Coding the Golden Code

Doing some arithmetics in a quaternion algebra

Jean-Claude Belfiore†
Joint work with
David Champion † Ghaya Rekaya† Emanuele Viterbo‡

†École Nationale Supérieure des Télécommunications, Paris, FRANCE

‡Politecnico di Torino, ITALY

December, 9th 2005

Email: belfiore@enst.fr
http://www.comelec.enst.fr/~belfiore

IISc Symposium on Coding Theory
Bangalore, India

- In standards for which a space-time code solution is defined (it can be the **Alamouti code**, the **Spatial Multiplexing (VBLAST)** or the **Golden Code**), a binary outer code is concatenated (convolutional code, LDPC code, turbo-code).
- These standards are
  - IEEE 802.11n (WiFi)
  - IEEE 802.16e (WiMax and WiBro)
  - 3GPP (3G systems)
- Concatenating a binary outer code is quite easy to do for the Alamouti code and the S.M.
- But we do not know how to correctly label the Golden Code
- This talk will give a first answer to this question, but it will also ask some new questions and enlight new problems.

Outline

Outline

1. *Outer-Coded Space-Time Block Codes*
   - The quasi static fading channel
   - The inner/outer codes
2. Code construction a la Ungerboeck
   - An example in $\mathbb{Z}$
   - Another example
3. The Golden Code
4. A quaternary partition
   - The partitionning ideal
   - The Gosset Lattice E_8
5. How to increase the coding gain?
6. The Golden Leech Lattice $\mathscr{G}\Lambda_{24}$
7. A trellis-coded Golden modulation
   - Code and simulation results

The quasi static fading channel

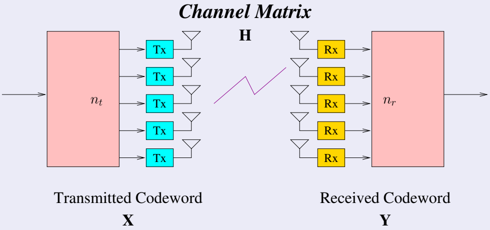


Figure: The Channel Model

- 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.
- **H** is assumed constant during the transmission of one codeword.

Code construction criterions

- $\mathbf{X}_i - \mathbf{X}_j$ is the difference between two codewords.
- Some common claims
  1. Rank Criterion: The minimum rank of the difference of any pair of non equal codewords should be maximized
  2. Determinant criterion: Maximize (only for high SNR)

$$\min_{\substack{\mathbf{X}_i \neq \mathbf{X}_j \\ \mathbf{X}_i, \mathbf{X}_j \in \mathscr{C}}} \det\left((\mathbf{X}_i - \mathbf{X}_j)(\mathbf{X}_i - \mathbf{X}_j)^\dagger\right)$$

  3. Trace criterion: Maximize (only for low SNR)

$$\min_{\substack{\mathbf{X}_i \neq \mathbf{X}_j \\ \mathbf{X}_i, \mathbf{X}_j \in \mathscr{C}}} \mathrm{Tr}\left((\mathbf{X}_i - \mathbf{X}_j)(\mathbf{X}_i - \mathbf{X}_j)^\dagger\right)$$

- We will satisfy all these criteria, but some surprises could happen

Code construction criterions

- $\mathbf{X}_i - \mathbf{X}_j$ is the difference between two codewords.
- Some common claims
  1. Rank Criterion: The minimum rank of the difference of any pair of non equal codewords should be maximized
  2. Determinant criterion: Maximize (only for high $\mathtt{SNR}$)

$$\min_{\substack{\mathbf{X}_i \neq \mathbf{X}_j \\ \mathbf{X}_i, \mathbf{X}_j \in \mathscr{C}}} \det\left((\mathbf{X}_i - \mathbf{X}_j)(\mathbf{X}_i - \mathbf{X}_j)^{\dagger}\right)$$

  3. Trace criterion: Maximize (only for low $\mathtt{SNR}$)

$$\min_{\substack{\mathbf{X}_i \neq \mathbf{X}_j \\ \mathbf{X}_i, \mathbf{X}_j \in \mathscr{C}}} \mathrm{Tr}\left((\mathbf{X}_i - \mathbf{X}_j)(\mathbf{X}_i - \mathbf{X}_j)^{\dagger}\right)$$

- We will satisfy all these criteria, but some surprises could happen

Code construction criterions

- $\mathbf{X}_i - \mathbf{X}_j$ is the difference between two codewords.
- Some common claims
  1. Rank Criterion: The minimum rank of the difference of any pair of non equal codewords should be maximized
  2. Determinant criterion: Maximize (only for high SNR)

$$\min_{\substack{\mathbf{X}_i \neq \mathbf{X}_j \\ \mathbf{X}_i, \mathbf{X}_j \in \mathscr{C}}} \det\left((\mathbf{X}_i - \mathbf{X}_j)(\mathbf{X}_i - \mathbf{X}_j)^\dagger \right)$$

  3. Trace criterion: Maximize (only for low SNR)

$$\min_{\substack{\mathbf{X}_i \neq \mathbf{X}_j \\ \mathbf{X}_i, \mathbf{X}_j \in \mathscr{C}}} \mathrm{Tr}\left((\mathbf{X}_i - \mathbf{X}_j)(\mathbf{X}_i - \mathbf{X}_j)^\dagger \right)$$

- We will satisfy all these criteria, but some surprises could happen

- Inner and outer coding on a MIMO channel have very different roles (see figure)
  1. Inner code ⟶ Space-Time Block Code
  2. Outer Code ⟶ Binary code (Convolutional, Block, LDPC, Turbo,...)

Encoding scheme

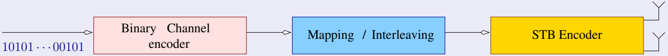


Figure: How to do the mapping?

- We propose here a Ungerboeck-type binary labelling for the Golden code

Inner and Outer Codes for MIMO Channels

- Inner and outer coding on a MIMO channel have very different roles (see figure)
    1. Inner code ⟶ Space-Time Block Code
    2. Outer Code ⟶ Binary code (Convolutional, Block, LDPC, Turbo,...)

