A class of iterated fast decodable space-time codes for $2n$ Tx antennas

Markin, Nadya; Oggier, Frederique

2012

Markin, N., & Oggier, F. (2012). A class of iterated fast decodable space-time codes for $2n$ Tx antennas. 2012 IEEE International Symposium on Information Theory Proceedings, pp.2826-2830.

<https://hdl.handle.net/10356/94798>

<https://doi.org/10.1109/ISIT.2012.6284039>

© 2012 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [DOI: <http://dx.doi.org/10.1109/ISIT.2012.6284039>].

Downloaded on 26 Apr 2023 18:11:11 SGT

A Class of Iterated Fast Decodable Space-Time Codes for 2^n Tx Antennas

Nadya Markin and Frédérique Oggier
 Division of Mathematical Sciences
 School of Physical and Mathematical Sciences
 Nanyang Technological University, Singapore
 Email: {NMarkin, frederique}@ntu.edu.sg

Abstract—We present an iterative construction of algebraic space-time codes. Starting from a division algebra $\mathcal{D}$, we show how to embed it into a larger ring $\mathcal{A} = \mathcal{A}(\mathcal{D})$ and give conditions for $\mathcal{A}$ to be a new division algebra. Starting from a quaternion division algebra $\mathcal{D}_1$, we thus obtain a sequence $\mathcal{D}_1 \subset \mathcal{D}_2 \subset \dots$ of division algebras where $\mathcal{D}_i = \mathcal{A}(\mathcal{D}_{i-1})$. Each of the $\mathcal{D}_i$ can be used as an underlying structure to build a space-time $\mathcal{C}_i$. Furthermore, the iteration step is done such that fast-decodability of the original code is preserved. We illustrate our technique by creating an iterative version of the Silver code.

Index Terms—Fast-decodability, Quaternion algebras, Space-time codes.

I. INTRODUCTION

Space-time codes arising from division algebras [1] have been used for several years and many codes with good performance are available. While supplying full diversity, these codes also possess a lattice structure which incurs a high complexity of Maximum Likelihood (ML) decoding, typically implemented with a sphere decoder [2]. A line of research on *fast-decodable* codes initiated in [3] yielded several families of codes with reduced ML decoding complexity, notably in [4]–[6], where different notions of fast-decodability are studied and categorized. Codes for the Multiple Input Double Output (MIDO) channel have been of special interest due to their potential application to digital video broadcasting, where the number of receive antennas is limited by the size of the user's portable device. In particular, several constructions of fast-decodable MIDO codes have been proposed [7]–[9]. Sequences of fast-decodable codes when the number of transmit antennas increases can be found in [10].

In this paper, we are similarly interested in addressing the design of fast-decodable codes for possibly large number of transmit antennas, and present an iterative construction of minimum delay algebraic space-time codes - generalizing the method proposed in [11] - which generates for each $i \geq 1$ a family of fast-decodable full-rate MIDO $2^i \times 2^i$ codes.

Each code in this family is a *full-rate MIDO* code contained in the ring of $2^i \times 2^i$ matrices $\text{Mat}_{2^i \times 2^i}(K)$ with coefficients in a number field K . At each step of the iteration, the resulting space-time code actually carries an algebra structure, and we supply criteria which determine when this algebra is division, or alternatively put, when the code is fully diverse. It is worth highlighting that the matrix representation of these codes is not

the left regular representation typically employed in the area [1]. While codes arising from a division algebra are no novelty, the iterative nature of this construction endows the resulting codes with fast-decodable properties. This is achieved using a scaling technique, which allows us to preserve fast-decodable properties of the initial code throughout the iterative process.

The sketch of our construction is as follows. Let $\mathcal{D}$ be a division algebra contained in the ring $\text{Mat}_{n \times n}(K)$ of $n \times n$ matrices with coefficients in a number field K (in this context, the property of being *division* means that every matrix in $\mathcal{D}$ is invertible). We provide a general construction which allows us to embed the algebra $\mathcal{D}$ into a bigger algebra $\mathcal{A} = \mathcal{A}(\mathcal{D}) \subset \text{Mat}_{2n \times 2n}(K)$. Given that the initial algebra $\mathcal{D}$ was division, a criterion decides when the algebra $\mathcal{A}$ is also division. The process can thus be repeated, starting with $\mathcal{A}(\mathcal{D})$ instead of $\mathcal{D}$ to construct a sequence of division algebras, whose elements are matrices with coefficients in K . At each stage of the iteration, a new fully-diverse space-time code is derived from the corresponding division algebra.

