Wireless Network Coding over Finite Rings

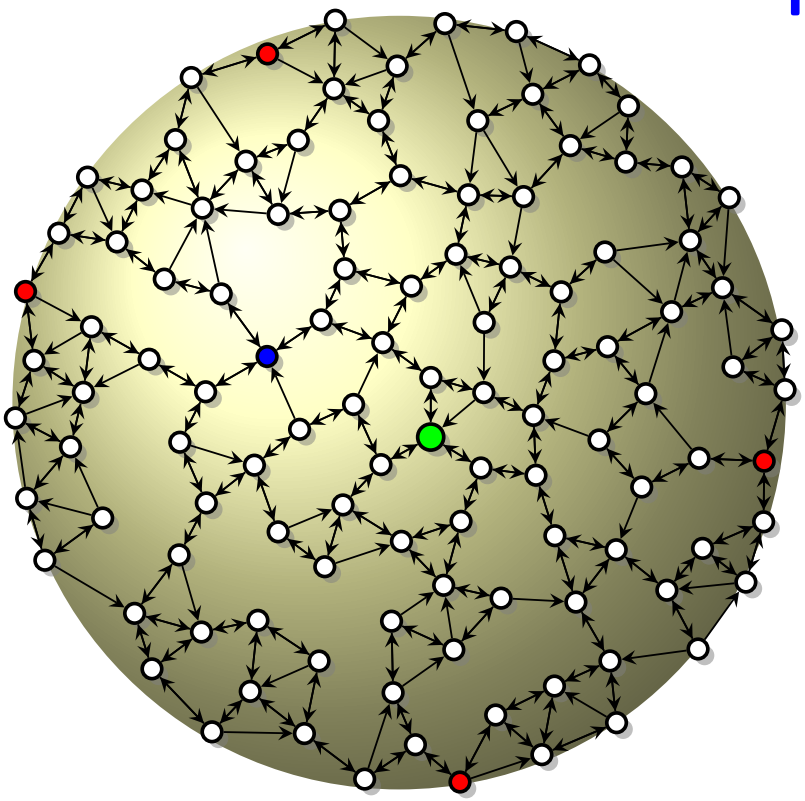
Chen Feng
University of British Columbia, Canada

joint work with:
Frank Kschischang, University of Toronto, Canada
Roberto Nóbrega, Danilo Silva, Federal University of Santa Catarina, Brazil

July 7, 2016

Heslington, York, United Kingdom

Network Coding over Finite Fields



Packet Network

Random Linear Network Coding

- **Transmitter** injects *packets*: vectors from $\mathbb{F}_q^m$, the rows of a matrix X
- Intermediate nodes forward random $\mathbb{F}_q$-linear combinations of packets
- **Errors** may also be injected, which randomly mix with the legitimate packets
- (Each) **receiver** gathers as many packets as possible, forming the rows of matrix Y

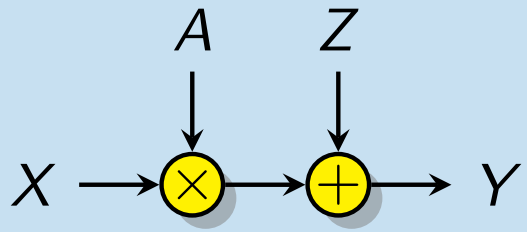
At any particular receiver:

$$Y = AX + Z$$

where: X is $n \times m$; Y, Z are $N \times m$; and A is $N \times n$.

A Basic Model

Multiplicative-Additive Matrix Channel (MAMC)



Previous work[1] considered a basic stochastic linear matrix channel model:

$$Y = AX + Z$$

where

- X and Y are $n \times m$ matrices over $\mathbb{F}_q$;
- A is $n \times n$, nonsingular, drawn uniformly at random;
- Z is $n \times m$ with rank t, drawn uniformly at random;
- X, A, and Z are independent.

[1] Silva, Kschischang, and Kötter, "Communication over Finite-Field Matrix Channels," *IEEE Trans. Inf. Theory*, vol. 56, pp. 1296–1305, Mar. 2010.

MAMC: Capacity

Theorem (upper bound)

For $n \leq m/2$,

$$C_{\mathrm{MAMC}} \leq (n-t)(m-n) + \log_q 4(n+1)(t+1).$$

Theorem (lower bound)

Assume $n \leq m$. For any $\epsilon \geq 0$, we have

$$C_{\mathrm{MAMC}} \geq (n-t-\epsilon t)(m-n) - \log_q 4 - \frac{2tnm}{q^{1+\epsilon t}}.$$

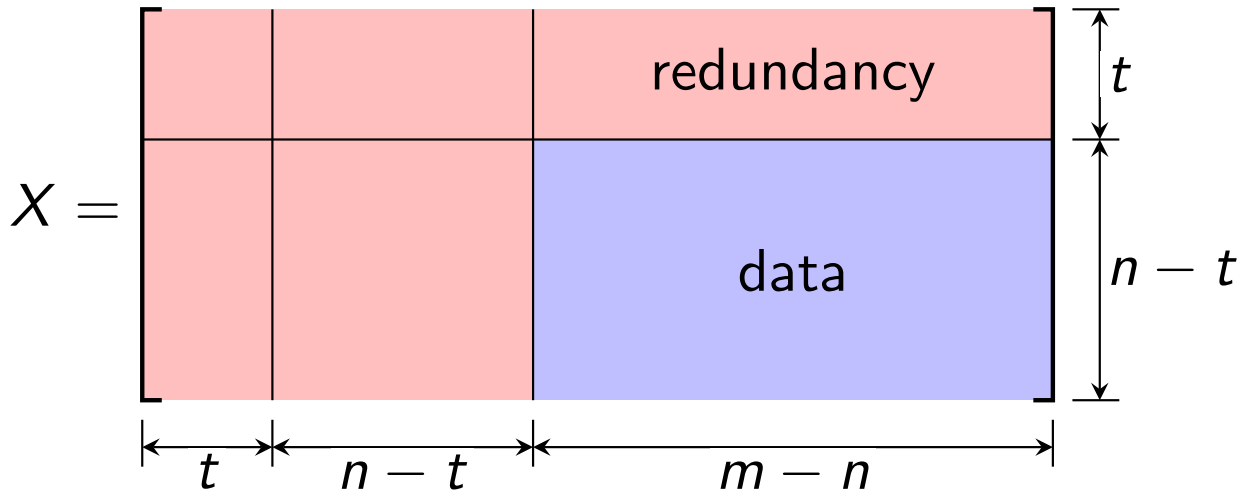
These upper and lower bounds match when $q \to \infty$ or $n \to \infty$ (with t/n and m/n fixed).