Encoding scheme

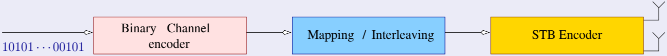


Figure: How to do the mapping?

- We propose here a Ungerboeck-type binary labelling for the Golden code

Outline

1. Outer-Coded Space-Time Block Codes
   - The quasi static fading channel
   - The inner/outer codes
2. *Code construction a la Ungerboeck*
   - An example in $\mathbb{Z}$
   - Another example
3. The Golden Code
4. A quaternary partition
   - The partitionning ideal
   - The Gosset Lattice E_8
5. How to increase the coding gain?
6. The Golden Leech Lattice $\mathscr{G}\Lambda_{24}$
7. A trellis-coded Golden modulation
   - Code and simulation results

Partition of $\mathbb{Z}$

Partition of a 4 PAM

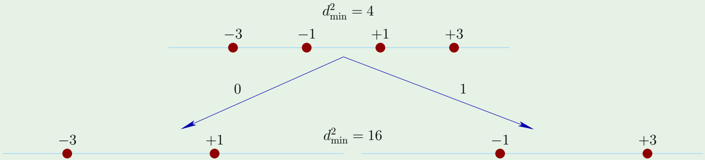


Figure: Partition a la Ungerboeck: the Euclidean minimum distance is increased

Lattice formulation

Lattice $\mathbb{Z}$ is partitionned into 2 subsets:

1. Even integers $2\mathbb{Z}$
2. Odd integers $2\mathbb{Z}+1$

- The set $\mathbb{Z}/2\mathbb{Z}$ is a quotient ring isomorphic to $\mathbb{F}_2$.
- A quaternary partition (multiple of 4) would give a labelling with the alphabet $\mathbb{Z}/4\mathbb{Z}$, isomorphic to $\mathbb{Z}_4$.

Partition of a 4 PAM

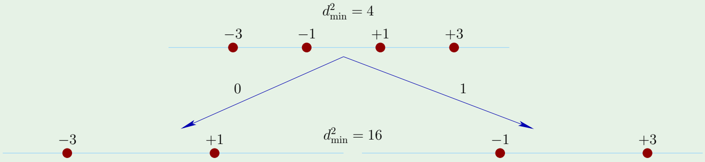


Figure: Partition a la Ungerboeck: the Euclidean minimum distance is increased

Lattice formulation

Lattice $\mathbb{Z}$ is partitionned into 2 subsets:

1. Even integers $2\mathbb{Z}$
2. Odd integers $2\mathbb{Z}+1$

- The set $\mathbb{Z}/2\mathbb{Z}$ is a quotient ring isomorphic to $\mathbb{F}_2$.
- A quaternary partition (multiple of 4) would give a labelling with the alphabet $\mathbb{Z}/4\mathbb{Z}$, isomorphic to $\mathbb{Z}_4$.

Partition of $\mathbb{Z}$

Partition of a 4 PAM

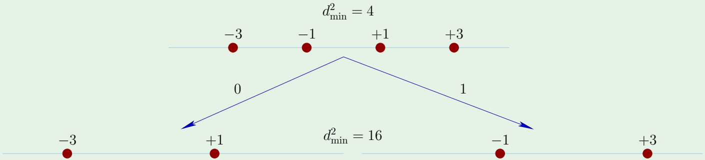


Figure: Partition a la Ungerboeck: the Euclidean minimum distance is increased

Lattice formulation

Lattice $\mathbb{Z}$ is partitionned into 2 subsets:

1. Even integers $2\mathbb{Z}$
2. Odd integers $2\mathbb{Z}+1$

- The set $\mathbb{Z}/2\mathbb{Z}$ is a quotient ring isomorphic to $\mathbb{F}_2$.
- A quaternary partition (multiple of 4) would give a labelling with the alphabet $\mathbb{Z}/4\mathbb{Z}$, isomorphic to $\mathbb{Z}_4$.

Binary partition of $\mathbb{Z}[i]$

Partition of a 16 QAM

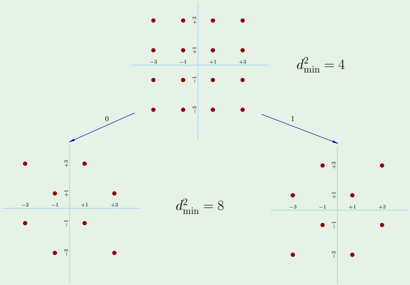


Figure: Partition a la Ungerboeck: the Euclidean minimum distance is increased

Lattice formulation

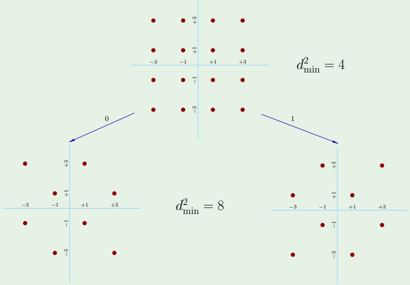
Lattice $\mathbb{Z}[i]$ is partitionned into 2 subsets:

1. Multiples of $1+i$: $(1+i)\mathbb{Z}[i]$ (Do not forget that $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i) = |1+i|^2 = 2$)
2. The other integers: $(1+i)\mathbb{Z}[i]+1$

- The set $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$ is a quotient ring isomorphic to $\mathbb{F}_2$.

Binary partition of $\mathbb{Z}[i]$

Partition of a 16 QAM



$d^2_{\min} = 4$

$d^2_{\min} = 8$

Figure: Partition a la Ungerboeck: the Euclidean minimum distance is increased

Lattice formulation

Lattice $\mathbb{Z}[i]$ is partitionned into 2 subsets:

1. Multiples of $1+i$: $(1+i)\mathbb{Z}[i]$ (Do not forget that $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i) = |1+i|^2 = 2$)
2. The other integers: $(1+i)\mathbb{Z}[i]+1$

- The set $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$ is a quotient ring isomorphic to $\mathbb{F}_2$.

