FAST-DECODABLE MIDO CODES FROM NONASSOCIATIVE ALGEBRAS

S. PUMPLÜN AND A. STEELE

Abstract. By defining a multiplication on a direct sum of n copies of a given cyclic division algebra, we obtain new unital nonassociative algebras. We employ their left multiplication to construct rate-n and rate-2 fully diverse fast ML-decodable space-time block codes for a multiple input-double output (MIDO) system. We give examples of fully diverse rate-2 4×2, 6×2, 8×2 and 12×2 space-time block codes and of a rate-3 6×2 code. All are fast ML-decodable. Our approach generalizes the iterated codes in [20].

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

Central simple associative division algebras over number fields, in particular cyclic division algebras, have been used to systematically build space-time block codes for an arbitrary number of antennas (cf. for instance [1], [2], [3], [4], [5], [6], [7]). Similarly built nonassociative division algebras can also be used in code design, see for instance [8], [9], [10] or [11]. In order to obtain a family of complex matrices which can be used as STBC, the matrix representing left multiplication in the (associative or nonassociative) algebra is calculated. In the process, the algebras are usually viewed as right K-vector spaces over a maximal subfield K, in order to obtain matrices with entries in K, which in a nonassociative setting is only possible for certain well behaved algebras.

Date: 14.10.2014.

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

Key words and phrases. Iterated space-time code constructions, nonassociative division algebras, fast-decodable, rate n, MIDO system.

The goal is to construct space-time codes which are fast-decodable in the sense of [12], [13], [14], also when there are less receive than transmit antennas, which support higher rates and have the potential to be systematically built for given numbers of transmit/receive antennas.

Fast-decodable codes are treated by Biglieri, Hong and Viterbo [15], Vehkalahti, Hollanti and Oggier [16], [17], Luzzi and Oggier [18], Markin and Oggier [19], and in [13], [14] and [9], to name just a few.

Srinath and Rajan [21] build fully diverse, rate-2 STBCs which are full-rate for MIDO systems and are fast ML-decodable, have large coding gain and non-vanishing determinant (NVD). Their approach uses certain nonassociative algebras in the code construction, employing as main ingredients a cyclic division algebra D over a field F and some invertible element $d \in D$. The resulting codes coincide with the iterated codes from Markin and Oggier [20], if $n = 2$ and if the element $d \in D$ used in the algebra (resp. code) construction lies in F.

We use a new family of nonassociative algebras to build fully diverse rate-2 and rate-3 fast-decodable MIDO codes. Again, we use a cyclic division algebra D over a field F and some invertible element $d \in D$ as main ingredients of the construction of the algebra. Our codes canonically generalize the iterated codes from [20] (for any invertible $d \in D$ used in the construction) and look very similar to the ones in [21]. The case $n = 2$ yields the nonassociative algebras and related iterated codes also mentioned in [11].

1.1. **Contribution and Organization.** We propose an algebraic construction to build rate-n (for n transmit antennas) fully diverse STBCs which canonically generalize the iterated codes from [20] and cannot be obtained through the left regular representation of some associative division algebra. The nonassociative algebras used in the construction can be viewed as generalizations of cyclic associative (or nonassociative) algebras. They generalize the nonassociative algebra behind the codes built in [20]. Their algebraic structure theory is similar to the classical one for associative cyclic algebras.

We show how to obtain STBCs using the left multiplication of these new nonassociative algebras and prove that division algebras yield fully diverse codes. We construct a fast-decodable rate-3 fully diverse STBC for a 6×2 MIDO system, which is two-group decodable.

We construct rate-2 fully diverse STBCs for 4×2, 6×2, 8×2 and 12×2 MIDO systems which look similar to the ones obtained in [21]. They have the same low ML-decoding complexity as the ones obtained in [21] and are fast-decodable. After the preliminaries in Section 2, we explain the mathematical model for our code construction in Section 3. Section 4 explains how the corresponding STBCs are designed and gives a condition for them to be fast-decodable, and Section 5 gives examples of fast-decodable STBCs for 4×2, 6×2, 8×2 and 12×2 MIDO systems. Section 6 discusses the ML-decoding complexity, Section 7 contains some simulation results, and Section 8 the conclusions and suggestions for future work.

2. Preliminaries

2.1. **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 $\mathcal{A}$, where the difference of any two code words has full rank, i.e. with $\det(X - X') \neq 0$ for all matrices $X \neq X'$, $X, X' \in \mathcal{A}$.

If the minimum determinant of the code, defined as

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

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

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

If $\mathcal{A}$ is fully diverse, $\delta(\mathcal{A})$ defines the *coding gain* $\delta(\mathcal{A})^{\frac{1}{n_t}}$. The larger $\delta(\mathcal{A})$ 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 [22]).

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 both the rate-n case (where mn^2 symbols are sent) and the rate-2 case. 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 $\mathcal{A}$ encodes s symbols. If the decoding complexity by sphere decoder needs only $\mathcal{O}(M^l)$, $l < s$ computations, then $\mathcal{A}$ is called *fast-decodable*.

For a matrix B, let B^* denote its Hermitian transpose. Consider a code $\mathcal{A}$ of rate n. Any $X \in \mathcal{A} \subset \mathrm{Mat}_{mn\times mn}(\mathbb{C})$ 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 $B_1, \ldots, B_{nm^2}$, 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 $\{1, \ldots, s\}$ into l nonempty subsets $\Gamma_1, \ldots, \Gamma_l$, so that $M_{g,k} = 0$, where g, k lie in disjoint subsets $\Gamma_i, \ldots, \Gamma_j$. The code $\mathcal{A}$ then has decoding complexity $\mathcal{O}(|S|^L)$, where $L = max_{1\leq i\leq l}|\Gamma_i|$.

2.2. **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 [23], pp. 15, 16. Let $A^\times = \{x \in A \,|\, x \text{ invertible}\}$. If A is a division algebra then $A^\times = A \setminus \{0\}$.

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, $x(yz) = (xy)z$ whenever one of the elements x, y, z is in $\mathrm{Nuc}(A)$.

2.3. **Cyclic Algebras.** Let K/F be a cyclic field extension of degree m with Galois group generated by the automorphism σ. For an element $\gamma \in F^\times$, the *cyclic algebra* $(K/F, \sigma, \gamma)$ of degree m is the right K-vector space

$$K \oplus eK \oplus e^2K \oplus \cdots \oplus e^{m-1}K,$$

with multiplication defined by the rules $ke = e\sigma(k)$ and $e^m = \gamma$. The associative and distributive laws then give us the full multiplication for the algebra $(K/F, \sigma, \gamma)$. The set $\{1, e, e^2, \ldots, e^{m-1}\}$ is called the standard basis for the cyclic algebra (viewed as a right K-vector space). A cyclic algebra is called a *division algebra* if it contains no zero divisors. $(K/F, \sigma, \gamma)$ is a division algebra for all $\gamma \in F^\times$ with $\gamma^s \notin N_{K/F}(K^\times)$ for all s, $1 \leq s \leq m-1$, which are prime divisors of m.

