INFORMATION LOSSLESS FULL-RATE FULL-DIVERSITY TRACE-ORTHOGONAL SPACE-TIME CODES

Antonio Fasano, Sergio Barbarossa

INFOCOM Dpt., University of Rome “La Sapienza”, Via Eudossiana 18, 00184 Rome, Italy
E-mail: `<fasano,sergio>@infocom.uniroma1.it`

ABSTRACT

Trace-orthogonality is an important property of linear space-time codes that has emerged relatively recently. In this work we propose a quite general procedure for the generation of such codes for any number of transmit antennas and uses of the channel. Simulations suggest that the use of rectangular encoding matrices, in place of square ones, could be beneficial to the coding gain. Moreover we are able to guarantee full-diversity of the proposed codes when information symbols are carved from the quadratic field $\mathbb{Q}(j)$. Since the components of any complex number can be approximated with arbitrary precision by rational numbers, our scheme could be used to guarantee full-diversity for any conceivable complex constellation.

1. INTRODUCTION

Multi-antenna Multi-Input Multi-Output (MIMO) systems have attracted a lot of research in the recent years because of their potential great increment of spectral efficiency over scattering–rich wireless channels [7]. A huge literature is by now available on space-time coding, as the basic tool to exploit the potentials of multi-antenna systems. The basic problem in the design of space-time coding systems is how to strike the best balance between three fundamental issues: i) performance, typically expressed in terms of bit error rate (BER) or, more appropriately for fading channels, average BER or out of service probability; ii) capacity, and iii) receiver complexity. Orthogonal space-time block coding [8] is an example of method capable to collect the full diversity gain, using a very simple scalar decoder, but it is not optimal from the point of view of capacity [9]. On the contrary, Vertical-BLAST methods [10] guarantee full rate, but at the expenses of diversity gain or complexity. Hassibi and Hochwald in [11] proposed a rather general method to design linear dispersion (LD) codes, where the transmitted symbols are dispersed over space and time through spreading matrices that are built in order to maximize the ergodic capacity of the MIMO system. In the effort of designing codes that are guaranteed to have good performance in terms of *both* rate and BER, Ma and Giannakis in [12] and El Gamal and Damen in [13] provided general methods for building codes capable of being information lossless while guaranteeing, at the same time, full-diversity. An important property of linear space-time encoders that emerged relatively recently, is *trace-orthogonality* [14], [15], [16], [17], [18] that is the property of a linear space-time code to have encoding matrices orthogonal with respect to the trace inner product between matrices. Trace-orthogonality is the key property for lossless information transfer, and together with the additional property (5), that we refer to as *unitarity*, comes in useful to find suboptimal methods to achieve a good balance between rate, BER and complexity [15], [18]. We will refer to a space-time code having both the properties of trace-orthogonality and unitarity as a *Unitary Trace-Orthogonal Design* (UTOD). It is worth of interest to devise systematic procedures for the construction of UTODs which are able to guarantee full-diversity [18]. In this regard, the schemes currently known are affected by some drawbacks: the procedure proposed in [12] is able to generate codes only with square encoding matrices; the scheme in [18] extends the construction to rectangular matrices but constraining the number of columns (corresponding to the channel uses) to be a multiple of the number of transmit antennas. Moreover, both schemes are able to guarantee full-diversity if information symbols are carved from the ring of Gaussian Integers $\mathbb{Z}[j] = \{z \in \mathbb{C} | z = a + bj,\ a, b \in \mathbb{Z}\}$, with $j = \sqrt{-1}$, thus limiting the practical implementation to the use of QAM constellations.

In this work we propose a systematic procedure for the generation of UTODs for *any number* of transmit antennas and uses of the channel, i.e. with rectangular encoding matrices with unconstrained dimensions[1]. This is useful, besides the considerations in [18], since augmenting the number of columns of the encoding matrices we may potentially increase the coding gain of the UTOD, as the simulations suggest. Moreover we are able to guarantee full-diversity when information symbols are carved from the quadratic field $\mathbb{Q}(j) = \{z \in \mathbb{C} | z = a + bj,\ a, b \in \mathbb{Q}\} \subset \mathbb{Z}[j]$. This is extremely useful from a practical point of view, in fact, as the components of any complex number can be approximated with arbitrary precision by rational numbers, the proposed scheme could be used to guarantee full-diversity for any conceivable complex constellation.

The paper is organized as follows. The system model is outlined in Section 2 where a formal definition of UTOD is provided. In Section 3 we give the necessary and sufficient condition for the existence of UTODs and propose a procedure for its generation. In Section 4 we give the conditions guaranteeing full-diversity and in Section 5 we provide some practical examples of design. Section 6 follows with numerical simulations and some conclusive remarks.

2. SYSTEM MODEL

Consider a flat fading MIMO system with n_T transmit and n_R receive antennas. After matched filtering and symbol-rate sampling, the input-output relation can be written as

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{v}, \tag{1}$$

where $\boldsymbol{H} \in \mathbb{C}^{n_R \times n_T}$ is the channel matrix, $\boldsymbol{x} \in \mathbb{C}^{n_T}$ is the vector of transmitted symbols and $\boldsymbol{v} \in \mathbb{C}^{n_R}$ is the noise vector. Assuming the channel constant over Q consecutive channel uses (quasi-static fading), stacking the transmitted vectors and the received ones in

---

This work has been supported by the project IST-4-027187-STP-SURFACE funded by the European Union.

