Fuchsian Codes

Dionís Remón

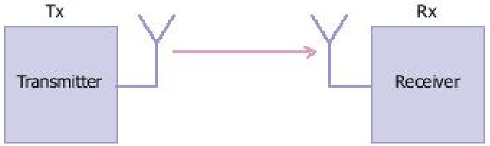
Universitat de Barcelona

18 April 2013

joint work with
Ivan Blanco-Chacón and Camilla Hollanti
(Aalto University, Finland)

Basics on coding theory

One transmit antenna (Tx)
One receive antenna (Rx)
This situation corresponds to SISO channels.



Picture. Single Input Single Output (SISO)
One antenna at both the transmitter and the receiver.

We can transmit complex numbers $\mathbb{C}$. The subset of elements of $\mathbb{C}$ which we can transmit is named codebook, and we will denote it C. The elements of C are named codewords. The codebook C is a finite set.

Let $x = a + bi \in C$. We define the energy of x by $E_x := |x|^2 = a^2 + b^2$. The average energy of the codebook (or just the energy of the codebook) is defined by $E_C = \frac{1}{|C|} \sum_{k=1}^{|C|} E_{x_k}$ with $\{x_k\}_{k=1}^{|C|} = C$.

Definition

The *signal to noise ratio* (SNR) attached to C is defined by

$$SNR = \frac{E_C}{\sigma_0^2},$$

where E_C is the average energy of the codebook and the σ_0^2 is the variance of the noise of the channel.

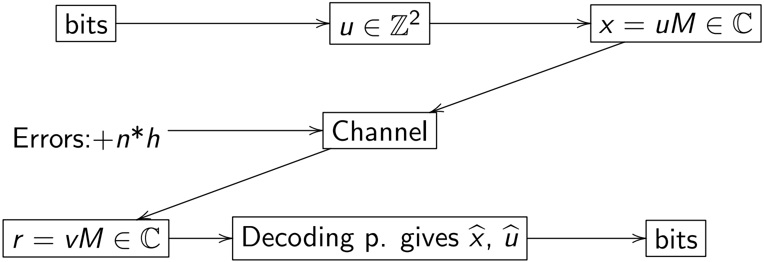
1. Classical transmission system model

- With a bit mapper we obtain vectors u in a lattice $\Lambda \subset \mathbb{R}^2$.
- A matrix M attached to the lattice gives us elements $x \in C \subseteq \mathbb{C}$ by doing $x = uM = (x_1, x_2)$, and $x = x_1 + ix_2$.
- We receive $r = hx + n$, where $h, n \in \mathbb{C}$ are random numbers. We use a matrix lattice detection to recover x.
- We obtain the initial information in bits by using a bit demapper.

Random variables

The number n is distributed as $\mathbb{C}N(0, \sigma_0^2/2)$. We can write $h = \rho e^{i\theta}$ where ρ is Rayleigh distributed and θ is uniform distributed in $[0, 2\pi]$.

Classical diagram



$r = r(u, t)$

The complexity of the algorithm is linear in the size of the codebook.

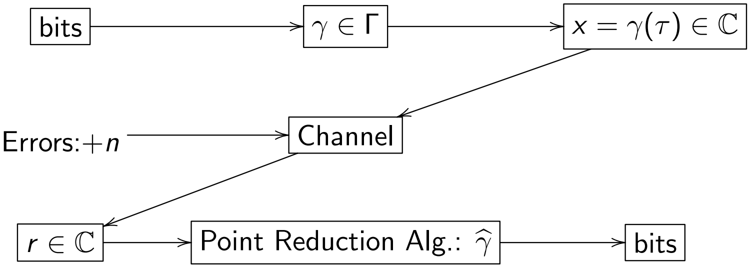
2. Fuchsian transmission system model

- With a bit mapper (for instance, we can use the map ϕ which will be explained in the generating constellation section) we obtain an element γ in a Fuchsian group Γ.
- We choose a suitable τ in $\mathcal{H}$ and we obtain an element $x \in C \subseteq \mathbb{C}$ by doing $x = \gamma(\tau)$. We send x.
- We receive $r = x + n$ (AWGN), where n is a random number. We use the reduction point algorithm to recover $\widehat{\gamma}$.
- We obtain the information in bits by using a bit demapper.