MAMC: Capacity

Corollary

For large n or large q,

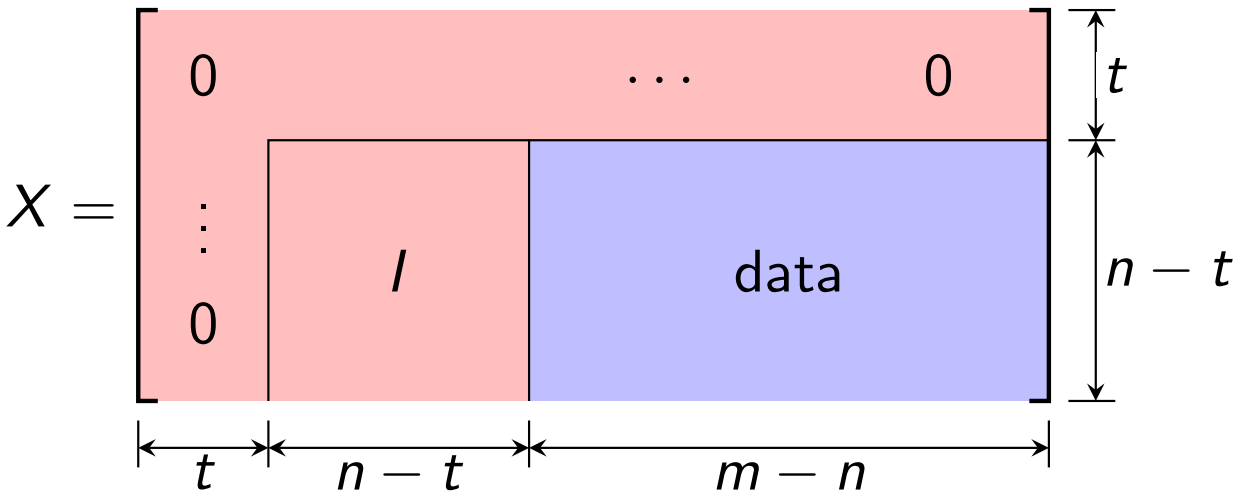
$$C_{\text{MAMC}} \approx (n-t)(m-n).$$



A Simple Coding Scheme

Strategy: Channel Sounding + Error Trapping

Use channel sounding "inside" and error trapping "outside" (but not the opposite!)



MAMC: A Coding Scheme

First, rewrite the channel model as

$$Y = AX + Z = A(X + A^{-1}Z) = A(X + W), \quad \text{where } W = A^{-1}Z.$$

MAMC: A Coding Scheme

First, rewrite the channel model as

$$Y = AX + Z = A(X + A^{-1}Z) = A(X + W), \quad \text{where } W = A^{-1}Z.$$

Suppose a "genie" gives the receiver $X + W$.
Let data matrix D be $(n - t) \times (m - n)$.
We have:

$$X = \begin{bmatrix} 0 & 0 & 0 \\ 0 & I & D \end{bmatrix} \qquad W = \begin{bmatrix} W_1 & W_2 & W_3 \\ W_4 & W_5 & W_6 \end{bmatrix}$$

MAMC: A Coding Scheme

First, rewrite the channel model as

$$Y = AX + Z = A(X + A^{-1}Z) = A(X + W), \quad \text{where } W = A^{-1}Z.$$

Suppose a "genie" gives the receiver $X + W$.
Let data matrix D be $(n - t) \times (m - n)$.
We have:

$$X = \begin{bmatrix} 0 & 0 & 0 \\ 0 & I & D \end{bmatrix} \qquad W = \begin{bmatrix} W_1 & W_2 & W_3 \\ W_4 & W_5 & W_6 \end{bmatrix}$$

Assume that rank $W_1 = t = \text{rank}\, W$ $(= \text{rank}\, Z)$. In this case, for some matrix B, we have

$$W = \begin{bmatrix} W_1 & W_2 & W_3 \\ BW_1 & BW_2 & BW_3 \end{bmatrix}$$

Now convert $X + W$ to reduced row echelon (RRE) form:

$$
\begin{aligned}
X + W &= \begin{bmatrix} W_1 & W_2 & W_3 \\ BW_1 & I + BW_2 & D + BW_3 \end{bmatrix} \\
&\xrightarrow{\text{row op.}} \begin{bmatrix} I & W_1^{-1}W_2 & W_1^{-1}W_3 \\ BW_1 & I + BW_2 & D + BW_3 \end{bmatrix} \\
&\xrightarrow{\text{row op.}} \begin{bmatrix} I & W_1^{-1}W_2 & W_1^{-1}W_3 \\ 0 & I & D \end{bmatrix} \\
&\xrightarrow{\text{row op.}} \begin{bmatrix} I & 0 & \tilde{W}_3 \\ 0 & I & D \end{bmatrix} = \mathrm{RRE}(X + W).
\end{aligned}
$$

But we have Y, not $X + W$!

Now convert $X + W$ to reduced row echelon (RRE) form:

$$X + W = \begin{bmatrix} W_1 & W_2 & W_3 \\ BW_1 & I + BW_2 & D + BW_3 \end{bmatrix}$$

$$\xrightarrow{\text{row op.}} \begin{bmatrix} I & W_1^{-1}W_2 & W_1^{-1}W_3 \\ BW_1 & I + BW_2 & D + BW_3 \end{bmatrix}$$

$$\xrightarrow{\text{row op.}} \begin{bmatrix} I & W_1^{-1}W_2 & W_1^{-1}W_3 \\ 0 & I & D \end{bmatrix}$$

$$\xrightarrow{\text{row op.}} \begin{bmatrix} I & 0 & \tilde{W}_3 \\ 0 & I & D \end{bmatrix} = \text{RRE}(X + W).$$

But we have Y, not $X + W$!

Observation

$Y = A(X + W)$, A is full rank, so Y and $X + W$ have the same row space, which implies that

$$\text{RRE}(Y) = \text{RRE}(X + W).$$

Thus, D is exposed by reducing Y to RRE form!

MAMC: A Coding Scheme

- Decoding amounts to performing full Gaussian elimination on the received matrix Y.

  Complexity: $\mathcal{O}(n^2 m)$ operations in $\mathbb{F}_q$ to recover $(n-t)(m-n)$ symbols. Defining $R = (n-t)(m-t)/mn$, we have a complexity of $\mathcal{O}(n/R)$ operations per decoded symbol.

- The scheme fails if W_1 is not invertible.
  The probability of failure falls exponentially (for fixed n) in the number of bits per field-element, or exponentially (for fixed q) in n (assuming fixed aspect ratio of m/n and fixed t/n).

Theorem

This coding scheme can achieve the capacity of the MAMC when either $q \to \infty$ or $n \to \infty$.

This Talk:

Generalize
from
finite-field matrix channels
to
finite-ring matrix channels.

Why?

A: it could be useful for **compute-and-forward**[2]

[2]Bobak Nazer and Michael Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, pp. 6463–6486, Oct. 2011.

From Network Coding to Compute-and-Forward

Conventional network coding

Message space is $\mathbb{F}_q^m$.

Compute-and-forward

Message space is

$$T/\langle a_1 \rangle \times \cdots \times T/\langle a_m \rangle$$

for some nonzero, non-unit $a_1, \ldots, a_m \in T$ such that $a_1 \mid \cdots \mid a_m$.

- T is a discrete subring of $\mathbb{C}$ forming a principal ideal domain[3]

[3] F., D. Silva, F. Kschischang, "An Algebraic Approach to Physical-Layer Network Coding," *IEEE Trans. Inf. Theory*, vol. 59, pp. 7576–7596, Nov. 2013.

