

# Teoria da Informação Quântica de Erro-Zero

Francisco M. de Assis  
Universidade Federal de Campina Grande  
Departamento de Engenharia Elétrica  
Instituto de Estudos em Computação e Informação Quânticas

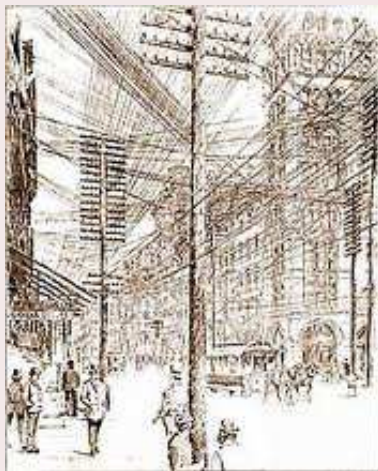
13 de outubro de 2010

# Origem da teoria da Informação: necessidade!

## Alguns pioneiros

- **Nyquist**(1924):  
Amostragem
- **Fisher**(1925):  
Inferência
- **Hartley**(1928): Medida  
log
- **Shannon**(1948):  
Sequências típicas
- **Wiener**(1948): Canais  
contínuos
- **Kotelnikov**(1947):  
Geometrização

## Anos 30: paisagem urbana



## Do que trata a Teoria da Informação?

- **Medidas de informação:** entropia, capacidade
- **Limites fundamentais:** equipartição assintótica
- **Orientação de projetos de aplicações :** processamento de informação

## Termos: mensagem, código, sinal, canal, ruído, distorção, etc...

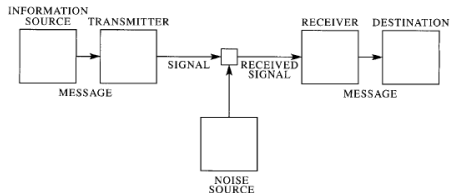


Fig. 1—Schematic diagram of a general communication system.

1948

---

## A Mathematical Theory of Communication

By C. E. SHANNON

### INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist<sup>1</sup> and Hartley<sup>2</sup> on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

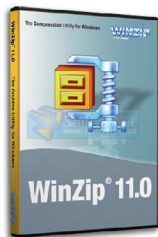
The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are

Published in THE BELL SYSTEM TECHNICAL JOURNAL  
Vol. 27, pp. 379-423, 623-656, July, October, 1948  
Copyright 1948 by AMERICAN TELEPHONE AND TELEGRAPH CO.  
*Printed in U. S. A.*

### Universal Data Compression

---

- J. Ziv and A. Lempel, "A Universal algorithm for sequential data compression," *IEEE Trans. Information Theory*, IT-24, pp. 337-343, May 1977



## Codificação de canal: MIMO

### Multiantenna

---



Capacity of Coherent MIMO: grows as  $\min\{n_T, n_R\}$

- G. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multiple antennas," *Bell Labs Technical Journal* 2, Vol. 1, no. 2, pp 41-59, 1996
- E. Telatar. Capacity of multi-antenna Gaussian channels. *European Trans. on Telecomm.*, 10:585–596, 1999.

### Voiceband Modems

---



**TCM** G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Information Theory*, vol. IT-28, pp. 55-67, 1982.

**BICM** E. Zehavi, 8-PSK trellis codes for a Rayleigh channel, *IEEE Trans. Communications*, vol. 40, no. 5, pp. 873884, May 1992.

G. Caire, G., and E. Biglieri, Bit-interleaved coded modulation, *IEEE Trans. Information Theory*, vol. 44, no. 3, pp. 927946, May 1998.

