Iterated fast decodable space-time codes from crossed-products

Markin, Nadya; Oggier, Frederique

2012

Markin, N., & Oggier, F. (2012). Iterated fast decodable space-time codes from crossed-products. 20th International Symposium on Mathematical Theory of Networks and Systems Proceedings.

https://hdl.handle.net/10356/79790

ITERATED FAST-DECODABLE SPACE-TIME CODES FROM CROSSED-PRODUCTS

NADYA MARKIN AND FRÉDÉRIQUE OGGIER *

Key words. space-time coding, division algebras, crossed-products

AMS subject classifications. 16K20, 16U99, 11T71

EXTENDED ABSTRACT. We consider the following coding problem arising in wireless communication. Suppose we have transmission over a coherent Rayleigh fading channel with 8 Tx antennas, 2 Rx antennas and perfect channel state information at the receiver:

$$Y = H_{2\times 8}X_{8\times 8} + V_{2\times 8}, \tag{0.1}$$

where $H_{2\times 8}$ is the channel matrix, $V_{2\times 8}$ is the noise at the receiver, and both matrices have complex Gaussian independently distributed coefficients with zero mean. The matrix $X_{8\times 8} = g_1B_1 + \cdots + g_rB_r$ is a codeword from a space-time codebook $\mathcal{C}$, defined by the generating matrices $B_1, \ldots, B_r$, also called $\mathbb{Z}$-basis of the code. The information symbols $g_1, \ldots, g_r$ are assumed to be scaled integers (PAM symbols) in some set S. We consider *full-rate* codes, that is the case $r = 32$.

Each 2×8 matrix $H_{2\times 8}B_j$ corresponds via vectorization to a vector $\mathbf{b}_j \in \mathbb{R}^r$ obtained by stacking the columns of $H_{2\times 8}B_j$ followed by separating the real and imaginary parts. We define the matrix $B = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_r) \in M_{r\times r}(\mathbb{R})$, so every received codeword can be represented as a real vector $B\mathbf{g}$, with $\mathbf{g} = (g_1, \ldots, g_r)^T \in S^r$. Maximum-likelihood (ML) decoding amounts to finding, with respect to the Euclidean norm,

$$\arg\min\{||\mathbf{y} - B\mathbf{g}||_E^2\}_{\mathbf{g}\in S^r} = \arg\min\{||Q^*\mathbf{y} - R\mathbf{g}||_E^2\}_{\mathbf{g}\in S^r} \tag{0.2}$$

where $\mathbf{y}$ is the vectorization of the received matrix 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 R determines the complexity of the decoding via sphere decoder [1]: the *ML decoding complexity* is the minimum number of values of $\mathbf{g} \in S^r$ for which the distance in (0.2) should be computed. The worst case $O(|S|^\kappa)$ with $\kappa = r$ corresponds to exhaustive search, when R is a full triangular matrix. The exponent κ is called the *complexity order* of the code. If the code structure is such that $\kappa < r$, the code is said to be *fast-decodable*. It was proven [2] that fast-decodability follows from the zero structure of the Hurwitz-Radon matrix M, defined by orthogonality relations of the basis elements $B_1, \ldots, B_r$, in Frobenius norm:

$$M_{k,l} = ||B_kB_l^* + B_lB_k^*||_F. \tag{0.3}$$

Our construction, based on division algebras, will take advantage of this property.

*The authors are with Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. ({NMarkin,frederique}@ntu.edu.sg). The work 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.

Division algebras are a known mathematical tool for constructing fully-diverse space-time codes [3], that is, codes satisfying $\det(X - X') \neq 0$ for every $X \neq X' \in \mathcal{C}$. By linearity of an algebra, this criterion reduces to checking that $\det(X) \neq 0$ whenever $X \in \mathcal{C}$ is non-zero. We propose a construction which uses a 4×4 crossed-product code to construct an 8×8 fast-decodable full-rate space-time code. Let K/F be a biquadratic extension of a number field F with Galois group $G = Gal(K/F) = \{id, \sigma, \tau, \sigma\tau\}$. For an element $g \in G$, let K^g denote the fixed field of the subgroup $\langle g \rangle$. Fix three elements $a \in K^\sigma, b \in K^\tau$ and $u \in K$ satisfying $u\sigma(u) = \frac{a}{\tau(a)}$, $u\tau(u) = \frac{b}{\sigma(b)}$. The crossed-product $\mathcal{A} = (K/F, a, b, u)$ is the algebra given by the vector space of dimension 4 over K

