HOW TO OBTAIN DIVISION ALGEBRAS USED FOR FAST-DECODABLE SPACE-TIME BLOCK CODES

Susanne Pumplün

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

Abstract. We present families of unital algebras obtained through a doubling process from a cyclic central simple algebra $D = (K/F, \sigma, c)$, employing a K-automorphism τ and an element $d \in D^\times$. These algebras appear in the construction of iterated space-time block codes. We give conditions when these iterated algebras are division which can be used to construct fully diverse iterated codes. We also briefly look at algebras (and codes) obtained from variations of this method.

1. Introduction

Space-time coding is used for reliable high rate transmission over wireless digital channels with multiple antennas at both the transmitter and receiver ends. From the mathematical point of view, designing space-times codes means to design well-behaved families of matrices over the complex numbers, often using the representation matrix of the left multiplication of an algebra. Central simple associative division algebras over number fields, in particular cyclic division algebras, have been used highly successfully to systematically build space-time block codes (cf. for instance [1], [2], [3], [4], [5], [6], [7]). Nonassociative division algebras over number fields, like nonassociative quaternion algebras or cyclic algebras, can also be used in code design, see for instance [8], [9] or [10].

In [11], Markin and Oggier propose an ad hoc code construction to build $2n \times 2n$ asymmetric space-time block codes 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 inherit fast-decodability from the code $\mathcal{D}$. The idea is to use well performing codes $\mathcal{D}$ in the construction and double them, hoping not to lose much if anything of their good performance in the process.

The iterated construction [11] starts with a cyclic division algebra D over a number field F and a $\mathbb{Q}$-automorphism τ of K, where K is a maximal subfield of the F-algebra D. It

1991 *Mathematics Subject Classification.* Primary: 17A35, 94B05.

Key words and phrases. Space-time block code,fast-decodable, asymmetric, non-associative division algebra, iterated code.

employs a map

$$\alpha_\theta : \mathcal{D} \times \mathcal{D} \to \mathrm{Mat}_2(K), \tag{1}$$

$$\alpha_\theta : (X, Y) \mapsto \begin{bmatrix} X & \Theta\tau(Y) \\ Y & \tau(X) \end{bmatrix}, \tag{2}$$

where $\mathcal{D} = \lambda(D) \subset \mathrm{Mat}_n(K)$ is the canonical embedding of elements of the algebra D into $\mathrm{Mat}_n(K)$ via left regular representation, and where $\Theta \in \mathcal{D}$, i.e., $\theta \in D$ is identified with its matrix representation $\Theta = \lambda(\theta)$. For instance,

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

if $D = \mathrm{Cay}(K, d) = K \oplus K$ is a quaternion algebra with canonical involution σ and $\theta = \theta_0 + j\theta_1 \in D$. $\tau(X)$ simply is the matrix obtained from X by applying τ to each entry of X. With the right choice of τ and $\theta \in F_0 = \mathrm{Fix}(\tau) \cap F$, the matrices in $\alpha_\theta(\mathcal{D} \times \mathcal{D})$ form a $\mathbb{Q}$-algebra of finite dimension $2n^2[F : \mathbb{Q}]$ and are the representation of a central simple associative algebra.

In this paper we present the algebras behind this iteration process for any choice of θ and τ: the codebooks $\alpha_\theta(\mathcal{D} \times \mathcal{D})$ consist of the matrix representations of left multiplication of certain algebras over F_0 we will call *iterated algebras*. If $\theta \in D \setminus F_0$, these algebras are nonassociative. By putting the code constructions into a general algebraic framework, we are able to systematically investigate the codes obtained through the matrices of the left multiplication in a suitable iterated algebra. We also extend the existing iteration process for codes to include the case of employing the map

$$\beta_\theta : \mathcal{D} \times \mathcal{D} \to \mathrm{Mat}_{2n}(K),$$

$$\beta_\theta : (X, Y) \mapsto \begin{bmatrix} X & \tau(Y)\Theta \\ Y & \tau(X) \end{bmatrix} \tag{3}$$

instead of α_θ. We then give conditions on when a code α_θ resp. β_θ is fully diverse without having to restrict the choice of θ to the field F.

The paper is organized as follows: Let F always be a field of characteristic not 2. Notations and basic definitions used are given in Section 2. Starting with a cyclic central simple algebra $D = (K/F, \sigma, c)$ over F of degree n, we define doubling processes involving D, $\tau \in \mathrm{Aut}(K)$ and $d \in D^\times$ in Section 3. In order to do so, we canonically extend τ to a map $\widetilde{\tau}$ on D. Depending on where d is placed, these doublings yield new unital algebras $\mathrm{It}_l(D, \tau, d)$, $\mathrm{It}_m(D, \tau, d)$ or $\mathrm{It}_r(D, \tau, d)$ over F_0, which have $D = (K/F, \sigma, c)$ as a subalgebra. We call them *iterated algebras*. If τ and σ commute, an iterated algebra is division if D is division and $N_{D/F}(d) \neq N_{D/F}(z\widetilde{\tau}(z))$ for all $z \in D$. In special cases, some iterated algebras are subalgebras of the tensor product of the cyclic algebra D and a nonassociative quaternion

algebra. The connection between iterated algebras and code constructions is explored in Section 4. Most notably, the iterated codes explicitly constructed in the literature so far all require (apart from one example), apart from $\tau(c) = c$ and that τ and σ commute, also that $d \in F^\times$, so that $d \notin F$ generally is not considered. Since the considerations in [11], Section IV.A., on iterating the Silver code given by $D = (-1,-1)_F$, $F = \mathbb{Q}(\sqrt{-7})$, generalize to the case that $\theta \in F(i)$ and not in F, the code $\alpha_\theta(\mathcal{D} \times \mathcal{D})$ inherits fast-decodability from the Silver code, as Lemma 15 in [11] still holds in this setting. This supports the explicit calculation in [11], Section IV.A., that the decoding complexity for $\theta = i$ is $O(|S|^{13})$. In particular, we show in Exampe 16 that the code built and simulated in [11], Section IV.A, with $\theta = i$, is indeed fully diverse and has NVD. Moreover, in Example 17 we build a code which the same ML-decoding complexity as the 4×2 SR-code discussed for instance in [12] and is fast-decodable. Iterated algebras inside the tensor product of a cyclic division algebra and a (nonassociative) quaternion algebra are considered in Section 5. These are the algebras dealt with in the examples for iterated code constructions of [11]. For the sake of completeness, we briefly consider variations of this doubling process in Section 6, like a generalized Cayley-Dickson doubling of D based on the same idea, using $\widetilde{\tau}$ and $d \in D$ when defining the multiplication. For D a quaternion algebra, $\widetilde{\tau}$ is never the standard involution on D. The resulting algebras are division under the same conditions as the iterated algebras.

2. Preliminaries

2.1. **Nonassociative algebras.** Let F be a field. By "F-algebra" we mean a finite dimensional unital nonassociative algebra over F.

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 ([17], pp. 15, 16).

For an F-algebra A, associativity in A is measured by the *associator* $[x,y,z] = (xy)z - x(yz)$. The *left nucleus* of A is defined as $\mathrm{Nuc}_l(A) = \{x \in A \,|\, [x,A,A] = 0\}$, the *middle nucleus* of A is defined as $\mathrm{Nuc}_m(A) = \{x \in A \,|\, [A,x,A] = 0\}$ and the *right nucleus* of A is defined as $\mathrm{Nuc}_r(A) = \{x \in A \,|\, [A,A,x] = 0\}$. Their intersection $\mathrm{Nuc}(A) = \{x \in A \,|\, [x,A,A] = [A,x,A] = [A,A,x] = 0\}$ is the *nucleus* of A. 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 $\mathrm{Nuc}(A)$.

2.2. **Nonassociative quaternion division algebras.** A *nonassociative quaternion algebra* is a four-dimensional F-algebra A whose nucleus is a separable quadratic field extension of F [19]. Let S be a quadratic étale algebra over F with canonical involution σ. For every invertible $b \in S \setminus F$, the vector space $\mathrm{Cay(S, b)} = \mathrm{S} \oplus \mathrm{S}$ becomes a nonassociative quaternion algebra over F with unit element $(1,0)$ and nucleus S under the multiplication

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

for $u, u', v, v' \in S$. Given any nonassociative quaternion algebra A over F with nucleus S, there exists an element $b \in S \setminus F$ such that $A \cong \mathrm{Cay}(S, b)$ [16], Lemma 1.

Nonassociative quaternion algebras are neither power-associative nor quadratic. $\mathrm{Cay}(S, b)$ is a division algebra if and only if S is a separable quadratic field extension of F.

Nonassociative quaternion division algebras were first discovered by Dickson [15] and Albert [14].

2.3. **Cyclic algebras.** Let K/F be a cyclic Galois extension of degree n, with Galois group $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ and $c \in F^\times$. A *cyclic algebra* $D = (K/F, \sigma, c)$ of degree n over F is an n-dimensional K-vector space

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

with multiplication given by the relations

$$e^n = c, \ xe = e\sigma(x), \tag{4}$$

for all $x \in K$. We call $\{1, e, e^2, \ldots, e^{n-1}\}$ the *standard basis* of the right K-vector space D.

The left multiplication λ_y of elements of D with $y = y_0 + ey_1 + \cdots + e^{n-1}y_{n-1} \in D$ induces a representation $\lambda : D \to \mathrm{Mat}_n(K)$ which maps elements of D to matrices of the form

$$\begin{bmatrix} y_0 & c\sigma(y_{n-1}) & c\sigma^2(y_{n-2}) & \ldots & c\sigma^{n-1}(y_1) \\ y_1 & \sigma(y_0) & c\sigma^2(y_{n-1}) & \ldots & c\sigma^{n-1}(y_2) \\ \vdots & & \vdots & & \vdots \\ y_{n-2} & \sigma(y_{n-3}) & \sigma^2(y_{n-4}) & \ldots & c\sigma^{n-1}(y_{n-1}) \\ y_{n-1} & \sigma(y_{n-2}) & \sigma^2(y_{n-3}) & \ldots & \sigma^{n-1}(y_0) \end{bmatrix} \tag{5}$$

where $y_0, \ldots, y_{n-1} \in K$. Obviously, we have $X \pm Y \in \lambda(D)$ for all $X, Y \in \lambda(D)$. Thus $\mathcal{D} = \lambda(D)$ is a linear codebook. If D is division, the codebook $\mathcal{D} = \lambda(D)$ is fully diverse. In the following, we often identify elements $x \in D$ with their standard matrix representation $X = \lambda(x) \in \mathcal{D}$ and use upper case letters for them.

