This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2009 proceedings

Algebraic reduction for the Golden Code

Ghaya Rekaya-Ben Othman, Laura Luzzi and Jean-Claude Belfiore

TELECOM ParisTech, 46 rue Barrault, 75013 Paris, France
E-mail: {rekaya, luzzi, belfiore}@telecom − paristech.fr

***Abstract*—In this paper we introduce a new right preprocessing method for the decoding of 2×2 algebraic space-time codes, called *algebraic reduction*, which exploits the multiplicative structure of the code. The principle of the new reduction is to absorb part of the channel into the code, by approximating the channel matrix with an element of the maximal order of the code algebra.**
We prove that algebraic reduction attains the receive diversity when followed by a simple zero-forcing (ZF) detection. Simulation results for the Golden Code show that using minimum mean squared error generalized decision feedback equalization (MMSE-GDFE left preprocessing), algebraic reduction with simple ZF detection has a loss of only $3\,\mathrm{dB}$ with respect to optimal decoding.
***Index Terms*—Algebraic reduction, right preprocessing, Golden Code, space-time codes, decoding**

I. Introduction

Space-time coding for multiple antenna systems is an efficient device to compensate the effects of fading in wireless channels through diversity techniques, and allows for increased data rates. A new generation of space-time code designs for MIMO channels, based on suitable subsets of division algebras, has been recently developed [12]. The algebraic constructions guarantee that these codes are full-rank, full-rate and information-lossless, and have the non-vanishing determinant property.
Up to now, the decoding of algebraic space-time codes has been performed using their lattice point representation. In particular, maximum likelihood decoders such as the Sphere Decoder or the Schnorr-Euchner algorithm are currently employed. However, the complexity of these decoders is prohibitive for practical implementation[1].
On the other side, suboptimal decoders like ZF, DFE, MMSE have low complexity but they don't preserve the diversity order of the system. The use of preprocessing before decoding improves the performance of suboptimal decoders, and reduces considerably the complexity of ML decoders [7]. Two types of preprocessing are possible:

- *Left preprocessing* (MMSE-GDFE) to obtain a better conditioned channel matrix;
- *Right preprocessing* (lattice reduction) in order to have a quasi-orthogonal lattice. The most widely used lattice reduction is the LLL reduction.

[1]The worst case complexity of sphere decoding for a 2×2 space-time code is of the order of M^4, where M is the size of the constellation. However, space-time codes that admit a reduced ML complexity of M^2 have been recently proposed [13, 9].

We are interested here in the right preprocessing stage; we propose a new reduction method for 2×2 space-time codes based on quaternion algebras which directly exploits the multiplicative structure of the space-time code. Up to now, algebraic tools have been used exclusively for coding but never for decoding. *Algebraic reduction* consists in absorbing a part of the channel into the code. This is done by approximating the channel matrix with a unit of a maximal order of the quaternion algebra.
The algebraic reduction has already been implemented by Rekaya et al. [11] for the fast fading channel, in the case of rotated constellations based on algebraic number fields. In this context, the units in the ring of integers of the field form an abelian multiplicative group whose generators are described by Dirichlet's unit theorem [6]. For quaternion skewfields, which are the object of this paper, the situation is more complicated because the unit group is not commutative. However, it is still possible to find a finite presentation of the group, that is a finite set of generators and relations.
As an example, we consider the Golden Code, and exhibit a set of generators for the unit group of its maximal order. Our simulation results for the Golden Code show that using MMSE-GDFE left preprocessing, the performance of algebraic reduction with ZF decoding is within $3\,\mathrm{dB}$ of the ML.

II. System model and notation

A. System model

We consider a quasi-static 2×2 MIMO system employing a space-time block code. The received signal is given by

$$Y = HX + W, \qquad X, H, Y, W \in M_2(\mathbb{C}) \tag{1}$$

The entries of H are i.i.d. complex Gaussian random variables with zero mean and variance per real dimension equal to $\frac{1}{2}$, and W is the Gaussian noise with i.i.d. entries of zero mean and variance N_0. X is the transmitted codeword.
In this paper we are interested in STBCs that are subsets of a principal ideal $\mathcal{O}\alpha$ of a maximal order $\mathcal{O}$ in a cyclic division algebra $\mathcal{A}$ of index 2 over $\mathbb{Q}(i)$ (a quaternion algebra). We refer to [12] for the necessary background about space-time codes from cyclic division algebras, and to [5] for a discussion of codes based on maximal orders.

