Códigos de Subespaço aplicados a Codificação de Rede

Roberto Wanderley da Nóbrega
Orientador: Bartolomeu Ferreira Uchôa Filho, Ph.D.

Grupo de Pesquisa em Comunicações
Departamento de Engenharia Elétrica
Universidade Federal de Santa Catarina

7 de agosto de 2009

Conteúdo

Conteúdo

Conteúdo

Conteúdo

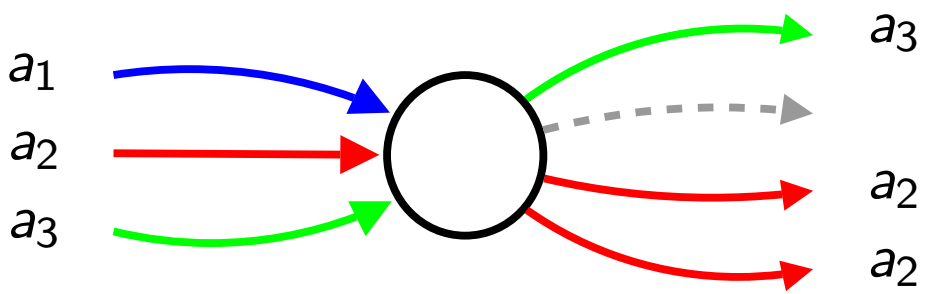
Conteúdo

Conteúdo

Introdução

Roteamento *vs* codificação de rede

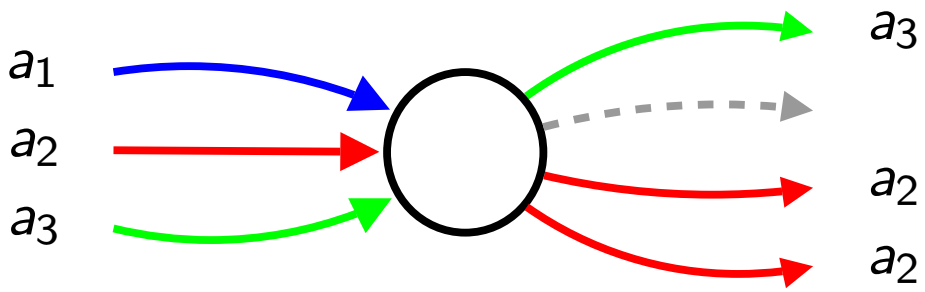
Mudança de paradigma



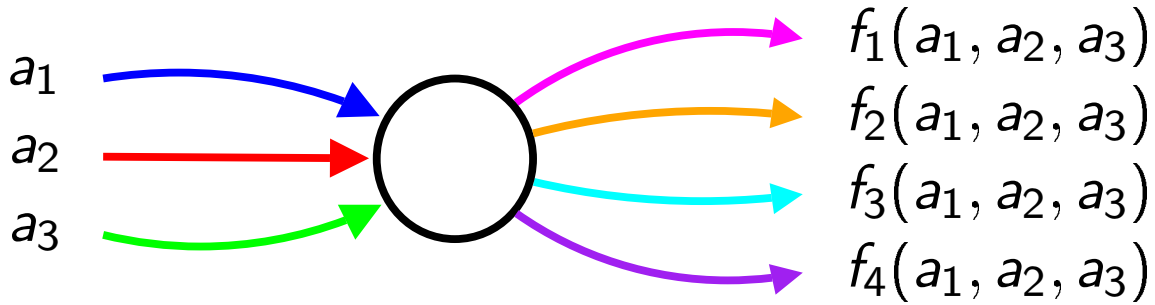
Comutador

Roteamento *vs* codificação de rede

Mudança de paradigma



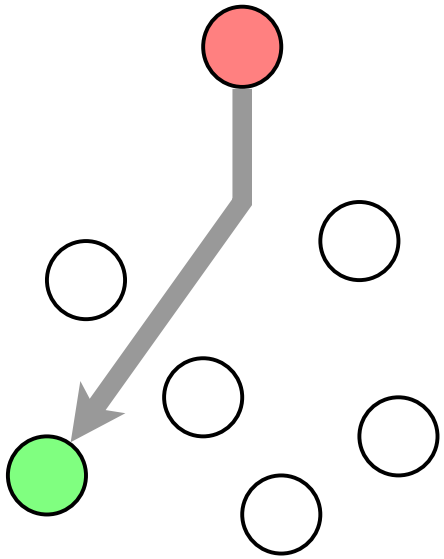
Comutador



Codificador

Fluxo de informação em redes

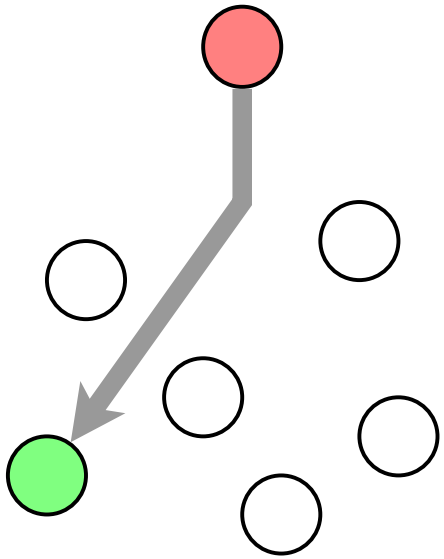
Dois casos particulares



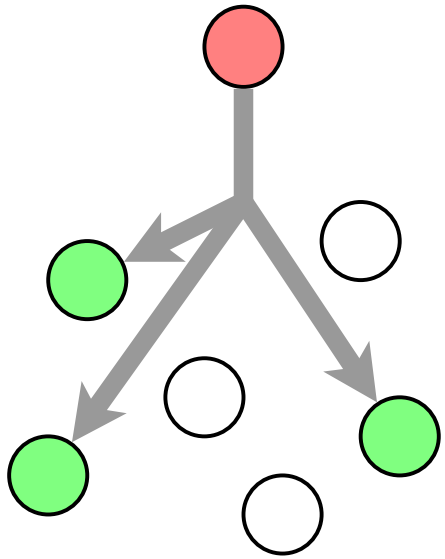
Unidifusão

Fluxo de informação em redes

Dois casos particulares



Unidifusão



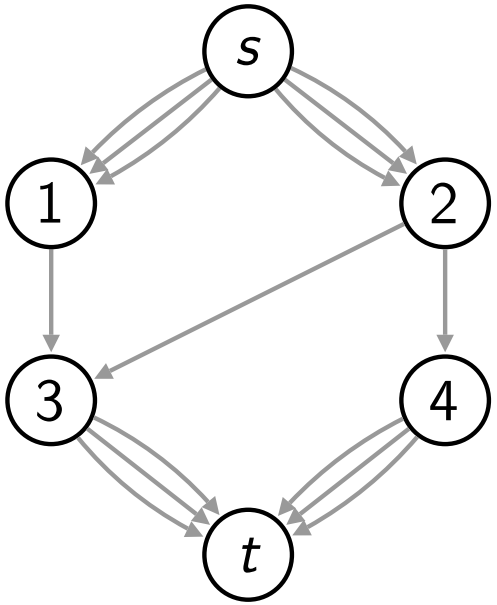
Multidifusão

Fluxo de informação em redes

Problema do fluxo máximo

Fato

Roteamento é suficiente para o caso unidifusão



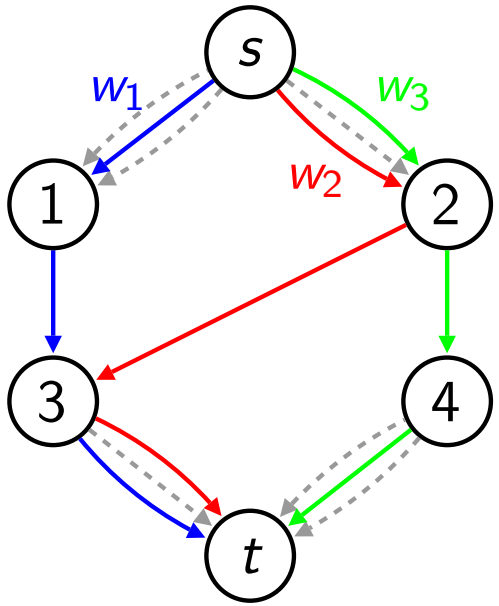
Fluxo de informação em redes

Problema do fluxo máximo

Fato

Roteamento é suficiente para o caso unidifusão

Fluxo máximo
(maxflow)



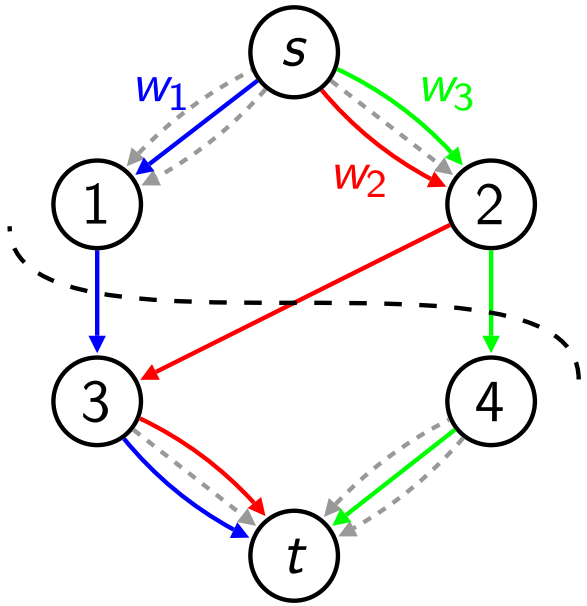
Fluxo de informação em redes

Problema do fluxo máximo

Fato

Roteamento é suficiente para o caso unidifusão

Fluxo máximo
(maxflow)



Corte mínimo
(mincut)

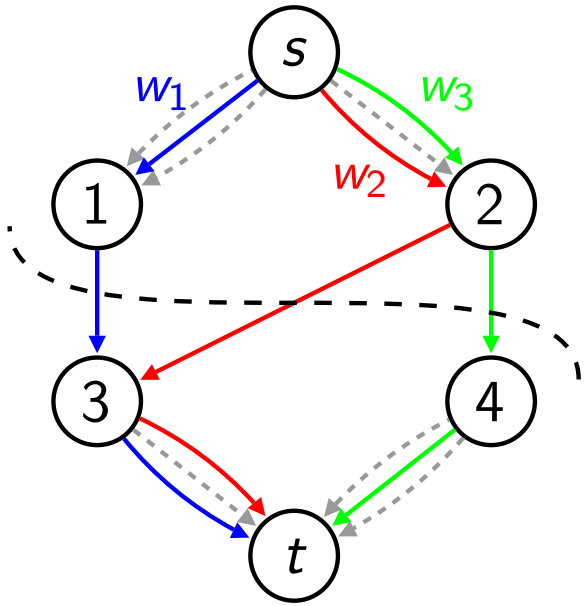
Fluxo de informação em redes

Problema do fluxo máximo

Fato

Roteamento é suficiente para o caso unidifusão

Fluxo máximo
(maxflow)

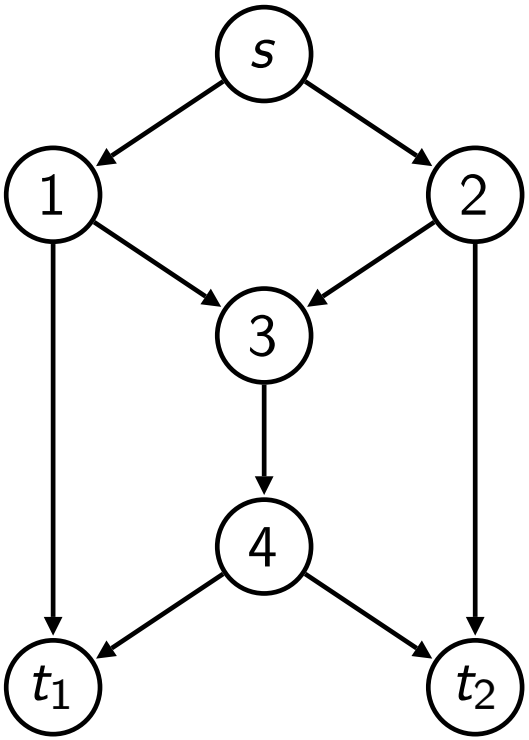


Corte mínimo
(mincut)

Possível solução: algoritmo de Ford-Fulkerson

Rede borboleta

Exemplo multidifusão

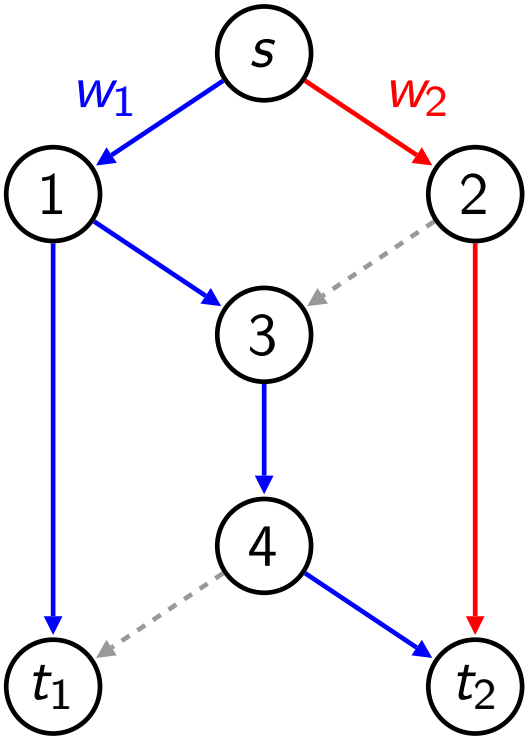


Citação

"A teoria do fluxo de informação não tem as mesmas respostas simples que a teoria do fluxo de água em canos."
— Cover & Thomas

Rede borboleta

Solução com roteamento

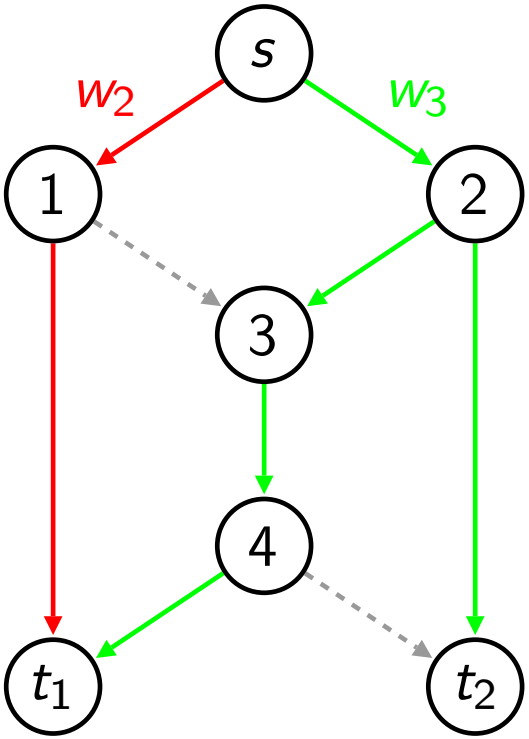


Após o instante 1:

- Nó t_1 tem w_1
- Nó t_2 tem w_1, w_2

Rede borboleta

Solução com roteamento

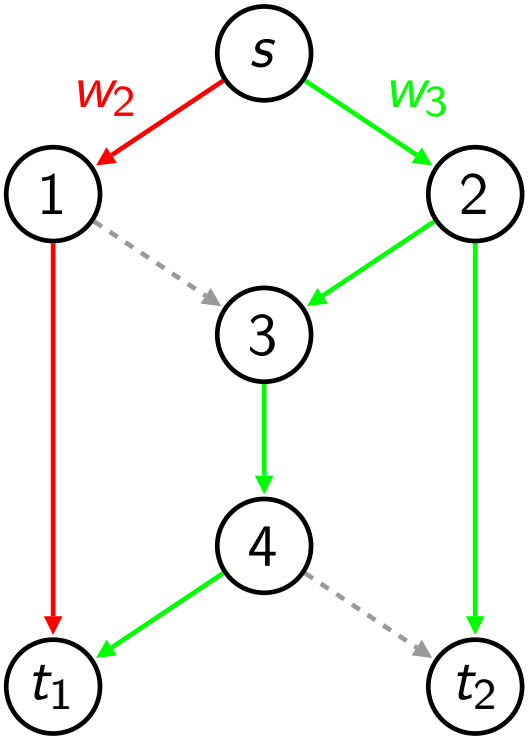


Após o instante 2:

- Nó t_1 tem w_1, w_2, w_3
- Nó t_2 tem w_1, w_2, w_3

Rede borboleta

Solução com roteamento



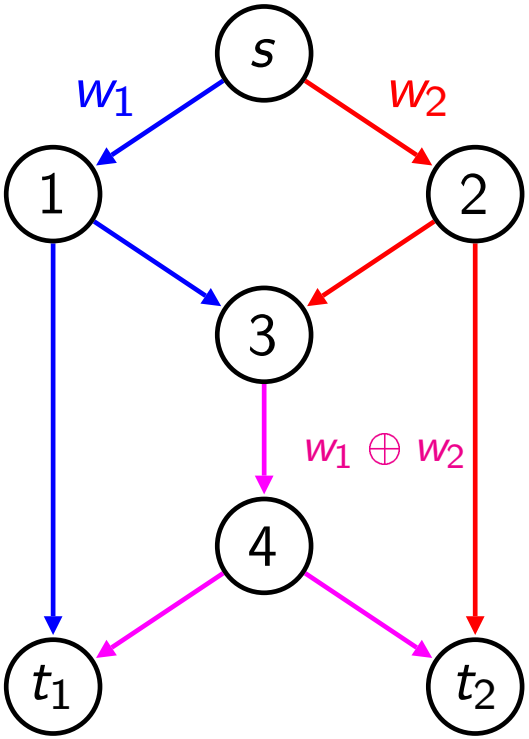
Multidifusão de 3 bits
em 2 instantes de tempo

Desempenho

1,5 bits / instante de tempo

Rede borboleta

Solução com codificação de rede

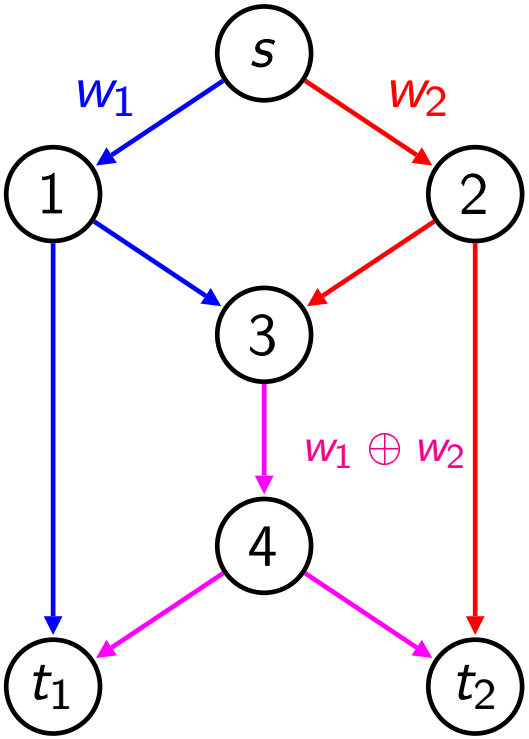


Funcionamento:

- Nó 3 combina o que recebe
- Nó t_1 tem w_1 e $w_1 \oplus w_2$
- Nó t_2 tem w_2 e $w_1 \oplus w_2$
- Ambos recuperam w_1 e w_2

Rede borboleta

Solução com codificação de rede



Multidifusão de 2 bits
em 1 instante de tempo

Desempenho

2 bits / instante de tempo

Fundamentos de Codificação de Rede

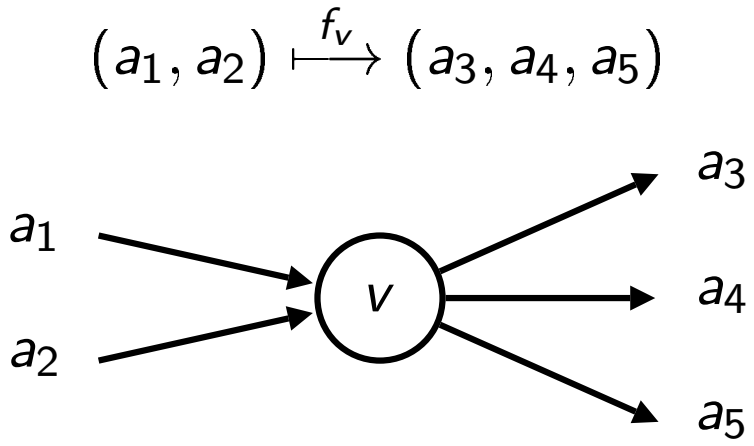
Códigos de rede

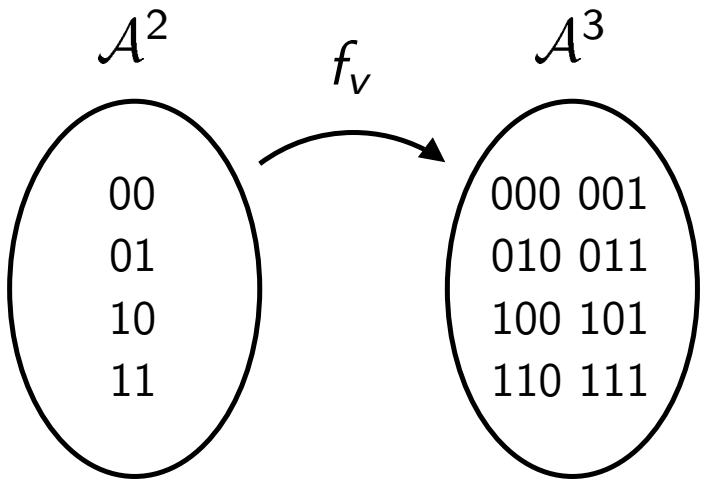
Descrição local de um código de rede

Mapeamentos de codificação locais

Um para cada nó não-fonte v:

$$f_v : \mathbf{a}_{\mathrm{In}(v)} \longmapsto \mathbf{a}_{\mathrm{Out}(v)}$$

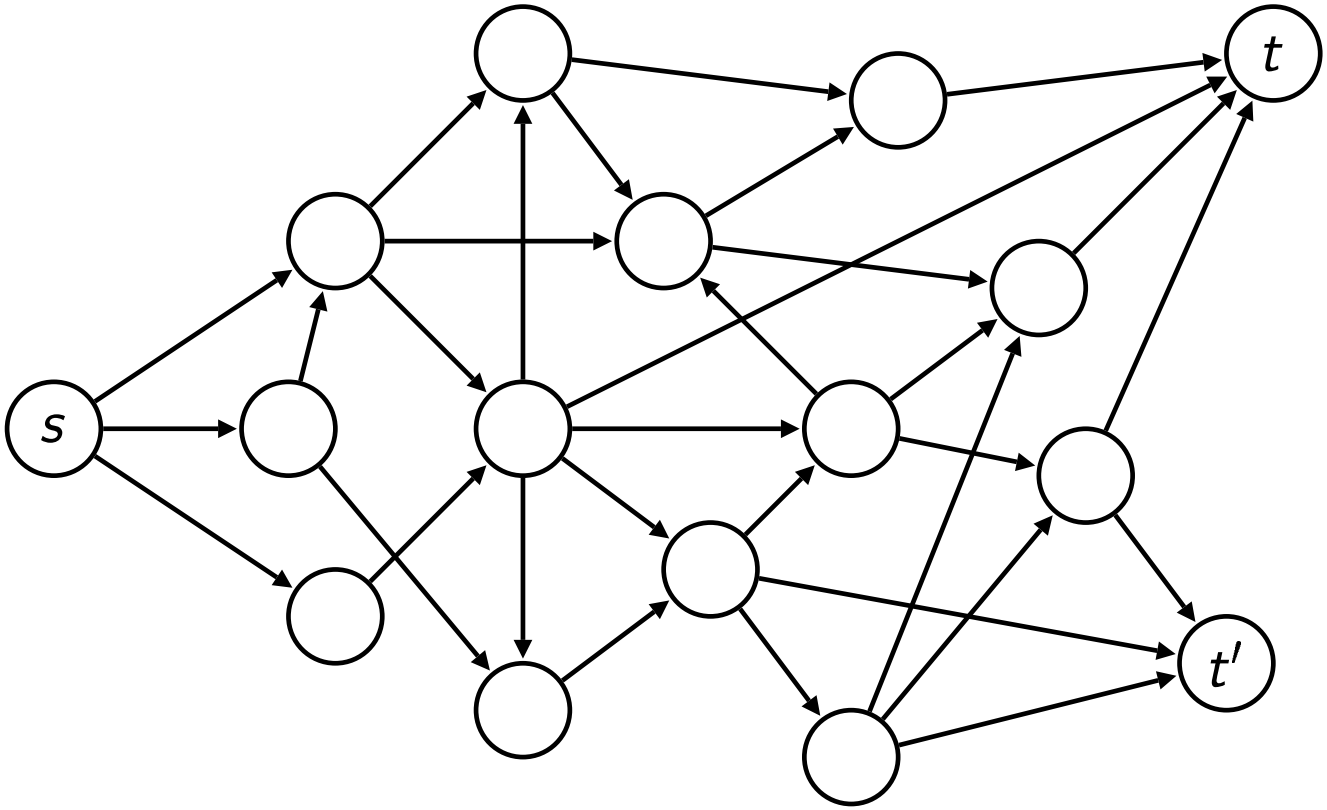




Códigos de rede

Funções de transferência

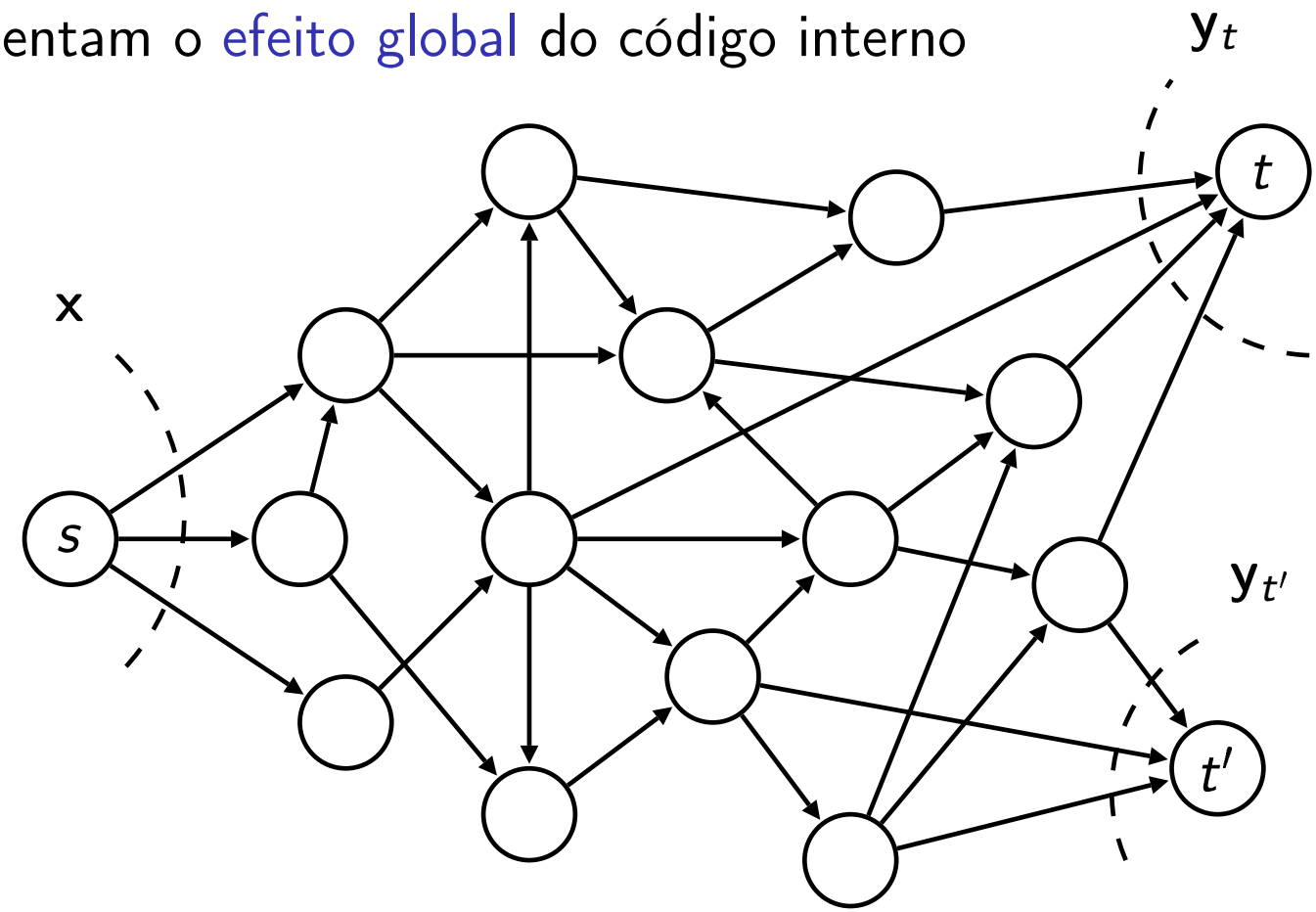
Representam o efeito global do código interno



Códigos de rede

Funções de transferência

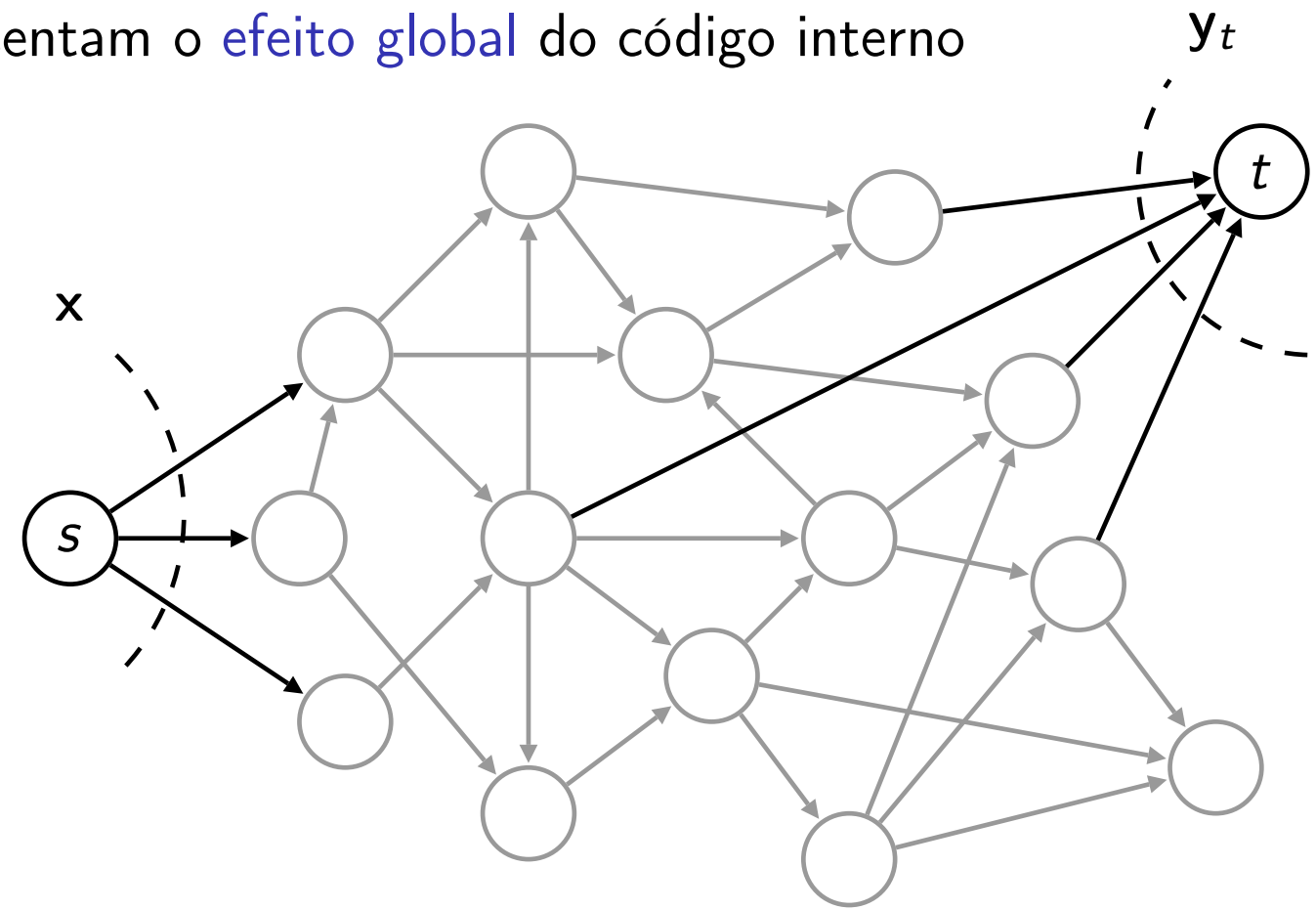
Representam o efeito global do código interno



Códigos de rede

Funções de transferência

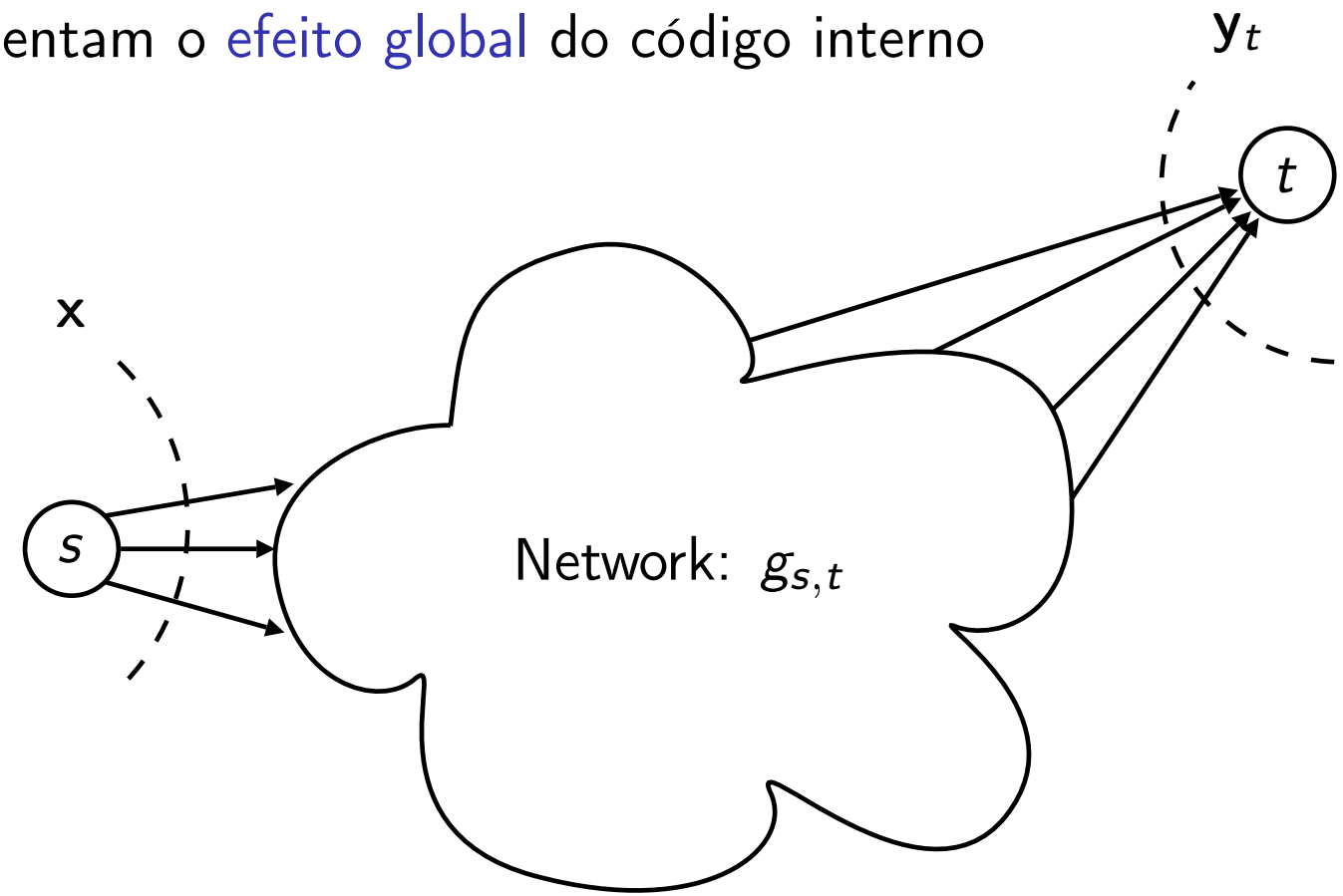
Representam o efeito global do código interno