For the standard terminology for code design we use, we refer the reader to [11].

3. Iterated algebras

Let K/F be a Galois field extension of F of degree n with $\mathrm{Gal}(K/F) = \langle \sigma \rangle$. Let $D = (K/F, \sigma, c)$ be a cyclic algebra over F of degree n with norm $N_{D/F}$, $\tau \in \mathrm{Aut}(K)$ and $F_0 = \mathrm{Fix}(\tau) \cap F$. For $x = x_0 + ex_1 + e^2x_2 + \cdots + e^{n-1}x_{n-1} \in D$, define the map $\widetilde{\tau} : D \to D$ via

$$\widetilde{\tau}(x) = \tau(x_0) + e\tau(x_1) + e^2\tau(x_2) + \cdots + e^{n-1}\tau(x_{n-1}).$$

$\widetilde{\tau}$ is $\mathrm{Fix}(\tau)$-linear. Let $d \in D^\times$. Then the $2n$-dimensional F-vector space $D \oplus D$ can be made into a unital algebra over F_0 via the multiplication

$$(u, v) \cdot_l (u', v') = (uu' + d\widetilde{\tau}(v)v', vu' + \widetilde{\tau}(u)v')$$

for $u, u', v, v' \in D$. The unit element is given by $1 = (1, 0)$. An algebra obtained from such a doubling of D is denoted by $\mathrm{It}_l(D, \tau, d)$.

If $d \in D^\times$ is not contained in F, we also define multiplications

$$(u, v) \cdot_m (u', v') = (uu' + \widetilde{\tau}(v)dv', vu' + \widetilde{\tau}(u)v')$$

resp.

$$(u, v) \cdot_r (u', v') = (uu' + \widetilde{\tau}(v)v'd, vu' + \widetilde{\tau}(u)v')$$

on $D \oplus D$ and denote the corresponding F_0-algebras by $\mathrm{It}_m(D, \tau, d)$, resp. $\mathrm{It}_r(D, \tau, d)$. $\mathrm{It}_l(D, \tau, d)$, $\mathrm{It}_m(D, \tau, d)$ and $\mathrm{It}_r(D, \tau, d)$ are called *iterated algebras*.

If $d \in K$, then the $2n$-dimensional F-vector space $K \oplus K$ can be made into an algebra over F_0 with unit element $1 = (1, 0)$ via the multiplication

$$(u, v)(u', v') = (uu' + d\tau(v)v', vu' + \tau(u)v')$$

for $u, u', v, v' \in K$. We denote the algebra by $\mathrm{It}(K, \tau, d)$. K is a subalgebra of $\mathrm{It}(K, \tau, d)$. Note that for $d \in K$, $\mathrm{It}(K, \tau, d)$ is a subalgebra of $\mathrm{It}_l(D, \tau, d)$, $\mathrm{It}_m(D, \tau, d)$ and $\mathrm{It}_r(D, \tau, d)$.

Remark 1. (i) Let $K/\mathrm{Fix}(\tau)$ be a Galois field extension of degree 2. Then $\mathrm{It}(K, \tau, d)$ is isomorphic to the (associative or nonassociative) quaternion algebra $(K/\mathrm{Fix}(\tau), \tau, d) = \mathrm{Cay}(K, d)$. If $d \in \mathrm{Fix}(\tau)^\times$, $(K/\mathrm{Fix}(\tau), \sigma, d)$ is an associative quaternion algebra, if $d \in K \setminus \mathrm{Fix}(\tau)$, it is a nonassociative quaternion algebra (for the definition, see [19]).
(ii) (Steele) For $u, v, u', v' \in D$, multiplication in $\mathrm{It}_l(D, \tau, d)$ can be written as

$$(u, v) \cdot_l (u', v') = (\begin{bmatrix} u & d\widetilde{\tau}(v) \\ v & \widetilde{\tau}(u) \end{bmatrix} \begin{bmatrix} u' \\ v' \end{bmatrix})^T,$$

and multiplication in $\mathrm{It}_m(D, \tau, d)$ as

$$(u, v) \cdot_m (u', v') = (\begin{bmatrix} u & \widetilde{\tau}(v)d \\ v & \widetilde{\tau}(u) \end{bmatrix} \begin{bmatrix} u' \\ v' \end{bmatrix})^T.$$

If $\tau(c) = c$, the representation matrices of the left multiplication of $\mathrm{It}_l(D, \tau, d)$ appear in the iterated space-time code construction of [11], but were not recognized as matrices representing left multiplication in a nonassociative algebra.

In the following, let

$$A_l = \mathrm{It}_l(D, \tau, d), A_m = \mathrm{It}_m(D, \tau, d) \text{ or } A_r = \mathrm{It}_r(D, \tau, d).$$

Clearly, D is a subalgebra of A_l, A_m and A_r. Put $f = (0, 1_D)$. Then $f^2 = d$ and the multiplication in, for instance, $\mathrm{It}_l(D, \tau, d)$ can also be written as

$$(u + fv) \cdot_l (u' + fv') = (uu' + d\widetilde{\tau}(v)v') + f(vu' + \widetilde{\tau}(u)v'))$$

for $u, u', v, v' \in D$. We call

$$\{1, e, e^2, \ldots, e^{n-1}, f, fe, fe^2, \ldots, fe^{n-1}\}$$

the *standard basis* of the right K-vector space A_i, $i \in \{l, r, m\}$.

For $i \in \{l, r, m\}$, A_i is a free right D-modules of rank 2, since $x(bc) = (xb)c$ for all $b, c \in D$ and $x \in A_i$. After a choice of D-basis, e.g. $\{1, f\}$, we can embed $\mathrm{End}_D(A_i)$ into the module $\mathrm{Mat}_2(D)$.

Furthermore, for $i \in \{l, m\}$ left multiplication L_x with $x \in A_i$ is a right D-module endomorphism, so that we have a well-defined additive map

$$L : A_i \to \mathrm{End}_D(A_i) \hookrightarrow \mathrm{Mat}_2(D), \quad x \mapsto L_x \mapsto L(x) = X$$

which is injective if A_i is division.

Lemma 2. *(i) For $i \in \{l, r, m\}$, A_i is not power-associative if $\widetilde{\tau}(d) \neq d$. In particular, if $d \in K$ then A_i is not power-associative if $d \notin \mathrm{Fix}(\tau)$.*
(ii) Let $B = (K'/F, \sigma', c')$ and $D = (K/F, \sigma, c)$ be two cyclic algebras over F and $f : D \to B$ an algebra isomorphism. Suppose τ is a K-automorphism and τ' a K'-automorphism, such that $f(\widetilde{\tau}(u)) = \widetilde{\tau'}(f(u))$ for all $u \in D$. Let $a \in B^\times$. For $u, v \in D$, the map

$$G : D \oplus D \to B \oplus B, \quad G(u, v) = (f(u), a^{-1} f(v))$$

defines the following algebra isomorphisms:

$$\mathrm{It}_l(D, \tau, d) \cong \mathrm{It}_l(B, \tau', \widetilde{\tau'}(a) a f(d)),$$

$$\mathrm{It}_m(D, \tau, d) \cong \mathrm{It}_m(B, \tau', \widetilde{\tau'}(a) a f(d)),$$

and

$$\mathrm{It}_r(D, \tau, d) \cong \mathrm{It}_r(B, \tau', \widetilde{\tau'}(a) f(d) a).$$

In particular, for $a \in \mathrm{Fix}(\tau)^\times$,

$$\mathrm{It}_l(D, \tau, d) \cong \mathrm{It}_l(D, \tau, a^2 d),$$

$$\mathrm{It}_m(D, \tau, d) \cong \mathrm{It}_m(D, \tau, a^2 d)$$

and

$$\mathrm{It}_r(D, \tau, d) \cong \mathrm{It}_r(D, \tau, a^2 d).$$

Proof. (i) We have $f^2 = (d, 0)$ and $f f^2 = (0, \widetilde{\tau}(d))$ while $f^2 f = (0, d)$. Therefore A is not power-associative, if $\widetilde{\tau}(d) \neq d$, i.e. for $d \in K$ if $d \notin \mathrm{Fix}(\tau)$.
(ii) is a straightforward calculation. □

Proposition 3. *Suppose τ commutes with σ. Let $D' = (K/F, \sigma, \tau(c))$ with standard basis $\{1, e', \ldots, e'^{n-1}\}$. For $y = y_0 + e y_1 + \cdots + e^{n-1} y_{n-1} \in D$ define a corresponding element $y_{D'} = y_0 + e' y_1 + \cdots + e'^{n-1} y_{n-1} \in D'$. Then*

$$N_{D/F}(\widetilde{\tau}(y)) = \tau(N_{D'/F}(y_{D'})).$$

If $c \in \mathrm{Fix}(\tau)$ then

$$N_{D/F}(\widetilde{\tau}(y)) = \tau(N_{D/F}(y)),$$

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

Proof. The left multiplication of elements of $D = (K/F, \sigma, c)$ with $y = y_0 + ey_1 + \cdots + e^{n-1}y_{n-1} \in D$ induces a representation $\lambda : D \to \mathrm{Mat}_n(K)$ which maps elements of D to matrices of the form

