On the Capacity of Multiplicative Finite-Field Matrix Channels

Roberto W. Nóbrega
Bartolomeu F. Uchôa-Filho
Danilo Silva

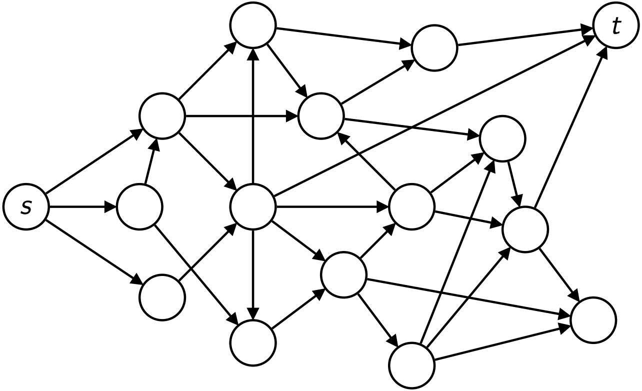
Federal University of Santa Catarina
Department of Electrical Engineering
Communications Research Group

2011 IEEE International Symposium on Information Theory
August 1, 2011, Saint Petersburg, Russia

Table of contents

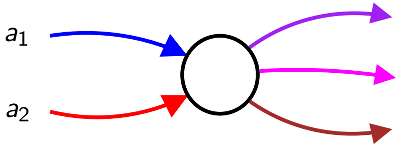
Motivation

Linear network coding



Linear network coding

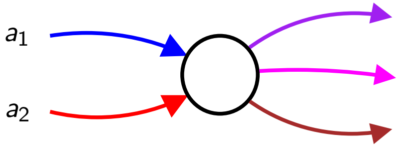
- On each node: output is a linear combination of the input



$$a_3 = F_{31} a_1 + F_{32} a_2$$
$$a_4 = F_{41} a_1 + F_{42} a_2$$
$$a_5 = F_{51} a_1 + F_{52} a_2$$

Linear network coding

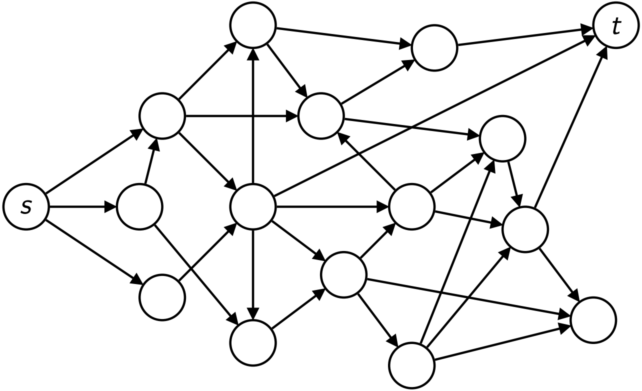
- On each node: output is a linear combination of the input



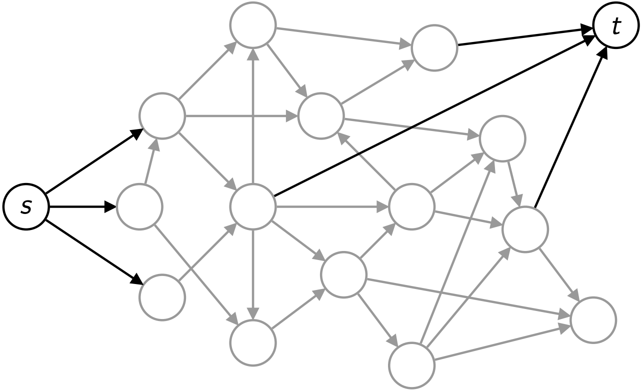
$$a_3 = F_{31} a_1 + F_{32} a_2$$
$$a_4 = F_{41} a_1 + F_{42} a_2$$
$$a_5 = F_{51} a_1 + F_{52} a_2$$

