# An Algebraic Coding Scheme for Wireless Relay Networks with Multiple-Antenna Nodes

Frédérique Oggier* and Babak Hassibi[1]

Department of Electrical Engineering

California Institute of Technology

Pasadena, CA 91125

{frederique,hassibi}@systems.caltech.edu

Phone:+1 (626) 395 41 84, Fax:+1 (626) 564 93 07

January 15, 2007

**Abstract**

We consider the problem of coding over a half-duplex wireless relay network where both the transmitter and the receiver have respectively several transmit and receive antennas, whereas each relay is a small device with only a single antenna. Since in this scenario requiring the relays to decode results in severe rate hits, we propose a full rate strategy where the relays do a simple operation before forwarding the signal, based on the idea of distributed space-time coding. Our scheme relies on division algebras, an algebraic object which allows to design fully diverse matrices. The code construction is applicable to systems with any number of transmit/receive antennas and relays, and has better performance than random code constructions, with much less encoding complexity. Finally, the robustness of the proposed distributed space-time codes to node failures is considered.

EDICS: SEN-DCSC

[1]This work was supported in part by the Swiss National Science Foundation grant PBEL2-110209 and by NSF grant CCR-0133818, by Caltech's Lee Center for Advanced Networking and by a grant from the David and Lucille Packard Foundation.

# 1 Introduction

It is well known that the use of multiple antennas at both the transmitter and receiver of a wireless channel can greatly increase its capacity and reliability. Recently, attention has been focused on wireless networks, where researchers have been looking for so-called *cooperative diversity* methods, to exploit spatial diversity using the antennas of different users in the network.

## 1.1 Previous work on cooperative diversity schemes

In [16], a scheme where pairs of users cooperate is considered. Each of the two partners is responsible for transmitting both its own information and the information of its partner which it will receive and detect. The aim is to gain spatial diversity. One of the first scheme to obtain spatial diversity for an arbitrary half-duplex wireless network has been given in [11]: first, the source broadcasts its information to the destination as well as to potential relays. In a second phase, relays that are able to decode either repeat or utilize a space-time code to simultaneously transmit to the destination. The mutual information and outage probability of the network are analyzed.

Protocols for wireless networks are usually categorized into two main classes: the *amplify-and-forward* scheme and the *decode-and-forward* scheme, depending on whether we assume the ability of decoding at the relays. Indeed, decoding at the relays is not always a valid assumption. This implies enough computational power, which for example sensor networks do not have. Furthermore, when, to increase the data rate, the transmitter and receiver employ multiple antennas but the relays do not, decoding means a bottleneck at the relays, resulting in a loss in the data rate.

In [8], *distributed* space-time coding is presented, where the relays cooperate in such a way that the received signal is seen as a space-time code, so as to obtain the diversity known to be achieved by traditional space-time codes. The pairwise error probability is computed to determine the diversity of the system. Distributed space-time coding can be seen as a more sophisticated form of amplify-and-forward protocol, where the relays do more than just amplifying the signal.

In [1], the Zheng-Tse diversity-multiplexing gain (DMG) tradeoff [22] is used as a mean to evaluate the performance of new cooperative schemes, including a *non-orthogonal* amplify-and-

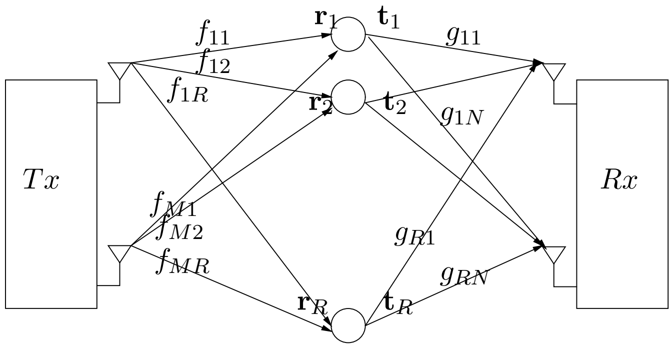


Figure 1: A wireless relay network with several antennas at both the transmitter and receiver.

forward protocol, where the source terminal is allowed to transmit during all the time (by opposition to *orthogonal* schemes). Several works have followed the DMG approach, like [5] where the authors present families of cooperative schemes based on algebraic space-time codes that achieve the DMG tradeoff. The scenario of [1] has been generalized in [21] for a network where all the nodes (including the relay nodes) have several antennas. Note that in [21], the relays amplify the signal, and do not perform a linear transformation as it will be the case in this work. The DMG tradeoff for this network has been analyzed, and the codes built shown to be optimal with respect to that tradeoff.

Let us now briefly recall about distributed space-time coding, and the network model presented in [9], since this is the model we will consider in this paper.

## 1.2 Distributed space-time coding

Consider a wireless network with $R+2$ nodes, where the receiver and transmitter node are equipped with respectively $M$ and $N$ antennas, to increase the data rate of the network. The other $R$ nodes serve as relays. They are assumed to be small devices with low power and few resources, with thus only one antenna (see Fig. 1). This is for example a suitable model for many sensor networks.

Channels are denoted by $f_{mj}$ from the transmit antenna $m$ to the $j$-th relay, and by $g_{jn}$ from the $j$-th relay to the receive antenna $n$. Note that we do not assume a direct path from the transmitter to the receiver. Noise is denoted by $v_j$ at the $j$-th relay, and by $w_n$ at the $n$-th receive antenna. Both channels and noises are assumed to be i.i.d complex Gaussian with zero-mean and unit-variance.

Channels are unknown at the relays and at the transmitter, but we assume that the receiver knows the equivalent channel $\mathbf{H}$ described in (1) below (see also Remark 1). Let $T$ denote a coherence interval during which $f_{mj}$ and $g_{jn}$ are constant. The information bits are thus encoded into $T \times M$ matrices $\mathbf{S} = [\mathbf{s}_1, \ldots, \mathbf{s}_M]$, where $\mathbf{s}_m$ is a $T$-dimensional signal sent by the $m$-th transmit antenna. The signal $\mathbf{S}$ is normalized as $\mathrm{E}[Tr(\mathbf{S}^*\mathbf{S})] = M$. The average total power for $T$ transmissions is $P_1 T$ at the transmitter, and $P_2 T$ at every relay. The transmission schemes is: from time 1 to $T$, $\sqrt{P_1 T/M}\mathbf{S}$ is sent. Each relay $j$ gets a received signal $\mathbf{r}_j$, which is multiplied by a *unitary matrix* $A_j$ (see Remark 2) before being forwarded during time $T+1$ to $2T$. The received signal $\mathbf{y}_n$ at the $n$-th antenna is a sum of each signal $\mathbf{t}_j$ transmitted by each relay $j$:

$$\mathbf{r}_j = \sqrt{P_1 T/M} \sum_{m=1}^{M} f_{mj}\mathbf{s}_m + \mathbf{v}_j,\ \ \mathbf{t}_j = \sqrt{\frac{P_2}{P_1+1}} A_j \mathbf{r}_j,\ \ \mathbf{y}_n = \sum_{j=1}^{R} g_{jn}\mathbf{t}_i + \mathbf{w}_n.$$

This can be summarized, setting $\mathbf{f}_j = (f_{1j}, \ldots, f_{Mj})^T$, as

$$\mathbf{y}_n = \sqrt{\frac{P_1 P_2 T}{(P_1+1)M}} [A_1\mathbf{S} \quad A_2\mathbf{S} \quad \cdots \quad A_R\mathbf{S}] \begin{bmatrix} \mathbf{f}_1 g_{1n} \\ \vdots \\ \mathbf{f}_R g_{Rn} \end{bmatrix} + \sqrt{\frac{P_2}{P_1+1}} \sum_{j=1}^{R} g_{in} A_j \mathbf{v}_j + \mathbf{w}_n.$$

By defining $\mathbf{Y} = [\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N]$, $\mathbf{X} = [A_1\mathbf{S}, A_2\mathbf{S}, \ldots, A_R\mathbf{S}]$, $\mathbf{g}_j = [g_{j1}, g_{j2}, \ldots, g_{jN}]$, $\mathbf{H} = [\mathbf{f}_1\mathbf{g}_1, \ldots, \mathbf{f}_R\mathbf{g}_R]^T$, and $\mathbf{W} = \left[ \sqrt{\frac{P_2}{P_1+1}} \sum_{j=1}^{R} g_{j1} A_j \mathbf{v}_j + \mathbf{w}_1 \quad \ldots \quad \sqrt{\frac{P_2}{P_1+1}} \sum_{j=1}^{R} g_{jN} A_j \mathbf{v}_j + \mathbf{w}_N \right]$, we finally get that the channel model can be written as

$$\mathbf{Y} = \sqrt{\frac{P_1 P_2 T}{(P_1+1)M}} \mathbf{X}\mathbf{H} + \mathbf{W}. \tag{1}$$

**Remark 1** In order for the receiver to estimate $\mathbf{H}$, a block of known training symbols using the same space-time coding scheme is sent, so that the receiver solves for the equivalent channel matrix, using its knowledge of $\mathbf{X}$ and $\mathbf{Y}$.