Let $a = a_0 + ea_1 + \cdots + e^{m-1}a_{m-1} \in (K/F, \sigma, \gamma)$. The left regular representation $\lambda(a)$ of a yields an $m \times m$ matrix with entries in K:

$$\lambda(a) = \begin{bmatrix} a_0 & \gamma\sigma(a_{m-1}) & \gamma\sigma^2(a_{m-2}) & \cdots & \gamma\sigma^{m-1}(a_1) \\ a_1 & \sigma(a_0) & \gamma\sigma^2(a_{m-1}) & \cdots & \gamma\sigma^{m-1}(a_2) \\ a_2 & \sigma(a_1) & \sigma^2(a_0) & \cdots & \gamma\sigma^{m-1}(a_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m-1} & \sigma(a_{m-2}) & \sigma^2(a_{m-3}) & \cdots & \sigma^{m-1}(a_0) \end{bmatrix}. \tag{1}$$

If we represent elements of $(K/F, \sigma, \gamma)$ as column vectors $a = (a_0, a_1, \ldots, a_{m-1})^T$, $b = (b_0, b_1, \ldots, b_{m-1})^T$, then we can write the multiplication in $(K/F, \sigma, \gamma)$ as the matrix multiplication

$$ab = \lambda(a)b.$$

It follows that if a is not a left zero divisor in $(K/F, \sigma, \gamma)$, i.e. $ab = 0$ if and only if $b = 0$, then the matrix $\lambda(a)$ is invertible. Let $D = (K/F, \sigma, \gamma)$ be a cyclic algebra of degree m, then the left regular representation $\lambda : D \to Mat_{m\times m}(K)$ is an algebra homomorphism, i.e. $\lambda(x)\lambda(y) = \lambda(xy)$ for all $x, y \in D$. Moreover, if D is a division algebra then the set $\{\lambda(a) \mid 0 \neq a \in D\}$ is an infinite set of invertible matrices and gives rise to a fully diverse linear STBC when we work over appropriate base fields (usually number fields).

3. Mathematical background: an iterated construction method for nonassociative algebras out of associative cyclic algebras

In the following, let F and L be fields, 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: $\sigma\tau = \tau\sigma$

and $F_0 = L \cap F$. Let $D = (K/F, \sigma, \gamma)$ be a cyclic division algebra of degree m for some suitable element $\gamma \in F_0$. For $x = x_0 + ex_1 + e^2x_2 + \cdots + e^{n-1}x_{n-1} \in D$, define the L-linear map $\widetilde{\tau} : D \to D$ via

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

Definition 1. Pick $d \in D^\times$ and define an algebra multiplication on the right D-module

$$It^n(D, \tau, d) = D \oplus fD \oplus f^2D \oplus \cdots \oplus f^{n-1}D$$

with basis $1, f, \ldots, f^{n-1}$ by the rules

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

for all $x, y \in D$.

$It^n(D, \tau, d)$ is a unital nonassociative algebra over F_0. For $n = 2$, this algebra is studied in [11]; it is implicitly used in the iterated codes constructed in [20].

Remark 1. (i) Our assumption that γ is also an element of L implies that $\widetilde{\tau}(xy) = \widetilde{\tau}(x)\widetilde{\tau}(y)$ for all $x, y \in D$.
(ii) The fact that $\tau(\gamma) = \gamma$ also implies that $\lambda(\widetilde{\tau}(x)) = \tau(\lambda(x))$ for all $x \in D$, where, for any matrix X, $\tau(X)$ means applying τ to each entry of the matrix. In particular, this means that for $d \in D^\times$, the condition that $d \neq z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{n-1}(z)$ for all $z \in D$ is equivalent to $\lambda(d) \neq Z\tau(Z)\cdots\tau^{n-1}(Z)$ for all $Z = \lambda(z) \in \lambda(D)$.
(iii) $A = It^n(D, \tau, d)$ is a right D-module and left multiplication λ_x in A is a D-linear map, so that we have a well-defined injective additive map $\lambda : A \to \mathrm{End}_D(A) \subset \mathrm{Mat}_n(D), \quad x \mapsto \lambda_x$ and we can consider the matrix given by left multiplication with entries in D.
(iv) If $d \in F^\times$, the algebra $It^n(D, \tau, d)$ is identical to the algebra used in [21]: The multiplication of the algebra $It^n_R(D, \tau, d)$ used in [21] is defined on the right K-module $D \oplus fD \oplus f^2D \oplus \cdots \oplus f^{n-1}D$ via

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

for all $x, y \in D$, hence is different when $i + j \geq n$ and $d \notin F$: the coefficient of $f^{(i+j)-n}$ in the product is $d\widetilde{\tau}^j(x)y$. Only by choosing $d \in L^\times$, this left multiplication λ_x becomes a K-endomorphism and can be represented by a matrix with entries in K. (This is why $d \in L \setminus F$ is assumed in the design procedure of the codes of [21].)

The difference between our codes and those in [21] is that in our codes, the matrix multiplication $\lambda(d)\tau^i(\lambda(x_i))$ will appear as entries above the main diagonal, whereas in [21], the corresponding entries are given by scalar multiplication $d\tau^i(\lambda(x_i))$, with d being restricted to be an element of L. We give conditions for both our codes and the ones treated in [21] to be fully diverse, see Theorem 6.

For $x = x_0 + fx_1 + f^2x_2 + \cdots + f^{n-1}x_{n-1} \in It^n(D, \tau, d)$, where $x_i \in D$, we define the $n \times n$ matrix

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

with entries in D. If we represent $y = y_0 + fy_1 + \cdots f^{n-1}y_{n-1} \in It^n(D, \tau, d)$ as a column vector $(y_0, y_1, \ldots, y_{n-1})^T$, where each $y_i \in D$, then we can write the product of $x, y \in$

$It^n(D,\tau,d)$ as the matrix multiplication

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

Since D is a right K-vector space of dimension m, $It^n(D,\tau,d)$ is a right K-vector space of dimension mn. If $\{1, e, \ldots, e^{m-1}\}$ is the standard basis for D, then

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

is a basis for $It^n(D,\tau,d)$ as a right K-vector space. Taking this into consideration, we write elements in $It^n(D,\tau,d)$ as column vectors of length mn with entries in K. We can now express the product of two elements $x, y \in It^n(D,\tau,d)$ by the matrix multiplication

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

where $\lambda(M(x))$ is the $mn \times mn$ matrix defined by taking the left regular representation of each entry in the matrix $M(x)$. We write the matrix $\lambda(M(x))$ as

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

with $x_i \in D$; it is the matrix of left multiplication by the element x.

