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

S. PUMPLÜN

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 employs a map

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

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

Date: 24.7.2013.

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

Key words and phrases. Iterated space-time code construction, division algebra.

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 $\theta = \theta_1 + j\theta_2 \in K \oplus K = \mathrm{Cay}(K, d) = D$ is a quaternion algebra. $\tau(X)$ simply is the matrix obtained from X by applying τ to each entry of X. 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 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 $\alpha_\theta(\mathcal{D}, \mathcal{D})$ consist of the matrix representations of left multiplication of certain algebras we will call *iterated algebras*. If $\theta \in D \setminus (\mathrm{Fix}(\tau) \cap F)$, 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 their left multiplication and also extend the existing iteration process to include the case of employing the map

$$\beta_\theta : \mathrm{Mat}_n(K) \times \mathrm{Mat}_n(K) \to \mathrm{Mat}_{2n}(K),$$
$$\beta_\theta : (X, Y) \to \begin{bmatrix} X & \tau(Y)\Theta \\ Y & \tau(X) \end{bmatrix}$$

instead. We are also able to give conditions on when a code is fully diverse without having to restrict the choice of θ to the base field.

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 1. 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 $\mathrm{It}(D, \tau, d)$, $\mathrm{It}_m(D, \tau, d)$ or $\mathrm{It}_r(D, \tau, d)$ over F, which have $D = (K/F, \sigma, c)$ as a subalgebra. We call them *iterated cyclic 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, that $d \in F^\times$. 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 $\alpha_\theta(\mathcal{D}, \mathcal{D})$ 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 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 looks very similar to the SR-code discussed for instance in [12] and is fast-decodable. It has the same ML-decoding complexity as the SR-code. 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 doublings 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 $\mathrm{Cay}(S, b) = S \oplus S$ 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

$$e^n = c, \ xe = e\sigma(x), \tag{1}$$

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

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

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 $D = (K/F, \sigma, c)$ be a cyclic algebra over F of degree n and $\tau \in \mathrm{Aut}(K)$. 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 $A = D \oplus D$ can be made into a unital algebra over F via the multiplication

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

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 $\mathrm{It}(D, \tau, d)$.

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

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

resp.

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

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

Let K/F be a Galois field extension of F of degree n with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Let $\tau \in \mathrm{Aut}(K)$, $F_0 = \mathrm{Fix}(\tau) \cap F$ and $d \in K$. Then the $2n$-dimensional F-vector space $K \oplus K$ can be made into a unital 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 $\mathrm{It}(D, \tau, d)$, $\mathrm{It}_m(D, \tau, d)$ and $\mathrm{It}_r(D, \tau, d)$.

Remark 1. Let K/F be a Galois field extension of F of degree 2 with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Then $\mathrm{It}(K, \sigma, d)$ is isomorphic to the opposite algebra of the (associative or nonassociative) quaternion algebra $(K/F, \sigma, c) = \mathrm{Cay}(K, c)$. If $c \in F^\times$, $(K/F, \sigma, c)$ is an associative quaternion algebra, if $c \in K \setminus F$, it is a nonassociative quaternion algebra (for the definition, see [19]).

In the following, let

$$A = \mathrm{It}(D, \tau, d), A = \mathrm{It}_m(D, \tau, d) \text{ or } A = \mathrm{It}_r(D, \tau, d).$$

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

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

for $u, u', v, v' \in D$. For a cyclic algebra $D = (K/F, \sigma, c)$ of degree n over F, we call

$$\{1, e, e^2, \dots, e^{n-1}, l, le, le^2, \dots, le^{n-1}\}$$

the *standard basis* of the right K-vector space A.