- Alphabet: finite field $\mathbb{F}_q$

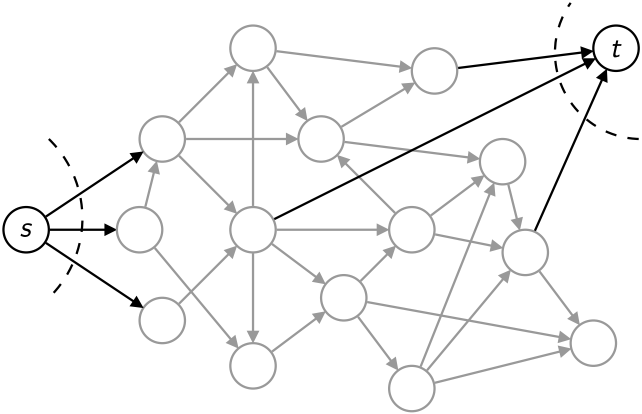
End-to-end approach



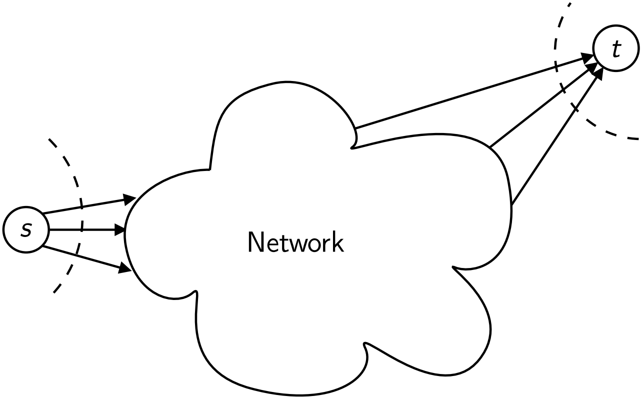
End-to-end approach



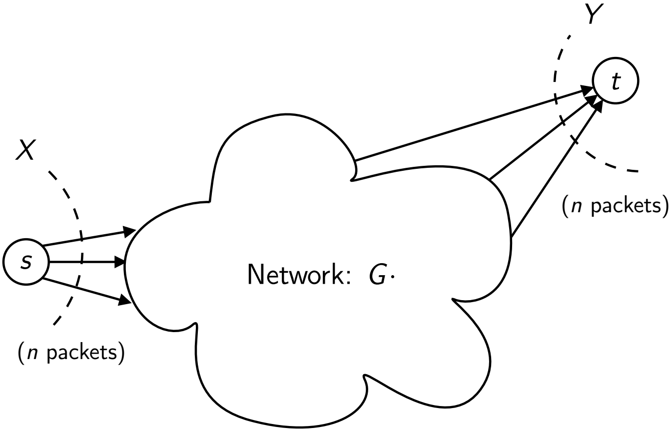
End-to-end approach



End-to-end approach



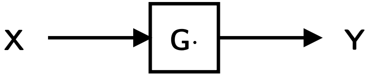
End-to-end approach



Packet length: m

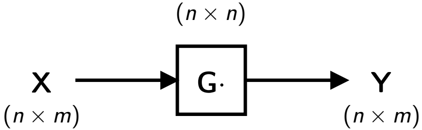
Channel model

Multiplicative finite-field matrix channels



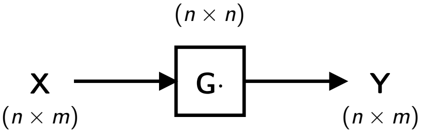
$$Y = GX$$

Multiplicative finite-field matrix channels



$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

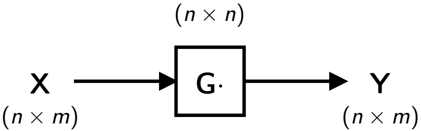
Multiplicative finite-field matrix channels



$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

- Probabilistic model: matrices are random variables (**bold**)

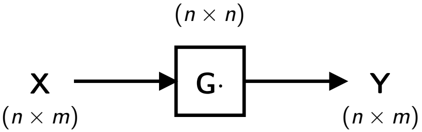
Multiplicative finite-field matrix channels