Random variables (2): Why is AWGN channel realistic?

Generally speaking it is not true. But, there are some situations where we can suppose that h is negligible. Also, we consider this work as a first approximation to the general problem.

Fuchsian diagram



$r = r(\gamma, t)$, where τ is the center of the code.

The complexity of the algorithm is logarithmic in the size of the codebook.

Fuchsian groups

Let us consider $\mathbf{SL}(2,\mathbb{R})$, the group of real matrices

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with determinant $\det(g) = ad - bc = 1$.

Fractional linear transformations of $\mathbb{C}$

The group $\mathbf{SL}(2,\mathbb{R})$ acts on $\mathcal{H}$ via $\mathbf{PSL}(2,\mathbb{R})$

$$z \mapsto g(z) := \frac{az+b}{cz+d}, \ g \in \mathbf{SL}(2,\mathbb{R}), z \in \mathcal{H}.$$

The product of two transformations corresponds to the product of their matrices.

Definition

A *Fuchsian group* Γ is a discrete subgroup of $\mathbf{PSL}(2, \mathbb{R})$.

Example

Let us consider the group which consists of all transformations

$$z \mapsto \frac{az+b}{cz+d},\ z \in \mathcal{H},$$

with $a, b, c, d \in \mathbb{Z}$, and $ad - bc = 1$. It is a Fuchsian group, called the modular group, and it is denoted by $\mathbf{PSL}(2, \mathbb{Z})$.

Definition

A closed region $\mathcal{F} \subset \mathcal{H}$ which is a clousure of a non-empty open set $\mathring{\mathcal{F}}$, called the interior of $\mathcal{F}$, is said to be a *fundamental region* for Γ if

1. $\bigcup_{g\in\Gamma} g(\mathcal{F}) = \mathcal{H}$,
2. $\mathring{\mathcal{F}} \cap g(\mathring{\mathcal{F}}) = \emptyset$ for all $g \in \Gamma \setminus \{\mathrm{Id}\}$.

Observe that the fundamental domain of a Fuchsian group Γ is not unique.

Fundamental domains

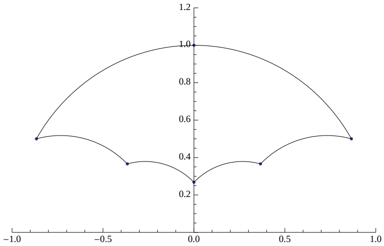


Figure: $\Gamma(6,1)$: cocompact

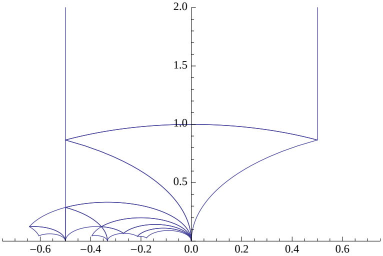


Figure: $\Gamma(1,6)$: no - cocompact

We are interested in cocompact Fuchsian groups.

Reduction point algorithm

Definition

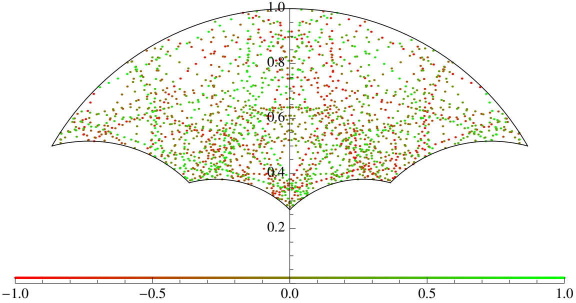
Given a pair $(\Gamma, \mathcal{F}(\Gamma))$ and a point $z_0 \in \mathcal{H}$, the *reduction point algorithm problem* asks for an explicit transformation $\gamma \in \Gamma$ such that $\gamma(z_0) \in \mathcal{F}(\Gamma)$.

