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 \( \rightarrow \) (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 (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 \( \rightarrow \) (in dim 2) the Golden code, constructed by carefully choosing a lattice in the generalized quaternion algebra \( \left( \frac{i,5}{Q(i)} \right) \).
- 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 → (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 \( \rightarrow \) (in dim 2) the Golden code, constructed by carefully choosing a lattice in the generalized quaternion algebra \( \left( \frac{i, 5}{Q(i)} \right) \).
- Minimize error probability under **iterative decoding** thanks to the Genie conditions of Boutros-Gresset-Brunel (2003).
**Channel model**

\[ Y = HX + N \]

where \( H \) is \( n_r \times n_t \), \( X \) is \( n_t \times T \), and \( Y \) and \( N \) are \( n_r \times T \).

We will suppose \( n_r = n_t = n \).

**Linear space-time block code**

\[ X_c = c_1 M_1 + \cdots + c_k M_k \]

where \( M_1, \ldots, M_k \) are the generating codewords, the code has dimension \( k \leq nT \), and \( c = (c_1, \ldots, c_k) \) 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 $\gamma$, the pairwise error probability is upper bounded as

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

where: $t = \text{rk}(X - X') \leq \min(n, T)$, the $\lambda_i$ are the non-zero eigenvalues of $(X - X')(X - X')^*$, 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 $\gamma$, the pairwise error probability is upper bounded as

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

where: $t = \text{rk}(X - X') \leq \min(n, T)$, the $\lambda_i$ are the non-zero eigenvalues of $(X - X')(X - X')^*$, 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

\[ D^2 = \|HX_c - HX_{c'}\|^2 = \|HX_{c-c'}\|^2, \]

where \( c - c' = (0 \ldots 0 \Delta 0 \ldots 0) \) (say \( \Delta \) in \( j \)-th position), so that

\[ D^2 = |\Delta|^2 \|HM_j\|^2. \]

How to optimize distribution for \( D^2 \)?

When \( H \) has complex gaussian entries, properties of \( \chi^2 \) distributions show error probability is minimal when the \( M_j \) 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

\[ D^2 = \|H \mathbf{x}_c - H \mathbf{x}_{c'} \|^2 = \|H \mathbf{x}_{c-c'} \|^2, \]

where \( \mathbf{c} - \mathbf{c'} = (0 \ldots 0 \Delta 0 \ldots 0) \) (say \( \Delta \) in \( j \)-th position), so that

\[ D^2 = |\Delta|^2 \|HM_j\|^2. \]

How to optimize distribution for \( D^2 \)?

When \( H \) has complex gaussian entries, properties of \( \chi^2 \) distributions show error probability is minimal when the \( M_j \) 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

<table>
<thead>
<tr>
<th>Find $n \times n$ complex matrices $M_1, \ldots, M_{n^2}$ such that:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• they lie in $U(n)$, the unitary group – Genie condition (G)</td>
</tr>
<tr>
<td>• they form an orthogonal basis of $M_n(\mathbb{C})$ – shaping condition (S)</td>
</tr>
<tr>
<td>• the code they generate has minimal determinant as big as possible.</td>
</tr>
</tbody>
</table>

Remark: problem remains unchanged if replace each $M_j$ with $UM_jV$ for some $U, V \in U(n)$. 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 $M_1, \ldots, M_{n^2}$ such that:

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

Remark: problem remains unchanged if replace each $M_j$ with $UM_jV$ for some $U, V \in U(n)$. This defines an equivalence relation.
In the $2 \times 2$ MIMO case, diagonalization theorem for unitary matrices gives:

**Theorem 1**

Any $M_1, \ldots, M_4$ in $M_2(\mathbb{C})$ satisfying (G) and (S) are equivalent to some

$$
\begin{align*}
M_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & M_2 &= \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix} & M_3 &= \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix} & M_4 &= \begin{pmatrix} 0 & \gamma \\ -\gamma & 0 \end{pmatrix}
\end{align*}
$$

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

For $M_1, \ldots, M_4$ as in the above Theorem and for $c \in A^4$, one has

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

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

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

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 $z = (z_1, z_2, z_3, z_4) \in \mathbb{C}^4$, define

$$q_{u,v,w}(z) = z_2^2 - uz_2^2 - vz_3^2 + wz_4^2$$

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

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

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

**Corollary 1**

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

$$\frac{1}{2} \max q_{\min}(\mathcal{A}).$$
From this Corollary: A perfect $2 \times 2$ space-time code satisfying the Genie conditions exists if and only if $\max q \min(\mathcal{A}) > 0$. 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

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

where

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

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 $2 \times 2$ space-time code satisfying the Genie conditions exists if and only if $\max q_{\text{min}}(\mathcal{A}) > 0$. 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

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

where

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

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 $2 \times 2$ space-time code satisfying the Genie conditions exists if and only if $\max q_{\min}(\mathcal{A}) > 0$. 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

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

where

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

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!
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 $(\frac{u,v}{K})$, 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 $q_{u,v,w}(c) \in \frac{1}{d}\mathcal{A}$ for $c \in \mathcal{A}^4$.

