Course on (algebraic aspects of) Convolutional Codes

Diego Napp

Department of Mathematics, Universidad of Aveiro, Portugal

CENTRO DE I&D EM MATEMÁTICA E APLICAÇÕES
CENTER FOR R&D IN MATHEMATICS AND APPLICATIONS

CIMPA RESEARCH SCHOOL

July 6, 2017

My most heartfelt thanks to the organizers

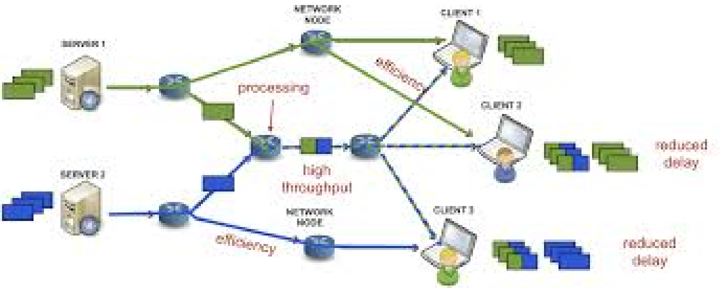
CIMPA RESEARCH SCHOOL

ALGEBRAIC METHODS IN CODING THEORY

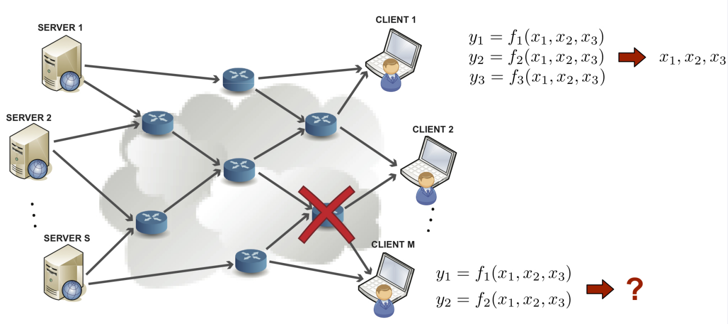
Overview

1. Error-correcting codes: From block codes to convolutional codes
   - Basics: Polynomial encoders
2. Distance properties of convolutional codes
   - Maximum Distance Profile (MDP) and Maximum Distance Separable (MDS)
   - Construction of MDP and MDS: Superregular matrices
3. Decoding of Convolutional codes
   - Viterbi algorithm
   - Decoding of convolutional codes over the erasure channel
4. Network coding with convolutional codes
5. Avenues for further research
   - Motivated by applications: Video streaming and storage systems
   - More theoretical: Multidimensional convolutional codes and convolutional codes over $\mathbb{Z}_{p^r}$

Day 4: Convolutional codes for Network coding



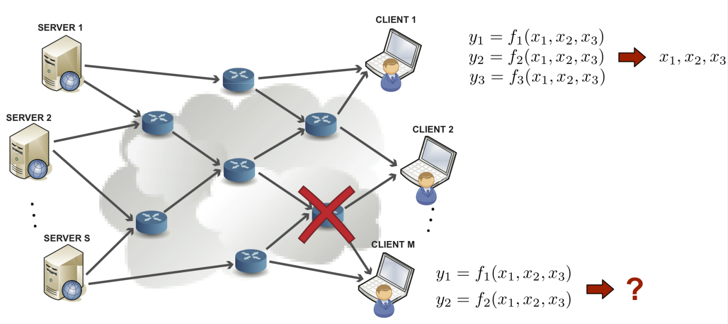
Network Coding



We live in a network world.

How is the best way to disseminate information over a network?

Network Coding



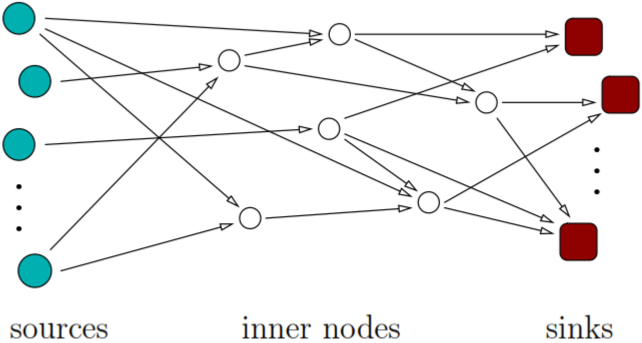
We live in a network world.

How is the best way to disseminate information over a network?