**Remark 2** The choice of $A_j$ unitary makes the protocol equitable among different users, which is reasonable since there is no reason to advantage a user rather than another, or a particular time instant over another. It also guarantees that the noise forwarded by the relays remains white at the receiver, though it has been shown recently [18] that for that purpose, it is enough to require the $A_j\mathbf{v}_j$, $j = 1, \dots, R$ to be uncorrelated.

In [9], the pairwise error probability of such a system has been analyzed, and it has been shown that similarly to the multiple-antenna case, the "full diversity" condition holds. That is, the difference of two distinct codewords $\mathbf{X}_k - \mathbf{X}_l$ has to be full-rank in order to maximize the decay rate of the pairwise probability of error. The following theorem has been proved

**Theorem 1 (Diversity for wireless relay network)** *Assume that $T \geq MR$ and the distributed space-time code is fully diverse. For large total transmit power $P$, the diversity of the wireless relay network is*

$$div = \begin{cases} \min\{M,N\}R & M \neq N \\ MR\left(1 - \frac{1}{M}\frac{\log\log P}{\log P}\right) & M = N. \end{cases}$$

### 1.3 Organization and contribution of this work

In this work, we are interested in constructing codes for a half duplex wireless relay network where a transmitter and a receiver have several antennas, while the $R$ relays are small devices with low power and little computational resources. In this scenario, decoding at the relays is not desirable, since the relay nodes can only decode at the rates offered by a MISO system, whereas the overall system can operate at MIMO rates.

We thus propose a coding scheme based on distributed space-time codes [9] as described above, where it is recalled that the main design criterion is full-diversity. Note that while good codes have been recently proposed for the case of one antenna at the transmitter and receiver [10, 14], no coding scheme has been proposed in the multiple antenna case, not even using random codes. The contribution of this work is thus to present a technique to design distributed space-time codes for multiple antennas receiver and transmitter node, where full diversity is proved. It consists of jointly optimizing a space-time code at the transmitter and unitary matrices at the relays.

We focus on minimizing the pairwise probability of error, both when all the relay nodes are active and when some of them are not able to transmit. We propose a scheme which is suitable for any number of transmit/receive antennas and nodes, based on division algebras, an algebraic object known to enable the construction of fully diverse matrices. To reach high data rate, we exploit the $\min\{M,N\}T$ degrees of freedom of the channel, and call such codes *full rate*. We compare our code to a random code construction, which is also fully-diverse, and show that the algebraic coding scheme has better performance, due to its higher coding gain. Furthermore, it requires much less encoding complexity, in particular at the relay nodes.

The organization of the paper is as follows. Since our construction relies on the way division algebras provide fully-diverse matrices, Section 2 introduces division algebras and explain how those algebraic objects can be used to obtain codewords. We then present the distributed scheme itself, and detail the particular case when only one antenna is used at both the transmitter and receiver. In Section 4, we consider the robustness of distributed space-time codes to node failures. Simulations are provided in the last section, where the algebraic construction is compared to random codes.

## 2 Division algebras and fully-diverse matrices

Recall from the introduction (Subsection 1.2) that the pairwise probability of error of a distributed space-time code is first governed by the *diversity*. The coding problem that we address in this paper is thus to construct distributed space-time codes that are fully diverse.

### 2.1 Introducing division algebras

Division algebras are *noncommutative* fields. They became of interest for traditional space-time coding [17, 12] since they naturally provide linear families of fully-diverse matrices, as we will now explain, using as example a particular family of division algebras called *cyclic division algebras*.

The interested reader may refer to the original papers [17, 12] or to a self-contained tutorial [3] for more details. We start by recalling definitions related to number fields, before introducing the definition of cyclic algebra.

To start our construction, we need to consider two *number fields*, that we denote by $L$ and $K$. Number fields can be seen as vector spaces over $\mathbb{Q}$, the field of rational numbers. For example, $\mathbb{Q}(i) = \{a + bi,\ a, b \in \mathbb{Q}\}$ is a vector space of dimension 2 over $\mathbb{Q}$, whose basis is $\{1, i\}$. More generally, $L$ is a vector space of dimension $n$ over $K$. We say that $L$ is a field *extension* of $K$ if $K \subset L$, which we denote by $L/K$. The dimension of $L$ over $K$ as a vector space is called the *degree*.

**Example 1** We have that $F = \mathbb{Q}(i, \sqrt{5}) = \{c + d\sqrt{5},\ c, d \in \mathbb{Q}(i)\}$ is a vector space of dimension 2 over $K = \mathbb{Q}(i)$. Similarly, let $\zeta_{15} = e^{2i\pi/15}$, and consider the number field

$$L = \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}, i) = \{a + b(\zeta_{15} + \zeta_{15}^{-1}) + c(\zeta_{15} + \zeta_{15}^{-1})^2 + d(\zeta_{15} + \zeta_{15}^{-1})^3 \mid a, b, c, d \in \mathbb{Q}(i)\},$$

which is a vector space of dimension 4 over $K = \mathbb{Q}(i)$. Since $(\zeta_{15} + \zeta_{15}^{-1})^3 = (-1 + \sqrt{5})/2$, $F \subset L$ and $L$ is an extension of $F$.

Another way of thinking of a number field is to add a root of a polynomial to a field, and to add also all its powers and multiples so that the resulting set is indeed a field. For example, $\mathbb{Q}(i)$ is built by adding the roots of the polynomial $X^2 + 1$ to $\mathbb{Q}$. The field extension $L/K$ can similarly be seen as adding the element $\theta$, the root of a polynomial $p(X)$, to $K$. For our purpose, we are interested in a field extension $L/K$ such that all roots $\theta_1, \ldots, \theta_n$ of $p(X)$ are related to each other as follows: there exists a map $\sigma$ such that $\sigma^i(\theta_1) = \theta_j$, $i, j = 1, \ldots, n$.

**Example 2** Consider again $L = \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}, i)$, which is obtained from $\mathbb{Q}(i)$ by adding $\zeta_{15} + \zeta_{15}^{-1}$, which is a root of the polynomial $p(X) = X^4 - X^3 - 4X^2 + 4X + 1$, whose other roots are $\zeta_{15}^2 + \zeta_{15}^{-2}, \zeta_{15}^4 + \zeta_{15}^{-4}, \zeta_{15}^8 + \zeta_{15}^{-8}$. Set $\sigma : \zeta_{15} + \zeta_{15}^{-1} \mapsto \zeta_{15}^2 + \zeta_{15}^{-2}$. We see that each root is connected to the other by $\sigma$, for example, $\sigma(\zeta_{15}^2 + \zeta_{15}^{-2}) = \zeta_{15}^4 + \zeta_{15}^{-4}$, and $\sigma(\zeta_{15}^8 + \zeta_{15}^{-8}) = \zeta_{15} + \zeta_{15}^{-1}$.

In such case, $L/K$ is called a *cyclic Galois* extension, and $\{\sigma^j,\ j = 1, \ldots, n\}$, is called a *Galois group*. For example, $\mathbb{Q}(i)$ is a cyclic extension of degree 2, since there exists $\sigma : i \mapsto -i$. Similarly $L$ from Example 2 is a cyclic extension of degree 4.

Let us now give the definition of a *cyclic algebra*. We consider $L/K$ a field extension of degree $n$ such that its Galois group $\{\sigma^j,\ j = 1\ldots, n\}$ is cyclic, as explained above. Choose $0 \neq \gamma \in K$. We construct a non-commutative *cyclic algebra*, denoted by $\mathcal{A} = (L/K, \sigma, \gamma)$, as follows:

$$\mathcal{A} = L \oplus eL \oplus \ldots \oplus e^{n-1}L,$$

that is, we take $n$ copies of the field $L$, which gives a vector space structure with basis $\{1, e, \ldots, e^{n-1}\}$, and an element $x \in \mathcal{A}$ corresponds to the vector $(x_0, \ldots, x_{n-1})$, since $x$ can be written as

$$x = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1},\ x_i \in L \text{ for all } i.$$

The basis element $e$ is asked to satisfy $e^n = \gamma$, meaning that one can choose any $\gamma$, and the basis will be given by $e = \gamma^{1/n}$ and its powers. Since we want an algebra, we need to be able to multiply elements in $\mathcal{A}$. Since scalars multiply on the right, we need to know what happens when multiplication occurs on the left, and we set the following rule:

$$\lambda e = e\sigma(\lambda) \text{ for } \lambda \in L.$$

**Example 3** Let again $L = \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}, i)$ and $\sigma : \zeta_{15} + \zeta_{15}^{-1} \mapsto \zeta_{15}^2 + \zeta_{15}^{-2}$, we choose $\gamma = i$ which defines the cyclic algebra $\mathcal{A} = (L/\mathbb{Q}(i), \sigma, i)$ given by

$$\mathcal{A} = L \oplus eL \oplus e^2L \oplus e^3L.$$

### 2.2 Codewords from cyclic algebras

Let us now see how cyclic algebras provide families of matrices. This is by associating to the element $x \in \mathcal{A}$ the matrix of multiplication by $x$. Let us do the whole computation when $n = 2$.

