On Multiplicative Matrix Channels over Finite Chain Rings

Roberto W. Nóbrega*, Chen Feng†,
Danilo Silva*, Bartolomeu F. Uchôa-Filho*

*Department of Electrical Engineering, Federal University of Santa Catarina, Brazil
†Department of Electrical and Computer Engineering, University of Toronto, Canada

2013 IEEE International Symposium on Network Coding
June 7, 2013, Calgary, Alberta

What Are Rings?

- Rings are algebraic structures with two operations ($+$ and $\times$).
  - Unlike fields, non-zero elements need not be invertible.

What Are Rings?

- Rings are algebraic structures with two operations ($+$ and $\times$).
  - Unlike fields, non-zero elements need not be invertible.
- Examples of finite rings:
  - Finite fields ($\mathbb{F}_q$);
  - Integers modulo n ($\mathbb{Z}_n$);
  - Quotients of Gaussian integers (e.g., $\mathbb{Z}_n[i]$);
  - Finite chain rings (including some of the above).
  - Products of those (e.g., $\mathbb{Z}_2 \times \mathbb{Z}_4$).

What Are Rings?

- Rings are algebraic structures with two operations ($+$ and $\times$).
    - Unlike fields, non-zero elements need not be invertible.
- Examples of finite rings:
    - Finite fields ($\mathbb{F}_q$);
    - Integers modulo n ($\mathbb{Z}_n$);
    - Quotients of Gaussian integers (e.g., $\mathbb{Z}_n[i]$);
    - Finite chain rings (including some of the above).
    - Products of those (e.g., $\mathbb{Z}_2 \times \mathbb{Z}_4$).
- Modules are the ring-theoretic counterpart of vector spaces.
    - Let R be a ring, and let Ω be a module over R.
    - Unlike vector spaces, we do not necessarily have $\Omega \cong R^n$.

Multiplicative Matrix Channels

Let R be a ring, and let n, m, ℓ be positive integers.

Definition

A multiplicative matrix channel (MMC) over R is a communication channel in which the input $\boldsymbol{X} \in R^{n \times \ell}$ and the output $\boldsymbol{Y} \in R^{m \times \ell}$ are matrices related by

$$\boldsymbol{Y} = \boldsymbol{A}\boldsymbol{X},$$

where $\boldsymbol{A} \in R^{m \times n}$ is called the transfer matrix.

- MMCs over finite fields have been studied before.

Multiplicative Matrix Channels

Let R be a ring, and let n, m, ℓ be positive integers.

Definition

A multiplicative matrix channel (MMC) over R is a communication channel in which the input $\boldsymbol{X} \in R^{n \times \ell}$ and the output $\boldsymbol{Y} \in R^{m \times \ell}$ are matrices related by

$$\boldsymbol{Y} = \boldsymbol{A}\boldsymbol{X},$$

where $\boldsymbol{A} \in R^{m \times n}$ is called the transfer matrix.

- MMCs over finite fields have been studied before.
- MMCs over finite rings are considered here.

Multiplicative Matrix Channels

Let R be a ring, and let n, m, ℓ be positive integers.

Definition

A multiplicative matrix channel (MMC) over R is a communication channel in which the input $\boldsymbol{X} \in R^{n \times \ell}$ and the output $\boldsymbol{Y} \in R^{m \times \ell}$ are matrices related by