Example (**The Golden Code**)**.** The Golden Code falls into this category (see [1, 5]). It is based on the cyclic algebra $\mathcal{A} = (\mathbb{Q}(i,\theta)/\mathbb{Q}(i), \sigma, i)$, where $\theta = \frac{\sqrt{5}+1}{2}$ and $\sigma : x \mapsto \bar{x}$ is

978-1-4244-3435-0/09/$25.00 ©2009 IEEE

such that $\sigma(\theta) = \bar{\theta} = 1-\theta$ and σ leaves the elements of $\mathbb{Q}(i)$ fixed. It has been shown in [5] that

$$\mathcal{O} = \left\{ \begin{pmatrix} x_1 & x_2 \\ i\bar{x}_2 & \bar{x}_1 \end{pmatrix},\ x_1, x_2 \in \mathbb{Z}[i,\theta] \right\} \tag{2}$$

is a maximal order of $\mathcal{A}$. $\mathcal{O}$ can be written as $\mathcal{O} = \mathbb{Z}[i,\theta] \oplus \mathbb{Z}[i,\theta]j$, where

$$j = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix} \tag{3}$$

Up to a scaling constant, the Golden Code is a subset of the two-sided ideal $\mathcal{O}\alpha = \alpha\mathcal{O}$, with $\alpha = 1 + i\bar{\theta}$. Every codeword of $\mathcal{G}$ has the form

$$X = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha x_1 & \alpha x_2 \\ \bar{\alpha} i \bar{x}_2 & \bar{\alpha}\bar{x}_1 \end{pmatrix}$$

with $x_1 = s_1 + s_2\theta$, $x_2 = s_3 + s_4\theta$. The symbols s_1, s_2, s_3, s_4 belong to a QAM constellation.

B. Notation

Notation (Vectorization of matrices). *Let ϕ be the function $M_2(\mathbb{C}) \to \mathbb{C}^4$ that vectorizes matrices:*

$$\phi : \begin{pmatrix} a & c \\ b & d \end{pmatrix} \mapsto (a, b, c, d)^t \tag{4}$$

The left multiplication function $A_l : M_2(\mathbb{C}) \to M_2(\mathbb{C})$ that maps B to AB induces a linear mapping $\mathbf{A}_l = \phi \circ A_l \circ \phi^{-1} : \mathbb{C}^4 \to \mathbb{C}^4$. That is, $\phi(AB) = \mathbf{A}_l\phi(B) \quad \forall A, B \in M_2(\mathbb{C})$, with $\mathbf{A}_l = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$.

Notation (Lattice point representation). *Consider a basis $\{w_1, w_2, w_3, w_4\}$ of $\alpha\mathcal{O}$ as a $\mathbb{Z}[i]$-module. Every codeword X can be written as*

$$X = \sum_{i=1}^{4} s_i w_i, \quad \mathbf{s} = (s_1, s_2, s_3, s_4)^t \in \mathbb{Z}[i]^4$$

If $\mathbf{\Phi}$ is the matrix whose columns are $\phi(w_1)$, $\phi(w_2)$, $\phi(w_3)$, $\phi(w_4)$, the lattice point corresponding to X is

$$\mathbf{x} = \phi(X) = \sum_{i=1}^{4} s_i \phi(w_i) = \mathbf{\Phi s}$$

We denote by Λ the $\mathbb{Z}[i]$-lattice with generator matrix $\mathbf{\Phi}$.

The following remark explains the relation between the units of the maximal order $\mathcal{O}$ of the code algebra and unimodular transformations of the code lattice. This property is fundamental for algebraic reduction.

