Perfect Space-Time Block Codes for parallel MIMO channels

Sheng Yang
ENST
46, rue Barrault
75013 Paris, France
syang@enst.fr

Jean-Claude Belfiore
ENST
46, rue Barrault
75013 Paris, France
belfiore@enst.fr

Ghaya Rekaya - Ben Othman
ENST
46, rue Barrault
75013 Paris, France
rekaya@enst.fr

***Abstract*— The problem of designing Space-Time codes on the MIMO quasi-static channel have received considerable attention these last years. We now know how to design Perfect Space-Time Block Codes, that is linear information preserving codes achieving the Diversity-Multiplexing gain (D-M) tradeoff [1], [2]. Recent standards using multiple antennas terminals such as IEEE 802.11n or IEEE 802.16e, for example, are based on OFDM. By using interleaving, such OFDM systems can be seen as parallel MIMO quasi-static channels. We propose, here, new perfect space-time block codes for parallel MIMO channels.**

I. Introduction

Recent multiple antennas wireless standards, such as IEEE 802.11n or IEEE 802.16e for example, are based on OFDM. There has been some literature dealing with space-time-frequency codes for OFDM systems (see for example [3], [4], [5]). But most of these references were dealing with codes that were not full rate (for example, orthogonal designs). Here, we are concerned with the design of codes for parallel uncorrelated MIMO channels (which is the case of OFDM when frequencies are perfectly interleaved). We consider a (N, n_t, n_r) channel where N is the number of MIMO channels, n_t is the number of transmit antennas per channel and n_r is the number of receive antennas per channel. The constructed space-time codes are minimum delay codes, which means that their codelength is $T = n_t$. Finally, we assume that $n_r \geq n_t$.

Next section details the system model. Then, we define what are perfect space-time codes for parallel MIMO channels. We give then, as an example the case when $n_t = 2$. Finally, some general construction recipes are given and numerical results are presented for some channels.

II. System Model

A. Wireless MIMO OFDM systems

As an example of parallel MIMO channel, we can consider the case of a MIMO OFDM system. On each subcarrier, the channel is considered flat. When two such subcarriers f_i and f_j are separated by at least the channel coherence bandwidth B_c, then channel coefficients on these subcarriers are decorrelated. Such an assumption may be satisfied if a frequency interleaver is used. Figure 1 gives an example.

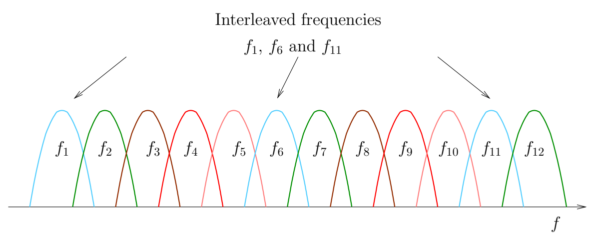

Fig. 1. OFDM multiplex: here, channel coefficients on frequencies f_1, f_6, and f_{11} are considered decorrelated

B. Notations and system model

We denote n_t the number of transmit antennas, n_r the number of receive antennas and N the number of parallel channels. Received signal is

$$\mathbf{Y}_{Nn_r \times T} = \mathbf{H}_{Nn_r \times Nn_t} \cdot \mathbf{X}_{Nn_t \times T} + \mathbf{Z}_{Nn_r \times T}$$

where $\mathbf{X}$ is the transmitted codeword, $\mathbf{Z}$ is the noise matrix with i.i.d. Gaussian coefficients and $\mathbf{H}$ is the channel matrix. Subscripts indicate the dimensions of matrices. More precisely, we have

$$\mathbf{H} = \text{diag}\ (\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_N)$$

where $\mathcal{H}_i$ is a $n_r \times n_t$ submatrix corresponding to channel i (for example the interleaved subcarrier f_y in an OFDM system). We assume that coefficients of $\mathbf{H}$ are zero-mean Gaussian i.i.d.

III. Perfect codes for the parallel MIMO channel

A. The Diversity-Multiplexing tradeoff of a MIMO parallel channel

The D-M tradeoff has been defined in [6]. For a MIMO channel, it is a piecewise linear function $d_{n_t,n_r}(r)$.

