\mathrm{Nuc}(A) = \{x \in A \,|\, [x, A, A] = [A, x, A] = [A, A, x] = 0\}$. The nucleus is an associative subalgebra of A containing $F1$ and $x(yz) = (xy)z$ whenever one of the elements x, y, z is in $\mathrm{Nuc}(A)$. The *center* of A is defined as $\mathrm{C}(A) = \{x \in A \,|\, x \in \mathrm{Nuc}(A) \text{ and } xy = yx \text{ for all } y \in A\}$.

3.1. **Representation over a maximal subfield.** For coding purposes, an associative division algebra A is often considered as a vector space over some subfield K of the algebra A. Usually K is maximal with respect to inclusion. Given a nonassociative F-algebra A with a maximal subfield K, this is not always possible.

Let K be a subfield of the F-algebra A. Assume K is contained in the nucleus of A, then A is a right K-vector space, since

$$x(cd) = (xc)d \text{ for all } x \in A, c, d \in K.$$

Moreover, then left multiplication λ_a is a linear endomorphism of the right K-vector space A, i.e. $(\alpha a)x = \alpha(ax)$ for all $\alpha \in K$, $a, x \in A$,

$$\lambda_{\alpha a}(x) = (\alpha a)x = \alpha(ax) = \alpha\lambda_a(x)$$

for all $a, x \in A$, $\alpha \in K$ and $\lambda_a \in \mathrm{End}_K(A)$, so $\lambda : A \hookrightarrow \mathrm{End}_K(A), a \mapsto \lambda_a$.

Thus, let K be a subfield of A, maximal with respect to inclusion and assume that K lies in the nucleus of A. Consider A as a right K-vector space. After a choice of K-basis for A, we can embed $\mathrm{End}_K(A)$ into the vector space $\mathrm{Mat}_r(K)$ where $r = \dim_K(A)$. In this way we get an embedding

$$\lambda : A \hookrightarrow \mathrm{Mat}_r(K)$$

of vector spaces. $\mathcal{A} = \lambda(A)$ constitutes a linear codebook. To avoid confusion we will use upper case letters to denote the representation of elements of an algebra A in $\lambda(A)$, i.e. $\lambda(x) = X$. Codebooks obtained from an algebra A, C, $D, \ldots$ respectively, will be denoted by $\mathcal{A} = \lambda(A)$, $\mathcal{C} = \lambda(C)$, $\mathcal{D} = \lambda(D)$.

In the following, we always assume that F is a field of characteristic not 2.

3.2. **Nonassociative quaternion division algebras.** Nonassociative quaternion algebras were studied for instance in [16], [13] or [17]. Let K be a quadratic étale algebra over F of dimension 2 (i.e., a quadratic field extension of F or the algebra $F \times F$), with nontrivial Galois automorphism σ and let $b \in K \setminus F$. The F-vector space $K \oplus K$ becomes a unital F-algebra with unit element $(1,0)$, called a *nonassociative quaternion algebra*, via the multiplication

$$(u,v)(u',v') = (uu' + bv'\sigma(v), \sigma(u)v' + u'v)$$

for $u, u', v, v' \in K$. We denote the algebra by $\mathrm{Cay}(K,b)$.

Remark 1. The multiplication is thus defined just as for quaternion algebras with the exception that we require the scalar b to lie outside of F: Suppose $b \in F^\times$. If $K = F(\sqrt{a})$, then $\mathrm{Cay}(K,b) = (a,b)_F$, if $K = F \times F$, then $\mathrm{Cay}(K,b) \cong \mathrm{Mat}_2(F)$.

The multiplication of $\mathrm{Cay}(K,b)$ is not associative and not even third power-associative, meaning that in general for an element $x \in \mathrm{Cay}(K,b)$, $(x^2)x \neq x(x^2)$. The nonassociative quaternion algebra $\mathrm{Cay}(K,b)$ has nucleus K and is a division algebra over F if and only if K is a field extension. Products involving a factor from K are still associative.

Let $K = F(\sqrt{a}) = F(i)$ be a quadratic field extension and let $b \in K \setminus F$. Let $A = \mathrm{Cay}(K,b)$ be a nonassociative quaternion division algebra. Put

$$j = (0,1) \in \mathrm{Cay}(K,b).$$

Then $\mathrm{Cay}(K,b)$ has F-basis $\{1,i,j,ij\}$ such that $i^2 = a$, $j^2 = b$ and $xj = j\sigma(x)$ for all $x \in K$ (so in particular $ij = -ji$), which is called the *standard basis* of $\mathrm{Cay}(K,b)$.

3.3. **Codes from nonassociative quaternion division algebras.** Write

$$\mathrm{Cay}(F(\sqrt{c}),d) = F(\sqrt{c}) \oplus jF(\sqrt{c}), \quad j^2 = d \in F(\sqrt{c}),$$

where $F(\sqrt{c})$ is a quadratic field extension with Galois group $\mathrm{Gal}(F(\sqrt{c})/F) = \langle\sigma\rangle$. Since $\mathrm{Cay}(F(\sqrt{c}),d)$ has nucleus $F(\sqrt{c})$, we can embed $\mathrm{Cay}(F(\sqrt{c}),d)$ into $\mathrm{Mat}_2(F(\sqrt{c}))$: For $x \in \mathrm{Cay}(F(\sqrt{c}),d)$, the left multiplication $\lambda_x : Q \to Q$, $a \mapsto xa$, is a K-linear endomorphism of the right K-vector space $\mathrm{Cay}(F(\sqrt{c}),d)$. Therefore $\lambda_x \in \mathrm{End}_K(\mathrm{Cay}(F(\sqrt{c}),d))$ and we get an injective K-linear map

$$\lambda : \mathrm{Cay}(F(\sqrt{c}),d) \hookrightarrow \mathrm{End}_K(\mathrm{Cay}(F(\sqrt{c}),d)), x \mapsto \lambda_x.$$

The matrix representation of an element $x = x_0 + jx_1 \in \mathrm{Cay}(F(\sqrt{c}),d))$ under λ is given by

$$\begin{bmatrix} x_0 & d\tau(x_1) \\ x_1 & \tau(x_0) \end{bmatrix}. \tag{2}$$

$\mathrm{Cay}(F(\sqrt{c}),d)$ is division and the codebook is fully diverse ([13], Lemma 7.2).

3.4. **Associative and nonassociative cyclic algebras.** Let K/F be a cyclic Galois extension of degree n, with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$.

Let $\gamma \in F$ be a nonzero element. An (associative) cyclic algebra $D = (K/F, \sigma, \gamma)$ of degree n over F is an n-dimensional (right) K-vector space

$$D = K \oplus Ke \oplus Ke^2 \oplus \cdots \oplus Ke^{n-1},$$

with multiplication given by the relations

$$e^n = \gamma,\ el = \sigma(l)e, \tag{3}$$

for all $l \in K$.

For any $\gamma \in K \backslash F$, a nonassociative algebra denoted $(K/F, \sigma, \gamma)$ can be formed as follows. Let $A = (K/F, \sigma, \gamma)$ be the n-dimensional K-vector space with K-basis given by $\{1, e, e^2, \ldots, e^{n-1}\}$, such that

$$A = K \oplus Ke \oplus Ke^2 \oplus \cdots \oplus Ke^{n-1}.$$

Define a multiplication on A via the following rules for all $l, m \in K, 0 \leq i, j, < n$, which then are extended linearly to all elements of A:

$$(le^i)(me^j) = \begin{cases} l\sigma^i(m)e^{i+j} & \text{if } i+j < n \\ l\sigma^i(m)ae^{(i+j)-n} & \text{if } i+j \geq n \end{cases}$$

Note that the nonassociative cyclic algebra $(K/F, \sigma, \gamma)$ ($\gamma \in K \setminus F$) is built similar to the associative cyclic algebra $(K/F, \sigma, \gamma)$, where $\gamma \in F^\times$ (3): we again obtain that

$$el = \sigma(l)e \text{ and } e^ie^j = \gamma$$

for all integers i, j such that $i + j = n$, so that the expression e^n is well-defined and

$$e^n = \gamma.$$

However, $(K/F, \sigma, \gamma)$ is not $(n+1)$th power associative since $(e^{n-1}e)e = ae$ and $e(e^{n-1}e) = ea = \sigma(a)e$ which are not equal since $\gamma \in K \setminus F$.

The nucleus of the nonassociative cyclic algebra $(K/F, \sigma, \gamma)$ is K and its center is F. These algebras are unital nonassociative division algebras and treated in [19]. We call $(K/F, \sigma, \gamma)$ with $\gamma \in K \setminus F$ a *nonassociative cyclic algebra of degree* n.

It should be noted that the 'degree n' in the name of these algebras refers only to the field extension used to construct the algebra. They are not of degree n themselves as in the associative case.

3.5. **Codes from associative or nonassociative cyclic algebras.** Let K/F be a cyclic field extension of degree n. 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 $n \times n$ 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 because the subfield K of $(K/F, \sigma, \gamma)$ is such that $K = \mathrm{Nuc}(A)$.

Therefore in both the associative and nonassociative case, A is as a right K-vector space of dimension n and, 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 $\mathrm{Mat}_n(K)$. This way we get an embedding

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

of vector spaces such that $X \pm Y \in \lambda(A)$ for all $X, Y \in \lambda(A)$. Thus the difference of two distinct elements of $\mathcal{A}$ will also lie in $\lambda(A)$, and $\mathcal{C}$ is a linear codebook.

The left multiplication of elements of $A = (K/F, \sigma, \gamma)$ (for both the associative case where $\gamma \in F^\times$ and the nonassociative one where $\gamma \in K \setminus F$) with $y = y_0 + y_1 e + \cdots + y_{n-1}e^{n-1} \in D$ induces a representation $\lambda : A \to \mathrm{Mat}_n(K)$ which maps elements of A to matrices of the form

$$\begin{bmatrix} y_0 & \gamma\sigma(y_{n-1}) & \gamma\sigma^2(y_{n-2}) & \dots & \gamma\sigma^{n-1}(y_1) \\ y_1 & \sigma(y_0) & \gamma\sigma^2(y_{n-1}) & \dots & \gamma\sigma^{n-1}(y_2) \\ \vdots & & \vdots & & \vdots \\ y_{n-2} & \sigma(y_{n-3}) & \sigma^2(y_{n-4}) & \dots & \gamma\sigma^{n-1}(y_{n-1}) \\ y_{n-1} & \sigma(y_{n-2}) & \sigma^2(y_{n-3}) & \dots & \sigma^{n-1}(y_0) \end{bmatrix} \tag{4}$$

where $y_0, \dots, y_{n-1} \in K$. In the following, we often identify elements $x \in A$ with their standard matrix representation $X = \lambda(x) \in \mathcal{A}$ and use upper case letters for them.

We note that codewords obtained from a nonassociative cyclic algebra $(K/F, \sigma, \gamma)$ look identical to those obtained from the associative cyclic algebra $(K/F, \sigma, \gamma)$, apart from the choice of the element γ, which for them lies in $K \setminus F$.

Remark 2. (i) If $\gamma \in F^\times$, there is a canonical algebra isomorphism $h : D \otimes_F K \to \mathrm{Mat}_n(K)$. The matrix corresponding to $h(x \otimes 1)$ turns out to be the same as (4).
(ii) If $\gamma \in K \setminus F$, 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.

A codebook formed by such matrices is fully diverse if and only if the algebra $(K/F, \sigma, \gamma)$ is division [19]. This is the case for any choice of γ in K but not in F, such that $1, \gamma, \dots, \gamma^{n-1}$ are linearly independent over F [19], and for all $\gamma \in F^\times$ with $\gamma^s \notin N_{K/F}(K^\times)$ for all s, $1 \leq s \leq n-1$, which are prime divisors of n.

Example 3. (i) Nonassociative quaternion division algebras are nonassociative cyclic algebras of degree 2.
(ii) Let K/F be a cyclic Galois extension of degree 4 with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. a nonzero element $\gamma \in K \setminus F$. The nonassociative cyclic algebra $A = (K/F, \sigma, \gamma)$ is the 4-dimensional K-vector space with K-basis given by $\{1, e, e^2, e^3\}$, such that

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

and multiplication on A given by

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

for all $l, m \in K$. The 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

$$\begin{bmatrix}
y_0 & \sigma(y_3)\gamma & \sigma^2(y_2)\gamma & \sigma^3(y_1)\gamma \\
y_1 & \sigma(y_0) & \sigma^2(y_3)\gamma & \sigma^3(y_2)\gamma \\
y_2 & \sigma(y_1) & \sigma^2(y_0) & \sigma^3(y_3)\gamma \\
y_3 & \sigma(y_2) & \sigma^2(y_1) & \sigma^3(y_0)
\end{bmatrix}. \tag{5}$$

The codebook $\mathcal{A}$ formed by such matrices is fully diverse for any choice of $\gamma \in K \setminus F$, such that $1, \gamma, \gamma^2, \gamma^3$ are linearly independent over F [11].