Remark 1 (Units and unimodular transformations). Suppose that $U \in \mathcal{O}^*$ is an invertible element: then $\{Uw_1, Uw_2, Uw_3, Uw_4\}$ is still a basis of the $\mathbb{Z}[i]$-lattice $\alpha\mathcal{O}$. The codeword X can be expressed in the new basis:

$$X = \sum_{i=1}^{4} s'_i (Uw_i), \quad \mathbf{s}' = (s'_1, s'_2, s'_3, s'_4)^t \in \mathbb{Z}[i]^4$$

The vectorized signal is

$$\mathbf{\Phi s} = \phi(X) = \sum_{i=1}^{4} \phi(Uw_i) = \sum_{i=1}^{4} s'_i \mathbf{U}_l \phi(w_i) =$$
$$= \mathbf{U}_l \sum_{i=1}^{4} s'_i \phi(w_i) = \mathbf{U}_l \mathbf{\Phi s}'$$

Now consider the change of coordinates matrix $\mathbf{T}_U = \mathbf{\Phi}^{-1}\mathbf{U}_l\mathbf{\Phi} \in M_4(\mathbb{C})$ between the basis $\{\phi(w_i)\}_{i=1,\dots,4}$ and $\{\phi(Uw_i)\}_{i=1,\dots,4}$. We have $\det(\mathbf{T}_U) = \det(\mathbf{U}_l) = \det(U)^2 = \pm 1$. Moreover, $\forall \mathbf{s} \in \mathbb{Z}[i]^4$, $\mathbf{s}' = \mathbf{T}_U\mathbf{s} \in \mathbb{Z}[i]^4$. Then $\mathbf{T}_U$ is unimodular, and the lattice generated by $\mathbf{\Phi T}_U$ is still Λ.

III. Algebraic reduction

In this section we introduce the principle of algebraic reduction. First of all, we consider a normalization of the received signal. In the system model (1), the channel matrix H has nonzero determinant with probability 1, and so it can be rewritten as

$$H = \sqrt{\det(H)} H_1, \quad H_1 \in SL_2(\mathbb{C})$$

Therefore the system is equivalent to

$$Y_1 = \frac{Y}{\sqrt{\det(H)}} = H_1 X + W_1$$

Algebraic reduction consists in approximating the normalized channel matrix H_1 with a unit U of norm 1 of the maximal order $\mathcal{O}$ of the algebra of the considered STBC, that is an element U of $\mathcal{O}$ such that $\det(U) = 1$.

A. Perfect approximation

In order to simplify the exposition, we first consider the ideal case where we have a perfect approximation: $H_1 = U$. Of course this is extremely unlikely in practice; the general case will be treated in the next paragraph.
The received signal can be written:

$$Y_1 = UX + W_1 \tag{5}$$

and UX is still a codeword. In fact, since U is invertible,

$$\{UX \mid X \in \mathcal{O}\alpha\} = \mathcal{O}\alpha$$

Applying ϕ to both sides of equation (5), we find that the equivalent system in vectorized form is

$$\mathbf{y}_1 = \mathbf{U}_l \mathbf{\Phi s} + \mathbf{w}_1$$

where $\mathbf{\Phi}$ is the generator matrix of the code, $\mathbf{s} \in \mathbb{Z}[i]^4$, $\mathbf{y}_1 = \phi(Y_1)$, $\mathbf{w}_1 = \phi(W_1)$. Since U is a unit,

$$\mathbf{U}_l \mathbf{\Phi} = \mathbf{\Phi T}_U,$$

with $\mathbf{T}_U$ unimodular (see Remark 1), therefore

$$\mathbf{y}_1 = \mathbf{\Phi T}_U \mathbf{s} + \mathbf{w}_1 = \mathbf{\Phi s_1} + \mathbf{w}_1, \quad \mathbf{s_1} \in \mathbb{Z}[i]^4$$

In order to decode, we can simply consider ZF detection:

$$\hat{\mathbf{s}}_\mathbf{1} = \left\lfloor \mathbf{\Phi}^{-1}\mathbf{y}_1 \right\rceil$$

where $[\ ]$ denotes the rounding of each vector component to the nearest (Gaussian) integer.
If $\mathbf{\Phi}$ is unitary, as in the case of the Golden Code, algebraic reduction followed by ZF detection gives optimal (ML) performance.

