Cyclic algebras with involution: applications to unitary Space-Time coding

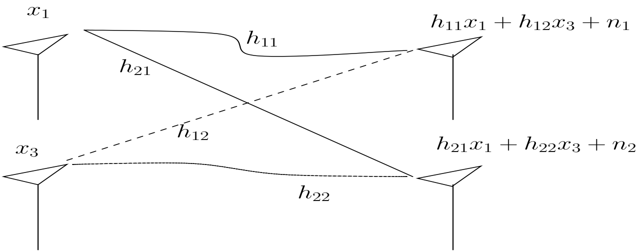
Frédérique Oggier
frederique@systems.caltech.edu

California Institute of Technology

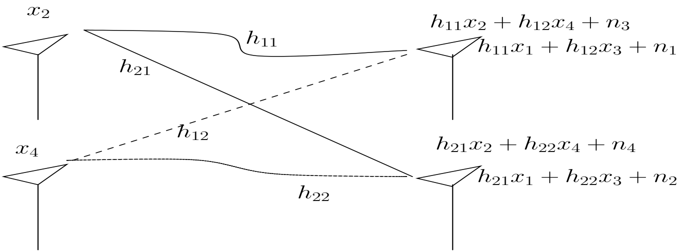
California State University of Northridge, Department of Mathematics, November 28th 2006

Space-Time Coding

Space-Time Coding

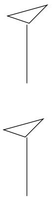


Space-Time Coding



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 $\mathcal{C}$:

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

the x_i are functions of the information symbols.

- Reliability is based on the *pairwise probability of error* of sending $\mathbf{X}$ and decoding $\hat{\mathbf{X}} \neq \mathbf{X}$.
- Assuming that the receiver knows the channel (called the *coherent case*), decoding consists of

$$\hat{\mathbf{X}} = \arg\min \|\mathbf{Y} - \mathbf{H}\mathbf{X}\|^2.$$

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.

- Reliability is based on the *pairwise probability of error* of sending $\mathbf{X}$ and decoding $\hat{\mathbf{X}} \neq \mathbf{X}$.
- Assuming that the receiver knows the channel (called the *coherent case*), decoding consists of

$$\hat{\mathbf{X}} = \arg\min \|\mathbf{Y} - \mathbf{HX}\|^2.$$

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.

- Reliability is based on the *pairwise probability of error* of sending $\mathbf{X}$ and decoding $\hat{\mathbf{X}} \neq \mathbf{X}$.
- Assuming that the receiver knows the channel (called the *coherent case*), decoding consists of

$$\hat{\mathbf{X}} = \arg\min \|\mathbf{Y} - \mathbf{HX}\|^2.$$

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

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

  where $z_t \in \{0, \dots, L-1\}$ is the data to be transmitted, and $\mathcal{C} = \{\mathbf{X}_0, \dots, \mathbf{X}_{L-1}\}$ 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 $\mathbf{S}_0 = \mathbf{I}$)

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

  where $z_t \in \{0, \dots, L-1\}$ is the data to be transmitted, and $\mathcal{C} = \{\mathbf{X}_0, \dots, \mathbf{X}_{L-1}\}$ 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

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

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

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

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

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

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*

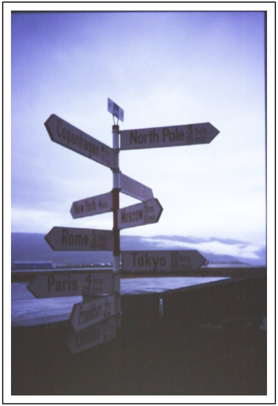
$$\zeta_{\mathcal{C}} = \frac{1}{2}\min_{\mathbf{X}_i \neq \mathbf{X}_j} |\det(\mathbf{X}_i - \mathbf{X}_j)|^{1/M} \qquad \forall\ \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}$$

Problem statement

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

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

Outline



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

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

Division Algebras
- The idea behind Division Algebras
- How to build Division Algebras

Cyclic Division Algebras
- Basic definitions and properties
- The unitary constraint

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*

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

- 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*

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

- as we did for the Hamiltonian Quaternions.

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

Codewords based on cyclic algebras

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

$$\mathcal{C} = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix} : x_0, x_1 \in L = \mathbb{Q}(i, \sqrt{d}) \right\}$$

- $\mathcal{C}$ 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*.

Codewords based on cyclic algebras

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

$$\mathcal{C} = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix} : x_0, x_1 \in L = \mathbb{Q}(i, \sqrt{d}) \right\}$$

- $\mathcal{C}$ 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*.

Codewords based on cyclic algebras

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

$$\mathcal{C} = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix} : x_0, x_1 \in L = \mathbb{Q}(i, \sqrt{d}) \right\}$$

- $\mathcal{C}$ 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*.

Codewords based on cyclic algebras

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

$$\mathcal{C} = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix} : x_0, x_1 \in L = \mathbb{Q}(i, \sqrt{d}) \right\}$$

- $\mathcal{C}$ 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*.

Encoding and rate

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

$$\mathcal{C} = \left\{ \begin{bmatrix} a + b\sqrt{d} & c + d\sqrt{d} \\ \gamma(c + d\sigma(\sqrt{d})) & a + b\sigma(\sqrt{d}) \end{bmatrix} : a, b, c, d \in \mathbb{Z}[i] \right\}$$

- 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.

