Multishot Codes for Network Coding using Rank-Metric Codes

Roberto Wanderley da Nóbrega
Bartolomeu Ferreira Uchôa-Filho

Communications Research Group
Department of Electrical Engineering
Federal University of Santa Catarina, Brazil

3rd IEEE International Workshop on Wireless Network Coding
June 21, 2010, Boston, Massachusetts

Table of contents

Table of contents

Table of contents

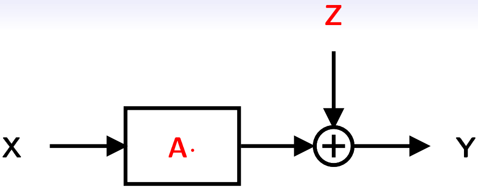
Table of contents

Table of contents

Table of contents

Introduction

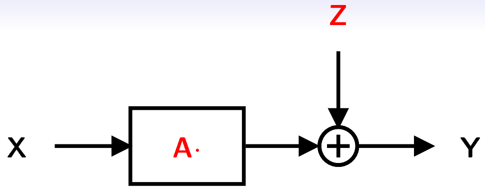
The matrix channel



$$\mathbf{Y} = \mathbf{A} \cdot \mathbf{X} + \mathbf{Z}$$

- Input, output: $\mathbf{X}, \mathbf{Y} \in \mathbb{F}_q^{N \times T}$
- Transfer matrix: $\mathbf{A} \in \mathbb{F}_q^{N \times N}$
  - Unknown in a noncoherent scenario
  - Depends on network topology and coding coefficients
- Error matrix: $\mathbf{Z} \in \mathbb{F}_q^{N \times T}$
  - Related to link errors

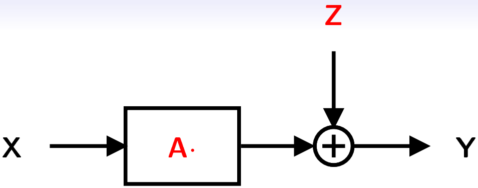
The matrix channel



$$\mathbf{Y} = \mathbf{A} \cdot \mathbf{X} + \mathbf{Z}$$

- Input, output: $\mathbf{X}, \mathbf{Y} \in \mathbb{F}_q^{N \times T}$
- Transfer matrix: $\mathbf{A} \in \mathbb{F}_q^{N \times N}$
  - Unknown in a noncoherent scenario
  - Depends on network topology and coding coefficients
- Error matrix: $\mathbf{Z} \in \mathbb{F}_q^{N \times T}$
  - Related to link errors

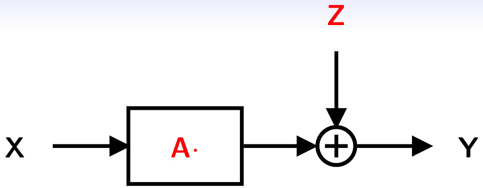
The matrix channel



$$\mathbf{Y} = \mathbf{A} \cdot \mathbf{X} + \mathbf{Z}$$

- Input, output: $\mathbf{X}, \mathbf{Y} \in \mathbb{F}_q^{N \times T}$
- Transfer matrix: $\mathbf{A} \in \mathbb{F}_q^{N \times N}$
  - Unknown in a noncoherent scenario
  - Depends on network topology and coding coefficients
- Error matrix: $\mathbf{Z} \in \mathbb{F}_q^{N \times T}$
  - Related to link errors

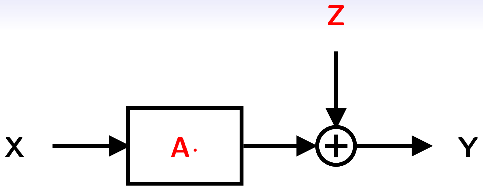
The matrix channel



$$\mathbf{Y} = \mathbf{A} \cdot \mathbf{X} + \mathbf{Z}$$

- Input, output: $\mathbf{X}, \mathbf{Y} \in \mathbb{F}_q^{N \times T}$
- Transfer matrix: $\mathbf{A} \in \mathbb{F}_q^{N \times N}$
  - Unknown in a noncoherent scenario
  - Depends on network topology and coding coefficients
- Error matrix: $\mathbf{Z} \in \mathbb{F}_q^{N \times T}$
  - Related to link errors

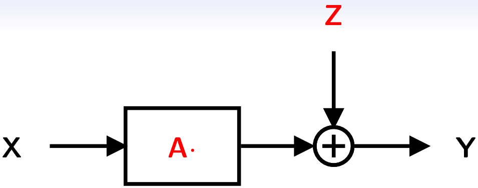
The matrix channel



$$\mathbf{Y} = \mathbf{A} \cdot \mathbf{X} + \mathbf{Z}$$

- Input, output: $\mathbf{X}, \mathbf{Y} \in \mathbb{F}_q^{N \times T}$
- Transfer matrix: $\mathbf{A} \in \mathbb{F}_q^{N \times N}$
  - Unknown in a noncoherent scenario
  - Depends on network topology and coding coefficients
- Error matrix: $\mathbf{Z} \in \mathbb{F}_q^{N \times T}$
  - Related to link errors

The matrix channel



$$\mathbf{Y} = \mathbf{A} \cdot \mathbf{X} + \mathbf{Z}$$

- Input, output: $\mathbf{X}, \mathbf{Y} \in \mathbb{F}_q^{N \times T}$
- Transfer matrix: $\mathbf{A} \in \mathbb{F}_q^{N \times N}$
  - Unknown in a noncoherent scenario
  - Depends on network topology and coding coefficients
- Error matrix: $\mathbf{Z} \in \mathbb{F}_q^{N \times T}$
  - Related to link errors

Coding for this channel

- Subspace coding [Koetter-Kschischang '08]
  - Encode information in the subspace spanned by the rows of $\mathbf{X}$
- Lifting [Silva-K-K '08] a.k.a. channel training [Yang-H-M-Y-Y '10]
  - Special case of subspace coding
  - Roots on Chou's pratical network coding [Chou-W-K '03]
- Approaches (error model)
  - Combinatorial (algebraic)
    [Koetter-Kschischang '08] [Silva-K-K '08] [Silva-K '09]
  - Information-theoretic
    [Montanari-Urbanke '07] [Silva-K-K '10] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]

Coding for this channel

- Subspace coding [Koetter-Kschischang '08]
  - Encode information in the subspace spanned by the rows of $\mathbf{X}$
- Lifting [Silva-K-K '08] a.k.a. channel training [Yang-H-M-Y-Y '10]
  - Special case of subspace coding
  - Roots on Chou's pratical network coding [Chou-W-K '03]
- Approaches (error model)
  - Combinatorial (algebraic)
    [Koetter-Kschischang '08] [Silva-K-K '08] [Silva-K '09]
  - Information-theoretic
    [Montanari-Urbanke '07] [Silva-K-K '10] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]

