Aladdin's Code

and other Pythagorean Space–Time Block Codes

J.J. Boutros and H. Randriam

Texas A&M University at Qatar
&
Telecom ParisTech, Paris, France

ISIT, Seoul, July 2009
Presented by Hugues Randriambololona

Aladdin's Code

and other Pythagorean Space–Time Block Codes

J.J. Boutros and H. Randriam

Texas A&M University at Qatar
&
Telecom ParisTech, Paris, France

ISIT, Seoul, July 2009
Presented by Hugues Randriambololona

What is Golden and contains a Genie?

- Aladdin's Lamp (first published 1710, as an addition by Galland to his French translation of the 1001 Nights)
- Aladdin's Code (J.J.B.+ H.R., December 2008)

(a new answer to a 300 year old question, although for both you have to rub them a little to see they are golden).

Two design criteria for Space–Time Block Codes

- Minimize error probability under ML decoding thanks to a non-vanishing determinant condition $\longrightarrow$ (in dim 2) the Golden code, constructed by carefully choosing a lattice in the generalized quaternion algebra $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$.
- Minimize error probability under iterative decoding thanks to the Genie conditions of Boutros-Gresset-Brunel (2003).

What is Golden and contains a Genie?

- Aladdin's Lamp (first published 1710, as an addition by Galland to his French translation of the 1001 Nights)
- Aladdin's Code (J.J.B.+ H.R., December 2008)

(a new answer to a 300 year old question, although for both you have to rub them a little to see they are golden).

Two design criteria for Space–Time Block Codes

- Minimize error probability under ML decoding thanks to a non-vanishing determinant condition $\longrightarrow$ (in dim 2) the Golden code, constructed by carefully choosing a lattice in the generalized quaternion algebra $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$.
- Minimize error probability under iterative decoding thanks to the Genie conditions of Boutros-Gresset-Brunel (2003).

What is Golden and contains a Genie?

- Aladdin's Lamp (first published 1710, as an addition by Galland to his French translation of the 1001 Nights)
- Aladdin's Code (J.J.B.+ H.R., December 2008)

(a new answer to a 300 year old question, although for both you have to rub them a little to see they are golden).

Two design criteria for Space–Time Block Codes

- Minimize error probability under ML decoding thanks to a non-vanishing determinant condition $\longrightarrow$ (in dim 2) the Golden code, constructed by carefully choosing a lattice in the generalized quaternion algebra $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$.
- Minimize error probability under iterative decoding thanks to the Genie conditions of Boutros-Gresset-Brunel (2003).

What is Golden and contains a Genie?

- Aladdin's Lamp (first published 1710, as an addition by Galland to his French translation of the 1001 Nights)
- Aladdin's Code (J.J.B.+ H.R., December 2008)

(a new answer to a 300 year old question, although for both you have to rub them a little to see they are golden).

Two design criteria for Space–Time Block Codes

- Minimize error probability under ML decoding thanks to a non-vanishing determinant condition $\longrightarrow$ (in dim 2) the Golden code, constructed by carefully choosing a lattice in the generalized quaternion algebra $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$.
- Minimize error probability under iterative decoding thanks to the Genie conditions of Boutros-Gresset-Brunel (2003).

What is Golden and contains a Genie?

- Aladdin's Lamp (first published 1710, as an addition by Galland to his French translation of the 1001 Nights)
- Aladdin's Code (J.J.B.+ H.R., December 2008)

(a new answer to a 300 year old question, although for both you have to rub them a little to see they are golden).

Two design criteria for Space–Time Block Codes

- Minimize error probability under ML decoding thanks to a non-vanishing determinant condition $\longrightarrow$ (in dim 2) the Golden code, constructed by carefully choosing a lattice in the generalized quaternion algebra $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$.
- Minimize error probability under iterative decoding thanks to the Genie conditions of Boutros-Gresset-Brunel (2003).

Channel model

$$\mathbf{Y} = \mathbf{HX} + \mathbf{N}$$

where $\mathbf{H}$ is $n_r \times n_t$, $\mathbf{X}$ is $n_t \times T$, and $\mathbf{Y}$ and $\mathbf{N}$ are $n_r \times T$.
We will suppose $n_r = n_t = n$.