4. The iterative construction

Let F be a number field. Let K/F be a cyclic Galois extension of degree n with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Let $\gamma \in F$ be a nonzero element and $D = (K/F, \sigma, \gamma)$ a cyclic associative division algebra of degree n over F. $(K/F, \sigma, \gamma)$ is an n-dimensional right K-vector space with basis $\{1, e, e^2, \ldots, e^{n-1}\}$, where $e^{n-1} = \gamma$. If D is division, the codebook $\mathcal{D}$ in (4) is fully diverse. Let $\theta \in D$. Write $\theta = \theta_0 + e\theta_1 + \cdots + e^{n-1}\theta_{n-1}$ ($\theta_i \in K$) and identify θ with its matrix representation $\Theta = \lambda(\theta) \in \mathcal{D} = \lambda(D)$ which is given by a matrix as in (4) with entries θ_i. Let τ be a $\mathbb{Q}$-automorphism of K. Suppose that

$$\tau(\gamma) = \gamma, \quad \tau\sigma = \sigma\tau. \tag{6}$$

In the iterative construction of [1], the map

$$\alpha_\theta : \mathrm{Mat}_n(K) \times \mathrm{Mat}_n(K) \to \mathrm{Mat}_{2n}(K),$$

$$\alpha_\theta : (X, Y) \to \begin{bmatrix} X & \Theta\tau(Y) \\ Y & \tau(X) \end{bmatrix} \tag{7}$$

where in the top right block we mean matrix multiplication, is used to build a new code out of $\mathcal{D}$. α_θ embeds $\mathcal{D} \times \mathcal{D}$ into $\mathrm{Mat}_{2n}(K)$.

Lemma 4. *(cf. [1], Lemma 6, 7, Corollary 1, Remark 9) Let $D = (K/F, \sigma, \gamma)$ be a cyclic algebra over a number field F, $\theta \in F$, $\mathcal{D} = \lambda(D)$ and $\mathcal{A} = \alpha_\theta(\mathcal{D}, \mathcal{D})$. Let $\tau \in \mathrm{Gal}(K/F)$ such that*

$$\tau(\gamma) = \gamma \text{ and } \tau\sigma = \sigma\tau. \tag{6}$$

(i) If $\tau^2 = id$ then $\mathcal{A}$ is a $\mathbb{Q}$-algebra of dimension $2n^2[F : \mathbb{Q}]$.
(ii) Let D be a division algebra. Then every matrix in $\mathcal{A}$ has determinant in F and is

invertible iff $\theta \neq z\tau(z)$ for all $z \in D$.
If, additionally, $\tau^2 = id$ then $\det(\alpha_\theta(x,y)) \in \mathrm{Fix}(\tau)$ for all $x, y \in \mathcal{D}$.
(iii) Let D be a division algebra and $\tau^2 = id$. If $\theta \in \mathrm{Fix}(\tau) \cap F$ then $\mathcal{A}$ is an algebra and division if and only if $\theta \neq z\tau(z)$ for all $z \in D$.
In particular, if $\tau \in \mathrm{Gal}(K/F) = \langle\sigma\rangle$ then $\mathcal{A} \cong (K'/F', \sigma, \gamma)$ for suitable K', F'.

We generalize Lemma 4 (ii) as follows:

Theorem 5. *Let F be a field of characteristic not two and K/F be a cyclic Galois extension of degree n with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Let $\tau : K \to K$ be an automorphism of K. Let $(K/F, \sigma, \gamma)$ be a cyclic division algebra over F and $\theta \in D^\times$. Suppose*

$$\tau(\gamma) = \gamma \text{ and } \tau\sigma = \sigma\tau. \tag{6}$$

For $x = x_0 + ex_1 + \cdots + e^{n-1}x_{n-1}$ $(x_i \in K)$ define

$$\widetilde{\tau}(x) = \tau(x_0) + e\tau(x_1) + \cdots + e^{n-1}\tau(x_{n-1}).$$

The codebook defined by $\alpha_\theta(\mathcal{D}, \mathcal{D})$,

$$\alpha_\theta : (X, Y) \to \begin{bmatrix} X & \Theta\tau(Y) \\ Y & \tau(X) \end{bmatrix},$$

is fully diverse, if and only if $\theta \neq z\widetilde{\tau}(z)$ for all $z \in D$. The determinant of a matrix in $\alpha_\theta(\mathcal{D}, \mathcal{D})$ is an element of F.

Proof. If $X \in \mathcal{D}$ or $Y \in \mathcal{D}$ is the zero matrix, $\alpha_\theta(X, Y)$ is invertible, so assume $X, Y \in \mathcal{D}$ are both non-zero matrices. Then the determinant of α_θ is given by

$$\det(X)\det(\tau(X) - YX^{-1}\Theta\tau(Y)).$$

Suppose $\det(\alpha_\theta(X, Y)) = 0$, then, since $\det(X)$ is nonzero, we must have $\det(\tau(X) - YX^{-1}\Theta\tau(Y)) = 0$. Since $\tau(\gamma) = \gamma$, we have

$$\lambda(\widetilde{\tau}(x)) = \tau(\lambda(x)).$$

Thus

$$\begin{aligned} \tau(X) - YX^{-1}\Theta\tau(Y) &= \tau(\lambda(x)) - \lambda(y)\lambda(x^{-1})\lambda(\theta)\tau(\lambda(y)) \\ &= \lambda(\widetilde{\tau}(x)) - \lambda(y)\lambda(x^{-1})\lambda(\theta)\lambda(\widetilde{\tau}(y)) \\ &= \lambda(\widetilde{\tau}(x) - yx^{-1}\theta\widetilde{\tau}(y)) \end{aligned}$$

and so

$$\det(\tau(X) - YX^{-1}\Theta\tau(Y)) = \det(\lambda(\widetilde{\tau}(x) - yx^{-1}\theta\widetilde{\tau}(y))) = N_{D/F}(\tau(x) - yx^{-1}\theta\tau(y)).$$

Since D is division, we know $N_{D/F}(z) = 0$ iff $z = 0$ for all $z \in D$, therefore $\tau(x) - yx^{-1}\theta\tau(y) = 0$, i.e. $\tau(x) = yx^{-1}\theta\tau(y)$. Rearranging gives

$$\theta = xy^{-1}\tau(x)\tau(y)^{-1} = z\tau(z),$$

where $z = xy^{-1}$, a contradiction of our hypothesis. Moreover, we conclude that the determinant of $\alpha_\theta(X, Y)$ can be written as

$$N_{D/F}(x)N_{D/F}(\tau(x) - yx^1\theta\tau(y)),$$

and therefore takes values in F.

Conversely, if $\theta = z\widetilde{\tau}(z)$ for some $z \in D$ then $\alpha_\theta(Z, I_n)$ has determinant zero, because $\det(\tau(Z)) = \det(\det(\lambda(\widetilde{\tau}(z) - z^{-1}z\widetilde{\tau}(z))) = 0$. □

We point out that the condition that $\theta \neq z\tau(z)$ for all $z \in D$ is equivalent to $\Theta \neq Z\tau(Z)$ for all $Z \in \mathcal{D}$ here, since $\tau(\gamma) = \gamma$.

4.1. **Classical results.** For the sake of the reader, we summarize two classical results on tensor products of central simple associative algebras:

Theorem 6. *([14], Theorem 1.9.8) Let $(K/F, \sigma, \gamma)$ be a cyclic algebra of prime degree r, D a central division algebra over F such that $D_K = D \otimes_F K$ is a division algebra, and let σ be the extension of σ to D_K so that $\sigma|_D = id_D$. Then*

$$(K/F, \sigma, \gamma) \otimes_F D$$

is a division algebra if and only if

$$\sigma^{r-1}(a) \cdots \sigma(a)a \neq \gamma$$

for all $a \in D_K$.

Lemma 7. *([14], Lemma 2.7.6) Let D_1 and D_2 be two finite dimensional division algebras such that D_1 is central and $gcd([D_1 : F], [D_2 : F]) = 1$. Then $D_1 \otimes D_2$ is a division algebra.*

5. The tensor product of a cyclic and a quaternion algebra

In this Section, we consider a case where $\tau \notin \mathrm{Gal}(K/F) = \langle\sigma\rangle$.

5.1. **Matrix representations of the tensor product of a cyclic and a quaternion algebra.** Let $C = (K_0/F, \sigma, \gamma)$ be a cyclic division algebra of degree n over F and $(c, d)_F$ a quaternion division algebra over F. Let $\mathrm{Gal}(K_0/F) = \langle\sigma\rangle$ and $K_1 = F(\sqrt{c})$ with $\mathrm{Gal}(K_1/F) = \langle\tau\rangle$. Define $\mathcal{C} = \lambda(C)$, then the codebook $\mathcal{C}$ is fully diverse. Let $\{1, e, e^2, \ldots, e^{n-1}\}$ be the standard basis of the right K_0-vector space $(K_0/F, \sigma, \gamma)$ and view $(c, d)_F$ as two-dimensional right $F(\sqrt{c})$-vector space with basis $\{1, j_2\}$, i.e. $j_2^2 = d$.

We assume that

$$A = (K_0/F, \sigma, \gamma) \otimes_F (c, d)_F$$

is a division algebra over F. By Lemma 7 this is always true for n odd. Then $K = K_0 \otimes_F F(\sqrt{d}) = K_0(\sqrt{d})$ is a maximal subfield of A (the composite of K_0 and $F(\sqrt{d})$) of degree $[K : F] = 2[K_0 : F]$ with Galois group

$$\mathrm{Gal}(K/F) = \{id, \sigma, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \ldots, \tau\sigma^{n-1}\},$$

where σ and τ denote the canonical extensions of σ and τ to K and

$$\sigma^i\tau = \tau\sigma^i, \quad 1 \leq i \leq n-1.$$

A K-basis for the tensor product algebra A is given by $\{1 \otimes 1, e \otimes 1, \ldots, e^{n-1} \otimes 1, 1 \otimes j_2, e \otimes j_2, e^{n-1} \otimes j_2\}$. A is a right K-vector space of dimension $2n$ which can be identified with

$$K \oplus eK \oplus \cdots \oplus e^{n-1}K \oplus j_2K \oplus ej_2K \oplus \cdots \oplus e^{n-1}j_2K.$$

An element in $\lambda(A) = \mathcal{A}$ has the form

$$\begin{bmatrix} X & d\tau\sigma(Y) \\ Y & \tau\sigma(X) \end{bmatrix} \tag{8}$$

with $X, Y \in \mathcal{C}$. $\mathcal{A}$ is fully diverse since the algebra A is division, and $\det(A) \in F^\times$ for all non-zero $A \in \mathcal{A}$.

Example 8. How to obtain space-time block codes from biquaternion algebras (i.e., here $n = 2$) was addressed already in [12]: Let $(a, b)_F$ and $(c, d)_F$ be division algebras over F. $A = (a, b)_F \otimes_F (c, d)_F$ is a biquaternion division algebra over F, if and only if The quadratic form $\langle a, b, -ab, -c, -d, cd\rangle$ is anisotropic over F (see [12]), if and only if $(a, b)_F$ and $(c, d)_F$ do not contain isomorphic quadratic subfields (see [14], Theorem 2.10.3).

Let $\mathrm{Gal}(F(\sqrt{a})/F) = \langle\sigma\rangle$ and $\mathrm{Gal}(F(\sqrt{c})/F) = \langle\tau\rangle$. Then an element in $\lambda(A) = \mathcal{A}$ has the form

$$\begin{bmatrix} x_0 & b\sigma(x_1) & d\tau(x_2) & db\tau\sigma(x_3) \\ x_1 & \sigma(x_0) & d\tau(x_3) & d\tau\sigma(x_2) \\ x_2 & b\sigma(x_3) & \tau(x_0) & b\tau(x_1) \\ x_3 & \sigma(x_2) & \tau(x_1) & \tau(x_0) \end{bmatrix} \tag{9}$$

with all $x_i \in K = F(\sqrt{c}, \sqrt{a})$, cf. [12], Section 5 and Theorem 5.5., and $\det(X) \in F^\times$ for all non-zero $X \in \mathcal{A}$.