Theorem 2. *Let $D = (K/F, \sigma, \gamma)$ be a cyclic division algebra and let $A = It^n(D,\tau,d)$ for some $d \in D$.*
(i) For all $x = x_0 + fx_1 + \cdots + f^{n-1}x_{n-1} \in A$, $\det(\lambda(M(x)) \in F$.
(ii) If $d \in F_0$ then $\det(\lambda(M(x))) \in F_0$.
(iii) A is division if and only if $\lambda(M(x))$ is an invertible matrix for all non-zero $x \in A$.
(iv) If all the elements of $\lambda(M(x))$ belong to $\mathcal{O}_K$, the ring of integers of K (i.e. $\gamma \in \mathcal{O}_L$), then $\det(\lambda(M(x)) \in F \cap \mathcal{O}_K = \mathcal{O}_F$.

Proof. (i) Clearly $\det(\lambda(M(x)) \in K$. To show it belongs to F we calculate $\sigma(\det(\lambda(M(x))) = \det(\sigma(\lambda(M(x)))$. For all elements $u = u_0 + eu_1 + \cdots e^{m-1}u_{m-1} \in D$, we have $\lambda(u) = P\sigma(\lambda(x))P^{-1}$ where P is the matrix

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & \gamma \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix},$$

and P^{-1} is the matrix

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \gamma^{-1} & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

In particular, this is also true for the entries $\lambda(d)\lambda(\widetilde{\tau}^i(x))$ which appear above the main diagonal in the matrix $\lambda(M(x))$ since they are again representations of elements in D. It follows that

$$\lambda(M(x)) = \mathrm{diag}[P, P, \ldots, P]\sigma(\lambda(M(x)))\mathrm{diag}[P^{-1}, \ldots, P^{-1}],$$

and thus $\det(\sigma(\lambda(M(x))) = \det(\lambda(M(x)))$.
(ii) If $d \in F_0$, then the matrix $\lambda(M(x))$ is exactly the matrix M considered in [21] in which it is shown that the determinant belongs to L.
(iii) is proved in [26] and (iv) follows from (ii). □

Matrices representing left multiplication with elements in $It^n(D, \tau, d)$ will form our space-time codes. Because the matrices $\lambda(M(x))$ define multiplication in $It^n(D, \tau, d)$, we get the following, more general, version of Theorem 2 in [21].

Theorem 3. *Let $A = It^n(D, \tau, d)$ and let $x \in A$ be nonzero. If x is not a left zero divisor in A, then the matrix of left multiplication by x, $\lambda(M(x))$ has nonzero determinant. In particular, if $C \subseteq A$ is a linear subset of A such that every $x \in C$ is not a left zero divisor, then*

$$\mathcal{C} = \{\lambda(M(x)) \mid x \in C\}$$

forms a fully diverse, linear STBC.

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

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

has a non-trivial solution $(y_0, \ldots, y_{mn-1}) \in K^{mn}$ which contradicts the assumption that x is not a left zero divisor in A. □

Employing that $D = \mathrm{Nuc}_m(\mathrm{It}^n(D, \tau, d))$ [26] and following the proof of in [21, Theorem 1] (note that $D \subset \mathrm{Nuc}_m(\mathrm{It}^n_R(D, \tau, d))$ is also required for the proof of [21, Theorem 1] to work), we obtain:

Theorem 4. *Let $D = (K/F, \sigma, \gamma)$ be a cyclic division algebra of degree m such that $\gamma \in L$ and let $A = It^n(D, \tau, d)$. All elements in A of the form $x = x_0 + fx_1$ are not left zero divisors if and only if $d \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)\ldots\widetilde{\tau}^{n-1}(z)$ for all $z \in D$.*

Corollary 5. *Let $D = (K/F, \sigma, \gamma)$ be a cyclic division algebra of degree m such that $\gamma \in L$ and let $A = \mathrm{It}^n(D, \tau, d)$.*
(i) If $N_{D/F}(d) \neq a\tau(a)\cdots\tau^{n-1}(a)$ for all $a \in N_{D/F}(D^\times)$, then all elements in A of the form $x = x_0 + fx_1$ are not left zero divisors.
(ii) Suppose $F \subset L$ and $N_{D/F}(d) \notin N_{D/F}(D^\times)^n$, then all elements in A of the form $x = x_0 + fx_1$ are not left zero divisors.
(iii) Suppose F/F_0 is a cyclic extension of degree n with Galois group generated by the automorphism τ. If $N_{D/F}(d) \notin N_{F/F_0}(F)$, then all elements of A of the form $x = x_0 + fx_1$ are not left zero divisors.

Proof. Let $N_{D/F}$ be the norm of D. Since $\gamma \in \mathrm{Fix}(\tau) = L$ we have $N_{D/F}(\widetilde{\tau}(x)) = \tau(N_{D/F}(x))$ for all $x \in D$ by [11], Proposition 4. Assume $d = z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{n-1}(z)$, then

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

Put $a = N_{D/F}(z)$ to obtain (i). If additionally $F \subset L = \mathrm{Fix}(\tau)$, this means that $N_{D/F}(d) = N_{D/F}(z)^n$ and we have proved (ii). Since $N_{D/F}(z) \in F$ for all $z \in D$ and $N_{F/F_0}(u) = u\tau(u)\ldots\tau^{n-1}(u)$ for all u in F, (iii) follows directly from (i). □

More generally, we know:

Theorem 6. *Let $A = \mathrm{It}^n(D, \tau, d)$, $d \in F^\times$, or $A = \mathrm{It}^n_R(D, \tau, d)$, and $\mathcal{C} = \{\lambda(M(x)) \mid x \in A\}$.*
(i) $\mathcal{C}$ is a fully diverse, linear STBC 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 F_0 contains a primitive nth root of unity. Then $\mathcal{C}$ is a fully diverse, linear STBC 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) Suppose that $n = 3$. Then $\mathcal{C}$ is a fully diverse, linear STBC if and only if

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

for all $z \in D$.

Proof. $\mathcal{C}$ is a fully diverse, linear STBC if and and only if A is a division algebra by Theorem 2. Now A is a division algebra if and only if
(i) $f(t) = t^n - d \in D[t; \widetilde{\tau}^{-1}]$ is irreducible [26].
(ii) $d \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)\cdots\widetilde{\tau}^{n-1}(z)$ and $\widetilde{\tau}^{n-1}(d) \neq z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{n-1}(z)$ for all $z \in D$ [26].
(iii) $d \neq z\widetilde{\tau}(z)\widetilde{\tau}(z)^2$ and $\widetilde{\tau}^2(d) \neq z\widetilde{\tau}(z)\widetilde{\tau}(z)^2$ for all $z \in D$ [26]. □

Analogously, using results from [26], we obtain:

Proposition 7. *Let $A = \mathrm{It}^n(D,\tau,d)$ and $d \in F$, or $A = \mathrm{It}^n_R(D,\tau,d)$, and $\mathcal{C} = \{\lambda(M(x)) \mid x \in A\}$.*
(i) Suppose that n is prime and 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 $\mathcal{C}$ is a fully diverse, linear STBC.
(ii) Let $n = 3$. If $\tau(d^m) \neq d^m$ and $\tau^2(d^m) \neq d^m$ for all $z \in D$, then $\mathcal{C}$ is a fully diverse, linear STBC.