[1] Apart from the constraint that guarantees UTODs existence.

matrices, we obtain the following relation

$$\boldsymbol{Y} = \boldsymbol{H}\boldsymbol{X} + \boldsymbol{V}, \tag{2}$$

where $\boldsymbol{V}$ is the $n_R \times Q$ received noise matrix, and $\boldsymbol{X}$ is the space-time $n_T \times Q$ code matrix. We assume that information symbols are encoded into $\boldsymbol{X}$ using a full-rate *Unitary Trace-Orthogonal Design* (UTOD) [15]. That is a vector of $n_s = n_T Q$ (full-rate condition) complex symbols $\boldsymbol{s} = (s_1\ s_2\ \cdots\ s_{n_s})^T$ is mapped onto the code matrix $\boldsymbol{X}$ according to the rule

$$\boldsymbol{X} = \sum_{k=1}^{n_s} \boldsymbol{A}_k s_k \tag{3}$$

where the encoding matrices $\boldsymbol{A}_k$ $(k = 1, \ldots, n_s)$ satisfy the following relations which define a Unitary Trace-Orthogonal Design:

$$\operatorname{tr}\left(\boldsymbol{A}_k^H \boldsymbol{A}_j\right) = \delta_{jk}, \qquad k, j \in \{1, \cdots, n_s\}, \tag{4}$$

where δ_{jk} denotes the Kronecker delta, and

$$\boldsymbol{A}_i \boldsymbol{A}_i^H = \frac{1}{n_T} \boldsymbol{I}_{n_T}, \qquad i \in \{1, \cdots, n_s\}, \tag{5}$$

where $\boldsymbol{I}_n$ denotes the $n \times n$ identity matrix. In [15], and [16] it was proven that (4) is a necessary and sufficient condition for lossless information transmission and (5) is a necessary and sufficient condition, for the decoder composed by the cascade of the linear MMSE estimator followed by hard decision, to achieve minimum BER.

3. UNITARY TRACE-ORTHOGONAL DESIGN SYNTHESIS

In this section we give a necessary and sufficient condition for the existence of UTODs and provide a systematic procedure for generating a large class of such encoding matrices.

Before proceeding, we start recalling the notion of *Latin rectangle*. A $k \times n$ *Latin rectangle* is a $k \times n$ matrix[2] $\boldsymbol{L}_{k\times n}$ in which each of the numbers $1, 2, \ldots, n$ occurs exactly once in each row and at most once in each column. When $k = n$, the special case of *Latin square* results. For each size, there are many different ways to generate a Latin rectangle. As an example a 3×4 Latin rectangle can be built as $\boldsymbol{L}_{3\times 4}(i, j) = (j - i) \bmod 4 + 1$, for $i = 1, \ldots, 3$, and $j = 1, \ldots, 4$, and results in the following array

$$\boldsymbol{L}_{3\times 4} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}. \tag{6}$$

It is useful to remark that in a Latin rectangle any two columns have the elements with the same row index different. This property will be exploited in the construction of the coding matrices.

Now, let us consider the problem of existence for UTODs which is answered by the following theorem

Theorem 1. *A Unitary Trace-Orthogonal Design with encoding matrices $\boldsymbol{A}_k$ $(k = 1, \ldots, Q \cdot n_T)$ having dimensions $n_T \times Q$ exists* if and only if $Q \geq n_T$.

Proof. Necessity stems from the fact that for a UTOD, encoding matrices satisfy

$$\boldsymbol{A}_k \boldsymbol{A}_k^H = \frac{1}{n_T} \boldsymbol{I}_{n_T}, \quad k = 1, \ldots, Q \cdot n_T, \tag{7}$$

which can hold true only if $Q \geq n_T$. Sufficiency is a consequence of the existence of a procedure for generating matrices $\boldsymbol{A}_k$ when $Q \geq n_T$. Such a procedure is described below. □

For the sake of clarity, it is useful to refer to the encoding matrices by means of a two-index notation $\boldsymbol{\mathcal{A}}_{i,j}$, with $i = 1, \ldots, n_T$, and $j = 1, \ldots, Q$. The link with the notation $\boldsymbol{A}_k$, with $k = 1, \ldots, Qn_T$, used so far, is settled by the following relation

$$\boldsymbol{A}_{(i-1)\cdot Q + j} = \boldsymbol{\mathcal{A}}_{i,j}, \tag{8}$$

where $i \in \{1, 2, \ldots, n_T\}$, and $j \in \{1, 2, \ldots, Q\}$.

Synthesis of UTOD encoding matrices with size $n_T \times Q$ $(Q \geq n_T)$

1. Generate an $n_T \times Q$ Latin rectangle $\boldsymbol{L}_{n_T \times Q}$.
2. Build the Q matrices $\boldsymbol{S}_k$ $(k = 1, \ldots, Q)$ with size $n_T \times Q$ according to the rule

$$\begin{cases} \boldsymbol{S}_k(i, j) = \boldsymbol{I}_Q(\boldsymbol{L}_{n_T\times Q}(i, k), j) \\ i = 1, \ldots, n_T, \quad j = 1, \ldots, Q. \end{cases} \tag{9}$$