Example 9. For $n = 3$, an element in $\mathcal{A}$ has the form

$$\begin{bmatrix} x_0 & \gamma\sigma(x_2) & \gamma\sigma^2(x_1) & d\tau(x_3) & d\gamma\tau\sigma(x_5) & d\tau\sigma(x_4) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_2) & d\tau(x_4) & d\tau\sigma(x_3) & d\gamma\tau\sigma(x_5) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & d\tau(x_5) & d\tau\sigma(x_4) & d\tau\sigma(x_3) \\ x_3 & \gamma\sigma(x_5) & \gamma\sigma(x_4) & \tau(x_0) & \gamma\tau\sigma(x_2) & \gamma\tau\sigma^2(x_1) \\ x_4 & \sigma(x_3) & \gamma\sigma(x_5) & \tau(x_1) & \tau\sigma(x_0) & \gamma\tau\sigma^2(x_2) \\ x_5 & \sigma(x_4) & \sigma(x_3) & \tau(x_2) & \tau\sigma(x_1) & \tau\sigma^2(x_0) \end{bmatrix} \tag{10}$$

with $x_i \in K = K_0(\sqrt{d})$ and is fully diverse for any choice of division algebras $(K_0/F, \sigma, \gamma)$ of degree 3 and $(c, d)_F$.

5.2. **Connection with iterated codes.** Since $A = (K_0/F, \sigma, \gamma) \otimes_F (c, d)_F$ is a division algebra over F, $K_1 = F(\sqrt{c}) \subset (c, d)_F$ cannot be a splitting field of A and

$$D = (K_0/F, \sigma, \gamma) \otimes_F F(\sqrt{c}) = (K/K_1, \sigma, \gamma)$$

is a division algebra over $K_1 = F(\sqrt{c})$. It contains the maximal subfield $K = K_0(\sqrt{c})$ of degree n with $\mathrm{Gal}(K/K_0) = \langle\sigma\rangle$. We thus have

$$\alpha_d : \mathrm{Mat}_n(K) \times \mathrm{Mat}_n(K) \to \mathrm{Mat}_{2n}(K),$$

$$\alpha_d : (X, Y) \to \begin{bmatrix} X & d\tau(Y) \\ Y & \tau(X) \end{bmatrix}$$

with $d \in F$ and τ an F-automorphism of K satisfying $\tau \notin \mathrm{Gal}(K_0/F)$ by construction, as well as (6). Thus $\mathcal{A} = \alpha_d(\mathcal{D}, \mathcal{D})$. We summarize:

Theorem 10. *(i) Let K_0/F be a cyclic field extension of degree n with $\mathrm{Gal}(K_0/F) = \langle\sigma\rangle$. Let $A = (K_0/F, \sigma, \gamma) \otimes_F (c, d)_F$ be a division algebra over F, $K_1 = F(\sqrt{c})$ with $\mathrm{Gal}(K_1/F) = \langle\tau\rangle$ and define $D = (K_0/F, \sigma, \gamma) \otimes_F K_1$. Extend τ and σ canonically to $K = K_0(\sqrt{c})$. Then the iterated code $\mathcal{A} = \alpha_d(\mathcal{D}, \mathcal{D})$,*

$$\alpha_d : (X, Y) \to \begin{bmatrix} X & d\tau(Y) \\ Y & \tau(X) \end{bmatrix}$$

for all $X, Y \in \mathcal{D}$, is fully diverse and $\det(X) \in F^\times$ for all non-zero $X \in \alpha_d(\mathcal{D}, \mathcal{D})$.
Moreover, $\mathcal{A} = \alpha_d(\mathcal{D}, \mathcal{D})$ is isomorphic to the algebra $(K_0/F, \sigma, \gamma) \otimes_F (c, d)_F$.
(ii) For any cyclic division algebra $(K_0/F, \sigma, \gamma)$ of odd degree and quaternion division algebra $(c, d)_F$, the iterated code $\mathcal{A} = \alpha_d(\mathcal{D}, \mathcal{D})$ in (i) is fully diverse and $\det(X) \in F^\times$ for all non-zero $X \in \alpha_d(\mathcal{D}, \mathcal{D})$.

Note that (ii) is a direct consequence of Lemma 7.

Remark 11. By Lemma 4, (iii), the above code $\mathcal{A} = \alpha_d(\mathcal{D}, \mathcal{D})$ is fully diverse iff $d \neq z\tau(z)$ for all $z \in D$. In the above setup, Theorem 6 implies: Assume that $(c, d)_F$ is division and that $D = (K_0/F, \sigma, \gamma)$ a central division algebra over F such that $D_{K_1} = D \otimes_F K_1$ is a division algebra. Let τ be the extension of τ to D_{K_1} so that $\tau|_D = id_D$. Then

$$(K_0/F, \sigma, \gamma) \otimes_F (c, d)_F$$

is a division algebra if and only if $\tau(a)a \neq d$ for all $a \in D_{K_1}$.

Example 12. Let $A = (a, b)_F \otimes_F (c, d)_F$ be a biquaternion division algebra over F and $\mathcal{A} = \lambda(A)$. By Example 8, $(a, b)_F \otimes_F F(\sqrt{c}) = \mathrm{Cay}(K, b)$ is a division algebra over $K_1 = F(\sqrt{c})$ with maximal quadratic subfield $K = F(\sqrt{c}, \sqrt{a})$ where $\mathrm{Gal}(K/K_1) = \langle\sigma\rangle$. For $D = (a, b)_F \otimes_F F(\sqrt{c})$ over K_1, $\mathcal{D} = \lambda(D)$, we obtain $\mathcal{A} = \alpha_d(\mathcal{D}, \mathcal{D})$ with

$$\alpha_d : \mathrm{Mat}_2(K) \times \mathrm{Mat}_2(K) \to \mathrm{Mat}_4(K),$$

$$\alpha_d : (X, Y) \to \begin{bmatrix} X & d\tau(Y) \\ Y & \tau(X) \end{bmatrix} \tag{11}$$

where τ is an F-automorphism of K of order two satisfying $\tau \notin \mathrm{Gal}(K/K_1) = \langle\sigma\rangle$, as well as the requirements $\tau(b) = b, \quad \tau\sigma = \sigma\tau$ from (6). The algebra $\alpha_d(\mathcal{D}, \mathcal{D})$ is isomorphic to the biquaternion algebra $A = (a, b)_F \otimes_F (c, d)_F$ over F.

Corollary 13. *Let $K = F(\sqrt{a}, \sqrt{c})/F$ be a biquadratic field extension with Galois group $\mathrm{Gal}(K/F) = \{id, \sigma, \tau, \sigma\tau\}$, $K_0 = F(\sqrt{a})$, $K_1 = F(\sqrt{c})$ and $\mathrm{Gal}(K_0/F) = \langle\sigma\rangle$, $\mathrm{Gal}(K_1/F) = \langle\tau\rangle$. Choose $b \in F^\times$, $d \in F^\times$, such that*

$$A = (a, b)_F \otimes_F (c, d)_F$$

is a biquaternion division algebra over F and put $D = (a, b)_{K_1}$, $\mathcal{D} = \lambda(D)$. Then the iterated code $\mathcal{A} = \alpha_d(\mathcal{D}, \mathcal{D})$,

$$\alpha_d : (X, Y) \to \begin{bmatrix} X & d\tau(Y) \\ Y & \tau(X) \end{bmatrix} \tag{12}$$

with $X, Y \in \mathcal{D}$ is fully diverse and $\det(\alpha_d(X, Y)) \in F^\times$ for all $X, Y \in \mathcal{D}$, $(X, Y) \neq (0, 0)$.

Example 14. Let $\omega = e^{2\pi i/3}$ be a third root of unity, ζ_7 a primitive 7th root of unity, $F = \mathbb{Q}(\omega)$ and $K_1 = \mathbb{Q}(\omega, \theta)$ with $\theta = \xi_7 + \xi_7^{-1}$. The division algebra

$$(\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\omega), \sigma, \omega)$$

of degree 3 is used to construct the perfect code for three transmit antennas, with

$$\sigma(\xi_7 + \xi_7^{-1}) = \xi_7^2 + \xi_7^{-2}.$$

For any quaternion division algebra $D = (c, d)_{\mathbb{Q}(\omega)}$, let $A = (K_0/F, \sigma, \gamma) \otimes_F (c, d)_F$ and $\tau : F(\sqrt{c}) \to F(\sqrt{c})$, $\tau(\sqrt{c}) = -\sqrt{c}$, then the code

$$\begin{bmatrix} x_0 & \omega\sigma(x_2) & \omega\sigma^2(x_1) & d\tau(x_3) & d\omega\tau\sigma(x_5) & d\tau\sigma(x_4) \\ x_1 & \sigma(x_0) & \omega\sigma^2(x_2) & d\tau(x_4) & d\tau\sigma(x_3) & d\omega\tau\sigma(x_5) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & d\tau(x_5) & d\tau\sigma(x_4) & d\tau\sigma(x_3) \\ x_3 & \omega\sigma(x_5) & \omega\sigma(x_4) & \tau(x_0) & \omega\tau\sigma(x_2) & \omega\tau\sigma^2(x_1) \\ x_4 & \sigma(x_3) & \omega\sigma(x_5) & \tau(x_1) & \tau\sigma(x_0) & \omega\tau\sigma^2(x_2) \\ x_5 & \sigma(x_4) & \sigma(x_3) & \tau(x_2) & \tau\sigma(x_1) & \tau\sigma^2(x_0) \end{bmatrix} \tag{13}$$

with $x_i \in K = \mathbb{Q}(\omega, \theta, \sqrt{c})$, is fully diverse. For instance, $(c, d)_{\mathbb{Q}(\omega)} = (2 + \sqrt{-3}, d)_{\mathbb{Q}(\omega)}$ is a division algebra over $\mathbb{Q}(\omega)$ for all $d = 3, 5$, or 6 modulo 7, by [12], Example 7.6. For $d = 3$, this yields the fully diverse code

$$\begin{bmatrix} x_0 & \omega\sigma(x_2) & \omega\sigma^2(x_1) & 3\tau(x_3) & 3\omega\tau\sigma(x_5) & 3\tau\sigma(x_4) \\ x_1 & \sigma(x_0) & \omega\sigma^2(x_2) & 3\tau(x_4) & 3\tau\sigma(x_3) & 3\omega\tau\sigma(x_5) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & 3\tau(x_5) & 3\tau\sigma(x_4) & 3\tau\sigma(x_3) \\ x_3 & \omega\sigma(x_5) & \omega\sigma(x_4) & \tau(x_0) & \omega\tau\sigma(x_2) & \omega\tau\sigma^2(x_1) \\ x_4 & \sigma(x_3) & \omega\sigma(x_5) & \tau(x_1) & \tau\sigma(x_0) & \omega\tau\sigma^2(x_2) \\ x_5 & \sigma(x_4) & \sigma(x_3) & \tau(x_2) & \tau\sigma(x_1) & \tau\sigma^2(x_0) \end{bmatrix}. \tag{14}$$

Example 15. The quaternion division algebra $(-1, -1)_{\mathbb{Q}(\sqrt{-7})}$ is used in the construction of the Silver Code. Let ζ_7 be a primitive 7th root of unity and

$$(\mathbb{Q}(\zeta_7)/\mathbb{Q}(\sqrt{-7}), \sigma_2, 3)$$

the cyclic division algebra of degree 3 over $\mathbb{Q}(\sqrt{-7})$ with $\sigma : \zeta_7 \to \zeta_7^2$, see [1], Example 5. Consider the tensor product

$$A = (\mathbb{Q}(\zeta_7)/\mathbb{Q}(\sqrt{-7}), \sigma, 3) \otimes_{\mathbb{Q}(\sqrt{-7})} (-1, -1)_{\mathbb{Q}(\sqrt{-7})}.$$

Here, we have the number fields $F = \mathbb{Q}(\sqrt{-7})$, $K_0 = \mathbb{Q}(\zeta_7)$ and $K_1 = \mathbb{Q}(\sqrt{-7}, i)$ which are linearly independent over F, and $K = K_0 \cdot K_1 = \mathbb{Q}(\zeta_7, \sqrt{-7}, i)$. We have

$$\tau(w_0 + iw_1) = w_0 - iw_1$$

for all $w_0, w_1 \in \mathbb{Q}(\sqrt{-7})$, so that τ is not the complex conjugation.