$A = \mathrm{It}(D, \tau, d)$ and $A = \mathrm{It}_m(D, \tau, d)$ are right D-modules and free of rank 2, since $x(bc) = (xb)c$ for all $b, c \in D$ and $x \in A$. After a choice of D-basis for A, e.g. $1, l$, we can embed $\mathrm{End}_D(A)$ into the module $\mathrm{Mat}_2(D)$. Furthermore, left multiplication L_x with $x \in A$ is a D-linear map, so that we have a well-defined injective additive map

$$L : A \to \mathrm{End}_D(A) \subset \mathrm{Mat}_2(D), \quad x \to L_x.$$

Lemma 2. *(Steele) Let 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 $D = (K/F, \sigma, c)$ be a cyclic division algebra over F and $d \in D^\times$. For $u, v, u', v' \in D$, multiplication in $\mathrm{It}(D, \tau, d)$ can be written as*

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

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

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

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

Lemma 3. *(i) $A = \mathrm{It}(D, \tau, d), \mathrm{It}_m(D, \tau, d)$, resp., $\mathrm{It}_r(D, \tau, d)$, is not power-associative if $d \not\in \mathrm{Fix}(\tau)$.*
(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:

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

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

and

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

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

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

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

Proposition 4. *Let $N_{D/F}$ denote the norm of D. Suppose τ commutes with σ. Let $D' = (K/F, \sigma, \tau(c))$ with standard basis $1, f, \dots, f^{n-1}$. For $y = y_0 + ey_1 + \dots + e^{n-1}y_{n-1} \in D$ define a corresponding element $y_{D'} = y_0 + fy_1 + \dots + f^{n-1}y_{n-1} \in D'$. 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 $D = (K/F, \sigma, \gamma)$ with $y = y_0 + ey_1 + \dots + e^{n-1}y_{n-1} \in D$ induces a representation $\lambda : A \to \mathrm{Mat}_n(K)$ 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

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

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

The rest is trivial. □

Remark 5. If $D = (a, c)_F$ is a quaternion algebra, $D' = (a, \tau(c))_F$, we have $N_{D/F}(\widetilde{\tau}(x)) = N_{D/F}(\tau(x_0) + j\tau(x_1)) = N_{K/F}(\tau(x_0)) - cN_{K/F}(\tau(x_1)) = \tau(x_0)\sigma(\tau(x_0)) - c\tau(x_1)\sigma(\tau(x_1)) = \tau(x_0)\tau(\sigma(x_0)) - b\tau(x_1)\tau(\sigma(\tau(x_1)) = \tau(N_{K/F}(\tau(x_0))) - \tau(\tau(c)N_{K/F}(\tau(x_1))) = \tau(N_{D'/F}(x_{D'}))$ as special case.

With this result, we are now able to prove:

Theorem 6. *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 $A = \mathrm{It}(D, \tau, d)$, $A = \mathrm{It}_m(D, \tau, d)$ or $A = \mathrm{It}_r(D, \tau, d)$.*
(i) A 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 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) $\mathrm{It}(D, \tau, d)$, resp. $\mathrm{It}_m(D, \tau, d)$, is a division algebra if and only if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$. $\mathrm{It}_r(D, \tau, d)$ is a division algebra if $d \neq v^{-1}z\widetilde{\tau}(z)v$ for all $v, z \in D$.
(b) A 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 is a division algebra if $N_{D/F}(d) \notin N_{D/F}(D^\times)^2$.

Proof. Let $A = \mathrm{It}(D, \tau, d)$ (the other two cases of iterated algebras work analogously unless stated otherwise).
(i) Suppose

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

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

$$uu' + d\widetilde{\tau}(v)v' = 0 \text{ and } vu' + \widetilde{\tau}(u)v' = 0. \tag{3}$$

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 4, 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

$$N_{D/F}(d) = N_{D/F}(u')N_{D/F}(v')^{-1}\tau(N_{D'/F}(u'_{D'})N_{D'/F}({v'}_D^{-1})) \tag{4}$$