We refer the reader to [26] for some additional criteria for A to be a division algebra, which make the corresponding $\mathcal{C}$ a fully diverse, linear STBC.

3.1. **Special Case:** If $n = 2$ in Definition 1, $A = It^2(D,\tau,d) = D \oplus fD$ for some cyclic division algebra D, cf. [20] and [11]. $\mathrm{It}^2(D,\tau,d)$ is a division algebra if and only if $d \neq z\widetilde{\tau}(z)$ for all $z \in D^\times$ [11]. The fully diverse STBC corresponding to our construction then consists of the matrices

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

of left multiplication by elements in the division algebra A, where $x_0, x_1 \in D$.

Example 8. Suppose that D is a quaternion division algebra and let $d = d_0 + ed_1 \in D$ be such that $d \neq z\widetilde{\tau}(z)$ for all $z \in D$. Let $x = x_0 + ex_1, y = y_0 + ey_1 \in D^\times$, where $x_i, y_i \in K$. Then

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

The matrix of left multiplication by the element $x + fy \in A = It^2(D,\tau,d)$ is represented by

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

with

$$\lambda(d)\tau(\lambda(y)) = \begin{bmatrix} d_0\tau(y_0) + \gamma\sigma(d_1)\tau(y_1) & \gamma(d_0\sigma\tau(y_1) + \sigma(d_1)\sigma\tau(y_0)) \\ d_1\tau(y_0) + \sigma(d_0)\tau(y_1) & d_1\gamma\sigma\tau(y_1) + \sigma(d_0)\sigma\tau(y_0) \end{bmatrix} = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix}.$$

Thus, the 4×4 matrix of left multiplication by $x + fy$ is given by

$$\begin{bmatrix} x_0 & \gamma\sigma(x_1) & u_1 & u_2 \\ x_1 & \sigma(x_0) & u_3 & u_4 \\ y_0 & \gamma\sigma(y_1) & \tau(x_0) & \gamma\tau(\sigma(x_1)) \\ y_1 & \sigma(y_0) & \tau(x_1) & \tau(\sigma(x_0)) \end{bmatrix}.$$

Since by our assumption that $\gamma \in F_0$, the algebra D is defined over F_0, we know that for all choices of $d \in F \setminus F_0$, this code always is fully diverse and in fact, represents left multiplication in the tensor product of two quaternion algebras, one of them nonassociative [26, Theorem 14]. (Even for $d \in L$, these are still different codewords to those built in [21, p. 5], since by assumption, σ acts non-trivially on L.)

Example 9. Let $F = \mathbb{Q}(\sqrt{5})$ and let K be the quadratic extension of F, $K = \mathbb{Q}(i, \sqrt{5})$. The automorphism $\sigma : K \to K$ is defined by $\sigma(i) = -i$. Let D be the quaternion algebra $(\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(\sqrt{5}), \sigma, -1) = (-1, -1)_{\mathbb{Q}(\sqrt{5})}$ which is a subalgebra of Hamilton's quaternion algebra and, therefore, is a division algebra.

Let $L = \mathbb{Q}(i)$ so that K/L is a quadratic separable field extension with nontrivial automorphism $\tau : \sqrt{5} \mapsto -\sqrt{5}$. The algebra $It^2(D, \tau, i)$ will be considered later in Section 5; here we give a few more examples when $It^2(D, \tau, d)$ is a division algebra for some $d \in D$.

Let $\varphi = \frac{1+\sqrt{5}}{2}$ be the golden ratio. Consider $\varphi = \varphi + e0 \in D$, then $N_{D/F}(\varphi) = \varphi^2 \notin \mathbb{Q}$ so by Corollary 5 (iii), $It^2(D, \tau, \varphi)$ is a division algebra. Similarly we could consider $d = 0 + e\varphi$. Again $N_{D/F}(d) = \varphi^2$, so $It^2(D, \tau, d)$ is division and we get another fully diverse code.

Example 10. Suppose that $D = (K/F, \sigma, \gamma)$ is a cyclic division algebra of degree 3 and let $d \in K$. Let $x = x_0 + ex_1 + e^2x_2, y = y_0 + ey_1 + e^2y_2 \in D$ where each $x_i, y_i \in K$. Then

$$\lambda(x) = \begin{bmatrix} x_0 & \gamma\sigma(x_2) & \gamma\sigma^2(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) \end{bmatrix}.$$

We have $\lambda(d) = \mathrm{diag}[d, \sigma(d), \sigma^2(d)]$. For the element $x + fy \in It^2(D, \tau, d) = A$, the 6×6 left multiplication matrix is given by

$$\begin{bmatrix} x_0 & \gamma\sigma(x_2) & \gamma\sigma^2(x_1) & d\tau(y_0) & d\gamma\tau\sigma(y_2) & d\gamma\tau\sigma^2(y_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_2) & \sigma(d)\tau(y_1) & \sigma(d)\tau\sigma(y_0) & \sigma(d)\gamma\tau\sigma^2(y_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & \sigma^2(d)\tau(y_2) & \sigma^2(d)\tau\sigma(y_1) & \sigma^2(d)\tau\sigma^2(y_0) \\ y_0 & \gamma\sigma(y_2) & \gamma\sigma^2(y_1) & \tau(x_0) & \gamma\tau\sigma(x_2) & \gamma\tau\sigma^2(x_1) \\ y_1 & \sigma(y_0) & \gamma\sigma^2(y_2) & \tau(x_1) & \tau\sigma(x_0) & \gamma\tau\sigma^2(x_2) \\ y_2 & \sigma(y_1) & \sigma^2(y_0) & \tau(x_2) & \tau\sigma(x_1) & \tau\sigma^2(x_0) \end{bmatrix}.$$

4. Design Procedure for Space-Time Block Codes

4.1. To construct fully diverse space-time block codes for mn transmit antennas we make the following assumptions.

(1) Let L, F be number fields, and L or F be either $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$, where ω is a primitive third root of unity. This allows us to use the QAM constellation (a finite subset of $\mathbb{Z}(i)$) or the HEX constellation (a finite subset of $\mathbb{Z}(\omega)$).
(2) Let $D = (K/F, \sigma, \gamma)$ be a cyclic division algebra of degree m over F, where K is a cyclic extension of L of degree n with Galois group generated by τ.
(3) σ and τ commute.
(4) $\gamma \in F_0$.
(5) $A = It^n(D, \tau, d)$ with $d \in D$ is such that $f(t) = t^n - d \in D[t; \widetilde{\tau}^{-1}]$ is irreducible, or, if we look at the sparse codes treated in 4.2, such that $d \neq z\widetilde{\tau}(z) \dots \widetilde{\tau}^{n-1}(z)$.

