Canais Matriciais Multiplicativos sobre Corpos e Anéis Finitos com Aplicações em Codificação de Rede

Roberto Wanderley da Nóbrega

Orientador: Prof. Bartolomeu Ferreira Uchôa Filho, Ph.D.
Co-orientador: Prof. Danilo Silva, Ph.D.

Departamento de Engenharia Elétrica
Universidade Federal de Santa Catarina

Florianópolis, 15 de outubro de 2013.

Objetivos

Estudo do canal matricial multiplicativo (MMC):

- Cálculo da capacidade.
- Projeto de esquemas de codificação.
- Aplicações práticas:
  - Codificação de rede tradicional.
  - Codificação de rede na camada física (Phy-NC).

Introdução

Canais matriciais multiplicativos

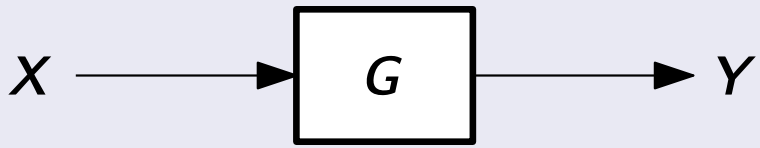
Sejam $\mathbb{F}_q$ um corpo finito e n, m, ℓ inteiros positivos.

Definição

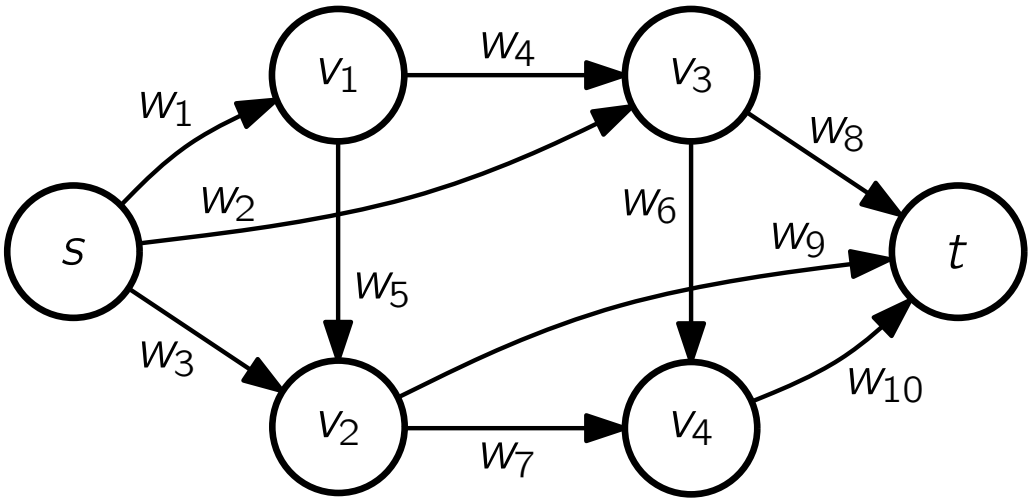
Um MMC sobre $\mathbb{F}_q$ é um canal de comunicação no qual a entrada $\boldsymbol{X} \in \mathbb{F}_q^{n \times \ell}$ e a saída $\boldsymbol{Y} \in \mathbb{F}_q^{m \times \ell}$ são matrizes relacionadas por

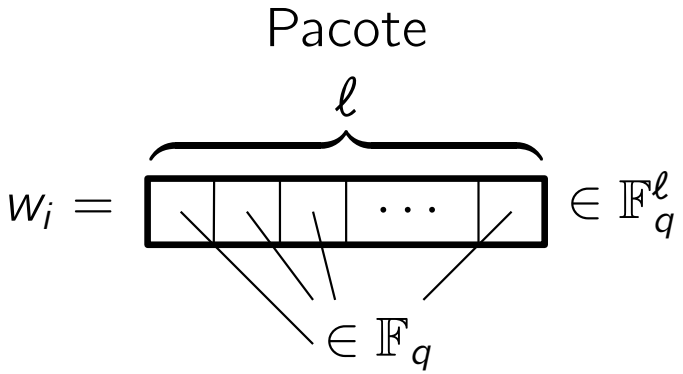
$$\boldsymbol{Y} = \boldsymbol{G}\boldsymbol{X},$$

em que $\boldsymbol{G} \in \mathbb{F}_q^{m \times n}$ é chamada de matriz de transferência.



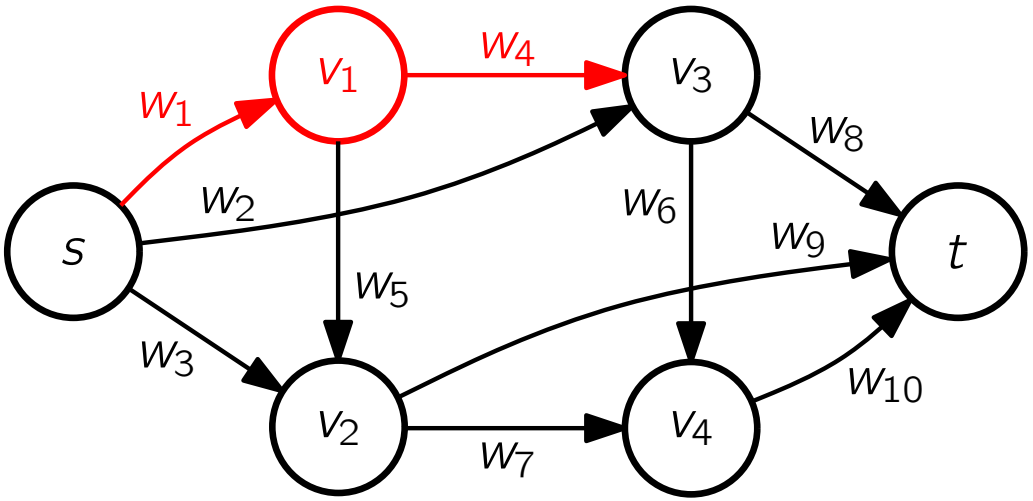
Codificação de rede linear: Fundamentos





- Cada enlace transporta um pacote.
- Cada nó intermediário calcula e envia combinações lineares (com coeficientes em $\mathbb{F}_q$) dos pacotes que recebe.

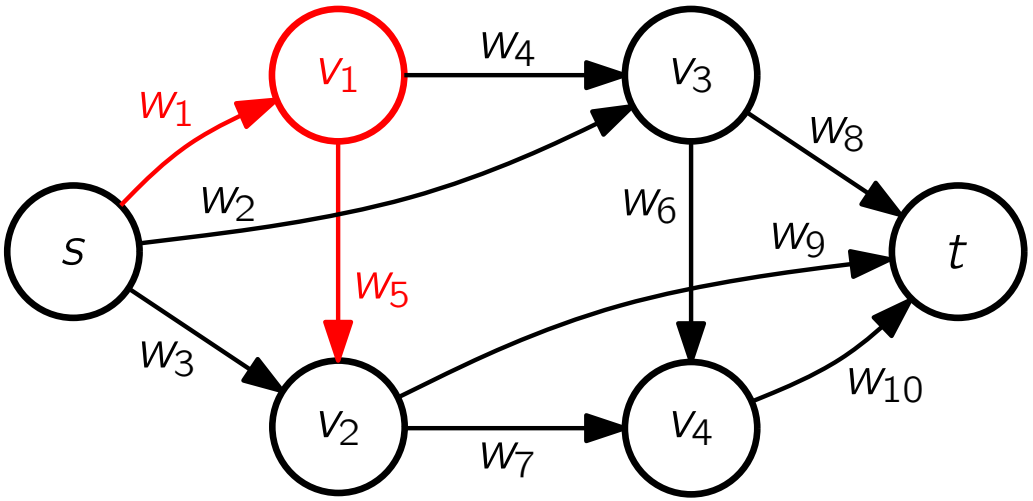
Codificação de rede linear: Fundamentos



$w_4 = a_{14} w_1$

- Cada enlace transporta um pacote.
- Cada nó intermediário calcula e envia combinações lineares (com coeficientes em $\mathbb{F}_q$) dos pacotes que recebe.

Codificação de rede linear: Fundamentos

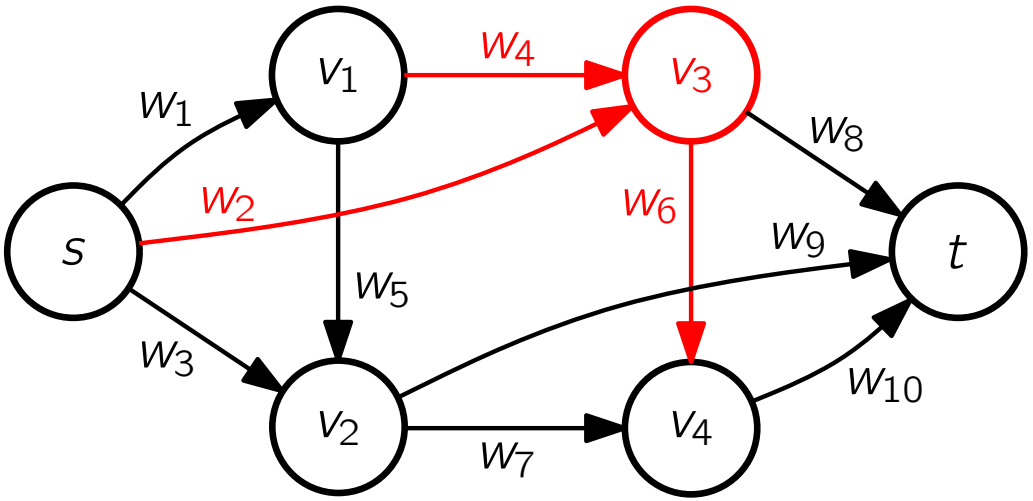


$$w_4 = a_{14} w_1$$

$$w_5 = a_{15} w_1$$

- Cada enlace transporta um pacote.
- Cada nó intermediário calcula e envia combinações lineares (com coeficientes em $\mathbb{F}_q$) dos pacotes que recebe.

Codificação de rede linear: Fundamentos



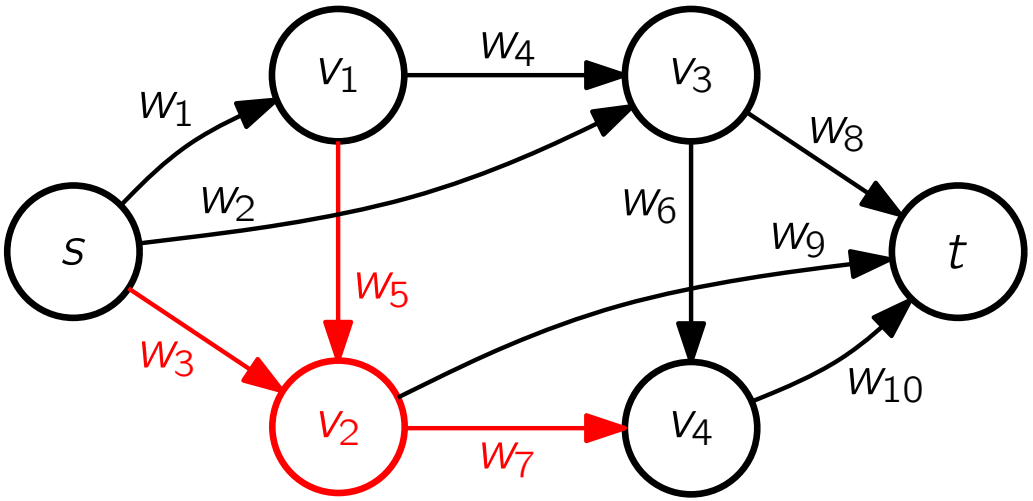
$$w_4 = a_{14} w_1$$

$$w_5 = a_{15} w_1$$

$$w_6 = a_{26} w_2 + a_{46} w_4$$

- Cada enlace transporta um pacote.
- Cada nó intermediário calcula e envia combinações lineares (com coeficientes em $\mathbb{F}_q$) dos pacotes que recebe.

Codificação de rede linear: Fundamentos



$$w_4 = a_{14} w_1$$

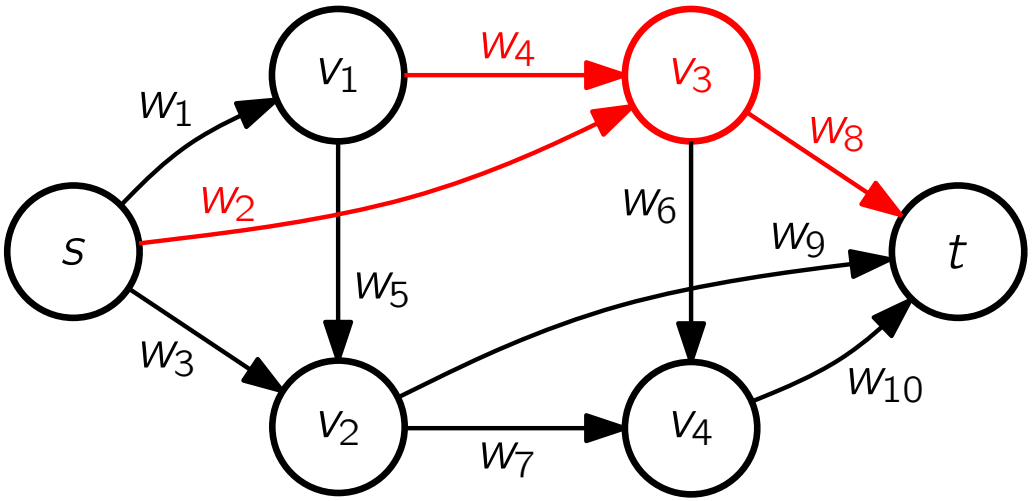
$$w_5 = a_{15} w_1$$

$$w_6 = a_{26} w_2 + a_{46} w_4$$

$$w_7 = a_{37} w_3 + a_{57} w_5$$

- Cada enlace transporta um pacote.
- Cada nó intermediário calcula e envia combinações lineares (com coeficientes em $\mathbb{F}_q$) dos pacotes que recebe.

Codificação de rede linear: Fundamentos



$$w_4 = a_{14} w_1$$

$$w_5 = a_{15} w_1$$

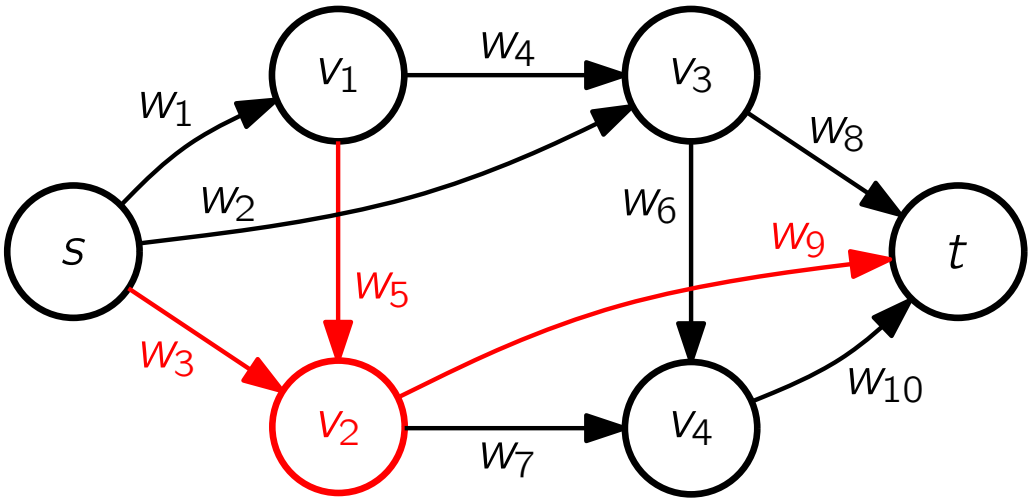
$$w_6 = a_{26} w_2 + a_{46} w_4$$

$$w_7 = a_{37} w_3 + a_{57} w_5$$

$$w_8 = a_{28} w_2 + a_{48} w_4$$

- Cada enlace transporta um pacote.
- Cada nó intermediário calcula e envia combinações lineares (com coeficientes em $\mathbb{F}_q$) dos pacotes que recebe.

Codificação de rede linear: Fundamentos



$$w_4 = a_{14} w_1$$

$$w_5 = a_{15} w_1$$

$$w_6 = a_{26} w_2 + a_{46} w_4$$

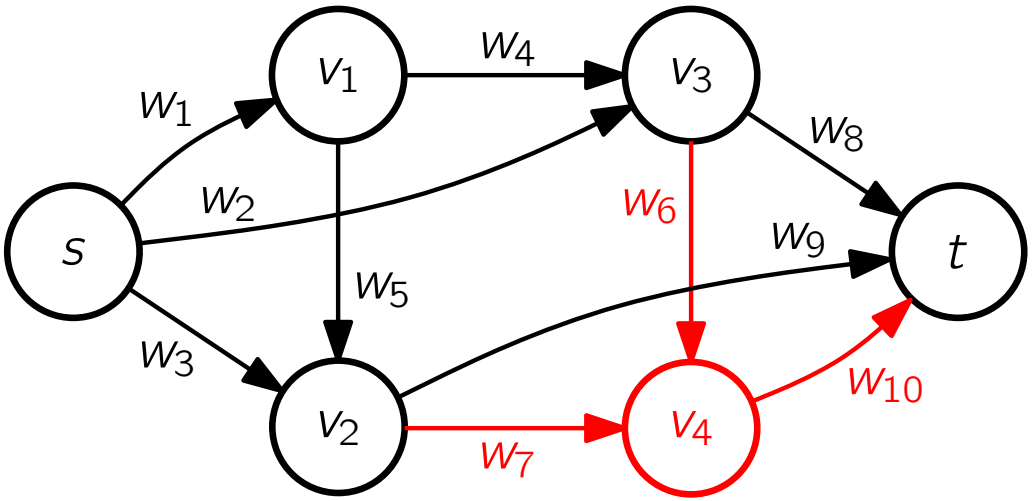
$$w_7 = a_{37} w_3 + a_{57} w_5$$

$$w_8 = a_{28} w_2 + a_{48} w_4$$

$$w_9 = a_{39} w_3 + a_{59} w_5$$

- Cada enlace transporta um pacote.
- Cada nó intermediário calcula e envia combinações lineares (com coeficientes em $\mathbb{F}_q$) dos pacotes que recebe.

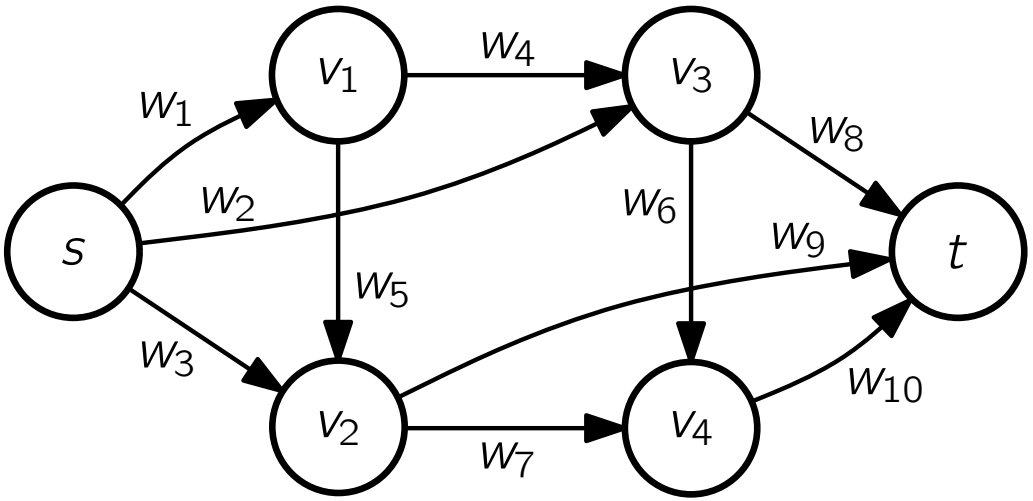
Codificação de rede linear: Fundamentos



$$w_4 = a_{14} w_1$$
$$w_5 = a_{15} w_1$$
$$w_6 = a_{26} w_2 + a_{46} w_4$$
$$w_7 = a_{37} w_3 + a_{57} w_5$$
$$w_8 = a_{28} w_2 + a_{48} w_4$$
$$w_9 = a_{39} w_3 + a_{59} w_5$$
$$w_{10} = a_{60} w_6 + a_{70} w_7$$

- Cada enlace transporta um pacote.
- Cada nó intermediário calcula e envia combinações lineares (com coeficientes em $\mathbb{F}_q$) dos pacotes que recebe.

