Differential Distributed Cayley Space-Time Codes

Frédérique Oggier and Emmanuel Lequeu *

April 14, 2009

Abstract

We consider a wireless relay network with no channel information, which implements differential distributed space-time coding. We propose a coding strategy based on Cayley codes, which yields high data rate codes available for an arbitrary number of relay nodes.

Keywords. differential distributed space-time coding, Cayley codes.

1 Introduction

We address the problem of designing codes for wireless relay networks with no channel information. The idea behind coding for wireless networks in general (with or without channel information) is to use the relay nodes between the sink and the source to obtain the diversity known to be achieved by multiple antenna systems [18, 11]. A huge amount of work has been done recently to propose wireless relay network coding schemes offering high diversity gain, for all kind of scenarios, e.g. amplify-and-forward protocols [1, 3], amplify-and-forward protocols with several antennas [21], distributed space-time coding [8], asynchronous cooperative diversity schemes [13], multi-hop protocols [22], to name a few.

In this work, we are interested in the case where none of the transmitter, receiver, nor relays have channel information. To deal with this situation, several authors independently suggested to adapt unitary differential space-time coding to distributed space-time coding [10, 15, 16, 9]. All the authors concluded that suitable differential codes are families of unitary commuting matrices (this will be made more precise later). Examples of such codes already in the literature are cyclic codes, namely diagonal unitary codes proposed originally for differential space-time coding [6, 5]. However the size of the codewords corresponds to the

*F. Oggier is with Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371. E-mail: frederique@ntu.edu.sg. E. Lequeu is with Chaire de Structures Algébriques et Géométriques, Ecole Polytechnique Fédérale de Lausanne, MA C3 604, Station 8, CH-1015 Lausanne. E-mail: emmanuel.lequeu@epfl.ch. Part of this work appeared in the proceedings of ISIT 2008.

number of antennas (typically smaller than 6), while in a distributed settings, it corresponds to the number of users (which can be larger than 6). Generalized constructions of cyclic codes suitable for larger number of users have been proposed in [17]. However, cyclic codes stay difficult to decode and to build for high rates. In [9], circulant codes, that is codes based on circulant matrices are proposed. In [19], differential distributed space-time coding is extended to consider scaled unitary matrices, and codes are constructed using Clifford algebras, which furthermore have low decoding complexity. They are however available for number of relays which are powers of 2.

Before going on further, let us first start by recalling the system model in which differential distributed space-time coding has been defined.

1.1 System model

We consider a wireless relay network with R half-duplex relay nodes, that we assume synchronized. The coding protocol we will now describe belongs to the family of *distributed space-time coding* protocols [8]. Note that we give the main idea and skip the details on purpose (the reader may refer to [8]). During a first phase, the source broadcasts a signal $\mathbf{s}$ to the R relays, which are equipped with a unitary matrix A_i, $i = 1, \ldots, R$, computed beforehand. Each relay receives a signal $\mathbf{r}_i$ through a SISO channel, and multiplies its received vector $\mathbf{r}_i$ by A_i, before forwarding $A_i\mathbf{r}_i$ to the sink. The sink gathers the sum of all its received signal, and it can be shown that what it senses is actually a *distributed codeword*, that is a codeword of the form

$$(A_1\mathbf{s}, \ldots, A_R\mathbf{s}),$$

called distributed since it has been encoded by both the source and the R relays. Differential modulation is now implemented as follows [15, 16]. Let $\mathbf{s}$ be a fix initial vector, and let U_j, $j = 1, \ldots, L$ be unitary codewords encoding the data to be sent. At the first step of transmission, the initial signal $\mathbf{s}$ is sent. At the next step, we send $\mathbf{s}_1 = U_1\mathbf{s}$, and more generally at the jth step,

$$\mathbf{s}_j = U_j\mathbf{s}_{j-1},$$

where $\mathbf{s}_{j-1}$ denotes the signal at time $j-1$. The corresponding distributed codeword is thus of the form

$$(A_1U\mathbf{s}, \ldots, A_RU\mathbf{s}).$$

Now assuming that $A_iU_j\mathbf{s} = U_jA_i\mathbf{s}$ for all $i = 1, \ldots, R$, $j = 1, \ldots, L$, then we have that

$$U(A_1\mathbf{s}, \ldots, A_R\mathbf{s}).$$

Using the classical idea behind differential modulation [5, 6], we can thus replace the term $(A_1U\mathbf{s}, \ldots, A_RU\mathbf{s})$ in $U(A_1U\mathbf{s}, \ldots, A_RU\mathbf{s})$ by the signal received at the previous time, and thus decode U without knowledge of the channel. The pairwise probability of this strategy has been analyzed in [15, 16], where it has been show that the full diversity criterion holds, namely $\mathcal{C} = \{U_1, \ldots, U_L\}$ has to satisfy $\det(U_l - U_{l'}) \neq 0$ for all $l \neq l'$.

The problem is similar to standard differential space-time coding, with many more constraints, since it involves the design of both unitary matrices A_i, $i = 1, \ldots, R$ and unitary codewords $\mathcal{C} = \{U_1, \ldots, U_L\}$, with the requirement that every U_j commute with every A_i. Furthermore [15, 16], the matrix $(A_1\mathbf{s}, \ldots, A_R\mathbf{s})$ is required to be unitary.

