Fast decodable codes for 6Tx-3Rx MIMO systems

Markin, Nadya; Oggier, Frederique

2012

Markin, N., & Oggier, F. (2012). Fast decodable codes for 6Tx-3Rx MIMO systems. International Conference on Signal Processing and Communications (SPCOM), 2012, pp.1-5.

<https://hdl.handle.net/10356/94797>

<https://doi.org/10.1109/SPCOM.2012.6290041>

© 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: <http://dx.doi.org/10.1109/SPCOM.2012.6290041>.

Downloaded on 26 Apr 2023 20:21:25 SGT

Fast Decodable Codes for 6Tx-3Rx MIMO Systems

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 propose an iterative full-rate code construction for multiple antenna channels, with 6Tx and 3Rx antennas. We start with two 3×3 codes arising from a cyclic division algebra, and combine them to obtain a 6×6 codeword. We provide a sufficient criterion for when the resulting code is fully diverse. Furthermore, this construction preserves fast-decodability of the original code.

Index Terms—Cyclic Algebras, Fast-Decodability, Space-Time Coding.

I. INTRODUCTION

Since the early nineties, space-time codes have been used in multiple antenna wireless communication to achieve high data rate and reliability. One of the basic design criteria for space-time codes is *full diversity*, established in [1], which requires the family of space-time codewords to consist of matrices whose difference is full-rank. It was first established in [2] that division algebras can be used to construct fully-diverse space-time codes; many good codes have been available since. The lattice structure of these codes, however, results in high decoding complexity of ML (Maximum Likelihood) decoding, typically implemented with a sphere decoder [3]. The search for codes with reduced sphere decoding complexity, subsequently called *fast-decodable codes*, was initiated in [4], where the notion of fast-decodability was defined. Since then, several families of fast-decodable codes have been studied (e.g [5], [14]) and conditions for fast-decodability have been refined, notably in [6]–[8], where criteria for fast-decodability and group-decodability can be found; it is important to highlight that sufficient criteria were also provided in terms independent of the realization channel matrix.

Codes for asymmetric MIMO (Multiple Input Multiple Output) channels present special interest, in particular their application in digital broadcasting to a portable device, a scenario imposing a limitation on the possible number of receive antennas. The special case of MIDO (Multiple Input Double Output) channel has been in the spotlight recently, with fast-decodable code constructions ensuing including [9], and codes based on crossed product algebras [11], [12].

In the present paper we propose an iterative full-rate construction, which maps two 3×3 algebraic codewords into a 6×6 codeword, extending the construction proposed in [13] for MIDO codes. The resulting family of 6×6 codewords, while not always affording the structure of an algebra, gives rise to fully-diverse codes. Due to the recursive nature of

the construction, fast-decodability of the initial 3×3 code is inherited by the 6×6 code.

This paper is organized as follows: we recall the system model and the notion of fast decodability in Section II. The generic code construction and discussion on the code diversity are presented in Section III, while the resulting decoding complexity is detailed in Section IV. A few code examples are computed in Section V.

II. SYSTEM MODEL AND FAST DECODABILITY

We consider transmission over a coherent Rayleigh fading channel with 6 Tx antennas, 3 Rx antennas and perfect channel state information at the receiver (CSIR):

$$Y_{3 \times 6} = H_{3 \times 6} X_{6 \times 6} + V_{3 \times 6}^1, \quad (1)$$

where X is a space-time code coming from a codebook $\mathcal{C}$, H is the channel matrix, and V is the noise at the receiver, and both matrices H, V have complex Gaussian independently distributed coefficients with zero mean.

We are interested in high data rate, that is we exploit the $\min\{6, 3\}6 = 18$ degrees of freedom of the channel to transmit 18 complex (say QAM) information symbols per codeword, or equivalently 36 real (say PAM) information symbols. In that sense, we say that the resulting codes are *full-rate*. In terms of number of complex symbols per channel use (cspcu), the proposed codes are of rate three, three being maximal for 3 Rx antennas.

Maximum-likelihood decoding amounts to searching the code $\mathcal{C}$ for the codeword

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

closest to the received matrix Y with respect to the squared Frobenius norm.

