From the Golden Code to Perfect Space-Time Block Codes

joint work with
Jean-Claude Belfiore and Ghaya Rekaya, ENST, Paris, France
Emanuele Viterbo, Politecnico di Torino, Torino, Italy

Algo & LMA Seminar

November 18th, 2004

Frédérique Oggier

Institut de Mathématiques Bernoulli

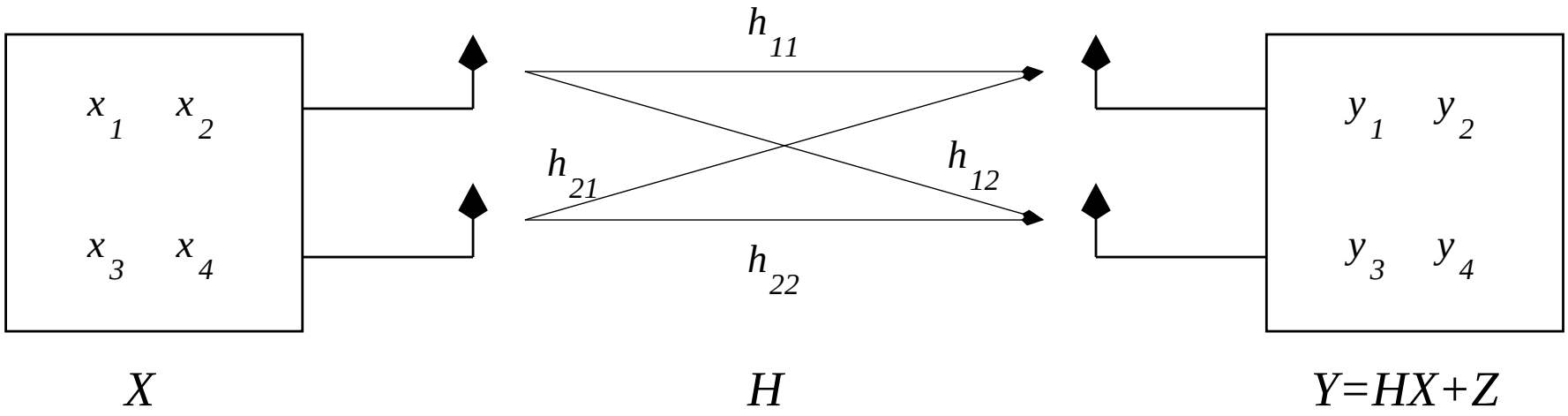
Ecole Polytechnique Fédérale de Lausanne

frederique.oggier@epfl.ch

Outline

- Channel model and code design criteria
- The Golden code
  - a shaping constraint
  - a discrete minimum determinant
  - performance of the Golden code
- The Perfect Space-Time codes
  - definition
  - constructions of perfect Space-Time codes
  - performance of perfect Space-Time codes

The 2×2 *MIMO channel*



- X: 2×2 matrix *codeword* from a *space-time code*

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

  the x_i may belong to a signal constellation S with $|S| = m$ (e.g. PSK, QAM) or be functions of the information symbols taken from S.

- H: 2×2 *channel matrix* is a complex Gaussian matrix with independent, zero mean, entries.

- Z: 2×2 *complex Gaussian noise* matrix.

Code design criteria

- To achieve the maximum diversity we need *full rank* codeword differences, i.e.,

$$rank(\mathbf{X_1} - \mathbf{X_2}) = 2 \qquad \forall\, \mathbf{X_1} \neq \mathbf{X_2} \in \mathcal{C}$$

- To maximize the throughput, we use *full rate* codes, i.e., the four symbols x_1, x_2, x_3, x_4 in the codewords are *functions* of four symbols independently chosen from S and yield $|\mathcal{C}| = m^4$ distinct codewords.

- Note that Alamouti's code $\mathbf{X} = \begin{pmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{pmatrix}$ is full rank but not full rate in a 2×2 MIMO.

- The asymptotic coding gain is given by the *minimum determinant* of $\mathcal{C}$

$$\delta_{\min}(\mathcal{C}) = \min_{\mathbf{X_1} \neq \mathbf{X_2} \in \mathcal{C}} |\det(\mathbf{X_1} - \mathbf{X_2})|^2$$

- A good code will attempt to *maximize* $\delta_{\min}(\mathcal{C})$.