$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

- Probabilistic model: matrices are random variables
- DMC defined by $(\mathcal{X}, p(Y|X), \mathcal{Y})$

Multiplicative finite-field matrix channels

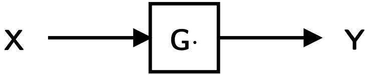


$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

- Probabilistic model: matrices are random variables
- DMC defined by $(\mathcal{X}, p(Y|X), \mathcal{Y})$
- $p(Y|X)$ induced by $p(G)$ through the channel law:

$$p(Y|X) = \sum_G p(G)\, 1[Y = GX]$$

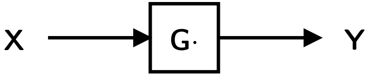
Previous works



$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

- $\mathbf{G}$ full-rank, uniform [Silva et al., 2010]
- $\mathbf{G}$ with uniform i.i.d. entries $\equiv$ $\mathbf{G}$ uniform [Jafari et al., 2011]

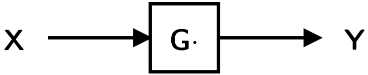
Previous works



$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

- $\mathbf{G}$ full-rank, uniform [Silva et al., 2010]
- $\mathbf{G}$ with uniform i.i.d. entries $\equiv$ $\mathbf{G}$ uniform [Jafari et al., 2011]
  - Too particular: may not be accurate

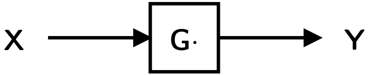
Previous works



$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

- $\mathbf{G}$ full-rank, uniform [Silva et al., 2010]
- $\mathbf{G}$ with uniform i.i.d. entries $\equiv$ $\mathbf{G}$ uniform [Jafari et al., 2011]
  - Too particular: may not be accurate
- $\mathbf{G}$ with arbitrary distribution [Yang et al., 2010]

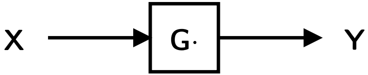
Previous works



$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

- **G** full-rank, uniform [Silva et al., 2010]
- **G** with uniform i.i.d. entries $\equiv$ **G** uniform [Jafari et al., 2011]
  - Too particular: may not be accurate
- **G** with arbitrary distribution [Yang et al., 2010]
  - Too general: complex channel description (q^{nm})

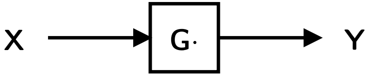
This work



$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

- $\mathbf{G}$ uniform given rank (u.g.r.) $\triangleq$ matrices with same rank are equiprobable

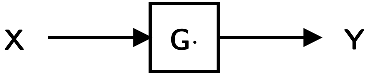
This work



$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

- $\mathbf{G}$ uniform given rank (u.g.r.) $\triangleq$ matrices with same rank are equiprobable
  - Simple channel description $(n+1)$

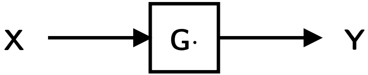
This work



$$\mathsf{Y} = \mathsf{GX}$$

- **G** uniform given rank (u.g.r.) $\triangleq$ matrices with same rank are equiprobable
  - Simple channel description $(n+1)$
  - Keeps the essence of non-coherence

This work

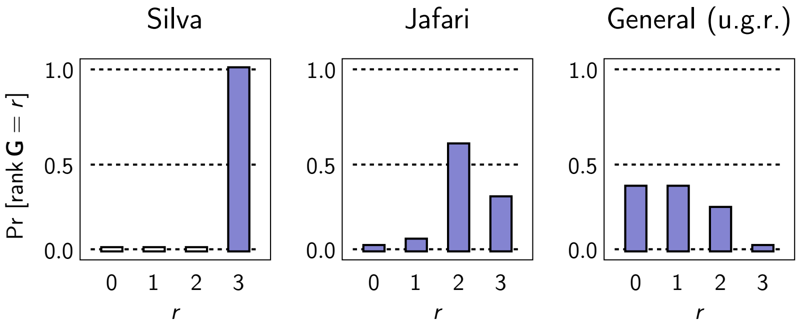


$$Y = GX$$

- **G** uniform given rank (u.g.r.) $\triangleq$ matrices with same rank are equiprobable
  - Simple channel description $(n + 1)$
  - Keeps the essence of non-coherence
  - Serves a lower bound on the capacity for the general case:

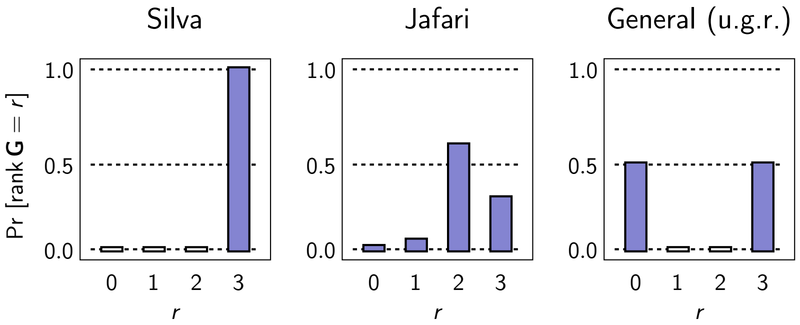
Comparison

- Example: $\mathbf{G}$ of dimension 3×3, binary field



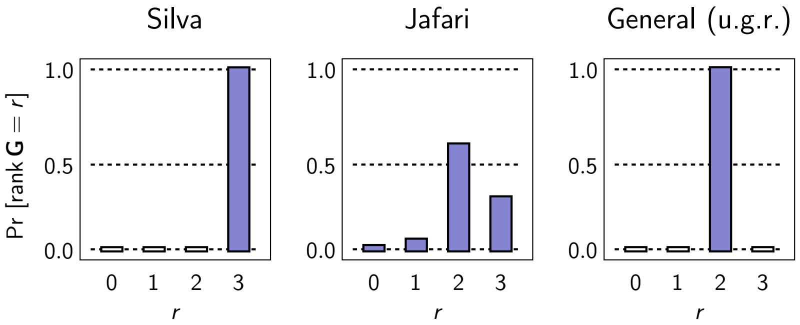
Comparison

- Example: $\mathbf{G}$ of dimension 3×3, binary field



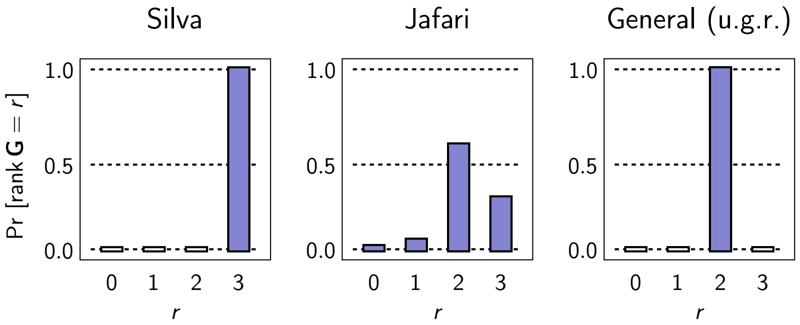
Comparison

- Example: **G** of dimension 3×3, binary field



Comparison

- Example: **G** of dimension 3×3, binary field



- Rank distribution depends on the topology, the link erasure probabilities, and the linear combinations

Our results

Channel transition probability

$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

$$\mathsf{u} \triangleq \operatorname{rank} \mathbf{X} \qquad \mathsf{v} \triangleq \operatorname{rank} \mathbf{Y} \qquad \mathsf{r} \triangleq \operatorname{rank} \mathbf{G}$$

Channel transition probability

$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

$$\mathbf{u} \triangleq \operatorname{rank} \mathbf{X} \qquad \mathbf{v} \triangleq \operatorname{rank} \mathbf{Y} \qquad \mathbf{r} \triangleq \operatorname{rank} \mathbf{G}$$