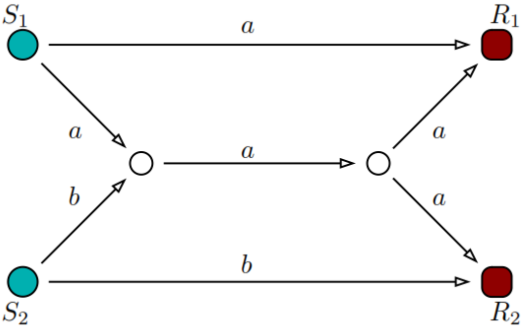
Linear random network coding

It has been proven that network coding is enough to achieve the upper bound in multicast problems with one or more sources. It optimizes the throughput.

Linear Network Coding

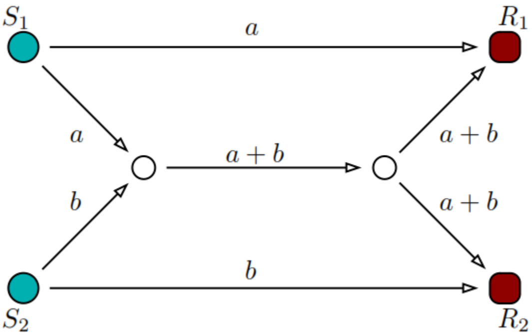


Example (The Butterfly Network):

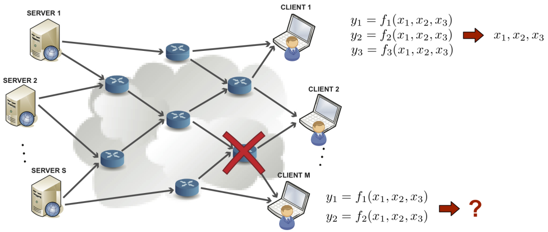


Linear Network Coding

Example (The Butterfly Network):

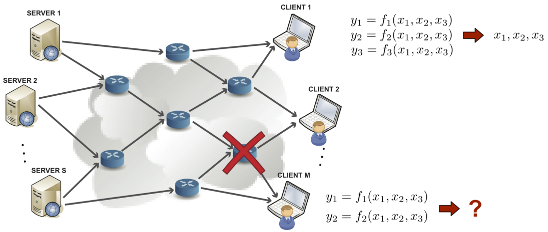


Linear Network Coding



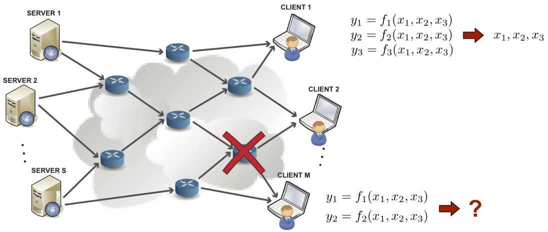
- During one *shot* the transmitter injects a number of packets into the network, each of which may be regarded as a row vector over a finite field $\mathbb{F}_{q^m}$.

Linear Network Coding



- During one *shot* the transmitter injects a number of packets into the network, each of which may be regarded as a row vector over a finite field $\mathbb{F}_{q^m}$.
- These packets propagate through the network. Each node creates a random -linear combination of the packets it has available and transmits this random combination.

Linear Network Coding



- During one *shot* the transmitter injects a number of packets into the network, each of which may be regarded as a row vector over a finite field $\mathbb{F}_{q^m}$.
- These packets propagate through the network. Each node creates a random -linear combination of the packets it has available and transmits this random combination.
- Finally, the receiver collects such randomly generated packets and tries to infer the set of packets injected into the network

- Subspaces remain the same under any linear operations on the basis

- Subspaces remain the same under any linear operations on the basis
- Subspace codes recently received a lot of attention since Koetter and Kschischang showed (in a award winning paper in 2008) that they are exactly what is needed for error-correction in random network coding.

- Subspaces remain the same under any linear operations on the basis
- Subspace codes recently received a lot of attention since Koetter and Kschischang showed (in a award winning paper in 2008) that they are exactly what is needed for error-correction in random network coding.
- The generalized projective space $\mathcal{P}_q(n)$ of order n over $\mathbb{F}_q$ is the set of all subspaces of $\mathbb{F}_q^n$. The set of all subspaces of dimension k is the Grassmannian $\mathcal{G}_q(k, n)$.