2×2 *Space–Time codes*

- Let $\mathbb{K} = \mathbb{Q}(\theta) = \{a + b\theta \mid a, b \in \mathbb{Q}(i)\}$. It is a quadratic extension of $\mathbb{Q}(i)$.
- We define the *infinite lattice code* $\mathcal{C}_\infty$ as

$$\mathcal{C}_\infty = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} a + b\theta & c + d\theta \\ \gamma(c + d\bar{\theta}) & a + b\bar{\theta} \end{bmatrix} : a, b, c, d \in \mathbb{Z}[i],\ \gamma \in \mathbb{C} \right\}$$

- $\mathcal{C}_\infty$ is a linear code, i.e., $\mathbf{X_1} + \mathbf{X_2} \in \mathcal{C}_\infty$ for all $\mathbf{X_1}, \mathbf{X_2} \in \mathcal{C}_\infty$
- The *finite code* $\mathcal{C}$ is obtained by limiting the *information symbols* to $a, b, c, d \in S \subset \mathbb{Z}[i]$.
- The signal constellation S is a 2^b–QAM, with in-phase and quadrature components equal to $\pm 1, \pm 3, \ldots$ and b bits per symbol.
- The *minimum determinant* of $\mathcal{C}_\infty$ is given by

$$\delta_{\min}(\mathcal{C}_\infty) = \min_{\mathbf{X}_1 \neq \mathbf{X}_2 \in \mathcal{C}_\infty} |\det(\mathbf{X_1} - \mathbf{X_2})|^2 = \min_{\mathbf{0} \neq \mathbf{X} \in \mathcal{C}_\infty} |\det(\mathbf{X})|^2$$

The Golden code: first ingredients

- The Golden code is related to the *Golden number* $\theta = \frac{1+\sqrt{5}}{2}$, one of the roots of $\theta^2 - \theta - 1 = 0$ ($\bar{\theta} = \frac{1-\sqrt{5}}{2}$ is the other one)
- Consider $\mathbb{K} = \mathbb{Q}(i, \sqrt{5}) = \{a + b\theta | a, b \in \mathbb{Q}(i)\}$ as a relative quadratic extension of $\mathbb{Q}(i)$.
- The determinant of $\mathbf{X} \in \mathcal{C}_\infty$ is

$$\begin{aligned} \det(\mathbf{X}) &= (a + b\theta)(a + b\bar{\theta}) - \gamma(c + d\bar{\theta})(c + d\theta) \\ &= N_{\mathbb{K}/\mathbb{Q}(i)}(a + b\theta) - \gamma N_{\mathbb{K}/\mathbb{Q}(i)}(c + d\theta). \end{aligned}$$

- For an element $z = a + b\theta \in \mathbb{K}$, the *relative norm* is

$$N_{\mathbb{K}/\mathbb{Q}(i)}(z) = (a + b\theta)(a + b\bar{\theta}) = a^2 + ab - b^2.$$

- Thus

$$0 = \det(\mathbf{X}) \iff \gamma = N_{\mathbb{K}/\mathbb{Q}(i)}(a + b\theta)/N_{\mathbb{K}/\mathbb{Q}(i)}(c + d\theta) \iff \gamma = N_{\mathbb{K}/\mathbb{Q}(i)}(z)$$

  for an element $z = a + b\theta \in \mathbb{K}$.
- Choose γ which is *not a norm*.

The Golden code: a Space-Time lattice code

- A complex lattice Λ is given by its *generator matrix*:

$$\Lambda = \{M\mathbf{v} \mid \mathbf{v} \in \mathbb{Z}[i]^n\}$$

- Note that $\mathbf{X} \in \mathcal{C}_\infty$ can be written

$$\mathbf{X} = \text{diag}\left(M \begin{bmatrix} a \\ b \end{bmatrix}\right) + \text{diag}\left(M \begin{bmatrix} c \\ d \end{bmatrix}\right) \cdot \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix} = \begin{bmatrix} a+b\theta & c+d\theta \\ \gamma(c+d\bar{\theta}) & a+b\bar{\theta} \end{bmatrix},$$

  where

$$M = \begin{bmatrix} 1 & \theta \\ 1 & \bar{\theta} \end{bmatrix}.$$

- We add a structure of lattice on each layer.
- The Golden code is found as a sublattice of the ST lattice code in order to obtain a "cubic" shaped constellation, which guarantees *no shaping loss*.
- In particular, the vectors (x_1, x_2, x_3, x_4) should belong to a rotated version of the complex lattice $\mathbb{Z}[i]^4$ and the finite constellation should be contained in a rotated hypercube.

The Golden code: a Space-Time lattice code (2)

- We define $\mathcal{C}_\mathcal{I} \subset \mathcal{C}_\infty$ by restricting

$$x_1, x_2, x_3, x_4 \in \mathcal{I} = (\alpha)\mathbb{Z}[i][\sqrt{5}],\ \alpha = 1 + i - i\theta,$$

where $\mathbb{Z}[i][\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}[i]\}$, so that we get a rotated $M\mathbb{Z}[i]^2$ complex lattice on each layer, hence a rotated $\mathbb{Z}[i]^4$, when the code matrices are vectorized.

