Introduction to Space-Time Coding

Frédérique Oggier
frederique@ntu.edu.sg

Division of Mathematical Sciences
Nanyang Technological University, Singapore

Noncommutative Rings and their Applications V, Lens, 12-15 June 2017

Last Time

1. A fully diverse space-time code is a family $\mathcal{C}$ of (square) complex matrices such that $\det(\mathbf{X} - \mathbf{X}') \neq 0$ when $\mathbf{X} \neq \mathbf{X}'$.
2. Division algebras whose elements can be represented as matrices satisfy full diversity by definition.
3. Hamilton's quaternions provide such a family of fully diverse space-time codes.

Outline

Division Algebras
Cyclic Algebras
Crossed Product Algebras
Quotients of Space-Time Codes
2×2 Space-Time Coded Modulation

Cyclic Algebras: Definition

- Consider the quadratic extension $\mathbb{Q}(i) = \{a + ib,\ a, b\ \in \mathbb{Q}\}$ (or more generally K a number field).

Cyclic Algebras: Definition

- Consider the quadratic extension $\mathbb{Q}(i) = \{a + ib,\ a, b\ \in \mathbb{Q}\}$ (or more generally K a number field).
- Let $L/\mathbb{Q}(i)$ be a *cyclic* extension of de degree n, of Galois group $\langle\sigma\rangle$.

Cyclic Algebras: Definition

- Consider the quadratic extension $\mathbb{Q}(i) = \{a + ib,\ a, b\ \in \mathbb{Q}\}$ (or more generally K a number field).
- Let $L/\mathbb{Q}(i)$ be a *cyclic* extension of de degree n, of Galois group $\langle\sigma\rangle$.
- A *cyclic algebra* $\mathcal{A}$ is defined by

$$\mathcal{A} = \{(x_0, x_1, \ldots, x_{n-1}) \mid x_i \in L\}$$

Cyclic Algebras: Definition

- Consider the quadratic extension $\mathbb{Q}(i) = \{a + ib,\ a, b \in \mathbb{Q}\}$ (or more generally K a number field).
- Let $L/\mathbb{Q}(i)$ be a *cyclic* extension of de degree n, of Galois group $\langle\sigma\rangle$.
- A *cyclic algebra* $\mathcal{A}$ is defined by

$$\mathcal{A} = \{(x_0, x_1, \ldots, x_{n-1}) \mid x_i \in L\}$$

in the basis $\{1, e, \ldots, e^{n-1}\}$ with $e^n = \gamma \in \mathbb{Q}(i)$.

Cyclic Algebras: Definition

- Consider the quadratic extension $\mathbb{Q}(i) = \{a + ib,\ a, b\ \in \mathbb{Q}\}$ (or more generally K a number field).
- Let $L/\mathbb{Q}(i)$ be a *cyclic* extension of de degree n, of Galois group $\langle \sigma \rangle$.
- A *cyclic algebra* $\mathcal{A}$ is defined by

$$\mathcal{A} = \{(x_0, x_1, \ldots, x_{n-1}) \mid x_i \in L\}$$

  in the basis $\{1, e, \ldots, e^{n-1}\}$ with $e^n = \gamma \in \mathbb{Q}(i)$.
- *Multiplication* rule: $\lambda e = e\sigma(\lambda)$, $\sigma : L \to L$, the generator of the Galois group of $L/\mathbb{Q}(i)$.

Cyclic Algebras: Coding ($n = 2$)

1. For $n = 2$, compute the *multiplication* by x of $y \in \mathcal{A}$:

$$\begin{aligned} xy &= (x_0 + ex_1)(y_0 + ey_1) \\ &= x_0 y_0 + e\sigma(x_0)y_1 + ex_1 y_0 + \gamma\sigma(x_1)y_1 && \lambda e = e\sigma(\lambda) \\ &= [x_0 y_0 + \gamma\sigma(x_1)y_1] + e[\sigma(x_0)y_1 + x_1 y_0] && e^2 = \gamma \end{aligned}$$

Cyclic Algebras: Coding ($n = 2$)

1. For $n = 2$, compute the *multiplication* by x of $y \in \mathcal{A}$:

$$\begin{aligned} xy &= (x_0 + ex_1)(y_0 + ey_1) \\ &= x_0 y_0 + e\sigma(x_0)y_1 + ex_1 y_0 + \gamma\sigma(x_1)y_1 & \lambda e = e\sigma(\lambda) \\ &= [x_0 y_0 + \gamma\sigma(x_1)y_1] + e[\sigma(x_0)y_1 + x_1 y_0] & e^2 = \gamma \end{aligned}$$