Linear space-time block code

$$\mathbf{X_c} = c_1\mathbf{M}_1 + \cdots + c_k\mathbf{M}_k$$

where $\mathbf{M}_1, \ldots, \mathbf{M}_k$ are the generating codewords, the code has dimension $k \leq nT$, and $\mathbf{c} = (c_1, \ldots, c_k)$ is the information vector with entries c_j in some (finite or infinite) constellation $\mathcal{A}$ in $\mathbb{C}$, e.g. $\mathcal{A} = \mathbb{Z}[i]$.

Shaping condition

To optimize energetic efficiency the generating codewords have to make an orthonormal family (up to some scalar) in the space of $n \times T$ matrices (for the L^2 norm).

Under ML decoding, for SNR γ, the pairwise error probability is upper bounded as

$$P(\mathbf{X} \to \mathbf{X}') \quad \leq \quad \left(\frac{1}{\prod_{i=1}^{t}(1+\lambda_i \gamma/4n)} \right)^n \quad \leq \quad \left(\frac{g\gamma}{4n} \right)^{-tn}$$

where: $t = \mathrm{rk}(\mathbf{X}-\mathbf{X}') \leq \min(n, T)$, the λ_i are the non-zero eigenvalues of $(\mathbf{X}-\mathbf{X}')(\mathbf{X}-\mathbf{X}')^*$, and $g = (\lambda_1 \lambda_2 \cdots \lambda_t)^{1/t}$ its normalized determinant.

The famous design criteria for ML decoding can be recalled as follows:

- Rank: Full diversity is achieved if $t = n$ $(\leq T)$.
- Product distance: Coding gain is maximized by maximizing the determinant.

Full diversity can be attained with $T = n$ if a suitable unitary coding scheme is applied.

Under ML decoding, for SNR γ, the pairwise error probability is upper bounded as

$$P(\mathbf{X} \to \mathbf{X}') \quad \leq \quad \left(\frac{1}{\prod_{i=1}^{t}(1+\lambda_i \gamma/4n)} \right)^n \quad \leq \quad \left(\frac{g\gamma}{4n} \right)^{-tn}$$

where: $t = \mathrm{rk}(\mathbf{X}-\mathbf{X}') \leq \min(n, T)$, the λ_i are the non-zero eigenvalues of $(\mathbf{X}-\mathbf{X}')(\mathbf{X}-\mathbf{X}')^*$, and $g = (\lambda_1 \lambda_2 \cdots \lambda_t)^{1/t}$ its normalized determinant.

The famous design criteria for ML decoding can be recalled as follows:

- Rank: Full diversity is achieved if $t = n$ $(\leq T)$.
- Product distance: Coding gain is maximized by maximizing the determinant.

Full diversity can be attained with $T = n$ if a suitable unitary coding scheme is applied.

Under iterative decoding, assuming perfect a priori produced by a decoder, the performance depends on the squared Euclidean metric $D^2 = \|\mathbf{HX_c} - \mathbf{HX_{c'}}\|^2 = \|\mathbf{HX_{c-c'}}\|^2$, where $\mathbf{c} - \mathbf{c}' = (0 \dots 0\ \Delta\ 0 \dots 0)$ (say Δ in j-th position), so that

$$D^2 = |\Delta|^2 \|\mathbf{HM}_j\|^2.$$

How to optimize distribution for D^2 ?

When $\mathbf{H}$ has complex gaussian entries, properties of χ^2 distributions show error probability is minimal when the $\mathbf{M}_j$ are chosen to be unitary matrices (up to some scalar).
This reformulates, and unifies, the two Genie conditions of Boutros-Gresset-Brunel (2003).

Under iterative decoding, assuming perfect a priori produced by a decoder, the performance depends on the squared Euclidean metric $D^2 = \|\mathbf{HX_c} - \mathbf{HX_{c'}}\|^2 = \|\mathbf{HX_{c-c'}}\|^2$, where $\mathbf{c} - \mathbf{c}' = (0 \dots 0\ \Delta\ 0 \dots 0)$ (say Δ in j-th position), so that

$$D^2 = |\Delta|^2 \|\mathbf{HM}_j\|^2.$$

How to optimize distribution for D^2 ?

When $\mathbf{H}$ has complex gaussian entries, properties of χ^2 distributions show error probability is minimal when the $\mathbf{M}_j$ are chosen to be unitary matrices (up to some scalar).
This reformulates, and unifies, the two Genie conditions of Boutros-Gresset-Brunel (2003).