B. General case

In general, the approximation is not perfect with probability 1 and we must take into account the approximation error E. We have $H_1 = EU$, and the vectorized received signal is

$$\mathbf{y}_1 = \mathbf{E}_l\mathbf{U}_l\mathbf{\Phi}\mathbf{s} + \mathbf{w}_1 = \mathbf{E}_l\mathbf{\Phi}\mathbf{T}_U\mathbf{s} + \mathbf{w}_1 = \mathbf{E}_l\mathbf{\Phi}\mathbf{s_1} + \mathbf{w}_1$$

The estimated signal after ZF detection is

$$\begin{aligned}\hat{\mathbf{s}}_\mathbf{1} &= \left[\mathbf{\Phi}^{-1}\mathbf{E}_l^{-1}\mathbf{y}_1\right] = \\ &= \left[\mathbf{s_1} + \frac{1}{\sqrt{\det(H)}}\mathbf{\Phi}^{-1}\mathbf{E}_l^{-1}\mathbf{w}\right] = [\mathbf{s}_1 + \mathbf{n}] \end{aligned} \tag{6}$$

Finally, one can recover an estimate of the initial signal $\hat{\mathbf{s}} = \mathbf{T}_U^{-1}\hat{\mathbf{s}}_\mathbf{1}$. Thus, the system is equivalent to a non-fading system where the noise $\mathbf{n}$ is no longer white Gaussian.

C. Choice of U for the ZF decoder

We suppose here for simplicity that the generator matrix $\mathbf{\Phi}$ is unitary, but a similar criterion can be established in a more general case. Ideally the error term E should be unitary in order to have optimality for the ZF decoder, so we should choose the unit U in such a way that $E = H_1U^{-1}$ is quasi-orthogonal. We require that the Frobenius norm $\|E\|_F^2$ should be minimized[2]:

$$U = \underset{\substack{U\in\mathcal{O},\\ \det(U)=1}}{\operatorname{argmin}} \left\|UH_1^{-1}\right\|_F^2 \tag{7}$$

This criterion corresponds to minimizing the trace of the covariance matrix of the new noise $\mathbf{n}$ in (6):

$$\begin{aligned}\operatorname{tr}(\operatorname{Cov}(\mathbf{n})) &= \frac{N_0}{|\det(H)|}\left\|\mathbf{\Phi}^{-1}\mathbf{E}_l^{-1}\right\|_F^2 = \\ &= \frac{N_0}{|\det(H)|}\left\|\mathbf{E}_l^{-1}\right\|_F^2 = \frac{2N_0}{|\det(H)|}\left\|E^{-1}\right\|_F^2 \end{aligned} \tag{8}$$

IV. The approximation algorithm

In this section we describe an algorithm to find the nearest unit U to the normalized channel matrix H_1 with respect to the criterion (7). To do this we need to understand the structure of the group of units of the maximal order $\mathcal{O}$.

Remark 2 (Units of norm 1). The set

$$\mathcal{O}^1 = \{U \in \mathcal{O}^* \mid \det(U) = 1\}$$

is a multiplicative subgroup of $\mathcal{O}^*$. In fact, if U is a unit of the $\mathbb{Z}[i]$-order $\mathcal{O}$, then $\mathrm{N}_{\mathcal{A}/\mathbb{Q}(i)}(U) = \det(U)$ is a unit in $\mathbb{Z}[i]$, that is, $\det(U) \in \{1, -1, i, -i\}$. $\mathcal{O}^1$ is the kernel of the reduced norm mapping $\mathrm{N} = \mathrm{N}_{\mathcal{A}/\mathbb{Q}(i)} : \mathcal{O}^* \to \{1, -1, i, -i\}$.

[2]Remark that since $\det(E) = 1$, $\|E\|_F^2 = \left\|E^{-1}\right\|_F^2$.

Table I
Generators of $\mathcal{O}^1$.

$$\begin{aligned} U_1 &= \begin{pmatrix} i\theta & 0 \\ 0 & i\bar{\theta} \end{pmatrix} & U_5 &= \begin{pmatrix} 1+i & 1+i\bar{\theta} \\ i(1+\theta) & 1+i \end{pmatrix} \\ U_2 &= \begin{pmatrix} i & 1+i \\ i-1 & i \end{pmatrix} & U_6 &= \begin{pmatrix} 1+i & 1+i\theta \\ i(1+\bar{\theta}) & 1+i \end{pmatrix} \\ U_3 &= \begin{pmatrix} \theta & 1+i \\ i-1 & \bar{\theta} \end{pmatrix} & U_7 &= \begin{pmatrix} 1-i & \bar{\theta}+i \\ i(\theta+i) & 1-i \end{pmatrix} \\ U_4 &= \begin{pmatrix} \theta & -1-i \\ -i+1 & \bar{\theta} \end{pmatrix} & U_8 &= \begin{pmatrix} 1-i & \theta+i \\ i(\bar{\theta}+i) & 1-i \end{pmatrix} \end{aligned}$$