Message Space: Examples

Example 1: [Ordentlich, Zhan, Erez, Gastpar, Nazer, ISIT'11]

- Λ is obtained using Construction A applied to binary $(n = 64800, k = 54000)$ LDPC code C, with mod-4 shaping:

$$\Lambda = C + 2\mathbb{Z}^n, \quad \Lambda' = 4\mathbb{Z}^n.$$

- Message space: $\mathbb{Z}_2^{10800} \times \mathbb{Z}_4^{54000}$

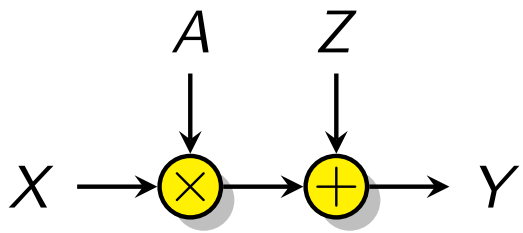
Example 2: Turbo Lattices [Sakzad, Sadeghi, Panario, Allerton'10]

- Λ is obtained using Construction D applied to nested turbo codes $C_2 : (n = 10131, k_2 = 3377)$ and $C_1 : (n = 10131, k_1 = 5065)$;

$$\Lambda = C_2 + 2C_1 + 4\mathbb{Z}^n, \quad \Lambda' = 4\mathbb{Z}^n.$$

- Message space: $\mathbb{Z}_2^{1688} \times \mathbb{Z}_4^{3377}$

Objective



$$Y = AX + Z$$

where each row of X, Y, and Z is from the message space

$$T/\langle a_1 \rangle \times \cdots \times T/\langle a_m \rangle$$

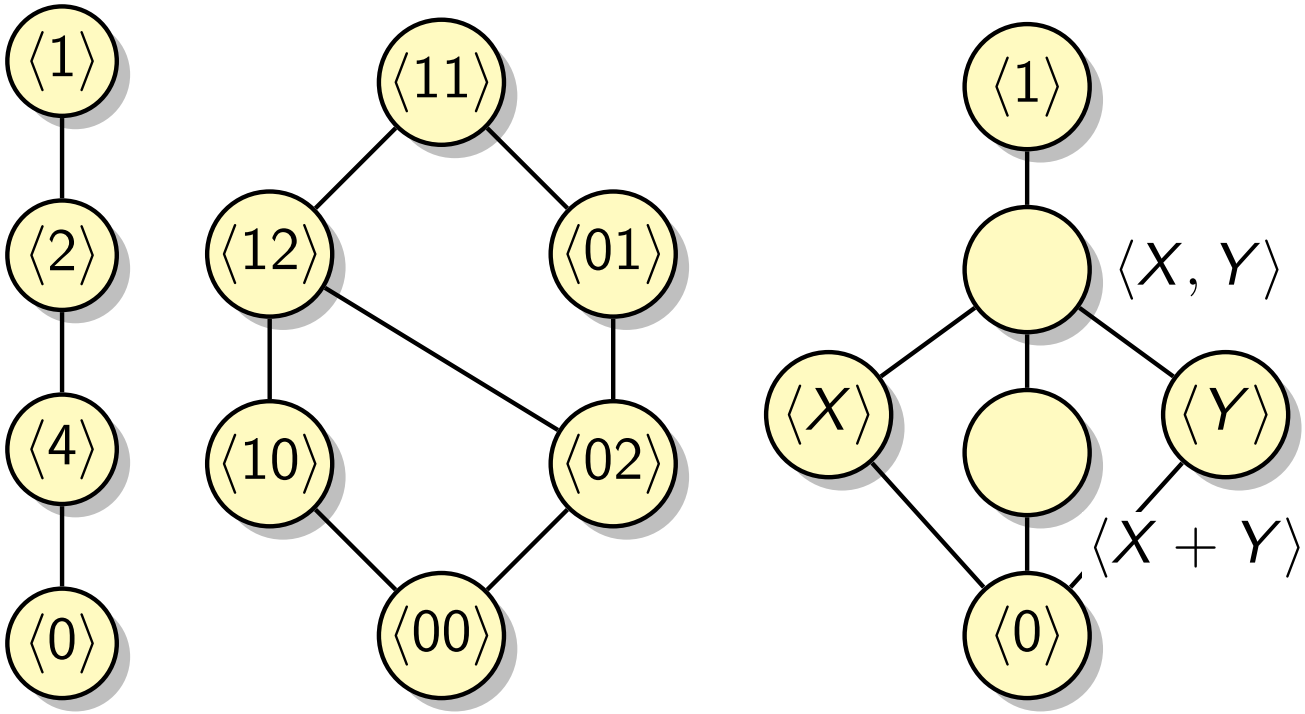
Objective:

- Capacity bounds
- Simple coding schemes

Finite-Ring Toolkit

Commutative Rings with Identity $1 \neq 0$

- Ideals in a ring can be partially ordered by subset inclusion.
- The resulting poset is called the lattice of ideals of the ring.



Chain ring: ideals are linearly ordered. Ex: $\mathbb{Z}_8$.

Principal ring: every ideal generated by 1 element. Ex: $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Local ring: unique maximal proper ideal. Ex: $\mathbb{Z}_8$, $\mathbb{Z}_2[X, Y]/\langle X, Y\rangle^2$.

Finite Rings: Important Facts

Proposition

If R is a ring and N is a **maximal** ideal of R, then R/N is a **field**.

This is called a residue field.

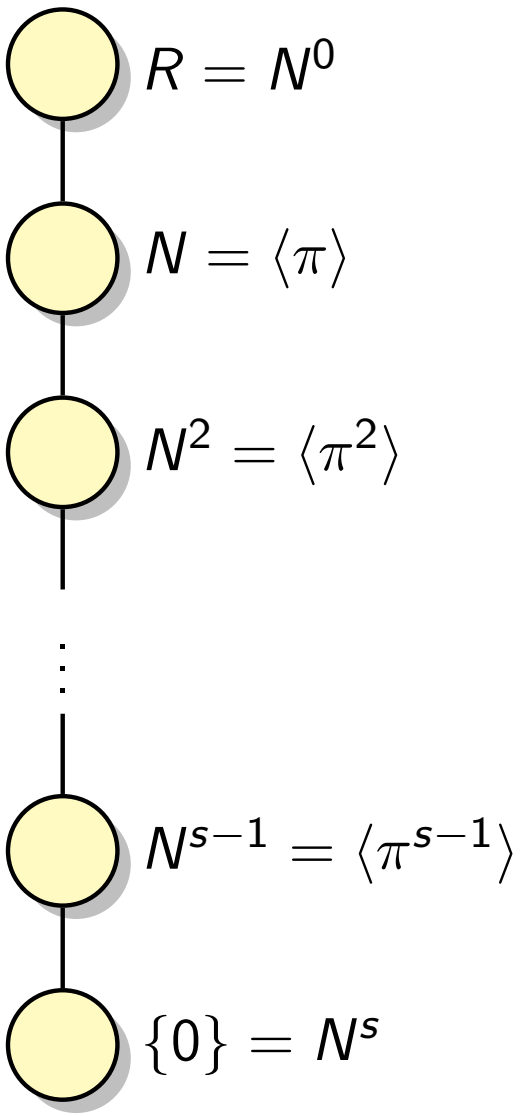
Proposition

A finite ring is a **chain** ring if and only if it is both **local** and **principal**.

Proposition

Every finite **principal** ring is a product of finite **chain** rings.

Finite Chain Rings: The Ideals



Let R be a finite chain ring, where

- N is the unique maximal ideal,
- π is any generator for N,
- q is the order of the residue field,
- s is the number of proper ideals.