Up to normalization by some scalar constant, this leads us to our:

Main mathematical problem

Find $n \times n$ complex matrices $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ such that:

- they lie in $\mathbf{U}(n)$, the unitary group – Genie condition (G)
- they form an orthogonal basis of $\mathbf{M}_n(\mathbb{C})$ – shaping condition (S)
- the code they generate has minimal determinant as big as possible.

Remark: problem remains unchanged if replace each $\mathbf{M}_j$ with $U\mathbf{M}_j V$ for some $U, V \in \mathbf{U}(n)$. This defines an equivalence relation.

Up to normalization by some scalar constant, this leads us to our:

Main mathematical problem

Find $n \times n$ complex matrices $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ such that:

- they lie in $\mathbf{U}(n)$, the unitary group – Genie condition (G)
- they form an orthogonal basis of $\mathbf{M}_n(\mathbb{C})$ – shaping condition (S)
- the code they generate has minimal determinant as big as possible.

Remark: problem remains unchanged if replace each $\mathbf{M}_j$ with $U\mathbf{M}_j V$ for some $U, V \in \mathbf{U}(n)$. This defines an equivalence relation.

In the 2×2 MIMO case, diagonalization theorem for unitary matrices gives:

Theorem 1

Any $\mathbf{M}_1, \ldots, \mathbf{M}_4$ in $M_2(\mathbb{C})$ satisfying (G) and (S) are equivalent to some

$$\mathbf{M}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \; \mathbf{M}_2 = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix} \; \mathbf{M}_3 = \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix} \; \mathbf{M}_4 = \begin{pmatrix} 0 & \gamma \\ -\gamma & 0 \end{pmatrix}$$

for $\alpha, \beta, \gamma \in \mathbb{C}$ with $|\alpha| = |\beta| = |\gamma| = 1$.

For $\mathbf{M}_1, \ldots, \mathbf{M}_4$ as in the above Theorem and for $\mathbf{c} \in \mathcal{A}^4$, one has

$$\mathbf{X}_\mathbf{c} = \frac{1}{\sqrt{2}} \begin{pmatrix} c_1 + \alpha c_2 & \beta c_3 + \gamma c_4 \\ \beta c_3 - \gamma c_4 & c_1 - \alpha c_2 \end{pmatrix}$$

(here we took care of the normalization constant), so that

$$\det \mathbf{X}_\mathbf{c} = \frac{1}{2}(c_1^2 - \alpha^2 c_2^2 - \beta^2 c_3^2 + \gamma^2 c_4^2) = \frac{1}{2} q_{u,v,w}(\mathbf{c})$$

where $u = \alpha^2$, $v = \beta^2$, $w = \gamma^2$, and the quadratic form $q_{u,v,w}$ is defined in the next slide.

For $u, v, w \in \mathbb{C}$ with $|u| = |v| = |w| = 1$, for $\mathbf{z} = (z_1, z_2, z_3, z_4) \in \mathbb{C}^4$, define

$$q_{u,v,w}(\mathbf{z}) = z_1^2 - uz_2^2 - vz_3^2 + wz_4^2$$

For any subset $\mathcal{A}$ of $\mathbb{C}$, define

$$\text{maxqmin}(\mathcal{A}) = \sup_{|u|=|v|=|w|=1} \left(\inf_{\mathbf{c} \in \mathcal{A}^4 \setminus \{\mathbf{0}\}} |q_{u,v,w}(\mathbf{c})| \right)$$

Then, if $\mathcal{A}$ is an additive subgroup of $\mathbb{C}$, we get:

Corollary 1

The supremum value of the minimum determinant of 2×2 linear space-time codes on $\mathcal{A}$ satisfying the shaping and Genie conditions is

$$\frac{1}{2} \text{maxqmin}(\mathcal{A}).$$

From this Corollary: A perfect 2×2 space-time code satisfying the Genie conditions exists if and only if $\mathrm{maxqmin}(\mathcal{A}) > 0$. If the latter is attained for a particular value of u, v, w, then there exists a corresponding code with optimal coding gain.

So we are reduced to computing

$$\mathrm{maxqmin}(\mathcal{A}) = \sup_{|u|=|v|=|w|=1} \left(\inf_{\mathbf{c} \in \mathcal{A}^4 \setminus \{\mathbf{0}\}} |q_{u,v,w}(\mathbf{c})| \right)$$

where

$$q_{u,v,w}(\mathbf{z}) = z_1^2 - u z_2^2 - v z_3^2 + w z_4^2.$$

Now let $\mathcal{A} = \mathbb{Z}[i]$ or $\mathbb{Z}[j]$, and $K = \mathcal{A}_{\mathbb{Q}} = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$.
First we'll get a lower bound, and then an upper bound, on this quantity.