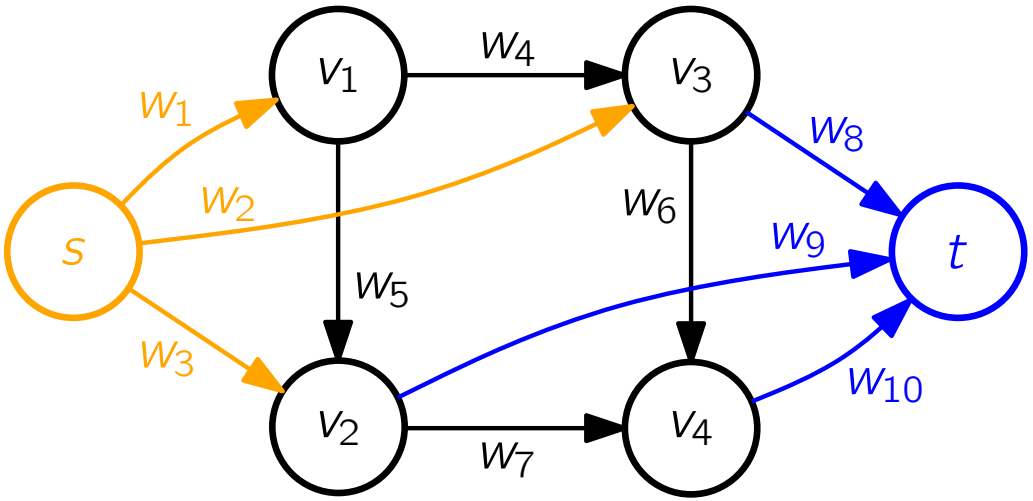
Codificação de rede linear: Fundamentos



$$w_4 = a_{14} w_1$$
$$w_5 = a_{15} w_1$$
$$w_6 = a_{26} w_2 + a_{46} w_4$$
$$w_7 = a_{37} w_3 + a_{57} w_5$$
$$w_8 = a_{28} w_2 + a_{48} w_4$$
$$w_9 = a_{39} w_3 + a_{59} w_5$$
$$w_{10} = a_{60} w_6 + a_{70} w_7$$

- Cada enlace transporta um pacote.
- Cada nó intermediário calcula e envia combinações lineares (com coeficientes em $\mathbb{F}_q$) dos pacotes que recebe.

Codificação de rede linear: Fundamentos

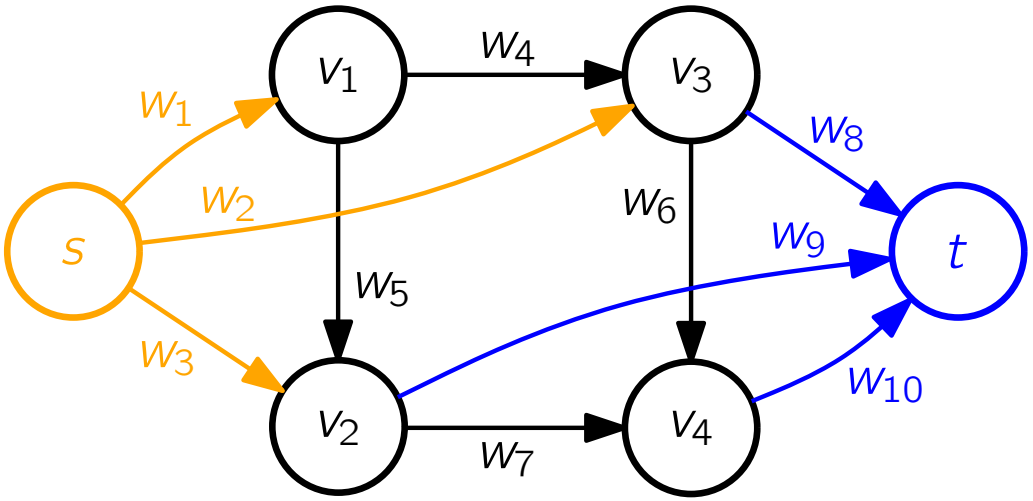


$$
\begin{aligned}
w_4 &= a_{14}\, w_1 \\
w_5 &= a_{15}\, w_1 \\
w_6 &= a_{26}\, w_2 + a_{46}\, w_4 \\
w_7 &= a_{37}\, w_3 + a_{57}\, w_5 \\
w_8 &= a_{28}\, w_2 + a_{48}\, w_4 \\
w_9 &= a_{39}\, w_3 + a_{59}\, w_5 \\
w_{10} &= a_{60}\, w_6 + a_{70}\, w_7
\end{aligned}
$$

Resolvendo:

$$
\begin{cases}
w_8 = (a_{14}\, a_{48})\, w_1 + (a_{28})\, w_2 \\
w_9 = (a_{15}\, a_{59})\, w_1 + (a_{39})\, w_3 \\
w_{10} = (a_{14}\, a_{46}\, a_{60} + a_{15}\, a_{57}\, a_{70})\, w_1 + (a_{26}\, a_{60})\, w_2 + (a_{37}\, a_{70})\, w_3
\end{cases}
$$

Codificação de rede linear: Fundamentos



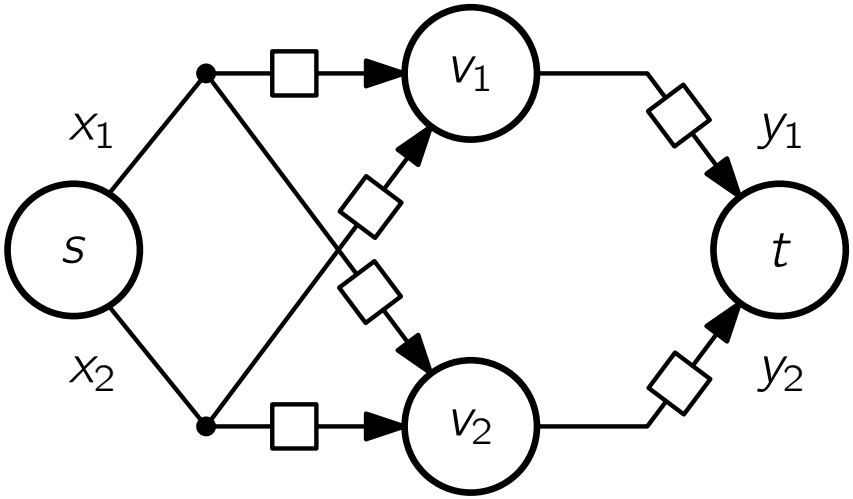
$$
\begin{aligned}
w_4 &= a_{14}\, w_1 \\
w_5 &= a_{15}\, w_1 \\
w_6 &= a_{26}\, w_2 + a_{46}\, w_4 \\
w_7 &= a_{37}\, w_3 + a_{57}\, w_5 \\
w_8 &= a_{28}\, w_2 + a_{48}\, w_4 \\
w_9 &= a_{39}\, w_3 + a_{59}\, w_5 \\
w_{10} &= a_{60}\, w_6 + a_{70}\, w_7
\end{aligned}
$$

Forma matricial:

$$
\underbrace{\begin{bmatrix} — & w_8 & — \\ — & w_9 & — \\ — & w_{10} & — \end{bmatrix}}_{Y} = \underbrace{\begin{bmatrix} a_{14}a_{48} & a_{28} & 0 \\ a_{15}a_{59} & 0 & a_{39} \\ a_{14}a_{46}a_{60} + a_{15}a_{57}a_{70} & a_{26}a_{60} & a_{37}a_{70} \end{bmatrix}}_{G} \underbrace{\begin{bmatrix} — & w_1 & — \\ — & w_2 & — \\ — & w_3 & — \end{bmatrix}}_{X}
$$

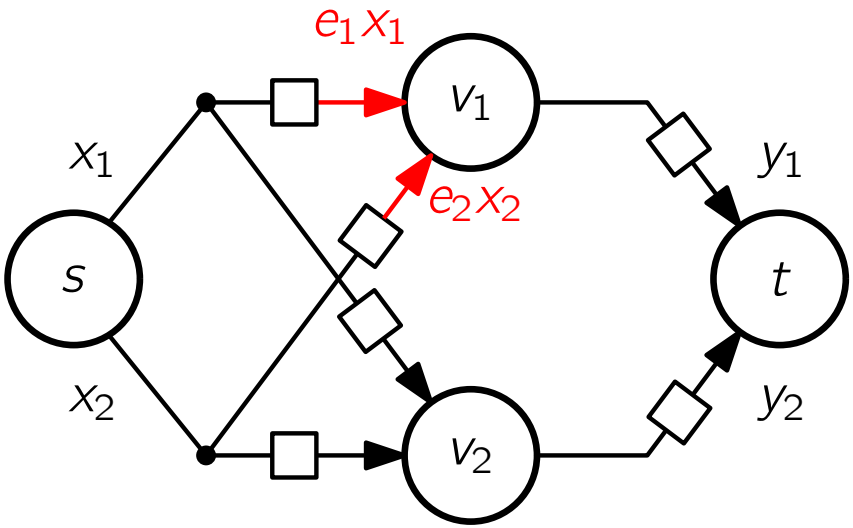
Codificação de rede linear: Difusão e apagamentos

Modelo com enlaces de difusão (*broadcast*) e apagamentos:



Codificação de rede linear: Difusão e apagamentos

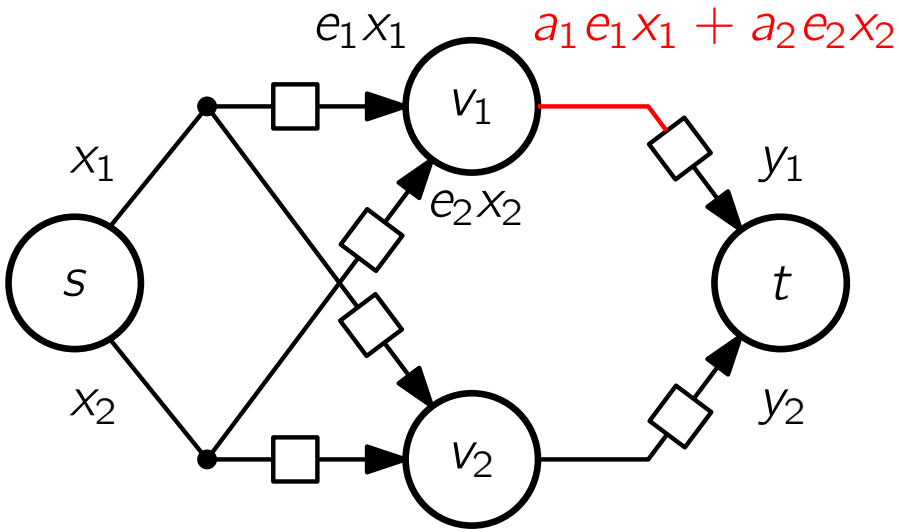
Modelo com enlaces de difusão (*broadcast*) e apagamentos:



Apagamentos:
$e_i \in \{0, 1\}$

Codificação de rede linear: Difusão e apagamentos

Modelo com enlaces de difusão (*broadcast*) e apagamentos:

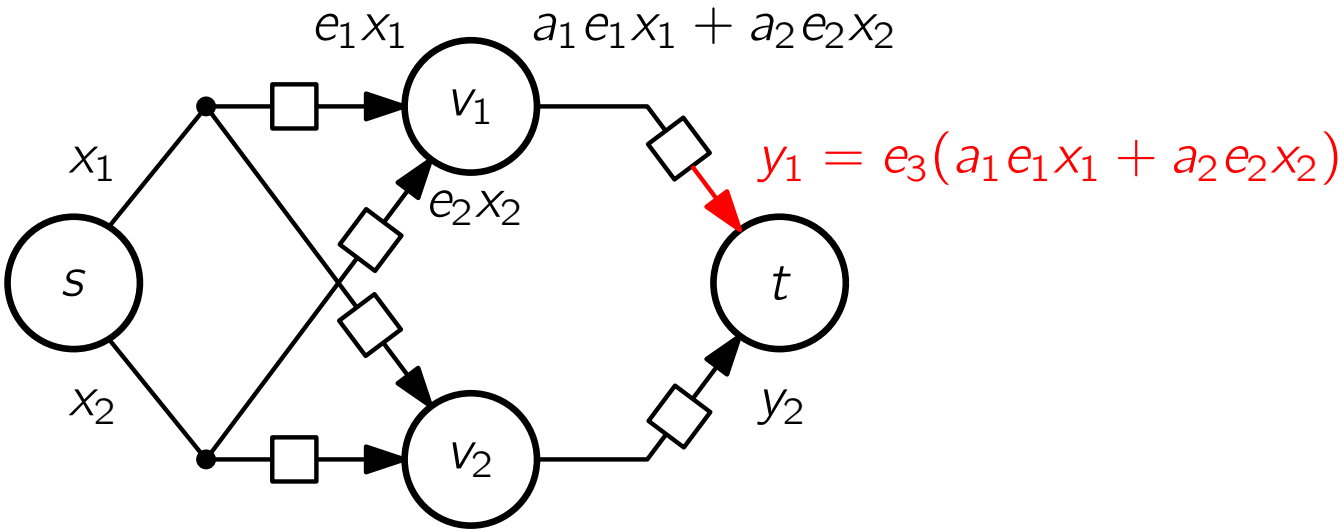


Apagamentos:
$e_i \in \{0, 1\}$

Combinações lineares:
$a_i \in \mathbb{F}_q$

Codificação de rede linear: Difusão e apagamentos

Modelo com enlaces de difusão (*broadcast*) e apagamentos:

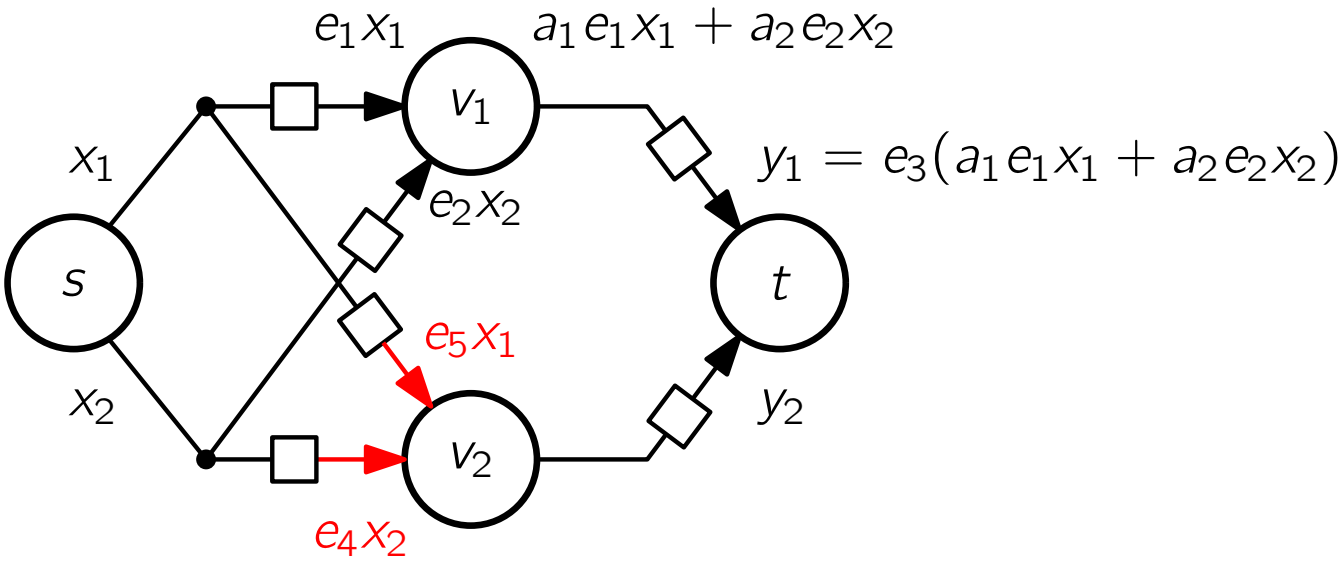


Apagamentos:
$e_i \in \{0, 1\}$

Combinações lineares:
$a_i \in \mathbb{F}_q$

Codificação de rede linear: Difusão e apagamentos

Modelo com enlaces de difusão (*broadcast*) e apagamentos:

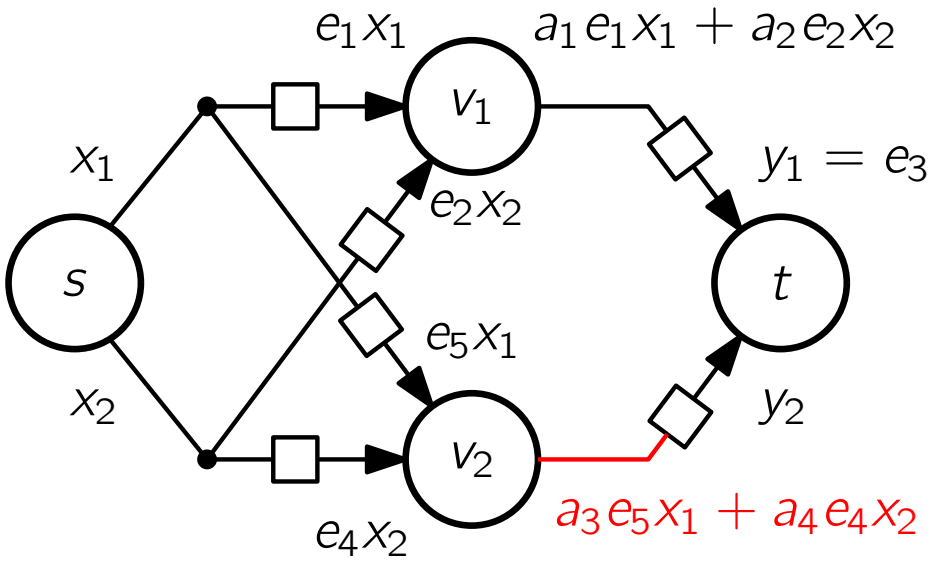


Apagamentos:
$e_i \in \{0, 1\}$

Combinações lineares:
$a_i \in \mathbb{F}_q$

Codificação de rede linear: Difusão e apagamentos

Modelo com enlaces de difusão (*broadcast*) e apagamentos:

