Space-Time Block Codes from Cyclic Division Algebras

Codes, Encoders and Decoders

Jean-Claude Belfiore

Dept Communications & Electronics
École Nationale Supérieure des Télécommunications (ENST)
46, rue Barrault, 75013 Paris, France
Email: belfiore@enst.fr
http://www.comelec.enst.fr/~belfiore

July, 18$^{\text{th}}$ 2006

Sequences and Codes
SFU, Vancouver, BC

Part I

Introduction

Outline

Paths recombination

- Each path is characterized by its magnitude α_i, its phase θ_i and its delay, τ_i.

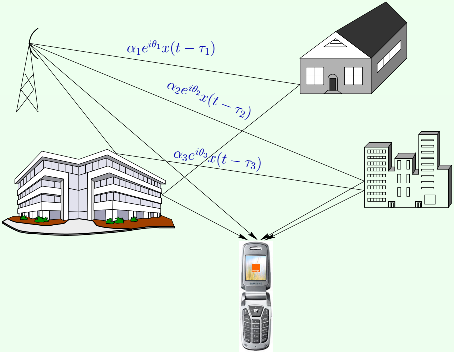


Figure: Destructive recombination due to phases $\longrightarrow$ *fadings* (here, $x(t)$ is the transmitted signal)

Phases dependencies

Phase terms

$$\theta_i = -2\pi f_0 \tau_i$$

where f_0 is the carrier (or subcarrier) frequency.

- Fadings vary as a function of
  - frequency
  - antennas position (since τ_i are different from one antenna to the other one)
  - time (obstacles and terminals may move)
  - ...

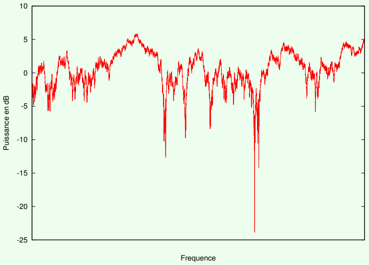


Figure: Received power as a function of the frequency

Outline

Diversity

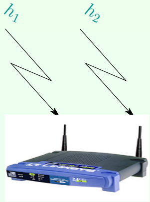
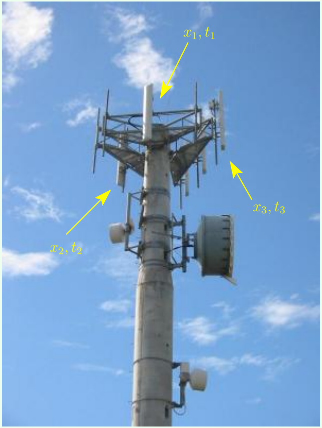


Figure: Access Point 802.11g : Selection of antenna 1 *iff* $|h_1|^2 > |h_2|^2$

- **Space diversity:** Selection or Maximum Ratio Combining
- **Time or Frequency or Space-Time diversity:** Same techniques, but transmitter must introduce redundancy on different time slots, frequencies, or antennas $\rightsquigarrow$ bad resource use.

Space-Time diversity



- Example of a GSM Base station
- At each time burst t_i, antenna i transmits burst x_i.
- Antennas are assumed spaced enough so that fadings can be assumed independent

Space-Time Coding

It is a primitive example of space-time coding

Outline

Error Correcting Codes vs Space-Time Codes

Error correcting codes

Codes defined on a finite alphabet (usually $\mathbb{F}_{2^m}$) $\in$ **Binary World**.

Error Correcting Codes vs Space-Time Codes

Error correcting codes

Codes defined on a finite alphabet (usually $\mathbb{F}_{2^m}$) $\in$ **Binary World**.

Space-Time Codes

Codes defined on $\mathbb{C}$. These codes act as an interface $\in$ **Signal space World**.

Error Correcting Codes vs Space-Time Codes

Error correcting codes

Codes defined on a finite alphabet (usually $\mathbb{F}_{2^m}$) $\in$ **Binary World**.

Space-Time Codes

Codes defined on $\mathbb{C}$. These codes act as an interface $\in$ **Signal space World**.

1. Inner "code" $\longrightarrow$ Space-Time Block Code
2. Outer "code" $\longrightarrow$ Binary (or non binary) code (Convolutional, Block, LDPC, Turbo,...)

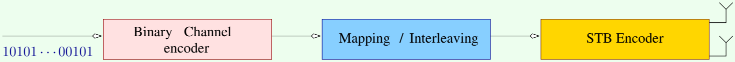


Figure: The MIMO communication chain

Part II

The MIMO Channel

Outline

The quasi static fading channel

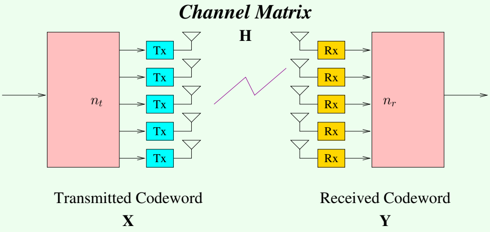


Figure: The Channel Model

- Received signal

$$\mathbf{Y}_{n_r \times T} = \mathbf{H}_{n_r \times n_t} \cdot \mathbf{X}_{n_t \times T} + \mathbf{W}_{n_r \times T} \quad (1)$$

  with **H** perfectly known at the receiver (coherent case).
- **H** is assumed constant during the transmission of one codeword.

Pairwise Error Probability

- Pairwise error probability for a quasi-static Rayleigh fading channel is upper bounded by

$$P(\mathbf{X_1} \to \mathbf{X_2}) \leq \left(\prod_{i=1}^{n_t} \frac{1}{1+\lambda_i^2 \frac{E_s}{4N_0}} \right)^{n_r} \quad (2)$$

with λ_i^2 being the eigenvalues of $(\mathbf{X}_1 - \mathbf{X}_2)^\dagger \cdot (\mathbf{X}_1 - \mathbf{X}_2)$ counting the multiplicities

Pairwise Error Probability

- Pairwise error probability for a quasi-static Rayleigh fading channel is upper bounded by

$$P\left(\mathbf{X_1} \to \mathbf{X_2}\right) \leq \left(\prod_{i=1}^{n_t} \frac{1}{1+\lambda_i^2 \frac{E_s}{4N_0}}\right)^{n_r} \tag{2}$$

with λ_i^2 being the eigenvalues of $(\mathbf{X}_1 - \mathbf{X}_2)^\dagger \cdot (\mathbf{X}_1 - \mathbf{X}_2)$ counting the multiplicities

- **Two criteria**
  - **The rank criterion** : In order to achieve maximum diversity $n_t \cdot n_r$, the matrix $(\mathbf{X}_1 - \mathbf{X}_2)$ must be of maximum rank n_t.
  - **The coding advantage** : In order to maximize the coding gain, the quantity

$$\min_{\mathbf{X_1} \neq \mathbf{X_2}} \det\left(\mathbf{X}_1 - \mathbf{X}_2\right)^\dagger \cdot \left(\mathbf{X}_1 - \mathbf{X}_2\right) \tag{3}$$

must be maximized.