### Dirty-paper coding

---

- M. Costa "Writing on dirty paper" *IEEE Trans. Information Theory*, 29: 439441, May 1983

#### 'Dirty Paper' Codecs



Challenge: develop world's first capacity-approaching real-time information-embedding system

Solution: 400,000 gate FPGA codecs for transparent 6 Mb/s data stream and 6 MHz NTSC video host stream

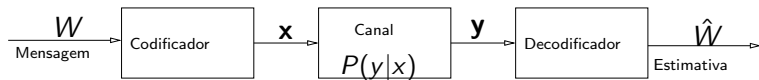
---

1999-2001 Laboratory Partnership with Chinook Communications, Inc.



# TI ordinária: Canais Discretos sem Memória (DMC)

## Modelo com definições



- DMC:  $(\mathcal{X}, P(y|x), \mathcal{Y})$ ,  $x \in \mathcal{X}$ ,  $y \in \mathcal{Y}$ ,  $P(y|x)$  (matriz estocástica)
- Blocos:  $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathcal{X}^n$ ,  $\mathbf{y} = (y_1, y_2, \dots, y_n) \in \mathcal{Y}^n$
- Conjunto de Mensagens:  $W \in \mathcal{W} = \{1, 2, \dots, M(n)\}$
- Alfabeto do código:  $\mathcal{X}$ , e.g.  $\mathcal{X} = \{0, 1\}$  para códigos binários
- Codificador:  $f : w \mapsto c(w) = \mathbf{x}$
- Super-canal:  $(\mathcal{X}^n, P(\mathbf{y}|\mathbf{x}), \mathcal{Y}^n)$

$$P^{(n)}(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^n P(y_i|x_i) \text{ note que } P^{(n)} = \underbrace{P \otimes P \otimes \dots \otimes P}_{n \text{ v\u00e9zes}}$$

# Princípio da Equipartição Assintótica

## Lei fraca dos grandes números

Se  $X_1, X_2, \dots$  i.i.d.  $\sim p(x)$  então

$$-\frac{1}{n} \log p(X_1, X_2, \dots, X_n) = -\frac{1}{n} \sum_i \log p(X_i) \rightarrow -\mathbb{E} \log(p(X)) = H(X)$$

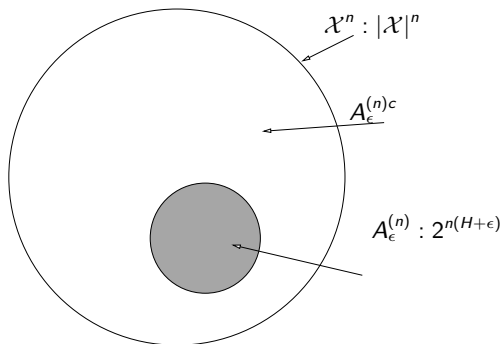
Note que  $p(X_1, X_2, \dots, X_n) \approx 2^{-n(H(X) \pm \epsilon)}$  constante!

## Conjuntos típicos

$$A_\epsilon^{(n)} \triangleq \left\{ (x_1, x_2, \dots, x_n) : 2^{-n(H(X)+\epsilon)} \leq p(x_1, x_2, \dots, x_n) \leq 2^{-n(H(X)-\epsilon)} \right\}$$

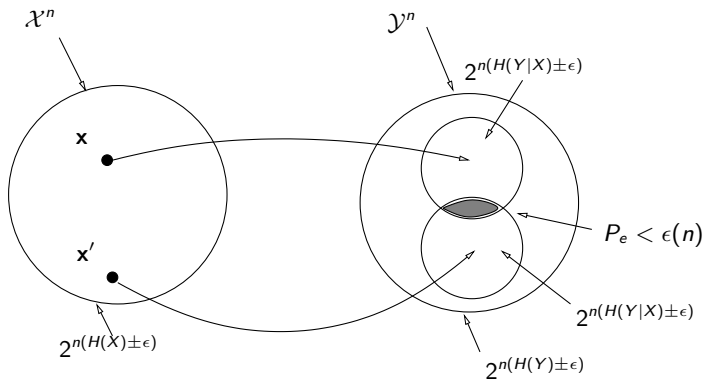
Partição induzida:  $\mathcal{X}^n = \underbrace{A_\epsilon^{(n)}}_{\text{típico: } \tilde{H} \approx H(X)} \cup \underbrace{A_\epsilon^{(n)c}}_{\text{não-típico:}}$