Each codeword X can be represented as a linear combination $g_1 B_1 + \dots + g_{36} B_{36}$ of generating matrices $B_1, \dots, B_{36}$, weighted by coefficients $g_1, \dots, g_{36}$, which are PAM information symbols. The matrices $B_1, \dots, B_{36}$ will sometimes be referred to as a basis of the code $\mathcal{C}$, as they indeed define one. Each 3×6 matrix $H B_i$ corresponds, via vectorization, to a vector $\mathbf{b}_i \in \mathbb{R}^{36}$ obtained by stacking the columns followed by separating the real and imaginary parts of $H B_i$. We define the (generating) matrix

$$B = (\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_{36}) \in M_{36 \times 36}(\mathbb{R}),$$

¹Having fixed the indices of the matrices involved, we omit them from now on.

Fig. 1. Field extension used for the proposed iterative code construction.

so every received codeword can be represented as a real vector $B\mathbf{g}$, with $\mathbf{g} = (g_1, \dots, g_{36})^T$ having coefficients in the real alphabet S in use.

Now finding $\arg \min \{\|Y - HX\|_F^2\}_{X \in \mathcal{C}}$ becomes equivalent to finding $\arg \min \{\|\mathbf{y} - B\mathbf{g}\|_E^2\}_{\mathbf{g} \in S^{36}}$ with respect to the Euclidean norm, where $\mathbf{y}$ is the vectorization of the received matrix Y . The latter search is performed using a real sphere decoder [3], with the complexity of exhaustive search amounting to $O(|S|^{36})$, as the coefficients of $\mathbf{g}$ run over all the values of S . The complexity of decoding can, however, be reduced if the code has additional structure [6]. Performing a QR decomposition of B , $B = QR$, with $Q^\dagger Q = \mathbf{I}$, reduces finding $\arg \min \{\|\mathbf{y} - B\mathbf{g}\|_E^2\}_{\mathbf{g}}$ to minimizing

$$\|\mathbf{y} - QR\mathbf{g}\|_E^2 = \|Q^\dagger \mathbf{y} - R\mathbf{g}\|_E^2 \quad (3)$$

where R is an upper right triangular matrix. The number and structure of zeros of the matrix R may improve the *decoding complexity* (formally defined [4] to be the minimum number of vectors $\mathbf{g}$ over which the difference in (3) must be computed). When the structure of the code allows for the degree (i.e., the exponent of $|S|$) of decoding complexity to be less than the rank of the code, we say that the code is *fast-decodable*.

III. CODE CONSTRUCTION

Let L/F be a Galois extension of number fields with Galois group $C_2 \times C_3 \simeq C_6$, where σ denotes the generator of the cyclic group C_3 and τ that of C_2 (see Fig. 1). Let K be the fixed field of σ , so that L/K forms a cyclic extension of degree 3. Using a suitable algebra structure, called cyclic algebra, it is well known [2] that one can obtain a space-time code $\mathcal{D}$ whose codewords are of the form

$$\begin{bmatrix} a & \gamma\sigma(c) & \gamma\sigma(b) \\ b & \sigma(a) & \gamma\sigma(c) \\ c & \sigma(b) & \sigma(a) \end{bmatrix}, \quad a, b, c \in L, \quad (4)$$

where $\gamma \in K$ is a *non-norm element* in L/K , that is, for no proper divisor k of 3, does there exist an element $d \in L$ such that the norm $N_{L/K}(d) := d\sigma(d)\sigma^2(d) = \gamma^k$. This latter condition ensures [2] that every matrix in $\mathcal{D}$ is invertible, that is

$$\det(X) \neq 0, \quad X \in \mathcal{D}, \quad (5)$$

which guarantees full diversity since

$$\det(X - X') \neq 0, \quad X \neq X' \in \mathcal{D}, \quad (6)$$

is satisfied, using that $X \pm X' \in \mathcal{C}$ for all $X, X' \in \mathcal{D}$.

