

Cyclic algebras: a tool for Space-Time Coding

CMI seminar, Caltech

January 20th, 2005

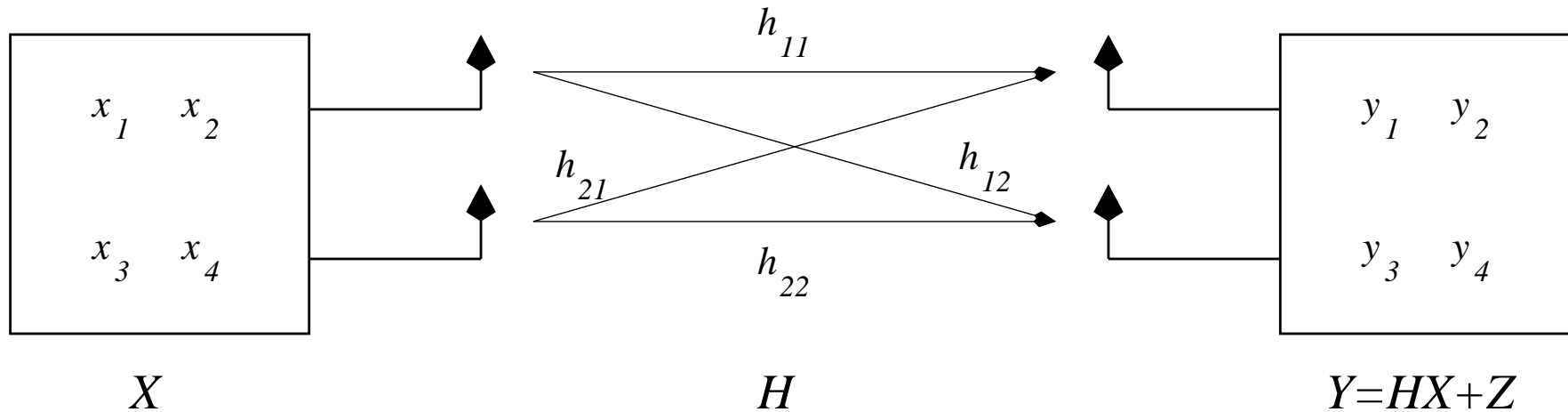
Frédérique Oggier

joint work with

Jean-Claude Belfiore and Ghaya Rekaya, ENST, Paris, France

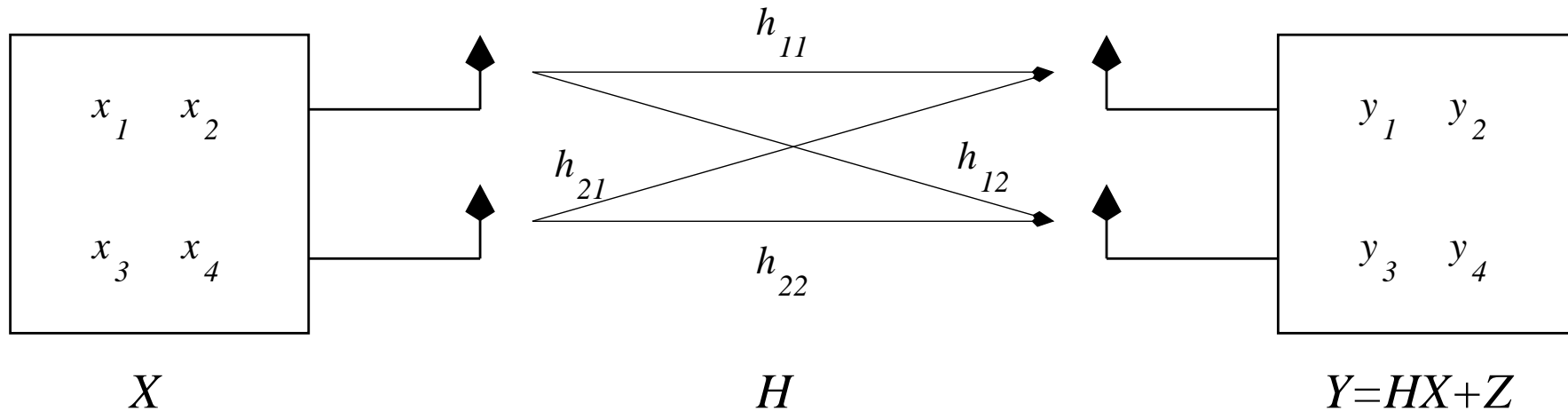
Emanuele Viterbo, Politecnico di Torino, Torino, Italy