The two bounds will match!

From this Corollary: A perfect 2×2 space-time code satisfying the Genie conditions exists if and only if $\mathrm{maxqmin}(\mathcal{A}) > 0$. If the latter is attained for a particular value of u, v, w, then there exists a corresponding code with optimal coding gain.

So we are reduced to computing

$$\mathrm{maxqmin}(\mathcal{A}) = \sup_{|u|=|v|=|w|=1} \left(\inf_{\mathbf{c} \in \mathcal{A}^4 \setminus \{\mathbf{0}\}} |q_{u,v,w}(\mathbf{c})| \right)$$

where

$$q_{u,v,w}(\mathbf{z}) = z_1^2 - u z_2^2 - v z_3^2 + w z_4^2.$$

Now let $\mathcal{A} = \mathbb{Z}[i]$ or $\mathbb{Z}[j]$, and $K = \mathcal{A}_{\mathbb{Q}} = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$.
First we'll get a lower bound, and then an upper bound, on this quantity.

The two bounds will match!

From this Corollary: A perfect 2×2 space-time code satisfying the Genie conditions exists if and only if $\mathrm{maxqmin}(\mathcal{A}) > 0$. If the latter is attained for a particular value of u, v, w, then there exists a corresponding code with optimal coding gain.

So we are reduced to computing

$$\mathrm{maxqmin}(\mathcal{A}) = \sup_{|u|=|v|=|w|=1} \left(\inf_{\mathbf{c} \in \mathcal{A}^4 \setminus \{\mathbf{0}\}} |q_{u,v,w}(\mathbf{c})| \right)$$

where

$$q_{u,v,w}(\mathbf{z}) = z_1^2 - u z_2^2 - v z_3^2 + w z_4^2.$$

Now let $\mathcal{A} = \mathbb{Z}[i]$ or $\mathbb{Z}[j]$, and $K = \mathcal{A}_{\mathbb{Q}} = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$.
First we'll get a lower bound, and then an upper bound, on this quantity.

The two bounds will match!

Lower bound on the minimal determinant...

We start with the following remarks:

- Take $u, v \in K$ and $w = uv$, then $q_{u,v,w}$ is the reduced norm form of the generalized quaternion algebra $\left(\frac{u,v}{K}\right)$, which is the central simple K-algebra of dimension 4 with basis $1, e, f, g$ satisfying $e^2 = u$, $f^2 = v$, and $g = ef = -fe$ (so $g^2 = -w$).
- If this quaternion algebra is a division algebra, then $q_{u,v,w}$ does not represent 0 over K.
- If $d \in \mathcal{A}$ is a common denominator for u, v, w, then $q_{u,v,w}(\mathbf{c}) \in \frac{1}{d}\mathcal{A}$ for $\mathbf{c} \in \mathcal{A}^4$.

Thus, for any non-zero $\mathbf{c} \in \mathcal{A}^4$ we have a lower bound

$$|q_{u,v,w}(\mathbf{c})| \geq \frac{1}{|d|}.$$

... or: Where algebraic number theory enters the scene

Strategy

Take $u, v \in K$ with smallest possible denominators (e.g. in $\mathcal{A}$?) satisfying the constraints:

- $|u| = |v| = 1$
- the quaternion algebra $\left(\frac{u,v}{K}\right)$ is a division algebra.

Remarks:

- the set of elements in K with $|.| = 1$ forms a subgroup $K_1^\times$ of $K^\times$, with structure easy to determine
- last condition is equivalent to u not a square in K and v not a norm from $K(\sqrt{u})$ to K.

Lemma 1

The group $K_1^\times$ is generated by the units in $\mathcal{A}$ and the elements $x_p/\overline{x_p}$ where $p = x_p\overline{x_p}$ are the primes that split in K ($p \equiv 1 \bmod 4$ for $\mathcal{A} = \mathbb{Z}[i]$, or $p \equiv 1 \bmod 3$ for $\mathcal{A} = \mathbb{Z}[j]$).

Lemma 2

The units in $\mathcal{A}$ that are not squares in K are $\{\pm i\}$ for $\mathcal{A} = \mathbb{Z}[i]$ and $\{-1, -j, -j^2\}$ for $\mathcal{A} = \mathbb{Z}[j]$.
If we take u such a unit, then all other units are norms from $K(\sqrt{u})$ to K.

