Physical-layer Network Coding: Design of Constellations over Rings.

I. de Zarza i Cubero.

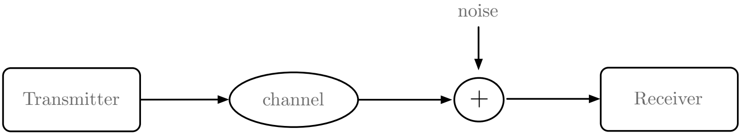
Cerdanyola del Vallès (Barcelona), 2013.

Outline

Outline

Introduction

Universitat Autònoma de Barcelona



Note

Intermediate nodes can be added. These nodes would originally have the only function of forwarding the received messages.

Outline

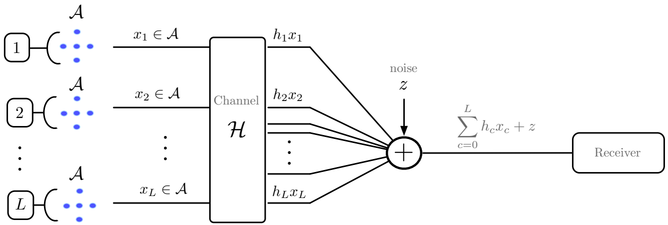
Universitat Autònoma de Barcelona

1 Introduction
- Physical-layer Network Coding
- The Role of a Signal Constellation in the System

Physical-layer Network Coding

Network Coding

Allows intermediate nodes to combine messages before forwarding them.



Physical-layer Network Coding

Exploits the network coding operation performed by nature.

Outline

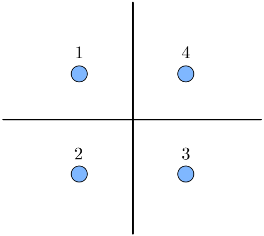
Universitat Autònoma de Barcelona

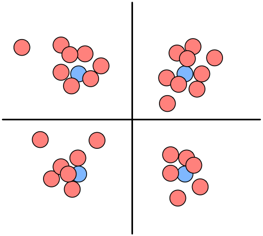
1 Introduction
- Physical-layer Network Coding
- The Role of a Signal Constellation in the System

The Role of a Signal Constellation

Definition

A signal constellation is a set of points in the complex plane used to describe all possible symbols used by a system to transmit data.





Points of transmission and reception.

Outline

Objective

Universitat Autònoma de Barcelona

General Objective

We tackle the design of new signal constellations for Physical-layer Network Coding. Towards this aim, the appropriate algebraic tools need to be identified.

Design Objective

We aim at defining a design methodology and propose the best performing constellations. Performance will depend on the algebraically induced geometry.

Outline

Outline

UAB Universitat Autònoma de Barcelona

Commutative Rings

We are going to design constellations carved from the rings $\mathbb{Z}[i]$ and $\mathbb{Z}[w]$.

$$\{\text{Commutative Rings}\} \supset \{\text{PIDs}\} \supset \{\text{Euclidean Domains}\} \supset \{\text{Fields}\}$$

We Are Looking For

R/aR field, R PID and aR ideal.

The Ring $\mathbb{Z}[i]$

Universitat Autònoma de Barcelona

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$$

Definition

For $\alpha = a + ib \in \mathbb{Z}[i]$, its norm is defined as

$$N(\alpha) = \alpha\alpha^* = (a + bi)(a - bi) = a^2 + b^2.$$

Theorem: Norm Is Multiplicative.

For α and β in $\mathbb{Z}[*]$, $N(\alpha\beta) = N(\alpha)N(\beta)$.

$$N(\alpha\beta) = (\alpha\beta)(\alpha\beta)^* = \alpha\beta\alpha^*\beta^* = (\alpha\alpha^*)(\beta\beta^*) = N(\alpha)N(\beta).$$

The Ring $\mathbb{Z}[i]$

Universitat Autònoma de Barcelona

Theorem of Division

For $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there are $\gamma, \rho \in \mathbb{Z}[i]$ such that

$$\alpha = \beta\gamma + \rho \text{ where } N(\rho) < N(\beta).$$

Proof.

- Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Then $\alpha/\beta \in \mathbb{C} \Rightarrow \alpha/\beta = u + iv$ with $u, v \in \mathbb{R}$.
  - $a \in \mathbb{Z}$ close to $u \Rightarrow |u - a| \leq 1/2$.
  - $b \in \mathbb{Z}$ close to $v \Rightarrow |v - b| \leq 1/2$.

  Set $\gamma = a + ib \in \mathbb{Z}[i]$. Set $\rho = \alpha - \gamma\beta \in \mathbb{Z}[i]$.
- Remains to prove $N(\rho) < N(\beta)$. (Note $\beta \neq 0 \Rightarrow N(\beta) \neq 0$).
  - $N(\rho) = N((\rho/\beta)\beta) = N(\rho/\beta)N(\beta)$:
  - $N(\rho) < N(\beta) \Leftrightarrow N(\rho/\beta) < 1$
  - $\rho/\beta = (\alpha - \gamma\beta)/\beta = \alpha/\beta - \gamma = (u + iv) - (a + ib) = (u - a) + i(v - b)$.
  - $N(\rho/\beta) = (u - a)^2 + (v - b)^2 \leq 1/4 + 1/4 = 1/2 < 1$.

  Therefore $\alpha = \gamma\beta + \rho$ with $N(\rho) < N(\beta)$.

$\square$

The Ring $\mathbb{Z}[i]$

$\mathbb{Z}[i]$ as a PID

Universitat Autònoma de Barcelona

Definition

An integral domain R is said to be an Euclidean domain if there is a function N from the set of non-zero elements of R to the set of non-negative integers such that

- (Theorem of Division) given $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that $a = bq + r$ where $N(r) < N(b)$, and
- for all non-zero elements a and b of R we have $N(a) \leq N(ab)$.

Theorem

Euclidean domains are PIDs.

Proof.

Let C be any non-zero ideal of the Euclidean domain R, and $d \in C$ be a non-zero element of minimum norm.
We claim $(d) = C$. Certainly, $(d) \subseteq C$.
Let $a \in C$. By the Theorem of Division, $a = qd + r$, with $r = 0$ or $N(r) < N(d)$. Since $a - qd = r \in C$, by minimality of $N(d)$ we see $r = 0$ and $a = qd \in (d)$. □

The Ring $\mathbb{Z}[w]$

Universitat Autònoma de Barcelona

$$\mathbb{Z}[w] = \{a + bw | a, b \in \mathbb{Z}\}$$

with w is a primitive cube root of 1:

$$w = e^{2\pi i/3} = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = \frac{1}{2}\left(-1 + i\sqrt{3}\right).$$

Definition

For $\alpha = a + wb \in \mathbb{Z}[w]$, its norm is defined as

$$N(\alpha) = \alpha\alpha^* = a^2 + b^2 - ab.$$

Outline

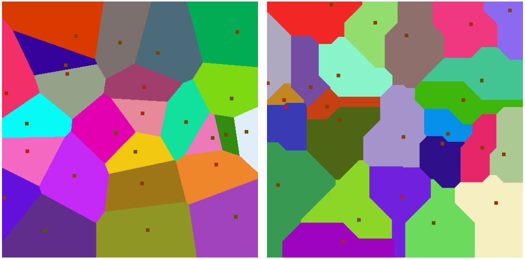
Universitat Autònoma de Barcelona

3 What Do We Need in Order to Design?
- Mathematical Theory
- Performance Metrics
  - Decision Regions
  - Probability of Error
- A Reference to Compare
- System Model
- Proposed Methodology

Decision Regions

Definition

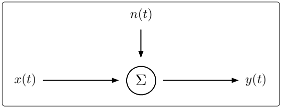
The decision region for a point x_c in the constellation $\mathcal{A} = \{x_c\}_{c=0,\cdots,M}$, denoted $\mathcal{R}_{x_c}$, is the set of points of the complex plane that are closer to x_c than to any other point of the signal constellation.