II. SYSTEM MODEL AND FAST DECODABILITY

For each integer $i \geq 1$, let $T = 2^i$ denote the number of Tx antennas. We consider transmission over a coherent Rayleigh fading channel with T Tx antennas, 2 Rx antennas and perfect channel state information at the receiver (CSIR):

$$Y = HX + V, \quad (1)$$

where H is the $2 \times T$ channel matrix, V is the $2 \times T$ Gaussian noise at the receiver, and $X \in \mathcal{C}_i$ is a $T \times T$ codeword that can be represented as a linear combination $g_1 B_1 + \dots + g_{r_i} B_{r_i}$ of generating matrices $B_1, \dots, B_{r_i}$ of the code $\mathcal{C}_i$, weighted by coefficients $g_1, \dots, g_{r_i}$, which are PAM information symbols. The matrices $B_1, \dots, B_{r_i}$ will sometimes be referred to as a basis of the code $\mathcal{C}_i$ and r_i as the rank of the code. For each $i \geq 1$, we construct a code $\mathcal{C}_i \subset \text{Mat}_{2^i \times 2^i}(K)$, such that the $\mathbb{R}$ -rank r_i of each iterated code is 2^{i+2} . Since each codeword can transmit up to $4T = 2^{i+2}$ PAM information symbols (equivalently 2^{i+1} complex symbols), the resulting codes are *full-rate MIDO* codes. Alternatively, in terms of number of complex symbols per channel use (cspcu), the proposed codes are of rate two for each i , which is maximal for a MIDO code. Maximum-likelihood decoding amounts to searching the code

$\mathcal{C}_i$ for the codeword

$$Z = \arg \min \{ \|Y - HX\|_F^2 \}_{X \in \mathcal{C}_i} \quad (2)$$

closest to the received matrix Y with respect to the squared Frobenius norm. Each $2 \times T$ matrix HB_j corresponds, via vectorization, to a vector $\mathbf{b}_j \in \mathbb{R}^{r_i}$ obtained by stacking the columns followed by separating the real and imaginary parts of HB_j . We define the (generating) matrix

$$B = (\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_{r_i}) \in M_{r_i \times r_i}(\mathbb{R}),$$

so every received codeword can be represented as a real vector $B\mathbf{g}$, with $\mathbf{g} = (g_1, \dots, g_{r_i})^T$ having coefficients in the real alphabet S in use, and ML decoding amounts to finding

$$\arg \min \{ \|\mathbf{y} - B\mathbf{g}\|_E^2 \}_{\mathbf{g} \in S^{r_i}} = \arg \min \{ \|Q^* \mathbf{y} - R\mathbf{g}\|_E^2 \}_{\mathbf{g} \in S^{r_i}} \quad (3)$$

with respect to the Euclidean norm, where $\mathbf{y}$ is the vectorization of Y , and R is an upper right triangular matrix obtained through the QR decomposition $B = QR$, with Q unitary.

The number and position of nonzero elements in the upper right part of R determine the complexity of the sphere decoding [3]: if r_i is the number of independent real information symbols from S within one codeword from $\mathcal{C}_i$, then the *ML decoding complexity* is the minimum number of values of $\mathbf{g}$ used in (3) while performing ML decoding. The worst case, when the matrix R is a full upper right triangular matrix, is the complexity of the exhaustive-search ML decoder, that is $O(|S|^{r_i})$, where $|S|$ is the number of PAM symbols in use. Fast decodability is achieved whenever the code structure is such that the decoding complexity has an exponent κ_i of $|S|$ smaller than r_i . We call κ_i the complexity order of the code.

Given an ordered basis $B_1, \dots, B_{r_i}$, we can determine the zero structure of R by the zero structure of the matrix M , defined by orthogonality relations of the basis elements:

$$M_{k,l} = \|B_k B_l^* + B_l B_k^*\|_F. \quad (4)$$

It was shown in [4, Lemma 2] that if M has the form

$$M = \begin{bmatrix} \Delta & B_1 \\ B_2 & B_3 \end{bmatrix},$$

where Δ is a d -dimensional diagonal matrix, then the matrix R of the QR decomposition in the sphere decoder as in (3) satisfies

$$R = \begin{bmatrix} \Delta & B \\ 0 & R_1 \end{bmatrix}.$$

A code $\mathcal{C}_i$ corresponding to such an R has complexity order $\kappa_i = r_i - d + 1$. It was also proven in [4, Lemma 10] that the matrix R has the form

$$R = \begin{bmatrix} R_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & R_g \end{bmatrix}$$

where R_j are d_j -dimensional square matrices, whenever

$$M = \begin{bmatrix} M_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & M_g \end{bmatrix}.$$

A code $\mathcal{C}_i$ with such a matrix R is said to be *g-group decodable* and has complexity order $\kappa_i = \max_{1 \leq j \leq g} d_j$.