1.2 Contribution and organization

Implementing differential modulation for distributed space-time coding as described above requires the following codebook:

Definition 1 *A differential distributed space-time code consists of a codebook of unitary matrices $U_1, \ldots, U_L$ of size R satisfying the following properties :*

- *The family $\{U_l\}$ is fully-diverse.*
- *There are unitary matrices $A_1, \ldots, A_R$ of size R and a column vector $\mathbf{s}$ of length R such that the matrix $[A_1\mathbf{s}, \ldots, A_R\mathbf{s}]$ is unitary and that we have $A_iU_l\mathbf{s} = U_lA_i\mathbf{s}$, $i = 1, \ldots, R$ and $l = 1, \ldots, L$.*

Note that, for the last requirement to be satisfied, it is enough to have $A_iU_l = U_lA_i$, $i = 1, \ldots, R$ and $l = 1, \ldots, L$.

The main issue we address in this work is to design families of codes satisfying the above design criterion, which are available for any number of relays, for high rates, and which come with an efficient decoding algorithm. To do so, we present a construction based on Cayley codes [4]. We will prove that the proposed distributed Cayley codes have the following properties:

- they provide a unitary fully diverse codebook $\mathcal{C} = \{U_l,\ l = 0, \ldots, L-1\}$ (see Section 2) as well as the corresponding commuting relay matrices $\{A_i\}$, $i = 1, \ldots, R$,
- they can be built for an arbitrary number of relay nodes (see Section 3 for examples in small dimensions and Section 4 for a method to extend to higher dimensions using tensor products).

Furthermore, Cayley codes allow a linear and flexible encoding which enables high data rate, where changing the rate of the code only depends on the size of the information symbol set, and not on the encoding matrices, designed once for all for a given dimension. Finally Cayley codes can be decoded using a linearized sphere decoder algorithm [4].

The paper is organized as follows. In Section 2, Cayley codes are recalled, and a general method to design fully-diverse Cayley codes jointly with encoding matrices at the relays is proposed. Examples in small dimensions, for 2, 3 and 4 relays are detailed in Section 3. A generalization for arbitrary number of relays based on tensor product is given in Section 4. Finally, simulation results are provided in Section 5, with comparison to previously proposed codes.

2 Distributed Cayley codes

Let us start by recalling the definition of Cayley codes. Let X be a Hermitian matrix. Its unitary Cayley transform U is defined by

$$U = (\mathbf{I} + iX)^{-1}(\mathbf{I} - iX).$$

It is easy to check that U is indeed unitary. Since X is Hermitian, all its eigenvalues are real, thus all the eigenvalues of iX are complex, making sure that -1 is not an eigenvalue of iX so that $(\mathbf{I} + iX)$ is indeed invertible.

Definition 2 *A* Cayley code $\mathcal{C}$ *of cardinality* L *is thus a family of* $R \times R$ *unitary matrices* U_l *such that*

$$U_l = (\mathbf{I} + iX_l)^{-1}(\mathbf{I} - iX_l),\ l = 0, \ldots, L-1,$$

for a family $\{X_l\}$ *of Hermitian matrices.*

Let $\mathcal{A}$ be the signal set. Encoding of information symbols $\alpha_1, \ldots, \alpha_Q \in \mathcal{A}$ is done using a basis Φ_q, $q = 1, \ldots, Q$ of Hermitian matrices:

$$X_l = \sum_{q=1}^{Q} \alpha_{l,q}\Phi_q,\ l = 1, \ldots, L.$$

The rate $R_{\mathcal{C}}$ of a Cayley code is thus

$$R_{\mathcal{C}} = \frac{1}{R}\log_2 |\mathcal{A}|^Q.$$

2.1 Fully diverse Cayley codes

Cayley codes have been introduced in [4] for differential MIMO transmission. Though it has been proved in [4] that a Cayley code $\{U_l,\ l = 0, \ldots, L-1\}$ is fully diverse if and only if the family $\{X_l,\ l = 0, \ldots, L-1\}$ is fully diverse, it is only in [14] that a way to construct fully diverse Cayley codes has been provided, by designing $\{X_l,\ l = 0, \ldots, L-1\}$ from division algebras. In this work, we consider Cayley codes based on field extensions in order to similarly get fully diverse codes.

Let K/F be a Galois number field extension of degree n, and let $\{\omega_1, \ldots, \omega_n\}$ be a F-basis of K as vector space over F.

Definition 3 *The* matrix M_x of multiplication *by* x *is defined by*

$$(\omega_1, \ldots, \omega_n)M_x = x(\omega_1, \ldots, \omega_n)$$

where M_x *has coefficients in* F.

Lemma 1 *Let $\{\sigma_1;\sigma_2;\ldots;\sigma_n\}$ be the Galois group of K/F. Then we have*

$$M_x = P^{-1}\begin{pmatrix}\sigma_1(x) & & \\ & \ddots & \\ & & \sigma_n(x)\end{pmatrix}P,\ P=\begin{pmatrix}\sigma_1(\omega_1) & \ldots & \sigma_1(\omega_n)\\ & & \\ \sigma_n(\omega_1) & \ldots & \sigma_n(\omega_n)\end{pmatrix}$$

for all $x \in K$.

Proof. It is clear from the definition of M_x that

$$PM_x = \begin{pmatrix}\sigma_1(x) & & \\ & \ddots & \\ & & \sigma_n(x)\end{pmatrix}P,$$

since $\sigma_1,\ldots,\sigma_n$ are F-linear.

