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 \( \mathbb{Z}^2 \). 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 \( \text{SNR} = 10 \log_{10} (E/\sigma^2) \), 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 \( n \) 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 \( \left[ \begin{array}{c} 1 \\ i/\sqrt{2} \end{array} \right] \), rate 2, complexity \( O(2^{|c|^2}) \).
• Al mouati Code (3GPP, OMA): Attached to Hamilton \( Q \)-quaternions, rate 1, complexity \( O(2^{|c|^2}) \).

Example: \( Q(\theta)/Q \) normal extension of degree \( n \). If \( \alpha, \beta \in \mathbb{Z} \) 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.

ARBITRARY RATE CODES

Let \( K/Q \) 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 \( C = \{ \gamma(c) \}_{c \in \mathcal{O}_K} \), where \( \gamma = \left( \begin{array}{cc} x & \sqrt{n}y \\ z & \sqrt{n}t \end{array} \right) \in \mathbb{Z}^2 \) for the group \( \Gamma_3 \) of the group \( \mathbb{Z}^2 \).

An arithmetic Fuchsian group (see next section). The decoding complexity for linear codes is typically \( O(|\mathcal{O}|^{1.5}) \). Our method uses a point reduction algorithm \( ([1]) \) and the complexity is \( O(|\mathcal{O}|) \). Fixed a fundamental region \( \mathcal{F} \) for the group and \( \tau \) the interior of \( \mathcal{F} \) from now on.

If \( \Gamma \) and \( \tau \) are chosen in a suitable way, \( \gamma(\tau) + n \in \gamma(\mathcal{F}) \) with high probability. Decoding \( \gamma(\tau) + n \) by point reduction to obtain \( \gamma \).

THE TECHNICAL CORE

Definition
Let \( K/Q \) be a number field. Given \( a, b \in \mathcal{O}_K \setminus \{0\} \), the quaternion \( \mathbb{K} \)-algebra \( (\mathbb{K} \times \mathbb{K})/\mathbb{K} \) is a ring of the form \( A = K \otimes \mathbb{K}/K \otimes \mathbb{K} \) with \( i^2 = b^2 = a, j = -i \). An order in \( A \) is an \( \mathcal{O}_A \)-lattice of maximal rank such that it is also a ring. The reduced norm of a quaternion \( x + yi + zj + \theta k \) is defined as \( x^2 - y^2 - z^2 + ab\theta^2 \).

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

Definition
An arithmetic Fuchsian group \( \Gamma \) is a discrete subgroup of \( \text{SL}(2, \mathbb{R}) \) such that there exists some \( f(\mathcal{O}^\ast) \) with \( f(\mathcal{O}^\ast) \cap f(\mathcal{O}^\ast) = \{ \} \) and \( f(\mathcal{O}^\ast) \cap f(\mathcal{O}^\ast) < \{ \} \).

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 an error correction mechanism is under research. For high SNR and small code size (for the moment), our codes are a good alternative for linear codes.