We have a fixed pair $(\Gamma, \mathcal{F}(\Gamma))$. We assume that we know a set of generators of the group Γ, i. e., $\langle g_i \rangle_{i=1}^{\lambda} = \Gamma$. We have also a point $z_0 \in \mathcal{H}$ we want to put in the fundamental domain (of course if $z_0 \in \mathcal{F}$ we are done).

Existence and complexity of reduction point algorithms

Theorem

Given a cocompact Fuchsian group Γ, and a codebook C of size n, there exists a reduction point decoding algorithm whose complexity is $\mathrm{O}(\log(n))$.



Generating a $\Gamma(6,1)$ constellation

We assume we are in an algebra whose its normic equation is $x^2 - 3y^2 + z^2 - 3t^2 = 1$ and the group is $\Gamma(6,1)$.
The elements $\gamma \in \Gamma$ can be seen as elements $(x, y, z, t) \in \mathbb{Z}^4$ such that

$$x^2 - 3y^2 + z^2 - t^2 + xt - 3yt + zt = 1.$$

Let ε be the fundamental unit of $\mathbb{Q}(\sqrt{3})$. Given (n, k_1, k_2) a triple of non-negative integers, define $a_n + \sqrt{3}b_n = \varepsilon^n$. We have $a_n^2 - 3b^2 = (\varepsilon^n)(\varepsilon')^n = 1$. Now, set $x_{n,k_1} + \sqrt{3}y_{n,k_1} := a_n\varepsilon^{k_1}$ and $z_{n,k_1} + \sqrt{3}t_{n,k_1} := \sqrt{3}\varepsilon^{k_2}$. Notice that $x_{n,k_1}^2 + 3y_{n,k_1}^2 = a_n^2$ i $z_{n,k_2}^2 + 3t_{n,k_2}^2 = -3b_n^2$, hence, the 4-tuple $(x_{n,k_1}, y_{n,k_1}, z_{n,k_2}, t_{n,k_2})$ satisfies

$$x_{n,k_1}^2 - 3y_{n,k_1}^2 + z_{n,k_2}^2 - 3t_{n,k_2}^2 = a_n^2 - 3b_n^2 = 1.$$

We will denote by $\phi(n, k_1, k_2)$ the so constructed 4-tuple. In this way we have parametrized by three variables an infinite subset of points of the hyperquadric $x^2 - 3y^2 + z^2 - 3t^2 = 1$.

Proposition

The map ϕ is bijective over its image, which is contained in the set $\{(x, y, z, t) \in \mathbb{Z}_{\geq 0} : x^2 - 3y^2 = n^2, z^2 - 3t^2 = -3m^2$, for some $n, m \in \mathbb{Z}\}$.

$\phi(1,0,1) = (2,0,3,2)$	$\phi(0,1,1) = (2,1,0,0)$
$\phi(2,0,1) = (7,0,12,8)$	$\phi(2,1,1) = (14,7,12,8)$

Alphabet

Our alphabet consists of a finite constellation of 4-tuples of integers $C = \{(x_i, y_i, z_i, t_i)\}_{i=1}^{|C|}$ where $|C| < \infty$ is its size. These 4-tuples satisfy that if $(x, y, z, t) \in C$ then

$$x^2 - ay^2 - cz^2 + abt^2 = 1,$$

for fixed $a, b \in \mathbb{Z}$. Geometrically, this means that our alphabet is contained in a 4-dimensional hyperquadric.

Given $\tau \in \mathcal{F}$, we will send a 4-tuple as the complex signal $\gamma(\tau)$ where

$$\gamma = \begin{bmatrix} x+\sqrt{a}y & z+\sqrt{a}t \\ b(z-\sqrt{a}t) & x-\sqrt{a}y \end{bmatrix}.$$

We obtain an embedding

$$\begin{array}{llll} F: & \text{Alphabet} & \to & \mathbb{C} \\ & (x,y,z,t) & \to & \gamma(\tau), \gamma \in \Gamma \end{array}$$

The set $\mathrm{Im} F$ will correspond to the chosen codebook C. Let $n = |C|$. We will refer to the set C of codewords obtained in this way as nonuniform Fuchsian constellation (n-NUF).