Example (The Golden Code). In the case of the Golden Code, N is surjective since $\mathrm{N}(1) = 1$, $\mathrm{N}(\theta) = \theta\bar{\theta} = -1$, $\mathrm{N}(j) = -j^2 = -i$, $\mathrm{N}(j\theta) = i$. So $\{1, -1, i, -i\} \cong \mathcal{O}^*/\mathcal{O}^1$, and $\mathcal{O}^1$ is a normal subgroup of index 4 of $\mathcal{O}^*$. Its cosets can be obtained by multiplying for one of the coset leaders $\{1, \theta, j, \theta j\}$.

Our problem is then reduced to studying the subgroup $\mathcal{O}^1$. In particular, we need to find a *presentation* of this group: a set of generators S and a set of relations R among these generators. In fact, one can show that $\mathcal{O}^1$ is *finitely presentable*, that is it admits a presentation with S and R finite.

Example (Generators and relations in the case of the Golden Code). The group $\mathcal{O}^1$ is generated by 8 units, that are displayed in Table I.

The proof of the previous fact is omitted due to lack of space. The method for finding a presentation is rather complex and is based on the Swan algorithm [14, 2].

A. Action of the group on the hyperbolic space $\mathbb{H}^3$

The search algorithm is based on the action of the group on a suitable space. We use the fact that $\mathcal{O}^1$ is a subgroup of the special linear group $SL_2(\mathbb{C})$, and consider the action of $SL_2(\mathbb{C})$ on the hyperbolic 3-space $\mathbb{H}^3$ (see [4, 8]). We refer to the upper half-space model

$$\mathbb{H}^3 = \{(z, r) \mid z \in \mathbb{C},\ r \in \mathbb{R}, r > 0\} \tag{9}$$

endowed with the hyperbolic distance ρ such that if $P = (z, r)$, $P' = (z', r')$,

$$\cosh\rho(P, P') = 1 + \frac{|z - z'|^2 + (r - r')^2}{2rr'}$$

Given a matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{C})$, its action on a point $P = (z, r)$ is defined as follows:

$$M(z, r) = (z^*, r^*), \quad \text{with } \begin{cases} z^* = \frac{(az+b)(\bar{c}\bar{z}+\bar{d})+a\bar{c}r^2}{|cz+d|^2+|c|^2r^2}, \\ r^* = \frac{r}{|cz+d|^2+|c|^2r^2} \end{cases}$$

(Here we denote by $\bar{z}$ the complex conjugate of z).
The action of M and $-M$ is the same, so there is an induced action of $PSL_2(\mathbb{C}) = SL_2(\mathbb{C})/\{\mathbb{1}, -\mathbb{1}\}$. $PSL_2(\mathbb{C})$ can be identified with the group $\mathrm{Isom}^+(\mathbb{H}^3)$ of orientation-preserving isometries of $\mathbb{H}^3$ with respect to the metric we

defined previously ([4], Proposition 1.3).
Consider the action of $PSL_2(\mathbb{C})$ on the special point

$$J = (0, 1) \tag{10}$$

which has the following nice property ([4], Proposition 1.7):

$$\forall M \in SL_2(\mathbb{C}), \quad \|M\|_F^2 = 2\cosh\rho(J, M(J)) \tag{11}$$

As anticipated in Section III, given the normalized channel matrix $H_1 \in SL_2(\mathbb{C})$ we want to find

$$\hat{U} = \operatorname*{argmin}_{U\in\mathcal{O}^1} \left\|UH_1^{-1}\right\|_F^2 = \operatorname*{argmin}_{U\in\mathcal{O}^1} \cosh(\rho(J, UH_1^{-1}(J))) =$$
$$= \operatorname*{argmin}_{U\in\mathcal{O}^1} \rho(J, UH_1^{-1}(J)) = \operatorname*{argmin}_{U\in\mathcal{O}^1} \rho(U^{-1}(J), H_1^{-1}(J))$$

since U is an isometry.