III. AN ITERATED CODE CONSTRUCTION

We start with a 4-dimensional algebra $\mathcal{D}_1$, and obtain a sequence $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \dots$ of division algebras with $\mathcal{D}_1 \in \text{Mat}_{2 \times 2}(K)$, $\mathcal{D}_2 \in \text{Mat}_{4 \times 4}(K)$, $\mathcal{D}_3 \in \text{Mat}_{8 \times 8}(K)$, etc. For $i \geq 1$, the code $\mathcal{C}_i$ corresponding to $\mathcal{D}_i$ is a subset of the matrix ring $\text{Mat}_{2^i \times 2^i}(K)$ for some number field K . A codeword in $\mathcal{C}_i$ encodes 2^{i+2} real symbols (i.e., 4 real symbols pcu).

A. The Algebraic Framework

We describe the general iterative step first. Let K be a number field, and $\mathcal{D}$ be a division algebra contained in the ring $\text{Mat}_{n \times n}(K)$ of $n \times n$ matrices over K (n is some 2^i at the i th iteration). Given an automorphism τ of K , we extend it to a homomorphism of $\mathcal{D}$ (still denoted by τ by abuse of notation) by pointwise action on K -coefficients of elements of $\mathcal{D}$, i.e., for a matrix $A \in \mathcal{D} \subset \text{Mat}_{n \times n}(K)$, we have

$$\tau : (A_{ij}) \mapsto (\tau(A_{ij})).$$

Note that $\tau(A)\tau(B) = \tau(AB)$, hence $\tau(A^{-1}) = \tau(A)^{-1}$ for A invertible. In our construction τ will have to in fact be an automorphism of $\mathcal{D}$, i.e., satisfy $\tau(\mathcal{D}) = \mathcal{D}$.

We next define a map α_θ which embeds $\mathcal{D} \times \mathcal{D}$ into a larger ring. Given an element θ of the center $Z(\mathcal{D})$ of $\mathcal{D}$, let $\alpha_\theta : \mathcal{D} \times \mathcal{D} \rightarrow \text{Mat}_{2 \times 2}(\mathcal{D})$ be the map defined by

$$\alpha_\theta : (x, y) \mapsto \begin{bmatrix} x & \theta\tau(y) \\ y & \tau(x) \end{bmatrix}, \quad (5)$$

which is seen as an embedding of $\mathcal{D} \times \mathcal{D}$ into $\text{Mat}_{2n \times 2n}(K)$.

For this construction to be iterative, $\mathcal{A} := \alpha_\theta(\mathcal{D}, \mathcal{D})$ needs to again be a division algebra. We start with a criterion which determines when $\mathcal{A}$ has the structure of a $Z(\mathcal{D})$ -algebra¹. The question of whether it is division is discussed below.

Lemma 1: Let τ be an automorphism of K of order 2, which extends to an automorphism of $\mathcal{D}$ and fixes its center pointwise, i.e., $\tau(z) = z$ for $z \in Z(\mathcal{D})$. If $\theta \in Z(\mathcal{D})$, then the image $\mathcal{A}$ of α_θ forms an algebra of dimension $2d^2$ over $Z(\mathcal{D})$, where d^2 is the dimension of $\mathcal{D}$ over its center.

Proof: Note that $\mathcal{A} = \alpha_\theta(\mathcal{D}, \mathcal{D})$ is both additively and multiplicatively closed, since clearly

$$\begin{aligned} \alpha_\theta(x, y) + \alpha_\theta(u, v) &= \begin{bmatrix} x & \theta\tau(y) \\ y & \tau(x) \end{bmatrix} + \begin{bmatrix} u & \theta\tau(v) \\ v & \tau(u) \end{bmatrix} \\ &= \alpha_\theta(x + u, y + v), \end{aligned}$$

while

$$\begin{aligned} \alpha_\theta(x, y)\alpha_\theta(u, v) &= \begin{bmatrix} xu + \theta\tau(y)v & \theta x\tau(v) + \theta\tau(y)\tau(u) \\ yu + \tau(x)v & \theta y\tau(v) + \tau(x)\tau(u) \end{bmatrix} \\ &= \alpha_\theta(xu + \theta\tau(y)v, yu + \tau(x)v) \end{aligned}$$

¹ $Z(\mathcal{D})$ is generally only a subset of $Z(\mathcal{A})$.