**Example 4** For $n = 2$, we have $\mathcal{A} = L \oplus eL$ with $e^2 = \gamma$ and $\lambda e = e\sigma(\lambda)$ for $\lambda \in L$. An element

$x \in \mathcal{A}$ can be written $x = x_0 + ex_1$. Let us compute the multiplication by $x$ of any element $y \in \mathcal{A}$.

$$\begin{aligned} xy &= (x_0 + ex_1)(y_0 + ey_1) \\ &= x_0 y_0 + e\sigma(x_0) y_1 + ex_1 y_0 + \gamma\sigma(x_1) y_1 \\ &= [x_0 y_0 + \gamma\sigma(x_1) y_1] + e[\sigma(x_0) y_1 + x_1 y_0], \end{aligned}$$

since $e^2 = \gamma$ and using the noncommutativity rule $\lambda e = e\sigma(\lambda)$.

In the basis $\{1, e\}$, this yields

$$xy = \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}.$$

There is thus a correspondence

$$x = x_0 + ex_1 \in \mathcal{A} \leftrightarrow \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}, \; e \in \mathcal{A} \leftrightarrow \begin{pmatrix} 0 & \gamma \\ 1 & 0 \end{pmatrix}.$$

In the general case, we have

$$x_i \leftrightarrow \begin{pmatrix} x_i & 0 & & 0 \\ 0 & \sigma(x_i) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \sigma^{n-1}(x_i) \end{pmatrix} \text{for all } i, \; e \leftrightarrow \begin{pmatrix} 0 & 0 & 0 & & & \gamma \\ 1 & 0 & 0 & & & 0 \\ 0 & & & \ddots & & \\ 0 & & & & 1 & 0 \end{pmatrix},$$

and for $x = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1}$, $x_i \in L$ for all $i$,

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

Consider now a codebook $\mathcal{C}$ made of matrices of the form (2). Note that $\mathcal{C}$ is linear (since $\sigma$ is). Thus

$$\det(\mathbf{X}-\mathbf{X}') = \det(\mathbf{X}),\ \mathbf{0} \neq \mathbf{X} \in \mathcal{C},\ \text{ for all } \mathbf{X} \neq \mathbf{X}' \in \mathcal{C},$$

so that $\mathcal{C}$ is fully-diverse if

$$\det(\mathbf{X}) \neq 0,\ \mathbf{X} \in \mathcal{C}.$$

Thus *cyclic division algebras*, i.e., cyclic algebras that are fields (where all nonzero elements are invertible), yield full diversity.

Let us assume that we transmit QAM information symbols. We take $K = \mathbb{Q}(i) \supset$ QAM. Each codeword carries $n^2$ information symbols, since each matrix contains $n$ coefficients $x_j$, and each $x_j$ is itself a linear combination of $n$ QAM symbols, since $L$ is a vector space of dimension $n$ over $K$.

## 2.3 Distributed space-time codes

Matrices of the form (2) are fully-diverse, however they are clearly impossible to use as such for distributed space-time coding. Indeed, an adequate codeword is such that each block of $M$ columns is obtained linearly from an $T \times M$ matrix $\mathbf{S}$, which the map $\sigma$ makes impossible. We will now see how this can be remedied. Let us start with an intuitive explanation, and assume, to start with, that the distributed codewords are square, that is $T = MR$, with $T$ the coherence time, $M$ the number of transmit antennas and $R$ the number of relays.

In order for a codeword (2) to be of the form $[A_1\mathbf{S}, \ldots, A_R\mathbf{S}]$, we need to replace the map $\sigma$ by a map, say $\tau$, such that $\tau^M = Id$, the identity map. If such a map could exist and be compatible with the algebra structure that yields full diversity, then we would set

$$\mathbf{S} = \begin{bmatrix} x_0 & \gamma\tau(x_{T-1}) & \ldots & \gamma\tau^{M-1}(x_{T-(M-1)}) \\ x_1 & \tau(x_0) & \ldots & \gamma\tau^{M-1}(x_{T-(M-2)}) \\ \vdots & & & \vdots \\ x_{T-2} & \tau(x_{T-3}) & \ldots & \tau^{M-1}(x_{T-(M+1)}) \\ x_{T-1} & \tau(x_{T-2}) & \ldots & \tau^{M-1}(x_{T-M}) \end{bmatrix}$$

$$
\begin{tikzcd}
& L \arrow[dl, dash, "R"'] \arrow[dd, dash, "T=MR"] \\
F \arrow[dr, dash, "M"'] & \\
& K=\mathbb{Q}(i)
\end{tikzcd}
$$

Figure 2: Suitable field extensions to construct a distributed $T \times T$ space-time code. The degrees are written on the branches.

and a distributed codeword would be indeed of the form $[A_1\mathbf{S}, \ldots, A_R\mathbf{S}]$ with

$$
A_i = \begin{pmatrix} 0 & 0 & \ldots & 0 & \gamma \\ 1 & 0 & & 0 & 0 \\ 0 & & \ddots & 0 & \\ 0 & 0 & & 1 & 0 \end{pmatrix}^{M(i-1)}.
$$

To prove the existence of such a map $\tau$, we recur to a standard result of Galois theory (see for example [19]) that states that if $\{\eta^j,\ j = 1, \ldots, R\}$ is a subgroup of $\{\sigma^j,\ j = 1, \ldots, MR\}$, then there exists a subfield $F$ of $L$ given by $F = \{x \in L \mid \eta(x) = x\}$, and the Galois group of $F$ over $K = \mathbb{Q}(i)$ is $\{\tau^j,\ j = 1, \ldots, M\}$. In particular $\tau^M = Id$ and $\sigma$ restricted to $F$, denoted by $\sigma|_F$, is $\tau$. This means that it is enough to restrict the coefficients of the distributed space-time codewords to $F$ instead of $L$. Figure 2 illustrates the hierarchy of the field extensions we consider.

In the next section, we describe more precisely the code construction.

# 3 Code Construction

Recall that we consider $M$ transmit antennas, $N$ receive antennas, $R$ relays and a coherence time $T$. For the purpose of code construction, we shall henceforth assume $T = MR$. In practice, of course, $M$ and $T$ are determined by the system parameters, whereas $R$ is often random and depends on the number of functioning relays available. Thus $T > MR$ or $T < MR$ may both happen. The case

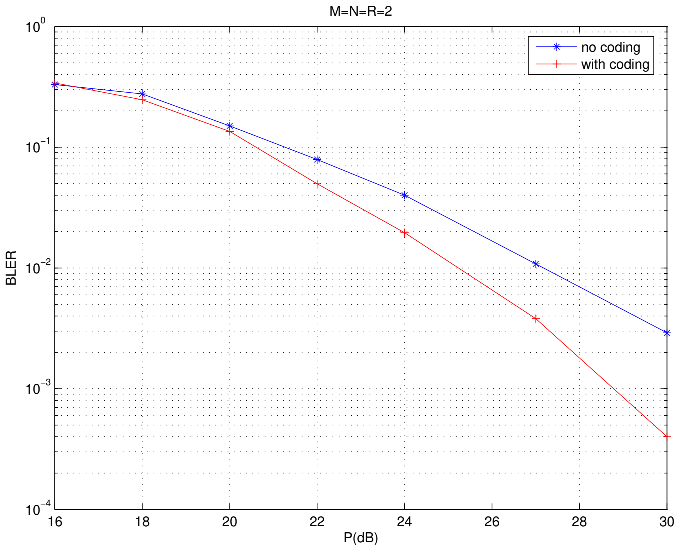


Figure 3: For $M = N = 2$ transmit and receive antennas, $R = 2$ relays, comparison of the BLER with and without coding at the transmitter. Random coding is used at the relays. We see a clear loss in the diversity when no coding is used at the transmitter.

$T > MR$ is discussed in Section 4, where we show it corresponds to having relay failures. When $T < MR$ however, the diversity is determined by $T$ (and not by $MR$, see [9]) and so the extra $R - \lfloor \frac{T}{M} \rfloor$ relay nodes do not contribute in the diversity. In this case, to save the battery power of the relays, it is best if the excess relays do not cooperate in the communications. We are therefore justified in considering $T = MR$ for the purpose of code construction.

Note that the transmitter has to send a space-time code to the relays. Otherwise, nothing prevents both antennas from sending the same signal, resulting in a loss of diversity (see Fig. 3). Our construction consists thus of two steps:

1. Construction of the space-time code at the transmitter.

2. Construction of the distributed space-time code at the relays.

### 3.1 Space-Time Code at the Transmitter

The space-time code built at the transmitter is a $T \times M$ matrix, with $\min\{M, N\}T$ information symbols $\{s_{ij}\}$, $i = 1, \ldots, \min\{M, N\}$, $j = 1, \ldots, T$. In order to obtain at the receiver a $T \times T$

distributed space-time code, we need a cyclic extension $L$ of degree $T = MR$ over $\mathbb{Q}(i)$, which contains a subextension $F$ of degree $M$ over $\mathbb{Q}(i)$ (cf. Fig. 2).