Proposition 1: The diversity-multiplexing tradeoff of a parallel channel with N i.i.d. $n_t \times n_r$ MIMO Rayleigh subchannels is

$$d_{N,n_t,n_r}(r) = N\, d_{n_t,n_r}(r/N) \tag{1}$$

where $d_{n_t,n_r}(r)$ is the diversity-multiplexing tradeoff of a $n_t \times n_r$ MIMO Rayleigh channel.

Proof: The proof is left in appendix. ∎

$$\mathcal{C}_\infty = \left\{ \begin{pmatrix} x_0 & x_1 & \ldots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & \ldots & \sigma(x_{n-2}) \\ \vdots & & & \vdots \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix} \mid x_i \in \mathbb{K},\ i = 0, \ldots, n-1 \right\}. \tag{2}$$

B. Perfect Space-Time Block codes

We remind here what perfect space-time block codes are. Perfect STBCs were first introduced in [1] for 2, 3, 4 and 6 transmit antennas. These codes were then generalized in [2] for any MIMO channel. We first give the definition of a *perfect* STBC code for the MIMO parallel channel. Let $q = \min(n_t, n_r)$.

Definition 1: a STBC is called a *perfect* code for the parallel N-MIMO channel if and only if

1) it is a full rate linear dispersion code [7] using $q \cdot N$ information symbols either QAM or HEX.
2) the minimum determinant of the code is lower bounded by a strictly positive constant that does not depend on the size of the constellation (so that in particular the rank criterion is satisfied). This property combined with property 1 is also known as the Non Vanishing Determinant (NVD) property. It is known (see [8]) that a NVD code achieves the Diversity-Multiplexing tradeoff. These NVD codes are also approximately universal [9].
3) the $2M^2$–dimensional real lattice generated by the vectorized codewords, is either $\mathbb{Z}^{2 \cdot M^2}$ or $A_2^{M^2}$. This property guarantees that the space-time block code preserves mutual information [10].
4) it induces uniform average transmitted energy per antenna in all T time slots., i.e., all the coded symbols in the code matrix have the same average energy.

C. Codes from cyclic division algebras

Perfect space-time block codes are constructed from cyclic division algebras.

We recall here the most relevant concepts about cyclic algebras and how to use them to build space-time block codes. We let the reader refer to [11] for more details. In the following, we consider number field extensions $\mathbb{K}/\mathbb{F}$, where $\mathbb{F}$ denotes the base field. The set of non-zero elements of $\mathbb{F}$ (resp. $\mathbb{K}$) is denoted by $\mathbb{F}^*$ (resp. $\mathbb{K}^*$).

Let $\mathbb{K}/\mathbb{F}$ be a cyclic extension of degree n, and σ the generator of the cyclic Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Let $\mathcal{A} = (\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ be its corresponding *cyclic algebra* of degree n, that is

$$\mathcal{A} = \mathbb{K} \cdot 1 \oplus \mathbb{K} \cdot e \oplus \ldots \oplus \mathbb{K} \cdot e^{n-1}$$

with $e \in \mathcal{A}$ such that $x \cdot e = e \cdot \sigma(x)$ for all $x \in \mathbb{K}$ and $e^n = \gamma \in \mathbb{F}^*$. Recall that one can associate a matrix to any element $x \in \mathcal{A}$ as follows. Let λ_x be the multiplication by x of an element $y \in \mathcal{A}$:

$$\begin{array}{rcl} \lambda_x : \mathcal{A} & \rightarrow & \mathcal{A} \\ y & \mapsto & \lambda_x(y) = x \cdot y. \end{array}$$

The matrix of the multiplication by λ_x, with $x = x_0 + x_1 \cdot e + \ldots + x_{n-1} \cdot e^{n-1}$, is easily checked to be

$$\begin{pmatrix} x_0 & x_1 & x_2 & \ldots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & \sigma(x_1) & \ldots & \sigma(x_{n-2}) \\ \vdots & & & & \vdots \\ \gamma\sigma^{n-2}(x_2) & \gamma\sigma^{n-2}(x_3) & \gamma\sigma^{n-2}(x_4) & \ldots & \sigma^{n-2}(x_1) \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \gamma\sigma^{n-1}(x_3) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix}. \tag{3}$$