The matrix representation of the division algebra A is given by

$$\begin{bmatrix} x_0 & 3\sigma(x_2) & 3\sigma^2(x_1) & -\tau(x_3) & -3\tau\sigma(x_5) & -3\tau\sigma(x_4) \\ x_1 & \sigma(x_0) & 3\sigma^2(x_2) & -\tau(x_4) & -\tau\sigma(x_3) & -3\tau\sigma(x_5) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & -\tau(x_5) & -\tau\sigma(x_4) & -\tau\sigma(x_3) \\ x_3 & 3\sigma(x_5) & 3\sigma(x_4) & \tau(x_0) & 3\tau\sigma(x_2) & 3\tau\sigma^2(x_1) \\ x_4 & \sigma(x_3) & 3\sigma(x_5) & \tau(x_1) & \tau\sigma(x_0) & 3\tau\sigma^2(x_2) \\ x_5 & \sigma(x_4) & \sigma(x_3) & \tau(x_2) & \tau\sigma(x_1) & \tau\sigma^2(x_0) \end{bmatrix}. \tag{15}$$

with the $x_i \in K$. Since F is an imaginary number field, the resulting fully diverse code has the non-vanishing property (NVD).

6. Matrix representations of the tensor products of two cyclic algebras

6.1. Let $C_0 = (K_0/F, \sigma, \gamma)$ be a cyclic division algebra of degree n over F and $C_1 = (K_1/F, \tau, \theta)$ be a cyclic division algebra of degree m over F. Define $\mathcal{C}_i = \lambda(C_i)$, $i = 0, 1$, then the codebooks $\mathcal{C}_i$ are fully diverse. Let $\{1, e, e^2, \ldots, e^{n-1}\}$ be the standard basis of the right K_0-vector space C_0 and $\{1, f, f^2, \ldots, f^{n-1}\}$ be the standard basis of the right K_1-vector space C_1. We assume that the tensor product

$$A = (K_0/F, \sigma, \gamma) \otimes_F (K_1/F, \tau, \theta)$$

is a division algebra over F (this is for instance the case if m and n are prime).

$K = K_0 \otimes_F K_1 = K_0 \cdot K_1$ is a maximal subfield of A (the composite of K_0 and K_1 over F) of degree $[K : F] = [K_0 : F] \cdot [K_1 : F]$ with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle \times \langle\tau\rangle$, where σ and τ are canonically extended to K, that is $\sigma|_{K_1} = id$, and $\tau|_{K_0} = id$. Note that

$$\sigma^i\tau^j = \tau^j\sigma^i, \quad 1 \le i \le n-1, 1 \le j \le m-1.$$

A K-basis for the tensor product algebra A is given by $\{1 \otimes 1, e \otimes 1, \ldots, e^{n-1} \otimes 1, 1 \otimes f, e \otimes f, \ldots, e^{n-1} \otimes f^{m-1}\}$. A is a right K-vector space of dimension nm which can be identified with

$$K \oplus eK \oplus \cdots \oplus e^{n-1}K \oplus fK \oplus efK \oplus \cdots \oplus e^{n-1}f^{m-1}K.$$

Now an element in $\lambda(A) = \mathcal{A}$ has the form

$$\begin{bmatrix} Y_0 & \theta\tau(Y_{n-1}) & \theta\tau^2(Y_{n-2}) & \ldots & \theta\tau^{m-1}(Y_1) \\ Y_1 & \tau(Y_0) & \theta\tau^2(Y_{n-1}) & \ldots & \theta\tau^{m-1}(Y_2) \\ \vdots & & \vdots & & \vdots \\ Y_{n-2} & \tau(Y_{n-3}) & \tau^2(Y_{n-4}) & \ldots & \theta\tau^{m-1}(Y_{n-1}) \\ Y_{n-1} & \tau(Y_{n-2}) & \tau^2(Y_{n-3}) & \ldots & \tau^{m-1}(Y_0) \end{bmatrix} \tag{16}$$

with the $Y_i \in \mathcal{C}_0 \subset \mathrm{Mat}_n(K)$. The codebook $\mathcal{A}$ is fully diverse since A is division and $\det(A) \in F^\times$ for all non-zero $A \in \mathcal{A}$. In particular, for $m = 3$, elements in $\mathcal{A}$ have the form

$$\begin{bmatrix} Y_0 & \theta\tau(Y_2) & \theta\tau^2(Y_1) \\ Y_1 & \tau(Y_0) & \theta\tau^2(Y_2) \\ Y_2 & \tau(Y_1) & \tau^2(Y_0) \end{bmatrix} \tag{17}$$

with $Y_i \in \mathcal{C}_0 \subset \mathrm{Mat}_n(K)$.

To check when the tensor product $A = (K_0/F, \sigma, \gamma) \otimes_F (K_1/F, \tau, \theta)$ is a division algebra we use Theorem 6:

Corollary 16. *Let $(K_1/F, \tau, \theta)$ be a cyclic division algebra of prime degree. Suppose that $D = (K_0/F, \sigma, \gamma)$ is a central division algebra over F such that $(K_0/F, \sigma, \gamma)_{K_1} = (K_0/F, \sigma, \gamma) \otimes_F K_1$ is a division algebra. Let τ be the extension of τ to D_{K_1} so that $\tau|_D = id_D$. For all $a \in D_{K_1}$, define*

$$N(a) = \tau^2(a)\tau(a)a.$$

Then A is a division algebra if and only if $N(z) \neq \theta$ for all $z \in D_{K_1}$.

If the base field F we choose for our tensor product division algebras $A = (K_0/F, \sigma, \gamma) \otimes_F (K_1/F, \tau, \theta)$ is $\mathbb{Q}$ or a quadratic imaginary number field, all constructed fully diverse codes with $\gamma, \theta \in \mathcal{O}_F$, $\mathcal{O}_F$ the ring of integers of F, will automatically have NVD. Hence they are DMT-optimal for their respective MIDO system.

6.2. Comparison with the MIDO codes from Srinath and Rajan. Comparing our method with the different one presented in [2], we can use the above fully diverse STBC to construct rate-m STBCs as follows:

Suppose $m \geq 3$ and $A = (K_0/F, \sigma, \gamma) \otimes_F (K_1/F, \tau, \theta)$ is division. Then setting $Y_2 = \cdots = Y_{n-1} = 0$ in (16) we obtain the fully diverse code

$$S_{m\times n} = \{ \begin{bmatrix} Y_0 & 0 & 0 & \dots & \theta\tau^{m-1}(Y_1) \\ Y_1 & \tau(Y_0) & 0 & \dots & 0 \\ 0 & \tau(Y_1) & \tau^2(Y_0) & \dots & 0 \\ 0 & 0 & \tau^2(Y_1) & \tau^3(Y_0) & \dots \\ \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & \tau^{m-1}(Y_0) \end{bmatrix} \} \tag{18}$$

with $\det(X) \in F^\times$ for all non-zero $X \in S_{m\times n}$. For instance,

$$Y_i = \begin{bmatrix} x_{i0} & \gamma\sigma(y_{i1}) \\ y_{i1} & \sigma(x_{i0}) \end{bmatrix} \tag{19}$$

where $x_{ij}, y_{ij} \in K$, for $n = 2$. This is a fully diverse STBC for a $2m \times 2$ system.

Remark 17. (i) Comparing these STBCs with the at first glance similar ones achieved in [2], we point out that the parameters applied in the construction in [2] differ from ours. They also use two number fields, E and L, $E \neq L$, contained in a larger field K, and assume that σ generates the Galois group of K/E and τ the one of K/L, $\gamma \in E \cap L$, $\theta \in L \setminus E$, whereas we assume σ generates the Galois group of $E/E \cap L$ and τ the one of $L/E \cap L$, and our $\gamma, \theta \in (E \cap L)^\times$.
(ii) For code design, we would choose examples with $\mathbb{Q} \subset K$, preferably even $\mathbb{Q}(i) \subset K$ or $\mathbb{Q}(\omega) \subset K$, because the QAM constellation is a finite subset of $\mathbb{Z}[i]$ and the HEX constellation a finite subset of $\mathbb{Z}[\omega]$.

Analogously as in [2], Proposition 1 and 2, we conclude:

Proposition 18. *Let $\mathbb{Q}(i) \subset K$ or $\mathbb{Q}(\omega) \subset K$.*
(i) The rate of the STBC in (18) is two complex symbols per channel use.
(ii) The STBC in (18) has the NVD property if $\gamma, \theta \in \mathcal{O}_F$.

For $m = 3$ and $n = 2$ we thus have the fully diverse rate-2 STBC

$$S_{6\times 2} = \{ \begin{bmatrix} Y_0 & 0 & \theta\tau^2(Y_1) \\ Y_1 & \tau(Y_0) & 0 \\ 0 & \tau(Y_1) & \tau^2(Y_0) \end{bmatrix} \} \tag{20}$$

for a 6×2 system, with matrix entries in K.

Example 19. Let $F = \mathbb{Q}(\omega)$ and $K_1 = \mathbb{Q}(\omega, \theta)$ with ζ_7 a primitive 7th root of unity and with $\theta = \xi_7 + \xi_7^{-1}$. The division algebra $(\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\omega), \tau, \omega)$ is used to construct the perfect code for three transmit antennas, with

$$\tau(\xi_7 + \xi_7^{-1}) = \xi_7^2 + \xi_7^{-2}.$$

For every quaternion division algebra $D = (a, b)_{\mathbb{Q}(\omega)}$, the rate-2 STBC for 6 transmit antennas given by

$$S_{6\times 2} = \{ \begin{bmatrix} Y_0 & 0 & \omega\tau^2(Y_1) \\ Y_1 & \tau(Y_0) & 0 \\ 0 & \tau(Y_1) & \tau^2(Y_0) \end{bmatrix} \} \tag{21}$$

with the Y_i of the form

$$\begin{bmatrix} y_0 & b\sigma(y_1) \\ y_1 & \sigma(y_0) \end{bmatrix} \tag{22}$$

with entries $y_i \in K = \mathbb{Q}(\omega, \theta, \sqrt{a})$, is fully diverse. Here, $\sigma : F(\sqrt{a}) \to F(\sqrt{a})$, $\sigma(\sqrt{a}) = -\sqrt{a}$. For instance, let $(a, b) = (2 + \sqrt{-3}, 3)$ as in Example 14, then

$$S_{6\times 2} = \{ \begin{bmatrix} Y_0 & 0 & \omega\tau^2(Y_1) \\ Y_1 & \tau(Y_0) & 0 \\ 0 & \tau(Y_1) & \tau^2(Y_0) \end{bmatrix} \} \tag{23}$$

with the Y_i of the form

$$\begin{bmatrix} y_0 & 3\sigma(y_1) \\ y_1 & \sigma(y_0) \end{bmatrix} \tag{24}$$

is fully diverse, rate-2 and $\det(X) \in \mathbb{Q}(\omega)^\times$ for all non-zero $X \in S_{6\times 3}$. Since $\omega, 3 \in \mathbb{Z}[\omega]$, it has NVD by Proposition 18. We conclude that the minimum determinant of this (still unnormalized for SNR) code is at least 1, when restricting entries to $\mathbb{Z}[\omega]$. More precisely, let $\theta_1, \theta_2, \theta_3$ be a basis of a principal ideal in $\mathcal{O}_{\mathbb{Q}(\omega,\theta)}$ generated by θ_1 with $\theta_1 = 1 + \omega + \theta$, $\theta_2 = -1 - 2\omega + \omega\theta^2$, $\theta_3 = (-1 - 2\omega) + (1 + \omega)\theta + (1 + \omega)\theta^2$. Imitating [2], IV.C, p. 9, let

$$Y_k = \begin{bmatrix} \sum_{i=1}^3 y_{ki}\theta_i & 3\sigma(\sum_{i=1}^3 y_{k(i+3)}\theta_i) \\ \sum_{i=1}^3 y_{k(i+3)}\theta_i & \sigma(\sum_{i=1}^3 y_{ki}\theta_i) \end{bmatrix},$$

where $s_{kj} \in M$-HEX $\subset \mathbb{Z}[\omega]$, $k = 0, 1$, $i = 1, \dots 6$. The perfect code for three antennas has its entries from a principal ideal in $\mathcal{O}_{\mathbb{Q}(\omega,\theta)}$ generated by θ_1. Analogously as in [2], IV.C, p. 9, we can conclude that the minimum determinant is

$$|N_{\mathbb{Q}(\omega,\theta)/\mathbb{Q}(\omega)}(\theta_1)|^4 = 49.$$

Using an M-HEX constellation, thus the normalized minimum determinant must be

$$\frac{1}{7^4 E^6},$$

taking into account the normalization factor $\frac{1}{\sqrt{28E}}$. However, we cannot easily analyse the ML-decoding complexity of this code, as here σ is not complex conjugation.

