FUCHSIAN CODES: A NON-LINEAR PROPOSAL FOR THE PHYSICAL LAYER

M. Alsina (Polytechnic University of Catalonia), I. Blanco-Chacón (Aalto University), C. Hollanti (Aalto University), D. Remón (University of Barcelona)

BACKGROUND

CHANNELS, SIGNALS AND MODULATION

Wireless channels can distort sent messages. two lines of approach:

- Low level (physical layer): physical/wave level. We focus on this.
- Logical level: digital signal level (classical Error Correcting Codes).

There are two sources of noise:

- Fading: Superposition, reflection, Doppler effect, obstacles. Independent sequence of Gaussian random variables $h = CN(0,1)$.
- Additive White Gaussian Noise (AWGN): At the receiver side. Independent (*white*) sequence of Gaussian random variables $n = CN(0,\sigma)$.

We assume that the receiver knows h (sending pilots). Signal coding is used to tackle the noise. Coding means redundancy (diversity). We transmit simultaneously by several antennas, and transmit versions of the signal several times (space-time block codes).

Digital information is sent by modulating a baseband signal. Used modulation schemes: PAM (phase/amplitude modulation) and QAM (quadrature/amplitude modulation). A QAM alphabet is a symmetric subset of $\mathbb{Z}[i]^2$. Early designs of CODEC transmission used non-uniform alphabets, as we will do.

SOME INFORMATION THEORY

Definition

For a code $C = \{c_i\}_{i=1}^N$, the signal-to-noise ratio is $SNR = 10\log_{10}(E/\sigma^2)$, where E is the average energy of the code (i.e. $E = 1/N\sum_{i=1}^{N}|c_i|^2$). Denote by BEP the bit error probability of decoding.

Definition

Data rate: $R_C = k/n$, k is the number of independent information items per codeword and n is the number of channel uses.

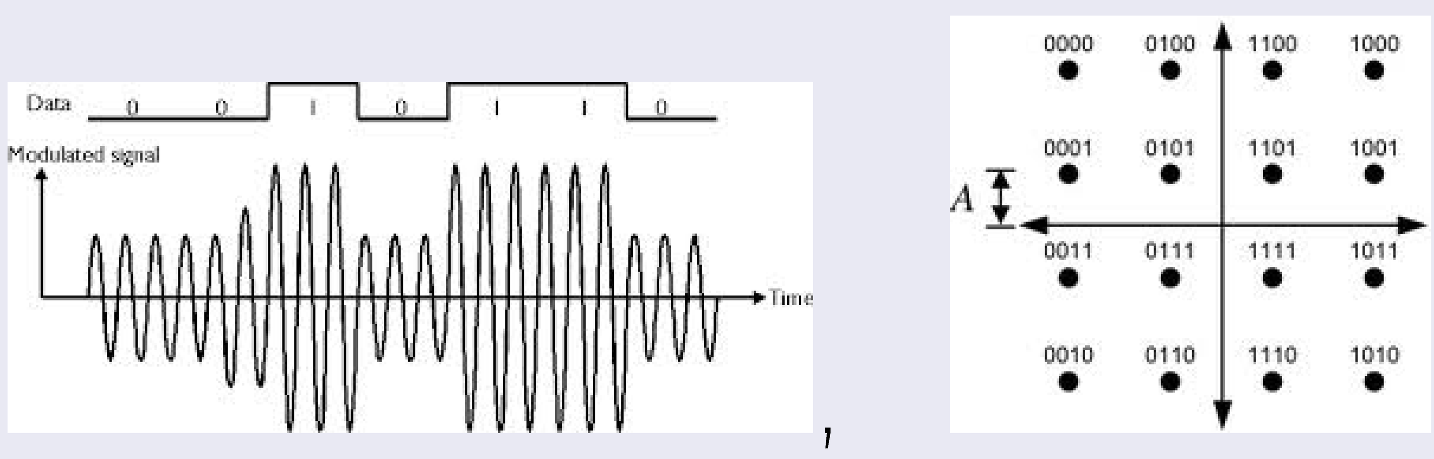

Figure : left: QAM modulation, right: QAM alphabet and digital information

ALGEBRAIC CODES

Lattices from rings of integers of algebraic number fields/cyclic division algebras are used for coding. Decoding is by Maximum-Likelihood. Arithmetic properties translate into diversity properties.