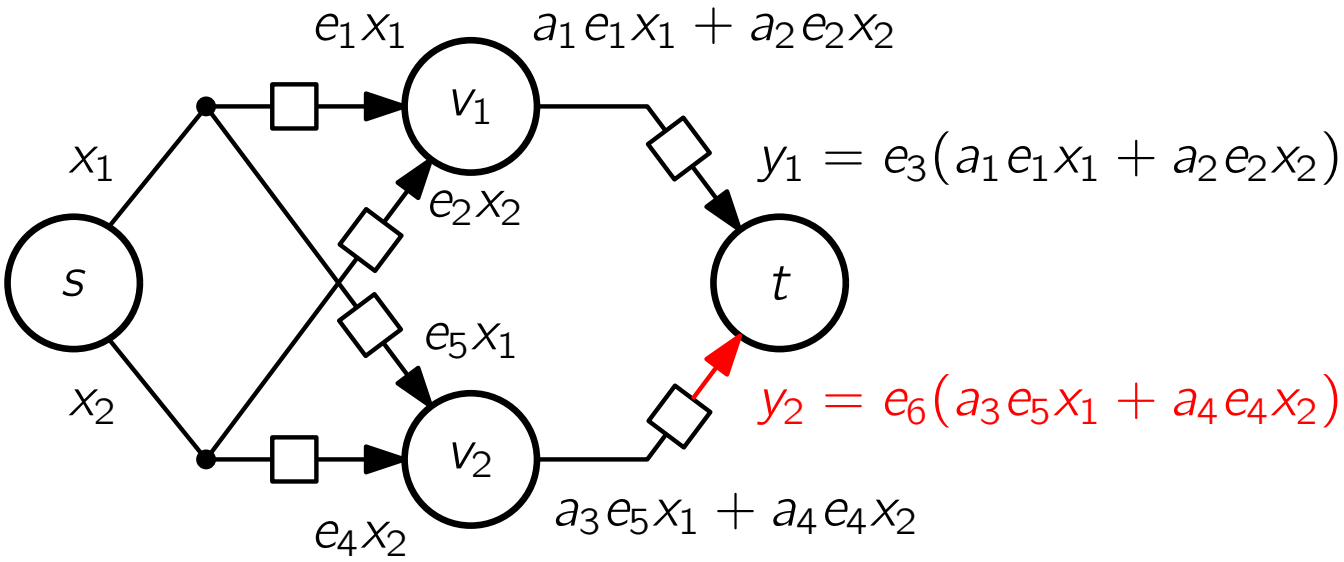


Apagamentos:
$e_i \in \{0, 1\}$

Combinações lineares:
$a_i \in \mathbb{F}_q$

Codificação de rede linear: Difusão e apagamentos

Modelo com enlaces de difusão (*broadcast*) e apagamentos:

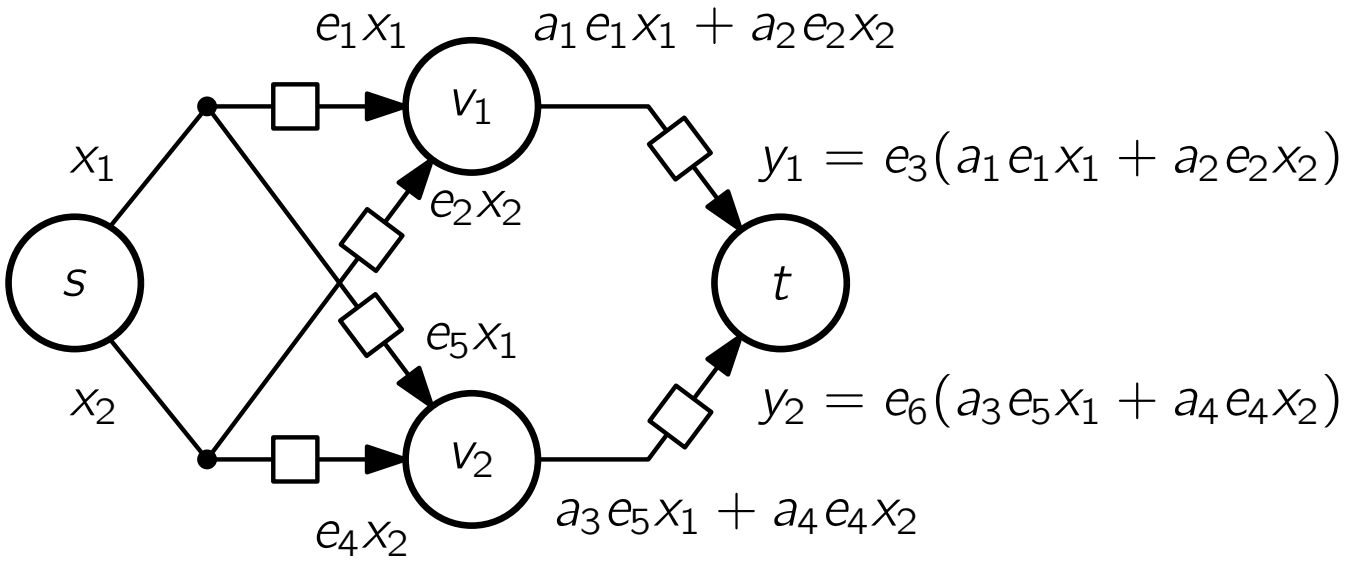


Apagamentos:
$e_i \in \{0, 1\}$

Combinações lineares:
$a_i \in \mathbb{F}_q$

Codificação de rede linear: Difusão e apagamentos

Modelo com enlaces de difusão (*broadcast*) e apagamentos:

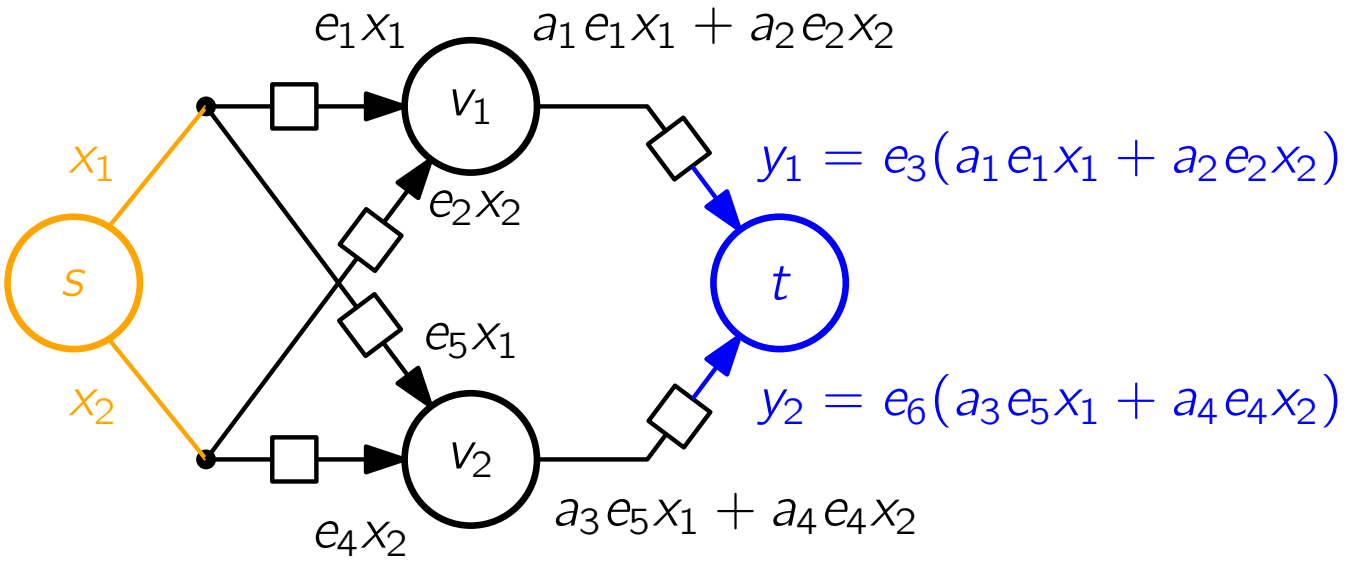


Apagamentos:
$e_i \in \{0, 1\}$

Combinações lineares:
$a_i \in \mathbb{F}_q$

Codificação de rede linear: Difusão e apagamentos

Modelo com enlaces de difusão (*broadcast*) e apagamentos:



Apagamentos:
$e_i \in \{0, 1\}$

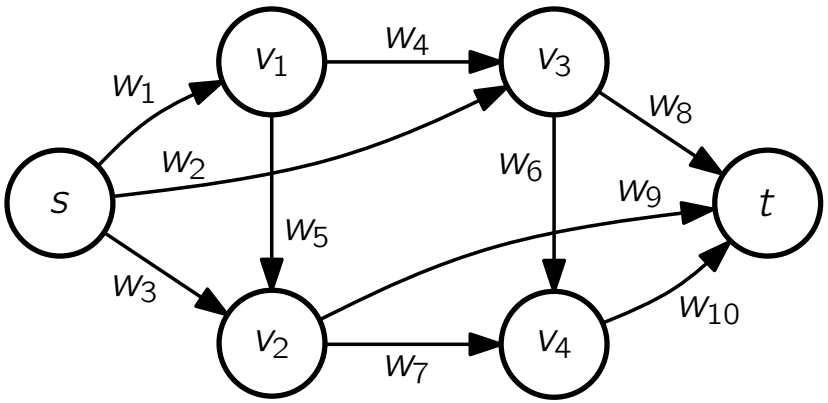
Combinações lineares:
$a_i \in \mathbb{F}_q$

Forma matricial:

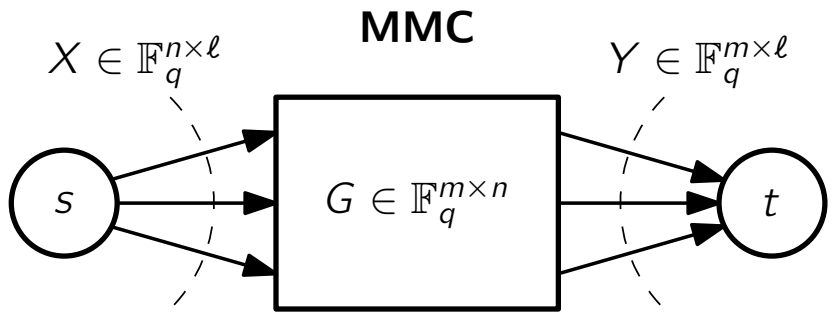
$$\underbrace{\begin{bmatrix} — & y_1 & — \\ — & y_2 & — \end{bmatrix}}_{Y} = \underbrace{\begin{bmatrix} e_3a_1e_1 & e_3a_2e_2 \\ e_6a_3e_5 & e_6a_4e_4 \end{bmatrix}}_{G} \underbrace{\begin{bmatrix} — & x_1 & — \\ — & x_2 & — \end{bmatrix}}_{X}$$

Codificação de rede linear: Modelo fim-a-fim

Modelo fim-a-fim de codificação de rede linear:



$\Longrightarrow$



n: # pacotes enviados m: # pacotes recebidos

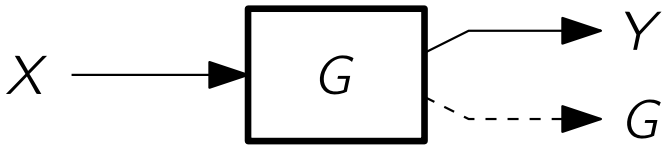
ℓ: comprimento do pacote

A matriz de transferência depende de:

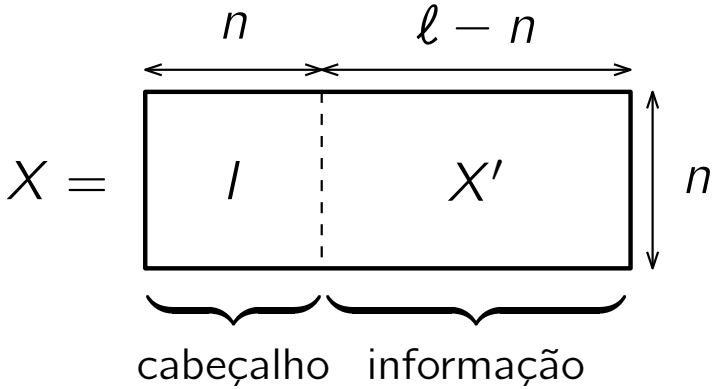
- Topologia da rede (possivelmente variante no tempo).
- Combinações lineares (possivelmente aleatórias).
- Probabilidades de apagamento.

Cenários de interesse

Cenário coerente

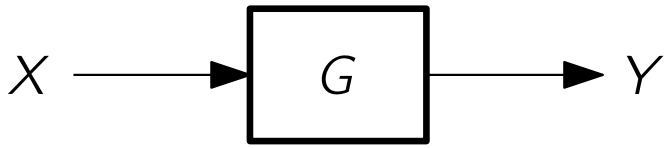


- G conhecida pelo receptor.
- Na prática, através de cabeçalhos:



$$Y = GX = G[I \;\; X'] = [G \;\; GX']$$

Cenário não-coerente



- G desconhecida pelo receptor.
- Por exemplo, comunicação via subespaços. Para G de posto completo:

$$\langle Y \rangle = \langle GX \rangle = \langle X \rangle$$

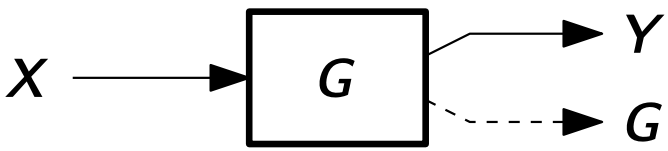
MMC sob a luz da teoria da informação

- Adota-se um modelo probabilístico:
  - $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{G}$ são variáveis aleatórias
  - $\boldsymbol{X}$ e $\boldsymbol{G}$ independentes
  - $\boldsymbol{G}$ é i.i.d. de acordo com $p_{\boldsymbol{G}}$ a cada uso do canal.

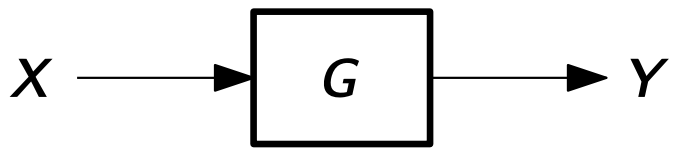
- Obtém-se um canal discreto sem memória (DMC):
  - Probabilidade de transição induzida por $p_{\boldsymbol{G}}$:

$$p_{\boldsymbol{Y},\boldsymbol{G}|\boldsymbol{X}}(Y, G|X) = p_{\boldsymbol{G}}(G)1[Y = GX] \qquad \text{(coerente)}$$

$$p_{\boldsymbol{Y}|\boldsymbol{X}}(Y|X) = \sum_{G} p_{\boldsymbol{G}}(G)1[Y = GX] \qquad \text{(não-coerente)}$$



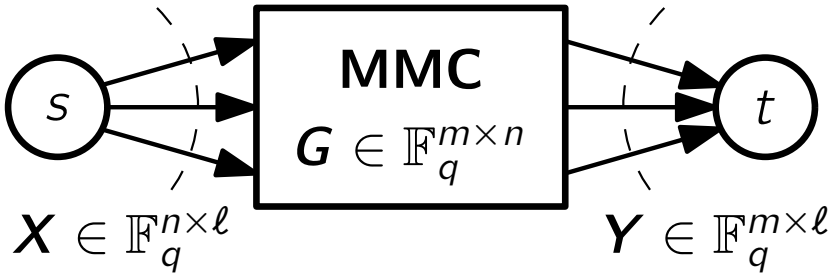
coerente

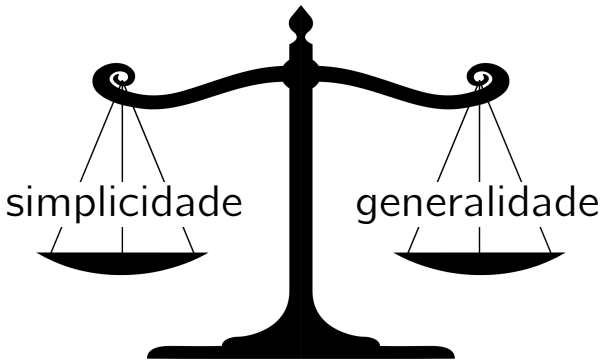


não-coerente

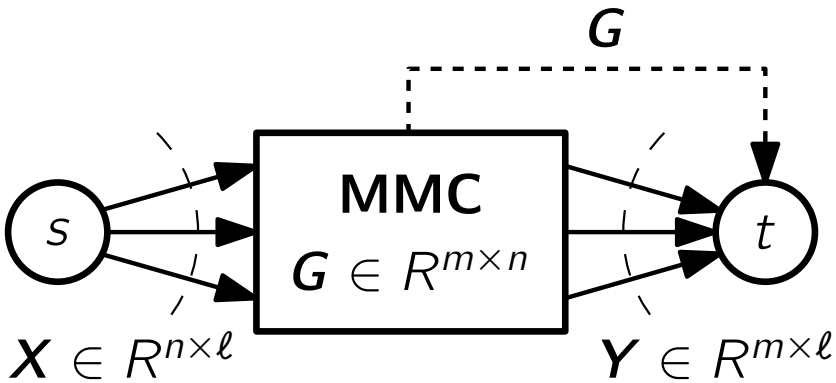
Problemas abordados na tese

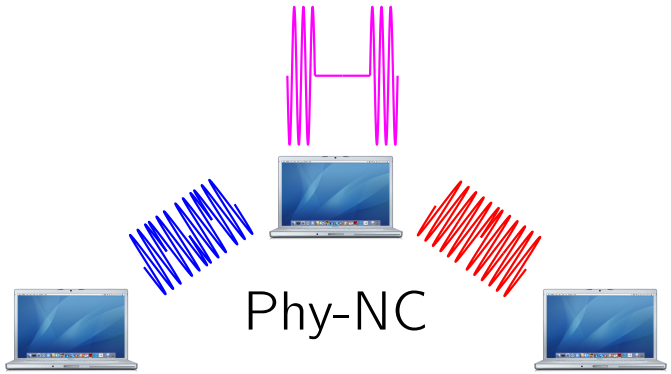
MMC não-coerente sobre corpos finitos





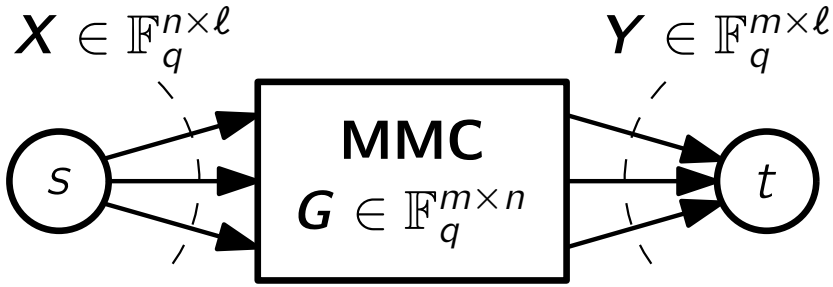
MMC coerente sobre anéis de cadeia finitos





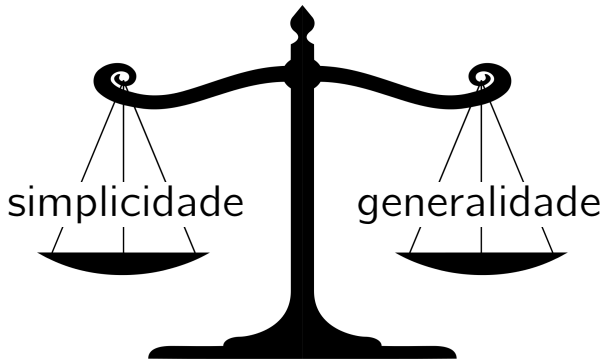
MMC não-coerente sobre corpos finitos com matriz de transferência uniforme dado o posto

Motivação



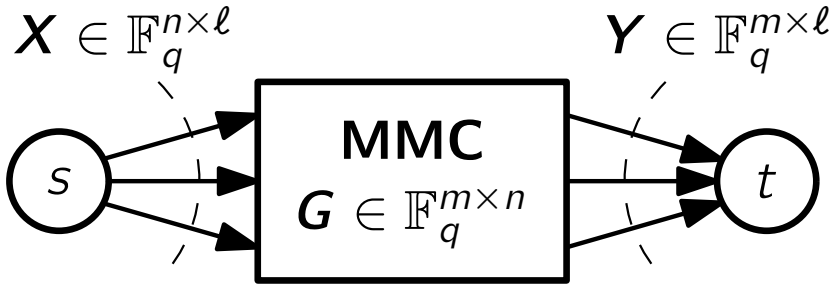
n: # pacotes enviados m: # pacotes recebidos

ℓ: comprimento do pacote Hipótese: $\ell \geq n, m$



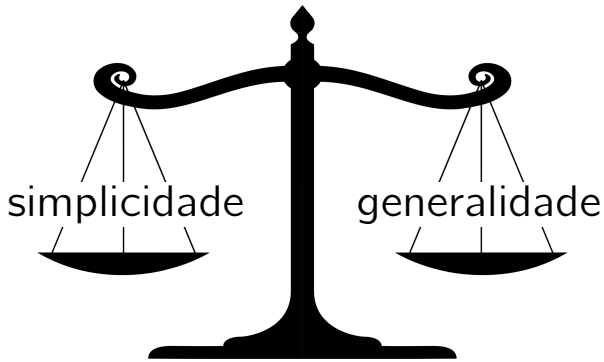
- [Silva et al. '10]: simples e particular.
  - $\boldsymbol{G}$ uniforme sobre todas as matrizes de posto completo.
- [Jafari et al. '11]: simples e particular.
  - $\boldsymbol{G}$ com entradas i.i.d. uniformes $\equiv$ $\boldsymbol{G}$ uniforme sobre todas as matrizes.
- [Yang et al. '10]: complexo e geral.
  - $\boldsymbol{G}$ com distribuição qualquer.
  - Canal: $p_{\boldsymbol{G}} \rightarrow q^{nm}$ parâmetros.