The problem we are interested in



- ▶ Codes for multiple antennas, with M transmit and M receive antennas.
- ▶ Also called *Space-Time Codes*.

The 2×2 MIMO channel



- ▶ X : 2×2 matrix *codeword* from a *space-time code*

$$\mathcal{C} = \left\{ \mathbf{X} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \mid x_1, x_2, x_3, x_4 \in \mathbb{C} \right\}$$

the x_i are functions of the information symbols taken from a constellation S (e.g. PSK, QAM).

- ▶ H : 2×2 *channel matrix* is a complex Gaussian matrix with independent, zero mean, entries.
- ▶ Z : 2×2 *complex Gaussian noise* matrix.

The code design

The goal is the design of the **codebook** \mathcal{C} :

$$\mathcal{C} = \left\{ \mathbf{X} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \mid x_1, x_2, x_3, x_4 \in \mathbb{C} \right\}$$

the x_i are functions of the information symbols taken from a constellation S (e.g. PSK, QAM).

- ▶ The *pairwise probability of error* of sending \mathbf{X} and decoding $\hat{\mathbf{X}} \neq \mathbf{X}$ is upper bounded by

$$P(\mathbf{X} \rightarrow \hat{\mathbf{X}}) \leq \frac{\text{const}}{|\det(\mathbf{X} - \hat{\mathbf{X}})|^{2M}}.$$

- ▶ We assume the receiver knows the channel (this is called the *coherent case*).

A simplified problem

Find a family \mathcal{C} of $M \times M$ matrices such that

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

A simplified problem

- ▶ Find a family \mathcal{C} of $M \times M$ matrices such that

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

Such a family \mathcal{C} is said *fully-diverse*.

- ▶ Furthermore

$$|\det(\mathbf{X}_i - \mathbf{X}_j)|^2 \geq \text{const}, \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}.$$

The idea behind division algebras

- ▶ The difficulty in building \mathcal{C} such that

$$\det(\mathbf{X}_i - \mathbf{X}_j) \neq 0, \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C},$$

comes from the *non-linearity* of the determinant.

- ▶ An algebra of matrices is *linear*, so that

$$\det(\mathbf{X}_i - \mathbf{X}_j) = \det(\mathbf{X}_k),$$

\mathbf{X}_k a matrix in the algebra.

The idea behind division algebras

- ▶ The problem is now to build a family \mathcal{C} of matrices such that

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

or equivalently, such that each $\mathbf{0} \neq \mathbf{X} \in \mathcal{C}$ is *invertible*.

- ▶ By definition, a *field* is a set such that every (nonzero) element in it is invertible.
- ▶ Take \mathcal{C} inside an algebra of matrices which is also a field.
- ▶ A *division algebra* is a non-commutative field.

The leitmotiv

Let \mathcal{C} be a subset of an algebra of matrices which is a division algebra, then

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

Outline

- ▶ Division algebras do exist: the Hamiltonian Quaternions
- ▶ Introducing number fields
- ▶ Introducing cyclic algebras
- ▶ Encoding and Rate
- ▶ Full diversity