To minimize denominators, first take u such a unit. Then v cannot be taken a unit anymore, so we'll take $v = x_p/\overline{x_p}$ with p as small as possible, but still giving a division algebra:

Lemma 3

A necessary and sufficient condition for v not to be a norm from $K(\sqrt{u})$ to K, is that $p \equiv 5 \bmod 8$ for $\mathcal{A} = \mathbb{Z}[i]$, or $p \equiv 7 \bmod 12$ for $\mathcal{A} = \mathbb{Z}[j]$.

- Alphabet $\mathcal{A} = \mathbb{Z}[i]$.
- Let r be a product of split primes. Then one can write $r = a^2 + b^2$ and put $x_r = a + ib$. Let also $x_r^2 = c + id$, so $c = a^2 - b^2$ and $d = 2ab$.
- Then $r^2 = c^2 + d^2$, and (c, d, r) is known as a Pythagorean triple.
- For $u = i$, $v = x_r/\overline{x_r} = x_r^2/r$, and $w = uv$, the quadratic form is

$$q_{u,v,w}(\mathbf{z}) = (z_1^2 - iz_2^2) - \tfrac{c+id}{r}(z_3^2 - iz_4^2)$$

and the code can be constructed by putting in Theorem 1:
$\alpha = \sqrt{u} = e^{i\pi/4}$, $\beta = \sqrt{v} = x_r/\sqrt{r}$, and $\gamma = \sqrt{w} = \alpha\beta$.

- If moreover $r = p$ is a prime $\equiv 5 \bmod 8$, then $q_{u,v,w}$ does not represent zero and has absolute value always at least

$$\frac{1}{|\overline{x_p}|} = \frac{1}{\sqrt{p}}.$$

- The corresponding Pythagorean code has minimum determinant at least

$$\frac{1}{2\sqrt{p}}.$$

- Alphabet $\mathcal{A} = \mathbb{Z}[i]$.
- Let r be a product of split primes. Then one can write $r = a^2 + b^2$ and put $x_r = a + ib$. Let also $x_r^2 = c + id$, so $c = a^2 - b^2$ and $d = 2ab$.
- Then $r^2 = c^2 + d^2$, and (c, d, r) is known as a Pythagorean triple.
- For $u = i$, $v = x_r/\overline{x_r} = x_r^2/r$, and $w = uv$, the quadratic form is

$$q_{u,v,w}(\mathbf{z}) = (z_1^2 - iz_2^2) - \tfrac{c+id}{r}(z_3^2 - iz_4^2)$$

and the code can be constructed by putting in Theorem 1:
$\alpha = \sqrt{u} = e^{i\pi/4}$, $\beta = \sqrt{v} = x_r/\sqrt{r}$, and $\gamma = \sqrt{w} = \alpha\beta$.

- If moreover $r = p$ is a prime $\equiv 5 \bmod 8$, then $q_{u,v,w}$ does not represent zero and has absolute value always at least

$$\frac{1}{|\overline{x_p}|} = \frac{1}{\sqrt{p}}.$$

- The corresponding Pythagorean code has minimum determinant at least

$$\frac{1}{2\sqrt{p}}.$$

Upper bound on the minimal determinant

So far we get:

- $\mathcal{A} = \mathbb{Z}[i]$, $u = i$, $p = 5 \longrightarrow \text{maxqmin}(\mathbb{Z}[i]) \geq \frac{1}{\sqrt{5}}$
- $\mathcal{A} = \mathbb{Z}[j]$, $u = -1$, $p = 7 \longrightarrow \text{maxqmin}(\mathbb{Z}[j]) \geq \frac{1}{\sqrt{7}}$.

What is the optimal value?

On the opposite direction,

$$\text{maxqmin}(\mathcal{A}) \leq \text{maxqmin}(\mathcal{B})$$

for any $\mathcal{B} \subset \mathcal{A}$. If we choose $\mathcal{B}$ finite, then

$$\text{maxqmin}(\mathcal{B}) = \sup_{|u|=|v|=|w|=1} \left(\inf_{\mathbf{c} \in \mathcal{B}^4 \setminus \{\mathbf{0}\}} |q_{u,v,w}(\mathbf{c})| \right)$$

can be computed analytically exactly (piecewise smooth function over a smooth compact set!).