Let $\mathcal{B} = \{\theta_1, \theta_2, \ldots, \theta_M\}$ be a $\mathbb{Z}[i]$-basis of $F$, and denote by $\{\tau^j,\ j = 1, \ldots, M\}$ the Galois group of $F/\mathbb{Q}(i)$. Consider the matrix $\mathbf{M}$ defined as follows:

$$\mathbf{M} = \begin{pmatrix} \theta_1 & \theta_2 & \ldots & \theta_M \\ \tau(\theta_1) & \tau(\theta_2) & \ldots & \tau(\theta_M) \\ \vdots & & & \\ \tau^{M-1}(\theta_1) & \tau^{M-1}(\theta_2) & \ldots & \tau^{M-1}(\theta_M) \end{pmatrix}.$$

The first part of the encoding consists of applying $\mathbf{M}$ to the vectors given by $\tilde{\mathbf{s}}_j = (s_{1j}, \ldots, s_{Mj})^T$, $j = 1, \ldots, T$, as follows:

$$\mathbf{M}\tilde{\mathbf{s}}_j = (\sum_{k=1}^{M} \theta_k s_{kj}, \ldots, \sum_{k=1}^{M} \tau^{M-1}(\theta_k) s_{kj})^T.$$

Note here that if we have $N < M$, we only need $NT$ information symbols, and can just set the coefficients $s_{M-N+1,j}, \ldots, s_{M,j}$ to be zero, $j = 1, \ldots, T$. If we denote $s_j = \sum_{k=1}^{M} \theta_k s_{kj}$, we can rewrite shortly, by linearity of $\tau$,

$$\mathbf{M}\tilde{\mathbf{s}}_j = (s_j, \tau(s_j), \ldots, \tau^{M-1}(s_j))^T.$$

In order not to change the energy of the signal constellation, it is important to choose the matrix $\mathbf{M}$ to be unitary, which means taking the right basis $\mathcal{B}$. Such basis can be found by looking at $\mathbf{M}$ as the generator matrix of the lattice $\mathbb{Z}[i]^M$, and then use the theory of algebraic lattices [13]. Note that not all fields allow this construction. We thus need to choose $L$ carefully.

The second stage of the encoding consists of putting the signals $s_j, \tau(s_j), \ldots, \tau^{M-1}(s_j)$ into the space-time code to be sent. This is done as follows. Denote by $\mathbf{J}_i$ the $T \times M$ matrix containing only zeros, apart from an $M \times M$ identity matrix, whose first row is at the $i$th row of $\mathbf{J}_i$,

$$\mathbf{J}_i = \begin{pmatrix} \mathbf{0}_{i-1,M} \\ \mathbf{I}_M \\ \mathbf{0}_{T-M-(i-1),M} \end{pmatrix}.$$

Define also the matrices $\mathbf{K}_i$ similarly as $\mathbf{J}_i$, except that the index of the rows are considered modulo $T$, so that a coefficient appearing on row $T+1$ when starting the identity matrix at row $T-(M-2)$ will be on row 1. All coefficients 1 that are shifted modulo $T$ are multiplied by $\gamma$, $\gamma$ being an element of $\mathbb{Q}(i)$ such that $|\gamma|^2 = 1$. For example

$$\mathbf{K}_{T-(M-2)} = \begin{pmatrix} 0 & \dots & 0 & \gamma \\ & \mathbf{0}_{T-M,M} & & \\ & \mathbf{I}_{M-1,M} & & \end{pmatrix}.$$

The $T \times M$ space-time code sent by the transmitter is given by (see subsection 3.3 for an example)

$$\sum_{k=1}^{T-(M-1)} \mathbf{J}_k diag(s_k, \dots, \tau^{M-1}(s_k)) + \sum_{k=T-(M-2)}^{T} \mathbf{K}_k diag(s_k, \dots, \tau^{M-1}(s_k)).$$

### 3.2 Distributed Space-Time Codes at the relays

At the $j$th relay, the received signal is $\mathbf{r}_j = \sqrt{P_1 T/M} \sum_{m=1}^{M} f_{mj} \mathbf{s}_m + \mathbf{v}_j$, where $P_1$ is the average total power at the transmitter, which can be written

$$\mathbf{r}_j = \sqrt{P_1 T/M} \begin{pmatrix} s_1 & \gamma\tau(s_T) & \dots & \gamma\tau^{M-1}(s_{T-(M-2)}) \\ \vdots & & & \\ s_T & \tau(s_{T-1}) & & \tau^{M-1}(s_{T-(M-1)}) \end{pmatrix} \begin{pmatrix} f_{1j} \\ \vdots \\ f_{Mj} \end{pmatrix} + \mathbf{v}_j.$$

The $j$th relay multiplies $\mathbf{r}_j$ by $A_j$, where $A_j = \Gamma^{M(j-1)}$ and $\Gamma$ is defined as

$$\Gamma = \begin{pmatrix} 0 & 0 & \dots & 0 & \gamma \\ 1 & 0 & & 0 & 0 \\ 0 & & \ddots & 0 & \\ 0 & 0 & & 1 & 0 \end{pmatrix}. \quad (3)$$

Let us emphasize the simplicity of the encoding at the relays. Compared to random codes, multiplication by a full unitary matrix is replaced by simple shifting and scaling of the received vector.

### 3.3 A worked out example

Consider the simple case when we have $M = 2$ antennas at the transmitter, and $R = 2$ relays. By assumption, $T = 4$. The transmitter sends to the relays a space-time code, built as follows. Let $\{s_{1j}, s_{2j}\}$, $j = 1, \dots, 4$ be the 8 information symbols to be sent. Set $\zeta_{15} = e^{2i\pi/15}$. Let $L = \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}, i)$ be an extension of degree $MR = 4$ over $K = \mathbb{Q}(i)$ and let $F = \mathbb{Q}(\sqrt{5}, i)$ be a subextension of $L$ of degree $M = 2$ (see Example 1). Let $\mathcal{B} = \{1, \theta = \frac{1+\sqrt{5}}{2}\}$ be a $\mathbb{Z}[i]$-basis of $F$. Let $\tau$ be defined by $\tau : \sqrt{5} \mapsto -\sqrt{5}$. The encoding matrix is a priori given by $\begin{bmatrix} 1 & \theta \\ 1 & \tau(\theta) \end{bmatrix}$, which is not unitary. A unitary matrix $\mathbf{M}$ is obtained by multiplying $\mathcal{B}$ by $\alpha = 1 + i - i\theta$ and normalizing:

$$\mathbf{M} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha & \alpha\theta \\ \tau(\alpha) & \tau(\alpha\theta) \end{pmatrix}.$$

Thus

$$\frac{1}{\sqrt{5}} \begin{pmatrix} \alpha & \alpha\theta \\ \tau(\alpha) & \tau(\alpha\theta) \end{pmatrix} \begin{pmatrix} s_{1j} \\ s_{2j} \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha(s_{1j} + \theta s_{2j}) \\ \tau(\alpha(s_{1j} + \theta s_{2j})) \end{pmatrix} =: \begin{pmatrix} s_j \\ \tau(s_j) \end{pmatrix}, \ j = 1, \dots, 4.$$

The space-time code is given by

$$
\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}
\begin{bmatrix} s_1 & 0 \\ 0 & \tau(s_1) \end{bmatrix}
+
\begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}
\begin{bmatrix} s_2 & 0 \\ 0 & \tau(s_2) \end{bmatrix}
+
\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}
\begin{bmatrix} s_3 & 0 \\ 0 & \tau(s_3) \end{bmatrix}
+
\begin{bmatrix} 0 & i \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}
\begin{bmatrix} s_4 & 0 \\ 0 & \tau(s_4) \end{bmatrix}
$$

and the received signal at the two relays can be written as

$$
\mathbf{r}_i = \sqrt{2P_1} \begin{pmatrix} s_1 & i\tau(s_4) \\ s_2 & \tau(s_1) \\ s_3 & \tau(s_2) \\ s_4 & \tau(s_3) \end{pmatrix} \begin{pmatrix} f_{1i} \\ f_{2i} \end{pmatrix} + \mathbf{v}_i, \; i = 1, 2.
$$

The relay 1 multiplies $\mathbf{r}_1$ by $A_1 = \mathbf{I}_4$, the identity matrix and the relay 2 multiplies $\mathbf{r}_2$ by $A_2$, with

$$
A_2 = \begin{pmatrix} 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},
$$

so that

$$
A_2\mathbf{r}_2 = \sqrt{2P_1} \begin{pmatrix} is_3 & i\tau(s_2) \\ is_4 & i\tau(s_3) \\ s_1 & i\tau(s_4) \\ s_2 & \tau(s_3) \end{pmatrix} \begin{pmatrix} f_{1i} \\ f_{2i} \end{pmatrix} + \mathbf{v}_i, \; i = 1, 2.
$$

