THE NONASSOCIATIVE ALGEBRAS USED TO BUILD FAST-DECODABLE SPACE-TIME BLOCK CODES

S. PUMPLÜN AND A. STEELE

Abstract. Let K/F and K/L be two cyclic Galois field extensions and $D=(K/F,\sigma,c)$ a cyclic algebra. Given an invertible element $d\in D$, we present three families of unital nonassociative algebras over $L\cap F$ defined on the direct sum of n copies of D. Two of these families appear either explicitly or implicitly in the designs of fast-decodable space-time block codes in papers by Srinath, Rajan, Markin, Oggier, and the authors. We present conditions for the algebras to be division and propose a construction for fully diverse fast decodable space-time block codes of rate-m for nm transmit and m receive antennas. We present a DMT-optimal rate-3 code for 6 transmit and 3 receive antennas which is fast-decodable, with ML-decoding complexity at most $\mathcal{O}(M^{15})$.

1. Introduction

Space-time block codes (STBCs) are 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, a space-time block code is a set of complex $n\times m$ matrices, the codebook, that satisfies a number of properties which determine how well the code performs.

Recently, several different constructions of nonassociative algebras appeared in the literature on fast decodable STBCs, cf. for instance Markin and Oggier [1], Srinath and Rajan [2], or [4], [5], [8], [9]. There are two different types of algebras involved. The aim of this paper is to present them in a unified manner and investigate their structure, in order to be able to build the associated (fully diverse, fast-decodable) codes more efficiently in the future.

Let K/L be a cyclic Galois field extension with Galois group $\mathrm{Gal}(K/L)=\langle\tau\rangle$ of degree n and K/F a cyclic Galois field extension with Galois group $\mathrm{Gal}(K/F)=\langle\sigma\rangle$ of degree m. Put $F_0=F\cap L$. Given the direct sum A of n copies of a cyclic algebra $D=(K/F,\sigma,c)$, $c\in F_0$, we define three different multiplications on A, which each turn A into a unital nonassociative algebra over F_0. We canonically extend τ to an L-linear map $\widetilde{\tau}:D\to D$, choose an element $d\in D^\times$ and define a multiplication on the right D-module

$$D\oplus fD\oplus f^2D\oplus\cdots\oplus f^{n-1}D$$

Date: 17.11.2014.

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

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

via

$$(f^ix)(f^jy)=\begin{cases} f^{i+j}\widetilde{\tau}^j(x)y & \text{if } i+j<n,\\ f^{(i+j)-n}d\widetilde{\tau}^j(x)y & \text{if } i+j\geq n,\end{cases}$$

$$(f^ix)(f^jy)=\begin{cases} f^{i+j}\widetilde{\tau}^j(x)y & \text{if } i+j<n,\\ f^{(i+j)-n}\widetilde{\tau}^j(x)dy & \text{if } i+j\geq n,\end{cases}$$

or

$$(f^ix)(f^jy)=\begin{cases} f^{i+j}\widetilde{\tau}^j(x)y & \text{if } i+j<n,\\ f^{(i+j)-n}\widetilde{\tau}^j(x)yd & \text{if } i+j\geq n\end{cases}$$

for all $x,y\in D$, $0\leq i,j<n$. We call the resulting algebra $\mathrm{It}^n(D,\tau,d)$, $\mathrm{It}^n_M(D,\tau,d)$ or $It^n_R(D,\tau,d)$, respectively.

For $A=\mathrm{It}^n(D,\tau,d)$ and $A=\mathrm{It}^n_M(D,\tau,d)$, the left multiplication L_x with a non-zero element $x\in A$ can be represented by an $nm\times nm$ matrix with entries in K (considering A as a right K-vector space of dimension mn).

For $d\in L^\times$, left multiplication L_x with a non-zero element $x\in A=It^n_R(D,\tau,d)$ is a K-endomorphism as well, and can be represented by an $nm\times nm$ matrix with entries in K.

The family of matrices representing left multiplication in any of the three cases can be used to define a STBC $\mathcal{C}$, which is fully diverse if and only if A is division, and fast-decodable for the right choice of D.

The three algebra constructions in this paper generalize the three types of *iterated algebras* presented in [5] (the $n=2$ case). A first question concerning their existence can be found in Section VI. of [1]; the iterated codes treated there arise from the algebra $\mathrm{It}^2(D,\tau,d)$. The algebras $\mathrm{It}^n(D,\tau,d)$ and $\mathrm{It}^n_R(D,\tau,d)$ appear when designing fast-decodable asymmetric multiple input double output (MIDO) codes: $\mathrm{It}^n_R(D,\tau,d)$ is implicitly used in [2] but not mentioned there, the algebras $\mathrm{It}^n(D,\tau,d)$ are canonical generalizations of the ones behind the iterated codes of [1], and are employed in [4]. Both times they are used to design fast decodable rate-2 MIDO space-time block codes with n antennas transmitting and 2 antennas receiving the data. All codes for $n>2$ transmit antennas presented in [2] and [4] have sparse entries and therefore do not have a high data rate.

We include the third family, $\mathrm{It}^n_M(D,\tau,d)$, for completeness.

After the preliminaries in Section 2, the algebras $\mathrm{It}^n(D,\tau,d)$ and $\mathrm{It}^n_M(D,\tau,d)$ are investigated in Section 3. Necessary and sufficient conditions for $\mathrm{It}^n(D,\tau,d)$ to be a division algebra are given if $d\in F^\times$. Section 4 deals with the algebras $\mathrm{It}^n_R(D,\tau,d)$ which were defined by B. S. Rajan and L. P. Natarajan (and for $d\in L\setminus F$ yield the codes in [2]). They were already defined previously in a little known paper by Petit [3] using twisted polynomial rings. Necessary and sufficient conditions for $\mathrm{It}^n_R(D,\tau,d)$ to be a division algebra are given and simplified for special cases. E.g., if D is a quaternion division algebra, $\mathrm{It}^3_R(D,\tau,d)$ is a division algebra for all $d\in L\setminus F$ with $d\not\in N_{K/L}(K^\times)$ (Theorem 17).

How to design fully diverse fast-decodable multiple input multiple output (MIMO) codes for nm transmit and m receive antennas employing $\mathrm{It}_R^n(D,\tau,d)$ is explained in Section 5: if the code associated to D is fast-decodable, then so is the one associated to $\mathrm{It}_R^n(D,\tau,d)$. We are interested in a high data rate and use the mn^2 degrees of freedom of the channel to transmit mn^2 complex symbols. Our method yields codes of rate-m for nm transmit and m receive antennas, which is maximal rate for m receive antennas. We present an example of a DMT-optimal rate-3 code for 6 transmit and 3 receive antennas which is fast-decodable, and has normalized minimum determinant $49(\frac{2}{\sqrt{28E}})^{18} = 1/7^7E^9$. Its ML-decoding complexity is at most $\mathcal{O}(M^{15})$ (using the M-HEX constellation). We also give an example of a rate-4 code for 8 transmit and 4 receive antennas which is fast-decodable with ML-decoding complexity at most $\mathcal{O}(M^{26})$ (using the M-QAM constellation). The suggested codes thus have maximal rate in terms of the number of complex symbols per channel use (cspcu).

2. Preliminaries

2.1. Nonassociative algebras.

Let F be a field. By "F-algebra" we mean a finite dimensional nonassociative algebra over F with unit element 1.

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 [10, pp. 15, 16].

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

For coding purposes, often algebras are considered as a vector space over some subfield K, $F \subset K \subset A$. Usually K is maximal with respect to inclusion. For nonassociative algebras, this is for instance possible if $K \subset \mathrm{Nuc}(A)$.

If then left multiplication L_x is a K-linear map for an algebra A over F we can consider the map

$$\lambda : A \to \mathrm{End}_K(A), x \mapsto L_x$$

which induces a map

$$\lambda : A \to \mathrm{Mat}_s(K), x \mapsto L_x \mapsto \lambda(x) = X$$

with $s = [A:K]$, after choosing a K-basis for A and expressing the endomorphism L_x in matrix form. For an associative algebra, this is the left regular representation of A.

If A is a division algebra, λ is an embedding of vector spaces.

Similarly, given an associative subalgebra D of A such that A is a free right D-module and such that left multiplication L_x is a right D-module endomorphism, we can consider the map

$$\lambda : A \to \mathrm{End}_D(A), x \mapsto L_x$$

which induces a map

$$\lambda : A \to \mathrm{Mat}_t(D), x \mapsto L_x \mapsto \lambda(x) = X$$

with $t = \dim_D A$, after choosing a D-basis for A.

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

Let $c \in F^\times$. An *associative cyclic algebra* $A = (K/F, \sigma, c)$ *of degree* m over F is an m-dimensional K-vector space $A = K \oplus eK \oplus e^2K \oplus \cdots \oplus e^{m-1}K$, with multiplication given by the relations

$$e^m = c, \ xe = e\sigma(x),$$

for all $x \in K$. If $c^s \neq N_{K/L}(x)$ for all $x \in K$ and all $1 \leq s \leq m-1$, then A is a division algebra.

For any $c \in K \backslash F$, the *nonassociative cyclic algebra* $A = (K/F, \sigma, c)$ *of degree* m is given by the m-dimensional K-vector space $A = K \oplus eK \oplus e^2K \oplus \cdots \oplus e^{m-1}K$ together with the rules

$$(e^ix)(e^jy) = \begin{cases} e^{i+j}\sigma^j(x)y & \text{if } i+j < m \\ e^{(i+j)-m}c\sigma^j(x)y & \text{if } i+j \geq m \end{cases}$$

for all $x, y \in K, 0 \leq i, j, < m$, which are extended linearly to all elements of A to define the multiplication of A.

The unital algebra $(K/F, \sigma, c)$, $c \in K \setminus F$ is not $(n+1)$st power associative, but is built similar to the associative cyclic algebra $(K/F, \sigma, c)$, where $c \in F^\times$: we again have

$$xe = e\sigma(x) \text{ and } e^ie^j = c$$

for all integers i, j such that $i+j = m$, so that e^m is well-defined and $e^m = c$. $(K/F, \sigma, c)$ has nucleus K and center F. If $c \in K \setminus F$ is such that $1, c, c^2, \ldots, c^{m-1}$ are linearly independent over F, then A is a division algebra. In particular, if m is prime, then A is division for any choice of $c \in K \setminus F$. Nonassociative cyclic algebras are studied extensively in [15].