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

where $y_0, \dots, y_{n-1} \in K$. We have $\det(Y) = N_{D/F}(y)$. Thus

$$\begin{aligned} & N_{D/F}(\widetilde{\tau}(y)) \\ =& \det\left(\begin{bmatrix} \tau(y_0) & c\sigma(\tau(y_{n-1})) & c\sigma^2(\tau(y_{n-2})) & \dots & c\sigma^{n-1}(\tau(y_1)) \\ \tau(y_1) & \sigma(\tau(y_0)) & c\sigma^2(\tau(y_{n-1})) & \dots & c\sigma^{n-1}(y_2) \\ \vdots & & \vdots & & \vdots \\ \tau(y_{n-2}) & \sigma(\tau(y_{n-3})) & \sigma^2(\tau(y_{n-4})) & \dots & c\sigma^{n-1}(\tau(y_{n-1})) \\ \tau(y_{n-1}) & \sigma(\tau(y_{n-2})) & \sigma^2(\tau(y_{n-3})) & \dots & \sigma^{n-1}(\tau(y_0)) \end{bmatrix} \right) \\ =& \tau\left(\begin{bmatrix} y_0 & \tau(c)\sigma(y_{n-1}) & \tau(c)\sigma^2(y_{n-2}) & \dots & \tau(c)\sigma^{n-1}(y_1) \\ y_1 & \sigma(y_0) & \tau(c)\sigma^2(y_{n-1}) & \dots & \tau(c)\sigma^{n-1}(y_2) \\ \vdots & & \vdots & & \vdots \\ y_{n-2} & \sigma(y_{n-3}) & \sigma^2(y_{n-4}) & \dots & \tau(c)\sigma^{n-1}(y_{n-1}) \\ y_{n-1} & \sigma(y_{n-2}) & \sigma^2(y_{n-3}) & \dots & \sigma^{n-1}(y_0) \end{bmatrix} \right) \\ =& \tau(N_{D'/F}(y_{D'})). \end{aligned} \tag{6}$$

The rest is trivial. □

Remark 4. If $D = (a, c)_F$ is a quaternion algebra, $D' = (a, \tau(c))_F$, we have $N_{D/F}(\widetilde{\tau}(x)) = N_{D/F}(\tau(x_0) + j\tau(x_1)) = N_{K/F}(\tau(x_0)) - cN_{K/F}(\tau(x_1)) = \tau(x_0)\sigma(\tau(x_0)) - c\tau(x_1)\sigma(\tau(x_1)) = \tau(x_0)\tau(\sigma(x_0)) - c\tau(x_1)\tau(\sigma(\tau(x_1)) = \tau(N_{K/F}(\tau(x_0))) - \tau(\tau(c)N_{K/F}(\tau(x_1))) = \tau(N_{D'/F}(x_{D'}))$ as special case.

With this result, we are now able to prove:

Theorem 5. *Let D be a cyclic division algebra of degree n over F and $d \in D^\times$. Suppose $\tau \in \mathrm{Aut}(K)$ commutes with σ. Let $i \in \{l, r, m\}$.*
(i) A_i is a division algebra if

$$N_{D/F}(d) \neq N_{D/F}(z\widetilde{\tau}(z))$$

for all $z \in D$. Conversely, if A_i is a division algebra then $d \neq z\widetilde{\tau}(z)$ for all $z \in D^\times$.
(ii) Suppose $c \in \mathrm{Fix}(\tau)$. Then:
(a) A_i is a division algebra if and only if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.

(b) A_i is a division algebra if $N_{D/F}(d) \neq a\tau(a)$ for all $a \in N_{D/F}(D^\times)$.
(iii) Suppose $F \subset \mathrm{Fix}(\tau)$. Then A_i is a division algebra if $N_{D/F}(d) \notin N_{D/F}(D^\times)^2$.

Proof. Consider A_l (the other two cases of iterated algebras work analogously unless stated otherwise).
(i) Suppose

$$(0,0) = (u,v) \cdot_l (u',v') = (uu' + d\widetilde{\tau}(v)v', vu' + \widetilde{\tau}(u)v')$$

for $u, v, u', v' \in D$. This is equivalent to

$$uu' + d\widetilde{\tau}(v)v' = 0 \text{ and } vu' + \widetilde{\tau}(u)v' = 0. \tag{7}$$

Assume $v' = 0$, then $uu' = 0$ and $vu' = 0$. Hence either $u' = 0$ and so $(u', v') = 0$ or $u' \neq 0$ and $u = v = 0$. Also, if $v = 0$ then $uu' = 0$ and $\widetilde{\tau}(u)v' = 0$, thus $u = 0$ and $(u, v) = 0$, or $(u', v') = 0$ and we are done.

So let $v' \neq 0$ and $v \neq 0$. Then $v' \in D^\times$ and $vu' = -\widetilde{\tau}(u)v'$ yields $\widetilde{\tau}(u) = -vu'v'^{-1}$, i.e. $u = -\widetilde{\tau}(vu'v'^{-1})$. Substituted into the first equation this gives

$$\widetilde{\tau}(vu'v'^{-1})u' = d\widetilde{\tau}(v)v'.$$

Applying the norm $N_{D/F}$ to both sides of this equation we get

$$N_{D/F}(\widetilde{\tau}(vu'v'^{-1}))N_{D/F}(u') = N_{D/F}(d)N_{D/F}(\widetilde{\tau}(v))N_{D/F}(v').$$

Employing Proposition 3, we obtain

$$N_{D/F}(d)\tau(N_{D'/F}(v_{D'}))N_{D/F}(v') = \tau(N_{D'/F}(v_{D'}))\tau(N_{D'/F}(u'_{D'}))\tau(N_{D'/F}(v'^{-1}_{D'}))N_{D/F}(u'),$$

so that

$$\begin{aligned} N_{D/F}(d) &= N_{D/F}(u')N_{D/F}(v')^{-1}\tau(N_{D'/F}(u'_{D'})N_{D'/F}(v'^{-1}_D)) \\ &= N_{D/F}(u'v'^{-1})\tau(N_{D'/F}(u'_D v'^{-1}_D)) = N_{D/F}(u'v'^{-1})N_{D/F}(\widetilde{\tau}(u'v'^{-1})) \end{aligned} \tag{8}$$

We conclude that A_l is division for all $d \in D^\times$ such that

$$N_{D/F}(d) \neq N_{D/F}(z\widetilde{\tau}(z))$$

for all $z \in D$. Conversely, if there is $z \in D^\times$ such that $d = z\widetilde{\tau}(z)$, then

$$(z,1)(-\widetilde{\tau}(z),1) = (-z\widetilde{\tau}(z) + d, -\widetilde{\tau}(z) + \widetilde{\tau}(z)) = (0,0),$$

so A_l contains zero divisors. We conclude that if A_l is division then $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
(ii) (a) From (7) we obtain for $v' \neq 0$ that $u' = -v^{-1}\widetilde{\tau}(u)v'$ for any of the three types of algebras.
For A_l, hence $uv^{-1}\widetilde{\tau}(u)v' = d\widetilde{\tau}(v)v'$. Rearranging gives $d = uv^{-1}\widetilde{\tau}(u)\widetilde{\tau}(v^{-1}) = uv^{-1}\widetilde{\tau}(uv^{-1})$ since $c \in \mathrm{Fix}(\tau)$. Therefore A_l is division if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
For A_m this gives $uv^{-1}\widetilde{\tau}(u)v' = \widetilde{\tau}(v)dv'$. Rearranging gives $d = \widetilde{\tau}(v^{-1})uv^{-1}\widetilde{\tau}(u) = \widetilde{\tau}(v^{-1})u\widetilde{\tau}(\widetilde{\tau}(v^{-1})u)$ since $c \in \mathrm{Fix}(\tau)$. Therefore A_m is division if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.

For A_r this gives $uv^{-1}\widetilde{\tau}(u)v' = \widetilde{\tau}(v)v'd$. Rearranging gives $d = v'^{-1}\widetilde{\tau}(v^{-1})uv^{-1}\widetilde{\tau}(u)v'$. Therefore A_r is a division algebra if $d \neq v^{-1}z\widetilde{\tau}(z)v$ for all $v, z \in D$.

Since by Lemma 2, we have $A_r \cong \mathrm{It}_r(D, \tau, v^{-1}dv)$ for all $v \in D^\times$, A_r is a division algebra iff $\mathrm{It}_r(D, \tau, v_0 dv_0^{-1})$ is division for all $v_0 \in D^\times$. Suppose A_r is not division, then $\mathrm{It}_r(D, \tau, v_0 dv_0^{-1})$ is not division, so we have $v_0 dv_0^{-1} = v^{-1}z\widetilde{\tau}(z)v$ for all $v, z \in D$ by the above calculation, in particular for $v = v_0$ which yields $d = z\widetilde{\tau}(z)$ for all $z \in D$. We conclude that A_r is a division algebra if and only if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
(b) If $c \in \mathrm{Fix}(\tau)$, then (8) becomes

$$N_{D/F}(d) = N_{D/F}(u'v'^{-1})\tau(N_{D/F}(u'v'^{-1})) \tag{9}$$

and so A_l is division if

$$N_{D/F}(d) \neq a\tau(a)$$

for all $a \in N_{D/F}(D)$.
(iii) If $F \subset \mathrm{Fix}(\tau)$, (9) becomes

$$N_{D/F}(d) = N_{D/F}(u'v'^{-1})\tau(N_{D'/F}(u'v'^{-1})) = N_{D/F}(u'v'^{-1})^2.$$

For the multiplications in A_m and A_r, the order of the factors in the first equation changes, which however does not affect the proofs. □

Proposition 6. *Let $K = F[x]/(f(x))$ be a Galois field extension of F of degree n with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Let $\tau \in \mathrm{Aut}(K)$ and suppose τ commutes with σ. Then*
(i) $N_{K/F}(\tau(x)) = \tau(N_{K'/F}(x_{K'}))$, where $K' = F[x]/(\tau(f(x)))$.
(ii) If $c \in \mathrm{Fix}(\tau)$ then $N_{K/F}(\tau(x)) = N_{K/F}(x)$.
(iii) $\mathrm{It}(K, \tau, d)$ is a division algebra for every $d \in K$, such that $N_{K/F}(d) \neq N_{K/F}(z\tau(z))$ for all $z \in K$.
(iv) If $c \in \mathrm{Fix}(\tau)$ then $\mathrm{It}(K, \tau, d)$ is a division algebra if and only if $d \neq z\widetilde{\tau}(z)$ for all $z \in K$.
(v) If $F \subset \mathrm{Fix}(\tau)$, then $\mathrm{It}(K, \tau, d)$ is a division algebra if $N_{K/F}(d) \notin N_{K/F}(K^\times)^2$.

This is proved analogously as Proposition 3 and Theorem 5.