The space-time code is seen at the receiver as

$$
[A_1\mathbf{s} \;\; A_2\mathbf{s}] = \begin{pmatrix} s_1 & i\tau(s_4) & is_3 & i\tau(s_2) \\ s_2 & \tau(s_1) & is_4 & i\tau(s_3) \\ s_3 & \tau(s_2) & s_1 & i\tau(s_4) \\ s_4 & \tau(s_3) & s_2 & \tau(s_3) \end{pmatrix}. \tag{4}
$$

Let us now check that this matrix is coming from a cyclic algebra. Recall that we consider the cyclic extension $L = \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}, i)$ of degree 4 over $\mathbb{Q}(i)$, with Galois group generated by $\sigma : \zeta_{15} + \zeta_{15}^{-1} \mapsto \zeta_{15}^2 + \zeta_{15}^{-2}$. We consider the cyclic algebra $\mathcal{A} = (L/\mathbb{Q}(i), \sigma, i)$ of Example 3. An element $x \in \mathcal{A}$ can be written $x = x_0 + ex_1 + e^2x_2 + e^3x_3$, $e^4 = i$. Its corresponding matrix is given by

$$\begin{pmatrix} x_0 & i\sigma(x_3) & i\sigma^2(x_2) & i\sigma^3(x_1) \\ x_1 & \sigma(x_0) & i\sigma^2(x_3) & i\sigma^3(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & i\sigma^3(x_3) \\ x_3 & \sigma(x_2) & \sigma^2(x_1) & \sigma^3(x_0) \end{pmatrix}. \tag{5}$$

Now consider the subgroup $\{\eta = \sigma^2, \eta^2 = Id\}$. We have that $F = \{u \in L \mid \eta(u) = u\}$, which can be seen by solving explicitly this equation, which yields that $u = u_0 + u_1(\zeta_{15}^3 + \zeta_{15}^{-3})$, $u_0, u_1 \in \mathbb{Q}(i)$. Since $\zeta_{15}^3 + \zeta_{15}^{-3} = (-1 + \sqrt{5})/2$, $u \in F = \mathbb{Q}(i, \sqrt{5})$. We have that $\sigma|_{\mathbb{Q}(i,\sqrt{5})} = \tau$, and the matrix (4) is similar to (5), when the coefficients $x_i$, $i = 0, \dots, 3$ are restricted to $\mathbb{Q}(i, \sqrt{5})$. By choice of the encoding at the transmitter, the signals $s_j$, $j = 1, \dots, 4$ are encoded as elements of $\mathbb{Q}(i, \sqrt{5})$.

Since $\mathcal{A} = (L/\mathbb{Q}(i), \sigma, i)$ is a division algebra [12], this codebook is fully diverse.

### 3.4 Computation of the coding gain

Let us now compute the coding gain of the above codes. Recall from [9] that similarly to the point-to-point case, once the code is fully diverse, performance is given by the coding gain. Roughly speaking, the larger $\det(\mathbf{X}_k - \mathbf{X}_l)^*(\mathbf{X}_k - \mathbf{X}_l)$, the smaller the upper bound on the pairwise error probability. For the case when codewords are square matrices, we compute $\min |\det(\mathbf{X})|^2$, where $\mathbf{X}$ is a matrix from a distributed space-time code. It is a standard fact [15, p. 296,p. 316] that when considering the matrix representation $\mathbf{X}$ of an element $x \in \mathcal{A}$, where $\mathcal{A}$ is a $\mathbb{Q}(i)$-algebra, that the determinant belongs to $\mathbb{Q}(i)$. If furthermore the coefficients of $\mathbf{X}$ are given in a $\mathbb{Z}[i]$-basis, and $\gamma \in \mathbb{Z}[i]$, then the determinant is in $\mathbb{Z}[i]$, so that $\min |\det(\mathbf{X})|^2 \in \mathbb{Z}$. The minimum is thus 1 (it cannot be zero in a division algebra). Note that if instead with choose $\gamma = \gamma_1/\gamma_2 \in \mathbb{Q}(i)$, then the coding gain is given by $1/|\gamma_2|^{2(T-1)}$, since the denominator has to be in factor to again use the argument that all the coefficients of the matrix are in $\mathbb{Z}[i]$. The coding gain is thus clearly optimized by choosing $\gamma \in \mathbb{Z}[i]$.

In the example of subsection 3.3, we have seen that a normalizing factor for the encoding matrix $\mathbf{M}$ may be required in order to encode the information symbols with a unitary matrix. The normalizing factor depends on $L$, and is thus, with $\gamma$, a second factor influencing the coding gain. Thus $L$ has to be chosen with a normalizing factor $1/d$ where $d$ is as big as possible (see for example [13] for more details). Note that it is misleading to believe that renouncing in a unitary matrix for the encoding would improve the good performance. It would increase the minimum determinant but also change the energy of the system, and yield shaping loss which will actually deteriorate the performance of the code.

The results on diversity and coding gain discussed so far are obtained by considering only the highest order term of the power $P$ in the bound on the pairwise probability of error [9]. It is important to keep in mind that in the distributed case, not only the highest order is important, but also how dominant is it, and thus, what are the contributions of the other high order terms of $P$. The $i$th order term is obtained by dropping $i-1$ columns from the codeword, which is equivalent to saying that $i-1$ relay nodes are not transmitting. This will be discussed further in Section 4.

### 3.5 The Single antenna case

The case where the transmitter and receiver only have a single antenna is a particular case of our construction. (See Fig. 4). In this scenario, no space-time coding is required at the transmitter. Thus the signal to be transmitted is $\mathbf{s} = (s_1, \ldots, s_T)$. From time 1 to $T$, the transmitter sends the signals $\sqrt{P_1 T} s_1, \ldots, \sqrt{P_1 T} s_T$ to each relay $j$, which multiplies its received signal $\mathbf{r}_j$ by a $T \times T$ unitary matrix $A_j$ and forwards $\mathbf{t}_j$ to the receiver, which gets the signal $\mathbf{y}$, with

$$\mathbf{r}_j = \sqrt{P_1 T} f_i \mathbf{s} + \mathbf{v}_j, \;\; \mathbf{t}_j = \sqrt{\frac{P_2}{P_1 + 1}} A_j \mathbf{r}_j, \;\; \mathbf{y} = \sum_{j=1}^{R} g_j \mathbf{t}_j + \mathbf{w}.$$

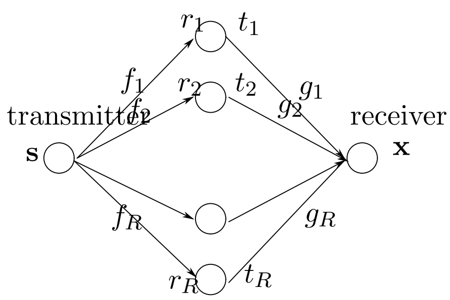


Figure 4: The wireless network with a single antenna at the transmitter and receiver.

The received signal is given by

$$\mathbf{y} = \sqrt{\frac{P_1 P_2 T}{P_1 + 1}} \mathbf{X}\mathbf{h} + \mathbf{w}', \tag{6}$$

with $\mathbf{X} = [A_1\mathbf{s} \cdots A_R\mathbf{s}]$, $\mathbf{h} = [f_1 g_1, \ldots, f_R g_R]^T$ and $\mathbf{w}' = \sqrt{\frac{P_2}{P_1+1}} \sum_{j=1}^{R} g_j A_j \mathbf{v}_j + \mathbf{w}$. The strategy described above consists here of multiplying the received signal at the $j$-th relay by the matrix $\Gamma^j$, where $\Gamma$ is given by (3). Note that in the case of $M = 1$ transmit and $N = 1$ receive antennas, the algebra structure we are considering is too heavy for our purpose, since the same coding strategy can be obtained more easily as follows [14]. Recall (see Subsection 2.3) that using $M$ transmit antennas means looking for a number field of degree $M$ over $\mathbb{Q}(i)$ in $L$. If $M = 1$, we are taking the field $\mathbb{Q}(i)$ itself. We then just need a vector space of dimension $T = R$ over $\mathbb{Q}(i)$. There is thus no need for an algebra structure. One can just take a number field which contains $\mathbb{Q}(i)$, and get as codeword the matrix of multiplication by an element $x$ of this field. Let us be more precise, and give the construction on a family of number fields called *cyclotomic fields*.

Let $\zeta = \zeta_{2^n} = e^{2i\pi/2^n}$ be a $2^n$ root of unity. We consider the *cyclotomic field* $\mathbb{Q}(\zeta)$ defined by

$$\mathbb{Q}(\zeta) = \{x = \sum_{l=0}^{2^{n-1}-1} x_l \zeta^l,\ x_l \in \mathbb{Q}\}.$$

For example, if $n = 2$, $\mathbb{Q}(\zeta) = \mathbb{Q}(i) = \{x = x_0 + ix_1,\ x_0, x_1 \in \mathbb{Q}\}$. The field $\mathbb{Q}(\zeta)$ has a structure of vector space of dimension $2^{n-1}$ over $\mathbb{Q}$. A $\mathbb{Q}$-basis is given by $\{1, \zeta, \ldots, \zeta^{2^{n-1}-1}\}$.