The Hamiltonian Quaternions: definition

- ▶ Let $\{1, i, j, k\}$ be a basis for a vector space of dimension 4 over \mathbb{R} .
- ▶ We have the rule that $i^2 = -1$, $j^2 = -1$, and $ij = -ji$.
- ▶ The *Hamiltonian Quaternions* is the set \mathbb{H} defined by

$$\mathbb{H} = \{x + yi + zj + wk \mid a, b, c, d \in \mathbb{R}\}.$$

Hamiltonian Quaternions are a division algebra

- ▶ Define the *conjugate* of a quaternion $q = x + yi + zk$:

$$\bar{q} = x - yi - zk.$$

- ▶ Compute that

$$q\bar{q} = x^2 + y^2 + z^2 + w^2, \quad x, y, z, w \in \mathbb{R}.$$

- ▶ The inverse of the quaternion q is given by

$$q^{-1} = \frac{\bar{q}}{q\bar{q}}.$$

Hamiltonian Quaternions: a matrix formulation

- ▶ Any quaternion $q = x + yi + zj + wk$ can be written as

$$(x + yi) + j(z - wi) = \alpha + j\beta, \quad \alpha, \beta \in \mathcal{C}.$$

- ▶ Now compute the multiplication by q :

$$\begin{aligned}(\alpha + j\beta)(\gamma + j\delta) &= \alpha\gamma + j\bar{\alpha}\delta + j\beta\gamma + j^2\bar{\beta}\delta \\ &= (\alpha\gamma - \bar{\beta}\delta) + j(\bar{\alpha}\delta + \beta\gamma)\end{aligned}$$

- ▶ Write this equality in the basis $\{1, j\}$:

$$\begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \bar{\beta}\delta \\ \bar{\alpha}\delta + \beta\gamma \end{pmatrix}$$

Hamiltonian Quaternions and Cyclic Algebras

A handwaving parallel:

$$\begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \leftrightarrow \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}$$

$$\mathbb{C} \leftrightarrow \text{a number field}$$

$$\bar{x} \leftrightarrow \sigma(x)$$

$$-1 \leftrightarrow \gamma$$

Number fields: the idea

- ▶ The set \mathbb{Q} is easily checked to be a field.
- ▶ Take i , such that $i^2 = -1$. One can build a new field “adding” i to \mathbb{Q} , the same way i is added to \mathbb{R} to create \mathbb{C} .
- ▶ To get a field, we add all the multiples and powers of i . We obtain $\mathbb{Q}(i)$.
- ▶ Note we can start with the field $\mathbb{Q}(i)$ and add $\sqrt{5}$, we get a new field, denoted by $\mathbb{Q}(i, \sqrt{5})$.
- ▶ We say that $\mathbb{Q}(i, \sqrt{5})$ is an *extension* of $\mathbb{Q}(i)$, which is itself an *extension* of \mathbb{Q} .

Number field: the definition

- ▶ If L/K is a field extension, then L has a natural structure as a vector space over K
- ▶ An element $x \in \mathbb{Q}(i, \sqrt{5})$ can be written as $w = x + y\sqrt{5}$, where $\{1, \sqrt{5}\}$ are the basis “vectors” and $x, y \in \mathbb{Q}(i)$ are the scalars.
- ▶ Also $w = (a + ib) + \sqrt{5}(c + id)$, $a, b, c, d \in \mathbb{Q}$. Thus $\mathbb{Q}(i, \sqrt{5})$ is a vector space of dimension 2 over $\mathbb{Q}(i)$, or of dimension 4 over \mathbb{Q}
- ▶ A finite field extension of \mathbb{Q} is called a *number field*.

Hamiltonian Quaternions and Cyclic Algebras

A handwaving parallel:

$$\begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \leftrightarrow \begin{pmatrix} a_0 + \sqrt{5}b_0 & \gamma\sigma(a_1 + \sqrt{5}b_1) \\ a_1 + \sqrt{5}b_1 & \sigma(a_0 + \sqrt{5}b_0) \end{pmatrix}, \quad a_0, a_1, b_0, b_1 \in \mathbb{Q}(i)$$

$$\mathbb{C} \leftrightarrow \mathbb{Q}(i, \sqrt{5})$$

$$\bar{x} \leftrightarrow \sigma(x)$$

$$-1 \leftrightarrow \gamma$$

Number field and polynomial

- ▶ A way to describe i is to say it is the solution of the equation $X^2 + 1 = 0$. Building $\mathbb{Q}(i)$, we thus add to \mathbb{Q} the solution of a polynomial equation.
- ▶ Such a polynomial is called the *minimal polynomial*
- ▶ The polynomial $X^2 + 1$ is the minimal polynomial of i over \mathbb{Q} . Similarly, $X^2 - 5$ is the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}(i)$.