A quaternary partition of $\mathbb{Z}[i]$

- Take an element with norm 4. Obviously, 2 is OK. $2\mathbb{Z}[i]$ is a principal ideal of norm 4.
- Form the quotient $\mathbb{Z}[i]/2\mathbb{Z}[i]$. This quotient ring has cardinality 4 (the norm of the ideal $2\mathbb{Z}[i]$) and the class representatives are $0, 1, i, 1+i$.
- We have in fact

$$\mathbb{Z}[i]/2\mathbb{Z}[i] \cong \mathbb{F}_2 \oplus u \cdot \mathbb{F}_2 \quad u^2 = 0$$

  by associating u to the class whose representative is $1+i$.
  - Check that $(1+i)^2 = 2i$ is a multiple of 2
- Now replace $\mathbb{Z}[i]$ by the Golden Code ...
  - Things are becoming (much) less obvious

Criterion for partition

We propose to partition the Golden Code in order to have a chain with increasing minimum determinant and (perhaps) increasing minimum Euclidean distance. Note that the norm is replaced here by the reduced norm.

A quaternary partition of $\mathbb{Z}[i]$

- Take an element with norm 4. Obviously, 2 is OK. $2\mathbb{Z}[i]$ is a principal ideal of norm 4.
- Form the quotient $\mathbb{Z}[i]/2\mathbb{Z}[i]$. This quotient ring has cardinality 4 (the norm of the ideal $2\mathbb{Z}[i]$) and the class representatives are $0, 1, i, 1+i$.
- We have in fact
$$\mathbb{Z}[i]/2\mathbb{Z}[i] \cong \mathbb{F}_2 \oplus u \cdot \mathbb{F}_2 \quad u^2 = 0$$
by associating u to the class whose representative is $1+i$.
  - Check that $(1+i)^2 = 2i$ is a multiple of 2
- Now replace $\mathbb{Z}[i]$ by the Golden Code ...
  - Things are becoming (much) less obvious

Criterion for partition

We propose to partition the Golden Code in order to have a chain with increasing minimum determinant and (perhaps) increasing minimum Euclidean distance. Note that the norm is replaced here by the reduced norm.

A quaternary partition of $\mathbb{Z}[i]$

- Take an element with norm 4. Obviously, 2 is OK. $2\mathbb{Z}[i]$ is a principal ideal of norm 4.
- Form the quotient $\mathbb{Z}[i]/2\mathbb{Z}[i]$. This quotient ring has cardinality 4 (the norm of the ideal $2\mathbb{Z}[i]$) and the class representatives are $0, 1, i, 1+i$.
- We have in fact

$$\mathbb{Z}[i]/2\mathbb{Z}[i] \cong \mathbb{F}_2 \oplus u \cdot \mathbb{F}_2 \quad u^2 = 0$$

  by associating u to the class whose representative is $1+i$.
  - Check that $(1+i)^2 = 2i$ is a multiple of 2
- Now replace $\mathbb{Z}[i]$ by the Golden Code ...
  - Things are becoming (much) less obvious

Criterion for partition

We propose to partition the Golden Code in order to have a chain with increasing minimum determinant and (perhaps) increasing minimum Euclidean distance. Note that the norm is replaced here by the reduced norm.

A quaternary partition of $\mathbb{Z}[i]$

- Take an element with norm 4. Obviously, 2 is OK. $2\mathbb{Z}[i]$ is a principal ideal of norm 4.
- Form the quotient $\mathbb{Z}[i]/2\mathbb{Z}[i]$. This quotient ring has cardinality 4 (the norm of the ideal $2\mathbb{Z}[i]$) and the class representatives are $0, 1, i, 1+i$.
- We have in fact

  $$\mathbb{Z}[i]/2\mathbb{Z}[i] \cong \mathbb{F}_2 \oplus u \cdot \mathbb{F}_2 \quad u^2 = 0$$

  by associating u to the class whose representative is $1+i$.
  - Check that $(1+i)^2 = 2i$ is a multiple of 2
- Now replace $\mathbb{Z}[i]$ by the Golden Code ...
  - Things are becoming (much) less obvious

Criterion for partition

We propose to partition the Golden Code in order to have a chain with increasing minimum determinant and (perhaps) increasing minimum Euclidean distance. Note that the norm is replaced here by the **reduced** norm.

A quaternary partition of $\mathbb{Z}[i]$

- Take an element with norm 4. Obviously, 2 is OK. $2\mathbb{Z}[i]$ is a principal ideal of norm 4.
- Form the quotient $\mathbb{Z}[i]/2\mathbb{Z}[i]$. This quotient ring has cardinality 4 (the norm of the ideal $2\mathbb{Z}[i]$) and the class representatives are $0, 1, i, 1+i$.
- We have in fact

$$\mathbb{Z}[i]/2\mathbb{Z}[i] \cong \mathbb{F}_2 \oplus u \cdot \mathbb{F}_2 \quad u^2 = 0$$

  by associating u to the class whose representative is $1+i$.
    - Check that $(1+i)^2 = 2i$ is a multiple of 2
- Now replace $\mathbb{Z}[i]$ by the Golden Code ...
    - Things are becoming (much) less obvious

Criterion for partition

We propose to partition the Golden Code in order to have a chain with increasing minimum determinant and (perhaps) increasing minimum Euclidean distance. Note that the norm is replaced here by the **reduced** norm.

Outline

- $\mathbb{Q}(i)$ is the base field (QAM modulations)
- $\mathbb{K} = \mathbb{Q}(i,\theta)$ is a quadratic extension over $\mathbb{Q}(i)$ whose Galois group is $\{1,\sigma\}$. $\gamma \in \mathbb{Q}(i)$ is not a norm of an element of $\mathbb{K}$.
- A quaternion algebra is a cyclic division algebra of index 2.