- Codewords of the Golden code $\mathcal{C}_\mathcal{I}$ are given by

$$\mathbf{X} = \text{diag}\left(M \begin{bmatrix} a \\ b \end{bmatrix}\right) + \text{diag}\left(M \begin{bmatrix} c \\ d \end{bmatrix}\right) \cdot \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(a + b\theta) & \alpha(c + d\theta) \\ \gamma\bar{\alpha}(c + d\bar{\theta}) & \bar{\alpha}(a + b\bar{\theta}) \end{bmatrix}$$

where $a, b, c, d \in \mathbb{Z}[i]$, $\bar{\alpha} = 1 + i(1 - \bar{\theta})$, and

$$M = \begin{bmatrix} \alpha & \alpha\theta \\ \bar{\alpha} & \bar{\alpha}\bar{\theta} \end{bmatrix}.$$

Choosing γ for the Golden code

- The determinant of a codeword $\mathbf{X}$ is now

$$\det(\mathbf{X}) = \frac{1}{5}\left(N_{\mathbb{K}/\mathbb{Q}(i)}(z_1) - \gamma N_{\mathbb{K}/\mathbb{Q}(i)}(z_2)\right) \qquad \forall\ z_1 = \alpha(a+b\theta) \in \mathcal{I},\ \ z_2 = \alpha(c+d\theta) \in \mathcal{I}.$$

- Choose a γ which is not norm of elements of $\mathbb{K}$ to guarantee non-zero determinants.

- Choose a $\gamma \in \mathbb{Z}[i]$, so that

$$\det(\mathbf{X}) \in \frac{1}{d}\mathbb{Z}[i] \text{ for all } \mathbf{X}.$$

  This guarantees *discrete non-vanishing determinants* as the spectral efficiency increases.

- Choose $|\gamma| = 1$, to guarantee that the same average energy is transmitted from each antenna at each channel use. This limits the choice to $\gamma = \pm 1, \pm i$.

- We choose $\gamma = i$, since we can prove that it is not a norm of an element of $\mathbb{K} = \mathbb{Q}(i, \sqrt{5})$.

The minimum determinant of the Golden code

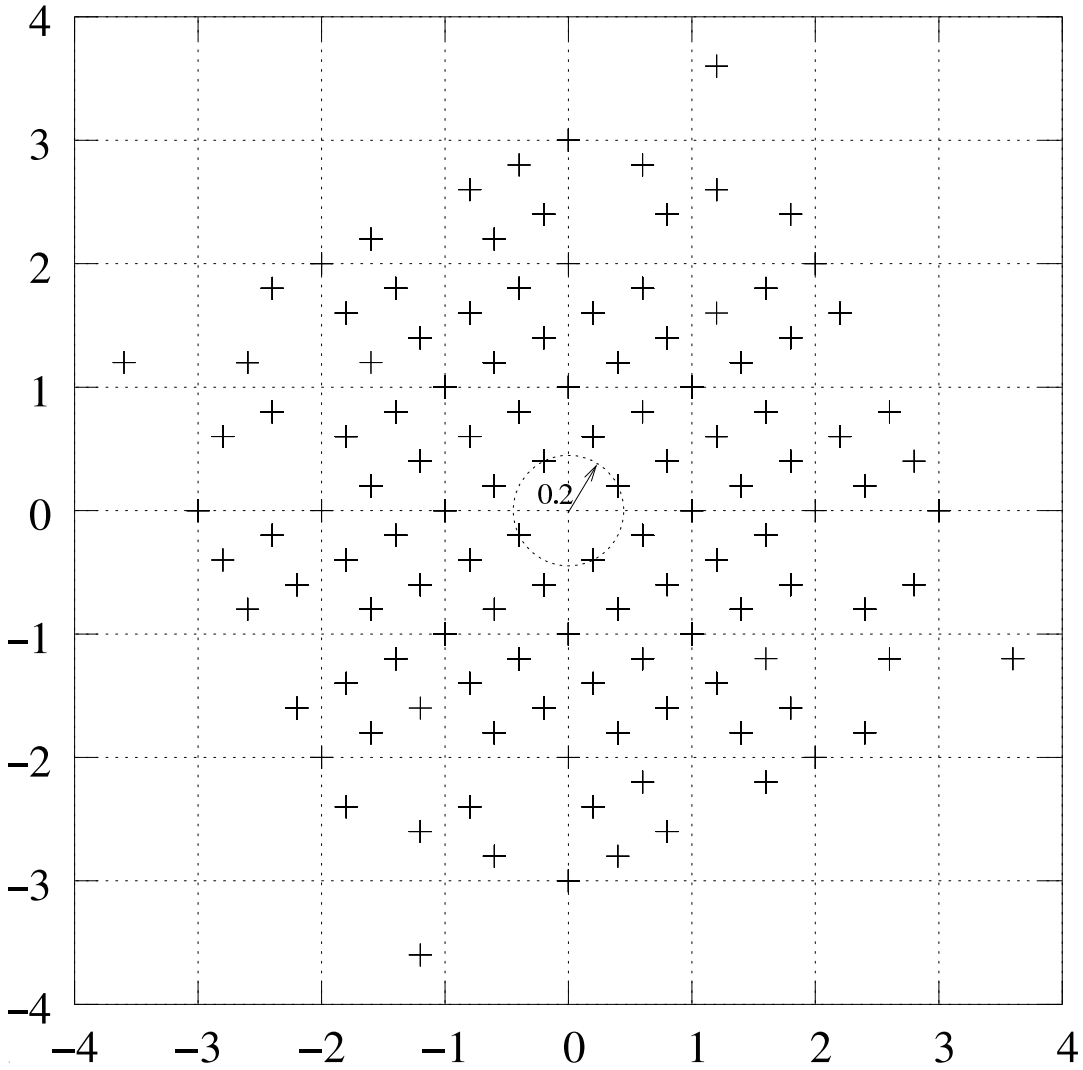
- Let us relate the minimum determinant to the algebraic structure of the code. We have

