Division algebras:
\textit{a tool for Space-Time Coding}

CMI Seminar
January 27, 2006

Frédérique Oggier
The problem we are interested in

\[ X \rightarrow H \rightarrow Y = HX + Z \]

- Codes for multiple antennas (\textit{Space-Time Codes}), with \( M \) transmit and \( N \) receive antennas.
- We call \textit{coherent case} when we assume knowledge of the channel (\( H \)) at the receiver, resp. \textit{noncoherent case} otherwise.
Outline

- The coherent case
- The noncoherent differential case
- Open questions
The coherent case: the Golden code

- channel model and code design criteria
- the non-vanishing determinant property
- performance of the Golden code
- higher dimension codes

joint work with
Jean-Claude Belfiore and Ghaya Rekaya, ENST, Paris, France
Emanuele Viterbo, Politecnico di Torino, Torino, Italy
The $2 \times 2$ MIMO channel

$X$  
\[ X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \]

$H$  
\[ H = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \]

$Y = HX + Z$

$X$: $2 \times 2$ matrix codeword from a space-time code

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

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

$H$: $2 \times 2$ channel matrix is a complex Gaussian matrix with independent, zero mean, entries.

$Z$: $2 \times 2$ complex Gaussian noise matrix.
The code design

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

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

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

- The design criterion is to minimize the pairwise probability of error, that is the probability of sending $\mathbf{X}$ and decoding $\hat{\mathbf{X}} \neq \mathbf{X}$.
- We assume the receiver knows the channel (this is called the coherent case).
The pairwise probability of error

The goal is to upper bound the pairwise probability of error \( P(X \rightarrow \hat{X}) \). Recall that \( Y = HX + W \).

- We have that

\[
P(X \rightarrow \hat{X}|H) = P(\|Y - H\hat{X}\| \leq \|Y - HX\|)
= P(\|H(X - \hat{X}) + W\| \leq \|W\|)
\leq \exp(-d^2(X, \hat{X})\text{const}(\sigma(W)))
\]

- On averaging with respect to \( H \)

\[
P(X \rightarrow \hat{X}) \leq \frac{\text{const}}{|\det(X - \hat{X})|^{2M}}.
\]
Code design criteria

- Find a family $C$ of $M \times M$ matrices such that
  \[ \det(X_i - X_j) \neq 0, \; X_i \neq X_j \in C. \]
  
  Such a family $C$ is said fully-diverse.

- A good code $C$ attempts to maximize
  \[ \delta_{\min}(C) = \min_{X_i \neq X_j} \left| \det(X_i - X_j) \right|^2. \]
The Golden Code: definition

The Golden code is related to the Golden number \( \theta = \frac{1+\sqrt{5}}{2} \), one of the roots of \( x^2 - x - 1 = 0 \) (\( \bar{\theta} = \frac{1-\sqrt{5}}{2} \) is the other one).

We define the code \( \mathcal{C} \) as
\[
\mathcal{C} = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} a + b\theta & c + d\theta \\ i(c + d\bar{\theta}) & a + b\bar{\theta} \end{bmatrix} : a, b, c, d \in \mathbb{Z}[i] \right\}
\]

This code has been built from the cyclic algebra \( \mathcal{A} \), given by
\[
\mathcal{A} = \{ y = (u + v\theta) + e(w + z\theta) \mid e^2 = i, \ u, v, w, z \in \mathbb{Q}(i) \}.
\]
The Golden code: minimum determinant

- We have the code $\mathcal{C}$ as
  $$
  \mathcal{C} = \left\{ \begin{bmatrix}
  x_1 & x_2 \\
  x_3 & x_4 
  \end{bmatrix} = \begin{bmatrix}
  a + b\theta & c + d\theta \\
  i(c + d\theta) & a + b\bar{\theta}
  \end{bmatrix} : a, b, c, d \in \mathbb{Z}[i] \right\}
  $$

- $\mathcal{C}$ is a linear code, i.e., $X_1 + X_2 \in \mathcal{C}$ for all $X_1, X_2 \in \mathcal{C}$.

- The minimum determinant of $\mathcal{C}$ is given by
  $$
  \delta_{\min}(\mathcal{C}) = \min_{X_1 \neq X_2 \in \mathcal{C}} |\det(X_1 - X_2)|^2 = \min_{0 \neq X \in \mathcal{C}} |\det(X)|^2 \neq 0
  $$
  by choice of $\mathcal{A}$, a division algebra.
The Golden code: encoding and rate

- We have the code $\mathcal{C}$ as

$$\mathcal{C} = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} a + b\theta & c + d\theta \\ i(c + d\bar{\theta}) & a + b\bar{\theta} \end{bmatrix} : a, b, c, d \in \mathbb{Z}[i] \right\}$$

- The finite code $\mathcal{C}$ is obtained by limiting the information symbols to $a, b, c, d \in S \subset \mathbb{Z}[i]$ (QAM signal constellation).