2.3. **Iterated algebras** [5]**.** Let K/F be a cyclic Galois extension of degree m with Galois group $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ and $\tau \in \mathrm{Aut}(K)$. Define $L = \mathrm{Fix}(\tau)$ and $F_0 = L \cap F$. Let $D = (K/F, \sigma, c)$ be an associative cyclic algebra over F of degree m. For $x = x_0 + ex_1 + e^2x_2 + \cdots + e^{m-1}x_{m-1} \in D$, define the L-linear map $\widetilde{\tau} : D \to D$ via

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

If $\tau^m = id$ then $\widetilde{\tau}^m = id$.

Remark 1. Let $c \in L$.
(i) $\widetilde{\tau}(xy) = \widetilde{\tau}(x)\widetilde{\tau}(y)$ and $\lambda(\widetilde{\tau}(x)) = \tau(\lambda(x))$ for all $x, y \in D$, where for any matrix $X = \lambda(x)$ representing left multiplication with x, $\tau(X)$ means applying τ to each entry of the matrix.
(ii) Let $D' = (K/F, \sigma, \tau(c))$ with standard basis $1, e', \dots, {e'}^{m-1}$. For $y = y_0 + ey_1 + \dots + e^{m-1}y_{m-1} \in D$ define $y_{D'} = y_0 + e'y_1 + \dots + {e'}^{m-1}y_{m-1} \in D'$. By [5, Proposition 4], $N_{D/F}(\widetilde{\tau}(y)) = \tau(N_{D/F}(y))$.

Choose $d \in D^\times$. Then the $2m^2$-dimensional F-vector space $A = D \oplus D$ can be made into a unital algebra over F_0 via the multiplication

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

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

resp.

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

for $u, u', v, v' \in D$ with unit element $1 = (1_D, 0)$. The corresponding algebras are denoted by $\mathrm{It}(D, \tau, d)$, $\mathrm{It}_M(D, \tau, d)$, resp. $\mathrm{It}_R(D, \tau, d)$, and have dimension $2m^2[F : F_0]$ over F_0. $\mathrm{It}(D, \tau, d)$, $\mathrm{It}_M(D, \tau, d)$ and $\mathrm{It}_R(D, \tau, d)$ are called *iterated algebras* over F.

Every iterated algebra A as above is a right D-modules with D-basis $\{1, f\}$. We can therefore embed $\mathrm{End}_D(A)$ into the module $\mathrm{Mat}_2(D)$. Furthermore, for $A = \mathrm{It}(D, \tau, d)$ and $A = \mathrm{It}_M(D, \tau, d)$ left multiplication L_x with $x \in A$ is a D-linear map, so that we have a well-defined additive map

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

which is injective if A is division. L_x can also be viewed as a K-linear map and after a choice of K-basis for A, we can embed $\mathrm{End}_K(A)$ into the vector space $\mathrm{Mat}_{2m}(K)$ via $\lambda : A \to \mathrm{Mat}_{2m}(K)$, $x \mapsto L_x$.

By restricting $d \in L^\times$, we achieve that left multiplication L_x in $\mathrm{It}_R(D, \tau, d)$ is a K-endomorphism and thus also can be represented by a matrix with entries in K, as for the two other algebras. Therefore if $d \in L^\times$, we can embed $\mathrm{End}_K(A)$ into the vector space $\mathrm{Mat}_{2m}(K)$ via $\lambda : A \to \mathrm{Mat}_{2m}(K)$, $x \mapsto L_x$ for $A = \mathrm{It}_R(D, \tau, d)$ as well.

Theorem 2. *(*[5, Theorem 3.2], [2, Theorem 1]*) Let D be a cyclic division algebra of degree n over F with norm $N_{D/F}$ 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) A is a division algebra if and only if $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.

(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 $N_{D/F}(d) \notin N_{D/F}(D^\times)^2$.

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

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

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

If the minimum determinant of the code, defined as

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

is bounded below by a constant, even if the codebook $\mathcal{C}$ is infinite, the code $\mathcal{C}$ has *non-vanishing determinant* (NVD). Since our codebooks $\mathcal{C}$ are based on the matrix representing left multiplication in an algebra, they are linear and thus their minimum determinant is given by

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

If $\mathcal{C}$ is fully diverse, $\delta(\mathcal{C})$ defines the *coding gain* $\delta(\mathcal{C})^{\frac{1}{n_t}}$. The larger $\delta(\mathcal{C})$ is, the better the error performance of the code is expected to be.

If a STBC has NVD then it will perform well independently of the constellation size we choose. The NVD property guarantees that a full rate linear STBC has optimal diversity-multiplexing gain trade-off (DMT) and also an asymmetric linear STBC with NVD often has DMT (for results on the relation between NVD and DMT-optimality for asymmetric linear STBCs, cf. for instance [6]).

We look at transmission over a MIMO fading channel with $n_t = nm$ transmit and n receive antennas, and assume the channel is coherent, that is the receiver has perfect knowledge of the channel. We consider the rate-n case (where mn^2 symbols are sent). The system is modeled as

$$Y = \sqrt{\rho} HS + N,$$

with Y the complex $n_r \times T$ matrix consisting of the received signals, S the the complex $n_t \times T$ codeword matrix, H is the the complex $n_r \times n_t$ channel matrix (which we assume to be known) and N the the complex $n_r \times T$ noise matrix, their entries being identically independently distributed Gaussian random variables with mean zero and variance one. ρ is the average signal to noise ratio.

Since we assume the channel is coherent, ML-decoding can be obtained via sphere decoding. The hope is to find codes which are easy to decode with a sphere decoder, i.e. which are fast-decodable: Let M be the size of a complex constellation of coding symbols and assume the code $\mathcal{C}$ encodes s symbols. If the decoding complexity by sphere decoder needs only $\mathcal{O}(M^l)$, $l < s$ computations, then $\mathcal{C}$ is called *fast-decodable*.

For a matrix B, let B^* denote its Hermitian transpose. Consider a code $\mathcal{C}$ of rate n. Any $X \in \mathcal{C} \subset \mathrm{Mat}_{mn\times mn}(\mathbb{C})$ can be written as a linear combination

$$X = \sum_{i=1}^{nm^2} g_i B_i,$$

of nm^2 $\mathbb{R}$-linearly independent basis matrices $B_1, \dots, B_{nm^2}$, with $g_i \in \mathbb{R}$. Define

$$M_{g,k} = ||B_g B_k^* + B_k B_g^*||.$$

Let S be a real constellation of coding symbols. A STBC with $s = nm^2$ linear independent real information symbols from S in one code matrix is called *l-group decodable*, if there is a partition of $\{1, \dots, s\}$ into l nonempty subsets $\Gamma_1, \dots, \Gamma_l$, so that $M_{g,k} = 0$, where g, k lie in disjoint subsets $\Gamma_i, \dots, \Gamma_j$. The code $\mathcal{C}$ then has decoding complexity $\mathcal{O}(|S|^L)$, where $L = max_{1\leq i\leq l}|\Gamma_i|$.

3. General iteration processes I and II

We will use the notation defined below throughout the remainder of the paper: Let F and L be fields and let K be a cyclic extension of both F and L such that

(1) $Gal(K/F) = \langle\sigma\rangle$ and $[K : F] = m$,
(2) $Gal(K/L) = \langle\tau\rangle$ and $[K : L] = n$,
(3) σ and τ commute: $\sigma\tau = \tau\sigma$.

Let $F_0 = F \cap L$. Let $D = (K/F, \sigma, c)$ be an associative cyclic division algebra over F of degree m with norm $N_{D/F}$ and $c \in F_0$. The condition that $c \in F_0$ means that $\widetilde{\tau} \in \mathrm{Aut}_{F_0}(D)$ of order n, see the definition of $\widetilde{\tau}$ in Section 2.3.

Definition 1. Pick $d \in D^\times$. Define a multiplication on the right D-module $D \oplus fD \oplus f^2D \oplus \cdots \oplus f^{n-1}D$ via
(i)

$$(f^i x)(f^j y) = \begin{cases} f^{i+j}\widetilde{\tau}^j(x)y & \text{if } i+j < n \\ f^{(i+j)-n} d\widetilde{\tau}^j(x)y & \text{if } i+j \geq n \end{cases}$$

for all $x, y \in D$, $i, j < n$, and call the resulting algebra $\mathrm{It}^n(D, \tau, d)$, or via
(ii)

$$(f^i x)(f^j y) = \begin{cases} f^{i+j}\widetilde{\tau}^j(x)y & \text{if } i+j < n \\ f^{(i+j)-n} \widetilde{\tau}^j(x)dy & \text{if } i+j \geq n \end{cases}$$

for all $x, y \in D$, $i, j < n$, and call the resulting algebra $\mathrm{It}_M^n(D, \tau, d)$.

$\mathrm{It}^n(D,\tau,d)$ and $\mathrm{It}^n_M(D,\tau,d)$ are both nonassociative algebras over F_0 of dimension $nm^2[F:F_0]$ with unit element $1\in D$ and contain D as a subalgebra. For both, $f^{n-1}f=d=ff^{n-1}$. If $d\in F^\times$ then $\mathrm{It}^n(D,\tau,d)=\mathrm{It}^n_M(D,\tau,d)$.

Moreover, $\mathrm{It}^2(D,\tau,d)=\mathrm{It}(D,\tau,d)$ and $\mathrm{It}^2_M(D,\tau,d)=\mathrm{It}_M(D,\tau,d)$ are the iterated algebras from Section 2.3. The algebras $\mathrm{It}^n(D,\tau,d)$ are canonical generalizations of the ones behind the iterated codes of [1], and employed in [4].

Let A be either $\mathrm{It}^n(D,\tau,d)$ or $\mathrm{It}^n_M(D,\tau,d)$, unless specified differently.