Códigos de rede

Funções de transferência

Representam o efeito global do código interno



Taxas alcançáveis

Teorema fundamental da multidifusão

Teorema

A fonte é capaz de multidifundir a uma taxa h *iff*

$$h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$$

- Em geral, codificação de rede é necessária (ex. borboleta)
- Códigos de rede lineares são suficientes

Taxas alcançáveis

Teorema fundamental da multidifusão

Teorema

A fonte é capaz de multidifundir a uma taxa h *iff*

$$h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$$

- Em geral, codificação de rede é necessária (ex. borboleta)
- Códigos de rede lineares são suficientes

Taxas alcançáveis

Teorema fundamental da multidifusão

Teorema

A fonte é capaz de multidifundir a uma taxa h *iff*

$$h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$$

- Em geral, codificação de rede é necessária (ex. borboleta)
- Códigos de rede lineares são suficientes

Codificação de rede linear

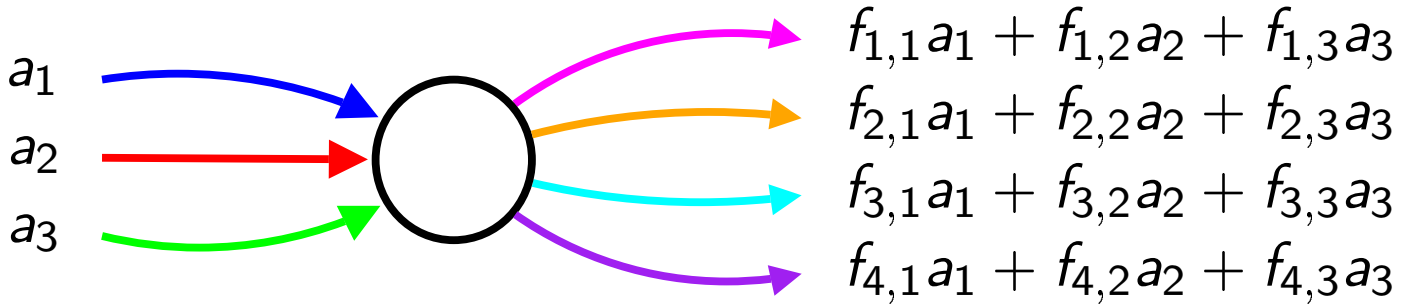
Códigos de rede lineares

- Saída dos nós são combinações lineares das entradas
- Alfabeto: corpo finito $\mathbb{F}_q$
- Mapeamentos de codificação são representados por matrizes

Codificação de rede linear

Códigos de rede lineares

- Saída dos nós são combinações lineares das entradas

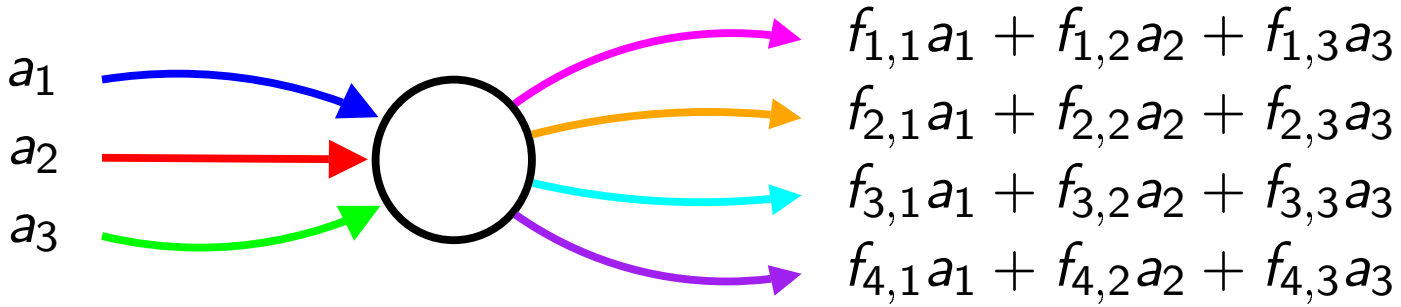


- Alfabeto: corpo finito $\mathbb{F}_q$
- Mapeamentos de codificação são representados por matrizes

Codificação de rede linear

Códigos de rede lineares

- Saída dos nós são combinações lineares das entradas

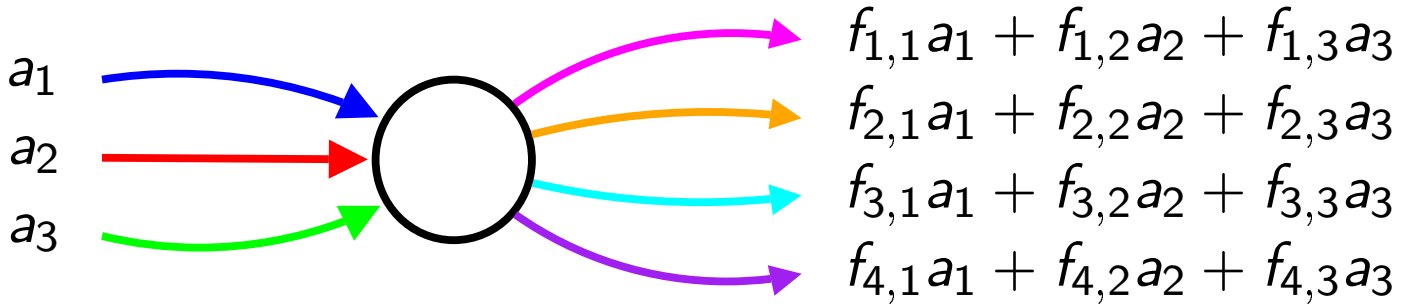


- Alfabeto: corpo finito $\mathbb{F}_q$
- Mapeamentos de codificação são representados por matrizes

Codificação de rede linear

Códigos de rede lineares

- Saída dos nós são combinações lineares das entradas



- Alfabeto: corpo finito $\mathbb{F}_q$
- Mapeamentos de codificação são representados por matrizes

Codificação de rede linear

Matrizes de transferência

- Funções de transferência são representadas por matrizes

- Sistema MIMO linear sobre corpos finitos

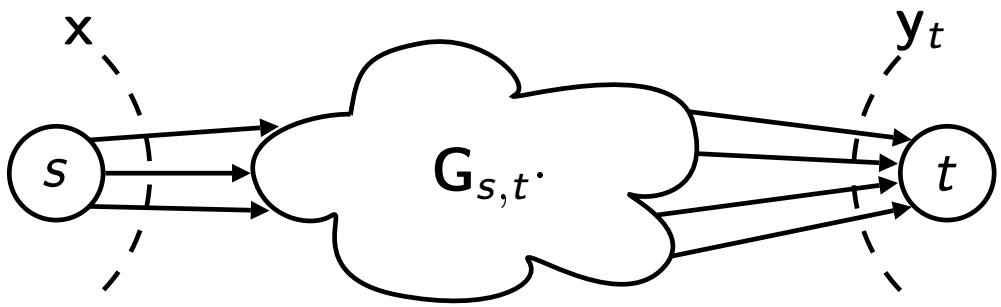
Teorema fundamental da multidifusão

É possível escolher $\mathbf{G}_{s,t}$ com posto h *iff* $h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$

Codificação de rede linear

Matrizes de transferência

- Funções de transferência são representadas por matrizes



- Sistema MIMO linear sobre corpos finitos

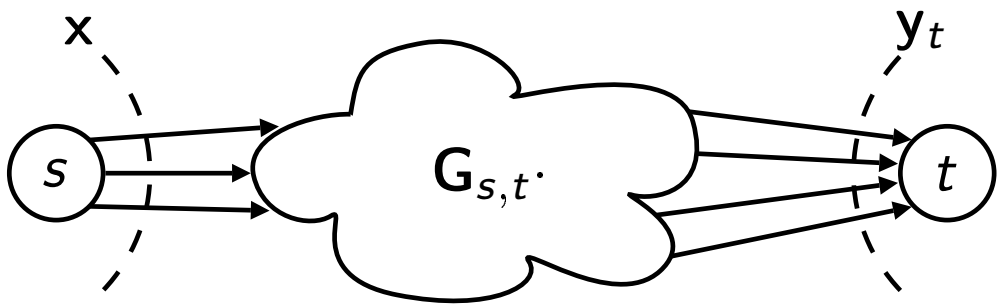
Teorema fundamental da multidifusão

É possível escolher $\mathbf{G}_{s,t}$ com posto h *iff* $h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$

Codificação de rede linear

Matrizes de transferência

- Funções de transferência são representadas por matrizes



- Sistema MIMO linear sobre corpos finitos

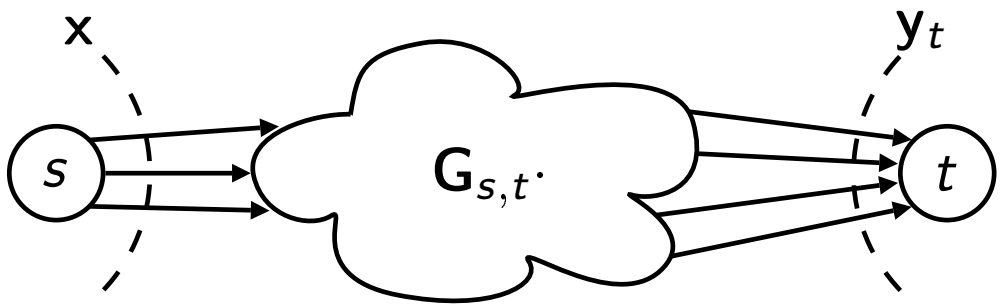
Teorema fundamental da multidifusão

É possível escolher $\mathbf{G}_{s,t}$ com posto h *iff* $h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$

Codificação de rede linear

Matrizes de transferência

- Funções de transferência são representadas por matrizes



- Sistema MIMO linear sobre corpos finitos

Teorema fundamental da multidifusão

É possível escolher $\mathbf{G}_{s,t}$ com posto h *iff* $h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$

Codificação de rede linear

Codificação de rede aleatória

- Nós efetuam combinações lineares aleatórias
- Alta probabilidade de código bem-sucedido quando q é grande
- Funcionamento descentralizado do sistema

Codificação de rede linear

Codificação de rede aleatória

- Nós efetuam combinações lineares aleatórias
- Alta probabilidade de código bem-sucedido quando q é grande
- Funcionamento descentralizado do sistema

Codificação de rede linear

Codificação de rede aleatória

- Nós efetuam combinações lineares aleatórias
- Alta probabilidade de código bem-sucedido quando q é grande
- Funcionamento descentralizado do sistema

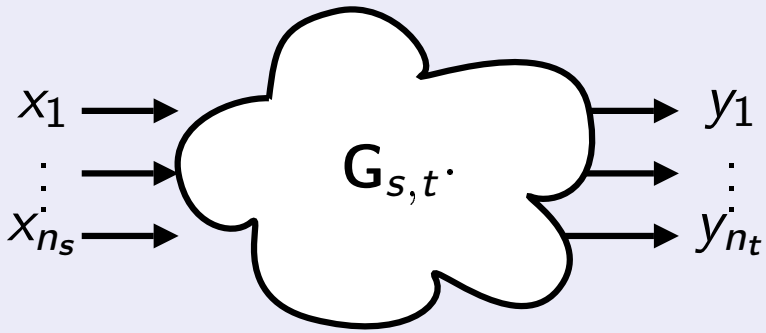
Codificação de rede vetorial linear

Códigos escalares *vs* códigos vetoriais

- Generalização dos códigos lineares escalares

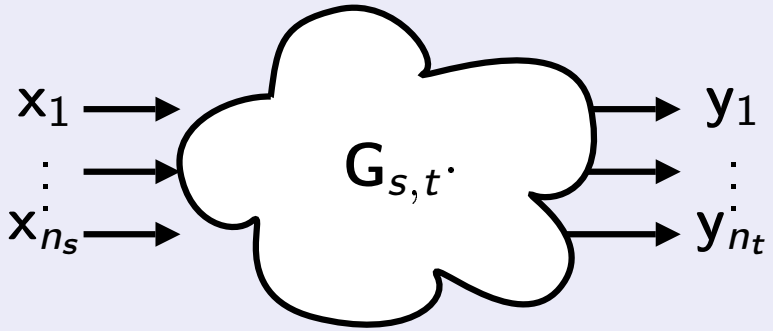
Escalar

Escalares
de um corpo finito $\mathbb{F}_q$



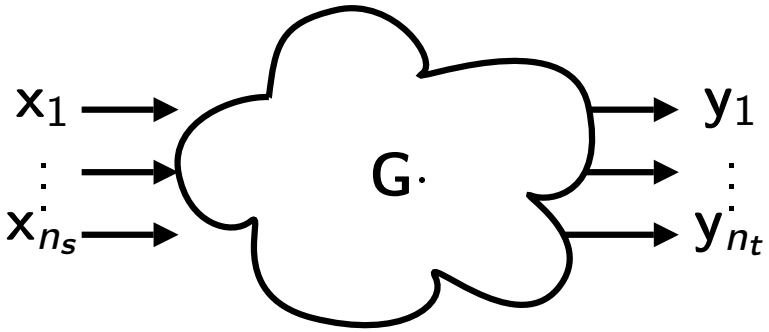
Vetorial

Vetores (m-tuplas)
de um espaço vetorial $\mathbb{F}_q^m$



Codificação de rede vetorial linear

Representação matricial

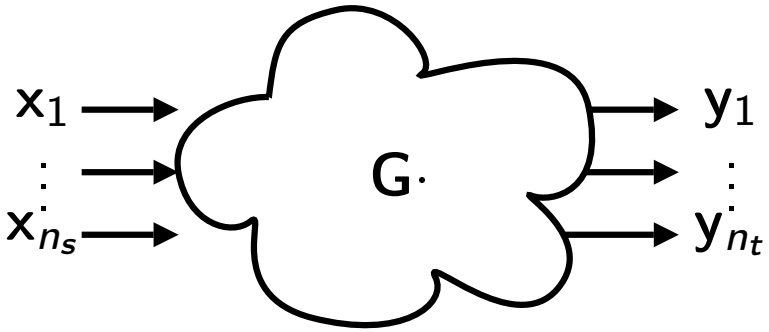


Formam-se as matrizes de entrada $\mathbf{X}$ e saída $\mathbf{Y}$:

$$\mathbf{X} = \begin{bmatrix} \longleftarrow & x_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & x_{n_s} & \longrightarrow \end{bmatrix}_{n_s \times m} \qquad \mathbf{Y} = \begin{bmatrix} \longleftarrow & y_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & y_{n_t} & \longrightarrow \end{bmatrix}_{n_t \times m}$$

Codificação de rede vetorial linear

Representação matricial

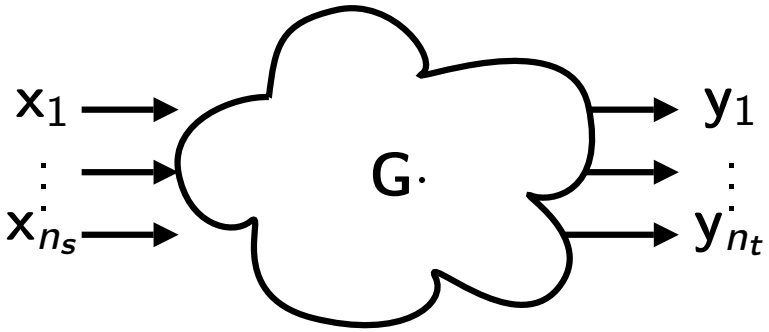


Formam-se as matrizes de entrada $\mathbf{X}$ e saída $\mathbf{Y}$:

$$\mathbf{X} = \begin{bmatrix} \longleftarrow & x_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & x_{n_s} & \longrightarrow \end{bmatrix}_{n_s \times m} \qquad \mathbf{Y} = \begin{bmatrix} \longleftarrow & y_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & y_{n_t} & \longrightarrow \end{bmatrix}_{n_t \times m}$$

Codificação de rede vetorial linear

Representação matricial



Formam-se as matrizes de entrada $\mathbf{X}$ e saída $\mathbf{Y}$:

$$\mathbf{X} = \begin{bmatrix} \longleftarrow & x_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & x_{n_s} & \longrightarrow \end{bmatrix}_{n_s \times m} \qquad \mathbf{Y} = \begin{bmatrix} \longleftarrow & y_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & y_{n_t} & \longrightarrow \end{bmatrix}_{n_t \times m}$$

Codificação de rede vetorial linear

Representação matricial

Hipóteses: $n_s = n_t = h$, em que $h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$

Teorema fundamental da multidifusão

É possível escolher $\mathbf{G} \in \mathbb{F}_q^{h \times h}$ inversível

Codificação de rede linear aleatória

Para q grande, $\mathbf{G} \in \mathbb{F}_q^{h \times h}$ é inversível com alta probabilidade

Fato

Qualquer que seja $\mathbf{X} \in \mathbb{F}_q^{h \times m}$, é possível recuperá-lo: $\mathbf{X} = \mathbf{G}^{-1} \cdot \mathbf{Y}$

Codificação de rede vetorial linear

Representação matricial

Hipóteses: $n_s = n_t = h$, em que $h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$

Teorema fundamental da multidifusão

É possível escolher $\mathbf{G} \in \mathbb{F}_q^{h \times h}$ inversível

Codificação de rede linear aleatória

Para q grande, $\mathbf{G} \in \mathbb{F}_q^{h \times h}$ é inversível com alta probabilidade

Fato

Qualquer que seja $\mathbf{X} \in \mathbb{F}_q^{h \times m}$, é possível recuperá-lo: $\mathbf{X} = \mathbf{G}^{-1} \cdot \mathbf{Y}$

Codificação de rede vetorial linear

Representação matricial

Hipóteses: $n_s = n_t = h$, em que $h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$

Teorema fundamental da multidifusão

É possível escolher $\mathbf{G} \in \mathbb{F}_q^{h \times h}$ inversível

Codificação de rede linear aleatória

Para q grande, $\mathbf{G} \in \mathbb{F}_q^{h \times h}$ é inversível com alta probabilidade

Fato

Qualquer que seja $\mathbf{X} \in \mathbb{F}_q^{h \times m}$, é possível recuperá-lo: $\mathbf{X} = \mathbf{G}^{-1} \cdot \mathbf{Y}$

Codificação de rede vetorial linear

Representação matricial

Hipóteses: $n_s = n_t = h$, em que $h \leq \min_{t \in \mathcal{T}} \text{mincut}(s, t)$

Teorema fundamental da multidifusão

É possível escolher $\mathbf{G} \in \mathbb{F}_q^{h \times h}$ inversível

Codificação de rede linear aleatória

Para q grande, $\mathbf{G} \in \mathbb{F}_q^{h \times h}$ é inversível com alta probabilidade

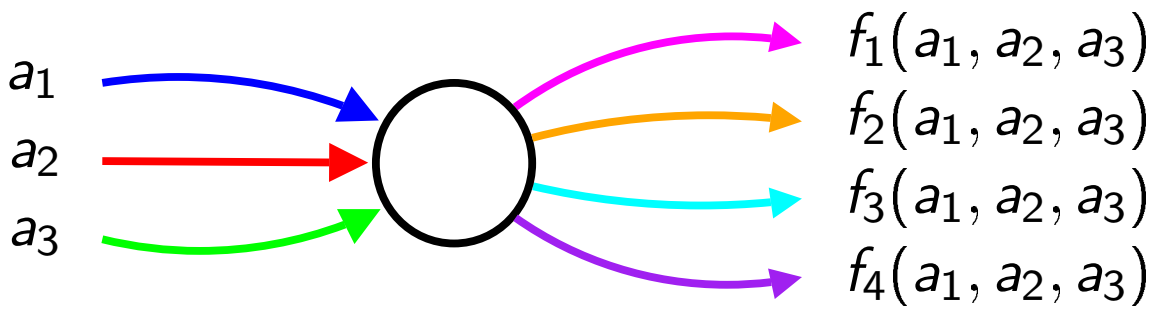
Fato

Qualquer que seja $\mathbf{X} \in \mathbb{F}_q^{h \times m}$, é possível recuperá-lo: $\mathbf{X} = \mathbf{G}^{-1} \cdot \mathbf{Y}$