   In words, $\boldsymbol{S}_k$ is built[3] collecting the n_T rows of $\boldsymbol{I}_Q$ with indices belonging to the k-th column of the Latin rectangle.
3. Generate Q unitary matrices[4] $\boldsymbol{W}^{(k)}$ $(k = 1, \ldots, Q)$ with size $n_T \times n_T$, having constant modulus[5] elements, and denote by $\boldsymbol{w}_j^{(k)}$ $(j = 1, \ldots, n_T)$ the j-th column of $\boldsymbol{W}^{(k)}$.
4. Generate an $n_T \times n_T$ unitary matrix $\boldsymbol{U}$.
5. Generate a $Q \times Q$ unitary matrix $\boldsymbol{R}$.
6. Synthesize encoding matrices $\boldsymbol{\mathcal{A}}_{j,k}$, for $j = 1, \ldots, n_T$ and $k = 1, \ldots, Q$, according to the rule

$$\boldsymbol{\mathcal{A}}_{j,k} = \boldsymbol{U} \operatorname{diag}\{\boldsymbol{w}_j^{(k)}\} \boldsymbol{S}_k \boldsymbol{R}, \tag{10}$$

   where $\operatorname{diag}\{\boldsymbol{w}_j^{(k)}\}$ denotes the diagonal matrix whose diagonal elements are the components of $\boldsymbol{w}_j^{(k)}$. If $Q = n_T$, the encoding matrices can be synthesized also according to the rule

$$\boldsymbol{\mathcal{A}}_{j,k} = \boldsymbol{U} \boldsymbol{S}_k \operatorname{diag}\{\boldsymbol{w}_j^{(k)}\} \boldsymbol{R}. \tag{11}$$

To prove that this procedure generates a Unitary Trace-Orthogonal Design, it is useful to remark some properties of matrix $\boldsymbol{S}_k$, introduced in (9). More precisely we have:

1. $\boldsymbol{S}_k \boldsymbol{S}_k^H = \boldsymbol{I}_{n_T}$;
2. $\boldsymbol{S}_k \boldsymbol{S}_j^H$, with $k \neq j$, has all entries on the main diagonal equal to zero. When $Q = n_T$, the same holds true for $\boldsymbol{S}_k^H \boldsymbol{S}_j$.

We are now ready to prove that (10) and (11) constitute Unitary Trace-Orthogonal Designs. For the sake of simplicity, in the subsequent proof we make explicit reference to (10) only. Following similar arguments, we can prove the same results for (11).
Let us start showing that $\boldsymbol{\mathcal{A}}_{j,k}$ in (10) satisfies (7):

$$\begin{aligned} \boldsymbol{\mathcal{A}}_{j,k} \boldsymbol{\mathcal{A}}_{j,k}^H &= \boldsymbol{U} \operatorname{diag}\{\boldsymbol{w}_j^{(k)}\} \boldsymbol{S}_k \boldsymbol{R} \boldsymbol{R}^H \boldsymbol{S}_k^H \operatorname{diag}\{\boldsymbol{w}_j^{(k)}\}^H \boldsymbol{U}^H \\ &= \boldsymbol{U} \operatorname{diag}\{\boldsymbol{w}_j^{(k)}\} \operatorname{diag}\{\boldsymbol{w}_j^{(k)}\}^H \boldsymbol{U}^H = \frac{1}{n_T} \boldsymbol{I}_{n_T}, \end{aligned} \tag{12}$$

since $\operatorname{diag}\{\boldsymbol{w}_j^{(k)}\} \operatorname{diag}\{\boldsymbol{w}_j^{(k)}\}^H = \frac{1}{n_T} \boldsymbol{I}_{n_T}$.
To prove orthonormality, we consider the following cases for the indices of matrices $\boldsymbol{\mathcal{A}}_{j_1,k_1}$ and $\boldsymbol{\mathcal{A}}_{j_2,k_2}$:

---

[2] $k \leq n$ is assumed.

[3] Using Matlab notation for indices, $\boldsymbol{S}_k = \boldsymbol{I}_Q(\boldsymbol{L}_{n_T\times Q}(:, k), :)$.

[4] We may choose $\boldsymbol{W}^{(1)} = \boldsymbol{W}^{(2)} = \cdots = \boldsymbol{W}^{(Q)}$.

[5] The modulus must necessarily be $\sqrt{1/n_T}$.

- $k_1 \neq k_2$. In this case

  $$\begin{aligned}&\mathrm{tr}\left(\boldsymbol{\mathcal{A}}_{j_1,k_1}\boldsymbol{\mathcal{A}}^H_{j_2,k_2}\right)\\&\quad= \mathrm{tr}\left(\mathrm{diag}\{\boldsymbol{w}^{(k_1)}_{j_1}\}\boldsymbol{S}_{k_1}\boldsymbol{S}^H_{k_2}\,\mathrm{diag}\{\boldsymbol{w}^{(k_2)}_{j_2}\}^H\right) = 0\,,\end{aligned}$$

  since $\boldsymbol{S}_{k_1}\boldsymbol{S}^H_{k_2}$ with $k_1 \neq k_2$ is a matrix with zero diagonal elements and the multiplication by any other diagonal matrix does not change this characteristic.

- $k_1 = k_2$ and $j_1 \neq j_2$. In this case $\boldsymbol{S}_{k_1}\boldsymbol{S}^H_{k_2} = \boldsymbol{I}_{n_T}$ and thus

  $$\begin{aligned}\mathrm{tr}\left(\boldsymbol{\mathcal{A}}_{j_1,k_1}\boldsymbol{\mathcal{A}}^H_{j_2,k_2}\right) &= \mathrm{tr}\left(\mathrm{diag}\{\boldsymbol{w}^{(k_1)}_{j_1}\}\,\mathrm{diag}\{\boldsymbol{w}^{(k_1)}_{j_2}\}^H\right)\\&= \left[\boldsymbol{w}^{(k_1)}_{j_2}\right]^H\left[\boldsymbol{w}^{(k_1)}_{j_1}\right] = 0\,,\end{aligned}$$

  since for $k_1 = k_2$ distinct columns of $\boldsymbol{W}^{(k_1)} = \boldsymbol{W}^{(k_2)}$ are orthogonal.

