Fast decodable MIDO codes from crossed product algebras

Oggier, Frederique; Roope, Vehkalahti; Hollanti, Camilla

2010

Oggier, F., Roope, V., & Camilla, H. (2010). Fast decodable MIDO codes from crossed product algebras. IEEE International Symposium on Information Theory.

<https://hdl.handle.net/10356/95630>

<https://doi.org/10.1109/ISIT.2010.5513709>

© 2010 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE. This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder. <http://www.ieee.org/portal/site> This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

Fast-decodable MIDO Codes from Crossed Product Algebras

Frédérique Oggier

Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore
Email: frederique@ntu.edu.sg

Roope Vehkalahti and Camilla Hollanti

Department of Mathematics
University of Turku
Finland
Email: {roiive,cajoho}@utu.fi

Abstract—The goal of this paper is to design fast-decodable space-time codes for four transmit and two receive antennas. The previous attempts to build such codes have resulted in codes that are not full rank and hence cannot provide full diversity or high coding gains. Extensive work carried out on division algebras indicates that in order to get, not only non-zero but perhaps even non-vanishing determinants (NVD) one should look at division algebras and their orders. To further aid the decoding, we will build our codes so that they consist of four generalized Alamouti blocks which allows decoding with reduced complexity. The level of reduction depends on whether one is willing to compromise the ML performance. As far as we know, the resulting codes are the first having reduced decoding complexity and at the same time allow one to give a proof of the NVD property.

I. INTRODUCTION

One of the most interesting wireless applications currently is the design of 4×2 multiple input-double output (MIDO) codes. Such asymmetric systems can be used in the communication between, for instance, a TV station and a portable digital-TV device. Codes with the so-called non-vanishing determinant (NVD) property and excellent performance for this purpose have been designed in e.g. [6], [9], [7], but all the codes require high complexity decoding, namely full-dimensional sphere decoding.

In order to reduce decoding complexity, an approach similar to the construction of the Silver code [8] was adopted in [2]. Namely, the Silver code is formed by adding together two copies of Alamouti code: one is the original Alamouti code, the other copy consists of elements that come from a unitary transformation of the original information symbols. Before addition, the unitarily transformed copy is yet to be multiplied with a diagonal twist matrix. The Silver code lattice has an orthogonal basis and the NVD property — putting it into the family of Perfect codes [10]. The MIDO code proposed in [2], for its part, is constructed in a similar manner by combining a quasi-orthogonal code [13] with a twisted unitary transformation of another quasi-orthogonal code. Unfortunately this resulted in a MIDO code that does have lower decoding complexity, but then does not have full rank. This is of course acceptable, because good performance is still achieved and with one dimension less in the sphere decoder. The most recent development can be found from

[12], where the authors propose a code with lowered decoding complexity and structure that might provide the code NVD property. While it is likely that the code in [12] does have NVD, it has not been proven yet.

The question we address in this paper is: can we get a code construction having reduced complexity and guaranteed NVD property. Of course we could continue to combine different quasi-orthogonal codes and hope that we would find a code with full diversity and with reduced complexity. However, this path is so natural that it might be already walked by many wanderers. Instead we forget the pedestrian approach and ask help from a mathematical oracle [4]. Let us consider a cyclic division algebra $\mathcal{A} = (\mathbb{Q}(\zeta_5)/\mathbb{Q}, \sigma, -2)$. It is then a known result [4] from the theory of *central simple algebras* that we have an injective map

$$\mathcal{A} \xrightarrow{f} M_2(H).$$

The 4×4 matrices in $M_2(H) \subseteq M_4(\mathbb{C})$ have form $(A_1, A_2; A_3, A_4)$, where each A_i has the Alamouti structure (see Definition 1). In particular if we have an *order* Λ in $\mathcal{A}$, $f(\Lambda)$ is a 16-dimensional lattice of matrices and each matrix $A \in f(\Lambda)$ has Alamouti-block structure and $|\det(A)| \geq 1$. Such a code lattice is not only a fully diverse MIDO code with NVD, but this special structure will allow us to drop the dimension of a sphere decoder by one. If one is willing to compromise the full ML performance, decoupling of the blocks is also possible. By doing this, we are able to replace a sphere decoder by two sphere decoders each with only half of the dimensions, giving us significant reduction in complexity.