Problemas em Codificação de Rede

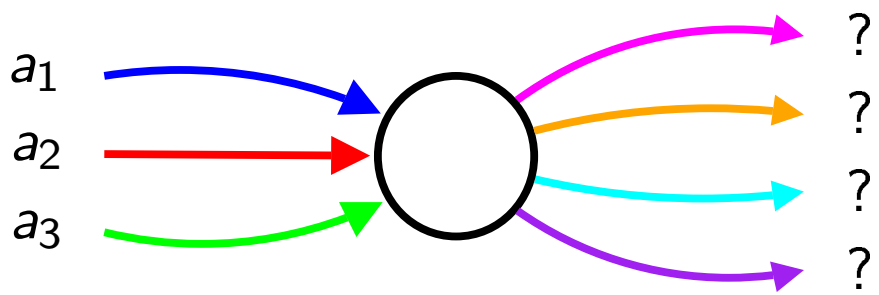
Problemas em codificação de rede

Desconhecimento do código de rede



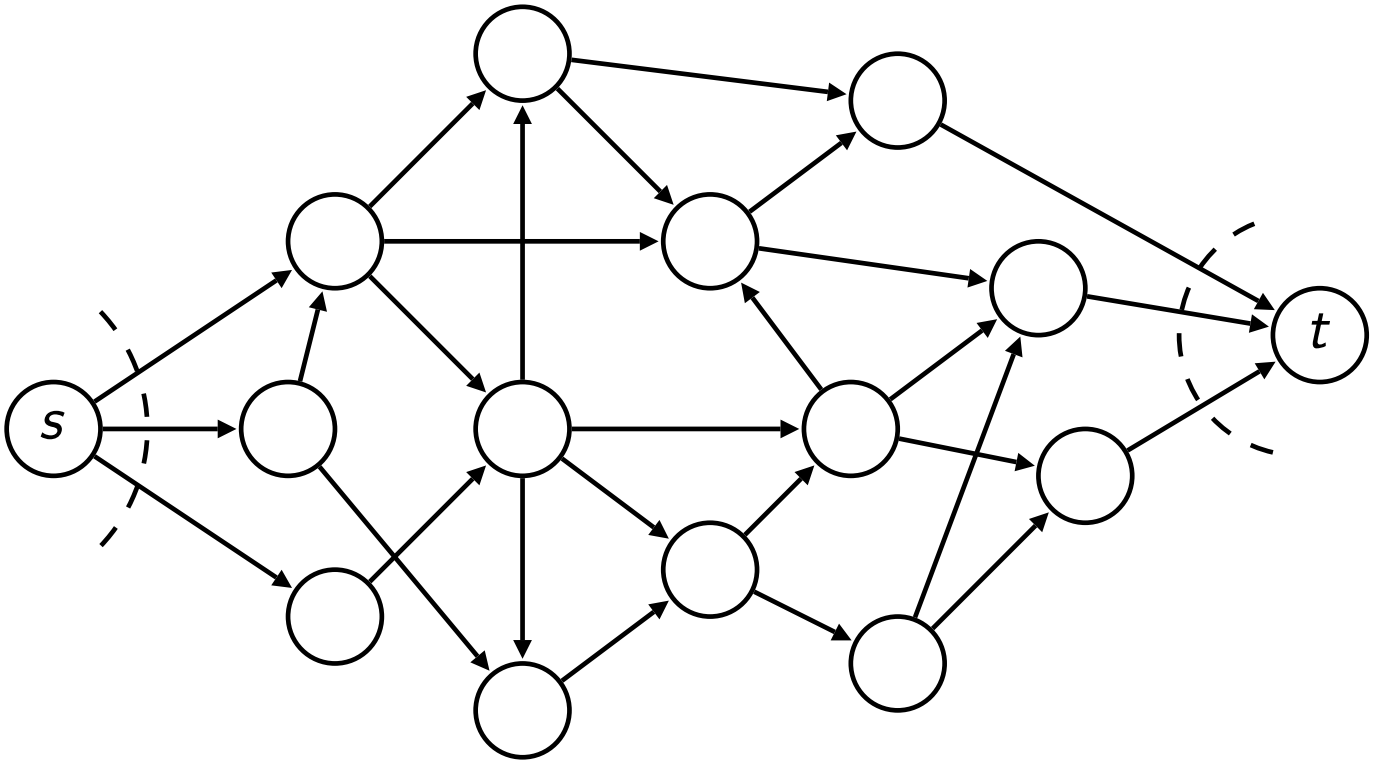
Problemas em codificação de rede

Desconhecimento do código de rede



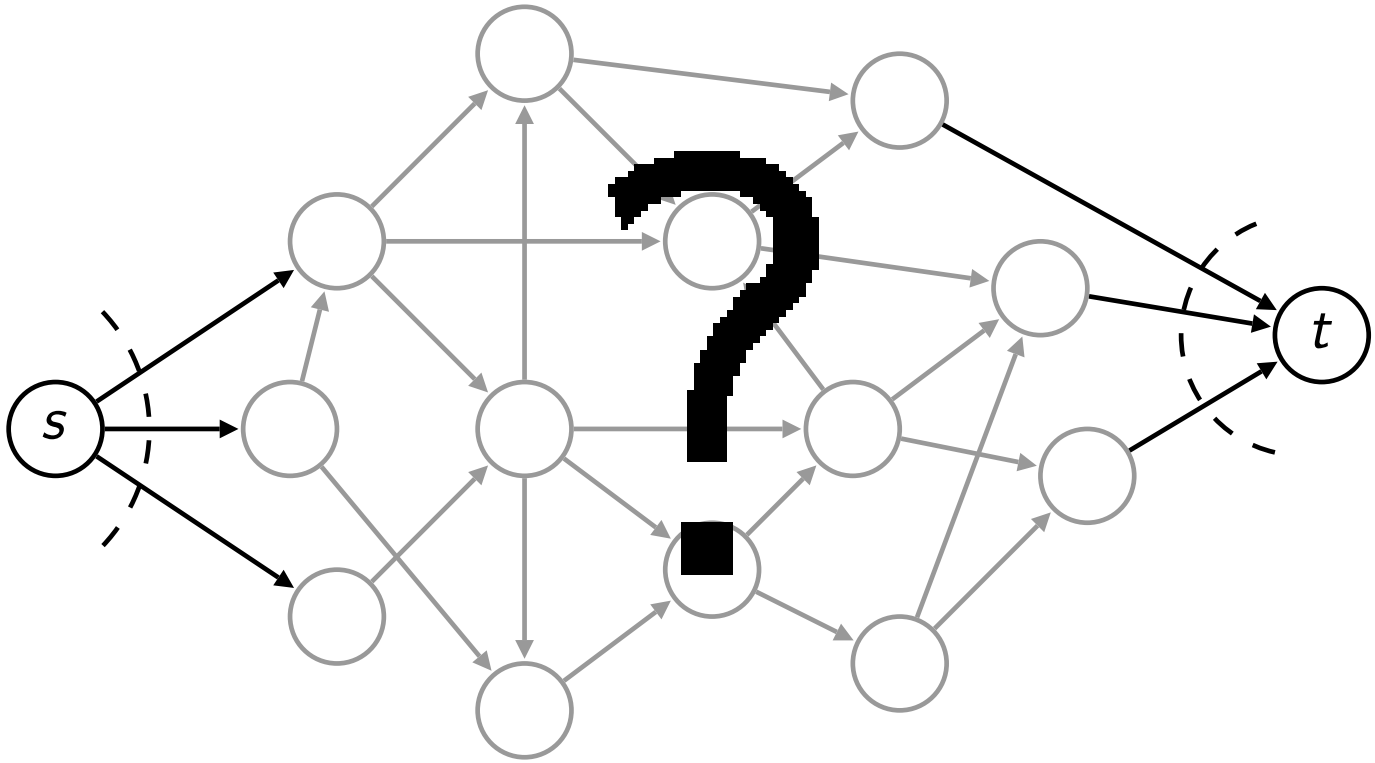
Problemas em codificação de rede

Desconhecimento da topologia



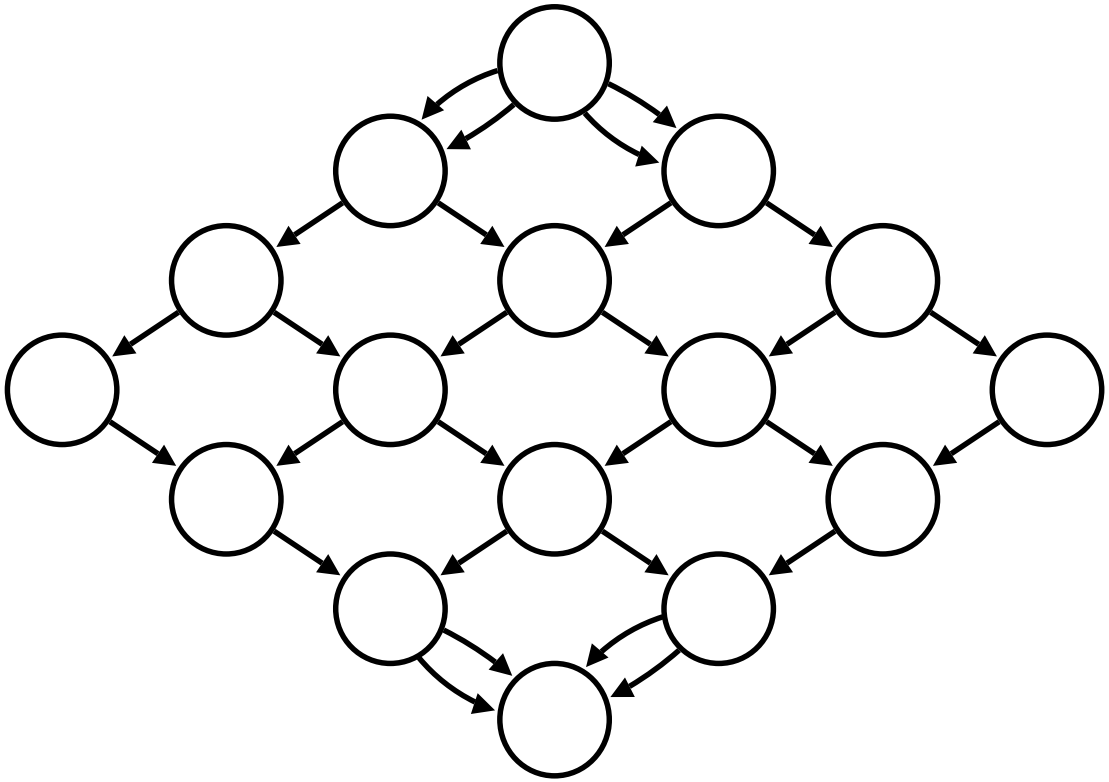
Problemas em codificação de rede

Desconhecimento da topologia



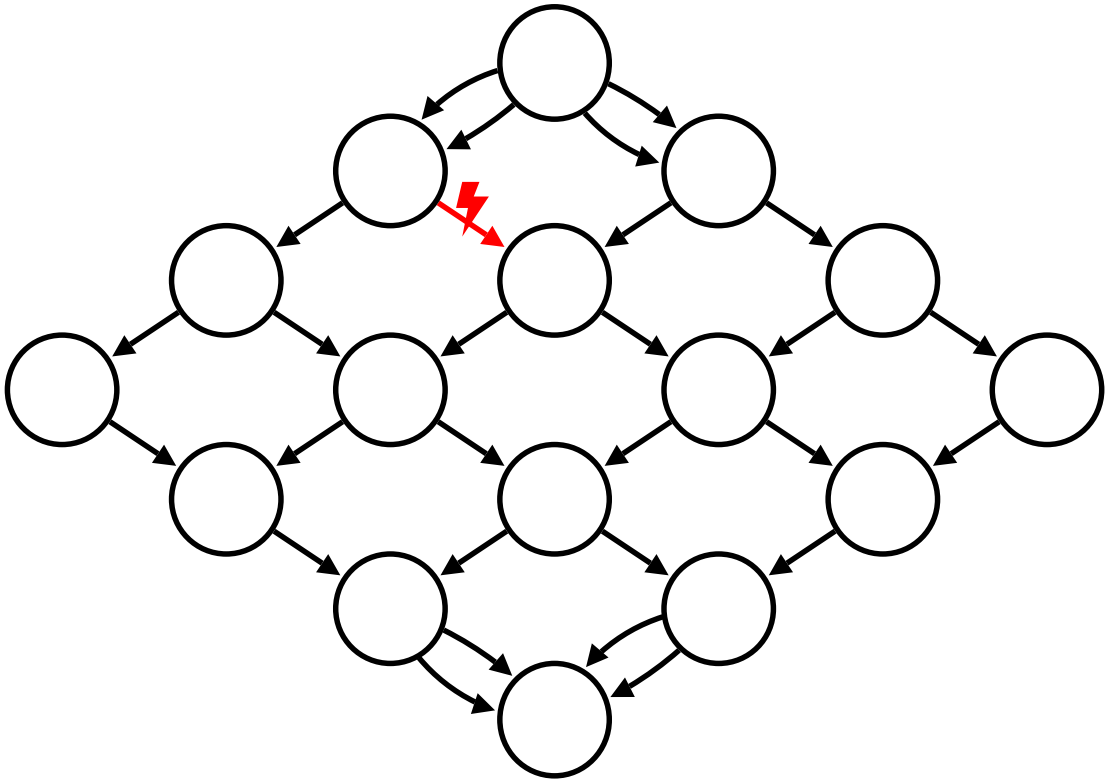
Problemas em codificação de rede

Erros nos canais



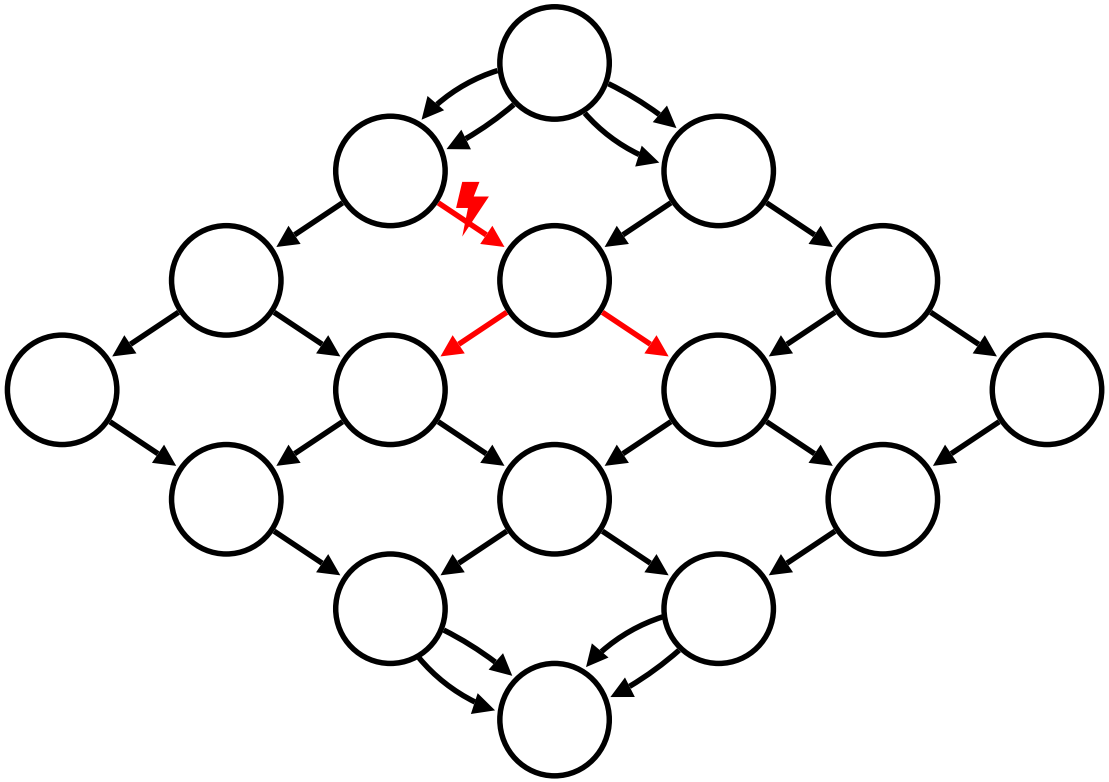
Problemas em codificação de rede

Erros nos canais



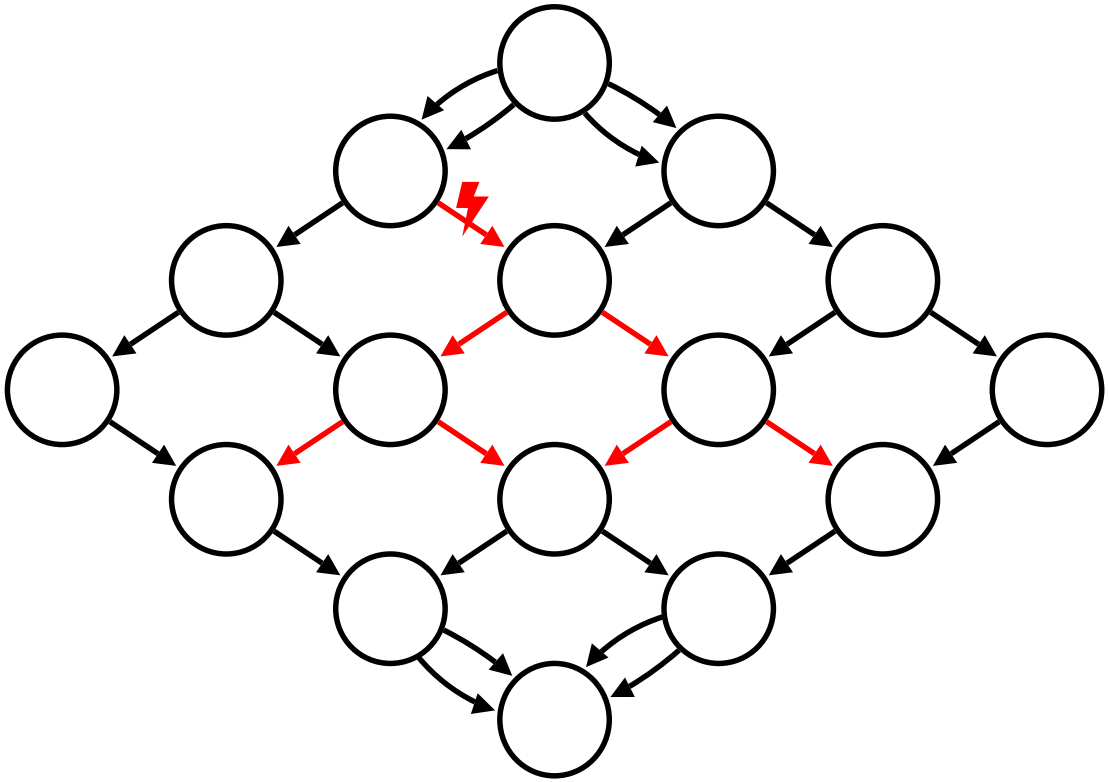
Problemas em codificação de rede

Erros nos canais



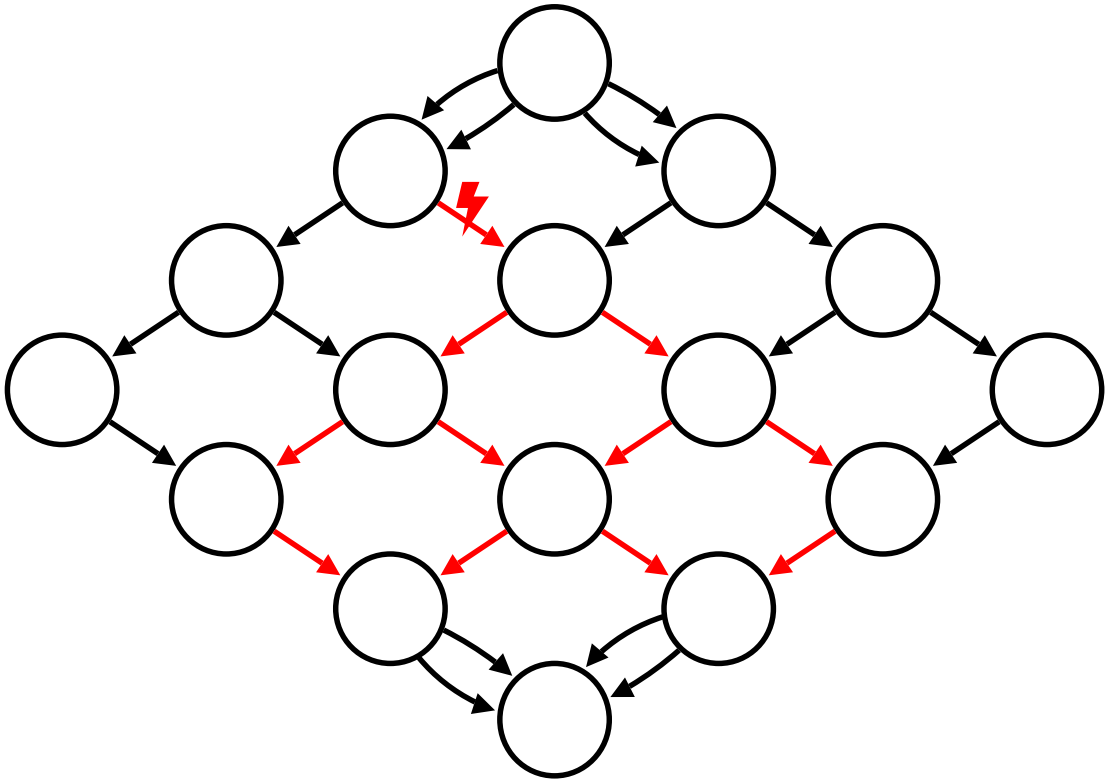
Problemas em codificação de rede

Erros nos canais



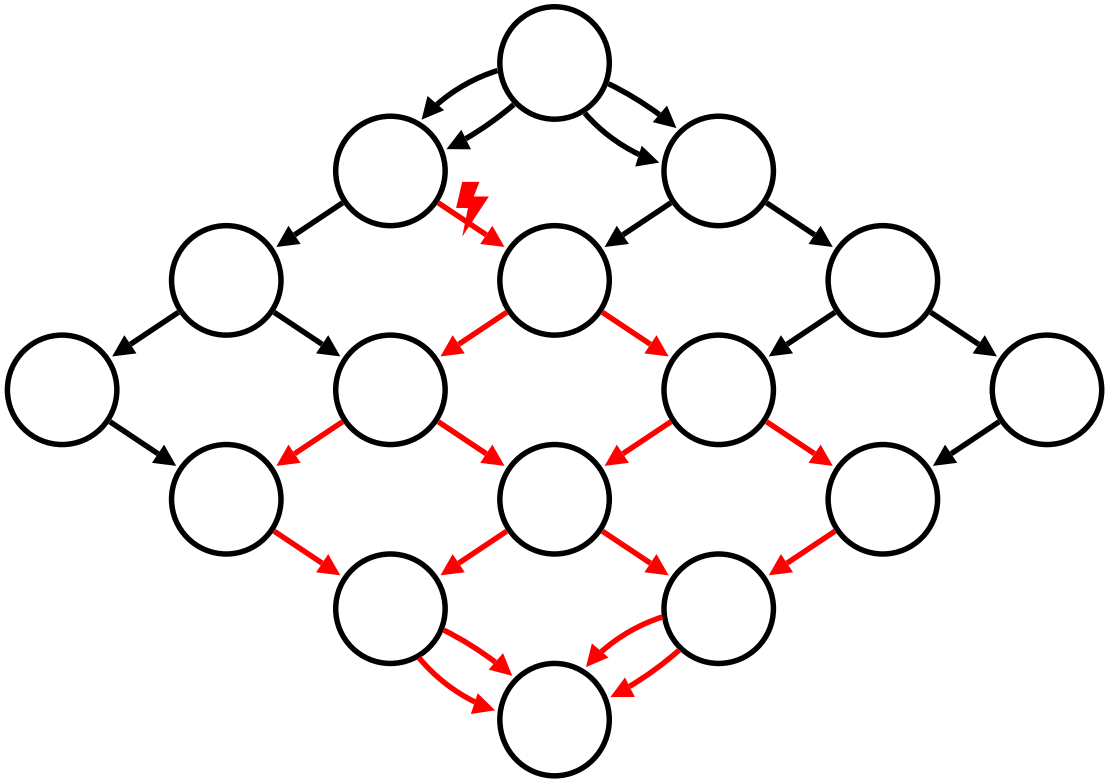
Problemas em codificação de rede

Erros nos canais



Problemas em codificação de rede

Erros nos canais



Problemas em codificação de rede

Outros problemas

- Perdas de pacotes
- Em codificação de rede linear aleatória:
  - Escolha infeliz das combinações lineares
  - mincut superestimado

Problemas em codificação de rede

Outros problemas

- Perdas de pacotes
- Em codificação de rede linear aleatória:
  - Escolha infeliz das combinações lineares
  - mincut superestimado

Não-coerência

Descrição e proposta

- Transmissor e receptor desconhecem a matriz **G**
- Como proceder? Através de códigos matriciais externos:
  - Limitar as possíveis entradas a um subconjunto $\mathcal{X} \subseteq \mathbb{F}_q^{h \times m}$
  - Preço: redução da taxa
- Duas propostas:
  - Chou *et. al.*
  - Koetter & Kschischang

Não-coerência

Descrição e proposta

- Transmissor e receptor desconhecem a matriz **G**
- Como proceder? Através de códigos matriciais externos:
  - Limitar as possíveis entradas a um subconjunto $\mathcal{X} \subseteq \mathbb{F}_q^{h \times m}$
  - Preço: redução da taxa
- Duas propostas:
  - Chou *et. al.*
  - Koetter & Kschischang

Não-coerência

Descrição e proposta

- Transmissor e receptor desconhecem a matriz **G**
- Como proceder? Através de códigos matriciais externos:
  - Limitar as possíveis entradas a um subconjunto $\mathcal{X} \subseteq \mathbb{F}_q^{h \times m}$
  - Preço: redução da taxa
- Duas propostas:
  - Chou *et. al.*
  - Koetter & Kschischang

Não-coerência

Chou *et. al.*

- Cabeçalho em cada vetor formando matriz identidade
- Palavras de $\mathcal{X}$ são da forma

$$\mathbf{X} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & x'_{1,1} & x'_{1,2} & \cdots & x'_{1,(m-h)} \\ 0 & 1 & 0 & \cdots & 0 & x'_{2,1} & x'_{2,2} & \cdots & x'_{2,(m-h)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & x'_{h,1} & x'_{h,2} & \cdots & x'_{h(m-h)} \end{bmatrix}$$

$$= \left[\begin{array}{c|c} \mathbf{I} & \mathbf{X}' \end{array} \right]$$

- Submatriz $\mathbf{I}$: estimar o "canal"
- Submatriz $\mathbf{X}'$: contém informação

Não-coerência

Chou *et. al.*

- Cabeçalho em cada vetor formando matriz identidade
- Palavras de $\mathcal{X}$ são da forma

$$\mathbf{X} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & x'_{1,1} & x'_{1,2} & \cdots & x'_{1,(m-h)} \\ 0 & 1 & 0 & \cdots & 0 & x'_{2,1} & x'_{2,2} & \cdots & x'_{2,(m-h)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & x'_{h,1} & x'_{h,2} & \cdots & x'_{h(m-h)} \end{bmatrix}$$

$$= \begin{bmatrix} \mathbf{I} & | & \mathbf{X}' \end{bmatrix}$$

- Submatriz $\mathbf{I}$: estimar o "canal"
- Submatriz $\mathbf{X}'$: contém informação

Não-coerência

Chou *et. al.*

- Cabeçalho em cada vetor formando matriz identidade
- Palavras de $\mathcal{X}$ são da forma

$$\mathbf{X} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & x'_{1,1} & x'_{1,2} & \cdots & x'_{1,(m-h)} \\ 0 & 1 & 0 & \cdots & 0 & x'_{2,1} & x'_{2,2} & \cdots & x'_{2,(m-h)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & x'_{h,1} & x'_{h,2} & \cdots & x'_{h(m-h)} \end{bmatrix}$$

$$= \left[\begin{array}{c|c} \mathbf{I} & \mathbf{X}' \end{array} \right]$$

- Submatriz $\mathbf{I}$: estimar o "canal"
- Submatriz $\mathbf{X}'$: contém informação

Não-coerência

Chou *et. al.*

- Cabeçalho em cada vetor formando matriz identidade
- Palavras de $\mathcal{X}$ são da forma

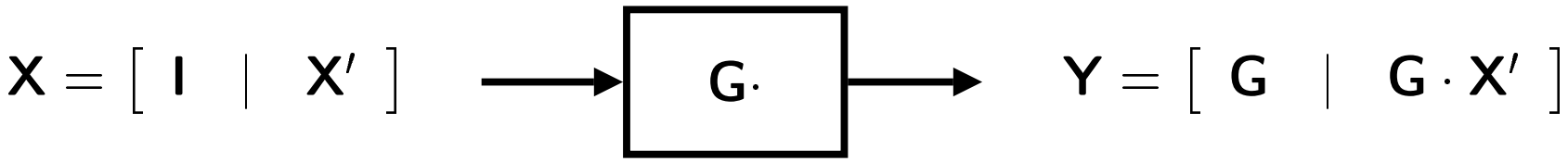
$$\mathbf{X} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & x'_{1,1} & x'_{1,2} & \cdots & x'_{1,(m-h)} \\ 0 & 1 & 0 & \cdots & 0 & x'_{2,1} & x'_{2,2} & \cdots & x'_{2,(m-h)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & x'_{h,1} & x'_{h,2} & \cdots & x'_{h(m-h)} \end{bmatrix}$$

$$= \left[\begin{array}{c|c} \mathbf{I} & \mathbf{X}' \end{array} \right]$$

- Submatriz $\mathbf{I}$: estimar o "canal"
- Submatriz $\mathbf{X}'$: contém informação

Não-coerência

Chou *et. al.*



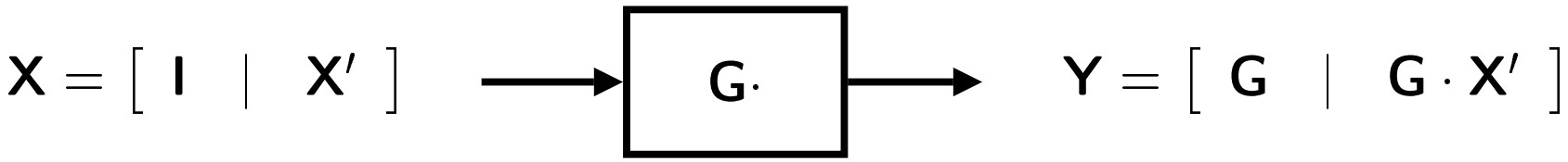
- Receptor consegue descobrir a matriz **G**
- Dos hm símbolos, h^2 não carregam informação

Taxa

$$R(\mathcal{X}) = \frac{hm - h^2}{hm} = 1 - \frac{h}{m}$$

Não-coerência

Chou *et. al.*



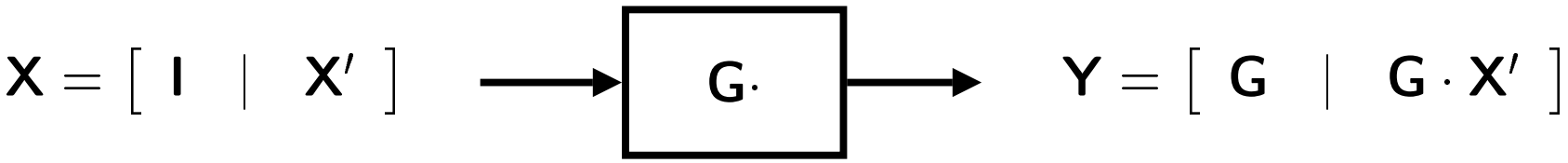
- Receptor consegue descobrir a matriz **G**
- Dos hm símbolos, h^2 não carregam informação

Taxa

$$R(\mathcal{X}) = \frac{hm - h^2}{hm} = 1 - \frac{h}{m}$$

Não-coerência

Chou *et. al.*



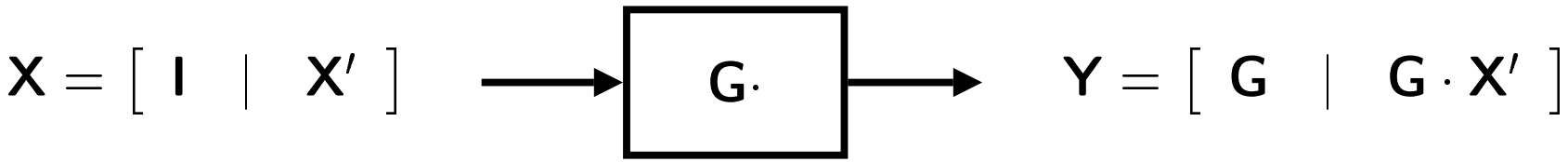
- Receptor consegue descobrir a matriz **G**
- Dos hm símbolos, h^2 não carregam informação

Taxa

$$R(\mathcal{X}) = \frac{hm - h^2}{hm} = 1 - \frac{h}{m}$$

Não-coerência

Chou *et. al.*



- Receptor consegue descobrir a matriz **G**
- Dos hm símbolos, h^2 não carregam informação

Taxa

$$R(\mathcal{X}) = \frac{hm - h^2}{hm} = 1 - \frac{h}{m}$$

Não-coerência

Koetter & Kschischang

- Subespaço vetorial gerado pelas linhas de $\mathbf{X}$ é preservado:

$$\langle \mathbf{Y} \rangle = \langle \mathbf{X} \rangle$$

- Ideia: codificar informação em subespaços

Não-coerência

Koetter & Kschischang

- Subespaço vetorial gerado pelas linhas de $\mathbf{X}$ é preservado:

$$\langle \mathbf{Y} \rangle = \langle \mathbf{X} \rangle$$

- Ideia: codificar informação em subespaços

Não-coerência

Koetter & Kschischang

Coeficiente binomial gaussiano

$$\binom{m}{k}_q = \prod_{i=0}^{k-1} \frac{q^m - q^i}{q^k - q^i}$$

Mede o número de subespaços k-dimensionais de $\mathbb{F}_q^m$

Taxa

$$R(\mathcal{X}) = \frac{1}{hm} \log_q \sum_{k=0}^{h} \binom{m}{k}_q$$

Não-coerência

Koetter & Kschischang

Coeficiente binomial gaussiano

$$\binom{m}{k}_q = \prod_{i=0}^{k-1} \frac{q^m - q^i}{q^k - q^i}$$

Mede o número de subespaços k-dimensionais de $\mathbb{F}_q^m$

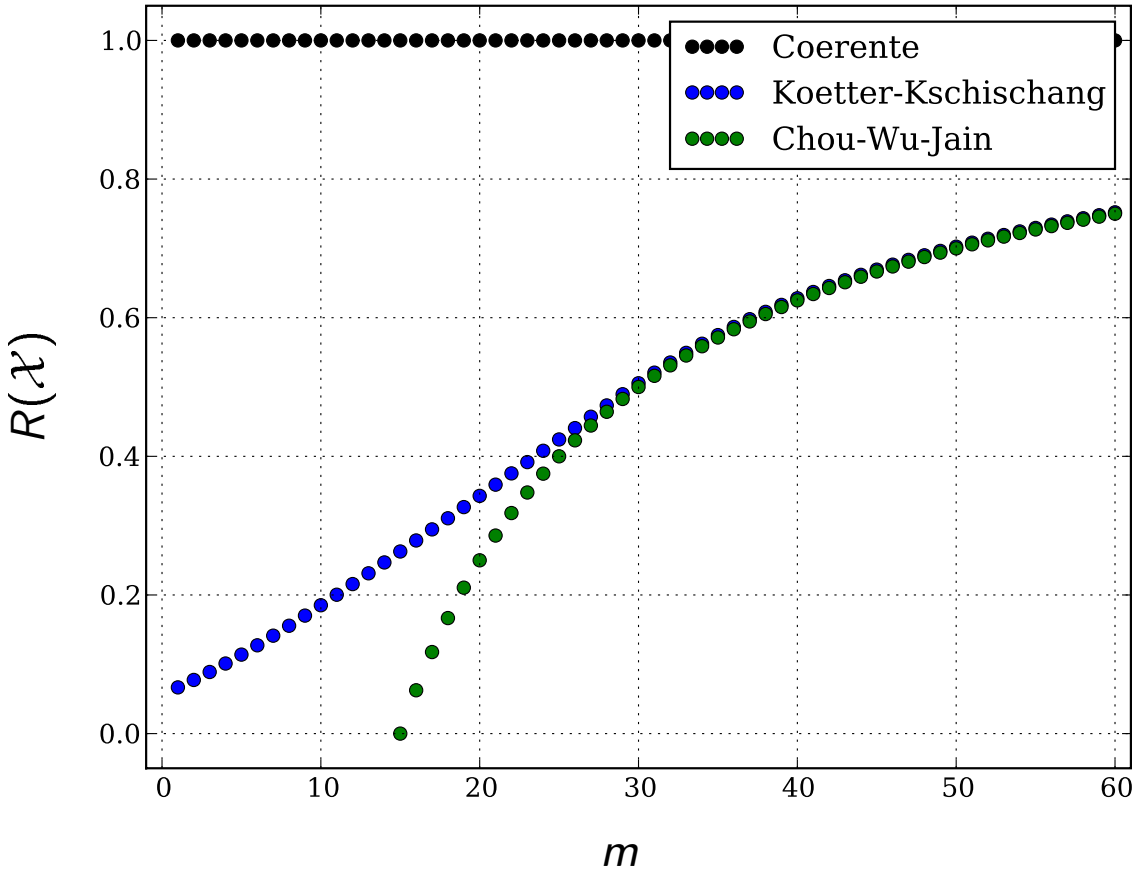
Taxa

$$R(\mathcal{X}) = \frac{1}{hm} \log_q \sum_{k=0}^{h} \binom{m}{k}_q$$

Não-coerência

Comparação entre os métodos

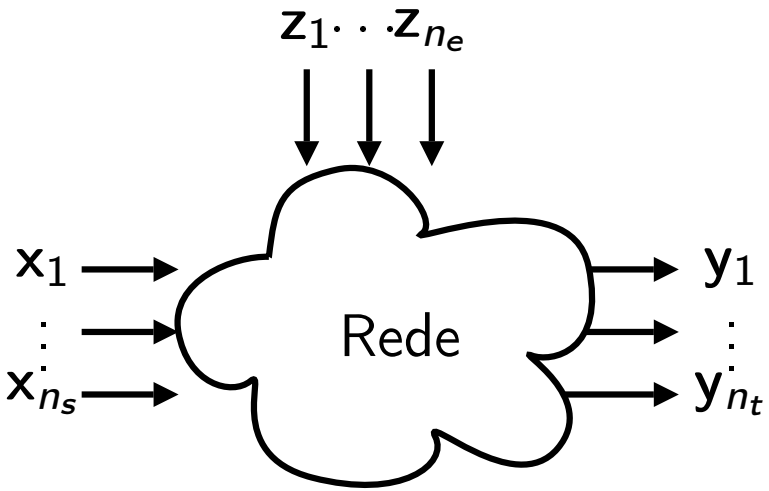
Curvas para $q = 2$ e $h = 15$



Controle de erros

Modelo da rede com erros

São injetados n_e vetores de erro



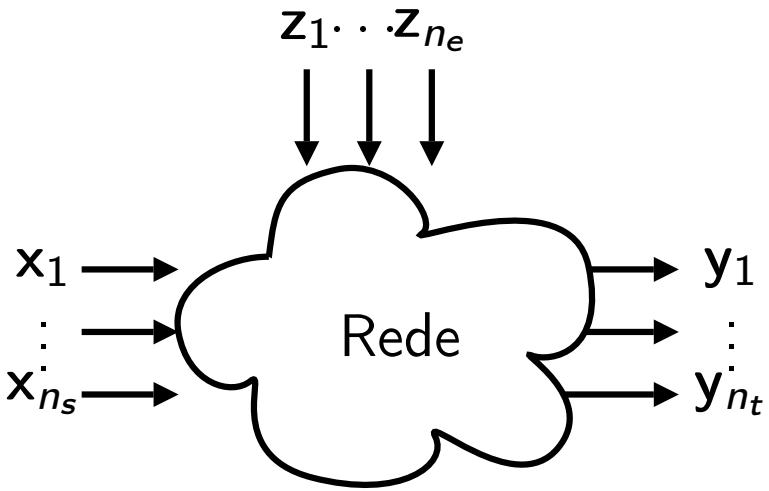
Matriz de erros:

$$Z = \begin{bmatrix} \longleftarrow & z_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & z_{n_e} & \longrightarrow \end{bmatrix}_{n_e \times m}$$

Controle de erros

Modelo da rede com erros

São injetados n_e vetores de erro

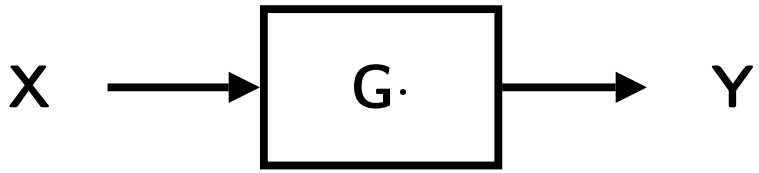


Matriz de erros:

$$Z = \begin{bmatrix} \longleftarrow & z_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & z_{n_e} & \longrightarrow \end{bmatrix}_{n_e \times m}$$

Controle de erros

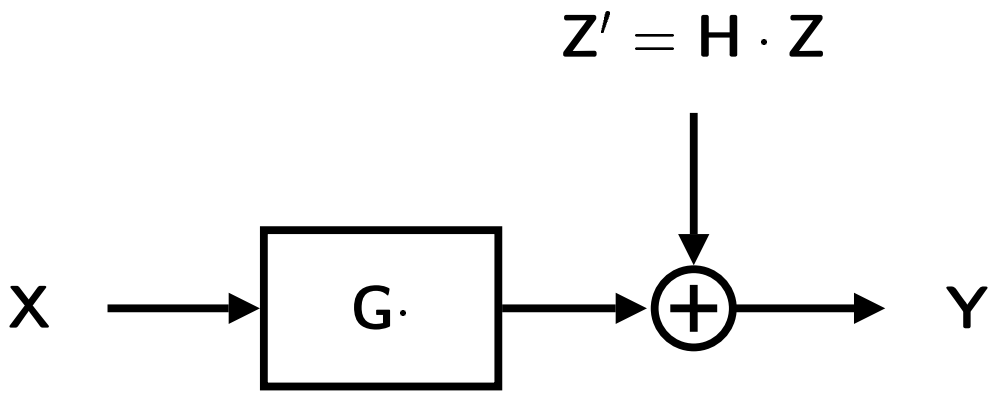
Modelo da rede com erros



$$Y = G \cdot X$$

Controle de erros

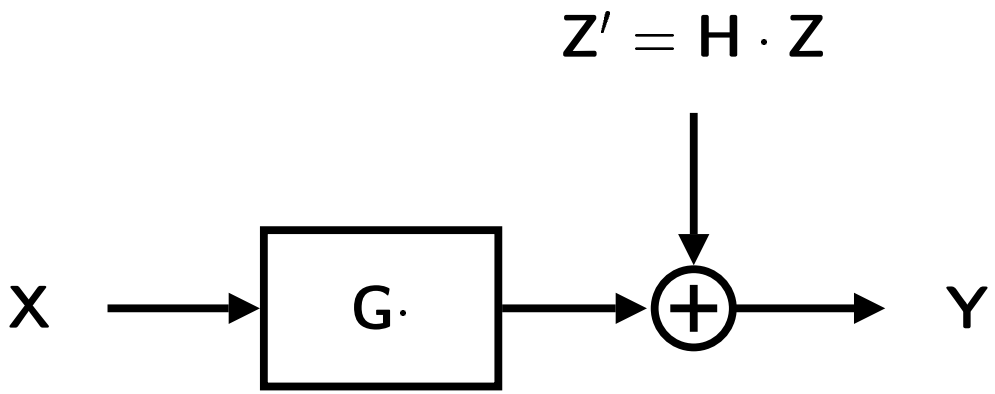
Modelo da rede com erros



$$Y = G \cdot X + H \cdot Z$$

Controle de erros

Modelo da rede com erros

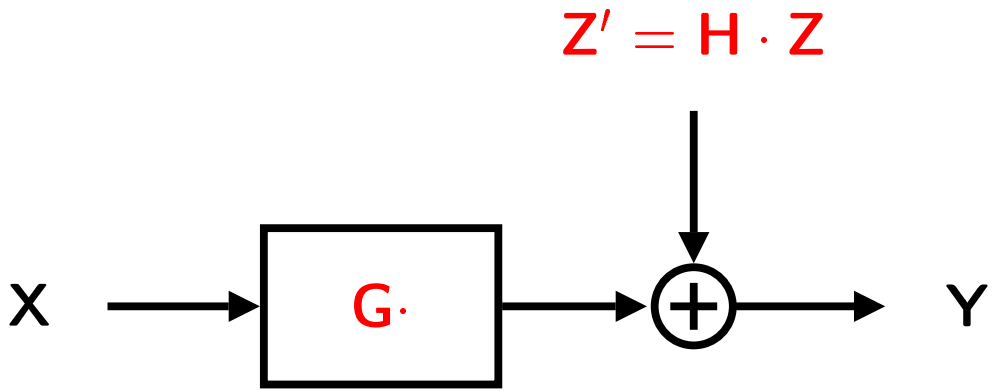


$$Y = G \cdot X + H \cdot Z$$

- Será considerado o caso não-coerente

Controle de erros

Modelo adversário: caso não-coerente

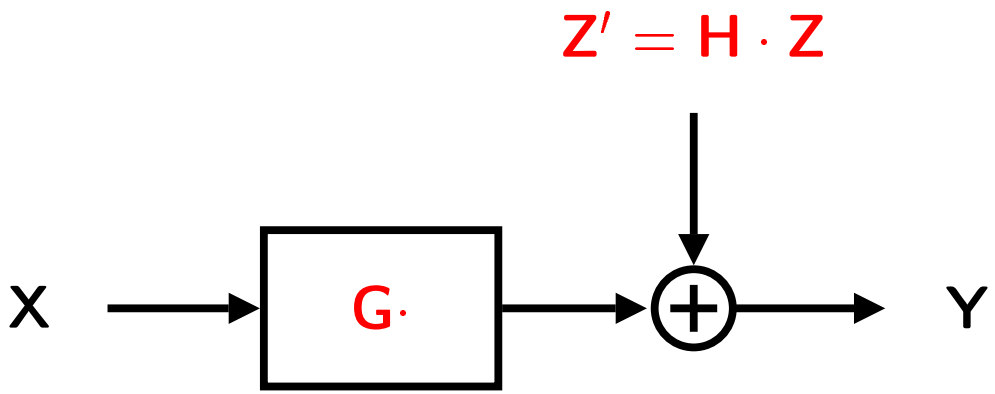


$$\mathbf{Y} = \mathbf{G} \cdot \mathbf{X} + \mathbf{H} \cdot \mathbf{Z}$$

- Fonte e destino desconhecem **G**, **H** e **Z**
- Adversário conhece **X** e escolhe **G**, **H** e **Z**
- n_e é limitado por τ e rankdef **G** é limitada por ρ

Controle de erros

Modelo adversário: caso não-coerente

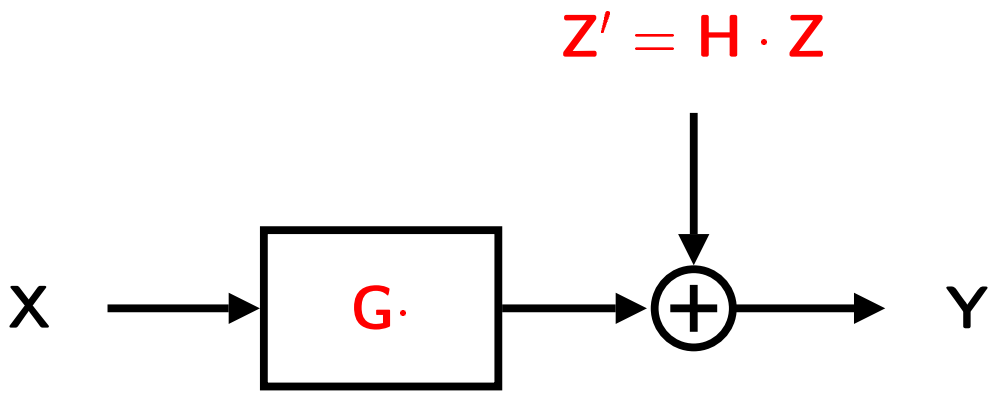


$$\mathbf{Y} = \mathbf{G} \cdot \mathbf{X} + \mathbf{H} \cdot \mathbf{Z}$$

- Fonte e destino desconhecem **G**, **H** e **Z**
- Adversário conhece **X** e escolhe **G**, **H** e **Z**
- n_e é limitado por τ e rankdef **G** é limitada por ρ

Controle de erros

Modelo adversário: caso não-coerente

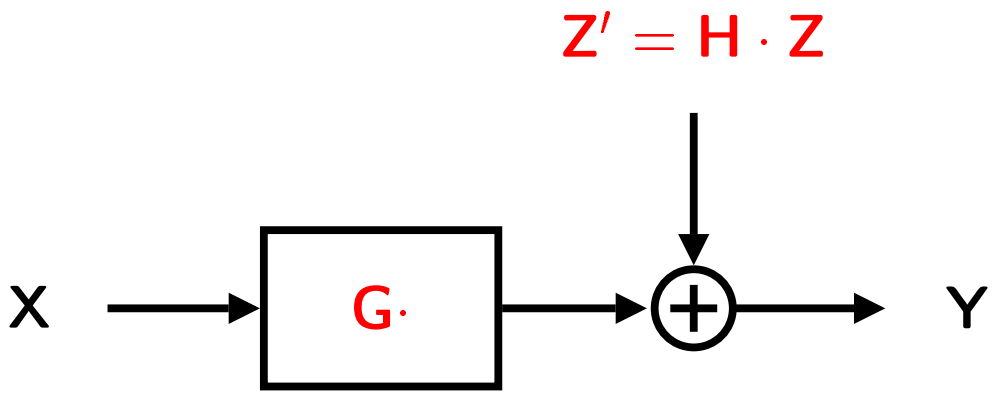


$$\mathbf{Y} = \mathbf{G} \cdot \mathbf{X} + \mathbf{H} \cdot \mathbf{Z}$$

- Fonte e destino desconhecem **G**, **H** e **Z**
- Adversário conhece **X** e escolhe **G**, **H** e **Z**
- n_e é limitado por τ e rankdef **G** é limitada por ρ