Lemma 3. *(i) If $d\in K^\times$, then $(K/L,\tau,d)$, viewed as an algebra over F_0, is a subalgebra of A. If $d\in L^\times$, then $(K/L,\tau,d)$ is an associative cyclic algebra of degree n, if $d\in K\setminus L$, $(K/L,\tau,d)$ is a nonassociative cyclic algebra of degree n.*
(ii) $A\otimes_F K=\mathrm{Mat}_m(K)\oplus f\mathrm{Mat}_m(K)\oplus\cdots\oplus f^{n-1}\mathrm{Mat}_m(K)$ contains the F_0-algebra $\mathrm{Mat}_m(K)$ as a subalgebra and has zero divisors.
If $d\in L^\times$ then $A\otimes_F K$ also contains the F_0-algebra $\mathrm{Mat}_n(K)$ as a subalgebra.
(iii) Let $n=2s$ for some integer s. Then $\mathrm{It}(D,\tau^s,d)$ (resp. $\mathrm{It}_M(D,\tau^s,d)$) is isomorphic to a subalgebra of $\mathrm{It}^n(D,\tau,d)$ (resp. $\mathrm{It}^n_M(D,\tau,d)$).
(iv) D is contained in the middle nucleus of $\mathrm{It}^n(D,\tau,d)$.

Proof. (i) Restricting the multiplication of A to entries in K proves the assertion immediately: By slight abuse of notation, we have $\mathrm{It}^n(K,\tau,d)=(K/L,\tau,d)$.
(ii) is trivial as $D\otimes_F K\cong\mathrm{Mat}_m(K)$ splits. If $d\in L^\times$ then A has the F_0-subalgebra $(K/L,\tau,d)$, which as an algebra has splitting field K.
(iii) It is straightforward to check that A is isomorphic to $D\oplus f^sD$, which is a subalgebra of A under the multiplication inherited from A.
(iv) By linearity of multiplication, we only need to show that

$$((f^ix)y)f^jz=f^ix(y(f^jz)),$$

for all $x,y,z\in D$ and all integers $0\le i,j\le n-1$. A straightforward calculation shows that these are equal if and only if $\widetilde{\tau}(x)\widetilde{\tau}(y)=\widetilde{\tau}(xy)$ for all $x,y\in D$. This is true if and only if $\tau(c)=c$. □

Lemma 3 (iii) can be generalized to the case where n is any composite number if needed.

A is a free right D-module of rank n, with right D-basis $\{1,f,\dots,f^{n-1}\}$ and we can embed $\mathrm{End}_D(A)$ into $\mathrm{Mat}_n(D)$. Left multiplication L_x with $x\in A$ is a right D-endomorphism, so that we obtain a well-defined additive map

$$\lambda:A\to\mathrm{Mat}_n(D),\quad x\mapsto L_x.$$

Let $x,y\in A$, $x=x_0+fx_1+f^2x_2+\cdots+f^{n-1}x_{n-1}$, $y=y_0+fy_1+\cdots f^{n-1}y_{n-1}$ with $x_i,y_i\in D$. If we represent y as a column vector $(y_0,y_1,\dots,y_{n-1})^T$, then we can write the product of x and y in A as a matrix multiplication

$$xy=M(x)y,$$

where $M(x)$ is an $n \times n$ matrix with entries in D given by

$$M(x) = \begin{bmatrix} x_0 & d\widetilde{\tau}(x_{n-1}) & d\widetilde{\tau}^2(x_{m-2}) & \cdots & d\widetilde{\tau}^{n-1}(x_1) \\ x_1 & \widetilde{\tau}(x_0) & d\widetilde{\tau}^2(x_{n-1}) & \cdots & d\widetilde{\tau}^{n-1}(x_2) \\ x_2 & \widetilde{\tau}(x_1) & \widetilde{\tau}^2(x_0) & \cdots & d\widetilde{\tau}^{n-1}(x_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \widetilde{\tau}(x_{n-2}) & \widetilde{\tau}^2(x_{n-3}) & \cdots & \widetilde{\tau}^{n-1}(x_0) \end{bmatrix}$$

if $A = \mathrm{It}^n(D, \tau, d)$ and

$$M(x) = \begin{bmatrix} x_0 & \widetilde{\tau}(x_{n-1})d & \widetilde{\tau}^2(x_{m-2})d & \cdots & \widetilde{\tau}^{n-1}(x_1)d \\ x_1 & \widetilde{\tau}(x_0) & \widetilde{\tau}^2(x_{n-1})d & \cdots & \widetilde{\tau}^{n-1}(x_2)d \\ x_2 & \widetilde{\tau}(x_1) & \widetilde{\tau}^2(x_0) & \cdots & \widetilde{\tau}^{n-1}(x_3)d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \widetilde{\tau}(x_{n-2}) & \widetilde{\tau}^2(x_{n-3}) & \cdots & \widetilde{\tau}^{n-1}(x_0) \end{bmatrix}$$

if $A = \mathrm{It}^n_M(D, \tau, d)$.

Example 4. Let $A = \mathrm{It}^3(D, \tau, d)$ or $A = \mathrm{It}^3_M(D, \tau, d)$ with $d \in D$. For $f = (0, 1, 0)$, we have $f^2 = (0, 0, 1)$ and $f^2 f = (d, 0, 0) = f f^2$. The multiplication in $\mathrm{It}^3(D, \tau, d)$ is given by

$$(u, v, w)(u', v', w') = (\begin{bmatrix} u & d\widetilde{\tau}(w) & d\widetilde{\tau}^2(v) \\ v & \widetilde{\tau}(u) & d\widetilde{\tau}^2(w) \\ w & \widetilde{\tau}(v) & \widetilde{\tau}^2(u) \end{bmatrix} \begin{bmatrix} u' \\ v' \\ w' \end{bmatrix})^T,$$

for $u, v, w, u', v', w' \in D$, i.e.

$$(u, v, w)(u', v', w') = (uu' + d\widetilde{\tau}(w)v' + d\widetilde{\tau}^2(v)w', vu' + \widetilde{\tau}(u)v' + d\widetilde{\tau}^2(w)w', wu' + \widetilde{\tau}(v)v' + \widetilde{\tau}^2(u)w').$$

The multiplication in $\mathrm{It}^3_M(D, \tau, d)$ is given by

$$(u, v, w)(u', v', w') = (\begin{bmatrix} u & \widetilde{\tau}(w)d & \widetilde{\tau}^2(v)d \\ v & \widetilde{\tau}(u) & \widetilde{\tau}^2(w)d \\ w & \widetilde{\tau}(v) & \widetilde{\tau}^2(u) \end{bmatrix} \begin{bmatrix} u' \\ v' \\ w' \end{bmatrix})^T,$$

for $u, v, w, u', v', w' \in D$, hence

$$(u, v, w)(u', v', w') = (uu' + \widetilde{\tau}(w)dv' + \widetilde{\tau}^2(v)dw', vu' + \widetilde{\tau}(u)v' + \widetilde{\tau}^2(w)dw', wu' + \widetilde{\tau}(v)v' + \widetilde{\tau}^2(u)w').$$

If $\{1, e, \dots, e^{m-1}\}$ is the standard basis for D, then

$$\{1, e, \dots, e^{m-1}, f, fe, \dots, f^{n-1}e^{m-1}\}$$

is a basis for the right K-vector space A. Writing elements in A as column vectors of length mn with entries in K, we obtain

$$xy = \lambda(M(x))y,$$

where

$$\lambda(M(x)) = \begin{bmatrix} \lambda(x_0) & \lambda(d)\tau(\lambda(x_{n-1})) & \cdots & \lambda(d)\tau^{n-1}(\lambda(x_1)) \\ \lambda(x_1) & \tau(\lambda(x_0)) & \cdots & \lambda(d)\tau^{n-1}(\lambda(x_2)) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda(x_{n-1}) & \tau(\lambda(x_{n-2})) & \cdots & \tau^{n-1}(\lambda(x_0)) \end{bmatrix} \tag{1}$$

for $A = \mathrm{It}^n(D, \tau, d)$, and

$$\lambda(M(x)) = \begin{bmatrix} \lambda(x_0) & \tau(\lambda(x_{n-1}))\lambda(d) & \cdots & \tau^{n-1}(\lambda(x_1))\lambda(d) \\ \lambda(x_1) & \tau(\lambda(x_0)) & \cdots & \tau^{n-1}(\lambda(x_2))\lambda(d) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda(x_{n-1}) & \tau(\lambda(x_{n-2})) & \cdots & \tau^{n-1}(\lambda(x_0)) \end{bmatrix} \tag{2}$$

for $A = \mathrm{It}^n_M(D, \tau, d)$, is the $mn \times mn$ matrix obtained by taking the left regular representation of each entry in the matrix $M(x)$. The matrix $\lambda(M(x))$ represents the left multiplication by the element x in A.

Remark 5. For all $X = \lambda(M(x)) = \lambda(x) \in \lambda(A) \subset \mathrm{Mat}_{nm}(K)$, we have $\det X \in F$. This is proved in [4] for $It^n(D, \tau, d)$. For $\mathrm{It}^n_M(D, \tau, d)$, the proof is analogous. (For $n = 2$ this is [5, Theorem 19].)

Theorem 6. *(i) Let $x \in A$ be nonzero. If x is not a left zero divisor in A, then* $\det \lambda(M(x)) \neq 0$.
(ii) A is division if and only if $\lambda(M(x))$ is invertible for every nonzero $x \in A$.

Proof. (i) Suppose $\lambda(M(x))$ is a singular matrix. Then the system of mn linear equations

$$\lambda(M(x))(y_0, \dots, y_{mn-1}) = 0$$

has a non-trivial solution $(y_0, \dots, y_{mn-1}) \in K^{mn}$ which contradicts the assumption that x is not a left zero divisor in A.
(ii) It remains to show that $\lambda(M(x))$ is invertible for every nonzero $x \in A$ implies that A is division: for all $x \neq 0$, $y \neq 0$ we have that $xy = \lambda(M(x))y = 0$ implies that $y = \lambda(M(x))^{-1}0 = 0$, a contradiction. □

The following result concerning left zero divisors is proved analogously to [2], Appendix A and requires Lemma 8:

Theorem 7. *If $d \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)\dots\widetilde{\tau}^{n-1}(z)$ for all $z \in D$, then no element $x = x_0 + fx_1 \in A$ is a left zero divisor.*

3.1. In this section, $A = It^n(D, \tau, d)$. We assume $d \in F^\times$, unless explicitly stated otherwise.

Lemma 8. *(i) If $d \notin F_0$ then $D = \mathrm{Nuc}_m(A) = \mathrm{Nuc}_l(A)$.*
(ii) Let F' and L' be fields and let K' be a cyclic extension of both F' and L' such that $Gal(K'/F) = \langle \sigma' \rangle$ and $[K : F] = m'$, $Gal(K'/L') = \langle \tau' \rangle$ and $[K : L] = n'$, σ' and τ'

commute. Assume $F_0 = F' \cap L'$ and $d' \in F'^{\times}$. Let $D' = (K'/F', \sigma', c')$ be a cyclic division algebra over F' of degree m', $c' \in F_0$. If $It^n(D, \tau, d) \cong It^{n'}(D', \tau', d')$ then $D \cong D'$ and thus also $F \cong F'$, $m = m'$ and $n = n'$.