$$\det(\mathbf{X}) = \frac{1}{5} N_{\mathbb{K}/\mathbb{Q}(i)}(\alpha) \cdot \left(N_{\mathbb{K}/\mathbb{Q}(i)}(a + b\theta) - \gamma N_{\mathbb{K}/\mathbb{Q}(i)}(c + d\bar{\theta}) \right) \qquad \forall\, a, b, c, d \in \mathbb{Z}[i]$$

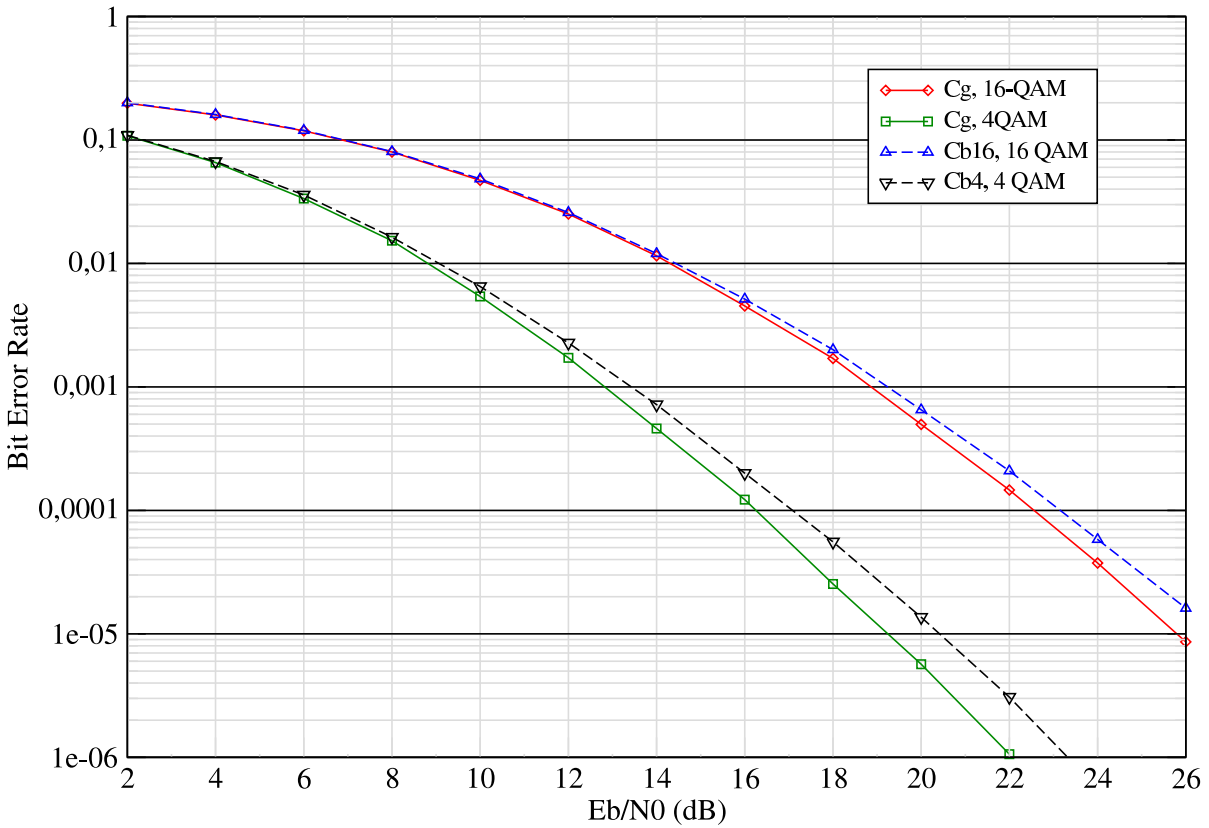
- As the second term in the above equation only takes values in $\mathbb{Z}[i]$ and its minimum modulus is equal to 1 (take $a = 1$ and $b = c = d = 0$), we conclude that the Golden code has