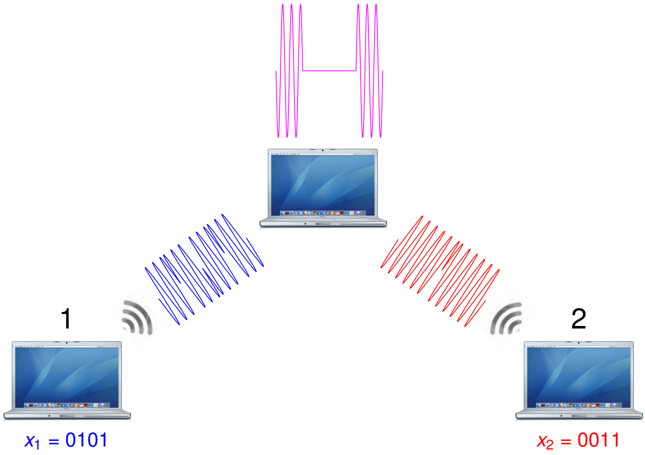
$$\boldsymbol{Y} = \boldsymbol{AX},$$

where $\boldsymbol{A} \in R^{m \times n}$ is called the transfer matrix.

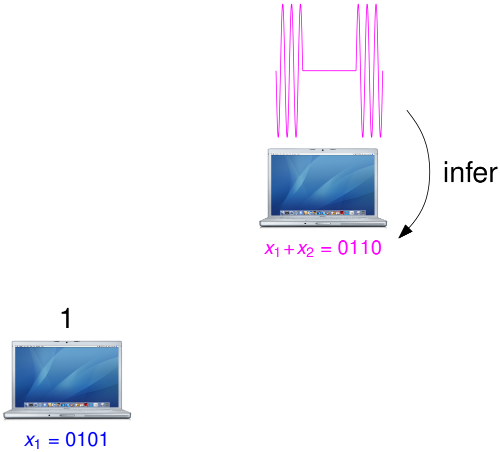
- MMCs over finite fields have been studied before.
- MMCs over finite rings are considered here. Why?

Physical-Layer Network Coding

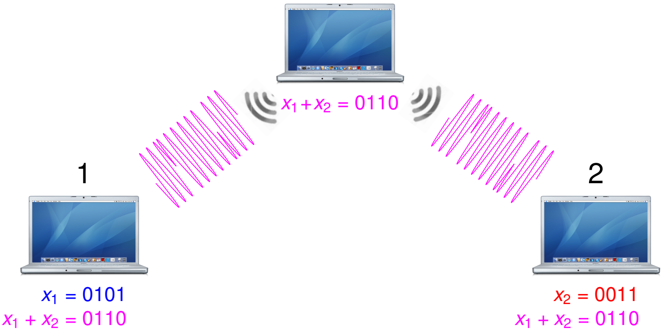
Physical-Layer Network Coding



Physical-Layer Network Coding



Physical-Layer Network Coding



Physical-Layer Network Coding

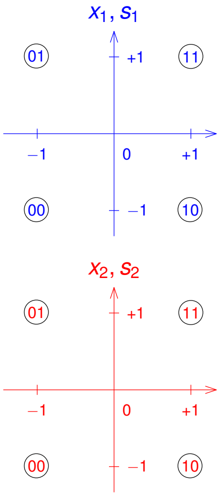
1

$x_1 = 0101$
$x_1 + x_2 = 0110$
$x_2 = 0011$

2

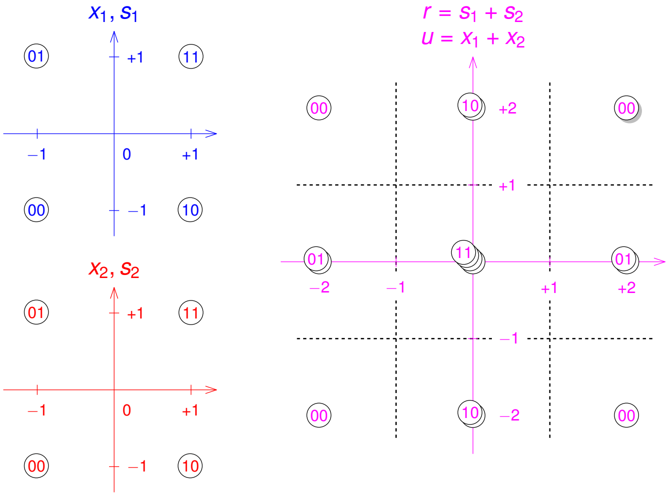
$x_2 = 0011$
$x_1 + x_2 = 0110$
$x_1 = 0101$