- $k_1 = k_2$ and $j_1 = j_2$. In this case from (12) it follows

  $$\mathrm{tr}\left(\boldsymbol{\mathcal{A}}_{j_1,k_1}\boldsymbol{\mathcal{A}}^H_{j_2,k_2}\right) = 1\,.$$

The proposed procedure is quite general and allows the generation of a large class of UTODs due to the degrees of freedom we have in choosing the design matrices $\boldsymbol{R}$, $\boldsymbol{W}^{(k)}$ ($k = 1, \ldots, Q$), $\boldsymbol{U}$, and Latin rectangle $\boldsymbol{L}_{n_T\times Q}$. This generality is extremely useful for optimization purposes. It is worthwhile noting that (10) and (11) subsume, as special cases, previously known information lossless space-time codes. In particular, when $Q = n_T$, setting $\boldsymbol{U} = \boldsymbol{R} = \boldsymbol{I}_{n_T}$ in (11), we obtain the *shift and multiply bases*[6], proposed in [14]. Moreover, the *full-diversity full-rate* (FDFR) complex-field space-time codes proposed in [12] belong to the class of UTODs. In fact, using the complex parameter β and the unitary matrix $\boldsymbol{\Theta}$, both defined in [12, eq. (8)], FDFR coding matrices can be generated through (11) setting $Q = n_T$, $\boldsymbol{L}_{n_T\times n_T}(i,j) = (i-j) \bmod n_T + 1$ with $i, j \in \{1, \ldots, n_T\}$, $\boldsymbol{U} = \boldsymbol{R} = \boldsymbol{I}_{n_T}$, and $\boldsymbol{W}^{(k)} = \beta^{k-1}\boldsymbol{\Theta}$. This result is important since it demonstrates that it is possible to achieve *full-diversity* using a Unitary Trace-Orthogonal Design, at least for square encoding matrices. Actually, UTOD allows for full-diversity, *for any number* of transmit antennas n_T and channel uses Q, as the results of the next section demonstrate. Moreover, within this context, it is noteworthy to put in evidence the tight connection between codes generated through our procedure, though slightly modified, and threaded space time coding [13]. In fact, looking at step (3), we may relax the requirements for matrices $\boldsymbol{W}^{(k)}$, giving up the constraint on constant modulus entries. The coding matrices generated in such a case constitute a Trace-Orthogonal Design[7] since (12) fails short. However, in this case, they provide us with the ability of generating information lossless Threaded Algebraic Space-Time (TAST) codes [13]. In fact, with reference to the complex parameter ϕ_k and the unitary matrix $\boldsymbol{M}_k$, both defined in [13, eq. (5)], we get symmetric TAST codes setting $Q = n_T$, $\boldsymbol{L}_{n_T\times n_T}(i,j) = (i-j) \bmod n_T + 1$ with $i, j \in \{1, \ldots, n_T\}$, $\boldsymbol{U} = \boldsymbol{R} = \boldsymbol{I}_{n_T}$, and $\boldsymbol{W}^{(k)} = \phi_k\boldsymbol{M}_k$. It is worthwhile noting that the threaded structure of the code is guaranteed by matrices $\boldsymbol{S}_k$ $(k = 1, \ldots, Q)$ at step (2) of the procedure. These last, in turn, depend on the current choice of Latin rectangle $\boldsymbol{L}_{Q\times n_T}$, which actually settles the threads.

4. FULL-DIVERSITY UNITARY TRACE-ORTHOGONAL DESIGN

A Unitary Trace-Orthogonal Design can guarantee full-diversity, if it is generated according to the following theorem.

Theorem 2. *Assume that information symbols are carved from* $\mathbb{Q}(j)$*, and for any Latin rectangle* $\boldsymbol{L}_{n_T\times Q}$*, consider a full-rate Unitary Trace-Orthogonal Design with the following positions in formula (10):*

$$\begin{aligned}&\boldsymbol{U} \textit{ is any } n_T \times n_T \textit{ unitary matrix}\,,\\&\boldsymbol{R} \textit{ is any } Q \times Q \textit{ unitary matrix}\,,\\&\boldsymbol{W}^{(k)} = e^{j\theta_k}\boldsymbol{F}\,\mathrm{diag}\{1, \omega, \ldots, \omega^{n_T-1}\} \quad (k = 1, \ldots, Q)\,,\end{aligned} \tag{13}$$

where $\boldsymbol{F}$ *is the IDFT matrix of order* n_T*, i.e., for* $h, l \in \{1, \cdots, n_T\}$ $\boldsymbol{F}(h,l) = \frac{1}{\sqrt{n_T}}\,e^{\frac{j(h-1)(l-1)2\pi}{n_T}}$. *Then, it is a full-diversity Unitary Trace-Orthogonal Design if* ω *has unit modulus and is algebraic of degree at least* n_T *over the field*[8] $\mathbb{Q}(j, e^{j\frac{2\pi}{n_T}})$*, and* $\theta_1, \ldots, \theta_Q$ *are real algebraic numbers linearly independent*[9] *over the rationals.*