$$\delta_{\min}(\mathcal{C}_{\mathcal{I}}) = \frac{1}{25} |N_{\mathbb{K}/\mathbb{Q}(i)}(\alpha)|^2 = \frac{1}{25} |2 + i|^2 = \frac{1}{5}$$

Some determinants for the codewords of $\mathcal{C}_{\mathcal{I}}$



Performance of the Golden Code



The Golden code from a cyclic division algebra

- Recall that a codeword of the Golden code is of the form

$$\mathbf{X} = \begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix} + \begin{bmatrix} x_3 & 0 \\ 0 & x_4 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix} = \begin{bmatrix} x_1 & x_3 \\ \gamma x_4 & x_2 \end{bmatrix}$$

  where $x_1, x_2, x_3, x_4 \in \mathbb{K}$ and γ is not an algebraic norm of any element of $\mathbb{K}$.

- This is the form in which we can represent the elements of a *cyclic division algebra* $\mathcal{A}$ of degree 2 over $\mathbb{K}$.

- Division algebras guarantee that $\det(\mathbf{X}) \neq 0$ for all codewords.

- Isomorphic versions of the Golden code were independently derived by [Yao, Wornell, 2003] and by [Dayal, Varanasi, 2003] by analytic optimization.

- Our algebraic construction enables to generalize to some larger $n \times n$ systems.

Perfect Space-Time codes

We define a *perfect Space-Time code* to be a $n \times n$ linear dispersion block code that

- is full rate (codewords contain n^2 symbols from 2^b-QAM or 2^b-HEX)
- has minimum non zero determinant which is constant for increasing spectral efficiency (non-vanishing determinant)
- gives a cubic constellation shaping
- is constructed from cyclic division algebras.

Cyclic Algebras: linear full-rate codes

- Elements in a cyclic algebra $\mathcal{A}$ of degree n can be represented by matrices of the form

$$\begin{pmatrix} x_0 & x_1 & \dots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & \dots & \sigma(x_{n-2}) \\ \vdots & & & \vdots \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \dots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

  with $x_i \in \mathbb{K}$.

- The n^2 information symbols $u_{\ell,k}$ are encoded into codewords by

$$x_\ell = \sum_{k=0}^{n-1} u_{\ell,k}\nu_k, \qquad \ell = 0, \dots, n-1$$

  where $\{\nu_k\}_{k=0}^{n-1}$ is a basis of $\mathbb{K}$.

- Information symbols $u_{\ell,k}$ considered are QAM ($\mathbb{Z}[i]$) and HEX ($\mathbb{Z}[j]$). Thus

$$\mathbb{Q}(i) \subset \mathbb{K} \text{ or } \mathbb{Q}(j) \subset \mathbb{K}$$

  where j is a third root of unity.

Cyclic Division Algebras: the rank criterion

- Cyclic Division Algebras: these are cyclic algebras where all matrices are invertible.
- Recall that a cyclic algebra depends on a parameter γ.
- **Proposition.**
  If γ and its powers $\gamma^2, \ldots, \gamma^{n-1}$ are not a norm, then the cyclic algebra $\mathcal{A}$ is a division algebra.

Cyclic Division Algebras: the lattice structure

- We restrict the elements of $\mathcal{A}$ to those where $x_i \in \mathcal{I}, \mathcal{I} \subset \mathbb{K}$. We thus get a STBC of the form

$$\mathcal{C}_{\mathcal{I}} = \left\{ \begin{pmatrix} x_0 & x_1 & \dots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & \dots & \sigma(x_{n-2}) \\ \vdots & & & \vdots \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \dots & \sigma^{n-1}(x_0) \end{pmatrix} \mid x_i \in \mathcal{I} \subseteq \mathbb{K},\ i = 0, \dots, n-1 \right\}.$$

- The n^2 information symbols $u_{\ell,k} \in \mathbb{Z}[i]$ or $\mathbb{Z}[j]$ are encoded into codewords by

$$x_\ell = \sum_{k=0}^{n-1} u_{\ell,k}\nu_k \qquad \ell = 0, \dots, n-1$$

  where $\{\nu_k\}_{k=0}^{n-1}$ is a basis of $\mathcal{I}$.