# Consequências da AEP: compressão de dados



Codificação de fonte:  $\frac{\log 2^{n(H(X) \pm \epsilon)}}{n} \approx H(X)$  bits/mensagem

# Consequências da AEP: Capacidade de canal



$$C \approx \max_{\bar{p}} \log \frac{2^{n(H(Y) \pm \epsilon)}}{2^{n(H(Y|X) \pm \epsilon)}} = \max_{\bar{p}} I(X; Y) = \lim_{n \rightarrow \infty, P_e \rightarrow 0} \frac{\log(M(n, P_e))}{n} \text{ bits por uso}$$

# Caracterização da TI ordinária

- $M(n, P_e)$  representa o número de mensagens que podem ser transmitidas pelo canal com uma probabilidade de erro assintoticamente pequena com o tamanho do bloco  $n$ .
- Note que  $\lceil \log M(n, P_e) \rceil$  representa o número de bits necessários para indexar uma mensagem
- Taxa:  $R \triangleq \frac{\log M(n, P_e)}{n}$  (bits de informação por transmissão )
- Gallager:  $P_e < 2^{-nE(R, \vec{p})}$  em que  $E(R, \vec{p})$  é a função expoente do erro. Como  $E(R, \vec{p}) > 0$  se  $R < C$ ,  $P_e$  diminui exponencialmente com  $n$

## TI erro-zero

- O problema muda radicalmente se exigirmos  $P_e = 0$  em lugar de  $P_e \rightarrow 0$ .
- Agora a Combinatória ocupa o lugar da Estatística....

# C.E. Shannon, "Zero-error capacity of a noisy channel", IRE Trans. on IT, Vol. 40, pp. 8-19, 1956

## THE ZERO ERROR CAPACITY OF A NOISY CHANNEL

Claude E. Shannon

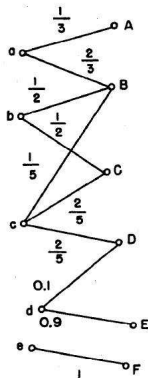
Bell Telephone Laboratories, Murray Hill, New Jersey  
Massachusetts Institute of Technology, Cambridge, Mass.

### Abstract

The zero error capacity  $C_0$  of a noisy channel is defined as the least upper bound of rates at which it is possible to transmit information with zero probability of error. Various properties of  $C_0$  are studied; upper and lower bounds and methods of evaluation of  $C_0$  are given. Inequalities are obtained for the  $C_0$  relating to the "sum" and "product" of two given channels. The analogous problem of zero error capacity  $C_{0F}$  for a channel with a feedback link is considered. It is shown that while the ordinary capacity of a memoryless channel with feedback is equal to that of the same channel without feedback, the zero error capacity may be greater. A solution is given to the problem of evaluating  $C_{0F}$ .

### Introduction

The ordinary capacity  $C$  of a noisy channel may be thought of as follows. There exists a sequence of codes for the channel of increasing block length such that the input rate of transmission approaches  $C$  and the probability of error in decoding at the receiving point approaches zero. Furthermore, this is not true for any value higher than  $C$ . In some situations it may be of interest to consider, rather than codes



# Teoria da Informação de Erro-Zero

O problema da teoria da informação é reproduzir em um ponto (destino) exata ou aproximadamente uma mensagem selecionada em outro ponto (fonte).