Proof. Since $|\omega| = 1$ and $\theta_k \in \mathbb{R}$, $\boldsymbol{W}^{(k)}$ is a unitary matrix with constant modulus entries. Thus the proposed scheme is a Unitary Trace-Orthogonal Design. So, let us prove the full-diversity property. According to the rank criterion [8], ML decoding achieve maximum diversity if the error matrix $\boldsymbol{\Xi}(\boldsymbol{s}', \boldsymbol{s}'') = \boldsymbol{X}(\boldsymbol{s}') - \boldsymbol{X}(\boldsymbol{s}'')$ corresponding two any pair of different encoded symbols vectors $\boldsymbol{s}'$ and $\boldsymbol{s}''$, has full-rank. Let us build such a matrix taking into account the assumptions of Theorem 2 and using a two-index notation both for the encoding matrices $\boldsymbol{\mathcal{A}}_{j,k}$ and the information symbols $s'_{j,k}$, and $s''_{j,k}$, where $j \in \{1, \ldots, n_T\}$ and $k \in \{1, \ldots, Q\}$ since we assume full-rate design. Denote by $z_{j,k} = s'_{j,k} - s''_{j,k}$, $\boldsymbol{z}_k = [z_{1,k} \cdots z_{n_T,k}]^T$, and $\boldsymbol{z} = [\boldsymbol{z}_1^T \cdots \boldsymbol{z}_Q^T]^T$. Note that $z_{j,k} \in \mathbb{Q}(j)$, since the symbols are carved from $\mathbb{Q}(j)$. We have

$$\begin{aligned}\operatorname*{rank}_{\boldsymbol{s}'\neq\boldsymbol{s}''}\left(\boldsymbol{\Xi}(\boldsymbol{s}', \boldsymbol{s}'')\right) &= \operatorname*{rank}_{\boldsymbol{z}\neq\boldsymbol{0}}\left(\boldsymbol{U}\left[\sum_{k=1}^{Q}\sum_{j=1}^{n_T}\mathrm{diag}\{\boldsymbol{w}^{(k)}_j\}\boldsymbol{S}_k z_{j,k}\right]\boldsymbol{R}\right)\\&= \operatorname*{rank}_{\boldsymbol{z}\neq\boldsymbol{0}}\left(\sum_{k=1}^{Q}\mathrm{diag}\left\{\sum_{j=1}^{n_T}\boldsymbol{w}^{(k)}_j z_{j,k}\right\}\boldsymbol{S}_k\right)\\&= \operatorname*{rank}_{\boldsymbol{z}\neq\boldsymbol{0}}\left(\sum_{k=1}^{Q}\mathrm{diag}\left\{\boldsymbol{W}^{(k)}\boldsymbol{z}_k\right\}\boldsymbol{S}_k\right)\,.\end{aligned} \tag{14}$$

Note that since the multiplication by unitary matrices does not alter the rank it is proved that diversity is not affected by the choice of $\boldsymbol{U}$ and $\boldsymbol{R}$. Now, using (13) we get

$$\boldsymbol{W}^{(k)}\boldsymbol{z}_k = e^{j\theta_k}\boldsymbol{F}\,\mathrm{diag}\{1, \omega, \ldots, \omega^{n_T-1}\}\boldsymbol{z}_k = e^{j\theta_k}\boldsymbol{c}_k\,, \tag{15}$$

with $\boldsymbol{c}_k = \boldsymbol{F}\,\mathrm{diag}\{1, \omega, \ldots, \omega^{n_T-1}\}\boldsymbol{z}_k$. Denoting by $\boldsymbol{c}_k(l)$ and $\boldsymbol{z}_k(l)$ the l-th component of vectors $\boldsymbol{c}_k$ and $\boldsymbol{z}_k$ respectively, (15)

---

[6] They have many traits in common with layered space-time coding.

[7] That is only (4) holds.

[8] $\mathbb{Q}(\gamma_1, \gamma_2, \ldots, \gamma_n)$ is the smallest field containing $\mathbb{Q}$ and the numbers $\gamma_1, \gamma_2, \ldots, \gamma_n$.

[9] Complex numbers $z_1, \ldots, z_Q$ are linearly independent over the rationals if $\sum_{k=1}^{Q}\alpha_k z_k = 0 \iff \alpha_1 = \cdots = \alpha_Q = 0$, when $\alpha_1, \ldots, \alpha_Q \in \mathbb{Q}$. Note that independence over rationals is equivalent to independence over integers, where $\mathbb{Z}$ is substituted to $\mathbb{Q}$, in the former definition.

implies

$$\boldsymbol{c}_k(l) = \frac{1}{\sqrt{n_T}} \sum_{r=1}^{n_T} e^{\frac{j2\pi(l-1)(r-1)}{n_T}} \boldsymbol{z}_k(r)\omega^{r-1}\,, \quad (l = 1, \ldots, n_T). \tag{16}$$

Because of the hypotheses, $e^{\frac{j2\pi(l-1)(r-1)}{n_T}} \boldsymbol{z}_k(r) \in \mathbb{Q}(j, e^{\frac{j2\pi}{n_T}})$, and since ω is algebraic over $\mathbb{Q}(j, e^{\frac{j2\pi}{n_T}})$ with degree at least n_T, the sum[10] in (16) is zero if and only if $\boldsymbol{z}_k = \boldsymbol{0}$. This means that $\boldsymbol{c}_k$ has all entries different from zero if and only if $\boldsymbol{z}_k$ has at least one non-null component, that is

$$\boldsymbol{z}_k \neq \boldsymbol{0} \quad \Longleftrightarrow \quad \prod_{l=1}^{n_T} \boldsymbol{c}_k(l) \neq 0\,. \tag{17}$$