- We choose $\mathcal{I} \subseteq \mathbb{K}$ so that the signal constellation on each layer is a finite subset of the rotated versions of the lattices $\mathbb{Z}^{2n}$ or A_2^n (the hexagonal lattice).

Cyclic Division Algebras: choosing γ

- Choose γ such that none of its power is a norm to get a non-zero determinant.
- Choose $\gamma \in \mathbb{Z}[i]$ or $\mathbb{Z}[j]$ so that we get *discrete non-vanishing determinants*. That is

$$\det(\mathbf{X}) \in \frac{1}{d}\mathbb{Z}[i] \text{ or } \frac{1}{d}\mathbb{Z}[j].$$

- Choose $|\gamma| = 1$, to guarantee that the same average energy is transmitted from each antenna at each channel use. This limits the choice to

$$\gamma \in \{\pm 1, \pm i\} \subset \mathbb{Z}[i] \text{ or } \gamma \in \{1, j, j^2, -1, -j, j^2\} \subset \mathbb{Z}[j].$$

Cyclic Division Algebras: the minimum determinant

- $\det(\mathbf{X})$ is called the *reduced norm* of $\mathbf{X}$.
- Thanks to the property of the reduced norm, we have

$$\delta_{\min}(\mathcal{C}_{\mathcal{I}}) \geq \frac{1}{d} N(\mathcal{I})$$

where $N(\mathcal{I}) \in \mathbb{N}$ is called the *norm of* $\mathcal{I}$.

Perfect Space-Time codes: summary

Take $\mathcal{A}$ a cyclic division algebra.

- cyclic algebras: yields a full-rate linear code
- cyclic division algebras: fullfills the rank criterion
- the restriction to $\mathcal{I}$: good shaping, and thus energy efficient codes
- the choice of γ: same average energy transmitted from each antenna
- discrete minimum determinant, which is non-vanishing.

All the perfect ST codes

- There exists an entire *family of* 2×2 perfect ST codes based on the fields $\mathbb{K} = \mathbb{Q}(i, \sqrt{p})$ where $p \equiv 5\,(8)$ is a prime. The other codes have $\delta_{\min}(\mathcal{C}_\infty) = 1/p$, hence the Golden code is the best one.

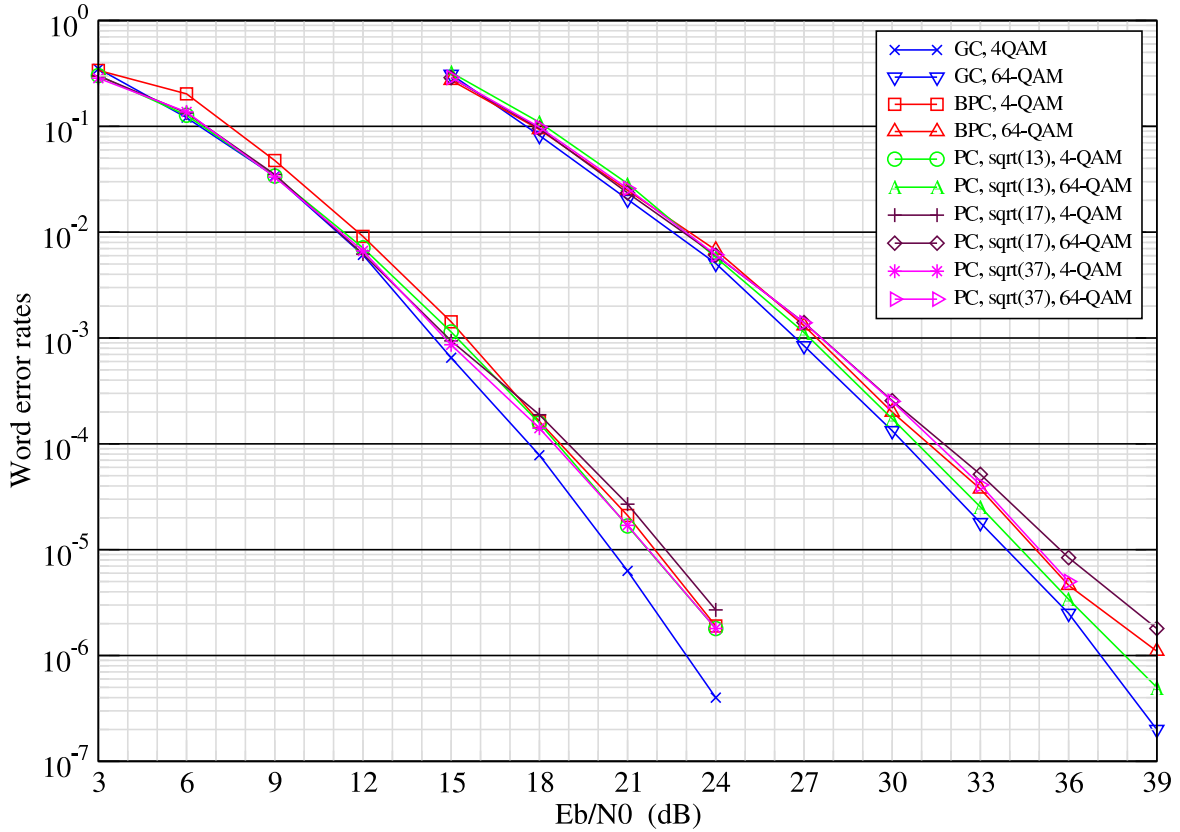
- The 4×4 perfect ST code is found from $\mathbb{K} = \mathbb{Q}(i, 2\cos(2\pi/15))$ and $\gamma = i$. We find the rotated complex lattice $\mathbb{Z}[i]^4$ with the principal ideal generated by $\alpha = 1 - 3i + i\theta^2$ and get $\delta_{\min} = 1/1125$.