Example: QPSK Modulation [1]

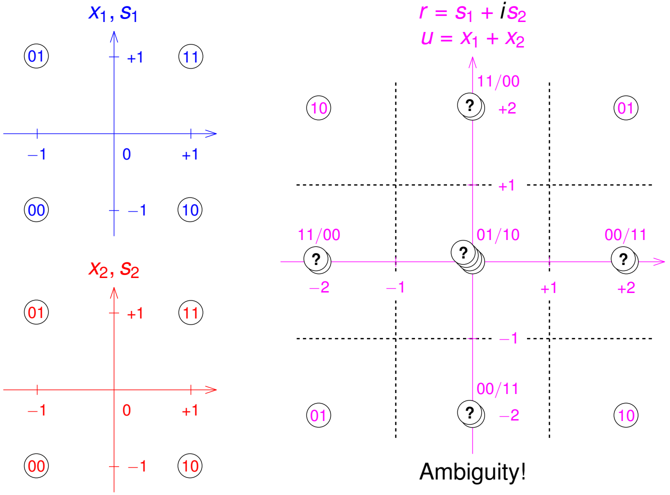


$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{00, 10, 01, 11\}$$

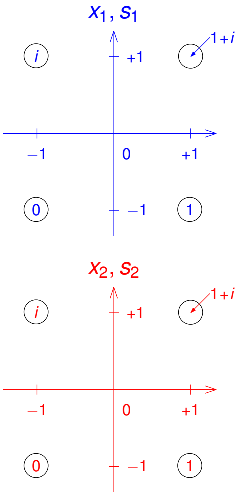
Example: QPSK Modulation [1]



Example: QPSK Modulation [1]



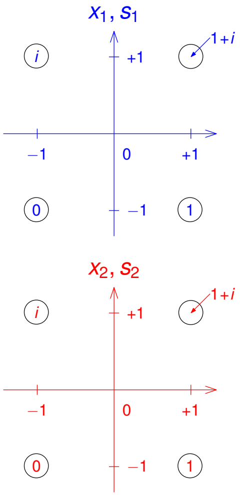
Example: QPSK Modulation [2]

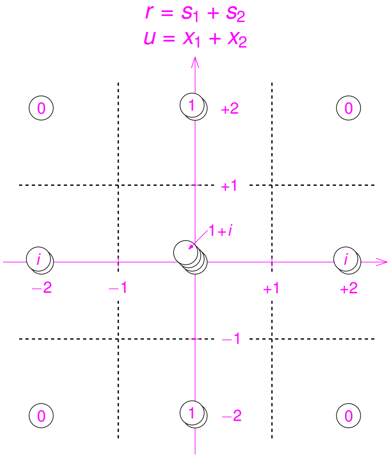


Solution:

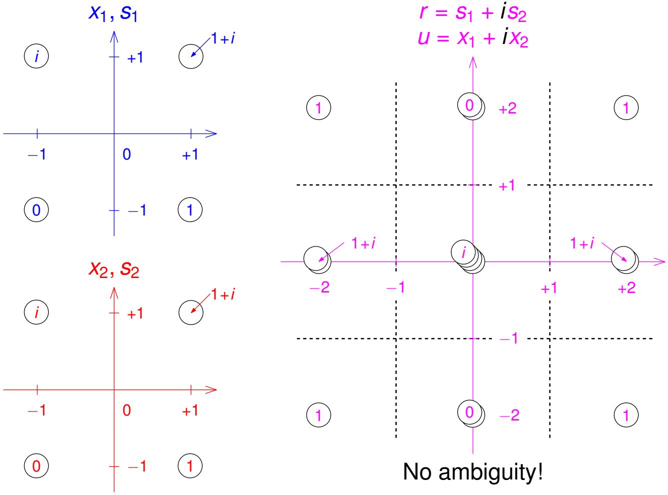
$$\mathbb{Z}_2[i] = \{0, 1, i, 1+i\}$$

Example: QPSK Modulation [2]





Example: QPSK Modulation [2]



No ambiguity!