Outline

The Gaussian MIMO channel

- Denote $\mathbf{Q}$ the covariance matrix of the Gaussian channel input $\mathbf{X}$,

$$\mathbf{Q} = \mathbb{E}\left[\mathbf{X}^{\dagger}\mathbf{X}\right].$$

Then, mutual information is

$$I(\mathbf{X};\mathbf{Y}) = \log_2 \det\left(\mathbf{I}_{n_r} + \frac{1}{\sigma^2}\mathbf{H}^{\dagger}\mathbf{Q}\mathbf{H}\right)$$

The Gaussian MIMO channel

- Denote **Q** the covariance matrix of the Gaussian channel input **X**,

$$\mathbf{Q} = \mathbb{E}\left[\mathbf{X}^{\dagger}\mathbf{X}\right].$$

Then, mutual information is

$$I(\mathbf{X};\mathbf{Y}) = \log_2 \det\left(\mathbf{I}_{n_r} + \frac{1}{\sigma^2}\mathbf{H}^{\dagger}\mathbf{Q}\mathbf{H}\right)$$

If we choose a channel entry such that $\mathbf{Q} = \frac{P_{\mathbf{X}}}{n_t}\mathbf{I}_{n_t}$, then we get,

$$I(\mathbf{X};\mathbf{Y}) = \log_2 \det\left(\mathbf{I}_{n_r} + \frac{\gamma}{n_t}\mathbf{H}^{\dagger}\mathbf{H}\right) \tag{4}$$

The ergodic capacity

- The channel varies fast enough so that the temporal and probabilistic averages are equal.
  - It does not correspond to a practical case
    - The channel must vary very fast
    - No delay constraint

The ergodic capacity

- The channel varies fast enough so that the temporal and probabilistic averages are equal.
  - It does not correspond to a practical case
    - The channel must vary very fast
    - No delay constraint

In this case, we get the ergodic capacity

$$\begin{aligned} C(\gamma) &= \mathbb{E}_{\mathbf{H}}\left[\log_2 \det\left(\mathbf{I}_{n_r} + \frac{\gamma}{n_t}\mathbf{H}^{\dagger}\mathbf{H}\right)\right] \\ &= \min\{n_t, n_r\}\log_2 \gamma + O(1) \end{aligned} \quad (5)$$

where $\min\{n_t, n_r\}$ is the number of degrees of freedom of the channel.

The outage probability (I)

- Consider $C(\mathbf{H})$ as the optimized mutual information for the MIMO Gaussian channel,

$$C(\mathbf{H}) = \log_2 \det\left(\mathbf{I}_{n_r} + \frac{\gamma}{n_t}\mathbf{H}^{\dagger}\mathbf{H}\right)$$

The outage probability (I)

- Consider $C(\mathbf{H})$ as the optimized mutual information for the MIMO Gaussian channel,

$$C(\mathbf{H}) = \log_2 \det \left(\mathbf{I}_{n_r} + \frac{\gamma}{n_t} \mathbf{H}^\dagger \mathbf{H} \right)$$

- We consider $C(\mathbf{H})$ as a random variable (Block Fading Channel)

The outage probability (I)

- Consider $C(\mathbf{H})$ as the optimized mutual information for the MIMO Gaussian channel,

$$C(\mathbf{H}) = \log_2 \det\left(\mathbf{I}_{n_r} + \frac{\gamma}{n_t}\mathbf{H}^\dagger\mathbf{H}\right)$$

- We consider $C(\mathbf{H})$ as a random variable (Block Fading Channel)
- The outage probability is

$$P_{\text{out}} = \Pr\{C(\mathbf{H}) \leq R\}$$

where R is the binary rate of the system.

The outage probability (II)

Asymptotic behavior

For a high SNR γ, we get

$$P_{\text{out}} = O\left(\frac{1}{\gamma^d}\right)$$

where d is the physical diversity of the system.

The outage probability (II)

Asymptotic behavior

For a high SNR γ, we get

$$P_{\text{out}} = O\left(\frac{1}{\gamma^d}\right)$$

where d is the physical diversity of the system.

- The physical diversity is the maximal obtainable order of diversity

The outage probability (II)

Asymptotic behavior

For a high SNR γ, we get

$$P_{\text{out}} = O\left(\frac{1}{\gamma^d}\right)$$

where d is the physical diversity of the system.

- The physical diversity is the maximal obtainable order of diversity
- For a quasistatic channel, and decorrelated transmit and receive antennas, we have

$$d = n_t \cdot n_r$$

The Diversity vs. Multiplexing Gain tradeoff (I)

- We have seen two main results
  - For ergodic channels, the capacity is asymptotically equal to

$$C(\gamma) = \min(n_t, n_r)\log_2 \gamma + O(1)$$

where $r = \min(n_t, n_r)$ is the number of degrees of freedom or the multiplexing gain of the system

The Diversity vs. Multiplexing Gain tradeoff (I)

- We have seen two main results
  - For ergodic channels, the capacity is asymptotically equal to

$$C(\gamma) = \min(n_t, n_r) \log_2 \gamma + O(1)$$

where $r = \min(n_t, n_r)$ is the number of degrees of freedom or the multiplexing gain of the system

For block fading channels, the outage probability is asymptotically equal to

$$P_{\text{out}} = O\left(\frac{1}{\gamma^d}\right)$$

where d is the diversity of the system.

The Diversity vs. Multiplexing Gain tradeoff (I)

- We have seen two main results
  - For ergodic channels, the capacity is asymptotically equal to

$$C(\gamma) = \min(n_t, n_r) \log_2 \gamma + O(1)$$

where $r = \min(n_t, n_r)$ is the number of degrees of freedom or the multiplexing gain of the system

For block fading channels, the outage probability is asymptotically equal to

$$P_{\text{out}} = O\left(\frac{1}{\gamma^d}\right)$$

where d is the diversity of the system.

- We are interested in block fading channels. Can we have both the diversity and the multiplexing gain ?

TELECOM PARIS école nationale supérieure des télécommunications

The Diversity vs. Multiplexing Gain tradeoff (I)

- We have seen two main results
  - For ergodic channels, the capacity is asymptotically equal to

$$C(\gamma) = \min(n_t, n_r) \log_2 \gamma + O(1)$$

    where $r = \min(n_t, n_r)$ is the number of degrees of freedom or the multiplexing gain of the system

For block fading channels, the outage probability is asymptotically equal to

$$P_{\text{out}} = O\left(\frac{1}{\gamma^d}\right)$$

where d is the diversity of the system.