$$\mathcal{A} = K \oplus e_\sigma K \oplus e_\tau K \oplus e_{\sigma\tau} K$$

with the following rules

$$e_\sigma^2 = a, e_\tau^2 = b, e_\tau e_\sigma = e_\sigma e_\tau u = e_{\sigma\tau} u, x e_g = e_g g(x) \ \forall x \in K, \ \forall g \in G.$$

We view elements of the crossed-product via left regular representation as 4×4 matrices over K, where each element $x + e_\sigma y + e_\tau v + e_{\sigma\tau} w$ corresponds the the matrix

$$\begin{bmatrix} A & b\tau(B) \\ B & \tau(A) \end{bmatrix}, \text{ with } A = \begin{bmatrix} x & a\sigma(y) \\ y & \sigma(x) \end{bmatrix}, \ B = \begin{bmatrix} v & \tau(a)u\sigma(w) \\ w & u\sigma(v) \end{bmatrix}$$

and τ acts on coefficients of matrices. A space-time code $\mathcal{C}$ can be obtained by considering matrices whose coefficients x, y, v, w are algebraic integers of K. When $\mathcal{A}$ is division, i.e., every nonzero element of $\mathcal{A}$ is invertible, the corresponding code $\mathcal{C}$ is fully-diverse. Given a fast-decodable 4×4 crossed-product code (see e.g. [4], [5]), we show that the 8×8 code generated by our construction naturally results in a matrix M in (0.3) which implies fast-decodability.

An Iterated Code Construction. We start with a crossed-product which we view via left regular representation as a subring of 4×4 matrices $Mat_{4\times4}(K)$. We show how to iteratively construct a larger algebra, which is a subset of $Mat_{8\times8}(K)$, that inherits fast-decodable properties of the crossed-product. We highlight the fact that matrices arising in the iterative step are not obtained via left regular representation, as is usually done in the literature. In fact, this technique gives rise to interesting division algebras, which can be further studied in terms of their center, degree, and maximal subfields.

Consider an F-automorphism ρ of K, extended to $\mathcal{A}$ by pointwise action on K-coefficients of elements of $\mathcal{A}$, i.e., for a matrix $A \in \mathcal{A} \subset Mat_{4\times4}(K)$, we have $\rho : (A_{ij}) \mapsto (\rho(A_{ij}))$. Given such an automorphism ρ, we define a map α_θ which embeds $\mathcal{A} \times \mathcal{A}$ into $Mat_{8\times8}(K)$ by letting $\alpha_\theta : \mathcal{A} \times \mathcal{A} \to Mat_{2\times2}(\mathcal{A})$ be defined by

$$\alpha_\theta : (X, Y) \mapsto \begin{bmatrix} X & \theta\rho(Y) \\ Y & \rho(X) \end{bmatrix}. \tag{0.4}$$

Remark that this construction is available for quaternion algebras [6], for cyclic algebras more generally [7], and in fact can be repeated iteratively.

It can be shown that the image $\mathcal{A}_2$ of α_θ has the structure of an F-algebra.

LEMMA 0.1. *Let $\theta \in F$ and $\rho \in Gal(K/F)$. Then the image $\mathcal{A}_2$ of α_θ forms an algebra of dimension 8 over F.*