Moreover, it is evident from (16) that $\boldsymbol{c}_k(l)$ is an algebraic number. Substituting (15) in (14), we get, eventually

$$\operatorname*{rank}_{\boldsymbol{s}' \neq \boldsymbol{s}''} \left(\boldsymbol{\Xi}(\boldsymbol{s}', \boldsymbol{s}'')\right) = \operatorname*{rank}_{\boldsymbol{z} \neq \boldsymbol{0}} \left(\sum_{k=1}^{Q} e^{j\theta_k} \operatorname{diag}\{\boldsymbol{c}_k\} \boldsymbol{S}_k \right). \tag{18}$$

The condition $\boldsymbol{z} \neq \boldsymbol{0}$ is equivalent to say that there exists at least one index $\tilde{k}$ ($1 \leq \tilde{k} \leq Q$), for which $\boldsymbol{z}_{\tilde{k}} \neq \boldsymbol{0}$. This implies, according to (17), that for the same index we have $\prod_{l=1}^{n_T} \boldsymbol{c}_{\tilde{k}}(l) \neq 0$, which comes in useful in proving that $\boldsymbol{\Xi}(\boldsymbol{s}', \boldsymbol{s}'')$ in (18) is full-rank. To this end, let us consider the $n_T \times n_T$ submatrix $\boldsymbol{M}(\boldsymbol{c}_{\tilde{k}})$ of $\boldsymbol{\Xi}(\boldsymbol{s}', \boldsymbol{s}'')$ gathering the elements of $\boldsymbol{c}_{\tilde{k}}$. Note that the entries of $\boldsymbol{c}_{\tilde{k}}$ span exactly n_T rows and n_T columns[11], so their indices univocally single out $\boldsymbol{M}(\boldsymbol{c}_{\tilde{k}})$. The submatrix $\boldsymbol{M}(\boldsymbol{c}_{\tilde{k}})$ has the important property that it is full-rank. To prove this statement, let us develop the determinant

$$|\boldsymbol{M}(\boldsymbol{c}_{\tilde{k}})| = \sum_{k_1 \cdots k_{n_T}} \operatorname{sgn}[k_1, \cdots, k_{n_T}] \prod_{l=1}^{n_T} \boldsymbol{c}_{i_{k_l}}(l) e^{j\theta_{i_{k_l}}}\,, \tag{19}$$

where the sum runs over all permutations of the sequence $(1, \ldots, n_T)$, $\operatorname{sgn}[k_1, \cdots, k_{n_T}] \in \{1, -1\}$ is the sign of a permutation [1], and index $i_{k_l} \in \{1, 2, \cdots, Q\}$, with current value depending on the submatrix $\boldsymbol{M}(\boldsymbol{c}_{\tilde{k}})$. Regardless of the values of i_{k_l}, (19) is a linear combination with algebraic coefficients of exponentials of the form $e^{[j \sum_{l=1}^{n_T} \theta_{i_{k_l}}]}$, where each exponent $[j \sum_{l=1}^{n_T} \theta_{i_{k_l}}]$ is an algebraic number. Resorting to Lindemann's theorem [3] we can prove that $|\boldsymbol{M}(\boldsymbol{c}_{\tilde{k}})| \neq 0$ if we are able to show that (19), after collecting[12] equal exponentials, has at least one non-null term. Actually this is the case, in fact $\boldsymbol{M}(\boldsymbol{c}_{\tilde{k}})$ has been chosen to gather all the components of $\boldsymbol{c}_{\tilde{k}}$ and, as a consequence, sum in (19) has to contain the term

$$\pm \left(\prod_{l=1}^{n_T} \boldsymbol{c}_{\tilde{k}}(l) \right) e^{jn_T\theta_{\tilde{k}}}\,, \tag{20}$$

where sign depends on $\boldsymbol{M}(\boldsymbol{c}_{\tilde{k}})$. We observe that (20) is non-null, since $\prod_{l=1}^{n_T} \boldsymbol{c}_{\tilde{k}}(l) \neq 0$, and moreover it is the only term in (19) which contains the exponential $e^{jn_T\theta_{\tilde{k}}}$. This is a consequence of the hypothesis on linear independence over rationals of $\theta_1, \cdots, \theta_Q$, which implies that

$$n_T\theta_{\tilde{k}} = \sum_{l=1}^{n_T} \theta_{i_{k_l}} \iff \theta_{i_{k_l}} = \theta_{\tilde{k}} \tag{21}$$

regardless of the values of $i_{k_l} \in \{1, 2, \cdots, Q\}$. This is sufficient to guarantee that $|\boldsymbol{M}(\boldsymbol{c}_{\tilde{k}})| \neq 0$. This proves that for any choice of error vector $\boldsymbol{z} \neq \boldsymbol{0}$, i.e. any choice of symbol vectors $\boldsymbol{s}' \neq \boldsymbol{s}''$, there exists an $n_T \times n_T$ minor of error matrix $\boldsymbol{\Xi}(\boldsymbol{s}', \boldsymbol{s}'')$ which is non-null, that is $\boldsymbol{\Xi}(\boldsymbol{s}', \boldsymbol{s}'')$ has full-rank. The proof is complete. ☐

It is worthwhile noting that the result of Theorem 2 can be greatly strengthened. It is possible to prove [19] that choosing ω carefully, UTOD can guarantee full-diversity when information symbols are carved from the field of *algebraic numbers*. As a consequence full-diversity can be guaranteed for any practical complex constellation.