■

In particular, we will consider field extensions of the form $\mathbb{Q}(\zeta_{nR})/\mathbb{Q}(\zeta_n)$, where ζ_n denotes a primitive nth root of unity (say $\exp(2i\pi/n)$), such that any prime divisor of R is a prime divisor of n, obtained by considering the minimal polynomial $p(x) = x^R - \zeta_n$ over $\mathbb{Q}(\zeta_n)$. Indeed, we have the following

Proposition 1 *The polynomial $p(x) = x^R - \zeta_n$ is irreducible over $\mathbb{Q}(\zeta_n)$ if and only if any prime divisor of R is a prime divisor of n.*

Proof. The polynomial $x^R - \zeta_n$ is irreducible over $\mathbb{Q}(\zeta_n)$ if and only if the extension $\mathbb{Q}(\zeta_{nR})/\mathbb{Q}(\zeta_n)$ is of degree R. Now, the extensions $\mathbb{Q}(\zeta_{nR})/\mathbb{Q}$ and $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ are respectively of degree $\varphi(nR)$ and $\varphi(n)$, where φ denotes the Euler function. Therefore, the extension $\mathbb{Q}(\zeta_{nR})/\mathbb{Q}(\zeta_n)$ is of degree

$$\frac{\varphi(nR)}{\varphi(n)} = R\prod_q\left(1-\frac{1}{q}\right),$$

where q runs through the set of primes that divide R and do not divide n. The proposition follows.

■

Let now $x_l = x_{l,0} + x_{l,1}\zeta_{nR} + \ldots + x_{l,R-1}\zeta_{nR}^{R-1} \in K$. Its multiplication matrix is given by

$$\begin{pmatrix} x_{l,0} & \zeta_n x_{l,R-1} & \ldots & \zeta_n x_{l,1}\\ x_{l,1} & x_{l,0} & \ldots & \zeta_n x_{l,2}\\ \vdots & \vdots & & \vdots\\ x_{l,R-1} & x_{l,R-2} & \ldots & x_{l,0}\end{pmatrix}. \tag{1}$$

We consider Cayley codes where $X_l = M_{x_l}$ for some $x_l \in K$. This ensures us of a fully-diverse codebook $\mathcal{C}$, since

$$\det(X_l - X_{l'}) = \det(M_{x_l} - M_{x_{l'}}) = \det(M_{x_l - x_{l'}}) = 0 \iff x_l - x_{l'} = 0 \iff l = l'. \quad (2)$$

Hermitian matrices X_l can be found by explicitly requesting $X_l = X_l^*$. In the case of the matrix (1), the conditions are

$$x_{l,0} = x_{l,0}^*,\ \zeta_n x_{l,R-j} = x_{l,j}^*,\ j = 1, \ldots, R-1.$$

One can verify that these conditions are satisfied if and only if x_l lies in $\mathbb{R}$. This follows from

Lemma 2 *Let $x \in \mathbb{Q}(\zeta_{nR})/\mathbb{Q}(\zeta_n)$ and let M_x be its multiplication matrix as above. Then we have $M_x^* = M_{x^*}$.*

Proof. This follows from Lemma 1, using the fact that, in this case, the matrix P is such that $P^{-1} = \frac{1}{R}P^*$.

■

2.2 Commuting matrices at the relays

In order to design coding matrices at the relays, we are now interested in commuting properties of the matrices $\{X_l,\ l = 0, \ldots, L-1\}$. Note that by contrast, a Cayley code based on division algebras [14] does not have of course the property of commuting, which makes them unsuitable for designing distributed codes.

Lemma 3 *Let M_x be the matrix of multiplication by x as above and A be a matrix. If $AM_x = M_x A$, then*

$$A(\mathbf{I} - M_x)(\mathbf{I} + M_x)^{-1} = (\mathbf{I} - M_x)(\mathbf{I} + M_x)^{-1}A.$$

As a corollary to the above lemma, we get a systematic way of constructing codes as described in Definition 1.

Proposition 2 *Consider the Cayley codebook $\mathcal{C}$ of unitary matrices*

$$\{U_l = (\mathbf{I} + iM_{x_l})^{-1}(\mathbf{I} - iM_{x_l}),\ M_{x_l} \text{ as in (1)},\ l = 0, \ldots, L-1\}$$

with the condition that for all l,

$$x_{l,0} = x_{l,0}^*,\ \zeta_n x_{l,R-j} = x_{l,j}^*,\ j = 1, \ldots, R-1. \quad (3)$$

Take furthermore for the unitary coding matrices at the relays the encoding matrices

$$\{A_j = M_{x_j},\ x_j = \zeta_{Rn}^{j-1},\ j = 1, \ldots, R\}.$$

Then this code satisfies the requirements of Definition 1.

Proof. Note first that the Cayley transform is well defined since the conditions (3) yield Hermitian matrices M_{x_l} for all l.

- The family $\{U_l\}$ is fully-diverse since we consider matrices of multiplication of field elements.
- By definition, we have taken $A_j = M_{x_j},\ x_j = \zeta_{Rn}^{j-1},\ j = 1, \ldots, R$, which implies that

$$A_j = \begin{pmatrix} 0 & 0 & & & \zeta_n \\ 1 & 0 & & & 0 \\ & 1 & \ddots & & \\ & & \ddots & & \\ & & & 1 & 0 \end{pmatrix}^{j-1},$$

  which is clearly unitary. Furthermore, if we take $\mathbf{s} = (1, 0, \ldots, 0)^T$,

$$[A_1\mathbf{s},\ A_2\mathbf{s}, \ldots,\ A_R\mathbf{s}] = \mathbf{I}$$

  which is clearly unitary too.
- We have that

$$A_j U_l = U_l A_j,\ j = 1, \ldots, R, l = 0, \ldots, L-1,$$

  as a consequence of the above lemma.

■

3 Constructions in small dimensions

We now give examples of code constructions for 2,3, and 4 relays.