2. In the basis $\{1, e\}$, we have

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

Cyclic Algebras: Coding ($n = 2$)

1. For $n = 2$, compute the *multiplication* by x of $y \in \mathcal{A}$:

$$\begin{aligned} xy &= (x_0 + ex_1)(y_0 + ey_1) \\ &= x_0 y_0 + e\sigma(x_0) y_1 + ex_1 y_0 + \gamma\sigma(x_1) y_1 & \lambda e = e\sigma(\lambda) \\ &= [x_0 y_0 + \gamma\sigma(x_1) y_1] + e[\sigma(x_0) y_1 + x_1 y_0] & e^2 = \gamma \end{aligned}$$

2. In the basis $\{1, e\}$, we have

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

3. Correspondence between x and its *multiplication matrix*.

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

Cyclic Algebras: Encoding

- In general:

$$x \leftrightarrow \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \dots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \dots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \dots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \dots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

Cyclic Algebras: Encoding

- In general:

$$x \leftrightarrow \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \dots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \dots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \dots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \dots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

- Every $x_i \in L$ *encodes* n information symbols.

Cyclic Division Algebras

- *Remember*: Given $L/\mathbb{Q}(i)$, a cyclic algebra $\mathcal{A}$ is defined by

$$\mathcal{A} = \{(x_0, x_1, \ldots, x_{n-1}) \mid x_i \in L\}$$

in the basis $\{1, e, \ldots, e^{n-1}\}$ with $e^n = \gamma \in \mathbb{Q}(i)$.

Cyclic Division Algebras

- *Remember*: Given $L/\mathbb{Q}(i)$, a cyclic algebra $\mathcal{A}$ is defined by

$$\mathcal{A} = \{(x_0, x_1, \ldots, x_{n-1}) \mid x_i \in L\}$$

  in the basis $\{1, e, \ldots, e^{n-1}\}$ with $e^n = \gamma \in \mathbb{Q}(i)$.
- **Proposition.** If γ and its powers $\gamma^2, \ldots, \gamma^{n-1}$ are not algebraic norms (there is no $x \in L$ with $N_{L/\mathbb{Q}(i)}(x) = \gamma^j$, $j = 1, \ldots n-1$), then the cyclic algebra $\mathcal{A}$ is a *division algebra*.

A Recipe

To obtain *space-time codes*:

1. Take a *cyclic extension* $L/\mathbb{Q}(i)$ of degree n (# antennas).

A Recipe

To obtain *space-time codes*:

1. Take a *cyclic extension* $L/\mathbb{Q}(i)$ of degree n (# antennas).
2. Build a *cyclic division algebra*.

A Recipe

To obtain *space-time codes*:

1. Take a *cyclic extension* $L/\mathbb{Q}(i)$ of degree n (# antennas).
2. Build a *cyclic division algebra*.
3. This gives *fully diverse* codes and a practical encoding for *every n*.

[F. Oggier, G. Rekaya, J.-C. Belfiore, E. Viterbo, "Perfect Space-Time Block Codes."]

An Example: the Golden Code

- The *Golden number* is $\theta = \frac{1+\sqrt{5}}{2}$, a root of $x^2 - x - 1 = 0$ ($\sigma(\theta) = \frac{1-\sqrt{5}}{2}$ is the other root).

An Example: the Golden Code

- The *Golden number* is $\theta = \frac{1+\sqrt{5}}{2}$, a root of $x^2 - x - 1 = 0$ ($\sigma(\theta) = \frac{1-\sqrt{5}}{2}$ is the other root).
- Take $L = \mathbb{Q}(i, \theta)$, the cyclic extension $L/\mathbb{Q}(i)$ and *the cyclic algebra* which is division

$$\mathcal{A} = \{y = (u + v\theta) + e(w + z\theta) \mid e^2 = i,\ u, v, w, z \in \mathbb{Q}(i)\}$$

An Example: the Golden Code

- The *Golden number* is $\theta = \frac{1+\sqrt{5}}{2}$, a root of $x^2 - x - 1 = 0$ ($\sigma(\theta) = \frac{1-\sqrt{5}}{2}$ is the other root).
- Take $L = \mathbb{Q}(i, \theta)$, the cyclic extension $L/\mathbb{Q}(i)$ and *the cyclic algebra* which is division

$$\mathcal{A} = \{y = (u + v\theta) + e(w + z\theta) \mid e^2 = i,\ u, v, w, z \in \mathbb{Q}(i)\}$$