Controle de erros

Modelo adversário: caso não-coerente



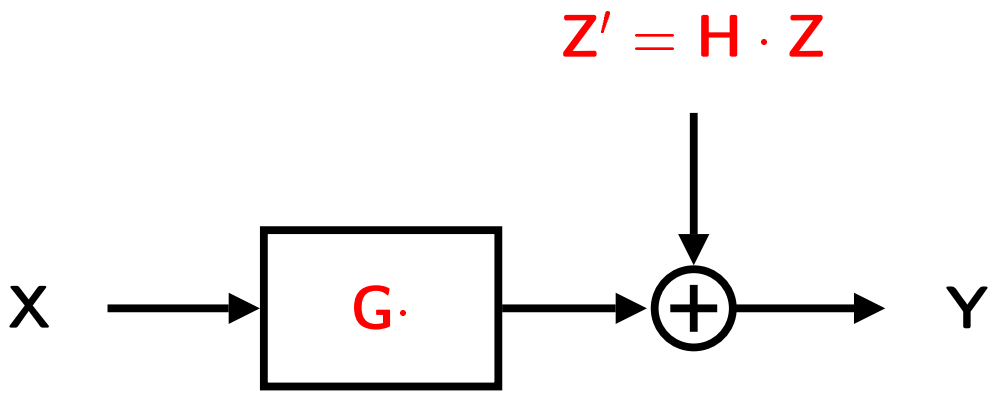
$$\mathbf{Y} = \mathbf{G} \cdot \mathbf{X} + \mathbf{H} \cdot \mathbf{Z}$$

Problemas

- Erros nos canais de transmissão ($\mathbf{Z}'$ com $\tau \neq 0$)
- Código de rede infeliz e perda de pacotes ($\mathbf{G}$ com $\rho \neq 0$)

Controle de erros

Modelo adversário: caso não-coerente



$$Y = G \cdot X + H \cdot Z$$

Solução

- Códigos de subespaço: transmitir um subconjunto de subespaços

Codificação de Subespaço

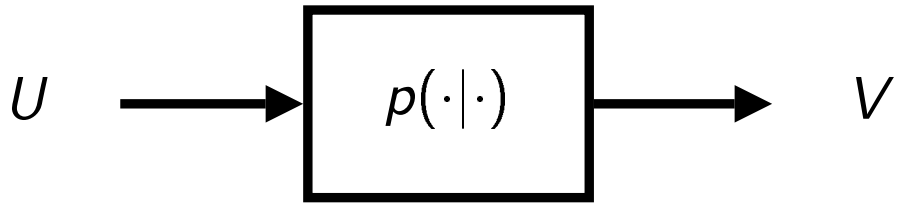
Canal de subespaço

Definição

Definição

O canal de subespaço é um "DMC" dado por

$$(\mathcal{P}(\mathbb{F}_q^m), p(\cdot|\cdot), \mathcal{P}(\mathbb{F}_q^m))$$



Notação

Espaço projetivo $\mathcal{P}(\mathbb{F}_q^m)$: conjunto de todos os subespaços de $\mathbb{F}_q^m$

Abordagem: teoria da codificação *vs* ~~teoria da informação~~

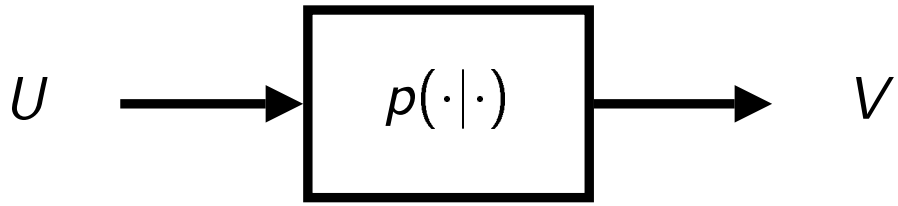
Canal de subespaço

Definição

Definição

O canal de subespaço é um "DMC" dado por

$$(\mathcal{P}(\mathbb{F}_q^m), p(\cdot|\cdot), \mathcal{P}(\mathbb{F}_q^m))$$



Notação

Espaço projetivo $\mathcal{P}(\mathbb{F}_q^m)$: conjunto de todos os subespaços de $\mathbb{F}_q^m$

Abordagem: teoria da codificação *vs* ~~teoria da informação~~

Distância de subespaço

Diagrama de Hasse

Mede o número mínimo de remoções e inserções de dimensões

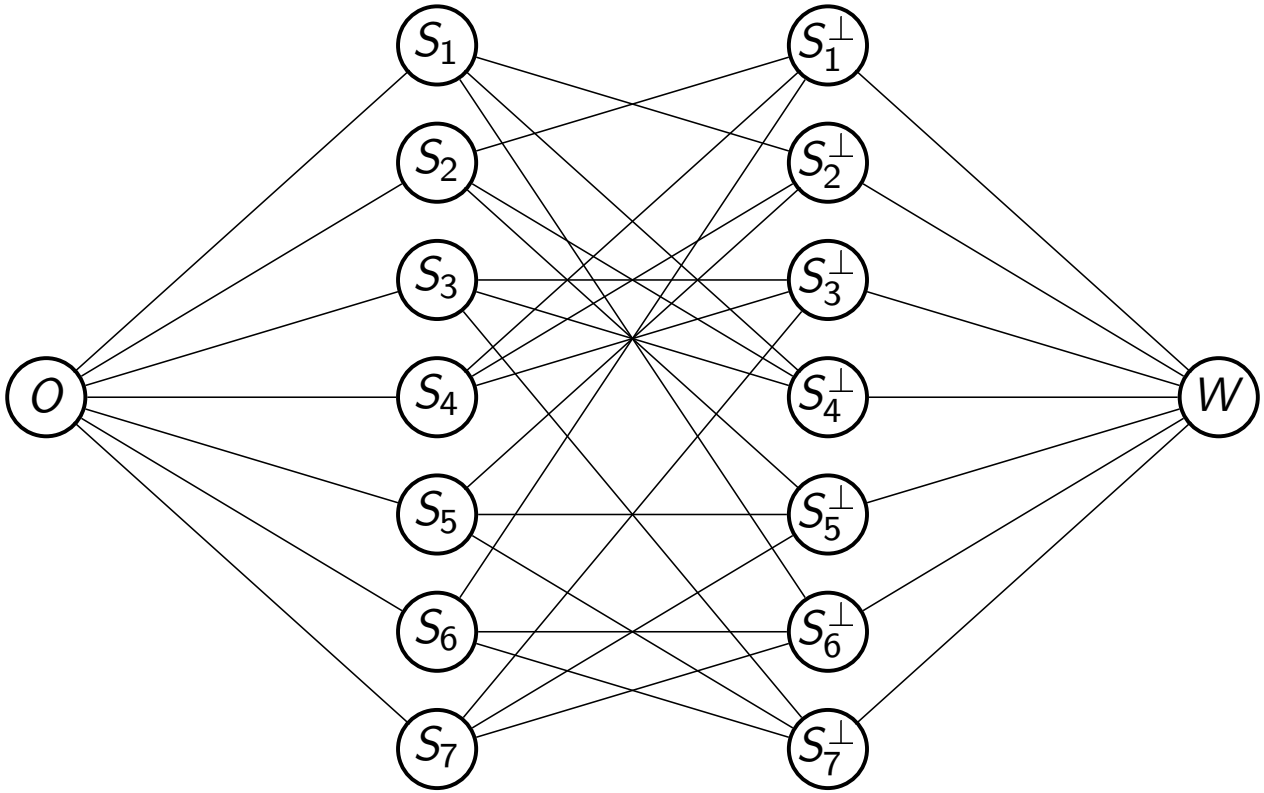
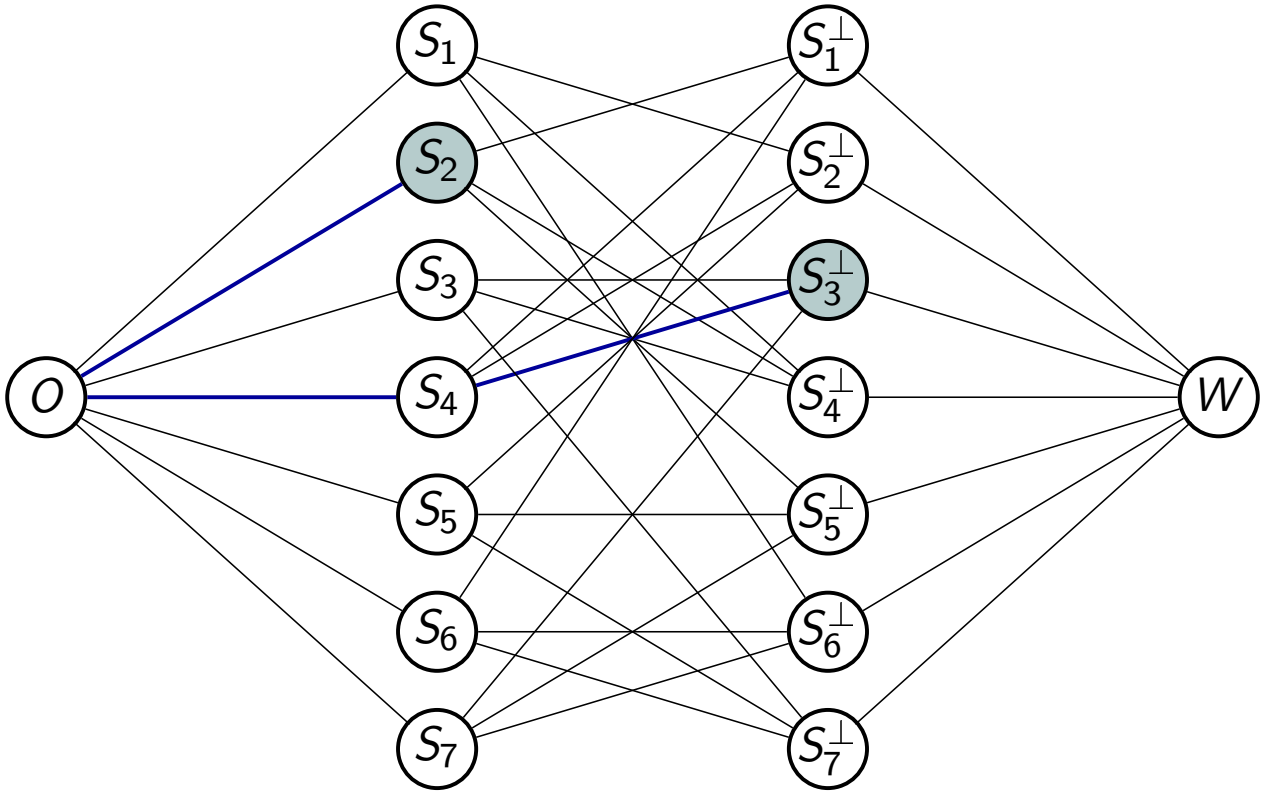


Diagrama de Hasse de $\mathcal{P}(\mathbb{F}_2^3)$

Distância de subespaço

Diagrama de Hasse

Mede o número mínimo de remoções e inserções de dimensões

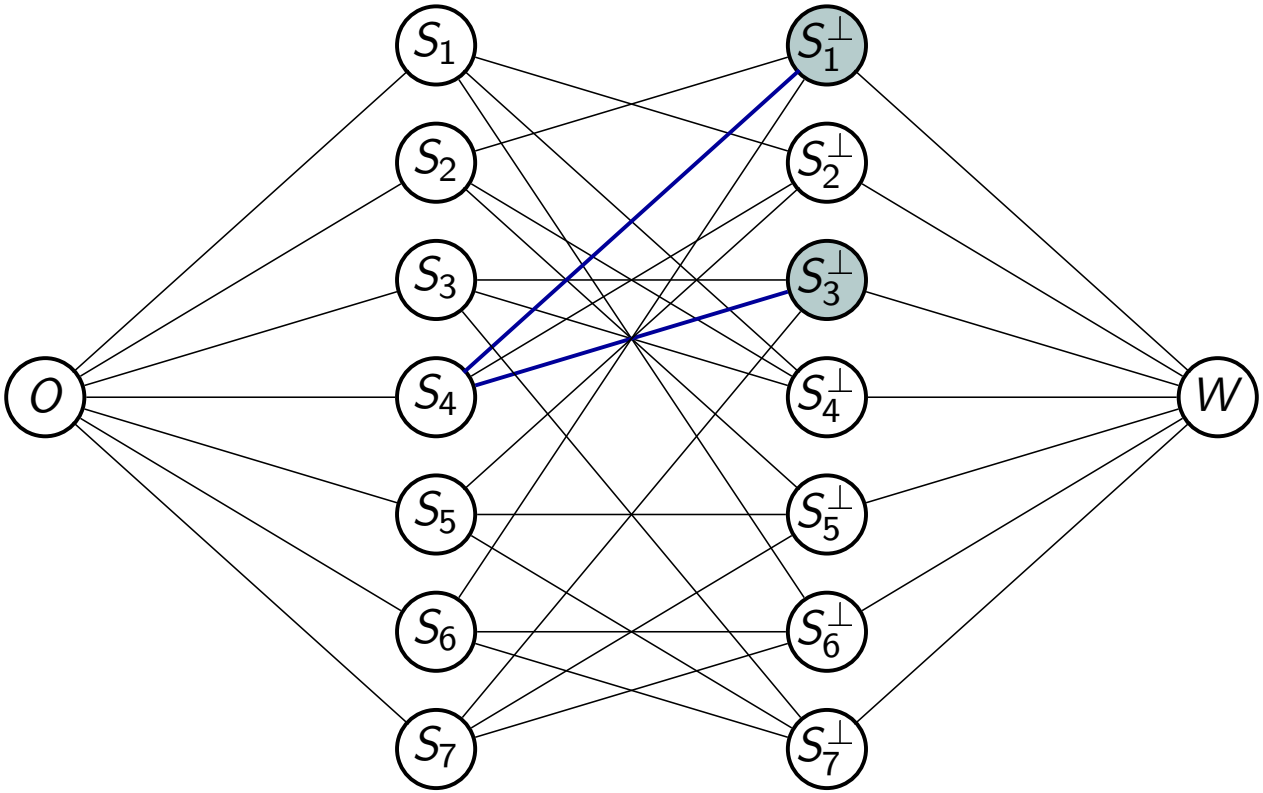


$$d_S(S_2, S_3^{\perp}) = 3$$

Distância de subespaço

Diagrama de Hasse

Mede o número mínimo de remoções e inserções de dimensões



$$\mathrm{d_S}(S_1^\perp, S_3^\perp) = 2$$

Distância de subespaço

Definição algébrica

Definição

A distância de subespaço é dada por

$$d_S(V_1, V_2) = \dim(V_1 \dotplus V_2) - \dim(V_1 \cap V_2)$$

Teorema

$d_S(\cdot, \cdot)$ é uma métrica em $\mathcal{P}(\mathbb{F}_q^m)$

Distância de subespaço

Definição algébrica

Definição

A distância de subespaço é dada por

$$d_S(V_1, V_2) = \dim(V_1 \dotplus V_2) - \dim(V_1 \cap V_2)$$

Teorema

$d_S(\cdot, \cdot)$ é uma métrica em $\mathcal{P}(\mathbb{F}_q^m)$

Códigos de subespaço

Citações

Citação

"Dado um espaço métrico, é possível definir códigos."

— Etzion & Vardy

Citação

"Assim como o hipercubo de Hamming é apropriado no contexto dos códigos corretores de erro 'clássicos', o diagrama de Hasse é apropriado para o controle de erros em codificação de rede não coerente."

— Koetter & Kschischang

Códigos de subespaço

Citações

Citação

"Dado um espaço métrico, é possível definir códigos."

— Etzion & Vardy

Citação

"Assim como o hipercubo de Hamming é apropriado no contexto dos códigos corretores de erro 'clássicos', o diagrama de Hasse é apropriado para o controle de erros em codificação de rede não coerente."

— Koetter & Kschischang

Códigos de subespaço

Definição e parâmetros

Definição

Um código de subespaço $\mathcal{C}$ é um subconjunto não vazio de $\mathcal{P}(\mathbb{F}_q^m)$

Definição

A cardinalidade (tamanho) do código $\mathcal{C}$ é dada por $|\mathcal{C}|$

Definição

A distância mínima do código $\mathcal{C}$ é dada por

$$d_S(\mathcal{C}) = \min_{V \neq U} d_S(V, U)$$

Códigos de subespaço

Definição e parâmetros

Definição

Um código de subespaço $\mathcal{C}$ é um subconjunto não vazio de $\mathcal{P}(\mathbb{F}_q^m)$

Definição

A cardinalidade (tamanho) do código $\mathcal{C}$ é dada por $|\mathcal{C}|$

Definição

A distância mínima do código $\mathcal{C}$ é dada por

$$d_S(\mathcal{C}) = \min_{V \neq U} d_S(V, U)$$

Códigos de subespaço

Definição e parâmetros

Definição

Um código de subespaço $\mathcal{C}$ é um subconjunto não vazio de $\mathcal{P}(\mathbb{F}_q^m)$

Definição

A cardinalidade (tamanho) do código $\mathcal{C}$ é dada por $|\mathcal{C}|$

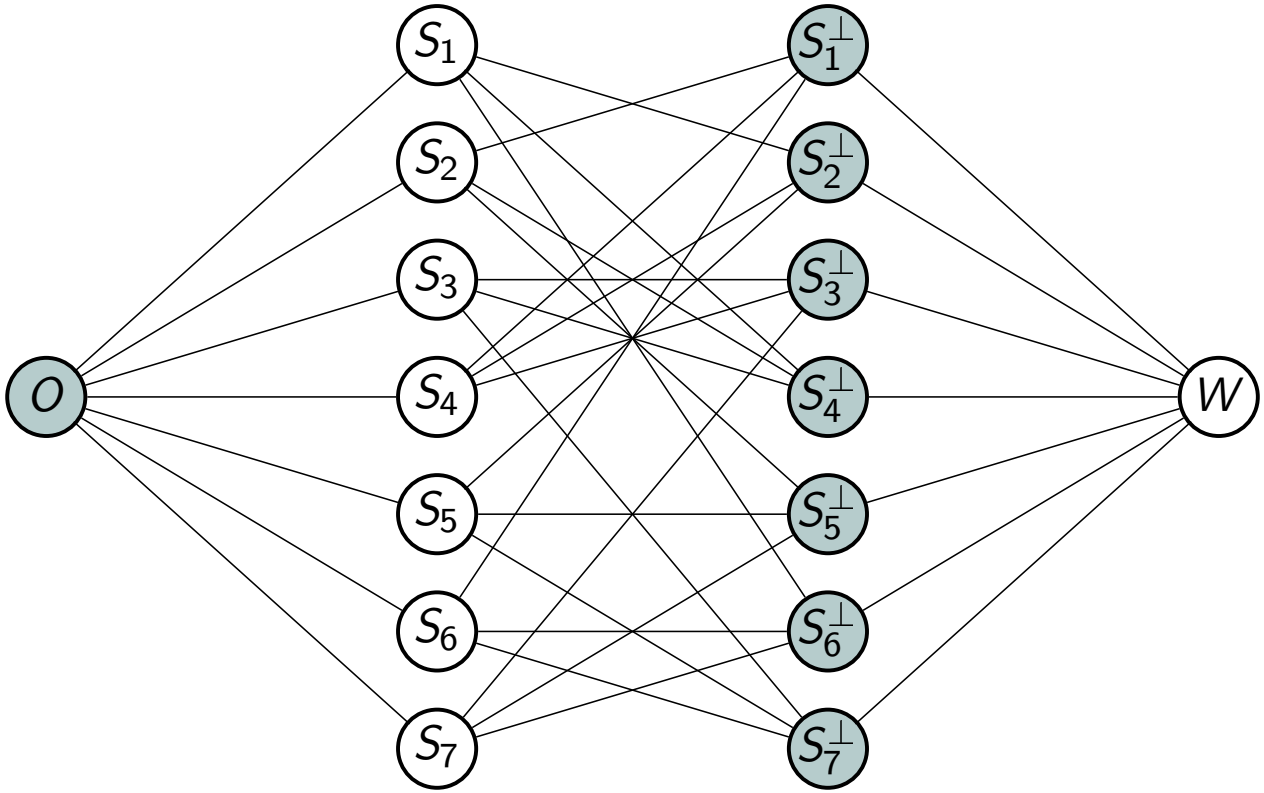
Definição

A distância mínima do código $\mathcal{C}$ é dada por

$$d_S(\mathcal{C}) = \min_{V \neq U} d_S(V, U)$$

Códigos de subespaço

Exemplo



$|\mathcal{C}| = 8$ e $\mathsf{d_S}(\mathcal{C}) = 2$

Códigos de subespaço

Compromisso entre taxa e capacidade de correção

- Cardinalidade $|\mathcal{C}|$: determina a taxa de informação
- Distância mínima $d_S(\mathcal{C})$: determina a capacidade de correção
- Objetivos conflitantes: maximizar ambos

Pergunta natural

Qual a maior cardinalidade dada uma certa distância mínima?

R: Não existe fórmula exata

Códigos de subespaço

Compromisso entre taxa e capacidade de correção

- Cardinalidade $|\mathcal{C}|$: determina a taxa de informação
- Distância mínima $d_S(\mathcal{C})$: determina a capacidade de correção
- Objetivos conflitantes: maximizar ambos

Pergunta natural

Qual a maior cardinalidade dada uma certa distância mínima?

R: Não existe fórmula exata

Códigos de subespaço

Compromisso entre taxa e capacidade de correção

- Cardinalidade $|\mathcal{C}|$: determina a taxa de informação
- Distância mínima $d_S(\mathcal{C})$: determina a capacidade de correção
- Objetivos conflitantes: maximizar ambos

Pergunta natural

Qual a maior cardinalidade dada uma certa distância mínima?

R: Não existe fórmula exata

Códigos de subespaço

Compromisso entre taxa e capacidade de correção

- Cardinalidade $|\mathcal{C}|$: determina a taxa de informação
- Distância mínima $d_S(\mathcal{C})$: determina a capacidade de correção
- Objetivos conflitantes: maximizar ambos

Pergunta natural

Qual a maior cardinalidade dada uma certa distância mínima?

R: Não existe fórmula exata

Códigos de subespaço

Compromisso entre taxa e capacidade de correção

- Cardinalidade $|\mathcal{C}|$: determina a taxa de informação
- Distância mínima $d_S(\mathcal{C})$: determina a capacidade de correção
- Objetivos conflitantes: maximizar ambos

Pergunta natural

Qual a maior cardinalidade dada uma certa distância mínima?

R: Não existe fórmula exata

Limitantes

- Determinam regiões no plano $|\mathcal{C}| \times \mathrm{d_S}(\mathcal{C})$ que asseguram a existência ou a inexistência de códigos
- São particularizados limitantes válidos para quaisquer espaços métricos

Limitantes

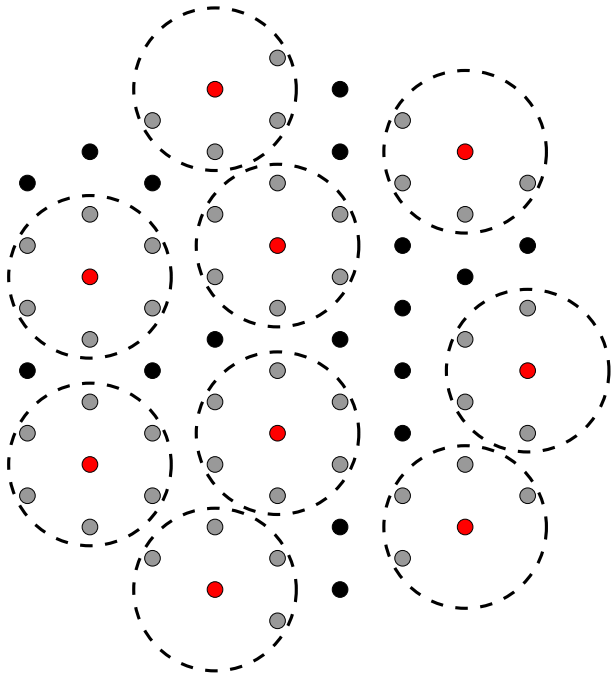
Digressão: limitante superior de Hamming

Empacota esferas disjuntas no espaço métrico $\mathcal{M}$

Teorema

Para todo código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d vale

$$|\mathcal{C}| \leq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\min}\left(\left\lfloor \frac{d-1}{2} \right\rfloor\right)}$$



Limitantes

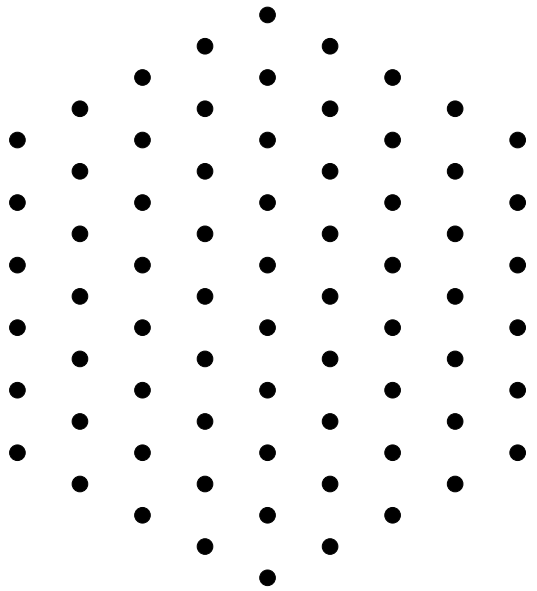
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

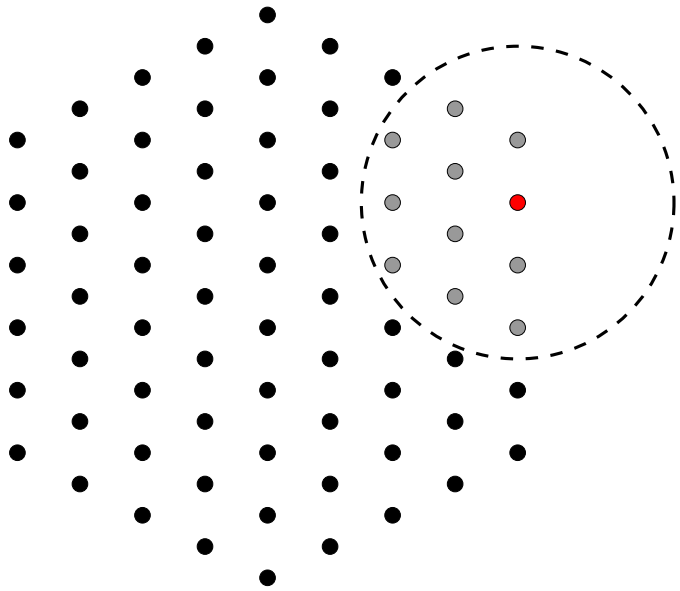
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

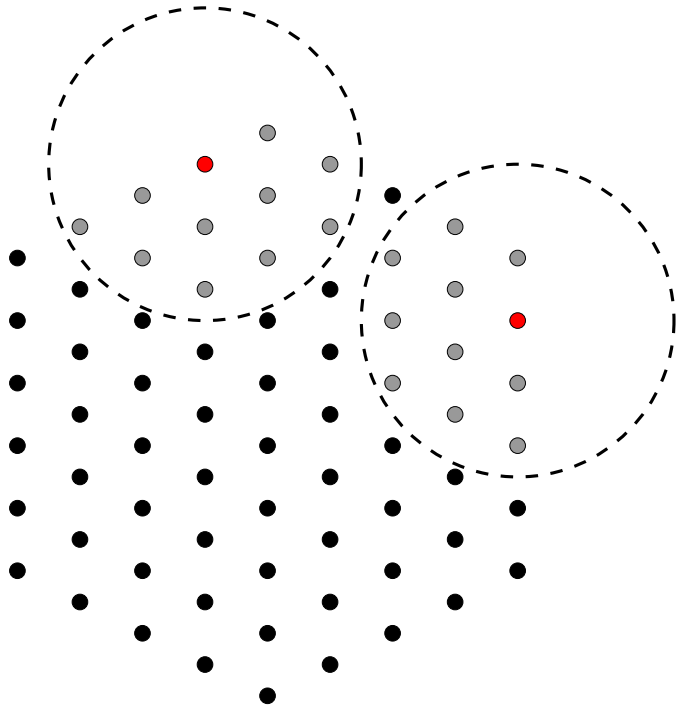
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

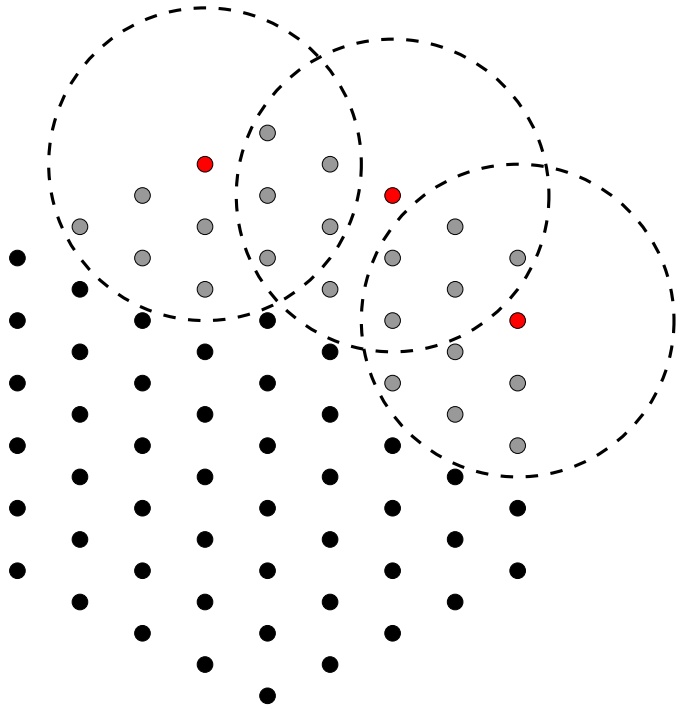
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

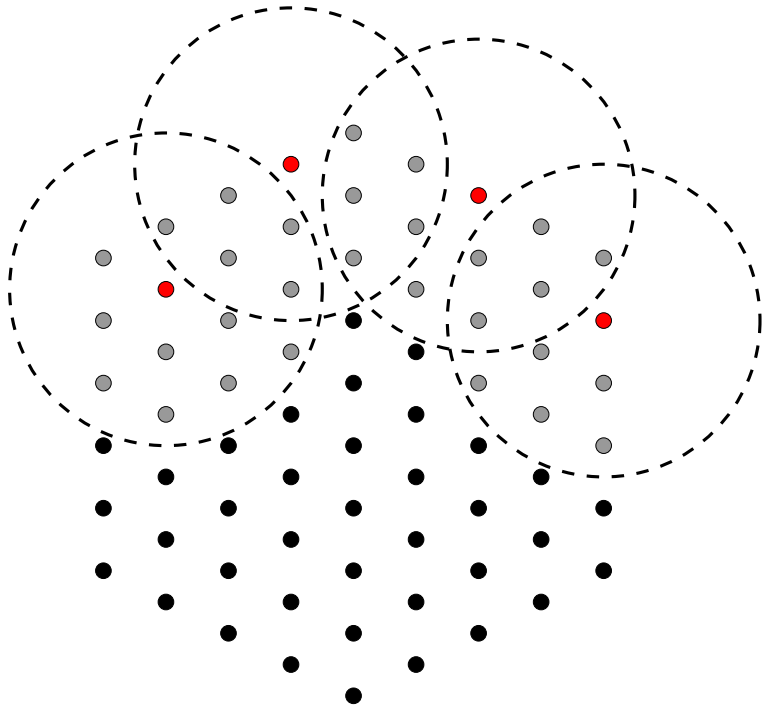
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

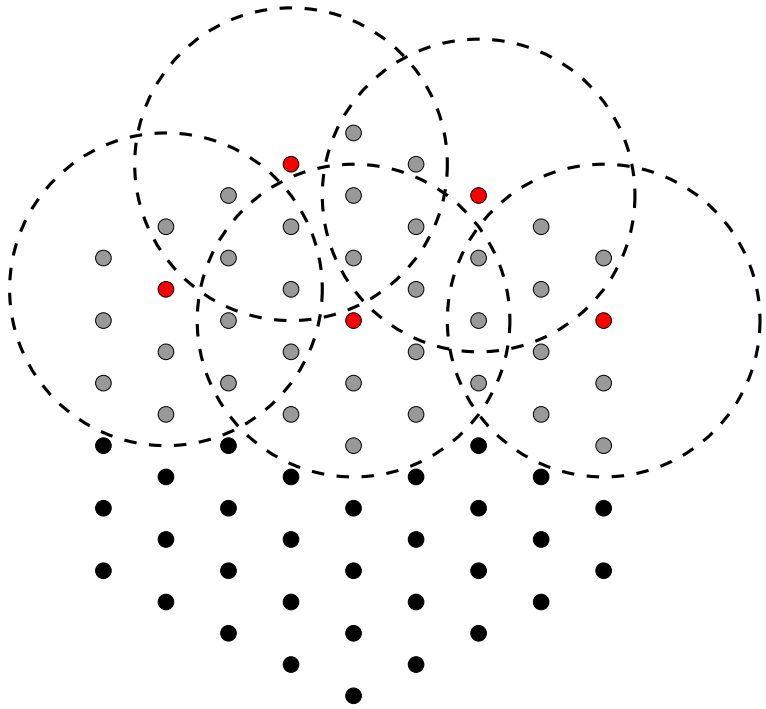
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

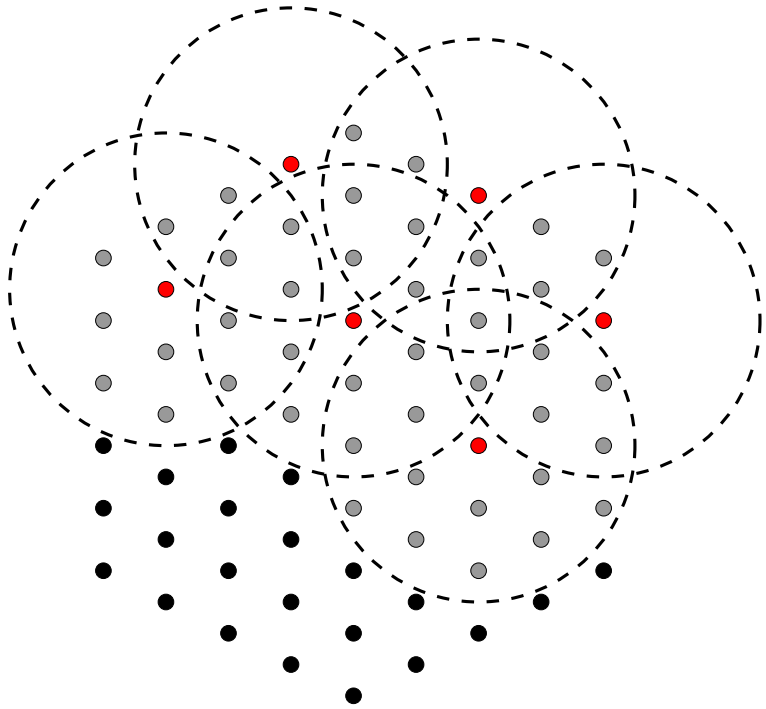
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

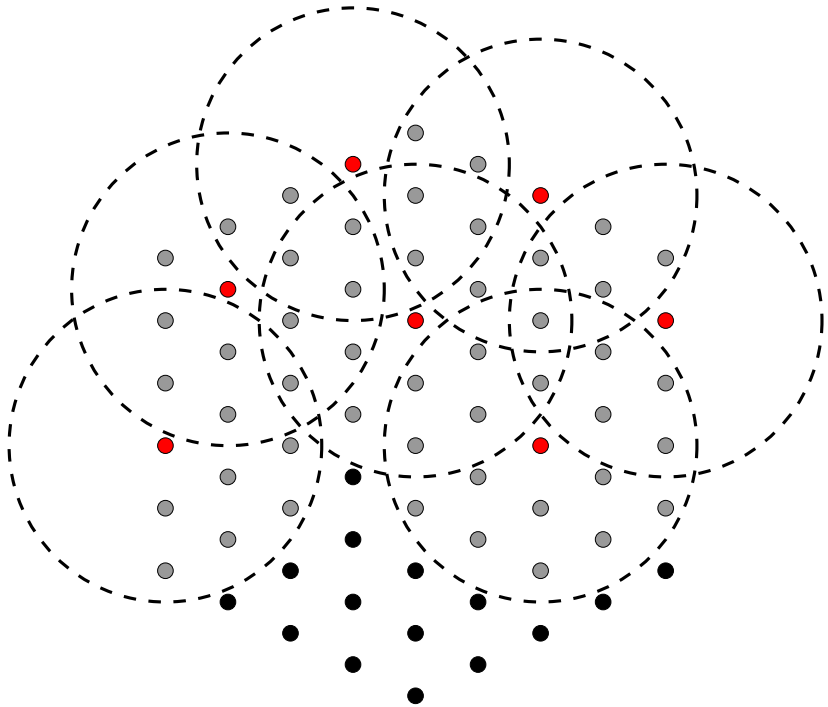
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