Motivação



n: # pacotes enviados m: # pacotes recebidos

ℓ: comprimento do pacote Hipótese: $\ell \geq n, m$



- Modelo proposto: compromisso entre simplicidade e generalidade.
  - $\boldsymbol{G}$ uniforme dado o posto (u.g.r., *uniform given rank*).
    - Distribuição de posto p_r qualquer.
    - Matrizes de mesmo posto equiprováveis.
  - Casos particulares:
    - $\boldsymbol{G}$ uniforme de posto completo [Silva et al. '10].
    - $\boldsymbol{G}$ com entradas i.i.d. uniformes [Jafari et al. '11].
  - Canal: $p_r \rightarrow \min\{n, m\} + 1$ parâmetros.

O modelo u.g.r. como o pior caso

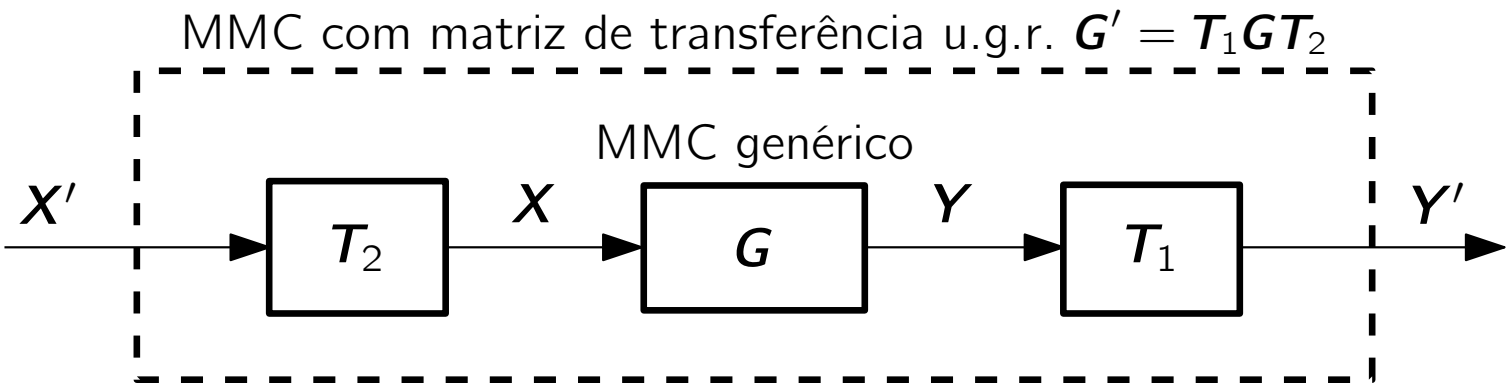
Sejam $\boldsymbol{T}_1$ e $\boldsymbol{T}_2$ matrizes inversíveis uniformemente distribuídas.

Teorema

Se $\boldsymbol{G} \in \mathbb{F}_q^{m \times n}$ é uma matriz aleatória com distribuição qualquer, então

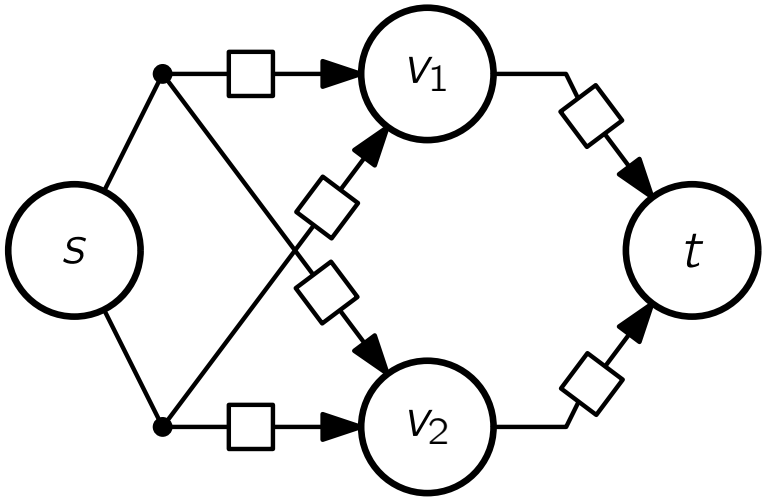
$$\boldsymbol{G}' = \boldsymbol{T}_1 \boldsymbol{G} \boldsymbol{T}_2$$

é u.g.r. e possui a mesma distribuição de posto de $\boldsymbol{G}$.

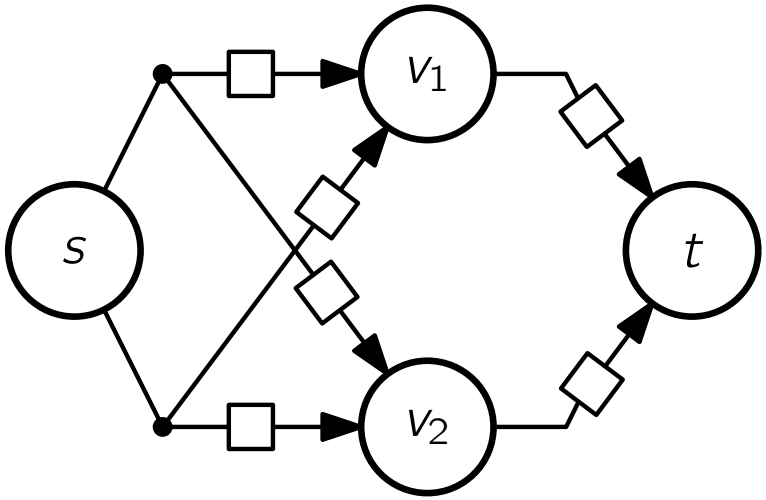


$\Longrightarrow$ Capacidade u.g.r. é um limitante inferior para a capacidade real.

Exemplo 1: Obtendo a distribuição de G

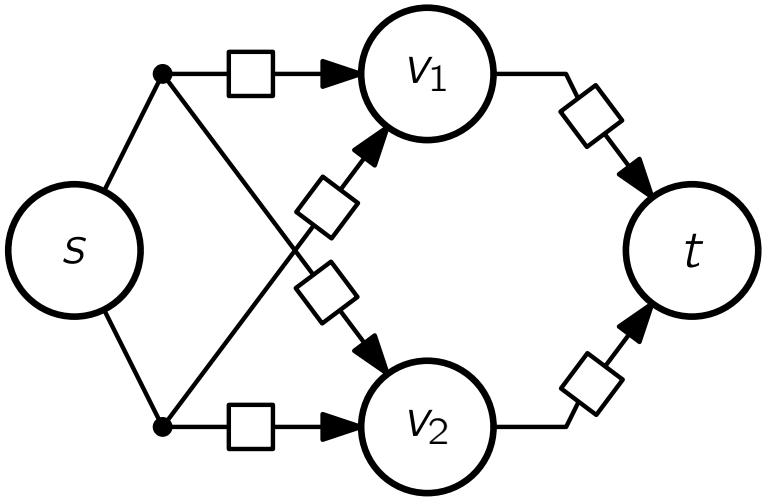


Exemplo 1: Obtendo a distribuição de G



$$G = \begin{bmatrix} e_3 a_1 e_1 & e_3 a_2 e_2 \\ e_6 a_3 e_5 & e_6 a_4 e_4 \end{bmatrix} \in \mathbb{F}_2^{2\times 2}$$

Exemplo 1: Obtendo a distribuição de G

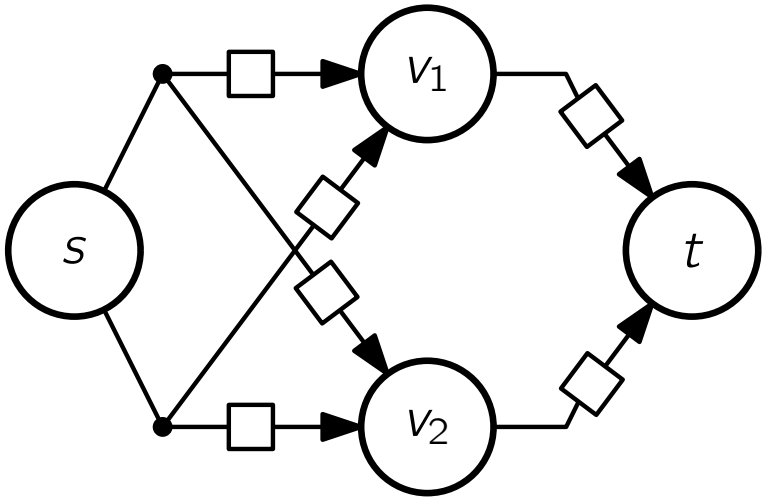


$$G = \begin{bmatrix} e_3 a_1 e_1 & e_3 a_2 e_2 \\ e_6 a_3 e_5 & e_6 a_4 e_4 \end{bmatrix} \in \mathbb{F}_2^{2\times 2}$$

$$e_i \sim \begin{cases} 0, & \text{w.p. } 1/4 \\ 1, & \text{w.p. } 3/4 \end{cases}$$

$$a_i \sim \text{Unif}(\mathbb{F}_2)$$

Exemplo 1: Obtendo a distribuição de G



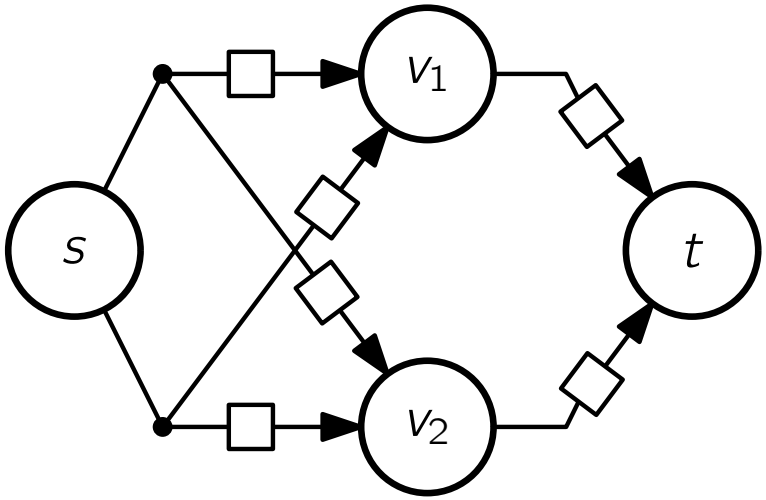
$$G = \begin{bmatrix} e_3 a_1 e_1 & e_3 a_2 e_2 \\ e_6 a_3 e_5 & e_6 a_4 e_4 \end{bmatrix} \in \mathbb{F}_2^{2\times 2}$$

$$e_i \sim \begin{cases} 0, & \text{w.p. } 1/4 \\ 1, & \text{w.p. } 3/4 \end{cases}$$

$$a_i \sim \text{Unif}(\mathbb{F}_2)$$

$\begin{bmatrix}0&0\\0&0\end{bmatrix}$ 0,295	$\begin{bmatrix}1&0\\0&0\end{bmatrix}$ 0,095	$\begin{bmatrix}0&1\\0&0\end{bmatrix}$ 0,095	$\begin{bmatrix}0&0\\1&0\end{bmatrix}$ 0,095
$\begin{bmatrix}0&0\\0&1\end{bmatrix}$ 0,095	$\begin{bmatrix}1&1\\0&0\end{bmatrix}$ 0,057	$\begin{bmatrix}0&0\\1&1\end{bmatrix}$ 0,057	$\begin{bmatrix}1&0\\1&0\end{bmatrix}$ 0,031
$\begin{bmatrix}0&1\\0&1\end{bmatrix}$ 0,031	$\begin{bmatrix}1&1\\1&1\end{bmatrix}$ 0,011	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$ 0,031	$\begin{bmatrix}0&1\\1&0\end{bmatrix}$ 0,031
$\begin{bmatrix}1&1\\1&0\end{bmatrix}$ 0,019	$\begin{bmatrix}1&1\\0&1\end{bmatrix}$ 0,019	$\begin{bmatrix}1&0\\1&1\end{bmatrix}$ 0,019	$\begin{bmatrix}0&1\\1&1\end{bmatrix}$ 0,019

Exemplo 1: Obtendo a distribuição de G

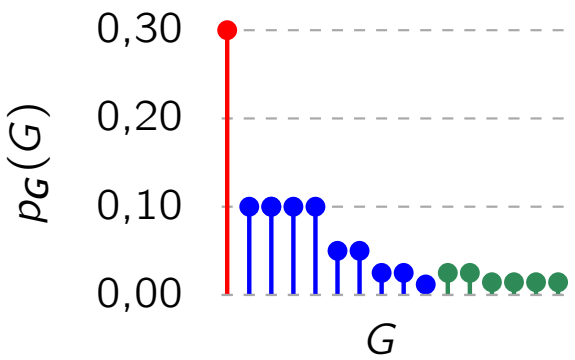


$$G = \begin{bmatrix} e_3 a_1 e_1 & e_3 a_2 e_2 \\ e_6 a_3 e_5 & e_6 a_4 e_4 \end{bmatrix} \in \mathbb{F}_2^{2\times 2}$$

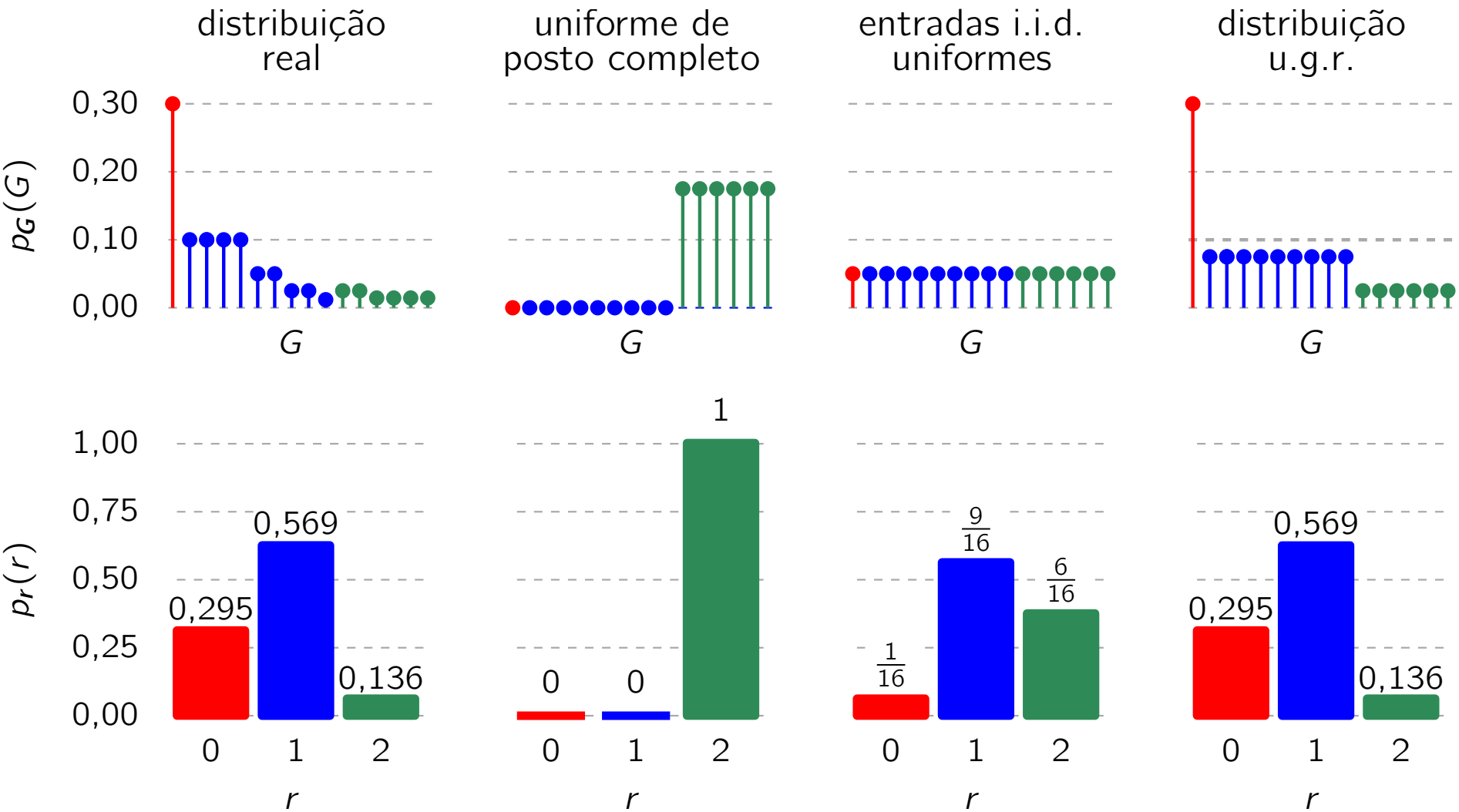
$$e_i \sim \begin{cases} 0, & \text{w.p. } 1/4 \\ 1, & \text{w.p. } 3/4 \end{cases}$$

$$a_i \sim \text{Unif}(\mathbb{F}_2)$$

$\begin{bmatrix}0&0\\0&0\end{bmatrix}$ 0,295	$\begin{bmatrix}1&0\\0&0\end{bmatrix}$ 0,095	$\begin{bmatrix}0&1\\0&0\end{bmatrix}$ 0,095	$\begin{bmatrix}0&0\\1&0\end{bmatrix}$ 0,095
$\begin{bmatrix}0&0\\0&1\end{bmatrix}$ 0,095	$\begin{bmatrix}1&1\\0&0\end{bmatrix}$ 0,057	$\begin{bmatrix}0&0\\1&1\end{bmatrix}$ 0,057	$\begin{bmatrix}1&0\\1&0\end{bmatrix}$ 0,031
$\begin{bmatrix}0&1\\0&1\end{bmatrix}$ 0,031	$\begin{bmatrix}1&1\\1&1\end{bmatrix}$ 0,011	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$ 0,031	$\begin{bmatrix}0&1\\1&0\end{bmatrix}$ 0,031
$\begin{bmatrix}1&1\\1&0\end{bmatrix}$ 0,019	$\begin{bmatrix}1&1\\0&1\end{bmatrix}$ 0,019	$\begin{bmatrix}1&0\\1&1\end{bmatrix}$ 0,019	$\begin{bmatrix}0&1\\1&1\end{bmatrix}$ 0,019