- We define the code $\mathcal{C}$ by

$$\left\{ \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} a + b\theta & c + d\theta \\ i(c + d\sigma(\theta)) & a + b\sigma(\theta) \end{pmatrix} : a, b, c, d \in \mathbb{Z}[i] \right\}$$

The Golden code: $\gamma = i$ not a norm (I)

- The determinant of $\mathbf{X} \in \mathcal{C}$ is

$$\begin{aligned}\det(\mathbf{X}) &= \det\begin{pmatrix} a+b\theta & c+d\theta \\ i(c+d\sigma(\theta)) & a+b\sigma(\theta) \end{pmatrix} \\ &= (a+b\theta)(a+b\sigma(\theta)) - i(c+d\theta)(c+d\sigma(\theta)).\end{aligned}$$

- Thus

$$0 = \det(\mathbf{X}) \iff i = \frac{(a+b\theta)(a+b\sigma(\theta))}{(c+d\theta)(c+d\sigma(\theta))}$$

- Make sure $\gamma = i$ is *not a norm*.

The Golden code: $\gamma = i$ not a norm (II)

- To see: $N_{L/\mathbb{Q}(i)}(x) \neq i, \ \forall x \in L$.

The Golden code: $\gamma = i$ not a norm (II)

- To see: $N_{L/\mathbb{Q}(i)}(x) \neq i,\ \forall x \in L$.
- Consider
  $\mathbb{Q}_5 = \{a_{-m}\frac{1}{5^m} + a_{-m+1}\frac{1}{5^{m-1}} + \ldots + a_{-1}\frac{1}{5} + a_0 + a_1 5 + \ldots\}$
  the field of 5-adic numbers, and
  $\mathbb{Z}_5 = \{a_0 + a_1 5 + a_2 5^2 + \ldots\} = \{x \in \mathbb{Q}_5 | \nu_5(x) \geq 0\}$ its valuation ring.

The Golden code: $\gamma = i$ not a norm (II)

- To see: $N_{L/\mathbb{Q}(i)}(x) \neq i, \ \forall x \in L$.
- Consider $\mathbb{Q}_5 = \{a_{-m}\frac{1}{5^m} + a_{-m+1}\frac{1}{5^{m-1}} + \ldots + a_{-1}\frac{1}{5} + a_0 + a_1 5 + \ldots\}$ the field of 5-adic numbers, and $\mathbb{Z}_5 = \{a_0 + a_1 5 + a_2 5^2 + \ldots\} = \{x \in \mathbb{Q}_5 | \nu_5(x) \geq 0\}$ its valuation ring.
- Then $\mathbb{Q}(i)$ can be embedded into $\mathbb{Q}_5$ by

$$i \mapsto 2 + 5\mathbb{Z}_5$$

(the polynomial $X^2 + 1$ has roots in $\mathbb{Z}_5$, because it has roots in $\mathbb{F}_5$, then use Hensel's Lemma).

The Golden code: $\gamma = i$ not a norm (II)

- To see: $N_{L/\mathbb{Q}(i)}(x) \neq i, \ \forall x \in L$.
- Consider
  $\mathbb{Q}_5 = \{a_{-m}\frac{1}{5^m} + a_{-m+1}\frac{1}{5^{m-1}} + \ldots + a_{-1}\frac{1}{5} + a_0 + a_1 5 + \ldots\}$
  the field of 5-adic numbers, and
  $\mathbb{Z}_5 = \{a_0 + a_1 5 + a_2 5^2 + \ldots\} = \{x \in \mathbb{Q}_5 | \nu_5(x) \geq 0\}$ its valuation ring.
- Then $\mathbb{Q}(i)$ can be embedded into $\mathbb{Q}_5$ by

$$i \mapsto 2 + 5\mathbb{Z}_5$$

  (the polynomial $X^2 + 1$ has roots in $\mathbb{Z}_5$, because it has roots in $\mathbb{F}_5$, then use Hensel's Lemma).
- Let $x = a + b\sqrt{5} \in K$ with $a, b \in \mathbb{Q}(i)$ then we must show that

$$N_{L/\mathbb{Q}(i)}(x) = a^2 - 5b^2 = i$$

  has no solution for $a, b \in \mathbb{Q}(i)$.

The Golden code: $\gamma = i$ not a norm (III)

- We can lift the norm equation in the 5-adic field $\mathbb{Q}_5$

$$a^2 - 5b^2 = 2 + 5x \quad a, b \in \mathbb{Q}(i),\ x \in \mathbb{Z}_5$$

and show that it has no solution there.