$\Gamma_{g=1,e=2}$ - Constellation

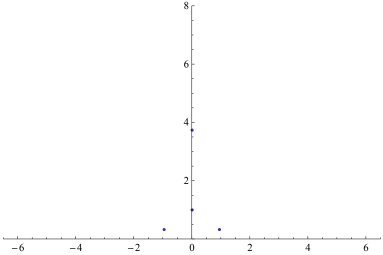


Figure: Points

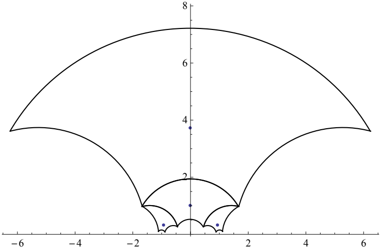


Figure: Hit - Regions

$\Gamma(6,1)$ - Constellation

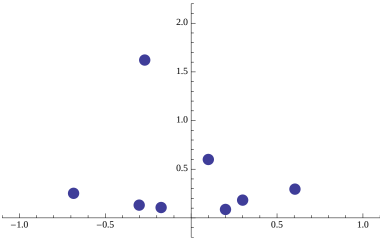


Figure: Points

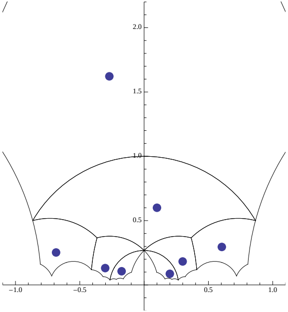


Figure: Hit - Regions

Duplicating the size

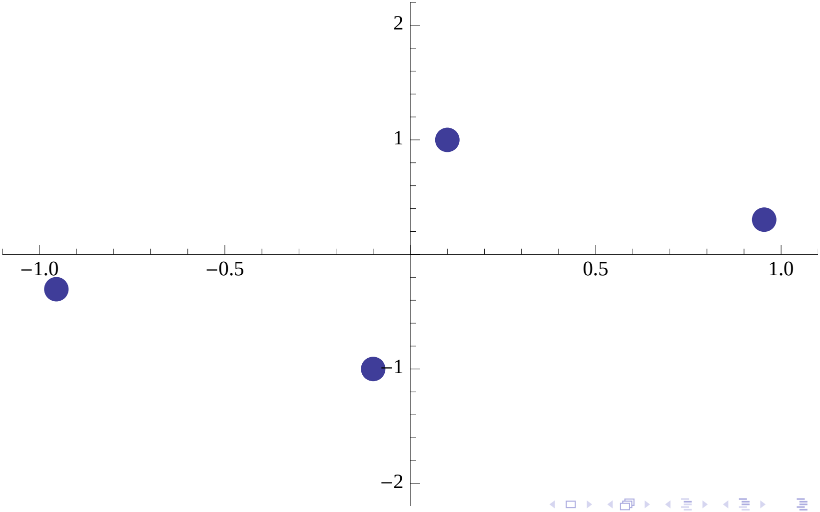
In order to obtain one 4-NUF symbols we need 4 matrices of the chosen Fuchsian group Γ. Remember that Fuchsian groups act on the upper half-plane.

Duplicating the size

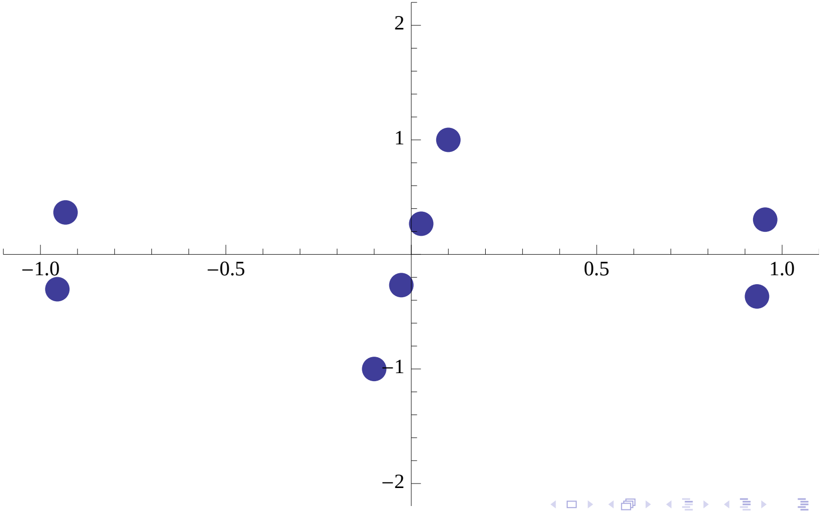
In order to obtain one 4-NUF symbols we need 4 matrices of the chosen Fuchsian group Γ. Remember that Fuchsian groups act on the upper half-plane.

