Division Algebras: A Tool for Space-Time Coding

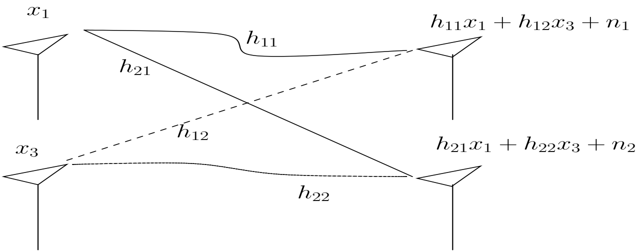
Frédérique Oggier
frederique@systems.caltech.edu

California Institute of Technology

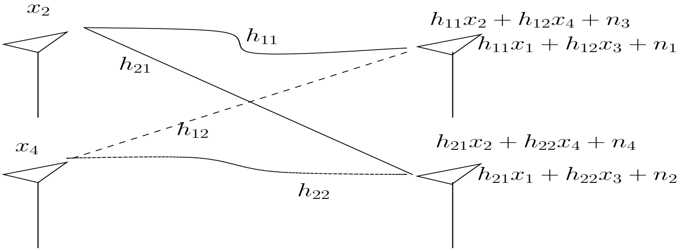
UCSD, CWC Seminar, February 17th 2006

Space-Time Coding

Space-Time Coding



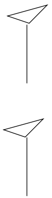
Space-Time Coding



Space-Time Coding:The model

$$\mathbf{Y} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} + \mathbf{W}, \ \mathbf{W}, \ \mathbf{H} \text{ complex Gaussian}$$

	time $T=1$	time $T=2$
	$h_{11}x_1 + h_{12}x_3 + n_1$	$h_{11}x_2 + h_{12}x_4 + n_3$
	$h_{21}x_1 + h_{22}x_3 + n_2$	$h_{11}x_2 + h_{12}x_4 + n_4$



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.

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

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

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

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.

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

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

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

A simplified problem

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

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

- Such a family $\mathcal{C}$ is said *fully-diverse*.
- Encoding, decoding

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*.
- Encoding, decoding

Outline

- Division Algebras
  - The idea behind Division Algebras
  - How to build Division Algebras
- The Golden Code
  - Cyclic Division Algebras
  - A 2×2 Space-Time Code
- Other applications
  - Differential Space-Time Coding
  - Wireless Relay Networks

The first ingredient: linearity

- 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 first ingredient: linearity

- 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 second ingredient: invertibility

- 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.

The second ingredient: invertibility

- 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.

The second ingredient: invertibility

- 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.

Division algebra: the definition

A *division algebra* is a non-commutative field.

The Hamiltonian Quaternions: the 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

$$\mathbb{H} = \{x + yi + zj + wk \mid x, y, z, w \in \mathbb{R}\}.$$

Hamiltonian Quaternions are a division algebra

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

$$\bar{q} = x - yi - zj - wk.$$

- Compute that

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

- The inverse of the quaternion q is given by

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

Hamiltonian Quaternions are a division algebra

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

$$\bar{q} = x - yi - zj - wk.$$

- Compute that

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

- The inverse of the quaternion q is given by

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

Hamiltonian Quaternions are a division algebra

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

$$\bar{q} = x - yi - zj - wk.$$

- Compute that

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

- The inverse of the quaternion q is given by

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

The Hamiltonian Quaternions: how to get matrices

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

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

- Now compute the *multiplication* by q:

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

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

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

The Hamiltonian Quaternions: how to get matrices

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

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

- Now compute the *multiplication* by q:

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

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

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

The Hamiltonian Quaternions: how to get matrices

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

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

- Now compute the *multiplication* by q:

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

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

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

The Hamiltonian Quaternions: the Alamouti Code

$$q = \alpha + j\beta,\ \alpha,\ \beta \in \mathbb{C} \Longleftrightarrow \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix}$$

Joint work with

Prof. Jean-Claude Belfiore, Ghaya Rekaya, ENST Paris, France.

Prof. Emanuele Viterbo, Politecnico di Torino, Italy.