Probability of Error

Hypothesis

We assume an AWGN (Additive White Gaussian Noise) channel.



$$\equiv \quad y(t) = x(t) + n(t)$$

The noise $n(t)$ is a 1 dimensional random signal Gaussian with zero mean, variance σ^2 and probability distribution:

$$P_n(u) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2\sigma^2}u^2}.$$

Assumption

The computation of P_e assumes the inputs x_c equally likely: $p_x(c) = \frac{1}{M} \forall c$.

Probability of Error

Universitat Autònoma de Barcelona

ML Detector Is the Optimum Detector

Which has decision rule of taking the point of the constellation the detected point is nearest to.

The Exact P_e

Corresponds to the sum of probabilities of having an error when transmitting a given symbol

$$P_e = \sum_{c=0}^{M-1} P_{e|c} \cdot P(c) = \frac{1}{M} \sum_{c=0}^{M-1} P_{e|c} = 1 - \frac{1}{M} \sum_{c=0}^{M-1} P_{r|c}.$$

Probability of Error

Universitat Autònoma de Barcelona

Union Bound

The probability of error for the ML detector on the AWGN channel, with a M-point signal constellation with minimum distance $d_{\min}$ is bounded by

$$P_e \leq (M-1)Q\left[\frac{d_{\min}}{2\sigma}\right].$$

The Nearest Neighbor Union Bound

The probability of error for the ML detector on the AWGN channel, with a M-point signal constellation with minimum distance $d_{\min}$ is bounded by

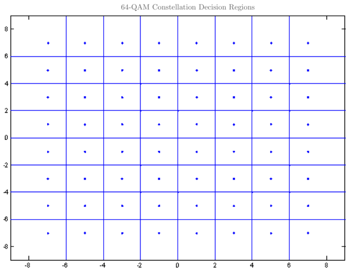
$$P_e \leq N_e Q\left[\frac{d_{\min}}{2\sigma}\right].$$

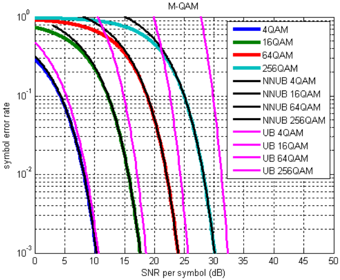
Outline

M-QAM Constellation

$$\mathcal{A} = \{a[n]\} = \{A(a_r[n] + i a_c[n])\},$$

with $a_*[n]$ odd integers around zero.