Thus, via λ_x, we have a *matrix representation* of an element $x \in \mathcal{A}$. The space-time block code is then obtained in eq. (2). All the coefficients of such matrices are in $\mathbb{K}$. The code is obtained by considering a discrete subset of the base field $\mathbb{F}$ as information symbols. Since $\mathbb{K}$ can be seen as a vector space over $\mathbb{F}$, the code matrix entries are linear combinations of n information symbols.

The key point of this algebraic scheme is that we have a criterion to decide whether the STBC $\mathcal{C}_\infty$ satisfies the rank criterion [12]. Namely, when the cyclic algebra is a division algebra, all its elements are invertible; hence the codeword matrices have non zero determinants.

Theorem 1: [13] The algebra $\mathcal{A} = (\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ of degree n is a division algebra if the smallest positive integer t such that γ^t is the norm of some element in $\mathbb{K}^*$ is n.

D. Construction of codes for parallel MIMO channels

The idea is to construct a NVD space-time block code having a block diagonal structure since the channel itself is block diagonal. More precisely, each codeword would contain N square $n_t \times n_t$ blocks. The full-rate property implies that such a codeword corresponds to $N \cdot n_t^2$ information symbols (QAM or HEX). In order to have the Non Vanishing Determinant property, we impose to the determinant of a codeword to belong to a fractional ideal [14] of $\mathbb{Z}[i]$ or $\mathbb{Z}[j]$. Let a codeword be

$$\mathbf{X} = \begin{bmatrix} \Xi_1 & & & \\ & \Xi_2 & & \\ & & \ddots & \\ & & & \Xi_N \end{bmatrix} \tag{4}$$

We have

$$\det \mathbf{X} = \prod_{i=1}^{N} \det \Xi_i.$$

In order to have $\det \mathbf{X}$ in $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[j]$), we impose that $\det \Xi_i$ be some conjugate of an algebraic integer z in an extension field $\mathbb{F}$, so that $\prod_{i=1}^{N} \det \Xi_i = N(z) \in \mathbb{Z}[i]$ (resp. $\mathbb{Z}[j]$).

So, the major point in the construction of perfect space-time block codes is to choose as a base field $\mathbb{F}$, a Galois extension of degree N of $\mathbb{Q}(i)$ (resp. $\mathbb{Q}(j)$) with Galois group

$$\text{Gal}\ (\mathbb{F}/\mathbb{Q}(i)) = \{\tau_1, \tau_2, \ldots, \tau_N\}.$$

Then, we construct $n_t \times n_t$ matrices $\boldsymbol{\Xi}$ from a cyclic division algebra. The NVD code for parallel channels is constructed from (4) by setting $\boldsymbol{\Xi}_i = \tau_i(\boldsymbol{\Xi})$.

IV. The two transmit antennas case: Generalized Golden Codes

A. One MIMO channel

If there is just one MIMO channel, then it is known that the Golden code [15] is a perfect space-time block code for $n_t = 2$ transmit antennas and $n_r \geq 2$ receive antennas. In fact, the Golden code is the base code in order to construct perfect STBCs for $N \geq 2$ parallel channels.

