# On Multiplicative Matrix Channels over Finite Chain Rings

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

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

## INTRODUCTION

Let $R$ be a ring. 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 related by

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

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

~

MMCs turn out to be suitable models for the end-to-end channel between a source node and a sink node in wireless networks employing compute-and-forward over a generic nested lattice [1]. In this context, $\boldsymbol{X}$ and $\boldsymbol{Y}$ are matrices whose rows are the $n$ transmitted packets and $m$ received packets, respectively, and $\boldsymbol{A}$ is a matrix whose entries are determined by the random choices of the network coding coefficients. Most importantly, the underlying ring $R$ is not necessarily a finite field, but a finite *principal ideal ring* (PIR), with the packets belonging to some finite $R$-module.

~

Since every finite PIR is a product of finite chain rings, it is natural to consider the study of *MMCs over finite chain rings*. In this work, we assume *channel side information at the receiver* (CSIR), that is, we assume that the instances of the transfer matrix $\boldsymbol{A}$ are unknown to the transmitter, but available at the receiver. Our results [2] extend (and make use of) some of those in [3]. A related work is [4].

## FINITE CHAIN RINGS

### ▶ *Definition and notation*

A *chain ring* is a ring in which the ideals are linearly ordered under subset inclusion ($\subseteq$).

| | |
|---|---|
| $R$ | a finite chain ring |
| $\pi$ | any generator for the maximal ideal of $R$ |
| $s$ | the nilpotency index of $\pi$ |
| $q$ | the order of the residue field $R/\langle\pi\rangle$ |
| $\Gamma$ | any set of coset representatives for $R/\langle\pi\rangle$ |

### ▶ *The ideals of $R$*

$R$ has precisely $s+1$ ideals, namely,

$$R = \langle 1 \rangle \supset \langle \pi \rangle \supset \langle \pi^2 \rangle \supset \cdots \supset \langle \pi^{s-1} \rangle \supset \langle \pi^s \rangle = \{0\}.$$

### ▶ *The $\pi$-adic decomposition*

Every element $x \in R$ can be written *uniquely* as

$$x = x^{(0)} + x^{(1)}\pi + x^{(2)}\pi^2 + \cdots + x^{(s-1)}\pi^{s-1},$$

where $x^{(i)} \in \Gamma$.

## MODULES AND MATRICES OVER CHAIN RINGS

### ▶ *Definitions*

An *$s$-shape* $\mu = (\mu_0, \mu_1, \ldots, \mu_{s-1})$ is a non-decreasing sequence of $s$ non-negative integers. We define

$$R^\mu \triangleq \underbrace{\langle 1 \rangle \times \cdots \times \langle 1 \rangle}_{\mu_0} \times \underbrace{\langle \pi \rangle \times \cdots \times \langle \pi \rangle}_{\mu_1 - \mu_0} \times \cdots \times \underbrace{\langle \pi^{s-1} \rangle \times \cdots \times \langle \pi^{s-1} \rangle}_{\mu_{s-1} - \mu_{s-2}},$$

which is an $R$-module.

### ▶ *Structure theorem for finite $R$-modules*

If $M$ is a finite $R$-module, then

$$M \cong R^\mu$$

for some *unique* $s$-shape $\mu$. We write $\mu = \operatorname{shape} M$. *The shape of an $R$-module generalizes the concept of dimension of a vector space.*

### ▶ *The shape of a matrix*

The shape of a matrix $A$ is defined as

$$\operatorname{shape} A = \operatorname{shape}(\operatorname{row} A) = \operatorname{shape}(\operatorname{col} A),$$

where $\operatorname{row} A$ and $\operatorname{col} A$ are the row and column spaces of $A$, respectively. *The shape of a matrix generalizes the concept of rank.*

### ▶ *The Smith normal form*

Two matrices $A, B \in R^{m \times n}$ are *equivalent* if $A = PBQ$ for some invertible matrices $P$ and $Q$. If $\operatorname{shape} A = \rho$, then $A \in R^{m \times n}$ is equivalent to

$$\operatorname{diag}(\underbrace{1, \ldots, 1}_{\rho_0}, \underbrace{\pi, \ldots, \pi}_{\rho_1 - \rho_0}, \ldots, \underbrace{\pi^{s-1}, \ldots, \pi^{s-1}}_{\rho_{s-1} - \rho_{s-2}}) \in R^{m \times n},$$

which is called the *Smith normal form* of $A$.