Example 20. Let us consider the situation of Example 15, i.e. let $F = \mathbb{Q}(\sqrt{-7})$, $K_0 = \mathbb{Q}(\zeta_7)$, $K_1 = \mathbb{Q}(\sqrt{-7}, i)$ and $K = K_0 \cdot K_1 = \mathbb{Q}(\zeta_7, \sqrt{-7}, i)$. Consider the representation of the tensor product

$$A = (-1,-1)_{\mathbb{Q}(\sqrt{-7})} \otimes_{\mathbb{Q}(\sqrt{-7})} (\mathbb{Q}(\zeta_7)/\mathbb{Q}(\sqrt{-7}), \sigma, 3).$$

Then the STBC for 6 transmit antennas given by

$$S_{6\times 2} = \{ \begin{bmatrix} Y_0 & 0 & 3\sigma^2(Y_1) \\ Y_1 & \sigma(Y_0) & 0 \\ 0 & \sigma(Y_1) & \sigma^2(Y_0) \end{bmatrix} \} \tag{25}$$

with the Y of the form

$$\begin{bmatrix} y_0 & -\tau(y_1) \\ y_1 & \tau(y_0) \end{bmatrix} \tag{26}$$

with entries $y_i \in K = \mathbb{Q}(\zeta_7, \sqrt{-7}, i)$, is fully diverse and $\det(X) \in \mathbb{Q}(\sqrt{-7})^\times$ for all non-zero $X \in S_{6\times 3}$.

The matrix representation of the division algebra A with the choice of $Y_3 = 0$ is therefore given by

$$\begin{bmatrix} x_0 & -\tau(x_1) & 0 & 0 & 3\sigma^2(x_2) & -3\sigma^2(\tau(x_3)) \\ x_1 & \tau(x_0) & 0 & 0 & 3\sigma^2(x_3) & 3\sigma^2(\tau(x_2)) \\ x_2 & -\tau(x_3) & \sigma(x_0) & -\sigma(\tau(x_1)) & 0 & 0 \\ x_3 & \tau(x_2) & \sigma(x_1) & \sigma(\tau(x_0)) & 0 & 0 \\ 0 & 0 & \sigma(x_2) & -\sigma(\tau(x_0)) & \sigma^2(x_0) & -\sigma^2(\tau(x_1)) \\ 0 & 0 & \sigma(x_3) & \sigma(\tau(x_0)) & \sigma^2(x_1) & \sigma^2(\tau(x_0)) \end{bmatrix}. \tag{27}$$

with the $x_i \in K$. Since F is an imaginary number field, the resulting fully diverse code has the non-vanishing property (NVD).

7. Matrix representations of the tensor product of a quaternion division algebra and a nonassociative quaternion division algebra

If we want to study the tensor product A of an associative and a nonassociative algebra, we have to be aware that this changes our situation substantially. The resulting algebra A will be nonassociative. The following can be shown by a straightforward calculation and will be needed in our constructions:

Proposition 21. *Let C and D be two nonassociative algebras over F. Then*

$$\mathrm{Nuc}(C) \otimes_F \mathrm{Nuc}(D) \subset \mathrm{Nuc}(C \otimes_F D).$$

Thus we can consider the tensor product $A = C \otimes_F D$ as a right R-module over any $R \subset \mathrm{Nuc}(C) \otimes_F \mathrm{Nuc}(D)$ and calculate the representation matrix of left multiplication as usual.

7.1. Take the tensor product

$$A = (a,b)_F \otimes_F \mathrm{Cay}(F(\sqrt{c}), d)$$

of a quaternion division algebra $(a,b)_F$ and a nonassociative quaternion algebra $\mathrm{Cay}(F(\sqrt{c}), d)$ with $d \in F(\sqrt{c})$ and $d \notin F$. $\mathrm{Cay}(F(\sqrt{c}), d)$ always is a division algebra over F. Write $\mathrm{Cay}(F(\sqrt{c}), d) = F(\sqrt{c}) \oplus j_2 F(\sqrt{c}), \quad j_2^2 = d \in F(\sqrt{c})$. $K_0 = F(\sqrt{a})$ is a quadratic field extension with Galois group $\mathrm{Gal}(F(\sqrt{a})/F) = \langle \sigma \rangle$. $K_1 = F(\sqrt{c})$ is a quadratic field extension with Galois group $\mathrm{Gal}(F(\sqrt{c})/F) = \langle \tau \rangle$. Let us assume that

$$K_0 \text{ and } K_1 \text{ are not isomorphic.}$$

Then $K = K_0 \otimes_F K_1 = F(\sqrt{a}, \sqrt{c})$. By Section 3.2, the matrix representation of an element $x = x_0 + j x_1 \in \mathrm{Cay}(F(\sqrt{c}), d))$ under λ is given by

$$\begin{bmatrix} x_0 & d\tau(x_1) \\ x_1 & \tau(x_0) \end{bmatrix}.$$

Moreover, K is contained in the nucleus of A since

$$K = F(\sqrt{a}) \otimes_F F(\sqrt{c}) \subset \mathrm{Nuc}((a,b)_F) \otimes_F \mathrm{Nuc}(\mathrm{Cay}(F(\sqrt{c}), d))) \subset \mathrm{Nuc}((a,b)_F \otimes_F \mathrm{Cay}(F(\sqrt{c}), d)).$$

View $(a,b)_F$ as two-dimensional right $F(\sqrt{a})$-vector space with basis $\{1, j_1\}$, $\mathrm{Cay}(F(\sqrt{c}), d))$ as two-dimensional right $F(\sqrt{c})$-vector space with basis $\{1, j_2\}$.

The field $K = F(\sqrt{a}, \sqrt{c})$ is a subfield of A of degree 4 with Galois group $\mathrm{Gal}(K/F) = \{id, \sigma, \tau, \sigma\tau\}$, where σ and τ are determined by $\sigma(\sqrt{a}) = -\sqrt{a}$ and $\tau(\sqrt{c}) = -\sqrt{c}$, so $\sigma\tau = \tau\sigma$. A K-basis for A is given by

$$\{1 \otimes 1, j_1 \otimes 1, 1 \otimes j_2, j_1 \otimes j_2\}$$

and the right K-vector space A can be identified with

$$K \oplus j_1 K \oplus j_2 K \oplus j_1 j_2 K.$$

The usual embedding $\lambda(A)$ is one of vector spaces and $\mathcal{A} = \lambda(A)$ does not carry an algebra structure. An element in $\lambda(A) = \mathcal{A}$ has the form

$$\begin{bmatrix} x_0 & b\sigma(x_1) & d\tau\sigma(x_2) & db\tau\sigma(x_3) \\ x_1 & \sigma(x_0) & d\tau\sigma(x_3) & d\tau\sigma(x_2) \\ x_2 & b\sigma(x_3) & \sigma(x_0) & b\sigma(x_1) \\ x_3 & \sigma(x_2) & \sigma(x_1) & \sigma(x_0) \end{bmatrix} \tag{28}$$

with all $x_i \in K$, $d \in K_1 \setminus F$, $b \in F$. Nonetheless, if A is a division algebra, $\mathcal{A}$ is a fully diverse linear codebook, cf. [13] or [11].

We point out that here the element $d \in F(\sqrt{c}) \setminus F$, whereas in Section **??** it was contained in F.

7.2. Connection with iterated codes. Read $Q = (a,b)_{K_1}$ from above as a quaternion algebra over K_1. In the more general situation where $\theta = \theta_0 + j\theta_1 \in Q^\times$, $\Theta \in Mat_{2\times 2}(K_1)$ is given by

$$\Theta = \begin{bmatrix} \theta_0 & \gamma\sigma(\theta_1) \\ \theta_1 & \sigma(\theta_0) \end{bmatrix},$$

for $A, B \in Mat_{2\times 2}(K_1)$,

$$\alpha_\theta(A,B) = \begin{bmatrix} A & \Theta\tau(B) \\ B & \tau(A) \end{bmatrix}.$$

In particular, for $x = x_0 + jx_1$ and $y = y_0 + jy_1$ elements of Q, we have

$$\Theta\tau(Y) = \begin{bmatrix} \theta_0\tau(y_0) + \gamma\sigma(\theta_1)\tau(y_1) & \gamma(\theta_0\sigma\tau(y_1) + \sigma(\theta_1)\sigma\tau(y_0)) \\ \theta_1\tau(y_0) + \sigma(\theta_0)\tau(y_1) & \theta_1\gamma\sigma\tau(y_1) + \sigma(\theta_0)\sigma\tau(y_0) \end{bmatrix} = \begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix}.$$

The explicit map α_θ is given by

$$\alpha_\theta(\begin{bmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix}, \begin{bmatrix} y_0 & \gamma\sigma(y_1) \\ y_1 & \sigma(y_0) \end{bmatrix}) \to \begin{bmatrix} x_0 & \gamma\sigma(x_1) & f_1 & f_2 \\ x_1 & \sigma(x_0) & f_3 & f_4 \\ y_0 & \gamma\sigma(y_1) & \tau(x_0) & \gamma\tau(\sigma(x_1)) \\ y_1 & \sigma(y_0) & \tau(x_1) & \tau(\sigma(x_0)) \end{bmatrix}, \tag{29}$$

where f_i, defined above, are the entries of the matrix ΘY.

Thus the top right block of the codewords given by $\alpha_\theta(Q,Q)$ lose their nice shape. By Theorem 5, if Q is division over K_1, the codebook (28) (which is the special case that $d = \theta \in K_1 \setminus F$), resp. (29), defined by $\alpha_\theta(\mathcal{Q},\mathcal{Q})$, is fully diverse, if and only if $\theta \neq z\widetilde{\tau}(z)$ for all $z \in Q$. The determinant of a matrix in $\alpha_\theta(\mathcal{Q},\mathcal{Q})$ is an element of K_1.

Remark 22. More generally, if K_0 and $F(\sqrt{c})$ are linearly independent over F, we can look at the tensor product of any cyclic division algebra $C = (K_0/F, \sigma, \gamma)$ over F and the nonassociative quaternion algebra $\mathrm{Cay}(F(\sqrt{c}), d)$, to get a codebook

$$\begin{bmatrix} X_0 & d\tau(X_1) \\ X_1 & \tau(X_0) \end{bmatrix}$$

with $X, Y \in \mathcal{C} = \lambda(C)$ having entries in the field $K = K_0(\sqrt{c})$. By Theorem 5, if C is a division algebra over $K_1 = F(\sqrt{c})$, this codebook is fully diverse if and only if $\theta \neq z\widetilde{\tau}(z)$ for all $z \in C$.

8. Tensor products of two algebras with a common subfield

All previous considerations carry over to the case where the tensor product $A = C \otimes_F D$ contains zero divisors. At first glance, this case does not seem to be relevant, as the resulting codebooks are not fully diverse. However, the code constructions from [1] all deal with codebooks which can be obtained as subsets of matrices from codebooks constructed from these tensor product algebras. The method should be clear by now, so let us treat the associative and nonassociative setup together in our next cases.