5. DESIGN EXAMPLES

We show now examples of application of the scheme proposed in Theorem 2. Since the choice of Latin rectangle $\boldsymbol{L}_{n_T \times Q}$, and unitary matrices $\boldsymbol{U}$ and $\boldsymbol{R}$ does not affect the diversity, we concentrate on settling ω, and θ_1, θ_2, $\cdots$, θ_Q. In the sequel we use the following notation: $[\mathbb{F} : \mathbb{K}]$ denotes the degree of the extension field $\mathbb{F}/\mathbb{K}$; $\phi(n)$ is the Euler's totient function; $\operatorname{lcm}(n_1, n_2, \cdots, n_M)$ is the least common multiple of $n_1, n_2, \cdots, n_M$. We assume that the reader is familiar with the basic definitions in algebraic number theory, which can be found, for example, in [2].

5.1. The determination of w

A possible choice is:

$$w = e^{j\frac{2\pi}{K}}\,, \quad \text{with } K \textit{ any prime number greater than } n_T. \tag{22}$$

In fact, according to Theorem 2, ω has to be unit modulus and algebraic of degree at least n_T over the field $\mathbb{Q}(j, e^{j\frac{2\pi}{n_T}})$. The last condition is equivalent to require

$$[\mathbb{Q}(j, e^{j\frac{2\pi}{n_T}}, \omega) : \mathbb{Q}(j, e^{j\frac{2\pi}{n_T}})] \geq n_T. \tag{23}$$

Choosing $\omega = e^{j\frac{2\pi}{K}}$, K is to be determined in order to satisfy (23). To this end we exploit the relation among the degrees of successive field extensions

$$\begin{aligned} &[\mathbb{Q}(j, e^{j\frac{2\pi}{n_T}}, e^{j\frac{2\pi}{K}}) : \mathbb{Q}] \\ &\quad = [\mathbb{Q}(j, e^{j\frac{2\pi}{n_T}}, e^{j\frac{2\pi}{K}}) : \mathbb{Q}(j, e^{j\frac{2\pi}{n_T}})] \cdot [\mathbb{Q}(j, e^{j\frac{2\pi}{n_T}}) : \mathbb{Q}], \end{aligned} \tag{24}$$

which is equivalent to

$$\begin{aligned} &\phi\left(\operatorname{lcm}(4, n_T, K)\right) \\ &\quad = [\mathbb{Q}(j, e^{j\frac{2\pi}{n_T}}, e^{j\frac{2\pi}{K}}) : \mathbb{Q}(j, e^{j\frac{2\pi}{n_T}})] \cdot \phi\left(\operatorname{lcm}(4, n_T)\right), \end{aligned} \tag{25}$$

since $\mathbb{Q}(j, e^{j\frac{2\pi}{n_T}}, e^{j\frac{2\pi}{K}})$ and $\mathbb{Q}(j, e^{j\frac{2\pi}{n_T}})$ are cyclotomic extensions of $\mathbb{Q}$, whose degree is a known function of $\phi(\cdot)$ [4]. Using (25), relation (23) is satisfied if K is such that

$$\frac{\phi\left(\operatorname{lcm}(4, n_T, K)\right)}{\phi\left(\operatorname{lcm}(4, n_T)\right)} \geq n_T\,. \tag{26}$$

---

[10] Note that (16) is a polynomial of degree at most $n_T - 1$ in ω with coefficients in $\mathbb{Q}(j, e^{\frac{j2\pi}{n_T}})$.

[11] This is due to the fact that $\boldsymbol{S}_k$ has only n_T non-null entries which are equal to 1 and span n_T rows and n_T columns. Moreover $\sum_{k=1}^{Q} \boldsymbol{S}_k$ is a matrix of all ones.

[12] Note that collected coefficients are again algebraic numbers.

Noteworthy, inequality (26) is satisfied if K is taken to be *any prime number greater than* n_T. Let us prove this claim for[13] $n_T \geq 2$. If K is prime and greater than n_T, then it is coprime[14] to $\mathrm{lcm}(4, n_T)$. As a consequence the numerator of (26) can be written as

$$\begin{aligned} \phi\left(\mathrm{lcm}(4, n_T, K)\right) &= \phi\left(K \cdot \mathrm{lcm}(4, n_T)\right) \\ &= \phi(K) \cdot \phi(\mathrm{lcm}(4, n_T)) = (K-1) \cdot \phi(\mathrm{lcm}(4, n_T)), \quad (27) \end{aligned}$$

where the properties of $\phi(\cdot)$ have been exploited. Substituting (27) in (26) the resulting inequality is always satisfied since $K > n_T$, and (22) is proven.

5.2. The determination of $\theta_1, \theta_2, \ldots, \theta_Q$

Among several viable alternatives, a possible choice is:

$$\theta_k = \beta^{k-1}, \qquad k = 1, \ldots, Q, \tag{28}$$

where β is any real algebraic number of degree at least Q. In such a case, in fact, the first $Q-1$ powers of β are linear independent over the rationals. For example, we may choose $\beta = \sqrt[Q]{p}$, where p is any prime number. The corresponding minimal polynomial is indeed $x^Q - p$, which, according to Eisenstein's lemma [2], is irreducible over $\mathbb{Q}$.