Coding for this channel

- Subspace coding [Koetter-Kschischang '08]
  - Encode information in the subspace spanned by the rows of $\mathbf{X}$
- Lifting [Silva-K-K '08] a.k.a. channel training [Yang-H-M-Y-Y '10]
  - Special case of subspace coding
  - Roots on Chou's pratical network coding [Chou-W-K '03]
- Approaches (error model)
  - Combinatorial (algebraic)
    [Koetter-Kschischang '08] [Silva-K-K '08] [Silva-K '09]
  - Information-theoretic
    [Montanari-Urbanke '07] [Silva-K-K '10] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]

Coding for this channel

- Subspace coding [Koetter-Kschischang '08]
  - Encode information in the subspace spanned by the rows of $\mathbf{X}$
- Lifting [Silva-K-K '08] a.k.a. channel training [Yang-H-M-Y-Y '10]
  - Special case of subspace coding
  - Roots on Chou's pratical network coding [Chou-W-K '03]
- Approaches (error model)
  - Combinatorial (algebraic) [Koetter-Kschischang '08] [Silva-K-K '08] [Silva-K '09]
  - Information-theoretic [Montanari-Urbanke '07] [Silva-K-K '10] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]

Coding for this channel

- Subspace coding [Koetter-Kschischang '08]
  - Encode information in the subspace spanned by the rows of $\mathbf{X}$
- Lifting [Silva-K-K '08] a.k.a. channel training [Yang-H-M-Y-Y '10]
  - Special case of subspace coding
  - Roots on Chou's pratical network coding [Chou-W-K '03]
- Approaches (error model)
  - Combinatorial (algebraic)
    [Koetter-Kschischang '08] [Silva-K-K '08] [Silva-K '09]
  - Information-theoretic
    [Montanari-Urbanke '07] [Silva-K-K '10] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]

Coding for this channel

- Subspace coding [Koetter-Kschischang '08]
  - Encode information in the subspace spanned by the rows of $\mathbf{X}$
- Lifting [Silva-K-K '08] a.k.a. channel training [Yang-H-M-Y-Y '10]
  - Special case of subspace coding
  - Roots on Chou's pratical network coding [Chou-W-K '03]
- Approaches (error model)
  - Combinatorial (algebraic)
    [Koetter-Kschischang '08] [Silva-K-K '08] [Silva-K '09]
  - Information-theoretic
    [Montanari-Urbanke '07] [Silva-K-K '10] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]

Coding for this channel

- Subspace coding [Koetter-Kschischang '08]
  - Encode information in the subspace spanned by the rows of $\mathbf{X}$
- Lifting [Silva-K-K '08] a.k.a. channel training [Yang-H-M-Y-Y '10]
  - Special case of subspace coding
  - Roots on Chou's pratical network coding [Chou-W-K '03]
- Approaches (error model)
  - Combinatorial (algebraic)
    [Koetter-Kschischang '08] [Silva-K-K '08] [Silva-K '09]
  - Information-theoretic
    [Montanari-Urbanke '07] [Silva-K-K '10] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]

Coding for this channel

- Subspace coding [Koetter-Kschischang '08]
  - Encode information in the subspace spanned by the rows of $\mathbf{X}$
- Lifting [Silva-K-K '08] a.k.a. channel training [Yang-H-M-Y-Y '10]
  - Special case of subspace coding
  - Roots on Chou's pratical network coding [Chou-W-K '03]
- Approaches (error model)
  - Combinatorial (algebraic)
    [Koetter-Kschischang '08] [Silva-K-K '08] [Silva-K '09]
  - Information-theoretic
    [Montanari-Urbanke '07] [Silva-K-K '10] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]

One-shot vs. multishot

- Mainly so far: one-shot codes
  - Use the channel only once
  - Okay if T can grow
- Proposed [Koetter-Kschischang '08] but not explored: multishot codes
  - Use the channel many times

This work: Block codes [Nobrega-Uchoa '09]

Transmit sequences of n matrices (or subspaces):

$$(\mathbf{X}_0, \ldots, \mathbf{X}_{n-1})$$

One-shot vs. multishot

- Mainly so far: one-shot codes
  - Use the channel only once
  - Okay if T can grow
- Proposed [Koetter-Kschischang '08] but not explored: multishot codes
  - Use the channel many times

This work: Block codes [Nobrega-Uchoa '09]

Transmit sequences of n matrices (or subspaces):

$$(\mathbf{X}_0, \ldots, \mathbf{X}_{n-1})$$

One-shot vs. multishot

- Mainly so far: one-shot codes
  - Use the channel only once
  - Okay if T can grow
- Proposed [Koetter-Kschischang '08] but not explored: multishot codes
  - Use the channel many times

This work: Block codes [Nobrega-Uchoa '09]

Transmit sequences of n matrices (or subspaces):

$$(\mathbf{X}_0, \ldots, \mathbf{X}_{n-1})$$

One-shot vs. multishot

- Mainly so far: one-shot codes
  - Use the channel only once
  - Okay if T can grow
- Proposed [Koetter-Kschischang '08] but not explored: multishot codes
  - Use the channel many times

This work: Block codes [Nobrega-Uchoa '09]

Transmit sequences of n matrices (or subspaces):

$$(\mathbf{X}_0, \ldots, \mathbf{X}_{n-1})$$

One-shot vs. multishot

- Mainly so far: one-shot codes
  - Use the channel only once
  - Okay if T can grow
- Proposed [Koetter-Kschischang '08] but not explored: multishot codes
  - Use the channel many times

This work: Block codes [Nobrega-Uchoa '09]

Transmit sequences of n matrices (or subspaces):

$$(\mathbf{X}_0, \ldots, \mathbf{X}_{n-1})$$

One-shot vs. multishot

- Mainly so far: one-shot codes
  - Use the channel only once
  - Okay if T can grow
- Proposed [Koetter-Kschischang '08] but not explored: multishot codes
  - Use the channel many times

This work: Block codes [Nobrega-Uchoa '09]

Transmit sequences of n matrices (or subspaces):

$$(\mathbf{X}_0, \ldots, \mathbf{X}_{n-1})$$

Why use multishot codes?

- Two results:
  - **Channel capacity** can be achieved for large T [Silva-K-K '10]
  - **Combinatorial codes** are nearly optimal for large T [Silva-K '09]
- What if packet size T cannot be made too large?
  - For example: fast topology-changing networks
- Under this condition:
  - **Information theory**: use the channel many times to achieve capacity [Shannon!] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]
  - **Algebraic coding**: increase code length to improve code rate × minimum distance tradeoff
- Network fading:
  - Multishot can correct entirely lost shots (intershot redundancy)

Why use multishot codes?

- Two results:
  - **Channel capacity** can be achieved for large T [Silva-K-K '10]
  - **Combinatorial codes** are nearly optimal for large T [Silva-K '09]
- What if packet size T cannot be made too large?
  - For example: fast topology-changing networks
- Under this condition:
  - **Information theory**: use the channel many times to achieve capacity [Shannon!] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]
  - **Algebraic coding**: increase code length to improve code rate × minimum distance tradeoff
- Network fading:
  - Multishot can correct entirely lost shots (intershot redundancy)

Why use multishot codes?