using that $\tau(\theta) = \theta$, since $\tau \in Z(\mathcal{D})$, and $\tau^2 = 1$. The center of $\mathcal{D}$ embeds into the center of $\mathcal{A}$ via

$$z \mapsto \alpha_\theta(z, 0) = \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix}.$$

Since $\mathcal{A}$ is additionally a vector space over $Z(\mathcal{D})$, it has the structure of a $Z(\mathcal{D})$ -algebra. It is of dimension $2d^2$ over $Z(\mathcal{D})$. ■

We now give a criterion on θ which guarantees that the $Z(\mathcal{D})$ -algebra $\mathcal{A} = \alpha_\theta(\mathcal{D}, \mathcal{D})$ is division, in other words every nonzero element of $\mathcal{A}$ is invertible. The following lemma is a slight generalization of [11, Lemma 1].

Lemma 2: Let $\mathcal{D}$ be a division algebra, whose elements correspond to $n \times n$ matrices over a field K . Let τ and θ satisfy the hypothesis of Lemma 1. Then $\mathcal{A} = \alpha_\theta(\mathcal{D}, \mathcal{D})$ is division if and only if $\theta \neq z\tau(z)$ for all $z \in \mathcal{D}$.

Proof: Suppose that $\theta \neq z\tau(z)$ for all $z \in \mathcal{D}$. We will show that $\mathcal{A}$ is division. Consider a nonzero element

$$\alpha_\theta(x, y) = \begin{bmatrix} x & \theta\tau(y) \\ y & \tau(x) \end{bmatrix}$$

where the entries x, y are $n \times n$ matrices from the division algebra $\mathcal{D}$. If $x = 0$ (resp. $y = 0$), the matrix is clearly invertible. Let us thus assume that both $x, y \in \mathcal{D}$ are nonzero, hence invertible. The formula (sometimes referred to as Schur complement) for the determinant of a block matrix gives

$$\det \begin{bmatrix} x & \theta\tau(y) \\ y & \tau(x) \end{bmatrix} = \det(x) \det(\tau(x) - yx^{-1}\theta\tau(y)).$$

Now since $\tau(x) - yx^{-1}\theta\tau(y) \in \mathcal{D}$, and hence invertible when nonzero, we have

$$\det(\tau(x) - yx^{-1}\theta\tau(y)) \neq 0 \iff \tau(x) - yx^{-1}\theta\tau(y) \neq 0.$$

It thus suffices to demonstrate $\tau(x) - yx^{-1}\theta\tau(y) \neq 0$. Since y is invertible, and recalling that for $x \in \mathcal{D}$, $\tau(x^{-1}) = \tau(x)^{-1}$, the latter inequality is equivalent to $xy^{-1}\tau(xy^{-1}) \neq \theta$. Letting $z = xy^{-1}$, by our assumption on θ , we have $\theta \neq z\tau(z)$. Hence $\det(\alpha_\theta(x, y)) \neq 0$.

Conversely, suppose $\theta = z\tau(z)$ for some $z \in \mathcal{D}$. We verify that $\det(\alpha_\theta(z, I_n)) = 0$, where I_n is the identity matrix. Indeed

$$\begin{aligned} \det(\alpha_\theta(z, I_n)) &= \det(z) \det(\tau(z) - I_n z^{-1}\theta) \\ &= \det(z) \det(\tau(z) - I_n z^{-1}z\tau(z)) \\ &= \det(z) \det(0) = 0. \end{aligned}$$

Hence $\mathcal{A}$ is not division.

B. The General Code Construction

Let us now detail how the above general iterative construction induces a family of space-time codes, by fixing for the first step ($i=1$) an algebra $\mathcal{D}_1$ of dimension 4.

Let F be a number field, and let $\mathcal{D}_1 = (a, b)_F$ be a generalized quaternion algebra [12]. By definition, $\mathcal{D}_1$ is of dimension 4 over its center F , and has for maximal subfield $K = F(\sqrt{a})$. For coding purposes, what is important to know

is that elements of $\mathcal{D}_1$ can be viewed as 2×2 matrices over K via left regular representation, namely:

$$\begin{bmatrix} c & b\tau(d) \\ d & \tau(c) \end{bmatrix},$$

where $\tau : \sqrt{a} \mapsto -\sqrt{a}$ is a Galois F -automorphism, $b \in F$ and $c, d \in K$. The code $\mathcal{C}_1$ consists of the subset of $\mathcal{D}_1$, whose coefficients c, d are algebraic integers of K . When F is an imaginary quadratic of $\mathbb{Q}$, each symbol from F corresponds to 2 rational symbols. Hence each codeword carries 2 K -symbols, that is 4 F -symbols, or 8 $\mathbb{Q}$ -symbols. The rank r_1 of the code $\mathcal{C}_1$ is hence 8. Restricting the symbols in F to be algebraic integers means that the 8 $\mathbb{Q}$ -symbols are in $\mathbb{Z}$.