Defining automorphisms

- ▶ We define *automorphisms* of a number field L using the roots of the minimal polynomial.
- ▶ For $\mathbb{Q}(\sqrt{5})$, $X^2 - 5 = (X + \sqrt{5})(X - \sqrt{5})$, there are thus two automorphisms

$$\begin{aligned}\sigma_1 : \quad & \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{Q}(\sqrt{5}) \\ & a + b\sqrt{5} \mapsto a + b\sqrt{5}\end{aligned}$$

$$\begin{aligned}\sigma_2 : \quad & \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{Q}(\sqrt{5}) \\ & a + b\sqrt{5} \mapsto a - b\sqrt{5}\end{aligned}$$

- ▶ True for $a, b \in \mathbb{Q}(i)$ or \mathbb{Q} .
- ▶ Note that $\sigma_2(\sigma_2(a + b\sqrt{5})) = a + b\sqrt{5}$.

Hamiltonian Quaternions and Cyclic Algebras

A handwaving parallel:

$$\begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \leftrightarrow \begin{pmatrix} a_0 + \sqrt{5}b_0 & \gamma\sigma(a_1 + \sqrt{5}b_1) \\ a_1 + \sqrt{5}b_1 & \sigma(a_0 + \sqrt{5}b_0) \end{pmatrix}, \quad a_0, a_1, b_0, b_1 \in \mathbb{Q}(i)$$

$$\mathbb{C} \leftrightarrow \mathbb{Q}(i, \sqrt{5})$$

$$\bar{x} \leftrightarrow \sigma(a_0 + \sqrt{5}b_0) = a_0 - \sqrt{5}b_0$$

$$-1 \leftrightarrow \gamma$$

Cyclic algebras

- ▶ Let L/K be a Galois extension of degree n such that its Galois group $G = \text{Gal}(L/K)$ is cyclic, with generator σ . Denote by K^* (resp. L^*) the non-zero elements of K (resp. L), and choose an element $\gamma \in K^*$. We construct a non-commutative algebra, denoted $\mathcal{A} = (L/K, \sigma, \gamma)$, as follows:

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

such that e satisfies

$$e^n = \gamma \quad \text{and} \quad \lambda e = e\sigma(\lambda) \quad \text{for } \lambda \in L.$$

Such an algebra is called a *cyclic algebra*.

- ▶ The algebra \mathcal{A} is defined as a direct sum of copies of L , thus an element x in the algebra is written

$$x = x_0 + ex_1 + \dots + e^{n-1}x_{n-1},$$

with $x_i \in L$.

- ▶ Since the algebra is noncommutative, the rule $\lambda e = e\sigma(\lambda)$ explains how to do the computation if the element e is multiplied by the left.

Cyclic algebras: matrix formulation

We illustrate the computation on an example. For $n = 2$, we have

$$\begin{aligned}xy &= (x_0 + ex_1)(y_0 + ey_1) \\ &= x_0y_0 + x_0ey_1 + ex_1y_0 + ex_1ey_1 \\ &= x_0y_0 + e\sigma(x_0)y_1 + ex_1y_0 + \gamma\sigma(x_1)y_1,\end{aligned}$$

since $e^2 = \gamma$. In matrix form, this yields

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

Cyclic algebras: matrix formulation



$$\mathcal{A} = L \oplus eL$$

such that e satisfies

$$e^2 = \gamma \quad \text{and} \quad \lambda e = e\sigma(\lambda) \quad \text{for } \lambda \in L.$$



$$x = x_0 + ex_1 \in \mathcal{A} \leftrightarrow \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}$$



$$e \in \mathcal{A} \leftrightarrow \begin{pmatrix} 0 & \gamma \\ 1 & 0 \end{pmatrix}$$