An alternative choice is based on a result from Besicovitch [5], which states that the square roots of distinct square-free[15] integers are linearly independent over the rationals. Thus, we may choose:

$$\theta_k = \sqrt{p_k}, \qquad k = 1, \ldots, Q, \tag{29}$$

where $p_1, \ldots, p_Q$ are distinct square-free integers.

Again, following Besicovitch it is possible to prove [6] that the reciprocals of the numbers in (29) are linearly independent over the rationals. Thus, an alternative choice is:

$$\theta_k = \frac{1}{\sqrt{p_k}}, \qquad k = 1, \ldots, Q, \tag{30}$$

where $p_1, \ldots, p_Q$ are distinct square-free integers. Note that prime numbers are an example of square-free integers.

6. SIMULATION RESULTS AND CONCLUSION

In Figure 1 we consider a MIMO system with $n_T = n_R = 2$ affected by flat Rayleigh fading with uncorrelated channel coefficients. Information symbols are carved from a QPSK constellation and ML decoding is assumed. We compare the BER, averaged over 10^4 channel realizations, of FDFR scheme in [12] with two different UTODs, generated using (30), having 2×2 and 2×3 encoding matrices. The simulation suggests that increasing the number of columns of the encoding matrices could be beneficial to the coding gain.

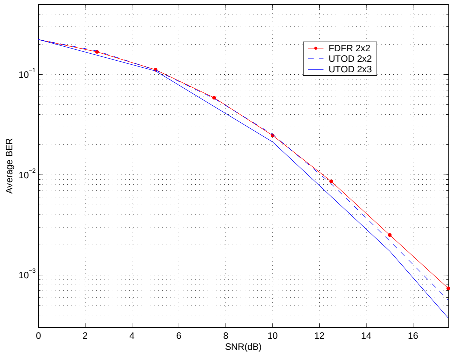

Fig. 1. Average BER for QPSK in a 2×2 MIMO system with ML decoding. FDFR with 2×2 encoding matrices (continuous line with dots) versus full-diversity UTOD with 2×2 (dashed line) and 2×3 (continuous line) matrices.

7. REFERENCES

[1] R. Horn, C. Johnson, *Matrix Analysis*, Cambridge University Press, 1994.

[2] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.

[3] A. Baker, *Transcendental Number Theory*, Cambridge University Press, London, 1975.

[4] L.C. Washington, *Introduction to Cyclotomic Fields*, 2nd Ed., Springer, 1997.

[5] A. S. Besicovitch, "On the linear independence of fractional powers of integers," *J. London Math. Soc.* 15 (1940), 3–6.

[6] D. Richardson, A. El-Sonbaty, "Use of algebraically independent numbers for zero recognition of polynomial terms," *Journal of Complexity*, vol. 19, Issue 5, pp. 631-637, Oct. 2003.

[7] E. Telatar, "Capacity of multi-antenna Gaussian channels," *European Trans. on Telecommunications*, vol. 10, no. 6, pp. 585–596, Nov. 1999.

[8] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Spacetime block codes from orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1456-1467, July 1999.

[9] S. Sandhu and A. Paulraj, "Space-time block codes: A capacity perspective," *IEEE Comm. Letters*, vol. 4, no. 12, pp. 384–386, Dec. 2000.

[10] G.D. Golden, C.J. Foschini, R.A. Valenzuela, and P.W. Wolniansky, "Detection algorithm and initial laboratory results using V-BLAST space-time communication architecture," *IEEE Electr. Lett.*, Vol. 35, pp. 14–15, Jan. 1999.

[11] B. Hassibi and B.M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inf. Theory*, pp. 1804–1824, July 2002.

[12] X. Ma and G.B. Giannakis, "Full-diversity full-rate complex-field space-time coding," *IEEE Trans. on Signal Processing*, Vol. 49, pp. 2917–2930, Nov. 2003.

[13] H. El Gamal and M.O. Damen, "Universal space-time coding," *IEEE Trans. Inf. Theory*, Vol. 49, May 2003, pp. 1097–1119.

[14] S. Barbarossa, "Trace-orthogonal design of MIMO systems with simple scalar detectors, full diversity and (almost) full rate," *SPAWC 2004*, Lisbon, Portugal, July 11–14, 2004.

[15] S. Barbarossa and A. Fasano, "Trace-Orthogonal space-time coding for multiuser systems," *ICASSP 2005*, Philadelphia, PA, USA, March 18–23, 2005.

[16] S. Barbarossa, *Multiantenna Wireless Communication Systems*, Artech House Publishers, 2005.

[17] J. K. Zhang, K. M. Wong, and T. N. Davidson, "Information lossless full rate full diversity cyclotomic linear dispersion codes," *SPAWC 2004*, Lisbon, Portugal, July 11–14, 2004.

[18] J.K. Zhang, J. Liu, and K.M. Wong, "Trace-orthogonal full diversity cyclotomic space-time codes," Chapter 5 in *Space-Time Processing for MIMO Communications*, John Wiley & Sons, 2005.

[19] A. Fasano and S. Barbarossa, "Trace-Orthogonal Space-Time Coding," *submitted to IEEE Trans. on Signal Processing*.

---

[13] The claim is true also for $n_T = 1$, but the proof is slightly different.

[14] Two integers are coprime if their greatest common divisor is 1.

[15] A natural number is said to be square-free if its prime decomposition contains no repeated factors. The number 1 is by convention taken to be square-free.