First we note that τ is of order 2, and extends to an automorphism of $\mathcal{D}_1$:

$$\tau \left(\begin{bmatrix} c & b\tau(d) \\ d & \tau(c) \end{bmatrix} \right) = \begin{bmatrix} \tau(c) & b\tau(\tau(d)) \\ \tau(d) & \tau(\tau(c)) \end{bmatrix} = \begin{bmatrix} \tau(c) & bd \\ \tau(d) & c \end{bmatrix}$$

is in $\mathcal{D}_1$, since $\tau(b) = b$. Adding that $\tau(z) = z$ for every $z \in Z(\mathcal{D}_1) = F$, we can use it for the iterative step in α_θ .

Now for any $\theta_1 \in Z(\mathcal{D}_1) = F$, let θ_1 also denote the matrix

$$\begin{bmatrix} \theta_1 & 0 \\ 0 & \theta_1 \end{bmatrix} \in \mathcal{D}_1.$$

Indeed, this is an element of $\mathcal{D}_1$ since $\tau(\theta_1) = \theta_1$. The first step of the iteration gives us the algebra $\mathcal{D}_2 = \alpha_\theta(\mathcal{D}_1, \mathcal{D}_1)$ whose elements are matrices of the form

$$\begin{bmatrix} c & b\tau(d) & \theta_1\tau(e) & \theta_1bf \\ d & \tau(c) & \theta_1\tau(f) & \theta_1e \\ e & b\tau(f) & \tau(c) & bd \\ f & \tau(e) & \tau(d) & c \end{bmatrix}.$$

The code $\mathcal{C}_2$ is obtained as the image $\alpha_{\theta_1}(\mathcal{C}_1, \mathcal{C}_1)$ of $\mathcal{C}_1$. Similarly, the second step gives the algebra $\mathcal{D}_2$ whose elements are 8×8 matrices of the form

$$\begin{bmatrix} A & \theta_2\tau(B) \\ B & \tau(A) \end{bmatrix}$$

where $A, B \in \mathcal{D}_1$ and θ_2 is an element of F , possibly equal to θ_1 . Continuing, we obtain an iterative sequence of algebras $\mathcal{D}_i = \alpha_{\theta_{i-1}}(\mathcal{D}_{i-1}, \mathcal{D}_{i-1})$, whose elements are in $\text{Mat}_{2^i \times 2^i}(K)$. The corresponding codes are $\mathcal{C}_i = \alpha_{\theta_{i-1}}(\mathcal{C}_{i-1}, \mathcal{C}_{i-1})$. From Lemma 2, $\theta_i, i \geq 1$ must satisfy

$$\theta_i \neq z\tau(z), \quad z \in \mathcal{D}_i.$$

C. Scaling

We now define a scaled version $\tilde{\alpha}_\theta$ of the map α_θ , which will be useful in constructing fast-decodable codes from the iterated construction. Recall the map α_θ defined in (5):

$$\alpha_\theta : (x, y) \mapsto \begin{bmatrix} x & \theta\tau(y) \\ y & \tau(x) \end{bmatrix},$$

where τ and θ are as in the assumptions of Lemma 1 to ensure that $\alpha_\theta(\mathcal{D}, \mathcal{D})$ has a $Z(\mathcal{D})$ -algebra structure.

Let $u, v, x, y \in \mathcal{D}$ be $n \times n$ matrices with coefficients in K . We denote by ζ a 4th root of unity, it does not have to be

primitive, that is $\zeta \in \{\pm 1, \pm i\}$. Let $\theta = \zeta\theta'$ with $\theta' > 0$, we have that the map

$$\alpha_{\zeta\theta'} : (u, v) \mapsto \begin{bmatrix} u & \zeta\theta'\tau(v) \\ v & \tau(u) \end{bmatrix}$$

and the map $\tilde{\alpha}_{\zeta\sqrt{\theta'}}$ defined by

$$\tilde{\alpha}_{\zeta\sqrt{\theta'}} : (u, v) \mapsto \begin{bmatrix} u & \zeta\sqrt{\theta'}\tau(v) \\ \sqrt{\theta'}v & \tau(u) \end{bmatrix}$$

satisfies that $\det(\alpha_{\zeta\theta}(u, v)) = \det(\tilde{\alpha}_{\zeta\sqrt{\theta'}}(u, v))$, for all u, v . In particular, the image of $\tilde{\alpha}$ retains the full diversity property.