Rings and Modules Found in Practice

Uncoded modulation:

- 4-ASK $\longrightarrow$ $R = \mathbb{Z}_4$
- QPSK $\longrightarrow$ $R = \mathbb{Z}_2[i]$
- 16-QAM $\longrightarrow$ $R = \mathbb{Z}_4[i]$
- 64-QAM $\longrightarrow$ $R = \mathbb{Z}_8[i]$

In all the cases above, $\Omega = R^\ell$.

Rings and Modules Found in Practice

Uncoded modulation:

- 4-ASK $\longrightarrow$ $R = \mathbb{Z}_4$
- QPSK $\longrightarrow$ $R = \mathbb{Z}_2[i]$
- 16-QAM $\longrightarrow$ $R = \mathbb{Z}_4[i]$
- 64-QAM $\longrightarrow$ $R = \mathbb{Z}_8[i]$

In all the cases above, $\Omega = R^\ell$.

Beyond uncoded modulation: Nested-lattice-based PNC

- [Ordentlich, Zhan, Erez, Gastpar, Nazer, ISIT'11]
  Construction A applied to a binary LDPC code.
  $\longrightarrow$ $R = \mathbb{Z}_4$ and $\Omega = R^{54000} \times (2R)^{10800}$
- [Sakzad, Sadeghi, Panario, Allerton'10]
  Construction D applied to nested turbo codes.
  $\longrightarrow$ $R = \mathbb{Z}_4$ and $\Omega = R^{3377} \times (2R)^{1688}$

Rings and Modules Found in Practice

Uncoded modulation:

- 4-ASK $\longrightarrow$ $R = \mathbb{Z}_4$
- QPSK $\longrightarrow$ $R = \mathbb{Z}_2[i]$
- 16-QAM $\longrightarrow$ $R = \mathbb{Z}_4[i]$
- 64-QAM $\longrightarrow$ $R = \mathbb{Z}_8[i]$

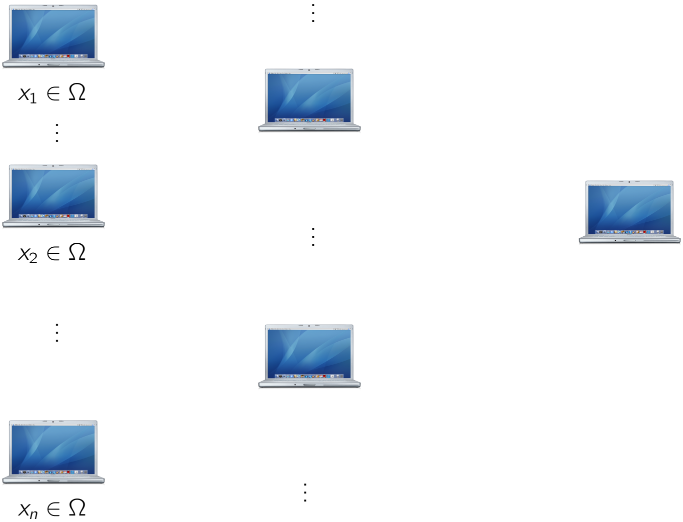
In all the cases above, $\Omega = R^\ell$.