### ▶ *Matrices with row constraints*

Let $n$ and $\ell$ be positive integers, and let $\lambda$ be an $s$-shape with $\lambda_{s-1} = \ell$. The subset of matrices in $R^{n \times \ell}$ whose rows belong to $R^\lambda$ is denoted by $R^{n \times \lambda}$.

## CHANNEL MODEL

Let the following be given.

| | |
|---|---|
| $n$ | an integer (number of transmitted packets) |
| $m$ | an integer (number of received packets) |
| $\lambda$ | an $s$-shape (shape of packet space) |
| $p_{\boldsymbol{A}}$ | a probability distribution over $R^{m \times n}$ |

Define $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}, \lambda)$ as a DMC with input $\boldsymbol{X} \in R^{n \times \lambda}$, output $(\boldsymbol{Y}, \boldsymbol{A}) \in R^{m \times \lambda} \times R^{m \times n}$, and transition probability

$$p_{\boldsymbol{Y},\boldsymbol{A}|\boldsymbol{X}}(Y, A|X) = \begin{cases} p_{\boldsymbol{A}}(A), & \text{if } Y = AX, \\ 0, & \text{otherwise.} \end{cases}$$

## CHANNEL CAPACITY

*Theorem:* The capacity of $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}, \lambda)$ is given by

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

where $\rho = \operatorname{shape} \boldsymbol{A}$.

## CODING SCHEME

Before we begin, define the following.

| | |
|---|---|
| $\mathbb{F}_q = R/\langle\pi\rangle$ | the residue field |
| $\varphi : R \to \mathbb{F}_q$ | the natural projection map |
| $\bar{\varphi} : \mathbb{F}_q \to \Gamma$ | the coset representative selector |
| $x^i \in R$ | $x^i = x^{(0)} + x^{(1)}\pi + \cdots + x^{(i-1)}\pi^{i-1}$ |

*Layered approach:* Combine $s$ codes over the residue field to obtain a code over the chain ring.

### ▶ *Codebook $\mathcal{C}$*

Let $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{s-1}$ be a sequence of matrix codes over the residue field, where $\mathcal{C}_i \subseteq \mathbb{F}_q^{n \times \lambda_i}$. We define

$$\mathcal{C} = \left\{ \sum_{i=0}^{s-1} X^{(i)}\pi^i : X_i \in \mathcal{C}_i, 0 \leq i < s \right\},$$

where $X^{(i)} = \begin{bmatrix} \bar{\varphi}(X_i) & 0 \end{bmatrix} \in \Gamma^{n \times \ell}$.

### ▶ *Multistage decoding algorithm*

*Input:* $(Y, A) \in R^{m \times \lambda} \times R^{m \times n}$, with $\operatorname{shape} A \triangleq \rho$.

*Output:* $X \in \mathcal{C}$ such that $Y = AX$.

*Step 1:* Compute $P, D, Q$ such that $A = PDQ$, where $D$ is the Smith normal form of $A$, and $P, Q$ are invertible.

*Step 2:* Set $\tilde{X} \triangleq QX$ (unknown) and $\tilde{Y} \triangleq P^{-1}Y$ (known), so that $Y = AX$ is equivalent to

$$\tilde{Y} = D\tilde{X}.$$

From this, compute $\tilde{X}^{(0)}_{\rho_{s-1} \times \lambda_0}, \tilde{X}^{(1)}_{\rho_{s-2} \times \lambda_1}, \ldots, \tilde{X}^{(s-1)}_{\rho_1 \times \lambda_{s-1}}$.