3.1 Codes for 2 relays

Consider the minimal polynomial $p(x) = x^2 - i$ (that is $R = 2$ and $n = 4$), defined over $F(i)$, $F \subset \mathbb{R}$. Let ζ_8 be a primitive 8th root of unity, and let $F(\zeta_8, i)/F(i)$ be a field extension with $F(i)$-basis $\{1, \zeta_8\}$. The multiplication matrix M_x of $x = x_0 + \zeta_8 x_1 \in F(\zeta_8, i)$ is given by

$$M_x = \begin{pmatrix} x_0 & ix_1 \\ x_1 & x_0 \end{pmatrix}. \tag{4}$$

For M_x to be a Hermitian matrix, we need $x_0^* = x_0$ and $x_1^* = ix_1$, that is, if we write $x_0 = a_0 + ib_0$ and $x_1 = a_1 + ib_1$, $a_0, b_0, a_1, b_1 \in F$

$$\begin{aligned} a_0 - ib_0 &= a_0 + ib_0, \\ a_1 - ib_1 &= i(a_1 + ib_1). \end{aligned}$$

This yields $b_0 = 0$ and $a_1 = -b_1$, which gives the Hermitian multiplication matrix

$$\begin{pmatrix} a_0 & ia_1(1-i) \\ a_1(1-i) & a_0 \end{pmatrix},\ a_0, a_1 \in F. \tag{5}$$

A Cayley codebook is obtained by considering the Cayley transform of the Hermitian matrices (5).

The encoding matrices at the relays are

$$A_1 = \mathbf{I}_2,\ A_2 = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}.$$

In the above construction, the encoding of the information symbols a_0, a_1 is done as follows:

$$X = a_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_1 \begin{pmatrix} 0 & i(1-i) \\ 1-i & 0 \end{pmatrix}.$$

Thus, if a_0, a_1 take value in a set $\mathcal{A} \subset F$, the rate $R_{\mathcal{C}}$ of the code is

$$R_{\mathcal{C}} = \frac{1}{2}\log_2 |\mathcal{A}|^2 = \log_2 |\mathcal{A}|.$$

An alternative construction is given by taking the minimal polynomial $p(x) = x^2 + \zeta_3$ (that is $R = 2$ and $n = 6$) over $F(\zeta_3)$. By similar computations as above, we get that a Hermitian multiplication matrix is given by

$$\begin{pmatrix} a_0 & -\zeta_3 b_1(2+\zeta_3) \\ b_1(2+\zeta_3) & a_0 \end{pmatrix},\ a_0, b_1 \in F \subset \mathbb{R},$$

for which suitable encoding matrices at the relays are

$$A_1 = \mathbf{I}_2,\ A_2 = \begin{pmatrix} 0 & -\zeta_3 \\ 1 & 0 \end{pmatrix}.$$

3.2 Codes for 3 relays

Let ζ_3 be a primitive 3rd root of unity. Consider the minimal polynomial $p(x) = x^3 - \zeta_3$ (that is $R = 3$ and $n = 3$), defined over $F(\zeta_3)$, $F \subset \mathbb{R}$, and let θ be such that $p(\theta) = 0$. Consider now the field extension $F(\theta, \zeta_3)/F(\zeta_3)$, with $F(\zeta_3)$-basis $\{1, \theta, \theta^2\}$. Let $x = x_0 + \theta x_1 + \theta^2 x_2 \in F(\theta, \zeta_3)$, and let M_x be its multiplication matrix given by

$$M_x = \begin{pmatrix} x_0 & \zeta_3 x_2 & \zeta_3 x_1 \\ x_1 & x_0 & \zeta_3 x_2 \\ x_2 & x_1 & x_0 \end{pmatrix}. \tag{6}$$

We write $x_j = a_j + \zeta_3 b_j$, $a_j, b_j \in F$, $j = 1, 2, 3$. It is easy to check that the matrix M_x of (6) is Hermitian if and only if the following two conditions hold: $x_0^* = x_0$ and $x_1^* = \zeta_3 x_2$, namely

$$b_0 = 0,\ a_2 = -a_1,\ b_2 = b_1 - a_1.$$

This yields $x_0 = a_0$ $x_1 = a_1 + \zeta_3 b_1$ $x_2 = -a_1 + (b_1 - a_1)\zeta_3$. We thus obtain the following family of Hermitian matrices

$$\begin{pmatrix} a_0 & a_1 - b_1 - \zeta_3 b_1 & -b_1 + (a_1 - b_1)\zeta_3 \\ a_1 + \zeta_3 b_1 & a_0 & a_1 - b_1 - \zeta_3 b_1 \\ -a_1 + (b_1 - a_1)\zeta_3 & a_1 + \zeta_3 b_1 & a_0 \end{pmatrix} \tag{7}$$

for all $a_0, a_1, b_1 \in F$. A Cayley codebook is obtained by considering the Cayley transform of the Hermitian matrices (7).