Coding the Golden Code

D. Champion, J.-C. Belfiore, G. Rekaya and E. Viterbo

Introduction

Outer-Coded Space-Time Block Codes

Code construction a la Ungerboeck

The Golden Code

A quaternary partition

How to increase the coding gain?

The Golden Leech Lattice $\mathcal{G}\Lambda_{24}$

A trellis-coded Golden modulation

Conclusion

Tools (Cyclic algebra of index 2)

- $\mathbb{Q}(i)$ is the base field (QAM modulations)
- $\mathbb{K} = \mathbb{Q}(i, \theta)$ is a quadratic extension over $\mathbb{Q}(i)$ whose Galois group is $\{1, \sigma\}$. $\gamma \in \mathbb{Q}(i)$ is not a norm of an element of $\mathbb{K}$.
- A quaternion algebra is a cyclic division algebra of index 2.

Formal construction

- **Cyclic algebra:** $\mathscr{A} = \{z_1 + z_2 \cdot e\}$ with $z_1, z_2 \in \mathbb{K}$ $e^2 = \gamma$ and $z \cdot e = e \cdot \sigma(z)$
- **Conjugate:** If $q = z_1 + z_2 \cdot e$, then $\tilde{q} = \sigma(z_1) - z_2 \cdot e$
- **Reduced Norm:** $N_r(q) = q\tilde{q} \in \mathbb{Q}(i)$

Matrix construction

- **Cyclic algebra:** $$\mathscr{A} = \left\{ \mathbf{X}_q = \begin{bmatrix} z_1 & z_2 \\ \gamma \cdot \sigma(z_2) & \sigma(z_1) \end{bmatrix} \right\}$$ with $z_1, z_2 \in \mathbb{K}$.
- **Conjugate:** Matrix of cofactors
- **Reduced Norm:** $N_r(q) = \det \mathbf{X}_q$

Tools (Cyclic algebra of index 2)

- $\mathbb{Q}(i)$ is the base field (QAM modulations)
- $\mathbb{K} = \mathbb{Q}(i, \theta)$ is a quadratic extension over $\mathbb{Q}(i)$ whose Galois group is $\{1, \sigma\}$. $\gamma \in \mathbb{Q}(i)$ is not a norm of an element of $\mathbb{K}$.
- A quaternion algebra is a cyclic division algebra of index 2.

Formal construction

- **Cyclic algebra:** $\mathscr{A} = \{z_1 + z_2 \cdot e\}$ with $z_1, z_2 \in \mathbb{K}$ $e^2 = \gamma$ and $z \cdot e = e \cdot \sigma(z)$
- **Conjugate:** If $q = z_1 + z_2 \cdot e$, then $\tilde{q} = \sigma(z_1) - z_2 \cdot e$
- **Reduced Norm:** $N_r(q) = q\tilde{q} \in \mathbb{Q}(i)$

Matrix construction

- **Cyclic algebra:**
$$\mathscr{A} = \left\{ \mathbf{X}_q = \begin{bmatrix} z_1 & z_2 \\ \gamma \cdot \sigma(z_2) & \sigma(z_1) \end{bmatrix} \right\}$$
with $z_1, z_2 \in \mathbb{K}$.
- **Conjugate:** Matrix of cofactors
- **Reduced Norm:** $N_r(q) = \det \mathbf{X}_q$

Tools (Cyclic algebra of index 2)

- $\mathbb{Q}(i)$ is the base field (QAM modulations)
- $\mathbb{K} = \mathbb{Q}(i, \theta)$ is a quadratic extension over $\mathbb{Q}(i)$ whose Galois group is $\{1, \sigma\}$. $\gamma \in \mathbb{Q}(i)$ is not a norm of an element of $\mathbb{K}$.
- A quaternion algebra is a cyclic division algebra of index 2.

Formal construction

- **Cyclic algebra:** $\mathscr{A} = \{z_1 + z_2 \cdot e\}$ with $z_1, z_2 \in \mathbb{K}$ $e^2 = \gamma$ and $z \cdot e = e \cdot \sigma(z)$
- **Conjugate:** If $q = z_1 + z_2 \cdot e$, then $\tilde{q} = \sigma(z_1) - z_2 \cdot e$
- **Reduced Norm:** $N_r(q) = q\tilde{q} \in \mathbb{Q}(i)$

Matrix construction

- **Cyclic algebra:**
$$\mathscr{A} = \left\{ \mathbf{X}_q = \begin{bmatrix} z_1 & z_2 \\ \gamma \cdot \sigma(z_2) & \sigma(z_1) \end{bmatrix} \right\}$$
with $z_1, z_2 \in \mathbb{K}$.
- **Conjugate:** Matrix of cofactors
- **Reduced Norm:** $N_r(q) = \det \mathbf{X}_q$

The Golden Code

- Extracted from a cyclic algebra of index 2 $\mathscr{A} \triangleq (\mathbb{K} = \mathbb{Q}(i,\theta)/\mathbb{Q}(i), \sigma, i)$ with $\theta = \frac{1+\sqrt{5}}{2}$ and $\sigma : \theta \mapsto \bar{\theta} = \frac{1-\sqrt{5}}{2}$.
  - Ring of integers of $\mathbb{K}$ is $\mathscr{O}_{\mathbb{K}} = \{a + b\theta \mid a, b \in \mathbb{Z}[i]\}$.
  - Let $\alpha = 1 + i - i\theta$ and $\mathscr{I}_\alpha = (\alpha)$ be the principal ideal generated by α.