Let us make the assumption that γ is furthermore chosen in F , that is, $\tau(\gamma) = \gamma$. Given an element θ of K , let $\alpha_\theta : M_3(L) \times M_3(L) \rightarrow M_6(L)$ be the map defined by

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

where $\tau(A)$ is defined componentwise, so that

$$\alpha_\theta : \left(\begin{bmatrix} a & \gamma\sigma(c) & \gamma\sigma(b) \\ b & \sigma(a) & \gamma\sigma(c) \\ c & \sigma(b) & \sigma(a) \end{bmatrix}, \begin{bmatrix} a' & \gamma\sigma(c') & \gamma\sigma(b') \\ b' & \sigma(a') & \gamma\sigma(c') \\ c' & \sigma(b') & \sigma(a') \end{bmatrix} \right) \mapsto \begin{bmatrix} a & \gamma\sigma(c) & \gamma\sigma(b) & \theta\tau(a') & \theta\gamma\tau\sigma(c') & \theta\gamma\tau\sigma(b') \\ b & \sigma(a) & \gamma\sigma(c) & \theta\tau(b') & \theta\tau\sigma(a') & \theta\gamma\tau\sigma(c') \\ c & \sigma(b) & \sigma(a) & \theta\tau(c') & \theta\tau\sigma(b') & \theta\tau\sigma(a') \\ a' & \gamma\sigma(c') & \gamma\sigma(b') & \tau(a) & \gamma\tau\sigma(c) & \gamma\tau\sigma(b) \\ b' & \sigma(a') & \gamma\sigma(c') & \tau(b) & \tau\sigma(a) & \gamma\tau\sigma(c) \\ c' & \sigma(b') & \sigma(a') & \tau(c) & \tau\sigma(b) & \tau\sigma(a) \end{bmatrix}. \quad (7)$$

Define the codebook

$$\mathcal{C} = \{\alpha_\theta(X, Y), \quad X, Y \in \mathcal{D}\}.$$

Let us first discuss when the codewords of $\mathcal{C}$ are fully diverse. The technique used for the beginning of the proof is similar to that presented in [13].

Lemma 1: Let θ belong to K such that $\tau(\theta^3) \neq \theta^3$. Then nonzero codewords of $\mathcal{C}$ have nonzero determinant.

Proof: Consider a nonzero codeword

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

where the entries X, Y are 3×3 matrices of the form (4), that is, in particular, either $\mathbf{0}$ or invertible with coefficients in L . We demonstrate that the determinant of the codeword is nonzero. If $X = \mathbf{0}$ (resp. $Y = \mathbf{0}$), the matrix is clearly invertible. Hence we assume that X and Y are both nonzero, and thus, both invertible. The determinant of a block matrix

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

when A is invertible, is given by $\det(A) \det(D - CA^{-1}B)$. Then

$$\det \begin{bmatrix} X & \theta\tau(Y) \\ Y & \tau(X) \end{bmatrix} = \det(X) \det(\tau(X) - YX^{-1}\theta\tau(Y)).$$

Now since

$$\tau(X) = \begin{bmatrix} \tau(a) & \gamma\sigma(\tau(c)) & \gamma\sigma(\tau(b)) \\ \tau(b) & \sigma(\tau(a)) & \gamma\sigma(\tau(c)) \\ \tau(c) & \sigma(\tau(b)) & \sigma(\tau(a)) \end{bmatrix}$$

for

$$X = \begin{bmatrix} a & \gamma\sigma(c) & \gamma\sigma(b) \\ b & \sigma(a) & \gamma\sigma(c) \\ c & \sigma(b) & \sigma(a) \end{bmatrix}$$

using that $\tau(\gamma) = \gamma$ and that τ and σ commute, we can deduce that $\tau(X) - YX^{-1}\theta\tau(Y)$ is again a codeword of the form (4), and hence invertible when nonzero. We thus have

$$\det(\tau(X) - YX^{-1}\theta\tau(Y)) \neq 0 \iff$$

$$\tau(X) - YX^{-1}\theta\tau(Y) \neq \mathbf{0},$$

and it suffices to demonstrate

$$\tau(X) - YX^{-1}\theta\tau(Y) \neq \mathbf{0}.$$

Since Y is invertible (it is nonzero), and noting that $\tau(X^{-1}) = \tau(X)^{-1}$, the latter inequality is equivalent to

$$XY^{-1}\tau(XY^{-1}) \neq \theta\mathbf{I}_3.$$

Let $Z = XY^{-1}$ and write it as

$$Z = \begin{bmatrix} u & \gamma\sigma(w) & \gamma\sigma(v) \\ v & \sigma(u) & \gamma\sigma(w) \\ w & \sigma(v) & \sigma(u) \end{bmatrix}, \quad u, v, w \in L.$$