Proof. (i) follows from Theorem 9 [3, (2)].
(ii) follows from (i), since every isomorphism preserves the middle nucleus. □

Theorem 9. $\mathrm{It}^n(D, \tau, d)$ *is a division algebra if and only if the polynomial*

$$f(t) = t^n - d$$

is irreducible in the twisted polynomial ring $D[t; \widetilde{\tau}^{-1}]$.

Proof. Let $R = D[t; \widetilde{\tau}^{-1}]$ as defined in [14] and $f(t) = t^n - d \in R$. Let $\mathrm{mod}_r f$ denote the remainder of right division by f in R. Then the vector space $V = \{g \in D[t; \widetilde{\tau}^{-1}] \,|\, \deg(g) < n\}$ together with the multiplication

$$g \circ h = gh \ \mathrm{mod}_r f$$

becomes a nonassociative algebra denoted $S_f = (V, \circ)$ over F_0 [3]. A straighforward calculation shows that $\mathrm{It}^n(D, \tau, d) = S_f$ [7]. By [3, p. 13-08 (9)], $\mathrm{It}^n(D, \tau, d) = S_f$ is division if f is irreducible. Conversely, if $f = f_1 f_2$ is reducible then f_1 and f_2 yield zero divisors in $\mathrm{It}^n(D, \tau, d) = S_f$. □

Theorem 9 together with the results in [3] imply:

Theorem 10. *Suppose that n is prime and in case $n \neq 3$, additionally that F_0 contains a primitive nth root of unity. Then* $\mathrm{It}^n(D, \tau, d)$ *is a division algebra if and only if*

$$d \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z) \cdots \widetilde{\tau}^{n-1}(z) \ \text{and} \ \tau^{n-1}(d) \neq z\widetilde{\tau}(z) \cdots \widetilde{\tau}^{n-1}(z)$$

for all $z \in D$.

From Theorem 9 we obtain:

Theorem 11. *(equivalent to* [7, Theorem 22, 23]*) Let F_0 be of characteristic not 2 and $d \in F \setminus F_0$.*
(i) If $D = (a, c)_{F_0} \otimes_{F_0} F$ is a division algebra over F, then $t^2 - d \in D[t, \widetilde{\tau}^{-1}]$ is irreducible and $\mathrm{It}^2(D, \tau, d)$ *is a division algebra.*
(ii) Let $F = F_0(\sqrt{b})$. Let $D_0 = (L/F_0, \sigma, c)$ be a cyclic algebra of degree 3 such that $D = D_0 \otimes_{F_0} F$ is a division algebra over F. If $d = d_0 + \sqrt{b} d_1 \in F \setminus F_0$ with $d_0, d_1 \in F_0$, such that $3d_0^2 + bd_1^2 \neq 0$, then $t^2 - d \in D[t, \widetilde{\tau}^{-1}]$ is irreducible and $\mathrm{It}^2(D, \tau, d)$ *is a division algebra. In particular, if $F_0 = \mathbb{Q}$ and $b > 0$, or if $b < 0$ and $-\frac{b}{3} \notin \mathbb{Q}^{\times 2}$ then* $\mathrm{It}^2(D, \tau, d)$ *is a division algebra.*

Proposition 12. [7] *Suppose that n is prime and in case $n \neq 3$, additionally that F_0 contains a primitive nth root of unity. If $\tau(d^m) \neq d^m$ and $\tau^{n-1}(d^m) \neq d^m$ for all $z \in D$, then* $\mathrm{It}^n(D, \tau, d)$ *is a division algebra.*

Note that this generalizes [1, Proposition 13].

Corollary 13. *Suppose that n is prime and that for $n \neq 3$ that F_0 contains a primitive nth root of unity. If $d^m \neq a\tau(a)\cdots\tau^{n-1}(a)$ and $\tau^{n-1}(d^m) \neq a\tau(a)\cdots\tau^{n-1}(a)$ for all $a \in F^\times$, then A is a division algebra.*

Proof. Since $c \in \mathrm{Fix}(\tau) = L$ we have $N_{D/F}(\widetilde{\tau}(x)) = \tau(N_{D/F}(x))$ for all $x \in D$ by [5, Proposition 4]. Assume $d = z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{n-1}(z)$, then

$$N_{D/F}(d) = N_{D/F}(z)N_{D/F}(\widetilde{\tau}(z))\cdots N_{D/F}(\widetilde{\tau}^{n-1}(z)) = N_{D/F}(z)\tau(N_{D/F}(z))\cdots\tau^{n-1}(N_{D/F}(z)).$$

Assume $\widetilde{\tau}^{n-1}(d) = z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{n-1}(z)$, then

$$\tau^{n-1}(N_{D/F}(d)) = N_{D/F}(z)\tau(N_{D/F}(z))\cdots\tau^{n-1}(N_{D/F}(z)).$$

Put $a = N_{D/F}(z)$ and use that $N_{D/F}(d) = d^m$. □

4. General iteration process III: Natarajan and Rajan's algebras

4.1. We use the same setup and notation as in Section 3 and now formally define the algebra behind the codes in [2].

Definition 2. (B. S. Rajan and L. P. Natarajan) Pick $d \in D^\times$. Define a multiplication on the right D-module

$$D \oplus fD \oplus f^2D \oplus \cdots \oplus f^{n-1}D,$$

via the rules

$$(f^ix)(f^jy) = \begin{cases} f^{i+j}\widetilde{\tau}^j(x)y & \text{if } i+j<n \\ f^{(i+j)-n}\widetilde{\tau}^j(x)yd & \text{if } i+j \geq n \end{cases}$$

for all $x, y \in D$, $i, j < n$, and call the resulting algebra $\mathrm{It}_R^n(D,\tau,d)$.

$\mathrm{It}_R^n(D,\tau,d)$ is an algebra over F_0 of dimension $nm^2[F:F_0]$ with unit element $1 \in D$, contains D as a subalgebra, and $f^{n-1}f = d = ff^{n-1}$. For $d \in F^\times$,

$$\mathrm{It}_R^n(D,\tau,d) = \mathrm{It}^n(D,\tau,d) = \mathrm{It}_M^n(D,\tau,d).$$

If $d \in F_0$ and $F \neq L$ then $\mathrm{It}_R^n(D,\tau,d) = \mathrm{It}^n(D,\tau,d) = \mathrm{It}_M^n(D,\tau,d)$ is an associative F_0-algebra, cf. [2, Remark 1]. $\mathrm{It}_R^2(D,\tau,d) = \mathrm{It}_R(D,\tau,d)$ is an iterated algebra.

Lemma 14. *Let $A = \mathrm{It}_R^n(D,\tau,d)$.*
(i) If $d \notin F_0$ then $D = \mathrm{Nuc}_m(A) = \mathrm{Nuc}_l(A)$.
(ii) Let F' and L' be fields and let K' be a cyclic extension of both F' and L' such that $Gal(K'/F) = \langle\sigma'\rangle$ and $[K:F] = m'$, $Gal(K'/L') = \langle\tau'\rangle$ and $[K:L] = n'$, σ' and τ' commute. Assume $F_0 = F' \cap L'$. Let $D' = (K'/F',\sigma',c')$ be a cyclic division algebra over F' of degree m', $c' \in F_0$. If $It_R^n(D,\tau,d) \cong It_R^{n'}(D',\tau',d')$ then $D \cong D'$ and thus also $F \cong F'$, $m = m'$ and $n = n'$.
(iii) If $d \in K^\times$, then the (associative or nonassociative) cyclic algebra $(K/L,\tau,d)$ of degree

n, viewed as algebra over F_0, is a subalgebra of A.
(iv) For $n > 3$, n even, $\mathrm{It}_R(D,\tau,d)$ is isomorphic to a proper subalgebra of $It_R^n(D,\tau,d)$.
(v) $A \otimes_F K \cong \mathrm{Mat}_m(K) \oplus f\mathrm{Mat}_m(K) \oplus \cdots \oplus f^{n-1}\mathrm{Mat}_m(K)$ contains the F_0-algebra $\mathrm{Mat}_m(K)$ as subalgebra and has zero divisors.

The proofs of (i) and (ii) are analogous to the one of Lemma 8, the ones of (iii), (iv), (v) to the ones in Lemma 3.

Theorem 15. *(i) $\mathrm{It}_R^n(D,\tau,d)$ is a division algebra if and only if the polynomial*

$$f(t) = t^n - d$$

is irreducible in the twisted polynomial ring $D[t;\widetilde{\tau}^{-1}]$.
(ii) Suppose that n is prime and in case $n \neq 3$, additionally that F_0 contains a primitive nth root of unity. Then $\mathrm{It}_R^n(D,\tau,d)$ is a division algebra if and only if

$$d \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)\cdots\widetilde{\tau}^{n-1}(z) \text{ and } \widetilde{\tau}^{n-1}(d) \neq z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{n-1}(z)$$

for all $z \in D$.
(iii) (cf. [19]) $\mathrm{It}_R^4(D,\tau,d)$ is a division algebra if and only if

$$d \neq z\widetilde{\tau}(z)\widetilde{\tau}(z)^2\widetilde{\tau}(z)^3 \text{ and } \widetilde{\tau}^3(d) \neq z\widetilde{\tau}(z)\widetilde{\tau}(z)^2\widetilde{\tau}(z)^3$$

and

$$\widetilde{\tau}^2(z_1)\widetilde{\tau}^3(z_1)z_1 + \widetilde{\tau}^2(z_0)z_1 + \widetilde{\tau}^2(z_1)\widetilde{\tau}^3(z_0) \neq 0 \text{ or } \widetilde{\tau}^2(z_0)z_0 + \widetilde{\tau}^2(z_1)\widetilde{\tau}^3(z_0)z_0 \neq d$$

for all $z_0, z_1 \in D$.
(iv) Suppose that n is prime and in case $n \neq 3$, additionally that F_0 contains a primitive nth root of unity. Let $d \in K^\times$. If $\tau(d^m) \neq d^m$ and $\tau^{n-1}(d^m) \neq d^m$ for all $z \in D$, then $\mathrm{It}_R^n(D,\tau,d)$ is a division algebra.