- The Golden Code is

Formal construction

Matrix construction

- Minimum squared determinant is

- Extracted from a cyclic algebra of index 2 $\mathscr{A} \triangleq (\mathbb{K} = \mathbb{Q}(i,\theta)/\mathbb{Q}(i), \sigma, i)$ with $\theta = \frac{1+\sqrt{5}}{2}$ and $\sigma : \theta \mapsto \bar{\theta} = \frac{1-\sqrt{5}}{2}$.
  - Ring of integers of $\mathbb{K}$ is $\mathscr{O}_{\mathbb{K}} = \{a + b\theta \mid a,b \in \mathbb{Z}[i]\}$.
  - Let $\alpha = 1 + i - i\theta$ and $\mathscr{I}_\alpha = (\alpha)$ be the principal ideal generated by α.
- The Golden Code is

Formal construction

$\mathscr{G} = \left\{ \frac{1}{\sqrt{5}} (z_1 + z_2 \cdot e) \right\}$ with $z_1, z_2 \in \mathscr{I}_\alpha$, $e^2 = i$ and $z \cdot e = e \cdot \sigma(z)$

Matrix construction

$\mathscr{G} = \left\{ \frac{1}{\sqrt{5}} \begin{bmatrix} z_1 & z_2 \\ i \cdot \sigma(z_2) & \sigma(z_1) \end{bmatrix} \right\}$ with $z_i = \alpha(x_i + y_i\theta)$ and $x_i, y_i \in \mathbb{Z}[i]$.

- Minimum squared determinant is

$$\delta_{\min}(\mathscr{G}) = \min_{\substack{\mathbf{X} \in \mathscr{G} \\ \mathbf{X} \neq \mathbf{0}}} |\det \mathbf{X}|^2 = \frac{1}{25} |N_{\mathbb{K}/\mathbb{Q}(i)}(\alpha)|^2 = \frac{1}{25} |2+i|^2 = \frac{1}{5}$$

- Extracted from a cyclic algebra of index 2 $\mathscr{A} \triangleq (\mathbb{K} = \mathbb{Q}(i,\theta)/\mathbb{Q}(i), \sigma, i)$ with $\theta = \frac{1+\sqrt{5}}{2}$ and $\sigma : \theta \mapsto \bar{\theta} = \frac{1-\sqrt{5}}{2}$.
  - Ring of integers of $\mathbb{K}$ is $\mathscr{O}_{\mathbb{K}} = \{a + b\theta \mid a, b \in \mathbb{Z}[i]\}$.
  - Let $\alpha = 1 + i - i\theta$ and $\mathscr{I}_\alpha = (\alpha)$ be the principal ideal generated by α.
- The Golden Code is

Formal construction

$\mathscr{G} = \left\{ \frac{1}{\sqrt{5}} (z_1 + z_2 \cdot e) \right\}$ with $z_1, z_2 \in \mathscr{I}_\alpha$,
$e^2 = i$ and $z \cdot e = e \cdot \sigma(z)$

Matrix construction

$\mathscr{G} = \left\{ \frac{1}{\sqrt{5}} \begin{bmatrix} z_1 & z_2 \\ i \cdot \sigma(z_2) & \sigma(z_1) \end{bmatrix} \right\}$ with
$z_i = \alpha(x_i + y_i\theta)$ and $x_i, y_i \in \mathbb{Z}[i]$.

- Minimum squared determinant is

$$\delta_{\min}(\mathscr{G}) = \min_{\substack{\mathbf{X} \in \mathscr{G} \\ \mathbf{X} \neq \mathbf{0}}} |\det \mathbf{X}|^2 = \frac{1}{25} |N_{\mathbb{K}/\mathbb{Q}(i)}(\alpha)|^2 = \frac{1}{25} |2+i|^2 = \frac{1}{5}$$

The Golden Code

- Extracted from a cyclic algebra of index 2 $\mathscr{A} \triangleq (\mathbb{K} = \mathbb{Q}(i,\theta)/\mathbb{Q}(i), \sigma, i)$ with $\theta = \frac{1+\sqrt{5}}{2}$ and $\sigma : \theta \mapsto \bar{\theta} = \frac{1-\sqrt{5}}{2}$.
  - Ring of integers of $\mathbb{K}$ is $\mathscr{O}_{\mathbb{K}} = \{a + b\theta \mid a, b \in \mathbb{Z}[i]\}$.
  - Let $\alpha = 1 + i - i\theta$ and $\mathscr{I}_\alpha = (\alpha)$ be the principal ideal generated by α.
- The Golden Code is

Formal construction

$\mathscr{G} = \left\{ \frac{1}{\sqrt{5}} (z_1 + z_2 \cdot e) \right\}$ with $z_1, z_2 \in \mathscr{I}_\alpha$, $e^2 = i$ and $z \cdot e = e \cdot \sigma(z)$

Matrix construction

$\mathscr{G} = \left\{ \frac{1}{\sqrt{5}} \begin{bmatrix} z_1 & z_2 \\ i \cdot \sigma(z_2) & \sigma(z_1) \end{bmatrix} \right\}$ with $z_i = \alpha (x_i + y_i \theta)$ and $x_i, y_i \in \mathbb{Z}[i]$.

- Minimum squared determinant is

$$\delta_{\min}(\mathscr{G}) = \min_{\substack{\mathbf{X} \in \mathscr{G} \\ \mathbf{X} \neq \mathbf{0}}} |\det \mathbf{X}|^2 = \frac{1}{25} |N_{\mathbb{K}/\mathbb{Q}(i)}(\alpha)|^2 = \frac{1}{25} |2 + i|^2 = \frac{1}{5}$$

- Extracted from a cyclic algebra of index 2 $\mathscr{A} \triangleq (\mathbb{K} = \mathbb{Q}(i,\theta)/\mathbb{Q}(i), \sigma, i)$ with $\theta = \frac{1+\sqrt{5}}{2}$ and $\sigma : \theta \mapsto \bar{\theta} = \frac{1-\sqrt{5}}{2}$.
  - Ring of integers of $\mathbb{K}$ is $\mathscr{O}_{\mathbb{K}} = \{a + b\theta \mid a, b \in \mathbb{Z}[i]\}$.
  - Let $\alpha = 1 + i - i\theta$ and $\mathscr{I}_\alpha = (\alpha)$ be the principal ideal generated by α.
- The Golden Code is

Formal construction

$\mathscr{G} = \left\{ \frac{1}{\sqrt{5}} (z_1 + z_2 \cdot e) \right\}$ with $z_1, z_2 \in \mathscr{I}_\alpha$, $e^2 = i$ and $z \cdot e = e \cdot \sigma(z)$

Matrix construction

$\mathscr{G} = \left\{ \frac{1}{\sqrt{5}} \begin{bmatrix} z_1 & z_2 \\ i \cdot \sigma(z_2) & \sigma(z_1) \end{bmatrix} \right\}$ with $z_i = \alpha(x_i + y_i\theta)$ and $x_i, y_i \in \mathbb{Z}[i]$.