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

We conclude that A 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 contains zero divisors. We conclude that if A is division then $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
(ii) (a) From (3) we obtain for $v' \neq 0$ that $u' = -v^{-1}\widetilde{\tau}(u)v'$ for any of the three types of algebras. For $A = \mathrm{It}(D, \tau, d)$ 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 $\mathrm{It}(D, \tau, d)$ is division if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
For $A = \mathrm{It}_m(D, \tau, d)$ 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 $\mathrm{It}_m(D, \tau, d)$ is division if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
For $A = \mathrm{It}_r(D, \tau, d)$ this gives $uv^{-1}\widetilde{\tau}(u)v' = \widetilde{\tau}(v)v'd$. Rearranging gives $d = v'^{-1}\widetilde{\tau}(v^{-1})uv^{-1}\widetilde{\tau}(u)v'$ which yields the assertion.
(b) If $c \in \mathrm{Fix}(\tau)$, then (4) becomes

$$N_{D/F}(d) = N_{D/F}(u'v'^{-1})\tau(N_{D/F}(u'v'^{-1})) \tag{5}$$

and so A is division if

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

for all $a \in N_{D/F}(D)$.
(iii) If $F \subset \mathrm{Fix}(\tau)$, (5) 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 the other two iterated algebras, the order of the factors in the first equation changes, which however does not affect the proofs. □

Proposition 7. *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 4 and Theorem 6.

Corollary 8. *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 $A = \mathrm{It}(D, \tau, d)$, $A = \mathrm{It}_m(D, \tau, d)$ or $A = \mathrm{It}_r(D, \tau, d)$.*
(i) A 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 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 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 is a division algebra if $N_{D/F}(d) \notin F^{\times 2}$.
(b) For $d \in F^\times$, A 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 9. Let $K = F(\sqrt{a})$, $D = (a, b)_F = \mathrm{Cay}(K, b)$ be a division algebra and $\mathrm{Gal}(F(\sqrt{a})/F) = \langle\sigma\rangle$.
(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 $\mathrm{It}(D, \sigma, d)$, $\mathrm{It}_m(D, \sigma, d)$ 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. $\mathrm{It}(D, \sigma, d)$, $\mathrm{It}_m(D, \sigma, d)$ 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 $\mathrm{It}(D, \tau, d)$, $\mathrm{It}_m(D, \sigma, d)$ 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 $\mathrm{It}(D, \sigma, d)$, $\mathrm{It}_m(D, \sigma, d)$ and $\mathrm{It}_r(D, \sigma, d)$ are division algebras.

We obtain the following more general rule:

Lemma 10. *Let F be an ordered field such that -1 is not a square and $(a, b)_F$ a division algebra over F with $a < 0$ and $b > 0$.*
(i) $\mathrm{It}(D, \sigma, d)$, $\mathrm{It}_m(D, \sigma, d)$ *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 $\mathrm{It}(D, \tau, d)$, $\mathrm{It}_m(D, \tau, d)$ *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

Let $D = (K/F, \sigma, c)$ be a cyclic associative division algebra of degree n over F. Let $d \in D^\times$. 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 (2) with entries d_i. Let τ be an automorphism of K such that $\tau(c) = c$ and $\tau\sigma = \sigma\tau$. In the iterative construction of [11], the map

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

$$\alpha_\theta : (X, Y) \to \begin{bmatrix} X & \Theta\tau(Y) \\ Y & \tau(X) \end{bmatrix} \tag{6}$$

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

An iterated algebra A is both a left and a right K-vector space, since $(bc)x = b(cx)$ and $x(bc) = (xb)c$ for all $b, c \in K$ and $x \in A$. After a choice of K-basis for A, we can embed $\mathrm{End}_K(A)$ into the vector space $\mathrm{Mat}_n(K)$.

For $A = \mathrm{It}(D, \tau, d)$ and $A = \mathrm{It}_m(D, \tau, d)$, left multiplication λ_x with an element $x \in A$ is a K-linear map (since $(xy)a = x(ya)$ for all $x, y \in A$, $a \in K$).

So let $A = \mathrm{It}(D, \tau, d)$ or $A = \mathrm{It}_m(D, \tau, d)$ and consider A as a right K-vector space. Since $\lambda_x(y) = \lambda_{x'}(y)$ for all $y \in A$ implies $(x - x')y = 0$ for all $y \in A$ and thus $x = x'$, $\lambda : A \hookrightarrow \mathrm{End}_K(A), x \mapsto \lambda_x$ is a well-defined injective additive map.