Em geral admite-se uma pequena probabilidade de erro, entretanto há situações em que a comunicação deve ser livre de erros:

## Exemplo

- Situações em que somente um número limitado de usos do canal pode ser feito. Resultados assintóticos não podem ser invocados
- Soluções de problemas da teoria da informação que podem ser resolvidos por meio de técnicas de erro-zero. ( Csizár e Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 1981)
- Permite desenvolver métodos aplicáveis para outras áreas em particular ciência da computação

## Exemplo de aplicação: hashing

### Definição [Yao]:

Dado um conjunto  $B$  com  $b$  elementos e números naturais  $k \leq b$  e  $n$  um conjunto  $C \subseteq B^n$  é dito ser  $k$ -separável se para toda  $k$ -upla de elementos distintos de  $C$  existe uma coordenada  $1 \leq i \leq n$  na qual  $k$  valores da  $i$ -ésima coordenada de  $k$  seqüências são todas distintas.

### Exemplo:

$$B = \{1, 2, 3\}, \quad b = |B| = 3, \quad n = 2, \quad k = 2$$

Temos

$$B^2 = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$$

O subconjunto

$$C = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 2)\}$$

é 2-separável?



# Exemplo de aplicação: hashing

Körner et al.: *New bounds for perfect hashing via information theory*, Euro. J. Combinatorics, vol. 9, pp.523-530, 1988

Denotando  $N(n, b, k)$  a cardinalidade do maior subconjunto  $k$ -separável de  $B^n$  e definindo

$$q(b, k) \triangleq \limsup_{n \rightarrow \infty} \frac{1}{n} \log N(n, b, k)$$

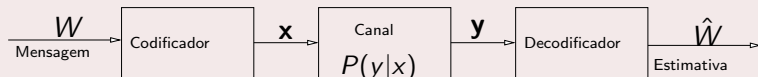
Körner e Marton provam que

$$q(b, k) \leq \min_{0 \leq j \leq k-2} g(b, j+1) \log \frac{b-j}{k-j-1}$$

em que

$$g(b, k) = \prod_{0 \leq i \leq k-1} \frac{b-i}{b}$$

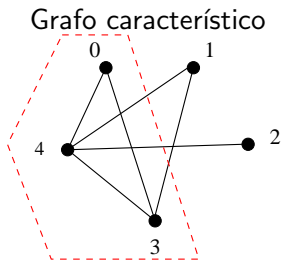
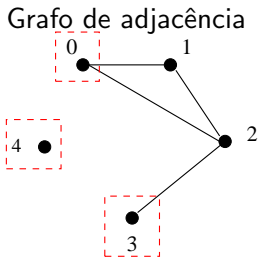
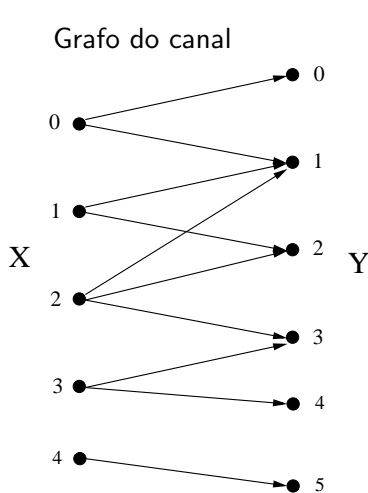
## De volta ao modelo



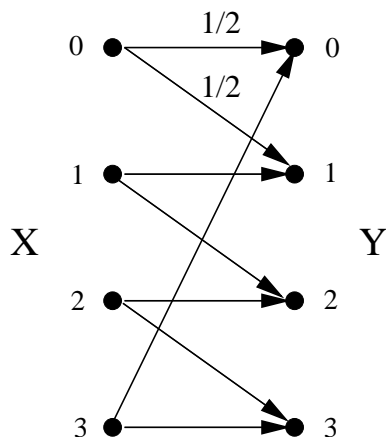
- Ausência de memória:  $P^{(n)}(\mathbf{y}|\mathbf{x})$  como produto
- Estacionaridade: a matriz estocástica é a mesma para  $i = 1, 2, \dots, n$
- Se duas sequências  $\mathbf{x} \neq \mathbf{x}'$  pode levar ao mesmo  $\mathbf{y}$ , com probabilidade não-nula elas são **indistinguíveis**:

$$P^{(n)}(\mathbf{y}|\mathbf{x}) > 0 \text{ e } P^{(n)}(\mathbf{y}|\mathbf{x}') > 0$$