Proposition 1. *There exists a constant $R_{\max} > 0$ such that $\forall H_1 \in SL_2(\mathbb{C})$, $\exists \hat{U} \in \mathcal{O}^1$ with $\rho(\hat{U}^{-1}(J), H_1^{-1}(J)) < R_{\max}$. Consequently, there exists a fixed constant $C_{\mathcal{O}}$ such that*

$$\left\|UH_1^{-1}\right\|_F^2 \leq C_{\mathcal{O}} \tag{12}$$

The proof of this Proposition is based on the existence of Dirichlet polyhedra for Kleinian groups (see [4, 2]). For the Golden Code, the methods of [2] allow to compute the constant $C_{\mathcal{O}}$ explicitly: $C_{\mathcal{O}} = 4.4720\cdots$.

B. The algorithm

Let $U_1, \ldots, U_r$ be a set of generators of $\mathcal{O}^1$, and $U_{r+1} = U_1^{-1}, \ldots, U_{2r} = U_r^{-1}$ their inverses. Suppose that the matrix form of the U_i has been stored in memory, together with the images $U_1(J), \ldots, U_{2r}(J)$ of J. Let

$$U_i(J) = (x_i, y_i, r_i), \quad i = 1, \ldots, 2r$$

INPUT: $H_1 \in SL_2(\mathbb{C})$.
Initialization: let $\overline{H} = H_1$, $\overline{U} = \mathbb{1}$, $i_0 = 0$.
REPEAT

1) *Compute* $\overline{H}^{-1}(J) = (x, y, r)$.
2) *Compute the distances*

$$d_i = 2\cosh\rho(\overline{H}^{-1}(J), \overline{U}_i(J)),$$
$$d_0 = 2\cosh\rho(\overline{H}^{-1}(J), J)$$

3) *Let* $i_0 = \operatorname{argmin}_{i\in\{0,1,\ldots,2r\}} d_i$. *(If several indices i attain the minimum, choose the smallest.)*
4) *Update* $\overline{U} \leftarrow \overline{U}U_{i_0}$, $\overline{H} \leftarrow \overline{H}U_{i_0}$.

UNTIL $i_0 = 0$.
OUTPUT: $\hat{U} = \overline{U}^{-1}$ *is the chosen unit.*

Remark 3. If the channel varies slowly from one time block to the next, the point $H_1^{-1}(J)$ will also vary little in time. Thus, this method requires only a slight adjustment of the previous search at each step. On the contrary, the LLL reduction method requires a full lattice reduction at each time block.

V. Performance of the algebraic reduction

A. Diversity

It has recently been proved [15] that MIMO decoding based on LLL reduction followed by zero-forcing achieves the receive diversity. The following Proposition shows that algebraic reduction is equivalent to LLL reduction in terms of diversity for the case of 2 transmit and 2 receive antennas:

Proposition 2. *The diversity order of the algebraic reduction method with ZF detection is* 2.

Proof: Suppose that the symbols s_i, $i = 1, \ldots, 4$ belong to an M-QAM constellation, with $M = 2^{2m}$. Let $\mathcal{E}_{\text{av}}$ be the average energy per symbol, and $\gamma = \frac{\mathcal{E}_{\text{av}}}{N_0}$ the SNR.
For a fixed realization of the channel matrix H, equation (6) is equivalent to an additive channel without fading where the noise $\mathbf{n}$ is no longer white.
With symbol by symbol ZF detection, $P_e(\gamma)$ is bounded by the error probability for each symbol. Using the classical expression of P_e in a Gaussian channel, for square QAM constellations ([10], §5.2.9), we obtain

$$P((\hat{\mathbf{s}}_\mathbf{1})_i \neq (\mathbf{s}_\mathbf{1})_i) \leq 4\,\text{erfc}\left(\sqrt{\frac{3\mathcal{E}_{\text{av}}}{\sigma^2(M-1)}}\right) \leq 4e^{-\frac{3\mathcal{E}_{\text{av}}}{2(M-1)\sigma_i^2}}$$

where σ_i^2 is the variance for complex dimension of the noise component n_i. Using the bound (8), we find

$$\sigma_i^2 \leq \text{tr}(\text{Cov}(\mathbf{n})) \leq \frac{CN_0}{|\det(H)|}$$

because $\left\|E^{-1}\right\|_F^2 = \left\|UH_1^{-1}\right\|_F^2 \leq C_{\mathcal{O}}$, see equation (12). Finally, we find

$$P_e(\gamma \mid H) \leq 16e^{-\left(\frac{3}{2(M-1)C}\right)|\det(H)|\frac{\mathcal{E}_{\text{av}}}{N_0}} = 16e^{-c|\det(H)|\gamma}$$