Channel transition probability

$$p(Y|X) = \begin{cases} \dfrac{p(v|u)}{|\mathcal{T}_q^{n\times u,v}|}, & \text{if } \langle Y \rangle \subseteq \langle X \rangle, \\ 0, & \text{else.} \end{cases}$$

Channel transition probability

$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

$$\mathbf{u} \triangleq \operatorname{rank} \mathbf{X} \qquad \mathbf{v} \triangleq \operatorname{rank} \mathbf{Y} \qquad \mathbf{r} \triangleq \operatorname{rank} \mathbf{G}$$

Channel transition probability

$$p(Y|X) = \begin{cases} \dfrac{p(v|u)}{|\mathcal{T}_q^{n \times u, v}|}, & \text{if } \langle Y \rangle \subseteq \langle X \rangle, \\ 0, & \text{else.} \end{cases}$$

- $p(v|u)$: rank transition probability:

$$p(v|u) = \sum_{r=0}^{n} p(r) \frac{|\mathcal{T}_q^{n \times u, v}|}{|\mathcal{T}_q^{n \times n, r}|} \phi_q(n; u, n, v, r),$$

calculated using a combinatorial result [Brawley and Carlitz, 1973]

Channel transition probability

$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

$$\mathbf{u} \triangleq \operatorname{rank} \mathbf{X} \qquad \mathbf{v} \triangleq \operatorname{rank} \mathbf{Y} \qquad \mathbf{r} \triangleq \operatorname{rank} \mathbf{G}$$

Channel transition probability

$$p(Y|X) = \begin{cases} \dfrac{p(v|u)}{|\mathcal{T}_q^{n\times u,v}|}, & \text{if } \langle Y \rangle \subseteq \langle X \rangle, \\ 0, & \text{else.} \end{cases}$$

- $p(Y|X)$: $q^{nm} \times q^{nm}$ matrix
- $p(v|u)$: $(n+1) \times (n+1)$ matrix

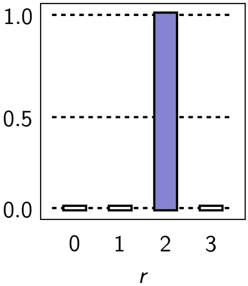
Rank transition probability

$$\mathbf{Y} = \mathbf{G}\mathbf{X}$$

$$\mathbf{u} \triangleq \operatorname{rank} \mathbf{X} \qquad \mathbf{v} \triangleq \operatorname{rank} \mathbf{Y} \qquad \mathbf{r} \triangleq \operatorname{rank} \mathbf{G}$$

- Example: $\mathbf{G}$ of dimension 3×3, binary field

$p(r) = (0, 0, 1, 0)$



$$p(v|u) = \begin{bmatrix} u \backslash v & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 0 & 0 \\ 1 & \frac{1}{7} & \frac{6}{7} & 0 & 0 \\ 2 & 0 & \frac{3}{7} & \frac{4}{7} & 0 \\ 3 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Channel capacity

- Maximization split in two stages:

$$C = \max_{p(X)} I(\mathbf{X}; \mathbf{Y})$$
$$= \max_{p(u)} \max_{p(X):p(u)} I(\mathbf{X}; \mathbf{Y})$$

Channel capacity

- Maximization split in two stages:

$$C = \max_{p(X)} I(\mathbf{X};\mathbf{Y})$$
$$= \max_{p(u)} \max_{p(X):p(u)} I(\mathbf{X};\mathbf{Y})$$

Inner stage: Solved, max achieved with u.g.r. input

$$\max_{p(X):p(u)} I(\mathbf{X};\mathbf{Y}) = \sum_{v} p(v) \log_q \frac{a_v}{p(v)} - \sum_{u} b_u p(u) \triangleq I^*(p(u))$$

Channel capacity

- Maximization split in two stages:

$$C = \max_{p(X)} I(\mathbf{X};\mathbf{Y})$$
$$= \max_{p(u)} \max_{p(X):p(u)} I(\mathbf{X};\mathbf{Y})$$