For the sake of contradiction, suppose $Z\tau(Z) = \theta\mathbf{I}_3$. Then

$$\det(Z)\det(\tau(Z)) = \det(Z)\tau(\det(Z)) = \theta^3.$$

Since $\det(Z)\tau(\det(Z))$ is fixed by τ , it should be that θ^3 is also fixed by τ , a contradiction. ■

Remark that by choosing θ not in F , the image of α_θ is not multiplicatively closed, thus it does not form an algebra.

IV. FAST DECODABILITY

The above construction can be used in order to create a fast decodable code out of an existing 3×3 fast decodable code. As discussed in [6], fast decodability of the code is a consequence of orthogonal relations on the generators of the code. For example a code is *g-group decodable* when we can divide the basis of the code into g disjoint groups, so that whenever two basis matrices B_j, B_k belong to different groups, we have

$$B_j B_k^* + B_k B_j^* = \mathbf{0}. \quad (8)$$

We start with a scaling technique. We denote by ζ a 4^{th} root of unity, it does not have to be primitive, that is $\zeta \in \{\pm 1, \pm i\}$. Setting that $\theta' > 0$ and $\theta = \zeta\theta'$, we have that the map

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

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

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

satisfy that $\det(\alpha_{\zeta\theta'}(A, B)) = \det(\tilde{\alpha}_{\zeta\sqrt{\theta'}}(A, B))$, for all A, B , in particular, the image of $\tilde{\alpha}_{\zeta\sqrt{\theta'}}$ retains the full diversity property.

Furthermore, assuming that complex conjugation commutes with τ on elements of $\mathcal{D}$, we get that

$$\begin{aligned} \tilde{\alpha}_{\zeta\sqrt{\theta'}}(A, B)^* &= \begin{bmatrix} A & \zeta\sqrt{\theta'}\tau(B) \\ \sqrt{\theta'}B & \tau(A) \end{bmatrix}^* \\ &= \begin{bmatrix} A^* & \sqrt{\theta'}B^* \\ \zeta^*\sqrt{\theta'}\tau(B^*) & \tau(A^*) \end{bmatrix}, \end{aligned}$$

so that letting $\tilde{\alpha}$ denote $\tilde{\alpha}_{\zeta\sqrt{\theta'}}$ we have

$$\begin{aligned} &\tilde{\alpha}(X, Y)\tilde{\alpha}(A, B)^* \\ &= \begin{bmatrix} X & \zeta\sqrt{\theta'}\tau(Y) \\ \sqrt{\theta'}Y & \tau(X) \end{bmatrix} \begin{bmatrix} A^* & \sqrt{\theta'}B^* \\ \zeta^*\sqrt{\theta'}\tau(B^*) & \tau(A^*) \end{bmatrix} \\ &= \begin{bmatrix} XA^* + \theta'\tau(YB^*) & \sqrt{\theta'}(XB^* + \zeta\tau(YA^*)) \\ \sqrt{\theta'}(YA^* + \zeta^*\tau(XB^*)) & \theta'AB^* + \tau(XA^*) \end{bmatrix}. \end{aligned}$$

Since ζ is a root of unity, we notice that $XB^* + \zeta\tau(YA^*) = \zeta(\zeta^*XB^* + \tau(YA^*))$ and

$$\tilde{\alpha}(X, Y)\tilde{\alpha}(A, V)^* = \tilde{\alpha}(XA^* + \theta\tau(YB^*), YA^* + \zeta^*\tau(XB^*)).$$