We are now armed with an existence result and set our goal to construct MIDO codes with NVD property and Alamouti-like block structure. The mapping f given previously, however, is not explicit. Yet we have gotten two clues that will suggest two approaches.

The first clue is coming from the look of the matrices in $M_2(H)$. The structure of the matrices we get from a natural presentation 2 of *crossed product algebras* does closely resemble the structure of the matrices in $M_2(H)$. Crossed product algebras have been proposed as space-time codes in [11], [1]. In Section III-A this approach will result into a code

having orthogonal structure that will not result in shaping loss when a simple modulation is applied.

The second clue is algebraic. In the Section III-B we will use the algebra $\mathcal{A} = (\mathbb{Q}(\zeta_5)/\mathbb{Q}, \sigma, -2)$ as a starting point and try to imitate the mapping f . The resulting code is not orthogonal, but the performance will be closer to the best known MIDO codes, when spherical shaping is applied.

We do not claim to achieve the best known performance, but as far as we know these constructions are the first MIDO codes with proven NVD property and reduced complexity. Our preliminary research does suggest that these two approaches have vast untapped potential.

The notion of Alamouti-like block codes has been formalized in [2] as follows.

Definition 1: Let $\alpha, \beta, y_1, y_2 \in \mathbb{C}$ with $|\alpha| = |\beta| = 1$, and let $()^*$ denote the complex conjugation. A code of the form

$$\begin{pmatrix} \alpha y_1 & -\beta y_2^* \\ \alpha y_2 & \beta y_1^* \end{pmatrix}$$

is called a *generalized Alamouti code*.

The code we want to construct, for its part, is going to look like

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

where the 2×2 blocks A, B, C, D are generalized Alamouti codes. The blocks do not necessarily have to be independent of each other, as long as the code will carry 8 complex information symbols.

We assume the coherent Rayleigh fading channel model with perfect channel state information at the receiver (CSIR).

II. CROSSED PRODUCT ALGEBRAS OF DEGREE 4

We are using only two receive antennas, so we want the code matrix to contain 8 complex information symbols (e.g. QAM symbols). To carry 8 information symbols, the algebra in use should be of dimension 16 over the rationals $\mathbb{Q}$. But on the other hand, as we set forth specific requirements on how the code should look like, it might actually be easier to pick up too big an algebra, as then we will have some degrees of freedom to fit the desired form. Hence, we will consider crossed product algebras of degree 4 carrying 32 information symbols, half of which we can sacrifice in the urge to get four Alamouti-like blocks. Let us start by recalling the definition of biquadratic crossed product algebras, and how we can obtain 4×4 space-time block codes out of them.

Consider a Galois biquadratic extension L/K (see Fig. 1), namely

$$L = K(\sqrt{d}, \sqrt{d'}).$$

Its Galois group is a product of two cyclic groups of order 2, that is $\text{Gal}(L/K) = \{1, \sigma, \tau, \sigma\tau\}$, where σ, τ are defined by

$$\sigma(\sqrt{d}) = \sqrt{d}, \sigma(\sqrt{d'}) = -\sqrt{d'}$$

$$\tau(\sqrt{d}) = -\sqrt{d}, \tau(\sqrt{d'}) = \sqrt{d'}.$$

Fig. 1. A biquadratic extension of K .

In this case, using a suitable change of generators, one can show that a crossed product algebra $\mathcal{A}$ over L/K may be described as follows:

$$\mathcal{A} = L \oplus eL \oplus fL \oplus efL$$

with

$$e^2 = a, f^2 = b, fe = efu, \lambda e = e\sigma(\lambda), \\ \lambda f = f\tau(\lambda) \text{ for all } \lambda \in L,$$

for some elements $a, b, u \in L^\times$ satisfying

$$\sigma(a) = a, \tau(b) = b, u\sigma(u) = \frac{a}{\tau(a)}, u\tau(u) = \frac{\sigma(b)}{b}. \quad (1)$$

Definition 2: A crossed product algebra $\mathcal{A}$ over a biquadratic extension L/K will be called a *biquadratic crossed product algebra*. We write $\mathcal{A} = (a, b, u, L/K)$.