**Lemma 1** *For $n \geq 2$, the field $\mathbb{Q}(\zeta)$ is a vector space of dimension $2^{n-2}$ over $\mathbb{Q}(i)$.*

**Proof.** We have that every $x$ in $\mathbb{Q}(\zeta)$ can be written as

$$x = \sum_{l=0}^{2^{n-2}-1} x_l\zeta^l + \sum_{l=2^{n-2}}^{2^{n-1}-1} x_l\zeta^l = \sum_{l=0}^{2^{n-2}-1} x_l\zeta^l + \zeta^{2^{n-2}} \sum_{k=0}^{2^{n-2}-1} x_{k+2^{n-2}}\zeta^k = \sum_{l=0}^{2^{n-2}-1} (x_l + ix_{l+2^{n-2}})\zeta^l,$$

since $\zeta^{2^{n-2}}$ is a fourth root of unity. Thus a $\mathbb{Q}(i)$-basis of $\mathbb{Q}(\zeta)$ is given by

$$\{1, \zeta, \dots, \zeta^{2^{n-2}-1}\}. \tag{7}$$

■

Let $x \in \mathbb{Q}(\zeta)$, written in the $\mathbb{Q}(i)$-basis (7). We define the matrix $M_x$ of multiplication by $x$ in this $\mathbb{Q}(i)$-basis by

$$(1, \zeta, \dots, \zeta^{2^{n-2}-1})M_x = (x, x\zeta, \dots, x\zeta^{2^{n-2}-1}), \tag{8}$$

where $M_x$ has coefficients in $\mathbb{Q}(i)$.

Let $m = 2^{n-2}$. If $x = \sum_{l=0}^{m-1} x_l\zeta^l$, we have

$$x\zeta = \sum_{l=0}^{m-1} x_l\zeta^{l+1} = \sum_{l=0}^{m-2} x_l\zeta^{l+1} + ix_{m-1} = ix_{m-1} + \sum_{k=1}^{m-1} x_{k-1}\zeta^k$$

since $\zeta^m = \zeta^{2^{n-2}}$ is a fourth root of unity. Similarly,

$$x\zeta^2 = \sum_{l=0}^{m-1} x_l\zeta^{l+2} = \sum_{l=0}^{m-3} x_l\zeta^{l+2} + ix_{m-2} + ix_{m-1}\zeta = ix_{m-2} + ix_{m-1}\zeta + \sum_{k=2}^{m-1} x_{k-2}\zeta^k.$$

More generally,

$$x\zeta^t = \sum_{l=0}^{m-1} x_l\zeta^{l+t} = \sum_{l=0}^{m-t-1} x_l\zeta^{l+t} + i\sum_{l'=1}^{t} x_{m-l'}\zeta^{t-l'} = i\sum_{l'=1}^{t} x_{m-l'}\zeta^{t-l'} + \sum_{k=t}^{m-1} x_{k-t}\zeta^k.$$

We thus have that $M_x$ is given by

$$\begin{pmatrix} x_0 & ix_{m-1} & ix_{m-2} & \dots & ix_1 \\ x_1 & x_0 & ix_{m-1} & & ix_2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_{m-1} & x_{m-2} & x_{m-3} & \dots & x_0 \end{pmatrix}.$$

Let $\mathbf{S} = (x_0, \dots, x_{m-1})$ be the transmitted signal. Choose $\gamma = i$. The matrix $M_x$ can be written as

$$M_x = [\Gamma^0\mathbf{S}\ \Gamma\mathbf{S}\ \cdots\ \Gamma^{m-2}\mathbf{S}\ \Gamma^{m-1}\mathbf{S}],$$

which is exactly the space-time code we are expected at the receiver, when $M = 1$.

# 4 Resistance to node failures

Distributed space-time codes assume that $R$ relay nodes are active in the network. However, it is reasonable to consider that some nodes may be down for some period of time (for example, for limited battery). It is thus important to make sure that if such failures happen, the whole coding strategy will not collapse. Recall from (1) that the channel model can be written as

$$\mathbf{Y} = \sqrt{\frac{P_1P_2T}{(P_1+1)M}}\mathbf{XH} + \mathbf{W}, \quad \mathbf{X} = [A_1\mathbf{S}\ \ A_2\mathbf{S}\ \ \dots\ \ A_R\mathbf{S}]. \tag{9}$$

The $A_j$ are unitary matrices used at each $j$th relay to encode the signal they receive, and $\mathbf{S}$ is the space-time code sent by the transmitter. If the $j$th relay does not transmit, it is equivalent to say that it uses as matrix $A_j$ the whole zero matrix. The matrix $\mathbf{X}$ can thus be seen as a $T \times M(R-d)$ rectangular matrix, where $d$ is the number of nodes that are down during the transmission. Clearly

**Proposition 1** *The codebook of $T \times M(R-d)$ matrices $\mathbf{X}$ obtained after failures of $d$ nodes in the network is fully diverse.*

The matrix $\mathbf{H}$ in (9) is an $RM \times N$ matrix, given by $\mathbf{H} = [\mathbf{f}_1\mathbf{g}_1, \mathbf{f}_2\mathbf{g}_2, \ldots, \mathbf{f}_R\mathbf{g}_R]$. If the $j$th relay node is not communicating, the fading $\mathbf{f}_j$ is not transmitted to the receiver. The matrix $\mathbf{H}$ is thus a $(R-d)M \times N$ matrix if $d$ nodes do not transmit. In case of $d$ node failures, we can then describe our system as in (9), with a $T \times M(R-d)$ signal matrix $\mathbf{X}$. Theorem 1 holds since the code is fully diverse. Note that the receiver does not need to know which relays are down.

To summarize, we expect a diversity of $M(R-d)$, meaning that a network of $R$ nodes with $d$ node failures should behave similarly as a $R-d$ nodes network, as far as diversity is concerned.

# 5 Simulation results

This section is devoted to the simulations of the coding scheme presented. Note that the plots have on the $x$-axis the power $P$ in dB of the whole system, given by $P = P_1 + RP_2$, and on the $y$-axis the Block Error Rate. The decoding is done using the Sphere Decoder [20, 6]. In order to apply the Sphere Decoder, an equivalent channel where the matrix $\mathbf{X}$ is vectorized has to be considered, so that encoding consists of applying a matrix on a vector formed by all the information symbols.

Let us first compare our construction with a random code construction. In Fig. 5, we show how the proposed algebraic construction compares to a random code. For $M = N = 1$, we do no coding at the transmitter. At the relays, random coding consists of generating random unitary matrices. Both codes clearly achieve the same diversity, but the algebraic scheme performs better.

In Fig. 6, we again compare random coding with our construction, but when 2 antennas are used at both the transmitter and receiver. This time, we need coding at the transmitter. The random code we use is a random linear dispersion (LD)-code [7]. Let us briefly recall the encoding. Let $s_1, \ldots, s_Q$ be the $Q$ information symbols to be sent. A linear dispersion (LD) code is given by

$$S = \sum_{q=1}^{Q} (\Re(s_q)A_q + i\Im(s_q)B_q),$$

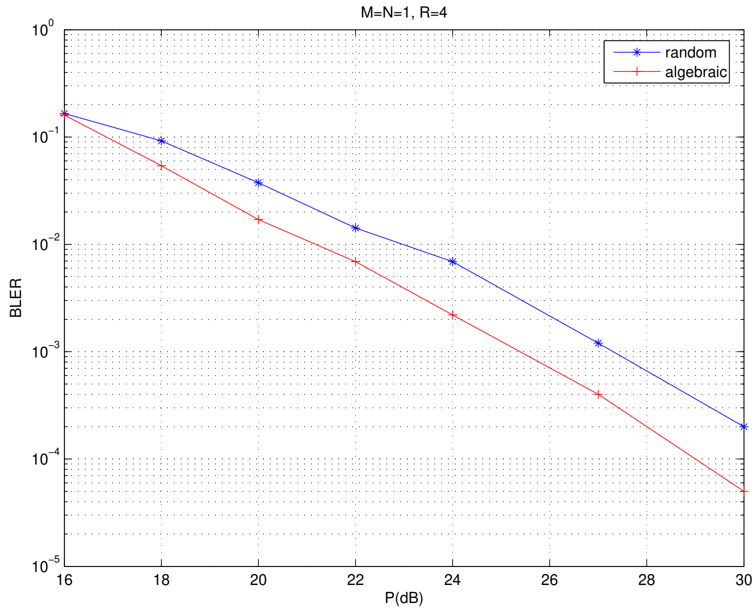


Figure 5: For $M = N = 1$ transmit and receive antennas, $R = 4$ relays, the BLER of random coding is compared to the proposed algebraic construction.

where $A_q$, $B_q$ are random $T \times M$ matrices, satisfying the following normalization constraint

$$\sum_{q=1}^{Q}(tr(A_q^* A_q) + tr(B_q^* B_q)) = 2TM.$$

Again, the algebraic and the random codes have same diversity, but the algebraic one yields a better performance. The figure also recalls the performance when no coding is used at the transmitter, that is, when the information symbols are placed as such as coefficients of the codeword.