Cyclic algebras: definition

- Let $L = \mathbb{Q}(i, \sqrt{d}) = \{u + \sqrt{d}v,\ u, v \in \mathbb{Q}(i)\}$. A *cyclic algebra* $\mathcal{A}$ is defined as follows

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

with $e^2 = \gamma$ and

$$\lambda e = e\sigma(\lambda) \text{ where } \sigma(u + \sqrt{d}v) = u - \sqrt{d}v.$$

- Recall that ($\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$)

$$\mathbb{H} = \mathbb{C} \oplus j\mathbb{C}$$

with

$$j^2 = -1 \text{ and } ij = -ji$$

Cyclic algebras: definition

- Let $L = \mathbb{Q}(i, \sqrt{d}) = \{u + \sqrt{d}v,\ u, v \in \mathbb{Q}(i)\}$. A *cyclic algebra* $\mathcal{A}$ is defined as follows

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

with $e^2 = \gamma$ and

$$\lambda e = e\sigma(\lambda) \text{ where } \sigma(u + \sqrt{d}v) = u - \sqrt{d}v.$$

- Recall that ($\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$)

$$\mathbb{H} = \mathbb{C} \oplus j\mathbb{C}$$

with

$$j^2 = -1 \text{ and } ij = -ji$$

Cyclic algebras: definition

- Let $L = \mathbb{Q}(i, \sqrt{d}) = \{u + \sqrt{d}v,\ u, v\ \in \mathbb{Q}(i)\}$. A *cyclic algebra* $\mathcal{A}$ is defined as follows

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

with $e^2 = \gamma$ and

$$\lambda e = e\sigma(\lambda) \text{ where } \sigma(u + \sqrt{d}v) = u - \sqrt{d}v.$$

- Recall that ($\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$)

$$\mathbb{H} = \mathbb{C} \oplus j\mathbb{C}$$

with

$$j^2 = -1 \text{ and } ij = -ji$$

Cyclic algebras: definition

- Let $L = \mathbb{Q}(i, \sqrt{d}) = \{u + \sqrt{d}v,\ u, v \ \in \mathbb{Q}(i)\}$. A *cyclic algebra* $\mathcal{A}$ is defined as follows

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

with $e^2 = \gamma$ and

$$\lambda e = e\sigma(\lambda) \text{ where } \sigma(u + \sqrt{d}v) = u - \sqrt{d}v.$$

- Recall that ($\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$)

$$\mathbb{H} = \mathbb{C} \oplus j\mathbb{C}$$

with

$$j^2 = -1 \text{ and } ij = -ji$$

Cyclic algebras: matrix formulation

- We associate to an element its *multiplication matrix*

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

- as we did for the Hamiltonian Quaternions.

$$q = \alpha + j\beta \in \mathbb{H} \leftrightarrow \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix}$$

Cyclic algebras: matrix formulation

- We associate to an element its *multiplication matrix*

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

- as we did for the Hamiltonian Quaternions.

$$q = \alpha + j\beta \in \mathbb{H} \leftrightarrow \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix}$$

The Golden Code: a 2 × 2 Space-Time Code

- The Golden code is related to the *Golden number* $\theta = \frac{1+\sqrt{5}}{2}$, a root of $x^2 - x - 1 = 0$ ($\sigma(\theta) = \bar{\theta} = \frac{1-\sqrt{5}}{2}$ is the other).
- 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: a 2 × 2 Space-Time Code

- The Golden code is related to the *Golden number* $\theta = \frac{1+\sqrt{5}}{2}$, a root of $x^2 - x - 1 = 0$ ($\sigma(\theta) = \bar{\theta} = \frac{1-\sqrt{5}}{2}$ is the other).
- 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: a 2 × 2 Space-Time Code

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

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

- $\mathcal{C}$ is a linear code, i.e., $\mathbf{X}_1 + \mathbf{X}_2 \in \mathcal{C}$ for all $\mathbf{X}_1, \mathbf{X}_2 \in \mathcal{C}$.
- The *minimum determinant* of $\mathcal{C}$ is given by

$$\delta_{\min}(\mathcal{C}) = \min_{\mathbf{X}_1 \neq \mathbf{X}_2 \in \mathcal{C}} |\det(\mathbf{X}_1 - \mathbf{X}_2)|^2 = \min_{\mathbf{0} \neq \mathbf{X} \in \mathcal{C}} |\det(\mathbf{X})|^2 \neq 0$$

by choice of $\mathcal{A}$, a *division algebra*.