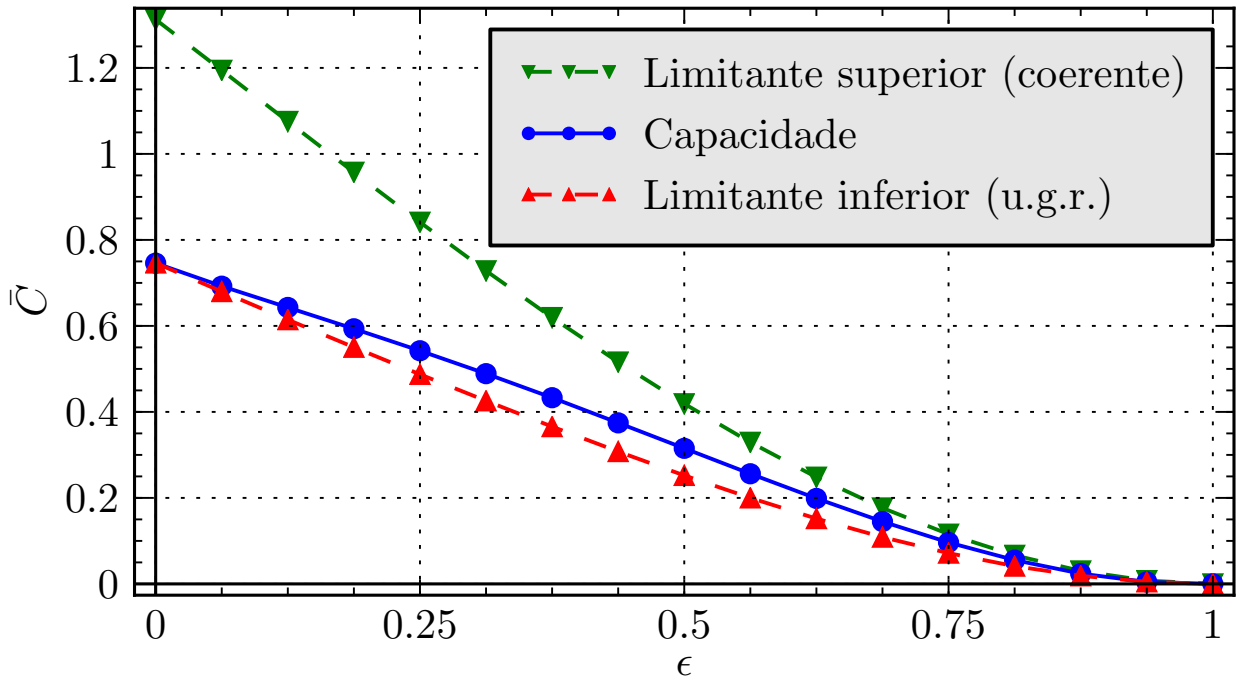


Exemplo 1: Comparação entre os modelos

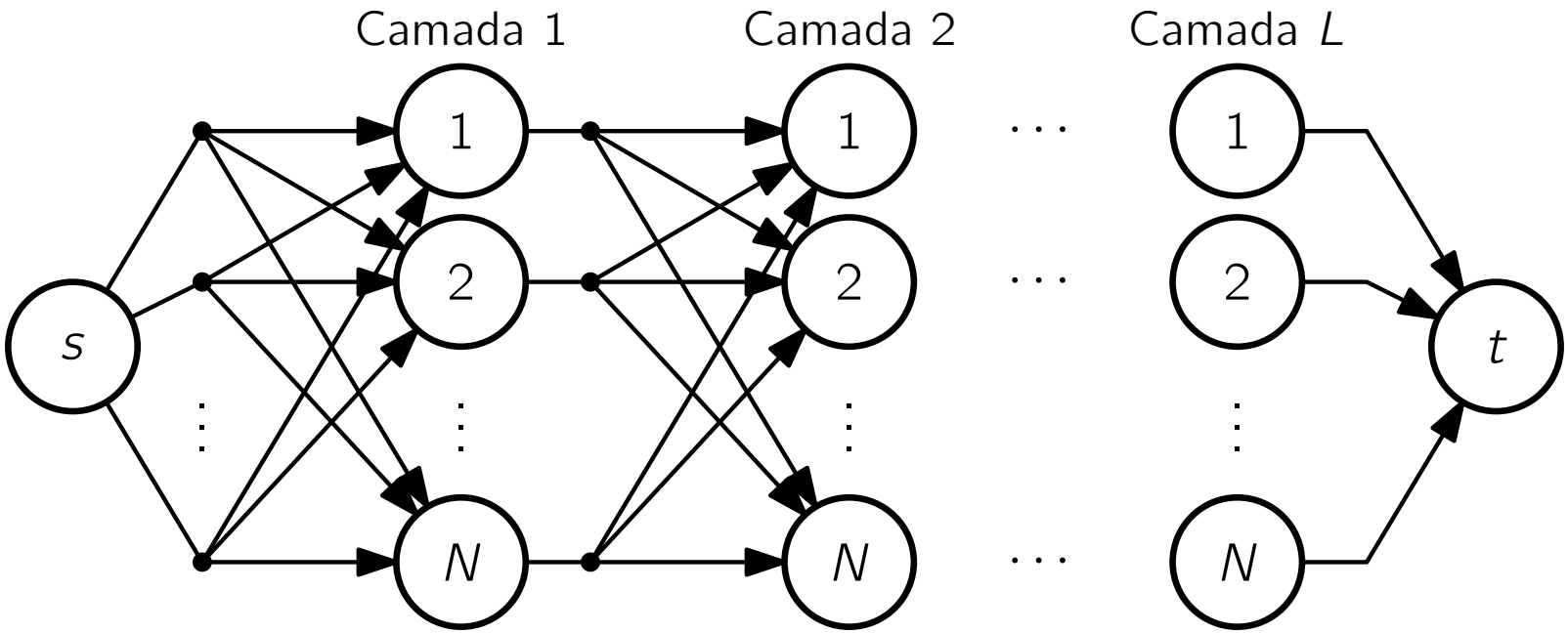


Exemplo 1: $q = 2$, $n = m = 2$, $\ell = 3$ $(q^{n\ell} = 64)$

Capacidade em função da probabilidade de apagamento ϵ:



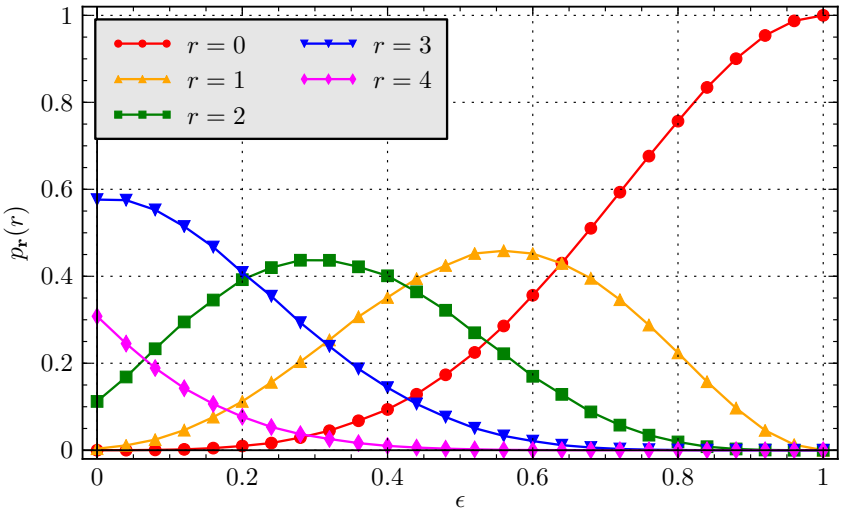
Exemplo 2: Rede sem-fio em camadas

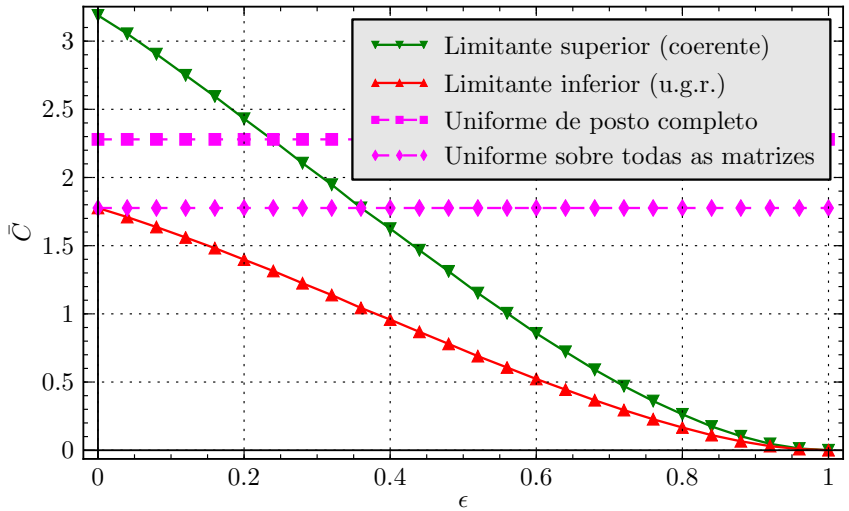


- L : # camadas
- N : # nós retransmissores por camada
- M: # pacotes por enlace $(n = m = NM)$

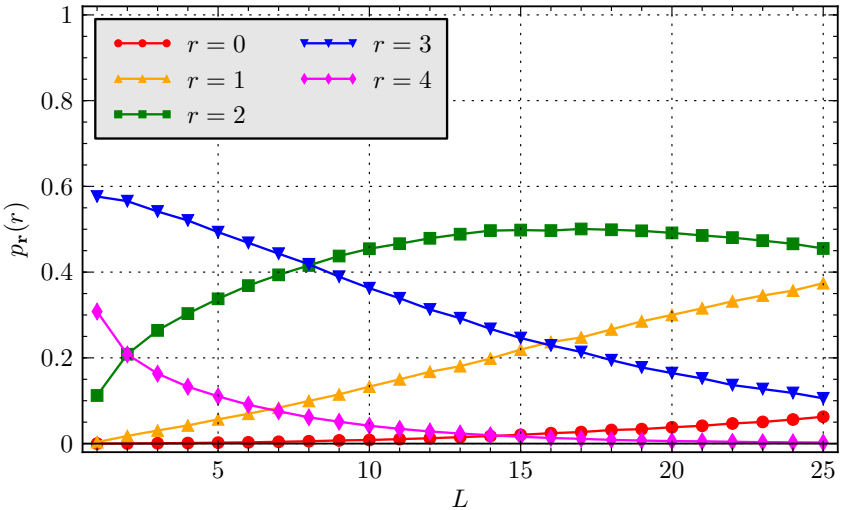
Exemplo 2: $q = 2$, $n = m = 4$, $\ell = 8$ $(q^{n\ell} = 2^{32})$

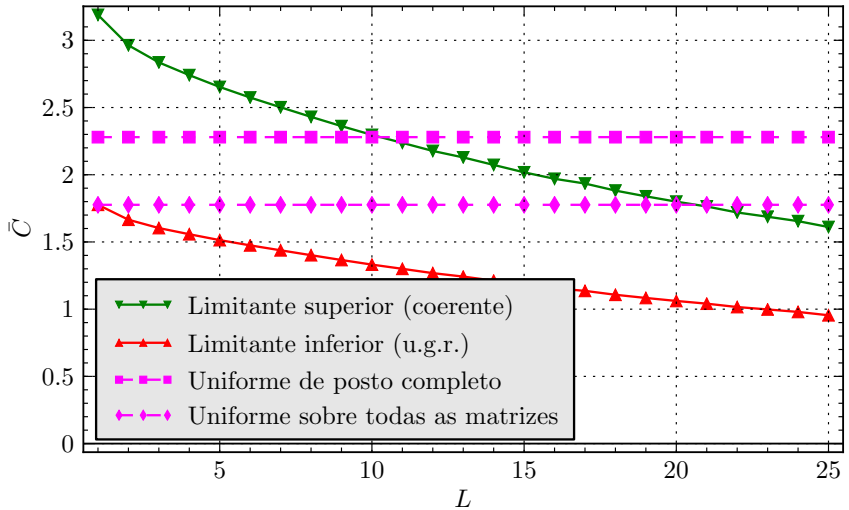
Distribuição de posto e capacidade em função de ϵ, para $L = 1$:





Distribuição de posto e capacidade em função de L, para $\epsilon = 0$:





Probabilidade de transição do canal

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

Teorema

A probabilidade de transição do canal é dada por

$$p_{\boldsymbol{Y}|\boldsymbol{X}}(Y|X) = \frac{p_{\boldsymbol{v}|\boldsymbol{u}}(v|u)}{|\mathcal{T}_v(\mathbb{F}_q^{m\times u})|} 1[\langle Y\rangle \subseteq \langle X\rangle],$$

em que

$$p_{\boldsymbol{v}|\boldsymbol{u}}(v|u) = \sum_r p_{\boldsymbol{r}}(r) \frac{\begin{bmatrix} u \\ v \end{bmatrix}_q}{\begin{bmatrix} n \\ r \end{bmatrix}_q} \begin{bmatrix} n-u \\ r-v \end{bmatrix}_q q^{v(n-u-r+v)}$$

é a probabilidade de transição do posto.

$\Longrightarrow$ Simetria: Probabilidade de transição depende apenas dos postos.

Probabilidade de transição do canal: Ideia da prova

O cálculo de $p_{\boldsymbol{Y}|\boldsymbol{X}}$ se reduz a um problema de contagem.

Problema: Dadas $X \in \mathbb{F}_q^{n\times\ell}$ de posto u e $Y \in \mathbb{F}_q^{m\times\ell}$ de posto v, quantas matrizes $G \in \mathbb{F}_q^{m\times n}$ de posto r são tais que $Y = GX$?

Solução: $|\mathcal{T}_{r-v}(\mathbb{F}_q^{(m-v)\times(n-u)})|q^{v(n-u)}$.

Capacidade do canal

Teorema

A capacidade do canal é dada por

$$C \triangleq \max_{p_{\boldsymbol{X}}} I(\boldsymbol{X};\boldsymbol{Y}) = \max_{p_{\boldsymbol{u}}} I^*(p_{\boldsymbol{u}}),$$

em que

$$I^*(p_{\boldsymbol{u}}) = \sum_{v} p_{\boldsymbol{v}}(v) \log_q \frac{|\mathcal{T}_v(\mathbb{F}_q^{m\times \ell})|}{p_{\boldsymbol{v}}(v)} - \sum_{u,v} p_{\boldsymbol{v}|\boldsymbol{u}}(v|u) \log_q \frac{|\mathcal{T}_v(\mathbb{F}_q^{m\times u})|}{p_{\boldsymbol{v}|\boldsymbol{u}}(v|u)} p_{\boldsymbol{u}}(u),$$

sendo alcançada com entrada u.g.r.

$\Longrightarrow$ Otimização convexa: redução de $q^{n\ell}$ para $n+1$ variáveis.

Capacidade do canal: Ideia da prova

A maximização é dividida em duas etapas:

$$C \triangleq \max_{p_{\boldsymbol{X}}} I(\boldsymbol{X};\boldsymbol{Y}) = \max_{p_{\boldsymbol{u}}} \max_{p_{\boldsymbol{X}}:p_{\boldsymbol{u}}} I(\boldsymbol{X};\boldsymbol{Y})$$

Etapa interna: Resolvida. Máximo é alcançado com entrada u.g.r.

$$\max_{p_{\boldsymbol{X}}:p_{\boldsymbol{u}}} I(\boldsymbol{X};\boldsymbol{Y}) = I^*(p_{\boldsymbol{u}}) = \text{formula do slide anterior}$$

Etapa externa: Não existe solução em forma fechada (em geral).

$$\max_{p_{\boldsymbol{u}}} I^*(p_{\boldsymbol{u}}) = \text{problema de otimização convexa}$$

Entrada de posto constante

- $C_u \rightarrow$ capacidade de posto u:
  Máxima informação mútua com entrada de posto u.
- $C_{u^*} \rightarrow$ capacidade de posto constante:
  Máximo entre os C_u, i.e., $C_{u^*} \triangleq \max_u C_u$.

Potencial simplificação dos esquemas de codificação.

Entrada de posto constante

- $C_u \rightarrow$ capacidade de posto u:
  Máxima informação mútua com entrada de posto u.
- $C_{u^*} \rightarrow$ capacidade de posto constante:
  Máximo entre os C_u, i.e., $C_{u^*} \triangleq \max_u C_u$.

Potencial simplificação dos esquemas de codificação.

Teorema

A capacidade de posto u do canal é dada por

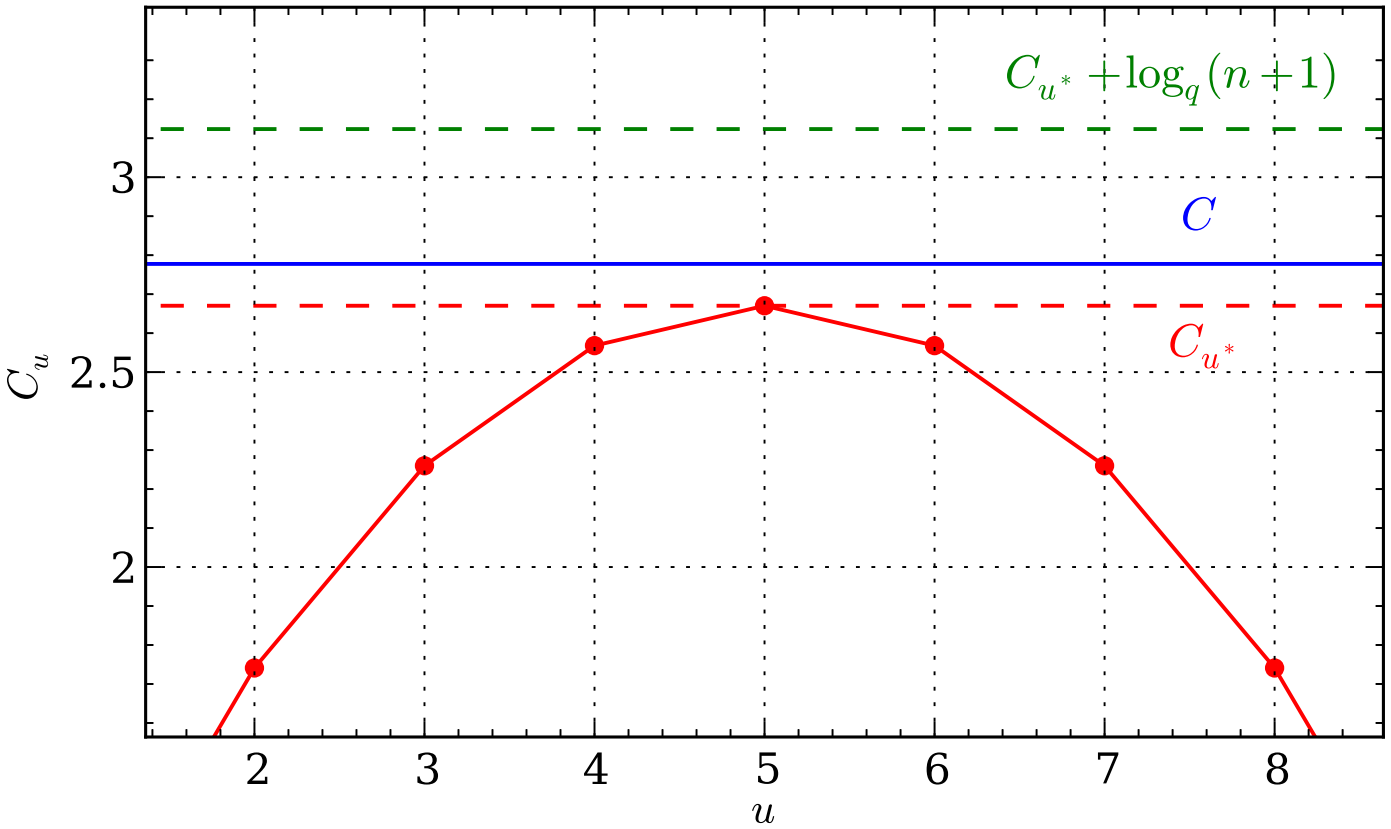
$$C_u = \sum_{v=0}^{n} p_{\boldsymbol{v}|\boldsymbol{u}}(v|u) \log_q \frac{\begin{bmatrix} m \\ v \end{bmatrix}_q}{\begin{bmatrix} u \\ v \end{bmatrix}_q},$$

sendo alcançada com entrada uniforme. Além disso,

$$C_{u^*} \leq C \leq C_{u^*} + \log_q(\min\{n, m\} + 1).$$

Exemplo 3: $q = 2$, $n = m = \ell = 10$

Capacidade de posto u para $\boldsymbol{G}$ uniforme de posto completo:



Comportamento assintótico

Entrada de posto constante é assintoticamente ótima (em q ou ℓ).