Note from (1) that we have that $a \in K(\sqrt{d})$ and $b \in K(\sqrt{d'})$.

Remark 1: In the case where the Galois group is not a product two smaller cyclic groups, but cyclic of degree 4, we recover the well known concept of cyclic algebra.

Example 1: Take $K = \mathbb{Q}(i)$, $d' = 5$ and $d = 2$. Let ζ_8 be a primitive 8th root of unity. Note that $L = \mathbb{Q}(i)(\zeta_8, \sqrt{5})$ since $\zeta_8 = \frac{1}{\sqrt{2}}(1+i)$. We have

$$\sigma(\sqrt{5}) = -\sqrt{5}, \tau(\sqrt{2}) = -\sqrt{2}, \tau(\zeta_8) = -\zeta_8.$$

The following choice of a, b, u is suitable: $a = \zeta_8$, $b = \sqrt{5}$, $u = i$. Clearly $\sigma(a) = a$ and $\tau(b) = b$. Finally

$$u\sigma(u) = -1 = \frac{\zeta_8}{-\zeta_8} \text{ and } u\tau(u) = -1 = \frac{-\sqrt{5}}{\sqrt{5}}.$$

Codewords from these algebras have the following form (see [1] for the proof and the details), given as usual by the left multiplication:

$$\begin{pmatrix} x_1 & a\sigma(x_\sigma) & b\tau(x_\tau) & ab\tau(u)\sigma\tau(x_{\sigma\tau}) \\ x_\sigma & \sigma(x_1) & b\tau(x_{\sigma\tau}) & b\tau(u)\sigma\tau(x_\tau) \\ x_\tau & \tau(a)u\sigma(x_{\sigma\tau}) & \tau(x_1) & \tau(a)\sigma\tau(x_\sigma) \\ x_{\sigma\tau} & u\sigma(x_\tau) & \tau(x_\sigma) & \sigma\tau(x_1) \end{pmatrix}. \quad (2)$$

If we denote by

$$A = \begin{pmatrix} x_1 & a\sigma(x_\sigma) \\ x_\sigma & \sigma(x_1) \end{pmatrix}, B = \begin{pmatrix} x_\tau & \tau(a)u\sigma(x_{\sigma\tau}) \\ x_{\sigma\tau} & u\sigma(x_\tau) \end{pmatrix},$$

we notice easily that if $\sigma\tau = \tau\sigma$, then the matrix (2) has the shape

$$M = \begin{pmatrix} A & b\tau(B) \\ B & \tau(A) \end{pmatrix}. \quad (3)$$

Criteria to decide whether crossed product algebras built on biquadratic extensions are division algebras are given in [1], where it is shown that the algebra of Example 1, namely

$$(a, b, u, L/K) = (\zeta_8, \sqrt{5}, i, \mathbb{Q}(i)(\sqrt{2}, \sqrt{5})/\mathbb{Q}(i))$$

is a division algebra. Since in this case $\sigma(\sqrt{5}) = -\sqrt{5}$ and $\tau(\sqrt{2}) = -\sqrt{2}$, we do have $\sigma\tau = \tau\sigma$, so that codewords coming from this algebra have the block shape form of (3). We can further normalize b so that $|b|^2 = 1$ to finally get the division algebra

$$(a, b, u, L/K) = (\zeta_8, \sqrt{\frac{1+2i}{1-2i}}, i, \mathbb{Q}(i)(\sqrt{2}, \sqrt{5})/\mathbb{Q}(i)).$$

III. CODE CONSTRUCTIONS

A. First Construction

We now use the division algebra

$$(a, b, u, L/K) = (\zeta_8, \sqrt{\frac{1+2i}{1-2i}}, i, \mathbb{Q}(i)(\sqrt{2}, \sqrt{5})/\mathbb{Q}(i))$$

built in the previous section to construct MIDO codes.