This allows us to compute

$$\begin{aligned} \tilde{\alpha}(X, \mathbf{0})\tilde{\alpha}(A, \mathbf{0})^* &= \tilde{\alpha}(XA^*, \mathbf{0}) \\ &= \begin{bmatrix} XA^* & \mathbf{0} \\ \mathbf{0} & \tau(XA^*) \end{bmatrix} \end{aligned} \quad (9)$$

$$\begin{aligned} \tilde{\alpha}(X, \mathbf{0})\tilde{\alpha}(\mathbf{0}, B)^* &= \tilde{\alpha}(\mathbf{0}, \zeta^*\tau(XB^*)) \\ &= \sqrt{\theta'} \begin{bmatrix} \mathbf{0} & XB^* \\ \zeta^*\tau(XB^*) & \mathbf{0} \end{bmatrix} \end{aligned} \quad (10)$$

$$\begin{aligned} \tilde{\alpha}(\mathbf{0}, Y)\tilde{\alpha}(A, \mathbf{0})^* &= \tilde{\alpha}(\mathbf{0}, YA^*) \\ &= \sqrt{\theta'} \begin{bmatrix} \mathbf{0} & \zeta\tau(YA^*) \\ YA^* & \mathbf{0} \end{bmatrix} \end{aligned} \quad (11)$$

$$\begin{aligned} \tilde{\alpha}(\mathbf{0}, Y)\tilde{\alpha}(\mathbf{0}, B)^* &= \tilde{\alpha}(\theta'\tau(YB^*), \mathbf{0}) \\ &= \begin{bmatrix} \theta'\tau(YB^*) & \mathbf{0} \\ \mathbf{0} & YB^* \end{bmatrix}. \end{aligned} \quad (12)$$

From the equations above, we see that fast decodable properties of the code $\mathcal{D}$ will be inherited by the image $\tilde{\alpha}_{\zeta\sqrt{\theta'}}(\mathcal{D}, \mathcal{D})$. More precisely:

Lemma 2: Let $\mathcal{D} \subset M_3(L)$ be a fully diverse codebook with basis $\{D_1, \dots, D_{18}\}$, and let $\mathcal{C} = \alpha_\theta(\mathcal{D}, \mathcal{D}) \subset M_3(L)$ be the newly constructed codebook. If

$$D_j D_k^* + D_k D_j^* = \mathbf{0}$$

for some j, k , then there is a basis $\{B_1, \dots, B_{36}\}$ of $\mathcal{C}$ such that

$$B_j B_k^* + B_k B_j^* = B_{18+j} B_{18+k}^* + B_{18+k} B_{18+j}^* = \mathbf{0}$$

Proof: Indeed, let $\{D_1, \dots, D_{18}\}$ be a basis for the code $\mathcal{D}$. A basis for $\mathcal{C}$ is given by

$$\{B_i = \tilde{\alpha}(D_i, \mathbf{0}), B_{18+i} = \tilde{\alpha}(\mathbf{0}, D_i), i = 1, \dots, 18\}.$$

We need to compute $B_j B_k^* + B_k B_j^*$ for two groups of indices: (1) $j, k \in \{1, \dots, 18\}$ (2) $j, k \in \{19, \dots, 36\}$. In the first case, we use (9) to see that

$$\begin{aligned} B_j B_k^* + B_k B_j^* &= \begin{bmatrix} D_j D_k^* & \mathbf{0} \\ \mathbf{0} & \tau(D_k D_j^*) \end{bmatrix} + \begin{bmatrix} D_k D_j^* & \mathbf{0} \\ \mathbf{0} & \tau(D_j D_k^*) \end{bmatrix} \\ &= \begin{bmatrix} D_j D_k^* + D_k D_j^* & \mathbf{0} \\ \mathbf{0} & \tau(D_j D_k^* + D_k D_j^*) \end{bmatrix} \end{aligned}$$

from which is it clear that the orthogonal relations among D_j determine those among B_j . The second set of indices can be handled similarly, using equation (12). ■

Fig. 2. Field extension used for the first code example.

V. CODE EXAMPLES

We now provide a few examples of explicit code constructions that fit the above setting.