Upper bound on the minimal determinant

So far we get:

- $\mathcal{A} = \mathbb{Z}[i]$, $u = i$, $p = 5 \longrightarrow \text{maxqmin}(\mathbb{Z}[i]) \geq \frac{1}{\sqrt{5}}$
- $\mathcal{A} = \mathbb{Z}[j]$, $u = -1$, $p = 7 \longrightarrow \text{maxqmin}(\mathbb{Z}[j]) \geq \frac{1}{\sqrt{7}}$.

What is the optimal value?

On the opposite direction,

$$\text{maxqmin}(\mathcal{A}) \leq \text{maxqmin}(\mathcal{B})$$

for any $\mathcal{B} \subset \mathcal{A}$. If we choose $\mathcal{B}$ finite, then

$$\text{maxqmin}(\mathcal{B}) = \sup_{|u|=|v|=|w|=1} \left(\inf_{\mathbf{c} \in \mathcal{B}^4 \setminus \{\mathbf{0}\}} |q_{u,v,w}(\mathbf{c})| \right)$$

can be computed analytically exactly (piecewise smooth function over a smooth compact set!).

By choosing a convenient $\mathcal{B}$ (e.g. $\mathcal{B} = 16$-QAM in case $\mathcal{A} = \mathbb{Z}[i]$), one shows equality:

- $\mathrm{maxqmin}(\mathbb{Z}[i]) = \frac{1}{\sqrt{5}}$
- $\mathrm{maxqmin}(\mathbb{Z}[j]) = \frac{1}{\sqrt{7}}$.

Moreover, up to the natural symmetries of the problem, the only values of u, v, w attaining this optimum are those given above.

Thus, the corresponding codes have minimum determinant $\frac{1}{2\sqrt{5}}$ and $\frac{1}{2\sqrt{7}}$ respectively, which is best possible, and are unique up to equivalence.

Aladdin's code

We construct Aladdin's code by taking $\mathcal{A} = \mathbb{Z}[i]$, $p = 5$ with $x_5 = 2 + i$, and associated Pythagorean triple $(3, 4, 5)$. The quadratic form is

$$q_{u,v,w}(\mathbf{z}) = (z_1^2 - iz_2^2) - \tfrac{3+4i}{5}(z_3^2 - iz_4^2)$$

and quaternion algebra $\left(\frac{i,x_5^2/5}{\mathbb{Q}(i)}\right) = \left(\frac{i,5}{\mathbb{Q}(i)}\right)$, the same as the Golden code.

However, we get a different lattice in that algebra (thus pay a small loss in minimum determinant in price for the Genie). In Theorem 1 we can put:

$$\alpha = \frac{1+i}{\sqrt{2}} = e^{i\pi/4} \qquad \beta = \frac{2+i}{\sqrt{5}} = e^{i\,\mathrm{atan}(1/2)} \qquad \gamma = \frac{1+3i}{\sqrt{10}} = e^{i\,\mathrm{atan}(3)}$$

and get as precoder matrix (in linearized form):

$$\mathbf{S}_{\text{Aladdin}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ \alpha & 0 & 0 & -\alpha \\ 0 & \beta & \beta & 0 \\ 0 & \gamma & -\gamma & 0 \end{pmatrix}$$

