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

Outline

Communication Channel: Discrete Channel (I)

Sender, message= $\mathbf{x}$ $\rightarrow$ Channel $\rightarrow$ Receiver, message= $\mathbf{y}$

Communication Channel: Discrete Channel (I)

Sender, message=$\mathbf{x}$ → Channel → Receiver, message=$\mathbf{y}$

- Discrete Channel: $\mathbf{y} = \mathbf{x} + \mathbf{w}$, $\mathbf{x} \in \mathbb{F}_2^n$, $\mathbb{F}_2 = \{0, 1\}$, $\mathbf{w}$ models erasures or errors.

Communication Channel: Discrete Channel (I)

Sender, message=$\mathbf{x}$ $\rightarrow$ Channel $\rightarrow$ Receiver, message=$\mathbf{y}$

- Discrete Channel: $\mathbf{y} = \mathbf{x} + \mathbf{w}$, $\mathbf{x} \in \mathbb{F}_2^n$, $\mathbb{F}_2 = \{0, 1\}$, $\mathbf{w}$ models erasures or errors.
- Encoding: The sender encodes an information vector $\mathbf{u} \in \mathbb{F}_2^k$ into a codeword $\mathbf{x}$ belonging to a code $\mathcal{C}$.
- Decoding: The receiver compares $\mathbf{y}$ with the list of possible $\mathbf{x}$.

Communication Channel: Discrete Channel (II)

- For example: $\mathbf{u} \in \{00, 10, 01, 11\}$, $\mathbf{x} \in \{000, 101, 011, 110\}$.

Communication Channel: Discrete Channel (II)

- For example: $\mathbf{u} \in \{00, 10, 01, 11\}$, $\mathbf{x} \in \{000, 101, 011, 110\}$.
- Suppose there is one erasure: $\mathbf{y} = *00$. There is no doubt, $\mathbf{x} = 000$ and $\mathbf{u} = 00$.
- Suppose there is one error: $\mathbf{y} = 100$. It could have been $\mathbf{x} = 000, 110, 101$.

Communication Channel: Discrete Channel (II)

- For example: $\mathbf{u} \in \{00, 10, 01, 11\}$, $\mathbf{x} \in \{000, 101, 011, 110\}$.
- Suppose there is one erasure: $\mathbf{y} = *00$. There is no doubt, $\mathbf{x} = 000$ and $\mathbf{u} = 00$.
- Suppose there is one error: $\mathbf{y} = 100$. It could have been $\mathbf{x} = 000, 110, 101$.
- Design Criterion: Hamming distance (and rate).

Communication Channel: Gaussian Channel (I)

Sender, message=$\mathbf{x}$	$\rightarrow$	Channel	$\rightarrow$	Receiver, message=$\mathbf{y}$

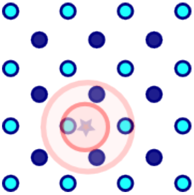
- Gaussian Channel (AWGN): $\mathbf{y} = \mathbf{x} + \mathbf{w} \in \mathbb{R}^n$, where $\mathbf{w}$ is Gaussian distributed.

Communication Channel: Gaussian Channel (I)

Sender, message=$\mathbf{x}$	$\rightarrow$	Channel	$\rightarrow$	Receiver, message=$\mathbf{y}$

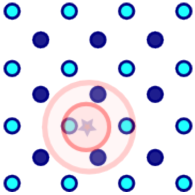
- Gaussian Channel (AWGN): $\mathbf{y} = \mathbf{x} + \mathbf{w} \in \mathbb{R}^n$, where $\mathbf{w}$ is Gaussian distributed.
- Decoding: The receiver compares $\mathbf{y}$ with the list of possible $\mathbf{x}$.

Communication Channel: Gaussian Channel (II)



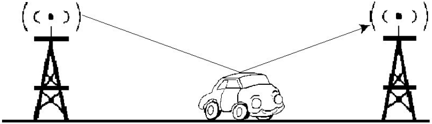
- The decoding is a closest neighbour decoding (Euclidean distance).

Communication Channel: Gaussian Channel (II)



- The decoding is a closest neighbour decoding (Euclidean distance).
- Knowing the noise variance, place the codewords accordingly.
- Energy constraint: this is packing problem.