The Golden code: minimum determinant

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

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

- $\mathcal{C}$ is a linear code, i.e., $\mathbf{X}_1 + \mathbf{X}_2 \in \mathcal{C}$ for all $\mathbf{X}_1, \mathbf{X}_2 \in \mathcal{C}$.
- The *minimum determinant* of $\mathcal{C}$ is given by

$$\delta_{\min}(\mathcal{C}) = \min_{\mathbf{X}_1 \neq \mathbf{X}_2 \in \mathcal{C}} |\det(\mathbf{X}_1 - \mathbf{X}_2)|^2 = \min_{\mathbf{0} \neq \mathbf{X} \in \mathcal{C}} |\det(\mathbf{X})|^2 \neq 0$$

by choice of $\mathcal{A}$, a *division algebra*.

The Golden code: minimum determinant

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

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

- $\mathcal{C}$ is a linear code, i.e., $\mathbf{X}_1 + \mathbf{X}_2 \in \mathcal{C}$ for all $\mathbf{X}_1, \mathbf{X}_2 \in \mathcal{C}$.
- The *minimum determinant* of $\mathcal{C}$ is given by

$$\delta_{\min}(\mathcal{C}) = \min_{\mathbf{X}_1 \neq \mathbf{X}_2 \in \mathcal{C}} |\det(\mathbf{X}_1 - \mathbf{X}_2)|^2 = \min_{\mathbf{0} \neq \mathbf{X} \in \mathcal{C}} |\det(\mathbf{X})|^2 \neq 0$$

by choice of $\mathcal{A}$, a *division algebra*.

The Golden code: minimum determinant

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

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

- $\mathcal{C}$ is a linear code, i.e., $\mathbf{X}_1 + \mathbf{X}_2 \in \mathcal{C}$ for all $\mathbf{X}_1, \mathbf{X}_2 \in \mathcal{C}$.
- The *minimum determinant* of $\mathcal{C}$ is given by

$$\delta_{\min}(\mathcal{C}) = \min_{\mathbf{X}_1 \neq \mathbf{X}_2 \in \mathcal{C}} |\det(\mathbf{X}_1 - \mathbf{X}_2)|^2 = \min_{\mathbf{0} \neq \mathbf{X} \in \mathcal{C}} |\det(\mathbf{X})|^2 \neq 0$$

by choice of $\mathcal{A}$, a *division algebra*.

The non-vanishing determinant property

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

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

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

- Thus

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

- Does *not* depend on the cardinality of $\mathcal{C}$.

The non-vanishing determinant property

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

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

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

- Thus

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

- Does *not* depend on the cardinality of $\mathcal{C}$.

The non-vanishing determinant property

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

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

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

- Thus

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

- Does *not* depend on the cardinality of $\mathcal{C}$.

The non-vanishing determinant property

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

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

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

- Thus

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

- Does *not* depend on the cardinality of $\mathcal{C}$.

The non-vanishing determinant property

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

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

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

- Thus

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

- Does *not* depend on the cardinality of $\mathcal{C}$.

The non-vanishing determinant property

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

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

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

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

- Does *not* depend on the cardinality of $\mathcal{C}$.

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 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 Golden code: encoding and rate

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

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

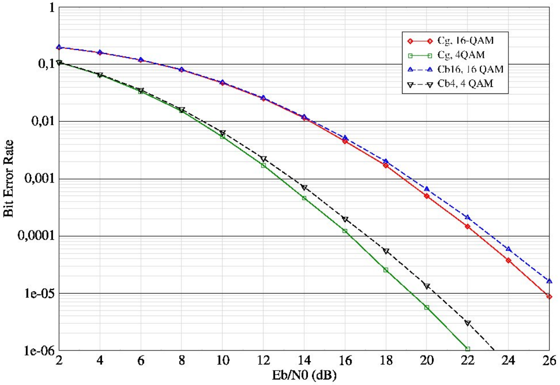
- The *finite code* $\mathcal{C}$ is obtained by limiting the *information symbols* to $a, b, c, d \in S \subset \mathbb{Z}[i]$ (QAM signal constellation).
- The code $\mathcal{C}$ is full rate.

Golden Code: summary of the properties

The Golden Code is a 2×2 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.

Decoding and 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.