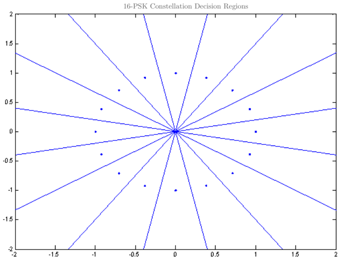


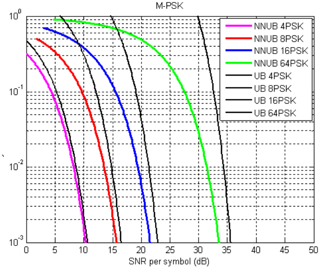


M-PSK Constellation

Universitat Autònoma de Barcelona

$$\mathcal{A} = \{Ae^{j2k\pi/M}\}, \quad k = 1, 2, \cdots, M.$$

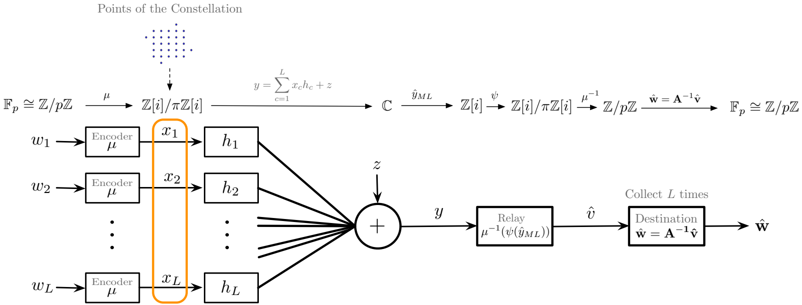




Outline

System Model

Universitat Autònoma de Barcelona



Outline

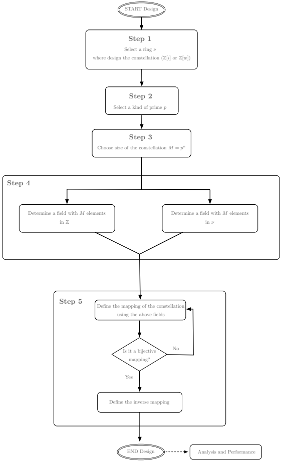
Universitat Autònoma de Barcelona

Proposed Methodology

Universitat Autònoma de Barcelona

Methodology

- Step 1: select a ring ν.
- Step 2: select a type of prime p.
- Step 3: choose size of the constellation $M = p^n$.
- Step 4: determine a field in $\mathbb{Z}$ and ν.
- Step 5: define the mapping of the constellation and its inverse.



Universitat Autònoma de Barcelona

Outline

Outline

Universitat Autònoma de Barcelona

4 Proposed Designs

- Designs in $\mathbb{Z}[i]$
  - $1 \bmod 4$ Constellation
  - $3 \bmod 4$ Constellation
  - Best Performance
- Designs in $\mathbb{Z}[w]$

$1 \bmod 4$ Constellation

Universitat Autònoma de Barcelona

Design 1

- Step 1: ring $\mathbb{Z}[i]$.
- Step 2: primes $p \in \mathbb{Z}^+$, $p \equiv 1 \bmod 4$ in $\mathbb{Z}[i]$ ($p = \pi\pi^*$).
- Step 3: $M = p$.
- Step 4: field with $M = p$ elements in $\mathbb{Z}$ and $\mathbb{Z}[i]$.
  - $\mathbb{Z}/p\mathbb{Z}$, $\#(\mathbb{Z}/p\mathbb{Z}) = |p| = p$.
  - $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$, $\#(\mathbb{Z}[i]/\pi\mathbb{Z}[i]) = N(\pi) = \pi\pi^* = p$.

Theorem

If R is a PID and $a \in R$ is irreducible then R/aR is a field.

$1 \bmod 4$ Constellation

Universitat Autònoma de Barcelona

Design 1

- Step 5: we are looking for $\mathbb{F}_p \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$.

The first mapping from $\mathbb{F}_p$ to $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is defined as follows. We first state the theorem of division in $\mathbb{Z}[i]$

$$x = \lambda\pi + \gamma,$$

$$\text{with } N(\gamma) < N(\pi),$$

$$\text{where } \lambda = \left[\frac{x}{\pi}\right] = \left[\frac{x\pi^*}{\pi\pi^*}\right].$$

If we solve for the residue

$$\gamma = x - \left[\frac{x\pi^*}{\pi\pi^*}\right]\pi.$$

$1 \bmod 4$ Constellation

The mapping of the constellation is defined as:

$$\mu : \mathbb{F}_p \longrightarrow \mathbb{Z}[i]/\pi\mathbb{Z}[i]$$
$$x \longmapsto \mu(x) = x - \left[\frac{x\pi^*}{\pi\pi^*}\right]\pi$$

The inverse mapping is defined as:

$$\mu^{-1} : \mathbb{Z}[i]/\pi\mathbb{Z}[i] \longrightarrow \mathbb{F}_p$$
$$a \longmapsto \mu^{-1}(a) = (a(v\pi^*) + a^*(u\pi^*)) \bmod p$$

with $u\pi + v\pi^* = 1$.