Proof. (i) Let $R = D[t;\widetilde{\tau}^{-1}]$ and $f(t) = t^n - d \in R$. Since $\mathrm{It}_R^n(D,\tau,d) = S_f$ [7], the assertion now follows as in the proof of Theorem 9.
(ii) follows from (i) together with [3], (iv) is proved in [7].
(iii) If $f(t) = t^4 - d$ is reducible then either f is divisible by a linear factor from the left, from the right, or $f = g_1(t)g_2(t)$ for two irreducible polynomials $g_1, g_2 \in R$ of degree 2. By [14, 1.3.11], f is divisible on the right by a factor $t - z$, $z \in D$, iff $\widetilde{\tau}^3(d) = z\widetilde{\tau}(z)\widetilde{\tau}(z)^2\widetilde{\tau}(z)^3$. A straightforward calculation shows that f is divisible on the left by a factor $t - z$, $z \in D$, iff $0 = z\widetilde{\tau}(z)\widetilde{\tau}(z)^2\widetilde{\tau}(z)^3 - d$, which is the remainder of right division of f by $t - z$. Moreover, f is divisible on the right by $g(t) = t^2 - z_1 t - z_0 \in R$ iff

$$[\widetilde{\tau}^2(z_1)\widetilde{\tau}^3(z_1)z_1 + \widetilde{\tau}^2(z_0)z_1 + \widetilde{\tau}^2(z_1)\widetilde{\tau}^3(z_0)]t + [\widetilde{\tau}^2(z_0)z_0 + \widetilde{\tau}^2(z_1)\widetilde{\tau}^3(z_0)z_0 - d] = 0$$

which is the remainder of right division of $f(t)$ by $g(t)$ (using $\widetilde{\tau}^4 = id$). This is equivalent to

$$\widetilde{\tau}^2(z_1)\widetilde{\tau}^3(z_1)z_1 + \widetilde{\tau}^2(z_0)z_1 + \widetilde{\tau}^2(z_1)\widetilde{\tau}^3(z_0) = 0 \text{ and } \widetilde{\tau}^2(z_0)z_0 + \widetilde{\tau}^2(z_1)\widetilde{\tau}^3(z_0)z_0 = d$$

and we have proved the assertion. □

Note that when building our codes later, we will look at $\mathrm{It}_R^n(D,\tau,d)$ where $d\in L\setminus F$, which simplifies the above criteria, as $d\in L=\mathrm{Fix}(\tau)$ implies that $\widetilde{\tau}(d)=d$.

Corollary 16. *Suppose that n is prime and in case $n\neq 3$ that F_0 contains a primitive nth root of unity. If $N_{D/F}(d)\neq a\tau(a)\cdots\tau^{n-1}(a)$ and $\tau^{n-1}(N_{D/F}(d))\neq a\tau(a)\cdots\tau^{n-1}(a)$ for all $a\in N_{D/F}(D^\times)$, then $\mathrm{It}_R^n(D,\tau,d)$ is division.*

Proof. Since $c\in\mathrm{Fix}(\tau)=L$ we have $N_{D/F}(\widetilde{\tau}(x))=\tau(N_{D/F}(x))$ for all $x\in D$ by [5, Proposition 4]. Assume $d=z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{n-1}(z)$, then

$$N_{D/F}(d)=N_{D/F}(z)N_{D/F}(\widetilde{\tau}(z))\cdots N_{D/F}(\widetilde{\tau}^{n-1}(z))=N_{D/F}(z)\tau(N_{D/F}(z))\cdots\tau^{n-1}(N_{D/F}(z)).$$

Assume $\widetilde{\tau}^{n-1}(d)=z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{n-1}(z)$, then

$$\tau^{n-1}(N_{D/F}(d))=N_{D/F}(z)\tau(N_{D/F}(z))\cdots\tau^{n-1}(N_{D/F}(z)).$$

Put $a=N_{D/F}(z)$. □

Theorem 17. *Let F_0 have characteristic not 2. Let $D=(e,c)_F$, $c\in F_0$, be a quaternion division algebra over F.*
(i) If $[K:L]=3$ and $d\in L\setminus F$ such that $d\notin N_{K/L}(K^\times)$, then $t^3-d\in D[t,\widetilde{\tau}^{-1}]$ is irreducible and $\mathrm{It}_R^3(D,\tau,d)$ is a division algebra.
(ii) If $[K:L]=4$ and $d\in L\setminus F$ such that $d^s\notin N_{K/L}(K^\times)$ for $t=1,2,3$, then $d\neq z\widetilde{\tau}(z)\widetilde{\tau}(z)^2\widetilde{\tau}(z)^3$ for all $z\in D$.

Proof. (i) By Theorem 15 (ii), since here $d\in L=\mathrm{Fix}(\tau)$, $\mathrm{It}_R^3(D,\tau,d)$ is a division algebra if and only if $d\neq z\widetilde{\tau}(z)\widetilde{\tau}(z)^2$ for all $z\in D$. Suppose that

$$d=z\widetilde{\tau}(z)\widetilde{\tau}(z)^2 \tag{3}$$

for some $z=a+jb\in D$, $a,b\in K$, then $a\neq 0$ and $b\neq 0$: suppose $a=0$, then $jbj\widetilde{\tau}(b)j^2\widetilde{\tau}^2(b)\in Kj$ contradicts that $d\in L^\times$; suppose $b=0$, then $d=a\tau(a)\tau^2(a)=N_{K/L}(a)$ contradicts that $d\notin N_{K/L}(K^\times)$. Equation (3) implies that $\widetilde{\tau}(d)^2=\widetilde{\tau}(z)^2z\widetilde{\tau}(z)$, since $d\in L$ therefore

$$z\widetilde{\tau}(z)\widetilde{\tau}(z)^2=\widetilde{\tau}(z)^2z\widetilde{\tau}(z).$$

Thus for $D=(e,c)_F$, $c\in F_0$,

$$z\widetilde{\tau}(z)=x+j\sigma(y)$$

with $x=a\tau(a)+c\sigma(b)\tau(b)$, $\sigma(y)=b\tau(a)+\sigma(a)\tau(b)$. From $(x+j\sigma(y))(\tau^2(a)+j\tau^2(b))=(\tau^2(a)+j\tau^2(b))(x+j\sigma(y))$ it follows that

$$\sigma(x)\tau^2(b)+\sigma(y)\tau^2(a)=\tau^2(b)x+\sigma(\tau^2(a))\sigma(y).$$

Equation (3) yields

$$d=x\tau^2(a)+cy\tau^2(b) \tag{4}$$

and

$$0=\sigma(x)\tau^2(b)+\sigma(y)\tau^2(a). \tag{5}$$

Now $x\neq 0$ (or else we get a contradiction), so Equations (4) and (5) together with Equation (3) imply that

$$\frac{\sigma(y)}{\tau^2(b)}=-\frac{x}{\sigma(\tau^2(a))}=\frac{\sigma(x)}{\tau^2(a)}$$

and

$$\frac{-\sigma(x)}{\tau^2(a)}=\frac{\sigma(y)}{\tau^2(b)},$$

so that

$$\frac{\sigma(x)}{\tau^2(a)}\in \mathrm{Fix}(\sigma)=F.$$

Use Equation (5) in Equation (4) to obtain

$$\frac{\tau^2(a)}{\sigma(x)}(x\sigma(x)-cy\sigma(y))=d.$$

Since $x\sigma(x)-cy\sigma(y)\in F$, the left-hand side lies in F, contradicting the choice of $d\in L\setminus F$. Thus $d\neq z\widetilde{\tau}(z)\widetilde{\tau}(z)^2$.

(ii) The proof is a straighforward calculation analogous to (i) or the proof of [2, Proposition 5]. □

4.2. $A=\mathrm{It}_R^n(D,\tau,d)$ is a right K-vector space of dimension mn. By choosing $d\in L^\times$, we achieve that left multiplication L_x is a K-endomorphism and can be represented by a matrix with entries in K.

For $d\in L^\times$, the algebras $A=\mathrm{It}_R^n(D,\tau,d)$ are behind the codes defined by Srinath and Rajan [2], even though they are not explicitly defined there as such. In the setup of [2], it is assumed that $d\in L\setminus F$ and that $L\neq F$. We do not assume that $L\neq F$ for now.

Example 18. Let F_0 have characteristic not 2 and $D=(K/F,\sigma,c)=K\oplus eK$ be a quaternion division algebra over F with multiplication

$$(x_0+ex_1)(u_0+eu_1)=\big(x_0u_0+c\sigma(x_1)u_1\big)+e\big(x_1u_0+\sigma(x_0)u_1\big), \tag{6}$$

for $x_i,u_i\in K$. Let K/L be a quadratic field extension with non-trivial automorphism τ, $d\in K^\times$. The iterated algebra

$$\mathrm{It}_R(D,\tau,d)=D\oplus fD=K\oplus eK\oplus fK\oplus feK,$$

has multiplication

$$(x+fy)(u+fv)=\big(xu+\widetilde{\tau}(y)vd\big)+f\big(yu+\widetilde{\tau}(x)v\big),$$

where $x=x_0+ex_1$, $y=y_0+ey_1$, $u=u_0+eu_1$, $v=v_0+ev_1\in D$, $x_i,y_i,u_i,v_i\in K$. Here,

$$xu \text{ is given in equation (6),}$$

$$\begin{aligned}\widetilde{\tau}(y)vd = (\widetilde{\tau}(y)v)d &= \Big(\big(\tau(y_0)v_0 + c\sigma\tau(y_1)v_1\big) + e\big(\tau(y_1)v_0 + \sigma\tau(y_0)v_1\big)\Big)(d+e0)\\ &= \big(\tau(y_0)v_0d + c\sigma\tau(y_1)v_1d\big) + e\big(\tau(y_1)v_0d + \sigma\tau(y_0)v_1d\big),\end{aligned}$$

$$\begin{aligned}yu &= \big(y_0u_0 + c\sigma(y_1)u_1\big) + e\big(y_1u_0 + \sigma(y_0)u_1\big),\\ \widetilde{\tau}(x)v &= \big(\tau(x_0)v_0 + c\sigma\tau(x_1)v_1\big) + e\big(\tau(x_1)v_0 + \sigma\tau(x_0)v_1\big).\end{aligned}$$

Thus we can write the multiplication in terms of the K-basis $\{1, e, f, fe\}$ as

$$\begin{aligned}(x+fy)(u+fv) = &\big(x_0u_0 + c\sigma(x_1)u_1 + \tau(y_0)v_0d + c\sigma\tau(y_1)v_1d\big)\\ &+ e\big(x_1u_0 + \sigma(x_0)u_1 + \tau(y_1)v_0d + \sigma\tau(y_0)v_1d\big)\\ &+ f\big(y_0u_0 + c\sigma(y_1)u_1 + \tau(x_0)v_0 + c\sigma\tau(x_1)v_1\big)\\ &+ fe\big(y_1u_0 + \sigma(y_0)u_1 + \tau(x_1)v_0 + \sigma\tau(x_0)v_1\big).\end{aligned}$$

Since $d \in K$, it commutes with the elements y_i and v_i in the above expression.