Corollary 7. *Let $D = (K/F, \sigma, c)$ be a cyclic division algebra and $d \in D^\times$. Let $\tau \in \mathrm{Aut}(K)$ and suppose τ commutes with σ. Let $i \in \{l, r, m\}$.*
(i) A_i is a division algebra if $N_{D/F}(d) \notin N_{D/F}(D^\times)$ for all $z \in D^\times$.
(ii) Suppose $c \in \mathrm{Fix}(\tau)$.
(a) A_i is a division algebra if $N_{D/F}(d) \neq a\tau(a)$ for all $a \in F^\times$.
(b) For $d \in F^\times$, A_i is a division algebra if $d^2 \neq a\tau(a)$ for all $a \in F^\times$.
(iii) Suppose $F \subset \mathrm{Fix}(\tau)$.
(a) A_i is a division algebra if $N_{D/F}(d) \notin F^{\times 2}$.
(b) For $d \in F^\times$, A_i is a division algebra if $d \notin \pm N_{D/F}(D^\times)$.

Note that $d \notin \pm N_{D/F}(D^\times)$ is never the case for $F = \mathbb{Q}$ ([21], Theorem 1.4, p. 378).

Example 8. Let $K = F(\sqrt{a})$, $D = (a,b)_F = \mathrm{Cay}(K,b)$ be a division algebra and $\mathrm{Gal}(K/F) = \langle\sigma\rangle$.
(i) Let $F = \mathbb{Q}$ or $F = \mathbb{Q}(\sqrt{e})$ with $e > 0$. Suppose $a > 0$, $b > 0$. Then for every $d = x_1 i + x_2 j \in D$ with $(x_1, x_2) \neq (0,0)$ we know that $N_{D/F}(d) = -(ax_1^2 + bx_2^2) < 0$ and thus not a square in F, thus $\mathrm{It}_l(D,\sigma,d)$, $\mathrm{It}_m(D,\sigma,d)$ and $\mathrm{It}_r(D,\sigma,d)$ are division algebras over F.
(ii) Let $F = \mathbb{Q}$ and $a < 0$, $b < 0$. Then D is always a division algebra. $\mathrm{It}_l(D,\sigma,d)$, $\mathrm{It}_m(D,\sigma,d)$ and $\mathrm{It}_r(D,\sigma,d)$ are division algebras for all $d = x_0 + x_1 i + x_2 j + x_3 k$, such that the positive rational number $N_{D/\mathbb{Q}}(d) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$ is not a square in $\mathbb{Q}$.
(iii) Let $F = \mathbb{Q}$. If $D = (-1,p)_{\mathbb{Q}}$, $p \not\equiv 1(4)$ an odd prime, D is a division algebra and we may for instance choose $d = x_2 i + x_3 k$ with $x_2, x_3 \in \mathbb{Q}$, $(x_1, x_2) \neq (0,0)$. Then $N_{D/\mathbb{Q}}(d) = -p(x_2^2 + x_3^2) < 0$, hence $\mathrm{It}_l(D,\sigma,d)$, $\mathrm{It}_m(D,\sigma,d)$ and $\mathrm{It}_r(D,\sigma,d)$ are division algebras.

If $D = (-2,p)_{\mathbb{Q}}$, $p \equiv 1,3\ (8)$ an odd prime, D is a division algebra and we may again choose $d = x_2 i + x_3 k$ with $x_2, x_3 \in \mathbb{Q}$, $(x_1, x_2) \neq (0,0)$. Then $N_{D/\mathbb{Q}}(c) = -(px_2^2 + 2px_3^2) < 0$, hence $\mathrm{It}_l(D,\sigma,d)$, $\mathrm{It}_m(D,\sigma,d)$ and $\mathrm{It}_r(D,\sigma,d)$ are division algebras.

We obtain the following more general rule:

Lemma 9. *Let F be an ordered field (such that -1 is in particular not a square) and $(a,b)_F$ a division algebra over F with $a < 0$ and $b > 0$.*
(i) $\mathrm{It}_l(D,\sigma,d)$, $\mathrm{It}_m(D,\sigma,d)$ and $\mathrm{It}_r(D,\sigma,d)$ are division algebras, for every $d = x_2 i + x_3 k \in D$ with $(x_1, x_2) \neq (0,0)$.
(ii) Suppose τ commutes with σ and $F \subset \mathrm{Fix}(\tau)$. Then $\mathrm{It}_l(D,\tau,d)$, $\mathrm{It}_m(D,\tau,d)$ and $\mathrm{It}_r(D,\tau,d)$ are division algebras, for every $d = x_2 i + x_3 k \in D$ with $(x_1, x_2) \neq (0,0)$.

Proof. We have $N_{D/F}(d) = -b(x_2^2 - ax_3^2) < 0$. □

4. Connection with iterated codes

In the following, let K/F be a cyclic Galois extension of degree n with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Let $D = (K/F, \sigma, c)$ be a cyclic associative division algebra of degree n over F and $d \in D^\times$. Let τ be an automorphism of K such that $\tau(c) = c$ and $\tau\sigma = \sigma\tau$.

Write $d = d_0 + ed_1 + \cdots + e^{n-1}d_{n-1}$ ($d_i \in K$) and identify d with its matrix representation $\Theta = \lambda(d) \in \mathcal{D} = \lambda(D)$ which is given by a matrix as in (5) with entries y_i replaced by d_i. In the iterative construction of [11], the map

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

$$\alpha_d : (X,Y) \mapsto \begin{bmatrix} X & \Theta\tau(Y) \\ Y & \tau(X) \end{bmatrix} \tag{10}$$

is used to build a new code $\alpha_d(\mathcal{D}\times\mathcal{D})$ out of $\mathcal{D}$, where in the top right block we mean matrix multiplication. The matrices in $\alpha_d(\mathcal{D}\times\mathcal{D})$ turn out to be the matrices of left multiplication in $A_l = \mathrm{It}_l(D,\tau,d)$, provided that $\tau(c) = c$.

An iterated algebra A_i, $i \in \{l,m,r\}$, is a K-vector space. After a choice of K-basis for A_i, we can embed $\mathrm{End}_K(A_i)$ into the vector space $\mathrm{Mat}_n(K)$.

For $A_l = \mathrm{It}_l(D,\tau,d)$ and $A_m = \mathrm{It}_m(D,\tau,d)$, left multiplication $\lambda_x : y \mapsto xy$ with an element x is a K-linear map (since $(xy)a = x(ya)$ for all $x,y \in A_i$, $a \in K$, $i \in \{l,m\}$).

So consider A_i as a right K-vector space and assume that A_i is a division algebra, $i \in \{l,m\}$. Since $\lambda_x(y) = \lambda_{x'}(y)$ for all $y \in A_i$ implies $(x-x')y = 0$ for all $y \in A_i$ and thus $x = x'$, $\lambda : A_i \hookrightarrow \mathrm{End}_K(A_i), x \mapsto \lambda_x$ is a well-defined injective additive map for $i \in \{l,m\}$.

Thus we get an injective additive map

$$\lambda : A_i \hookrightarrow \mathrm{Mat}_r(K), \quad x \mapsto X,$$

where $X = \lambda(x)$ is the matrix representing left multiplication with x. $\mathcal{A}_i = \lambda(A_i)$ constitutes a *linear codebook*, since for all $X, X' \in \lambda(A_i)$, we have $X \pm X' = \lambda(x) \pm \lambda(x') = \lambda(x \pm x') \in \lambda(A_i)$. We point out that the fact that a nonassociative algebra is division does not automatically imply that there is an associated fully diverse codebook $\mathcal{A}_i = \lambda(A_i)$ one can obtain from the matrices representing its left representation. This is only true in certain cases and turns out to be correct for the codes obtained from left multiplication in A_l or A_m treated in this paper.

For A_m (or $A_l = \mathrm{It}_l(D,\tau,d)$ with $d \in K^\times$) division, we have $(ax)y = a(xy)$ for all $a \in K$, $x,y \in A_i$, so

$$\lambda_{ax}(y) = (ax)y = a(xy) = a\lambda_x(y)$$

for all $x,y \in A_i$, $a \in K$, hence $\lambda : A_i \hookrightarrow \mathrm{End}_K(A_i), x \mapsto \lambda_x$ is even an embedding of K-vector spaces, $i \in \{l,m\}$. For our code constructions, however, it suffices that λ is an injective additive map.

Remark 10. It may be worth noting here that the codes described in the iterated code construction of [11] all have $d \in K^\times$, so that $\lambda(A_l)$ is a K-vector space. If one wants the matrices of the codebook to be a K-vector space for any $d \in D^\times$, it could make sense to rather look at the codes $\lambda(A_m)$ (where the matrix $\Theta = \lambda(d)$ appears on the right hand side in the right upper block matrix instead of on the left hand side). However, all considerations in [11] only require $\lambda(A_i)$ to be an F-vector space, which is true for $i \in \{l,m\}$.

To avoid confusion we will use upper case letters to denote the image of elements x 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 $\mathcal{A} = \lambda(A)$, $\mathcal{C} = \lambda(C)$, $\mathcal{D} = \lambda(D)$,...

Theorem 11. *Let $D = (K/F,\sigma,c)$ be a cyclic division algebra over F and $d \in D^\times$. Let $\tau \in \mathrm{Aut}(K)$ such that $\tau(c) = c$ and $\tau\sigma = \sigma\tau$.*

(i) The codebook defined by $\alpha_d(\mathcal{D}\times\mathcal{D})$,

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

is fully diverse, if and only if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
(ii) The codebook defined by $\beta_d(\mathcal{D}\times\mathcal{D})$,

$$\beta_d : (X,Y) \mapsto \begin{bmatrix} X & \tau(Y)\Theta \\ Y & \tau(X) \end{bmatrix},$$

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

Note that the condition $d \neq z\widetilde{\tau}(z)$ for all $z \in D$ is equivalent to $\Theta \neq Z\tau(Z)$ for all $Z \in \mathcal{D}$ here, since $\tau(c) = c$.