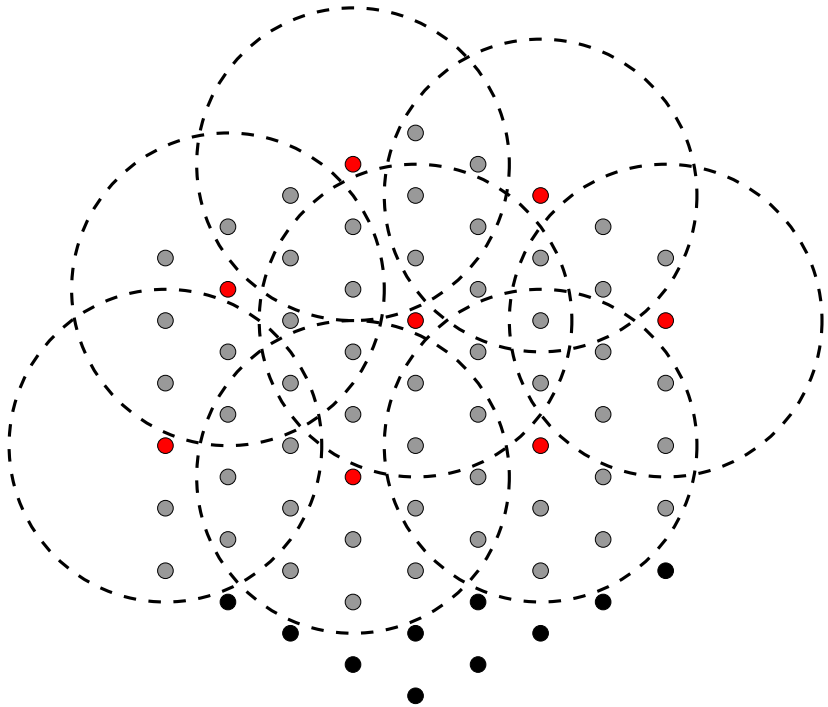
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

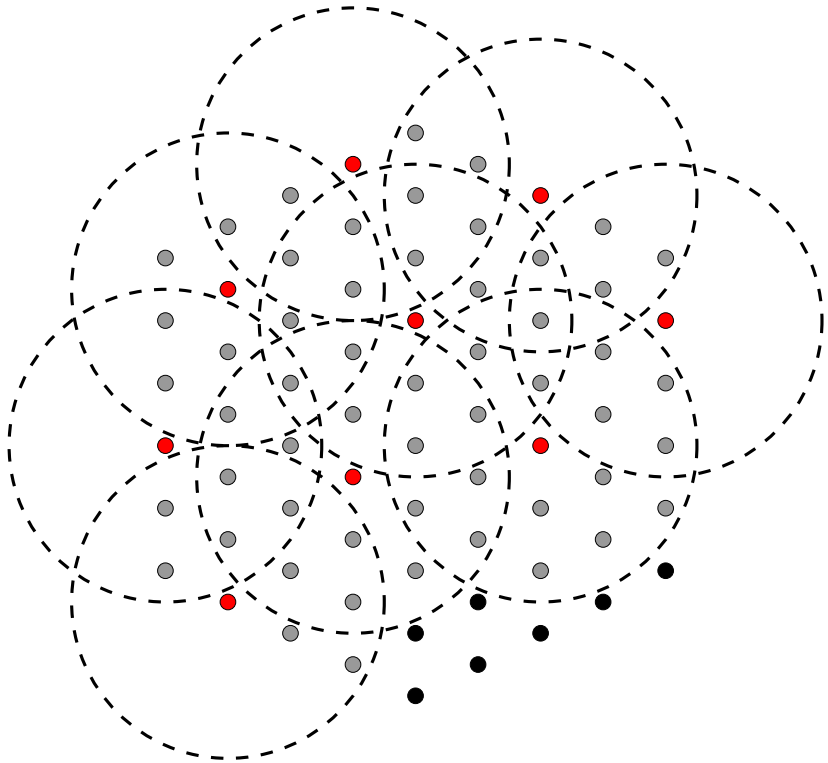
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

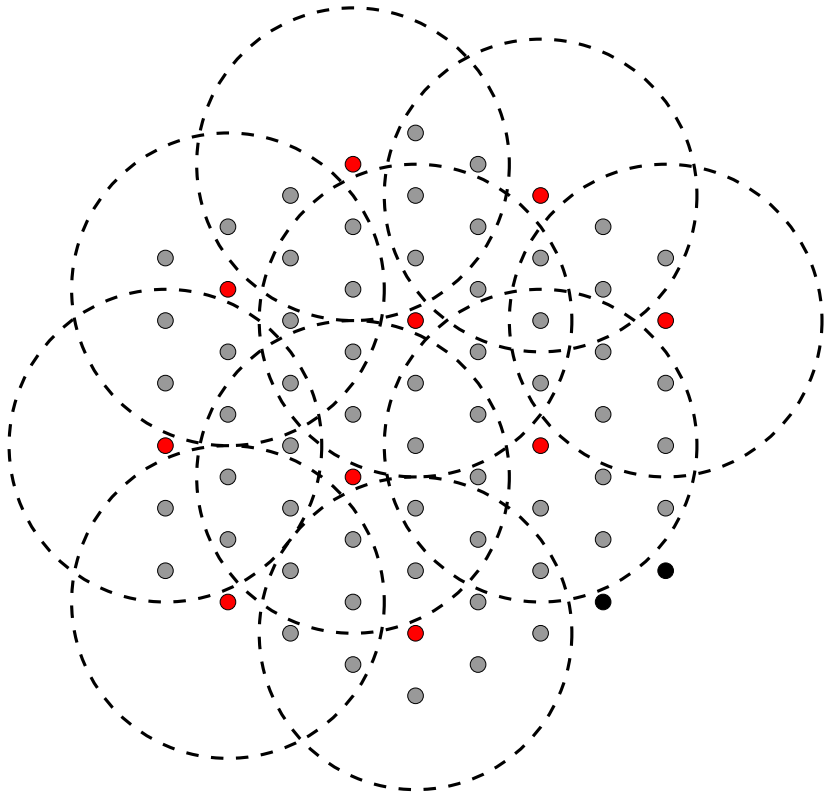
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

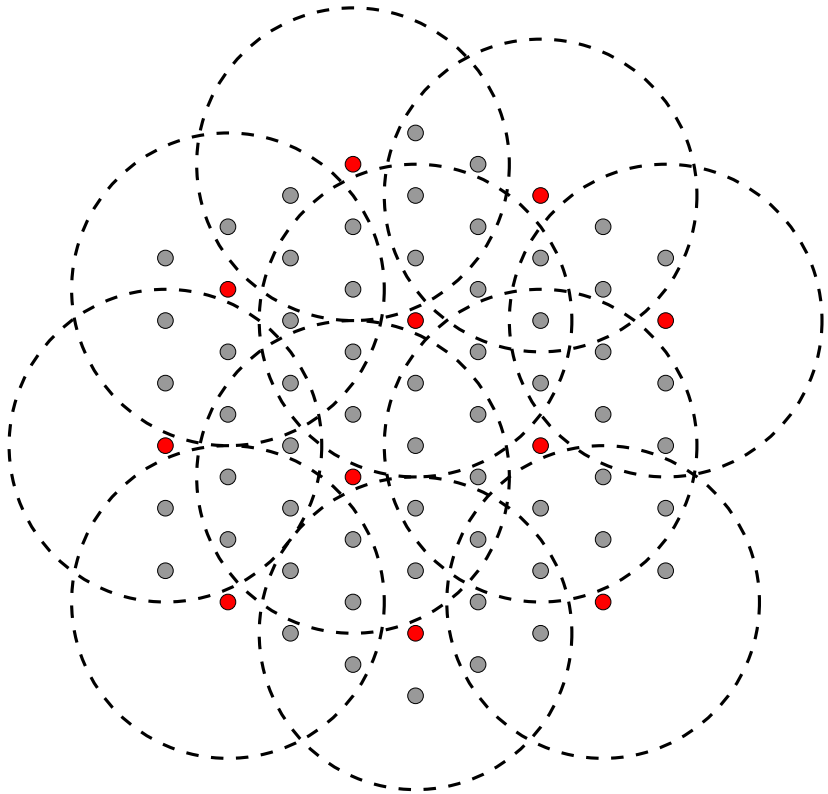
Digressão: limitante inferior de Gilbert-Varshamov

Cobre todo o espaço métrico $\mathcal{M}$ com esferas

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\max}(d-1)}$$



Limitantes

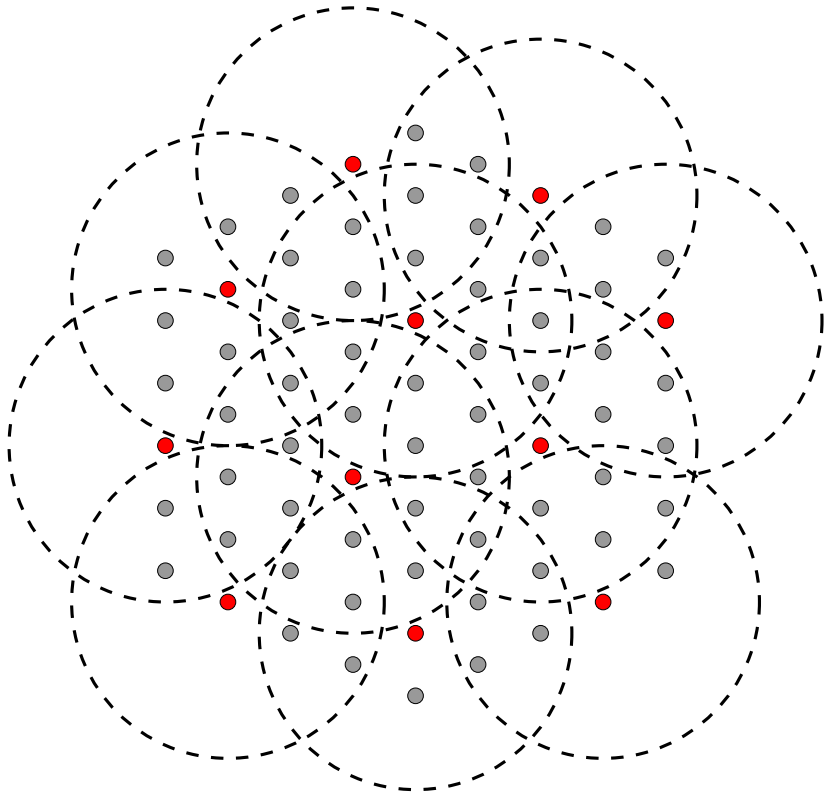
Digressão: limitante inferior generalizado de Gilbert-Varshamov

Resultado mais forte

Teorema

Existe código $\mathcal{C} \subseteq \mathcal{M}$ com distância mínima d tal que

$$|\mathcal{C}| \geq \frac{|\mathcal{M}|}{\mathrm{Vol}_{\mathrm{med}}(d-1)}$$



Limitantes

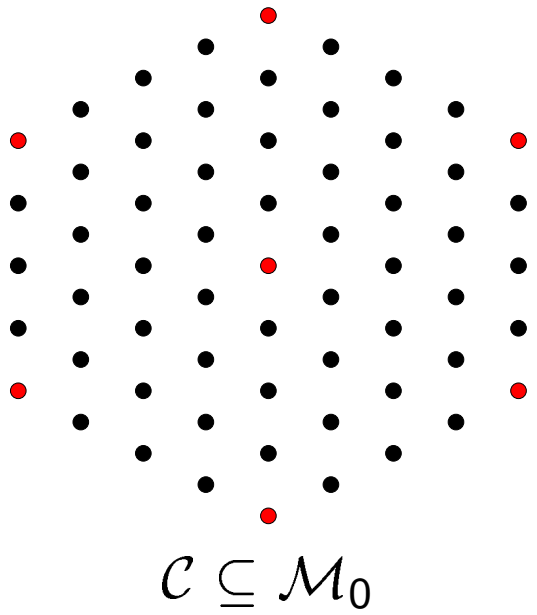
Digressão: limitante superior de Singleton

Puncionamento sucessivo de um código

Fato

Para o código $\mathcal{C} \subseteq \mathcal{M}$ vale

$$|\mathcal{C}| \leq |\mathcal{M}_2|$$



$\mathcal{C} \subseteq \mathcal{M}_0$

Cardinalidade se mantém: $|\mathcal{C}| = |\mathcal{C}^{\blacktriangledown}| = |\mathcal{C}^{\blacktriangledown\blacktriangledown}|$

Limitantes

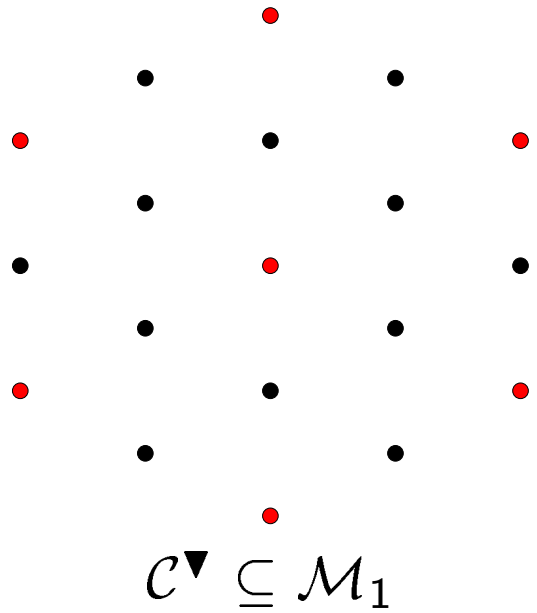
Digressão: limitante superior de Singleton

Puncionamento sucessivo de um código

Fato

Para o código $\mathcal{C} \subseteq \mathcal{M}$ vale

$$|\mathcal{C}| \leq |\mathcal{M}_2|$$



$\mathcal{C}^{\blacktriangledown} \subseteq \mathcal{M}_1$

Cardinalidade se mantém: $|\mathcal{C}| = |\mathcal{C}^{\blacktriangledown}| = |\mathcal{C}^{\blacktriangledown\blacktriangledown}|$

Limitantes

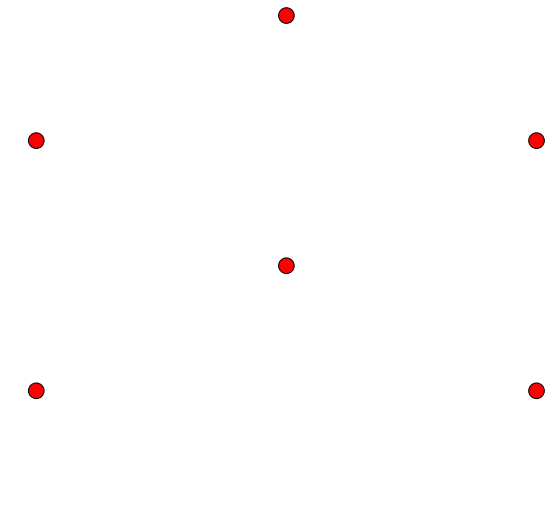
Digressão: limitante superior de Singleton

Puncionamento sucessivo de um código

Fato

Para o código $\mathcal{C} \subseteq \mathcal{M}$ vale

$$|\mathcal{C}| \leq |\mathcal{M}_2|$$

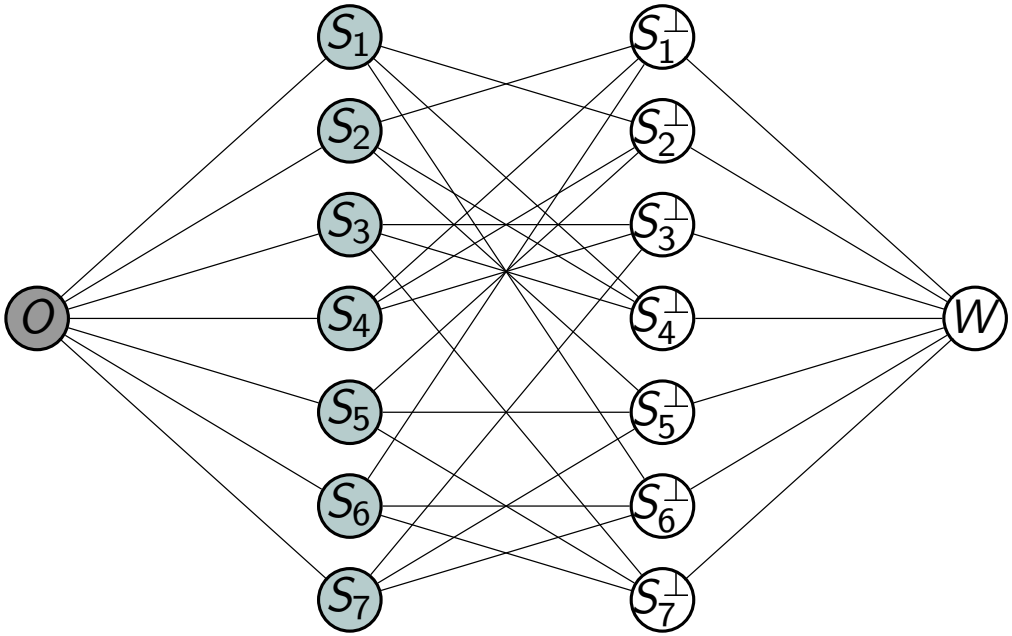


$$\mathcal{C}^{\blacktriangledown\blacktriangledown} \subseteq \mathcal{M}_2$$

Cardinalidade se mantém: $|\mathcal{C}| = |\mathcal{C}^{\blacktriangledown}| = |\mathcal{C}^{\blacktriangledown\blacktriangledown}|$

Limitantes
Volume de esferas

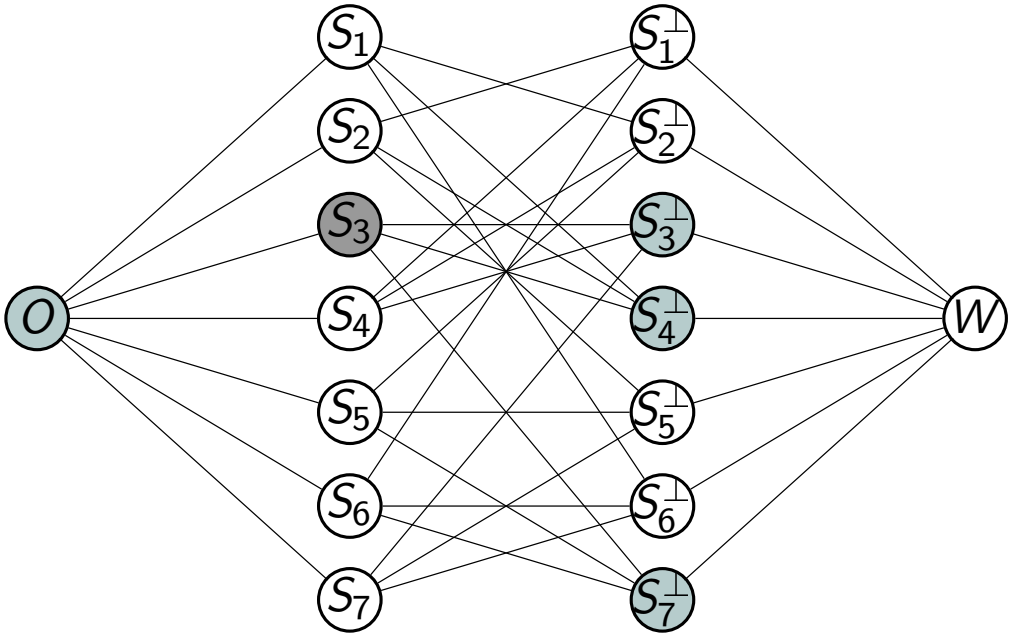
- No espaço projetivo, o volume da esfera depende do centro
- Mas apenas da dimensão do centro



$$\mathrm{Vol}(O, 1) = 8$$

Limitantes
Volume de esferas

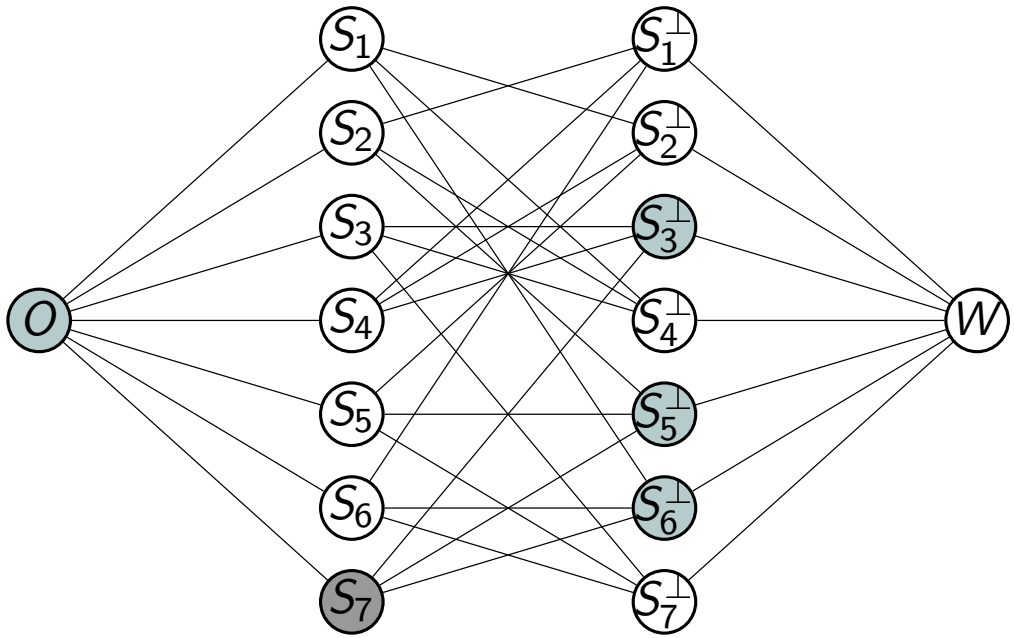
- No espaço projetivo, o volume da esfera depende do centro
- Mas apenas da dimensão do centro



$$\mathrm{Vol}(S_3, 1) = 5$$

Limitantes
Volume de esferas

- No espaço projetivo, o volume da esfera depende do centro
- Mas apenas da dimensão do centro



$$\mathrm{Vol}(S_7, 1) = 5$$

Limitantes
Volume de esferas

Teorema

O volume de uma esfera de centro V_0 e raio r é

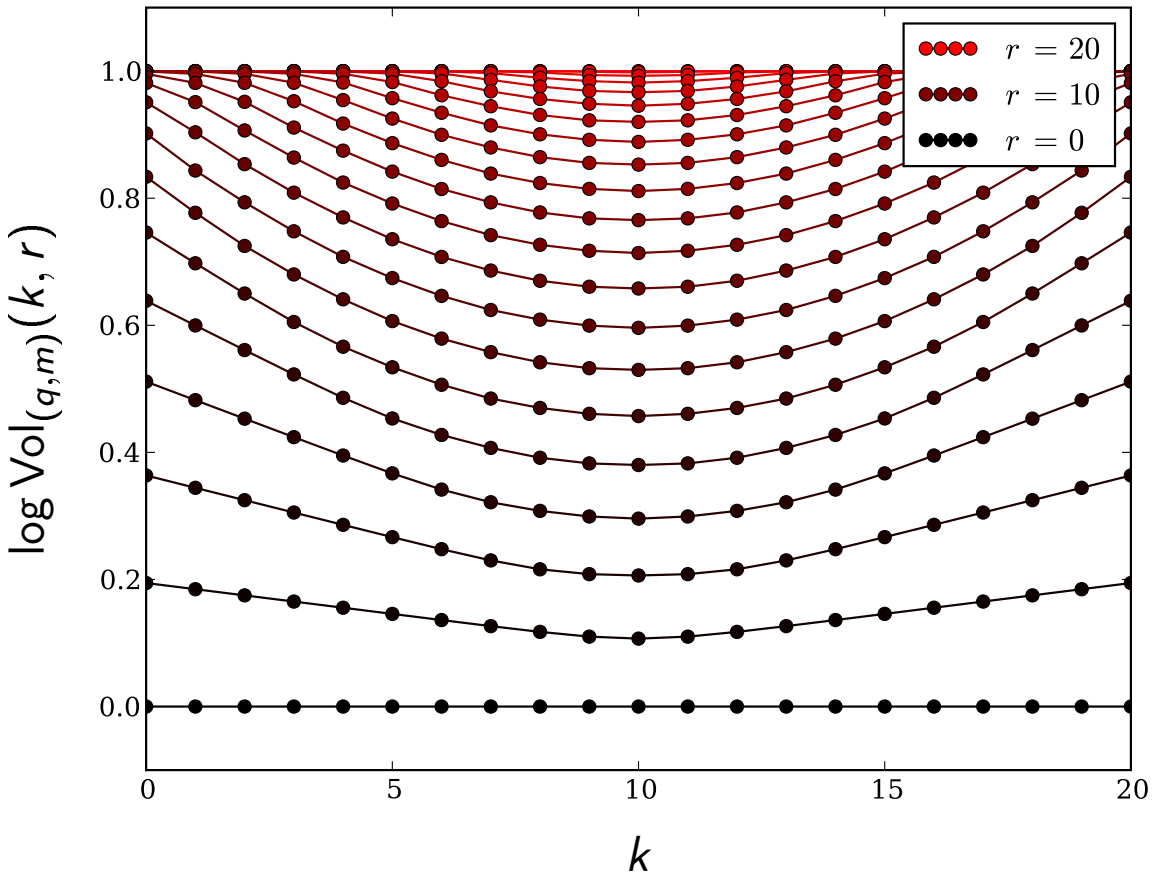
$$\mathrm{Vol}_{(q,m)}(V_0, r) = \sum_{j=0}^{r} \sum_{i=0}^{j} \begin{bmatrix} m-k \\ j-i \end{bmatrix}_q \begin{bmatrix} k \\ i \end{bmatrix}_q q^{i(j-i)},$$

em que $k = \dim V_0$.

Limitantes

Volume de esferas

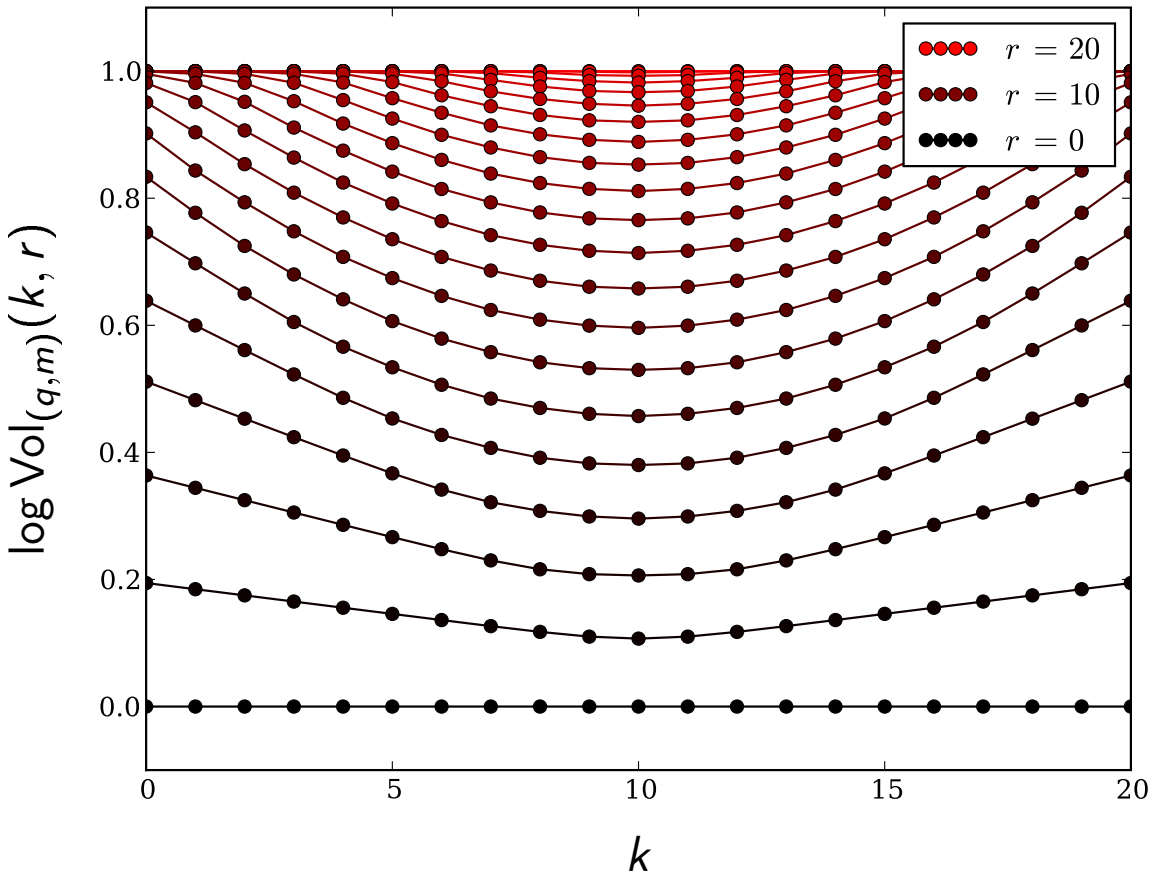
Volume é simétrico ao redor de $k = \lfloor m/2 \rfloor$



Limitantes

Volume de esferas

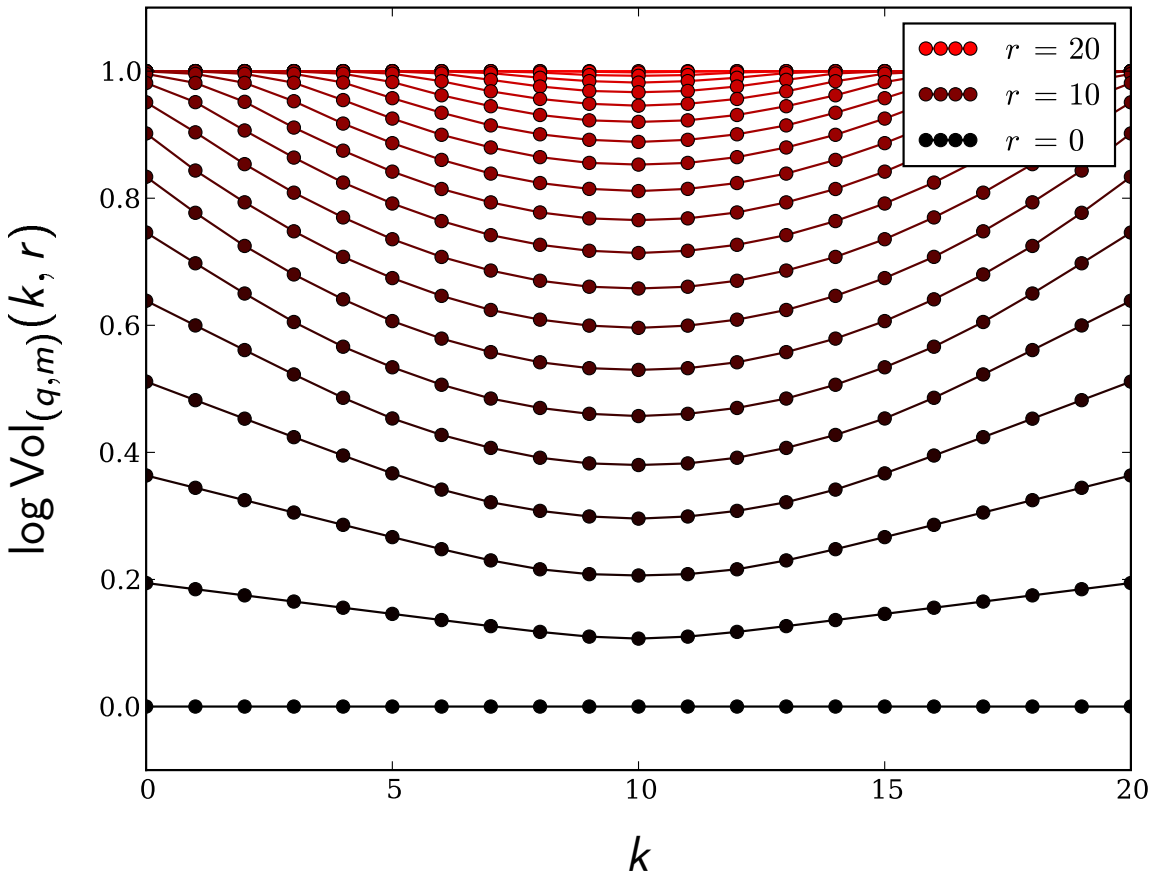
Volume decresce quando k varia de 0 a $\lfloor m/2 \rfloor$



Limitantes

Volume de esferas

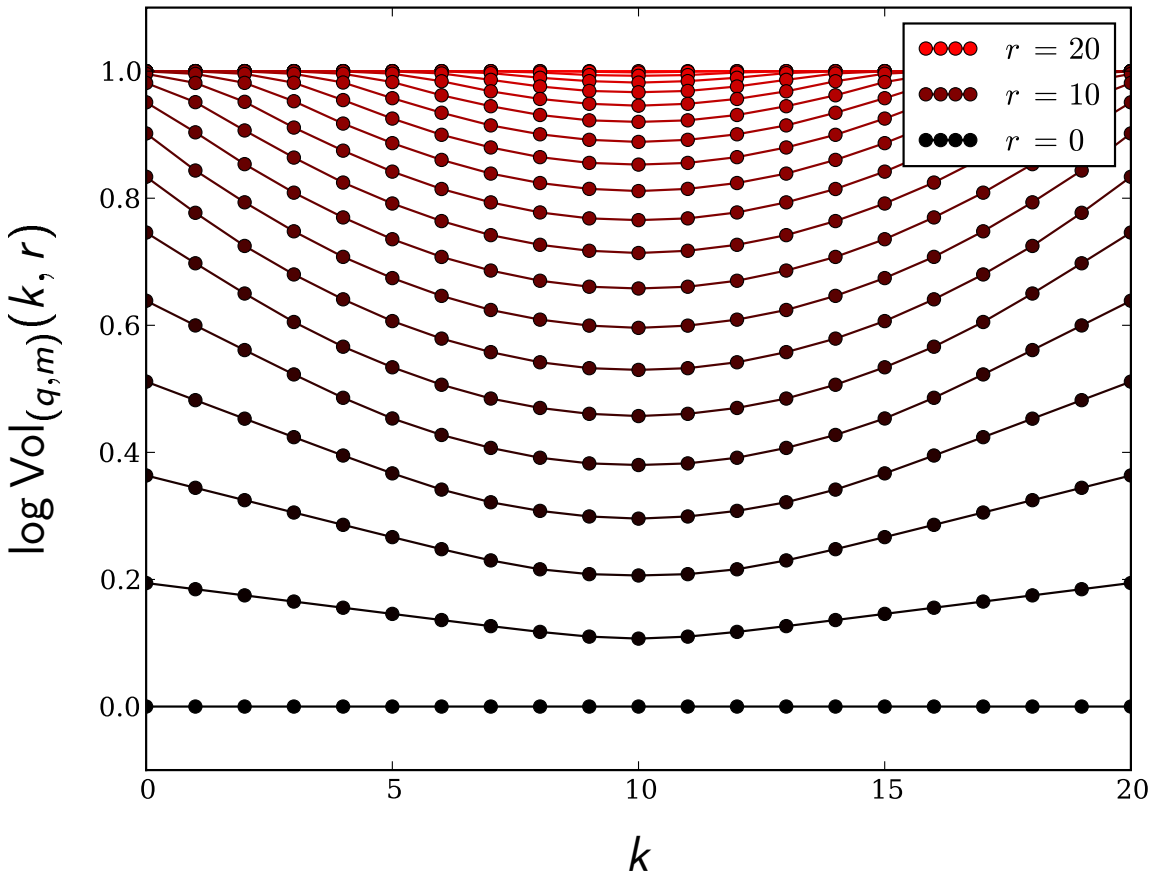
Volume cresce quando k varia de $\lfloor m/2 \rfloor$ a m