In order to compute $P_e(\gamma)$, we need the distribution of $|\det(H)|$. It is known [3] that the random variable $4\,|\det(H)|^2$ is distributed as the product of two independent chi square random variables $X \sim \chi^2(2)$,$Y \sim \chi^2(4)$. The cumulative distribution function of $Z = 2\,|\det(H)| = \sqrt{XY}$ is

$$F_Z(z) = P\{\sqrt{XY} \leq z\} = \iint_{\sqrt{xy}\leq z} \frac{1}{8} y e^{-\frac{x}{2}-\frac{y}{2}} dxdy$$

From the change of variables $u = y$, $v = \sqrt{xy}$, we obtain

$$F_Z(z) = \int_0^z \frac{v}{4}\left(\int_0^\infty e^{-\frac{v^2}{2u}-\frac{u}{2}} du\right) dv = \frac{z^2}{2}K_1(z)$$

where K_1 is the modified Bessel function of the second kind. Finally,

$$P_e(\gamma) \leq \mathbb{E}\left[16e^{-c'\gamma Z}\right] = 16\int_0^\infty \frac{z^2}{2}K_1(z)e^{-c'\gamma z}dz =$$
$$= 16\left(\frac{1}{(c'\gamma)^2} + \frac{2}{\pi(c'\gamma)^4}\sum_{k=0}^{\infty}\left(\frac{1}{(c'\gamma)^{2k}}\frac{\Gamma(k+\frac{5}{2})}{\Gamma(k+1)}\cdot\right.\right.$$
$$\left.\left.\cdot\left(\Psi\left(k+\frac{5}{2}\right) - \Psi(k+1) - 2\ln(c'\gamma)\right)\right)\right)$$

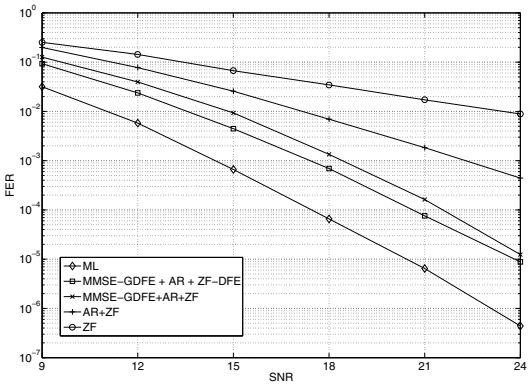

Figure 1. Performance of algebraic reduction followed by ZF or ZF-DFE decoders using 4-QAM constellations.

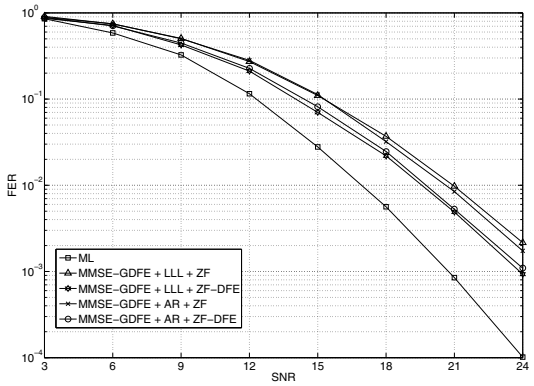

Figure 2. Comparison of algebraic reduction and LLL reduction using MMSE-GDFE preprocessing combined with ZF or ZF-DFE decoding with 16-QAM constellations.

where Ψ is the Digamma function. The series in the last expression being uniformly bounded for large γ, the leading term is of the order of $\frac{1}{\gamma^2}$. □

B. Simulation results

Figure 1 shows the performance of algebraic reduction followed by ZF and ZF-DFE decoding compared with ML decoding using 4-QAM constellations; the slope of the probability of error in the case of algebraic reduction with ZF detection (without preprocessing) is very close to -2, confirming the result of Proposition 2 concerning the diversity order.