- The 3×3 perfect ST code requires HEX symbols since it uses as base field $\mathbb{Q}(j)$ and $\mathbb{K} = \mathbb{Q}(j, 2\cos(2\pi/7))$. We find a rotated version of the lattice A_2^3 using the principal ideal generated by $\alpha = 1 + j + \theta$ and get $\delta_{\min} = 1/49$.

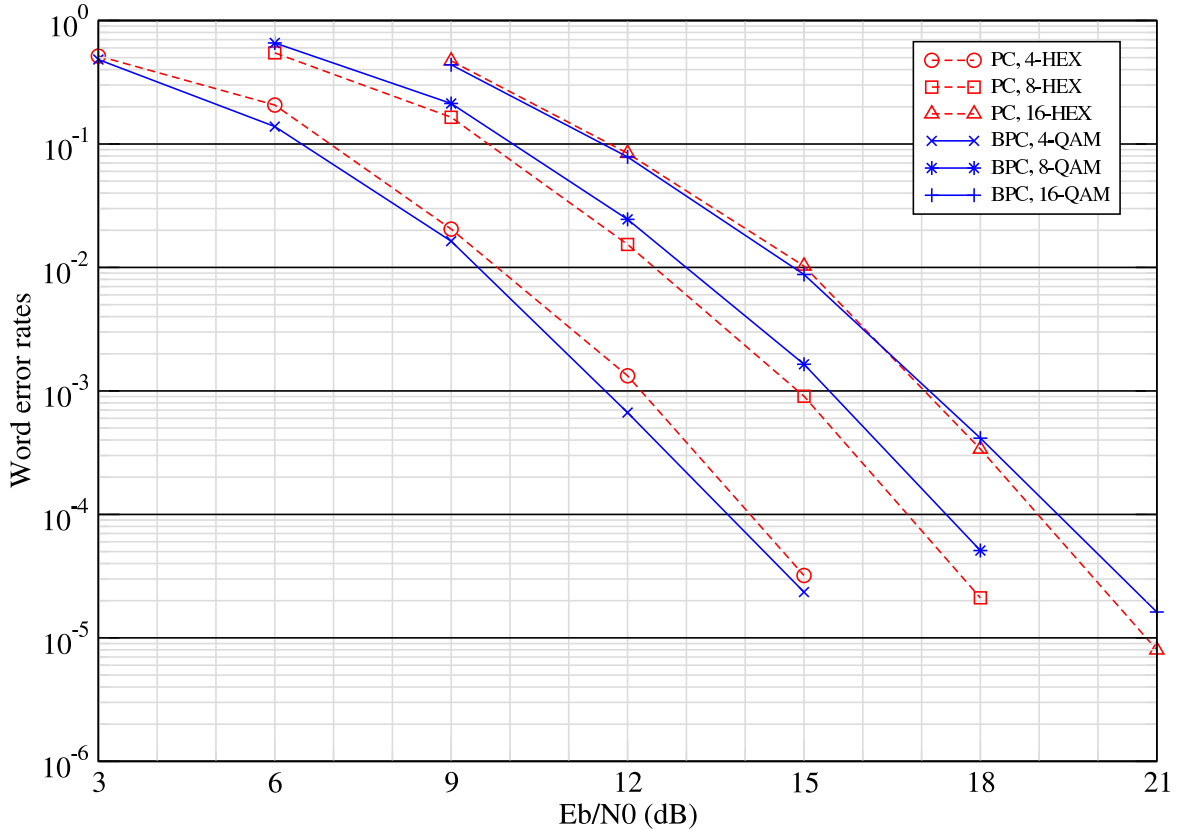
- The 6×6 perfect ST code requires HEX symbols since it uses as base field $\mathbb{Q}(j)$ and $\mathbb{K} = \mathbb{Q}(j, 2\cos(\pi/14))$. We find a rotated version of the lattice A_2^6 using a non principal ideal factor of $(7)\mathcal{O}_\mathbb{K}$ and get $2^{-6}7^{-5} \leq \delta_{\min} \leq 2^{-6}7^{-4}$.