Teorema

Assintoticamente em q, a capacidade é dada por

$$\lim_{q\to\infty} C = \max_{u} \left[(\ell - u) \sum_{r} p_{\boldsymbol{r}}^{\infty}(r) \min\{u, r\} \right],$$

sendo alcançada com entrada uniforme de posto constante.

Comportamento assintótico

Entrada de posto constante é assintoticamente ótima (em q ou ℓ).

Teorema

Assintoticamente em q, a capacidade é dada por

$$\lim_{q\to\infty} C = \max_{u} \left[(\ell - u) \sum_{r} p_{\boldsymbol{r}}^{\infty}(r) \min\{u, r\} \right],$$

sendo alcançada com entrada uniforme de posto constante.

Teorema

Assintoticamente em ℓ, a capacidade *normalizada* $\bar{C} = C/\ell$ é dada por

$$\lim_{\ell\to\infty} \bar{C} = \mathrm{E}[\boldsymbol{r}],$$

sendo alcançada com entrada uniforme de posto completo.

Comunicação via subespaços

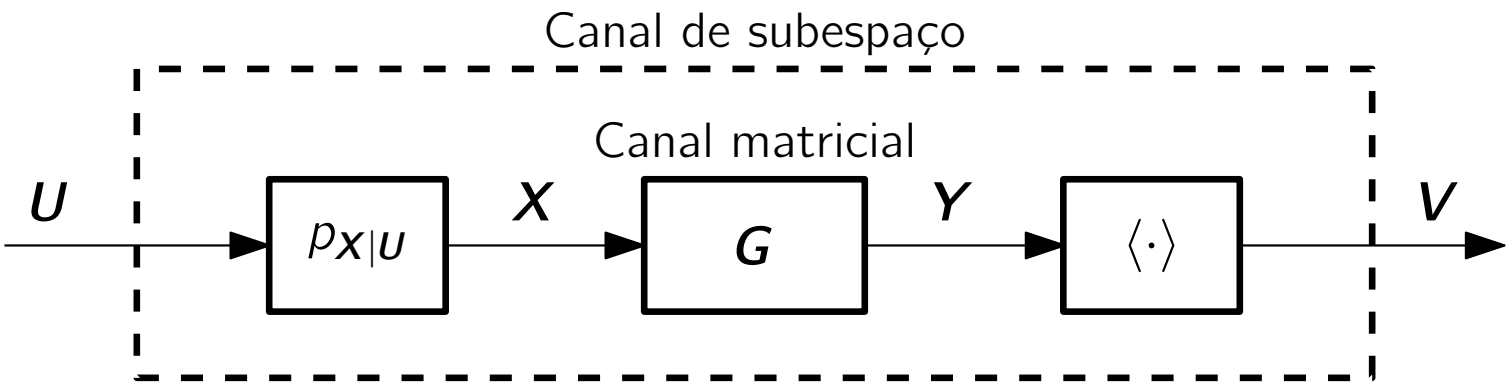
Sejam $\boldsymbol{U} = \langle \boldsymbol{X} \rangle$ e $\boldsymbol{V} = \langle \boldsymbol{Y} \rangle$.

Teorema

Comunicação via subespaços é ótima para $\boldsymbol{G}$ u.g.r. Isto é,

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

qualquer que seja a distribuição de entrada $p_{\boldsymbol{X}}$.



$\Longrightarrow$ Potencial simplificação dos esquemas de codificação.

MMC coerente sobre anéis de cadeia finitos

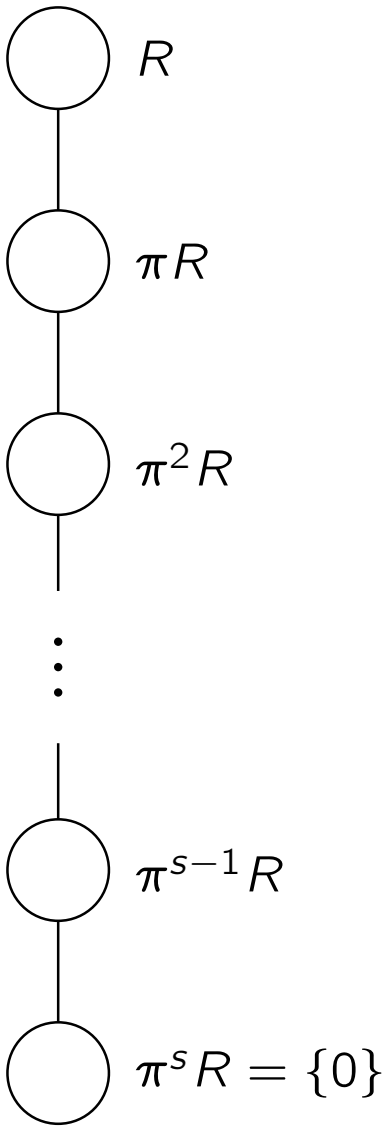
O que são anéis?

- Anéis são estruturas algébricas com duas operações ($+$ e $\times$).
  - Diferentemente de corpos, um elemento $\neq 0$ não precisa ser inversível.
  - Neste trabalho, apenas anéis comutativos com $1 \neq 0$.

O que são anéis?

- Anéis são estruturas algébricas com duas operações ($+$ e $\times$).
  - Diferentemente de corpos, um elemento $\neq 0$ não precisa ser inversível.
  - Neste trabalho, apenas anéis comutativos com $1 \neq 0$.
- Exemplos de anéis finitos:
  - Corpos finitos ($\mathbb{F}_q$).
  - Inteiros módulo-n ($\mathbb{Z}_n$).
  - Quocientes de inteiros Gaussianos (e.g., $\mathbb{Z}_n[i]$).
  - Anéis de cadeia finitos (incluindo $\mathbb{F}_q$, $\mathbb{Z}_{p^k}$, $\mathbb{Z}_{p^k}[i]$).

Anéis de cadeia finitos



Definição

Um anel de cadeia é um anel no qual os ideais são linearmente ordenados de acordo com inclusão de conjuntos ($\subseteq$).

Seja R um anel de cadeia finito, em que:

- π é um gerador do ideal máximo de R.
- s é o número de ideais não-nulos de R.
- q é a ordem do corpo residual $R/\pi R$.

Exemplo: Inteiros módulo-8 ($\mathbb{Z}_8$)

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$\times$	0	1	2	3	4	5	6	7	bin
0	0	0	0	0	0	0	0	0	000
1	0	1	2	3	4	5	6	7	001
2	0	2	4	6	0	2	4	6	010
3	0	3	6	1	4	7	2	5	011
4	0	4	0	4	0	4	0	4	100
5	0	5	2	7	4	1	6	3	101
6	0	6	4	2	0	6	4	2	110
7	0	7	6	5	4	3	2	1	111

Exemplo: Inteiros módulo-8 ($\mathbb{Z}_8$)

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$\times$	0	1	2	3	4	5	6	7	bin
0	0	0	0	0	0	0	0	0	000
1	0	1	2	3	4	5	6	7	001
2	0	2	4	6	0	2	4	6	010
3	0	3	6	1	4	7	2	5	011
4	0	4	0	4	0	4	0	4	100
5	0	5	2	7	4	1	6	3	101
6	0	6	4	2	0	6	4	2	110
7	0	7	6	5	4	3	2	1	111

$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Exemplo: Inteiros módulo-8 ($\mathbb{Z}_8$)

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$\times$	0	1	2	3	4	5	6	7	bin
0	0	0	0	0	0	0	0	0	000
1	0	1	2	3	4	5	6	7	001
2	0	2	4	6	0	2	4	6	010
3	0	3	6	1	4	7	2	5	011
4	0	4	0	4	0	4	0	4	100
5	0	5	2	7	4	1	6	3	101
6	0	6	4	2	0	6	4	2	110
7	0	7	6	5	4	3	2	1	111

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$$\Big|$$

$$2\mathbb{Z}_8 = \{0, 2, 4, 6\}$$

Exemplo: Inteiros módulo-8 ($\mathbb{Z}_8$)

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$\times$	0	1	2	3	4	5	6	7	bin
0	0	0	0	0	0	0	0	0	000
1	0	1	2	3	4	5	6	7	001
2	0	2	4	6	0	2	4	6	010
3	0	3	6	1	4	7	2	5	011
4	0	4	0	4	0	4	0	4	100
5	0	5	2	7	4	1	6	3	101
6	0	6	4	2	0	6	4	2	110
7	0	7	6	5	4	3	2	1	111

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$$\Big|$$

$$2\mathbb{Z}_8 = \{0, 2, 4, 6\}$$

$$\Big|$$

$$4\mathbb{Z}_8 = \{0, 4\}$$

Exemplo: Inteiros módulo-8 ($\mathbb{Z}_8$)

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$\times$	0	1	2	3	4	5	6	7	bin
0	0	0	0	0	0	0	0	0	000
1	0	1	2	3	4	5	6	7	001
2	0	2	4	6	0	2	4	6	010
3	0	3	6	1	4	7	2	5	011
4	0	4	0	4	0	4	0	4	100
5	0	5	2	7	4	1	6	3	101
6	0	6	4	2	0	6	4	2	110
7	0	7	6	5	4	3	2	1	111

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$$\vert$$

$$2\mathbb{Z}_8 = \{0, 2, 4, 6\}$$

$$\vert$$

$$4\mathbb{Z}_8 = \{0, 4\}$$

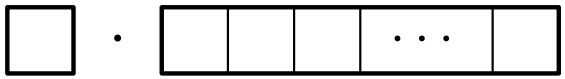
$$\vert$$

$$0\mathbb{Z}_8 = \{0\}$$

Codificação de rede sobre anéis

- Combinações lineares de pacotes.

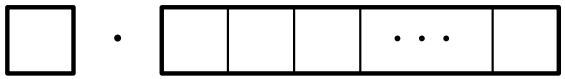
  Soma de pacotes: 

  Multiplicação por escalares: 

Codificação de rede sobre anéis

- Combinações lineares de pacotes.

  Soma de pacotes: 

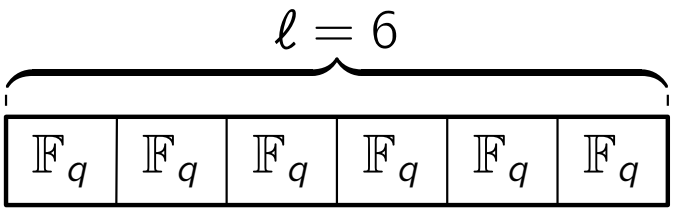
  Multiplicação por escalares: 

- Operações fechadas: Espaço de pacotes $\Omega \rightarrow$ "espaço vetorial".

Exemplo: "Espaços vetoriais" sobre $\mathbb{Z}_8$

Espaços vetoriais sobre $\mathbb{F}_q$

$\Omega =$ cópias do corpo



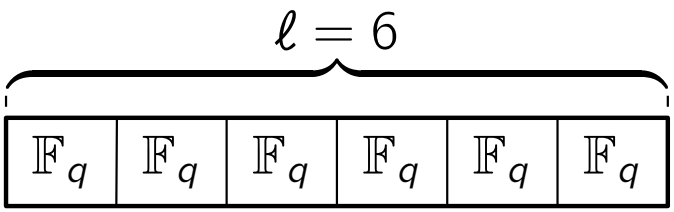
$\dim \Omega = \ell = 6$

dimensão

Exemplo: "Espaços vetoriais" sobre $\mathbb{Z}_8$

Espaços vetoriais sobre $\mathbb{F}_q$

Ω = cópias do corpo

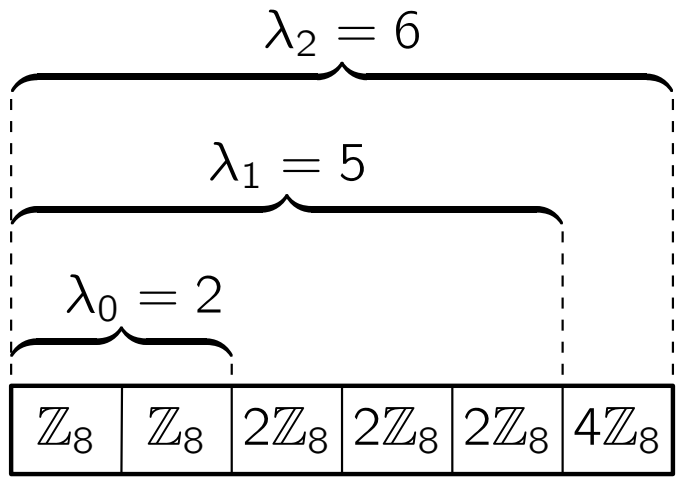


$\dim \Omega = \ell = 6$

dimensão

"Espaços vetoriais" sobre $\mathbb{Z}_8$

Ω pode ser mais geral



$\text{shape}\,\Omega = \lambda = (2, 5, 6)$

shape

Codificação de rede sobre anéis de cadeia finitos

Codificação de rede sobre anéis de cadeia finitos

Por quê?