First, we provide a MIDO code which contains 4 generalized Alamouti block codes and is fully diverse. By restricting the coefficients to the ring of integers, we further get the non-vanishing determinant property, that is $\min_{X \neq X'} \det(X - X')$ can be lower bounded prior to SNR normalization by a constant that does not depend on the size of the signal constellation.

We proceed as follows. Note that an element in $L = \mathbb{Q}(i)(\sqrt{2}, \sqrt{5})$ can be written in the $\mathbb{Q}(i)$ -basis $\{1, \zeta_8, \sqrt{5}, \zeta_8\sqrt{5}\}$ as

$$x = x_0 + x_1\zeta_8 + x_2\sqrt{5} + x_3\zeta_8\sqrt{5}, \quad x_0, \dots, x_3 \in \mathbb{Q}(i).$$

To x thus corresponds 8 symbols in $\mathbb{Q}$.

Consider the following elements in L , obtained by fixing 4 coefficients in $\mathbb{Q}$ (for example, write $x_1 = a_1 + ia'_1$ and choose $a'_1 = -a_1$ which gives $x_1 = a_1 - ia_1 = (1-i)a_1$):

$$\begin{aligned} y_1 &= a_0 + a_1(1-i)\zeta_8 + ia_2\sqrt{5} + a_3(1+i)\zeta_8\sqrt{5} \\ y_2 &= b_1 + ib_0 + (b_0 + ib_1)\zeta_8 + (-b_3 + ib_2)\sqrt{5} + (-b_2 + ib_3)\zeta_8\sqrt{5} \\ y_3 &= ic_0 + c_1(1+i)\zeta_8 + c_2\sqrt{5} + c_3(1-i)\zeta_8\sqrt{5} \\ y_4 &= d_1 + id_0 + (d_0 + id_1)\zeta_8 + (-d_3 + id_2)\sqrt{5} + (-d_2 + id_3)\zeta_8\sqrt{5}, \end{aligned}$$

where $a_j, b_j, c_j, d_j \in \mathbb{Z}$, $j = 0, \dots, 3$.

Remark 2: Out of the $4 \cdot 8$ elements in $\mathbb{Q}$ that could be obtained using the whole algebra, we are left with $4 \cdot 4$ real symbols, that is 8 complex symbols. This perfectly fits the MIDO setting.

It is an easy computation to check that

$$\begin{aligned} \sigma(y_1) &= y_1^* \\ \zeta_8\sigma(y_2) &= -y_2^* \\ \sigma(y_3) &= -y_3^* \\ -\zeta_8\sigma(y_4) &= y_4^*. \end{aligned}$$

If we look at the first 2 columns of the matrix (2), we get

$$\begin{pmatrix} x_1 & \zeta_8\sigma(x_\sigma) \\ x_\sigma & \sigma(x_1) \\ x_\tau & -\zeta_8i\sigma(x_{\sigma\tau}) \\ x_{\sigma\tau} & i\sigma(x_\tau) \end{pmatrix},$$

that is, after taking $x_1 = y_1$, $x_\sigma = y_2$, $x_\tau = y_3$ and $x_{\sigma\tau} = y_4$

$$\begin{pmatrix} y_1 & -y_2^* \\ y_2 & y_1^* \\ y_3 & iy_4^* \\ y_4 & -iy_3^* \end{pmatrix}.$$

Since $\tau^* = *\tau$, the whole codeword is given by:

$$\begin{pmatrix} y_1 & -y_2^* & b\tau(y_3) & bi\tau(y_4)^* \\ y_2 & y_1^* & b\tau(y_4) & -ib\tau(y_3)^* \\ y_3 & iy_4^* & \tau(y_1) & -\tau(y_2)^* \\ y_4 & -iy_3^* & \tau(y_2) & \tau(y_1)^* \end{pmatrix}. \quad (4)$$

Since we have obtained the above matrix by puncturing an order [14] of a division algebra, and the resulting lattice basis has an orthogonal Gram matrix, we have proven the following:

Proposition 1: The code $\mathcal{C}_1$ composed with codewords of the form (4) is a fully diverse orthogonal MIDO code with NVD containing 4 generalized Alamouti block codes.