Encoding and rate

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

$$\mathcal{C} = \left\{ \begin{bmatrix} a + b\sqrt{d} & c + d\sqrt{d} \\ \gamma(c + d\sigma(\sqrt{d})) & a + b\sigma(\sqrt{d}) \end{bmatrix} : a, b, c, d \in \mathbb{Z}[i] \right\}$$

- 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.

Encoding and rate

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

$$\mathcal{C} = \left\{ \begin{bmatrix} a + b\sqrt{d} & c + d\sqrt{d} \\ \gamma(c + d\sigma(\sqrt{d})) & a + b\sigma(\sqrt{d}) \end{bmatrix} : a, b, c, d \in \mathbb{Z}[i] \right\}$$

- 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.

So far...so good

Recall the *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.

Natural unitary matrices

- Recall that a matrix **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.

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.

A first family of unitary matrices (1)

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

$$E=\left(\begin{array}{ccc} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \zeta_3 & 0 & 0 \end{array}\right) \text{ and } D=\left(\begin{array}{ccc} \zeta_{21} & 0 & 0 \\ 0 & \zeta_{21}^4 & 0 \\ 0 & 0 & \zeta_{21}^{16} \end{array}\right),$$

$\sigma:\zeta_{21}\mapsto\zeta_{21}^4$.
- The family $\mathcal{C}=\{E^iD^j,\ i=0,1,2,\ j=0,\ldots,20\}$ 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 $\mathcal{C}$ is

$$R = \frac{\log_2(\#\mathcal{C})}{n} = \frac{\log_2(nm-1)}{n}.$$

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

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 $\mathcal{C}$ is

$$R = \frac{\log_2(\#\mathcal{C})}{n} = \frac{\log_2(nm-1)}{n}.$$

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

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 $\mathcal{C}$ is

$$R = \frac{\log_2(\#\mathcal{C})}{n} = \frac{\log_2(nm-1)}{n}.$$

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

Extending the construction (1)

- Recall that if $\bar{x}x = 1$ 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*

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

- We have

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

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

Translating the properties

the *cyclic algebra* $\mathcal{A}$ described formally

the *cyclic algebra* inside $\mathcal{M}_3(L)$

$$\begin{array}{ccc} & \mathcal{A} & \\ M_1 & L & M_2 \end{array}$$

the *subfields* of $\mathcal{A}$

The unitary constraint: summary

$$\alpha(x)x = 1 \iff N_{M/M^\alpha}(x) = 1 \iff \exists y \in M^* \text{ such that } x = y/\alpha(y).$$

the *cyclic algebra*
$\mathcal{A}$ described formally
$x\alpha(x) = 1,\ x \in \mathcal{A}$

$\longleftrightarrow$

the *cyclic algebra*
inside $\mathcal{M}_3(L)$
$\mathbf{X}\mathbf{X}^\dagger = \mathbf{I}_3,\ \mathbf{X} \in \mathcal{M}_3(L)$

$\updownarrow$

the *subfields* of $\mathcal{A}$

$$\begin{tikzcd}
 & \mathcal{A} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
M \arrow[d, dash] & L & M' \\
M^\alpha & &
\end{tikzcd}$$

A systematic procedure

1. Choose a cyclic algebra $\mathcal{A}$.
2. Take a commutative field M inside $\mathcal{A}$ with M^{α} as subfield.
3. Take an element y in M and compute $y/\alpha(y)$.
4. The corresponding matrix is unitary.

Extending the construction (2)

This simple result allows to construct codebooks of the form

$$\mathcal{C}(i) = \left\{ \begin{pmatrix} \zeta_{21} & 0 & 0 \\ 0 & \zeta_{21}^4 & 0 \\ 0 & 0 & \zeta_{21}^{16} \end{pmatrix}^l \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \zeta_3 & 0 & 0 \end{pmatrix}^k \begin{pmatrix} x & 0 & 0 \\ 0 & \sigma(x) & 0 \\ 0 & 0 & \sigma^2(x) \end{pmatrix}^i \right\},$$

$l = 0, \ldots, m-1,\ k = 0, \ldots, n-1$ with i varying into a chosen range, since x is no more a root of unity.

More generally

To increase the rate, one can consider

$$\mathcal{C}(i_1,\ldots,i_s)=\{D^lE^kF_1^{i_1}\cdots F_s^{i_s}\mid l=0,\ldots,m{-}1,\ k=0,\ldots,n{-}1\},$$

with $i_1,\ldots,i_s$ varying into a chosen range.

Conclusion

- Coding for wireless communication requires design of matrices with suitable properties.
- Cyclic division algebras have been proven to be a suitable tool for such code design.
- Endowed with a suitable involution, cyclic algebras are also useful for non-coherent space-time coding, which requires unitary matrices.

Conclusion

- Coding for wireless communication requires design of matrices with suitable properties.
- Cyclic division algebras have been proven to be a suitable tool for such code design.
- Endowed with a suitable involution, cyclic algebras are also useful for non-coherent space-time coding, which requires unitary matrices.

Conclusion

- Coding for wireless communication requires design of matrices with suitable properties.
- Cyclic division algebras have been proven to be a suitable tool for such code design.
- Endowed with a suitable involution, cyclic algebras are also useful for non-coherent space-time coding, which requires unitary matrices.

Thank you for your attention!