Remark 11. If L is either $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$ and we want the code to have NVD we have to choose $d \in \mathcal{O}_{F_0}$, such that $A = It^n(D, \tau, d)$ is division. Then $\det(X) \in L$ for all X in the

code built using left multiplication in A and the code has NVD, if all matrix entries are chosen in $\mathcal{O}_K$. If F is $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$ and $d \in \mathcal{O}_K$ is such that $It^n(D, \tau, d)$ is division then $\det(X) \in \mathcal{O}_F$ for all X in that code and the code has NVD, if all matrix entries are chosen in $\mathcal{O}_K$.
The next step depends on whether F or L is $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$. It L is either $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$ then proceed as described in the following, if F is either $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$, adjust the next step and consider matrix entries as linear combinations of m linear independent entries in F etc.

Each codeword in $\mathcal{C}$ is a matrix of the form given in (2), 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 $\{\theta_1, \theta_2, \ldots, \theta_n \mid \theta_i \in \mathcal{O}_K\}$ over $\mathcal{O}_L$. Thus an entry $\lambda(x)$ has the form

$$\lambda(x) = \begin{bmatrix} \sum_{i=1}^{n} s_i\theta_i & \gamma\sigma(\sum_{i=1}^{n} s_{i+nm-n}\theta_i) & \ldots & \gamma\sigma^{m-1}(\sum_{i=1}^{n} s_{i+n}\theta_i) \\ \sum_{i=1}^{n} s_{i+n}\theta_i & \sigma(\sum_{i=1}^{n} s_i\theta_i) & \ldots & \gamma\sigma^{m-1}(\sum_{i=1}^{n} s_{i+2n}\theta_i) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^{n} s_{i+nm-n}\theta_i & \sigma(\sum_{i=1}^{n} s_{i+nm-2n}\theta_i) & \ldots & \sigma^{m-1}(\sum_{i=1}^{n} s_i\theta_i) \end{bmatrix}. \tag{3}$$

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.

Proposition 12. *If mn channels are used the space-time block code $\mathcal{C}$ consisting of matrices S of the form (2) with entries as in (3) has a rate of n complex symbols per channel use.*

Proof. The matrices S encode $n \times mn$ independent complex information symbols in mn channel uses giving a rate of n complex symbols per channel use. □

If the decoding complexity of $\mathcal{C}$ is less than $\mathcal{O}(M^{mn^2})$, then $\mathcal{C}$ is fast-decodable.

Lemma 13. *If the subset of codewords in $\mathcal{C}$ made up of the diagonal block matrix*

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

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

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

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

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 (2). 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 $\mathcal{O}(M^{(n-1)(nm)+nm/l}) = \mathcal{O}(M^{mn^2-mn(l-1)/l})$ □

Example 14. If $D = \mathrm{Cay}(K/F, -1)$ is a quaternion division algebra which is a subalgebra of Hamilton's quaternion algebra (i.e., σ commutes with complex conjugation here), then a code consisting of the block diagonal matrices

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

with entries as in (3) is four-group decodable if take the values s_i from M-QAM and two group-decodable if take the values 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 [21, Proposition 7 and text after]. Therefore both times it is fast-decodable, since this is less than $\mathcal{O}(M^{2n^2})$. Recall that the Alamouti code has the best coding gain among known 2×1 codes of rate one, so in our examples in 5.1, 5.4, 5.5, we will use $D = (-1, -1)_F$.

4.2. Codes with sparse entries. Consider the linear subset $\{x + fy \,|\, x, y \in D, (x, y) \neq (0, 0)\}$ of A. By Theorem 4, this subset contains no left zero divisors of A. Our codes will consist of the matrices

$$\begin{bmatrix} \lambda(x) & 0 & \ldots & \lambda(d)\lambda(\widetilde{\tau}^{n-1}(y)) \\ \lambda(y) & \lambda(\widetilde{\tau}(x)) & \ldots & 0 \\ 0 & \lambda(\widetilde{\tau}(y)) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda(\widetilde{\tau}^{n-1}(x)) \end{bmatrix} \tag{4}$$

representing left multiplication with these elements, where $\lambda(x)$ is the $m \times m$ matrix given by the left regular representation of D. For $x \neq 0$, these are invertible $mn \times mn$ matrices with entries in K.

Proposition 15. *If mn channels are used the space-time block code consisting of matrices of the form given in (4) with entries as in (3) has a rate of 2 complex symbols per channel use.*

Proof. The matrices of (4) encode $2mn$ independent complex information symbols in mn channel uses giving a rate of 2 complex symbols per channel use. □

For the analysis of the ML-decoding complexity of such codes, the reader is referred to Section 6.

Remark 16. For the code constructions in [21], it is assumed that $d \in L \setminus F$ and that $L \neq F$. We do not assume that $L \neq F$ and do not restrict the choice of $d \in D$. Comparing their code matrices with ours, we note:

If $d \in F$ they would have the same shape (however, this case is not studied in [21]).
If $d \in L \setminus F$ (or even $d \in K \setminus L$), they differ.
Moreover, we do not need to restrict ourselves to sparse matrices with many zero entries anymore as was done in [21], since for $d \in F^\times$ we have conditions on the whole set of matrices to be a fully diverse code. We can therefore construct fast-decodable codes of rate n.

5. Specific Code Examples

We give five specific code examples using the same algebras and automorphisms as in the examples of [21]. Since the Alaouti code has the lowest ML-decoding complexity among the STBCs obtained from associative division algebras, the division algebra D will be a subalgebra of Hamilton's quaternions in each example. The choice of the extensions L and K from [21] seems optimal since they are related to the corresponding perfect STBCs in the respective dimensions. The code matrices obtained this way thus look similar to the ones of [21], and although both of our codes do not have NVD, the codeword error rates for the sparse 6×2 and 6×2 MIDO codes we present in 5.2 and 5.4 are similar.

Thus although the NVD property is sufficient for these types of asymmetric MIDO codes to have DMT-optimality [22], it may not always be required.

One advantage of our codes is that for $d \in F$ we have conditions for the underlying algebras to be division, and thus do not need to rely on Theorem 3 to build fully diverse ones, i.e. we can also build fully diverse codes which do not have zero entries using Theorem 6. We now also can build codes without zero entries using $A = \mathrm{It}_R^n(D, \tau, d)$ which we do in 5.3.

5.1. A 4×2 MIDO System. Let $F = \mathbb{Q}(\sqrt{5})$ and let K be the quadratic extension of F, $K = \mathbb{Q}(i, \sqrt{5})$. The automorphism $\sigma : K \to K$ is defined by $\sigma(i) = -i$. Let D be the quaternion algebra $(\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(\sqrt{5}), \sigma, -1) = (-1, -1)_{\mathbb{Q}(\sqrt{5})}$ which is a subalgebra of Hamilton's quaternion algebra and, therefore, is a division algebra.

Let $L = \mathbb{Q}(i)$ so that K/L is a quadratic separable field extension with nontrivial automorphism $\tau : \sqrt{5} \mapsto -\sqrt{5}$. Let $A = It^2(D, \tau, i)$. It was shown in [21, Proposition 3] that $i \neq z\widetilde{\tau}(z)$ for any $z \in D$ and so A is a division algebra by Theorem 4. It follows that the matrices of left multiplication by nonzero elements $x + fy \in A$, where $x = x_0 + ex_1, y = y_0 + ey_1 \in D^\times$, are invertible. Following the design procedure in the previous section and Example 8, our codewords are

$$\mathcal{C}_{4\times 2} = \left\{ \begin{bmatrix} x_0 & -\sigma(x_1) & i\tau(y_0) & -i\sigma\tau(y_1) \\ x_1 & \sigma(x_0) & -i\tau(y_1) & -i\sigma\tau(y_0) \\ y_0 & -\sigma(y_1) & \tau(x_0) & -\sigma\tau(x_1) \\ y_1 & \sigma(y_0) & \tau(x_1) & \sigma\tau(x_0) \end{bmatrix} \right\}. \tag{5}$$

We have $x_i = x_{i0}\theta_1 + x_{i1}\theta_2$ and $y_i = y_{i0}\theta_1 + y_{i1}\theta_2$ for $i = 0, 1$, where $\{\theta_1, \theta_2\}$ is a suitable $\mathbb{Q}(i)$ basis for $\mathbb{Q}(i, \sqrt{5})$ and each x_{ij} and y_{ij} take values in M-QAM $\subset \mathbb{Z}(i)$. Following [7], we pick $\theta_1 = \alpha, \theta_2 = \alpha\theta$, where $\alpha = 1 + i(1 - \theta)$ and $\theta = (1 + \sqrt{5})/2$ so that $\{\alpha, \alpha\theta\}$ is a basis of a principal ideal of $\mathcal{O}_K$ generated by α. By Theorem 2 (iv), the determinant of any nonzero codeword is an element in $\mathcal{O}_F$.

Remark 17. We observe that for all non-zero $a = a_0 + \sqrt{5}a_1$ 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 $x = x_0 + ix_1 + jx_2 + ijx_3 \in D$, we get $N_{K/F}(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2 \in \mathbb{Q}(\sqrt{5})$ with $x_i \in \mathbb{Q}(\sqrt{5})$. By Corollary 5, hence any $d \in D$ such that $N_{K/F}(d) \notin \mathbb{Q}$ will yield a division algebra $\mathrm{It}^2(D, \tau, d)$ and therefore a fully diverse code. E.g., any $d = d_0 + \sqrt{5}d_1$ with $d_0, d_1 \in \mathbb{Q}^\times$, will yield a division algebra $\mathrm{It}^2(D, \tau, d)$.

5.2. A 6×2 MIDO System. Let ω denote the primitive third root of unity and $\theta = \zeta_7 + \zeta_7^{-1} = 2\cos(\frac{2\pi}{7})$ 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 the quaternion division algebra $D = (K/F, \sigma, -1)$. Note that $\sigma : i \mapsto -i$ and therefore $\sigma(\omega) = \omega^2$. Finally, we let $L = \mathbb{Q}(\omega)$ so that K/L is a cubic cyclic field extension whose Galois group is generated by the automorphism $\tau : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}$. It was shown in [21] that $\omega \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)$ for all $z \in D$, therefore, in the algebra $A = It^3(D, \tau, \omega)$, all elements of the form $x + fy$ are not left zero divisors where $x, y \in D$ are nonzero. It follows that the code consisting of all matrices of the form

$$\begin{bmatrix} \lambda(x) & 0 & \lambda(\omega)\lambda(\widetilde{\tau}^2(y)) \\ \lambda(y) & \lambda(\widetilde{\tau}(x)) & 0 \\ 0 & \lambda(\widetilde{\tau}(y)) & \lambda(\widetilde{\tau}^2(x)) \end{bmatrix},$$

where x, y are not both zero, is fully diverse. If $x = x_0 + ex_1$ and $y = y_0 + ey_1$ where $x_i, y_i \in K$, then the 6×6 matrix is given by

$$\begin{bmatrix} x_0 & -\sigma(x_1) & 0 & 0 & \omega\tau^2(y_0) & -\omega\tau^2\sigma(y_1) \\ x_1 & \sigma(x_0) & 0 & 0 & \omega^2\tau^2\sigma(y_1) & \omega^2\tau^2\sigma(y_0) \\ y_0 & -\sigma(y_1) & \tau(x_0) & -\tau\sigma(x_1) & 0 & 0 \\ y_1 & \sigma(y_0) & \tau(x_1) & \tau\sigma(x_0) & 0 & 0 \\ 0 & 0 & \tau(y_0) & -\tau\sigma(y_1) & \tau^2(x_0) & -\tau^2\sigma(x_1) \\ 0 & 0 & \tau(y_1) & \tau\sigma(y_0) & \tau^2(x_1) & \tau^2\sigma(x_0) \end{bmatrix}.$$

Again, following [7], we let $\theta_1 = 1 + \omega + \theta$, $\theta_2 = -1 - 2\omega + \omega\theta^2$ and $\theta_3 = (-1 - 2\omega) + (1 + \omega)\theta + (1 + \omega)\theta^2$ so that $\{\theta_1, \theta_2, \theta_3\}$ is a basis of a principal ideal in $\mathcal{O}_K$ generated by θ_1. Thus, taking $x_i = x_{i1}\theta_1 + x_{i2}\theta_2 + x_{i3}\theta_3$, $y_i = y_{i1}\theta_1 + y_{i2}\theta_2 + y_{i3}\theta_3$, where the x_{ij}, y_{ij} are values in the M-HEX $\subset \mathbb{Z}[\omega]$ constellation, we encode 12 complex information symbols with each codeword. By Theorem 2, the determinant of any nonzero codeword is an element in $\mathcal{O}_F$.

5.3. Take the setup in Section 5.2 and note that $\widetilde{\tau}^2(\omega)=\omega$, thus also $\omega \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)$ for all $z \in D$ and so the algebra $It_R^3(D,\tau,\omega)$ behind the codes employed in [21] (cf. [26]) is division. Thus

$$\mathcal{C}_{6\times 2}=\begin{bmatrix} \lambda(x) & \omega\lambda(\widetilde{\tau}(z)) & \omega\lambda(\widetilde{\tau}^2(y)) \\ \lambda(y) & \lambda(\widetilde{\tau}(x)) & \omega\lambda(\widetilde{\tau}^2(z)) \\ \lambda(z) & \lambda(\widetilde{\tau}(y)) & \lambda(\widetilde{\tau}^2(x)) \end{bmatrix}, \tag{6}$$

with x,y,z not all zero, is a fully diverse code. 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 a 6×6 matrix in $\mathcal{C}_{6\times 2}$ is given by

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

and the code has rate 3. With the same encoding as in 5.2., we encode 18 complex information symbols with each codeword S. By [21], the determinant of any nonzero codeword S is an element in $\mathcal{O}_L$ and the code has NVD.