If we write the matrix (2) by block, we get

$$\begin{pmatrix} A & C \\ B & D \end{pmatrix}$$

with

$$A = \begin{pmatrix} y_1 & -y_2^* \\ y_2 & y_1^* \end{pmatrix}, \quad D = \begin{pmatrix} \tau(y_1) & -\tau(y_2)^* \\ \tau(y_2) & \tau(y_1)^* \end{pmatrix},$$

both blocks being Alamouti codes, and

$$B = \begin{pmatrix} y_3 & iy_4^* \\ y_4 & -iy_3^* \end{pmatrix}, \quad C = \begin{pmatrix} b\tau(y_3) & bi\tau(y_4)^* \\ b\tau(y_4) & -ib\tau(y_3)^* \end{pmatrix}$$

are generalized Alamouti code with resp. $\beta = -i$ for B and $\alpha = b$, $\beta = -ib$ for C . Note that $|-i|^2 = |b|^2 = |-ib|^2 = 1$.

Remark 3: The code can also be seen as a two-level MIMO code, into which we have embedded both a 4×4 and a 4×2 code. The full 4×4 code is known to have an excellent performance [1]. The MIDO code, for its part, is obtained by a simple puncturing as shown above. Unfortunately, its performance is not quite comparable to that of the other fast-decodable MIDO codes. The code has not been optimized, so we can count on a better performance after a serious optimization round.

B. Second construction

In this section we follow the algebraic clue we got at the beginning of this paper. The natural starting point is the previously mentioned cyclic algebra $\mathcal{A} = (\mathbb{Q}(\zeta_5)/\mathbb{Q}, \sigma, -2)$, where the mapping σ is defined by the equation $\sigma(\zeta_5) = \zeta_5^3$. The key point here is to notice that σ^2 is the complex conjugation. The usual cyclic representation then gives us matrices of type

$$\begin{pmatrix} x_0 & -2\sigma(x_3) & -2(x_2)^* & -2\sigma(x_1)^* \\ x_1 & \sigma(x_0) & -2(x_3)^* & -2\sigma(x_2)^* \\ x_2 & \sigma(x_1) & (x_0)^* & -2\sigma(x_3)^* \\ x_3 & \sigma(x_2) & (x_1)^* & \sigma(x_0)^* \end{pmatrix},$$

where $x_i = a_{i,1} + a_{i,2}\zeta_5 + a_{i,3}\zeta_5^2 + a_{i,4}\zeta_5^3$, $a_{i,j} \in \mathbb{Q}$. If we now restrict the coefficients $a_{i,j}$ to $\mathbb{Z}$ the resulting code has NVD. As the center of the algebra is $\mathbb{Q}$ we will get a 16-dimensional lattice. A known “energy normalization” trick will then give us code matrices of type

$$\begin{pmatrix} x_0 & -2\sigma(x_3) & -\sqrt{2}(x_2)^* & -\sqrt{2}\sigma(x_1)^* \\ x_1 & \sigma(x_0) & -\sqrt{2}(x_3)^* & -\sqrt{2}\sigma(x_2)^* \\ \sqrt{2}x_2 & \sqrt{2}\sigma(x_1) & (x_0)^* & -2\sigma(x_3)^* \\ \sqrt{2}x_3 & \sqrt{2}\sigma(x_2) & (x_1)^* & \sigma(x_0)^* \end{pmatrix}.$$

Let us now multiply the last column with -1, then switch second and third row and finally switch the second and third column. As a result we end up with code matrices of form

$$\begin{pmatrix} x_0 & -\sqrt{2}(x_2)^* & -2\sigma(x_3) & -\sqrt{2}\sigma(x_1)^* \\ \sqrt{2}x_2 & (x_0)^* & \sqrt{2}\sigma(x_1) & -2\sigma(x_3)^* \\ x_1 & -\sqrt{2}(x_3)^* & \sigma(x_0) & -\sqrt{2}\sigma(x_2)^* \\ \sqrt{2}x_3 & (x_1)^* & \sqrt{2}\sigma(x_2) & \sigma(x_0)^* \end{pmatrix}.$$

We point out that “energy normalization” or column and row swapping do not affect the NVD property. Therefore we have ended up with a 16-dimensional MIMO-lattice having NVD and Alamouti block structure. By the usual discriminant analysis [14] we will find that the resulting code has *normalized minimum determinant* of size 0.0316. This is far from the best known 0.1361, that belongs to the code IA_{max} in [5]. Yet the performance of the code is far better than the bare determinant calculation allows one to expect. Yet this approach is still in the very beginning and there is plenty of optimization to be done.