- Golden code (IEEE802.16): Attached to $\mathbb{Z}\left[i, \frac{1+\sqrt{5}}{2}\right]$, rate 2, complexity $O(2|C|^{0.625})$.
- Alamouti Code (3GPP, OMA): Attached to Hamilton $\mathbb{Q}$-quaternions, rate 1, complexity $O(|C|^{0.5})$.

Example: $\mathbb{Q}(\theta)/\mathbb{Q}$ normal extension of degree n. If $\oplus_{i=0}^{n}\theta^i\mathbb{Z}$ is the ring of integers, we can use this lattice to encode. The skewer the fundamental parallelogram, the harder to decode but the better the noise tolerance.

OUR APPROACH ([2])

Set $\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. The group $\mathrm{SL}(2,\mathbb{R})$ acts on $\mathcal{H}$ by Möbius transformations.

RATE 3 CODES

Our codes are $C = \{c_i = \gamma_i(\tau)\}_{i=1}^n$ where $\tau \in \mathcal{H}$,

$$\gamma_i = \begin{pmatrix} x_i + \sqrt{a}y_i & z_i + \sqrt{a}t_i \\ b(z_i - \sqrt{a}t_i) & x_i - \sqrt{a}y_i \end{pmatrix},$$

with $a > 0$, $b < 0$ integers and $(x_i, y_i, z_i, t_i) \in \mathbb{Z}^4$ with $x_i - ay_i - bz_i + abt^2 = 1$. For each codeword, only 3 symbols are independent. If we use 1 channel to transmit $\gamma_i(\tau)$, $R_C = 3$. How to produce the 4-tuples? Nested use of the Pell's equation in $\mathbb{Z}[\sqrt{a}]$.

Our matrices belong to **arithmetic Fuchsian group** (see next section). The decoding complexity for linear codes is typically $O(|C|^{0.5})$. Our method uses a point reduction algorithm ([1]) and the complexity is $O(\log(|C|))$. Fixed a fundamental region $\mathcal{F}$ for the group and τ in the interior of $\mathcal{F}$ from now on.

- Send (x, y, z, t) encoded as $\gamma(\tau)$ (γ as above). $\gamma(\tau) \in \gamma(\mathcal{F})$. The receiver obtains $\gamma(\tau) + n$, n an AWGN.
- If Γ and τ are chosen in a suitable way, $\gamma(\tau) + n \in \gamma(\mathcal{F})$ with high probability. Decode $\gamma(\tau) + n$ by point reduction to obtain γ.