A. Example 1

Let $F = \mathbb{Q}(i)$, $L = \mathbb{Q}(\zeta_7, i)$, where ζ_7 is a primitive 7th root of unity. The Galois group $\text{Gal}(L/\mathbb{Q}(i))$ is cyclic of order 6, generated by the automorphism $\sigma_3 : \zeta_7 \mapsto \zeta_7^3$. Note that the automorphism $\sigma_2 : \zeta_7 \mapsto \zeta_7^2$ is of order 3 and hence has a fixed field K which is of degree 2 over $\mathbb{Q}(i)$. Therefore $K = \mathbb{Q}(\sqrt{-7}, i) = \mathbb{Q}(\sqrt{7}, i)$, with the Galois $\mathbb{Q}(i)$ -automorphism $\tau : \sqrt{7} \mapsto -\sqrt{7}$, $\tau : i \mapsto i$.

Lemma 3: The cyclic algebra $\mathcal{D} = (L/K, \sigma_2, \gamma)$ is division.

Proof: Note that the ideal $7\mathbb{Z}$ remains inert in $\mathbb{Z}[i]$, in other words, its residue field $\mathbb{Z}[i]/7\mathbb{Z}[i]$ is the finite field $\mathbb{F}_{49}$ of 49 elements. We further note that the ideal $7\mathbb{Z}[i]$ is completely ramified in $\mathbb{Q}(\zeta_7, i)$, hence the residue field of its prime divisor in K remains to be $\mathbb{F}_{49}$. By local class field theory, the reciprocity map induces an epimorphism $\mathbb{F}_{49} \rightarrow C_6$, whose kernel contains the image of norm elements of L/K in the residue field $\mathbb{F}_{49}$. Hence if $\gamma \bmod 7\mathbb{Z}[i]$ is not mapped to identity, then γ is not a norm of L in K . We conclude that any element γ which multiplicatively generates the nonzero elements of $\mathbb{F}_{49}$ is a non-norm element in the extension $\mathbb{Q}(\zeta_7, i)/\mathbb{Q}(i, \sqrt{7})$ (see [10] for more detailed treatment of this type of argument).

For example, this allows us to conclude that $\gamma = 1 + i$ is not a norm in the extension L/K , hence the cyclic algebra $\mathcal{D} = (L/K, \sigma_2, \gamma)$ is division. $\blacksquare$

Additionally, $\tau(\gamma) = \gamma$, as required by the iterated construction. Note that $\theta = i\theta' = i\sqrt{7}$ satisfies the condition $\tau(\theta^3) \neq \theta^3$ of Lemma 1, hence the iterated code obtained via $\tilde{\alpha}_{i\sqrt{\theta}}(\mathcal{D}, \mathcal{D})$ will be fully-diverse. From Lemma 2, this code will inherit fast-decodable properties of $\mathcal{D}$. We are thus left to find a basis for $\mathcal{D}$ which will yield a fast-decodable code. We provide an example of one such basis below. Let $\{\nu_1, \nu_2, \nu_3\}$ be a K -basis of L , such that all $\nu_i \in \mathbb{R}$, for example we can take K -Galois conjugates of $\zeta_7 + \zeta_7^{-1}$. The left regular

representation of $\mathcal{D}$ gives a family of 3×3 matrices of the form

$$\sum_{k=0}^2 \begin{bmatrix} c_k & 0 & 0 \\ 0 & \sigma(c_k) & 0 \\ 0 & 0 & \sigma^2(c_k) \end{bmatrix} \Gamma^k,$$

where

$$\Gamma = \begin{bmatrix} 0 & 0 & \gamma \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

and c_0, c_1, c_2 are K -linear combinations of $\{\nu_1, \nu_2, \nu_3\}$, that is

$$\sum_{k=0}^2 \sum_{j=1}^3 c_{kj} \begin{bmatrix} \nu_j & 0 & 0 \\ 0 & \sigma(\nu_j) & 0 \\ 0 & 0 & \sigma^2(\nu_j) \end{bmatrix} \Gamma^k.$$

We can thus encode 9 elements of K . Since K is of degree 2 over $\mathbb{Q}(i)$, this is more rate than we can support, namely 18 complex symbols instead of 9. Let us write $d \in K$ as

$$d = d_0 + d_1 i + \sqrt{7} d_2 + \sqrt{7} i d_3, \quad d_1, d_2, d_3, d_4 \in \mathbb{Q}.$$