$3 \bmod 4$ Constellation

Universitat Autònoma de Barcelona

Design 2

- Step 1: ring $\mathbb{Z}[i]$.
- Step 2: primes $p \in \mathbb{Z}^+$, $p \equiv 3 \bmod 4$ in $\mathbb{Z}[i]$.
- Step 3: $M = p^2$.
- Step 4:
  - $\mathbb{Z}[i]/p\mathbb{Z}[i]$, $\#\left(\mathbb{Z}[i]/p\mathbb{Z}[i]\right) = N(p) = p^2$.
  - $\mathbb{F}_p[X]/(x^2+1)$, $\#\left(\mathbb{F}_p[X]/(x^2+1)\right) = p^2$.

Theorem

If R is a PID and $a \in R$ is irreducible then R/aR is a field.

$3 \mod 4$ Constellation

Universitat Autònoma de Barcelona

Design 2

- Step 5: we are looking for $\mathbb{F}_p[X]/(x^2+1) \cong \mathbb{Z}[i]/p\mathbb{Z}[i]$ with X corresponding to i.

We are going to see that the two fields are isomorphic to $\mathbb{Z}[X]/(p, x^2+1)$.

- First, $\mathbb{Z}[X]/(x^2+1) \cong \mathbb{Z}[i]$ with $X \to i$.

$$\begin{aligned} \psi : \mathbb{Z}[X] &\longrightarrow \mathbb{Z}[i] \\ P(X) &\longmapsto P(i) \end{aligned}$$

Surjective with kernel $(1+x^2)$.

$3 \bmod 4$ Constellation

Universitat Autònoma de Barcelona

By the NOETHER First Isomorphism Theorem:

$$\text{Image}(\psi) \cong \mathbb{Z}[X]/\text{Kernel}(\psi)$$

$$\begin{tikzcd}
\mathbb{Z}[X] \arrow[rr, "\psi"] \arrow[d, "\pi"'] & & \mathbb{Z}[i] = \text{Image}(\psi) \\
\begin{array}{c}\mathbb{Z}[X]/\text{Kernel}(\psi) \\ = \\ \mathbb{Z}[X]/(x^2+1)\end{array} \arrow[urr, "\cong", "\hat{\psi}"'] & &
\end{tikzcd}$$

We can assert $\psi^{-1}(p\mathbb{Z}[i]) = (p, x^2+1)$. Hence

$$\mathbb{Z}[i]/p\mathbb{Z}[i] \cong \mathbb{Z}[X]/(p, x^2+1).$$

$3 \bmod 4$ Constellation

- Since $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ we have

$$\begin{aligned}
\mathbb{F}_p[X]/(x^2+1) &\cong (\mathbb{Z}/p\mathbb{Z})[X]/(x^2+1), \\
&\cong (\mathbb{Z}[X]/(p))/(x^2+1), \\
&\cong \mathbb{Z}[X]/(p, x^2+1).
\end{aligned}$$

$3 \bmod 4$ Constellation

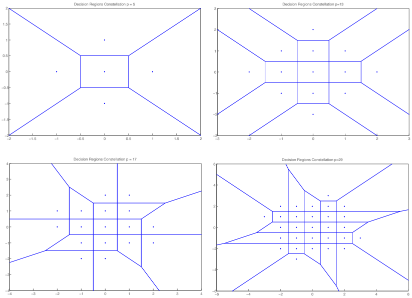
The mapping of the constellation is defined as:

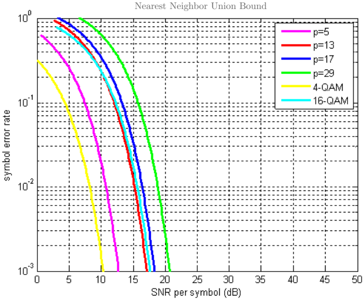
$$\begin{aligned} \gamma : \mathbb{F}_p[X]/(x^2+1) &\longrightarrow \mathbb{Z}[i]/p\mathbb{Z}[i] \\ x &\longmapsto i \end{aligned}$$