Proposition

The lattice of ideals of R is

$$R = N^0 \supset N \supset \cdots \supset N^{s-1} \supset N^s = \{0\}.$$

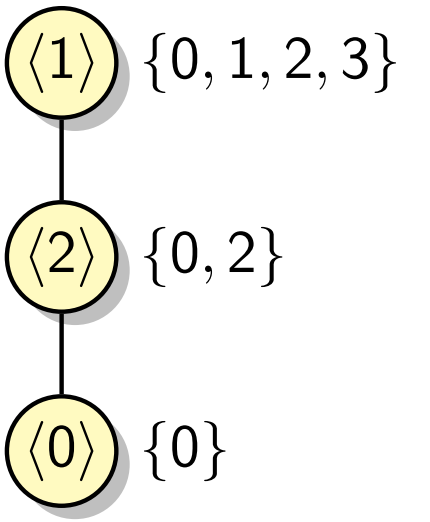
The size of each ideal is $|N^i| = q^{s-i}$.

Notation: (q, s) chain ring.

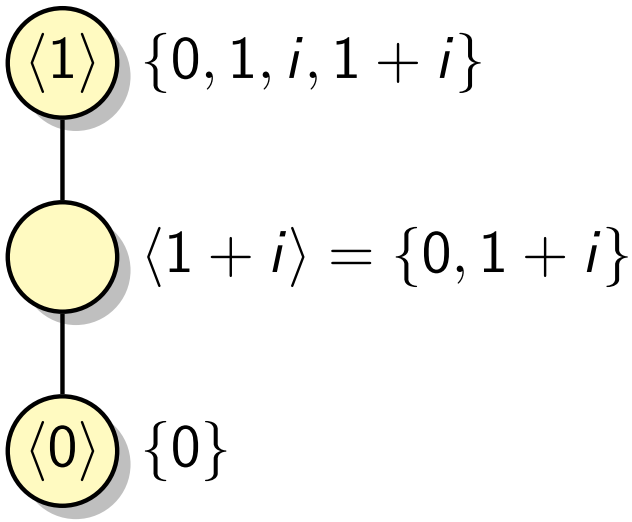
Finite Chain Rings: Examples

The following are two non-isomorphic $(q = 2, s = 2)$ chain rings.

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$



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



Finite Chain Rings: The π-adic Decomposition

Let R be a (q, s) chain ring, and N be its maximal ideal.

Proposition

Fix the following:

$\pi \in R$, a generator for the maximal ideal N (i.e., $\langle \pi \rangle = N$).

$F \subseteq R$, a set of coset representatives for the residue field R/N.

Then, every element $r \in R$ can be written uniquely as

$$r = r_0 + r_1\pi + r_2\pi^2 + \cdots + r_{\ell-1}\pi^{s-1}$$

where $r_i \in F$.

This is known as the π-adic decomposition.

Ex: over $\mathbb{Z}_8$, $5 = 1 + 0 \cdot 2 + 1 \cdot 2^2$.

Finite Chain Rings: Element Degree

Definition

The degree, $\deg(r)$, of a nonzero element $r \in R^*$, where

$$r = r_0 + r_1\pi + \cdots + r_{s-1}\pi^{s-1},$$

is defined as the *least* index j for which $r_j \neq 0$.

- by convention, $\deg(0) = s$
- units have degree zero
- a divides b if and only if $\deg(a) \leq \deg(b)$

Finite Chain Rings: Element Degree

Definition

The degree, $\deg(r)$, of a nonzero element $r \in R^*$, where

$$r = r_0 + r_1\pi + \cdots + r_{s-1}\pi^{s-1},$$

is defined as the *least* index j for which $r_j \neq 0$.

- by convention, $\deg(0) = s$
- units have degree zero
- a divides b if and only if $\deg(a) \leq \deg(b)$

For example, over $\mathbb{Z}_8$:

deg.	elements
0	$\{1, 3, 5, 7\}$
1	$\{2, 6\}$
2	$\{4\}$
3	$\{0\}$

Matrices over Finite Chain Rings: Reduced Row Echelon Form

We need an appropriate generalization of RREF.

The presence of zero divisors complicates the matters...

- Over a field, two matrices in echelon form with the same row span will have the same number of nonzero rows—the rank.
- Over a chain ring, this is not the case.

For example, the matrices

$$\begin{bmatrix} 2 & 1 & 1 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 2 & 1 & 1 & 2 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 2 & 2 \end{bmatrix} \text{ over } \mathbb{Z}_8$$

have the same row span but not the same number of nonzero rows. So, generalization of RREF seems non-trivial.

Matrices over Finite Chain Rings: Reduced Row Echelon Form

We need an appropriate generalization of RREF.

There are two matrix canonical forms that generalize RREF:

- Fuller, "A canonical set for matrices over a principal ideal ring modulo m," Canad. J. Math, 54–59, 1954.
- Howell, "Spans in the module $\mathbb{Z}_m^s$," Linear and Multilinear Algebra, 19:1, 67–77, 1986.

Matrices over Finite Chain Rings: Reduced Row Echelon Form

We need an appropriate generalization of RREF.

There are two matrix canonical forms that generalize RREF:

- Fuller, "A canonical set for matrices over a principal ideal ring modulo m," Canad. J. Math, 54–59, 1954.
- Howell, "Spans in the module $\mathbb{Z}_m^s$," Linear and Multilinear Algebra, 19:1, 67–77, 1986.

Example: the matrices

$$\begin{bmatrix} 2 & 1 & 1 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 2 & 1 & 1 & 2 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 2 & 2 \end{bmatrix} \text{ over } \mathbb{Z}_8$$

are Fuller and Howell canonical forms, respectively.

Matrices over Finite Chain Rings: Row Canonical Form

Definition

A matrix A is in **row canonical form** if it satisfies the following conditions.

1. Nonzero rows of A are above any zero rows.
2. The pivot of a row is of the form π^ℓ, and is the leftmost entry of the least degree.
3. For every pivot (say π^ℓ), all entries below and in the same column as the pivot are zero, and all entries above and in the same column as the pivot are residues of π^ℓ.
4. If A has two pivots of the same degree, the one that occurs earlier is above the one that occurs later. If A has two pivots of different degree, the one with smaller degree is above the one with larger degree.

For example, over $\mathbb{Z}_8$,

$$A = \begin{bmatrix} 0 & 2 & 0 & \bar{1} \\ \bar{2} & 2 & 0 & 0 \\ 0 & 0 & \bar{2} & 0 \\ 0 & \bar{4} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

is in row canonical form.

∗For details, see our paper and/or Kiermaier's thesis (in German).

Reduction to Row Canonical Form: Example

Reduction is a variant of **Gaussian elimination**.

An example over $\mathbb{Z}_8$:

$$A = \begin{bmatrix} 4 & 6 & 2 & \bar{1} \\ 0 & 0 & 0 & 2 \\ 2 & 4 & 6 & 1 \\ 2 & 0 & 2 & 1 \end{bmatrix} \rightarrow A_1 = \begin{bmatrix} 4 & 6 & 2 & 1 \\ 0 & 4 & 4 & 0 \\ \bar{6} & 6 & 4 & 0 \\ 6 & 2 & 0 & 0 \end{bmatrix} \rightarrow$$

$$A_1' = \begin{bmatrix} 4 & 6 & 2 & 1 \\ \bar{2} & 2 & 4 & 0 \\ 0 & 4 & 4 & 0 \\ 6 & 2 & 0 & 0 \end{bmatrix} \rightarrow A_2 = \begin{bmatrix} 0 & 2 & 2 & 1 \\ 2 & 2 & 4 & 0 \\ 0 & \bar{4} & 4 & 0 \\ 0 & 4 & 4 & 0 \end{bmatrix} \rightarrow$$

$$A_3 = \begin{bmatrix} 0 & 2 & 2 & \bar{1} \\ \bar{2} & 2 & 4 & 0 \\ 0 & \bar{4} & 4 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$ which is in row canonical form.