Beyond uncoded modulation: Nested-lattice-based PNC

- [Ordentlich, Zhan, Erez, Gastpar, Nazer, ISIT'11]
  Construction A applied to a binary LDPC code.
  $\longrightarrow$ $R = \mathbb{Z}_4$ and $\Omega = R^{54000} \times (2R)^{10800}$
- [Sakzad, Sadeghi, Panario, Allerton'10]
  Construction D applied to nested turbo codes.
  $\longrightarrow$ $R = \mathbb{Z}_4$ and $\Omega = R^{3377} \times (2R)^{1688}$

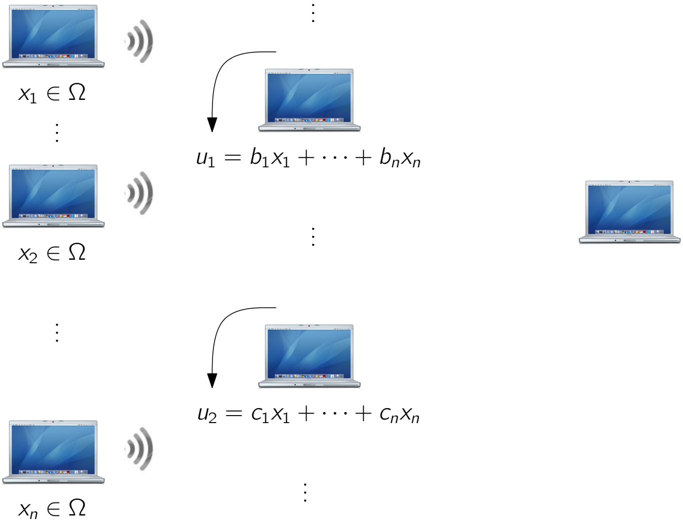
All of these are examples of finite chain rings.