B. Two parallel channels

For the 2-channel case, we propose the following code referred to as $\mathcal{C}_2$. Codewords are block diagonal matrices with 2 blocks. Let $\mathbb{F} = \mathbb{Q}(\zeta_8)$ with $\zeta_8 = e^{\frac{i\pi}{4}}$ be an extension of $\mathbb{Q}(i)$ of degree 2. We choose $\mathbb{K} = \mathbb{F}\left(\sqrt{5}\right) = \mathbb{Q}\left(\zeta_8, \sqrt{5}\right)$. In fact, we try to construct the Golden code on the base field $\mathbb{Q}(\zeta_8)$ instead of the base field $\mathbb{Q}(i)$. Moreover, the number γ is no more equal to i because i is a norm in $\mathbb{Q}(\zeta_8)$ (in fact, $i = N_{\mathbb{K}/\mathbb{F}}(\zeta_8)$). We choose here, in order to preserve the shaping of the code, $\gamma = \zeta_8$. We prove that $\zeta_8 \notin N_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$ and thus that this code satisfies the full rank and non vanishing determinant conditions. Such a code uses $N \cdot n_t^2 = 8$ QAM symbols. Let $\theta = \frac{1+\sqrt{5}}{2}$, $\gamma = i$ and $\sigma : \theta \mapsto \bar{\theta} = \frac{1-\sqrt{5}}{2}$. The ring of integers of $\mathbb{K}$ is $\mathcal{O}_{\mathbb{K}} = \{a + b\theta \mid a, b \in \mathbb{Z}[\zeta_8]\}$. Let $\alpha = 1 + i - i\theta$ and $\bar{\alpha} = 1 + i - i\bar{\theta}$. Codewords are given by

$$\mathbf{X} = \begin{bmatrix} \boldsymbol{\Xi} & \mathbf{0} \\ \mathbf{0} & \tau(\boldsymbol{\Xi}) \end{bmatrix}$$

with $\boldsymbol{\Xi}$ defined in eq. (5) and τ maps ζ_8 into $-\zeta_8$. This code is very similar to the Golden code and since the mapping

$$\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} a + b\zeta_8 \\ a - b\zeta_8 \end{pmatrix}$$

is a unitary mapping, then the linear function that maps the 8 information QAM symbols to the vector vec$\mathbf{X}$ is also unitary which means that vec$\mathbf{X}$ is a rotated QAM^8 vector.

C. $N = 2^m$ parallel channels

The same type of code can be constructed when $N = 2^m$. Consider then the base field $\mathbb{F} = \mathbb{Q}(\zeta_{2^{m+2}})$ and take $\mathbb{K} = \mathbb{Q}\left(\zeta_{2^{m+2}}, \sqrt{5}\right)$. We can also prove in the same way that $\zeta_{2^{m+2}}$ is not a norm. Since the mapping

$$\begin{pmatrix} a_0 \\ \vdots \\ a_{N-1} \end{pmatrix} \mapsto \begin{pmatrix} \tau_1\left(\sum_{i=0}^{N-1} a_i \zeta_{2^{m+2}}^i\right) \\ \vdots \\ \tau_N\left(\sum_{i=0}^{N-1} a_i \zeta_{2^{m+2}}^i\right) \end{pmatrix}$$

is unitary [16], then the shaping property is satisfied and finally, this code is a perfect STBC for the $(2^m, 2, 2)$ parallel channel.

V. General codes construction

A. Structure of the codewords

We give here a general construction for the $(N, n_t, n_r \geq n_t)$ parallel MIMO channel. We assume that we are constructing such codes with QAM constellations. The generalization to HEX constellations is straightforward.

Let $\mathbb{F}$ be a Galois extension of degree N on $\mathbb{Q}(i)$, and $\mathbb{K}$ be a cyclic extension of degree n_t on $\mathbb{F}$. We denote σ the generator of Gal $(\mathbb{K}/\mathbb{F})$ and assume that Gal $(\mathbb{F}/\mathbb{Q}(i)) = \{\tau_1, \tau_2, \ldots, \tau_N\}$. Let $\gamma \in \mathbb{F}$ such that $\gamma, \gamma^2, \ldots, \gamma^{n_t-1}$ are not norms of an element of $\mathbb{K}$. Then we construct the cyclic division algebra $\mathcal{A} = (\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ of degree n_t. The matrix representation of elements of $\mathcal{A}$ will be denoted $\boldsymbol{\Xi}$ ($n_t \times n_t$ matrices). Finally, we construct codewords

$$\mathbf{X} = \begin{bmatrix} \tau_1(\boldsymbol{\Xi}) & & & \\ & \tau_2(\boldsymbol{\Xi}) & & \\ & & \ddots & \\ & & & \tau_N(\boldsymbol{\Xi}) \end{bmatrix} \quad (6)$$