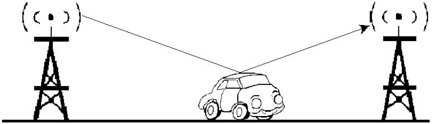
Communication Channel: Fading Channel (I)



Sender, message=$\mathbf{x}$ $\rightarrow$ Channel $\rightarrow$ Receiver, message=$\mathbf{y}$

- Fading Channel: $\mathbf{y} = \text{diag}(\mathbf{h})\mathbf{x} + \mathbf{w} \in \mathbb{R}^n$, $\mathbf{w} \sim \mathcal{N}(0, \sigma^2 I)$ is the noise and $\text{diag}(h_1, \ldots, h_n)$ is the channel *fading* matrix, h_i Rayleigh distributed.

Communication Channel: Fading Channel (I)

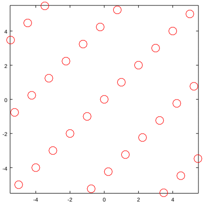


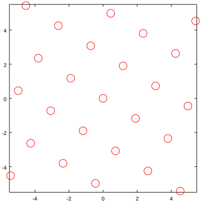
Sender, message=$\mathbf{x}$ → Channel → Receiver, message=$\mathbf{y}$

- Fading Channel: $\mathbf{y} = \mathrm{diag}(\mathbf{h})\mathbf{x} + \mathbf{w} \in \mathbb{R}^n$, $\mathbf{w} \sim \mathcal{N}(0, \sigma^2 I)$ is the noise and $\mathrm{diag}(h_1, \ldots, h_n)$ is the channel *fading* matrix, h_i Rayleigh distributed.
- Decoding: The receiver compares $\mathbf{y}$ with the list of possible $\mathbf{x}$, but knowing $\mathrm{diag}(\mathbf{h})$ is needed:

$$\hat{\mathbf{x}} = \arg \min_{\mathbf{x} \in S} \|\mathbf{y} - \mathbf{x}\mathrm{diag}(\mathbf{h})\|^2.$$

Communication Channel: Fading Channel (II)





- *Reliability* is modeled by the *pairwise probability of error*, bounded by

$$P(\mathbf{x} \to \hat{\mathbf{x}}) \leq \frac{1}{2} \prod_{x_i \neq \hat{x}_i} \frac{8\sigma^2}{(x_i - \hat{x}_i)^2} = \frac{1}{2} \frac{(8\sigma^2)^l}{\prod_{x_i \neq \hat{x}_i} |x_i - \hat{x}_i|^2}$$

  when the two codewords differ in l components.
- Design criterion: Maximize the *modulation diversity* $L = \min(l)$, ideally $L = n$.

[X. Giraud and J.-C. Belfiore, *Constellations Matched to the Rayleigh fading channel*, 1996.]

Algebraic lattices

- Let K be a number field of degree n and signature (r_1, r_2). The *canonical embedding* $\sigma : K \to \mathbb{R}^n$ is defined by

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \Re\sigma_{r_1+1}(\alpha), \Im\sigma_{r_1+1}(\alpha), \ldots)$$

Algebraic lattices

- Let K be a number field of degree n and signature (r_1, r_2). The *canonical embedding* $\sigma : K \to \mathbb{R}^n$ is defined by

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \Re\sigma_{r_1+1}(\alpha), \Im\sigma_{r_1+1}(\alpha), \ldots)$$

- Let $\mathcal{O}_K$ be the ring of integers of K with integral basis $\{\omega_1, \ldots, \omega_n\}$. An *algebraic lattice* $\Lambda = \sigma(\mathcal{O}_K)$ has *generator matrix*

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r_1}(\omega_1) & \ldots & \Im\sigma_{r_1+r_2}(\omega_1) \\ \vdots & & \vdots & & \vdots \\ \sigma_1(\omega_n) & \ldots & \sigma_n(\omega_{r_1}) & \ldots & \Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix}.$$

The modulation diversity

- Let K be a number field of signature (r_1, r_2).
  Theorem. Algebraic lattices exhibit a diversity

$$L = r_1 + r_2.$$

The modulation diversity

- Let K be a number field of signature (r_1, r_2).
  Theorem. Algebraic lattices exhibit a diversity

$$L = r_1 + r_2.$$

- In order to guarantee *maximal diversity*, we consider *totally real* number fields.

F. Oggier and E. Viterbo, *Algebraic number theory and code design for Rayleigh fading channels*.

A Quadratic Field

- Consider the ring $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \{a + b\frac{1+\sqrt{5}}{2},\ a, b \in \mathbb{Z}\}$.
- It is a subset of the field $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5},\ a, b \in \mathbb{Q}\}$.

A Quadratic Field

- Consider the ring $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \{a + b\frac{1+\sqrt{5}}{2},\ a, b \in \mathbb{Z}\}$.
- It is a subset of the field $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5},\ a, b \in \mathbb{Q}\}$.
- Intuitively, $\mathbb{Q}(\sqrt{5})$ is obtained from $\mathbb{Q}$ by adding $\sqrt{5}$, which is the root of the polynomial $X^2 - 5 = (X - \sqrt{5})(X + \sqrt{5})$.
- This gives us two ways of embedding $\mathbb{Q}(\sqrt{5})$ into $\mathbb{R}$:

$$\sigma_1 : \sqrt{5} \mapsto \sqrt{5},\ \sigma_2 : \sqrt{5} \mapsto -\sqrt{5}.$$

Its Corresponding Lattice (I)

- Embed $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ into $\mathbb{R}^2$ using the two embeddings σ_1, σ_2.
- We get a generator matrix

$$M = \begin{bmatrix} 1 & 1 \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix}$$

.

- The lattice is made of integral linear combinations of $(1, 1)$ and $(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2})$.

Its Corresponding Lattice (II)

- Its corresponding Gram matrix is

$$G = MM^T = \begin{bmatrix} 1 & 1 \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix} \begin{bmatrix} 1 & \sigma_1(\frac{1+\sqrt{5}}{2}) \\ 1 & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix}.$$

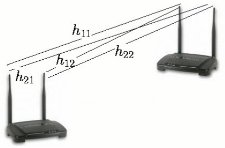
- Note that all entries are integers, because of the choice of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. In particular

$$(X - \tfrac{1+\sqrt{5}}{2})(X - \tfrac{1-\sqrt{5}}{2}) = X^2 - X + 1.$$

Summary so far

- What is the channel? which alphabet? how do we decode? code design.
- How to construct lattices from number fields (embeddings, $\mathbb{Z}$-basis).

MIMO Channel Model(I)

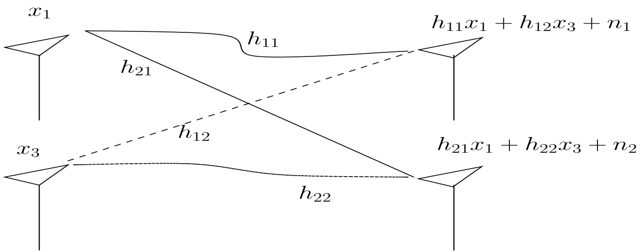


Sender, message=$\mathbf{x}$ $\rightarrow$ Channel $\rightarrow$ Receiver, message=$\mathbf{y}$

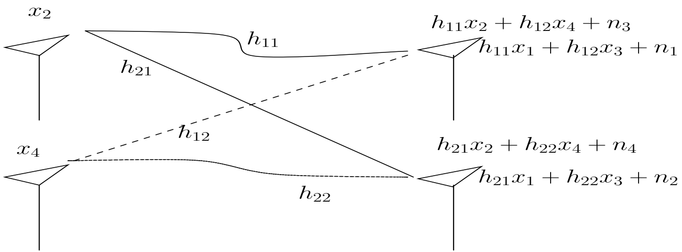
- Multiple Input Multiple Output

MIMO Channel Model (II)

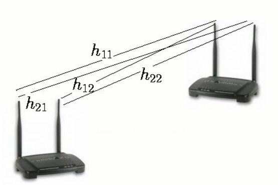
MIMO Channel Model (II)



MIMO Channel Model (II)



MIMO Channel Model (III)



1. At $t = 1, 2$, we get:

$$\underbrace{\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}}_{\mathbf{Y}} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \underbrace{\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}}_{space-time\ \ codeword\ \mathbf{X}} + \begin{pmatrix} n_1 & n_3 \\ n_2 & n_4 \end{pmatrix}.$$

[E. Telatar, *Capacity of multi-antenna Gaussian channels* , 1999.]

The Coding Problem

The goal is to obtain a family $\mathcal{C}$ of codewords:

$$\mathcal{C} = \left\{ \mathbf{X} = \underbrace{\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}}_{\textit{space-time codeword}} \middle| x_{11}, x_{12}, x_{21}, x_{22} \in \mathbb{C} \right\}$$

where the x_i are functions of the information symbols.

The Coding Problem

The goal is to obtain a family $\mathcal{C}$ of codewords:

$$\mathcal{C} = \left\{ \mathbf{X} = \underbrace{\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}}_{\text{space-time codeword}} \middle| x_{11}, x_{12}, x_{21}, x_{22} \in \mathbb{C} \right\}$$

where the x_i are functions of the information symbols.

- *Encoding* consists of associating the information symbols to the coefficients $x_{11}, x_{12}, x_{21}, x_{22}$.

The Coding Problem

The goal is to obtain a family $\mathcal{C}$ of codewords:

$$\mathcal{C} = \left\{ \mathbf{X} = \underbrace{\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}}_{\text{space-time codeword}} \middle| x_{11}, x_{12}, x_{21}, x_{22} \in \mathbb{C} \right\}$$

where the x_i are functions of the information symbols.

- *Encoding* consists of associating the information symbols to the coefficients $x_{11}, x_{12}, x_{21}, x_{22}$.
- *Decoding* consists of recovering the information symbols from the noisy coefficients $y_{11}, y_{12}, y_{21}, y_{22}$.

How to Design Space-Time Codes

- The *reliability* of a code $\mathcal{C}$ is modeled by the *probability* of sending $\mathbf{X}$ but of decoding $\hat{\mathbf{X}} \neq \mathbf{X}$.

How to Design Space-Time Codes

- The *reliability* of a code $\mathcal{C}$ is modeled by the *probability* of sending $\mathbf{X}$ but of decoding $\hat{\mathbf{X}} \neq \mathbf{X}$.
- This *pairwise error probability* (knowing $\mathbf{H}$) is upper bounded by

$$P(\mathbf{X} \to \hat{\mathbf{X}}) \leq f\left(SNR, |\det(\mathbf{X} - \hat{\mathbf{X}})|^{-1}\right).$$

where SNR=signal to noise ratio.

[V. Tarokh, N. Seshadri, A. R. Calderbank, *Space-time codes for high data rate wireless communications: Performance criterion and code construction*, 1998.]

Fading and Diversity

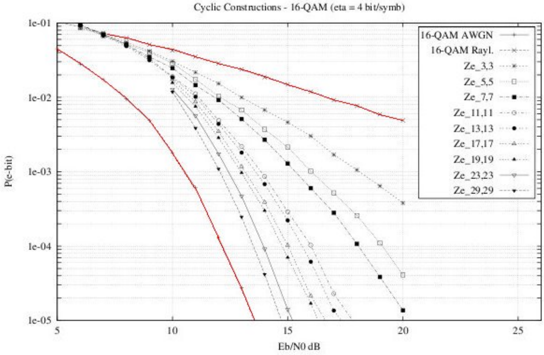
- Design a *fully-diverse* codebook $\mathcal{C}$ such that

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

Fading and Diversity

- Design a *fully-diverse* codebook $\mathcal{C}$ such that

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



Code Design Criterion

- We would like *fully diverse* codes:

$$\det(\mathbf{X}-\mathbf{X}') \neq 0 \quad \forall\, \mathbf{X} \neq \mathbf{X}'.$$

- Furthermore, we would like to maximize the *minimum determinant*

$$\min_{\mathbf{X}\neq\mathbf{X}'} |\det(\mathbf{X}-\mathbf{X}')|^2.$$

Code Design Criterion

- We would like *fully diverse* codes:

$$\det(\mathbf{X} - \mathbf{X}') \neq 0 \quad \forall\, \mathbf{X} \neq \mathbf{X}'.$$

- Furthermore, we would like to maximize the *minimum determinant*

$$\min_{\mathbf{X} \neq \mathbf{X}'} |\det(\mathbf{X} - \mathbf{X}')|^2.$$

[B. Hassibi and B.M. Hochwald, *High-Rate Codes That Are Linear in Space and Time*, 2002.
H. El Gamal and M.O. Damen, *Universal space-time coding* , 2003.]

Where Algebraists meet Engineers

- We need a family of matrices $\mathcal{C}$ such that

$$\det(\mathbf{X} - \mathbf{X}') \neq 0.$$

Where Algebraists meet Engineers

- We need a family of matrices $\mathcal{C}$ such that

$$\det(\mathbf{X} - \mathbf{X}') \neq 0.$$

- Such matrices can be found using *division algebras*.

  [A. Sethuraman, B. Sundar Rajan, V. Shashidar, *Full-diversity, high-rate space-time block codes from division algebras*, 2003]

The idea behind division algebras

- The difficulty: the *non-linearity* of the determinant

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

The idea behind division algebras

- The difficulty: the *non-linearity* of the determinant

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

- If $\mathcal{C}$ is taken inside an *algebra* of matrices, the problem simplifies to

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

The idea behind division algebras

- The difficulty: the *non-linearity* of the determinant

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

- If $\mathcal{C}$ is taken inside an *algebra* of matrices, the problem simplifies to

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

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

The Hamiltonian Quaternions: the definition (I)

- Recall: $\mathbb{C}$?

The Hamiltonian Quaternions: the definition (I)

- Recall: $\mathbb{C}$?
- $\mathbb{C}$=vector space of dimension 2 over $\mathbb{R}$, with basis

$$\{1, i\}.$$

The Hamiltonian Quaternions: the definition (I)

- Recall: $\mathbb{C}$?
- $\mathbb{C}$=vector space of dimension 2 over $\mathbb{R}$, with basis

$$\{1, i\}.$$

- $i^2 = -1.$

The Hamiltonian Quaternions: the definition (I)

- Recall: $\mathbb{C}$?
- $\mathbb{C}$=vector space of dimension 2 over $\mathbb{R}$, with basis

$$\{1, i\}.$$

- $i^2 = -1$.
- Now: $\mathbb{H}$?

The Hamiltonian Quaternions: the definition (I)

- Recall: $\mathbb{C}$?
- $\mathbb{C}$=vector space of dimension 2 over $\mathbb{R}$, with basis

$$\{1, i\}.$$

- $i^2 = -1$.
- Now: $\mathbb{H}$?
- $\mathbb{H}$=vector space of dimension 4 over $\mathbb{R}$, with basis

$$\{1, i, j, k\}.$$

The Hamiltonian Quaternions: the definition (I)

- Recall: $\mathbb{C}$?
- $\mathbb{C}$=vector space of dimension 2 over $\mathbb{R}$, with basis

$$\{1, i\}.$$

- $i^2 = -1$.
- Now: $\mathbb{H}$?
- $\mathbb{H}$=vector space of dimension 4 over $\mathbb{R}$, with basis

$$\{1, i, j, k\}.$$

- Rules: $i^2 = -1$, $j^2 = -1$, $k = ij = -ji$.

The Hamiltonian Quaternions: the definition (II)

Complex Numbers	*Hamiltonian Quaternions*
$\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}$	$\mathbb{H} = \{x + yi + zj + wk \mid x, y, z, w \in \mathbb{R}\}$

Hamiltonian Quaternions are a division algebra

- To see: $q = x + yi + wk \neq 0$ is invertible.

Hamiltonian Quaternions are a division algebra

- To see: $q = x + yi + wk \neq 0$ is invertible.
- Define the *conjugate* of q:

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

Hamiltonian Quaternions are a division algebra

- To see: $q = x + yi + wk \neq 0$ is invertible.
- Define the *conjugate* of q:

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

- Compute that

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

Hamiltonian Quaternions are a division algebra

- To see: $q = x + yi + wk \neq 0$ is invertible.
- Define the *conjugate* of q:

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

- 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

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

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:

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

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: Check list (I)

- 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 Hamiltonian Quaternions: Check list (I)

- Design of the codebook $\mathcal{C}$:

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

- Codebook from Quaternions:

$$\mathcal{C} = \left\{ \mathbf{X} = \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} | \alpha, \beta \in \mathbb{C} \right\}$$

The Hamiltonian Quaternions: Check list (II)

- Diversity:

$$\det(\mathbf{X} - \mathbf{X}') = ?$$

The Hamiltonian Quaternions: Check list (II)

- Diversity:

$$\det(\mathbf{X} - \mathbf{X}') = ?$$

- By linearity:

$$\det\left(\begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} - \begin{pmatrix} \alpha' & -\bar{\beta}' \\ \beta' & \bar{\alpha}' \end{pmatrix}\right) = \det\begin{pmatrix} \alpha - \alpha' & -(\overline{\beta - \beta'}) \\ \beta - \beta' & \overline{\alpha - \alpha'} \end{pmatrix}$$

The Hamiltonian Quaternions: Check list (III)

- Diversity:

$$\det(\mathbf{X} - \mathbf{X}') = \det \begin{pmatrix} \alpha - \alpha' & -(\overline{\beta - \beta'}) \\ \beta - \beta' & \overline{\alpha - \alpha'} \end{pmatrix} = 0$$
$$\iff |\alpha - \alpha'|^2 + |\beta - \beta|^2 = 0$$

The Hamiltonian Quaternions: the Alamouti Code

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

[S. M. Alamouti, "A simple transmit diversity technique for wireless communications", 1998.]

Summary

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.

Thank you for your attention!