We take for unitary matrices at the relays

$$A_1 = \mathbf{I}_3,\ A_2 = \begin{pmatrix} 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3 \\ 1 & 0 & 0 \end{pmatrix},\ A_3 = \begin{pmatrix} 0 & 0 & \zeta_3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

If the information symbols a_0, a_1, b_1 take value in a set $\mathcal{A} \subset F$, the rate $R_{\mathcal{C}}$ of the code is

$$R_{\mathcal{C}} = \frac{1}{3}\log_2 |\mathcal{A}|^3 = \log_2 |\mathcal{A}|.$$

Consider now the minimal polynomial $p(x) = x^3 - \zeta_9$ (that is $R = 3$ and $n = 9$) defined over $F(\zeta_9)$. By repeating similar computations as above, we find that a Hermitian multiplication matrix is given by

$$\sum_{k=0}^{5} a_0 H_k + \sum_{j=0}^{2} b_0 (\zeta_9 + \zeta_9^{-1})^j$$

where

$$H_k = \begin{pmatrix} 0 & \zeta^{-k} & \zeta^{k+1} \\ \zeta^k & 0 & \zeta^{-k} \\ \zeta^{-k-1} & \zeta^k & 0 \end{pmatrix},\ \zeta = \zeta_9,\ k = 0, \ldots, 5.$$

The rate $R_{\mathcal{C}}$ of this new code is now

$$R_{\mathcal{C}} = \frac{1}{3}\log_2 |\mathcal{A}|^9 = 3\log_2 |\mathcal{A}|.$$

3.3 Codes for 4 relays

We consider the minimal polynomial $p(x) = x^4 - i$ over $F(i)$. A Hermitian multiplication matrix is given by

$$\begin{pmatrix} a_0 & -i(b_1 + ia_1) & a_2(i-1) & i(a_1 + ib_1) \\ a_1 + ib_1 & a_0 & -i(b_1 + ia_1) & a_2(i-1) \\ a_2(1+i) & a_1 + ib_1 & a_0 & -i(b_1 + ia_1) \\ -(b_1 + ia_1) & a_2(1+i) & a_1 + ib_1 & a_0 \end{pmatrix},\ a_0, a_1, a_2, b_1 \in F$$

yielding a rate of $\log_2 |\mathcal{A}|$.

Alternatively, consider the minimal polynomial $p(x) = x^4 - \zeta_8$ over $F(\zeta_8)$. A Hermitian multiplication matrix can be computed similarly as above, which yields a basis of 8 Hermitian matrices as follows:

$$\mathbf{I}_4, (\zeta_8 + \zeta_8^{-1})\mathbf{I}_4,$$

corresponding to the diagonal elements being real,

$$\begin{pmatrix} 0 & 1 & 0 & \zeta_8 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -\zeta_8^3 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -\zeta_8^3 & 0 & \zeta_8^2 \\ \zeta_8 & 0 & -\zeta_8^3 & 0 \\ 0 & \zeta_8 & 0 & -\zeta_8^3 \\ -\zeta_8^2 & 0 & \zeta_8 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & -\zeta_8^2 & 0 & \zeta_8^3 \\ \zeta_8^2 & 0 & -\zeta_8^2 & 0 \\ 0 & \zeta_8^2 & 0 & -\zeta_8^2 \\ -\zeta_8 & 0 & \zeta_8^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -\zeta_8 & 0 & -1 \\ \zeta_8^3 & 0 & -\zeta_8 & 0 \\ 0 & \zeta_8^3 & 0 & -\zeta_8 \\ -1 & 0 & \zeta_8^3 & 0 \end{pmatrix},$$

and finally

$$\begin{pmatrix} 0 & 0 & 1+\zeta_8^3 & 0 \\ 0 & 0 & 0 & 1+\zeta_8^3 \\ 1-\zeta_8^3 & 0 & 0 & 0 \\ 0 & 1-\zeta_8^3 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \zeta_8^2-\zeta_8^3 & 0 \\ 0 & 0 & 0 & \zeta_8^2-\zeta_8^3 \\ \zeta_8-\zeta_8^2 & 0 & 0 & 0 \\ 0 & \zeta_8-\zeta_8^2 & 0 & 0 \end{pmatrix}.$$

This yields a rate of $2\log_2|\mathcal{A}|$.

4 Generalization to higher dimensions

In this section, we explain how to extend our code constructions in higher dimensions (that is for higher number of relays), using Kronecker's product of matrices.

4.1 A construction using tensor product

Let $A = (a_{i,j})$ and $B = (b_{k,l})$ be two matrices of size $n \times p$ and $m \times q$ respectively. Recall that the Kronecker's product of A and B, denoted $A \otimes B$, is the matrix $C = (c_{(i,k),(j,l)})$ of size $nm \times pq$ whose coefficients are defined by

$$c_{(i,k),(j,l)} = a_{i,j}b_{k,l},$$

the pairs (i,j) and (k,l) being ordered with lexicographic order.

Suppose we have two codebooks given respectively by

$$\{U_l = (\mathbf{I} + iX_l)^{-1}(\mathbf{I} - iX_l), l = 1, \ldots, L\}$$

of size R associated with relay matrices $A_1, \ldots, A_R$ and a column vector $\mathbf{s}$ of length R, and

$$\{V_m = (\mathbf{I} + iY_m)^{-1}(\mathbf{I} - iY_m), m = 1, \ldots, M\}$$

of size P associated with relay matrices $B_1, \ldots, B_P$ and a column vector $\mathbf{t}$ of length P, both satisfying the code design of Definition 1 (in particular we do require $A_i U_l = U_l A_i$, $i = 1, \ldots, R$, $l = 1, \ldots, L$ and $B_j V_m = V_m B_j$ $j = 1, \ldots, P$, $m = 1, \ldots, M$). We propose a construction of codes by tensor products as follows. Let $\{X_l, l = 1, \ldots, L\}$ and $\{Y_m, m = 1, \ldots, M\}$ be the two families of Hermitian matrices above. Consider the family

$$\{X_l \otimes Y_m, l = 1, \ldots, L, m = 1, \ldots, M\}$$

of Hermitian matrices. We consider for unitary matrices the Cayley transform of the above family, that is

$$\{W_{l,m} = (\mathbf{I} + iX_l \otimes Y_m)^{-1}(\mathbf{I} - iX_l \otimes Y_m), l = 1, \ldots, L, m = 1, \ldots, M\}.$$