- Two results:
  - **Channel capacity** can be achieved for large T [Silva-K-K '10]
  - **Combinatorial codes** are nearly optimal for large T [Silva-K '09]
- What if packet size T cannot be made too large?
  - For example: fast topology-changing networks
- Under this condition:
  - **Information theory**: use the channel many times to achieve capacity [Shannon!] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]
  - **Algebraic coding**: increase code length to improve code rate × minimum distance tradeoff
- Network fading:
  - Multishot can correct entirely lost shots (intershot redundancy)

Why use multishot codes?

- Two results:
  - **Channel capacity** can be achieved for large T [Silva-K-K '10]
  - **Combinatorial codes** are nearly optimal for large T [Silva-K '09]
- What if packet size T cannot be made too large?
  - For example: fast topology-changing networks
- Under this condition:
  - **Information theory**: use the channel many times to achieve capacity [Shannon!] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]
  - **Algebraic coding**: increase code length to improve code rate × minimum distance tradeoff
- Network fading:
  - Multishot can correct entirely lost shots (intershot redundancy)

Why use multishot codes?

- Two results:
  - **Channel capacity** can be achieved for large T [Silva-K-K '10]
  - **Combinatorial codes** are nearly optimal for large T [Silva-K '09]
- What if packet size T cannot be made too large?
  - For example: fast topology-changing networks
- Under this condition:
  - **Information theory**: use the channel many times to achieve capacity [Shannon!] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]
  - **Algebraic coding**: increase code length to improve code rate × minimum distance tradeoff
- Network fading:
  - Multishot can correct entirely lost shots (intershot redundancy)

Why use multishot codes?

- Two results:
  - **Channel capacity** can be achieved for large T [Silva-K-K '10]
  - **Combinatorial codes** are nearly optimal for large T [Silva-K '09]
- What if packet size T cannot be made too large?
  - For example: fast topology-changing networks
- Under this condition:
  - **Information theory**: use the channel many times to achieve capacity [Shannon!] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]
  - **Algebraic coding**: increase code length to improve code rate × minimum distance tradeoff
- Network fading:
  - Multishot can correct entirely lost shots (intershot redundancy)

Why use multishot codes?

- Two results:
  - **Channel capacity** can be achieved for large T [Silva-K-K '10]
  - **Combinatorial codes** are nearly optimal for large T [Silva-K '09]
- What if packet size T cannot be made too large?
  - For example: fast topology-changing networks
- Under this condition:
  - **Information theory**: use the channel many times to achieve capacity [Shannon!] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]
  - **Algebraic coding**: increase code length to improve code rate $\times$ minimum distance tradeoff
- Network fading:
  - Multishot can correct entirely lost shots (intershot redundancy)

Why use multishot codes?

- Two results:
  - **Channel capacity** can be achieved for large T [Silva-K-K '10]
  - **Combinatorial codes** are nearly optimal for large T [Silva-K '09]
- What if packet size T cannot be made too large?
  - For example: fast topology-changing networks
- Under this condition:
  - **Information theory**: use the channel many times to achieve capacity [Shannon!] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]
  - **Algebraic coding**: increase code length to improve code rate $\times$ minimum distance tradeoff
- Network fading:
  - Multishot can correct entirely lost shots (intershot redundancy)

Why use multishot codes?

- Two results:
  - **Channel capacity** can be achieved for large T [Silva-K-K '10]
  - **Combinatorial codes** are nearly optimal for large T [Silva-K '09]
- What if packet size T cannot be made too large?
  - For example: fast topology-changing networks
- Under this condition:
  - **Information theory**: use the channel many times to achieve capacity [Shannon!] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]
  - **Algebraic coding**: increase code length to improve code rate $\times$ minimum distance tradeoff
- Network fading:
  - Multishot can correct entirely lost shots (intershot redundancy)

Why use multishot codes?

- Two results:
  - **Channel capacity** can be achieved for large T [Silva-K-K '10]
  - **Combinatorial codes** are nearly optimal for large T [Silva-K '09]
- What if packet size T cannot be made too large?
  - For example: fast topology-changing networks
- Under this condition:
  - **Information theory**: use the channel many times to achieve capacity [Shannon!] [Jafari-M-F-D '09] [Yang-H-M-Y-Y '10]
  - **Algebraic coding**: increase code length to improve code rate $\times$ minimum distance tradeoff
- Network fading:
  - Multishot can correct entirely lost shots (intershot redundancy)

Combinatorial results

One-shot [Silva-K-K '08]

Let $\mathcal{X} \subseteq \mathbb{F}_q^{N \times T}$ be an one-shot code. If

$$\operatorname{rankdef} \mathbf{A} \leq \rho \quad \text{and} \quad \operatorname{rank} \mathbf{Z} \leq \tau$$

then codeword $\mathbf{X}$ can be decoded from $\mathbf{Y}$ provided

$$d_S(\langle \mathcal{X} \rangle) > 2(\rho + 2\tau)$$

where $\langle \mathcal{X} \rangle$ is the (one-shot) subspace code obtained from $\mathcal{X}$ and

$$d_S(U, V) \triangleq \dim(U \dotplus V) - \dim(U \cap V)$$

Combinatorial results

One-shot [Silva-K-K '08]

Let $\mathcal{X} \subseteq \mathbb{F}_q^{N \times T}$ be an one-shot code. If

$$\text{rankdef}\, \mathbf{A} \leq \rho \quad \text{and} \quad \text{rank}\, \mathbf{Z} \leq \tau$$

then codeword $\mathbf{X}$ can be decoded from $\mathbf{Y}$ provided

$$d_S(\langle \mathcal{X} \rangle) > 2(\rho + 2\tau)$$

where $\langle \mathcal{X} \rangle$ is the (one-shot) subspace code obtained from $\mathcal{X}$ and

$$d_S(U, V) \triangleq \dim(U \dotplus V) - \dim(U \cap V)$$

Multishot

Let $\boldsymbol{\mathcal{X}} \subseteq (\mathbb{F}_q^{N \times T})^n$ be a multishot code. If

$$\sum_{j=0}^{n-1} \text{rankdef}\, \mathbf{A}_j \leq \rho \quad \text{and} \quad \sum_{j=0}^{n-1} \text{rank}\, \mathbf{Z}_j \leq \tau$$

then codeword $(\mathbf{X}_0, \ldots \mathbf{X}_{n-1})$ can be decoded from $(\mathbf{Y}_0, \ldots \mathbf{Y}_{n-1})$ provided

$$d_S(\langle \boldsymbol{\mathcal{X}} \rangle) > 2(\rho + 2\tau)$$

where $\langle \boldsymbol{\mathcal{X}} \rangle$ is the (multishot) subspace code obtained from $\boldsymbol{\mathcal{X}}$ and

$$d_S(\boldsymbol{U}, \boldsymbol{V}) \triangleq \sum_{j=0}^{n-1} d_S(U_j, V_j)$$