The Golden code: $\gamma = i$ not a norm (III)

- We can lift the norm equation in the 5-adic field $\mathbb{Q}_5$

$$a^2 - 5b^2 = 2 + 5x \quad a, b \in \mathbb{Q}(i), \; x \in \mathbb{Z}_5$$

  and show that it has no solution there.
- We take the valuations of both sides:

$$\nu_5(a^2 - 5b^2) = \nu_5(2 + 5x)$$

  to show that a and b must be in $\mathbb{Z}_5$.

The Golden code: $\gamma = i$ not a norm (III)

- We can lift the norm equation in the 5-adic field $\mathbb{Q}_5$

$$a^2 - 5b^2 = 2 + 5x \quad a, b \in \mathbb{Q}(i), \; x \in \mathbb{Z}_5$$

  and show that it has no solution there.

- We take the valuations of both sides:

$$\nu_5(a^2 - 5b^2) = \nu_5(2 + 5x)$$

  to show that a and b must be in $\mathbb{Z}_5$.

- Since $x \in \mathbb{Z}_5$, $\nu_5(2+5x) = inf\{\nu_5(2), \nu_5(x) + 1\} = 0$. Now, $\nu_5(a^2 - 5b^2) = inf\{2\nu_5(a), b\nu_5(b) + 1\}$ must be 0, hence $\nu_5(a) = 0$ which implies $a \in \mathbb{Z}_5$ and consequently $b \in \mathbb{Z}_5$.

The Golden code: $\gamma = i$ not a norm (III)

- We can lift the norm equation in the 5-adic field $\mathbb{Q}_5$

$$a^2 - 5b^2 = 2 + 5x \quad a, b \in \mathbb{Q}(i),\; x \in \mathbb{Z}_5$$

and show that it has no solution there.

- We take the valuations of both sides:

$$\nu_5(a^2 - 5b^2) = \nu_5(2 + 5x)$$

to show that a and b must be in $\mathbb{Z}_5$.

- Since $x \in \mathbb{Z}_5$, $\nu_5(2+5x) = inf\{\nu_5(2), \nu_5(x)+1\} = 0$. Now, $\nu_5(a^2 - 5b^2) = inf\{2\nu_5(a), b\nu_5(b)+1\}$ must be 0, hence $\nu_5(a) = 0$ which implies $a \in \mathbb{Z}_5$ and consequently $b \in \mathbb{Z}_5$.
- We conclude by showing that

$$a^2 - 5b^2 = 2 + 5x \quad a, b, x \in \mathbb{Z}_5$$

has no solution. Reducing modulo $5\mathbb{Z}_5$ we find that 2 should be a square in $\mathbb{F}_5$, which is a contradiction.

The Golden Code: Minimum Determinant

- Let $\mathbf{X} \in \mathcal{C}$ be a codeword from the Golden code.

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

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

The Golden Code: Minimum Determinant

- Let $\mathbf{X} \in \mathcal{C}$ be a codeword from the Golden code.

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

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

- Thus

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

The Golden Code: Minimum Determinant

- Let $\mathbf{X} \in \mathcal{C}$ be a codeword from the Golden code.

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

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

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

- Is a property of *rings of integers*, can be generalized in dimension n.

The Golden code: a Space-Time lattice code (I)

- A complex lattice Λ is given by its *generator matrix*:

$$\Lambda = \{M\mathbf{v} \mid \mathbf{v} \in \mathbb{Z}[i]^n\}$$

- Note that $\mathbf{X} \in \mathcal{C}$ can be written

$$\begin{aligned} \mathbf{X} &= \operatorname{diag}\left(M \begin{bmatrix} a \\ b \end{bmatrix}\right) + \operatorname{diag}\left(M \begin{bmatrix} c \\ d \end{bmatrix}\right) \cdot \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix} \\ &= \begin{bmatrix} a + b\theta & c + d\theta \\ \gamma(c + d\sigma(\theta)) & a + b\sigma(\theta) \end{bmatrix}, \end{aligned}$$

where

$$M = \begin{bmatrix} 1 & \theta \\ 1 & \sigma(\theta) \end{bmatrix}.$$

- We add a structure of $\mathbb{Z}[i]^2$ lattice on each layer to guarantee *no shaping loss*.

The Golden code: a Space-Time lattice code (II)

- We recognize that
$$M = \begin{bmatrix} 1 & \theta \\ 1 & \bar{\theta} \end{bmatrix}$$
is the generator matrix of a lattice obtained from a quadratic number field.
- We add a structure of $\mathbb{Z}[i]^2$ lattice on each layer by defining $\mathcal{C}_{\mathcal{I}} \subset \mathcal{C}$ as
$$x_1, x_2, x_3, x_4 \in \mathcal{I} = (\alpha)\mathbb{Z}[i][\tfrac{1+\sqrt{5}}{2}],\ \alpha = 1 + i - i\theta,$$
where $\mathbb{Z}[i][\frac{1+\sqrt{5}}{2}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}[i]\}$.