IV. DECODING

Maximum-likelihood (ML) decoding consists of finding the code matrix X that achieves the minimum of the squared Frobenius norm

$$d(X) = \|Y - HX\|^2, \quad (5)$$

where Y and H denote the received matrix and the channel response matrix, respectively.

Definition 3: ([2, Def. 2]) The ML decoding complexity is the minimum number of values of $d(X)$ in (5) that should be computed in ML decoding. This number cannot exceed $|S|^\kappa$, the complexity of the exhaustive-search ML decoder. Here $|S|$ is the size of the complex signaling alphabet in use (e.g. a 4-QAM), and κ is the number of independent complex information symbols drawn from S carried within one code matrix.

Let us now look at the decoding of the previously proposed codes. As they have similar block structure, the decoding complexity as defined in Definition 3 is the same for both of these codes, and $\kappa = 8$. In the following we shall

concentrate on the first code. To speed up the decoding, the standard implementations of a sphere decoder use the QR decomposition, which we investigate next.

Let $Y = (y_{ij})$, $H = (h_{ij})$, $N = (n_{ij})$ be the received, channel response, and noise matrices, resp. The channel equation

$$Y = HX + N, \quad X \in \mathcal{C}_1$$

can be equivalently rewritten as

$$y = F's' + n, \quad (6)$$

where

$$\begin{aligned} F' &= (f'_1 | f'_2 | \dots | f'_8), \\ s' &= (x_1, x_2, x_3, x_4, \tau(x_1), \tau(x_2), \tau(x_3), d_3))^T, \\ y &= (y_{11}, y_{21}, y_{12}^*, y_{22}^*, y_{13}, y_{23}, y_{14}^*, y_{24}^*)^T, \\ n &= (n_{11}, n_{21}, n_{12}^*, n_{22}^*, n_{13}, n_{23}, n_{14}^*, n_{24}^*)^T. \end{aligned}$$

We can alternatively fully write F' as

$$F' = \begin{pmatrix} F'_{(1)} & 0 \\ 0 & F'_{(2)} \end{pmatrix},$$

where

$$F'_{(1)} = \begin{pmatrix} h_{11} & h_{12} & h_{13} & h_{14} \\ h_{21} & h_{22} & h_{23} & h_{24} \\ h_{12}^* & -h_{11}^* & ih_{14}^* & -ih_{13}^* \\ h_{22}^* & -h_{21}^* & ih_{24}^* & -ih_{23}^* \end{pmatrix}$$

and

$$F'_{(2)} = \begin{pmatrix} h_{13} & h_{14} & bh_{11} & bh_{12} \\ h_{23} & h_{24} & bh_{21} & bh_{22} \\ h_{14}^* & -h_{13}^* & ib^*h_{12}^* & -ib^*h_{11}^* \\ h_{24}^* & -h_{23}^* & ib^*h_{22}^* & -ib^*h_{21}^* \end{pmatrix}.$$

The problem now is that a sphere decoder cannot really see the dependence between x_i and $\tau(x_i)$. So albeit s' only contains 16 real information symbols, in the eye of a sphere decoder there are twice as many. For this reason, we now consider the real representation s of the information vector s' , that is

$$s = (a_0, \dots, a_4, b_1, \dots, b_4, c_1, \dots, c_4, d_1, \dots, d_4) \quad (7)$$

which consists of the 16 PAM symbols as described in (4).

We can now write the channel equation (6) as a function of real information symbols as $y = Fs + n$, where s is defined in (7), and F is constructed as follows.