Let us now recall (see Theorem 1) that the diversity of the network is given by

$$div = MR\left(1 - \frac{1}{M}\frac{\log\log P}{\log P}\right)$$

for $M = N$. In particular, it is linear in $R$.

In Figure 7, we simulate the simplest scenario, when we have $M = 1$ transmit antenna, and $N = 1$ receive antenna. There is no encoding at the transmitter, it is done at the relays. We

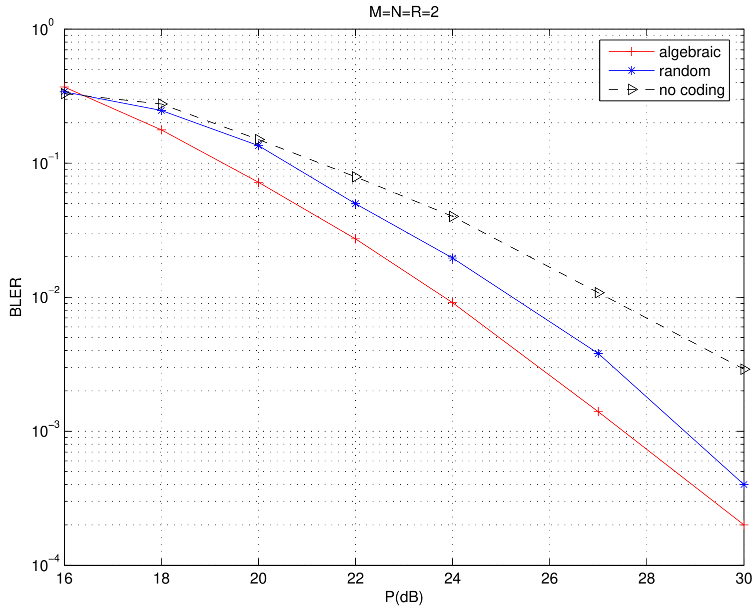


Figure 6: For $M = N = 2$ transmit and receive antennas, $R = 2$ relays, the BLER of random coding is compared to the proposed algebraic construction.

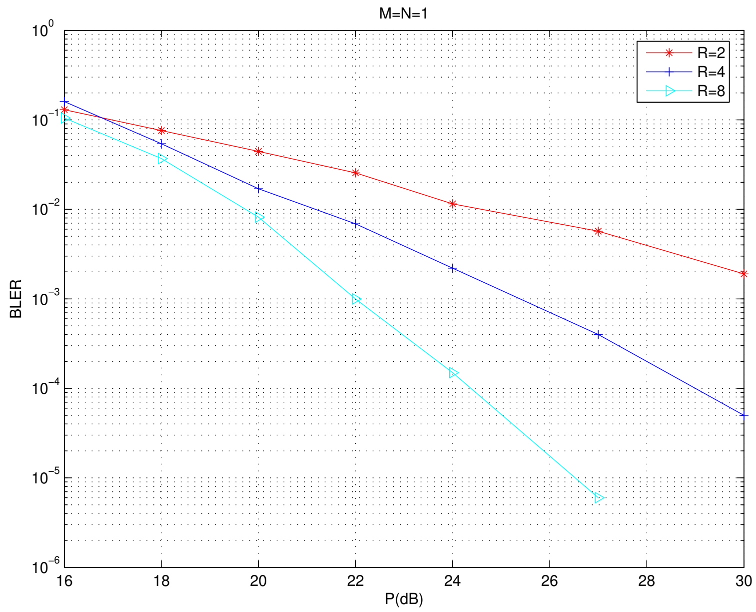


Figure 7: For $M = N = 1$ transmit and receive antennas, comparison of the BLER for $R = 2$, $R = 4$ and $R = 8$ relays.

consider $R = 2$, $R = 4$ and $R = 8$ relays, and use the codes based on cyclotomic fields described in Subsection 3.5. The diversity should be $div \approx MR$, which is here, respectively 2 and 4 for $R = 2$ and $R = 4$. Looking for example between 20 dB and 30 dB, we see that the curve for $R = 2$ decreases of roughly 1.5 magnitudes. Between 16 dB and 26 dB, the curve for $R = 4$ decreases of a bit less than 3 magnitudes. We also clearly see the diversity increasing with the number of relays.

On Figure 8, we compare transmissions with $M = 1$ and $M = 2$ antennas. For $M = 2$ and $R = 2$ relays, we use the code described in Subsection 3.3. For $M = 2$ and $R = 4$, we use the following construction. Denote by $\zeta_n$ a primitive $n$th root of unity. We choose the field $L = \mathbb{Q}(\zeta_{32})$, which is of degree $T = MR = 8$ over $\mathbb{Q}(i)$, with $K = \mathbb{Q}(\zeta_8) \subset L$, of degree $M = 2$ over $\mathbb{Q}(i)$. A choice for $\gamma$ is $\gamma = (1 + 2i)/(1 - 2i)$ (as showed in [4]). Since $M = 2$, the lattice generator matrix of $\mathbb{Z}[i]^2$ (see [2]) given by

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \zeta_8 \\ 1 & -\zeta_8 \end{pmatrix}$$

is the unitary matrix used for encoding at the transmitter. Since the diversity is $div \approx MR$, we expect the case when we use $M = 1$ antenna at the transmitter and $R = 4$ relay nodes to give the same slope as the case with $M = 2$ transmit antennas and $R = 2$ relay nodes. We indeed observe that the two corresponding curves are parallel. We also observe that for $R = 4$, the slope decreases quickly as expected.

Consider now the case when we assume that some nodes do not transmit. Recall from Section 4 that a network with $R$ relays and $d$ node failures is expected to have the same diversity order as a relay network with $R - d$ nodes. In Figure 9, we consider a network with $R = 8$ nodes, and look at its behavior if $d = 1, 2, 3, 4$ nodes are down. There is one transmit and one receive antenna. It appears clearly that the diversity decreases linearly in the number of nodes down.

In Figure 10, we compare the case when the network has 8 relay nodes but half of them do not transmit, to the case where the network has 4 relay nodes. As expected, the two networks have the same diversity. The gap between the two curves illustrates the difference of coding gain.

Finally, we consider the case where we have $M = N = 2$ transmit and receive antennas. We

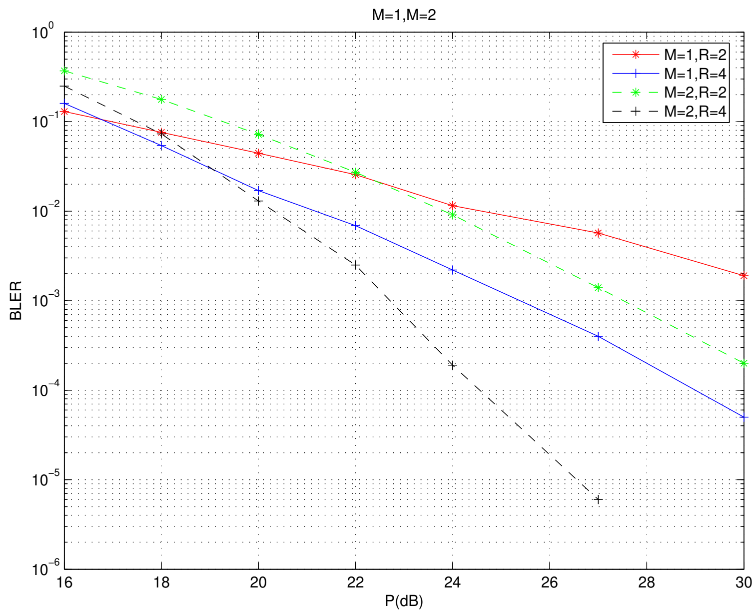


Figure 8: For $M = N = 2$ transmit and receive antennas, comparison of the BLER for $R = 2$ and $R = 4$ relays.

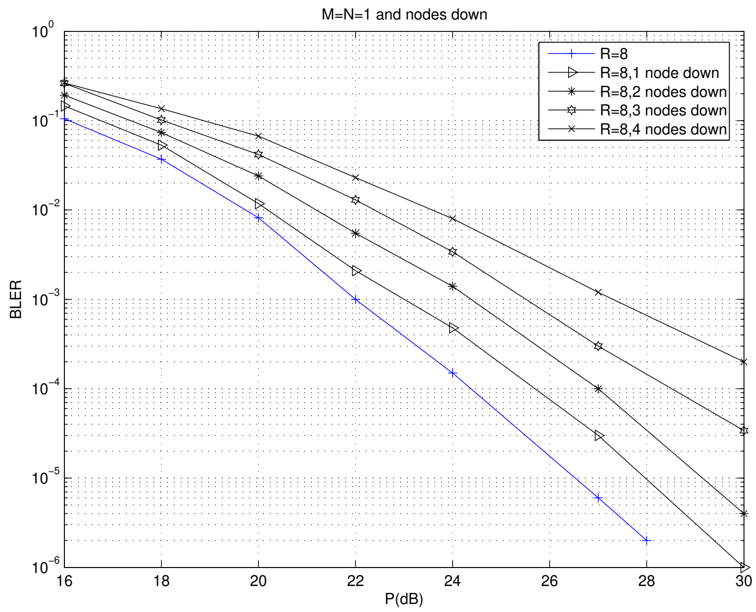


Figure 9: For $M = N = 1$ transmit and receive antennas, comparison of the BLER for $R = 8$ relays if $d = 1, 2, 3, 4$ nodes do not transmit.