Rank-Metric Codes

Definitions and results

- Studied by Gabidulin [Gabidulin '85] and Roth [Roth '91]
- Rank-metric codes: $\mathcal{R} \subseteq \mathbb{F}_{q^M}^N$
  - An (N, K, D) code over an extended field $\mathbb{F}_{q^M}$
- Metric of concern: rank distance:

$$d_R(\mathbf{u}, \mathbf{v}) = \text{rank}(\underline{\mathbf{v}} - \underline{\mathbf{u}})$$

where $\mathbf{u} \in \mathbb{F}_{q^M}^N$ is translated to $\underline{\mathbf{u}} \in \mathbb{F}_q^{N \times M}$

- Singleton bound is valid:

$$D \leq N - K + 1$$

achieved with Gabidulin codes [Gabidulin '85] provided $N \leq M$

Definitions and results

- Studied by Gabidulin [Gabidulin '85] and Roth [Roth '91]
- Rank-metric codes: $\mathcal{R} \subseteq \mathbb{F}_{q^M}^N$
  - An (N, K, D) code over an extended field $\mathbb{F}_{q^M}$
- Metric of concern: rank distance:

$$\mathrm{d_R}(\mathbf{u}, \mathbf{v}) = \mathrm{rank}(\underline{\mathbf{v}} - \underline{\mathbf{u}})$$

where $\mathbf{u} \in \mathbb{F}_{q^M}^N$ is translated to $\underline{\mathbf{u}} \in \mathbb{F}_q^{N \times M}$

- Singleton bound is valid:

$$D \leq N - K + 1$$

achieved with Gabidulin codes [Gabidulin '85] provided $N \leq M$

Definitions and results

- Studied by Gabidulin [Gabidulin '85] and Roth [Roth '91]
- Rank-metric codes: $\mathcal{R} \subseteq \mathbb{F}_{q^M}^N$
  - An (N, K, D) code over an extended field $\mathbb{F}_{q^M}$
- Metric of concern: rank distance:

$$\mathrm{d_R}(\mathbf{u}, \mathbf{v}) = \mathrm{rank}(\underline{\mathbf{v}} - \underline{\mathbf{u}})$$

where $\mathbf{u} \in \mathbb{F}_{q^M}^N$ is translated to $\underline{\mathbf{u}} \in \mathbb{F}_q^{N \times M}$

- Singleton bound is valid:

$$D \leq N - K + 1$$

achieved with Gabidulin codes [Gabidulin '85] provided $N \leq M$

Definitions and results

- Studied by Gabidulin [Gabidulin '85] and Roth [Roth '91]
- Rank-metric codes: $\mathcal{R} \subseteq \mathbb{F}_{q^M}^N$
  - An (N, K, D) code over an extended field $\mathbb{F}_{q^M}$
- Metric of concern: rank distance:

$$d_R(\mathbf{u}, \mathbf{v}) = \text{rank}(\underline{\mathbf{v}} - \underline{\mathbf{u}})$$

where $\mathbf{u} \in \mathbb{F}_{q^M}^N$ is translated to $\underline{\mathbf{u}} \in \mathbb{F}_q^{N \times M}$

- Singleton bound is valid:

$$D \leq N - K + 1$$

achieved with Gabidulin codes [Gabidulin '85] provided $N \leq M$

Application to network coding

Rank-metric code $\longrightarrow$ Matrix code for network coding

Lifting operation [Silva-K-K '08]

Identity matrix in the header:

$$\begin{aligned} \mathcal{I}: \mathbb{F}_{q^M}^{N} &\longrightarrow \mathbb{F}_q^{N \times T} \\ \mathbf{u} &\longmapsto \left[\ \mathbf{I} \ \middle|\ \underline{\mathbf{u}}\ \right] \end{aligned}$$

with $T = N + M$

- Key result:

$$d_S(\langle \mathcal{I}(\mathbf{u}) \rangle, \langle \mathcal{I}(\mathbf{v}) \rangle) = 2\, d_R(\mathbf{u}, \mathbf{v})$$

Application to network coding

Rank-metric code $\longrightarrow$ Matrix code for network coding

Lifting operation [Silva-K-K '08]

Identity matrix in the header:

$$\begin{aligned} \mathcal{I} : \mathbb{F}_{q^M}^{N} &\longrightarrow \mathbb{F}_q^{N \times T} \\ \mathbf{u} &\longmapsto \left[\begin{array}{c|c} \mathbf{I} & \underline{\mathbf{u}} \end{array}\right] \end{aligned}$$

with $T = N + M$

- Key result:

$$d_S(\langle \mathcal{I}(\mathbf{u}) \rangle, \langle \mathcal{I}(\mathbf{v}) \rangle) = 2\, d_R(\mathbf{u}, \mathbf{v})$$

Application to network coding

Rank-metric code $\longrightarrow$ Matrix code for network coding

Lifting operation [Silva-K-K '08]

Identity matrix in the header:

$$\begin{aligned} \mathcal{I} : \mathbb{F}_{q^M}^{N} &\longrightarrow \mathbb{F}_q^{N \times T} \\ \mathbf{u} &\longmapsto \left[\ \mathbf{I} \ \middle| \ \underline{\mathbf{u}} \ \right] \end{aligned}$$

with $T = N + M$

- Key result:

$$d_S(\langle \mathcal{I}(\mathbf{u}) \rangle, \langle \mathcal{I}(\mathbf{v}) \rangle) = 2\, d_R(\mathbf{u}, \mathbf{v})$$

Extension to multishot

- Multishot rank-metric codes: $\mathcal{R} \subseteq (\mathbb{F}_{q^M}^N)^n$
  - Codewords are n-sequences of N-tuples over $\mathbb{F}_{q^M}$:

$$\boldsymbol{u} = (\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}) \text{ where each } \mathbf{u}_j \in \mathbb{F}_{q^M}^N$$

- Metric: extended rank distance:

$$\mathrm{d_R}(\boldsymbol{u}, \boldsymbol{v}) = \sum_{j=0}^{n-1} \mathrm{d_R}(\mathbf{u}_j, \mathbf{v}_j),$$

Extension to multishot

- Multishot rank-metric codes: $\mathcal{R} \subseteq (\mathbb{F}_{q^M}^N)^n$
  - Codewords are n-sequences of N-tuples over $\mathbb{F}_{q^M}$:

$$\boldsymbol{u} = (\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}) \text{ where each } \mathbf{u}_j \in \mathbb{F}_{q^M}^N$$

- Metric: extended rank distance:

$$\mathrm{d_R}(\boldsymbol{u}, \boldsymbol{v}) = \sum_{j=0}^{n-1} \mathrm{d_R}(\mathbf{u}_j, \mathbf{v}_j),$$

Extension to multishot

- Multishot rank-metric codes: $\mathcal{R} \subseteq (\mathbb{F}_{q^M}^N)^n$
  - Codewords are n-sequences of N-tuples over $\mathbb{F}_{q^M}$:

$$\boldsymbol{u} = (\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}) \text{ where each } \mathbf{u}_j \in \mathbb{F}_{q^M}^N$$