By setting two d_i to zero, we obtain the right rate. We do so in such a way that the resulting $\mathbb{Q}$ -basis of K has one basis element, say μ_1 totally real (μ_1 is 1 or $\sqrt{7}$), and the other, say μ_2 totally imaginary (μ_2 is i or $i\sqrt{7}$). A basis of $\mathcal{D}$ can then be written explicitly, for $j = 1, 2, 3$, as

$$\begin{aligned} D_j &= \mu_1 V_j, \quad D_{3+j} = \mu_2 V_j, \\ D_{6+j} &= \mu_1 V_j \Gamma, \quad D_{9+j} = \mu_2 V_j \Gamma, \\ D_{12+j} &= \mu_1 V_j \Gamma^2, \quad D_{15+j} = \mu_2 V_j \Gamma^2 \end{aligned}$$

where we denote

$$V_j = \begin{bmatrix} \nu_j & 0 & 0 \\ 0 & \sigma(\nu_j) & 0 \\ 0 & 0 & \sigma^2(\nu_j) \end{bmatrix}$$

for short. We have

$$\mu_1 V_j \mu_2^* V_k^* + \mu_2 V_k \mu_1^* V_j^* = \mu_1 (\mu_2^* + \mu_2) V_j V_k = 0$$

using that V_j, V_k have only real coefficients, and commute with each other since they are diagonal. Furthermore, μ_1 was also real, while μ_2 is totally imaginary. Next

$$\begin{aligned} \mu_1 V_j \Gamma \mu_2^* \Gamma^* V_k^* + \mu_2 V_k \Gamma \mu_1^* \Gamma^* V_j^* \\ = \mu_1 (\mu_2^* + \mu_2) V_j \Gamma \Gamma^* V_k = 0 \end{aligned}$$

since

$$\Gamma \Gamma^* = \begin{bmatrix} 0 & 0 & \gamma \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \gamma^* & 0 & 0 \end{bmatrix} = \begin{bmatrix} |\gamma|^2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

commutes with diagonal matrices V_j, V_k . The same computation holds for the last set of basis elements, involving the generator Γ^2 .

At the price of sacrificing full-diversity, we may choose $\theta = -1$. This will result in additional relations:

$$\alpha_\theta(D_i, 0) \alpha_\theta(0, D_j)^* + \alpha_\theta(0, D_j) \alpha_\theta(D_j, 0)^* = 0$$

for all $i, j = 1, \dots, 6$ implying decoding complexity $O(|S|^{30})$ using [6, Lemma 2].

Fig. 3. Field extension used for the second code example.

B. Example 2

This construction is the same as in Example 1, but the ground field is $F = \mathbb{Q}$. Let $F = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_7)$, where ζ_7 is a primitive 7^{th} root of unity. The field L has a cyclic Galois group $\text{Gal}(L/\mathbb{Q})$ of order 6. The automorphism

$$\sigma_2 : \zeta_7 \mapsto \zeta_7^2$$

is of order 3 and hence has a fixed field $K = \mathbb{Q}(\sqrt{-7})$, whose Galois $\mathbb{Q}$ -automorphism is

$$\tau : \sqrt{-7} \mapsto -\sqrt{-7}.$$

By similar arguments as in Example 1, we can demonstrate that the element $\gamma = 3$ is a non-norm of the extension L/K : namely, 3 multiplicatively generates nonzero elements of $\mathbb{F}_7$, the residue field of the ideal above 7 in K . Therefore the algebra $\mathcal{D} = (L/K, \sigma_2, \gamma)$ is division. The left regular representation of $\mathcal{D}$ gives a family of 3×3 matrices which is again of the form

$$\sum_{k=0}^2 \begin{bmatrix} c_k 0 & 0 \\ 0 & \sigma(c_k) & 0 \\ 0 & 0 & \sigma^2(c_k) \end{bmatrix} \begin{bmatrix} 0 & 0 & \gamma \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}^k,$$

where c_0, c_1, c_2 are elements of L/K , except that this time K is of degree 2 over $\mathbb{Q}$, instead of 4, as in the previous example. This also means that this construction immediately gives the right rate.