One can add MMSE-GDFE left preprocessing to solve the shaping problem for finite constellations [7] in order to improve this performance. With MMSE-GDFE preprocessing, algebraic reduction is within $4.2\,\mathrm{dB}$ and $3.2\,\mathrm{dB}$ from the ML using ZF and ZF-DFE decoding, at the FER of 10^{-4}.

In the 16-QAM case, the loss is of $3.4\,\mathrm{dB}$ and $2.6\,\mathrm{dB}$ respectively for ZF and ZF-DFE decoding at the FER of 10^{-3} (Figure 2). In the same figure we compare algebraic reduction and LLL reduction. The two performances are very close; with ZF-DFE decoding, algebraic reduction has a slight loss ($0.3\,\mathrm{dB}$). On the contrary, with ZF decoding, algebraic reduction is slightly better ($0.4\,\mathrm{dB}$ gain), showing that the criterion (7) is indeed appropriate for this decoder.

Numerical simulations also evidence that the average complexity of algebraic reduction is low: in fact the average number of steps of the unit search algorithm is only 1.923.

VI. Conclusions

In this paper we have introduced a right preprocessing method for the decoding of space-time block codes based on quaternion algebras, which allows to improve the performance of suboptimal decoders and reduces the complexity of ML decoders.

The new method exploits the algebraic structure of the code, by approximating the channel matrix with a unit in the maximal order of the quaternion algebra. Our simulations show that algebraic reduction and LLL reduction have similar performance. Future work will deal with the generalization of algebraic reduction to higher-dimensional space time codes based on division algebras.

References

[1] J-C. Belfiore, G. Rekaya, E. Viterbo, "The Golden Code: a 2×2 full-rate Space-Time Code with non-vanishing determinants", *IEEE Trans. Inform. Theory*, vol 51 n.4, 2005

[2] C. Corrales, E. Jespers, G. Leal, A. del Rìo, "Presentations of the unit group of an order in a non-split quaternion algebra", *Advances in Mathematics*, 186 n. 2 (2004) 498–524

[3] A. Edelman, "Eigenvalues and condition numbers of random matrices", Ph.D. Thesis, MIT 1989

[4] J. Elstrodt, F. Grunewald, J. Mennicke, "Groups acting on Hyperbolic Space", Springer Monographs in Mathematics, 1998

[5] C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti, *On the densest MIMO lattices from cyclic division algebras*, submitted to *IEEE Trans. Inform. Theory*

[6] S. Lang, "Algebraic number theory", Springer-Verlag 2000

[7] A. D. Murugan, H. El Gamal, M. O. Damen, G. Caire, "A unified framework for tree search decoding: rediscovering the sequential decoder", *IEEE Trans. Inform. Theory*, vol 52 n. 3, 2006

[8] C. Maclachlan, A. W. Reid, "The arithmetic of hyperbolic 3-manifolds", Graduate texts in Mathematics, Springer, 2003

[9] J. Paredes, A.B. Gershman, M. Gharavi-Alkhansari, "A 2×2 space-time code with non-vanishing determinants and fast maximum likelihood decoding", ICASSP 2007

[10] J. Proakis, "Digital communications", McGraw-Hill 2001

[11] G. Rekaya, J-C. Belfiore, E. Viterbo, "A very efficient lattice reduction tool on fast fading channels", Proceedings of ISITA 2004, Parma, Italy

[12] B. A. Sethuraman, B. Sundar Rajan, V. Shashidar, "Full-diversity, high-rate space-time block codes from division algebras", *IEEE Trans. Inform. Theory*, vol 49 n. 10, 2003, pp. 2596–2616

[13] S. Sezginer, H. Sari, "Full-rate full-diversity 2×2 space-time codes of reduced decoder complexity", *IEEE Commun. Letters* vol 11 n. 12, 2007

[14] R. G. Swan, "Generators and relations for certain special linear groups", *Adv. Math.* 6, 1–77

[15] M. Taherzadeh, A. Mobasher, A. K. Khandani, "LLL reduction achieves the receive diversity in MIMO decoding", *IEEE Trans. Inform. Theory*, vol 53 n. 12, 2007, pp 4801–4805