Furthermore, assuming that complex conjugation commutes with τ on elements of $\mathcal{D}$, and letting $\tilde{\alpha}$ denote $\tilde{\alpha}_{\zeta\sqrt{\theta'}}$ for short, one can easily check that

$$\tilde{\alpha}(x, y)\tilde{\alpha}(u, v)^* = \tilde{\alpha}(xu^* + \theta\tau(yv^*), yu^* + \zeta^*\tau(xv^*)).$$

This allows us to compute

$$\tilde{\alpha}(x, 0)\tilde{\alpha}(u, 0)^* = \begin{bmatrix} xu^* & 0 \\ 0 & \tau(xu^*) \end{bmatrix} \quad (6)$$

$$\tilde{\alpha}(x, 0)\tilde{\alpha}(0, v)^* = \sqrt{\theta'} \begin{bmatrix} 0 & xv^* \\ \zeta^*\tau(xv^*) & 0 \end{bmatrix} \quad (7)$$

$$\tilde{\alpha}(0, y)\tilde{\alpha}(u, 0)^* = \sqrt{\theta'} \begin{bmatrix} 0 & \zeta\tau(yu^*) \\ yu^* & 0 \end{bmatrix} \quad (8)$$

$$\tilde{\alpha}(0, y)\tilde{\alpha}(0, v)^* = \begin{bmatrix} \theta'\tau(yv^*) & 0 \\ 0 & yv^* \end{bmatrix}. \quad (9)$$

From the calculations above, we can see how the fast decodable properties of the code $\mathcal{C}$ with underlying algebra $\mathcal{D}$ are inherited by the iterated code coming from $\mathcal{A}(\mathcal{D})$, as we summarize in the lemma below.

Lemma 1: Let $\mathcal{D}$ be a code with basis $\{D_1, \dots, D_r\}$. Then $\{\tilde{\alpha}(D_j, 0), \tilde{\alpha}(0, D_k) : 1 \leq j, k \leq r\}$ is a basis of $\mathcal{A}(\mathcal{D})$. Moreover, if the orthogonality relation

$$D_j D_k^* + D_k D_j^* = 0$$

holds for a pair (j, k) , then the following orthogonality relations hold for the basis of $\mathcal{A}(\mathcal{D})$ above:

$$\tilde{\alpha}(D_j, 0)\tilde{\alpha}(D_k, 0)^* + \tilde{\alpha}(D_k, 0)\tilde{\alpha}(D_j, 0)^* = 0$$

$$\tilde{\alpha}(0, D_j)\tilde{\alpha}(0, D_k)^* + \tilde{\alpha}(0, D_k)\tilde{\alpha}(0, D_j)^* = 0.$$

The corresponding code built over the algebra $\mathcal{A}(\mathcal{D})$ thus enjoys the same orthogonality relations, meaning that with each iteration i the worst case increase in complexity order is 2^i . This gives the following (very) loose bound.

Corollary 1: Let $\mathcal{D}_i$ be an iterated code with complexity order κ_i . Then $\kappa_{i+1} \leq 2^i + \kappa_i$.

IV. AN ITERATIVE SILVER CODE

We provide a detailed example, using as first code the Silver code. The Silver code, discovered in [13], and rediscovered in [14], is given by codewords of the form

$$\begin{bmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{bmatrix},$$

where

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \frac{1}{\sqrt{7}} \begin{bmatrix} 1+i & -1+2i \\ 1+2i & 1-i \end{bmatrix} \begin{bmatrix} x_3 \\ x_4 \end{bmatrix}$$

and $x_1, x_2, x_3, x_4 \in \mathbb{Z}[i]$ are the information symbols.

A basis for the Silver code is given by $\{B_j, j = 1, \dots, 8\}$, and a Silver codeword X can be written as

$$X = \sum_{j=1}^4 B_{2j-1}x_{j1} + B_{2j}x_{j2},$$

where $x_j = x_{j1} + ix_{j2}$, and $x_{j1}, x_{j2} \in \mathbb{Z}$ are PAM symbols. Fixing such an ordering of the basis yields an R matrix [4]

$$R = \begin{bmatrix} \Delta & B \\ 0 & R_1 \end{bmatrix}$$

where Δ is a 4-dimensional diagonal matrix, thus inducing a complexity order of $\kappa_1 = 8 - 4 + 1 = 5$.