- Subspaces remain the same under any linear operations on the basis
- Subspace codes recently received a lot of attention since Koetter and Kschischang showed (in a award winning paper in 2008) that they are exactly what is needed for error-correction in random network coding.
- The generalized projective space $\mathcal{P}_q(n)$ of order n over $\mathbb{F}_q$ is the set of all subspaces of $\mathbb{F}_q^n$. The set of all subspaces of dimension k is the Grassmannian $\mathcal{G}_q(k,n)$.
- A metric on $\mathcal{P}_q(n)$ is given by

$$d_S(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V)$$

- Subspaces remain the same under any linear operations on the basis
- Subspace codes recently received a lot of attention since Koetter and Kschischang showed (in a award winning paper in 2008) that they are exactly what is needed for error-correction in random network coding.
- The generalized projective space $\mathcal{P}_q(n)$ of order n over $\mathbb{F}_q$ is the set of all subspaces of $\mathbb{F}_q^n$. The set of all subspaces of dimension k is the Grassmannian $\mathcal{G}_q(k,n)$.
- A metric on $\mathcal{P}_q(n)$ is given by

$$d_S(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V)$$

- On $\mathcal{G}_q(k,n)$ it turns to

$$d_S(U,V) = 2(k - \dim(U \cap V))$$

- Subspaces remain the same under any linear operations on the basis
- Subspace codes recently received a lot of attention since Koetter and Kschischang showed (in a award winning paper in 2008) that they are exactly what is needed for error-correction in random network coding.
- The generalized projective space $\mathcal{P}_q(n)$ of order n over $\mathbb{F}_q$ is the set of all subspaces of $\mathbb{F}_q^n$. The set of all subspaces of dimension k is the Grassmannian $\mathcal{G}_q(k, n)$.
- A metric on $\mathcal{P}_q(n)$ is given by

$$d_S(U, V) = \dim(U) + \dim(V) - 2\dim(U \cap V)$$

- On $\mathcal{G}_q(k, n)$ it turns to

$$d_S(U, V) = 2(k - \dim(U \cap V))$$

- A subspace code is simply a subset of $\mathcal{P}_q(n)$, a constant dimension code (CDC) is a subset of $\mathcal{G}_q(k, n)$. If the distance between any two elements of a CDC is greater than or equal to 2 we say that the code has minimum distance 2

Rank metric codes are used in Network Coding

- Silva, Kschischang, and Koetter show that the subspace distance between $U = \text{rowspan}[I \quad A]$ and $V = \text{rowspan}[I \quad B]$ is

$$d_S(U, V) = 2 \text{ rank } (A - B)$$

Rank metric codes are used in Network Coding

- Silva, Kschischang, and Koetter show that the subspace distance between $U = \text{rowspan}[I \quad A]$ and $V = \text{rowspan}[I \quad B]$ is

$$d_S(U, V) = 2 \text{ rank } (A - B)$$

- Rank metric code: a block code over $\mathbb{F}_{q^m}$, where each codeword v is associated with a matrix $\phi(v)$; row i of $\phi(v)$ is the expansion of v_i w.r.t. a fixed basis for $\mathbb{F}_{q^m}$ over Fq.

Rank metric codes are used in Network Coding

- Silva, Kschischang, and Koetter show that the subspace distance between $U = \text{rowspan}[I \quad A]$ and $V = \text{rowspan}[I \quad B]$ is

$$d_S(U, V) = 2 \text{ rank } (A - B)$$

- Rank metric code: a block code over $\mathbb{F}_{q^m}$, where each codeword v is associated with a matrix $\phi(v)$; row i of $\phi(v)$ is the expansion of v_i w.r.t. a fixed basis for $\mathbb{F}_{q^m}$ over Fq.
- Since $\mathbb{F}_q^{m\times n} \cong \mathbb{F}_{q^m}^n$, any rank-metric code over the extension field can also be considered as a matrix code over the base field.

Rank metric codes are used in Network Coding

- Silva, Kschischang, and Koetter show that the subspace distance between $U = \text{rowspan}[I \quad A]$ and $V = \text{rowspan}[I \quad B]$ is

$$d_S(U, V) = 2 \text{ rank } (A - B)$$

- Rank metric code: a block code over $\mathbb{F}_{q^m}$, where each codeword v is associated with a matrix $\phi(v)$; row i of $\phi(v)$ is the expansion of v_i w.r.t. a fixed basis for $\mathbb{F}_{q^m}$ over Fq.
- Since $\mathbb{F}_q^{m\times n} \cong \mathbb{F}_{q^m}^n$, any rank-metric code over the extension field can also be considered as a matrix code over the base field.
- Rank metric codes are matrix codes $\mathcal{C} \subset \mathbb{F}_q^{m\times n}$, armed with the rank distance

$$d_{\text{rank}}(X, Y) = rank(X - Y), \text{ where } X, Y \in \mathbb{F}_q^{n\times m}.$$