Rede sem-fio bidirecional com nó intermediário

relay

1

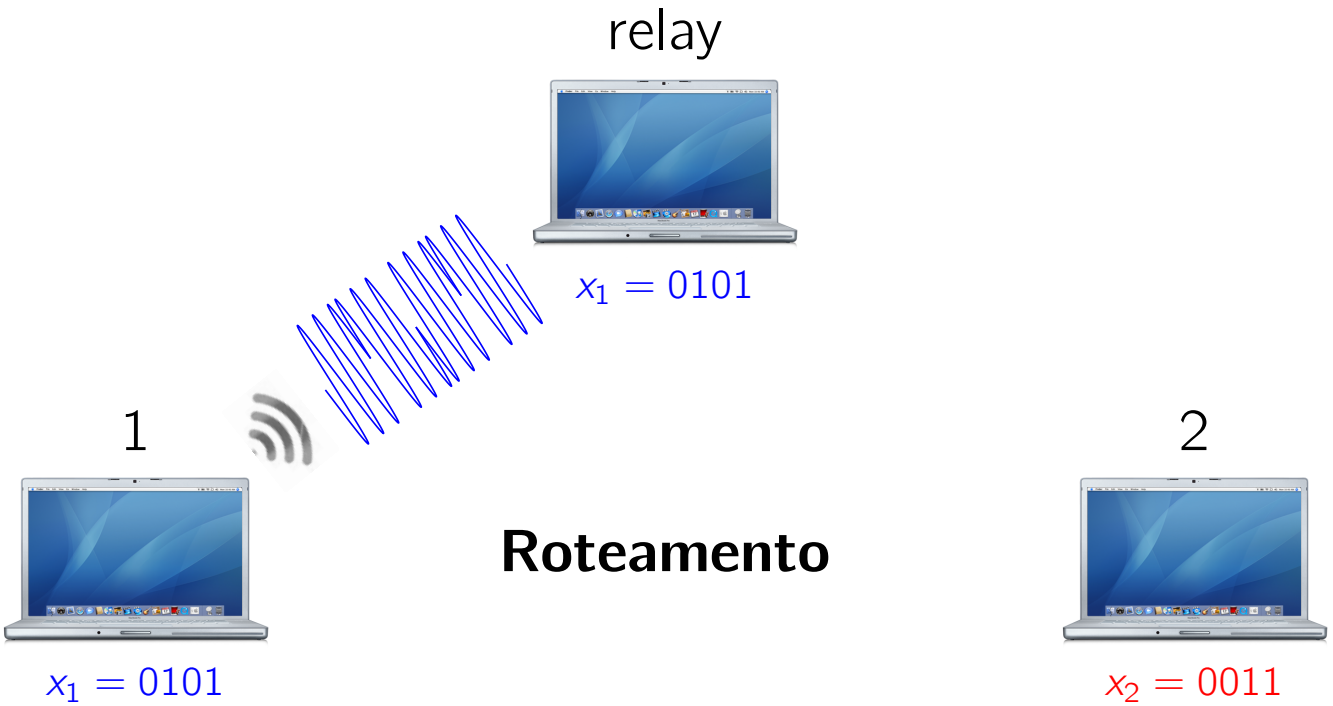
$x_1 = 0101$

Roteamento

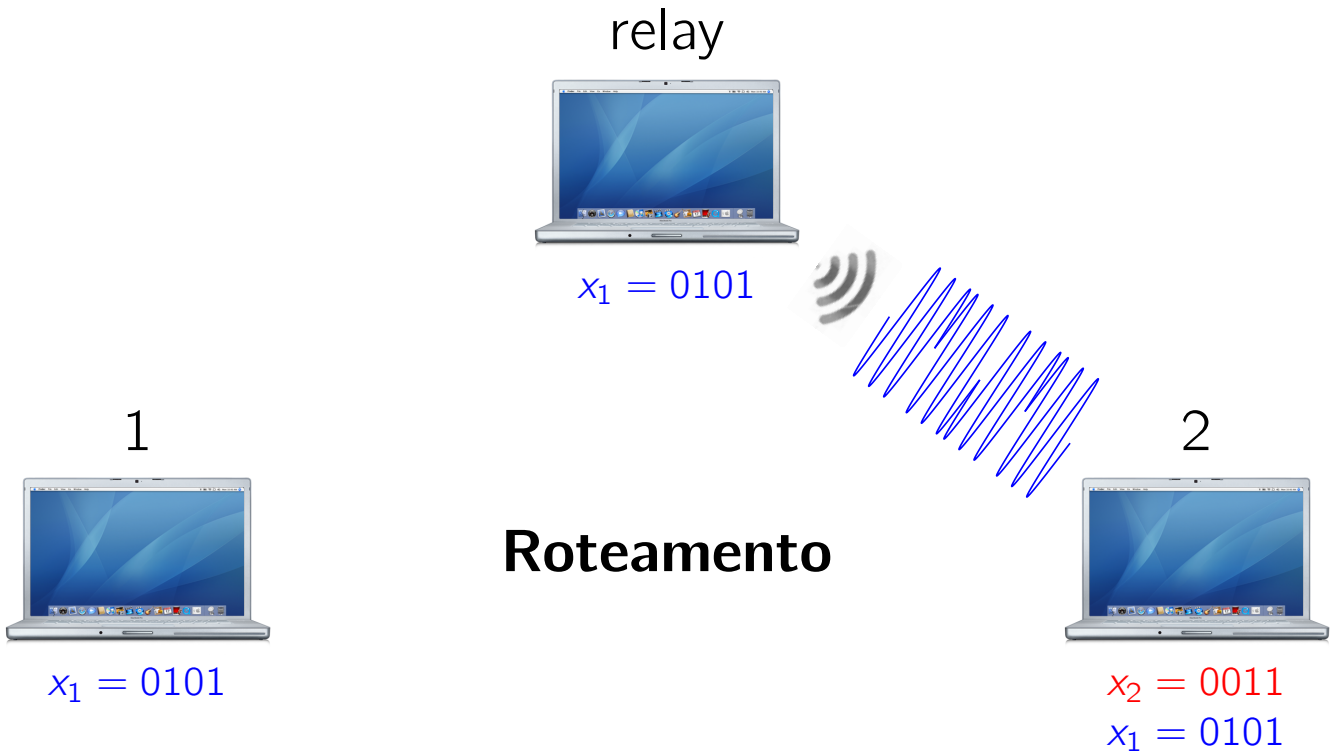
2

$x_2 = 0011$

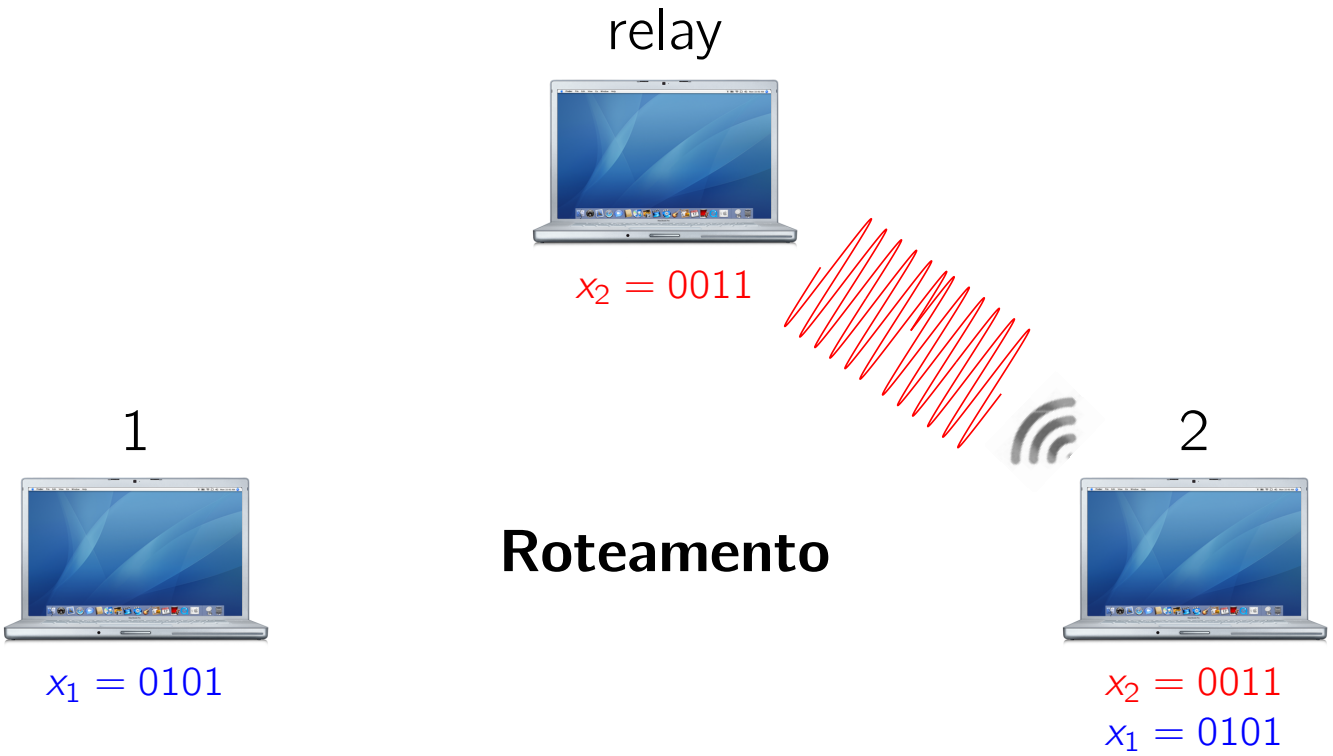
Rede sem-fio bidirecional com nó intermediário