- The code $\mathcal{C}$ is full rate.
The non-vanishing determinant property

Let $X \in \mathcal{C}$, then

$$
\det(X) = \det \begin{pmatrix}
 a + b\theta & c + d\theta \\
 i(c + d\bar{\theta}) & a + b\bar{\theta}
\end{pmatrix}
= (a + b\theta)(a + b\bar{\theta}) - i(c + d\theta)(c + d\bar{\theta})
= a^2 + ab(\bar{\theta} + \theta) - b^2 - i[c^2 + cd(\theta + \bar{\theta}) - d^2]
= a^2 + ab - b^2 + i(c^2 + cd - d^2),
$$

$a, b, c, d \in \mathbb{Z}[i]$.

Thus

$$
\det(X) \in \mathbb{Z}[i] \Rightarrow \delta_{\min}(\mathcal{C}) = |\det(X)|^2 \geq 1.
$$

Does not depend on the cardinality of $\mathcal{C}$. 
Some determinants for the codewords of $C$
An energy criterion

- We have the code $\mathcal{C}$ as

$$
\mathcal{C} = \left\{ \begin{bmatrix} x_1 & x_2 \\
 x_3 & x_4 \end{bmatrix} = \begin{bmatrix} a + b\theta & c + d\theta \\
 i(c + d\bar{\theta}) & a + b\bar{\theta} \end{bmatrix} : a, b, c, d \in \mathbb{Z}[i] \right\}
$$

- That $|i| = 1$ guarantees that the same average energy is transmitted from each antenna at each channel use.
Golden Code: summary of the properties

The Golden Code is a $2 \times 2$ code for the coherent MIMO channel that satisfies

- full rate
- minimum non zero determinant
- furthermore non-vanishing determinant
- same average energy is transmitted from each antenna at each channel use.
Performance of the Golden Code
Codes in higher dimensions

- Isomorphic versions of the Golden code were independently derived by [Yao, Wornell, 2003] and by [Dayal, Varanasi, 2003] by analytic optimization.
- Cyclic division algebras enable to generalize to larger $n \times n$ systems.
The differential noncoherent case

- channel model and differential modulation
- recall about cyclic algebras
- naive codebooks
The differential noncoherent MIMO channel

- Consider a channel with $M$ transmit antennas and $N$ receive antennas, with unknown channel information.

- How to do decoding?

- We use differential unitary space-time modulation. That is (assuming $S_0 = I$)

$$S_t = X_{z_t} S_{t-1}, \ t = 1, 2, \ldots,$$

where $z_t \in \{0, \ldots, L - 1\}$ is the data to be transmitted, and $C = \{X_0, \ldots, X_{L-1}\}$ the constellation to be designed.

- The matrices $X$ have to be unitary.
The decoding

- If we assume the channel is roughly constant, we have

\[ Y_t = S_t H + W_t \]
\[ = X_{zt} S_{t-1} H + W_t \]
\[ = X_{zt} (Y_{t-1} - W_{t-1}) + W_t \]
\[ = X_{zt} Y_{t-1} + W'_t. \]

- The matrix H does not appear in the last equation.

- The decoder is thus given by

\[ \hat{z}_t = \arg \min_{l=0, \ldots, |C|-1} \| Y_t - X_l Y_{t-1} \|. \]
Probability of error

- At high SNR, the pairwise block probability of error $P_e$ has the upper bound

$$P_e \leq \left( \frac{1}{2} \right) \left( \frac{8}{\rho} \right)^{MN} \frac{1}{|\det(X_i - X_j)|^{2N}}$$

- The quality of the code is measured by the diversity product

$$\zeta_C = \frac{1}{2} \min_{X_i \neq X_j} |\det(X_i - X_j)|^{1/M} \quad \forall X_i \neq X_j \in C$$

and full diversity is achieved when

$$\det(X_i - X_j) \neq 0 \quad \forall X_i \neq X_j \in C$$
Problem statement

Find a set $\mathcal{C}$ of *unitary* matrices ($X X^\dagger = I$) such that

$$\det(X_i - X_j) \neq 0 \quad \forall \; X_i \neq X_j \in \mathcal{C}$$
Cyclic Algebras: definition

- Elements in a cyclic algebra $A$ of degree 3 can be represented by matrices of the form
  \[
  \begin{pmatrix}
  x_0 & x_1 & x_2 \\
  \gamma \sigma(x_2) & \sigma(x_0) & \sigma(x_1) \\
  \gamma \sigma^2(x_1) & \gamma \sigma^2(x_2) & \sigma^2(x_0)
  \end{pmatrix}.
\]
  with $x_i \in L$ and $\sigma : L \rightarrow L$ such that $\sigma^3 = Id$.