Determinant of these codewords are

$$\det \mathbf{X} = \prod_{i=1}^{N} \det \tau_i(\boldsymbol{\Xi}) = \prod_{i=1}^{N} \tau_i(\det \boldsymbol{\Xi}) = N_{\mathbb{F}/\mathbb{Q}(i)}(\det \boldsymbol{\Xi}) \in \mathbb{Q}(i) \setminus \{0\} \quad (7)$$

Codes constructed on such cyclic division algebras are full rate and have the Non Vanishing Determinant Property (see (7)). This construction method is quite general but what remains hard is to find the good extension fields and the corresponding codes for each set of parameters.

B. Unitary transforms

In order to satisfy to the shaping constraint, we impose to the vectorized codeword to be a rotated version of a QAM$^{N \cdot n_t^2}$ constellation. Rotated constellations constructions from algebraic number fields are well-known now (see for example [17] for a comprehensive tutorial on this topic). In order to construct space-time codes with this shaping property, we take a perfect space-time block code for a single MIMO channel (general constructions are given in [2]). Instead of considering symbols in $\mathbb{Q}(i)$ or $\mathbb{Q}(j)$, replace the base field by a new field $\mathbb{F}$ of degree N over $\mathbb{Q}(i)$ or $\mathbb{Q}(j)$. In the MIMO perfect code construction, the cyclic division algebra used the number field $\mathbb{L}$ (of degree n_t over $\mathbb{Q}(i)$) with $\mathbb{L} = \mathbb{Q}(i, \theta)$ for some θ. Here, we choose $\mathbb{F}$ such that $\mathbb{F} \cap \mathbb{L} = \mathbb{Q}(i)$ and consider the extension $\mathbb{K} = \mathbb{F}(\theta)$. This extension remains cyclic with the same Galois group as Gal $(\mathbb{L}/\mathbb{Q}(i))$. We also assume that it is possible to construct, in $\mathbb{F}$, the lattice $\mathbb{Z}[i]^N$ (see [18] for example) and that it can be done by restricting the symbols to be in an ideal of $\mathbb{F}$, let's say $\mathcal{I}$.

$$\mathbf{\Xi} = \begin{bmatrix} \alpha \cdot (s_1 + s_2\zeta_8 + s_3\theta + s_4\zeta_8\theta) & \alpha \cdot (s_5 + s_6\zeta_8 + s_7\theta + s_8\zeta_8\theta) \\ \zeta_8\bar{\alpha} \cdot \left(s_5 + s_6\zeta_8 + s_7\bar{\theta} + s_8\zeta_8\bar{\theta}\right) & \bar{\alpha} \cdot \left(s_1 + s_2\zeta_8 + s_3\bar{\theta} + s_4\zeta_8\bar{\theta}\right) \end{bmatrix} \quad (5)$$

Finally, space-time codewords for the parallel MIMO channel will be as in (6) with

$$\mathbf{\Xi} = \begin{pmatrix} x_0 & x_1 & \dots & x_{n_t-1} \\ \gamma\sigma(x_{n_t-1}) & \sigma(x_0) & \dots & \sigma(x_{n_t-2}) \\ \vdots & & & \vdots \\ \gamma\sigma^{n_t-2}(x_2) & \gamma\sigma^{n_t-2}(x_3) & \dots & \sigma^{n_t-2}(x_1) \\ \gamma\sigma^{n_t-1}(x_1) & \gamma\sigma^{n_t-1}(x_2) & \dots & \sigma^{n_t-1}(x_0) \end{pmatrix}$$

and $x_0, x_1, \dots, x_{n_t-1}$ satisfy to

$$x_i = \sum_{j=0}^{n_t-1} a_{i,j}\omega_j$$

where $\omega_0, \omega_1, \dots, \omega_{n_t-1}$ are in $\mathbb{K}$ and $a_{i,j}$ are in $\mathcal{I}$.