Thus we get an injective additive map

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

where $X = \lambda(x)$ is the matrix representing left multiplication with x. $\mathcal{A} = \lambda(A)$ constitutes a *linear codebook*, since for all $X, X' \in \lambda(A)$, we have $X \pm X' = \lambda(x) \pm \lambda(x') = \lambda(x \pm x') \in \lambda(A)$.

We point out that the fact that a nonassociative algebra is division does not automatically imply that the associated codebook $\mathcal{A} = \lambda(A)$ is division, this is only true in certain cases and turns out to be correct for the codes obtained from left multiplication in $A = \mathrm{It}(D, \tau, d)$ or $A = \mathrm{It}_m(D, \tau, d)$ treated in this paper.

If $A = \mathrm{It}_m(D, \tau, d)$ (or $A = \mathrm{It}(D, \tau, d)$ with $d \in K^\times$), then $(ax)y = a(xy)$ for all $a \in K$, $x, y \in A$, so

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

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

Remark 11. 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 $\lambda(A)$ is a K-vector space. If one wants $\lambda(A)$ to be a K-vector space for any $d \in D^\times$, it could make sense to rather look at codes obtained through $A = \mathrm{It}_m(D, \tau, d)$ (where the matrix Θ appears on the right hand side in the right upper block matrix instead of on the left hand side). However, we believe all considerations in [11] only require $\lambda(A)$ to be an F-vector space, which is true in any case.

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, $D, \dots$ respectively, will be denoted by $\mathcal{A} = \lambda(A)$, $\mathcal{C} = \lambda(C)$, $\mathcal{D} = \lambda(D)$...

Theorem 5 in [18] together with Theorem 6 and Lemma 2 yields:

Theorem 12. *Let 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 $D = (K/F, \sigma, c)$ be a cyclic division algebra over F and $d \in D^\times$. Suppose $\tau(c) = c$ and $\tau\sigma = \sigma\tau$. Then the following are equivalent:*
(i) $A = \mathrm{It}(D, \tau, d)$ is a division algebra.
(ii) $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
(iii) The codebook $\alpha_d(\mathcal{D}, \mathcal{D})$ is fully diverse and its matrices are the representation matrices of left multiplication in A.
Moreover, the determinant of a matrix in $\alpha_d(\mathcal{D}, \mathcal{D})$ is an element of F.

4.1. 4×4 **iterated codes.** Let $D = (a, b)_F$. Take the standard basis $1, j, l, lj$ of the right K-vector space $\mathrm{It}(D, \tau, d)$. Let $K = F(\sqrt{a})$ and $\widetilde{\tau}(x) = \tau(x_0) + j\tau(x_1)$ for all $x = x_0 + jx_1 \in D$, where τ is an automorphism of K commuting with σ, where $\langle\sigma\rangle = \mathrm{Gal}(F(\sqrt{a})/F)$ and $\tau(b) = b$. Note that for $x = x_0 + jx_1$, $X = \lambda(x) \in Mat_2(K_1)$ is given by

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

For multiplication in $A = \mathrm{It}(D, \tau, d)$ we have to observe that for all $x \in K$, $d = d_0 + jd_1 \in D^\times$, $d_i \in K$:

(1) $xl = l\tau(x)$,

(2) $(lx)j=(lj)\sigma(x)$,

(3) $((lj)x)l=j\sigma(d_0)\tau(x)+b\sigma(d_1)\tau(x)$,

(4) $((lj)x)j=lb\sigma(x)$,

(5) $(jx)l=(lj)\tau(x)$,

(6) $(lx)l=\sigma(d)\tau(x)=d_0\tau(x)+jd_1\tau(x)$,

(7) $x(lj)=(lj)\tau(\sigma(x))$,

(8) $(jx)(lj)=lb\tau(\sigma(x))$,

(9) $(((lj)x)(lj)=d_0b\tau(\sigma(x))+jd_1b\tau(\sigma(x))$,

(10) $(lx)(lj)=j\sigma(d_0)\tau(\sigma(x))+b\sigma(d_1)\tau(\sigma(x))$,

(11) $x(lj)=(lj)\tau(\sigma(x))$.