Write $\Phi(x+fy)$ for the column vector with respect to the K-basis, i.e.,

$$\Phi(x+fy) = (x_0, x_1, y_0, y_1)^T \quad \text{and} \quad \Phi(u+fv) = (u_0, u_1, v_0, v_1)^T,$$

then we can write the product as

$$\Phi((x+fy)(u+fv)) = \begin{bmatrix} x_0u_0 + c\sigma(x_1)u_1 + d\tau(y_0)v_0 + dc\sigma\tau(y_1)v_1 \\ x_1u_0 + \sigma(x_0)u_1 + d\tau(y_1)v_0 + d\sigma\tau(y_0)v_1 \\ y_0u_0 + c\sigma(y_1)u_1 + \tau(x_0)v_0 + c\sigma\tau(x_1)v_1 \\ y_1u_0 + \sigma(y_0)u_1 + \tau(x_1)v_0 + \sigma\tau(x_0)v_1 \end{bmatrix} =$$

$$\begin{bmatrix} x_0 & c\sigma(x_1) & d\tau(y_0) & dc\sigma\tau(y_1) \\ x_1 & \sigma(x_0) & d\tau(y_1) & d\sigma\tau(y_0) \\ y_0 & c\sigma(y_1) & \tau(x_0) & c\sigma\tau(x_1) \\ y_1 & \sigma(y_0) & \tau(x_1) & \sigma\tau(x_0) \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ v_0 \\ v_1 \end{bmatrix}.$$

The matrix on the left side is equal to

$$\begin{bmatrix} \lambda(x) & d\lambda(\widetilde{\tau}(y)) \\ \lambda(y) & \lambda(\widetilde{\tau}(x)) \end{bmatrix}.$$

Thus for $d \in L^\times$, left multiplication L_x is a K-endomorphism and can be represented by the above matrix with entries in K.

In the following, $A = \mathrm{It}_R^n(D, \tau, d)$ and we assume $d \in L^\times$. Any element $x \in A$ can be identified with a unique column vector $\Phi(x) \in K^{mn}$ using the standard K-basis

$$\{1, e, \dots, e^{m-1}, f, fe, \dots, fe^{m-1}, \dots, f^{n-1}, f^{n-1}e, \dots, f^{n-1}e^{m-1}\}.$$

For $x = x_0 + fx_1 + f^2x_2 + \cdots + f^{n-1}x_{n-1}$, $x_0, \ldots, x_{n-1} \in D$, define

$$(7) \quad \Lambda(x) = \lambda(M(x)) = \begin{bmatrix} \lambda(x_0) & d\tau(\lambda(x_{n-1})) & d\tau^2(\lambda(x_{n-2})) & \cdots & d\tau^{n-1}(\lambda(x_1)) \\ \lambda(x_1) & \tau(\lambda(x_0)) & d\tau^2(\lambda(x_{n-1})) & \cdots & d\tau^{n-1}(\lambda(x_2)) \\ \lambda(x_2) & \tau(\lambda(x_1)) & \tau^2(\lambda(x_0)) & \cdots & d\tau^{n-1}(\lambda(x_3)) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda(x_{n-1}) & \tau(\lambda(x_{n-2})) & \tau^2(\lambda(x_{n-3})) & \cdots & \tau^{n-1}(\lambda(x_0)) \end{bmatrix},$$

where $\lambda(x_i)$, $x_i \in D$, is the $m \times m$ matrix with entries in K representing left multiplication by x_i in the cyclic division algebra D.

Lemma 19. *(B. S. Rajan and L. P. Natarajan)*
(i) For any $x \in \mathrm{It}_R^n(D, \tau, d)$, $\Lambda(x)$ is the matrix representing left multiplication by x in A, i.e., $\Phi(xy) = \Lambda(x)\Phi(y)$ for every $y \in A$.
(ii) A is division if and only if $\Lambda(x) = \lambda(M(x))$ is invertible for every nonzero $x \in A$.
(iii) For every $x \in A$, $det(\lambda(M(x))) \in L$.

Proof. (i) For any $r \in D$ with $r = r_0 + er_1 + \cdots + er^{m-1}$, where $r_0, \ldots, r_{m-1} \in K$, define $\phi(r) = [r_0, r_1, \ldots, r_{m-1}]^T$. Let $x = \sum_{i=0}^{n-1} f^i x_i$ and $y = \sum_{j=0}^{n-1} f^j y_j$ be elements of A, with $x_i, y_i \in D$. For any x_i and y_i, the multiplication in D is given by $\phi(x_i y_i) = \lambda(x_i)\phi(y_i)$. Moreover, since $d \in L$ we see that $\phi(d) = [d, 0, \ldots, 0]$, and therefore

$$\phi(y_i d) = \lambda(y_i)\phi(d) = \phi(y_i)d = d\phi(y_i).$$

Now it is straightforward to see that the matrix multiplication $\Lambda(x)\Phi(y)$ does indeed represent the multiplication in A.
(ii) A is division if and only if $xy \neq 0$ for every nonzero $x, y \in A$ [10], i.e., if and only if $\Lambda(x)\Phi(y) \neq 0$, or equivalently, if and only if $\Lambda(x)$ is invertible for every nonzero $x \in A$.
(iii) It enough to show that $\det(\Lambda(x)) = \tau(\det(\Lambda(x))) = \det(\tau(\Lambda(x)))$, where

$$\tau(\Lambda(x)) = \begin{bmatrix} \tau(\lambda(x_0)) & d\tau^2(\lambda(x_{n-1})) & \cdots & d\tau^{n-1}(\lambda(x_2)) & d\lambda(x_1) \\ \tau(\lambda(x_1)) & \tau^2(\lambda(x_0)) & \cdots & d\tau^{n-1}(\lambda(x_3)) & d\lambda(x_2) \\ \tau(\lambda(x_2)) & \tau^2(\lambda(x_1)) & \cdots & \tau^{n-1}(\lambda(x_4)) & d\lambda(x_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \tau(\lambda(x_{n-1})) & \tau^2(\lambda(x_{n-2})) & \cdots & \tau^{n-1}(\lambda(x_1)) & \lambda(x_0) \end{bmatrix}.$$

It follows that $\Lambda(x) = P\tau(\Lambda(x))P^{-1}$, with

$$P = \begin{bmatrix} 0 & 0 & \cdots & 0 & dI_m \\ I_m & 0 & \cdots & 0 & 0 \\ 0 & I_m & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & I_m & 0 \end{bmatrix} \text{ and } P^{-1} = \begin{bmatrix} 0 & I_m & 0 & \cdots & 0 \\ 0 & 0 & I_m & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I_m \\ d^{-1}I_m & 0 & 0 & \cdots & 0 \end{bmatrix},$$

where I_m is the $m \times m$ identity matrix and 0 is the $m \times m$ zero matrix which proves the assertion. □

4.3. We end this section by looking closer at the $n = 3$ case. The proofs of the following results were communicated to us by B. S. Rajan and L. P. Natarajan:

Lemma 20. *(B. S. Rajan and L. P. Natarajan) Let K/L be a cyclic Galois extension of degree 3.*
(i) If $d \in L^\times$ is not an eigenvalue of $Z\tau(Z)\tau^2(Z)$ for any $Z \in \mathrm{Mat}_m(K)$, then $d \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)$ for any $z \in D$, and $d^2 \neq z\widetilde{\tau}^2(z)\widetilde{\tau}(z)$ for any $z \in D$.
(ii) There exists an $x \in \{x_0 + fx_1 | x_0, x_1 \in D^\times\}$ with $\det(\Lambda(x)) = 0$ if and only if $d = z\widetilde{\tau}(z)\widetilde{\tau}^2(z)$ for some $z \in D$.
(iii) There exists an $x \in \{x_0 + f^2x_2 | x_0, x_2 \in D^\times\}$ with $\det(\Lambda(x)) = 0$ if and only if $d^2 = z\widetilde{\tau}^2(z)\widetilde{\tau}(z)$ for some $z \in D$.
(iv) There exists an $x \in \{fx_1 + f^2x_2 | x_1, x_2 \in D^\times\}$ with $\det(\Lambda(x)) = 0$ if and only if $d = z\widetilde{\tau}(z)\widetilde{\tau}^2(z)$ for some $z \in D$.
(v) Let $x = x_0 + fx_1 + f^2x_2$, $x_0, x_1, x_2 \in D^\times$. If d is not an eigenvalue of $Z\tau(Z)\tau^2(Z)$ for any $Z \in \mathrm{Mat}_m(K)$, then $\det(\Lambda(x)) \neq 0$.

Proof. (i) If $d = z\widetilde{\tau}(z)\widetilde{\tau}^2(z)$ for some $z \in D$, then $\lambda(d) = Z\tau(Z)\tau^2(Z)$ for $Z = \lambda(z)$. Since $\lambda(d)$ is a diagonal matrix with d as the first diagonal entry, we conclude that $Z\tau(Z)\tau^2(Z)$ has d as an eigenvalue.
If $d^2 = z\widetilde{\tau}^2(z)\widetilde{\tau}(z)$, then z is nonzero, and has a multiplicative inverse z^{-1} in D. Then, $\widetilde{\tau}(z^{-1})\widetilde{\tau}^2(z^{-1})z^{-1} = d^{-2}$. Hence d^{-2} is an eigenvalue of $\lambda\left(\widetilde{\tau}(z^{-1})\widetilde{\tau}^2(z^{-1})z^{-1}\right)$, and d is an eigenvalue of $d^3\lambda\left(\widetilde{\tau}(z^{-1})\widetilde{\tau}^2(z^{-1})z^{-1}\right) = Z\tau(Z)\tau^2(Z)$ for $Z = d\lambda(\widetilde{\tau}(z^{-1}))$.
(ii) - (iv) can be proved by a long computation [21]. □

Theorem 21. *(B. S. Rajan and L. P. Natarajan) Let K/L be a cyclic Galois extension of degree 3. Suppose that $d \in L^\times$ is not an eigenvalue of $Z\tau(Z)\tau^2(Z)$ for any $Z \in \mathrm{Mat}_m(K)$, then $\mathrm{It}_R^3(D, \tau, d)$ is a division algebra.*

Proof. Suppose that $d \in L^\times$ is not an eigenvalue of $Z\tau(Z)\tau^2(Z)$ for any $Z \in \mathrm{Mat}_m(K)$. From Lemma 20 (i), we see that $d \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)$ and $d^2 \neq z\widetilde{\tau}^2(z)\widetilde{\tau}(z)$ for any $z \in D$.