- Grafo de adjacência ou grafo de confusão
- Grafo característico: arcos definidos por nós dados por símbolos distinguíveis



# Indistinguibilidade e ortogonalidade: ilustração



$$P = (\Pr(y|x) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix})$$

Note que

$$P(\cdot|0) \perp P(\cdot|2)$$

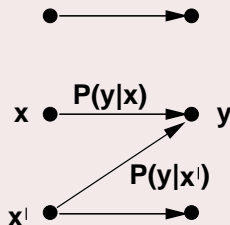
$$P(\cdot|1) \perp P(\cdot|3)$$

e que  $x = 0$  e  $x = 3$  são **indistinguíveis** pois

$$\Pr[y = 0|0] = \Pr[y = 0|3] = 1/2$$

# Indistinguibilidade e ortogonalidade

- Note que  $\mathbf{x}$  e  $\mathbf{x}'$  são distinguíveis se e somente se as linhas  $P^{(n)}(\cdot|\mathbf{x})$  e  $P^{(n)}(\cdot|\mathbf{x}')$  são ortogonais
- Os elementos de um código  $\mathcal{C} \subseteq \mathcal{X}^n$  podem ser usados sem erro se e somente se as linhas correspondentes são mutuamente ortogonais



# Código de bloco erro-zero clássico

Dado um canal DMC  $(\mathcal{X}, P(y|x), \mathcal{Y})$  definimos um código de bloco erro-zero de taxa  $R \triangleq \frac{1}{n} \log M(n)$  pelo sistema formado por

- 1 Um conjunto das mensagens  $\mathcal{W} = \{1, \dots, M(n)\}$
- 2 Uma função de codificação  $f : \mathcal{W} \rightarrow \mathcal{X}^{\otimes n}$
- 3 Uma função de decodificação  $g : \mathcal{Y}^n \rightarrow \mathcal{W}$
- 4 Uma condição

$$\Pr [g(\mathbf{y}) \neq w | f(w) = \mathbf{x}(w)] = 0 \text{ para todo } w \in \mathcal{W}$$

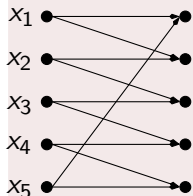
## Capacidade Erro-Zero Clássica de um Canal Discreto sem Memória

$$C_0(P) \triangleq \limsup_{n \rightarrow \infty} \frac{1}{n} \log M(n)$$

Note que  $M(n)$  é igual a cardinalidade do maior conjunto de linhas mutuamente ortogonais da matriz  $P^{(n)}$

# Exemplo (muito) famoso

## Canal



$$n = 1$$

$$M(n) = 2$$

$$\mathcal{X} = \{x_1, x_3\}$$

$$A_1 = \{x_1, x_2\}$$

$$A_2 = \{x_3, x_4\}$$

$$A_1 \cap A_2 = \emptyset$$

$$R = 1$$

## Código erro-zero

$$f(w) = \mathbf{x}$$

Conjuntos “típicos”

$$x_1 x_1 \rightarrow A_1 = \{x_1 x_1, x_1 x_2, x_2 x_1, x_2 x_2\}$$

$$x_2 x_3 \rightarrow A_2 = \{x_2 x_3, x_3 x_3, x_2 x_4, x_3 x_4\}$$

$$x_3 x_5 \rightarrow A_3 = \{x_3 x_5, x_4 x_5, x_3 x_1, x_4 x_1\}$$

$$x_4 x_2 \rightarrow A_4 = \{x_4 x_2, x_5 x_2, x_4 x_3, x_5 x_3\}$$

$$x_5 x_4 \rightarrow A_5 = \{x_5 x_4, x_1 x_4, x_5 x_5, x_1 x_5\}$$

- Note que  $A_i \cap A_j = \emptyset$  para  $i \neq j$ , portanto a taxa é  $R = \frac{M(2)}{2} = \frac{1}{2} \log 5 \approx 1.161$
- Lovász mostra que de fato  $C_0 = R$  para este canal
- Capacidade ordinária:  $C = \max_{\bar{p}} I(X; Y) = \log 5/2 \approx 1.322$