Then the matrix representing left multiplication λ_x in A 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 $x_i,y_i\in K=F(\sqrt{a})$ 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

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

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

$$(7)\qquad \alpha_\theta(\begin{bmatrix} x_0 & b\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix},\begin{bmatrix} y_0 & b\sigma(y_1) \\ y_1 & \sigma(y_0) \end{bmatrix})=\begin{bmatrix} x_0 & b\sigma(x_1) & f_1 & f_2 \\ x_1 & \sigma(x_0) & f_3 & f_4 \\ y_0 & b\sigma(y_1) & \tau(x_0) & \tau(b)\tau(\sigma(x_1)) \\ y_1 & \sigma(y_0) & \tau(x_1) & \tau(\sigma(x_0)) \end{bmatrix},$$

therefore $\alpha_\theta(\mathcal{D},\mathcal{D})=\mathcal{A}$, since $\tau(b)=b$. For $d\in K^\times$, the representation matrix of left multiplication in A 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, $\langle\sigma\rangle = \mathrm{Gal}(F(\sqrt{a})/F)$ and $d \in D^\times$. Let $\tau : K \to K$ be an automorphism of K such that $\tau(b) = b$ and $\tau\sigma = \sigma\tau$. Let $A = \mathrm{It}(D, \tau, d)$. Then the following are equivalent:*
(i) The codebook $\mathcal{A}$ in (7) is fully diverse.
(ii) $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
(iii) A 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 $d \in F(\sqrt{b})^\times$, the representation matrix of left multiplication in $\mathrm{It}((a, c)_K, \tau, d)$ (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 $\mathrm{It}(D, \tau, d)$, $\mathrm{It}_m(D, \tau, d)$ 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 $\mathrm{It}(D, \sigma, d)$, 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 $\sigma(x_0 + iy_0) = x_0 - iy_0$ 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, $\mathrm{It}(D,\sigma,17)$ is a division algebra (associative in this case, see loc. cit.).

Suppose $d=i\in K\setminus F$. By Theorem 13, $\mathrm{It}(D,\sigma,i)$ 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

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

is fully diverse and has NVD by Corollary 13. More generally, for all d such that

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

$A=\mathrm{It}(D,\sigma,d)$ 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 $\mathrm{It}(D,\sigma,1+i+j)$ is a division algebra, and analogously, so would be for instance also $\mathrm{It}(D,\sigma,1+i+ij)$, $\mathrm{It}(D,\sigma,i+j)$ etc. If, for coding theoretical purposes, we want to only consider $d\in K$, then a similar argument yields that $\mathrm{It}(D,\sigma,1+i)$ 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 $D=(5,i)_F$ with standard basis $1,I,J,IJ$, $F=\mathbb{Q}(i)$, $K=\mathbb{Q}(i)(\sqrt{5})$ and $\sigma(\sqrt{5})=-\sqrt{5}$. Then $\mathrm{It}(D,\sigma,d)$ 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 $a=b=0$, contradiction. Hence $\mathrm{It}(D,\sigma,1+\sqrt{5}+J)$ is a division algebra. Similarly, so is $\mathrm{It}(D,\sigma,\frac{1+\sqrt{5}}{2})$, 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_θ with $\theta=\frac{1+\sqrt{5}}{2}$ is fully diverse and has NVD.

(iii) Let $D=(-1,-1)_{\mathbb{Q}}$. Then $\mathrm{It}(D,\sigma,d)$ is division for all $d=x_0+x_1i+x_2j+x_3k$, 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 $D=(-1,-1)_{\mathbb{Q}(\sqrt{5})}$ 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 $\mathrm{It}(D,\tau,d)$ 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 is hence fully diverse and has matrices with determinant in $F = \mathbb{Q}(\sqrt{5})$ by Corollary 13. It looks very similar to the SR-code [13], discussed for instance in [12], Section IV.B., and only differs by two minus signs (one minus sign in entry $(2,3)$, one in $(2,4)$) from the SR-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. 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.
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 6 (b), hence any $d \in D^\times$ such that $N_{K/F}(d) \notin \mathbb{Q}$ will yield a division algebra $\text{It}(D, \tau, d)$ 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 $\text{It}^2(D, \tau, d)$. The determinants of the matrices in codes associated to the left multiplication in algebras $\text{It}(D, \tau, d)$ 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., by employing the map α_d with $\tau = \sigma$ and $d = \theta \in F^\times = \mathbb{Q}(\sqrt{-7})^\times$ in the base field, also generalize to the case that $d = \theta \in F(i) \setminus F$, considered in Example 16 (i). This mean that the code $\alpha_\theta(\mathcal{D}, \mathcal{D})$ 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 $\theta = i$ is $O(|S|^{13})$. We conjecture that the choice of $\theta = -i$ should give a decoding complexity of $O(|S|^{10})$, as a similar result to Lemma 16 of [11] should hold as well.