8.1. Take the tensor product

$$A = (K/F, \sigma, \gamma) \otimes_F \mathrm{Cay}(F(\sqrt{a}), \theta)$$

of a cyclic division algebra $C = (K/F, \sigma, \gamma)_F$ of even degree $n = 2m$ and a (perhaps nonassociative) quaternion algebra $\mathrm{Cay}(F(\sqrt{a}), d)$ with $\theta \in F(\sqrt{a})$ (if $\theta \notin F$, this is a quaternion algebra). Let $K_1 = F(\sqrt{a})$ be a subfield of K and $\mathrm{Gal}(K_1/F) = \langle \sigma^m \rangle$. $(K/F, \sigma, \gamma)$ is an n-dimensional right K-vector space with basis $\{1, e, e^2, \ldots, e^{n-1}\}$, where $e^n = \gamma$, view $(a, \theta)_F$ as two-dimensional right $F(\sqrt{a})$-vector space with basis $\{1, j\}$, where $j^2 = \theta$. A cannot be a division algebra, as it contains the split F-algebra

$$R = K \otimes_F K_1 \cong K \times K.$$

Since $R = K \otimes_F K_1 \subset \mathrm{Nuc}(A)$, A is a free right R-algebra of dimension $2n$ with R-basis $\{1 \otimes 1, e \otimes 1, \ldots, e^{n-1} \otimes 1, 1 \otimes j, e \otimes j, e^{n-1} \otimes j\}$. Identify

$$A = R \oplus eR \oplus \cdots \oplus e^{n-1}R \oplus jR \oplus ejR \oplus \cdots \oplus e^{n-1}jR.$$

An element in $\lambda(A)$ has the form

$$\begin{bmatrix} X & \theta\sigma^m(Y) \\ Y & \sigma^m(X) \end{bmatrix}. \tag{30}$$

Here, $X, Y \in \mathrm{Mat}_n(R)$, such that when restricting their entries x_i, $y_i \in R$ to elements in K, we obtain $X, Y \in \mathcal{C}$. $\mathcal{A}$ is not fully diverse. If we restrict the entries to $x_i \in K \subset R$, we get codebooks $\mathcal{A} = \alpha_\theta(\mathcal{C}, \mathcal{C})$ with

$$\alpha_\theta(X, Y) = \begin{bmatrix} X & \theta\sigma^m\sigma(Y) \\ Y & \sigma^m\sigma(X) \end{bmatrix}$$

with $X, Y \in \mathcal{C}$, $C = (K/F, \sigma, \gamma)$ and choice of $\theta \in K_1^\times$. By Theorem 5,

$$\det(A) \in F$$

for all $A \in \mathcal{A}$ and $\alpha_\theta(\mathcal{C}, \mathcal{C})$ is fully diverse if and only if $\theta \neq z\widetilde{\tau}(z)$ for all $z \in C$.

Example 23. Let

$$A = (a, \gamma)_F \otimes_F \mathrm{Cay}(F(\sqrt{a}), \theta)$$

be the tensor product of a quaternion division algebra $(a, \gamma)_F$ and a (perhaps nonassociative) quaternion algebra $\mathrm{Cay}(F(\sqrt{a}), d)$ with $\theta \in F(\sqrt{a})$ (if $\theta \in F$, this is a quaternion algebra). Let $K = F(\sqrt{a})$ and $\mathrm{Gal}(K/F) = \langle \sigma \rangle$. An element in $\lambda(A)$ has the form

$$\begin{bmatrix} x_0 & \gamma\sigma(x_1) & \theta\sigma(x_2) & \theta\gamma x_3 \\ x_1 & \sigma(x_0) & \theta\sigma(x_3) & \theta x_2 \\ x_2 & \gamma\sigma(x_3) & \sigma(x_0) & \gamma x_1 \\ x_3 & \sigma(x_2) & \sigma(x_1) & x_0 \end{bmatrix} \tag{31}$$

with all $x_i \in R = K \otimes_F K$. If we restrict the entries to $x_i \in K \subset R$, we obtain the codebook $\mathcal{A} = \alpha_\theta(\mathcal{D}, \mathcal{D})$ with

$$\alpha_\theta(X, Y) = \begin{bmatrix} X & \theta\sigma(Y) \\ Y & \sigma(X) \end{bmatrix},$$

where $X, Y \in \mathcal{D}$, $D = (a, \gamma)_F$ and $\theta \in K$. By Theorem 5, this restricted codebook is fully diverse if and only if $\theta \neq z\widetilde{\tau}(z)$ for all $z \in D$, and we have $\det(X) \in F$ for all $X \in \mathcal{A}$.

All codes considered in Section III and IV of [1] can be obtained from tensor products of two quaternion algebras containing the same subfield $F(\sqrt{a})$. Apart from one case mentioned in the next example, $\theta \in F$:

Example 24. (i) In IV.A of [1], the representation matrix of left multiplication in the associative tensor product

$$(-1,-1)_{\mathbb{Q}(\sqrt{-7})} \otimes_{\mathbb{Q}(\sqrt{-7})} \mathrm{Cay}(\mathbb{Q}(\sqrt{-7}, i), \theta)$$

is studied, $\theta \in \mathbb{Q}(\sqrt{-7})$, with matrix entries restricted from $R = \mathbb{Q}(\sqrt{-7}, i) \otimes_{\mathbb{Q}(\sqrt{-7})} \mathbb{Q}(\sqrt{-7}, i)$ to $\mathbb{Q}(\sqrt{-7}, i)$. It is fully diverse for the right choice of θ, e.g. for $\theta = -17$, and thus has NDV. The code is fast decodable as well.

The authors mention that they feel the choice of $\theta = i$ feels natural to them. Indeed, this choice corresponds to choosing the matrix representation of left multiplication in the nonassociative tensor product algebra

$$A = (-1,-1)_{\mathbb{Q}(\sqrt{-7})} \otimes_{\mathbb{Q}(\sqrt{-7})} \mathrm{Cay}(\mathbb{Q}(\sqrt{-7}, i), i)$$

involving the nonassociative quaternion division algebra $\mathrm{Cay}(\mathbb{Q}(\sqrt{-7}, i), i)$ instead, and then restricting entries in the matrices to $\mathbb{Q}(\sqrt{-7}, i)$. This code is fully diverse if and only if $i \neq z\widetilde{\tau}(z)$ for all $z \in (-1,-1)_{\mathbb{Q}(\sqrt{-7})}$.
(ii) In IV.B of [1], the representation matrix of the associative tensor product

$$(5, i)_{\mathbb{Q}(i)} \otimes_{\mathbb{Q}(i)} \mathrm{Cay}(\mathbb{Q}(i, \sqrt{5}), \theta)$$

is studied, $\theta \in \mathbb{Q}(i)$, with matrix entries restricted from $R = \mathbb{Q}(i, \sqrt{5}) \otimes_{\mathbb{Q}(i)} \mathbb{Q}(i, \sqrt{5})$ to $\mathbb{Q}(i, \sqrt{5})$. It is fully diverse for the right choice of θ, e.g. for $\theta = 1 - i$, and thus has NDV. The code is fast decodable as well.
(iii) In IV.C of [1], the representation matrix of the associative tensor product

$$(-1,-1)_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathrm{Cay}(\mathbb{Q}(i), \theta)$$

is studied, $\theta \in \mathbb{Q}$ with matrix entries restricted from $R = \mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(i)$ to $\mathbb{Q}(i)$. It is fully diverse for the right choice of θ, e.g. for $\theta = -3$, but not full-rate. Choosing $\theta = -1$ yields the quasi-orthogonal code from Jafarkhani [20], which is not fully diverse. It uses the representation matrices of left multiplication in

$$(-1,-1)_{\mathbb{Q}} \otimes_{\mathbb{Q}} (-1,-1)_{\mathbb{Q}}$$

with their entries restricted to $\mathbb{Q}(i)$.

Remark 25. If we iterate the construction and take the tensor products of, for example, more than two quaternion division algebras, i.e. $A = (a, b)_F \otimes (c_1, d_1)_F \otimes \cdots \otimes (c_m, d_m)_F$, and the corresponding matrix representations (assuming conditions where A is a division algebra to obtain fully diverse iterated codes), this amounts to applying different maps α_{d_i} with mutually non-identical automorphisms τ_i one after the other iteratively, similarly as noted in [1], Remark 4.

8.2. Which algebra is involved in the restriction process? The subspace

$$A_0 = K \oplus eK \oplus \cdots \oplus e^{n-1}K \oplus jK \oplus ejK \oplus \cdots \oplus e^{n-1}jK \subset A = (K/F, \sigma, \gamma) \otimes_F \mathrm{Cay}(F(\sqrt{a}), \theta)$$

has dimension $2n^2$ as F-vector space. A_0 is closed under multiplication for all $\theta \in K^\times$ and hence an F-subalgebra A_0 of A.

Restricting the matrix entries to elements in K obtain $\mathcal{A}$ amounts to computing the representation matrix for left multiplication in A_0 using an element $x \in A_0$ to compute λ_x

Lemma 26. *Suppose $\theta \in F^\times$.*
(i) A_0 has center $Z_0 = F \oplus e^m F = \mathrm{Cay}(F, \gamma\theta)$ and the maximal commutative subring $R_0 = K \oplus e^m K$. $Z_0 = F(\sqrt{\gamma\theta})$ iff $\gamma\theta \notin F^{\times 2}$. $R_0 = \mathrm{Cay}(Z_0, a)$ is a Z_0-algebra and $R_0 = F(\sqrt{\gamma\theta})(\sqrt{a})$ iff $\gamma\theta \notin F^{\times 2}$ and $a \notin Z_0^{\times 2}$.
(ii) If $d \neq Z\sigma(Z)$ for all $Z \in \lambda((a, \gamma)_K)$ then A_0 is division with center $F(\sqrt{\gamma\theta})$ and maximal subfield $K(\sqrt{\gamma\theta})$.
(iii) If $F(\sqrt{\gamma}) \neq F(\sqrt{\theta})$ then $Z_0 = F(\sqrt{\gamma\theta})$, if $F(\sqrt{\gamma\theta}) \neq F(\sqrt{a})$ then $R_0 = F(\sqrt{\gamma\theta})(\sqrt{a})$ is a field, and if, additionally,

$$\gamma^s \notin N_{K(\sqrt{\gamma\theta})/F(\sqrt{\gamma\theta})}(K(\sqrt{\gamma\theta})^\times)$$

for all s, $1 \leq s \leq n-1$, then $A_0 = (K(\sqrt{\gamma\theta})/F(\sqrt{\gamma\theta}), \sigma, \gamma)$ is division.
(iv) If $d \neq Z\sigma(Z)$ for all $Z \in \lambda((a, \gamma)_K)$ then $A_0 = (K(\sqrt{\gamma\theta})/F(\sqrt{\gamma\theta}), \sigma, \gamma)$ is division.

Proof. The proof of (i) is analogous to Lemma 8 of [1] and Lemma 25.
(ii) This is Corollary 1 of [1].
(iii) is clear.
(iv) is a straightforward calculation along the lines of the proof for Lemma 25 (ii). □

Corollary 27. *A necessary condition for A_0 to be division is that $F(\sqrt{\gamma\theta})$ is linearly disjoint to K and that $(K/F, \sigma, \gamma)_{F(\sqrt{\gamma\theta})}$ is a division algebra.*

For biquaternion algebras, we obtain:

Lemma 28. *Suppose $\theta \in F^\times$ and $A = (a, \gamma)_F \otimes_F (a, \theta)_F$. Let σ denote the canonical involution of (a, γ) and τ the canonical involution of (a, θ), then A has the involution $\sigma_0 = \sigma \otimes \tau$.*
(i) A_0 has center $Z_0 = F \oplus j_1 j_2 F = \mathrm{Cay}(F, \gamma\theta)$ and the maximal commutative subring $R_0 = K \oplus j_1 j_2 K$. $Z_0 = F(\sqrt{\gamma\theta})$ iff $\gamma\theta \notin F^{\times 2}$. $R_0 = \mathrm{Cay}(Z_0, a)$ is a Z_0-algebra and $R_0 = F(\sqrt{\gamma\theta})(\sqrt{a})$ iff $\gamma\theta \notin F^{\times 2}$ and $a \notin Z_0^{\times 2}$.
(ii) If $d \neq Z\sigma(Z)$ for all $Z \in \lambda((a, \gamma)_K)$ then A_0 is division with center $F(\sqrt{\gamma\theta})$ and maximal subfield $K(\sqrt{\gamma\theta})$.
(iii) $A_0 = \mathrm{Cay}(R_0, \gamma)$ is a Z_0-algebra. If $F(\sqrt{\gamma}) \neq F(\sqrt{\omega})$ then $Z_0 = F(\sqrt{\gamma\theta})$, if $F(\sqrt{\gamma\theta}) \neq F(\sqrt{a})$ then $R_0 = F(\sqrt{\gamma\theta})(\sqrt{a})$ is a field, and if, additionally,

$$\gamma \notin N_{F(\sqrt{\gamma\theta}, \sqrt{a})/F(\sqrt{\gamma\theta})}(F(\sqrt{\gamma\theta}, , \sqrt{a})^\times)$$

then $A_0 = (a, \gamma)_{F(\sqrt{\gamma\theta})}$ is division.
(iv) If $d \neq Z\sigma(Z)$ for all $Z \in \lambda((a, \gamma)_K)$ then $A_0 = (a, \gamma)_{F(\sqrt{\gamma\theta})}$ is division.