- **Grafo característico:** Vimos que  $G = (V(G), E(G))$  em que

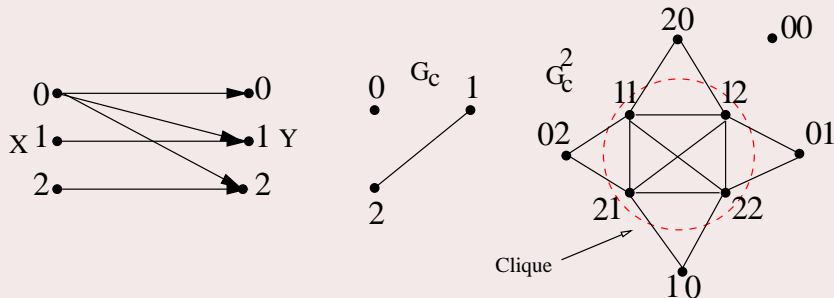
$$V(G) = \mathcal{X}$$

$$E(G) = \{(x', x'') : x' \perp x''\}$$

- **Grafo-característico-produto:**  $G^n = (V(G^n), E(G^n))$  em que
  - $V(G^n) = (V(G))^n$
  - $(x', x'') \in E(G^n)$  se e somente se  $x'_i \perp x''_i$  para pelo menos um  $1 \leq i \leq n$
- **Número de clique** ( $w(G)$ ): é a cardinalidade do maior sub-conjunto de vértices de  $G$  com todos os vértices dois a dois conectados



## Exemplo: grafo-característico-produto, clique



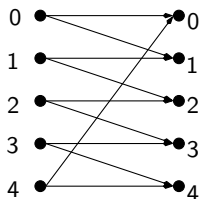
### Definição alternativa baseada em grafos

$$C_0 = \sup_n \frac{1}{n} \log \omega(G^n),$$

$\omega(G^n)$  é o número de clique do  $n$ -grafo-produto  $G^n$ . Note que no exemplo:  $\omega(G^2) = (\omega(G))^2$

# Super-multiplicatividade não-trivial

$$M(P, n + m) \geq M(W, n) \cdot M(P, m)$$



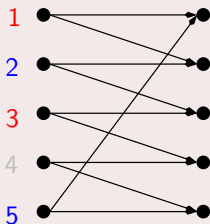
$$M(P, 2) = 5 > \\ M(P, 1) \times M(P, 1) = 4$$

$$P = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}$$

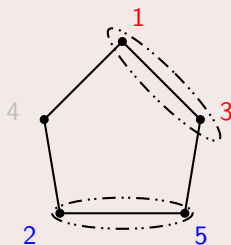
Note que  $P^{(2)} = P \otimes P$  é  $25 \times 25$ !

# Exemplo: pentágono. Distinguibilidade e grafo característico

Símbolos distinguíveis  
(não-adjacentes)



Grafo característico



# Teoria da informação em sistemas quânticos: comparação

Parâmetro	TI Clássica	TI Quântica
Sinais símbolos	$a$	$\rho$
Alfabeto	$a \in \{a_1, \dots, a_l\}$	$\rho \in \{\rho_1, \dots, \rho_l\}$
Palavra-código	$\bar{a} \in \{a_1, \dots, a_l\}^n$	$\bar{\rho} \in \{\rho_1, \dots, \rho_l\}^{\otimes n}$
Canal	$p(y x)$	$\mathcal{E}(\rho)$
Entropia	$H(X)$	$S(\rho) = -\text{tr} [\rho \log \rho]$
Capacidade	$\max I(X; Y)$	Holevo, outras
Decodificação	Algoritmos	POVM e algoritmos