Matrices at the relays are given by

$$C_{i,j} = A_i \otimes B_j,\ i = 1, \ldots, R,\ j = 1, \ldots, P,$$

and the initial transmitted vector is

$$\mathbf{u} = \mathbf{s} \otimes \mathbf{t}.$$

Lemma 4 *The above construction satisfies:*

1. *the matrices $W_{1,1}, \ldots, W_{L,M}$ are unitary ;*
2. *the matrix $[C_{1,1}\mathbf{u}, \ldots, C_{R,P}\mathbf{u}]$ is unitary ;*
3. *we have $C_{i,j}W_{l,m}\mathbf{u} = W_{l,m}C_{i,j}\mathbf{u}$, $i = 1, \ldots, R$, $j = 1, \ldots, P$ and $l = 1, \ldots, L$, $m = 1, \ldots, M$.*

Proof.

1. This is immediate by construction.
2. The proof is elementary from the definition of tensor product (though a little bit tedious).
3. We now check that $C_{i,j}W_{l,m} = W_{l,m}C_{i,j}$, where $C_{i,j} = A_i \otimes B_j$, $i = 1, \ldots, R$, $j = 1, \ldots, P$. First note that

$$C_{i,j}W_{l,m} = W_{l,m}C_{i,j} \iff C_{i,j}(X_l \otimes Y_m) = (X_l \otimes Y_m)C_{i,j}.$$

But it is now easy to see that

$$\begin{aligned} C_{i,j}(X_l \otimes Y_m) &= (A_i \otimes B_j)(X_l \otimes Y_m) \\ &= A_i X_l \otimes B_j Y_m \\ &= X_l A_i \otimes Y_m B_j \\ &= (X_l \otimes Y_m) C_{i,j}, \end{aligned}$$

where the third equality comes from the construction of the Cayley codes $U_1, \ldots, U_L$ and $V_1, \ldots, V_M$.

■

Let us now comment on encoding and decoding of the tensor product construction. For the encoding, we have that

$$X_l = \sum_{q=1}^{Q} \alpha_{l,q} \Phi_q, \; Y_m = \sum_{s=1}^{S} \beta_{m,s} \Psi_s$$

so that

$$\begin{aligned} X_l \otimes Y_m &= \sum_{q=1}^{Q} \alpha_{l,q} \Phi_q \otimes \sum_{s=1}^{S} \beta_{m,s} \Psi_s \\ &= \sum_{q=1}^{Q} \sum_{s=1}^{S} \alpha_{l,q} \beta_{m,s} (\Phi_q \otimes \Psi_s). \end{aligned}$$

We thus have a basis of QS Hermitian matrices to encode QS information symbols $\alpha_{l,q}\beta_{m,s}$, $s = 1, \ldots, S, q = 1, \ldots, Q$.

Since the codewords $W_{l,m}$ are obtained from a Cayley transform on a Hermitian matrix $X_l \otimes Y_m$, the Cayley code decoding as described in [4] applies.

We have therefore seen that this codebook in dimension RP satisfies all the code design properties, except the full-diversity property. In general, the family of matrices $\{W_{l,m}\}$ is not fully-diverse. It then remains to know in which cases full-diversity holds.

Proposition 3 *Consider two codebooks $\{U_l\}_{l=1}^{L}$ and $\{V_m\}_{m=1}^{M}$ that are constituted of the Cayley transforms of Hermitian multiplication matrices associated to elements of two linearly disjoint extensions of a same field K. Then the above construction is fully-diverse if in one of the two codebooks, any two different matrices are linearly independent over K.*

Proof. We want to prove that the codebook

$$\{W_{l,m} = (\mathbf{I} + iX_l \otimes Y_m)^{-1}(\mathbf{I} - iX_l \otimes Y_m), l = 1, \ldots, L, m = 1, \ldots, M\}$$

is fully diverse under the assumption stated above.

For that, we need to know when $\det(W_{l,m} - W_{l',m'}) = 0$, for which it is enough to consider $\det(X_l \otimes Y_m - X'_l \otimes Y'_m) = 0$. By construction, X_l, X'_l and Y_m, Y'_m are multiplication matrices of respectively the field E and E', so that $X_l \otimes Y_m$ and $X'_l \otimes Y'_m$ are again multiplication matrices, this time of $E \otimes E'$.

It is a well-known fact (see for example in [12]) that the tensor product of two linearly disjoint extensions of a same field is again a field, so that $X_l \otimes Y_m$ is a multiplication matrix of a field. Similarly to (2), we have that

$$\det(X_l \otimes Y_m - X'_l \otimes Y'_m) = 0$$

implies $X_l \otimes Y_m - X'_l \otimes Y'_m = 0$. Now if X_l is linearly dependent of X'_l, we have that $X_l = \alpha X'_l$, and $X_l \otimes Y_m = \alpha X'_l \otimes Y_m = X'_l \otimes \alpha Y_m$. Thus if there exists Y'_m such that $Y'_m = \alpha Y_m$, we have that $X_l \otimes Y_m = X'_l \otimes Y'_m$, without having $(X_l, Y_m) = (X'_l, Y'_m)$, hence the assumption on the linear independence to guarantee full-diversity.