- We are interested in block fading channels. Can we have both the diversity and the multiplexing gain ?

YES...but [Zheng Tse 2003]

We can both gain on r and d but there is a fundamental tradeoff between the two gains.

The Diversity vs. Multiplexing Gain tradeoff (II)

Definitions

Define the spatial multiplexing gain and the diversity gain

$$r = \lim_{\gamma \to \infty} \frac{R(\gamma)}{\log_2 \gamma} \quad d = -\lim_{\gamma \to \infty} \frac{\log P_e(\gamma)}{\log(\gamma)}.$$

Equivalently, we can write (exponential equality)

$$P_e(\gamma) \doteq \gamma^{-d}$$

The Diversity vs. Multiplexing Gain tradeoff (II)

Definitions

Define the spatial multiplexing gain and the diversity gain

$$r = \lim_{\gamma \to \infty} \frac{R(\gamma)}{\log_2 \gamma} \quad d = -\lim_{\gamma \to \infty} \frac{\log P_e(\gamma)}{\log(\gamma)}.$$

Equivalently, we can write (exponential equality)

$$P_e(\gamma) \doteq \gamma^{-d}$$

Theorem

The optimal tradeoff curve $d^*(r)$ is a piecewise-linear function connecting the points $d^*(k)$ for $k = 0, 1, \cdots, \min\{n_t, n_r\}$ where

$$d^*(k) = (n_t - k)(n_r - k)$$

The Diversity vs. Multiplexing Gain tradeoff (III)

$n_t = n_r = 4$

D-MG Tradeoff. Remark the extremal values: Maximum diversity 16 and maximum multiplexing gain 4

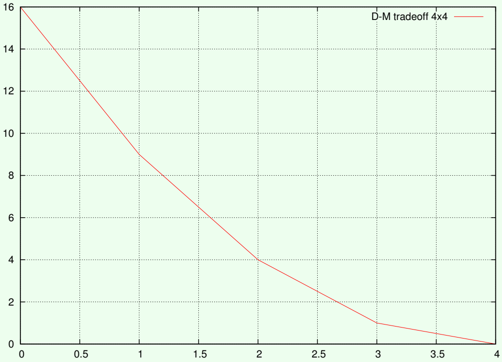


Figure: The D-MG tradeoff for $n_t = n_r = 4$

NVD Codes achieve the tradeoff (I)

Definition

Let $\mathscr{A}$ be an alphabet that is scalably dense, i.e.,

$$|\mathscr{A}(\mathsf{SNR})| \doteq \mathsf{SNR} \text{ and } a \in \mathscr{A}(\mathsf{SNR}) \Rightarrow |a|^2 \dot{\leq} \mathsf{SNR}.$$

Then, a $n_t \times n_t$ space-time code χ is called a rate-n NVD code if it

NVD Codes achieve the tradeoff (I)

Definition

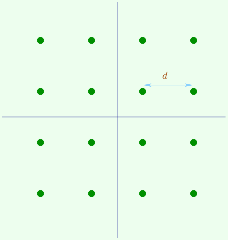
Let $\mathscr{A}$ be an alphabet that is scalably dense, i.e.,

$$|\mathscr{A}(\mathsf{SNR})| \doteq \mathsf{SNR} \text{ and } a \in \mathscr{A}(\mathsf{SNR}) \Rightarrow |a|^2 \dot{\leq} \mathsf{SNR}.$$

Then, a $n_t \times n_t$ space-time code χ is called a rate-n NVD code if it

1. is $\mathscr{A}$-linear
2. transmits on average n symbols **p**er **c**hannel **u**se (pcu) from the signal constellation $\mathscr{A}$.
3. has the non-vanishing determinant (NVD)[a] property.

[a] That means: a minimum determinant independent from the size of the constellation.



NVD Codes achieve the tradeoff (II)

Theorem

For any linear block fading channel

$$\mathbf{Y} = \mathbf{H} \cdot \mathbf{X} + \mathbf{Z}$$

where $\mathbf{H}$ *is a* $n_r \times n_t$ *channel with* $q = \min\{n_r, n_t\}$ *and* $\mathbf{Z}$ *is the AWGN with i.i.d. entries, the achievable D-M tradeoff of a rate-n NVD code* χ *satisfies*

$$d_{\chi}(r) \geq d_{out}\left(\frac{q}{n} r\right) \tag{6}$$

where $d_{out}(r)$ *is the outage upper bound of the D-M tradeoff for the channel* $\mathbf{H}$.

Outline

The Alamouti code and the D-M tradeoff

Properties of the Alamouti code

A codeword is

$$\mathbf{X} = \begin{bmatrix} s_1 & s_2 \\ -s_2^\star & s_1^\star \end{bmatrix} \quad (7)$$

with $s_1 = p_1 + iq_1$ and $s_2 = p_2 + iq_2$ being the 2 information symbols.

1. The code is linear
2. It has a non vanishing determinant (minimum Euclidean norm $|s_1|^2 + |s_2|^2$)
3. It is a rate-1 NVD code (1 symbol per channel use)

- It achieves the tradeoff $d_{\text{out}}(2r) = (2-2r)^+ \cdot (n_r - 2r)^+$.

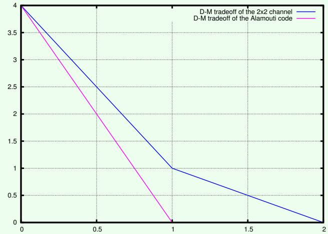


Figure: D-M tradeoff of the Alamouti code on the 2×2 channel

Cyclic division algebras (I)

- Let $\mathbb{F}$ be a field denoted the base field.
- Let $\mathbb{K}$ be a cyclic extension of degree n over $\mathbb{F}$. We define e such that $e^n = \gamma \in \mathbb{F}$ and

$$\forall z \in \mathbb{K}, z \cdot e = e \cdot \sigma(z)$$

  where σ is the generator of $\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$. Then a cyclic algebra is

$$\mathscr{A} = (\mathbb{K}/\mathbb{F}, \sigma, \gamma) = \left\{ \sum_{i=0}^{n-1} z_i e^i \quad z_i \in \mathbb{K} \right\}.$$

Cyclic division algebras (I)