Limitantes

Volume de esferas

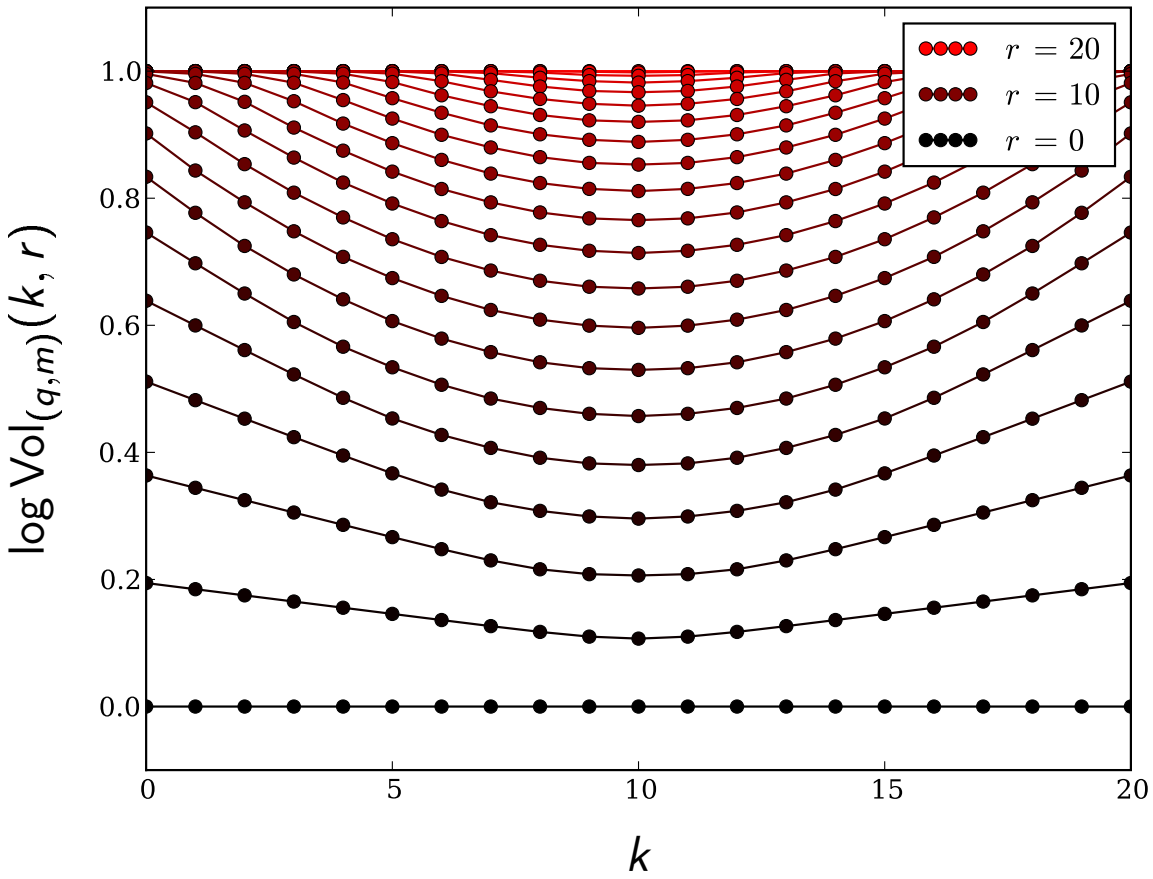
Volume é mínimo quando $k = \lfloor m/2 \rfloor$



Limitantes

Volume de esferas

Volume é máximo quando $k = 0$ ou m



Limitantes

Puncionamento no espaço projetivo

Definição

Puncionamento de um vetor:

$$\mathbf{v} = (v_1, v_2, \ldots, v_{n-1}, v_n) \longmapsto \quad \mathbf{v}^{\blacktriangledown} = (v_1, v_2, \ldots, v_{n-1}, \cancel{v_n})$$

Definição

Puncionamento de um subespaço:

$$V = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots\} \quad \longmapsto \quad V^{\blacktriangledown} = \{\mathbf{v}_1^{\blacktriangledown}, \mathbf{v}_2^{\blacktriangledown}, \mathbf{v}_3^{\blacktriangledown}, \ldots\}$$

Definição

Puncionamento de um código:

$$\mathcal{C} = \{V_1, V_2, V_3, \ldots\} \quad \longmapsto \quad \mathcal{C}^{\blacktriangledown} = \{V_1^{\blacktriangledown}, V_2^{\blacktriangledown}, V_3^{\blacktriangledown}, \ldots\}$$

Limitantes

Puncionamento no espaço projetivo

Definição

Puncionamento de um vetor:

$$\mathbf{v} = (v_1, v_2, \ldots, v_{n-1}, v_n) \longmapsto \quad \mathbf{v}^{\blacktriangledown} = (v_1, v_2, \ldots, v_{n-1}, \cancel{v_n})$$

Definição

Puncionamento de um subespaço:

$$V = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots\} \quad \longmapsto \quad V^{\blacktriangledown} = \{\mathbf{v}_1^{\blacktriangledown}, \mathbf{v}_2^{\blacktriangledown}, \mathbf{v}_3^{\blacktriangledown}, \ldots\}$$

Definição

Puncionamento de um código:

$$\mathcal{C} = \{V_1, V_2, V_3, \ldots\} \quad \longmapsto \quad \mathcal{C}^{\blacktriangledown} = \{V_1^{\blacktriangledown}, V_2^{\blacktriangledown}, V_3^{\blacktriangledown}, \ldots\}$$

Limitantes

Puncionamento no espaço projetivo

Definição

Puncionamento de um vetor:

$$\mathbf{v} = (v_1, v_2, \ldots, v_{n-1}, v_n) \longmapsto \quad \mathbf{v}^{\blacktriangledown} = (v_1, v_2, \ldots, v_{n-1}, \cancel{v_n})$$

Definição

Puncionamento de um subespaço:

$$V = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots\} \quad \longmapsto \quad V^{\blacktriangledown} = \{\mathbf{v}_1^{\blacktriangledown}, \mathbf{v}_2^{\blacktriangledown}, \mathbf{v}_3^{\blacktriangledown}, \ldots\}$$

Definição

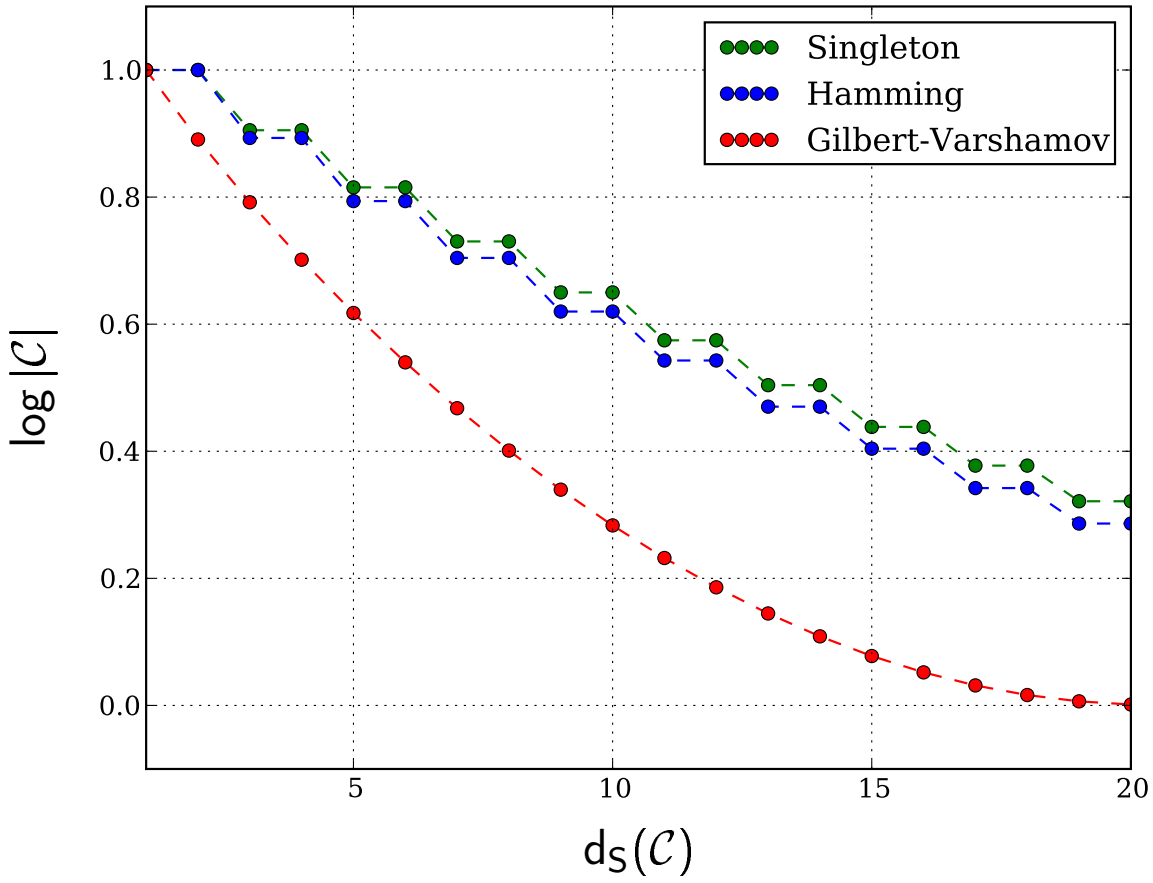
Puncionamento de um código:

$$\mathcal{C} = \{V_1, V_2, V_3, \ldots\} \quad \longmapsto \quad \mathcal{C}^{\blacktriangledown} = \{V_1^{\blacktriangledown}, V_2^{\blacktriangledown}, V_3^{\blacktriangledown}, \ldots\}$$

Limitantes

Gráficos

Limitantes para $q = 2$ e $m = 20$



Aplicação em codificação de rede

Definições e taxa

Um código de subespaço dá origem a um código matricial:

$$\mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^m) \qquad \Longrightarrow \qquad \mathcal{X} \subseteq \mathbb{F}_q^{h \times m}$$

em que

$$h = \ell(\mathcal{C})$$

é dimensão máxima dos subespaços de $\mathcal{C}$

Fato

A taxa de $\mathcal{X}$ é

$$R(\mathcal{X}) = \frac{\log_q |\mathcal{C}|}{m \cdot \ell(\mathcal{C})}$$

Aplicação em codificação de rede

Definições e taxa

Um código de subespaço dá origem a um código matricial:

$$\mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^m) \qquad \Longrightarrow \qquad \mathcal{X} \subseteq \mathbb{F}_q^{h \times m}$$

em que

$$h = \ell(\mathcal{C})$$

é dimensão máxima dos subespaços de $\mathcal{C}$

Fato

A taxa de $\mathcal{X}$ é

$$R(\mathcal{X}) = \frac{\log_q |\mathcal{C}|}{m \cdot \ell(\mathcal{C})}$$

Aplicação em codificação de rede

Capacidade de correção de erros

Seja $\mathcal{C}$ um código de subespaço com $\mathrm{d_S}(\mathcal{C}) = d$

Fato

$\mathcal{C}$ é bem-sucedido no canal de subespaço que comete até t erros *iff*

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq t$$

Seja $\mathcal{X}$ um código matricial originário de $\mathcal{C}$

Teorema

$\mathcal{X}$ é bem-sucedido no canal matricial definido por (ρ, τ) se

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq \rho + 2\tau$$

Aplicação em codificação de rede

Capacidade de correção de erros

Seja $\mathcal{C}$ um código de subespaço com $\mathrm{d_S}(\mathcal{C}) = d$

Fato

$\mathcal{C}$ é bem-sucedido no canal de subespaço que comete até t erros *iff*

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq t$$

Seja $\mathcal{X}$ um código matricial originário de $\mathcal{C}$

Teorema

$\mathcal{X}$ é bem-sucedido no canal matricial definido por (ρ, τ) se

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq \rho + 2\tau$$

Aplicação em codificação de rede

Capacidade de correção de erros

Seja $\mathcal{C}$ um código de subespaço com $\mathrm{d_S}(\mathcal{C}) = d$

Fato

$\mathcal{C}$ é bem-sucedido no canal de subespaço que comete até t erros *iff*

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq t$$

Seja $\mathcal{X}$ um código matricial originário de $\mathcal{C}$

Teorema

$\mathcal{X}$ é bem-sucedido no canal matricial definido por (ρ, τ) se

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq \rho + 2\tau$$

Aplicação em codificação de rede

Capacidade de correção de erros

Seja $\mathcal{C}$ um código de subespaço com $\mathrm{d_S}(\mathcal{C}) = d$

Fato

$\mathcal{C}$ é bem-sucedido no canal de subespaço que comete até t erros *iff*

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq t$$

Seja $\mathcal{X}$ um código matricial originário de $\mathcal{C}$

Teorema

$\mathcal{X}$ é bem-sucedido no canal matricial definido por (ρ, τ) se

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq \rho + 2\tau$$

Codificação de Subespaço Multishot

Ideia e proposta

Ideia

Utilizar o canal de subespaço repetidas vezes

Proposta

Códigos de bloco—transmitir sequências de n subespaços:

$$\mathbf{V} = (V_1, \ldots, V_n)$$

Ideia e proposta

Ideia

Utilizar o canal de subespaço repetidas vezes

Proposta

Códigos de bloco—transmitir sequências de n subespaços:

$$\mathbf{V} = (V_1, \ldots, V_n)$$

Justificativa

Por que usar códigos *multishot*?

- Se os parâmetros do sistema são imutáveis
  - Para aumentar a taxa ou a capacidade de correção é necessário aumentar q ou m
- Se a topologia da rede varia rapidamente
  - Tempo de coerência da rede é reduzido
  - Matriz $\mathbf{G}$ não permanece constante por muito tempo
- Complexidade computacional

Justificativa

Por que usar códigos *multishot*?

- Se os parâmetros do sistema são imutáveis
  - Para aumentar a taxa ou a capacidade de correção é necessário aumentar q ou m
- Se a topologia da rede varia rapidamente
  - Tempo de coerência da rede é reduzido
  - Matriz $\mathbf{G}$ não permanece constante por muito tempo
- Complexidade computacional

Justificativa

Por que usar códigos *multishot*?

- Se os parâmetros do sistema são imutáveis
  - Para aumentar a taxa ou a capacidade de correção é necessário aumentar q ou m
- Se a topologia da rede varia rapidamente
  - Tempo de coerência da rede é reduzido
  - Matriz $\mathbf{G}$ não permanece constante por muito tempo
- Complexidade computacional

Construção de um espaço métrico

Definições

Definição

Extensão do espaço projetivo:

$$\mathcal{P}(\mathbb{F}_q^m)^n = \mathcal{P}(\mathbb{F}_q^m) \times \cdots \times \mathcal{P}(\mathbb{F}_q^m)$$

Definição

Distância de subespaço estendida:

$$\mathrm{d_S}(\mathbf{V}, \mathbf{U}) = \mathrm{d_S}(V_1, U_1) + \cdots + \mathrm{d_S}(V_n, U_n)$$

Construção de um espaço métrico

Definições

Definição

Extensão do espaço projetivo:

$$\mathcal{P}(\mathbb{F}_q^m)^n = \mathcal{P}(\mathbb{F}_q^m) \times \cdots \times \mathcal{P}(\mathbb{F}_q^m)$$

Definição

Distância de subespaço estendida:

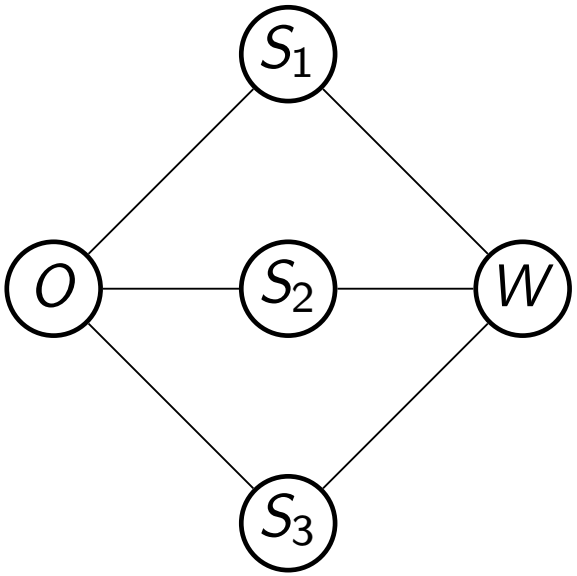
$$\mathrm{d_S}(\mathbf{V}, \mathbf{U}) = \mathrm{d_S}(V_1, U_1) + \cdots + \mathrm{d_S}(V_n, U_n)$$

Exemplo motivacional

Objetivo

Objetivo

Códigos *multishot* sobre $\mathcal{P}(\mathbb{F}_2^2)$ utilizando o canal 2 vezes e capazes de detectar 1 erro ($d = 2$)



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

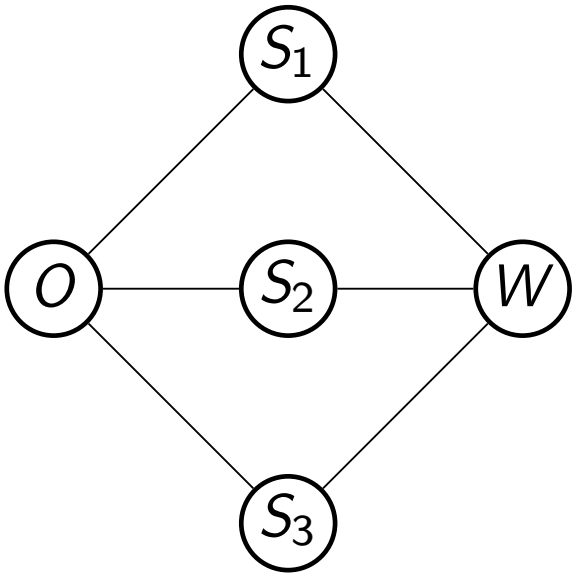
A seguir: três propostas

Exemplo motivacional

Objetivo

Objetivo

Códigos *multishot* sobre $\mathcal{P}(\mathbb{F}_2^2)$ utilizando o canal 2 vezes e capazes de detectar 1 erro ($d = 2$)



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

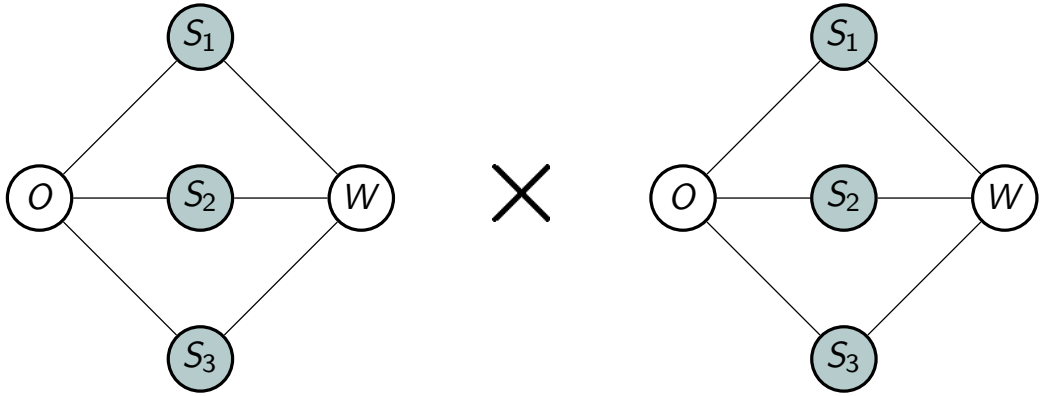
A seguir: três propostas

Exemplo motivacional

Proposta 1

Proposta 1

Estender o melhor código 1-*shot*



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

Cardinalidade

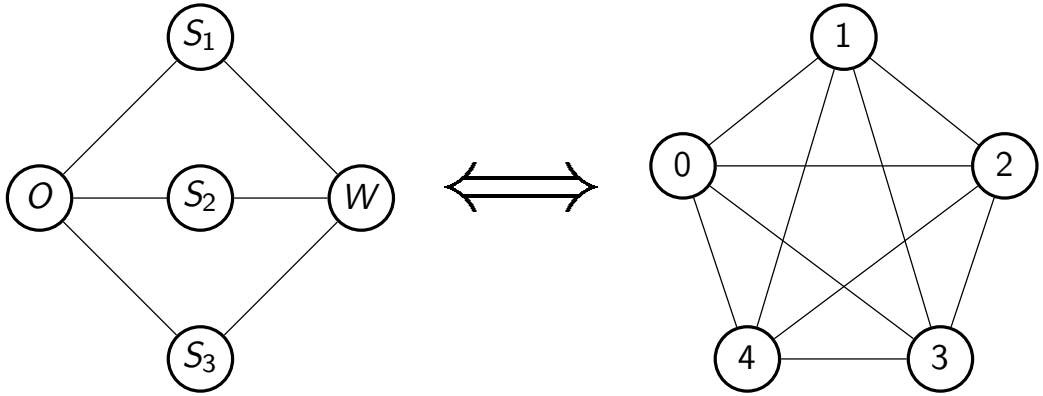
$$|\mathcal{C}_1| = 9$$

Exemplo motivacional

Proposta 2

Proposta 2

Codificação clássica sobre o espaço projetivo



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

Cardinalidade

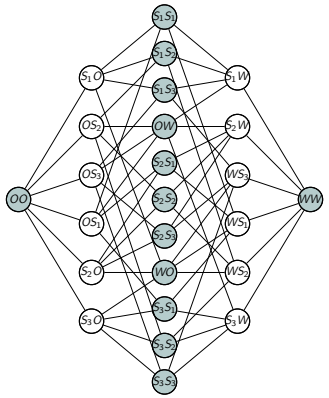
$$|\mathcal{C}_2| = 5$$

Exemplo motivacional

Proposta 3

Proposta 3

Considerar o espaço métrico $\mathcal{P}(\mathbb{F}_2^2)^2$



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

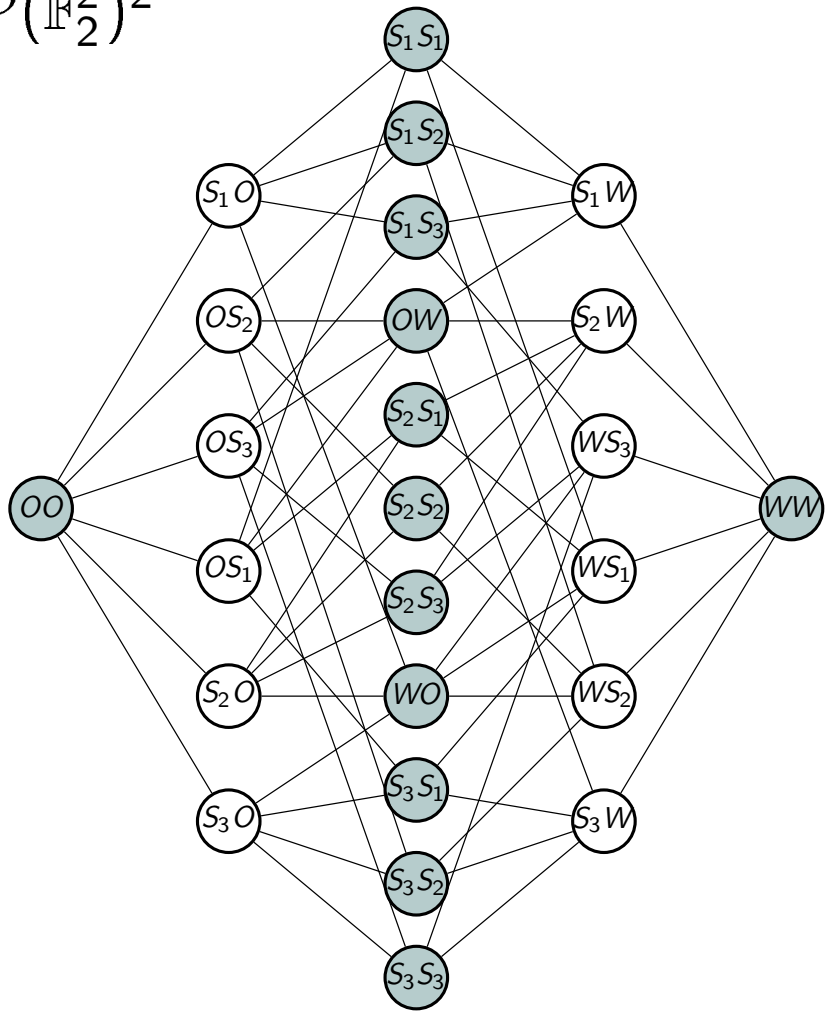
Cardinalidade

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

Exemplo motivacional

Proposta 3

Espaço métrico $\mathcal{P}(\mathbb{F}_2^2)^2$



Relação com códigos de subespaço *one-shot*

Resultados

Fato

Códigos 1-*shot* são um caso especial de códigos *n*-*shot*: $n = 1$

Recíproca também é verdadeira

Fato

Códigos *multishot* são um caso especial de códigos 1-*shot*:

$$\mathcal{P}(\mathbb{F}_q^m)^n \subseteq \mathcal{P}(\mathbb{F}_q^{mn})$$

Fato

Existe uma injeção de $\mathcal{P}(\mathbb{F}_q^m)^n$ para $\mathcal{P}(\mathbb{F}_q^{mn})$ que preserva distâncias

Relação com códigos de subespaço *one-shot*

Resultados

Fato

Códigos 1-*shot* são um caso especial de códigos *n*-*shot*: $n = 1$

Recíproca também é verdadeira

Fato

Códigos *multishot* são um caso especial de códigos 1-*shot*:

$$\mathcal{P}(\mathbb{F}_q^m)^n \subseteq \mathcal{P}(\mathbb{F}_q^{mn})$$

Fato

Existe uma injeção de $\mathcal{P}(\mathbb{F}_q^m)^n$ para $\mathcal{P}(\mathbb{F}_q^{mn})$ que preserva distâncias

Relação com códigos de subespaço *one-shot*

Resultados

Fato

Códigos 1-*shot* são um caso especial de códigos *n*-*shot*: $n = 1$

Recíproca também é verdadeira

Fato

Códigos *multishot* são um caso especial de códigos 1-*shot*:

$$\mathcal{P}(\mathbb{F}_q^m)^n \subseteq \mathcal{P}(\mathbb{F}_q^{mn})$$

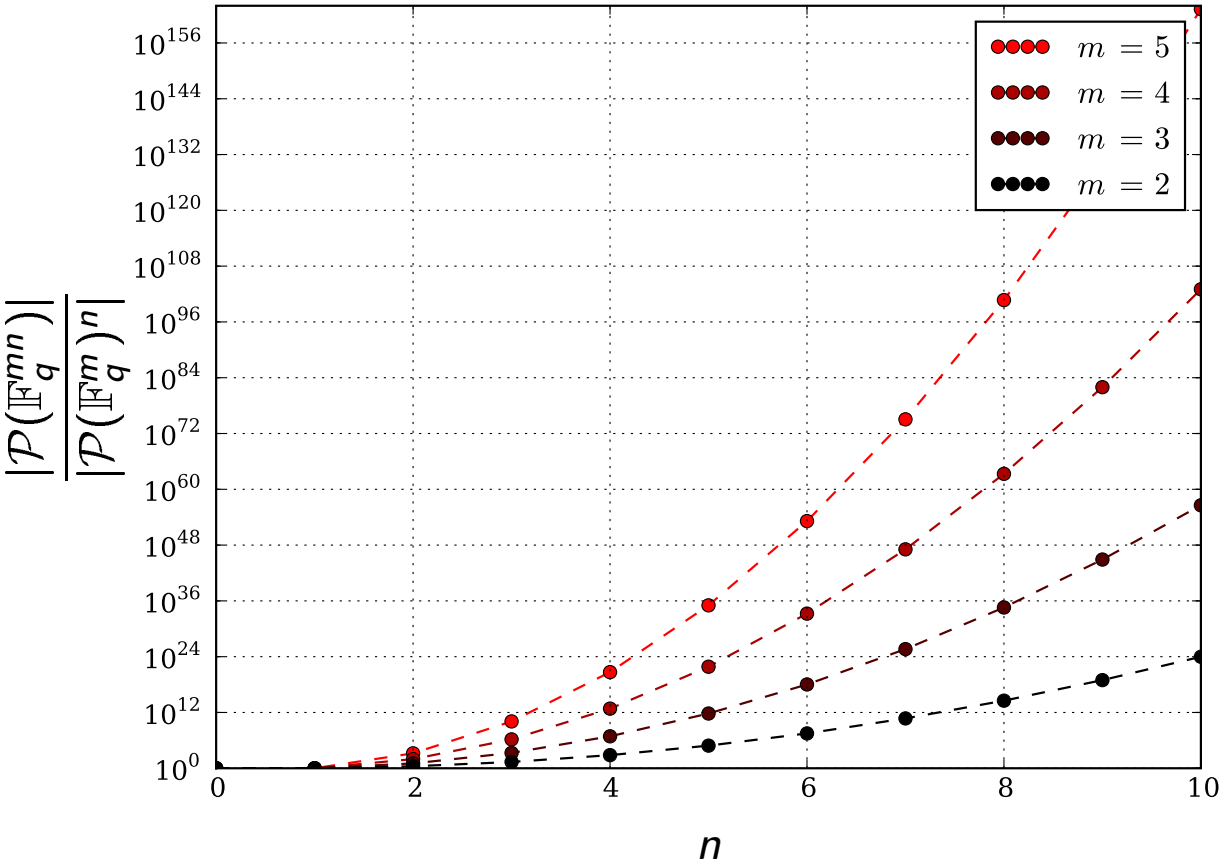
Fato

Existe uma injeção de $\mathcal{P}(\mathbb{F}_q^m)^n$ para $\mathcal{P}(\mathbb{F}_q^{mn})$ que preserva distâncias

Relação com códigos de subespaço *one-shot*

Comparação entre os tamanhos

Para $q = 2$



Limitantes

- Mesmos limitantes do caso *one-shot*:
  - Hamming
  - Gilbert-Varshamov
  - Singleton

Limitantes

Esferas no espaço projetivo estendido

Teorema

O volume de uma esfera de centro $\mathbf{V}$ e raio r é

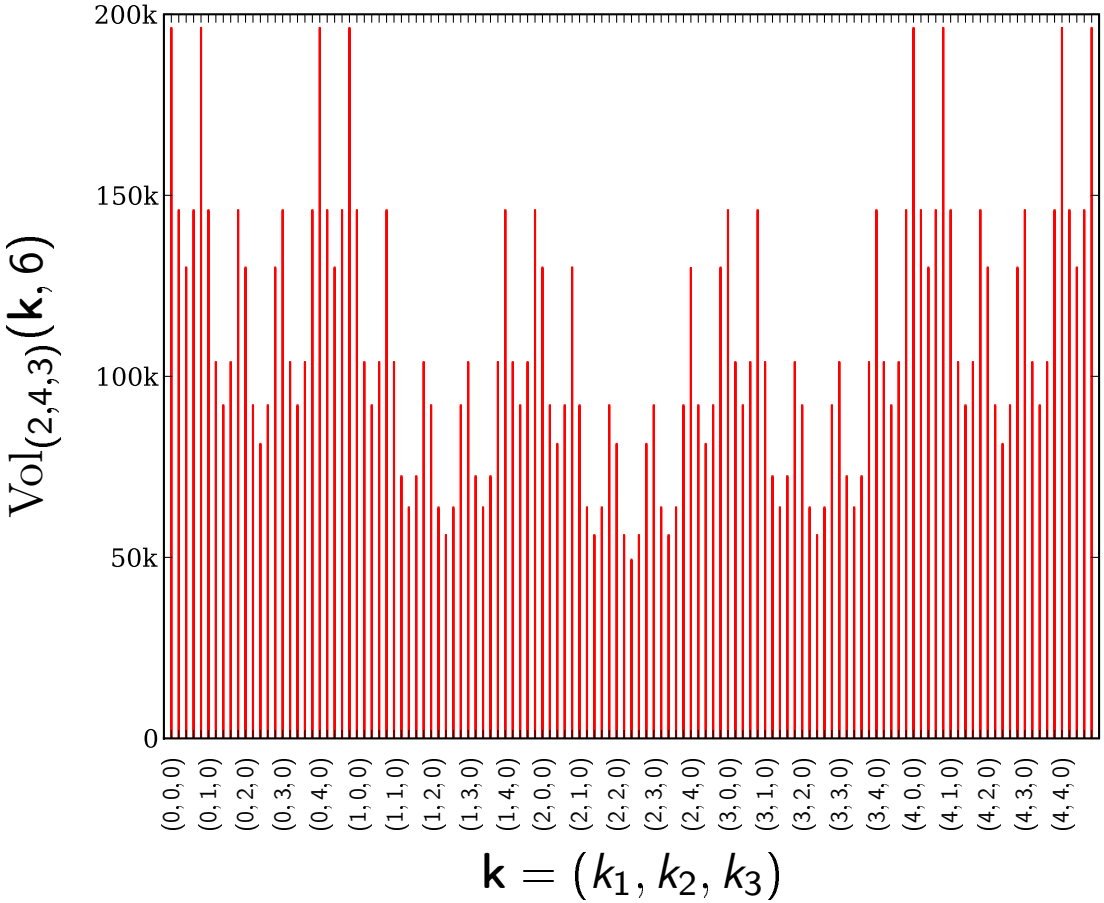
$$\mathrm{Vol}_{(q,m,n)}(\mathbf{V}, r) = \sum_{j=0}^{r} \sum_{\substack{\mathbf{j}\in\{0,\ldots,m\}^n: \\ j_1+\cdots+j_n=j}} \prod_{i=1}^{n} \mathrm{Vol}_{(q,m)}^{\mathrm{Casca}}(k_i, j_i)$$

em que $\mathbf{k} = (k_1, \ldots, k_n) = (\dim V_1, \ldots, \dim V_n)$.