By Lemma 19 (ii), we need to show that $\det(\Lambda(x)) \neq 0$ for every $x \in A \setminus \{0\}$. Let $x = x_0 + fx_1 + f^2x_2$, where $x_0, x_1, x_2 \in D$. If exactly one of x_0, x_1, x_2 is nonzero, it is straightforward to see that $\det(\Lambda(x)) \neq 0$. If exactly two of x_0, x_1, x_2 are nonzero, $\det(\Lambda(x)) \neq 0$ by Lemma 20 (ii), (iii), (iv). If x_0, x_1, x_2 are all nonzero, then $\det(\Lambda(x)) \neq 0$ by Lemma 20 (v). □

Lemma 20 (i) implies that Theorem 21 imposes a stricter constraint on the choice of $d \in L$ as Theorem 15 (iii), which only requires that $d \neq z\widetilde{\tau}(z)\widetilde{\tau}(z)^2$.

5. How to design fast-decodable Space-Time Block Codes using $\mathrm{It}_R^n(D, \tau, d)$

5.1. To construct fully diverse space-time block codes for mn transmit antennas we let L be either $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$, $\omega = e^{2\pi i/3}$, and $D = (K/F, \sigma, c)$ a cyclic division algebra of degree m over a number field $F \neq L$, $c \in F \cap L$, and where K is a cyclic extension of L of degree n

with Galois group generated by τ. We assume that σ and τ commute and choose $d \in L \setminus F$ such that $f(t) = t^n - d \in D[t; \widetilde{\tau}^{-1}]$ is irreducible.

Each codeword in $\mathcal{C}$ is a matrix of the form given in (7), where $\lambda(x)$ is the $m \times m$ matrix with entries in K given by the left regular representation in D. For A division, these are invertible $mn \times mn$ matrices with entries in K. Each entry of $\lambda(x_i)$ can be viewed as a linear combination of n independent elements of L. As such we express each entry of these as a linear combination of some chosen L-basis $\{\theta_1, \theta_2, \dots, \theta_n \mid \theta_i \in \mathcal{O}_K\}$ over $\mathcal{O}_L$. Thus an entry $\lambda(x)$ has the form

$$(8) \qquad \lambda(x) = \begin{bmatrix} \sum_{i=1}^n s_i\theta_i & c\sigma(\sum_{i=1}^n s_{i+nm-n}\theta_i) & \dots & c\sigma^{m-1}(\sum_{i=1}^n s_{i+n}\theta_i) \\ \sum_{i=1}^n s_{i+n}\theta_i & \sigma(\sum_{i=1}^n s_i\theta_i) & \dots & c\sigma^{m-1}(\sum_{i=1}^n s_{i+2n}\theta_i) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n s_{i+nm-n}\theta_i & \sigma(\sum_{i=1}^n s_{i+nm-2n}\theta_i) & \dots & \sigma^{m-1}(\sum_{i=1}^n s_i\theta_i) \end{bmatrix}.$$

The elements $s_i, 1 \leq i \leq mn$, are the complex information symbols with values from QAM ($\mathbb{Z}(i)$) or HEX ($\mathbb{Z}(\omega)$) constellations.

Contrary to [2], we are interested in high data rate, i.e. we use the mn^2 degrees of freedom of the channel to transmit mn^2 complex information symbols per codeword. If mn channels are used the space-time block code $\mathcal{C}$ consisting of matrices S of the form (7) with entries as in (8) has a rate of n complex symbols per channel use, which is maximal for n receive antennas.

Proposition 22. *If the subset of codewords in $\mathcal{C}$ made up of the diagonal block matrix*

$$S(\lambda(x_0)) = diag[\lambda(x_0), \tau(\lambda(x_0)) \dots, \tau^{n-1}(\lambda(x_0))]$$

is l-group decodable, then $\mathcal{C}$ has ML-decoding complexity $\mathcal{O}(M^{mn^2 - mn(l-1)/l})$ and is fast-decodable.

Proof. To analyze ML-decoding complexity, we have to minimize the ML-complexity metric

$$||Y - \sqrt{\rho}HS||^2$$

over all codewords $S \in \mathcal{C}$. Every $S \in \mathcal{C}$ can be written as

$$S = S(\lambda(x_0)) + S(\lambda(x_1)) + \dots + S(\lambda(x_{n-1}))$$

with $S(\lambda(x_0)) = diag[\lambda(x_0), \tau(\lambda(x_0)), \tau(\lambda(x_0))]$ and $S(\lambda(x_j))$ being the matrix obtained by putting $\lambda(x_j) = 0$, for all $j \neq i$ in (7). Each $S(\lambda(x_i))$ contains nm complex information symbols. Since $S(\lambda(x_0))$ is l-group decodable by assumption, we need $\mathcal{O}(M^{nm/l})$ computations to compute $\min_{S(\lambda(x_0)))}\{||Y - \sqrt{\rho}HS||^2\}$. So the ML-decoding complexity of $\mathcal{C}$ is $\mathcal{O}(M^{(n-1)(nm)+nm/l}) = \mathcal{O}(M^{mn^2 - mn(l-1)/l})$ □

Corollary 23. *If $D = \mathrm{Cay}(K/F, -1)$ is a subalgebra of Hamilton's quaternion algebra and $d \in L \setminus F$, then the corresponding code $\mathcal{C}$ in (7) has decoding complexity*

$$\mathcal{O}(M^{2n^2 - 3n/2})$$

if the s_i take values from M-QAM and decoding complexity

$$\mathcal{O}(M^{2n^2-n})$$

if the s_i take values from M-HEX.

Proof. If $D = \mathrm{Cay}(K/F, -1)$ is a quaternion division algebra which is a subalgebra of Hamilton's quaternion algebra, σ commutes with complex conjugation, and a code consisting of the block diagonal matrices $S(\lambda(x_0))$ above with entries as in (8) is four-group decodable if take the values s_i from M-QAM and two group-decodable if take the s_i from M-HEX. Consequently, $\mathcal{C}$ has decoding complexity $\mathcal{O}(M^{(n-1)(2n)+n/2}) = \mathcal{O}(M^{2n^2-3n/2})$ if the s_i take values from M-QAM and decoding complexity $\mathcal{O}(M^{(n-1)(2n)+n}) = \mathcal{O}(M^{2n^2-n})$ if the s_i take values from M-HEX [2, Proposition 7 ff.]. □

5.2. Specific code examples. We build codes using $A = \mathrm{It}_R^n(D, \tau, d)$. The Alamouti code has the best coding gain among known 2 × 1 codes of rate one, hence in our examples in we will use $D = (-1, -1)_F$.

Our two code examples have high data rate and use the same algebras and automorphisms as the examples of [2]: Since the Alamouti code has the lowest ML-decoding complexity among the STBCs obtained from associative division algebras, the choice of D as a a subalgebra of Hamilton's quaternions in each example guarantees best possible fast decodability. The choice of L and K in [2] seems optimal to us as well since the extensions are related to the corresponding perfect STBCs in the respective dimensions.

5.3. An 6×3 MIMO System. Take the setup of [2, Section IV.C.]. Let $\omega = \frac{-1+\sqrt{3}i}{2}$ be a primitive third root of unity, $\theta = \zeta_7 + \zeta_7^{-1} = 2\cos(\frac{2\pi}{7})$, where ζ_7 is a primitive 7^{th} root of unity and let $F = \mathbb{Q}(\theta)$. Let $K = F(\omega) = \mathbb{Q}(\omega, \theta)$ and take $D = (K/F, \sigma, -1)$ as the quaternion division algebra. Note that $\sigma : i \mapsto -i$ and therefore $\sigma(\omega) = \omega^2$. Let $L = \mathbb{Q}(\omega)$, so that K/L is a cubic cyclic field extension whose Galois group is generated by the automorphism $\tau : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}$. We do not need to restrict our considerations to the sparse code as done in [2] in order to get a fully diverse code: $\omega \notin N_{K/L}(K^\times)$ and so $\mathrm{It}_R^3(D, \tau, \omega)$ is a division algebra by Theorem 17. Hence the code consisting of all matrices of the form

$$\begin{bmatrix} \lambda(x) & \omega\lambda(\widetilde{\tau}(z)) & \omega\lambda(\widetilde{\tau}^2(y)) \\ \lambda(y) & \lambda(\widetilde{\tau}(x)) & \omega\lambda(\widetilde{\tau}^2(z)) \\ \lambda(z) & \lambda(\widetilde{\tau}(y)) & \lambda(\widetilde{\tau}^2(x)) \end{bmatrix},$$

with x, y, z not all zero, is fully diverse. Write $x = x_0 + ex_1$, $y = y_0 + ey_1$, $z = z_0 + ez_1$, where $x_i, y_i, z_i \in K$, then its 6×6 matrix is given by

$$S = \begin{bmatrix} x_0 & -\sigma(x_1) & \omega\widetilde{\tau}(z_0) & -\omega\widetilde{\tau}\sigma(z_1) & \omega\widetilde{\tau}^2(y_0) & -\omega\widetilde{\tau}^2\sigma(y_1) \\ x_1 & \sigma(x_0) & \omega\widetilde{\tau}(z_1) & \omega\widetilde{\tau}\sigma(z_0) & \omega\widetilde{\tau}^2\sigma(y_1) & \omega\widetilde{\tau}^2\sigma(y_0) \\ y_0 & -\sigma(y_1) & \widetilde{\tau}(x_0) & -\widetilde{\tau}\sigma(x_1) & \omega\widetilde{\tau}^2(z_0) & -\omega\widetilde{\tau}^2\sigma(z_0) \\ y_1 & \sigma(y_0) & \widetilde{\tau}(x_1) & \widetilde{\tau}\sigma(x_0) & \omega\widetilde{\tau}^2(z_1) & \omega\widetilde{\tau}^2\sigma(z_1) \\ z_0 & \sigma(z_0) & \widetilde{\tau}(y_0) & -\widetilde{\tau}\sigma(y_1) & \widetilde{\tau}^2(x_0) & -\widetilde{\tau}^2\sigma(x_1) \\ z_1 & -\sigma(z_1) & \widetilde{\tau}(y_1) & \widetilde{\tau}\sigma(y_0) & \widetilde{\tau}^2(x_1) & \widetilde{\tau}^2\sigma(x_0) \end{bmatrix}.$$

With the encoding from 5.1, we encode 18 complex information symbols with each codeword S. The code has rate 3 for 6 transmit and 3 receive antennas, i.e. maximal rate.