The inverse mapping is defined as:

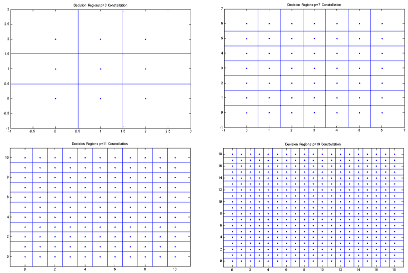
$$\begin{aligned} \gamma^{-1} : \mathbb{Z}[i]/p\mathbb{Z}[i] &\longrightarrow \mathbb{F}_p[X]/(x^2+1) \\ i &\longmapsto x \end{aligned}$$

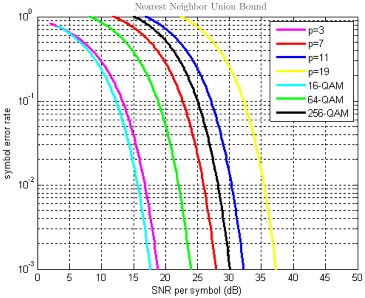
$1 \bmod 4$ Constellation





$3 \bmod 4$ Constellation





Outline

4 Proposed Designs
- Designs in $\mathbb{Z}[i]$
- Designs in $\mathbb{Z}[w]$
  - $1 \bmod 6$ Constellation
  - $2 \bmod 3$ Constellation
  - Best Performance

$1 \bmod 6$ Constellation

Universitat Autònoma de Barcelona

Design 3

- Step 1: ring $\mathbb{Z}[w]$.
- Step 2: primes $p \in \mathbb{Z}^+$, $p \equiv 1 \bmod 6$ in $Z[w]$ ($p = \pi\pi^*$).
- Step 3: $M = p$.
- Step 4:
  - $\mathbb{Z}/p\mathbb{Z}$, $\#(\mathbb{Z}/p\mathbb{Z}) = |p| = p$.
  - $\mathbb{Z}[w]/\pi\mathbb{Z}[w]$, $\#(\mathbb{Z}[w]/\pi\mathbb{Z}[w]) = N(\pi) = \pi\pi^* = p$.

Theorem

If R is a PID and $a \in R$ is irreducible then R/aR is a field.

$1 \bmod 6$ Constellation

Universitat Autònoma de Barcelona

Design 3

- Step 5: we are looking for $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[w]/\pi\mathbb{Z}[w]$.

The mapping of the constellation is defined as:

$$\begin{aligned} \tilde{\mu} : \mathbb{F}_p &\longrightarrow \mathbb{Z}[w]/\pi\mathbb{Z}[w] \\ x &\longmapsto \tilde{\mu}(x) = x - \left[\frac{x\pi^*}{\pi\pi^*}\right]\pi \end{aligned}$$

The inverse mapping is defined as:

$$\begin{aligned} \mu^{-1} : \mathbb{Z}[w]/\pi\mathbb{Z}[w] &\longrightarrow \mathbb{F}_p \\ a &\longmapsto \mu^{-1}(a) = (a(v\pi^*) + a^*(u\pi^*)) \bmod p \end{aligned}$$

with $u\pi + v\pi^* = 1$.

$2 \bmod 3$ Constellation

Design 4

- Step 1: ring $\mathbb{Z}[w]$.
- Step 2: primes $p \in \mathbb{Z}^+$, $p \equiv 2 \bmod 3$ in $Z[w]$.
- Step 3: $M = p^2$.
- Step 4:
  - $\mathbb{Z}[w]/p\mathbb{Z}[w]$, $\#\left(\mathbb{Z}[w]/p\mathbb{Z}[w]\right) = N(p) = p^2$.
  - $\mathbb{F}_p[X]/(x^2+x+1)$, $\#\left(\mathbb{F}_p[X]/(x^2+x+1)\right) = p^2$.