Once we have a choice of matrices of $\Gamma(D, N)$ and τ having the codebook $C = \{\gamma_k(\tau)\}_{k=1}^n$, we can consider the new codebook $C = \{\pm\gamma_k(\tau)\}_{k=1}^n$. That is we can define an action over the bottom-half plane.

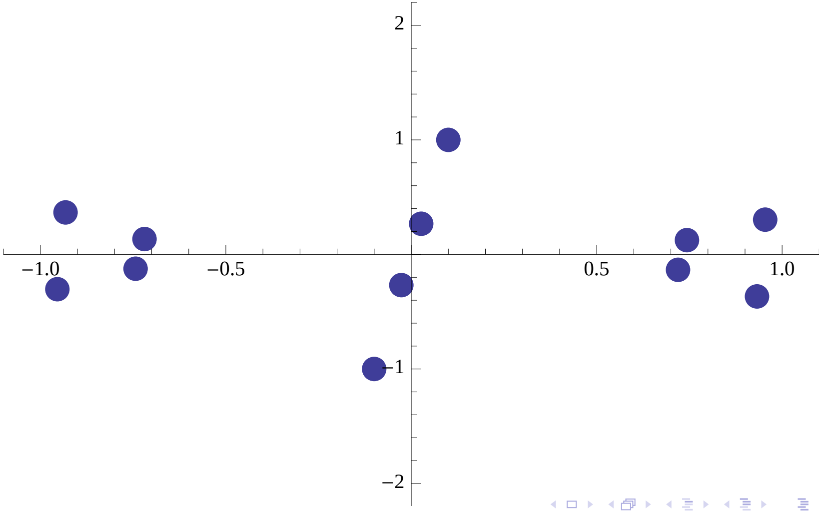
4 — $\Gamma_{g=1,e=2}$ - Constellation



8-$\Gamma_{g=1,e=2}$ - Constellation



$16 - \Gamma_{g=1,e=2}$ - Constellation



$\Gamma_{g=1,e=2}$ - Constellation

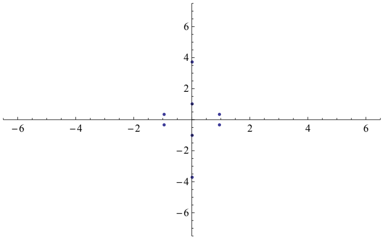


Figure: Points

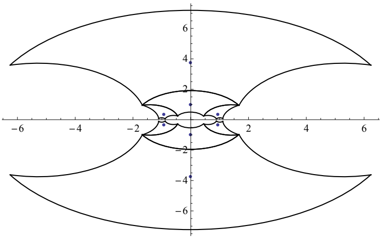
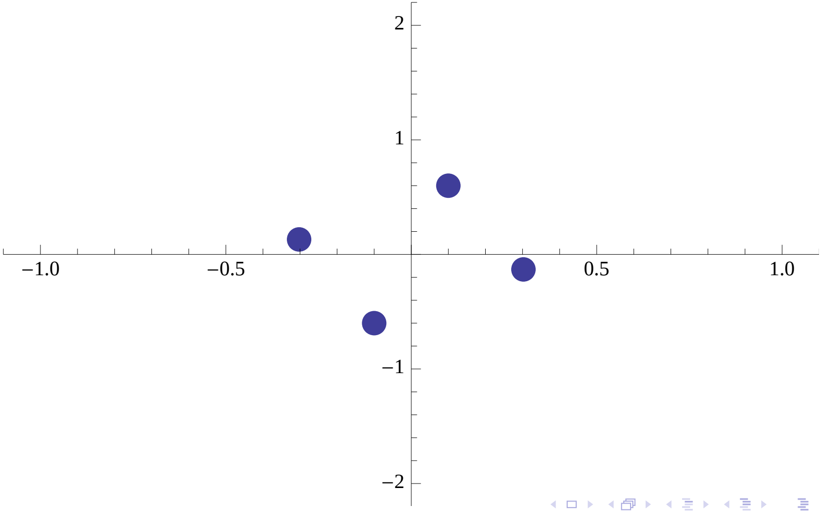