Rede sem-fio bidirecional com nó intermediário



Rede sem-fio bidirecional com nó intermediário



Rede sem-fio bidirecional com nó intermediário

Rede sem-fio bidirecional com nó intermediário

relay

1

$x_1 = 0101$
$x_2 = 0011$

Roteamento
4 instantes de tempo

2

$x_2 = 0011$
$x_1 = 0101$

Rede sem-fio bidirecional com nó intermediário

relay

1

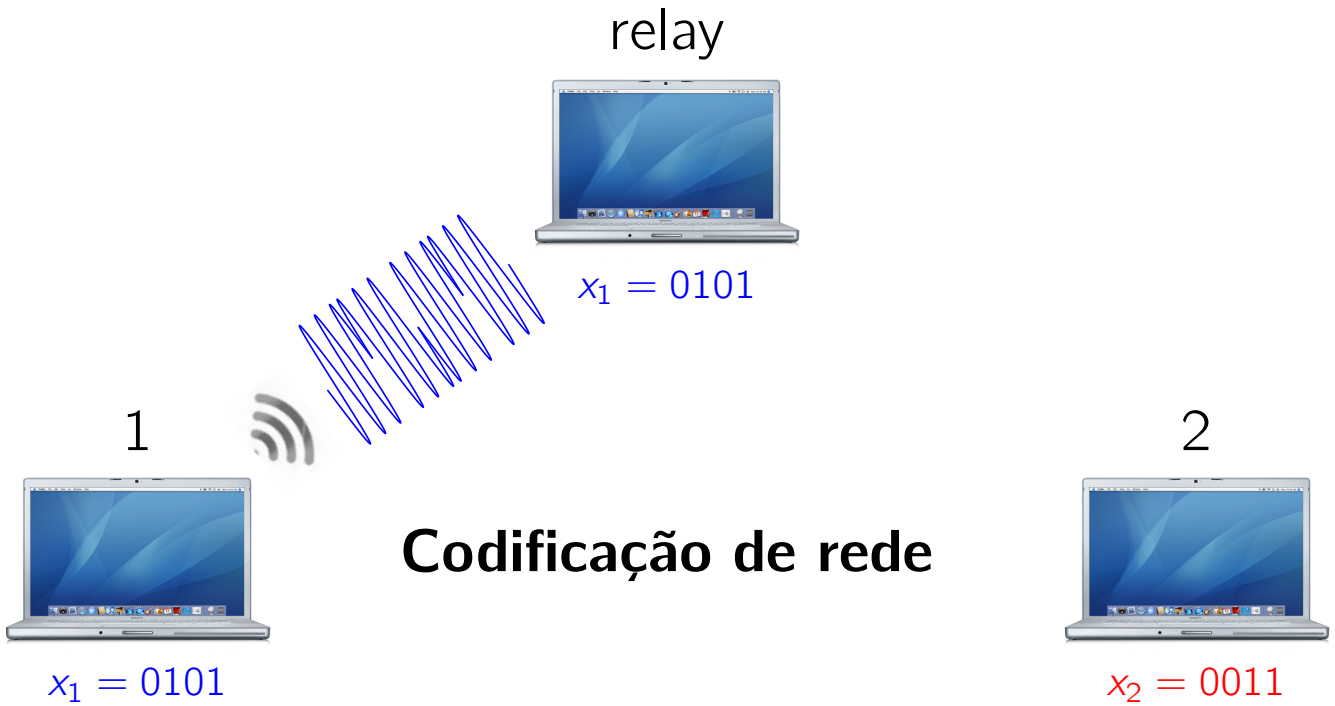
$x_1 = 0101$

Codificação de rede

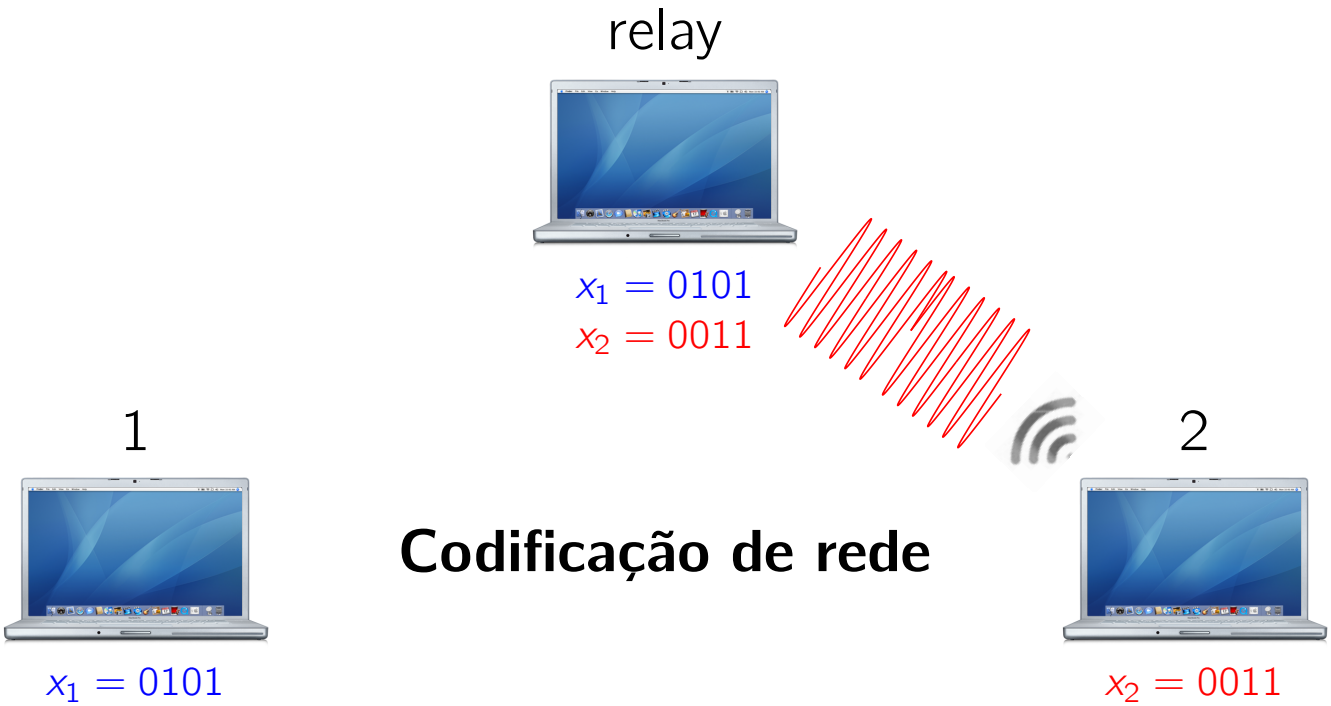
2

$x_2 = 0011$

Rede sem-fio bidirecional com nó intermediário



Rede sem-fio bidirecional com nó intermediário



Rede sem-fio bidirecional com nó intermediário

relay

$x_1 = 0101$

$x_2 = 0011$

$x_1 + x_2 = 0110$

1

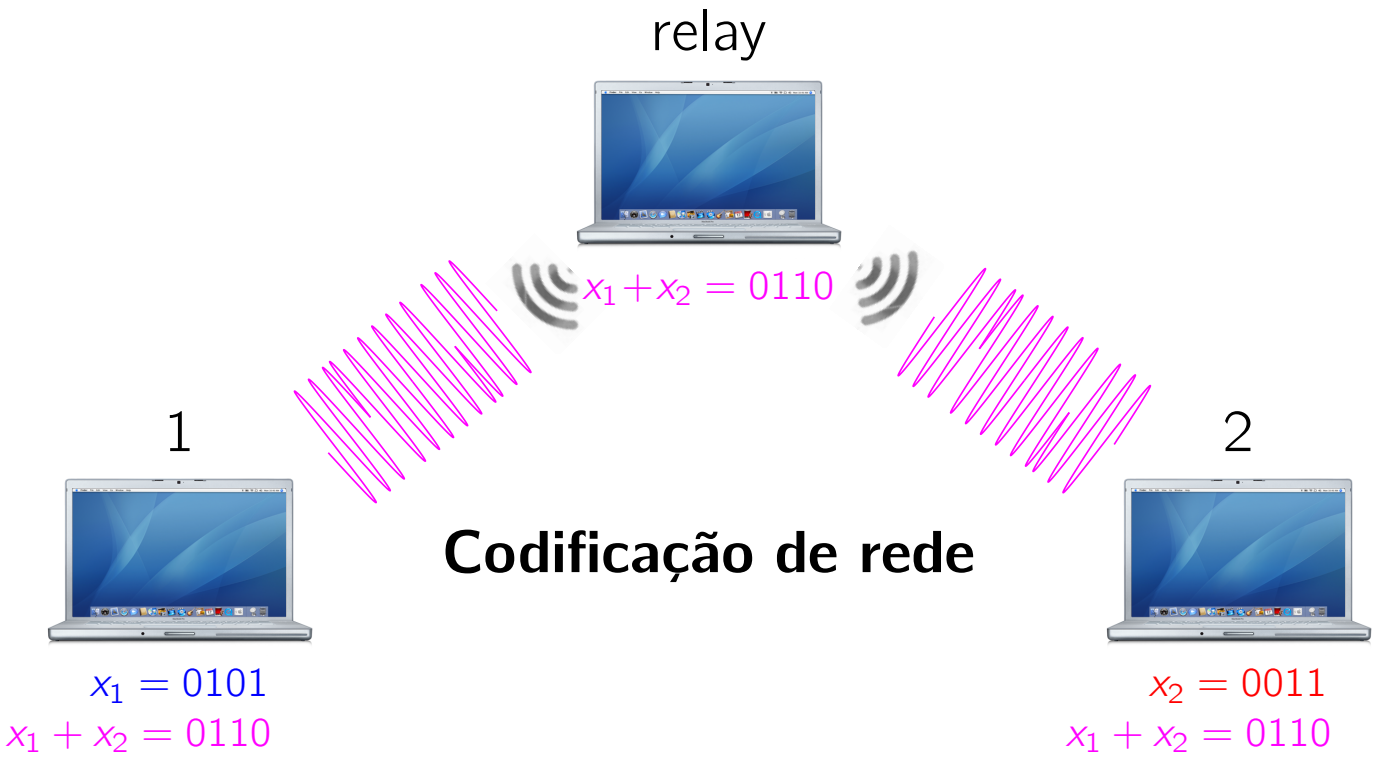
$x_1 = 0101$

Codificação de rede

2

$x_2 = 0011$

Rede sem-fio bidirecional com nó intermediário



Rede sem-fio bidirecional com nó intermediário

relay

1

$x_1 = 0101$

$x_1 + x_2 = 0110$

$x_2 = 0011$

Codificação de rede

2

$x_2 = 0011$

$x_1 + x_2 = 0110$

$x_1 = 0101$

Rede sem-fio bidirecional com nó intermediário

relay

1

$x_1 = 0101$

$x_1 + x_2 = 0110$

$x_2 = 0011$

Codificação de rede

3 instantes de tempo

2

$x_2 = 0011$

$x_1 + x_2 = 0110$

$x_1 = 0101$

Rede sem-fio bidirecional com nó intermediário

relay

1

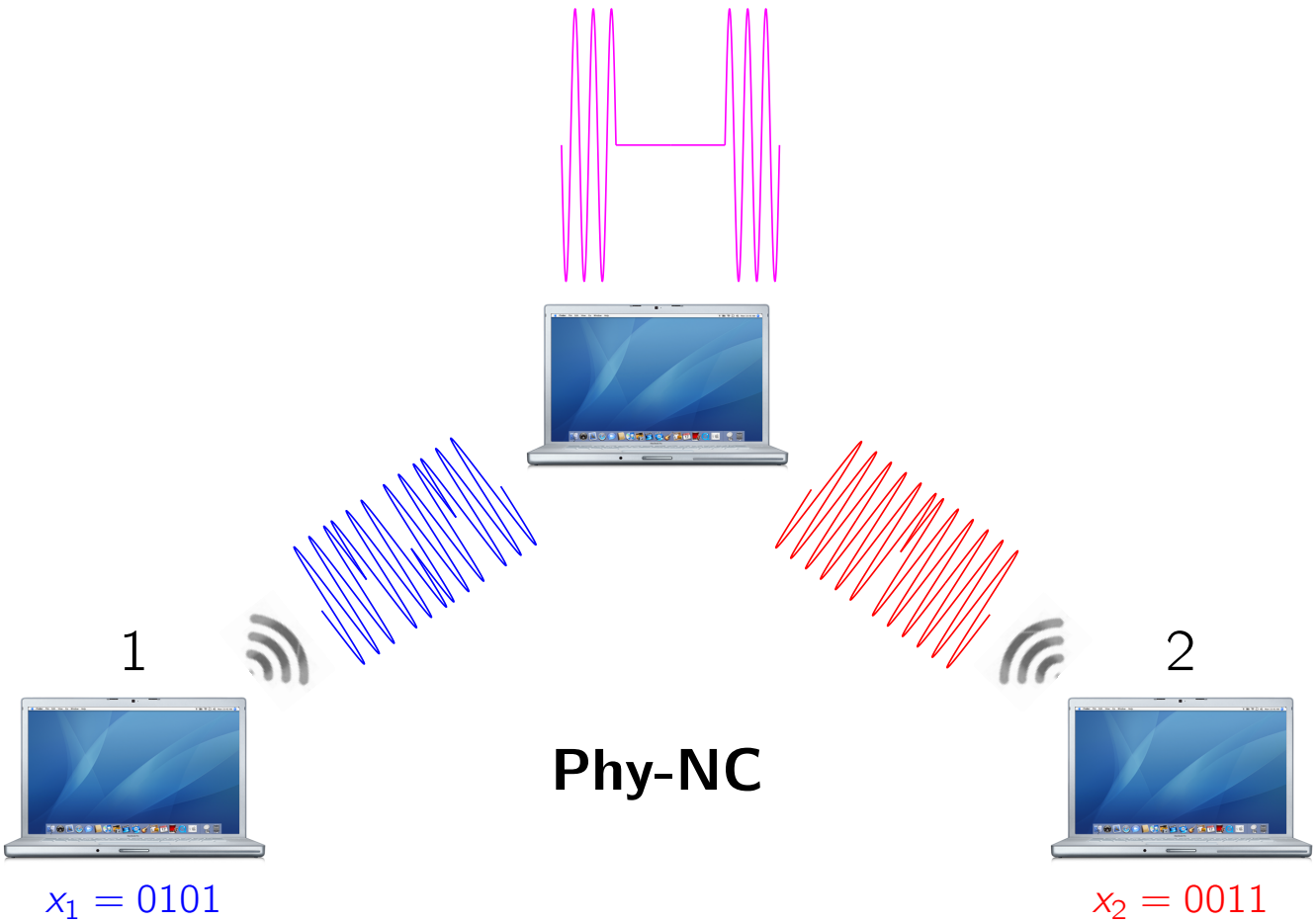
$x_1 = 0101$

Phy-NC

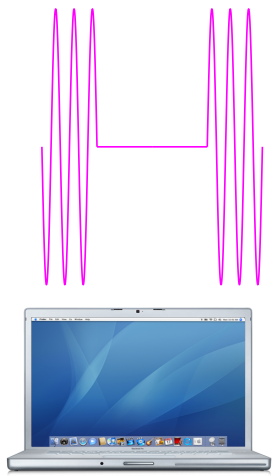
2

$x_2 = 0011$

Rede sem-fio bidirecional com nó intermediário



Rede sem-fio bidirecional com nó intermediário



infere

$x_1 + x_2 = 0110$

1

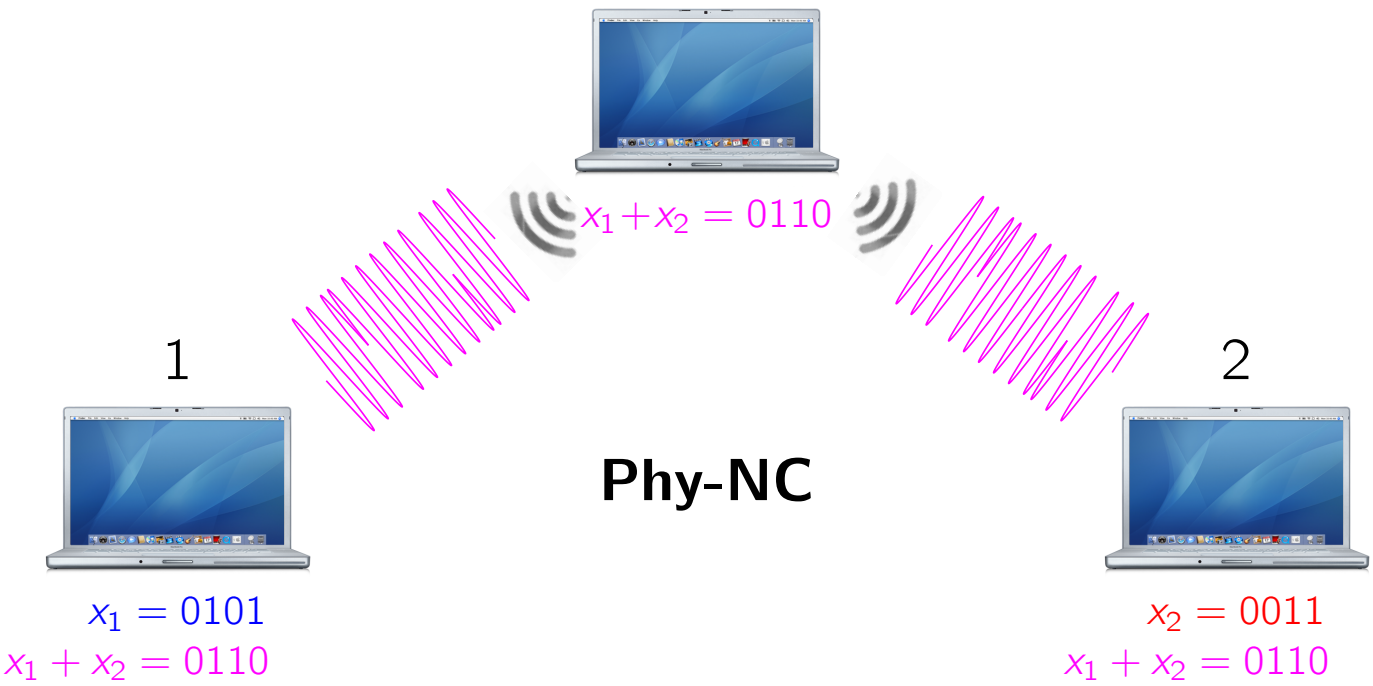
$x_1 = 0101$

Phy-NC

2

$x_2 = 0011$

Rede sem-fio bidirecional com nó intermediário



Rede sem-fio bidirecional com nó intermediário

1

$x_1 = 0101$

$x_1 + x_2 = 0110$

$x_2 = 0011$

Phy-NC

2

$x_2 = 0011$

$x_1 + x_2 = 0110$

$x_1 = 0101$

Rede sem-fio bidirecional com nó intermediário

1

$x_1 = 0101$

$x_1 + x_2 = 0110$

$x_2 = 0011$

Phy-NC

2 instantes de tempo

2

$x_2 = 0011$

$x_1 + x_2 = 0110$

$x_1 = 0101$

Anéis e espaços de pacote na prática

Phy-NC + Modulação não-codificada.

- 4-ASK $\longrightarrow$ $R = \mathbb{Z}_4$
- QPSK $\longrightarrow$ $R = \mathbb{Z}_2[i]$
- 16-QAM $\longrightarrow$ $R = \mathbb{Z}_4[i]$
- 64-QAM $\longrightarrow$ $R = \mathbb{Z}_8[i]$

Em todos esses casos, $\Omega = R^\ell$.

Anéis e espaços de pacote na prática

Phy-NC + Modulação não-codificada.

- 4-ASK $\longrightarrow$ $R = \mathbb{Z}_4$
- QPSK $\longrightarrow$ $R = \mathbb{Z}_2[i]$
- 16-QAM $\longrightarrow$ $R = \mathbb{Z}_4[i]$
- 64-QAM $\longrightarrow$ $R = \mathbb{Z}_8[i]$

Em todos esses casos, $\Omega = R^{\ell}$.

Phy-NC + Modulação codificada.

"Phy-NC via reticulados aninhados" [Nazar, Gastpar '11] [Feng et al. '13]

- Construção A + LDPC binário: [Ordentlich et al. '11]
  $\longrightarrow$ $R = \mathbb{Z}_4$ e $\Omega = R^{54000} \times (2R)^{10800}$
- Construção D + Códigos turbo: [Sakzad et al. '10]
  $\longrightarrow$ $R = \mathbb{Z}_4$ e $\Omega = R^{3377} \times (2R)^{1688}$

Anéis e espaços de pacote na prática

Phy-NC + Modulação não-codificada.

- 4-ASK $\longrightarrow$ $R = \mathbb{Z}_4$
- QPSK $\longrightarrow$ $R = \mathbb{Z}_2[i]$
- 16-QAM $\longrightarrow$ $R = \mathbb{Z}_4[i]$
- 64-QAM $\longrightarrow$ $R = \mathbb{Z}_8[i]$

Em todos esses casos, $\Omega = R^{\ell}$.

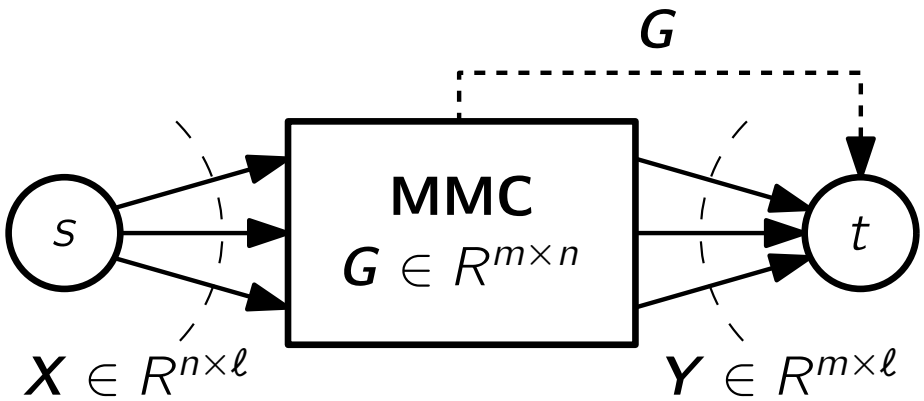
Phy-NC + Modulação codificada.

"Phy-NC via reticulados aninhados" [Nazar, Gastpar '11] [Feng et al. '13]

- Construção A + LDPC binário: [Ordentlich et al. '11]
  $\longrightarrow$ $R = \mathbb{Z}_4$ e $\Omega = R^{54000} \times (2R)^{10800}$
- Construção D + Códigos turbo: [Sakzad et al. '10]
  $\longrightarrow$ $R = \mathbb{Z}_4$ e $\Omega = R^{3377} \times (2R)^{1688}$

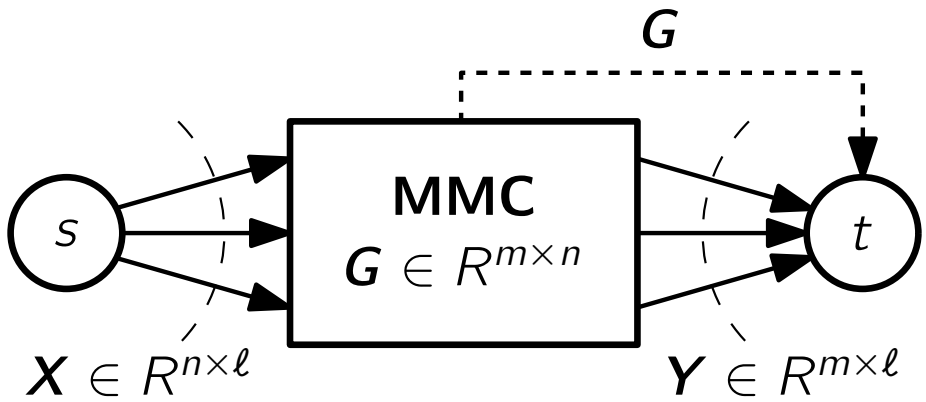
Todos esses são exemplos de anéis de cadeia finitos!
Em Phy-NC com modulação codificada, Ω tem forma geral.

Modelo do canal



R	anel de cadeia finito
n	número de pacotes transmitidos
m	número de pacotes recebidos
λ	shape do espaço de pacotes Ω
p_G	distribuição de probabilidade em $R^{m\times n}$

Modelo do canal



R	anel de cadeia finito
n	número de pacotes transmitidos
m	número de pacotes recebidos
λ	shape do espaço de pacotes Ω
$p_{\boldsymbol{G}}$	distribuição de probabilidade em $R^{m\times n}$

De agora em diante, por simplicidade, $R = \mathbb{Z}_8$.

Capacidade do canal

MMC coerente com matriz de transferência $\boldsymbol{G}$ e espaço de pacotes Ω.

Corpos finitos ($\mathbb{F}_q$)

Teorema [Yang et al. '10]

A capacidade do canal é dada por

$$C = \mathsf{E}[\boldsymbol{r}]\ell,$$

$\boldsymbol{r} = \operatorname{rank} \boldsymbol{G}$ e $\ell = \dim \Omega$.

$$\operatorname{rank} \boldsymbol{G} = \dim \langle \boldsymbol{G} \rangle$$

Capacidade do canal

MMC coerente com matriz de transferência $\boldsymbol{G}$ e espaço de pacotes Ω.

Corpos finitos $(\mathbb{F}_q)$

Teorema [Yang et al. '10]

A capacidade do canal é dada por

$$C = \mathsf{E}[\boldsymbol{r}]\ell,$$

$\boldsymbol{r} = \operatorname{rank} \boldsymbol{G}$ e $\ell = \dim \Omega$.

$$\operatorname{rank} \boldsymbol{G} = \dim \langle \boldsymbol{G} \rangle$$

Anéis de cadeia finitos $(\mathbb{Z}_8)$

Teorema

A capacidade do canal é dada por

$$C = \mathsf{E}[\boldsymbol{\rho}_2]\lambda_0 + \mathsf{E}[\boldsymbol{\rho}_1]\lambda_1 + \mathsf{E}[\boldsymbol{\rho}_0]\lambda_2,$$

$\boldsymbol{\rho} = \operatorname{shape} \boldsymbol{G}$ e $\lambda = \operatorname{shape} \Omega$.

$$\operatorname{shape} \boldsymbol{G} = \operatorname{shape} \langle \boldsymbol{G} \rangle$$

Esquema de codificação

Construção do código.

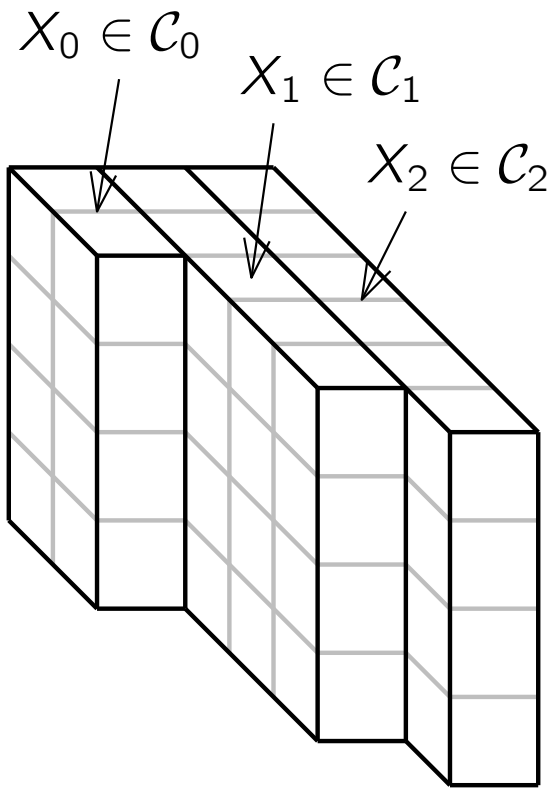
- Códigos componentes:

  $\mathcal{C}_0 \subseteq \mathbb{F}_2^{n\times\lambda_0} \quad \mathcal{C}_1 \subseteq \mathbb{F}_2^{n\times\lambda_1} \quad \mathcal{C}_2 \subseteq \mathbb{F}_2^{n\times\lambda_2}$

- Código composto:

  $\mathcal{C} = \{X_0 + 2X_1 + 4X_2 : X_i \in \mathcal{C}_i\} \subseteq \mathbb{Z}_8^{n\times\ell}$

Abordagem em camadas



$n = 4$

$\lambda = (2, 5, 6)$

Esquema de codificação

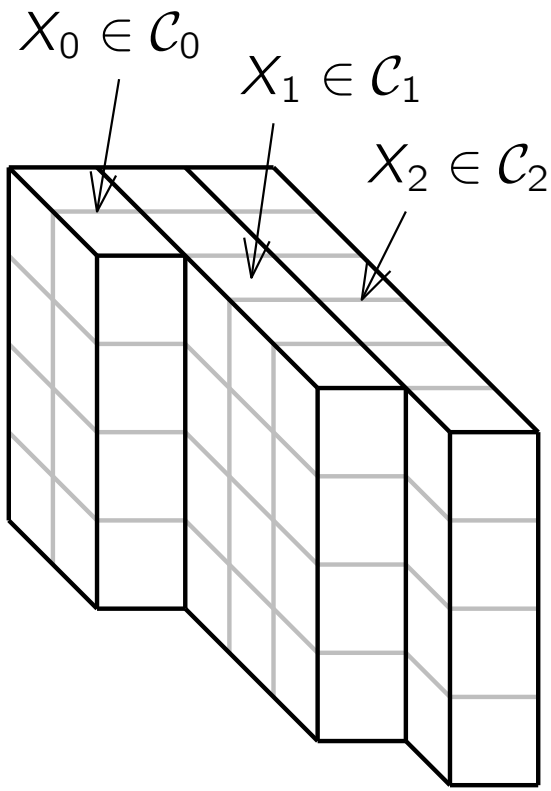
Construção do código.

- Códigos componentes:
  $\mathcal{C}_0 \subseteq \mathbb{F}_2^{n\times\lambda_0} \quad \mathcal{C}_1 \subseteq \mathbb{F}_2^{n\times\lambda_1} \quad \mathcal{C}_2 \subseteq \mathbb{F}_2^{n\times\lambda_2}$
- Código composto:
  $\mathcal{C} = \{X_0 + 2X_1 + 4X_2 : X_i \in \mathcal{C}_i\} \subseteq \mathbb{Z}_8^{n\times\ell}$

Decodificação (multi-estágio).

- Decodifica-se X_0.
- Decodifica-se X_1 com base em X_0.
- Decodifica-se X_2 com base em X_0 e X_1.

Abordagem em camadas



$n = 4$

$\lambda = (2, 5, 6)$

Características do código

Proposição

A taxa do código é dada por

$$\text{Rate}(\mathcal{C}) = \text{Rate}(\mathcal{C}_0) + \text{Rate}(\mathcal{C}_1) + \text{Rate}(\mathcal{C}_2)$$

e a probabilidade de erro é limitada por

$$\text{P}_{\text{err}}(\mathcal{C}) \leq \text{P}_{\text{err}}(\mathcal{C}_0) + \text{P}_{\text{err}}(\mathcal{C}_1) + \text{P}_{\text{err}}(\mathcal{C}_2).$$

Capacidade. O código $\mathcal{C}$ é capaz de alcançar a capacidade.

Complexidade. O esquema tem complexidade de tempo polinomial.

Universalidade. Não é necessário o conhecimento de $p_{\boldsymbol{G}}$, apenas de $\text{E}[\boldsymbol{\rho}]$.

Conclusão

Sumário das contribuições

MMC não-coerente u.g.r. sobre corpos finitos

- Modelo u.g.r.: compromisso entre tratabilidade e aplicabilidade.
- Cálculo da capacidade do canal de forma eficiente.
- Forma fechada para a capacidade de posto constante.
- Resultados assintóticos.
- Comunicação via subespaços é ótima.

MMC coerente sobre anéis de cadeia finitos

- Aplicações em codificação de rede na camada física.
- Forma fechada para a capacidade do canal.
- Esquema prático de codificação que alcança a capacidade.

Trabalhos futuros

Trabalhos futuros ou em andamento

- Cálculo da distribuição de posto em função da topologia.
- Esquemas de codificação para o MMC não-coerente u.g.r.
- Estudo do AMMC: $\boldsymbol{Y} = \boldsymbol{GX} + \boldsymbol{Z}$ (sobre corpos e anéis).
- Capacidade do MMC não-coerente sobre anéis de cadeia finitos.
- MMC sobre anéis de cadeia finitos sob um modelo adversarial.

Publicações resultantes

- **R.W. NÓBREGA**, B.F. UCHÔA-FILHO, D. SILVA.
  "On the Capacity of Multiplicative Finite-Field Matrix Channels".
  2011 IEEE International Symposium on Information Theory (ISIT'11).
  Saint Petersburg, Russia. Aug, 2011.
- **R.W. NÓBREGA**, D. SILVA, B.F. UCHÔA-FILHO.
  "On the Capacity of Multiplicative Finite-Field Matrix Channels".
  IEEE Transactions on Information Theory, vol. 59, no. 8. Aug, 2013.
- **R.W. NÓBREGA**, C. FENG, D, SILVA, B.F. UCHÔA-FILHO.
  "On Multiplicative Matrix Channels over Finite Chain Rings".
  2013 IEEE International Symposium on Network Coding (NetCod'13).
  Calgary, Alberta, Canada. Jun, 2013.
- C. FENG, **R.W. NÓBREGA**, F.R. KSCHISCHANG, D. SILVA.
  "Communication over Finite-Ring Matrix Channels".
  2013 IEEE International Symposium on Information Theory (ISIT'13).
  Istanbul, Turkey. Jul, 2013.
- **R.W. NÓBREGA**, C. FENG, D. SILVA, B.F. UCHÔA-FILHO.
  "Canais Matriciais Multiplicativos sobre Anéis de Cadeia Finitos".
  XXXI Simpósio Brasileiro de Telecomunicações (SBrT'13).
  Fortaleza, Ceará, Brazil. Sep, 2013.

Obrigado!

Roberto W. Nóbrega
http://gpqcom.ufsc.br/~rwnobrega/
rwnobrega@eel.ufsc.br