Theorem

If R is a PID and $a \in R$ is irreducible then R/aR is a field.

$2 \bmod 3$ Constellation

Universitat Autònoma de Barcelona

Design 4

- Step 5: we are looking for $\mathbb{Z}[w]/p\mathbb{Z}[w] \cong \mathbb{F}_p[X]/(x^2+x+1)$ with X corresponding to w.

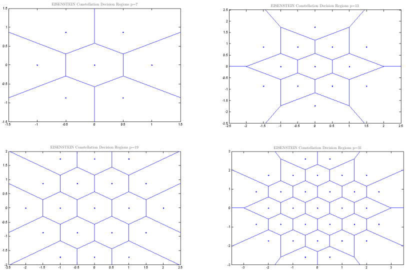
The mapping of the constellation is defined as:

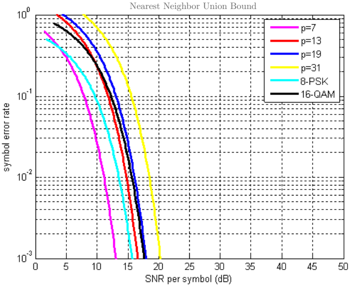
$$\begin{aligned} \tilde{\gamma} : \mathbb{F}_p[X]/(x^2+x+1) &\longrightarrow \mathbb{Z}[w]/p\mathbb{Z}[w] \\ x &\longmapsto w \end{aligned}$$

The inverse mapping is defined as:

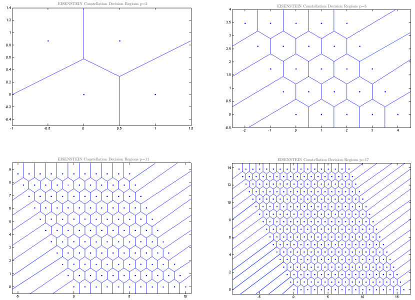
$$\begin{aligned} \tilde{\gamma}^{-1} : \mathbb{Z}[w]/p\mathbb{Z}[w] &\longrightarrow \mathbb{F}_p[X]/(x^2+x+1) \\ w &\longmapsto x \end{aligned}$$

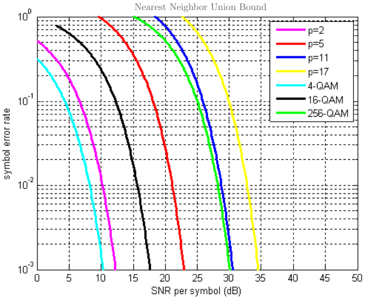
$1 \bmod 6$ Constellation





$2 \bmod 3$ Constellation





Outline

Conclusions

Universitat Autònoma de Barcelona

- Identification of algebraic theory:
  - PID. $\surd$
  - Euclidean domain. $\surd$
  - Fields. $\surd$
- Identification of performance metrics:
  - Decision regions. $\surd$
  - Nearest Neighbor Union Bound. $\surd$
- MATLAB parameters computation:
  - $d_{\min}$. $\surd$
  - N_e. $\surd$
- System model know how:
  - MATLAB implementation proposed. $\surd$

Conclusions

- Design and performance of the constellations:
  - $\mathbb{Z}[i]$:
    - $1 \mod 4$. $\surd$
    - $3 \mod 4$. $\surd$
  - $\mathbb{Z}[w]$:
    - $1 \mod 6$. $\surd$
    - $2 \mod 3$. $\surd$

Conclusions

And Finally the Best Constellations Are

- $1 \bmod 6$ constellation in $\mathbb{Z}[w]$ is the best performing constellation.
- $1 \bmod 4$ constellations in $\mathbb{Z}[i]$ appear as a good QAM alternative.
- QAM constellations have better performance than $3 \bmod 4$ in $\mathbb{Z}[i]$ and $2 \bmod 3$ in $\mathbb{Z}[w]$.

Thank You

DE ZARZA I CUBERO Irene.

Thank you.