4.2. **Codes obtained from** $\text{It}_m(D, \tau, d)$**.** For multiplication in $A = \text{It}_m(D, \tau, d)$ we have to observe that for all $x \in K$, $d = d_0 + jd_1$, $d_i \in K$:

(1) $xl = l\tau(x)$,
(2) $(lx)j = (lj)\sigma(x)$,
(3) $((lj)x)l = j\tau(x)d_0 + b\tau(\sigma(x))d_1$,
(4) $((lj)x)j = lb\sigma(x)$,
(5) $(jx)l = (lj)\tau(x)$,
(6) $(lx)l = \tau(x)d_0 + j\tau(\sigma(x))d_1$,
(7) $x(lj) = (lj)\tau(\sigma(x))$,
(8) $(jx)(lj) = lb\tau(\sigma(x))$,

(9) $(((lj)x)(lj) = b\tau(\sigma(x))\sigma(d_0) + j\tau(x)\sigma(d_1)b$,

(10) $(lx)(lj) = j\tau(\sigma(x))\sigma(d_0) + b\tau(x)\sigma(d_1)$,

(11) $x(lj) = (lj)\tau(\sigma(x))$.

This yields, correspondingly, that 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. Analogously as Theorem 5 in [18] we can prove:

Theorem 19. *Let $\tau : K \to K$ be an automorphism of K. Let $D = (K/F, \sigma, c)$ be a cyclic division algebra over F and $d \in D^\times$. Suppose*

$$\tau(c) = c \text{ and } \tau\sigma = \sigma\tau.$$

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

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

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

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

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

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

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

and so

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

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

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

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

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

and thus takes values in F.

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

Theorem 19 together with Theorem 6 and Lemma 2 yield:

Theorem 20. *Let 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 $D = (K/F, \sigma, c)$ be a cyclic division algebra over F and $d \in D^\times$. Suppose $\tau(c) = c$ and $\tau\sigma = \sigma\tau$. Then the following are equivalent:*
(i) $A = \mathrm{It}_m(D, \tau, d)$ is a division algebra.
(ii) $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
(iii) The codebook $\beta_d(\mathcal{D}, \mathcal{D})$ is fully diverse and its elements are the representation matrices of left multiplication in A.
Moreover, the determinant of a matrix in $\beta_d(\mathcal{D}, \mathcal{D})$ is an element of F.

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

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 $d \in K = F(\sqrt{a})$ is studied in in [11], Section V). Then $A = \mathrm{It}(D, \tau, d)$ 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 is a division algebra if and only if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$ by Theorem 12.

Example 21. Let ζ_7 be a primitive 7th root of unity.
(i) $D = (\mathbb{Q}(\zeta_7, i)/\mathbb{Q}(\sqrt{-7}, i), \sigma_2, 1 + i)$ is a cyclic division algebra of degree 3 over $K = \mathbb{Q}(\sqrt{-7}, i)$ with $\sigma : \zeta_7 \to \zeta_7^2$. Let $F = \mathbb{Q}(i)$, $K = \mathbb{Q}(\sqrt{-7}, i) = \mathbb{Q}(\sqrt{7}, i)$ 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 8, $A = \mathrm{It}(D, \tau, d)$ is division if