Rank metric codes are used in Network Coding

- For linear (n, k) rank metric codes over $\mathbb{F}_{q^m}$ with $m \geq n$ the following analog of the Singleton bound holds,

$$d_{\text{rank}}(\mathcal{C}) \leq n - k + 1.$$

Rank metric codes are used in Network Coding

- For linear (n, k) rank metric codes over $\mathbb{F}_{q^m}$ with $m \geq n$ the following analog of the Singleton bound holds,

$$d_{\mathrm{rank}}(\mathcal{C}) \leq n - k + 1.$$

- The code that achieves this bound is called Maximum Rank Distance (MRD). Gabidulin codes are a well-known class of MRD codes.

Rank metric codes are used in Network Coding

- For linear (n, k) rank metric codes over $\mathbb{F}_{q^m}$ with $m \geq n$ the following analog of the Singleton bound holds,

$$d_{\mathrm{rank}}(\mathcal{C}) \leq n - k + 1.$$

- The code that achieves this bound is called Maximum Rank Distance (MRD). Gabidulin codes are a well-known class of MRD codes.
- We will assume $n \leq m$ and study MRD codes $\mathcal{C} \subset \mathbb{F}_q^{m\times n}$ that are $\mathbb{F}_{q^m}$-linear. These codes have a generator matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ and a respective parity check matrix $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$.

Example

Let $\mathbb{F}_2^2 = \mathbb{F}_2[\alpha]$ and

$$G = (1, \alpha).$$

Then the code generated by G is

$$C = \{(0,0),(1,\alpha),(\alpha,\alpha^2),(\alpha^2,1)\}$$

$$\cong \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Theorem (Gabidulin)

Let $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ be a parity check matrix of the code C. Then C is MRD if and only if

$$\operatorname{rank}(VH^T) = n - k$$

for all $V \in \mathbb{F}_q^{(n-k)\times n}$ with $\operatorname{rank}(V) = n - k$.

Simplification: Since $\mathrm{GL}_{n-k}(q)$ does not change the rank of VH^T, it suffices to check the rank property for all elements of the left orbit of H^T under $\mathcal{G}_q(n-k, n)$ (i.e. only V in reduced row echelon form).

Theorem

A generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ gives rise to an MRD code if and only if any element of the orbit of G under $\mathrm{GL}_n(q)$ has only non-zero maximal minors.

Simplification: Instead of all of $\mathrm{GL}_n(q)$ it suffices to study the orbit of the subgroup of

- the upper triangular matrices (since swapping columns does not change the minors, up to sign)
- with an all-1 diagonal (since multiplying columns of the generator matrix with $\mathbb{F}_q^*$-scalars does not change the non-zero property of the minors).

Definition

Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. The code with generator matrix

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_n^{q^2} \\ \vdots & \vdots & & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix}$$

is called a *Gabidulin code* of length n and dimension k.

Theorem

Gabidulin codes are MRD codes.

THE IDEA: Multi-shot

- Coding can also be performed over multiple uses of the network, whose internal structure may change at each shot

THE IDEA: Multi-shot

- Coding can also be performed over multiple uses of the network, whose internal structure may change at each shot
- Creating dependencies among the transmitted codewords of different shots can improve the error-correction capabilities (Nobrega, R., Uchoa-Filho (2010), Wachter-Zeh, A., Stinner, M., Sidorenko (2015), Mahmood, R., Badr, A., Khisti(2015)).

THE IDEA: Multi-shot

- Coding can also be performed over multiple uses of the network, whose internal structure may change at each shot
- Creating dependencies among the transmitted codewords of different shots can improve the error-correction capabilities (Nobrega, R., Uchoa-Filho (2010), Wachter-Zeh, A., Stinner, M., Sidorenko (2015), Mahmood, R., Badr, A., Khisti(2015)).
- Ideal coding techniques for streaming communications must operate sequential encoding and decoding constrains, and as such they must inherently have a convolutional structure.