- Let $\mathbb{F}$ be a field denoted the base field.
- Let $\mathbb{K}$ be a cyclic extension of degree n over $\mathbb{F}$. We define e such that $e^n = \gamma \in \mathbb{F}$ and

$$\forall z \in \mathbb{K}, z \cdot e = e \cdot \sigma(z)$$

where σ is the generator of $\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$. Then a cyclic algebra is

$$\mathscr{A} = (\mathbb{K}/\mathbb{F}, \sigma, \gamma) = \left\{ \sum_{i=0}^{n-1} z_i e^i \quad z_i \in \mathbb{K} \right\}.$$

Matrix Formulation in dimension 3

$$\mathbf{X}_z = \begin{bmatrix} z & 0 & 0 \\ 0 & \sigma(z) & 0 \\ 0 & 0 & \sigma^2(z) \end{bmatrix} \qquad \mathbf{X}_e = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \gamma & 0 & 0 \end{bmatrix} \tag{8}$$

$$\mathbf{X} = \begin{bmatrix} z_0 & z_1 & z_2 \\ \gamma\sigma(z_2) & \sigma(z_0) & \sigma(z_1) \\ \gamma\sigma^2(z_1) & \gamma\sigma^2(z_2) & \sigma^2(z_0) \end{bmatrix}$$

Cyclic division algebras (II)

Definition

A cyclic algebra is a division algebra (CDA) *iff* each non zero element has an inverse. A cyclic division algebra is also named "skew field".

Cyclic division algebras (II)

Definition

A cyclic algebra is a division algebra (CDA) *iff* each non zero element has an inverse. A cyclic division algebra is also named "skew field".

Theorem

If

$$\gamma, \gamma^2, \ldots, \gamma^{n-1} \notin N_{\mathbb{K}/\mathbb{Q}}(\mathbb{K})$$

then the algebra is a cyclic division algebra.

Alamouti code and CDAs

Alamouti

Take $\mathbb{F} = \mathbb{R}$, $\mathbb{K} = \mathbb{C}$, $\gamma = -1$. $\sigma : x \mapsto x^*$. The algebraic norm of x is $|x|^2$. -1 is not a norm. Finally, we get the cyclic division algebra

$$\mathscr{A} = (\mathbb{K}/\mathbb{F}, \sigma, \gamma) = \left\{ \begin{bmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{bmatrix}, \quad x_1, x_2 \in \mathbb{C} \right\}$$

which corresponds to the Alamouti scheme (Hamilton quaternions). If $x_k \in \mathbb{Z}[i]$ (QAM), then minimum squared determinant is in $\mathbb{Z}^+ \setminus \{0\}$ (rate-1 NVD code). Alamouti code is tradeoff achieving for 1 receive antenna.

Alamouti code and CDAs

Alamouti

Take $\mathbb{F} = \mathbb{R}$, $\mathbb{K} = \mathbb{C}$, $\gamma = -1$. $\sigma : x \mapsto x^*$. The algebraic norm of x is $|x|^2$. -1 is not a norm. Finally, we get the cyclic division algebra

$$\mathscr{A} = (\mathbb{K}/\mathbb{F}, \sigma, \gamma) = \left\{ \begin{bmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{bmatrix}, \quad x_1, x_2 \in \mathbb{C} \right\}$$

which corresponds to the Alamouti scheme (Hamilton quaternions). If $x_k \in \mathbb{Z}[i]$ (QAM), then minimum squared determinant is in $\mathbb{Z}^+ \setminus \{0\}$ (rate-1 NVD code). Alamouti code is tradeoff achieving for 1 receive antenna.

2 receive antennas

- We would like in fact a rate-2 NVD code.
- **Idea:** Find another CDA on another base field.

Part III

From the Golden code to Perfect STBCs

Outline

The Golden algebra

- Take as a base field $\mathbb{F} = \mathbb{Q}(i)$. The extension of degree 2 over $\mathbb{F}$ is $\mathbb{Q}\left(i, \sqrt{5}\right)$. $\gamma = i \in \mathbb{Z}[i]$.

The Golden algebra

- Take as a base field $\mathbb{F} = \mathbb{Q}(i)$. The extension of degree 2 over $\mathbb{F}$ is $\mathbb{Q}\left(i, \sqrt{5}\right)$. $\gamma = i \in \mathbb{Z}[i]$.
- Generator of Galois group is $\sigma : \sqrt{5} \mapsto -\sqrt{5}$.

The Golden algebra

- Take as a base field $\mathbb{F} = \mathbb{Q}(i)$. The extension of degree 2 over $\mathbb{F}$ is $\mathbb{Q}\left(i, \sqrt{5}\right)$. $\gamma = i \in \mathbb{Z}[i]$.
- Generator of Galois group is $\sigma : \sqrt{5} \mapsto -\sqrt{5}$.

Matrix representation

$$\begin{pmatrix} a_1 + a_2\sqrt{5} & a_3 + a_4\sqrt{5} \\ i\left(a_3 - a_4\sqrt{5}\right) & a_1 - a_2\sqrt{5} \end{pmatrix}$$

with $a_k \in \mathbb{F} = \mathbb{Q}(i)$.

The Golden Code [Belfiore Rekaya Viterbo 04/05]

Rate-2 NVD Code

Codewords of the Golden Code are

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha\,(z_1 + z_2\theta) & \alpha\,(z_3 + z_4\theta) \\ i \cdot \bar{\alpha}\,(z_3 + z_4\bar{\theta}) & \bar{\alpha}\,(z_1 + z_2\bar{\theta}) \end{pmatrix} \tag{9}$$

with $\theta = \frac{1+\sqrt{5}}{2}$, $\bar{\theta} = \frac{1-\sqrt{5}}{2}$, $\alpha = 1 + i - i\theta$, $\bar{\alpha} = 1 + i - i\bar{\theta}$ and $z_j \in \mathbb{Z}[i]$.

The Golden Code [Belfiore Rekaya Viterbo 04/05]

Rate-2 NVD Code

Codewords of the Golden Code are

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha\left(z_1 + z_2\theta\right) & \alpha\left(z_3 + z_4\theta\right) \\ i \cdot \bar{\alpha}\left(z_3 + z_4\bar{\theta}\right) & \bar{\alpha}\left(z_1 + z_2\bar{\theta}\right) \end{pmatrix} \quad (9)$$

with $\theta = \frac{1+\sqrt{5}}{2}$, $\bar{\theta} = \frac{1-\sqrt{5}}{2}$, $\alpha = 1 + i - i\theta$, $\bar{\alpha} = 1 + i - i\bar{\theta}$ and $z_j \in \mathbb{Z}[i]$.

- We can also write (9) in a split form,

$$\mathrm{vec}\mathbf{X} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha & \alpha\theta & 0 & 0 \\ 0 & 0 & \alpha & \alpha\theta \\ 0 & 0 & i\bar{\alpha} & i\bar{\alpha}\bar{\theta} \\ \bar{\alpha} & \bar{\alpha}\bar{\theta} & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} \quad (10)$$

  - Equation (10) is useful for the decoder. α has been chosen such that matrix of eq. (10) is unitary.