Aladdin's code

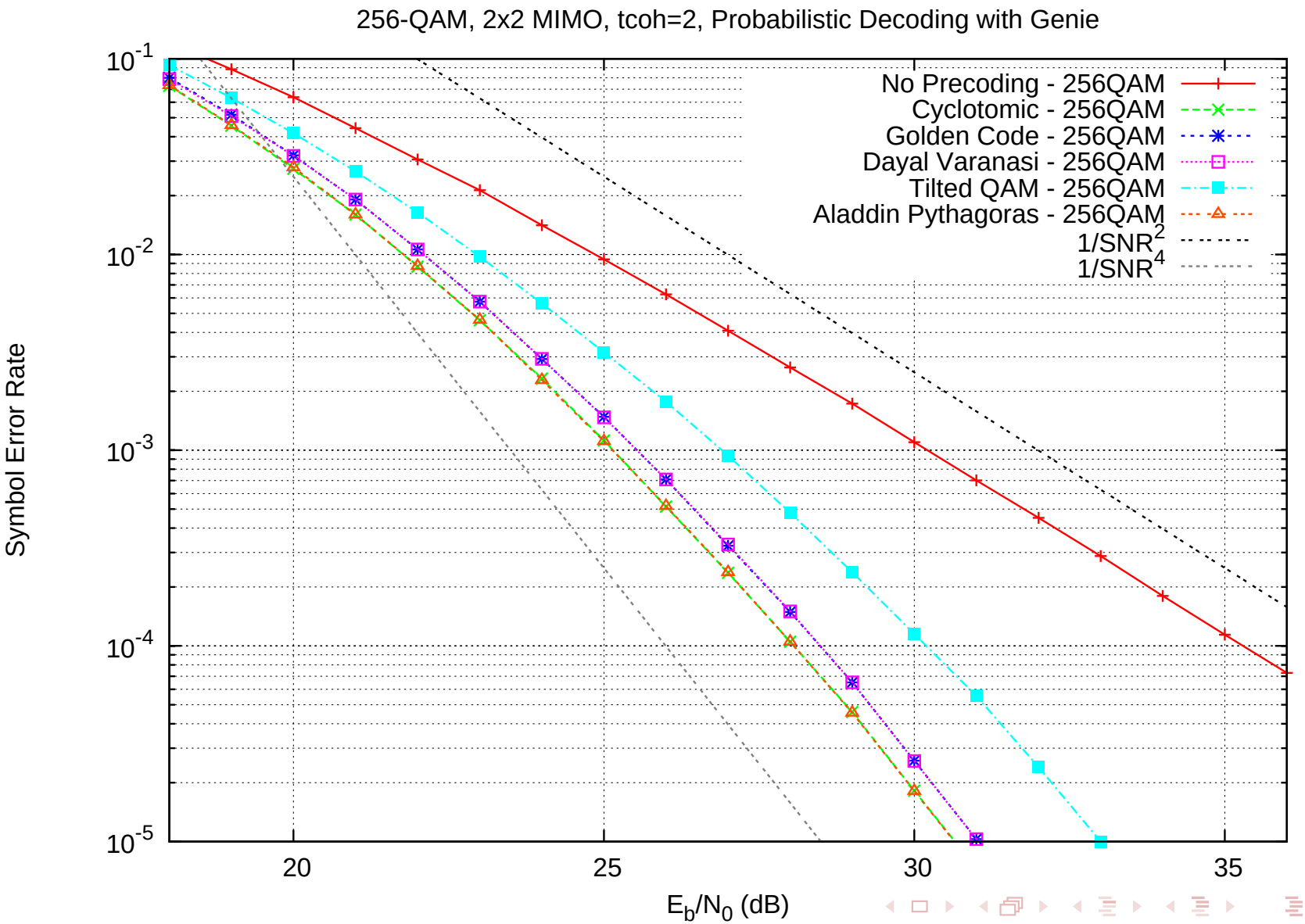
All in all:

Theorem 2

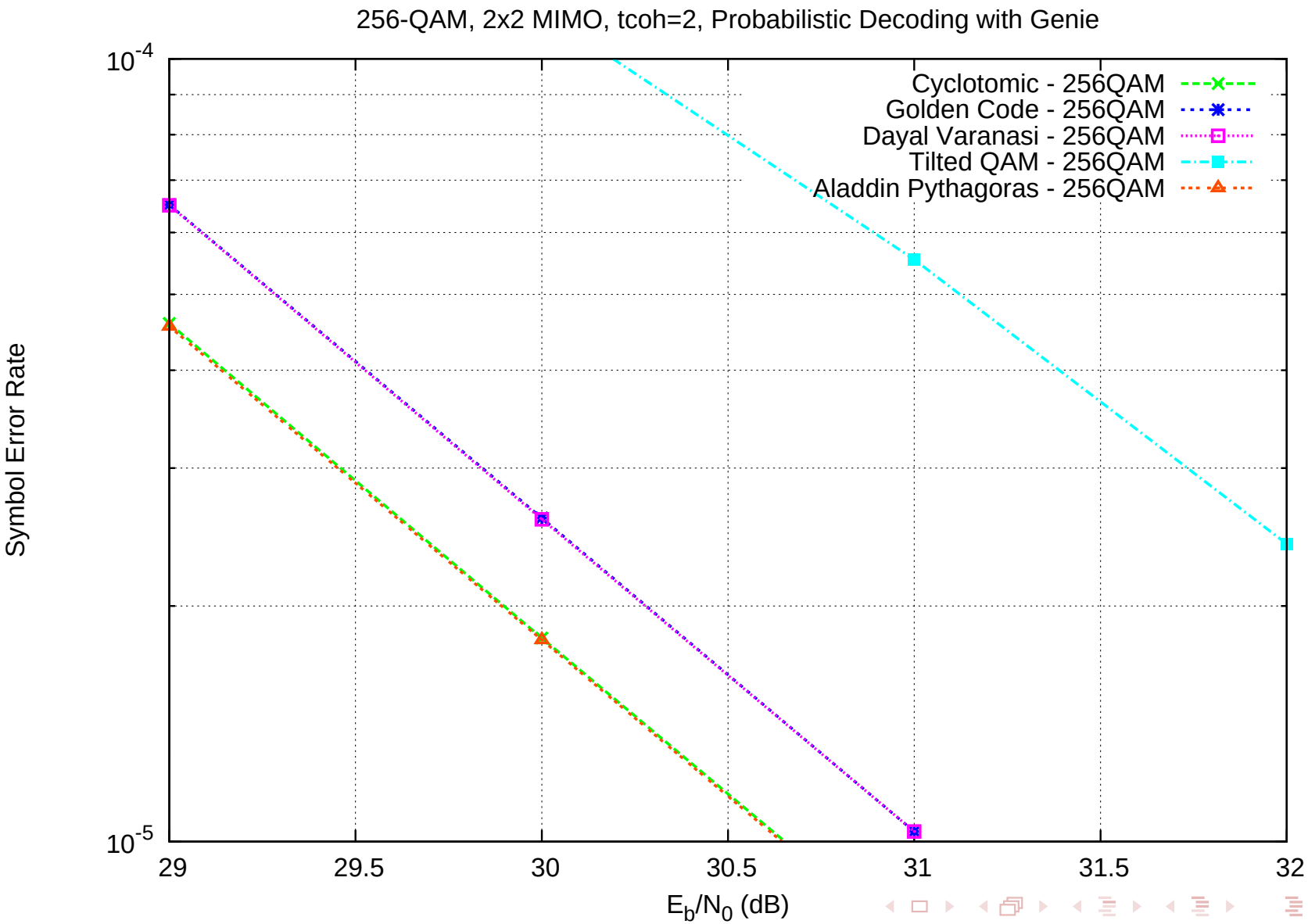
Aladdin's code is a perfect 2×2 space-time code over $\mathbb{Z}[i]$ satisfying the Genie conditions, with minimum determinant $\frac{1}{2\sqrt{5}}$.
Moreover, it has optimal coding gain: any code satisfying these properties has minimum determinant strictly less than $\frac{1}{2\sqrt{5}}$, unless it is equivalent to Aladdin's.
In fact, this optimality property already holds when restricted to a 16-QAM.

In the same way, we get a perfect 2×2 space-time code over $\mathbb{Z}[j]$ satisfying the Genie conditions, with minimum determinant $\frac{1}{2\sqrt{7}}$. This is optimal, and this code is unique up to equivalence.

Performance comparison with different precoders (1)



Performance comparison with different precoders (2)



Summary

- We reformulated and showed how to combine the Genie conditions and the rank criterion in an amenable way.
- The 2-dimensional case is completely solved: Over $\mathbb{Z}[i]$, perfect 2×2 STBC satisfying the Genie conditions can be easily constructed from Pythagorean triples satisfying some congruence conditions, and the triple $(3, 4, 5)$ gives rise to Aladdin's code, which is the unique optimum, with minimum determinant $\frac{1}{2\sqrt{5}}$. The same is done over $\mathbb{Z}[j]$, with minimum determinant $\frac{1}{2\sqrt{7}}$.

What next?

- Comparison with so-called cyclotomic codes.
- More simulations, e.g. in combination with LDPC codes.
- Algorithmic aspects (e.g. for the ML decoding stage).
- Higher-dimensional constructions.

Summary

- We reformulated and showed how to combine the Genie conditions and the rank criterion in an amenable way.
- The 2-dimensional case is completely solved: Over $\mathbb{Z}[i]$, perfect 2×2 STBC satisfying the Genie conditions can be easily constructed from Pythagorean triples satisfying some congruence conditions, and the triple $(3, 4, 5)$ gives rise to Aladdin's code, which is the unique optimum, with minimum determinant $\frac{1}{2\sqrt{5}}$. The same is done over $\mathbb{Z}[j]$, with minimum determinant $\frac{1}{2\sqrt{7}}$.

What next?

- Comparison with so-called cyclotomic codes.
- More simulations, e.g. in combination with LDPC codes.
- Algorithmic aspects (e.g. for the ML decoding stage).
- Higher-dimensional constructions.