By using this method, we can prove that vec$\mathbf{X}$ (6) belongs to a rotated version of $\mathbb{Z}[i]^{N \cdot n_t^2}$.

C. γ is not a norm

We have now to find $\gamma \in \mathbb{F}$ such that γ is not a norm and $|\gamma| = 1$. We can use the general method from [2]. We'll get some non-integer γ. In some cases, it is possible to find an integer γ when for example $N = 2^m$ or $N = 3 \times 2^m$ for some m since .

VI. Numerical results

Simulation results are given for 3 cases with $n_r = n_t$. Figure 2 gives the results.

A. Case $n_t = 2, N = 2$

We used here the code defined in subsection IV-B.

B. Case $n_t = 2, N = 4$

We used here one of the codes defined in subsection IV-C by choosing $\mathbb{K} = \mathbb{Q}\left(\zeta_{16}, \sqrt{5}\right)$ and $\gamma = \zeta_{16}$.

C. Case $n_t = 3, N = 2$

Here, we consider the following fields: $\mathbb{F} = \mathbb{Q}(\zeta_8)$ and $\mathbb{K} = \mathbb{F}\left(2\cos\left(\frac{2\pi}{7}\right)\right)$ which is a cyclic extension of degree 3 over $\mathbb{F}$. The rotation matrix (constructed over $\mathbb{Q}\left(2\cos\left(\frac{2\pi}{7}\right)\right)$is the one giving the best minimum product distance in dimension 3 [18]. Finally, we chose $\gamma = \frac{1+2i}{2+i}$ which is not a norm (see appendix).

VII. Conclusion

We developed here a framework for the construction of perfect space-time block codes for parallel MIMO channels (N, n_t, n_r), applicable to OFDM systems. These codes are constructed from cyclic division algebras whose base field is itself an extension field of $\mathbb{Q}(i)$ or $\mathbb{Q}(j)$. Perfect STBCs of [1], [2] are particular cases corresponding to $N = 1$. These codes can be applied to wireless MIMO systems when the number of uncorrelated frequencies is not so high. Moreover they are D-M achieving and preserve mutual information, so that they have a good behavior for a large range of SNR's.

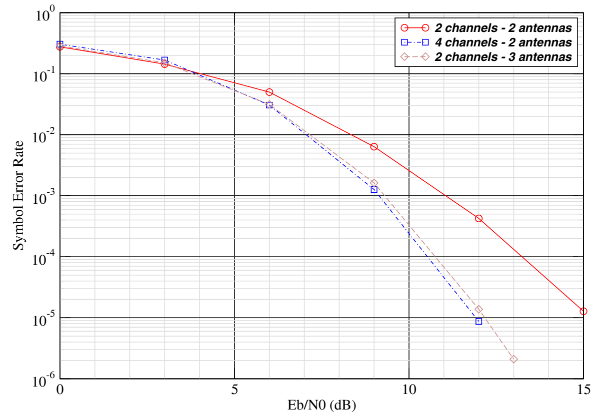

Fig. 2. Spectral efficiency is 4 bits for 2 antennas and 6 bits for 3 antennas; diversity is resp. 8, 16 and 18

Appendix I
The D-M tradeoff of parallel MIMO channels

The sketch of proof is as follows. Let $q \triangleq \min\{n_t, n_r\}$. From [6], we have

$$d_{n_t,n_r}(r) = \inf_{\mathcal{O}_{n_t,n_r}(\boldsymbol{\alpha},r)} \sum_{i=1}^{q} (2i - 1 + |n_t - n_r|)\,\alpha_i \quad (8)$$

with $\boldsymbol{\alpha} \triangleq [\alpha_1 \ \cdots \ \alpha_q]^{\mathsf{T}}$ being the ordered exponential orders of the q eigenvalues of the channel matrix and

$$\mathcal{O}_{n_t,n_r}(\boldsymbol{\alpha}, r) \triangleq \left\{ \boldsymbol{\alpha} \ : \ \sum_{i=1}^{q} (1-\alpha_i)^+ < r \right\}. \quad (9)$$