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

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

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

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

Thus

$$\begin{aligned} &\tau(X) - YX^{-1}\Theta\tau(Y) \\ =&\tau(\lambda(x)) - \lambda(y)\lambda(x^{-1})\lambda(\theta)\tau(\lambda(y)) \\ =&\lambda(\widetilde{\tau}(x)) - \lambda(y)\lambda(x^{-1})\lambda(\theta)\lambda(\widetilde{\tau}(y)) \\ =&\lambda(\widetilde{\tau}(x) - yx^{-1}\theta\widetilde{\tau}(y)) \end{aligned} \tag{11}$$

and so

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

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

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

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

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

and therefore takes values in F.

Conversely, if $d = z\widetilde{\tau}(z)$ for some $z \in D$ then $\alpha_d(Z, I_n)$ has determinant zero, because $\det(\tau(Z)) = \det(\det(\lambda(\widetilde{\tau}(z) - z^{-1}z\widetilde{\tau}(z))) = 0$.
(ii) is proved analogously as (i). Note that the determinant of $\beta_d(X, Y)$ can be written as

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

and thus takes values in F. □

Theorem 11 together with Theorem 5 and Remark 1(ii) yields:

Theorem 12. *Let $D = (K/F, \sigma, c)$ be a cyclic division algebra over F and $d \in D^\times$. Let $\tau \in \mathrm{Aut}(K)$ such that $\tau(c) = c$ and $\tau\sigma = \sigma\tau$. Then the following are equivalent:*
(i) A_l (resp., A_m) is a division algebra.
(ii) $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
(iii) The codebook $\alpha_d(\mathcal{D} \times \mathcal{D})$ (resp., $\beta_d(\mathcal{D} \times \mathcal{D})$) is fully diverse and its matrices are the representation matrices of left multiplication in A_l (resp., of left multiplication in A_m).

4.1. 4×4 **iterated codes from A_l.** Let $D = (a, b)_F$ and $K = F(\sqrt{a})$ with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Take the standard basis $1, j, f, fj$ of the K-vector space $A_l = \mathrm{It}_l(D, \tau, d)$. Let $\widetilde{\tau}(x) = \tau(x_0) + j\tau(x_1)$ for all $x = x_0 + jx_1 \in D$, where τ is an automorphism of K commuting with σ. and $\tau(b) = b$. Note that for $x = x_0 + jx_1$, $X = \lambda(x) \in Mat_2(K)$ is given by

$$\lambda(x) = \begin{bmatrix} x_0 & b\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix}.$$

For multiplication in A_l we have to observe that for all $x \in K$, $d = d_0 + jd_1 \in D^\times$, $d_i \in K$:

(1) $xf = f\tau(x)$,
(2) $(fx)j = (fj)\sigma(x)$,
(3) $((fj)x)f = j\sigma(d_0)\tau(x) + b\sigma(d_1)\tau(x)$,
(4) $((fj)x)j = fb\sigma(x)$,
(5) $(jx)f = (fj)\tau(x)$,
(6) $(fx)f = \sigma(d)\tau(x) = d_0\tau(x) + jd_1\tau(x)$,
(7) $x(fj) = (fj)\tau(\sigma(x))$,
(8) $(jx)(fj) = fb\tau(\sigma(x))$,
(9) $((fj)x)(fj) = d_0b\tau(\sigma(x)) + jd_1b\tau(\sigma(x))$,
(10) $(fx)(fj) = j\sigma(d_0)\tau(\sigma(x)) + b\sigma(d_1)\tau(\sigma(x))$,
(11) $x(fj) = (fj)\tau(\sigma(x))$.

Then the matrix representing left multiplication λ_x in A_l is given by

$$\begin{bmatrix} x_0 & b\sigma(x_1) & f_1 & f_2 \\ x_1 & \sigma(x_0) & f_3 & f_4 \\ y_0 & b\sigma(y_1) & \tau(x_0) & b\tau(\sigma(x_1)) \\ y_1 & \sigma(y_0) & \tau(x_1) & \tau(\sigma(x_0)) \end{bmatrix}$$

with $x_i, y_i \in K$ and

$$\begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix} = \begin{bmatrix} d_0\tau(x_2) + b\sigma(d_1)\tau(x_3) & b(d_0\sigma\tau(x_3) + \sigma(d_1)\sigma\tau(x_2)) \\ d_1\tau(x_2) + \sigma(d_0)\tau(x_3) & d_1b\sigma\tau(x_3) + \sigma(d_0)\sigma\tau(x_2) \end{bmatrix}.$$

Denote the linear codebook containing these matrices by $\mathcal{A}$.

For $X, Y \in Mat_2(K)$, $d = d_0 + jd_1 \in D$, $\Theta = \lambda(d)$, define

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

as in [11], where in the top right block we mean matrix multiplication, i.e.,

$$\Theta\tau(Y) = \begin{bmatrix} d_0\tau(x_2) + b\sigma(d_1)\tau(x_3) & b(d_0\sigma\tau(x_3) + \sigma(d_1)\sigma\tau(x_2)) \\ d_1\tau(x_2) + \sigma(d_0)\tau(x_3) & d_1b\sigma\tau(x_3) + \sigma(d_0)\sigma\tau(x_2) \end{bmatrix} = \begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix}.$$

Then

$$\alpha_d(\begin{bmatrix} x_0 & b\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix}, \begin{bmatrix} y_0 & b\sigma(y_1) \\ y_1 & \sigma(y_0) \end{bmatrix}) = \begin{bmatrix} x_0 & b\sigma(x_1) & f_1 & f_2 \\ x_1 & \sigma(x_0) & f_3 & f_4 \\ y_0 & b\sigma(y_1) & \tau(x_0) & \tau(b)\tau(\sigma(x_1)) \\ y_1 & \sigma(y_0) & \tau(x_1) & \tau(\sigma(x_0)) \end{bmatrix}, \tag{12}$$

therefore $\alpha_d(\mathcal{D} \times \mathcal{D}) = \mathcal{A}$, since $\tau(b) = b$. For $d \in K^\times$, the representation matrix of left multiplication in A_l is given by

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

with $x_i \in K = F(\sqrt{a})$.

As consequence of Theorem 12 we obtain:

Corollary 13. *Let $D = (a, b)_F$ be a division algebra, $K = F(\sqrt{a})$ with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ and $d \in D^\times$. Let $\tau \in \mathrm{Aut}(K)$ such that $\tau(b) = b$ and $\tau\sigma = \sigma\tau$. Let $A_l = \mathrm{It}_l(D, \tau, d)$. Then the following are equivalent:*
(i) The codebook $\mathcal{A}$ in (12) is fully diverse.
(ii) $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
(iii) A_l is a division algebra.
Moreover, the determinant of a matrix in $\mathcal{A}$ is an element of F.

Example 14. Let $F = \mathbb{Q}$ or $F = \mathbb{Q}(\sqrt{e})$ with $e > 0$. Let $L = F(\sqrt{a}, \sqrt{b})$, $K = F(\sqrt{b})$ with $\langle\sigma\rangle = \mathrm{Gal}(L/K)$ and $D = (a, c)_K$ a quaternion division algebra over K with $c \in F^\times$. Let $\langle\tau\rangle = \mathrm{Gal}(L/F(\sqrt{a}))$. For $d \in K^\times$, the representation matrix of left multiplication in

$\mathrm{It}_l((a,c)_K,\tau,d)$ (or $\mathrm{It}_m((a,c)_K,\tau,d)$, see below) has the form

$$\begin{bmatrix} x_0 & c\sigma(x_1) & d\tau(x_2) & dc\tau(\sigma(x_3)) \\ x_1 & \sigma(x_0) & d\tau(x_3) & d\tau(\sigma(x_2)) \\ x_2 & c\sigma(x_3) & \tau(x_0) & c\tau(x_1) \\ x_3 & \sigma(x_2) & \tau(x_1) & \tau(x_0) \end{bmatrix}.$$

For $d \in L \setminus F(\sqrt{b})$, it is

$$\begin{bmatrix} x_0 & c\sigma(x_1) & d\tau(x_2) & dc\tau(\sigma(x_3)) \\ x_1 & \sigma(x_0) & \sigma(d)\tau(x_3) & \sigma(d)\tau(\sigma(x_2)) \\ x_2 & c\sigma(x_3) & \tau(x_0) & c\tau(x_1) \\ x_3 & \sigma(x_2) & \tau(x_1) & \tau(x_0) \end{bmatrix}$$

with all $x_i \in L$ (using the standard basis both times). Let $c > 0$. Suppose $a > 0$, $c > 0$. Then for every $d = d_1 i + d_2 j \in D$ with $(d_1, d_2) \neq (0,0)$ (we do not need to restrict this to $d \in L^\times$, only that the matrix representing left multiplication loses its nice form for other d) we know that $N_{D/K}(d) = -(ad_1^2 + cd_2^2) < 0$, i.e $N_{D/K}(d) \notin N_{D/K}(D^\times)^2$. Hence $\mathrm{It}_l(D,\tau,d)$, $\mathrm{It}_m(D,\tau,d)$ and $\mathrm{It}_r(D,\tau,d)$ are division algebras over K.

Lemma 15. *For any $F = \mathbb{Q}(\sqrt{e})$, $x = a + \sqrt{e}b \in F$ with $a, b \in \mathbb{Q}$, we have*

$$F^{\times\,2} = \{(a^2 + eb^2) + 2ab\sqrt{e} \mid a, b \in \mathbb{Q}\}.$$

To obtain examples of well-performing (i.e., fast-decodable) codes from A_l, it seems preferable to choose F as a totally imaginary number field and $K \subset D$ such that the Galois automorphism σ of K/F commutes with complex conjugation, see [11], p. 21.

Example 16. (i) Let $D = (-1,-1)_F$ with $F = \mathbb{Q}(\sqrt{-7})$, $K = \mathbb{Q}(\sqrt{-7})(i)$ and $\sigma(x_0 + ix_1) = x_0 - ix_1$ for all $x_i \in F$ as in [11], Section IV.A. D is the division algebra over F used to construct the Silver Code.

$d = -17$ is not a square in K (loc. cit.) and by [11], Lemma 11, $\mathrm{It}_l(D,\sigma,-17)$ is a division algebra (associative in this case, see loc. cit.).