Row canonical form is not necessarily an echelon form!

Matrices over Finite Chain Rings: Smith Normal Form

Theorem

For any $A \in R^{n\times m}$, A can be decomposed as

$$A = PDQ,$$

for some invertible $n \times n$ and $m \times m$ matrices P and Q, where $D = \text{diag}(\pi^{t_1}, \ldots, \pi^{t_k})$ with $t_1 \leq \cdots \leq t_k$ and $k = \min\{n, m\}$.

Ex: $R = \mathbb{Z}_8$

$$D = \begin{bmatrix} 3 & & \\ 3 & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} 4 & 6 & 3 \\ 4 & 6 & 7 \\ & & \end{bmatrix} \begin{bmatrix} & & 1 \\ & 1 & \\ 1 & 6 & 4 \end{bmatrix} = \begin{bmatrix} 1 & & \\ & 0 & \\ & & 0 \end{bmatrix}.$$

Remark: The diagonal entries in D are precisely the pivots of the row canonical form of A

Shape of a Matrix

The shape is a tuple of non-decreasing integers.

Example: $\mu = (3,5)$

$$\begin{matrix} * & * & * \\ * & * & * & * & * \end{matrix}$$

$$R^{\mu} = \underbrace{\langle 1\rangle \times \cdots \times \langle 1\rangle}_{\mu_1} \times \underbrace{\langle \pi\rangle \times \cdots \times \langle \pi\rangle}_{\mu_2-\mu_1} \times \cdots \times \underbrace{\langle \pi^{s-1}\rangle \times \cdots \times \langle \pi^{s-1}\rangle}_{\mu_s-\mu_{s-1}}.$$

Shape of a Matrix

The shape is a tuple of non-decreasing integers.

Example: $\mu = (3,5)$

$$\begin{matrix} * & * & * \\ * & * & * & * & * \end{matrix}$$

$$R^\mu = \underbrace{\langle 1\rangle \times \cdots \times \langle 1\rangle}_{\mu_1} \times \underbrace{\langle \pi\rangle \times \cdots \times \langle \pi\rangle}_{\mu_2-\mu_1} \times \cdots \times \underbrace{\langle \pi^{s-1}\rangle \times \cdots \times \langle \pi^{s-1}\rangle}_{\mu_s-\mu_{s-1}}.$$

The shape of a module generalizes the concept of dimension.

Theorem

For any finite R-module M, there is a unique μ such that $M \cong R^\mu$.

We call μ the shape of M, and write $\mu = \operatorname{shape} M$.

Shape of a Matrix

The shape is a tuple of non-decreasing integers.

Example: $\mu = (3,5)$

$$\begin{matrix} * & * & * \\ * & * & * & * & * \end{matrix}$$

$$R^\mu = \underbrace{\langle 1\rangle \times \cdots \times \langle 1\rangle}_{\mu_1} \times \underbrace{\langle \pi\rangle \times \cdots \times \langle \pi\rangle}_{\mu_2-\mu_1} \times \cdots \times \underbrace{\langle \pi^{s-1}\rangle \times \cdots \times \langle \pi^{s-1}\rangle}_{\mu_s-\mu_{s-1}}.$$

The shape of a module generalizes the concept of dimension.

Theorem

For any finite R-module M, there is a unique μ such that $M \cong R^\mu$.

We call μ the shape of M, and write $\mu = \operatorname{shape} M$.

The shape of a matrix generalizes the concept of rank.

Definition

The shape of a matrix A is defined as the shape of the row span of A, i.e., $\operatorname{shape} A = \operatorname{shape}(\operatorname{row}(A))$.

Properties of the Shape

Matrix shape has several properties similar to matrix rank:

1. shape A = shape A^T.
2. For any invertible P, Q, shape A = shape PAQ.
3. shape $AB \preceq$ shape A, shape $AB \preceq$ shape B.
4. For any submatrix C of A, shape $C \preceq$ shape A.

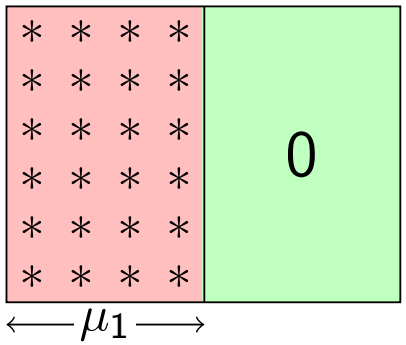
Enumeration Results

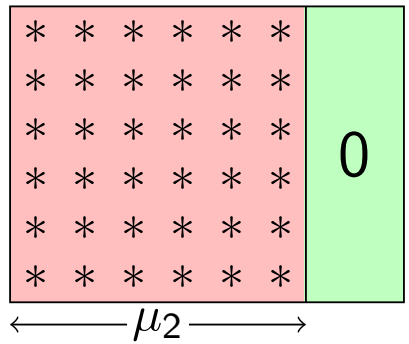
Notation

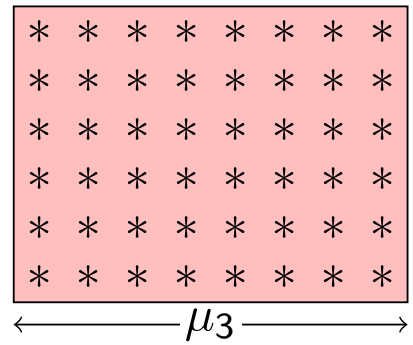
$R^{n\times\mu}$: The subset of matrices in $R^{n\times m}$ whose rows $\in R^{\mu}$.

- $|R^{n\times\mu}| = q^{n(\mu_1+\cdots+\mu_s)}$.

Example: $R = \mathbb{Z}_8$, $n = 6$, $\mu = (4, 6, 8)$, $X = X_0 + 2X_1 + 4X_2$

$X_0 =$ 

$X_1 =$ 

$X_2 =$ 

Enumeration Results

Notation

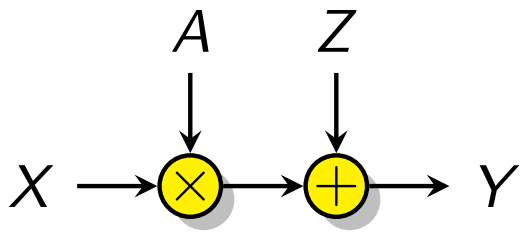
$\mathcal{T}_\tau(R^{n\times\mu})$: The subset of matrices in $R^{n\times\mu}$ whose shape is τ.

- $|\mathcal{T}_\tau(R^{n\times\mu})| = \begin{bmatrix}\mu\\ \tau\end{bmatrix}_q |R^{n\times\tau}| \prod_{i=0}^{\tau_s-1}(1-q^{i-n})$, where

$$\begin{bmatrix}\mu\\ \tau\end{bmatrix}_q = \prod_{i=1}^{s} q^{(\mu_i-\tau_i)\tau_{i-1}} \begin{bmatrix}\mu_i-\tau_{i-1}\\ \tau_i-\tau_{i-1}\end{bmatrix}_q,$$

and $\begin{bmatrix}m\\ k\end{bmatrix}_q$ is the Gaussian coefficient.