In the same way, the diversity-multiplexing tradeoff of the parallel MIMO channel is

$$d_{N,n_t,n_r}(r) = \inf_{\mathcal{O}_{T,n_t,n_r}(\boldsymbol{\alpha}_T,r)} \sum_{j=1}^{N}\sum_{i=1}^{q} (2i - 1 + |n_t - n_r|)\,\alpha_{i,j} \quad (10)$$

where $\boldsymbol{\alpha}_N \triangleq [\alpha_{1,1} \ \alpha_{2,1} \ \cdots \ \alpha_{q,N}]^{\mathsf{T}}$ with $[\alpha_{1,j} \ \cdots \ \alpha_{q,j}]^{\mathsf{T}}$ being the ordered exponential orders of the jth subchannel, and the constraint set is

$$\mathcal{O}_{N,n_t,n_r}(\boldsymbol{\alpha}_N, r) \triangleq \left\{ \boldsymbol{\alpha} \ : \ \sum_{j=1}^{N}\sum_{i=1}^{q} (1-\alpha_{i,j})^+ < r \right\}. \quad (11)$$

Note than $\alpha_{i,j}$'s are symmetric both in the objective function and in the constraint set for the same i's. Thus, setting $\alpha_{i,1} = \alpha_{i,2} = \cdots = \alpha_{i,N} \triangleq \alpha_i$ will be without loss of optimality

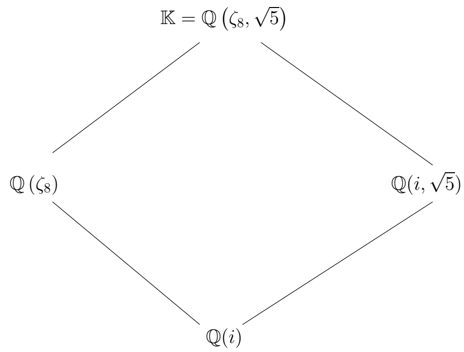

Fig. 3. Two ways of extending $\mathbb{Q}(i)$ up to $\mathbb{K}$

of the solution. Finally, with this assumption, some simpler manipulations lead to (1).

APPENDIX II
ζ_8 IS NOT A NORM IN $\mathbb{K}$

We prove, in this appendix, that ζ_8 is not a norm of an element of $\mathbb{K} = \mathbb{Q}\left(\zeta_8, \sqrt{5}\right)$. Assume that ζ_8 is a norm in $\mathbb{K}$. That means

$$\exists x \in \mathbb{K}, N_{\mathbb{K}/\mathbb{Q}(\zeta_8)}(x) = \zeta_8. \tag{12}$$

Consider now the extensions described in figure 3.

From eq. (12), by considering the left extension of figure 3, we deduce that

$$N_{\mathbb{K}/\mathbb{Q}(i)}(x) = N_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(i)}\left(N_{\mathbb{K}/\mathbb{Q}(\zeta_8)}(x)\right) = \zeta_8 \cdot \tau\left(\zeta_8\right) = -i. \tag{13}$$

Now, we deduce, from the right extension of figure 3 that

$$N_{\mathbb{K}/\mathbb{Q}(i)}(x) = N_{\mathbb{Q}\left(i,\sqrt{5}\right)/\mathbb{Q}(i)}\left(N_{\mathbb{K}/\mathbb{Q}\left(i,\sqrt{5}\right)}(x)\right) = -i. \tag{14}$$

Denote $y = N_{\mathbb{K}/\mathbb{Q}\left(i,\sqrt{5}\right)}(x) \in \mathbb{Q}\left(i, \sqrt{5}\right)$. Then the number

$$z = \frac{1+\sqrt{5}}{2} \cdot y$$

has an algebraic norm equal to i, and belongs to $\mathbb{Q}\left(i, \sqrt{5}\right)$. In [15], it has been proved that i was not a norm in $\mathbb{Q}\left(i, \sqrt{5}\right)$. So, ζ_8 is not a norm in $\mathbb{K}$.