Proof. Note that $\mathcal{A}_2 = \alpha_\theta(\mathcal{A}, \mathcal{A})$ is both additively and multiplicatively closed, since for any matrices X, Y, V, W representing elements of $\mathcal{A}$ we have

$$\alpha_\theta(X, Y) + \alpha_\theta(V, W) = \alpha_\theta(X + V, Y + W),$$

$$\alpha_\theta(X, Y)\alpha_\theta(V, W) = \alpha_\theta(XV + \theta\rho(Y)W, YV + \rho(X)W)$$

using the fact that $\rho(\theta) = \theta$ and $\rho^2 = id$. The center F of $\mathcal{A}$ embeds into the center of $\mathcal{A}_2$ via the map $Z \mapsto \alpha_\theta(Z, 0) = \begin{bmatrix} Z & 0 \\ 0 & Z \end{bmatrix}$. Since $\mathcal{A}_2$ is additionally a vector space over F, it has the structure of a F-algebra. Its dimension over F is 8, in particular this implies that the center of $\mathcal{A}_2$ is some quadratic extension of F. □

The following criterion on θ guarantees that the algebra $\mathcal{A}_2$ is division.

Lemma 0.2. *Let $\mathcal{A}$ be a division crossed-product algebra, whose elements correspond to 4×4 matrices over a field K. Let ρ and θ satisfy the hypothesis of Lemma 0.1. Then $\mathcal{A}_2 = \alpha_\theta(\mathcal{A}, \mathcal{A})$ is division if and only if $\theta \neq Z\rho(Z)$ for all $Z \in \mathcal{A}$.*

Proof. See [6, Lemma 1] for a proof of similar results for quaternion algebras. □

In order for $\alpha_\theta(\mathcal{A}, \mathcal{A})$ to have the structure of an algebra, the element θ must come from F. By dropping this requirement, we can still, however, obtain fully-diverse codes from $\alpha_\theta(\mathcal{A}, \mathcal{A})$. In fact, if $\theta \in K$, $\alpha_\theta(\mathcal{A}, \mathcal{A})$ is still additively closed and F-linear, thus demonstrating full-diversity reduces to showing that $\det(X) \neq 0$ for any non-zero matrix X, which holds whenever $\theta \neq Z\rho(Z)$. If we pick $\theta \in K$ such that $\rho(\theta^4) \neq \theta^4$, then surely $\theta \neq Z\rho(Z)$: else taking the determinant of both sides would tell us that θ^4 is fixed by ρ.

Fast-Decodability. For the purposes of fast-decodability, we next define a scaled version $\tilde{\alpha}_\theta$ of the map α_θ. Let $V, W, X, Y \in \mathcal{A}$ be elements of the crossed-product algebra viewed as 4×4 matrices with coefficients in K. We denote by ζ a 4^{th} root of unity, i.e., $\zeta \in \{\pm 1, \pm i\}$. Express $\theta = \zeta\theta'$ with $\theta' > 0$ and define the map $\tilde{\alpha}_{\zeta\sqrt{\theta'}}$

$$\tilde{\alpha}_{\zeta\sqrt{\theta'}} : (V, W) \mapsto \begin{bmatrix} V & \zeta\sqrt{\theta'}\rho(W) \\ \sqrt{\theta'}W & \rho(V) \end{bmatrix}.$$

Then $\det(\alpha_{\zeta\theta}(V, W)) = \det(\tilde{\alpha}_{\zeta\sqrt{\theta'}}(V, W))$ for all V, W. In particular, the image of $\tilde{\alpha}$ retains the full-diversity property. Furthermore, assuming that complex conjugation commutes with ρ on elements of $\mathcal{A}$, and letting $\tilde{\alpha}$ denote $\tilde{\alpha}_{\zeta\sqrt{\theta'}}$ for short, we establish that

$$\tilde{\alpha}(X, Y)\tilde{\alpha}(V, W)^* = \tilde{\alpha}(XV^* + \theta\rho(YW^*), YV^* + \zeta^*\rho(XW^*)).$$

As a consequence, fast-decodable properties of the original code are inherited over the iteration, as we summarize in the following lemma.