A. First iteration

To perform the first iteration, we need to identify the structure of a quaternion algebra. Consider $F = \mathbb{Q}(\sqrt{-7})$ and its Galois extension $K = F(i)$, with Galois automorphism $\tau : a + bi \mapsto a - bi$, where $a, b \in F$. Note that τ is not the complex conjugation since it fixes $\sqrt{-7}$. Silver codewords can also be viewed [15] as (scaled) matrices of the form

$$\begin{bmatrix} c & -\tau(d) \\ d & \tau(c) \end{bmatrix}, \quad (10)$$

where $c, d \in \mathbb{Z}[i] \oplus \mathbb{Z}[i](\frac{1+\sqrt{-7}}{2})$. To be more specific, the Silver code is obtained via left regular representation of the elements of the natural order of the quaternion algebra $\mathcal{D}_1 = (-1, -1)_F$. Thus for a pair of algebraic integers $c, d \in \mathbb{Q}(\sqrt{-7}, i)$ we have a Silver codeword (10) arising from $\mathcal{D}_1$. The automorphism τ of order 2 extends to $\mathcal{D}_1$ via

$$\tau : \begin{bmatrix} c & -\tau(d) \\ d & \tau(c) \end{bmatrix} \mapsto \begin{bmatrix} \tau(c) & -d \\ \tau(d) & c \end{bmatrix}.$$

Noting that $\tau(z) = z$ for every $z \in Z(\mathcal{D}_1) = F$, we can use τ for the iterative construction.

Given $\theta_1 \in Z(\mathcal{D}_1)$, the first iteration $\mathcal{D}_2 = \alpha_{\theta_1}(\mathcal{D}_1, \mathcal{D}_1)$ of the Silver code is given by matrices looking like

$$\begin{bmatrix} a & -\tau(b) & \theta_1\tau(c) & -\theta_1d \\ b & \tau(a) & \theta_1\tau(d) & \theta_1c \\ c & -\tau(d) & \tau(a) & -b \\ d & \tau(c) & \tau(b) & a \end{bmatrix}. \quad (11)$$

To make the corresponding code $\mathcal{C}_1$ fully diverse, by Lemma 2, we need to check that $z\tau(z) \neq \theta_1$, for any $z \in \mathcal{D}_1$, that is, writing z as in (10)

$$\begin{bmatrix} c & -\tau(d) \\ d & \tau(c) \end{bmatrix} \begin{bmatrix} \tau(c) & -d \\ \tau(d) & c \end{bmatrix} \neq \begin{bmatrix} \theta_1 & 0 \\ 0 & \theta_1 \end{bmatrix}.$$

By comparing the matrix coefficients, we obtain

$$\begin{aligned} c\tau(c) - \tau(d)^2 &= \theta_1 \\ c(d + \tau(d)) &= 0, \end{aligned}$$

which we do not want simultaneously satisfied for any choice of $c, d \in K$. By choosing $c = 0$, we obtain the first condition:

$$\theta_1 \neq -\tau(d)^2$$

for any $d \in K$. Suppose $c \neq 0$. Then for $d = d_1 + id_2$, the 2nd equality is satisfied only when $d_1 = 0$. Thus assume $d_1 = 0$, in which case we need that $c\tau(c) - \tau(d)^2 \neq \theta_1$ for $d = id_2$. Write $c = c_1 + ic_2$, this is equivalent to checking

$$(c_1 + ic_2)\tau(c_1 + ic_2) - \tau(id_2)^2 = c_1^2 + c_2^2 + d_2^2 \neq \theta_1$$

with $c_1, c_2, d_2 \in F = \mathbb{Q}(i\sqrt{7})$. For example, $\theta = -17$ satisfies the two conditions above. Clearly, $\theta/-1 = 17$ is not a square in K . For the second condition, by reducing modulo the ideal $I = (\frac{1+\sqrt{-7}}{2})^3 \mathcal{O}_F$, we see that $\theta \equiv -1 \pmod I$, which we verify is not a sum of three squares $\pmod I$.

By picking θ_1 of the form a positive multiple of a 4th root of unity, $\mathcal{D}_1$ will inherit orthogonal relations from $\mathcal{D}_1$, as explained in III-C. In fact, by being more restrictive and picking θ_1 to be of the form $-\theta'$ with $\theta' > 0$, one can get a better fast-decodability than what predicted in III-C, which is what we illustrate now. In that case, the left upper part of the R matrix that is obtained is of the form

$$R = \begin{bmatrix} R_1 & 0 & 0 & 0 \\ 0 & R_2 & 0 & 0 \\ 0 & 0 & R_3 & 0 \\ 0 & 0 & 0 & R_4 \end{bmatrix}$$

showing that R is 4-group decodable, once half of the symbols are decoding, showing a complexity order of $\kappa_2 = 10$. Note that this was already observed in the case of $\theta = -1$ in [11], though in this case the algebra cannot be division.