- Metric: extended rank distance:

$$\mathrm{d_R}(\boldsymbol{u}, \boldsymbol{v}) = \sum_{j=0}^{n-1} \mathrm{d_R}(\mathbf{u}_j, \mathbf{v}_j),$$

Extended lifting

Multishot rank-metric code $\longrightarrow$ Multishot matrix code

Extended lifting operation

Lifting of each element:

$$\begin{aligned} \mathcal{I} : (\mathbb{F}_{q^M}^{N})^n &\longrightarrow (\mathbb{F}_q^{N \times T})^n \\ (\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}) &\longmapsto (\mathcal{I}(\mathbf{u}_0), \ldots, \mathcal{I}(\mathbf{u}_{n-1})) \end{aligned}$$

with $T = N + M$

- Result:

$$\mathrm{d_S}(\langle \mathcal{I}(\boldsymbol{u}) \rangle, \langle \mathcal{I}(\boldsymbol{v}) \rangle) = 2\, \mathrm{d_R}(\boldsymbol{u}, \boldsymbol{v})$$

Extended lifting

Multishot rank-metric code $\longrightarrow$ Multishot matrix code

Extended lifting operation

Lifting of each element:

$$\begin{aligned} \mathcal{I} : (\mathbb{F}_{q^M}^{N})^n &\longrightarrow (\mathbb{F}_q^{N \times T})^n \\ (\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}) &\longmapsto (\mathcal{I}(\mathbf{u}_0), \ldots, \mathcal{I}(\mathbf{u}_{n-1})) \end{aligned}$$

with $T = N + M$

- Result:

$$\mathrm{d_S}(\langle \mathcal{I}(\boldsymbol{u}) \rangle, \langle \mathcal{I}(\boldsymbol{v}) \rangle) = 2\,\mathrm{d_R}(\boldsymbol{u}, \boldsymbol{v})$$

Extended lifting

Multishot rank-metric code $\longrightarrow$ Multishot matrix code

Extended lifting operation

Lifting of each element:

$$\begin{aligned} \mathcal{I} : (\mathbb{F}_{q^M}^N)^n &\longrightarrow (\mathbb{F}_q^{N \times T})^n \\ (\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}) &\longmapsto (\mathcal{I}(\mathbf{u}_0), \ldots, \mathcal{I}(\mathbf{u}_{n-1})) \end{aligned}$$

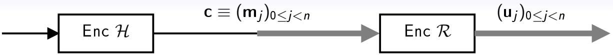
with $T = N + M$

- Result:

$$\mathrm{d}_\mathrm{S}(\langle \mathcal{I}(\boldsymbol{u}) \rangle, \langle \mathcal{I}(\boldsymbol{v}) \rangle) = 2\,\mathrm{d}_\mathrm{R}(\boldsymbol{u}, \boldsymbol{v})$$

Multilevel Construction

Concatenated codes



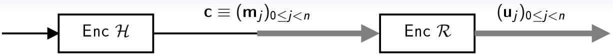
Ingredients

1. A p-ary (n, k, d) outer code $\mathcal{H}$ (typically Reed-Solomon)
2. A Q-ary (N, K, D) inner code $\mathcal{R}$
    - Originally binary: $Q = 2$
    - Here rank-metric: $Q = q^M$

- Requirement: $p = Q^K$

- Introduced by Forney [Forney '65]

Concatenated codes



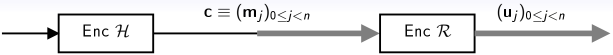
Ingredients

1. A p-ary (n, k, d) outer code $\mathcal{H}$ (typically Reed-Solomon)
2. A Q-ary (N, K, D) inner code $\mathcal{R}$
   - Originally binary: $Q = 2$
   - Here rank-metric: $Q = q^M$

- Requirement: $p = Q^K$

- Introduced by Forney [Forney '65]

Concatenated codes



Ingredients

1. A p-ary (n, k, d) outer code $\mathcal{H}$ (typically Reed-Solomon)
2. A Q-ary (N, K, D) inner code $\mathcal{R}$
    - Originally binary: $Q = 2$
    - Here rank-metric: $Q = q^M$

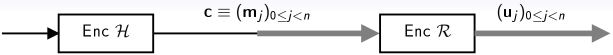
- Requirement: $p = Q^K$

- We have:

$$\mathbf{c} = (c_0, \ldots, c_{n-1}) \equiv (\mathbf{m}_0, \ldots, \mathbf{m}_{n-1})$$

where each $c_j \in \mathbb{F}_p = \mathbb{F}_{Q^K}$ is translated to $\mathbf{m}_j \in \mathbb{F}_Q^K$

Concatenated codes



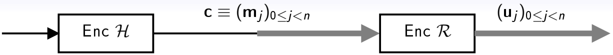
Ingredients

1. A p-ary (n, k, d) outer code $\mathcal{H}$ (typically Reed-Solomon)
2. A Q-ary (N, K, D) inner code $\mathcal{R}$
   - Originally binary: $Q = 2$
   - Here rank-metric: $Q = q^M$

- Requirement: $p = Q^K$

- There are:
  - 1 outer encoding: to form $\mathbf{c}$
  - n inner encodings: each $\mathbf{m}_j \in \mathbb{F}_Q^K$ is encoded to $\mathbf{u}_j \in \mathbb{F}_Q^N$

Concatenated codes



Ingredients

1. A p-ary (n, k, d) outer code $\mathcal{H}$ (typically Reed-Solomon)
2. A Q-ary (N, K, D) inner code $\mathcal{R}$
   - Originally binary: $Q = 2$
   - Here rank-metric: $Q = q^M$

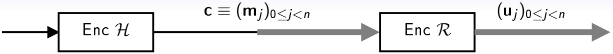
- Requirement: $p = Q^K$

- Result: a Q-ary (nN, kK) concatenated code with

$$d_{\min} \geq dD$$

or…

Concatenated codes



Ingredients

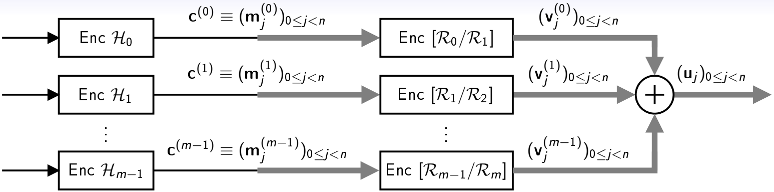
1. A p-ary (n, k, d) outer code $\mathcal{H}$ (typically Reed-Solomon)
2. A Q-ary (N, K, D) inner code $\mathcal{R}$
   - Originally binary: $Q = 2$
   - Here rank-metric: $Q = q^M$

- Requirement: $p = Q^K$

- Result: a multishot code $\boldsymbol{\mathcal{R}} \subseteq (\mathbb{F}_{q^M}^N)^n$ with $|\boldsymbol{\mathcal{R}}| = |\mathcal{H}|$ and