Lemma 0.3. *If $\mathcal{A}$ gives rise to a fast-decodable code, then the code built from $\tilde{\alpha}(\mathcal{A}, \mathcal{A})$ also has a reduced decoding complexity. Given a basis $\{D_1, \ldots, D_r\}$ of $\mathcal{A}$, we have a basis $\{\tilde{\alpha}(D_j, 0), \tilde{\alpha}(0, D_k) : 1 \leq j, k \leq r\}$ of $\tilde{\alpha}_\theta(\mathcal{A}, \mathcal{A})$. 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 elements of $\tilde{\alpha}(\mathcal{A}, \mathcal{A})$ above:*

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

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

For example, we can use the crossed-product algebra code constructed in [4] whose corresponding Hurwitz-Radon matrix has the zero structure

$$M = \begin{bmatrix} t & 0 & 0 & 0 & t & t & t & t \\ 0 & t & 0 & 0 & t & t & t & t \\ 0 & 0 & t & 0 & t & t & t & t \\ 0 & 0 & 0 & t & t & t & t & t \\ t & t & t & t & t & 0 & 0 & 0 \\ t & t & t & t & 0 & t & 0 & 0 \\ t & t & t & t & 0 & 0 & t & 0 \\ t & t & t & t & 0 & 0 & 0 & t \end{bmatrix}$$

where each entry is a 2×2 matrix; 0 denoting the zero matrix and t denoting any other. Then the Hurwitz-Radon matrix corresponding to the iterated code will have the zeros of

$$\begin{bmatrix} t & 0 & 0 & 0 & t & t & t & t & t & t & t & t & t & t & t & t \\ 0 & t & 0 & 0 & t & t & t & t & t & t & t & t & t & t & t & t \\ 0 & 0 & t & 0 & t & t & t & t & t & t & t & t & t & t & t & t \\ 0 & 0 & 0 & t & t & t & t & t & t & t & t & t & t & t & t & t \\ t & t & t & t & t & 0 & 0 & 0 & t & t & t & t & t & t & t & t \\ t & t & t & t & 0 & t & 0 & 0 & t & t & t & t & t & t & t & t \\ t & t & t & t & 0 & 0 & t & 0 & t & t & t & t & t & t & t & t \\ t & t & t & t & 0 & 0 & 0 & t & t & t & t & t & t & t & t & t \\ t & t & t & t & t & t & t & t & t & 0 & 0 & 0 & t & t & t & t \\ t & t & t & t & t & t & t & t & 0 & t & 0 & 0 & t & t & t & t \\ t & t & t & t & t & t & t & t & 0 & 0 & t & 0 & t & t & t & t \\ t & t & t & t & t & t & t & t & 0 & 0 & 0 & t & t & t & t & t \\ t & t & t & t & t & t & t & t & t & t & t & t & t & 0 & 0 & 0 \\ t & t & t & t & t & t & t & t & t & t & t & t & 0 & t & 0 & 0 \\ t & t & t & t & t & t & t & t & t & t & t & t & 0 & 0 & t & 0 \\ t & t & t & t & t & t & t & t & t & t & t & t & 0 & 0 & 0 & t \end{bmatrix}$$

where again each entry is a 2×2 matrix; 0 denoting the zero matrix and t denoting any other.

In this extended abstract, we presented the basic framework for iteratively constructing space-time codes, starting with crossed-product algebras. We gave a necessary and sufficient condition for the resulting codes to be fully-diverse. It would be an interesting problem for further research to establish precise arithmetic criteria for satisfying the condition of Lemma 0.2, as well as looking for concrete code examples to compare with the existing ones.

REFERENCES

[1] E. Biglieri, Y. Hong and E. Viterbo, "On fast-decodable space-time block codes," *IEEE Trans. Inform. Theory*, vol. 55, no. 2, Feb 2009.

[2] 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

[3] 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.

[4] L. Luzzi, F. Oggier, "A family of fast-decodable MIDO codes from crossed-product algebras over $\mathbb{Q}$," *Proc. IEEE Int. Symp. Inform. Theory*, St Petersburg, July 2011.

[5] R. Vehkalahti, C. Hollanti, F. Oggier, "Fast-Decodable Asymmetric Space-Time Codes from Division Algebras", *IEEE Transactions on Information Theory*, vol. 58, no. 4, April 2012.

[6] N. Markin, F. Oggier, "Iterated MIDO Space-Time Code Constructions," *Allerton Conference*, 2011.

[7] N. Markin, F. Oggier, "A Class of Iterated Fast Decodable Space-Time Codes for 2^n Tx Antennas", *Proc. IEEE Int. Symp. Inform. Theory*, Boston, 2012.