Minimum determinant

- The determinant of **X** is

$$
\begin{aligned}
\det \mathbf{X} &= \frac{1}{5}\left[N_{\mathbb{K}/\mathbb{Q}(i)}\left(\alpha\left(z_1+z_2\theta\right)\right) - iN_{\mathbb{K}/\mathbb{Q}(i)}\left(\alpha\left(z_3+z_4\theta\right)\right)\right] \\
&= \frac{2+i}{5}\left[N_{\mathbb{K}/\mathbb{Q}(i)}\left(z_1+z_2\theta\right) - iN_{\mathbb{K}/\mathbb{Q}(i)}\left(z_3+z_4\theta\right)\right]
\end{aligned}
$$

Minimum determinant

- The determinant of **X** is

$$\det \mathbf{X} = \frac{1}{5}\left[N_{\mathbb{K}/\mathbb{Q}(i)}\left(\alpha\left(z_1+z_2\theta\right)\right) - iN_{\mathbb{K}/\mathbb{Q}(i)}\left(\alpha\left(z_3+z_4\theta\right)\right)\right]$$
$$= \frac{2+i}{5}\left[N_{\mathbb{K}/\mathbb{Q}(i)}\left(z_1+z_2\theta\right) - iN_{\mathbb{K}/\mathbb{Q}(i)}\left(z_3+z_4\theta\right)\right]$$

- Since i is not a norm (*next slide*) of an element of $\mathbb{Q}(i)$, then

$$N_{\mathbb{K}/\mathbb{Q}(i)}\left(z_1+z_2\theta\right) - iN_{\mathbb{K}/\mathbb{Q}(i)}\left(z_3+z_4\theta\right) \quad \begin{matrix} \neq 0 \\ \in \mathbb{Z}[i] \end{matrix}$$

So,

$$\left|N_{\mathbb{K}/\mathbb{Q}(i)}\left(z_1+z_2\theta\right) - iN_{\mathbb{K}/\mathbb{Q}(i)}\left(z_3+z_4\theta\right)\right|^2 \geq 1$$

Minimum determinant

- The determinant of $\mathbf{X}$ is

$$\det \mathbf{X} = \frac{1}{5}\left[N_{\mathbb{K}/\mathbb{Q}(i)}\left(\alpha\left(z_1+z_2\theta\right)\right) - iN_{\mathbb{K}/\mathbb{Q}(i)}\left(\alpha\left(z_3+z_4\theta\right)\right)\right]$$
$$= \frac{2+i}{5}\left[N_{\mathbb{K}/\mathbb{Q}(i)}\left(z_1+z_2\theta\right) - iN_{\mathbb{K}/\mathbb{Q}(i)}\left(z_3+z_4\theta\right)\right]$$

- Since i is not a norm (*next slide*) of an element of $\mathbb{Q}(i)$, then

$$N_{\mathbb{K}/\mathbb{Q}(i)}\left(z_1+z_2\theta\right) - iN_{\mathbb{K}/\mathbb{Q}(i)}\left(z_3+z_4\theta\right) \quad \begin{array}{c}\neq 0 \\ \in \mathbb{Z}[i]\end{array}$$

So,

$$\left|N_{\mathbb{K}/\mathbb{Q}(i)}\left(z_1+z_2\theta\right) - iN_{\mathbb{K}/\mathbb{Q}(i)}\left(z_3+z_4\theta\right)\right|^2 \geq 1$$

Result

We get

$$\delta_{\min} = \min_{\mathbf{X}\neq 0} \left|\det \mathbf{X}\right|^2 = \left|\frac{2+i}{5}\right|^2 = \frac{1}{5}$$

i is not a norm

Sketch of proof [Oggier 04]

$\mathbb{Q}(i)$ can be embedded in $\mathbf{Q}_5$ by

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

- If i was a norm, then $\exists a + b\sqrt{5} \in \mathbb{Q}(i)$ such that $a^2 - 5b^2 = i$ which can be lifted in $\mathbf{Q}_5$ as $a^2 - 5b^2 = 2 + 5x, x \in \mathbf{Z}_5$.

i is not a norm

Sketch of proof [Oggier 04]

$\mathbb{Q}(i)$ can be embedded in $\mathbf{Q}_5$ by

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

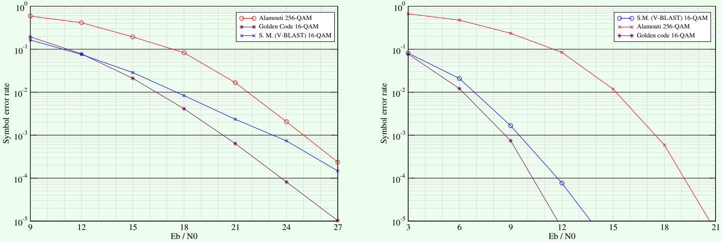
- If i was a norm, then $\exists a + b\sqrt{5} \in \mathbb{Q}(i)$ such that $a^2 - 5b^2 = i$ which can be lifted in $\mathbf{Q}_5$ as $a^2 - 5b^2 = 2 + 5x, x \in \mathbf{Z}_5$.
- It implies

$$v_5\left(a^2 - 5b^2\right) = \min\{2v_5(a), 2v_5(b) + 1\} = 0$$

so $a, b \in \mathbf{Z}_5$. Reducing equality mod $5\mathbf{Z}_5$, we find that 2 should be a square in $\mathbb{F}_5$.

Numerical results

Golden Code *vs* Alamouti and S.M.



(a) 2 receive antennas　　(b) 6 receive antennas

Figure: Numerical results 8 bits p.c.u.

Outline

Shaping

- Each layer of the code designed from cyclic division algebras is composed of a vector whose expression is $\left(z, \sigma(z), \ldots, \sigma^{n-1}(z)\right)$ (see (8)). z linearly depends on n information QAM or HEX symbols x_i. We have

$$\begin{pmatrix} z \\ \sigma(z) \\ \vdots \\ \sigma^{n-1}(z) \end{pmatrix} = \mathbf{G} \cdot \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix}$$

Shaping

- Each layer of the code designed from cyclic division algebras is composed of a vector whose expression is $\left(z,\sigma(z),\ldots,\sigma^{n-1}(z)\right)$ (see (8)). z linearly depends on n information QAM or HEX symbols x_i. We have

$$\begin{pmatrix} z \\ \sigma(z) \\ \vdots \\ \sigma^{n-1}(z) \end{pmatrix} = \mathbf{G}\cdot\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix}$$

- We impose, in order to preserve the mutual information of the MIMO channel, that $\mathbf{G}$ is a unitary matrix up to a normalization factor. This can usually be done by imposing that codewords components are in an ideal of $\mathscr{O}_{\mathbb{K}}$.
  - Moreover, we also impose that $|\gamma| = 1$ to balance the average energy over all the layers.