Crossed product algebras

- Codes for *4 antennas*: take L/K, with

$$L = K(\sqrt{d}, \sqrt{d'}),\ \mathrm{Gal}(L/K) = \{1, \sigma, \tau, \sigma\tau\}.$$

Crossed product algebras

- Codes for *4 antennas*: take L/K, with

$$L = K(\sqrt{d}, \sqrt{d'}),\ \mathrm{Gal}(L/K) = \{1, \sigma, \tau, \sigma\tau\}.$$

- A *crossed product algebra* $\mathcal{A} = (a, b, u, L/K)$ over L/K:

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

with

$$e^2 = a,\ f^2 = b,\ fe = efu,\quad \lambda e = e\sigma(\lambda),$$
$$\lambda f = f\tau(\lambda) \text{ for all } \lambda \in L,$$

for some elements $a, b, u \in L^\times$ satisfying

$$\sigma(a) = a, \tau(b) = b, u\sigma(u) = \frac{a}{\tau(a)}, u\tau(u) = \frac{\sigma(b)}{b}.$$

Codewords from crossed product algebras

- Let $x = x_1 + ex_\sigma + fx_\tau + efx_{\sigma\tau} \in \mathcal{A}$. Its left *multiplication matrix* X is given by

$$\begin{pmatrix} x_1 & a\sigma(x_\sigma) & b\tau(x_\tau) & ab\tau(u)\sigma\tau(x_{\sigma\tau}) \\ x_\sigma & \sigma(x_1) & b\tau(x_{\sigma\tau}) & b\tau(u)\sigma\tau(x_\tau) \\ x_\tau & \tau(a)u\sigma(x_{\sigma\tau}) & \tau(x_1) & \tau(a)\sigma\tau(x_\sigma) \\ x_{\sigma\tau} & u\sigma(x_\tau) & \tau(x_\sigma) & \sigma\tau(x_1) \end{pmatrix}.$$

Codewords from crossed product algebras

- Let $x = x_1 + ex_\sigma + fx_\tau + efx_{\sigma\tau} \in \mathcal{A}$. Its left *multiplication matrix* X is given by

$$\begin{pmatrix} x_1 & a\sigma(x_\sigma) & b\tau(x_\tau) & ab\tau(u)\sigma\tau(x_{\sigma\tau}) \\ x_\sigma & \sigma(x_1) & b\tau(x_{\sigma\tau}) & b\tau(u)\sigma\tau(x_\tau) \\ x_\tau & \tau(a)u\sigma(x_{\sigma\tau}) & \tau(x_1) & \tau(a)\sigma\tau(x_\sigma) \\ x_{\sigma\tau} & u\sigma(x_\tau) & \tau(x_\sigma) & \sigma\tau(x_1) \end{pmatrix}.$$

- Such codewords are *fully-diverse* if $\mathcal{A}$ is a division algebras.

A criterion for full-diversity

Theorem. Let K be a number field, and let $\mathcal{A} = (a, b, u, L/K)$. Then the following conditions are equivalent:

1. $\mathcal{A}$ is a division algebra,
2. the quaternion algebra $(d, N_{K(\sqrt{d'})/K}(b))$ is not split,
3. the quaternion algebra $(d', N_{K(\sqrt{d})/K}(a))$ is not split.

Encoding

- Let $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ be a $\mathbb{Q}(i)$-basis of L, G be the matrix of the embeddings of the basis, $\mathbf{x} = (x_1, x_2, x_3, x_4)$ be 4 information symbols, $x = x_1\omega_1 + x_2\omega_2 + x_3\omega_3 + x_4\omega_4 \in L$.