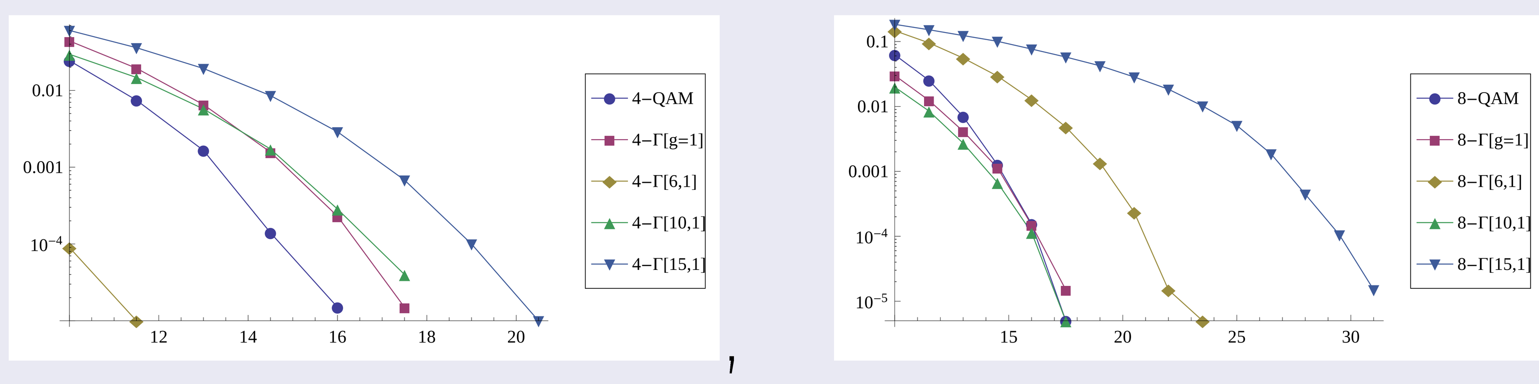

Figure : left: performance of 4-codes, right: performance of 8-codes

ARBITRARY RATE CODES

Let $K/\mathbb{Q}$ be a totally real number field of degree n and $\mathcal{O}_K$ its ring of integers. Take $a, b \in \mathcal{O}_K \setminus \{0\}$, with a totally positive and b totally negative (see next section). Our code is $C = \{\gamma_i(\tau)\}_{i=1}^n$ where $\gamma_i = \begin{pmatrix} x_i + \sqrt{a}y_i & z_i + \sqrt{a}t_i \\ b(z_i - \sqrt{a}t_i) & x_i - \sqrt{a}y_i \end{pmatrix}$, with $(x_i, y_i, z_i, t_i) \in \mathcal{O}_K^4$ satisfying $x_i - ay_i - bz_i + abt^2 = 1$.

Theorem (Alsina, B., Hollanti, Remón)

The so-constructed code has data rate $3n$ *(for one channel use).*

THE TECHNICAL CORE

Definition

Let $K/\mathbb{Q}$ be a number field. Given $a, b \in \mathcal{O}_K \setminus \{0\}$, the quaternion K-algebra $\left(\frac{a,b}{K}\right)$ is a ring of the form $A = K \oplus Ki \oplus Kj \oplus Kij$ with $i^2 = a$, $b^2 = b$, $ij = -ji$. An order in A is an $\mathcal{O}_K$-lattice of maximal rank such that it is also a ring. The reduced norm of a quaternion $x + yi + zj + tij$ is defined as $x^2 - ay^2 - bz^2 + abt^2$.

If $\mathcal{O} \subseteq A$ is a maximal order, denote by $\mathcal{O}_1^*$ its multiplicative subgroup of elements of reduced norm 1, and by $\Gamma(\mathcal{O}_1^*)$ the matrix image of this group.

Definition

An arithmetic Fuchsian group Γ is a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$ such that there exists some $\Gamma(\mathcal{O}_1^*)$ with $[\Gamma \cap \Gamma(\mathcal{O}_1^*) : \Gamma] < \infty$ and $[\Gamma \cap \Gamma(\mathcal{O}_1^*) : \Gamma(\mathcal{O}_1^*)] < \infty$.

APPLICATIONS

Our codes present arbitrary rates and logarithmic complexity. They can be regarded as information-compressing codes since we can transmit several symbols by one channel use. Our simulations for rate 3 codes show that some of our codes outperform *QAM* for size 4 and 8. Higher size constellations behave worse, and a correction mechanism is under research. For high SNR and small code size (for the moment), our codes are a good alternative for linear codes.

Bayer, P. Remón, D.: A reduction pont algorithm for cocompact Fuchsian groups (submitted).

Blanco-Chacón, I.; Hollanti, C.; Remón, D.: Fuchsian codes for AWGN channels. Proceedings of The International Workshop on Coding and Cryptography, WCC 2013. p. 496–507. Bergen (2013).