Definition

Space-Time Block codes associated to a matrix $\mathbf{G}$ which is a similitude and such that $|\gamma| = 1$ are said to have the "unitarity" property.

Perfect STBCs [Oggier *et al.* 04/06]

Definition

Perfect space-time block codes are codes constructed from a cyclic division algebra on $\mathbb{F} = \mathbb{Q}(i)$ (resp. $\mathbb{F} = \mathbb{Q}(j)$) by using QAM (resp. HEX) symbols that have the unitarity property.

Corollary

Perfect STBCs are tradeoff achieving and information preserving (optimum behavior at high and low signal to noise ratios).

Perfect STBCs [Oggier *et al.* 04/06]

Definition

Perfect space-time block codes are codes constructed from a cyclic division algebra on $\mathbb{F} = \mathbb{Q}(i)$ (resp. $\mathbb{F} = \mathbb{Q}(j)$) by using QAM (resp. HEX) symbols that have the unitarity property.

Corollary

Perfect STBCs are tradeoff achieving and information preserving (optimum behavior at high and low signal to noise ratios).

Example: The Golden Code

The Golden Code is a perfect space-time block code. The ideal of $\mathcal{O}_{\mathbb{K}}$ is a principal ideal generated by α.

Perfect STBCs [Oggier *et al.* 04/06]

Definition

Perfect space-time block codes are codes constructed from a cyclic division algebra on $\mathbb{F} = \mathbb{Q}(i)$ (resp. $\mathbb{F} = \mathbb{Q}(j)$) by using QAM (resp. HEX) symbols that have the unitarity property.

Corollary

Perfect STBCs are tradeoff achieving and information preserving (optimum behavior at high and low signal to noise ratios).

Example: The Golden Code

The Golden Code is a perfect space-time block code. The ideal of $\mathscr{O}_{\mathbb{K}}$ is a principal ideal generated by α.

Theorem

Perfect space-time block codes are rate-n_t NVD codes.

3, 4 and 6 antennas

3 antennas: the parameters

- $\mathbb{F} = \mathbb{Q}(j)$, $\mathbb{K} = \mathbb{Q}(j,\theta)$ with $\theta = 2\cos\left(\frac{2\pi}{7}\right)$
- $\gamma = j$, $\alpha = ((1+j)+\theta)$
- $\delta_{\min}(\mathscr{C}_\infty) = \frac{1}{49}$

3, 4 and 6 antennas

3 antennas: the parameters

- $\mathbb{F} = \mathbb{Q}(j)$, $\mathbb{K} = \mathbb{Q}(j, \theta)$ with $\theta = 2\cos\left(\frac{2\pi}{7}\right)$
- $\gamma = j$, $\alpha = ((1 + j) + \theta)$
- $\delta_{\min}(\mathscr{C}_\infty) = \frac{1}{49}$

4 antennas: the parameters

- $\mathbb{F} = \mathbb{Q}(i)$, $\mathbb{K} = \mathbb{Q}(i, \theta)$ with $\theta = 2\cos\left(\frac{2\pi}{15}\right)$
- $\gamma = i$, $\alpha = (1 - 3i) + i\theta^2)$
- $\delta_{\min}(\mathscr{C}_\infty) = \frac{1}{1125}$

TELECOM PARIS école nationale supérieure des télécommunications

3, 4 and 6 antennas

3 antennas: the parameters

- $\mathbb{F} = \mathbb{Q}(j)$, $\mathbb{K} = \mathbb{Q}(j, \theta)$ with $\theta = 2\cos\left(\frac{2\pi}{7}\right)$
- $\gamma = j$, $\alpha = ((1+j)+\theta)$
- $\delta_{\min}(\mathscr{C}_\infty) = \frac{1}{49}$

4 antennas: the parameters

- $\mathbb{F} = \mathbb{Q}(i)$, $\mathbb{K} = \mathbb{Q}(i, \theta)$ with $\theta = 2\cos\left(\frac{2\pi}{15}\right)$
- $\gamma = i$, $\alpha = (1-3i)+i\theta^2)$
- $\delta_{\min}(\mathscr{C}_\infty) = \frac{1}{1125}$

6 antennas: the parameters

- $\mathbb{F} = \mathbb{Q}(j)$, $\mathbb{K} = \mathbb{Q}(j, \theta)$ with $\theta = 2\cos\left(\frac{\pi}{14}\right)$
- $\gamma = -j$, non principal ideal
- $\frac{1}{2^6.7^5} \leq \delta_{\min}(\mathscr{C}_\infty) \leq \frac{1}{2^6.7^4}$

Other perfect STBCs

- [Elia et al. 05] found perfect STBCs for any number of antennas by relaxing the constraint on γ.
- γ is no more an integer.

Other perfect STBCs

- [Elia et al. 05] found perfect STBCs for any number of antennas by relaxing the constraint on γ.
- γ is no more an integer.

Hint

Take $\gamma = \frac{a \pm ib}{b \pm ia}$ $a, b \in \mathbb{Z}$ where $|a + ib|^2$ is not a norm of $\mathbb{K}/\mathbb{Q}(i)$.
To find non norm elements is quite easy. Take $p \equiv 1\ (4)$ such that $p\mathcal{O}_{\mathbb{K}}$ is a prime ideal. Decompose $p = a^2 + b^2$.

Part IV

Further applications

Outline

9 MIMO OFDM

10 Decoding

11 Encoding the Golden Code

System Model: An example

- Parallel MIMO channel: Consider the case of a MIMO OFDM system
  - On each subcarrier, the channel is considered flat
  - When two such subcarriers f_i and f_j are separated by at least the channel coherence bandwidth B_c, then channel coefficients on these subcarriers are decorrelated.

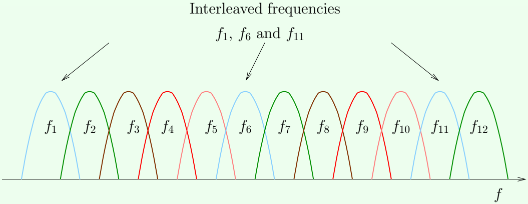


Figure: OFDM as parallel channels: here, channel coefficients on frequencies f_1, f_6, and f_{11} are considered decorrelated

System Model: The equivalent channel

- Denote n_t the number of transmit antennas, n_r the number of receive antennas and N the number of parallel channels

System Model: The equivalent channel

- Denote n_t the number of transmit antennas, n_r the number of receive antennas and N the number of parallel channels

Received signal

$$\boxed{\mathbf{Y}_{Nn_r \times T} = \mathbf{H}_{Nn_r \times Nn_t} \cdot \mathbf{X}_{Nn_t \times T} + \mathbf{Z}_{Nn_r \times T}}$$

where **X** is the transmitted codeword, **Z** is the i.i.d. noise and **H** is the channel matrix.