Limitantes

Esferas no espaço projetivo estendido

Volume de esferas para $q = 2$, $m = 4$, $n = 3$ e $r = 6$



Limitantes

Puncionamento no espaço projetivo estendido

Dois puncionamentos naturais

Puncionamento 1

Puncionamento de uma palavra-código:

$$\mathbf{V} = (V_1, V_2, \ldots, V_{n-1}, V_n) \longmapsto \quad \mathbf{V}^{\blacktriangledown_1} = (V_1^{\blacktriangledown}, V_2^{\blacktriangledown}, \ldots, V_{n-1}^{\blacktriangledown}, V_n^{\blacktriangledown})$$

Puncionamento 2

Puncionamento de uma palavra-código:

$$\mathbf{V} = (V_1, V_2, \ldots, V_{n-1}, V_n) \longmapsto \quad \mathbf{V}^{\blacktriangledown_2} = (V_1, V_2, \ldots, V_{n-1}, \cancel{V_n})$$

Limitantes

Puncionamento no espaço projetivo estendido

Dois puncionamentos naturais

Puncionamento 1

Puncionamento de uma palavra-código:

$$\mathbf{V} = (V_1, V_2, \ldots, V_{n-1}, V_n) \longmapsto \quad \mathbf{V}^{\blacktriangledown_1} = (V_1^{\blacktriangledown}, V_2^{\blacktriangledown}, \ldots, V_{n-1}^{\blacktriangledown}, V_n^{\blacktriangledown})$$

Puncionamento 2

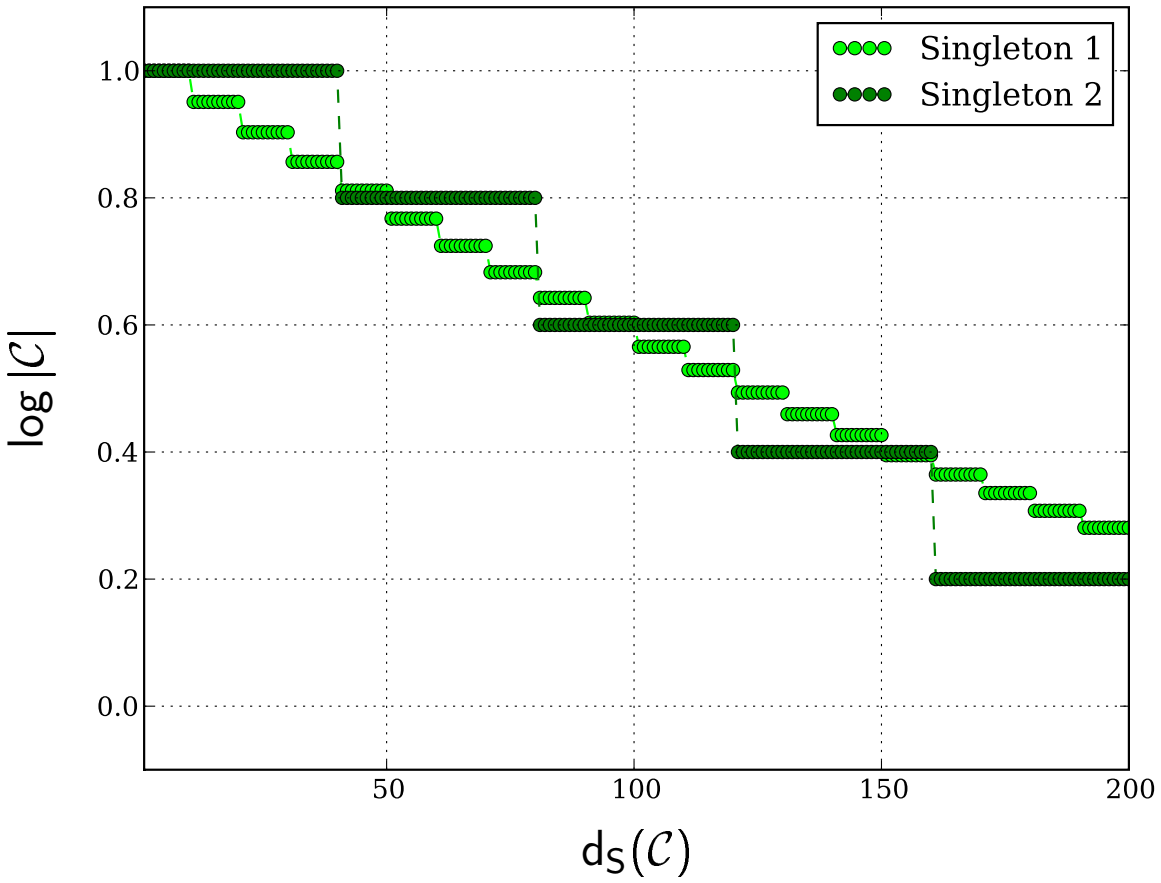
Puncionamento de uma palavra-código:

$$\mathbf{V} = (V_1, V_2, \ldots, V_{n-1}, V_n) \longmapsto \quad \mathbf{V}^{\blacktriangledown_2} = (V_1, V_2, \ldots, V_{n-1}, \cancel{V_n})$$

Limitantes

Puncionamento no espaço projetivo estendido

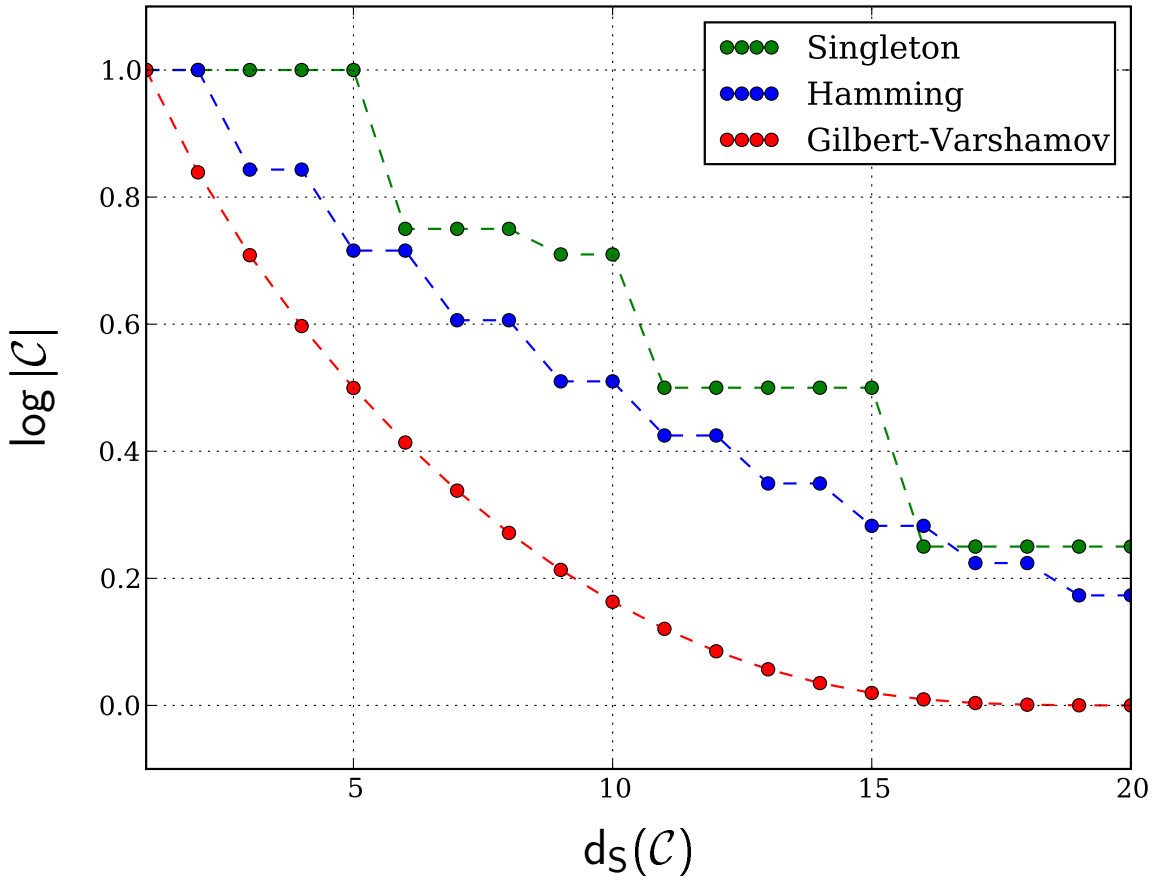
Limitantes de Singleton para $q = 2$, $m = 40$, $n = 5$



Limitantes

Gráficos

Limitantes para $q = 2$ e $m = 5$, $n = 4$



Construção multinível

Descrição do método

- Baseada em modulação codificada de bloco

Entrada

- Particionamento L-nível
- Códigos componentes para garantir distância mínima desejada

- Dois exemplos

Construção multinível

Descrição do método

- Baseada em modulação codificada de bloco

Entrada

- Particionamento L-nível
- Códigos componentes para garantir distância mínima desejada

- Dois exemplos

Construção multinível

Descrição do método

- Baseada em modulação codificada de bloco

Entrada

- Particionamento L-nível
- Códigos componentes para garantir distância mínima desejada

- Dois exemplos

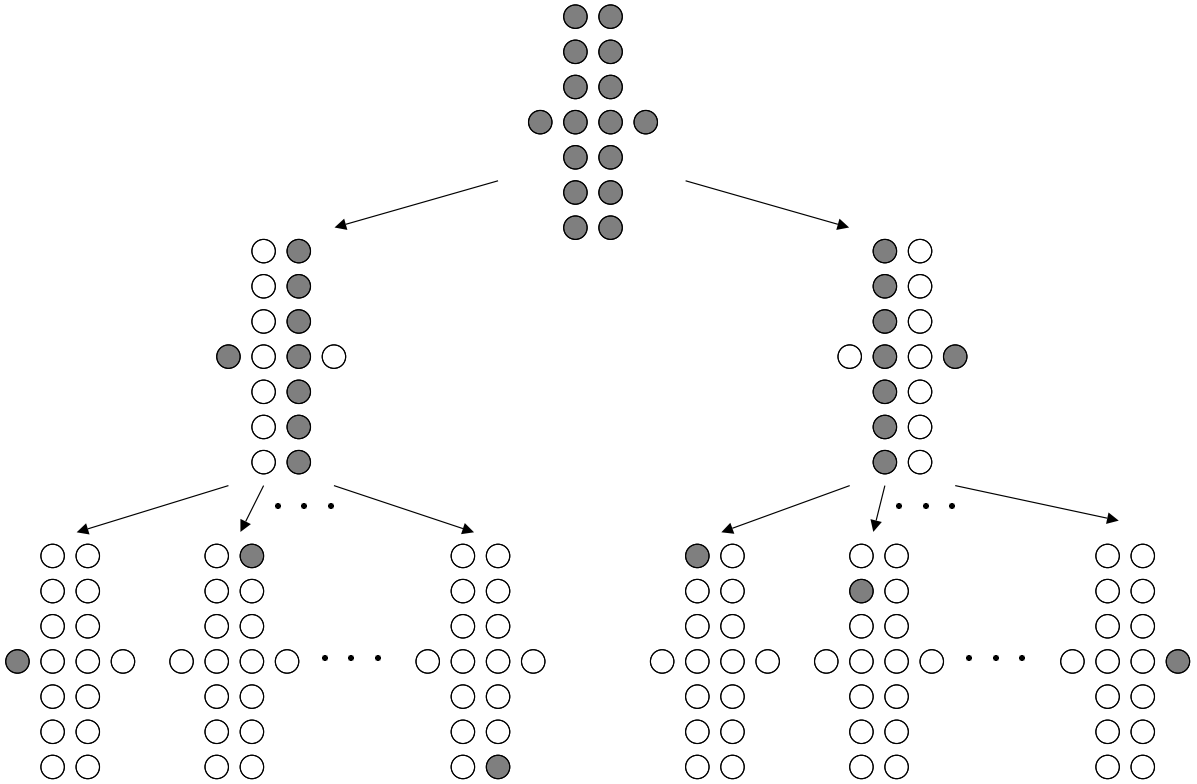
Construção multinível

Exemplo 1

Objetivo

Código 3-*shot* $\mathcal{C}_1$ sobre $\mathcal{P}(\mathbb{F}_2^3)$ com $\mathrm{d_S}(\mathcal{C}_1) = 3$

Particionamento binível



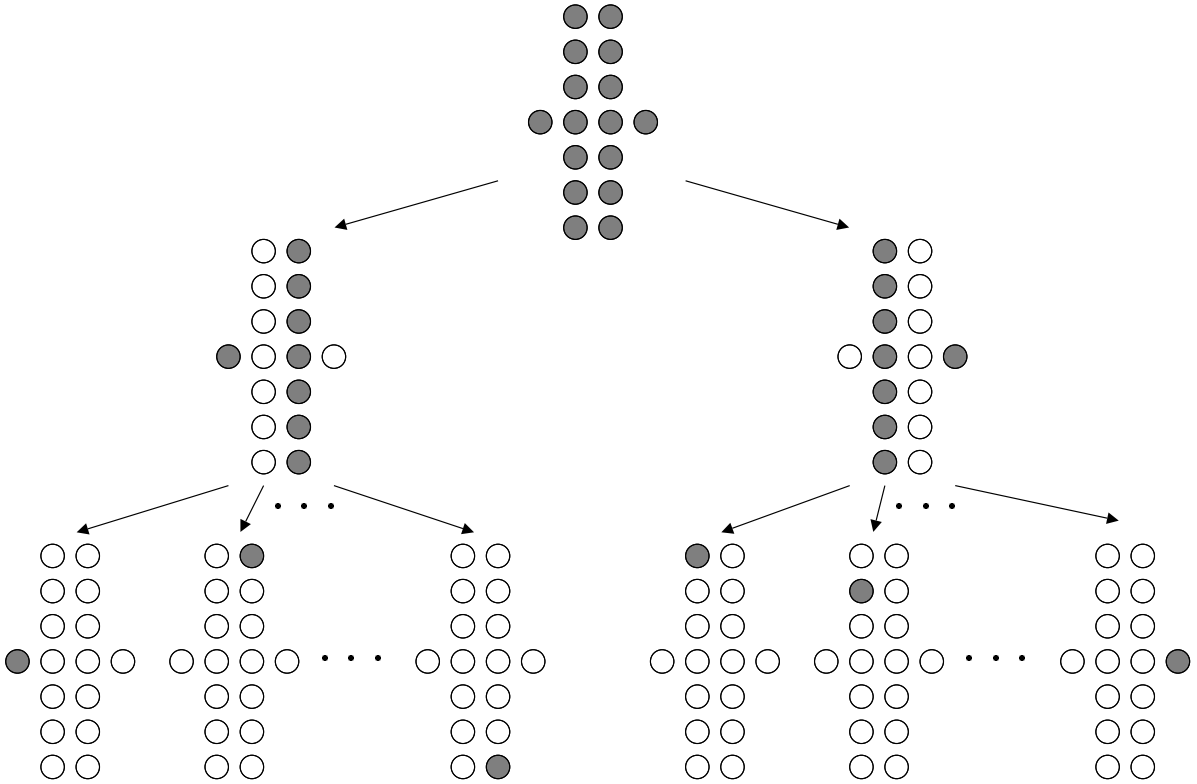
Construção multinível

Exemplo 1

Objetivo

Código 3-*shot* $\mathcal{C}_1$ sobre $\mathcal{P}(\mathbb{F}_2^3)$ com $\mathrm{d_S}(\mathcal{C}_1) = 3$

Distâncias *intrasubset*



$\mathrm{d_S}^{(0)} = 1$

$\mathrm{d_S}^{(1)} = 2$

$\mathrm{d_S}^{(2)} = \infty$

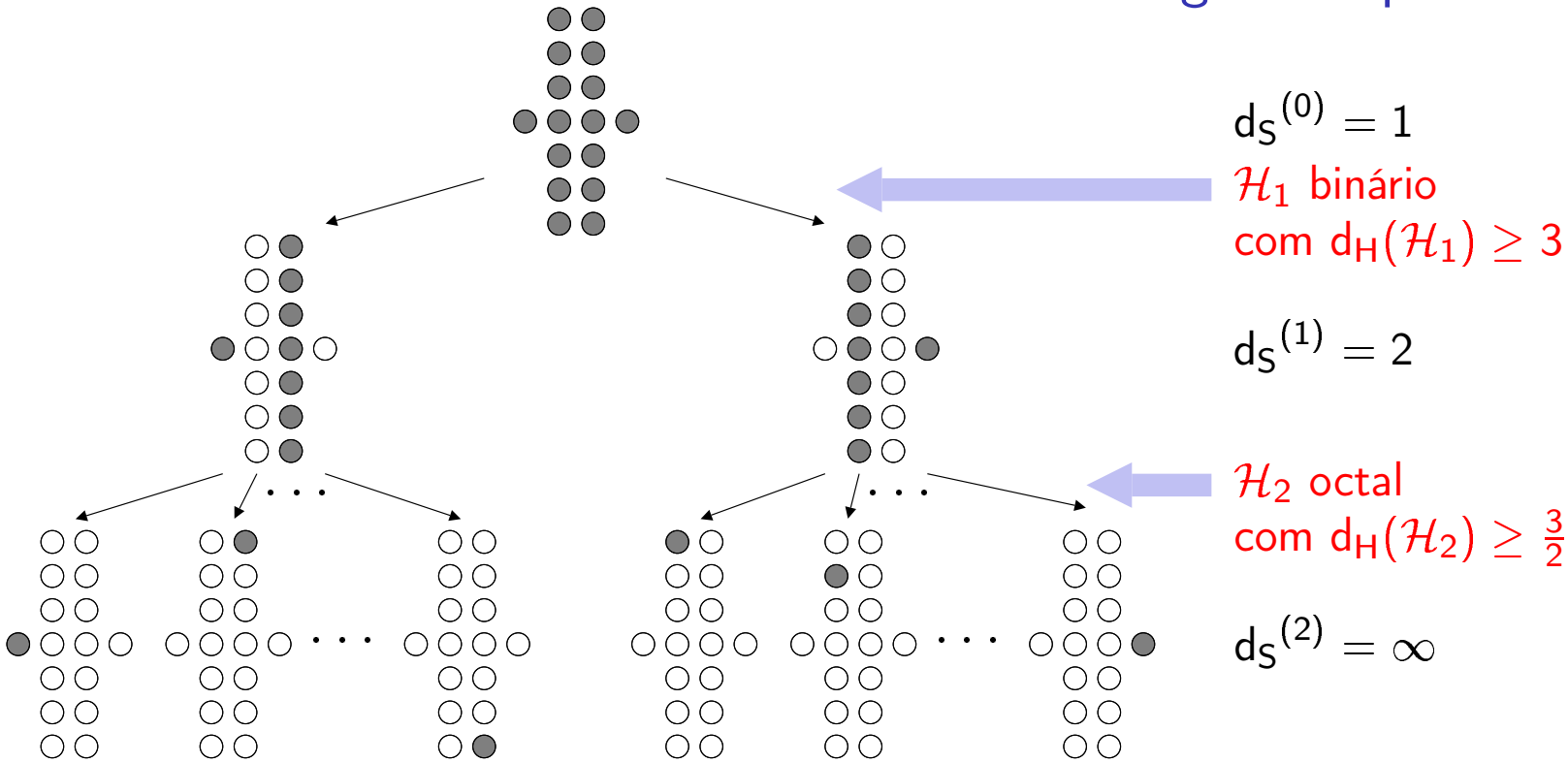
Construção multinível

Exemplo 1

Objetivo

Código 3-*shot* $\mathcal{C}_1$ sobre $\mathcal{P}(\mathbb{F}_2^3)$ com $\mathrm{d_S}(\mathcal{C}_1) = 3$

Códigos componentes



Construção multinível

Exemplo 1

Código componente

Código de repetição:

$$\mathcal{H}_1 = \{000, 111\}$$

$$\mathsf{d_H}(\mathcal{H}_1) = 3, \quad |\mathcal{H}_1| = 2$$

Código componente

Código de paridade:

$$\mathcal{H}_2 = \{000, 017, 026, \ldots, 772\}$$

$$\mathsf{d_H}(\mathcal{H}_2) = 2, \quad |\mathcal{H}_2| = 64$$

Combinações

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \cdots, \begin{bmatrix} 0 & 0 & 0 \\ 7 & 7 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 7 \end{bmatrix}, \cdots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$

Construção multinível

Exemplo 1

Código componente

Código de repetição:

$$\mathcal{H}_1 = \{000, 111\}$$

$$\mathrm{d_H}(\mathcal{H}_1) = 3, \quad |\mathcal{H}_1| = 2$$

Código componente

Código de paridade:

$$\mathcal{H}_2 = \{000, 017, 026, \ldots, 772\}$$

$$\mathrm{d_H}(\mathcal{H}_2) = 2, \quad |\mathcal{H}_2| = 64$$

Combinações

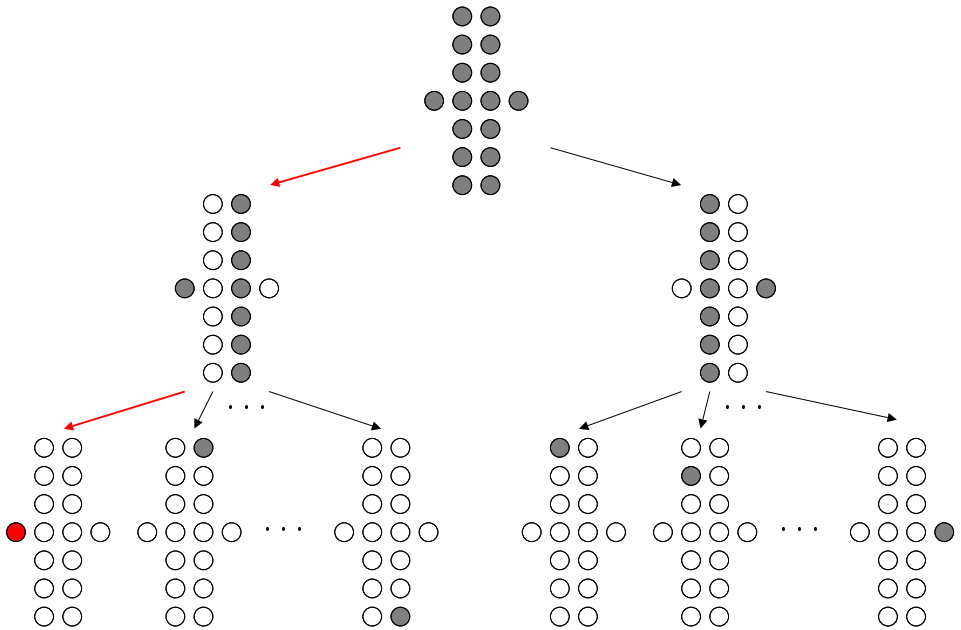
$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 0 & 0 & 0 \\ 7 & 7 & 2 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$

Construção multinível

Exemplo 1

Combinações

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$



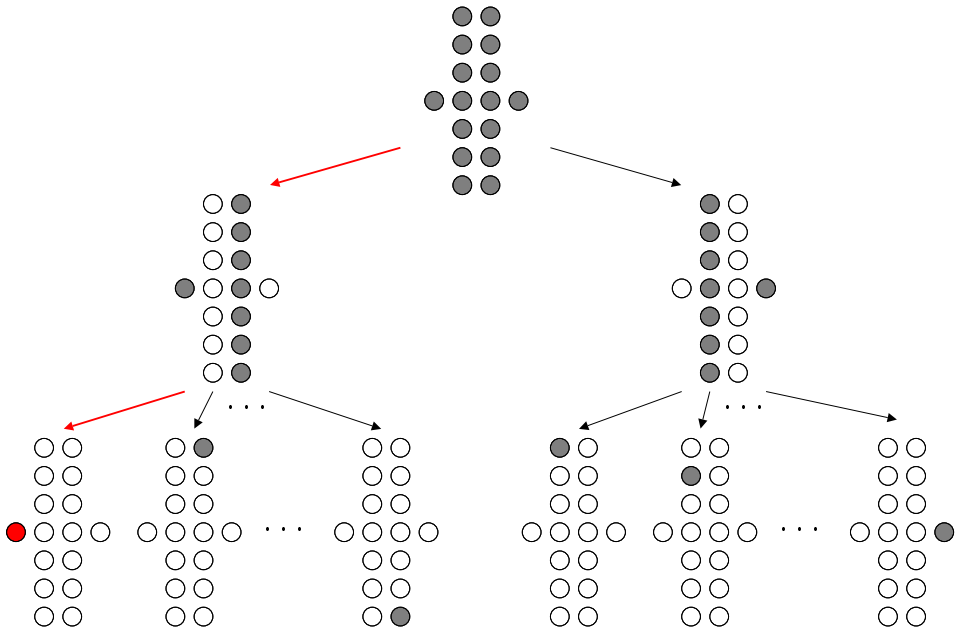
$$\mathcal{C}_1 = \{O, \ldots\}$$

Construção multinível

Exemplo 1

Combinações

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$



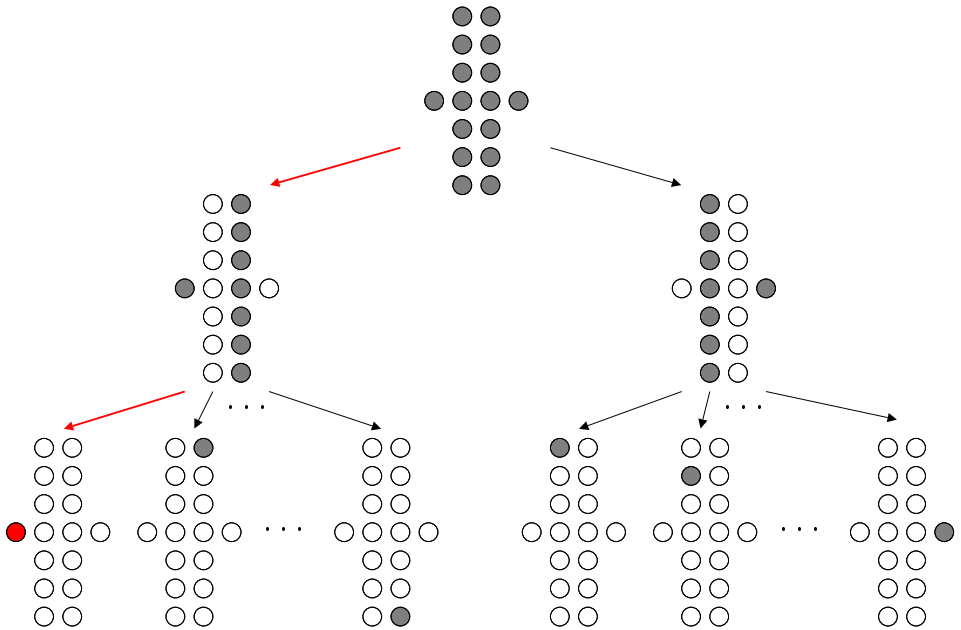
$$\mathcal{C}_1 = \{O O, \ldots\}$$

Construção multinível

Exemplo 1

Combinações

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$



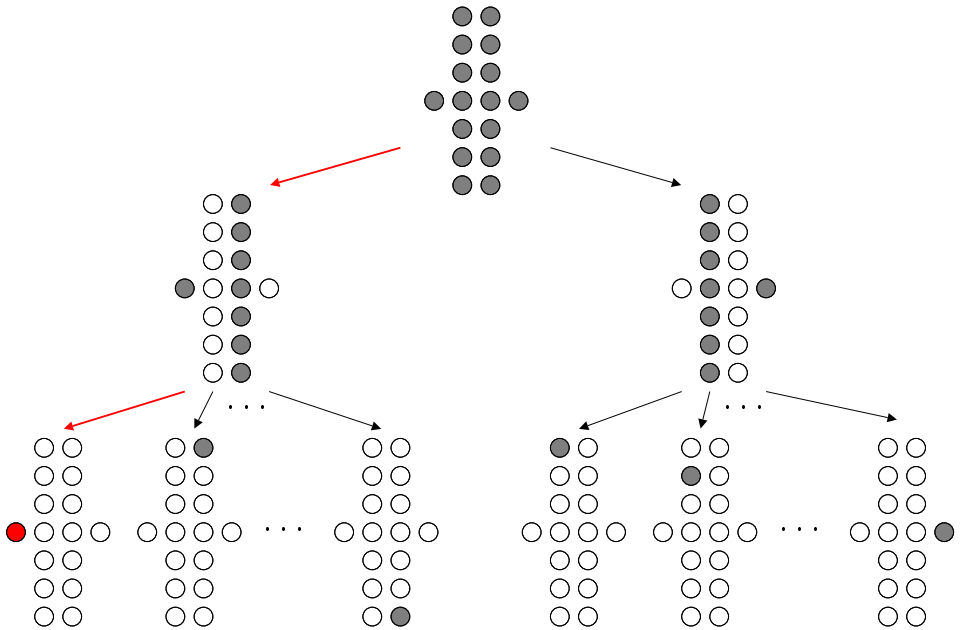
$$\mathcal{C}_1 = \{OOO, \ldots\}$$

Construção multinível

Exemplo 1

Combinações

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$



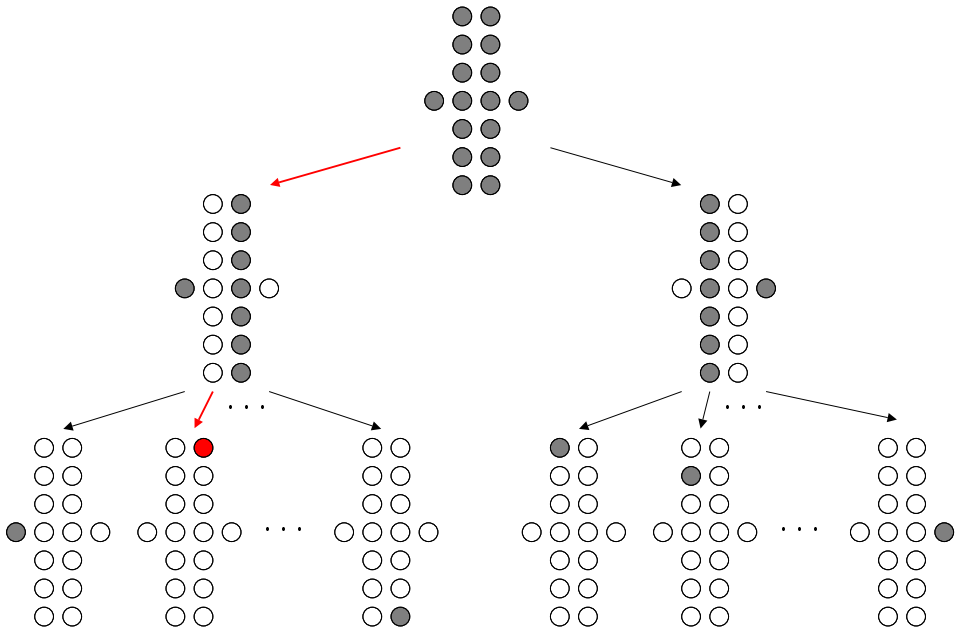
$$\mathcal{C}_1 = \{OOO, O\ldots\}$$

Construção multinível

Exemplo 1

Combinações

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$



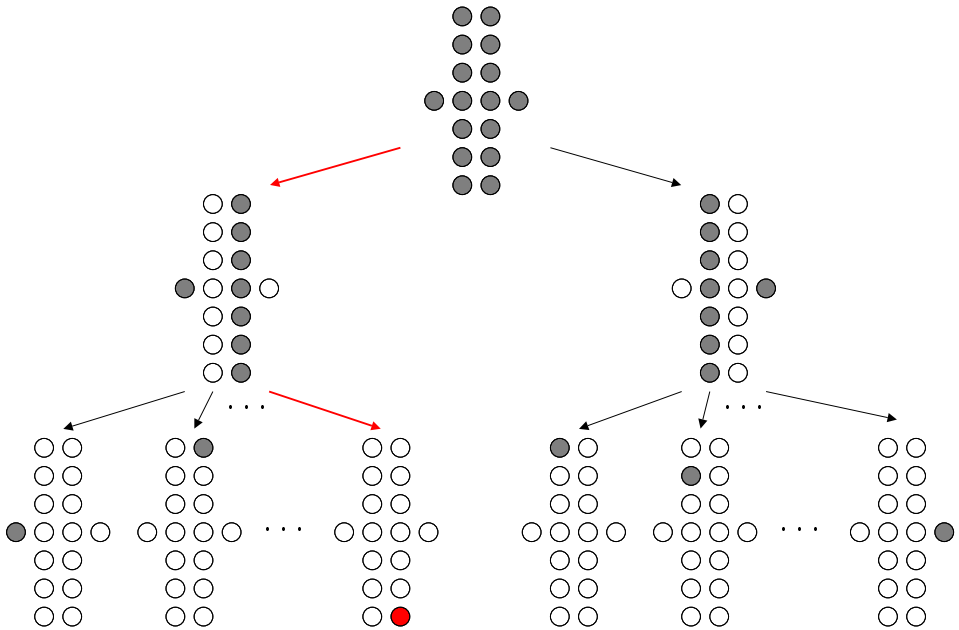
$$\mathcal{C}_1 = \{OOO, OS_1^{\perp} \ldots\}$$

Construção multinível

Exemplo 1

Combinações

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$



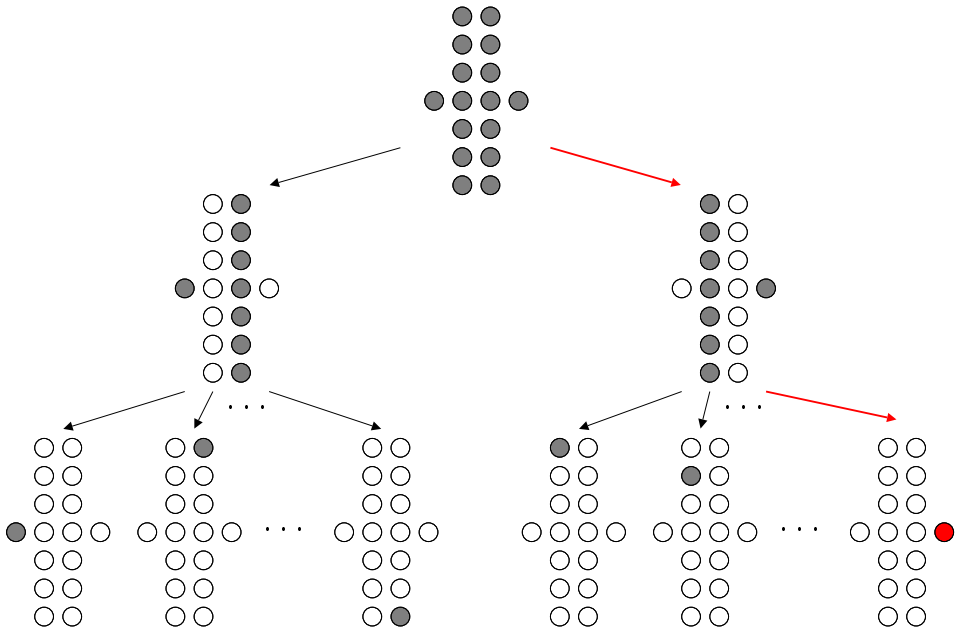
$$\mathcal{C}_1 = \{OOO, OS_1^{\perp} S_7^{\perp}, \ldots\}$$

Construção multinível

Exemplo 1

Combinações

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$



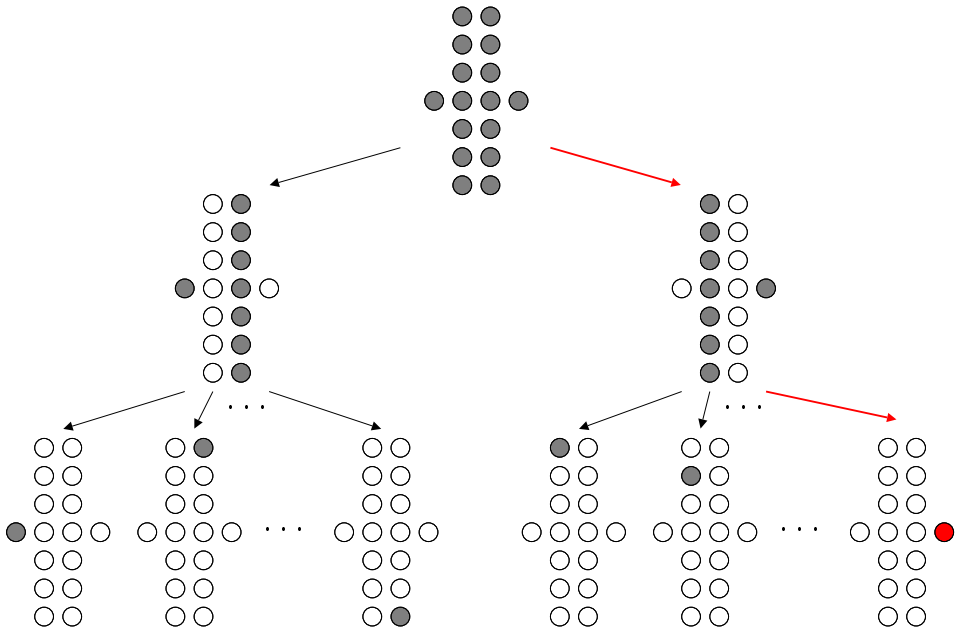
$$\mathcal{C}_1 = \{OOO, OS_1^{\perp}S_7^{\perp}, \ldots, W\}$$