- We prove that *these are the only existing perfect ST codes*.

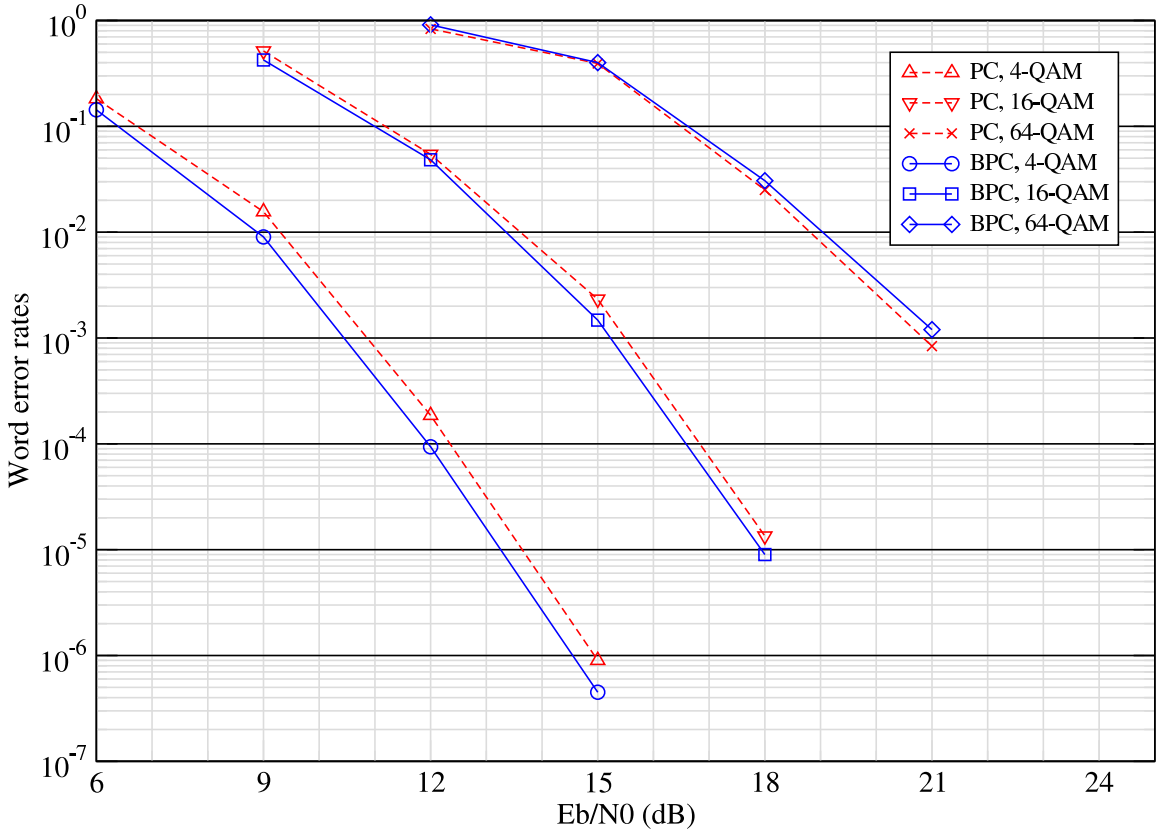
Performance of some 2×2 perfect ST codes



Performance of the 3×3 *perfect ST code*



Performance of the 4×4 *perfect ST code*



Conclusions

- It has been recently shown that codes constructed from cyclic division algebras with center $F = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$ with non-vanishing minimum determinant achieve the Diversity vs Multiplexing Gain tradeoff. [P. Elia, K.R. Kumar, S.A. Pawar, V.V. Kumar, Hsiao-feng Lu, 2004]

- They also propose some STBC algebraic constructions with non-vanishing minimum determinant, that are not perfect since they do not satisfy the cubic shaping condition.

Some references

- M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on the theory of numbers," *IEEE Trans. Inform. Theory*, vol. 48, no. 3, pp. 753–760, March 2002.
- H. El Gamal and M. O. Damen, "Universal space-time coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 5, pp. 1097–1119, May 2003.
- J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proceedings of the Information Theory Workshop*, Paris, March 31–April 4, 2003.
- B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2596–2616, October 2003.
- J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good Lattice Constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 502–518, March 1996.
- H. Cohn, *Advanced Number Theory*, Dover Publications, Inc. New York, 1980.