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 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 $\mathbf{S}_0 = \mathbf{I}$)

$$\mathbf{S}_t = \mathbf{X}_{z_t}\mathbf{S}_{t-1},\ t = 1, 2, \ldots,$$

  where $z_t \in \{0, \ldots, L-1\}$ is the data to be transmitted, and $\mathcal{C} = \{\mathbf{X}_0, \ldots, \mathbf{X}_{L-1}\}$ the constellation to be designed.
- The matrices $\mathbf{X}$ have to be *unitary*.

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 $\mathbf{S}_0 = \mathbf{I}$)

$$\mathbf{S}_t = \mathbf{X}_{z_t}\mathbf{S}_{t-1},\ t = 1, 2, \ldots,$$

  where $z_t \in \{0, \ldots, L-1\}$ is the data to be transmitted, and $\mathcal{C} = \{\mathbf{X}_0, \ldots, \mathbf{X}_{L-1}\}$ the constellation to be designed.
- The matrices $\mathbf{X}$ have to be *unitary*.

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 $\mathbf{S}_0 = \mathbf{I}$)

$$\mathbf{S}_t = \mathbf{X}_{z_t}\mathbf{S}_{t-1},\ t = 1, 2, \ldots,$$

  where $z_t \in \{0, \ldots, L-1\}$ is the data to be transmitted, and $\mathcal{C} = \{\mathbf{X}_0, \ldots, \mathbf{X}_{L-1}\}$ the constellation to be designed.
- The matrices $\mathbf{X}$ have to be *unitary*.

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 $\mathbf{S}_0 = \mathbf{I}$)

$$\mathbf{S}_t = \mathbf{X}_{z_t}\mathbf{S}_{t-1},\ t = 1, 2, \ldots,$$

  where $z_t \in \{0, \ldots, L-1\}$ is the data to be transmitted, and $\mathcal{C} = \{\mathbf{X}_0, \ldots, \mathbf{X}_{L-1}\}$ the constellation to be designed.
- The matrices $\mathbf{X}$ have to be *unitary*.

The decoding

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

$$\begin{aligned}\mathbf{Y}_t &= \mathbf{S}_t\mathbf{H} + \mathbf{W}_t \\ &= \mathbf{X}_{z_t}\mathbf{S}_{t-1}\mathbf{H} + \mathbf{W}_t \\ &= \mathbf{X}_{z_t}(\mathbf{Y}_{t-1} - \mathbf{W}_{t-1}) + \mathbf{W}_t \\ &= \mathbf{X}_{z_t}\mathbf{Y}_{t-1} + \mathbf{W}'_t.\end{aligned}$$

- The matrix **H** does *not* appear in the last equation.
- The decoder is thus given by

$$\hat{z}_t = \arg\min_{l=0,\dots,|\mathcal{C}|-1} \|\mathbf{Y}_t - \mathbf{X}_l\mathbf{Y}_{t-1}\|.$$

The decoding

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

$$\begin{aligned}\mathbf{Y}_t &= \mathbf{S}_t\mathbf{H} + \mathbf{W}_t \\ &= \mathbf{X}_{z_t}\mathbf{S}_{t-1}\mathbf{H} + \mathbf{W}_t \\ &= \mathbf{X}_{z_t}(\mathbf{Y}_{t-1} - \mathbf{W}_{t-1}) + \mathbf{W}_t \\ &= \mathbf{X}_{z_t}\mathbf{Y}_{t-1} + \mathbf{W}'_t.\end{aligned}$$

- The matrix **H** does *not* appear in the last equation.
- The decoder is thus given by

$$\hat{z}_t = \arg \min_{l=0,\ldots,|\mathcal{C}|-1} \|\mathbf{Y}_t - \mathbf{X}_l\mathbf{Y}_{t-1}\|.$$

The decoding

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

$$\begin{aligned}\mathbf{Y}_t &= \mathbf{S}_t\mathbf{H}+\mathbf{W}_t\\ &= \mathbf{X}_{z_t}\mathbf{S}_{t-1}\mathbf{H}+\mathbf{W}_t\\ &= \mathbf{X}_{z_t}(\mathbf{Y}_{t-1}-\mathbf{W}_{t-1})+\mathbf{W}_t\\ &= \mathbf{X}_{z_t}\mathbf{Y}_{t-1}+\mathbf{W}'_t.\end{aligned}$$