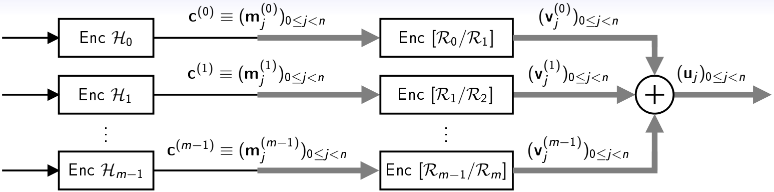
$$d_{\min} \geq dD$$

Generalized concatenated codes



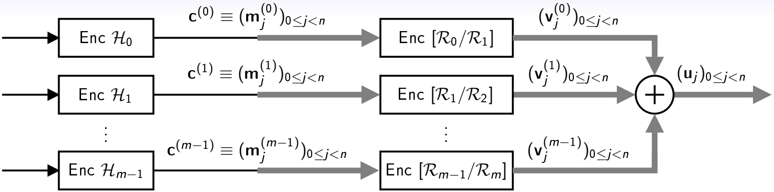
- Introduced by Blokh and Zyablov [Blokh-Zyablov '74]
- Also known as multilevel concatenated codes

Generalized concatenated codes



- Introduced by Blokh and Zyablov [Blokh-Zyablov '74]
- Also known as multilevel concatenated codes

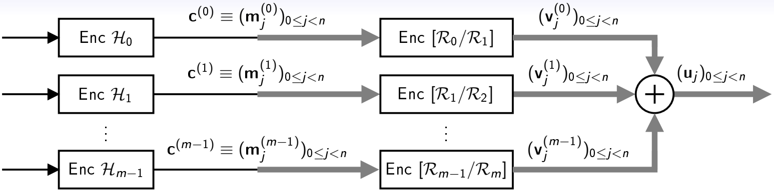
Generalized concatenated codes



Ingredients

1. m outer codes $\mathcal{H}_0, \ldots, \mathcal{H}_{m-1}$, (n_i, k_i, d_i), p_i-ary
2. $m+1$ subcodes $\mathcal{R}_0 \supseteq \cdots \supseteq \mathcal{R}_m$ of a parent code $\mathcal{R} = \mathcal{R}_0$
   - Each $\mathcal{R}_i$ is (N, K_i, D_i)
   - They are not the inner codes
   - Inner codes are the coset codes $[\mathcal{R}_i/\mathcal{R}_{i+1}]$

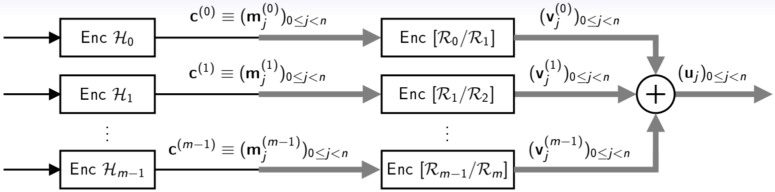
Generalized concatenated codes



Ingredients

1. m outer codes $\mathcal{H}_0, \ldots, \mathcal{H}_{m-1}$, (n_i, k_i, d_i), p_i-ary
2. $m+1$ subcodes $\mathcal{R}_0 \supseteq \cdots \supseteq \mathcal{R}_m$ of a parent code $\mathcal{R} = \mathcal{R}_0$
   - Each $\mathcal{R}_i$ is (N, K_i, D_i)
   - They are not the inner codes
   - Inner codes are the coset codes $[\mathcal{R}_i/\mathcal{R}_{i+1}]$

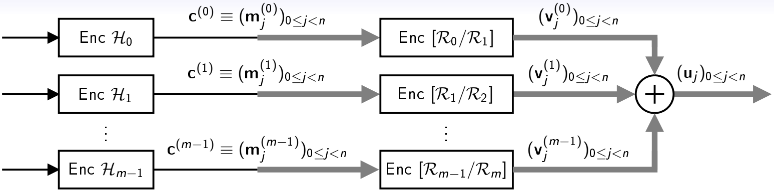
Generalized concatenated codes



Ingredients

1. m outer codes $\mathcal{H}_0, \ldots, \mathcal{H}_{m-1}$, (n_i, k_i, d_i), p_i-ary
2. $m+1$ subcodes $\mathcal{R}_0 \supseteq \cdots \supseteq \mathcal{R}_m$ of a parent code $\mathcal{R} = \mathcal{R}_0$
   - Each $\mathcal{R}_i$ is (N, K_i, D_i)
   - They are not the inner codes
   - Inner codes are the coset codes $[\mathcal{R}_i/\mathcal{R}_{i+1}]$

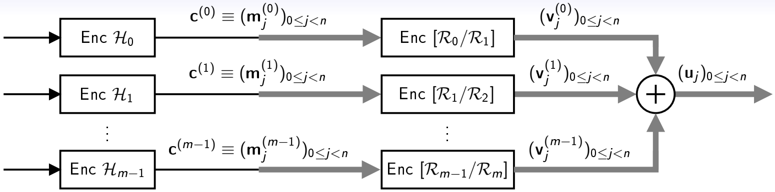
Generalized concatenated codes



Ingredients

1. m outer codes $\mathcal{H}_0, \ldots, \mathcal{H}_{m-1}$, (n_i, k_i, d_i), p_i-ary
2. $m+1$ subcodes $\mathcal{R}_0 \supseteq \cdots \supseteq \mathcal{R}_m$ of a parent code $\mathcal{R} = \mathcal{R}_0$
   - Each $\mathcal{R}_i$ is (N, K_i, D_i)
   - They are not the inner codes
   - Inner codes are the coset codes $[\mathcal{R}_i/\mathcal{R}_{i+1}]$

Generalized concatenated codes



Ingredients

1. m outer codes $\mathcal{H}_0, \ldots, \mathcal{H}_{m-1}$, (n_i, k_i, d_i), p_i-ary
2. $m+1$ subcodes $\mathcal{R}_0 \supseteq \cdots \supseteq \mathcal{R}_m$ of a parent code $\mathcal{R} = \mathcal{R}_0$
   - Each $\mathcal{R}_i$ is (N, K_i, D_i)
   - They are not the inner codes
   - Inner codes are the coset codes $[\mathcal{R}_i/\mathcal{R}_{i+1}]$

Parent code partitioning

Recipe

1. Start with a Q-ary (N, K, D) parent code $\mathcal{R}$ with generator matrix

$$\mathbf{G} = \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,K-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,K-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{N-1,0} & g_{N-1,1} & \cdots & g_{N-1,K-1} \end{bmatrix}$$

2. Choose a decreasing sequence of integers: $K = K_0 > \cdots > K_m = 0$
3. $[\mathcal{R}_i/\mathcal{R}_{i+1}]$ is the code generated by $\mathbf{G}[K_{i+1} : K_i - 1]$

Parent code partitioning

Recipe

1. Start with a Q-ary (N, K, D) parent code $\mathcal{R}$ with generator matrix

$$\mathbf{G} = \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,K-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,K-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{N-1,0} & g_{N-1,1} & \cdots & g_{N-1,K-1} \end{bmatrix}$$