System Model: The equivalent channel

- Denote n_t the number of transmit antennas, n_r the number of receive antennas and N the number of parallel channels

Received signal

$$\boxed{\mathbf{Y}_{Nn_r\times T} = \mathbf{H}_{Nn_r\times Nn_t}\cdot\mathbf{X}_{Nn_t\times T} + \mathbf{Z}_{Nn_r\times T}}$$

where $\mathbf{X}$ is the transmitted codeword, $\mathbf{Z}$ is the i.i.d. noise and $\mathbf{H}$ is the channel matrix.

- More precisely, we have

$$\mathbf{H} = \mathrm{diag}\left(\mathscr{H}_1, \mathscr{H}_2, \ldots, \mathscr{H}_N\right)$$

where $\mathscr{H}_i$ is a $n_r \times n_t$ submatrix corresponding to channel i (for example the interleaved subcarrier f_i in an OFDM system).

Block-Diagonal STBCs from division algebras

Idea

Let the base field be $\mathbb{F}$, an extension of degree N over $\mathbb{Q}(i)$ (resp. $\mathbb{Q}(j)$) with Galois group

$$\mathrm{Gal}\left(\mathbb{F}/\mathbb{Q}(i)\right) = \{\tau_1, \tau_2, \ldots, \tau_N\}.$$

$\mathbb{K}$ is a cyclic extension of degree n_t of $\mathbb{F}$. Codewords have the form

$$\mathbf{X} = \begin{bmatrix} \boxed{\tau_1(\Xi)} & & & \\ & \boxed{\tau_2(\Xi)} & & \\ & & \ddots & \\ & & & \boxed{\tau_N(\Xi)} \end{bmatrix}$$

where Ξ is the matrix representation of an element of a cyclic division algebra with base field $\mathbb{F}$ and maximal subfield $\mathbb{K}$.

Block-Diagonal STBCs from division algebras

Idea

Let the base field be $\mathbb{F}$, an extension of degree N over $\mathbb{Q}(i)$ (resp. $\mathbb{Q}(j)$) with Galois group

$$\mathrm{Gal}\left(\mathbb{F}/\mathbb{Q}(i)\right) = \left\{\tau_1, \tau_2, \ldots, \tau_N\right\}.$$

$\mathbb{K}$ is a cyclic extension of degree n_t of $\mathbb{F}$. Codewords have the form

$$\mathbf{X} = \begin{bmatrix} \boxed{\tau_1(\Xi)} & & & \\ & \boxed{\tau_2(\Xi)} & & \\ & & \ddots & \\ & & & \boxed{\tau_N(\Xi)} \end{bmatrix}$$

where Ξ is the matrix representation of an element of a cyclic division algebra with base field $\mathbb{F}$ and maximal subfield $\mathbb{K}$.

Non Vanishing Determinant

Minimum squared determinant is

$$\boxed{\det \mathbf{X} = \prod_{i=1}^{N} \det \tau_i(\Xi) = \prod_{i=1}^{N} \tau_i(\det \Xi) = N_{\mathbb{F}/\mathbb{Q}(i)}(\det \Xi) \in \mathbb{Z}[i] \setminus \{0\}}$$

Perfect Codes MIMO OFDM: An example

- Consider the case $n_t = n_r = 2$ and $N = 2$ parallel channels

Perfect Codes MIMO OFDM: An example

- Consider the case $n_t = n_r = 2$ and $N = 2$ parallel channels

2-Golden Code

Codeword is

$$\mathbf{X} = \begin{bmatrix} \Xi & \mathbf{0} \\ \mathbf{0} & \tau(\Xi) \end{bmatrix}$$

where

$$\Xi = \begin{bmatrix} \alpha\cdot(s_1 + s_2\zeta_8 + s_3\theta + s_4\zeta_8\theta) & \alpha\cdot(s_5 + s_6\zeta_8 + s_7\theta + s_8\zeta_8\theta) \\ \zeta_8\bar{\alpha}\cdot\left(s_5 + s_6\zeta_8 + s_7\bar{\theta} + s_8\zeta_8\bar{\theta}\right) & \bar{\alpha}\cdot\left(s_1 + s_2\zeta_8 + s_3\bar{\theta} + s_4\zeta_8\bar{\theta}\right) \end{bmatrix}$$

with $\theta = \frac{1+\sqrt{5}}{2}$, $\bar{\theta} = \frac{1-\sqrt{5}}{2}$, $\alpha = 1 + i - i\theta$, $\bar{\alpha} = 1 + i - i\bar{\theta}$, $\tau : \zeta_8 \mapsto -\zeta_8$ and $s_k \in \mathbb{Z}[i]$.

Perfect Codes MIMO OFDM: An example

- Consider the case $n_t = n_r = 2$ and $N = 2$ parallel channels

2-Golden Code

Codeword is

$$\mathbf{X} = \begin{bmatrix} \Xi & \mathbf{0} \\ \mathbf{0} & \tau(\Xi) \end{bmatrix}$$

where

$$\Xi = \begin{bmatrix} \alpha \cdot (s_1 + s_2 \zeta_8 + s_3 \theta + s_4 \zeta_8 \theta) & \alpha \cdot (s_5 + s_6 \zeta_8 + s_7 \theta + s_8 \zeta_8 \theta) \\ \zeta_8 \bar{\alpha} \cdot (s_5 + s_6 \zeta_8 + s_7 \bar{\theta} + s_8 \zeta_8 \bar{\theta}) & \bar{\alpha} \cdot (s_1 + s_2 \zeta_8 + s_3 \bar{\theta} + s_4 \zeta_8 \bar{\theta}) \end{bmatrix}$$

with $\theta = \frac{1+\sqrt{5}}{2}$, $\bar{\theta} = \frac{1-\sqrt{5}}{2}$, $\alpha = 1 + i - i\theta$, $\bar{\alpha} = 1 + i - i\bar{\theta}$, $\tau : \zeta_8 \mapsto -\zeta_8$ and $s_k \in \mathbb{Z}[i]$.