Back to Our Objective



$$Y = AX + Z$$

where

$$X, Y, Z \in R^{n \times \mu}$$

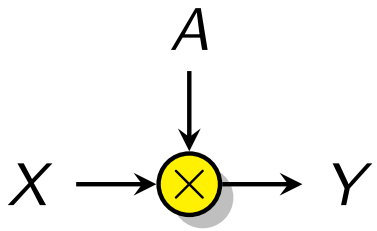
Objective:

- Capacity bounds
- Simple coding schemes

Multiplicative Matrix Channel

First warmup problem

The multiplicative matrix channel (MMC):



$$Y = AX$$

where

- $X, Y \in R^{n \times \mu}$;
- A: invertible, uniform;
- A and X are independent.

MMC: Review of [SKK10]

When R reduces to $\mathbb{F}_q$ and $R^{n\times\mu}$ reduces to $\mathbb{F}_q^{n\times m}$:

1. Exact capacity: A preserves the row span, so

$$C_{\mathsf{MMC}} = \log_q \left(\#\text{ of subspaces of } \mathbb{F}_q^m\right)$$

2. Capacity-achieving code: reduced row echelon form (RREF)

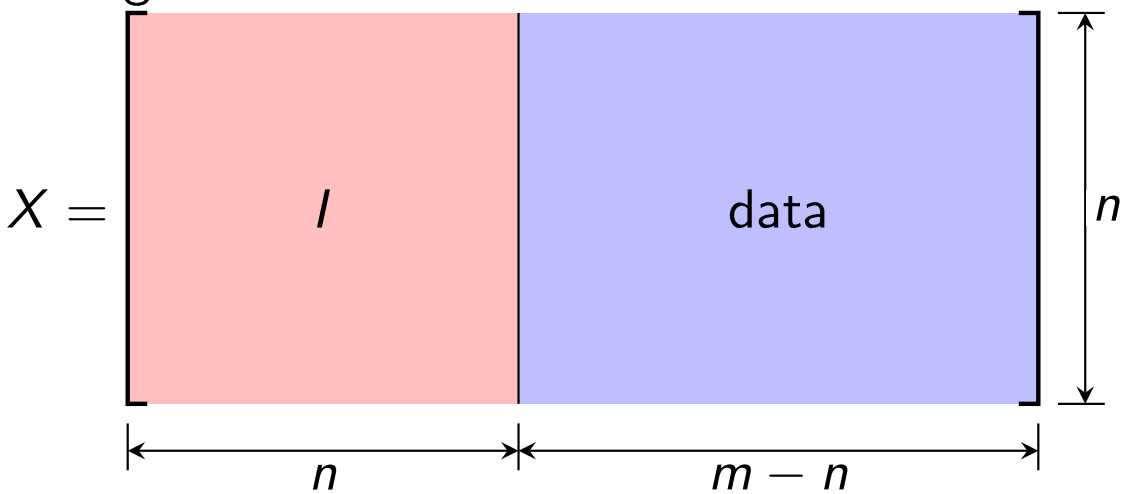
MMC: Review of [SKK10]

When R reduces to $\mathbb{F}_q$ and $R^{n\times\mu}$ reduces to $\mathbb{F}_q^{n\times m}$:

1. Exact capacity: A preserves the row span, so

$$C_{\mathrm{MMC}} = \log_q \left(\#\text{ of subspaces of } \mathbb{F}_q^m\right)$$

2. Capacity-achieving code: reduced row echelon form (RREF)
3. Efficient encoding-decoding:
   - encoding:



   - decoding: Gaussian elimination (reduction to RREF)

MMC: Exact Capacity

Theorem

The capacity of the MMC, in q-ary symbols per channel use, is

$$C_{\mathrm{MMC}} = \log_q \left(\#\text{ of submodules of } R^{\mu}\right).$$

$\#$ of submodules of R^{μ} is $\sum_{\lambda \preceq n,\mu} \left[\!\!\left[{\mu \atop \lambda} \right]\!\!\right]_q$ (see, e.g., [HL00][4]}), where

$$\left[\!\!\left[{\mu \atop \lambda} \right]\!\!\right]_q = \prod_{i=1}^{s} q^{(\mu_i - \lambda_i)\lambda_{i-1}} \begin{bmatrix} \mu_i - \lambda_{i-1} \\ \lambda_i - \lambda_{i-1} \end{bmatrix}_q,$$

and $\begin{bmatrix} m \\ k \end{bmatrix}_q$ is the Gaussian coefficient.

- note: $\lambda \preceq n, \mu$ means $\forall i,\ \lambda_i \leq n, \mu_i$

[4] Honold and Landjev, "Linear Codes over Finite Chain Rings," *The Electronic J. of Combinatorics*, vol. 7, 2000.

MMC: Efficient Encoding-Decoding

First attempt:

- Encoding: transmit a row canonical form (RCF)
- Decoding: reduction to RCF

The decoding complexity is $\mathcal{O}(n^2 m)$, but the encoding is hard.

Solution:

- Encoding: transmit a **principal** RCF
- Decoding: reduction to RCF

The encoding complexity is $\mathcal{O}(nm)$.
Principal RCFs occupy a significant portion of all RCFs.

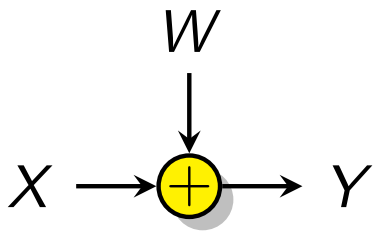
Hence,

The simple coding scheme asymptotically achieves the capacity.

Additive Matrix Channel

Second warmup problem

The additive matrix channel (AMC):



$$Y = X + W$$

where

- $X, Y \in R^{n \times \mu}$;
- W: shape τ, uniform;
- W and X are independent.

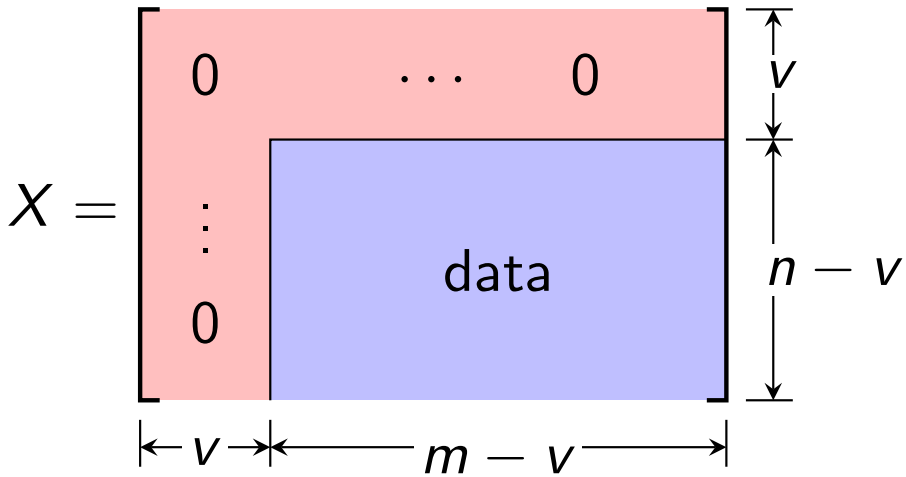
AMC: Review of [SKK10]

When R reduces to $\mathbb{F}_q$ and $R^{n\times\mu}$ reduces to $\mathbb{F}_q^{n\times m}$, shape τ reduces to rank t:

1. Exact capacity: a discrete symmetric channel

$$C_{\mathrm{AMC}} = nm - \log_q\left(\#\text{ of matrices of rank } t \text{ in } \mathbb{F}_q^{n\times m}\right)$$

2. Capacity-approaching code: v is a parameter



3. Efficient encoding-decoding:
   - encoding: error trapping
   - decoding: matrix completion

AMC: Exact Capacity

The AMC is an example of a discrete symmetric channel.