First, we define four vectors according to the four elements $y_1, \dots, y_4 \in L$ in (4):

$$\begin{aligned} a &= (1, (1-i)\zeta_8, i\sqrt{5}, (1+i)\zeta_8\sqrt{5}), \\ b &= (i + \zeta_8, 1 + i\zeta_8, (i - \zeta_8)\sqrt{5}, (-1 + i\zeta_8)\sqrt{5}), \\ c &= (i, (1+i)\zeta_8, \sqrt{5}, (1-i)\zeta_8\sqrt{5}), \text{ and} \\ d &= (i + \zeta_8, 1 + i\zeta_8, (i - \zeta_8)\sqrt{5}, (-1 + i\zeta_8)\sqrt{5}). \end{aligned}$$

Now $F = [f_1 | \dots | f_{16}]$ is an 8×16 matrix given by

$$\begin{bmatrix} f'_1 \otimes a & f'_2 \otimes b & f'_3 \otimes c & f'_4 \otimes d \\ f'_5 \otimes \tau(a) & f'_6 \otimes \tau(b) & f'_7 \otimes \tau(c) & f'_8 \otimes \tau(d) \end{bmatrix}, \quad (8)$$

where we have omitted the zero rows, $\otimes$ is the Kronecker product, and τ acts element-wise on the vectors.

Remark 4: The above real representation of s and the corresponding F (8) can of course be given a complex form as well. Note also that swapping columns in F (i.e., rows in s^T) is a legal operation, as we assumed perfect CSIR.

By abuse of notation, we denote again by s the complex information symbol vector, and by F the 8×8 matrix corresponding to this s . Now the QR decomposition of the matrix $F = QR$ tells us the dimensionality of the sphere decoder. Following [2], we denote $Q = [e_1, e_2, \dots, e_8]$. The upper triangular matrix R is then

$$R = \begin{pmatrix} \|d_1\| & \langle f_2, e_1 \rangle & \cdots & \langle f_\kappa, e_1 \rangle \\ 0 & \|d_2\| & \cdots & \langle f_\kappa, e_2 \rangle \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & \|d_\kappa\| \end{pmatrix},$$

where $d_1 = f_1$, $e_1 = \frac{d_1}{\|d_1\|} = \frac{f_1}{\|f_1\|}$, $d_i = f_i - \sum_{j=1}^{i-1} \text{Proj}_{e_j} f_i$, $e_i = \frac{d_i}{\|d_i\|}$, $i = 2, \dots, \kappa$, and $\text{Proj}_u v = \frac{\langle v, u \rangle}{\langle u, u \rangle} u$. Such formulation of the QR decomposition coincides with the Gram-Schmidt procedure applied to the column vectors of F . As pointed out in [3], the search procedure carried out by a sphere decoder can be visualized as a bounded tree search. If a standard sphere decoder is used for the decoding, we have κ levels of the complex tree, where the worst case computation complexity is $|S|^\kappa$. However, zeros appearing among the entries of R can lead to a simplified sphere decoder. Namely, if the condition

$$\langle f_2, e_i \rangle = \langle f_3, e_i \rangle = \cdots = \langle f_\kappa, e_i \rangle = 0 \quad (9)$$

is satisfied for $i = 1, \dots, k-1$ and for some $k \leq \kappa$, then k levels can be removed from the complex sphere decoding tree, and a $(\kappa - k)$ -dimensional sphere decoder can be employed instead. By doing this, the worst case complexity becomes $k|S|^{\kappa-k+1}$.

We immediately see that, for the real s , $\langle f_i, f_{i+j} \rangle = 0$ for $i = 1, 2, 3, 4$, $j = 4, 5, 6, 7$, and $i+j \leq 8$, and similarly $\langle f_k, f_{k+l} \rangle = 0$ for $k = 9, 10, 11, 12$, $l = 4, 5, 6, 7$, and $k+l \leq 16$. For the complex s , for its part, we get (by swapping the 2nd and 3rd complex information symbols) $\langle f_2, e_1 \rangle = \langle f_2, f_1 \rangle = 0$. Hence, according to Definition 3 and equation (9), the dimension of the search tree can be reduced by one, and the decoding complexity of the code C_1 (and of C_2) is $2|S|^7$ instead of $|S|^8$. Naturally, this is due to the orthogonality of the first and second code matrix column (4).