*Step 3:* Based on $\tilde{X} = QX$, we can show that

$$Y_i = A_i X_i,$$

where

$$Y_i = \begin{bmatrix} \varphi\left(\tilde{X}^{(i)}_{\rho_{s-i-1} \times \lambda_i}\right) - \varphi\left(\left(Q_{\rho_{s-i-1} \times n} X^i_{n \times \lambda_i}\right)^{(i)}\right) \\ 0 \end{bmatrix} \in \mathbb{F}_q^{m \times \lambda_i},$$

and

$$A_i = \begin{bmatrix} \varphi\left(Q_{\rho_{s-i-1} \times n}\right) \\ 0 \end{bmatrix} \in \mathbb{F}_q^{m \times n}.$$

From this, decode successively $X_0, X_1, \ldots, X_{s-1}$. Finally, compute $X$ according to the $\pi$-adic decomposition.

## CODE FEATURES

### ▶ *Rate and probability of error*

The rate of the code is given by

$$\mathrm{R}(\mathcal{C}) = \mathrm{R}(\mathcal{C}_0) + \mathrm{R}(\mathcal{C}_1) + \cdots + \mathrm{R}(\mathcal{C}_{s-1}),$$

and the probability of error is upper bounded as

$$\mathrm{P}_{\mathrm{err}}(\mathcal{C}) \leq \mathrm{P}_{\mathrm{err}}(\mathcal{C}_0) + \mathrm{P}_{\mathrm{err}}(\mathcal{C}_1) + \cdots + \mathrm{P}_{\mathrm{err}}(\mathcal{C}_{s-1}).$$

Thus, $\mathcal{C}$ is capacity-achieving in $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}, \lambda)$ if each $\mathcal{C}_i$ is capacity-achieving in $\mathrm{MMC}_{\mathrm{CSIR}}(\boldsymbol{A}_i, \lambda_i)$ (e.g., [3]).

### ▶ *Complexity*

The coding scheme has a polynomial time complexity.

### ▶ *Universality*

Similarly to [3], the complete knowledge of the probability distribution of $\boldsymbol{A}$ is not needed, but only the knowledge of $\mathrm{E}[\rho]$, where $\rho = \operatorname{shape} \boldsymbol{A}$.

## EXTENSIONS

- One-shot to multi-shot.
- CSIR to non-coherent: Prepend headers.

For more details, see [2].

## CONCLUSION

Motivated by nested-lattice-based physical-layer network coding, this work has considered communication in multiplicative matrix channels over finite chain rings. As contributions:

- The channel capacity has been determined, generalizing the corresponding result for finite fields.
- A polynomial-time capacity-achieving coding scheme was proposed, combining (through a layered approach) several codes over the residue field to obtain a code over the chain ring.

## REFERENCES


[1] C. Feng, D. Silva, and F. R. Kschischang, "An algebraic approach to physical-layer network coding," *To appear in the IEEE Transactions on Information Theory.*

[2] R. W. Nóbrega, C. Feng, D. Silva, and B. F. Uchôa-Filho, "On multiplicative matrix channels over finite chain rings," in *Proceedings of the 2013 IEEE International Symposium on Network Coding (NetCod'13)*, (Calgary, Alberta), June 2013.

[3] S. Yang, S.-W. Ho, J. Meng, E.-h. Yang, and R. W. Yeung, "Linear operator channels over finite fields," *Computing Research Repository (CoRR)*, vol. abs/1002.2293, Apr. 2010.

[4] C. Feng, R. W. Nóbrega, F. R. Kschischang, and D. Silva, "Communication over finite-ring matrix channels," in *Proceedings of the 2013 IEEE International Symposium on Information Theory (ISIT'13)*, (Istanbul, Turkey), July 2013.