## Motivação

É natural perguntar pelos análogos e extensões da teoria da informação erro-zero clássica para sistemas quânticos

## Exemplos de analogias e extensões

- Generalização da noção de capacidade erro-zero clássica
- Definição formal e interpretação baseada na teoria de grafos
- Condições (código e POVM) para alcançar a capacidade erro-zero
- Uma cota superior: a capacidade ordinária de HSW

# Capacidade erro-zero de canais quânticos

Capacidade de um canal (clássico ou quântico) é o **supremo das taxas em que a informação pode ser transmitida confiavelmente**. Em geral a capacidade depende do sistema físico e dos protocolos de comunicação. Considerando que sistemas quânticos exibem propriedades não compartilhadas por sistemas clássicos é natural que a capacidade dos canais quânticos apresentem características peculiares.

## Exemplo: capacidades segundo o protocolo utilizado

- Palavras-código produtos tensoriais & medições individuais
  - *on shot* e capacidade adaptativa
- Entrelaçamento entre várias entradas & medições individuais
- Palavras-código produtos tensoriais & medições coletivas
  - Capacidade Holevo-Schumacher-Westmoreland (HSW): extensão da capacidade ordinária de Shannon

# Capacidade erro-zero de canais quânticos: preliminares

## Estados puros

(unitário)  $|\psi\rangle \in \mathcal{H}_d$

$\{|0\rangle, |1\rangle, \dots, |d-1\rangle\} \Rightarrow$  base  $\mathcal{H}_d$

$$|0\rangle \equiv [1 \ 0 \ \dots \ 0]^T$$

$$|d-1\rangle \equiv [0 \ 0 \ \dots \ 1]^T$$

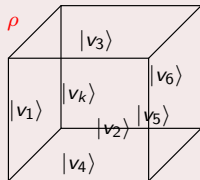
$$|+\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

## Estados mistos

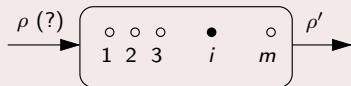
O sistema pode estar em  $|v_i\rangle$  com probabilidade  $p_i$

Operador de densidade

$$\rho = \sum_{i=1}^k p_i |v_i\rangle \langle v_i|$$



## Medições POVM



Aparato POVM

$$\text{POVM } \mathcal{P} = \{M_1, \dots, M_m\}; \quad \sum_i M_i = \mathbb{1}$$

$$\text{Prob[obter saída } i] = \text{tr}[\rho M_i]$$

von Neumann:  $M_i \Rightarrow$  projetores

# Capacidade erro-zero de canais quânticos: preliminares

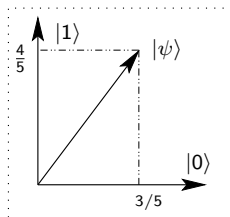
## Um exemplo - Medições Projetivas (von Neumann)

Considere o estado quântico  $|\psi\rangle = \frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$ . O operador de densidade é:

$$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} \frac{3}{5} \\ \frac{4}{5} \end{bmatrix} \begin{bmatrix} \frac{3}{5} & \frac{4}{5} \end{bmatrix} \Rightarrow \rho = \frac{1}{25} \begin{bmatrix} 9 & 12 \\ 12 & 16 \end{bmatrix}$$

Seja  $\mathcal{P}$  o POVM definido por  $\mathcal{P} = \{M_1, M_2\}$ , em que

$$M_1 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad M_2 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$



## Probabilidades

$$Prob[\text{obter 1}] = \text{tr}[\rho M_1] = \frac{9}{25} = \left(\frac{3}{5}\right)^2$$

$$Prob[\text{obter 2}] = \text{tr}[\rho M_2] = \frac{16}{25} = \left(\frac{4}{5}\right)^2$$