■

4.2 Examples

We now illustrate the above construction with a small example. Set $K = F(i, \zeta_3)$, with $F \subset \mathbb{R}$, and consider the following two field extensions: $E = K(\zeta_9)$ and $E' = K(\zeta_8)$, on which we respectively build the construction for 2 and 3 relays as in Subsection 3. Recall that the chosen Hermitian multiplication matrices for E' are given by

$$\begin{pmatrix} a_0 & ia_1(1-i) \\ a_1(1-i) & a_0 \end{pmatrix}, \tag{8}$$

while, for E, they are given by

$$\begin{pmatrix} a_0 & a_1 - b_1 - \zeta_3 b_1 & -b_1 + (a_1 - b_1)\zeta_3 \\ a_1 + \zeta_3 b_1 & a_0 & a_1 - b_1 - \zeta_3 b_1 \\ -a_1 + (b_1 - a_1)\zeta_3 & a_1 + \zeta_3 b_1 & a_0 \end{pmatrix}. \tag{9}$$

We now have

- a family of unitary matrices $U_1, \ldots, U_L$ of size 2, obtained by taking the Cayley transform of the matrices (8), 2 unitary matrices A_1, A_2, and a column vector $\mathbf{s} = (1, 0)^T$.
- a family of unitary matrices $V_1, \ldots, V_M$ of size 3, obtained by taking the Cayley transform of the matrices (9), with the corresponding unitary matrices B_1, B_2, B_3 of size 3 and a column vector $\mathbf{t} = (1, 0, 0)^T$.

The corresponding codebook for 6 relays is then obtained by taking the tensor product of the two above codebooks, as described above. Similarly, the matrices used at the relays are given by

$$C_{1,1} = A_1 \otimes B_1,\ C_{1,2} = A_1 \otimes B_2, C_{1,3} = \ A_1 \otimes B_3,$$

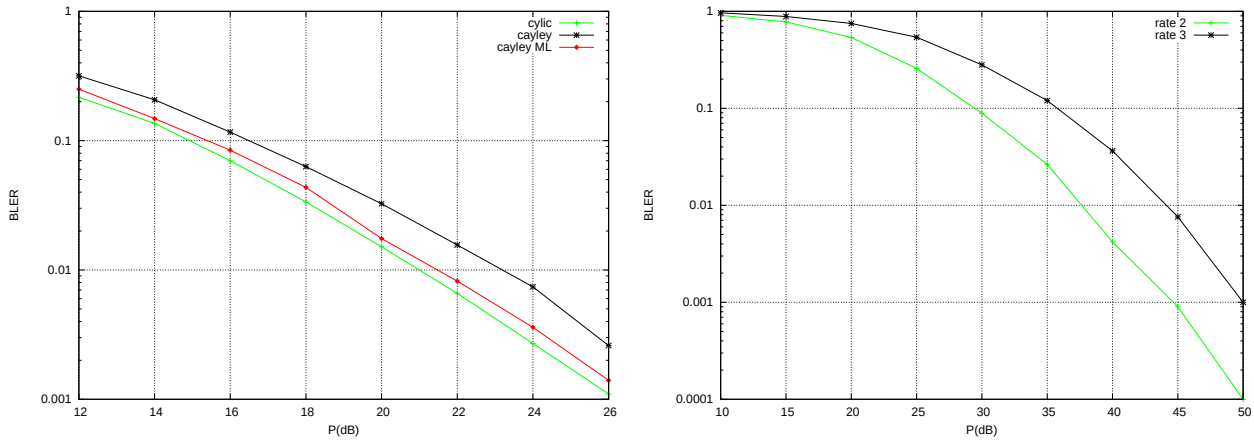

Figure 1: With 3 relay nodes, on the left, comparison between a cyclic code of rate 1, and a Cayley code of rate 1, decoded with maximum likelihood and linearized sphere decoder, on the right, Cayley codes at higher rates.

$$C_{2,1} = \ A_2 \otimes B_1, C_{2,2} = \ A_2 \otimes B_2, C_{2,3} = \ A_2 \otimes B_3,$$

with A_1, A_2 as above and

$$B_1 = \mathbf{I}_3, \ B_2 = \begin{pmatrix} 0 & 0 & \zeta_3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \ B_3 = \begin{pmatrix} 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3 \\ 1 & 0 & 0 \end{pmatrix}.$$

Finally, the matrix

$$[C_{1,1}\mathbf{u}, \ C_{1,2}\mathbf{u}, \ C_{1,3}\mathbf{u}, \ C_{2,1}\mathbf{u}, \ C_{1,2}\mathbf{u}, \ C_{2,3}\mathbf{u}]$$

can be checked to be unitary, with $\mathbf{u} = \mathbf{s} \otimes \mathbf{t}$.

5 Simulation results

We provide simulation results for the proposed constructions.

Plots show on the x-axis the average power P of the network, and on the y-axis the block error rate (BLER) or codeword error rate. By rate of the code, we recall that we mean

$$\frac{1}{M} \log_2 L,$$

while, to allow comparison with [19], the corresponding rate in bits per channel use is given by

$$\frac{1}{2M} \log_2 L.$$

All simulations are done using a linear sphere decoder algorithm, unless stated otherwise.

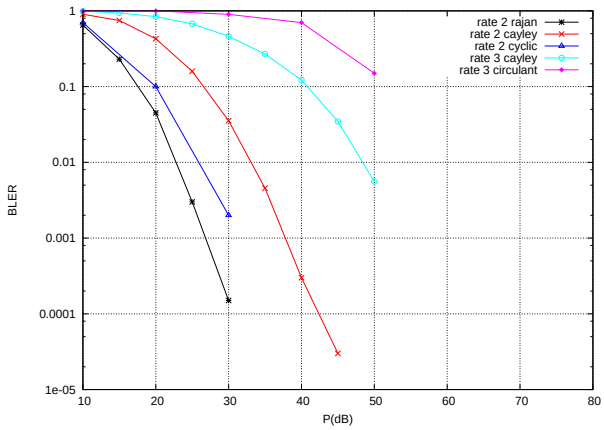

Figure 2: With 4 relay nodes, comparison among different codes at rate 2 and 3.