Proof. (i) This is Lemma 8 of [1]. It is easy to see that $Z_0 = \mathrm{Cay}(F, \gamma\theta)$ since $\gamma\theta \in F$, so $Z_0 = F(\sqrt{\gamma\theta})$ iff $\gamma\theta \notin F^{\times 2}$, else $Z_0 = F \times F$. Z_0 is an F-algebra. Similarly, $R_0 = \mathrm{Cay}(Z_0, a)$ with Z_0 now viewed as Z_0-algebra. $R_0 = F(\sqrt{\gamma\theta})(\sqrt{a})$ iff $\gamma\theta \notin F^{\times 2}$ and $a \notin Z_0^{\times 2}$.
(ii) and (iv): This is Corollary 1 of [1].
(iii) $A_0 = (K \oplus j_1 j_2 K) \oplus j_1(K \oplus j_1 j_2 K) = \mathrm{Cay}(R_0, \gamma)$, where the involution σ_0 restricted to R_0 is used in defining the usual multiplication in the Cayley-Dickson doubling process. A_0 is a Z_0-algebra. Note that $\sigma_0(j_1 j_2) = j_1 j_2$ and $\sigma_0(j_1) = -j_1$. The rest of the statement is now trivial. □

Suppose now $\theta \in K \setminus F$. The codebook obtained from restricting the entries in $\mathcal{A}$ to elements in K thus comes from a nonassociative subalgebra A_0 of A (and is not closed under multiplication).

Lemma 29. *Suppose $\theta \in K \setminus F$. Then A_0 has center F and the maximal commutative subring K.*

Proof. The proof is analogous to Lemma 8 of [1]. If

$$\begin{bmatrix} U & \theta\sigma(V) \\ V & \sigma(U) \end{bmatrix} \text{ commutes with all } \begin{bmatrix} X & \theta\sigma(Y) \\ Y & \sigma(X) \end{bmatrix}$$

with $X, Y, U, V \in \mathcal{D} = \lambda((a,b)_F)$, then for $Y = 0$ we get $UX = XU$, so that $U \in Z(\mathcal{D}) = F$, and $\sigma(X)V = VX$, $\theta\sigma(V)\sigma(X) = X\theta\sigma(V)$ (i.e. $\sigma(\theta)VX = \sigma(X)\sigma(\theta)V$) for all $X \in \mathcal{D}$. Now $\sigma(X)V = VX$ implies $V \in j_1 F$ and $\sigma(\theta)VX = \sigma(X)\sigma(\theta)V$ implies $\sigma(\theta)V \in j_1 F$, so $V = 0$, since we chose $\theta \in K \setminus F$. □

It is possible to give an explicit description of A_0. We refrain from doing this here, to keep the paper within reasonable length, and only say that they can be obtained by some sort of a Cayley-Dickson doubling process out of $(K/F, \sigma, \gamma)$, using $\widetilde{\tau}$ and a scalar $\theta \in (K/F, \sigma, \gamma)^\times$. This will be treated in a separate paper [21].

9. Tensor products where one algebra has zero divisors

Translated to our context of tensor products of algebras, Section V in [1] deals with the following situation:

Let L be a Galois extension with Galois group $\mathrm{Gal}(L/F) = C_2 \times C_n$ (i.e., $\cong C_{2n}$, if n odd), where σ generates C_n and τ generates C_2. Let $K = \mathrm{Fix}(\sigma)$, then $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Let $K = F(\sqrt{c})$ and $\mathrm{Gal}(K/F) = \langle\tau\rangle$. Let $\mathrm{Cay}(K, \theta)$ be a (perhaps nonassociative) quaternion division algebra over F with $\theta \in F(\sqrt{a})$ (if $\theta \notin F$, this is a quaternion algebra), and $C = (L/K, \sigma, \gamma)$ a cyclic division algebra over K of degree n. The K-algebra $\mathrm{Cay}(K, \theta) \otimes_F K$ contains the split quadratic étale K-algebra $T = K \otimes_F K \cong K \times K$.

$(L/K, \sigma, \gamma)$ is an n-dimensional right L-vector space with basis $\{1, e, e^2, \ldots, e^{n-1}\}$, where $e^{n-1} = \gamma$, and $\mathrm{Cay}(K, \theta) \otimes_F K = T \oplus jT$ a two-dimensional right T-module with basis $\{1, j\}$, where $j^2 = \theta$. Take the tensor product

$$A = (L/K, \sigma, \gamma) \otimes_K (\mathrm{Cay}(F(\sqrt{c}), \theta) \otimes_F K).$$

A is not a division algebra, as it contains the split K-algebra

$$R = L \otimes_K T \cong L \times L.$$

Since $L \otimes_K T \subset Nuc(A)$, A is a free right R-algebra of dimension $2n$ with R-basis $\{1 \otimes 1, e \otimes 1, \ldots, e^{n-1} \otimes 1, 1 \otimes j, e \otimes j, e^{n-1} \otimes j\}$ and we identify

$$A = R \oplus eR \oplus \cdots \oplus e^{n-1}R \oplus jR \oplus ejR \oplus \cdots \oplus e^{n-1}jR.$$

An element in $\lambda(A)$ has the form

$$\begin{bmatrix} X & \Theta\tau\sigma(Y) \\ Y & \tau\sigma(X) \end{bmatrix} \tag{32}$$

with $X, Y \in \mathrm{Mat}_n(R)$, such that when restricting the matrix entries of X, Y to elements in $L \subset R$, we obtain $X, Y \in \mathcal{C}$ and the codebook $\mathcal{A} = \alpha_\theta(\mathcal{C}, \mathcal{C})$. By Theorem 5, $\alpha_\theta(\mathcal{C}, \mathcal{C})$ is fully diverse if and only if $\theta \neq z\widetilde{\tau}(z)$ for all $z \in C$ and $\det(\alpha_\theta(X, Y)) \in K$ for all $X, Y \in \mathcal{C}$.

If $\theta \in F^\times$, $\mathcal{A}$ comes from the central simple associative algebra A over K. If we take $n = 3$, restrict the entries to $x_i \in L \subset R$, and choose $\theta \in K$, we get exactly the codebooks $\alpha_\theta(\mathcal{C}, \mathcal{C})$ from Section V of [1] where

$$\alpha_\theta(X, Y) = \begin{bmatrix} X & \Theta\tau\sigma(Y) \\ Y & \tau\sigma(X) \end{bmatrix}$$

with $X, Y \in \mathcal{C} = \lambda(C)$.

Example 30. Let ζ_7 be a primitive 7th root of unity.
(i) $(\mathbb{Q}(\zeta_7, i)/\mathbb{Q}(\sqrt{-7}, i), \sigma_2, 1+i)$ is a cyclic division algebra of degree 3 over $\mathbb{Q}(\sqrt{-7}, i)$ with $\sigma : \zeta_7 \to \zeta_7^2$. Let $K = \mathbb{Q}(\sqrt{-7}, i)$, $F = \mathbb{Q}(i)$ and $\tau(\sqrt{7}) = -\sqrt{7}$, $\tau(i) = i$. In [1], Example 4, the restricted matrix representation of the tensor product

$$A = (\mathbb{Q}(\zeta_7, i)/\mathbb{Q}(\sqrt{-7}, i), \sigma_2, 1+i) \otimes_{\mathbb{Q}(\sqrt{-7}, i)} (\mathrm{Cay}(\mathbb{Q}(\sqrt{-7}, i), i\sqrt{7}) \otimes_{\mathbb{Q}(i)} \mathbb{Q}(\sqrt{-7}, i)$$

with entries in $L = \mathbb{Q}(\zeta_7, i)$ is considered. The code has NVD and is fast-decodable.
(ii) $(\mathbb{Q}(\zeta_7)/\mathbb{Q}(\sqrt{-7}), \sigma_2, 3)$ is a cyclic division algebra of degree 3 over $\mathbb{Q}(\sqrt{-7})$ with $\sigma : \zeta_7 \to \zeta_7^2$. In [1], Example 5, the restricted matrix representation of the tensor product

$$A = (\mathbb{Q}(\zeta_7)/\mathbb{Q}(\sqrt{-7}), \sigma, 3) \otimes_{\mathbb{Q}(\sqrt{-7})} (\mathrm{Cay}(\mathbb{Q}(\sqrt{-7}), \sqrt{-7}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-7})).$$

with entries in $L = \mathbb{Q}(\zeta_7)$ is considered.

9.1. Which algebra is involved in the restriction process? Restricting the elements to have entries in L amounts to computing the representation matrix for the subspace

$$A_0 = L \oplus eL \oplus \cdots \oplus e^{n-1}K \oplus jL \oplus ejL \oplus \cdots \oplus e^{n-1}jL \subset A,$$

a right L-vector space of dimension n^2 and of dimension $2n^2$ as F-vector space. A straightforward check shows A_0 is closed under multiplication both for $\theta \in F^\times$ and $\theta \in K \setminus F$, and hence an F-subalgebra A_0 of A.

Lemma 31. *(i) Suppose $\gamma, \theta \in F^\times$.*
(a) A_0 has center F and maximal subfield L.
(b) If $d \neq Z\tau(Z)$ for all $Z \in \lambda((L/K, \sigma, \gamma))$ then A_0 is the crossed product algebra $(L/F, \gamma, \theta, 1)$ of degree $2n$.
(ii) Suppose $\gamma \in F^\times$, $\theta \in K \setminus F$. Then A_0 has center K and maximal subfield L.

Proof. (a) The proof of (i) is analogous to Lemma 8 of [1].
(ii) is Corollary 1 of [1] and Section III.B of [2].
(b) The proof is analogous to Lemma 8 of [1]. □

Example 32. Let $n = 2$, i.e. $L = F(\sqrt{a}, \sqrt{c})$, $K = F(\sqrt{c})$ and take the tensor product

$$A = (a, \gamma)_K \otimes_K (\mathrm{Cay}(K, \theta) \otimes_F K)$$

with $\theta \in F(\sqrt{c})$. An element in $\lambda(A) = \mathcal{A}$ with entries restricted to L has the form

$$\alpha_\theta(\mathcal{C}, \mathcal{C}) = \begin{bmatrix} x_0 & \gamma\sigma(x_1) & \theta\tau(x_2) & \theta\gamma\tau\sigma(x_3) \\ x_1 & \sigma(x_0) & \theta\tau(x_3) & \theta\tau\sigma(x_2) \\ x_2 & \gamma\sigma(x_3) & \tau(x_0) & \gamma\tau(x_1) \\ x_3 & \sigma(x_2) & \tau(x_1) & \tau(x_0) \end{bmatrix} \tag{33}$$

with all $x_i \in L$ for all $X \in \mathcal{A}$. By Theorem 5, $\alpha_\theta(\mathcal{C}, \mathcal{C})$ is fully diverse if and only if $\theta \neq z\widetilde{\tau}(z)$ for all $z \in C$ and $\det(\alpha_\theta(X, Y)) \in K$ for all $X, Y \in \mathcal{C}$. If $\gamma, \theta \in F^\times$ and $d \neq Z\tau(Z)$ for all $Z \in \lambda((a, \gamma)_K)$, then $A_0 = (L/F, \gamma, \sigma, 1)$ is division.

If $\theta \in K \setminus F$, the codebook obtained from restricting the entries in $\mathcal{A}$ to elements in K comes from a nonassociative subalgebra A_0 of A (and is not closed under multiplication).

10. Generalized iterations using two cyclic algebras

10.1. Let K_0/F be a cyclic Galois field extension with $\mathrm{Gal}(K_0/F) = \langle\sigma\rangle$, and K_0/F be a cyclic Galois field extension with $\mathrm{Gal}(K_0/F) = \langle\tau\rangle$. Let $C_0 = (K_0/F, \sigma, \gamma)$ be a (perhaps nonassociative) cyclic division algebra of degree n over F and $C_1 = (K_1/F, \tau, \theta)$ be a (perhaps nonassociative) cyclic algebra of degree m over F, i.e. $\theta \in K_1^\times$ (so these are associative cyclic algebras for $\gamma, \theta \in F^\times$).