5.4. An 8×2 MIDO 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) $A=It^4(D,\tau,i)$.

It was shown in [21] that $i\neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)\widetilde{\tau}^3(z)$ for any $z\in D$ and hence elements of the form $x+fy\in A$, $x,y\in D$ nonzero, are not left zero divisors. Therefore, the matrices of left multiplication by such elements are invertible and

$$\mathcal{C}_{8\times 2}=\left\{\begin{bmatrix} \lambda(x) & 0 & 0 & \lambda(i)\lambda(\widetilde{\tau}^3(y)) \\ \lambda(y) & \lambda(\widetilde{\tau}(x)) & 0 & 0 \\ 0 & \lambda(\widetilde{\tau}(y)) & \lambda(\widetilde{\tau}^2(x)) & 0 \\ 0 & 0 & \lambda(\widetilde{\tau}^2(y)) & \lambda(\widetilde{\tau}^3(x)) \end{bmatrix}\right\}$$

is fully diverse. If $x=x_0+ex_1$ for $x_0,x_1\in K$, then

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

and similarly for $\lambda(y)$. It should be noted that the top right block matrix now has the form

$$\begin{bmatrix} i\tau^3(y_0) & -i\tau^3\sigma(y_1) \\ -i\tau^3(y_1) & -i\tau^3\sigma(y_0) \end{bmatrix},$$

which is different from the matrix in [21, p. 9]. By Theorem 2 (iv), the determinant of any nonzero codeword is an element in $\mathcal{O}_F$.

5.5. A 12×2 MIDO System. In this configuration we have the following parameters:

(1) $\theta = \zeta_{28} + \zeta_{28}^{-1} = 2\cos\frac{\pi}{14}$ where ζ_{28} is a primitive 28^{th} root of unity and $F = \mathbb{Q}(\theta)$.
(2) $K = F(\omega)$ and $D = (K/F, \sigma, -1)$ which is a subalgebra of Hamilton's quaternions.
(3) $L = \mathbb{Q}(\omega)$ so that K/L is a cyclic field extension of degree 6 with Galois group generated by the automorphism $\tau : \zeta_{28} + \zeta_{28}^{-1} \mapsto \zeta_{28}^{2} + \zeta_{28}^{-2}$.
(4) $A = It^6(D, \tau, -\omega)$.

It was shown in [21] that $-\omega \neq z\widetilde{\tau}(z)\widetilde{\tau}^2(z)\ldots\widetilde{\tau}^5(z)$ for any $z \in D$ and hence elements of the form $x + fy \in A$, $x, y \in D$ nonzero, are not left zero divisors. Therefore, the matrices of left multiplication by such elements are invertible and

$$\mathcal{C}_{12\times 2} = \left\{ \begin{bmatrix} \lambda(x) & 0 & 0 & 0 & 0 & -\lambda(\omega)\lambda(\widetilde{\tau}^5(y)) \\ \lambda(y) & \lambda(\widetilde{\tau}(x)) & 0 & 0 & 0 & 0 \\ 0 & \lambda(\widetilde{\tau}(y)) & \lambda(\widetilde{\tau}^2(x)) & 0 & 0 & 0 \\ 0 & 0 & \lambda(\widetilde{\tau}^2(y)) & \lambda(\widetilde{\tau}^3(x)) & 0 & 0 \\ 0 & 0 & 0 & \lambda(\widetilde{\tau}^3(y)) & \lambda(\widetilde{\tau}^4(x)) & 0 \\ 0 & 0 & 0 & 0 & \lambda(\widetilde{\tau}^4(y)) & \lambda(\widetilde{\tau}^5(x)) \end{bmatrix} \right\}$$

is fully diverse. If $y = y_0 + ey_1$ for $y_0, y_1 \in K$, then

$$\lambda(x) = \begin{bmatrix} y_0 & -\sigma(y_1) \\ y_1 & \sigma(y_0) \end{bmatrix}.$$

Note that the top right block matrix has the form

$$\begin{bmatrix} -\omega\tau^5(y_0) & \omega\tau^5\sigma(y_1) \\ -\omega^2\tau^5(y_1) & -\omega^2\tau^5\sigma(y_0) \end{bmatrix},$$

which is different from the matrix in [21, p. 9]. By Theorem 2 (iv), the determinant of any nonzero codeword is an element in $\mathcal{O}_F$.

6. ML-decoding Complexity

The analysis of the ML-decoding complexity of our sparse codes 5.1, 5.2, 5.4. and 5.5 is exactly the same as that in [21, V.], because our codewords differ from those in [21] only in the top right block matrix, and the complexity of the off-diagonal block matrices is given by exhaustive search. The reduced complexity comes from the block matrices on the main diagonal which are exactly the same as in [21].

Using M-HEX complex constellations and the same notation as in [21], for the rate-3 code $\mathcal{C}_{6\times 2}$ in 5.3 each codeword $S(\lambda(x_0)) = diag[\lambda(x_0), \tau(\lambda(x_0)), \tau(\lambda(x_0))]$ is 2-group decodable [21, Proposition 7]. $S(\lambda(x_0))$, $S(\lambda(x_1))$ and $S(\lambda(x_2))$ contain each 6 complex information

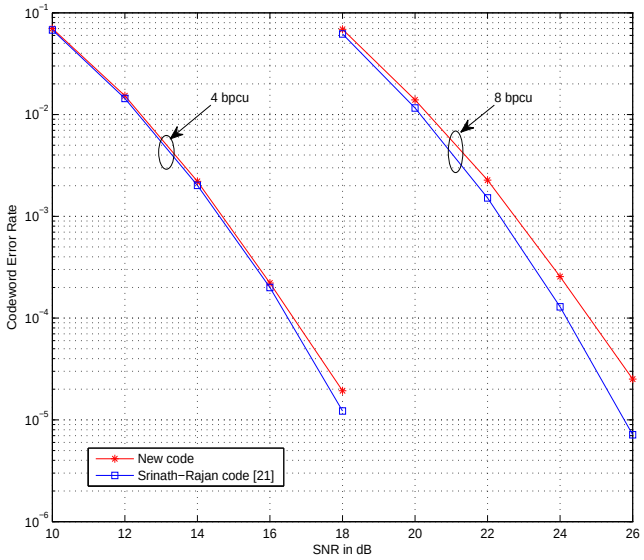

FIGURE 1. Comparison of codeword error rates for 4×2 MIMO, 4 and 8 bpcu.

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

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

over all codewords S. To calculate $\min_{S(\lambda(x_0)))}\{||Y - \sqrt{\rho}HS||^2\}$ requires $\mathcal{O}(M^3)$ computations [21], thus the decoding complexity of the rate-3 code in 5.2 is $\mathcal{O}(M^{6+6+3}) = \mathcal{O}(M^{15})$. It is fast-decodable. We are no experts in coding theory but assume that hard-limiting the code as done in [21] might reduce the ML-complexity further, by a factor of $\sqrt{M}$.