B. Second iteration

Let θ_3 be an element of $Z(\mathcal{D}_2)$. We can define the second iteration $\mathcal{D}_3 = \alpha_{\theta_3}(\mathcal{D}_2, \mathcal{D}_2)$, whose elements are 8×8 matrices with entries in K of the form

$$\begin{bmatrix} A & \theta_3 \tau(B) \\ B & \tau(A) \end{bmatrix},$$

where A, B are elements of $\mathcal{D}_2$ described in (11). To determine whether $\mathcal{D}_3$ is division, Lemma 2 is applied similarly as in the first iteration. A minimum gain in fast-decodability is ensured using the technique given in Subsection III-C, however, as shown for the first iteration, a more careful analysis could reveal more than the minimal gain predicted.

V. CONCLUSION

In this paper, we proposed a novel method to construct space-time codes from division algebras, where instead of using the classical left regular representation, we combine space-time codes in small dimension in an iterative manner. Techniques involving building codes from smaller ones have

been studied, however by exploiting the structure of algebraic space-time codes, we show here that we can derive conditions that generate a sequence of algebras, which can be division. Furthermore, we explain how the bigger code can inherit fast-decodability properties from the smaller codes.

Future work involves a more thorough investigation of the code parameters involved, as well as simulations to determine which code instances are giving the best performance, in terms of diversity, fast-decodability, and coding gain.

ACKNOWLEDGMENT

The research of N. Markin for this work is supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

The present work of F. Oggier is supported in part by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03 and by the Nanyang Technological University under Research Grant M58110049.

REFERENCES

- [1] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, Oct. 2003.
- [2] E. Viterbo, J. Boutros, "A universal lattice decoder for fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, 1999.
- [3] E. Biglieri, Y. Hong and E. Viterbo, "On fast-decodable space-time block codes", *IEEE Trans. Inform. Theory*, vol. 55, no. 2, Feb 2009.
- [4] G. R. Jithamitra, B. S. Rajan, "Minimizing the Complexity of Fast Sphere Decoding of STBCs," submitted, preprint available at <http://arxiv.org/abs/1004.2844>
- [5] L. P. Natarajan, B. S. Rajan, "Fast group-decodable STBCs via codes over GF(4)," *IEEE Int. Symp. Inform. Theory*, Austin, TX, June 2010
- [6] L. P. Natarajan and B. S. Rajan, "Fast-Group-Decodable STBCs via codes over GF(4): Further Results," *IEEE ICC 2011*, Kyoto, Japan, June 2011.
- [7] L. Luzzi, F. Oggier, "A family of fast-decodable MIMO codes from crossed-product algebras over $\mathbb{Q}$," *IEEE Int. Symp. Inform. Theory*, St Petersburg, July 2011.
- [8] F. Oggier, R. Vehkalahti, C. Hollanti, "Fast-decodable MIMO codes from crossed product algebras," *IEEE Int. Symp. Inform. Theory*, Austin, TX, June 2010
- [9] K. P. Srinath, B. S. Rajan, "Low ML-decoding complexity, large coding gain, full-diversity STBCs for 2×2 and 4×2 MIMO systems," *IEEE J. on Special Topics in Signal Processing: managing complexity in multi-user MIMO systems*, 2010
- [10] L. P. Natarajan and B. Sundar Rajan, "Asymptotically-Optimal, Fast-Decodable, Full-Diversity STBCs," *IEEE ICC 2011*, Kyoto, Japan, 06-09 June, 2011.
- [11] N. Markin, F. Oggier, "Iterated MIMO Space-Time Code Constructions," *Allerton Conference*, 2011.
- [12] T. Unger, N. Markin, "Quadratic Forms and Space-Time Block Codes from Generalized Quaternion and Biquaternion Algebras", *IEEE Trans. on Information Theory*, vol. 57 no. 9, pp. 6148-6156, Sept 2011.
- [13] A. Hottinen and O. Tirkkonen, "Precoder designs for high rate space-time block codes," *Conference on Information Sciences and Systems*, 2004.
- [14] J. Paredes, A.B. Gershman, and M. G. Alkhanari, "A 2x2 space-time code with non-vanishing determinants and fast maximum likelihood decoding," *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP2007)*, Hawaii, USA, 2007.
- [15] C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti, and E. Viterbo, "On the Algebraic Structure of the Silver Code," *IEEE Information Theory Workshop*, Portugal, 2008.
- [16] D. R. Estes and J. S. Hsia, "Sums of Three Integer Squares in Complex Quadratic Fields", *Proceedings of the American Mathematical Society*, vol. 89, no. 2, 1983.