We use M-HEX complex constellations and the notation from 5.1 (i.e., $s_j \in \mathbb{Z}[\omega]$): choose $\{\theta_1, \theta_2, \theta_3\}$ to be a basis of the principal ideal in $\mathcal{O}_K$ generated by θ_1 with $\theta_1 = 1 + \omega + \theta$, $\theta_2 = -1 - 2\omega + \omega\theta^2$, $\theta_3 = (-1 - 2\omega) + (1 + \omega)\theta + (1 + \omega)\theta^2$. Since all entries of the code matrix S lie in $\mathcal{O}_K$, here $\det(S) \in \mathcal{O}_L = \mathbb{Z}[\omega]$ by Lemma 19 (iii). Then the determinant of any nonzero codeword S is an element in $\mathbb{Z}[\omega]$ and, being fully diverse, the code has NVD which means the code is DMT-optimal [6]. Its minimum determinant (of the unnormalized code) is thus at least 1. By a similar argument as given in [2, C.], using a normalization factor of $1/\sqrt{28E}$, the normalized minimum determinant is

$$49\left(\frac{2}{\sqrt{28E}}\right)^{18} = 1/7^7 E^9.$$

Each codeword $S(\lambda(x_0)) = diag[\lambda(x_0), \tau(\lambda(x_0)), \tau(\lambda(x_0))]$ is 2-group decodable [2, Proposition 7]. $S(\lambda(x_0))$, $S(\lambda(x_1))$ and $S(\lambda(x_2))$ contain each 6 complex information symbols. By Proposition 22, the ML-decoding complexity of the code is at most $\mathcal{O}(M^{15})$ and the code is fast-decodable. We are no experts in coding theory but assume that hard-limiting the code as done in [2] might reduce the ML-complexity further, by a factor of $\sqrt{M}$, to at most $\mathcal{O}(M^{14.5})$.

In comparison, the fully diverse rate-3 VHO-code for 6 transmit and 3 receive antennas presented in [20, X.C] has a complexity of at most $\mathcal{O}(4M^{27})$. The fast decodable code rate-3 code for 6 transmit and 3 receive antennas proposed in [1, V.B] is not fully diverse and has decoding complexity $\mathcal{O}(M^{30})$.

5.4. An 8×4 MIMO System.

Let

(1) $\theta = \zeta_{15} + \zeta_{15}^{-1} = 2\cos\frac{2\pi}{15}$ where ζ_{15} is a primitive 15^{th} root of unity and $F = \mathbb{Q}(\theta)$;
(2) $K = F(i)$ and $D = (K/F, \sigma, -1)$ which is a subalgebra of Hamilton's quaternions;
(3) $L = \mathbb{Q}(i)$ so that K/L is a cyclic field extension of degree 4 with Galois group generated by the automorphism $\tau : \zeta_{15} + \zeta_{15}^{-1} \mapsto \zeta_{15}^2 + \zeta_{15}^{-2}$;
(4) $A = \mathrm{It}_R^4(D, \tau, i)$.

The associated code is

$$\mathcal{C}_{8\times 4} = \left\{ \begin{bmatrix} \lambda(x_0) & i\lambda(\widetilde{\tau}(x_3)) & i\lambda(\widetilde{\tau}^2(x_2)) & i\lambda(\widetilde{\tau}^3(x_1)) \\ \lambda(x_1) & \lambda(\widetilde{\tau}(x_0)) & i\lambda(\widetilde{\tau}^2(x_3)) & i\lambda(\widetilde{\tau}^3(x_2)) \\ \lambda(x_2) & \lambda(\widetilde{\tau}(x_1)) & \lambda(\widetilde{\tau}^2(x_0)) & i\lambda(\widetilde{\tau}^3(x_3)) \\ \lambda(x_3) & \lambda(\widetilde{\tau}(x_2)) & \lambda(\widetilde{\tau}^2(x_1)) & \lambda(\widetilde{\tau}^3(x_0)) \end{bmatrix} \right\}.$$

If $x_i = a_i + eb_i$ for $a_i, b_i \in K$, then

$$\lambda(x) = \begin{bmatrix} a_i & -\sigma(b_i) \\ b_i & \sigma(a_i) \end{bmatrix}.$$

With the encoding from 5.1, we encode 32 complex information symbols with each codeword S. The code has rate 4 for 8 transmit and 4 receive antennas which is maximal. Assuming $s_j \in \mathbb{Z}[i]$ are M-QAM-symbols and $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ is a basis of the principal ideal in $\mathcal{O}_K$ generated by $\theta_1 = \alpha = 1 - 3i + i\theta^2$ with $\theta_2 = \alpha\theta$, $\theta_3 = \alpha\theta(-3+\theta^2)$, $\theta_4 = \alpha(-1-3\theta+\theta^2+\theta^3)$. Since all entries of a code matrix $S \in \mathcal{C}_{8\times 4}$ lie in $\mathcal{O}_K$, $\det(S) \in \mathcal{O}_L = \mathbb{Z}[i]$ by Lemma 19 (iii).

By Proposition 22 or Corollary 23, the ML-decoding complexity of the code is at most $\mathcal{O}(M^{26})$ and the code is fast-decodable. Hard-limiting the code as done in [2] might reduce the ML-complexity further to $\mathcal{O}(M^{25.5})$.

We have $i \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)\widetilde{\tau}^3(z)$ for any $z \in D$ [2]. We are not able to check whether the code is fully diverse, since we cannot exclude the possibility that $F(t) = t^4 - i$ decomposes into two irreducible polynomials in $D[t; \widetilde{\tau}]$, we are only able to exclude some obvious cases.

6. Conclusion

One current goal in space-time block coding is to construct space-time block codes which are fast-decodable in the sense of [16], [17], [18] also when there are less receive than transmit antennas, support high data rates and have the potential to be systematically built for given numbers of transmit and receive antennas.

After obtaining conditions for the codes associated to the algebras $\mathrm{It}^n(D, \tau, d)$, $d \in F^\times$, and $\mathrm{It}^n_R(D, \tau, d)$, $d \in L \setminus F$, to be fully diverse, we construct fast decodable fully diverse codes for mn transmit and n receive antennas with maximum rate n out of fast decodable codes associated with central simple division algebras of degree m, for any choice of m and n. We thus answer the question for conditions to construct higher rare codes [2, VII.].

The conditions were simplified in the special case of a quaternion algebra D and an extension K/L with $[K : L] = 3$ in Theorem 17, yielding an easy way to construct fully diverse rate-3 codes for 6 transmit and 3 receive antennas. Since we are dealing with nonassociative algebras and skew polynomial rings, there is no well developed theory of valuations or similar yet which one could use to study the algebras over number fields. This would go beyond the scope of this paper and will be addressed in [19].

7. Acknowledgments

We would like to thank the referees for their comments and suggestions which greatly helped to improve the paper, and B. Sundar Rajan (Senior Member, IEEE) and L. P. Natarajan for allowing us to include Lemma 19 and Theorem 21.

References

[1] N. Markin, F. Oggier, "Iterated Space-Time Code Constructions from Cyclic Algebras," *IEEE Transactions on Information Theory*, vol. 59, no. 9, September 2013.

[2] K. P. Srinath, B. S. Rajan, "Fast-decodable MIDO codes with large coding gain", *IEEE Transactions on Information Theory* (2) 60 2014, 992-1007.

[3] J.-C. Petit, "Sur certains quasi-corps généralisant un type d'anneau-quotient", Séminaire Dubriel. Algèbre et théorie des nombres 20 (1966 - 67), 1–18.

[4] S. Pumplün, A. Steele, "Fast-decodable MIDO codes from nonassociative algebras," to appear in Int. J. of Information and Coding Theory (IJICOT). Available at `http://molle.fernuni-hagen.de/~loos/jordan/index.html`

[5] S. Pumplün, "How to obtain division algebras used for fast decodable space-time block codes", Adv. Math. Comm. 8 (3) (2014), 323 - 342.

[6] K. P. Srinath, B. S. Rajan, "DMT-optimal, low ML-complexity STBC-schemes for asymmetric MIMO systems." *2012 IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2012 , 3043-3047.

[7] S. Pumplün, "Tensor products of nonassociative cyclic algebras." Available at `http://molle.fernuni-hagen.de/~loos/jordan/index.html`

[8] 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.

[9] S. Pumplün, T. Unger, "Space-time block codes from nonassociative division algebras." Adv. Math. Comm. 5 (3) (2011), 609-629.

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

[11] W.C. Waterhouse, "Nonassociative quaternion algebras", *Algebras Groups Geom.* 4 (1987), no. 3, 365–378.

[12] Astier, V., Pumplün, S., "Nonassociative quaternion algebras over rings". *Israel J. Math.* 155 (2006), 125–147.

[13] Knus, M.A., Merkurjev, A., Rost, M., Tignol, J.-P., "The Book of Involutions", AMS Coll. Publications, Vol. 44 (1998).

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

[15] A. Steele, "Nonassociative cyclic algebras", Israel J. Math. 200 (1) (2014), 361-387.

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

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

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

[19] C. Brown, PhD Thesis University of Nottingham, in preparation.

[20] R. Vehkalahti, C. Hollanti, F. Oggier, "Fast-Decodable Asymmetric Space-Time Codes from Division Algebras", *IEEE Transactions on Information Theory*, (4) 58, April 2012.

[21] L. P. Natarajan, B. S. Rajan, written communication, 2013.

E-mail address: susanne.pumpluen@nottingham.ac.uk; pmxas4@nottingham.ac.uk

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