Suppose $d = i \in K \setminus F$. By Theorem 13, $\mathrm{It}_l(D,\sigma,i)$ is a division algebra if and only if $i \neq z\widetilde{\sigma}(z)$ for all $z \in D$. Now for $z = z_0 + jz_1$ we get

$$z\widetilde{\sigma}(z) = N_{K/F}(z_0) - \sigma(z_1)^2 + j\sigma(z_0)T_{K/F}(z_1)$$

and a straightforward calculation shows that $i \neq z\widetilde{\sigma}(z)$ for all $z \in D$. Thus the the iterated Silver code built in [11], Section IV.A., arising from α_i, i.e. given by

$$\begin{bmatrix} c & -\sigma(d) & i\sigma(e) & -if \\ d & \sigma(c) & -i\sigma(f) & -ie \\ e & -\sigma(f) & \sigma(c) & -d \\ f & \sigma(e) & \sigma(d) & c \end{bmatrix},$$

with $c,d,e,f \in K$, is fully diverse and has NVD by Corollary 13. More generally, for all $d \in D^\times$ such that

$$N_{D/F}(d) \notin F^{\times 2} = \{(a^2 - 7b^2) + 2ab\sqrt{-7} \,|\, a,b \in \mathbb{Q}\},$$

$\mathrm{It}_l(D,\sigma,d)$ is a division algebra. For instance, choose $d = 1+i+j$ then $N_{D/F}(1+i+j) = 3$ and assuming $3 = (a^2 - 7b^2) + 2ab\sqrt{-7}$ yields $a = 0$ or $b = 0$, hence that 3 is a square in $\mathbb{Q}$, a contradiction, or that $-3/7 = b^2$, again a contradiction. Therefore $\mathrm{It}_l(D,\sigma,1+i+j)$ is a division algebra, and analogously, so would be for instance also $\mathrm{It}_l(D,\sigma,1+i+ij)$, $\mathrm{It}_l(D,\sigma,i+j)$ etc. If, for coding theoretical purposes, we want to only consider $d \in K$, then a similar argument yields that $\mathrm{It}_l(D,\sigma,1+i)$ is division (2 is not a square in $\mathbb{Q}$, and neither is $-2/7$). All these choices yield fully diverse codes.
(ii) As in [11], Section IV.B., let $F = \mathbb{Q}(i)$, $K = \mathbb{Q}(i)(\sqrt{5})$, $D = (5,i)_F$ with standard basis $1, I, J, IJ$, and $\sigma(\sqrt{5}) = -\sqrt{5}$. Then $\mathrm{It}_l(D,\sigma,d)$ is division for all $d = x_0 + Ix_1 + Jx_2 + IJx_3$, such that $N_{D/\mathbb{Q}(i)}(d) = x_0^2 - 5x_1^2 - ix_2^2 + 5ix_3^2$ is not a square in $F = \mathbb{Q}(i)$. We have

$$F^{\times\, 2} = \{(a^2 - b^2) + 2abi \,|\, a,b \in \mathbb{Q}\}.$$

Now $N_{D/\mathbb{Q}(i)}(1+I+J) = -4 - i$ and assuming that $-4 - i = (a^2 - b^2) + 2abi$ yields $a = b = 0$, a contradiction. Hence $\mathrm{It}_l(D,\sigma,1+\sqrt{5}+J)$ is a division algebra. Similarly, so is $\mathrm{It}_l(D,\sigma,\frac{1+\sqrt{5}}{2})$, using the Golden number for d (as -1 is not a square in $\mathbb{Q}$). Therefore by Corollary 13, the iterated Golden code arising from α_d with $d = \frac{1+\sqrt{5}}{2}$ is fully diverse and has NVD.
(iii) Let $D = (-1,-1)_{\mathbb{Q}}$. Then $\mathrm{It}_l(D,\sigma,d)$ is division for all $d = x_0 + x_1 i + x_2 j + x_3 k$, such that the positive rational number $N_{D/\mathbb{Q}}(d) = x_0^2 + x_1^2 + x_2^2 + x_3^2$ is not a square in $\mathbb{Q}$, e.g. for $d = 1+i$. Its matrix representation of left multiplication yields a fully diverse codebook which however is not full-rate.

Example 17. Let $F = \mathbb{Q}(\sqrt{5})$, $D = (-1,-1)_{\mathbb{Q}(\sqrt{5})}$ and $\tau : \mathbb{Q}(i,\sqrt{5}) \to \mathbb{Q}(i,\sqrt{5})$ given by $\tau(\sqrt{5}) = -\sqrt{5}$, $\tau(i) = i$, the generator of the cyclic Galois group of $\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(\sqrt{5})$. Then $\mathrm{It}_l(D,\tau,d)$ is division for all $d \in D^\times$, such that $d \neq z\widetilde{\tau}(z)$ for all $z \in D$. This is for instance true for $d = i$, by an analogous argument as used in [12], Section IV.B. The corresponding code

$$\begin{bmatrix} c & -\sigma(d) & i\tau(e) & -i\tau\sigma(f) \\ d & \sigma(c) & -i\tau(f) & -i\tau\sigma(e) \\ e & -\sigma(f) & \tau(c) & -\tau\sigma(d) \\ f & \sigma(e) & \tau(d) & \tau\sigma(c) \end{bmatrix},$$

with $c,d,e,f \in \mathbb{Q}(i,\sqrt{5})$ chosen in the ring of integers $\mathcal{O}_K$ as usual, is hence fully diverse. Since analogous considerations as in [12] hold for this code (the proofs carry over verbatim), this iterated code has the same ML-decoding complexity as the SR-code and is fast-decodable. Note that the SR-code has the lowest ML-decoding complexity ($O(M^{4.5})$ for

square M-QAM) among currently known rate-2 space-time codes for a 4×2-MIDO system [12].

Despite looking very similar to the SR-code [13], discussed for instance in [12], Section IV.B., as it only differs by two minus signs (one minus sign in entry $(2,3)$, one in $(2,4)$) from the SR-code, this code, however, does not seem to have NVD as its matrices have determinant in F by Corollary 13, which distinguishes it from the SR-code which has NVD. We observe that for all $a \in F^\times$, $a = a_0 + \sqrt{5}a_1$ with $a_i \in \mathbb{Q}$, we have $a\tau(a) = (a_0 + \sqrt{5}a_1)(a_0 - \sqrt{5}a_1) = a_0^2 - 5a_1^2 \in \mathbb{Q}$, and that for $x = x_0 + ix_1 + jx_2 + ijx_3 \in D$ with $x_i \in \mathbb{Q}(\sqrt{5})$, we get $N_{K/F}(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2 \in \mathbb{Q}(\sqrt{5})$. By Theorem 5 (b), hence any $d \in D^\times$ such that $N_{K/F}(d) \notin \mathbb{Q}$ will yield a division algebra $\mathrm{It}_l(D, \tau, d)$ and therefore a fully diverse code. E.g., any $d \in F^\times$, $d = d_0 + \sqrt{5}d_1$ with $d_0, d_1 \in \mathbb{Q}$ both nonzero will yield a division algebra $\mathrm{It}_l(D, \tau, d)$. The determinants of the matrices in codes associated to the left multiplication in algebras $\mathrm{It}_l(D, \tau, d)$ with $d \in F$ are in $\mathbb{Q}(i)$ which implies these codes would have NVD. Since analogous considerations on the ML-decoding complexity as in [12] hold for these codes, they are fast-decodable as well.

Remark 18. The considerations on iterating the Silver code given in [11], Section IV. (where d is called θ), by employing the map α_d with $\tau = \sigma$ and $d \in F^\times = \mathbb{Q}(\sqrt{-7})^\times$ in the base field, also generalize to the case that $d \in F(i) \setminus F$, considered in Example 16 (i). This mean that the code $\alpha_d(\mathcal{D} \times \mathcal{D})$ inherits fast-decodability from the Silver code, as Lemma 15 in [11] still holds in this setting. This confirms the explicit calculation in [11], Section IV.A., that the decoding complexity for $d = i$ is $O(|S|^{13})$.

4.2. 4×4 **codes obtained from** A_m**.** Let $D = (a, b)_F$ and $K = F(\sqrt{a})$ with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Take the standard basis $1, j, f, fj$ of the right K-vector space $Am = \mathrm{It}_m(D, \tau, d)$. Let $\widetilde{\tau}(x) = \tau(x_0) + j\tau(x_1)$ for all $x = x_0 + jx_1 \in D$, where τ is an automorphism of K commuting with σ.

For multiplication in A_m we have to observe that for all $x \in K$, $d = d_0 + jd_1$, $d_i \in K$:

(1) $xf = f\tau(x)$,
(2) $(fx)j = (fj)\sigma(x)$,
(3) $((fj)x)f = j\tau(x)d_0 + b\tau(\sigma(x))d_1$,
(4) $((fj)x)j = fb\sigma(x)$,
(5) $(jx)f = (fj)\tau(x)$,
(6) $(fx)f = \tau(x)d_0 + j\tau(\sigma(x))d_1$,
(7) $x(fj) = (fj)\tau(\sigma(x))$,
(8) $(jx)(fj) = fb\tau(\sigma(x))$,
(9) $((fj)x)(fj) = b\tau(\sigma(x))\sigma(d_0) + j\tau(x)\sigma(d_1)b$,
(10) $(fx)(fj) = j\tau(\sigma(x))\sigma(d_0) + b\tau(x)\sigma(d_1)$,
(11) $x(fj) = (fj)\tau(\sigma(x))$.

Thus the representation matrix of left multiplication is given by

$$\begin{bmatrix} A & \tau(B)\Theta \\ B & \tau(A) \end{bmatrix},$$

with $A, B \in \mathcal{D}$ and $\Theta = \lambda(d)$ as before.

The considerations from Example 16 can easily be adjusted now to yield fully diverse codes of type $\beta_d(\mathcal{D} \times \mathcal{D})$. Whenever $d \in D \setminus K$, these codes will be of a different form than the ones obtained via $\alpha_d(\mathcal{D} \times \mathcal{D})$.

4.3. 6×3 **case.** The following setup is treated in [11], Section V for $n = 3$: 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 $K = F(\sqrt{a})$ and $D = (L/K, \sigma, c)$ a cyclic division algebra over K of degree n. Let $d \in D^\times$ (only $d \in K$ is studied in in [11], Section V). Then $A_l = \mathrm{It}_l(D, \tau, d)$ is division over K if

$$N_{D/K}(d) \neq N_{D/K}(z\widetilde{\tau}(z))$$

for all $z \in D$. If $c \in \mathrm{Fix}(\tau)$ as in all the examples treated in [11], Section V, then A_l is a division algebra if and only if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$ by Theorem 12.