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

for all $a \in K^\times$. It was already shown in [11] that $\mathrm{It}(D, \tau, i\sqrt{7})$ is an associative division algebra. The induced code has NVD and is fast-decodable. It is easy to see that for instance also $\mathrm{It}(D, \tau, \zeta_7)$ is a division algebra.
(ii) $D = (\mathbb{Q}(\zeta_7)/\mathbb{Q}(\sqrt{-7}), \sigma_2, 3)$ is a cyclic division algebra of degree 3 over $K = \mathbb{Q}(\sqrt{-7})$

with $\sigma : \zeta_7 \to \zeta_7^2$. 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 8, $\text{It}(D, \tau, d)$ 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 $\text{It}(D, \tau, \zeta_7)$ 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 22. *Let K/F be a cyclic field extension of degree $n = 2m$ with $\text{Gal}(K/F) = \langle\sigma\rangle$ and $K_1 = F(\sqrt{a})$ the subfield of K with $\text{Gal}(K_1/F) = \langle\sigma^m\rangle$. Let $D = (K/F, \sigma, c)$ be a cyclic division algebra and $d \in F(\sqrt{a})^\times$. Then*

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

is a subalgebra of the tensor product

$$A = D \otimes_F \text{Cay}(F(\sqrt{a}), d)$$

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

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

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

and we identify

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

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

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

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

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

Restricting the matrices and only allow entries in K amounts to computing the representation matrix of 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 $\mathrm{Cay}(F(\sqrt{c}), d)$ 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-subalgebra A_0 of A. Its representation matrix of left multiplication equals the one of $\mathrm{It}(D, \sigma^m, d)$ by Lemma 2, so $A_0 = \mathrm{It}(D, \sigma^m, d)$. □

Theorem 23. *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 $K = F(\sqrt{a})$, $d \in F(\sqrt{a})$, 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 $\mathrm{It}(D, \tau, d)$ is a subalgebra of the tensor product*

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

of D with the (perhaps nonassociative) split quaternion algebra $\mathrm{Cay}(F(\sqrt{a}), d) \otimes_F K$ over K.
In particular, if $d \in F^\times$ then $\mathrm{It}(D, \tau, d)$ 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 right L-vector space with basis $\{1, e, e^2, \dots, e^{n-1}\}$ 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 $R = L \otimes_K T \cong L \times L \subset Nuc(A)$. A is a free right R-algebra of dimension $2n$ with R-basis $\{1 \otimes 1, e \otimes 1, \dots, e^{n-1} \otimes 1, 1 \otimes j, e \otimes j, e^{n-1} \otimes j\}$ 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

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

with $\Theta = \lambda(d)$, $X, Y \in \mathrm{Mat}_n(R)$, such that when restricting the matrix entries of X, Y to elements in $L \subset R$, we obtain $X, Y \in \mathcal{D}$. Restricting the elements to have entries in L amounts to computing the representation matrix for 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-subalgebra A_0 of A. Its representation matrix of left multiplication equals the one of $\mathrm{It}(D_K, \tau, d)$ by Lemma 2, so $A_0 = \mathrm{It}(D_K, \tau, d)$. □

6. Generalized Cayley-Dickson algebras

Let $D=(K/F,\sigma,c)$ be a cyclic algebra over F of degree n, $\tau\in\mathrm{Aut}(K)$ 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 6 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 $A=\mathrm{It}(D,\tau,d)$ and $A=\mathrm{It}_m(D,\tau,d)$ stand out from the other, and important for developing space-time block codes, is the fact that they are right D-modules and $\lambda_x\in\mathrm{End}_D(A)$.

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 $A=D\oplus D$ is made into a unital algebra over F_0 with unit element $1=(1,0)$ via the multiplication

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

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

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

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

resp.

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

on $D\oplus D$ and denote the corresponding algebras by $\mathrm{Cay}_m(D,\tau,d)$, resp. $\mathrm{Cay}_r(D,\tau,d)$. Even if $\tau=\sigma$ and $d\in F^\times$ (so that 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 $\sigma(j)=-j$).