For the iterative construction, first we observe that $\theta = i\sqrt{7}$ is an element whose cube is not fixed by τ . Hence, by Lemma 1 the elements in the image of $\alpha_{i\sqrt{7}}$ have nonzero determinant. We set the code $\mathcal{C}$ to be the matrices in the image of $\tilde{\alpha}_{i\sqrt{7}}(\mathcal{D}, \mathcal{D})$, and by Lemma 2, the decoding complexity of $\mathcal{D}$ is left. Similar computations as in the previous example can be done. In fact, the key point here is that the fast decodability condition (8) requires the product of two basis matrices to be a skew-Hermitian matrix. This is most easily achieved in our setting by a basis which is a combination of totally real matrices on the one hand and totally imaginary matrices on the other hand, as shown earlier.

VI. CONCLUSION

In this paper, we presented an iterated construction to build fast decodable full-rate space-time codes for 6Tx - 3Rx MIMO

channels, starting from 3×3 algebraic space-time codewords. We gave a criterion to decide whether the proposed space-time codes are fully-diverse, and showed how the decoding complexity of the 6×6 codebook depends on the original 3×3 codewords. We gave two code examples as an illustration. Future work involves extending the construction for an arbitrary number of transmit antennas. Though generalizing the construction itself does not seem difficult, finding codes with good complexity reduction is not trivial. Also of interest would be a bound on the minimum decoding complexity that one can hope for given a full-rate code. Finally, another research direction would be the study of fast decodable codes for suboptimal decoders.

ACKNOWLEDGMENT

The research of N. Markin 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] V. Tarokh, N. Seshadri, A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Trans. on Information Theory*, vol. 44, no. 2, March 1998.
- [2] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. on Information Theory*, vol. 49, no. 10, pp. 2596-2616, Oct. 2003.
- [3] E. Viterbo, J. Boutros, "A universal lattice decoder for fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, 1999.
- [4] E. Biglieri, Y. Hong and E. Viterbo, "On fast-decodable space-time block codes", *IEEE Trans. Inform. Theory*, vol. 55, no. 2, Feb 2009.
- [5] , C. Hollanti, H.F. Lu "Construction Methods for Asymmetric and Multiblock Space-Time Codes", *IEEE Trans Inf. Theory*,
- [6] G. R. Jithamitra, B. S. Rajan, "A quadratic form approach to ML decoding complexity," preprint available at <http://arxiv.org/abs/1004.2844>.
- [7] L. P. Natarajan, B. S. Rajan, "Fast group-decodable STBCs via codes over GF(4)," *IEEE Int. Symp. Inform. Theory*, Austin, TX, June 2010.
- [8] L. P. Natarajan, B. S. Rajan, "Fast-Group-Decodable STBCs via codes over GF(4): Further Results," *IEEE ICC*, Kyoto, Japan, June 2011.
- [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] J. Lahtonen, N. Markin, G. McGuire "Construction of Space-Time Codes from Division Algebras with Roots of Unity as Non-Norm Elements", *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5231-5235, 2008.
- [11] 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.
- [12] F. Oggier, R. Vehkalahti, C. Hollanti, "Fast-decodable MIMO codes from crossed product algebras," *IEEE Int. Symp. Inform. Theory*, Austin, TX, June 2010.
- [13] N. Markin, F. Oggier, "Iterated MIMO Space-Time Code Constructions," *Allerton Conference*, 2011.
- [14] Natarajan and Rajan, "Asymptotically-Optimal, Fast-Decodable, Full-Diversity STBCs", *IEEE ICC*, 2011.
- [15] M.O. Sinnokrot, J. R. Barry, V.K. Madiseti "Embedded Alamouti Space-Time Codes for High Rate and Low Decoding Complexity", *Asilomar Conference on Signals, Systems, and Computers*, 2008.
- [16] H.E. Gamal, M.O. Damen, "Universal Space-Time Coding", *IEEE Trans. Inf. Theory*, Vol. 49, No. 5, pp. 1097-1119, May. 2003.