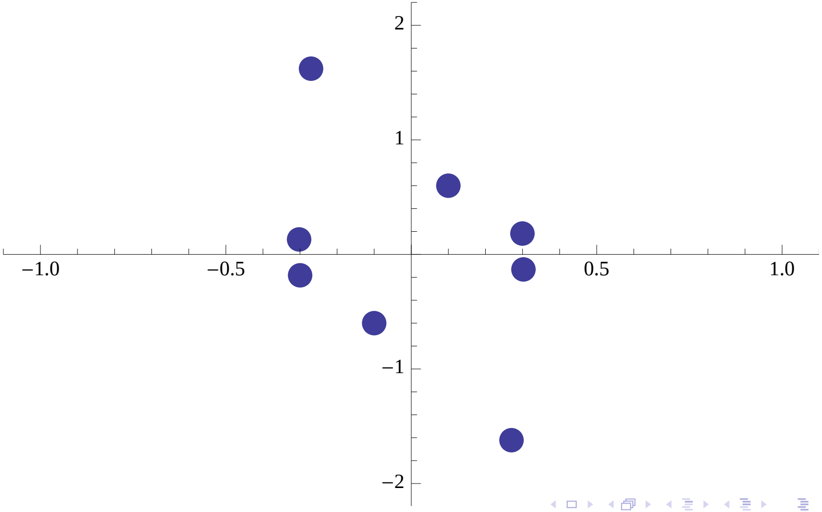


Figure: Hit - Regions

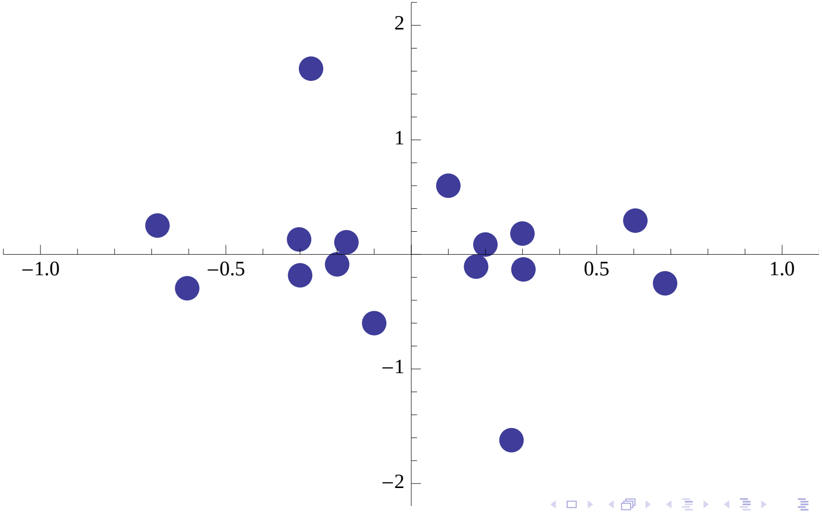
4 — $\Gamma(6,1)$ - Constellation



$8 - \Gamma(6,1)$ - Constellation



$16 - \Gamma(6,1)$ - Constellation



$\Gamma(6,1)$ - Constellation

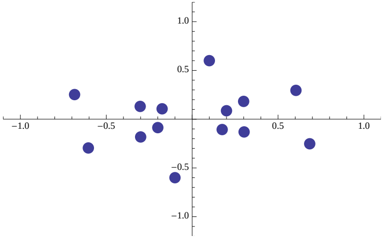


Figure: Points

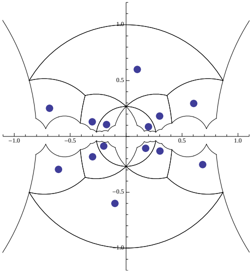


Figure: Hit - Regions

Further research

We have seen that the simulations depend on the group of a co-compact Fuchsian group and $\Gamma = \Gamma(D, N)$ and the point τ we are considering. Also we have seen simulations with different code size.