Determinant of X

$$\boxed{\det \mathbf{X} = N_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(i)} (\det \Xi) \in \mathbb{Z}[i] \setminus \{0\}}$$

Perfect Codes MIMO OFDM: An example

- Consider the case $n_t = n_r = 2$ and $N = 2$ parallel channels

2-Golden Code

Codeword is

$$\mathbf{X} = \begin{bmatrix} \Xi & \mathbf{0} \\ \mathbf{0} & \tau(\Xi) \end{bmatrix}$$

where

$$\Xi = \begin{bmatrix} \alpha \cdot (s_1 + s_2\zeta_8 + s_3\theta + s_4\zeta_8\theta) & \alpha \cdot (s_5 + s_6\zeta_8 + s_7\theta + s_8\zeta_8\theta) \\ \zeta_8\bar{\alpha} \cdot \left(s_5 + s_6\zeta_8 + s_7\bar{\theta} + s_8\zeta_8\bar{\theta}\right) & \bar{\alpha} \cdot \left(s_1 + s_2\zeta_8 + s_3\bar{\theta} + s_4\zeta_8\bar{\theta}\right) \end{bmatrix}$$

with $\theta = \frac{1+\sqrt{5}}{2}$, $\bar{\theta} = \frac{1-\sqrt{5}}{2}$, $\alpha = 1 + i - i\theta$, $\bar{\alpha} = 1 + i - i\bar{\theta}$, $\tau : \zeta_8 \mapsto -\zeta_8$ and $s_k \in \mathbb{Z}[i]$.

Determinant of X

$$\boxed{\det \mathbf{X} = N_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(i)}(\det \Xi) \in \mathbb{Z}[i] \setminus \{0\}}$$

Proposition

The 2−Golden Code is a perfect code for the $(2,2,2)$ parallel MIMO channel

Outline

Reduction-aided decoding

- Infinite code formulation

$$\mathbf{Y}_{n_t\times n_t} = \mathbf{H}_{n_t\times n_t}\cdot\mathbf{X}_{n_t\times n_t} + \mathbf{W}_{n_t\times n_t}$$

where **X** is a codeword derived from a cyclic division algebra.

Reduction-aided decoding

- Infinite code formulation

$$\mathbf{Y}_{n_t \times n_t} = \mathbf{H}_{n_t \times n_t} \cdot \mathbf{X}_{n_t \times n_t} + \mathbf{W}_{n_t \times n_t}$$

  where $\mathbf{X}$ is a codeword derived from a cyclic division algebra.

- Let $\mathbf{U}$ be a unit in the cyclic division algebra that approximate

$$\left(\frac{1}{|\det \mathbf{H}|}\right)^{\frac{1}{n_t}} \cdot \mathbf{H}$$

  Denote $\mathbf{E} = \mathbf{H} \cdot \mathbf{U}^{-1}$. Then, $\mathbf{Z} = \mathbf{U} \cdot \mathbf{X}$ remains in the code and the received signal becomes

$$\mathbf{Y} = \mathbf{E} \cdot \mathbf{Z} + \mathbf{W}$$

  up to a unitary matrix, with matrix $\mathbf{E}$ better conditioned for suboptimal decoding algorithms.

Outline

Binary labelling

- The encoder has binary symbols at its input and must label codewords of the Golden codes with these bits.

Ungerboeck-type labelling

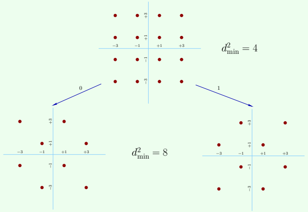


Figure: Ungerboeck labelling of a QAM constellation

Binary labelling

- The encoder has binary symbols at its input and must label codewords of the Golden codes with these bits.

Ungerboeck-type labelling

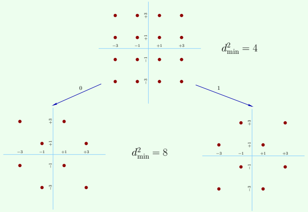


Figure: Ungerboeck labelling of a QAM constellation

- We propose here a Ungerboeck-type binary labelling for the Golden code that has the minimum determinant as design criterion.

Partition chain (I)

- Let β be an element of the Golden algebra $\beta = i\,(1-\theta) + (1-\theta)\,e$ with matrix representation

$$\mathbf{X}_\beta = \begin{bmatrix} i\,(1-\theta) & 1-\theta \\ i\left(1-\bar{\theta}\right) & i\left(1-\bar{\theta}\right) \end{bmatrix}$$

Partition chain (I)

- Let β be an element of the Golden algebra $\beta = i(1-\theta) + (1-\theta)e$ with matrix representation

$$\mathbf{X}_\beta = \begin{bmatrix} i(1-\theta) & 1-\theta \\ i(1-\bar{\theta}) & i(1-\bar{\theta}) \end{bmatrix}$$

Definition

We define the set

$$\mathfrak{P} = \{g \cdot \beta \mid g \in \mathscr{G}\}$$

Partition chain (I)

- Let β be an element of the Golden algebra $\beta = i(1-\theta)+(1-\theta)e$ with matrix representation

$$\mathbf{X}_\beta = \begin{bmatrix} i(1-\theta) & 1-\theta \\ i(1-\bar{\theta}) & i(1-\bar{\theta}) \end{bmatrix}$$

Definition

We define the set

$$\mathfrak{P} = \{g \cdot \beta \mid g \in \mathscr{G}\}$$

- Because $N_r(\beta) = 1+i$, the Golden code can be partitioned into 4 subsets: $\mathfrak{P}$ and 3 translated versions.
- Minimum determinant of each subset is $\boxed{\delta_{\text{min}} = 2 \cdot \delta_{\text{min}}(\mathscr{G})}$

Partition chain (II)

Lattice and ideal partition

$$
\begin{array}{ccc}
\mathbb{Z}[i]^4 \cong \mathbb{Z}^8 & \longleftrightarrow & \mathcal{G} \\
\downarrow & & \downarrow \\
D_4^2 & \longleftrightarrow & \mathfrak{P} \\
\downarrow & & \downarrow \\
E_8 & \longleftrightarrow & \mathfrak{P}^2 \\
\downarrow & & \downarrow \\
L_8 & \longleftrightarrow & (1+i)\mathfrak{P} \\
\downarrow & & \downarrow \\
2\mathbb{Z}^8 & \longleftrightarrow & 2\mathcal{G}
\end{array}
$$

Labelling

- Non-$\mathbb{Z}^8$ lattices based constellations to label (E_8 for example).

Labelling

- Non-$\mathbb{Z}^8$ lattices based constellations to label (E_8 for example).
- **Use construction A.**

Labelling

- Non-$\mathbb{Z}^8$ lattices based constellations to label (E_8 for example).
- **Use construction A.**

Figure: Details in a next talk

Thank you for your attention!