- Minimum squared determinant is

$$\delta_{\min}(\mathscr{G}) = \min_{\substack{\mathbf{X} \in \mathscr{G} \\ \mathbf{X} \neq \mathbf{0}}} |\det \mathbf{X}|^2 = \frac{1}{25} |N_{\mathbb{K}/\mathbb{Q}(i)}(\alpha)|^2 = \frac{1}{25} |2+i|^2 = \frac{1}{5}$$

Outline

What we are looking for...

An ideal whose norm is a power of 2 (Communication engineers want to send bits and not trits or everything else). This power must be as small as possible.

- We have adjoined to $\mathbb{K}$ the element e such that $e^2 = i$.

How to find the partitionning ideal?

What we are looking for...

An ideal whose norm is a power of 2 (Communication engineers want to send bits and not trits or everything else). This power must be as small as possible.

- We have adjoined to $\mathbb{K}$ the element e such that $e^2 = i$.

Methodology

Construct $\mathbb{L} \triangleq \mathbb{K}\left(\sqrt{i}\right) = \mathbb{Q}(\zeta_8, \theta)$ and look for ideals whose norms are a power of 2.

- The smallest power of 2 which works is 4 corresponding to a principal ideal generated by

$$(1-\theta)(i+\zeta_8)$$

- Replace ζ_8 by e but be carefull with the non commutativity!

How to find the partitionning ideal?

What we are looking for...

An ideal whose norm is a power of 2 (Communication engineers want to send bits and not trits or everything else). This power must be as small as possible.

- We have adjoined to $\mathbb{K}$ the element e such that $e^2 = i$.

Methodology

Construct $\mathbb{L} \triangleq \mathbb{K}\left(\sqrt{i}\right) = \mathbb{Q}(\zeta_8, \theta)$ and look for ideals whose norms are a power of 2.

- The smallest power of 2 which works is 4 corresponding to a principal ideal generated by

$$(1-\theta)(i+\zeta_8)$$

- Replace ζ_8 by e but be carefull with the non commutativity!

A quaternionic ideal with reduced norm 4

- Let β be the quaternion $\beta = i(1-\theta) + (1-\theta)e$ with matrix representation

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

Definition

The left quaternionic ideal generated by β is

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

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

- Let β be the quaternion $\beta = i(1-\theta)+(1-\theta)e$ with matrix representation

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

Definition

The left quaternionic ideal generated by β is

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

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

A quaternionic ideal with reduced norm 4

- Let β be the quaternion $\beta = i(1-\theta)+(1-\theta)e$ with matrix representation

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

Definition

The left quaternionic ideal generated by β is

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

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

The quotient ring

- In fact, the quotient ring is the commutative ring

$$\mathscr{G}/\mathfrak{P} \cong \mathbb{F}_2 \oplus u \cdot \mathbb{F}_2$$

with $u^2 = 0$.

- Representatives of the 4 classes are 0, α, αe and $\alpha(1+e)$; u is associated to $\alpha(1+e)$.

Multiplication table of $\mathbb{F}_2 \oplus u \cdot \mathbb{F}_2$ is

$\times$	0	1	u	$1+u$
0	0	0	0	0
1	0	1	u	$1+u$
u	0	u	0	u
$1+u$	0	$1+u$	u	1

- In fact, the quotient ring is the commutative ring

$$\mathcal{G}/\mathfrak{P} \cong \mathbb{F}_2 \oplus u \cdot \mathbb{F}_2$$

with $u^2 = 0$.

- Representatives of the 4 classes are 0, α, αe and $\alpha(1+e)$; u is associated to $\alpha(1+e)$.

Multiplication table of $\mathbb{F}_2 \oplus u \cdot \mathbb{F}_2$ is

$\times$	0	1	u	$1+u$
0	0	0	0	0
1	0	1	u	$1+u$
u	0	u	0	u
$1+u$	0	$1+u$	u	1

The partition chain

Lattice and ideal partition

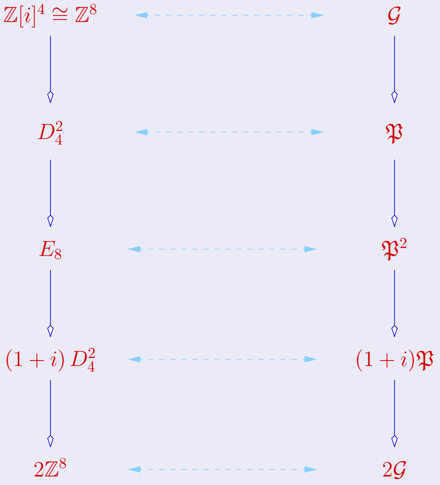


Figure: Partition chain

The Golden Gosset lattice $\mathscr{G}E_8$ (description)

- The principal left quaternionic ideal $\mathfrak{P}^2$ is isomorphic (as a lattice) to the Gosset lattice whose construction A is

$$E_8 = 2\mathbb{Z}^8 + (8,4,4)$$

where $(8,4,4)$ is the extended Hamming code (or Reed-Müller code).