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

$$|q_{u,v,w}(c)| \geq \frac{1}{|d|}.$$
... or: *Where algebraic number theory enters the scene*

**Strategy**

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

- $|u| = |v| = 1$
- the quaternion algebra $(\frac{u,v}{K})$ 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 $K$. 

Joseph J. Boutros and Hugues Randriam

ISIT'2009 - Seoul

July 2009 10 / 19
Lemma 1

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

Lemma 2

The units in $A$ that are not squares in $K$ are $\{\pm i\}$ for $A = \mathbb{Z}[i]$ and $\{-1, -j, -j^2\}$ for $A = \mathbb{Z}[j]$.

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 $v = x_p/x_p$ 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 $p \equiv 5 \mod 8$ for $A = \mathbb{Z}[i]$, or $p \equiv 7 \mod 12$ for $A = \mathbb{Z}[j]$. 
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 $u = i$, $v = x_r/x_r = x_r^2/r$, and $w = uv$, the quadratic form is

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

and the code can be constructed by putting in Theorem 1:

$$\alpha = \sqrt{u} = e^{i\pi/4}, \quad \beta = \sqrt{v} = x_r/\sqrt{r}, \quad \text{and} \quad \gamma = \sqrt{w} = \alpha\beta.$$ 

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

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

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

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

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 $\equiv 5 \mod 8$, then $q_{u,v,w}$ does not represent zero and has absolute value always at least

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

The corresponding Pythagorean code has minimum determinant at least

$$\frac{1}{2\sqrt{p}}.$$
Upper bound on the minimal determinant

So far we get:

1. \( \mathcal{A} = \mathbb{Z}[i], \ u = i, \ p = 5 \quad \rightarrow \quad \max q_{\min}(\mathbb{Z}[i]) \geq \frac{1}{\sqrt{5}} \)
2. \( \mathcal{A} = \mathbb{Z}[j], \ u = -1, \ p = 7 \quad \rightarrow \quad \max q_{\min}(\mathbb{Z}[j]) \geq \frac{1}{\sqrt{7}}. \)

What is the optimal value?

On the opposite direction,

\[ \max q_{\min}(\mathcal{A}) \leq \max q_{\min}(\mathcal{B}) \]

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

\[ \max q_{\min}(\mathcal{B}) = \sup_{|u|=|v|=|w|=1} \left( \inf_{c \in \mathcal{B} \setminus\{0\}} |q_{u,v,w}(c)| \right) \]

can be computed analytically exactly (piecewise smooth function over a smooth compact set!).
Upper bound on the minimal determinant

So far we get:

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

What is the optimal value?

On the opposite direction,

$$\maxqmin(A) \leq \maxqmin(B)$$

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

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

can be computed analytically exactly (piecewise smooth function over a smooth compact set!).
By choosing a convenient $B$ (e.g. $B = 16$-QAM in case $A = \mathbb{Z}[i]$), one shows equality:

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

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.
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

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

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:

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

and get as precoder matrix (in linearized form):

$$S_{\text{Aladdin}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ \alpha & 0 & 0 & -\alpha \\ 0 & \beta & \beta & 0 \\ 0 & \gamma & -\gamma & 0 \end{pmatrix}$$
All in all:

**Theorem 2**

Aladdin’s code is a perfect $2 \times 2$ 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 $2 \times 2$ 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)

256-QAM, 2x2 MIMO, tcoh=2, Probabilistic Decoding with Genie

Symbol Error Rate vs. $E_b/N_0$ (dB) for different precoders:
- No Precoding - 256QAM
- Cyclotomic - 256QAM
- Golden Code - 256QAM
- Dayal Varanasi - 256QAM
- Tilted QAM - 256QAM
- Aladdin Pythagoras - 256QAM

$1/SNR^2$, $1/SNR^4$
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 $2 \times 2$ 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 $2 \times 2$ 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.