Inner stage: Solved, max achieved with u.g.r. input

$$\max_{p(X):p(u)} I(\mathbf{X};\mathbf{Y}) = \sum_v p(v)\log_q \frac{a_v}{p(v)} - \sum_u b_u p(u) \triangleq I^*(p(u))$$

Outer stage: No closed-form solution

$$\max_{p(u)} I^*(p(u)) = \text{convex optimization problem}$$

Channel capacity

Original problem

$$C = \max_{p(X)} \; I(p(X))$$

Convex optimization on q^{nm} variables

Channel capacity

Original problem

$$C = \max_{p(X)} \; I(p(X))$$

Convex optimization on q^{nm} variables

New problem

$$C = \max_{p(u)} \; I^*(p(u))$$

Convex optimization on $n + 1$ variables

Channel capacity

Original problem

$$C = \max_{p(X)} I(p(X))$$

Convex optimization on q^{nm} variables

Problems are equivalent

New problem

$$C = \max_{p(u)} I^*(p(u))$$

Convex optimization on $n+1$ variables

Upper bound

#1 – Actual optimization problem

$$C = \max_{p(u)} \; I^*(p(u))$$

subject to $\quad p(0) + \ldots + p(n) = 1 \quad \forall u : p(u) \geq 0$

Upper bound

#1 – Actual optimization problem

$$C = \max_{p(u)} \; I^*(p(u))$$

subject to $\quad p(0) + \ldots + p(n) = 1 \quad \forall u : p(u) \geq 0$

#2 – Modified optimization problem

$$C = \max_{p(u)} \; I^*(p(u))$$

subject to $\quad p(0) + \ldots + p(n) = 1 \quad$ ~~$\forall u : p(u) \geq 0$~~

Upper bound

#1 – Actual optimization problem

$$C = \max_{p(u)} \; I^*(p(u))$$

subject to $p(0) + \ldots + p(n) = 1 \quad \forall u : p(u) \geq 0$

Problems are **not** equivalent

#2 – Modified optimization problem

$$C = \max_{p(u)} \; I^*(p(u))$$

subject to $p(0) + \ldots + p(n) = 1$ ~~$\forall u : p(u) \geq 0$~~

Upper bound

- Exact solution for #2:

$$\tilde{C} = \log_q \sum_{v=0}^{n} |\mathcal{T}_q^{n\times m,v}| q^{-c_v}$$

where c_v's are the solution of a triangular linear system of equations

Upper bound

- Exact solution for #2:

$$\tilde{C} = \log_q \sum_{v=0}^{n} |\mathcal{T}_q^{n \times m, v}| q^{-c_v}$$

where c_v's are the solution of a triangular linear system of equations

- Upper bound: $C \leq \tilde{C}$

Upper bound

- Exact solution for #2:

$$\tilde{C} = \log_q \sum_{v=0}^{n} |\mathcal{T}_q^{n\times m,v}| q^{-c_v}$$

where c_v's are the solution of a triangular linear system of equations

- Upper bound: $C \leq \tilde{C}$
- Sometimes this is also the solution for #1!

Constant-rank input

- Input matrices limited to have rank u

Constant-rank input

- Input matrices limited to have rank u

Rank-u capacity

$$C_u = \sum_{v=0}^{n} p(v|u) \log_q \frac{\begin{bmatrix} m \\ v \end{bmatrix}_q}{\begin{bmatrix} u \\ v \end{bmatrix}_q}$$

Constant-rank input

- Input matrices limited to have rank u

Rank-u capacity

$$C_u = \sum_{v=0}^{n} p(v|u) \log_q \frac{\begin{bmatrix} m \\ v \end{bmatrix}_q}{\begin{bmatrix} u \\ v \end{bmatrix}_q}$$

- Asymptotically optimal: $\max_u C_u \leq C \leq \max_u C_u + \log_q n$

Constant-rank input

- Input matrices limited to have rank u

Rank-u capacity

$$C_u = \sum_{v=0}^{n} p(v|u) \log_q \frac{\begin{bmatrix} m \\ v \end{bmatrix}_q}{\begin{bmatrix} u \\ v \end{bmatrix}_q}$$