- The set $L$ is a field, and can be seen as a vector space over $\mathbb{Q}$. 

Division algebras: a tool for Space-Time Coding • January 27th, 2005
Cyclic Algebras: basic properties

- **Linearity**, so that

\[
\det(X_1 - X_2) = \det(X), \quad 0 \neq X \in \mathcal{A} \ \forall \ X_1 \neq X_2 \in \mathcal{A}
\]

and *full diversity* is achieved when

\[
\det(X) \neq 0, \quad \forall 0 \neq X \in \mathcal{C}.
\]

- **Cyclic Division Algebras**: these are cyclic algebras where all matrices are invertible.

Thus cyclic division algebras *naturally* yield full diversity.
Natural unitary matrices

- Recall that a matrix $X$ in the algebra has the form
\[
\begin{pmatrix}
  x_0 & x_1 & x_2 \\
  \gamma \sigma(x_2) & \sigma(x_0) & \sigma(x_1) \\
  \gamma \sigma^2(x_1) & \gamma \sigma^2(x_2) & \sigma^2(x_0)
\end{pmatrix}.
\]

- There are natural unitary matrices:

\[
E = \begin{pmatrix}
  0 & 1 & 0 \\
  0 & 0 & 1 \\
  \gamma & 0 & 0
\end{pmatrix}
\quad \text{and} \quad
D = \begin{pmatrix}
  x & 0 & 0 \\
  0 & \sigma(x) & 0 \\
  0 & 0 & \sigma^2(x)
\end{pmatrix}, \quad x \in L.
\]

- If $\gamma$ satisfies $\gamma \bar{\gamma} = 1$, then $E^k$, $k = 0, 1, 2$, is unitary.

- If $x$ satisfies $x \bar{x} = 1$, $D$ and its powers will be unitary.
A first family of unitary matrices (1)

- Consider $L = \mathbb{Q}(\zeta_m)$ where $\zeta_m$ is a $m$th root of unity. Here $m = 21$.

- We have
  
  $$E = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \zeta_3 & 0 & 0 \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} \zeta_{21} & 0 & 0 \\ 0 & \zeta_{21}^4 & 0 \\ 0 & 0 & \zeta_{21}^{16} \end{pmatrix}, \quad \zeta_{21} \in L = \mathbb{Q}(\zeta_{21}).$$

  and $\sigma : \zeta_{21} \mapsto \zeta_{21}^4$

- The family $C = \{E^iD^j, \ i = 0, 1, 2, \ j = 0, \ldots, 20\}$ has 63 elements, and thus gives a constellation of rate almost 2 for 3 antennas.
A first family of unitary matrices (2)

- These families were obtained using representations of fixed point free groups.

- **Drawback of this construction:** the rate of the code $C$ is
  \[
  R = \frac{\log_2(\#C)}{n} = \frac{\log_2(nm - 1)}{n}.
  \]

- **Hope:** a cyclic algebra contains infinitely many elements, and we are using only $nm - 1$ of them!
Extending the construction

- Recall that if $xx = 1$ then the corresponding matrix

$$F = \begin{pmatrix} x & 0 & 0 \\ 0 & \sigma(x) & 0 \\ 0 & 0 & \sigma^2(x) \end{pmatrix}$$

is unitary.

- We consider the subfield of $L = \mathbb{Q}(\zeta_m)$ fixed by the complex conjugation

$$\mathbb{Q}(\zeta_m + \zeta^{-1}_m) = \{y \in L \mid \bar{y} = y\}$$

- We have

$$\bar{x}x = 1 \iff N_{L/\mathbb{Q}(\zeta_m + \zeta^{-1}_m)}(x) = 1$$

where $N_{L/\mathbb{Q}(\zeta_m + \zeta^{-1}_m)}(x)$ is the relative norm of $x$. 
Conclusions...

- Cyclic algebras have already proven to be an efficient tool for coherent Space-Time coding.
- It seems to me a promising tool for differential noncoherent Space-Time coding.
Some open questions:

- The coherent case: only the case for \( n = 2 \) is known to be optimal.
- The differential noncoherent case: high rate constructions?
- The “hot” topic now: wireless relay network.