Encoding

- Let $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ be a $\mathbb{Q}(i)$-basis of L, G be the matrix of the embeddings of the basis, $\mathbf{x} = (x_1, x_2, x_3, x_4)$ be 4 information symbols, $x = x_1\omega_1 + x_2\omega_2 + x_3\omega_3 + x_4\omega_4 \in L$.
- We encode 16 information symbols $G\mathbf{x}_1$, $G\mathbf{x}_\sigma$, $G\mathbf{x}_\tau$, $G\mathbf{x}_{\sigma\tau}$ with

$$G\mathbf{x} = (x, \sigma(x), \tau(x), \sigma\tau(x))^T.$$

Encoding

- Let $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ be a $\mathbb{Q}(i)$-basis of L, G be the matrix of the embeddings of the basis, $\mathbf{x} = (x_1, x_2, x_3, x_4)$ be 4 information symbols, $x = x_1\omega_1 + x_2\omega_2 + x_3\omega_3 + x_4\omega_4 \in L$.
- We encode 16 information symbols $G\mathbf{x}_1$, $G\mathbf{x}_\sigma$, $G\mathbf{x}_\tau$, $G\mathbf{x}_{\sigma\tau}$ with

$$G\mathbf{x} = (x, \sigma(x), \tau(x), \sigma\tau(x))^T.$$

- Define $\Gamma_1 = \mathbf{I}_4$, and Γ_j, $j = 2, 3, 4$ resp. as

$$\begin{pmatrix} 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \tau(a) \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & b & 0 \\ 0 & 0 & 0 & b\sigma(u) \\ 1 & 0 & 0 & 0 \\ 0 & \sigma\tau(u) & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & ab\sigma(u) \\ 0 & 0 & b & 0 \\ 0 & \tau(a)\tau(u) & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The codeword X is encoded as follows:

$$X = \Gamma_1 diag(G\mathbf{x}_1) + \Gamma_2 diag(G\mathbf{x}_\sigma) + \Gamma_3 diag(G\mathbf{x}_\tau) + \Gamma_4 diag(G\mathbf{x}_{\sigma\tau}).$$

Example of code

- Consider the algebra on $\mathbb{Q}(i)(\sqrt{2}, \sqrt{5})/\mathbb{Q}(i)$.
- We take

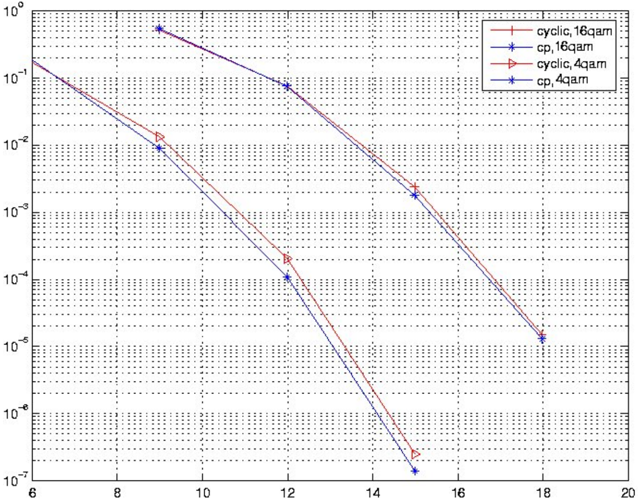
$$a = \zeta_8, \ b = \sqrt{\frac{1+2i}{1-2i}}, \ u = i.$$

Thus the encoding matrices Γ_i, $i = 2, 3, 4$ are *unitary*.

Example of code

- Consider the algebra on $\mathbb{Q}(i)(\sqrt{2},\sqrt{5})/\mathbb{Q}(i)$.
- We take
$$a=\zeta_8,\ b=\sqrt{\frac{1+2i}{1-2i}},\ u=i.$$
Thus the encoding matrices Γ_i, $i=2,3,4$ are *unitary*.
- We obtain a matrix G *unitary* by restricting to an ideal of L.
- This is a division algebra.

Comparison with previous codes



An Order View Point

- Replace copies of $\mathcal{O}_K$ by a maximal order with minimized discriminant.

[R. Vehkalahti, C. Hollanti, J. Lahtonen, K. Ranto, *On the densest MIMO lattices from cyclic division algebras*.]

Summary

To obtain fully diverse space-time codes from division algebras:

1. For n antennas, consider a cyclic extension of $\mathbb{Q}(i)$, or for $n = 4$, a biquadratic extension of $\mathbb{Q}(i)$. Construct a cyclic/crossed product division algebra.
2. Restrict coefficients to the ring of integers (minimum determinant).
3. Add lattices on each "layer".

Division Algebras
- Cyclic Algebras
- Crossed Product Algebras

Quotients of Space-Time Codes
- 2×2 Space-Time Coded Modulation

2×2 MIMO Slow Fading Channel

$$\underbrace{\mathbf{Y}}_{2\times 2L} = \underbrace{\mathbf{H}}_{2\times 2}\mathbf{X} + \underbrace{\mathbf{Z}}_{2\times 2L}$$

2×2 MIMO Slow Fading Channel

$$\underbrace{\mathbf{Y}}_{2\times 2L} = \underbrace{\mathbf{H}}_{2\times 2}\mathbf{X} + \underbrace{\mathbf{Z}}_{2\times 2L}$$

- $2L =$ frame length.
- $\mathbf{X} = [X_1, \ldots, X_L] \in \mathbb{C}^{2\times 2L}$.