Example 19. Let ζ_7 be a primitive 7th root of unity.
(i) $D = (\mathbb{Q}(\zeta_7, i)/\mathbb{Q}(\sqrt{-7}, i), \sigma, 1 + i)$ is a cyclic division algebra of degree 3 over $K = \mathbb{Q}(\sqrt{-7}, i) = \mathbb{Q}(\sqrt{7}, i)$ with $\sigma : \zeta_7 \mapsto \zeta_7^2$. Let $F = \mathbb{Q}(i)$ and $\tau(\sqrt{7}) = -\sqrt{7}$, $\tau(i) = i$ as in [11], Example 4. For $a = a_1 + ia_1 + \sqrt{7}a_2 + \sqrt{-7}ia_3 \in K$, $a_i \in \mathbb{Q}$ we have

$$a\tau(a) = (a_0^2 - a_1^2 - 7a_2^2 - 7a_3^2) + 2(a_0a_1 - 7a_1a_3)i.$$

By Corollary 7, $A_l = \mathrm{It}_l(D, \tau, d)$ is division if

$$N_{D/K}(d) \neq a\tau(a)$$

for all $a \in K^\times$. It was already shown in [11] that $\mathrm{It}_l(D, \tau, i\sqrt{7})$ is an associative division algebra. The induced code has NVD and is fast-decodable. It is easy to see that for instance also $\mathrm{It}_l(D, \tau, \zeta_7)$ is a division algebra.
(ii) $D = (\mathbb{Q}(\zeta_7)/\mathbb{Q}(\sqrt{-7}), \sigma, 3)$ is a cyclic division algebra of degree 3 over $K = \mathbb{Q}(\sqrt{-7})$ with $\sigma : \zeta_7 \mapsto \zeta_7^2$. Let $F = \mathbb{Q}(i)$ and $\tau(\sqrt{-7}) = -\sqrt{-7}$, as in [11], Example 5. For $a = a_0 + \sqrt{-7}a_1 \in \mathbb{Q}(\sqrt{-7})$, $a_i \in \mathbb{Q}$, we have

$$a\widetilde{\tau}(a) = a_0^2 + 7a_1^2 > 0.$$

By Corollary 7, $\mathrm{It}_l(D, \tau, d)$ is a division algebra over K if $N_{D/K}(d) \neq a\tau(a)$ for all $a \in N_{D/K}(D^\times)$. Now $d = \zeta_7 \in \mathbb{Q}(\zeta_7) \setminus \mathbb{Q}(\sqrt{-7})$ has $N_{D/K}(\zeta_7) = \zeta_7^6$. Hence $\mathrm{It}_l(D, \tau, \zeta_7)$ is division.

5. Iterated algebras inside the tensor product of a cyclic division algebra and a (nonassociative) quaternion algebra

The following two results deal with the setup treated in [11], Sections IV. and V.

Theorem 20. *Let K/F be a cyclic field extension of degree $n = 2m$ with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ and $K_1 = F(\sqrt{a})$ the subfield of K with $\mathrm{Gal}(K_1/F) = \langle\sigma^m\rangle$. Let $D = (K/F, \sigma, c)$ be a cyclic division algebra and $d \in K_1^\times$. Then*

$$\mathrm{It}_l(D, \sigma^m, d)$$

is a subalgebra of the tensor product

$$A = D \otimes_F \mathrm{Cay}(K_1, d)$$

of D and the (perhaps nonassociative) quaternion algebra $\mathrm{Cay}(K_1, d)$ over F.
In particular, if $d \in F^\times$ then $\mathrm{It}_l(D, \sigma^m, d)$ is associative.

Proof. $(K/F, \sigma, c)$ is an n-dimensional K-vector space with basis $\{1, e, e^2, \ldots, e^{n-1}\}$, where $e^n = c$, and $\mathrm{Cay}(K_1, d)$ a two-dimensional K_1-vector space with basis $\{1, j\}$, where $j^2 = d$. Since $R = K \otimes_F K_1 \subset \mathrm{Nuc}(A)$, A is a free right R-algebra of dimension $2n$ with R-basis

$$\{1 \otimes 1, e \otimes 1, \ldots, e^{n-1} \otimes 1, 1 \otimes j, e \otimes j, e^{n-1} \otimes j\}.$$

and we can identify

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

Since $R \subset \mathrm{Nuc}(A)$, $L_x \in \mathrm{End}_R(A)$ and $\lambda : A \to \mathrm{End}_R(A) \hookrightarrow \mathrm{Mat}_{2n}(R), x \mapsto L_x \mapsto \lambda(x) = X$ an R-linear map. An element in $\lambda(A)$ has the form

$$\begin{bmatrix} Y & \Theta\sigma^m(Z) \\ Z & \sigma^m(Y) \end{bmatrix}.$$

with $\Theta = \lambda(d)$, $Y, Z \in \mathrm{Mat}_n(R)$, such that when restricting the entries of Y, Z, x_i, $y_i \in R$, to elements in K, we obtain $X, Y \in \mathcal{D}$ and a codebook $\mathcal{A} = \alpha_d(\mathcal{D} \times \mathcal{D})$, where

$$\alpha_d(X, Y) = \begin{bmatrix} Y & \Theta\sigma^m\sigma(Z) \\ Z & \sigma^m\sigma(Y) \end{bmatrix}$$

Restricting the matrices and only allow entries in K amounts to computing the matrix representing left multiplication with an element in A_0 for the subspace

$$A_0 = K \oplus eK \oplus \cdots \oplus e^{n-1}K \oplus jK \oplus ejK \oplus \cdots \oplus e^{n-1}jK$$

of A. This has dimension $2n^2$ as F-vector space. If $\mathrm{Cay}(K_1, d)$ is associative, i.e. $d \in F^\times$, $\mathcal{A}$ is the representation of a central simple algebra A over F [18].

A_0 is a nonassociative F_0-subalgebra of A. Its representation matrix of left multiplication equals the one of $\mathrm{It}_l(D, \sigma^m, d)$ by Theorem 12, so $A_0 = \mathrm{It}_l(D, \sigma^m, d)$. □

Theorem 21. *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 is 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 $K = F(\sqrt{a})$, $d \in K$, and $\mathrm{Gal}(K/F) = \langle\tau\rangle$. Let $D = (L/K, \sigma, c)$ be a cyclic division algebra over K of degree n. Then $\mathrm{It}_l(D, \tau, d)$ is a subalgebra of the tensor product*

$$D \otimes_K (\mathrm{Cay}(K, d) \otimes_F K)$$

of D with the (perhaps nonassociative) split quaternion algebra $\mathrm{Cay}(K, d) \otimes_F K$ over K. In particular, if $d \in F^\times$ then $\mathrm{It}_l(D, \tau, d)$ is associative.

Proof. The K-algebra $\mathrm{Cay}(K, d) \otimes_F K$ contains the split quadratic étale K-algebra $T = K \otimes_F K \cong K \times K$. $D = (L/K, \sigma, c)$ is an n-dimensional L-vector space with basis $\{1, e, e^2, \ldots, e^{n-1}\}$ and $\mathrm{Cay}(K, d) \otimes_F K = T \oplus jT$ a two-dimensional right T-module with basis $\{1, j\}$, where $j^2 = d$. $A = (L/K, \sigma, c) \otimes_K (\mathrm{Cay}(F(\sqrt{a}), d) \otimes_F K)$ contains the K-algebra $R = L \otimes_K T \cong L \times L \subset \mathrm{Nuc}(A)$. A is a free right R-algebra of dimension $2n$ with R-basis $\{1 \otimes 1, e \otimes 1, \ldots, e^{n-1} \otimes 1, 1 \otimes j, e \otimes j, e^{n-1} \otimes j\}$ and we identify

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

Since $R \subset \mathrm{Nuc}(A)$, $L_x \in \mathrm{End}_R(A)$ and $\lambda : A \to \mathrm{End}_R(A) \hookrightarrow \mathrm{Mat}_{2n}(R), x \mapsto L_x \mapsto \lambda(x) = X$ an R-linear map. An element in $\lambda(A)$ has the form

$$\begin{bmatrix} Y & \Theta\tau\sigma(Z) \\ Z & \tau\sigma(Y) \end{bmatrix}$$

with $\Theta = \lambda(d)$, $Y, Z \in \mathrm{Mat}_n(R)$, such that when restricting the matrix entries of Y, Z to elements in $L \subset R$, we obtain $X, Y \in \mathcal{D}$. Restricting the elements to have entries in L amounts to computing the matrix representing left multiplication λ_x in the subspace

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

using elements $x, y \in A_0$ only. A_0 is an F_0-subalgebra of A. Its representation matrix of left multiplication equals the one of $\mathrm{It}_l(D, \tau, d)$ by Theorem 12, so $A_0 = \mathrm{It}_l(D, \tau, d)$.

□

6. Generalized Cayley-Dickson algebras

Let K/F be a cyclic field extension of degree n with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Let $D = (K/F, \sigma, c)$ be a cyclic algebra over F of degree n, $\tau \in \mathrm{Aut}(K)$, $F_0 = \mathrm{Fix}(\tau) \cap F$ and $d \in D^\times$. The previously discussed way to define a multiplication on the $2n$-dimensional F-vector space $D \oplus D$ can be changed by randomly permuting the factors inside the definition. Since the proof of Theorem 5 is independent of theses permutations, this yields algebras which are division under the same condition as the iterated ones and which display similar behaviour. What makes the iterated algebras A_l and A_m stand out from the others, and important for developing space-time block codes, is the fact that they are right D-modules with $\lambda_x \in \mathrm{End}_D(A_i)$ for $i \in \{l, m\}$.

To demonstrate this, we consider one case, where the factors are arranged as in the classical Cayley-Dickson doubling process. Then the $2n$-dimensional F-vector space $D \oplus D$ is made into an algebra over F_0 with unit element $1 = (1, 0)$ via the multiplication

$$(u, v) \circ_l (u', v') = (uu' + d\widetilde{\tau}(v')v, v'u + v\widetilde{\tau}(u'))$$

for $u, u', v, v' \in D$. An algebra obtained from such a doubling of D is denoted by $\mathrm{Cay}_l(D, \tau, d)$.