Equivalent E_8 lattice

In fact, $\mathfrak{P}^2$ and E_8 are equivalent lattices i.e. there is a unitary transform (to guarantee the diversity order) and a base change. For example, the unimodular transform matrix is (in complex form)

$$T = \begin{bmatrix} i & -i & 0 & i \\ -i & 0 & i & i \\ 1 & -1 & 0 & i \\ -1 & 0 & i & i \end{bmatrix}$$

- The principal left quaternionic ideal $\mathfrak{P}^2$ is isomorphic (as a lattice) to the Gosset lattice whose construction A is

$$E_8 = 2\mathbb{Z}^8 + (8,4,4)$$

where $(8,4,4)$ is the extended Hamming code (or Reed-Müller code).

Equivalent E_8 lattice

In fact, $\mathfrak{P}^2$ and E_8 are equivalent lattices i.e. there is a unitary transform (to guarantee the diversity order) and a base change. For example, the unimodular transform matrix is (in complex form)

$$T = \begin{bmatrix} i & -i & 0 & i \\ -i & 0 & i & i \\ 1 & -1 & 0 & i \\ -1 & 0 & i & i \end{bmatrix}$$

- Binary labelling after reduction

Quotient group	Coset leaders	Identification
$\mathscr{G}/\mathfrak{P}$	$\{10000000,\ 11000000\}$	
$\mathfrak{P}/\mathfrak{P}^2$	$\{10100000,\ 01010000\}$	
$\mathfrak{P}^2/(1+i)\mathfrak{P}$	$\{11100001,\ 11011000\}$	Reed-Müller
$(1+i)\mathfrak{P}/2\mathscr{G}$	$\{11111111,\ 10101010\}$	(8,4,4) code

- Columns permutation: $\begin{pmatrix} 1 & 2 & 5 & 4 & 7 & 6 & 3 & 8 \end{pmatrix}$

- Binary labelling after reduction

Quotient group	Coset leaders	Identification
$\mathcal{G}/\mathfrak{P}$	$\left\{\begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix}\right\}$	
$\mathfrak{P}/\mathfrak{P}^2$	$\left\{\begin{matrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{matrix}\right\}$	
$\mathfrak{P}^2/(1+i)\mathfrak{P}$	$\left\{\begin{matrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{matrix}\right\}$	Reed-Müller
$(1+i)\mathfrak{P}/2\mathcal{G}$	$\left\{\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{matrix}\right\}$	(8,4,4) code

- Columns permutation: $\begin{pmatrix} 1 & 2 & 5 & 4 & 7 & 6 & 3 & 8 \end{pmatrix}$

Simulation results

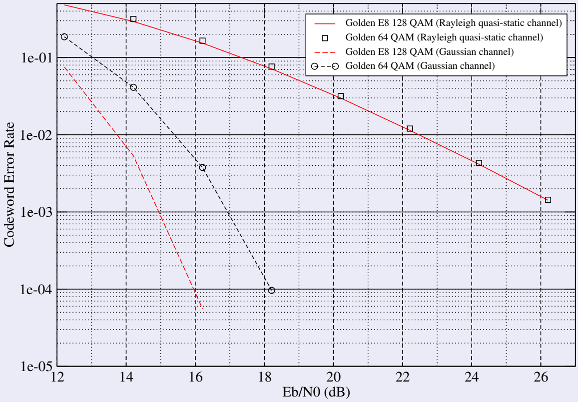


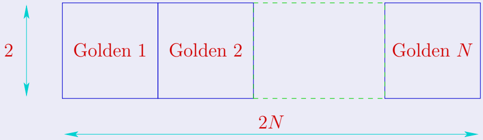
Figure: $\mathcal{G}E_8$ versus Golden Code (12 bits p.c.u.)

Outline

1. Outer-Coded Space-Time Block Codes
   - The quasi static fading channel
   - The inner/outer codes
2. Code construction a la Ungerboeck
   - An example in $\mathbb{Z}$
   - Another example
3. The Golden Code
4. A quaternary partition
   - The partitionning ideal
   - The Gosset Lattice E_8
5. *How to increase the coding gain?*
6. The Golden Leech Lattice $\mathscr{G}\Lambda_{24}$
7. A trellis-coded Golden modulation
   - Code and simulation results

The coding gain of codes with Golden symbols

Code $\mathscr{C}$ with symbols in $\mathscr{G}$



- Codeword is $\mathfrak{Q} = (q_1, q_2, \cdots q_N)$.

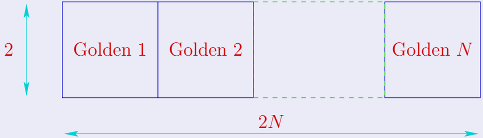
Minimum determinant

The minimum determinant is

$$\min_{\mathfrak{Q}\in\mathscr{C}\setminus\{0\}} \det \mathfrak{Q}\cdot\mathfrak{Q}^\dagger = \min_{\mathfrak{Q}\in\mathscr{C}\setminus\{0\}} \sum_{i=1}^{N} \det\left(q_i\cdot q_i^\dagger\right) + \sum_{j>i} \left\|\tilde{q}_i \cdot q_j\right\|_F^2$$

The coding gain of codes with Golden symbols

Code $\mathscr{C}$ with symbols in $\mathscr{G}$



- Codeword is $\mathfrak{Q} = (q_1, q_2, \cdots q_N)$.

Minimum determinant

The minimum determinant is

$$\min_{\mathfrak{Q}\in\mathscr{C}\setminus\{0\}} \det \mathfrak{Q}\cdot\mathfrak{Q}^\dagger = \min_{\mathfrak{Q}\in\mathscr{C}\setminus\{0\}} \sum_{i=1}^{N} \det\left(q_i \cdot q_i^\dagger\right) + \sum_{j>i} \left\|\tilde{q}_i \cdot q_j\right\|_F^2$$

Outline

Construction of Λ_{24} [Conway Sloane 86]

The Leech lattice Λ_{24} consists of the vectors

$$(e_1 + a + t,\ e_2 + b + t,\ e_3 + c + t)$$

with $e_1, e_2, e_3 \in E_8,\ a + b + c \equiv 0 \pmod{E_8}$ and a, b, c, t are in a list of cosets representatives.