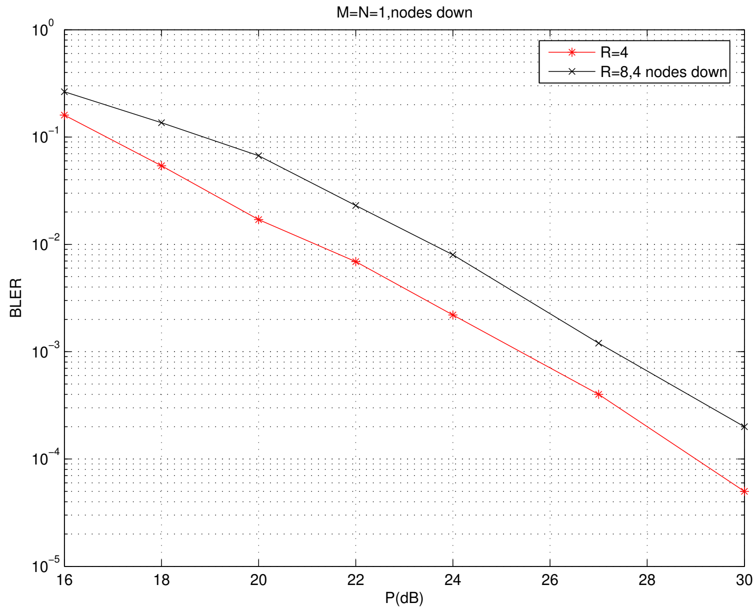


Figure 10: For $M = N = 1$ transmit and receive antennas, comparison of the BLER for $R = 4$ relays and $R = 8$ relays with half of them down.

simulate the case where in the $R = 4$ relay nodes network, one node does not transmit. We expect the diversity of the network with one node down to decrease by a factor of $dM = 2$. We observe that the diversity is in between the one of a 8 nodes network and one of a 4 nodes network.

# 6 Conclusion

In this paper, we studied the problem of coding for a half-duplex wireless relay network where both the transmitter and receiver have several antennas, while each relay has one. Due to the high transmission rate, we did not assume relays are able to decode, and thus proposed a distributed space-time scheme, where relays just do a simple operation on the received signal before forwarding it. The scheme relied on division algebra, an algebraic tool to achieve diversity. We showed how to use them to jointly optimize the design of a space-time code at the transmitter and of unitary matrices at the relays. The scheme is suitable for $M$ transmit and $N$ receive antennas, and arbitrary $R$ nodes. The code has been shown to perform better than random codes, and thus with much

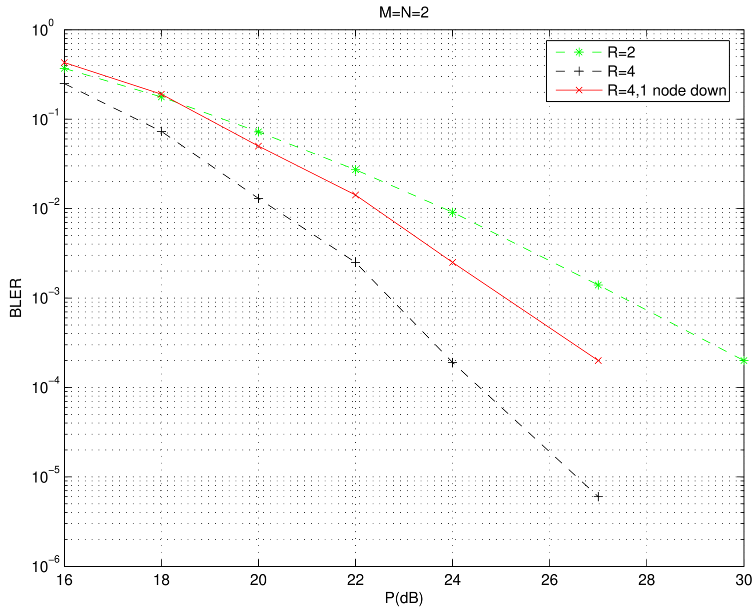


Figure 11: For $M = N = 2$ transmit and receive antennas, comparison of the BLER for $R = 2$, $R = 4$ relays, and $R = 4$ relays with one node down.

less encoding complexity. Furthermore, we considered the behavior of distributed space-time codes when facing node failures in the network. We showed that the diversity order in a network with $R$ nodes and $d$ node failures is the same as a network with $R - d$ nodes. Thus, distributed space-time coding offers a reliable coding scheme for wireless networks.

There are several directions of research one could consider at this point. An important problem is, following the space-time coding terminology, the non-coherent case. What would be a coding strategy if the receiver does not have knowledge of the channel? Channel information requires training, which is not always a practical assumption.

One generalization of the network model is to assume that there are multiple transmitter/receiver pairs in the network. The analysis and coding scheme in such a scenario are an open problem.

## References


[1] K. Azarian, H. El Gamal and P. Schniter,"On the achievable diversity-multiplexing tradeoff in half-duplex cooperative channels", *IEEE Trans. on Inf. Theory*, vol. 51, no 12, Dec. 2005.

[2] E. Bayer-Fluckiger, F. Oggier, E. Viterbo. "Algebraic lattice constellations: bounds on performance", *IEEE Trans. on Information Theory*, vol. 52, no 1,January 2006.

[3] J.-C. Belfiore, F. Oggier, E. Viterbo, "Cyclic division algebras: a tool for space-time coding", to appear in *Foundations and Trends in Communication and Information Theory*, 2007.

[4] P. Elia, B.A. Sethuraman, P.V. Kumar, "Perfect Space-Time Codes with Minimum and Non-Minimum Delay for Any Number of Antennas", in the proceedings of *International Conference on Wireless Networks, Communications and Mobile Computing*, 2005.

[5] P. Elia, P. Vijay Kumar, "Approximately universal optimality over dynamic and non-dynamic cooperative diversity strategies for wireless networks", subm. to *IEEE Trans. Inf. Theory*, Sept. 2004.

[6] B. Hassibi and H. Vikalo, "On sphere decoding algorithm. I. Expected complexity", *IEEE Trans. on Signal Processing*, vol. 53, no 8, August 2005, pp. 2806 - 2818.

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

[8] Y. Jing and B. Hassibi, "Distributed space-time coding in Wireless Relay Networks", *IEEE Transactions on Wireless Communications*, vol. 5, no 12, December 2006.

[9] Y. Jing and B. Hassibi, "Cooperative Diversity in Wireless Relay Networks with Multiple-Antenna Nodes", submitted to *IEEE Transactions on Signal Processing.*

[10] T. Kiran and B. Sundar Rajan, "Distributed space-time codes with reduced decoding complexity," in the proceedings of *ISIT 06*, Seattle.

[11] J.N. Laneman and G. W. Wornell, “Distributed space-time-coded protocols for exploiting cooperative diversity in wireless network”, *IEEE Trans. on Inf Theory*, vol. 49, Oct. 2003.

[12] F. E. Oggier, G. Rekaya, J.-C. Belfiore and E. Viterbo, ”Perfect Space-Time Block Codes”, *IEEE Trans. Inform. Theory*, vol. 52, no 9, September 2006.

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

[14] F. Oggier and B. Hassibi,“An Algebraic Family of Distributed Space-Time Codes for Wireless Relay Networks”, proceedings of *ISIT06*, Seattle.

[15] W. Scharlau, “Quadratic and Hermitian Forms”, Springer Verlag, 1985.

[16] A. Sendonaris, E. Erkip and B. Aazhang,”User cooperation diversity-part I: System description”, *IEEE Trans. on Communications*, vol. 51, pp. 1927-1938, Nov. 2003.

[17] 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, October 2003.

[18] G. Susinder Rajan, B. Sundar Rajan, “A Non-Orthogonal Distributed Space-Time Coded Protocol Part I: Signal Model and Design Criteria”, proceedings of *ITW06*, Chengdu.

[19] I. Stewart, “Galois Theory”, Chapman and Hall, 1989.

[20] E. Viterbo and J. Boutros: “A Universal Lattice Code Decoder for Fading Channels,” *IEEE Trans. on Information Theory*, vol. 45, no 5, pp. 1639–1642, July 1999.

[21] S. Yang and J.-C. Belfiore, “ Optimal space-time codes for the MIMO Amplify-and-Forward cooperative channel”, *IEEE Trans. on Inf. Theory*, vol. 53, no 2, February 2007.

[22] L. Zheng, D. Tse, “Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels,” *IEEE Trans. on Information Theory*, vol. 49, no 5, pp. 1073-1096, May 2003.