THE IDEA: Multi-shot

- Coding can also be performed over multiple uses of the network, whose internal structure may change at each shot
- Creating dependencies among the transmitted codewords of different shots can improve the error-correction capabilities (Nobrega, R., Uchoa-Filho (2010), Wachter-Zeh, A., Stinner, M., Sidorenko (2015), Mahmood, R., Badr, A., Khisti(2015)).
- Ideal coding techniques for streaming communications must operate sequential encoding and decoding constrains, and as such they must inherently have a convolutional structure.
- We propose the use of convolutional codes to add complex dependencies to data streams in a quite simple way.

THE IDEA: Multi-shot

- Coding can also be performed over multiple uses of the network, whose internal structure may change at each shot
- Creating dependencies among the transmitted codewords of different shots can improve the error-correction capabilities (Nobrega, R., Uchoa-Filho (2010), Wachter-Zeh, A., Stinner, M., Sidorenko (2015), Mahmood, R., Badr, A., Khisti(2015)).
- Ideal coding techniques for streaming communications must operate sequential encoding and decoding constrains, and as such they must inherently have a convolutional structure.
- We propose the use of convolutional codes to add complex dependencies to data streams in a quite simple way.
- Although the use of convolutional codes is widespread, its application to video streaming (or using the rank metric) is yet unexplored.

Network streaming problem

- Assume the network is used once at every time instance and j the decoding deadline.

Network streaming problem

- Assume the network is used once at every time instance and j the decoding deadline.
- $A = diag(A_0, A_1, \ldots, A_{t+j})$ is the channel matrix, $A_i \in \mathbb{F}_q^{n \times n}$

Network streaming problem

- Assume the network is used once at every time instance and j the decoding deadline.
- $A = diag(A_0, A_1, \ldots, A_{t+j})$ is the channel matrix, $A_i \in \mathbb{F}_q^{n \times n}$
- $$(y_0, y_1, \ldots, y_{t+j}) = (v_0, v_1, \ldots, v_{t+j}) \begin{pmatrix} A_0 & & \\ & \ddots & \\ & & A_{t+j} \end{pmatrix}$$

Network streaming problem

- Assume the network is used once at every time instance and j the decoding deadline.
- $A = diag(A_0, A_1, \dots, A_{t+j})$ is the channel matrix, $A_i \in \mathbb{F}_q^{n\times n}$
- $$(y_0, y_1, \dots, y_{t+j}) = (v_0, v_1, \dots, v_{t+j}) \begin{pmatrix} A_0 & & \\ & \ddots & \\ & & A_{t+j} \end{pmatrix}$$
- $\mathrm{rank}(A_i) = n$ during a perfect communication. But erasures may occur and rank drops.

Network streaming problem

- Assume the network is used once at every time instance and j the decoding deadline.
- $A = diag(A_0, A_1, \ldots, A_{t+j})$ is the channel matrix, $A_i \in \mathbb{F}_q^{n\times n}$
- $$(y_0, y_1, \ldots, y_{t+j}) = (v_0, v_1, \ldots, v_{t+j}) \begin{pmatrix} A_0 & & \\ & \ddots & \\ & & A_{t+j} \end{pmatrix}$$
- $\mathrm{rank}(A_i) = n$ during a perfect communication. But erasures may occur and rank drops.
- We want to obtain the v_t's

Distance notions

Definition

The *sum rank distance* of $\mathcal{C}$ is defined as

$$d_{SR}(\mathcal{C}) = \min_{0 \neq X(D) \in \mathcal{C}} \text{rank}\,(X(D)) := \min_{0 \neq X(D) \in \mathcal{C}} \sum_{i \geq 0} \text{rank}\,(X_i)$$

where

$$\text{rank}\,(X_i) := \sum_{j=0}^{K-1} \text{rank}\,(X_i^j).$$

And the *column sum rank distance* of $\mathcal{C}$ is defined as

$$d_{SR}^{j}(\mathcal{C}) = \min_{X(D) \in \mathcal{C} \text{ and } X_0^0 \neq 0} \sum_{i=0}^{j} \text{rank}\,(X_i),$$

Convolutional codes maximum Column Rank distance

Theorem [Mahmood, R., Badr, A., Khisti(2015)]

Let $\mathcal{C}$ be a convolutional code with $d_j^c(\mathcal{C}) = d$ and $A = diag(A_0, A_1, \ldots, A_j)$ the channel matrix. If $rank(A) = n(j+1) - d + 1$, then every message v_t is recoverable by time j. Conversely, if rank$A = n(j+1) - d$ then there exists at least one codeword for which x_0 cannot be recovered.

Problem

How do we construct $G(D)$ to achieve the maximum column sum distance??

Thanks for your attention