Remark 5: By imitating the decoding of the Alamouti code, it is also possible to decouple the blocks and then to separately decode the blocks by using two sphere decoders with only half of the dimensions. This will result in complexity $4|S|^3$. The reason why we can do this is the nice block structure of the matrix F : any 2×2 block multiplied by its transpose conjugate gives us a diagonal matrix. Hence multiplying the vector y with some suitable matrix will easily force more zeros into the matrix R . However, such decoupling requires operations

that will not necessarily maintain the ML performance, so the result will be a suboptimal decoder.

Further investigations are omitted due to lack of space.

ACKNOWLEDGMENT

The research of F. Oggier is supported in part by the Singapore National Research Foundation under Research Grant NRF-RF2009-07 and NRF-CRP2-2007-03, and in part by the Nanyang Technological University under Research Grant M58110049 and M58110070. The research of C. Hollanti and R. Vehkalahti is supported by the Emil Aaltonen Foundation's Young Researcher's Project, and by the Academy of Finland Grant XXX. This work was done while C. Hollanti was visiting the division of mathematical sciences, NTU, Singapore.

REFERENCES

- [1] Grégory Berhuy and Frédérique E. Oggier. Space-time codes from crossed product algebras of degree 4. In *Proc. Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17)*, pages 90–99, 2007.
- [2] E. Biglieri, Y. Hong, and E. Viterbo. On fast-decodable space-time block codes. *IEEE Trans. Inform. Theory*, 55(2), 2009.
- [3] M. O. Damen, H. El Gamal, and G. Caire. On maximum-likelihood detection and the search for the closest lattice point. *IEEE Trans. Inf. Theory*, 49(10):2389–2402, Oct. 2003.
- [4] JeanPaul Cerri Eva BayerFluckiger and Jérôme Chaubert. Euclidean minima and central division algebras. *International Journal of Number Theory*, 5:1155–1168, 2009.
- [5] C. Hollanti, J. Lahtonen, and H.-F. Lu. Maximal orders in the design of dense space-time lattice codes. *IEEE Trans. Inf. Theory*, 54(10):4493 – 4510, Oct. 2008.
- [6] Camilla Hollanti and H.-F. Lu. Construction methods for asymmetric and multi-block space-time codes. *IEEE Trans. Inf. Theory*, 55(3):1086 – 1103, 2009.
- [7] A. Hottinen, Y. Hong, E. Viterbo, C. Mehlführer, and C. F. Mecklenbrucker. A comparison of high rate algebraic and non-orthogonal stbcs. In *Proc. 2007 ITG/IEEE Workshop on Smart Antennas WSA*, Vienna, Austria, Feb. 2007.
- [8] A. Hottinen, O. Tirkkonen, and R. Wichman. *Multi-antenna Transceiver Techniques for 3G and Beyond*. WILEY publisher, UK, 2003.
- [9] H.-F. Lu and C. Hollanti. Optimal diversity multiplexing tradeoff and code constructions of constrained asymmetric MIMO systems. *IEEE Trans. on Inform. Theory*, submitted, May 2008.
- [10] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo. Perfect space time block codes. *IEEE Trans. Inf. Theory*, 52(9):3885–3902, Sept. 2006.
- [11] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman. Information-lossless STBCs from crossed-product algebras. *IEEE Trans. Inf. Theory*, 52:3913–3935, 2006.
- [12] K. Pavan Srinath and B. Sundar Rajan. Euclidean minima and central division algebras. *International Journal of Number Theory*, 5:1155–1168, 2009.
- [13] V. Tarokh, H. Jafarkhani, and A. R. Calderbank. Space-time block codes from orthogonal designs. *IEEE Trans. Inf. Theory*, 45:1456–1467, Jul. 1999.
- [14] R. Vehkalahti, C. Hollanti, J. Lahtonen, and K. Ranto. On the densest MIMO lattices from cyclic division algebras. *IEEE Trans. on Inform. Theory*, 55(8):3751–3780, Aug. 2009.