- The matrix $\mathbf{H}$ does *not* appear in the last equation.
- The decoder is thus given by

$$\hat{z}_t = \arg\min_{l=0,\dots,|\mathcal{C}|-1} \|\mathbf{Y}_t - \mathbf{X}_l\mathbf{Y}_{t-1}\|.$$

Probability of error

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

$$P_e \leq \left(\frac{1}{2}\right)\left(\frac{8}{\rho}\right)^{MN}\frac{1}{|\det(\mathbf{X}_i - \mathbf{X}_j)|^{2N}}$$

- The quality of the code is measure by the *diversity product*

$$\zeta_{\mathcal{C}} = \frac{1}{2}\min_{\mathbf{X}_i \neq \mathbf{X}_j}|\det(\mathbf{X}_i - \mathbf{X}_j)|^{1/M} \qquad \forall\ \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}$$

Problem statement

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

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

Natural unitary matrices

- Recall that a matrix $\mathbf{X}$ in the algebra has the form

$$\begin{pmatrix} x_0 & x_1 \\ \gamma\sigma(x_1) & \sigma(x_0) \end{pmatrix}.$$

- There are *natural* unitary matrices:

$$E = \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix} \text{ and } D = \begin{pmatrix} x & 0 \\ 0 & \sigma(x) \end{pmatrix}, \ x \in L.$$

- If γ satisfies $\gamma\bar{\gamma} = 1$, then E^k, $k = 0, 1$, is unitary.
- If x satisfies $x\bar{x} = 1$, D and its powers will be unitary.
- Yields the constructions given by *fixed point free groups*.

Natural unitary matrices

- Recall that a matrix $\mathbf{X}$ in the algebra has the form

$$\begin{pmatrix} x_0 & x_1 \\ \gamma\sigma(x_1) & \sigma(x_0) \end{pmatrix}.$$

- There are *natural* unitary matrices:

$$E = \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix} \text{ and } D = \begin{pmatrix} x & 0 \\ 0 & \sigma(x) \end{pmatrix},\ x \in L.$$

- If γ satisfies $\gamma\bar{\gamma} = 1$, then E^k, $k = 0, 1$, is unitary.
- If x satisfies $x\bar{x} = 1$, D and its powers will be unitary.
- Yields the constructions given by *fixed point free groups*.

Natural unitary matrices

- Recall that a matrix $\mathbf{X}$ in the algebra has the form

$$\begin{pmatrix} x_0 & x_1 \\ \gamma\sigma(x_1) & \sigma(x_0) \end{pmatrix}.$$

- There are *natural* unitary matrices:

$$E = \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix} \text{ and } D = \begin{pmatrix} x & 0 \\ 0 & \sigma(x) \end{pmatrix},\ x \in L.$$

- If γ satisfies $\gamma\bar{\gamma} = 1$, then E^k, $k = 0, 1$, is unitary.
- If x satisfies $x\bar{x} = 1$, D and its powers will be unitary.
- Yields the constructions given by *fixed point free groups*.

Natural unitary matrices

- Recall that a matrix $\mathbf{X}$ in the algebra has the form

$$\begin{pmatrix} x_0 & x_1 \\ \gamma\sigma(x_1) & \sigma(x_0) \end{pmatrix}.$$

- There are *natural* unitary matrices:

$$E = \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix} \text{ and } D = \begin{pmatrix} x & 0 \\ 0 & \sigma(x) \end{pmatrix},\ x \in L.$$

- If γ satisfies $\gamma\bar{\gamma} = 1$, then E^k, $k = 0, 1$, is unitary.
- If x satisfies $x\bar{x} = 1$, D and its powers will be unitary.
- Yields the constructions given by *fixed point free groups*.

Applications to Wireless Relay Networks

- Distributed Space-Time Codes
  Each relay encodes a column of the Space-Time code.
- MIMO Amplify-and-Forward Cooperative Channel
  Each terminal is equipped with *multiple antennas*.

The diversity criterion holds.

Applications to Wireless Relay Networks

- Distributed Space-Time Codes
  Each relay encodes a column of the Space-Time code.
- MIMO Amplify-and-Forward Cooperative Channel
  Each terminal is equipped with *multiple antennas*.

The diversity criterion holds.

Thank you for your attention!