Construção multinível

Exemplo 1

Combinações

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$



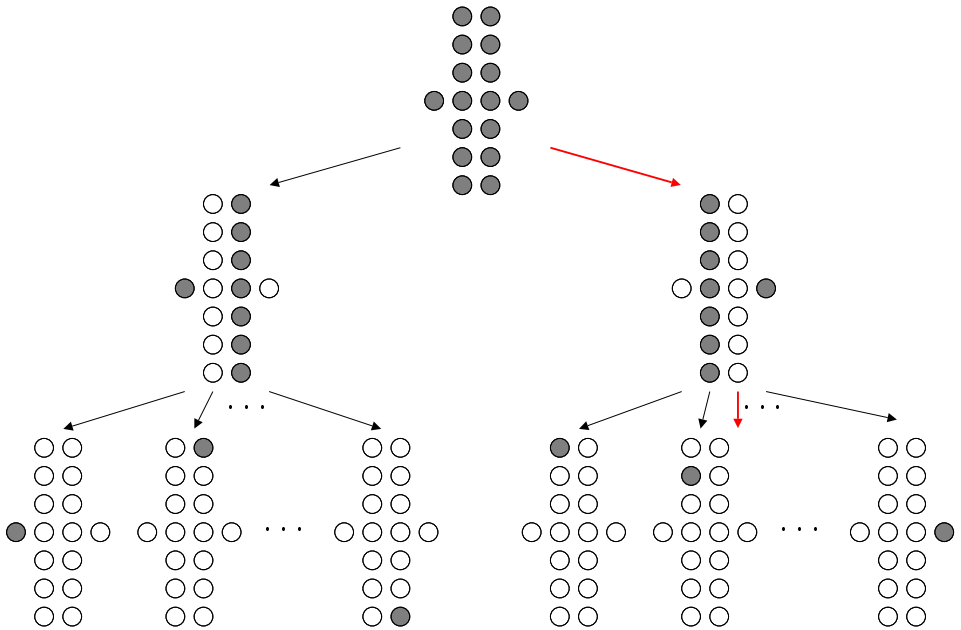
$$\mathcal{C}_1 = \{OOO, OS_1^{\perp}S_7^{\perp}, \ldots, WW\}$$

Construção multinível

Exemplo 1

Combinações

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 7 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 & 1 \\ 7 & 7 & 2 \end{bmatrix}$$



$$\mathcal{C}_1 = \{OOO, OS_1^{\perp}S_7^{\perp}, \ldots, WWS_3\}$$

Construção multinível

Exemplo 1

Resultado

$$\mathcal{C}_1 = \{OOO, OS_1^{\perp}S_7^{\perp}, \ldots, WWS_3\}$$

$$\mathsf{d_S}(\mathcal{C}_1) = 3, \quad |\mathcal{C}_1| = 128$$

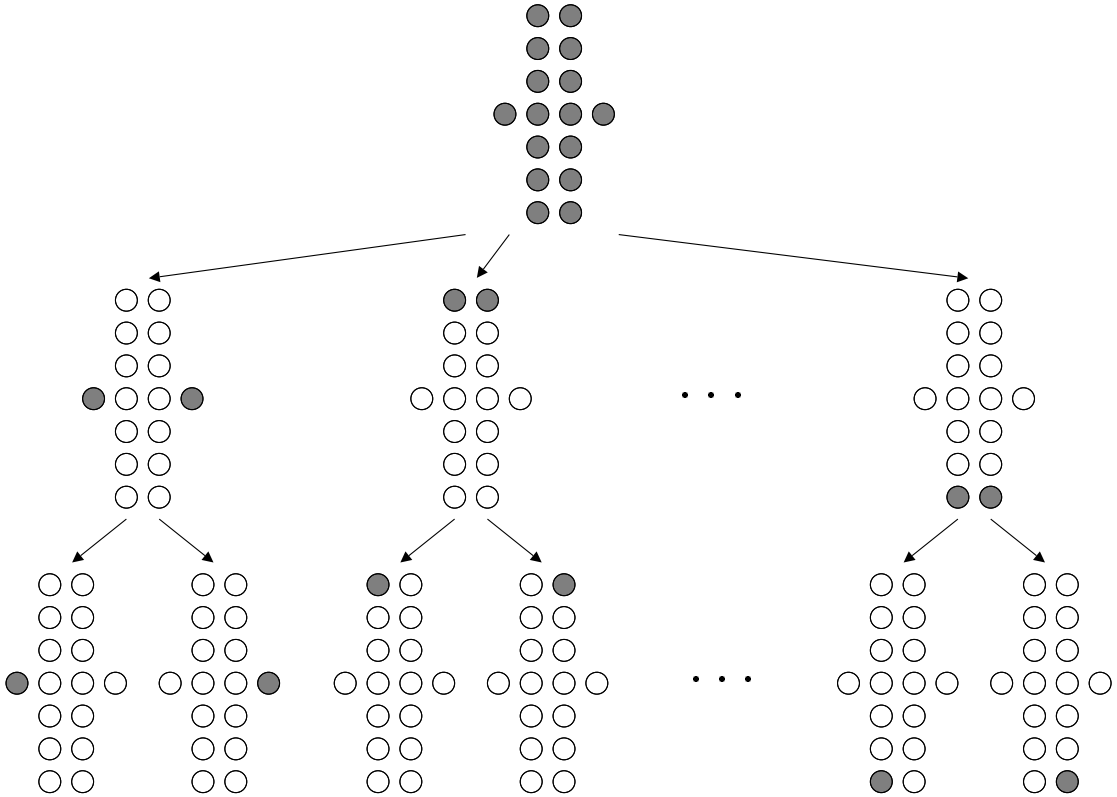
Construção multinível

Exemplo 2

Objetivo

Código 3-*shot* $\mathcal{C}_2$ sobre $\mathcal{P}(\mathbb{F}_2^3)$ com $\mathrm{d_S}(\mathcal{C}_2) = 3$

Particionamento binível



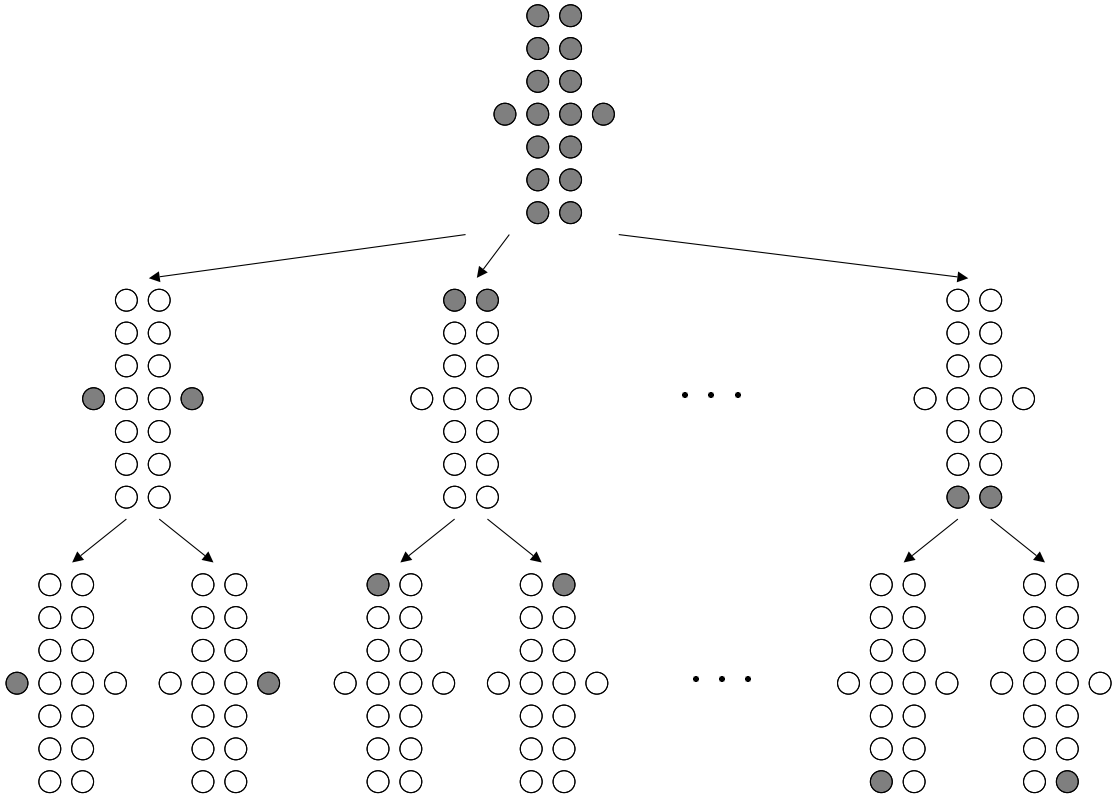
Construção multinível

Exemplo 2

Objetivo

Código 3-*shot* $\mathcal{C}_2$ sobre $\mathcal{P}(\mathbb{F}_2^3)$ com $\mathrm{d_S}(\mathcal{C}_2) = 3$

Distâncias *intrasubset*



$\mathrm{d_S}^{(0)} = 1$

$\mathrm{d_S}^{(1)} = 3$

$\mathrm{d_S}^{(2)} = \infty$

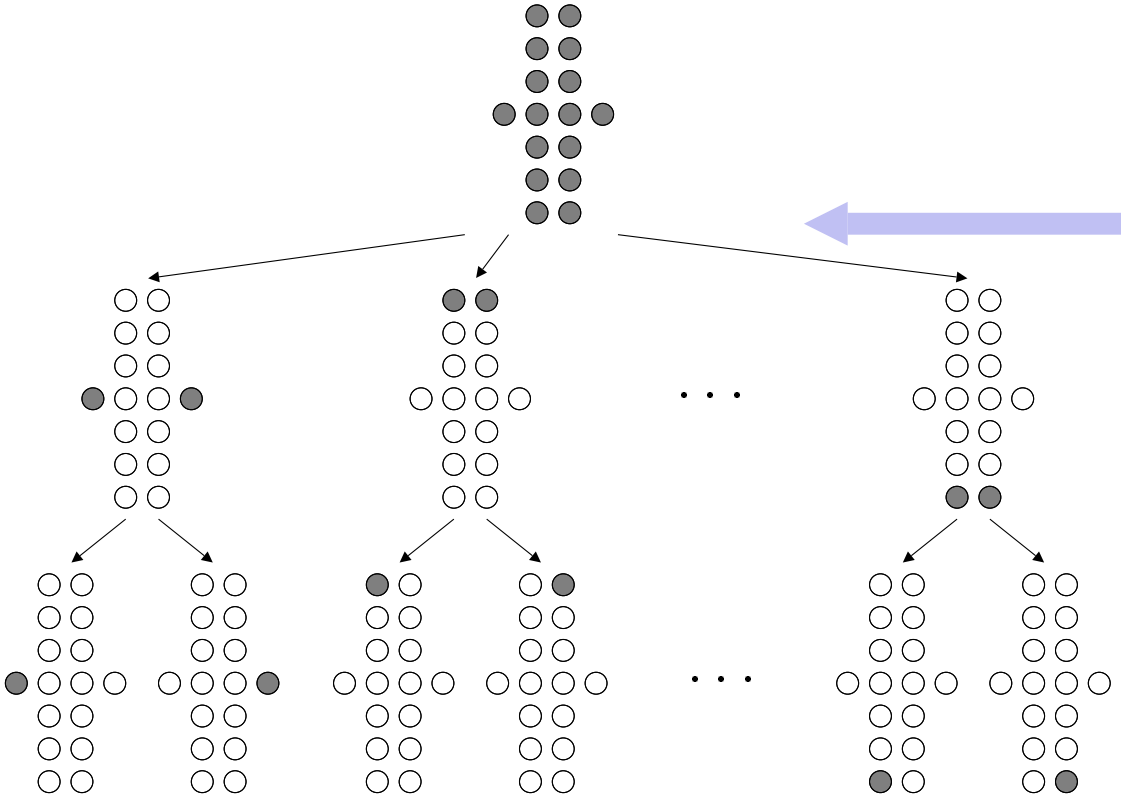
Construção multinível

Exemplo 2

Objetivo

Código 3-*shot* $\mathcal{C}_2$ sobre $\mathcal{P}(\mathbb{F}_2^3)$ com $\mathrm{d_S}(\mathcal{C}_2) = 3$

Códigos componentes



$\mathrm{d_S}^{(0)} = 1$

$\mathcal{H}_1$ octal
com $\mathrm{d_H}(\mathcal{H}_1) \geq 3$

$\mathrm{d_S}^{(1)} = 3$

$\mathrm{d_S}^{(2)} = \infty$

Construção multinível

Exemplo 2

Código componente

Código de repetição:

$$\mathcal{H}_1 = \{000, 111, \ldots, 777\}$$

$$\mathrm{d_H}(\mathcal{H}_1) = 3, \quad |\mathcal{H}_1| = 8$$

Combinações

$$\left[\begin{array}{ccc} 0 & 0 & 0 \end{array}\right], \left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right], \ldots, \left[\begin{array}{ccc} 7 & 7 & 7 \end{array}\right]$$

Construção multinível

Exemplo 2

Código componente

Código de repetição:

$$\mathcal{H}_1 = \{000, 111, \ldots, 777\}$$

$$\mathrm{d_H}(\mathcal{H}_1) = 3, \quad |\mathcal{H}_1| = 8$$

Combinações

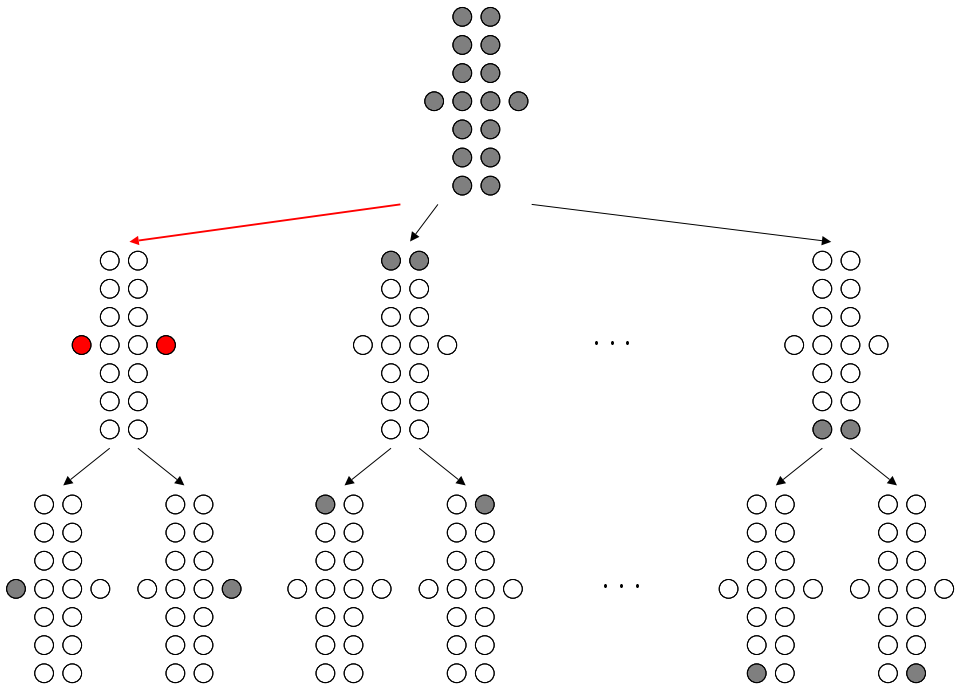
$$\left[\begin{array}{ccc} 0 & 0 & 0 \end{array}\right], \left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right], \ldots, \left[\begin{array}{ccc} 7 & 7 & 7 \end{array}\right]$$

Construção multinível

Exemplo 2

Combinações

$$\left[\begin{array}{ccc} 0 & 0 & 0 \end{array}\right], \left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right], \ldots, \left[\begin{array}{ccc} 7 & 7 & 7 \end{array}\right]$$



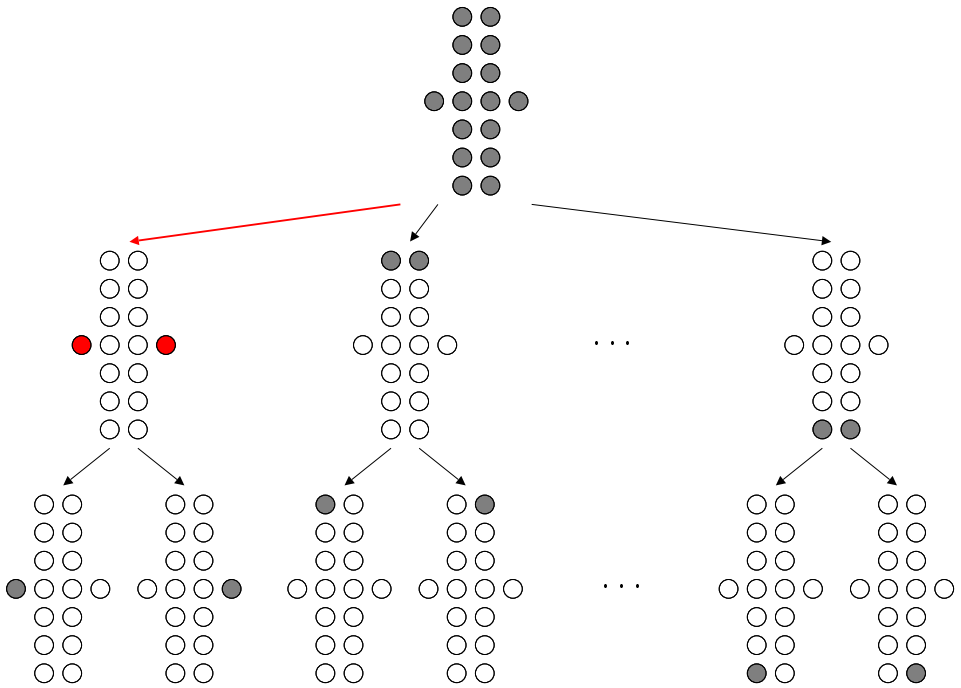
$$\mathcal{C}_2 = \{[O|W], \ldots\}$$

Construção multinível

Exemplo 2

Combinações

$$\left[\begin{array}{ccc} 0 & 0 & 0 \end{array}\right], \left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right], \ldots, \left[\begin{array}{ccc} 7 & 7 & 7 \end{array}\right]$$



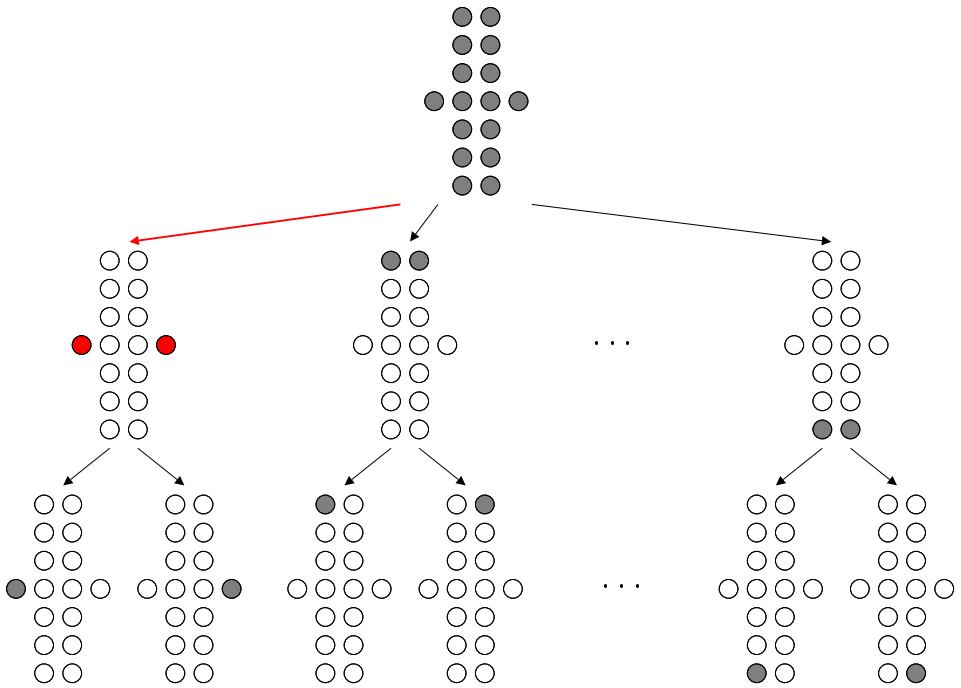
$$\mathcal{C}_2 = \{[O|W][O|W], \ldots\}$$

Construção multinível

Exemplo 2

Combinações

$$\left[\begin{array}{ccc} 0 & 0 & 0 \end{array}\right], \left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right], \ldots, \left[\begin{array}{ccc} 7 & 7 & 7 \end{array}\right]$$



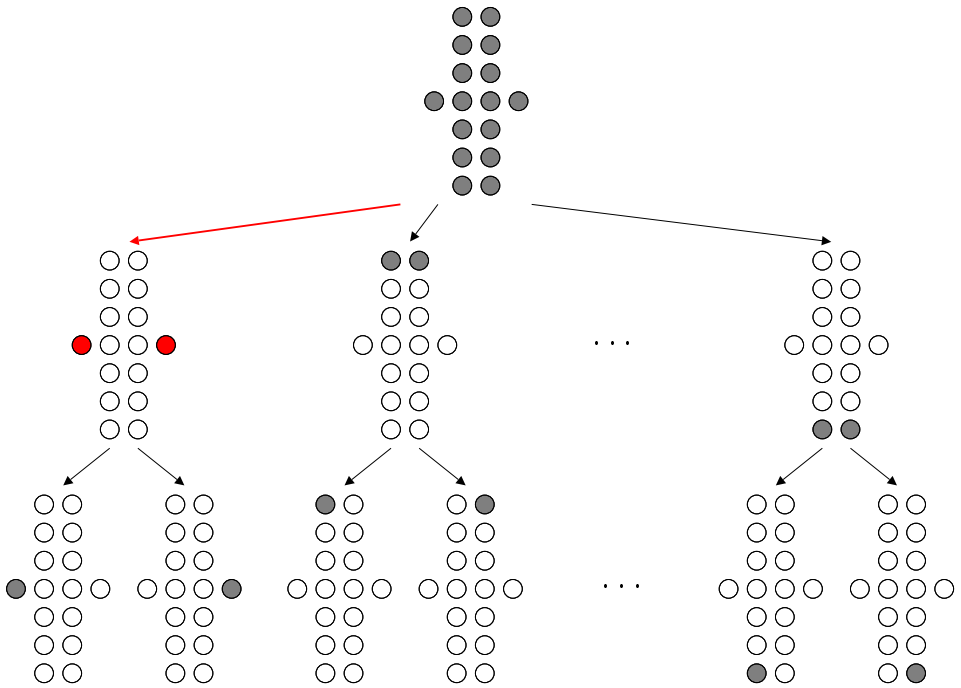
$$\mathcal{C}_2 = \{[O|W][O|W][O|W], \ldots\}$$

Construção multinível

Exemplo 2

Combinações

$$\left[\begin{array}{ccc} 0 & 0 & 0 \end{array}\right], \left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right], \ldots, \left[\begin{array}{ccc} 7 & 7 & 7 \end{array}\right]$$



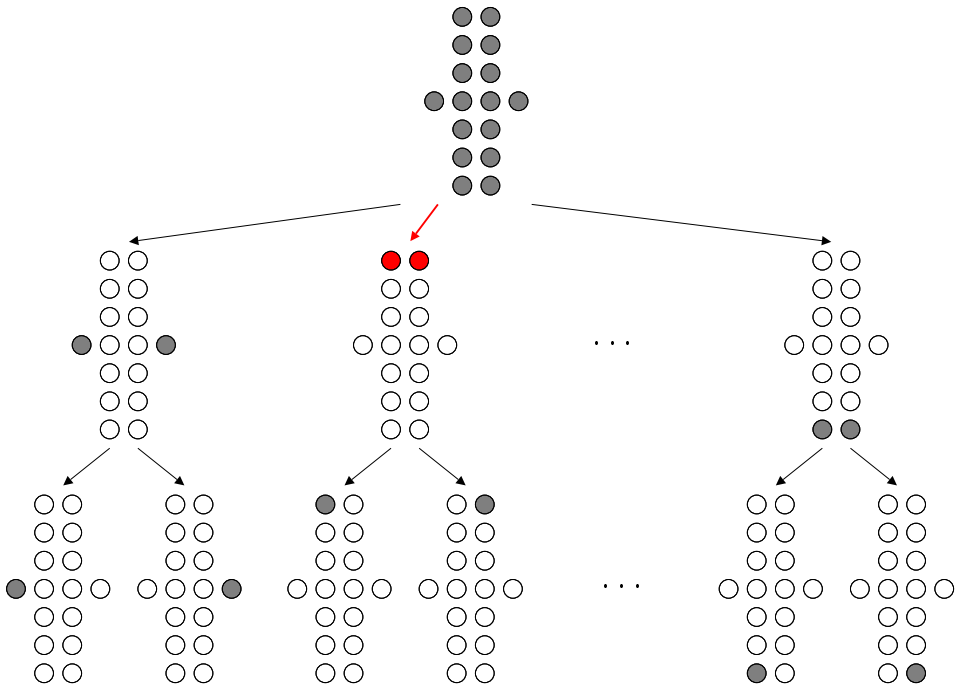
$$\mathcal{C}_2 = \{OOO, OOW, OWO, OWW, WOO, WOW, WWO, WWW, \ldots\}$$

Construção multinível

Exemplo 2

Combinações

$$\left[\begin{array}{ccc} 0 & 0 & 0 \end{array}\right], \left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right], \ldots, \left[\begin{array}{ccc} 7 & 7 & 7 \end{array}\right]$$



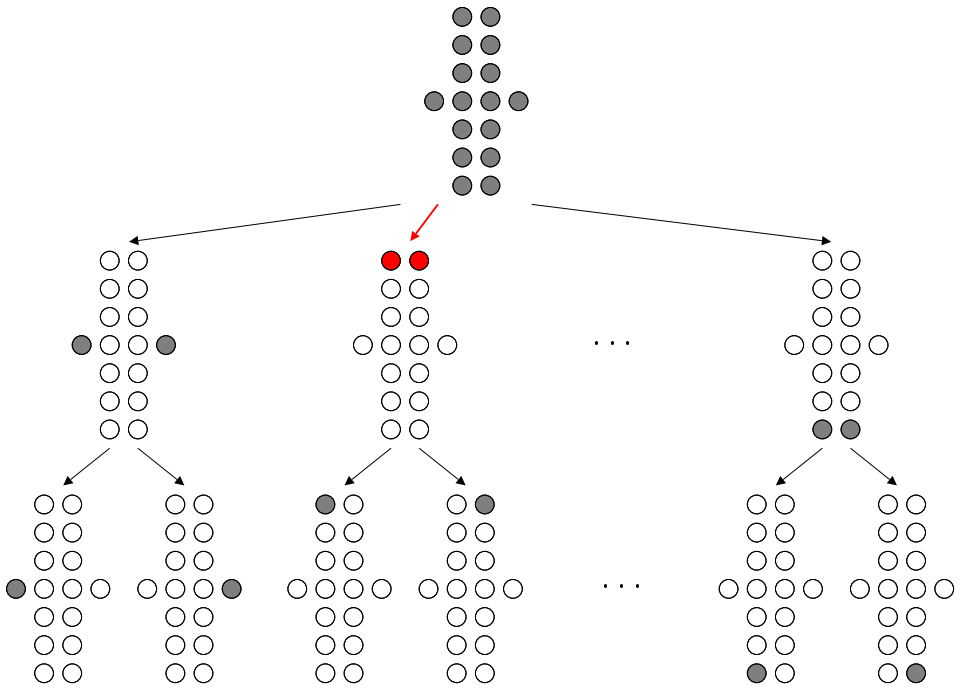
$$\mathcal{C}_2 = \{\ldots, [S_1 | S_1^{\perp}], \ldots\}$$

Construção multinível

Exemplo 2

Combinações

$$\left[\begin{array}{ccc} 0 & 0 & 0 \end{array}\right], \left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right], \ldots, \left[\begin{array}{ccc} 7 & 7 & 7 \end{array}\right]$$



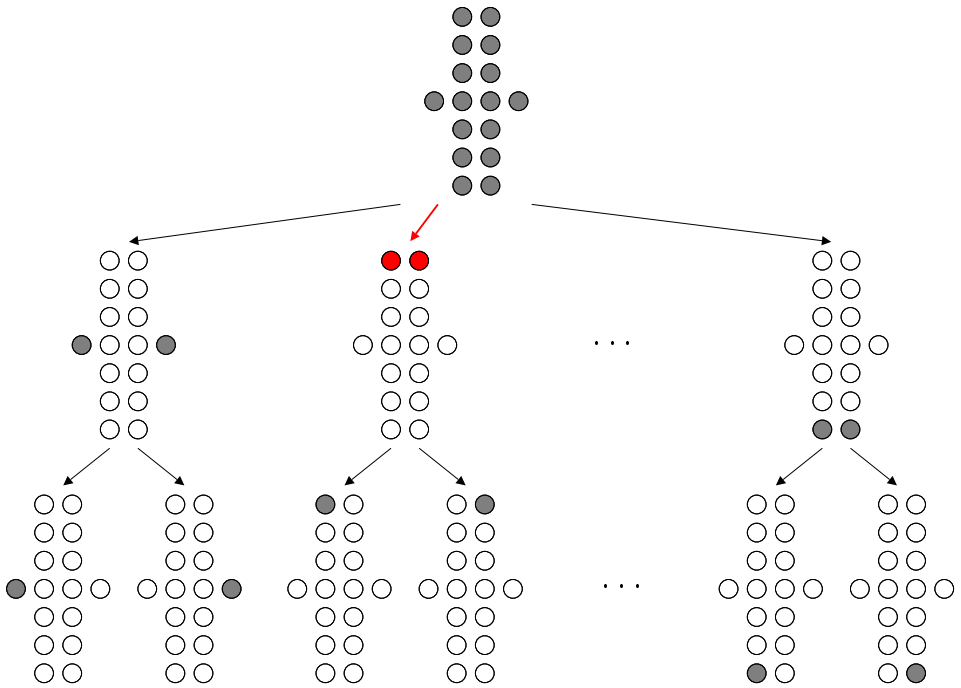
$$\mathcal{C}_2 = \{\ldots, [S_1|S_1^{\perp}][S_1|S_1^{\perp}], \ldots\}$$

Construção multinível

Exemplo 2

Combinações

$$\left[\begin{array}{ccc} 0 & 0 & 0 \end{array}\right], \left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right], \ldots, \left[\begin{array}{ccc} 7 & 7 & 7 \end{array}\right]$$



$$\mathcal{C}_2 = \{\ldots, [S_1|S_1^{\perp}][S_1|S_1^{\perp}][S_1|S_1^{\perp}], \ldots\}$$

Construção multinível

Exemplo 2

Resultado

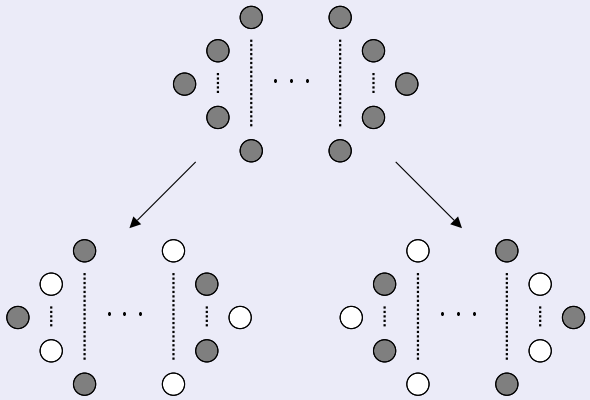
$$\mathcal{C}_2 = \{OOO, OOW, OWO, \ldots\}$$

$$\mathsf{d_S}(\mathcal{C}_2) = 3, \quad |\mathcal{C}_2| = 64$$

Construção multinível

Duas famílias de códigos

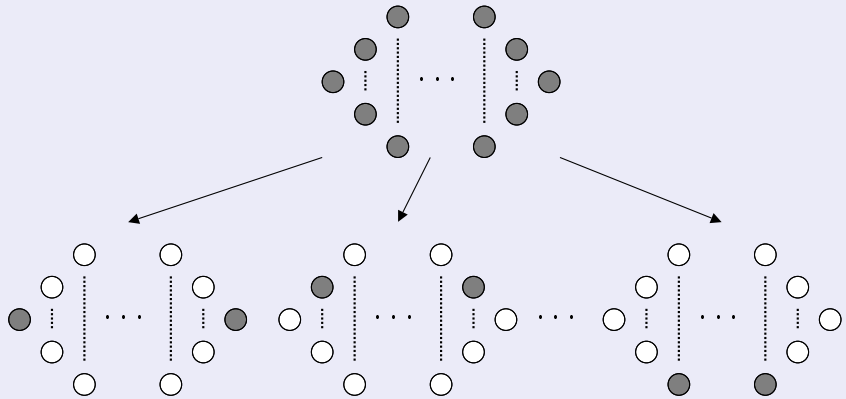
Família 1



$$d_S(\mathcal{C}) = 2$$

$$R(\mathcal{C}) = \log_2 \left|\mathcal{P}(\mathbb{F}_q^m)\right| - \frac{1}{n}$$

Família 2



$$d_S(\mathcal{C}) = m$$

$$R(\mathcal{C}) = 1 - \frac{1}{m} + \frac{1}{m} \log_2 \left|\mathcal{P}(\mathbb{F}_2^m)\right|$$

Conclusão

Conclusão

Sumário das contribuições

Codificação de subespaço *multishot*:

- Definição e motivação
- Relação com códigos *one-shot*
- Limitantes de Hamming, Singleton e Gilbert-Varshamov
- Construção multinível
- Aplicação no controle de erros em codificação de rede não-coerente

Conclusão

Sumário das contribuições

Codificação de subespaço *multishot*:

- Definição e motivação
- Relação com códigos *one-shot*
- Limitantes de Hamming, Singleton e Gilbert-Varshamov
- Construção multinível
- Aplicação no controle de erros em codificação de rede não-coerente

Conclusão

Sumário das contribuições

Codificação de subespaço *multishot*:

- Definição e motivação
- Relação com códigos *one-shot*
- Limitantes de Hamming, Singleton e Gilbert-Varshamov
- Construção multinível
- Aplicação no controle de erros em codificação de rede não-coerente

Conclusão

Sumário das contribuições

Codificação de subespaço *multishot*:

- Definição e motivação
- Relação com códigos *one-shot*
- Limitantes de Hamming, Singleton e Gilbert-Varshamov
- Construção multinível
- Aplicação no controle de erros em codificação de rede não-coerente

Conclusão

Sumário das contribuições

Codificação de subespaço *multishot*:

- Definição e motivação
- Relação com códigos *one-shot*
- Limitantes de Hamming, Singleton e Gilbert-Varshamov
- Construção multinível
- Aplicação no controle de erros em codificação de rede não-coerente

Conclusão
Trabalhos futuros

Propostas de pesquisa:

- Métricas de injeção e de posto
- Códigos convolucionais no lugar de códigos de bloco
- Comparação dos limitantes e da complexidade computacional
- Comportamento assintótico dos limitantes (em q, em m, em n)
- Simulações computacionais

Conclusão
Trabalhos futuros

Propostas de pesquisa:

- Métricas de injeção e de posto
- Códigos convolucionais no lugar de códigos de bloco
- Comparação dos limitantes e da complexidade computacional
- Comportamento assintótico dos limitantes (em q, em m, em n)
- Simulações computacionais

Conclusão
Trabalhos futuros

Propostas de pesquisa:

- Métricas de injeção e de posto
- Códigos convolucionais no lugar de códigos de bloco
- Comparação dos limitantes e da complexidade computacional
- Comportamento assintótico dos limitantes (em q, em m, em n)
- Simulações computacionais

Conclusão
Trabalhos futuros

Propostas de pesquisa:

- Métricas de injeção e de posto
- Códigos convolucionais no lugar de códigos de bloco
- Comparação dos limitantes e da complexidade computacional
- Comportamento assintótico dos limitantes (em q, em m, em n)
- Simulações computacionais

Conclusão
Trabalhos futuros

Propostas de pesquisa:

- Métricas de injeção e de posto
- Códigos convolucionais no lugar de códigos de bloco
- Comparação dos limitantes e da complexidade computacional
- Comportamento assintótico dos limitantes (em q, em m, em n)
- Simulações computacionais

Obrigado!

Roberto Wanderley da Nóbrega
rwnobrega@eel.ufsc.br