7. Simulation Results

We now present simulation results (done by B. Sundar Rajan and L. P. Natarajan) comparing the codeword error rate performance of the new codes with those from [21] for $n_t = 4, 6$ and 8 antennas under ML-decoding. In all the simulations we assume $n_r = 2$ receive antennas and perfect channel knowledge at the receiver.

Fig. 1 shows the error performance for 4×2 MIMO, for data rates of 4 and 8 bits per channel use (bpcu). Both the new sparse code and the code from [21] use 4-QAM and 16-QAM constellations to attain data rates of 4 and 8 bpcu respectively. The code from [21] shows superior performance.

The codeword error rates for the sparse 6×2 MIMO and 4 bpcu are shown in Fig. 2. Both codes use 4-HEX constellation to encode the information symbols, and both codes have similar error performances.

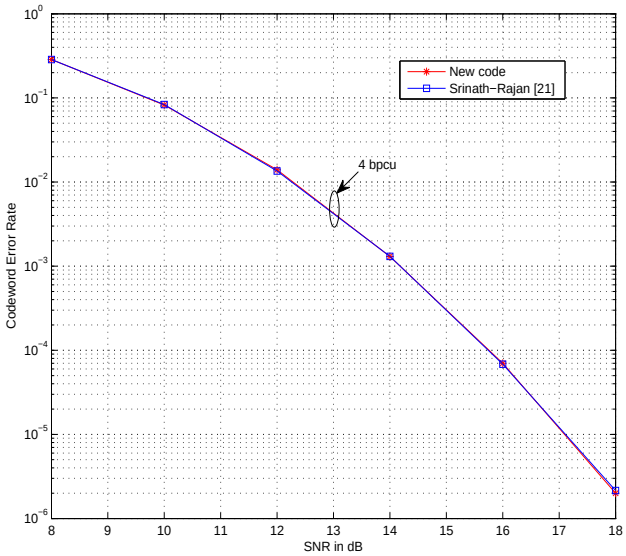

FIGURE 2. Comparison of codeword error rates for 6×2 MIMO, 4 bpcu.

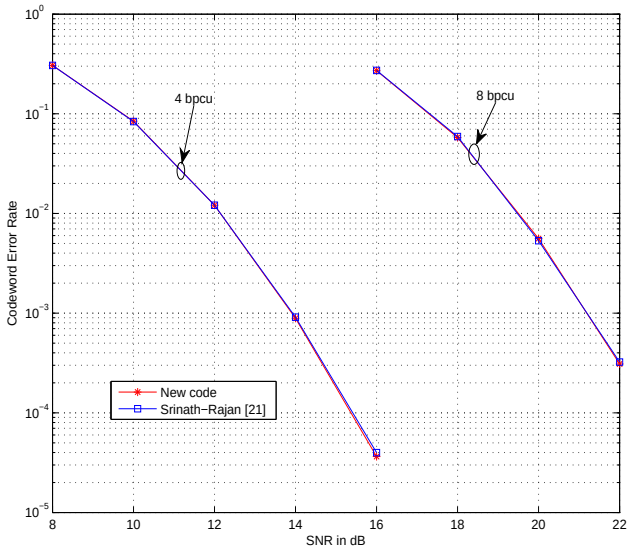

FIGURE 3. Comparison of codeword error rates for 8×2 MIMO, 4 and 8 bpcu.

The sparse $n_t = 8$ code of this paper and the eight antenna code from [21] are compared in Fig. 3 for 4 and 8 bpcu. Both codes use 4-QAM and 16-QAM constellations to achieve 4 and 8 bpcu respectively. We see that both the codes have similar error performance.

8. Conclusion and future work

Inspired by the work in [21] and [20] we defined a new family of nonassociative algebras $A = It^n(D, \tau, d)$, and use their left multiplication to build fully diverse fast-decodable STBCs of rate n: The definition employs several copies of a cyclic division algebra D which are then equipped with a multiplicative structure. The left multiplication of A written as a matrix provided us with STBCs which are fully diverse iff the algebra is division. We presented conditions for $A = \mathrm{It}^n(D, \tau, d)$, $d \in F^\times$, or $A = \mathrm{It}_R^n(D, \tau, d)$ to be a division algebra. This improves on previous code constructions: the fully diverse codes in [21] have zero entries as soon as n is larger than 2, and so their rate (number of independent complex symbols per channel use) is automatically limited to 2. We consequently were able to built a fast ML-decodable rate-3 code.

We believe our construction deserves further investigation: it is a straightforward generalization of the one successfully used by Marking and Oggier for the $n = 2$ case to arbitrary n, and can be applied to a range of different MIMO configurations.

We obtained conditions for the codes to be fully diverse for any n, if $d \in F^\times$.

The NVD property is guaranteed for the code in 5.3, but not for the other codes we constructed in Section 5, whereas the codes obtained in [21], despite also being sparse with lots of zero entries, as soon as n is larger than 2, were shown to have NVD. Nonetheless, the simulations we present for our sparse codes for $n_t = 6$ and $n_t = 8$ have similar error performances as the comparable codes from [21], so the NVD property is not reflected in their performance.

From a mathematical point of view, it makes sense to systematically investigate the nonassociative algebras used both here and in [21], see [26]. A better understanding might lead to a more refined way of using them in future code constructions. It would also be interesting to obtain bounds for fast-decodability for codes obtained from nonassociative algebras.

9. Acknowledgments

We would like to thank B. Sundar Rajan (Senior Member, IEEE) and L. P. Natarajan for providing us with Section 7 and the simulations.

We would like to thank the referee for his or her comments which greatly helped to improve the paper.

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. AMS Surveys and Monographs, 2013.

[6] G. Berhuy, F. Oggier, "Space-time codes from crossed product algebras of degree 4." S. Boztaş and H.F. Lu (Eds.), AAECC 2007, LNCS 4851, 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), Sept. 2006, 3885-3902.

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

[9] 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.

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

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

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

[13] 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

[14] 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.

[15] E. Biglieri, Y. Hong and E. Viterbo, "On fast-decodable space-time block codes", *IEEE Trans. Inform. Theory*, (2) 55, Feb 2009.

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

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

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

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

[20] N. Markin, F. Oggier, "Iterated Space-Time Code Constructions from Cyclic Algebras," *IEEE Transactions on Information Theory*, (9) 59, September 2013, 5966-5979.

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

[22] 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.

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

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

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

[26] S. Pumplün, A. Steele, "The nonassociative algebras used to build fast decodable space-time block codes", available at
http://molle.fernuni-hagen.de/~loos/jordan/archive/nonassoc_cyclic/index.html.

E-mail address: susanne.pumpluen@nottingham.ac.uk; andrew.steele@aquaq.co.uk

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