- How different the performance is if we change the point τ?
- We consider groups of type $\Gamma(D, N)$. How different are the performance of the code if we vary the parameters D and N and the constellations?
- We will compare the performance complexity for different code sizes $|C|$.

Parameter τ: Testing diferents centers

Tests with 16-NUF symbols for $\Gamma(6,1)$.

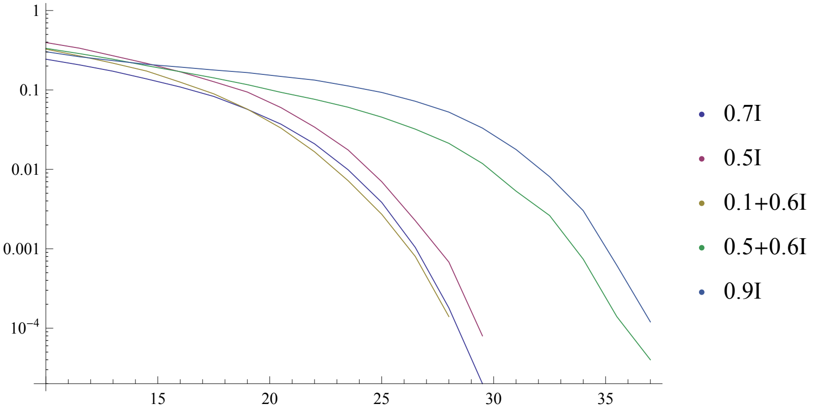


Figure: Testing different values of τ

Parameter D and N: Testing Fuchsian Codes

Tests with 4 symbols: 4-QAM, 4-NUF for $\Gamma_{g=1,e=2}$, $\Gamma(6,1)$, $\Gamma(10,1)$ and $\Gamma(15,1)$.

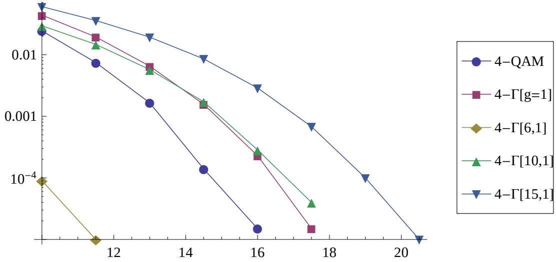


Figure: Testing with different Fuchsian groups

Parameter D and N: Testing Fuchsian Codess

Tests with 8 symbols: 8-QAM, 8-NUF for $\Gamma_{g=1,e=2}$, $\Gamma(6,1)$, $\Gamma(10,1)$ and $\Gamma(15,1)$.

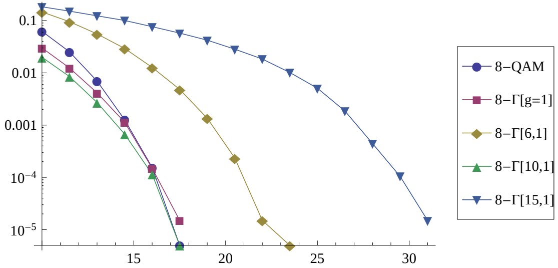


Figure: Testing with different groups

Towards the fading channel

Our scheme is valid only for AWGN channels, that is,

$$r = \gamma_k(\tau) + n.$$

However the common situation is the fading channel,

$$r = h\gamma_k(\tau) + n,$$

where h is a random variable $\mathbb{C}N(0,1)$, i. e.,

$$h = re^{i\theta},$$

r is Rayleight distributed and θ is uniformly distributed in $[0, 2\pi]$.

Our goal will be to find Fuchsian groups which are immune to channels with fading.

Thank you!

Takk!

Gràcies!

WCC 2013