Code Design Criteria

Design

$$\mathbf{X} = [X_1, \ldots, X_L] \in \mathbb{C}^{2\times 2L}$$

such that

1. X_i are fully diverse, $i = 1, \ldots, L$.
2. the minimum determinant

$$\begin{aligned}\Delta_{min} &= \min_{\mathbf{0}\neq\mathbf{X}} \det(\mathbf{X}\mathbf{X}^*) \\ &= \min_{\mathbf{0}\neq\mathbf{X}} \det(\sum_{i=1}^{L} X_i X_i^*) \\ &\geq \min_{\mathbf{0}\neq\mathbf{X}} (\sum_{i=1}^{L} |\det(X_i)|)^2\end{aligned}$$

is maximized.

Concatenated codes

1. Choose X_i, $i = 1, \ldots, L$ *independently*.

Concatenated codes

1. Choose X_i, $i = 1, \ldots, L$ *independently*.
2. Use a *concatenated code*:
   - *inner code* for diversity
   - *outer code* for coding gain

[L. Luzzi et al., *Golden Space-Time Block Coded Modulation*]

One example: the Golden Code $\mathcal{G}$

- The *inner code*:

$$X = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha(a+b\theta) & \alpha(c+d\theta) \\ i\sigma(\alpha)(c+d\sigma(\theta)) & \sigma(\alpha)(a+b\sigma(\theta)) \end{pmatrix} \in \mathcal{G}$$

- $a, b, c, d \in \mathbb{Z}[i]$, $\theta = \frac{1+\sqrt{5}}{2}$, $\sigma(\theta) = \frac{1-\sqrt{5}}{2}$, $\alpha = 1 + i - i\theta$ and $\sigma(\alpha) = 1 + i - i\sigma(\theta)$.

Coset codes

- We have $\mathcal{G} = \alpha(\mathbb{Z}[i,\theta] \oplus e\mathbb{Z}[i,\theta])$, $e^2 = i$ and (more later)

$$\mathcal{G}/(1+i)\mathcal{G} \simeq \mathcal{M}_2(\mathbb{F}_2).$$

Coset codes

- We have $\mathcal{G} = \alpha(\mathbb{Z}[i,\theta] \oplus e\mathbb{Z}[i,\theta])$, $e^2 = i$ and (more later)

$$\mathcal{G}/(1+i)\mathcal{G} \simeq \mathcal{M}_2(\mathbb{F}_2).$$

- Construct a code on $\mathcal{M}_2(\mathbb{F}_2)$ and lift it (*outer code*).

Coset codes

- We have $\mathcal{G} = \alpha(\mathbb{Z}[i,\theta] \oplus e\mathbb{Z}[i,\theta])$, $e^2 = i$ and (more later)

$$\mathcal{G}/(1+i)\mathcal{G} \simeq \mathcal{M}_2(\mathbb{F}_2).$$

- Construct a code on $\mathcal{M}_2(\mathbb{F}_2)$ and lift it (*outer code*).
- For a coset code (Luzzi et al.)

$$\Delta_{min} \geq \min_{\mathbf{0}\neq\mathbf{X}}(\sum_{i=1}^{L} |\det(X_i)|)^2 \geq \min\left(|1+i|^4\delta, d_{min}^2\delta\right),$$

$\delta=$ minimum determinant of $\mathcal{G}$, d_{min}=minimum distance.

Linking $\mathcal{M}_2(\mathbb{F}_2)$ and $\mathbb{F}_4$

- $\mathbb{F}_4 = \mathbb{F}_2(\omega)$, where $\omega^2 + \omega + 1 = 0$.