Cyclic Algebras: encoding and rate

- ▶ Information symbols are from QAM constellations, or HEX constellations.
- ▶ Since QAM symbols are in $\mathbb{Z}[i] \subseteq \mathbb{Q}(i)$.
- ▶ Consider our example, where $L = \mathbb{Q}(i, \sqrt{5})$. Then

$$\mathcal{C} = \left\{ \begin{pmatrix} a_0 + \sqrt{5}b_0 & \gamma(a_1 - \sqrt{5}b_1) \\ a_1 + \sqrt{5}b_1 & a_0 - \sqrt{5}b_0 \end{pmatrix}^T \mid a_0, a_1, b_0, b_1 \in \text{QQAM} \right\}.$$

- ▶ Codes made from cyclic algebras are said *full rate*: n^2 information symbols encoded for n^2 symbols transmitted.

Introducing the notion of norm

- ▶ We have defined *automorphisms* of a number field L using the roots of the minimal polynomial.
- ▶ For $\mathbb{Q}(\sqrt{5})$, $X^2 - 5 = (X + \sqrt{5})(X - \sqrt{5})$, there are thus two automorphisms

$$\begin{aligned}\sigma_1 : \quad & \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{Q}(\sqrt{5}) \\ & a + b\sqrt{5} \mapsto a + b\sqrt{5} \\ \sigma_2 : \quad & \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{Q}(\sqrt{5}) \\ & a + b\sqrt{5} \mapsto a - b\sqrt{5}\end{aligned}$$

- ▶ True for $a, b \in \mathbb{Q}(i)$ or \mathbb{Q} .
- ▶ The *norm* of x is defined by

$$N_{L/K}(x) = \prod_{i=1}^n \sigma_i(x)$$

Full diversity

- ▶ Remember that codes coming from cyclic algebras satisfy

$$\det(\mathbf{X}_i - \mathbf{X}_j) = \det(\mathbf{X}), \quad \mathbf{X}_i \neq \mathbf{X}_j, \quad \mathbf{X} \in \mathcal{C}.$$

- ▶ We want $\det(\mathbf{X}) \neq 0$ for all $\mathbf{X} \neq \mathbf{0}$.
- ▶ If $n = 2$, we have

$$\det \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} = x_0\sigma(x_0) - \gamma x_1\sigma(x_1) = N_{L/K}(x_0) - \gamma N_{L/K}(x_1).$$

Thus

$$\det(\mathbf{X}) = 0 \iff \gamma = N_{L/K} \left(\frac{x_0}{x_1} \right),$$

Full diversity

Theorem. Let L/K be a cyclic extension of degree n with Galois group $Gal(L/K) = \langle \sigma \rangle$. If $\gamma, \gamma^2, \dots, \gamma^{n-1} \in K^*$ are not a norm, then the cyclic algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ is a division algebra.

Summary of the construction

Suppose you want a code for M antennas.

- ▶ Take a number field of degree M , say $\mathbb{Q}(i, \sqrt{5})$ for $M = 2$. (with cyclic Galois group).
- ▶ Build the code

$$\mathcal{C} = \left\{ \begin{pmatrix} a_0 + \sqrt{5}b_0 & \gamma(a_1 - \sqrt{5}b_1) \\ a_1 + \sqrt{5}b_1 & a_0 - \sqrt{5}b_0 \end{pmatrix}^T \mid a_0, a_1, b_0, b_1 \in \text{QQAM} \right\}.$$

- ▶ Choose γ which is not a norm, to get a division algebra.

And next?

- ▶ In this talk, I explained how to build a *cyclic division algebra*.
- ▶ There are more properties one can get for these codes.
 1. a lower bound on the diversity
 2. the same average transmit energy per antenna
 3. shaping gain