- Asymptotically optimal: $\max_u C_u \leq C \leq \max_u C_u + \log_q n$

Unconstrained capacity, for $q \to \infty$

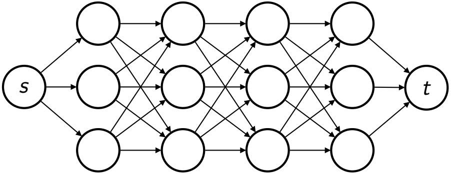
$$C = C_{u^*}$$

An example

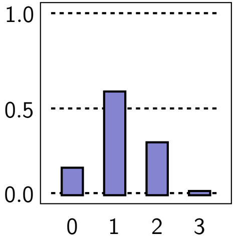
"Trellis network"

Pr[erasure] = 10% for each link, binary field

$n = 3 \quad m = 4$

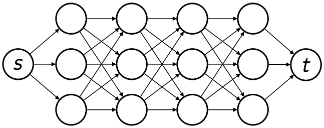


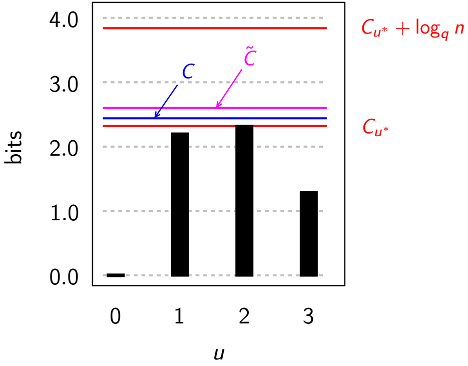
$p(r)$



An example

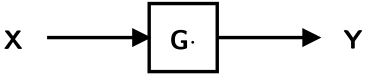
"Trellis network"





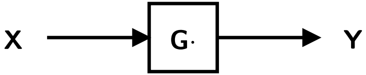
Communication via subspaces

- The matrix channel:

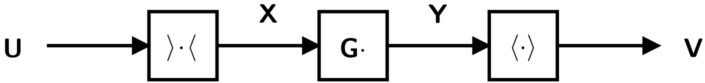


Communication via subspaces

- The matrix channel:

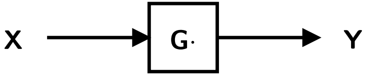


- The subspace channel:

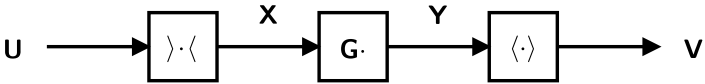


Communication via subspaces

- The matrix channel:



- The subspace channel:

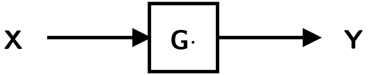


- Communication via subpaces is optimal for **G** u.g.r.:

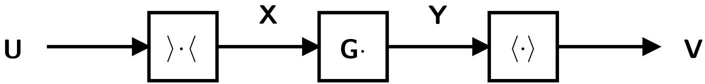
$$I(\mathbf{X};\mathbf{Y}) = I(\mathbf{U};\mathbf{V})$$

Communication via subspaces

- The matrix channel:



- The subspace channel:



- Communication via subpaces is optimal for **G** u.g.r.:

$$I(\mathbf{X};\mathbf{Y}) = I(\mathbf{U};\mathbf{V})$$

- Approach: "grouping of letters" in a DMC

Conclusion

Review

- U.g.r. transfer matrix: reasonable model for non-coherent networks

Review

- U.g.r. transfer matrix: reasonable model for non-coherent networks
- Capacity: optimization problem, bounds, special cases

Review

- U.g.r. transfer matrix: reasonable model for non-coherent networks
- Capacity: optimization problem, bounds, special cases
- Communication via subspaces: still optimal

Review

- U.g.r. transfer matrix: reasonable model for non-coherent networks
- Capacity: optimization problem, bounds, special cases
- Communication via subspaces: still optimal
- Main open problem: codes

Thank you!

Roberto W. Nóbrega
rwnobrega@eel.ufsc.br