If $d \in D^\times$ is not contained in F, define

$$(u, v) \circ_m (u', v') = (uu' + \widetilde{\tau}(v')dv, v'u + v\widetilde{\tau}(u'))$$

resp.

$$(u, v) \circ_r (u', v') = (uu' + \widetilde{\tau}(v')vd, v'u + v\widetilde{\tau}(u'))$$

on $D \oplus D$ and denote the corresponding F_0-algebras by $\mathrm{Cay}_m(D, \tau, d)$, resp. $\mathrm{Cay}_r(D, \tau, d)$. (Even if $\tau = \sigma$, $d \in F^\times$ and D is a quaternion algebra, this is not the classical Cayley-Dickson process, as $\widetilde{\tau}$ is not the canonical involution on D: $\widetilde{\tau}(j) = j$, whereas $\sigma(j) = -j$.)

In the following, write

$$C_l = \mathrm{Cay}_l(D, \tau, d),\ C_m = \mathrm{Cay}_m(D, \tau, d),\ C_r = \mathrm{Cay}_r(D, \tau, d).$$

Clearly, D is a subalgebra of C_i for $i \in \{l, m, r\}$. C_i is a K-vector space, however, here L_x is not always a K-linear map. Thus these algebras are less interesting for code constructions.

Put $f = (0, 1_D)$. Then for instance the multiplication in C_l can be written as

$$(u + fv) \circ_l (u' + fv') = (uu' + d\widetilde{\tau}(v')v) + f(v'u + v\widetilde{\tau}(u'))$$

for $u, u', v, v' \in D$.

Let $K = F[x]/(f(x))$ be a field extension of F of degree n with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, $\tau \in \mathrm{Aut}(K)$ and $d \in K^\times$. Then the $2n$-dimensional F-vector space $K \oplus K$ can be made into an algebra over F_0 with unit element $1 = (1, 0)$ via the multiplication

$$(u, v)(u', v') = (uu' + d\tau(v')v, v'u + v\tau(u'))$$

for $u, u', v, v' \in K$. This algebra is denoted by $\mathrm{Cay}(K, \tau, d)$. For $d \in K^\times$, $\mathrm{Cay}(K, \tau, d)$ is a subalgebra of C_i, $i \in \{l, m, r\}$. If K is a quadratic field extension and τ its non-trivial automorphism, $\mathrm{Cay}(K, \tau, d)$ is the classical Cayley-Dickson doubling $\mathrm{Cay}(K, d)$ of K and hence an (associative or nonassociative) quaternion algebra.

Lemma 22. *(i) C_i, $i \in \{l, m, r\}$, is not power-associative if $\widetilde{\tau}(d) \neq d$. In particular, if $d \in K$ then C_i is not power-associative if $d \notin \mathrm{Fix}(\tau)$.*
(ii) Let $B = (K'/F, \sigma', c')$ and $D = (K/F, \sigma, c)$ be two cyclic algebras over F and $f : D \to B$ an algebra isomorphism. Suppose $\tau \in \mathrm{Aut}(K)$ and $\tau' \in \mathrm{Aut}(K')$, such that $f(\widetilde{\tau}(u)) = \widetilde{\tau'}(f(u))$ for all $u \in D$. Let $a \in B^\times$. For $u, v \in D$, the map

$$G : D \oplus D \to B \oplus B, \quad G(u, v) = (f(u), a^{-1}f(v))$$

defines the following algebra isomorphisms:

$$\mathrm{Cay}_l(D,\tau,d) \cong \mathrm{Cay}_l(B,\tau',\widetilde{\tau'}(a)af(d)),$$

$$\mathrm{Cay}_m(D,\tau,d) \cong \mathrm{Cay}_m(B,\tau',\widetilde{\tau'}(a)af(d)),$$

and

$$\mathrm{Cay}_r(D,\tau,d) \cong \mathrm{Cay}_r(B,\tau',\widetilde{\tau'}(a)f(d)a).$$

In particular, for $a \in F^\times$,

$$\mathrm{Cay}_l(D,\tau,d) \cong \mathrm{Cay}_l(D,\tau,a^2d),$$

$$\mathrm{Cay}_m(D,\tau,d) \cong \mathrm{Cay}_m(D,\tau,a^2d),$$

$$\mathrm{Cay}_r(D,\tau,d) \cong \mathrm{Cay}_r(D,\tau,a^2d).$$

The proof is analogous to the one of Lemma 2. Analogous to Theorem 5 we can prove:

Theorem 23. *Let* D *be a cyclic division algebra of degree* n *over* F *and* $d \in D^\times$. *Let* $\tau \in \mathrm{Aut}(K)$ *and suppose* τ *commutes with* σ. *Let* $i \in \{l,r,m\}$.
(i) C_i *is a division algebra if*

$$N_{D/F}(d) \neq N_{D/F}(z\widetilde{\tau}(z))$$

for all $z \in D$. *Conversely, if* C_i *is a division algebra then* $d \neq z\widetilde{\tau}(z)$ *for all* $z \in D^\times$.
(ii) Suppose $c \in \mathrm{Fix}(\tau)$. *Then* C_i *is a division algebra if* $N_{D/F}(d) \neq a\tau(a)$ *for all* $a \in N_{D/F}(D^\times)$.
(iii) Suppose $F \subset \mathrm{Fix}(\tau)$. *Then* C_i *is a division algebra if* $N_{D/F}(d) \notin N_{D/F}(D^\times)^2$.

With analogous proofs as before, we obtain that corresponding versions of Corollary 7, Example 8 and Lemma 9 also hold for C_i, $i \in \{l,r,m\}$.

Remark 24. Another rather canonical way to define a unital algebra structure on $D \oplus D$ would be to choose

$$(u,v)(u',v') = (uu' + vd\widetilde{\tau}(v'), uv' + v\widetilde{\tau}(u'))$$

or

$$(u,v)(u',v') = (uu' + v\widetilde{\tau}(v')d, uv' + v\widetilde{\tau}(u')).$$

(For $u,v,u',v' \in K$, K/F quadratic and τ its non-trivial automorphism, this would be the multiplication in the associative or nonassociative quaternion algebra $\mathrm{Cay}(K,d)$.) Then

$$(u,v)(u',v') = (u,v)\begin{bmatrix} u' & v' \\ d\widetilde{\tau}(v') & \widetilde{\tau}(u') \end{bmatrix}$$

resp.,

$$(u,v)(u',v') = (u,v)\begin{bmatrix} u' & v' \\ \widetilde{\tau}(v')d & \widetilde{\tau}(u') \end{bmatrix}.$$

Now we would have left D-modules and look at matrices representing right multiplication instead. Concerning code constructions, these would not yield anything new, though.

References

[1] P. Elia, A. Sethuraman, P. V. Kumar, *Perfect space-time codes with minimum and non-minimum delay for any number of antennas*. Proc. Wireless Com 2005, International Conference on Wireless Networks, Communications and Mobile Computing.

[2] B. A. Sethuraman, B. S. Rajan, V. Sashidhar, *Full diversity, high rate space time block codes from division algebras*. IEEE Trans. Inf. Theory 49, Oct. 2003, 2596-2616.

[3] C. Hollanti, J. Lahtonen, K. Rauto, R. Vehkalahti, *Optimal lattices for MIMO codes from division algebras*. IEEE International Symposium on Information Theory, July 9 - 14, 2006, Seattle, USA, 783-787.

[4] G. Berhuy, F. Oggier, *On the existence of perfect space-time codes*. IEEE Trans. Inf. Theory 55 (5) May 2009, 2078-2082.

[5] G. Berhuy, F. Oggier, Introduction to central simple algebras and their applications to wireless communication. AMS Surveys and Monographs, 2013.

[6] G. Berhuy, F. Oggier, *Space-time codes from crossed product algebras of degree 4*. S. Boztaş and H.F. Lu (Eds.), AAECC 2007, LNCS 4851, 2007, 90-99.

[7] F. Oggier, G. Rekaya, J.-C. Belfiore , E. Viterbo, *Perfect space-time block codes.* IEEE Trans. Inf. Theory 32 (9), Sept. 2006, , 3885-3902.

[8] A. Deajim, D. Grant, *Space-time codes and nonassociative division algebras over elliptic curves*. Contemp. Math. 463 (2008), 29 – 44.

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

[10] 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.

[11] N. Markin, F. Oggier, *Iterated Space-Time Code Constructions from Cyclic Algebras*, IEEE Trans. Inf. Theory, vol. 59, no. 9, September 2013.

[12] K. P. Srinath, B. S. Rajan, *Fast decodable MIDO codes with large coding gain*, online at archiv:1208.1593v3[cs.IT]. To appear in IEEE Trans. Inf. Theory, vol. 99, 2013.

[13] R. Vehkalahti, C. Hollanti, F. Oggier, *Fast-Decodable Asymmetric Space-Time Codes from Division Algebras*, IEEE Trans. Inf. Theory, vol. 58, no. 4, April 2012.

[14] A. A. Albert, *On the power-associativity of rings*. Summa Braziliensis Mathematicae 2 (1948), 21-33.

[15] L. E. Dickson, *Linear Algebras with associativity not assumed.* Duke Math. J. 1, 113-125, 1935.

[16] S. Pumplün and V. Astier, *Nonassociative quaternion algebras over rings*. Israel J. Math. 155 (2006), 125-147.

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

[18] S. Pumplün, *Tensor products of central simple algebras and fast-decodable space-time block codes*. Preprint, available at http://molle.fernuni-hagen.de/ loos/jordan/index.html

[19] W.C. Waterhouse, *Nonassociative quaternion algebras*. Algebras Groups Geom. 4 (3) (1987), 365-378.

[20] A. Steele, *Nonassociative cyclic algebras*. To appear in Israel J. Math. 2014, online at http://link.springer.com/article/10.1007%2Fs11856-014-0021-7#page-1

[21] T. Y. Lam, Quadratic forms over fields. Graduate studies in Mathematics, Vol. 67, AMS Providence, Rhode Island, 2005.

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