Theorem

The capacity of the AMC, in q-ary symbols per channel use, is

$$C_{\text{AMC}} = \log_q |R^{n\times\mu}| - \log_q |\mathcal{T}_\tau(R^{n\times\mu})|.$$

We need the following:

- $|R^{n\times\mu}| = q^{n(\mu_1+\cdots+\mu_s)}$.
- $|\mathcal{T}_\tau(R^{n\times\mu})| = \left[\!\!\left[\begin{matrix} \mu \\ \tau \end{matrix} \right]\!\!\right]_q |R^{n\times\tau}| \prod_{i=0}^{\tau_s-1}(1-q^{i-n})$, where

$$\left[\!\!\left[\begin{matrix} \mu \\ \tau \end{matrix} \right]\!\!\right]_q = \prod_{i=1}^{s} q^{(\mu_i-\tau_i)\tau_{i-1}} \begin{bmatrix} \mu_i - \tau_{i-1} \\ \tau_i - \tau_{i-1} \end{bmatrix}_q.$$

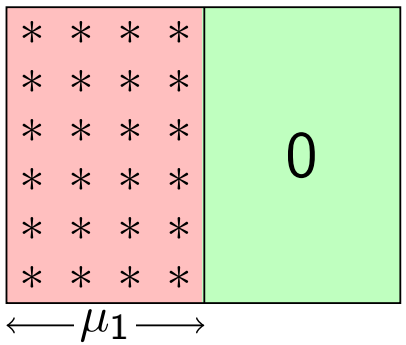
AMC: Capacity-Approaching Code Design

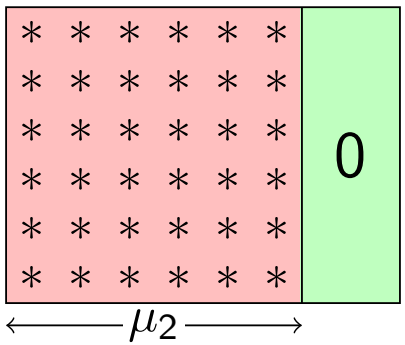
code design problem $\Rightarrow$ a generalization of error-trapping

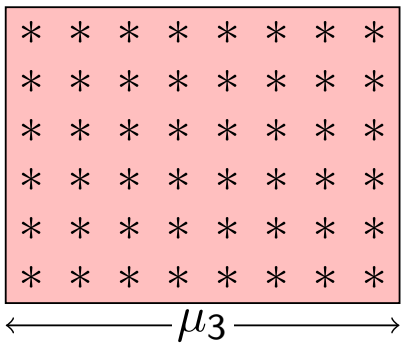
Solution: layered error-trapping

Note that every matrix in $R^{n\times\mu}$ admits a π-adic decomposition.

Example: $R = \mathbb{Z}_8$, $n = 6$, $\mu = (4, 6, 8)$, $X = X_0 + 2X_1 + 4X_2$

$X_0 =$ 

$X_1 =$ 

$X_2 =$ 

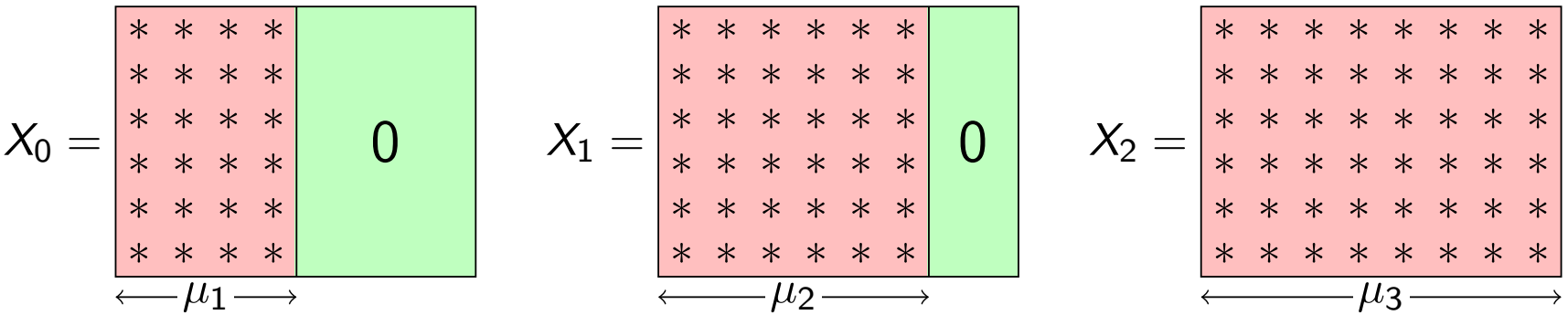
AMC: Capacity-Approaching Code Design

code design problem $\Rightarrow$ a generalization of error-trapping

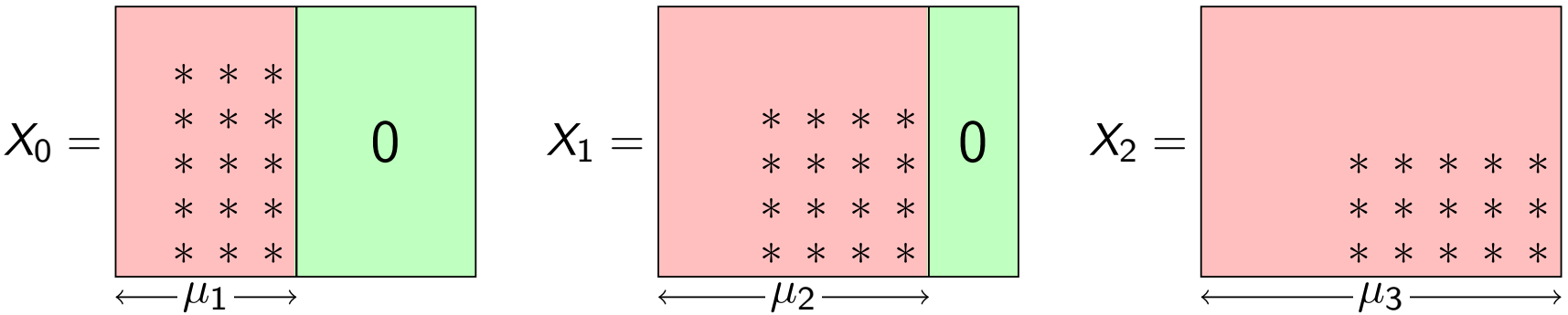
Solution: layered error-trapping

Note that every matrix in $R^{n\times\mu}$ admits a π-adic decomposition.