Extension to Larger Networks

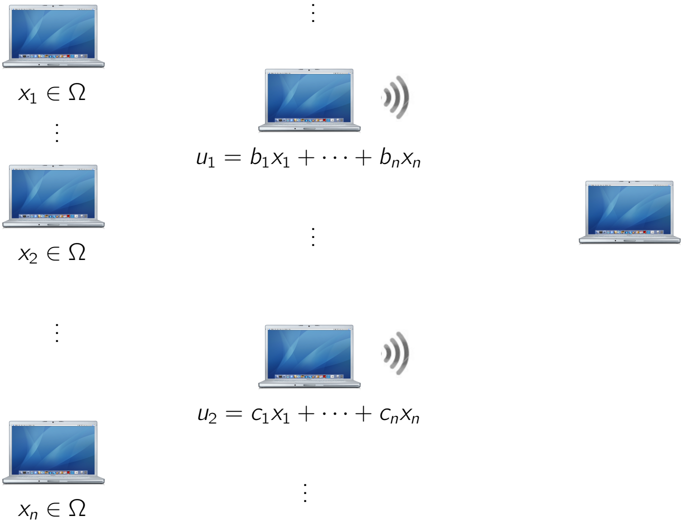


Extension to Larger Networks

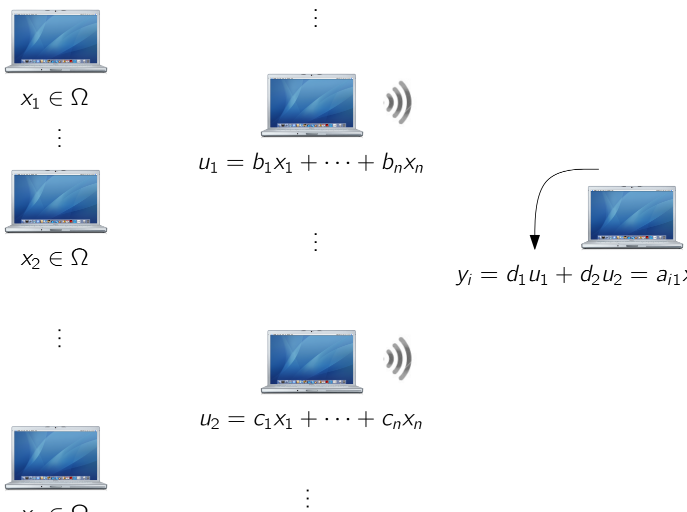
Extension to Larger Networks



Extension to Larger Networks



Extension to Larger Networks



$x_1 \in \Omega$

$x_2 \in \Omega$

$x_n \in \Omega$

$u_1 = b_1 x_1 + \cdots + b_n x_n$

$u_2 = c_1 x_1 + \cdots + c_n x_n$

$y_i = d_1 u_1 + d_2 u_2 = a_{i1} x_1 + \cdots + a_{in} x_n$

Extension to Larger Networks

$x_1 \in \Omega$

$\vdots$

$x_2 \in \Omega$

$\vdots$

$x_n \in \Omega$

$\vdots$

$u_1 = b_1 x_1 + \cdots + b_n x_n$

$\vdots$

$u_2 = c_1 x_1 + \cdots + c_n x_n$

$\vdots$

$$y_i = d_1 u_1 + d_2 u_2 = a_{i1} x_1 + \cdots + a_{in} x_n$$

$$\begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

$$Y = AX$$

Multiplicative matrix channel (MMC)

Extension to Larger Networks

$x_1 \in \Omega$

$\vdots$

$x_2 \in \Omega$

$\vdots$

$x_n \in \Omega$

$\vdots$

$u_1 = b_1 x_1 + \cdots + b_n x_n$

$\vdots$

$u_2 = c_1 x_1 + \cdots + c_n x_n$

$\vdots$

Remark: Erroneous packets are discarded via linear error-detecting codes (over the ring).

$$y_i = d_1 u_1 + d_2 u_2 = a_{i1} x_1 + \cdots + a_{in} x_n$$

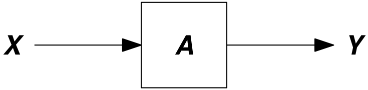
$$\begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

$$Y = AX$$

Multiplicative matrix channel (MMC)

The Problem

We study MMCs over finite chain rings.



Assumptions

- The probability distribution of $\boldsymbol{A}$ is arbitrary.
- $\boldsymbol{X}$ and $\boldsymbol{A}$ are independent.
- $\boldsymbol{A}$ is unknown at the transmitter, but known at the receiver (CSIR).

Contribution: Channel Capacity

Let s be the number of proper ideals of the finite chain ring.

Theorem

The channel capacity is achieved with uniform input and is given by

$$C = \sum_{i=0}^{s-1} \mathrm{E}[\rho_{s-i-1}]\lambda_i,$$

where $\lambda = \operatorname{shape} \Omega$, and $\rho = \operatorname{shape} \boldsymbol{A}$.

Contribution: Channel Capacity

Let s be the number of proper ideals of the finite chain ring.

Theorem

The channel capacity is achieved with uniform input and is given by

$$C = \sum_{i=0}^{s-1} \mathrm{E}[\rho_{s-i-1}]\lambda_i,$$

where $\lambda = \operatorname{shape}\Omega$, and $\rho = \operatorname{shape}\boldsymbol{A}$.

The shape is an s-tuple of integers.

- The shape of a module generalizes the concept of dimension.
- The shape of a matrix generalizes the concept of rank.

Contribution: Coding Scheme

Overview of the coding scheme

We propose a coding scheme that adopts a layered approach by combining *s* codes over the residue field to obtain an overall code over the finite chain ring.

- The *code construction* makes use of the π-adic expansion.
- *Decoding* is performed in a multistage fashion, layer by layer.

Contribution: Coding Scheme

Overview of the coding scheme

We propose a coding scheme that adopts a layered approach by combining s codes over the residue field to obtain an overall code over the finite chain ring.

- The *code construction* makes use of the π-adic expansion.
- *Decoding* is performed in a multistage fashion, layer by layer.

Code features

- Capacity-achieving;
- Polynomial time complexity;
- Universal: only the knowledge of $\mathrm{E}[\rho]$ is needed ($\rho =$ shape $\boldsymbol{A}$).

Thank you!

Roberto W. Nóbrega
http://gpqcom.ufsc.br/~rwnobrega/
rwnobrega@eel.ufsc.br