2. Choose a decreasing sequence of integers: $K = K_0 > \cdots > K_m = 0$
3. $[\mathcal{R}_i/\mathcal{R}_{i+1}]$ is the code generated by $\mathbf{G}[K_{i+1} : K_i - 1]$

Parent code partitioning

Recipe

1. Start with a Q-ary (N, K, D) parent code $\mathcal{R}$ with generator matrix

$$\mathbf{G} = \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,K-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,K-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{N-1,0} & g_{N-1,1} & \cdots & g_{N-1,K-1} \end{bmatrix}$$

2. Choose a decreasing sequence of integers: $K = K_0 > \cdots > K_m = 0$
3. $[\mathcal{R}_i/\mathcal{R}_{i+1}]$ is the code generated by $\mathbf{G}[K_{i+1} : K_i - 1]$

Parent code partitioning

Example

$(N, K) = (6, 4) \qquad m = 3 \qquad (K_0, K_1, K_2, K_3) = (4, 3, 1, 0)$

$$\begin{bmatrix} g_{0,0} & g_{0,1} & g_{0,2} & g_{0,3} \\ g_{1,0} & g_{1,1} & g_{1,2} & g_{1,3} \\ g_{2,0} & g_{2,1} & g_{2,2} & g_{2,3} \\ g_{3,0} & g_{3,1} & g_{3,2} & g_{3,3} \\ g_{4,0} & g_{4,1} & g_{4,2} & g_{4,3} \\ g_{5,0} & g_{5,1} & g_{5,2} & g_{5,3} \end{bmatrix}$$

Parent code partitioning

Example

$(N, K) = (6, 4)$ $m = 3$ $(K_0, K_1, K_2, K_3) = (4, 3, 1, 0)$

$[\mathcal{R}_0/\mathcal{R}_1]$ is generated by $\mathbf{G}[K_1 : K_0 - 1]$

$$\begin{bmatrix} & & & g_{0,3} & & \\ & & & g_{1,3} & & \\ & & & g_{2,3} & & \\ & & & g_{3,3} & & \\ & & & g_{4,3} & & \\ & & & g_{5,3} & & \end{bmatrix}$$

Parent code partitioning

Example

$(N, K) = (6, 4) \qquad m = 3 \qquad (K_0, K_1, K_2, K_3) = (4, 3, 1, 0)$

$[\mathcal{R}_1/\mathcal{R}_2]$ is generated by $\mathbf{G}[K_2 : K_1 - 1]$

$$\begin{bmatrix} & g_{0,1} & g_{0,2} & \\ & g_{1,1} & g_{1,2} & \\ & g_{2,1} & g_{2,2} & \\ & g_{3,1} & g_{3,2} & \\ & g_{4,1} & g_{4,2} & \\ & g_{5,1} & g_{5,2} & \end{bmatrix}$$

Parent code partitioning

Example

$(N, K) = (6, 4) \qquad m = 3 \qquad (K_0, K_1, K_2, K_3) = (4, 3, 1, 0)$

$[\mathcal{R}_2/\mathcal{R}_3]$ is generated by $\mathbf{G}[K_3 : K_2 - 1]$

$$\begin{bmatrix} g_{0,0} & & & & & \\ g_{1,0} & & & & & \\ g_{2,0} & & & & & \\ g_{3,0} & & & & & \\ g_{4,0} & & & & & \\ g_{5,0} & & & & & \end{bmatrix}$$

Code parameters

Result

A multishot rank-metric code $\mathcal{R} \subseteq (\mathbb{F}_{q^M}^N)^n$ with

$$|\mathcal{R}| = |\mathcal{H}_0| \cdots |\mathcal{H}_{m-1}|$$

and

$$d_{\min} \geq \min\{d_0 D_0, \ldots, d_{m-1} D_{m-1}\}$$

Proof.

Adaptation of Lin and Costello [Lin-Costello '04 (Chapter 15)]

□

Code parameters

Result

A multishot rank-metric code $\mathcal{R} \subseteq (\mathbb{F}_{q^M}^N)^n$ with

$$|\mathcal{R}| = |\mathcal{H}_0| \cdots |\mathcal{H}_{m-1}|$$

and

$$d_{\min} \geq \min\{d_0 D_0, \ldots, d_{m-1} D_{m-1}\}$$

Proof.

Adaptation of Lin and Costello [Lin-Costello '04 (Chapter 15)]

□

Two remarks

1. Connection with multilevel block-coded modulation of Imai and Hirakawa [Imai-Hirakawa '77]:
    - Originally for Euclidean metric codes (AWGN channel)
    - Starts with an m-level partitioning of a signal set (subset of $\mathbb{R}^2$)
    - Protects each level with classical component codes
2. Multilevel construction (or generalized concatenated codes) works as long as:
    - Overall metric is the sum of individual shot metrics
    - Component codes are Hamming metric

Two remarks

1. Connection with multilevel block-coded modulation of Imai and Hirakawa [Imai-Hirakawa '77]:
   - Originally for Euclidean metric codes (AWGN channel)
   - Starts with an m-level partitioning of a signal set (subset of $\mathbb{R}^2$)
   - Protects each level with classical component codes
2. Multilevel construction (or generalized concatenated codes) works as long as:
   - Overall metric is the sum of individual shot metrics
   - Component codes are Hamming metric

Two remarks

1. Connection with multilevel block-coded modulation of Imai and Hirakawa [Imai-Hirakawa '77]:
   - Originally for Euclidean metric codes (AWGN channel)
   - Starts with an m-level partitioning of a signal set (subset of $\mathbb{R}^2$)
   - Protects each level with classical component codes
2. Multilevel construction (or generalized concatenated codes) works as long as:
   - Overall metric is the sum of individual shot metrics
   - Component codes are Hamming metric

Two remarks

1. Connection with multilevel block-coded modulation of Imai and Hirakawa [Imai-Hirakawa '77]:
   - Originally for Euclidean metric codes (AWGN channel)
   - Starts with an m-level partitioning of a signal set (subset of $\mathbb{R}^2$)
   - Protects each level with classical component codes
2. Multilevel construction (or generalized concatenated codes) works as long as:
   - Overall metric is the sum of individual shot metrics
   - Component codes are Hamming metric

Two remarks

1. Connection with multilevel block-coded modulation of Imai and Hirakawa [Imai-Hirakawa '77]:
   - Originally for Euclidean metric codes (AWGN channel)
   - Starts with an m-level partitioning of a signal set (subset of $\mathbb{R}^2$)
   - Protects each level with classical component codes
2. Multilevel construction (or generalized concatenated codes) works as long as:
   - Overall metric is the sum of individual shot metrics
   - Component codes are Hamming metric