Put $l=(0,1_D)$. Then for instance the multiplication in $\mathrm{Cay}(D,\tau,d)$ can be written as

$$(u+lv)(u'+lv')=(uu'+d\widetilde{\tau}(v')v)+l(v'u+v\widetilde{\tau}(u'))$$

for $u,u',v,v'\in D$. For a cyclic algebra $D=(K/F,\sigma,c)$ of degree n over F, we call

$$\{1,e,e^2,\dots,e^{n-1},l,le,le^2,\dots,le^{n-1}\}$$

the *standard basis* of the right K-vector space $\mathrm{It}((K/F,\sigma,d),\tau,d)$, $\mathrm{It}_m(D,\tau,d)$, resp. $\mathrm{It}_r(D,\tau,d)$.

Let $K=F[x]/(f(x))$ be a field extension of F of degree n with $\mathrm{Gal}(K/F)=\langle\sigma\rangle$. Let $\tau\in\mathrm{Aut}(K)$ and $d\in K^\times$. Then the $2n$-dimensional F-vector space $K\oplus K$ can be made into a unital algebra over F 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 $\mathrm{Cay}(D,\tau,d)$, $\mathrm{Cay}_m(D,\tau,d)$ and $\mathrm{Cay}_r(D,\tau,d)$. If K is a quadratic field extension and τ its non-trivial automorphism, $\mathrm{Cay}(K,\tau,d)$ is th classical Cayley-Dickson doubling $\mathrm{Cay}(K,d)$ of K and hence a quaternion algebra.

In the following, let $A = \mathrm{Cay}(D, \tau, d)$, $A = \mathrm{Cay}_m(D, \tau, d)$ or $A = \mathrm{Cay}_r(D, \tau, d))$. Clearly, D is a subalgebra of A. A is a right K-vector space since $x(bc) = (xb)c$ for all $b, c \in K$ and $x \in A$. However, here L_x is not always a K-linear map. Thus these algebras are less interesting for code constructions.

Lemma 24. *(i) $A = \mathrm{Cay}(D, \tau, d)$, $A = \mathrm{Cay}_m(D, \tau, d)$, resp., $A = \mathrm{Cay}_r(D, \tau, d)$, 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:

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

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

and

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

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

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

The proof is analogous to the one of Lemma 3. Analogous to Theorem 6 we can prove:

Theorem 25. *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 $A = \mathrm{Cay}(D, \tau, d)$, $A = \mathrm{Cay}_m(D, \tau, d)$ or $A = \mathrm{Cay}_r(D, \tau, d)$.*
(i) A 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 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 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 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 8, Example 9 and Lemma 10 also hold for $\mathrm{Cay}(D, \tau, d)$, $\mathrm{Cay}_m(D, \tau, d)$ and $\mathrm{Cay}_r(D, \tau, d)$.

Remark 26. 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 $u, v, u', v' \in K$ and K/F quadratic, this would be the multiplication in the (associative or nonassociative) quaternion algebra $\mathrm{Cay}(K, d)$. Moreover, then

$$(u,v)(u',v') = (u,v) \left[\begin{array}{cc} u' & v' \\ d\widetilde{\tau}(v') & \widetilde{\tau}(u') \end{array} \right]$$

resp.,

$$(u,v)(u',v') = (u,v) \left[\begin{array}{cc} u' & v' \\ \widetilde{\tau}(v')d & \widetilde{\tau}(u') \end{array} \right].$$

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. Wirelss 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, pp. 2596 – 2616, Oct. 2003.

[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.* Transactions on Information Theory 55 (5) May 2009, 2078 – 2082.

[5] G. Berhuy, F. Oggier, Introduction to central simple algebras and their applications to wireless communication.
`http://www.foutier.ujf-grenoble.fr/~berhuy/fichiers/BOCSA.pdf`

[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, pp. 90 – 99, 2007.

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

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

[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*, online at arxiv:1205.5134v2[cs.IT], 2013.

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

[13] 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.

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

[15] Dickson, L. E. , *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 (1987), no. 3, 365–378.

[20] A. Steele, *Nonassociative cyclic algebras.* To appear in Israel J. Math., available at http://molle.fernuni-hagen.de/~loos/jordan/index.html

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

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

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