APPENDIX III
$\gamma = \frac{1+2i}{2+i}$ IS NOT A NORM IN $\mathbb{K} = \mathbb{Q}\left(\zeta_8, 2\cos\left(\frac{2\pi}{7}\right)\right)$

Consider the absolute extension $\mathbb{K}/\mathbb{Q}$. In this field, with some software like KANT [19], we can check that 5 is not a norm, which means that on $\mathbb{K}/\mathbb{Q}(i)$, neither $1+2i$ nor $2+i$ are norms. So, γ is not a norm.

REFERENCES

[1] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, “Perfect Space Time Block Codes.” submitted to *IEEE Trans. Inform. Theory*, 2004.

[2] P. Elia, B. A. Sethuraman, and P. Kumar, “Perfect space-time codes with minimum and non-minimum delay for any number of antennas.” submitted to *IEEE Trans. on Inform. Theory*, also available on arXiv cs.IT/0512028, Dec. 2005.

[3] D. Agrawal, V. Tarokh, A. Naguib, and N. Seshadri, “Space-time coded OFDM for high data rate wireless communication over wideband channels,” in *Proc.* 48^{th} *IEEE VTC*, vol. 3, pp. 2232–2236, May 1998.

[4] Z. Lin, Y. Xin, and G. Giannakis, “Space-time-frequency coded OFDM over frequency- selective fading channels,” *IEEE Trans. Signal Processing*, vol. 50, October 2002.

[5] W. Su, Z. Safar, and K. J. Liu, “Full-rate full-diversity space-frequency codes with optimum coding advantage,” *IEEE Trans. Inform. Theory*, vol. 51, June 2005.

[6] L. Zheng and D. Tse, “Diversity and Multiplexing: A fundamental tradeoff in multiple-antenna channels,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 1073–1096, May 2003.

[7] B. Hassibi and B. M. Hochwald, “High-rate codes that are linear in space and time,” *IEEE Trans. Inform. Theory*, vol. 48, pp. 1804–1824, July 2002.

[8] S. Yang and J.-C. Belfiore, “Optimal space-time codes for the MIMO amplify and forward cooperative channel.” submitted to *IEEE Trans. Inform. Theory*, September 2005. available on ArXiv.

[9] S. Tavildar and P. Viswanath, “Approximately universal codes over slow fading channels.” submitted to *IEEE Trans. on Inform. Theory*, Feb. 2005.

[10] H. El Gamal and M. O. Damen, “Universal space-time coding,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 1097–1119, May 2003.

[11] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, “Full-diversity, high-rate space-time block codes from division algebras,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 2596– 2616, October 2003.

[12] V. Tarokh, N.Seshadri, and A. Calderbank, “Space-time codes for high data rate wireless communication : Performance criterion and code construction,” *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, March 1998.

[13] A. A. Albert, “Structure of Algebras.” AMS Colloqium Pub. XXIV, 1961. AMS, Providence.

[14] A. Fröhlich and M. Taylor, *Algebraic number theory*. Cambridge University Press, 1991.

[15] J.-C. Belfiore, G. Rekaya, and E. Viterbo, “The Golden Code: A 2 × 2 full rate Space-Time Code with non vanishing Determinants,” *IEEE Trans. Inform. Theory*, vol. 51, pp. 1432–1436, April 2005.

[16] X. Giraud, E. Boutillon, and J.-C. Belfiore, “Algebraic tools to build modulation schemes for fading channels,” *IEEE Trans. Inform. Theory*, vol. 43, pp. 938–952, May 1997.

[17] F. Oggier and E. Viterbo, “Algebraic number theory and code design for Rayleigh fading channels,” in *Foundations and Trends in Communications and Information Theory*, vol. 1, pp. 333–415, 2004.

[18] E. Bayer, F. Oggier, and E. Viterbo, “New algebraic constructions of rotated $\mathbb{Z}^n$ lattice constellations for the Rayleigh fading channel,” *IEEE Trans. Inform. Theory*, April 2004.

[19] M. Daberkow, C. Fieker, J. Klners, M. Pohst, K. Roegner, and K. Wildanger, “KANT V4,” *J. Symbolic Comp.*, vol. 24, pp. 267–283, 1997.