Example: $R = \mathbb{Z}_8$, $n = 6$, $\mu = (4, 6, 8)$, $X = X_0 + 2X_1 + 4X_2$



after error-trapping...



AMC: Efficient Encoding-Decoding

- Encoding: layered error-trapping, $\mathcal{O}(nm)$ complexity
- Decoding: multistage matrix completion, $\mathcal{O}(n^2 m)$ complexity

Example: $R = \mathbb{Z}_8$, $X = X_0 + 2X_1 + 4X_2$. Note that

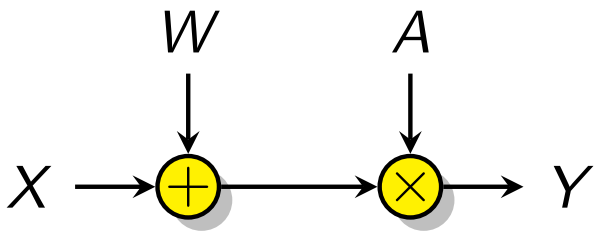
$$Y = X + W = X_0 + 2X_1 + 4X_2 + W.$$

1. Take mod 2: $[Y]_2 = X_0 + [W]_2$.
2. Decode X_0 by completing $[W]_2$.
3. Clear X_0 from Y: $Y' = Y - X_0 = 2X_1 + 4X_2 + W$.
4. Take mod 4: $[Y']_4 = 2X_1 + [W]_4$.
5. Decode $2X_1$ by completing $[W]_4$.
6. Clear X_1 from Y': $Y'' = Y' - 2X_1 = 4X_2 + W$.
7. We have $Y'' = 4X_2 + W$.
8. Decode $4X_2$ by completing W.

Additive-Multiplicative Matrix Channel

Now to the main event:

The additive-multiplicative matrix channel (AMMC):



$$Y = A(X + W)$$

where

- $X, Y \in R^{n \times \mu}$;
- A: invertible, uniform;
- W: shape τ, uniform;
- A, X and W are independent.

Remark: This model is statistically identical to $Y = AX + Z$.

AMMC: Upper Bound on Capacity

Theorem

The capacity of the AMMC, in q-ary symbols per channel use, is upper-bounded by

$$C_{\mathrm{AMMC}} \leq \sum_{i=1}^{s}(\mu_i - \xi_i)\xi_i + \sum_{i=1}^{s}(n-\mu_i)\tau_i + 2s\log_q 4 + \log_q \binom{n+s}{s}$$

$$+ \log_q \binom{\tau_s+s}{s} - \log_q \prod_{i=0}^{\tau_s-1}(1-q^{i-n}), \text{ where } \xi_i = \min\{n, \lfloor \mu_i/2 \rfloor\}.$$

In particular, when $\mu \succeq 2n$, the upper bound reduces to

$$C_{\mathrm{AMMC}} \leq \sum_{i=1}^{s}(n-\tau_i)(\mu_i - n) + 2s\log_q 4$$

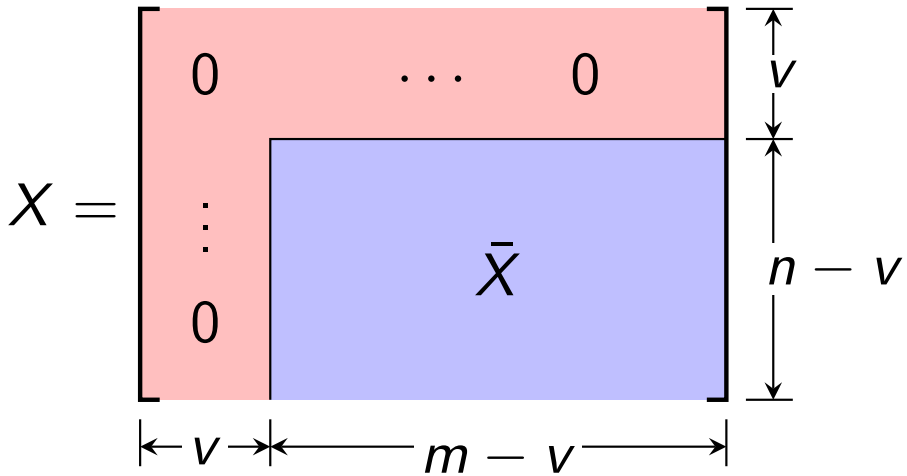
$$+ \log_q \binom{n+s}{s} + \log_q \binom{\tau_s+s}{s} - \log_q \prod_{i=0}^{\tau_s-1}(1-q^{i-n}).$$

AMMC: Coding Scheme

coding scheme = principal RCFs + layered error-trapping

However, the combination turns out to be non-trivial.
Hence, we focus on the special case when $\tau = (t, \ldots, t)$.

- Encoding:



- Decoding: upon receiving $Y = A(X + W)$, the decoder simply computes the RCF of Y, which exposes $\bar{X}$ with high probability.

This simple coding scheme asymptotically achieves the capacity for the special case when $\tau = (t, \ldots, t)$ and $\mu \succeq 2n$.

Concluding Remarks

1. New motivations
2. "User-friendly" tools
3. Need more workshops like this

Construction of Principal RCFs

Definition

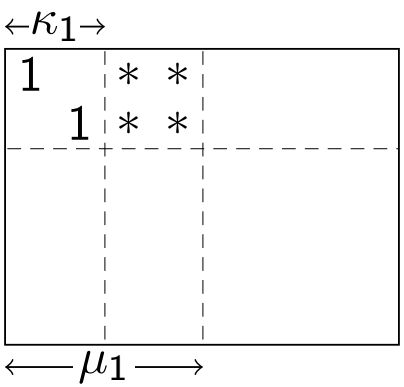
A row canonical form in $\mathcal{T}_\kappa(R^{n\times\mu})$ is called *principal* if its diagonal entries $d_1, d_2, \ldots, d_r$ $(r = \min\{n, m\})$ have the following form:

$$d_1, \ldots, d_r = \underbrace{1, \ldots, 1}_{\kappa_1}, \underbrace{\pi, \ldots, \pi}_{\kappa_2-\kappa_1}, \ldots, \underbrace{\pi^{s-1}, \ldots, \pi^{s-1}}_{\kappa_s-\kappa_{s-1}}, \underbrace{0, \ldots, 0}_{r-\kappa_s}.$$

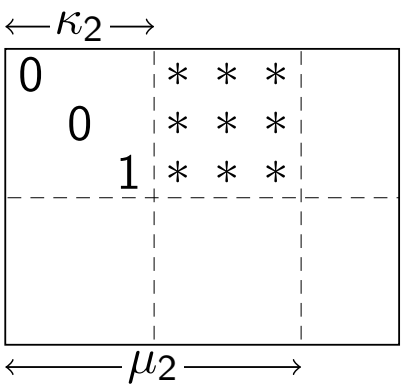
All principal RCFs in $\mathcal{T}_\kappa(R^{n\times\mu})$ can be constructed via a π-adic decomposition $X = X_0 + \pi X_1 + \cdots + \pi^{s-1}X_{s-1}$.

Example: $s = 3$, $n = 6$, $\mu = (4, 6, 8)$, and $\kappa = (2, 3, 4)$

$X_0 =$



$X_1 =$



$X_2 =$