Two remarks

1. Connection with multilevel block-coded modulation of Imai and Hirakawa [Imai-Hirakawa '77]:
    - Originally for Euclidean metric codes (AWGN channel)
    - Starts with an m-level partitioning of a signal set (subset of $\mathbb{R}^2$)
    - Protects each level with classical component codes
2. Multilevel construction (or generalized concatenated codes) works as long as:
    - Overall metric is the sum of individual shot metrics
    - Component codes are Hamming metric

Two remarks

1. Connection with multilevel block-coded modulation of Imai and Hirakawa [Imai-Hirakawa '77]:
    - Originally for Euclidean metric codes (AWGN channel)
    - Starts with an m-level partitioning of a signal set (subset of $\mathbb{R}^2$)
    - Protects each level with classical component codes
2. Multilevel construction (or generalized concatenated codes) works as long as:
    - Overall metric is the sum of individual shot metrics
    - Component codes are Hamming metric

Effect of the parent code dimension

Assumptions:

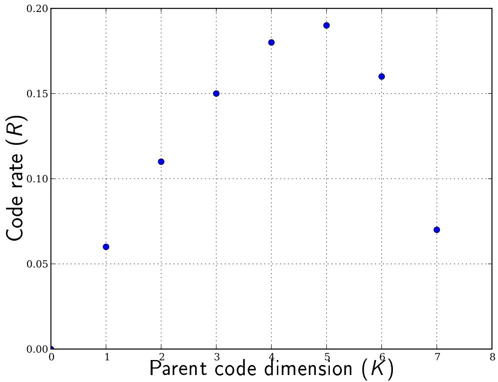
1. Partitioning is the "finest"
2. Rank metric codes $\mathcal{R}_i$ are MRD: Gabidulin codes
3. Component codes $\mathcal{H}_i$ are MDS: Reed-Solomon codes

How rate varies with parent code dimension K?

Effect of the parent code dimension

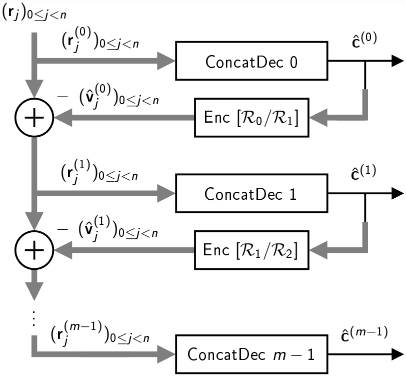
Binary: $q = 2$ Transmitted packets: $N = 8$ Packet size: $T = 40$, so $M = 32$

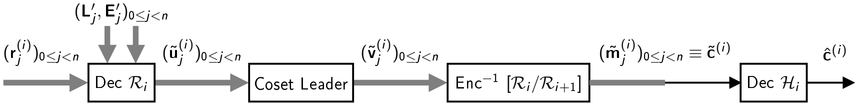
Number of shots: $n = 10$ Minimum distance: $d = \frac{1}{10} nT$



Decoding Procedure

Hard-decision multistage decoding





Conclusion

Conclusion

This work:

- Multishot codes for non-coherent network coding
- Construction based on generalized concatenated coding
- Encoding and decoding procedures

Future work:

- How good are these codes?
- Soft-decision multistage decoding

Conclusion

This work:

- Multishot codes for non-coherent network coding
- Construction based on generalized concatenated coding
- Encoding and decoding procedures

Future work:

- How good are these codes?
- Soft-decision multistage decoding

Conclusion

This work:

- Multishot codes for non-coherent network coding
- Construction based on generalized concatenated coding
- Encoding and decoding procedures

Future work:

- How good are these codes?
- Soft-decision multistage decoding

Conclusion

This work:

- Multishot codes for non-coherent network coding
- Construction based on generalized concatenated coding
- Encoding and decoding procedures

Future work:

- How good are these codes?
- Soft-decision multistage decoding

Conclusion

This work:

- Multishot codes for non-coherent network coding
- Construction based on generalized concatenated coding
- Encoding and decoding procedures

Future work:

- How good are these codes?
- Soft-decision multistage decoding

Thank you!

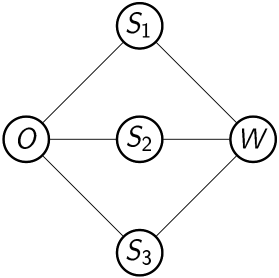
www.gpqcom.ufsc.br/~rwnobrega/

Backup Slides

Motivating example

Goal

A multishot code over $\mathcal{P}(\mathbb{F}_2^2)$ using the channel twice which is able to detect a single subspace error ($d = 2$)



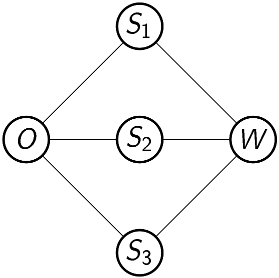
$$O = \{00\}$$
$$S_1 = \{00, 01\}$$
$$S_2 = \{00, 10\}$$
$$S_3 = \{00, 11\}$$
$$W = \{00, 01, 10, 11\}$$

Next: three proposals

Motivating example

Goal

A multishot code over $\mathcal{P}(\mathbb{F}_2^2)$ using the channel twice which is able to detect a single subspace error ($d = 2$)



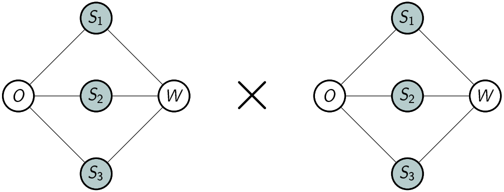
$$O = \{00\}$$
$$S_1 = \{00, 01\}$$
$$S_2 = \{00, 10\}$$
$$S_3 = \{00, 11\}$$
$$W = \{00, 01, 10, 11\}$$

Next: three proposals

First attempt

Proposal 1

To extend the best 1-shot code



$$\mathcal{C}_1 = \{S_1S_1, S_1S_2, S_1S_3, S_2S_1, S_2S_2, S_2S_3, S_3S_1, S_3S_2, S_3S_3\}$$

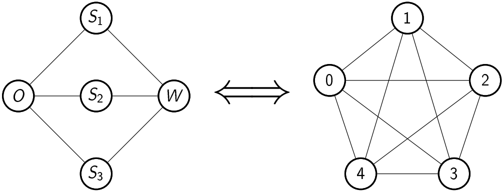
Cardinality

$$|\mathcal{C}_1| = 9$$

Second attempt

Proposal 2

Classic coding over the projective space



$$\mathcal{C}_2 = \{OO, S_1S_1, S_2S_2, S_3S_3, WW\}$$

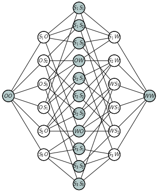
Cardinality

$$|\mathcal{C}_2| = 5$$

Third attempt

Proposal 3

To consider the metric space $\mathcal{P}(\mathbb{F}_2^2)^2$



$$\mathcal{C}_3 = \{OO, S_1S_1, S_1S_2, S_1S_3, OW, \ldots, S_3S_2, S_3S_3, WW\}$$

Cardinality

$$|\mathcal{C}_3| = 13$$

The metric space $\mathcal{P}(\mathbb{F}_2^2)^2$