Construction of $\mathscr{G}\Lambda_{24}$

Same construction as above. Simply replace E_8 with $\mathscr{G}E_8$ and use partition of figure 5.

Construction of Λ_{24} [Conway Sloane 86]

The Leech lattice Λ_{24} consists of the vectors

$$(e_1 + a + t,\, e_2 + b + t,\, e_3 + c + t)$$

with $e_1, e_2, e_3 \in E_8,\ a + b + c \equiv 0 \pmod{E_8}$ and a, b, c, t are in a list of cosets representatives.

Construction of $\mathcal{G}\Lambda_{24}$

Same construction as above. Simply replace E_8 with $\mathcal{G}E_8$ and use partition of figure 5.

Simulation results

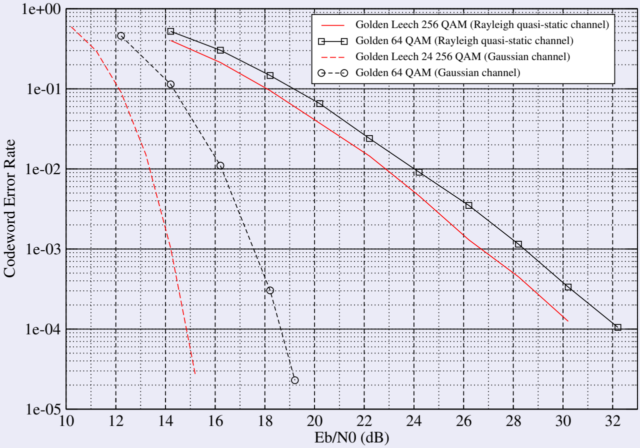


Figure: $\mathscr{G}\Lambda_{24}$ versus Golden Code (12 bits p.c.u.)

Outline

The partition

Partition Chain of $\mathscr{G}$

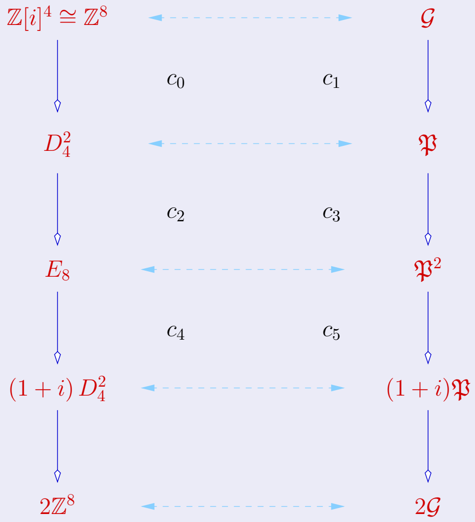
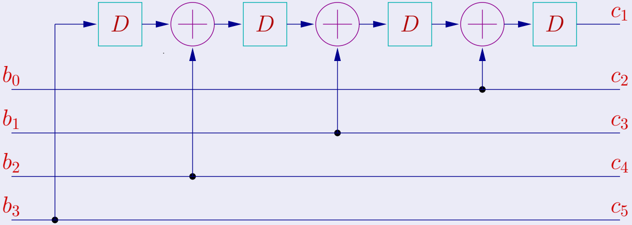


Figure: Partition chain for the trellis construction

- With a 4-state code, we can achieve 1.5dB gain
- With a 16-state code, it is possible to achieve 3dB gain

Convolutional code and bit labelling



Bit c_0 is set to 0.

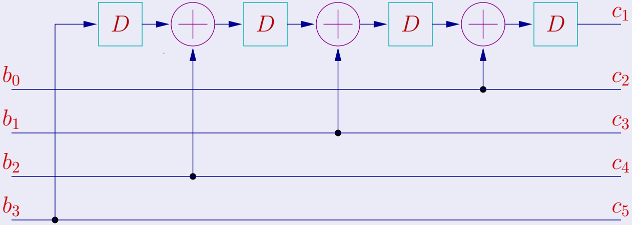
General Coding gain

In general, to achieve $1.5\,r$dB asymptotic gain compared to the Golden code, we need a trellis with 2^{2r} state.

Code

- With a 4-state code, we can achieve 1.5dB gain
- With a 16-state code, it is possible to achieve 3dB gain

Convolutional code and bit labelling



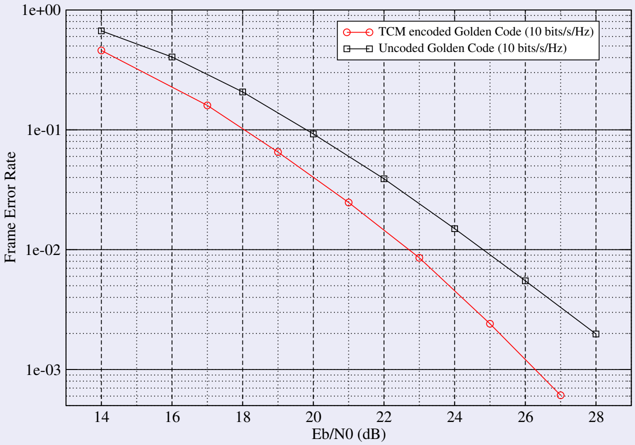
Bit c_0 is set to 0.

General Coding gain

In general, to achieve $1.5\,r$dB asymptotic gain compared to the Golden code, we need a trellis with 2^{2r} state.

Simulation results

Simulation results



- Lots of unsolved problems (roles of Euclidean distances and determinants, link with capacity approaching codes, new mappings, ...)
- But this first attempt gives encouraging results
- Generalization to other division algebras (perfect space-time block codes)

Conclusion

- Lots of unsolved problems (roles of Euclidean distances and determinants, link with capacity approaching codes, new mappings, ...)
- But this first attempt gives encouraging results
- Generalization to other division algebras (perfect space-time block codes)

Conclusion

- Lots of unsolved problems (roles of Euclidean distances and determinants, link with capacity approaching codes, new mappings, ...)
- But this first attempt gives encouraging results
- Generalization to other division algebras (perfect space-time block codes)

Thank you for your attention!