Linking $\mathcal{M}_2(\mathbb{F}_2)$ and $\mathbb{F}_4$

- $\mathbb{F}_4 = \mathbb{F}_2(\omega)$, where $\omega^2 + \omega + 1 = 0$.
- We have

$$\mathcal{M}_2(\mathbb{F}_2) \simeq \mathbb{F}_2(\omega) + \mathbb{F}_2(\omega)j \simeq \mathbb{F}_4 \times \mathbb{F}_4$$

where $j^2 = 1$ and $j\omega = \omega^2 j$, given by

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mapsto j, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \mapsto w.$$

Linking $\mathcal{M}_2(\mathbb{F}_2)$ and $\mathbb{F}_4$

- $\mathbb{F}_4 = \mathbb{F}_2(\omega)$, where $\omega^2 + \omega + 1 = 0$.
- We have

$$\mathcal{M}_2(\mathbb{F}_2) \simeq \mathbb{F}_2(\omega) + \mathbb{F}_2(\omega)j \simeq \mathbb{F}_4 \times \mathbb{F}_4$$

where $j^2 = 1$ and $j\omega = \omega^2 j$, given by

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mapsto j, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \mapsto w.$$

- This means:

$$\phi : (a, b) \in \mathbb{F}_4 \times \mathbb{F}_4 \mapsto M_{a,b} \in \mathcal{M}_2(\mathbb{F}_2).$$

An isometry between $\mathcal{M}_2(\mathbb{F}_2)$ and $\mathbb{F}_4$

- $\phi : (a, b) \in \mathbb{F}_4 \times \mathbb{F}_4 \mapsto M_{a,b} \in \mathcal{M}_2(\mathbb{F}_2)$ maps

  Hamming weight $1 \mapsto$ invertible.

An isometry between $\mathcal{M}_2(\mathbb{F}_2)$ and $\mathbb{F}_4$

- $\phi : (a, b) \in \mathbb{F}_4 \times \mathbb{F}_4 \mapsto M_{a,b} \in \mathcal{M}_2(\mathbb{F}_2)$ maps

  Hamming weight $1 \mapsto$ invertible.

- Define a weight on the matrices

$$w(M_{a,b}) = \begin{cases} 0 & M_{a,b} = 0 \\ 1 & M_{a,b} \text{invertible} \\ 2 & 0 \neq M_{a,b} \text{non-invertible} \end{cases} .$$

An isometry between $\mathcal{M}_2(\mathbb{F}_2)$ and $\mathbb{F}_4$

- $\phi : (a, b) \in \mathbb{F}_4 \times \mathbb{F}_4 \mapsto M_{a,b} \in \mathcal{M}_2(\mathbb{F}_2)$ maps

$$\text{Hamming weight } 1 \mapsto \text{invertible.}$$

- Define a weight on the matrices

$$w(M_{a,b}) = \begin{cases} 0 & M_{a,b} = 0 \\ 1 & M_{a,b} \text{invertible} \\ 2 & 0 \neq M_{a,b} \text{non-invertible} \end{cases}.$$

- ϕ is an isometry:

$$w(M_{a,b}) = w(\phi((a, b))) = w_H((a, b))$$

where w_H=Hamming weight.

Back to the outer code design

- For a coset code

$$\Delta_{min} \geq \min\left(4\delta, \frac{w_{min}^2}{2}\delta\right),$$

$\delta=$ minimum determinant of $\mathcal{G}$, w_{min}=minimum weight on code over $\mathbb{F}_4$.

Example

- Take the [6,3,4] hexacode over $\mathbb{F}_4$, with

$$y = (y_1, y_2, y_3, y_1 + \omega(y_2 + y_3), y_2 + \omega(y_1 + y_3), y_3 + \omega(y_1 + y_2)).$$

Example

- Take the [6,3,4] hexacode over $\mathbb{F}_4$, with

  $$y = (y_1, y_2, y_3, y_1 + \omega(y_2 + y_3), y_2 + \omega(y_1 + y_3), y_3 + \omega(y_1 + y_2)).$$

- Compute $\phi((y_1, y_2))$.

  $$\begin{aligned} (y_1, y_2) &\mapsto y_1 + y_2 j = (y_{11} + y_{12}\omega) + (y_{21} + y_{22}\omega) j \\ &\mapsto \begin{pmatrix} y_{11} & y_{12} \\ y_{12} & y_{11} + y_{12} \end{pmatrix} + \begin{pmatrix} y_{21} & y_{22} \\ y_{22} & y_{21} + y_{22} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= Y_1 \end{aligned}$$

- $$\phi(y) = (Y_1, Y_2, Y_3),$$

  with minimum weight $w_{min} = 4$.

Summary

- For coding for *MIMO slow fading channels*, joint design of an *inner and outer* code.

Summary

- For coding for *MIMO slow fading channels*, joint design of an *inner and outer* code.
- The outer code is a *coset code*, which addresses the problem of *codes over matrices*.

Summary

- For coding for *MIMO slow fading channels*, joint design of an *inner and outer* code.
- The outer code is a *coset code*, which addresses the problem of *codes over matrices*.
- Connection between *codes over matrices* and *codes over finite fields*.

Thank you for your attention!