On Figure 5, we have simulated codes for 3 relay nodes. On the left, the cyclic code

$$\mathcal{C} = \left\{ \begin{pmatrix} \zeta_8 & 0 & 0 \\ 0 & \zeta_8 & 0 \\ 0 & 0 & \zeta_8^3 \end{pmatrix}^l \mid l = 0, \ldots, 7 \right\}$$

of rate 1 is compared to the first Cayley code of Subsection 3.2. The Cayley code is decoded once with exhaustive search (yielding a maximum likelihood decoder) and once with a linearized sphere decoder. We can observe how much is lost by using a linearized sphere decoder. The performance of the Cayley code is very similar to the one of the cyclic code.On the right of Figure 5, Cayley codes at rate 2 and 3 are shown.

The design criterion we have considered is based on full diversity and not on coding gain. There are different ways of optimizing Cayley codes [4] which are beyond the scope of this work. However, this is natural to wonder how the proposed codes behave with respect to codes in the literature. On Figure 5, we compare the second code of Subsection 3.3 with the code of [19] and a code proposed in [9]. Clearly the code of Rajan et al. outperforms all the other codes, thanks to the work done for optimizing its coding gain. However though we do no work on the coding gain, the proposed code still outperforms the circulant code of [9].

6 Conclusion

In this work, we studied the design of Cayley codes for application to differential distributed space-time coding for wireless relay networks with no channel information. We gave a general construction for an arbitrary number of relays, which is fully-diverse, and available at high data rate.

Acknowledgments

The work of Frédérique Oggier is supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03. Most of this work was done when F. Oggier was visiting Research Center on Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan. She thanks RCIS for supporting this work during her stay.

References

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

[2] K. L. Clarkson, W. Sweldens and A. Zheng,"Fast Multiple Antenna Differential Decoding", *IEEE Trans. Commun.*, vol. 49, no 2, 2001.

[3] P. Dayal and M. K. Varanasi,"Distributed QAM-Based Space-Time Block Codes for Efficient Cooperative Multiple-Access Communication", submitted to *IEEE Trans. on Information Theory*, March 2006.

[4] B. Hassibi and B. Hochwald,"Cayley Differential Unitary Space-Time Codes", *IEEE Trans. on Information Theory*, vol.48, June 2002.

[5] B.M. Hochwald, W. Sweldens, "Differential unitary space-time modulation", *IEEE Trans. on Comm.*, Volume 48, Issue 12, Dec. 2000.

[6] B.L. Hughes, "Differential Space-Time Modulation", *IEEE Trans. on Inf. Theory*, Volume 46, Issue 7, Nov. 2000.

[7] B.L. Hughes, "Optimal Space-Time Constellations From Groups", *IEEE Trans. on Inf. Theory*, Volume 49, Issue 2, Feb. 2003.

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

[9] Y. Jing and H. Jafarkhani, " Distributed Differential Space-Time Coding for Wireless Relay Networks", to appear in *IEEE Trans. on Communications*, 2007.

[10] T. Kiran and B. Sundar Rajan, " Partially-coherent distributed space-time codes with differential encoder and decoder," *IEEE Journal on Selected Areas in Communications: Special issue on Cooperative Communications and Networking*, Vol.25, No.2, Feb. 2007, pp.426-433.

[11] J. N. Laneman and G. W. Wornell, "Distributed Space-Time Coded Protocols for Exploiting Cooperative Diversity in Wireless Networks," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2415-2525, Oct. 2003.

[12] S. Lang, "Algebra", *Graduate Texts in Mathematics*, vol. 211, third edition, Springer-Verlag, New York, 2002.

[13] Y. Li and X.-G. Xia, "A family of distributed space-time trellis codes with asynchronous cooperative diversity", *Proceedings of Fourth International Symposium on Information Processing in Sensor Networks*, April 2005.

[14] F. Oggier, B. Hassibi,"Algebraic Cayley differential Space-Time Codes", *IEEE Transactions on Information Theory*, vol. 53, no. 5, May 2007.

[15] F. Oggier and B. Hassibi,"A Coding Strategy for Wireless Networks with no Channel Information",*Allerton conference 2006*.

[16] F. Oggier and B. Hassibi, "Cyclic Distributed Space-Time Codes for Wireless Relay Networks with no Channel Information", submitted to *IEEE Trans. on Inf. Theory*, March 2007.

[17] F. Oggier, "Design of Algebraic Cyclic Codes", proceedings of *ITW08*.

[18] A. Sendonaris, E. Erkikp and B. Aazhang, "User cooperation diversity-Part I: System Description", *IEEE Transactions on Communications*, vol. 51, November 2003.

[19] G. Susinder Rajan and B. Sundar Rajan, "Algebraic Distributed Differential Space-Time Codes with Low Decoding Complexity," to appear in *IEEE Transactions on Wireless Communications*, 2008.

[20] A. Shokrollahi, B. Hassibi, B.M. Hochwald, W. Sweldens, "Representation theory for high-rate multiple antenna code design", *IEEE Trans. on Inf. Theory*, Volume 47, Issue 6, Sept. 2001.

[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] S. Yang and J.-C. and Belfiore, "Distributed Space-Time Codes for the Multi-Hop Channel", *Proceedings of International workshop on wireless networks: communication, cooperation and competition (WNC3), Greece*", 2007.