Define $\mathcal{C}_i = \lambda(C_i)$, $i = 0, 1$, then the codebooks $\mathcal{C}_i$ are fully diverse. Let $\{1, e, e^2, \ldots, e^{n-1}\}$ be the standard basis of the right K_0-vector space C_0 and $\{1, f, f^2, \ldots, f^{n-1}\}$ be the standard basis of the right K_1-vector space C_1. Let

$$A = (K_0/F, \sigma, \gamma) \otimes_F (K_1/F, \tau, \theta)$$

then $R = K_0 \otimes_F K_1 \subset Nuc(A)$ and A is a right R-vector space of dimension nm with R-basis $\{1 \otimes 1, e \otimes 1, \ldots, e^{n-1} \otimes 1, 1 \otimes f, e \otimes f, \ldots, e^{n-1} \otimes f^{m-1}\}$. Identify

$$A = R \oplus eR \oplus \cdots \oplus e^{n-1}R \oplus fR \oplus efR \oplus \cdots \oplus e^{n-1}f^{m-1}R.$$

An element in $\lambda(A)$ has the form

$$\begin{bmatrix} Y_0 & \theta\tau(Y_{n-1}) & \theta\tau^2(Y_{n-2}) & \dots & \theta\tau^{m-1}(Y_1) \\ Y_1 & \tau(Y_0) & \theta\tau^2(Y_{n-1}) & \dots & \theta\tau^{m-1}(Y_2) \\ \vdots & & \vdots & & \vdots \\ Y_{n-2} & \tau(Y_{n-3}) & \tau^2(Y_{n-4}) & \dots & \theta\tau^{m-1}(Y_{n-1}) \\ Y_{n-1} & \tau(Y_{n-2}) & \tau^2(Y_{n-3}) & \dots & \tau^{m-1}(Y_0) \end{bmatrix} \tag{34}$$

with the $Y_i \in \mathrm{Mat}_n(R)$ such that when their entries are restricted to K_0, $Y_i \in \mathcal{C}_0$. Denote the corresponding codebook with restricted entries by $\mathcal{A}$. It can be shown that for all $A \in \mathcal{A}$, $\det(A) \in F$ if $\gamma \in F\times$ [22]. In particular, for $m = 3$, $\mathcal{A}$ has entries in K_0 and contains matrices of the form

$$\beta_\theta(\mathcal{C}_0, \mathcal{C}_0) = \begin{bmatrix} Y_0 & \theta\tau(Y_2) & \theta\tau^2(Y_1) \\ Y_1 & \tau(Y_0) & \theta\tau^2(Y_2) \\ Y_2 & \tau(Y_1) & \tau^2(Y_0) \end{bmatrix} \tag{35}$$

with $Y_i \in \mathcal{C}_0$. With the right choice of θ and $\gamma \in F^\times$, this could be another way to iterate well-performing codes $\mathcal{C}_0$.

10.2. Tensor product of two cyclic algebra where one contains zero divisors. Let L be a Galois extension with Galois group $\mathrm{Gal}(L/F) = C_m \times C_n \cong C_{mn}$, m, n coprime, where σ generates C_n and τ generates C_m. Let $K = \mathrm{Fix}(\sigma)$, then $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ and $\mathrm{Gal}(K/F) = \langle\tau\rangle$. Note that

$$\sigma^i\tau^j = \tau^j\sigma^i, \quad 1 \le i \le n-1, \quad 1 \le j \le m-1.$$

Let $C_0 = (L/K, \sigma, \gamma)$ be a (perhaps nonassociative) cyclic division algebra of degree n over K and $C_1 = (K/F, \tau, \theta)$ be a (perhaps nonassociative) cyclic division algebra of degree m over F, i.e. $\gamma \in L$, $\theta \in K$. Define $\mathcal{C}_i = \lambda(C_i)$, $i = 0, 1$, then the codebooks $\mathcal{C}_i$ are fully diverse. Let $\{1, e, e^2, \dots, e^{n-1}\}$ be the standard basis of the right L-vector space C_0 and $\{1, f, f^2, \dots, f^{m-1}\}$ be the standard basis of the right K-vector space C_1.

The K-algebra $(K/F, \tau, \theta) \otimes_F K$ contains zero divisors, since it contains the split étale K-algebra

$$T = K \otimes_F K \cong K \times \cdots \times K \quad (m \text{ times}).$$

Choose $\{1, f, f^2, \dots, f^{m-1}\}$ as its T-basis and define

$$A = (L/K, \sigma, \gamma) \otimes_K (C_1 \otimes_F K).$$

A contains the split K-algebra $R = L \otimes_K T \cong L \times \cdots \times L$ (m times), we also have $R = L \otimes_K T \subset Nuc(A)$ and so A is a right R-vector space of dimension nm with R-basis $\{1 \otimes 1, e \otimes 1, \dots, e^{n-1} \otimes 1, 1 \otimes f, e \otimes f, \dots, e^{n-1} \otimes f^{m-1}\}$. Identify

$$A = R \oplus eR \oplus \cdots \oplus e^{n-1}R \oplus fR \oplus efR \oplus \cdots \oplus e^{n-1}f^{m-1}R.$$

An element in $\lambda(A)$ has the form

$$\begin{bmatrix} Y_0 & \theta\tau(Y_{n-1}) & \theta\tau^2(Y_{n-2}) & \dots & \theta\tau^{m-1}(Y_1) \\ Y_1 & \tau(Y_0) & \theta\tau^2(Y_{n-1}) & \dots & \theta\tau^{m-1}(Y_2) \\ \vdots & & \vdots & & \vdots \\ Y_{n-2} & \tau(Y_{n-3}) & \tau^2(Y_{n-4}) & \dots & \theta\tau^{m-1}(Y_{n-1}) \\ Y_{n-1} & \tau(Y_{n-2}) & \tau^2(Y_{n-3}) & \dots & \tau^{m-1}(Y_0) \end{bmatrix} \tag{36}$$

with the $Y_i \in \mathrm{Mat}_n(R)$ such that when their entries are restricted to L, $Y_i \in \mathcal{C}_0$. Denote this codebook with entries in L by $\mathcal{A}$. It can be shown that for all $A \in \mathcal{A}$, $\det(A) \in K^\times$ if $\gamma \in K$ [22]. For $m = 3$, matrices in $\mathcal{A}$ have the form

$$\beta_\theta(\mathcal{C}_0, \mathcal{C}_0) = \begin{bmatrix} Y_0 & \theta\tau(Y_2) & \theta\tau^2(Y_1) \\ Y_1 & \tau(Y_0) & \theta\tau^2(Y_2) \\ Y_2 & \tau(Y_1) & \tau^2(Y_0) \end{bmatrix} \tag{37}$$

with $Y_i \in \mathcal{C}_0$. With the right choice of θ, this could be another way to iterate well-performing codes $\mathcal{C}_0$.

Remark 33. In [2], the following setup is studied: Let F and L be two distinct number fields and K a Galois extension containing both F and L. Moreover, let $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ have order n, $\mathrm{Gal}(K/L) = \langle\tau\rangle$ have order n and assume that σ and τ commute. Let $D = (K/F, \sigma, \gamma)$ be a cyclic division algebra of degree m. A non-commutative ring $\mathcal{M}_\mathcal{D}$ which is an n-dimensional $\mathcal{D}$-bimodule is defined with basis $1, f, \dots, f^{n-1}$ such that $Af = f\tau(A)$ and $i^n = \theta$ for some $\theta \in D$. It is assumed that $\gamma \in L$.

The framework treated in [2] fits into ours as follows: if $\theta \in F \cap L$, the construction $\mathcal{M}_\mathcal{D}$ is the matrix representation of the associative tensor product

$$A = (K/F, \sigma, \gamma) \otimes_F ((F/F \cap L, \tau, \theta) \otimes_{F\cap L} F),$$

restricting entries to K, so that, automatically, $\det(X) \in F$ for all $X \in \mathcal{M}_\mathcal{D}$. This case which we briefly study in this Section is not treated in [2]. Instead, the focus is on $\theta \in L \setminus F$ and $\gamma \in F \cap L$.

Example 34. Put $Y_2 = \cdots = Y_{n-1} = 0$ in (36) to obtain code

$$S_{m\times n} = \{ \begin{bmatrix} Y_0 & 0 & 0 & \dots & \theta\tau^{m-1}(Y_1) \\ Y_1 & \tau(Y_0) & 0 & \dots & 0 \\ 0 & \tau(Y_1) & \tau^2(Y_0) & \dots & 0 \\ 0 & 0 & \tau^2(Y_1) & \tau^3(Y_0) & \dots \\ \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & \tau^{m-1}(Y_0) \end{bmatrix} \} \tag{38}$$

with entries in K, a STBC for a $2n \times 2$ system with $\det(X) \in K$ for all $X \in S_{m\times n}$, if $\gamma \in K$. When designing codes, one would choose $\mathbb{Q}(i) \subset K$ or $\mathbb{Q}(\omega) \subset K$, so that it is clear, analogously as in [2], Proposition 1 and 2, that the rate of the STBC is two complex symbols per channel use and so that it has the NVD property if it is fully diverse and $\gamma \in \mathcal{O}_K, \theta \in \mathcal{O}_F$.

11. Conclusion

We built STBCs out of tensor products of both associative and nonassociative cyclic algebras of degree n and m over number fields and investigated when they are fully diverse. We compared our constructions with the iterated method introduced in [1] and the ones using modules in [2].

We proposed a new method how to obtain fully diverse, rate-m STBCs from the tensor product of two cyclic algebras. In particular, we showed how to construct fully diverse, rate-2 STBCs for $2n \times 2$ systems out of any cyclic division algebra of degree n over a number field F and any quaternion division algebra over the same number field F if n odd. If n is even, we provided a condition for the code to be fully diverse. We found examples how to build rate-2 fully diverse STBCs with NVD for a 6×2 MIDO system. The codes obtained this way have a lot of zero entries if $m > 2$, i.e. if we look at numbers of antennas higher than used for the 4×2 case, which is not desirable and should be improved.

If the base field F we choose for our associative tensor product division algebras A is $F = \mathbb{Q}$ or a quadratic imaginary number field, all constructed fully diverse codes with $\gamma \in \mathcal{O}_F$, $\theta \in \mathcal{O}_K$ will automatically have NVD. Hence they are DMT-optimal for their respective MIDO system.

References

[1] N. Markin, F. Oggier, "Iterated Space-Time Code Constructions from Cyclic Algebras," arxiv:1205.5134v2 [cs.IT], 2013.

[2] K. P. Srinath, B. S. Rajan, "Fast decodable MIDO codes with large coding gain", online at archiv:1208.1593v3[cs.IT], 2013.

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

[4] F. Oggier, R. Vehkalahti, C. Hollanti, "Fas-decodable MIDO codes from crossed product algebras," ISIT 2010, Austin, Texas, June 2010.

[5] 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.

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

[7] N. Markin, F. Oggier, "Iterated MIDO Space-Time Code Constructions," 49th Annual Allerton Conference on Communication, Control, and Computing, 2011, 539-544.

[8] G. R. Jithamitra, B. S. Rajan, "Minimizing the complexity of fast-sphere decoding of STBCs," IEEE Int. Symposium on Information Theory Proceedings (ISIT), 2011.

[9] 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

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

[11] A. Steele, S. Pumplün, F. Oggier, "MIDO space-time codes from associative and non-associative cyclic algebras," Information Theory Workshop (ITW) 2012 IEEE (2012), 192-196.

[12] N. Markin, T. Unger, "Quadratic forms and space-time block Codes from generalized quaternion and biquaternion algebras," IEEE Trans. Inform. Theory 57 (9)(2011), 6148-6156.

[13] S. Pumplün, T. Unger, "Space-time block codes from nonassociative division algebras," Advances in Mathematics of Communications 5 (3) (2011), 609-629.

[14] N. Jacobson, "Finite-dimensional division algebras over fields," Springer Verlag, Berlin-Heidelberg-New York, 1996.

[15] G. Berhuy, F. Oggier, *Introduction to Central Simple Algebras and their Applications to Wireless Communication.*, AMS Surveys and Monographs, 2013.
[16] S. Pumplün, V. Astier, "Nonassociative quaternion algebras over rings", Israel J. Math. 155 (2006), 125–147.
[17] W.C. Waterhouse, "Nonassociative quaternion algebras", Algebras Groups Geom. 4 (1987), no. 3, 365–378.
[18] R.D. Schafer, "An Introduction to Nonassociative Algebras", Dover Publ., Inc., New York, 1995.
[19] A. Steele, "Some new classes of algebras," PhD Thesis, Nottingham, 2013.
[20] H. Jafarkhani, "A quasi-orthogonal space-time block code," IEEE Trans. on Communications 49 (1),January 2001.
[21] S. Pumplün, "How to obtain algebras used for fast decodable space-time block codes", preprint, 2013.
[22] S. Pumplün, A. Steele, "Iterating algebras", in preparation.

E-mail address: susanne.pumpluen@nottingham.ac.uk

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom