Algebraic Space-Time Block Codes

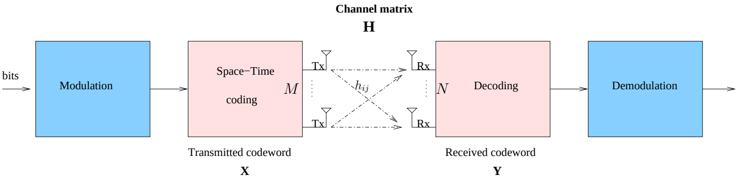
Ghaya Rekaya-Ben Othman

TELECOM ParisTech

Pisa 17 November 2008

Presentation outline

MIMO Transmission scheme



- Received signal : $\mathbf{Y}_{N\times T} = \mathbf{H}_{N\times M}.\mathbf{X}_{M\times T} + \mathbf{W}_{N\times T}$
- T (temporal code length) $= M$
- Block fading channel
- Perfect channel state information at the receiver (Coherent code)

STBC Design Criteria

- [Tarokh *et. al.*] proposed design criteria to construct good Space-Time Block Codes (STBC)
- Let $\mathbf{X}$ and $\mathbf{T}$ be two distinct codewords and $\mathbf{A} = \mathbf{X} - \mathbf{T}$. We define $\mathbf{B} = \mathbf{A}^H\mathbf{A}$. The pairwise error probability for quasi-static Rayleigh channel is asymptotically upper bounded by :

$$\mathrm{Prob}(\mathbf{X} \to \mathbf{T}) \leq \left(\prod_{i=1}^{r} \lambda_i\right)^{-N} \left(\frac{1}{\frac{E_S}{4N_0}}\right)^{rN}$$

where λ_i the eigenvalues of $\mathbf{B}$.

Rank criterion : in order to achieve maximum diversity MN, the matrix $\mathbf{A}$ must be of maximum rank M.

Coding Advantage : in order to maximize the coding gain, $\min_{c \neq T} \det(\mathbf{A})$ must be maximized.

Limitations of SM Scheme and Alamouti Code

- The Spatial Multiplexing Scheme for MIMO system with M transmit antennas and $N \geq M$ receive antennas have full rate but not full diversity.

Limitations of SM Scheme and Alamouti Code

- The Spatial Multiplexing Scheme for MIMO system with M transmit antennas and $N \geq M$ receive antennas have full rate but not full diversity.
- The Alamouti code, for a MIMO system with 2 transmit antennas and 1 receive antenna have full rate of 1sym/cu and full diversity of 2.

Limitations of SM Scheme and Alamouti Code

- The Spatial Multiplexing Scheme for MIMO system with M transmit antennas and $N \geq M$ receive antennas have full rate but not full diversity.
- The Alamouti code, for a MIMO system with 2 transmit antennas and 1 receive antenna have full rate of 1sym/cu and full diversity of 2.
- Full rate and full diversity Orthogonal Space-Time Block codes doesn't exist for a number of transmit antenna more than 2, and 1 receive antenna.

Limitations of SM Scheme and Alamouti Code

- The Spatial Multiplexing Scheme for MIMO system with M transmit antennas and $N \geq M$ receive antennas have full rate but not full diversity.
- The Alamouti code, for a MIMO system with 2 transmit antennas and 1 receive antenna have full rate of 1sym/cu and full diversity of 2.
- Full rate and full diversity Orthogonal Space-Time Block codes doesn't exist for a number of transmit antenna more than 2, and 1 receive antenna.
- The Alamouti code have the full diversity for a MIMO system with 2 transmit and 2 receive antennas, but is no more full rate.

Limitations of SM Scheme and Alamouti Code

- The Spatial Multiplexing Scheme for MIMO system with M transmit antennas and $N \geq M$ receive antennas have full rate but not full diversity.

- The Alamouti code, for a MIMO system with 2 transmit antennas and 1 receive antenna have full rate of 1sym/cu and full diversity of 2.

- Full rate and full diversity Orthogonal Space-Time Block codes doesn't exist for a number of transmit antenna more than 2, and 1 receive antenna.

- The Alamouti code have the full diversity for a MIMO system with 2 transmit and 2 receive antennas, but is no more full rate.

How to design full rate and full diversity STBC for MIMO system with M transmit antenna and N receive antennas ?

Limitations of SM Scheme and Alamouti Code

- The Spatial Multiplexing Scheme for MIMO system with M transmit antennas and $N \geq M$ receive antennas have full rate but not full diversity.
- The Alamouti code, for a MIMO system with 2 transmit antennas and 1 receive antenna have full rate of 1sym/cu and full diversity of 2.
- Full rate and full diversity Orthogonal Space-Time Block codes doesn't exist for a number of transmit antenna more than 2, and 1 receive antenna.
- The Alamouti code have the full diversity for a MIMO system with 2 transmit and 2 receive antennas, but is no more full rate.

How to design full rate and full diversity STBC for MIMO system with M transmit antenna and N receive antennas ?

For that we use Algebraic Tools.

Principle of DAST Codes

- DAST codes are Diagonal Algebraic Space Time Code designed for MIMO system with M transmit antennas and 1 receive antenna, that have :
  - **full rate** of 1sym/cu
  - **full diversity** of M

Principle of DAST Codes

- DAST codes are Diagonal Algebraic Space Time Code designed for MIMO system with M transmit antennas and 1 receive antenna, that have :
  - **full rate** of 1sym/cu
  - **full diversity** of M
- The Construction is based on unitary matrices constructed using number fields.
- Two steps of the construction:
  - Construction of an optimal unitary matrix of dimension M having the maximal diversity
  - Using Hadamard transformation to multiplex information symbols in space and in time.
- The construction is available for $M = 2$ and M multiple of 4.

2 × 2 DAST Code : unitary matrix construction

$$K = \mathbb{Q}(e^{\frac{i\pi}{4}}) \text{ number filed of degree 2 over } \mathbb{Q}(i).$$

- The minimum polynomial of $\theta = e^{\frac{i\pi}{4}}$ is $\mu_\theta(x) = X^2 - i$, its conjugate is $\overline{\theta} = -e^{\frac{i\pi}{4}}$.
- $B = (1, \theta)$ is the integral basis of K, each element x of K can be written as $x = a + b\theta,\ a,\ b \in \mathbb{Q}(i)$.
- Let $\sigma : \theta \mapsto -\theta$ be the generator of the Galois group of K
- Canonical embedding of K in $\mathbb{C}^2$is :

$$\begin{array}{llll} \sigma : & K & \longmapsto & \mathbb{C}^2 \\ & x & \longrightarrow & (x, \sigma(x)) \end{array}$$

- The lattice $\Lambda = \sigma(\mathcal{O}_K)$, where $\mathcal{O}_K$ the ring of integers $\mathcal{O}_K = \{a + b\theta, a, b \in \mathbb{Z}[i]\}$, have as generator matrix:

$$\mathbf{R} = \begin{bmatrix} 1 & 1 \\ \theta & \overline{\theta} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ e^{\frac{i\pi}{4}} & -e^{\frac{i\pi}{4}} \end{bmatrix}$$

- $\mathbf{R}' = \frac{1}{\sqrt{2}}\mathbf{R}$ is a unitary matrix of dimension 2.

2×2 DAST : Code construction (1)

- *First Step :*
  - Let $\mathbf{s} = (a_1, a_2)^T$ be the QAM information symbol vector
  - Vector $\mathbf{x}$ obtained by the rotation of vector $\mathbf{s}$ by $\mathbf{R}'$ is :

$$\mathbf{x} = \mathbf{R}' \cdot \mathbf{s} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \theta \\ 1 & -\theta \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + \theta a_2 \\ a_1 - \theta a_2 \end{bmatrix}$$

  - This operation alloaws to increase the algebraic dimension of the constellation, as K is a vector space of dimension 2 over $\mathbb{Q}(i)$.

2 × 2 DAST : Code construction (1)

- *First Step :*
  - Let $\mathbf{s} = (a_1, a_2)^T$ be the QAM information symbol vector
  - Vector $\mathbf{x}$ obtained by the rotation of vector $\mathbf{s}$ by $\mathbf{R}'$ is :

$$\mathbf{x} = \mathbf{R}' \cdot \mathbf{s} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \theta \\ 1 & -\theta \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + \theta a_2 \\ a_1 - \theta a_2 \end{bmatrix}$$

  - This operation alloaws to increase the algebraic dimension of the constellation, as K is a vector space of dimension 2 over $\mathbb{Q}(i)$.
  - The DAST codeword can be written in this form :

$$\mathbf{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + \theta a_2 & 0 \\ 0 & a_1 - \theta a_2 \end{bmatrix}$$

2×2 DAST : Code construction (2)

- *Second step :*
  - Hadamard matrix in dimension 2, verify $H_2^T \cdot H_2 = 2\mathbf{I}_2$ is :

$$\mathbf{H_2} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

  - A better balanced DAST codeword is :

$$\mathbf{X} = \mathbf{H_2} \cdot \mathrm{diag}(\mathbf{x}) = \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + \theta a_2 & -(a_1 - \theta a_2) \\ a_1 + \theta a_2 & a_1 - \theta a_2 \end{bmatrix}$$

- The coding gain is :

$$\delta(C) = \frac{1}{2} \min_{a_1 \neq a_2 \neq 0 \in S} (N_{K/\mathbb{Q}}(a_1 + \theta a_2)) \neq 0$$

$M \times M$ DAST : Code construction

- For MIMO System with $M = T$ multiple of 4 and $N = 1$.
- Construct an optimal unitary matrix of dimension M.
- Take $\mathbf{s} = (a_1, a_2, \ldots, a_M)^T$ QAM information symbol vector
- $\mathbf{H}_M$ is the Hadamard matrix in dimension M.
- The codeword matrix is :

$$\mathbf{X} = \mathbf{H}_M \cdot \mathrm{diag}(\mathbf{R} \cdot \mathbf{s})$$

Principle of TAST Codes

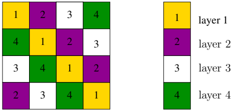
- TAST codes are Threaded Algebraic STBC designed for MIMO system with M transmit antennas and $N \geq M$, which have :
  - **Full rate** of M symbols/c.u
  - **Full diversity** of $M \cdot N$.

Principle of TAST Codes

- TAST codes are Threaded Algebraic STBC designed for MIMO system with M transmit antennas and $N \geq M$, which have :
  - **Full rate** of M symbols/c.u
  - **Full diversity** of $M \cdot N$.

- The idea is to design layered architecture code and to associate to each layer an algebraic sub-space (DAST Code), such that the layers are transparent to each others.

- An example of optimal layered architecture is :



2×2 TAST : Code construction

- We consider a MIMO system with $M = N = T = 2$
- $\mathbf{a} = (a_1, a_2, a_3, a_4)$ is the QAM information symbol vector.
- $\theta = \exp(i\lambda)$ with $\lambda \in \mathbb{R}$, and $\phi^2 = \theta$.
- A 2×2 DAST code is associated to each layer, and the two layers are separated by the parameter ϕ.

2×2 TAST : Code construction

- We consider a MIMO system with $M = N = T = 2$
- $\mathbf{a} = (a_1, a_2, a_3, a_4)$ is the QAM information symbol vector.
- $\theta = \exp(i\lambda)$ with $\lambda \in \mathbb{R}$, and $\phi^2 = \theta$.
- A 2×2 DAST code is associated to each layer, and the two layers are separated by the parameter ϕ.
- The codeword is:

$$\mathbf{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + \theta a_2 & \phi(a_3 + \theta a_4) \\ \phi(a_3 - \theta a_4) & a_1 - \theta a_2 \end{bmatrix}$$

- The coding gain is equal to : $\delta(C) = \frac{1}{2} \min(a_1^2 - a_3^2\theta - a_2^2\theta^2 + a_4^2\theta^3)$.

2×2 TAST : Code construction

- We consider a MIMO system with $M = N = T = 2$
- $\mathbf{a} = (a_1, a_2, a_3, a_4)$ is the QAM information symbol vector.
- $\theta = \exp(i\lambda)$ with $\lambda \in \mathbb{R}$, and $\phi^2 = \theta$.
- A 2×2 DAST code is associated to each layer, and the two layers are separated by the parameter ϕ.
- The codeword is:

$$\mathbf{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + \theta a_2 & \phi(a_3 + \theta a_4) \\ \phi(a_3 - \theta a_4) & a_1 - \theta a_2 \end{bmatrix}$$

- The coding gain is equal to : $\delta(C) = \frac{1}{2} \min(a_1^2 - a_3^2\theta - a_2^2\theta^2 + a_4^2\theta^3)$.
- Choice of θ:
  - To satisfy the rank criterion and so insure the full diversty, θ have to be choosing such that $\delta(C) \neq 0$.
  - Also, θ have be to be choosing to maximise $\delta(C)$ for a fixed constellation size.
  - θ could be an either algebraic or a transcendant number.

2×2 TAST Code : Coding Gain

- If θ is an algebraic number of degree 2 over $\mathbb{Q}(i)$, for example $\theta = e^{i\frac{\pi}{4}}$. As θ is not a norm of an element in $\mathcal{O}_K$, then :

$$\delta(C) = \frac{1}{2}\min(N_{K/\mathbb{Q}(i)}(x_1) - \theta N(x_2)_{K/\mathbb{Q}(i)}) \neq 0$$

where $x_1 = a_1 + a_2\theta$ and $x_2 = a_3 + a_4\theta$.

2×2 TAST Code : Coding Gain

- If θ is an algebraic number of degree 2 over $\mathbb{Q}(i)$, for example $\theta = e^{i\frac{\pi}{4}}$. As θ is not a norm of an element in $\mathcal{O}_K$, then :

$$\delta(C) = \frac{1}{2}\min(N_{K/\mathbb{Q}(i)}(x_1) - \theta N(x_2)_{K/\mathbb{Q}(i)}) \neq 0$$

where $x_1 = a_1 + a_2\theta$ and $x_2 = a_3 + a_4\theta$.

- If $\theta = e^{i\lambda}$ is transcendant, it is proved using Diophantine approximation that $\delta(C) \neq 0$. The values of λ maximizing the coding gain for a fixed constellation are obtained by numerical optimisation.

2×2 TAST Code : Coding Gain

- If θ is an algebraic number of degree 2 over $\mathbb{Q}(i)$, for example $\theta = e^{i\frac{\pi}{4}}$. As θ is not a norm of an element in $\mathcal{O}_K$, then :

$$\delta(C) = \frac{1}{2}\min(N_{K/\mathbb{Q}(i)}(x_1) - \theta N(x_2)_{K/\mathbb{Q}(i)}) \neq 0$$

where $x_1 = a_1 + a_2\theta$ and $x_2 = a_3 + a_4\theta$.

- If $\theta = e^{i\lambda}$ is transcendant, it is proved using Diophantine approximation that $\delta(C) \neq 0$. The values of λ maximizing the coding gain for a fixed constellation are obtained by numerical optimisation.

- For both cases the coding gain takes its values in $\mathbb{R}$.

2×2 TAST Code : Coding Gain

- If θ is an algebraic number of degree 2 over $\mathbb{Q}(i)$, for example $\theta = e^{i\frac{\pi}{4}}$. As θ is not a norm of an element in $\mathcal{O}_K$, then :

$$\delta(C) = \frac{1}{2}\min(N_{K/\mathbb{Q}(i)}(x_1) - \theta N(x_2)_{K/\mathbb{Q}(i)}) \neq 0$$

where $x_1 = a_1 + a_2\theta$ and $x_2 = a_3 + a_4\theta$.

- If $\theta = e^{i\lambda}$ is transcendant, it is proved using Diophantine approximation that $\delta(C) \neq 0$. The values of λ maximizing the coding gain for a fixed constellation are obtained by numerical optimisation.

- For both cases the coding gain takes its values in $\mathbb{R}$.

- Numerical optimisations lead to the values of λ giving the best coding gain

	$e^{i\frac{\pi}{8}}$	$e^{\frac{i}{2}}$	$e^{i0.448}$	$e^{i\frac{\pi}{4}}$
4-QAM	0.1304	0.2369	-	0.0858
16-QAM	0.059	0.0367	0.1397	0.0272

- The coding gain decreases when constellation size increases : **Vanishing Determinant**

$M \times M$ TAST : Code construction

- Let $K = \mathbb{Q}(i, \theta)$ be a cyclic extension of $\mathbb{Q}(i)$ of degree M, with $\theta = \exp(\frac{i\Pi}{2M})$.
- $B = (1, \theta, \ldots, \theta^{M-1})$ is an integral basis of K.
- K is a number field, unitary matrix **R** is obtained by canonical embedding of B in $\mathbb{C}^M$:

$$\mathbf{R} = \frac{1}{\sqrt{M}} \begin{bmatrix} 1 & \sigma(\theta) & \ldots & \sigma(\theta^{M-1}) \\ 1 & \sigma^2(\theta) & \ldots & \sigma^2(\theta^{M-1}) \\ 1 & \vdots & \ddots & \vdots \\ 1 & \sigma^{M-1}(\theta) & \ldots & \sigma^{M-1}(\theta^{M-1}) \end{bmatrix}$$

- Let $(a_1, \ldots, a_{M^2})$ be the QAM information symbol vector, divided in M vectors $\mathbf{v_1}, \ldots, \mathbf{v_M}$ of length M, and ϕ such that $\phi^M = \theta$.
- Construction of vectors $\beta_1, \ldots, \beta_{n_t}$, $\beta_i = \mathbf{R}.\mathbf{v}_i$.
- Matrix codeword is :

$$\mathbf{X} = (\phi^{|j-i|} \beta_{i,|j-i+1|})_{1 \le i,j \le M}$$

Principle of Quaternionic Codes

Quaternionic codes are STBC designed for MIMO systems with M transmit antenans and $N \geq M$ receive antennas, that have :

- **Full rate** : M symbols/c.u (q-QAM or q-HEX information symbols)
- **Full diversity** : diversity order $M \cdot N$
- **Non-Vanishing Determinants (NVD)** when spectral efficiency increases

For that we use Cyclic Division Algebras with center $L = \mathbb{Q}(i)$ or $L = \mathbb{Q}(j)$

2×2 Quaternionic : code construction (1)

- 2×2 Quaternionic code construction based on 2×2 TAST code
  - $\mathbf{a} = (a_1, a_2, a_3, a_4)$ QAM information symbol vector
  - $\theta = \exp(\frac{i\pi}{4})$
  - $\gamma \in K = \mathbb{Q}(e^{\frac{i\pi}{4}})$ the parameter used to separate the two layers
  - The codeword is:

$$\mathbf{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + \theta a_2 & (a_3 + \theta a_4) \\ \gamma(a_3 - \theta a_4) & a_1 - \theta a_2 \end{bmatrix}$$

  - The coding gain is equal to : $\delta(C) = \frac{1}{2} \min(N_{K/\mathbb{Q}(i)}(x_1) - \gamma N(x_2)_{K/\mathbb{Q}(i)})$

2×2 Quaternionic : code construction (1)

- 2×2 Quaternionic code construction based on 2×2 TAST code
  - $\mathbf{a} = (a_1, a_2, a_3, a_4)$ QAM information symbol vector
  - $\theta = \exp(\frac{i\pi}{4})$
  - $\gamma \in K = \mathbb{Q}(e^{\frac{i\pi}{4}})$ the parameter used to separate the two layers
  - The codeword is:
$$\mathbf{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + \theta a_2 & (a_3 + \theta a_4) \\ \gamma(a_3 - \theta a_4) & a_1 - \theta a_2 \end{bmatrix}$$
  - The coding gain is equal to : $\delta(C) = \frac{1}{2} \min(N_{K/\mathbb{Q}(i)}(x_1) - \gamma N(x_2)_{K/\mathbb{Q}(i)})$

- Choice of γ:
$$\begin{cases} \delta(C) \neq 0 & \Rightarrow \gamma \notin N(K^*) \\ \text{For non-vanishing determinant} & \Rightarrow \delta(C) \in \mathbb{Z}[i] \Rightarrow \gamma \in \mathbb{Z}[i] \end{cases}$$

2×2 Quaternionic : code construction (1)

- 2×2 Quaternionic code construction based on 2×2 TAST code
  - $\mathbf{a} = (a_1, a_2, a_3, a_4)$ QAM information symbol vector
  - $\theta = \exp(\frac{i\pi}{4})$
  - $\gamma \in K = \mathbb{Q}(e^{\frac{i\pi}{4}})$ the parameter used to separate the two layers
  - The codeword is:

$$\mathbf{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + \theta a_2 & (a_3 + \theta a_4) \\ \gamma(a_3 - \theta a_4) & a_1 - \theta a_2 \end{bmatrix}$$

  - The coding gain is equal to : $\delta(C) = \frac{1}{2} \min(N_{K/\mathbb{Q}(i)}(x_1) - \gamma N(x_2)_{K/\mathbb{Q}(i)})$

- Choice of γ:

$$\begin{cases} \delta(C) \neq 0 & \Rightarrow \gamma \notin N(K^*) \\ \text{For non-vanishing determinant} & \Rightarrow \delta(C) \in \mathbb{Z}[i] \Rightarrow \gamma \in \mathbb{Z}[i] \end{cases}$$

- We use ideal factorization :

$$5\mathbb{Z}[i] = (2 + i)(2 - i)$$

The Ideal $(2 + i)$ is a prime principal ideal, then taking $\gamma = 2 + i$ is a solution.

2×2 Quaternionic : Code construction (2)

- Codeword of the 2×2 Quaternionic Code is :

$$\mathbf{X} = \begin{bmatrix} a_1 + a_2\theta & a_3 + a_4\theta \\ (2+i)(a_3 - a_4\theta) & a_1 - a_2\theta \end{bmatrix}$$

- Coding gain:

$$\delta(C) = \mathbf{min} \left(N_{K/\mathbb{Q}(i)}(a_1 + a_2\theta) - (2+i)N_{K/\mathbb{Q}(i)}(a_3 + a_4\theta) \right) \in \mathbb{Z}[i] = 1$$

2×2 Quaternionic : Code construction (2)

- Codeword of the 2×2 Quaternionic Code is :

$$\mathbf{X} = \begin{bmatrix} a_1 + a_2\theta & a_3 + a_4\theta \\ (2+i)(a_3 - a_4\theta) & a_1 - a_2\theta \end{bmatrix}$$

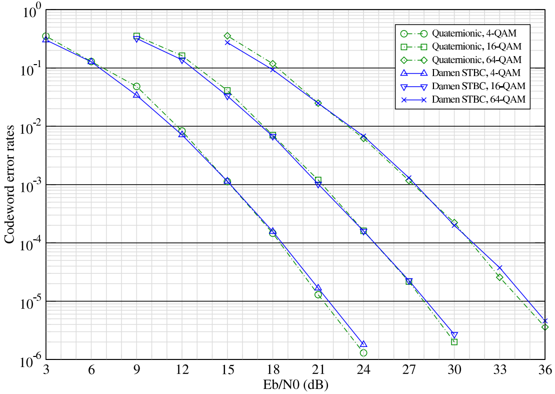
- Coding gain:

$$\delta(C) = \mathbf{min}\left(N_{K/\mathbb{Q}(i)}(a_1 + a_2\theta) - (2+i)N_{K/\mathbb{Q}(i)}(a_3 + a_4\theta)\right) \in \mathbb{Z}[i] = 1$$

- Let $\mathcal{A} = (K/L, \sigma, \gamma)$ be the Quaternion algebra $D_{i,\gamma}(L)$, where $L = \mathbb{Q}(i)$ is the base field (q-QAM information symbols), $K = \mathbb{Q}(e^{\frac{i\pi}{4}})$ cyclotomic extension, with $\theta = e^{\frac{i\pi}{4}}$, and$\sigma : \theta \mapsto -\theta$ the generator of the Galois group of K.

- The Quaternionic code C is a finite subset of $D_{i,\gamma}(L)$

2 × 2 Quaternionic Code : performance



Cyclic Division Algebras (1)

- Let K be a cyclic extension of L ($\mathbb{Q}(i)$ or $\mathbb{Q}(j)$) of degree M, with Galois group $\mathcal{G}_{K/L} = \langle \sigma \rangle$
- $\mathcal{A} = (K/L, \sigma, \gamma)$ is a cyclic algebra of degree M iff

$$\mathcal{A} = 1.K \oplus e.K \oplus \cdots \oplus e^{M-1}.K$$

$e \in \mathcal{A}$ such that $e^M = \gamma \in L$ and $x \cdot e = e \cdot \sigma(x)$.

Cyclic Division Algebras (1)

- Let K be a cyclic extension of L ($\mathbb{Q}(i)$ or $\mathbb{Q}(j)$) of degree M, with Galois group $\mathcal{G}_{K/L} = \langle \sigma \rangle$
- $\mathcal{A} = (K/L, \sigma, \gamma)$ is a cyclic algebra of degree M iff

$$\mathcal{A} = 1.K \oplus e.K \oplus \cdots \oplus e^{M-1}.K$$

$e \in \mathcal{A}$ such that $e^M = \gamma \in L$ and $x \cdot e = e \cdot \sigma(x)$.

- $\mathcal{A}$ is a **cyclic division algebra** iff $\gamma, \gamma^2, \cdots, \gamma^{M-1}$ are not norms in K^*
- Elements of $\mathcal{A}$ have matrix representation
- Non null elements of $\mathcal{A}$ have an inverse

$\Rightarrow$ A Space-Time code can be defined as a finite subset of $\mathcal{A}$

Cyclic Division Algebras (2)

- To obtain the matrix representation of Algebra elements, we define linear applications $\lambda_d : x \in \mathcal{A} \longmapsto d.x$, d element of $\mathcal{A}$.
- Example of cyclic division algebra of dimension 2:
  - Let $d = k_1 + ek_2$, where k_1 and k_2 are element of K.
  - $\lambda_d(1) = d = k_1 + ek_2$ and $\lambda_d(e) = (k_1 + ek_2).e = \gamma\sigma(k_2) + e\sigma(k_1)$:

$$M_d = \begin{bmatrix} k_1 & k_2 \\ \gamma\sigma(k_2) & \sigma(k_1) \end{bmatrix} = \begin{bmatrix} k_1 & 0 \\ 0 & \sigma(k_1) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} k_2 & 0 \\ 0 & \sigma(k_2) \end{bmatrix} \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix}$$

Cyclic Division Algebras (2)

- To obtain the matrix representation of Algebra elements, we define linear applications $\lambda_d : x \in \mathcal{A} \longmapsto d.x$, d element of $\mathcal{A}$.

- Example of cyclic division algebra of dimension 2:
  - Let $d = k_1 + ek_2$, where k_1 and k_2 are element of K.
  - $\lambda_d(1) = d = k_1 + ek_2$ and $\lambda_d(e) = (k_1 + ek_2).e = \gamma\sigma(k_2) + e\sigma(k_1)$:

$$M_d = \begin{bmatrix} k_1 & k_2 \\ \gamma\sigma(k_2) & \sigma(k_1) \end{bmatrix} = \begin{bmatrix} k_1 & 0 \\ 0 & \sigma(k_1) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} k_2 & 0 \\ 0 & \sigma(k_2) \end{bmatrix} \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix}$$

- In dimension M :

$$M_d = M_{k_1} I + M_{k_2} M_e + \cdots + M_{k_M} M_e^{M-1}$$

with $M_e = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ \gamma & \cdots & 0 & 0 \end{bmatrix}$ and $M_{k_i} = \begin{bmatrix} k_i & \cdots & 0 & 0 \\ \vdots & \sigma(k_i) & & 0 \\ 0 & & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma^{M-1}(k_i) \end{bmatrix}$

$M \times M$ Quaternionic : Code construction

1. Choice of base field : $L = \mathbb{Q}(i)$ (q-QAM constellations) or $L = \mathbb{Q}(j)$ (q-HEX constellations)

$M \times M$ Quaternionic : Code construction

1. Choice of base field : $L = \mathbb{Q}(i)$ (q-QAM constellations) or $L = \mathbb{Q}(j)$ (q-HEX constellations)

1. Choice of the extension field : K must be a cyclic extension of L of degree M, with Galois group $\mathcal{G}_{K/L} = \langle \sigma \rangle$

$M \times M$ Quaternionic : Code construction

1. Choice of base field : $L = \mathbb{Q}(i)$ (q-QAM constellations) or $L = \mathbb{Q}(j)$ (q-HEX constellations)

1. Choice of the extension field : K must be a cyclic extension of L of degree M, with Galois group $\mathcal{G}_{K/L} = \langle \sigma \rangle$

1. Definition of the cyclic algebra : $\mathcal{A} = (K/L, \sigma, \gamma)$ is a cyclic algebra of degree M

$M \times M$ Quaternionic : Code construction

1. Choice of base field : $L = \mathbb{Q}(i)$ (q-QAM constellations) or $L = \mathbb{Q}(j)$ (q-HEX constellations)

1. Choice of the extension field : K must be a cyclic extension of L of degree M, with Galois group $\mathcal{G}_{K/L} = \langle \sigma \rangle$

1. Definition of the cyclic algebra : $\mathcal{A} = (K/L, \sigma, \gamma)$ is a cyclic algebra of degree M

1. Choice of γ :

$$\begin{cases} \text{For non-vanishing determinants} \longrightarrow \gamma \in \mathcal{O}_L \\ \mathcal{A} \text{ be cyclic division algebra} \longrightarrow \gamma, \cdots \gamma^{M-1} \notin N(K^*) \end{cases}$$

$M \times M$ Quaternionic : Code construction

1. Choice of base field : $L = \mathbb{Q}(i)$ (q-QAM constellations) or $L = \mathbb{Q}(j)$ (q-HEX constellations)

1. Choice of the extension field : K must be a cyclic extension of L of degree M, with Galois group $\mathcal{G}_{K/L} = \langle \sigma \rangle$

1. Definition of the cyclic algebra : $\mathcal{A} = (K/L, \sigma, \gamma)$ is a cyclic algebra of degree M

1. Choice of γ :

$$\begin{cases} \text{For non-vanishing determinants} \longrightarrow \gamma \in \mathcal{O}_L \\ \mathcal{A} \text{ be cyclic division algebra} \longrightarrow \gamma, \cdots \gamma^{M-1} \notin N(K^*) \end{cases}$$

1. Construction of the ST code : the Quaternionic code is a finite subset of $\mathcal{A}$

$$\mathbf{X} = \begin{bmatrix} \sum_{i=1}^{M} a_{1,i} v_i & \sum_{i=1}^{M} a_{2,i} v_i & \cdots & \sum_{i=1}^{M} a_{M,i} v_i \\ \gamma\sigma(\sum_{i=1}^{M} a_{M,i} v_i) & \sigma(\sum_{i=1}^{M} a_{1,i} v_i) & \cdots & \sigma(\sum_{i=1}^{M} a_{M-1,i} v_i) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma\sigma^{M-1}(\sum_{i=1}^{M} a_{2,i} v_i) & \gamma\sigma^{M-1}(\sum_{i=1}^{M} a_{3,i} v_i) & \cdots & \sigma^{M-1}(\sum_{i=1}^{M} a_{1,i} v_i) \end{bmatrix}$$

$M \times M$ Quaternionic : code construction Validation

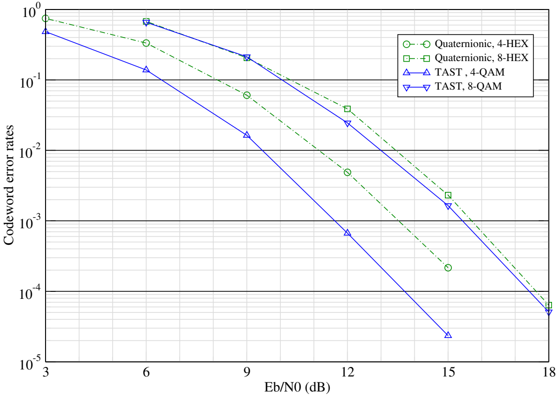
- **Full rate** : M symbols/c.u.
- **Full diversity** : $M \cdot N$
- **Non Vanishing Determinant** :
  - We have $\gamma \in \mathcal{O}_L$, and $a_{i,j} \in \mathcal{O}_L$ then $\sigma^l(s_{i,j}) \in \mathcal{O}_K \Rightarrow \det(\mathbf{X}) \in \mathcal{O}_K$
  - $\mathcal{A} = (K/L, \sigma, \gamma)$ is a cyclic division algebra, the reduced norm of an element of A (which is the determinant of X) belongs to L.

$$\det(\mathbf{X}) \in \mathcal{O}_K \cap L = \mathcal{O}_L$$

  - To obtain a discrete determinant : $\mathcal{O}_L = \mathbb{Z}[i]$ or $\mathbb{Z}[j]$.

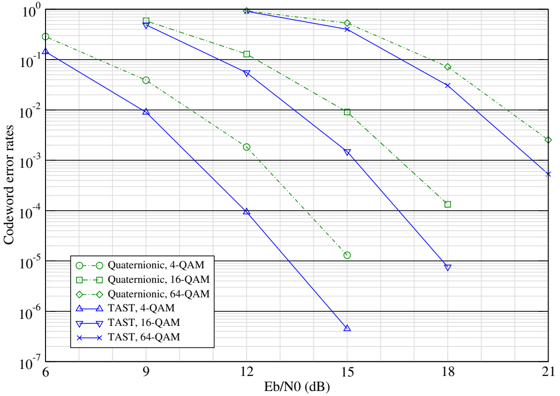
3×3 Quaternionic Code

- $L = \mathbb{Q}(j)$, $K = \mathbb{Q}(e^{\frac{i2\pi}{9}})$, $\theta = e^{\frac{i2\pi}{9}}$, $\sigma : \theta \mapsto j\theta$ and $\gamma = 3 + j$
- Quaternionic code 3×3 is a subset of the cyclic division algebra of degree 3, $\mathcal{A} = (K/L, \sigma, \gamma)$.



4×4 Quaternionic Code

- $L = \mathbb{Q}(i)$, $K = \mathbb{Q}(e^{\frac{i\pi}{16}})$, $\theta = e^{\frac{i\pi}{16}}$, $\sigma : \theta \mapsto i\theta$ and $\gamma = 2 + i$
- Quaternionic code 4×4 is a subset of the cyclic division algebra of degree 4 $\mathcal{A} = (K/L, \sigma, \gamma)$



Quaternionic Code : Achieved capacity

- The instantaneous MIMO channel capacity is :

$$C(\mathbf{H}) = \log_2 \det \left(\mathbf{I}_N + \frac{\mathrm{SNR}}{\mathrm{M}} \mathbf{H}\mathbf{H}^{\dagger} \right)$$

Quaternionic Code : Achieved capacity

- The instantaneous MIMO channel capacity is :

$$C(\mathbf{H}) = \log_2 \det\left(\mathbf{I}_N + \frac{\mathrm{SNR}}{\mathrm{M}}\mathbf{H}\mathbf{H}^\dagger\right)$$

- The instantaneous Channel capacity using STBC is :

$$C_{code}(\mathbf{H}) = \frac{1}{M}\log_2 \det\left(\mathbf{I}_{N.T} + \frac{\mathrm{SNR}}{\mathrm{M}}\mathbf{H_1}\Phi\Phi^\dagger\mathbf{H_1}^\dagger\right)$$

  - Example of 2×2 Quaternionic Code : the vectorisation of received signal, and isolation of information symbols lead to :

$$\begin{aligned}
\mathbf{y} &= \frac{1}{\sqrt{5}} \cdot \begin{bmatrix} \mathbf{H} & 0 \\ 0 & \mathbf{H} \end{bmatrix} \cdot \begin{bmatrix} 1 & \theta & 0 & 0 \\ 0 & 0 & 1 & \theta \\ 0 & 0 & \gamma & -\gamma\theta \\ 1 & -\theta & 0 & 0 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} + \mathbf{w} \\
&= \frac{1}{\sqrt{5}} \cdot \mathbf{H_1} \cdot \Phi \cdot \mathbf{s} + \mathbf{w}
\end{aligned}$$

Quaternionic Code : Achieved capacity

- The instantaneous MIMO channel capacity is :

$$C(\mathbf{H}) = \log_2 \det\left(\mathbf{I}_N + \frac{\text{SNR}}{\text{M}}\mathbf{H}\mathbf{H}^\dagger\right)$$

- The instantaneous Channel capacity using STBC is :

$$C_{code}(\mathbf{H}) = \frac{1}{M}\log_2 \det\left(\mathbf{I}_{N.T} + \frac{\text{SNR}}{\text{M}}\mathbf{H_1}\Phi\Phi^\dagger\mathbf{H_1}^\dagger\right)$$

  - Example of 2×2 Quaternionic Code : the vectorisation of received signal, and isolation of information symbols lead to :

$$\begin{aligned}\mathbf{y} &= \frac{1}{\sqrt{5}} \cdot \begin{bmatrix} \mathbf{H} & 0 \\ 0 & \mathbf{H} \end{bmatrix} \cdot \begin{bmatrix} 1 & \theta & 0 & 0 \\ 0 & 0 & 1 & \theta \\ 0 & 0 & \gamma & -\gamma\theta \\ 1 & -\theta & 0 & 0 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} + \mathbf{w} \\ &= \frac{1}{\sqrt{5}} \cdot \mathbf{H_1} \cdot \Phi \cdot \mathbf{s} + \mathbf{w}\end{aligned}$$

- The code is information lossless if $C_{code}(\mathbf{H}) = C(\mathbf{H})$, which is achieved if matrix Φ is unitary.

Quaternionic Code : Achieved capacity

- The instantaneous MIMO channel capacity is :

$$C(\mathbf{H}) = \log_2 \det \left(\mathbf{I}_N + \frac{\text{SNR}}{\text{M}} \mathbf{H}\mathbf{H}^\dagger \right)$$

- The instantaneous Channel capacity using STBC is :

$$C_{code}(\mathbf{H}) = \frac{1}{M} \log_2 \det \left(\mathbf{I}_{N.T} + \frac{\text{SNR}}{\text{M}} \mathbf{H_1} \Phi \Phi^\dagger \mathbf{H_1^\dagger} \right)$$

  - Example of 2×2 Quaternionic Code : the vectorisation of received signal, and isolation of information symbols lead to :

$$\begin{aligned} \mathbf{y} &= \frac{1}{\sqrt{5}} \cdot \begin{bmatrix} \mathbf{H} & 0 \\ 0 & \mathbf{H} \end{bmatrix} \cdot \begin{bmatrix} 1 & \theta & 0 & 0 \\ 0 & 0 & 1 & \theta \\ 0 & 0 & \gamma & -\gamma\theta \\ 1 & -\theta & 0 & 0 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} + \mathbf{w} \\ &= \frac{1}{\sqrt{5}} \cdot \mathbf{H_1} \cdot \Phi \cdot \mathbf{s} + \mathbf{w} \end{aligned}$$

- The code is information lossless if $C_{code}(\mathbf{H}) = C(\mathbf{H})$, which is achieved if matrix Φ is unitary.
- Unfortunately, Quaternionic codes are not information lossless, which explain their bad performances.

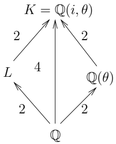
Principle of Perfect code

Perfect codes are STBC designed for MIMO systems with M transmit antenans and $N \geq M$ receive antennas, that have :

- **Full rate** (M symbols/c.u)
- **Full diversity** ($M \cdot N$)
- **Non-Vanishing Determinants** when the spectral efficiency increases
- **Energy efficiency**
  - Uniform energy distribution : the same average energy is transmitted by each antenna at each instant time
  - No shaping loss : the transmitted constellations have no shaping loss compared to signal constellation $\rightarrow$ Exploit the layered structure of the code constructed from division algebras: transmit on each layer a rotated version of $\mathbb{Z}[i]^M$ or A_2^M

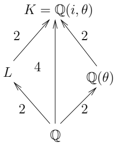
2×2 Perfect Code construction (1)

- Base field : $L = \mathbb{Q}(i)$ (q-QAM information symbols)
- Cyclic extension : let $\theta = \frac{1+\sqrt{5}}{2}$. Galois group $\mathcal{G}_{K/L} = \langle \sigma \rangle$, $\sigma : \theta \mapsto \bar{\theta} = \frac{1-\sqrt{5}}{2}$



2×2 Perfect Code construction (1)

- Base field : $L = \mathbb{Q}(i)$ (q-QAM information symbols)
- Cyclic extension : let $\theta = \frac{1+\sqrt{5}}{2}$. Galois group $\mathcal{G}_{K/L} = \langle \sigma \rangle$, $\sigma : \theta \mapsto \bar{\theta} = \frac{1-\sqrt{5}}{2}$

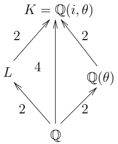


- As $\Lambda(\mathcal{O}_K)$ is not a rotated version of $\mathbb{Z}[i]^2$ we have to find an ideal $\mathcal{I}$ of $\mathcal{O}_K$ such that the lattice $\Lambda(\mathcal{I})$ is a rotated version of $\mathbb{Z}[i]^2$

$$\Rightarrow \mathcal{I} = (\alpha)\mathcal{O}_{\mathcal{K}} = (1 + i - i\theta)\mathcal{O}_K$$

2 × 2 Perfect Code construction (1)

- Base field : $L = \mathbb{Q}(i)$ (q-QAM information symbols)
- Cyclic extension : let $\theta = \frac{1+\sqrt{5}}{2}$. Galois group $\mathcal{G}_{K/L} = \langle\sigma\rangle$, $\sigma : \theta \mapsto \bar{\theta} = \frac{1-\sqrt{5}}{2}$



- As $\Lambda(\mathcal{O}_K)$ is not a rotated version of $\mathbb{Z}[i]^2$ we have to find an ideal $\mathcal{I}$ of $\mathcal{O}_K$ such that the lattice $\Lambda(\mathcal{I})$ is a rotated version of $\mathbb{Z}[i]^2$

$$\Rightarrow \mathcal{I} = (\alpha)\mathcal{O}_{\mathcal{K}} = (1 + i - i\theta)\mathcal{O}_K$$

- Choice of γ:

$$\begin{cases} \text{For non-vanishing determinants} \rightarrow \gamma \in \mathcal{O}_L \\ \text{For uniform energy distribution} \rightarrow |\gamma| = 1 \\ \mathcal{A} = (K/L, \sigma, \gamma) \text{ cyclic division algebra} \rightarrow \gamma \notin N(\mathbb{K}^*) \end{cases} \Rightarrow \text{ Solution } \gamma = \mathbf{i}$$

2×2 Perfect Code construction (2)

- 2×2 perfect code is a finite subset of the cyclic division algebra of degree 2, $\mathcal{A} = (K/L, \sigma, \gamma)$.

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(s_1 + \theta s_2) & 0 \\ 0 & \bar{\alpha}(s_1 + \bar{\theta} s_2) \end{bmatrix} \mathbf{I}_2 + \begin{bmatrix} \alpha(s_3 + \theta s_4) & 0 \\ 0 & \bar{\alpha}(s_3 + \bar{\theta} s_4) \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix}$$

- The codeword is :

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(s_1 + \theta s_2) & \alpha(s_3 + \theta s_4) \\ i\bar{\alpha}(s_3 + \bar{\theta} s_4) & \bar{\alpha}(s_1 + \bar{\theta} s_2) \end{bmatrix}$$

2×2 Perfect Code construction (2)

- 2×2 perfect code is a finite subset of the cyclic division algebra of degree 2, $\mathcal{A} = (K/L, \sigma, \gamma)$.

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(s_1 + \theta s_2) & 0 \\ 0 & \bar{\alpha}(s_1 + \bar{\theta} s_2) \end{bmatrix} \mathbf{I}_2 + \begin{bmatrix} \alpha(s_3 + \theta s_4) & 0 \\ 0 & \bar{\alpha}(s_3 + \bar{\theta} s_4) \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix}$$

- The codeword is :

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(s_1 + \theta s_2) & \alpha(s_3 + \theta s_4) \\ i\bar{\alpha}(s_3 + \bar{\theta} s_4) & \bar{\alpha}(s_1 + \bar{\theta} s_2) \end{bmatrix}$$

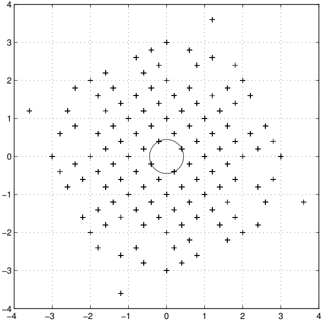
- 2×2 Perfect Code is called the **Golden Code**

- The Coding gain :

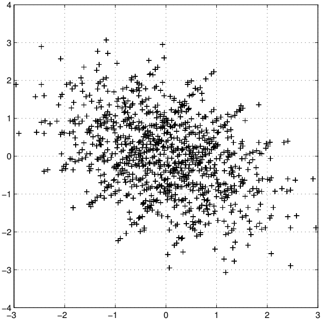
$$\delta(C) = \frac{1}{5^2} \left| N_{K/L}(\alpha) \right|^2 = \frac{1}{5} N_{K/\mathbb{Q}}(\alpha) = \frac{1}{5}$$

Determinant distributions

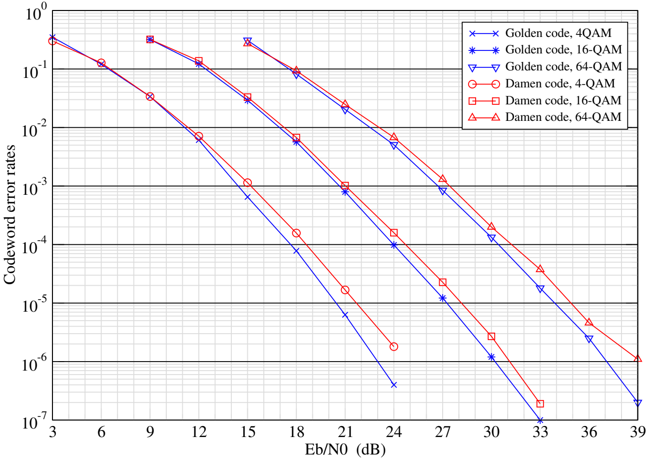
Golden code



TAST code 2×2



Golden code performance



$M \times M$ Perfect Code construction

1. Choice of base field : $L = \mathbb{Q}(i)$ or $L = \mathbb{Q}(j)$
2. Choice of field extension : K cyclic extension of L of degree M, σ the generator of the Galois group of K
3. Definition of the cyclic algebra : $\mathcal{A} = (K/L, \sigma, \gamma)$ is a cyclic algebra of degree M
4. Choice of γ :

$$\begin{cases} \text{For non-vanishing determinants} \rightarrow \gamma \in \mathcal{O}_L \\ \text{For uniform energy distribution} \rightarrow |\gamma| = 1 \\ \mathcal{A} \text{ be cyclic division algebra} \rightarrow \gamma, \cdots \gamma^{M-1} \notin N(\mathbb{K}^*) \end{cases}$$

5. Choice of the ideal : we must find an ideal $\mathcal{I}$ of $\mathcal{O}_K$, such that the lattice $\Lambda(\mathcal{I})$ is a rotated version of $\mathbb{Z}[i]^M$ or A_2^M.
6. Construction of the ST code : the ST code is a finite subset of $\mathcal{A}$.

$M \times M$ Perfect Code construction validation

- **Energy Efficiency** : Using the prime factorization of the discriminant $d_{K/\mathbb{Q}} = \prod p_k^{r_k}$, we can find an ideal $\mathcal{I}$ such that the volume of the real lattice $\Lambda^r(\mathcal{I})$ is

$$V\left(\Lambda^r(\mathcal{I})\right) = c^M \qquad \text{or} \qquad V\left(\Lambda^r(\mathcal{I})\right) = \left(\frac{\sqrt{3}}{2}\right)^M c^M$$

- **Non Vanishing Determinant** : The necessary assumptions needed to establish the proof of NVD for Quaternionic codes are still valid
  - if $\mathcal{I}$ is principal :

$$\delta(C) = N_{K/\mathbb{Q}}(\alpha) = \frac{1}{d_{\mathbb{Q}(\theta)}}$$

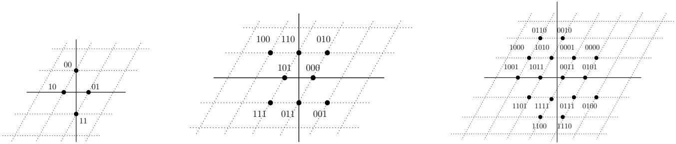
  - if $\mathcal{I}$ is not principal :

$$N(I) = \frac{1}{d_{\mathbb{Q}(\theta)}} \leq \delta(C) \leq \frac{1}{\mathrm{vol}\left(\Lambda^r(\mathcal{I})\right)} \min_{x \in \mathcal{I}} N_{K/\mathbb{Q}}(x)$$

Some Perfect Codes

- 3×3 Perfect code
  - $L = \mathbb{Q}(i)$, $K = \mathbb{Q}(i, \theta)$ with $\theta = 2\cos\left(\frac{2\pi}{15}\right)$
  - $\gamma = i$
  - $\mathcal{I} = (\alpha) = ((1 - 3i) + i\theta^2))$
  - $\delta_{\min}(C_\infty) = \frac{1}{1125}$
- 4×4 Perfect code
  - $L = \mathbb{Q}(j)$, $K = \mathbb{Q}(j, \theta)$ with $\theta = 2\cos\left(\frac{2\pi}{7}\right)$
  - $\gamma = j$
  - $\mathcal{I} = (\alpha) = ((1 + j) + \theta)$
  - $\delta_{\min}(C_\infty) = \frac{1}{49}$
- 6×6 Perfect code
  - $L = \mathbb{Q}(j)$, $K = \mathbb{Q}(j, \theta)$ with $\theta = 2\cos\left(\frac{\pi}{14}\right)$
  - $\gamma = -j$
  - $\mathcal{I}$ not principal
  - $\frac{1}{2^6 . 7^5} \leq \delta_{\min}(C_\infty) \leq \frac{1}{2^6 . 7^4}$

Hexagonal constellations



(a) 4-HEX (b) 8-HEX (c) 16-HEX

3 × 3 Perfect Code Performance