## Modelo do canal quântico

Representado matematicamente por um mapeamento positivo que preserva o traço:

$$\mathcal{E}(\rho) = \sum_a E_a \rho E_a^\dagger,$$

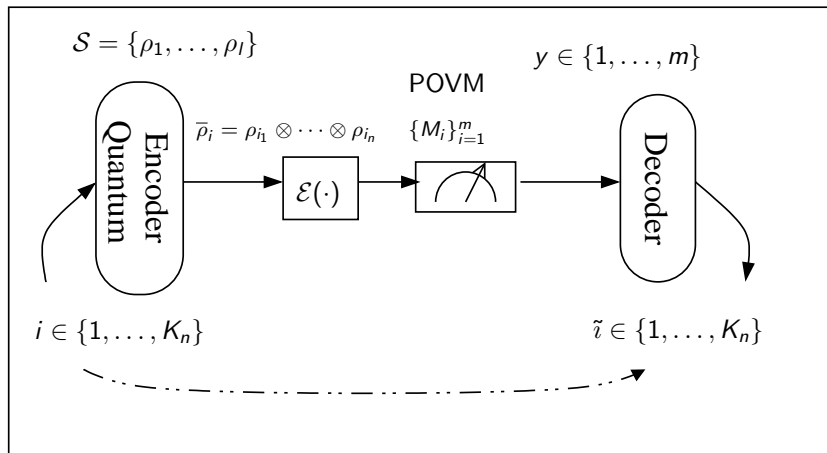
onde  $\sum_a E_a^\dagger E_a = \mathbb{1}$ .

Canal de atenuação de amplitude (dissipação de energia)

$$\mathcal{E}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger,$$

em que  $E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}$  e  $E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$ .

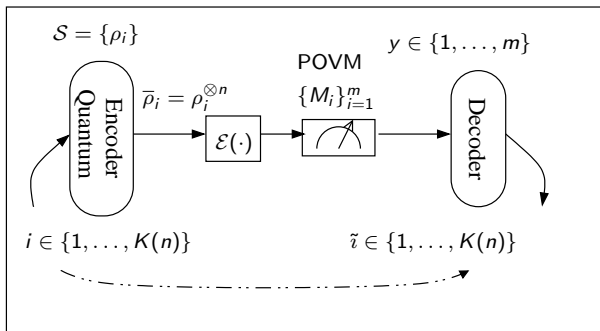
# Sistema de comunicações erro-zero para canais quânticos



# Definição: código de bloco quântico ( $K(n), n$ )

Dado o alfabeto  $\mathcal{S} = \{\rho_i\}_{i=1}^l$  definimos um código de bloco quântico erro-zero de taxa  $R \triangleq \frac{1}{n} \log K(n)$  pelo sistema formado por

- 1 Um conjunto das mensagens:  $\{1, \dots, K(n)\}$
- 2 Uma função de codificação:  $X^n : \{1, \dots, K(n)\} \rightarrow \mathcal{S}^{\otimes n}$
- 3 Uma função de decodificação:  $g : \{1, \dots, m\} \rightarrow \{1, \dots, K\}$
- 4 Uma condição:  $\Pr[g(y) \neq i | X^n = X^n(i)] = 0, i = 1, \dots, K(n)$



# Capacidade erro-zero de um canal quântico

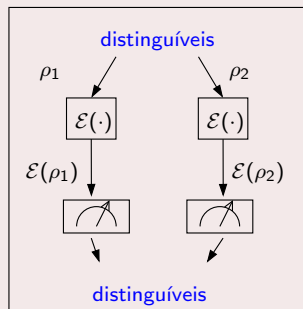
## Definição

A capacidade erro-zero de um canal quântico é definida por

$$C_0(\mathcal{E}) = \sup_n \frac{1}{n} \log K(n)$$

sendo  $K(n)$  a cardinalidade do maior conjunto de mensagens que podem ser transmitidas livres de erros usando um código quântico  $(K(n), n)$

## Distinguibilidade



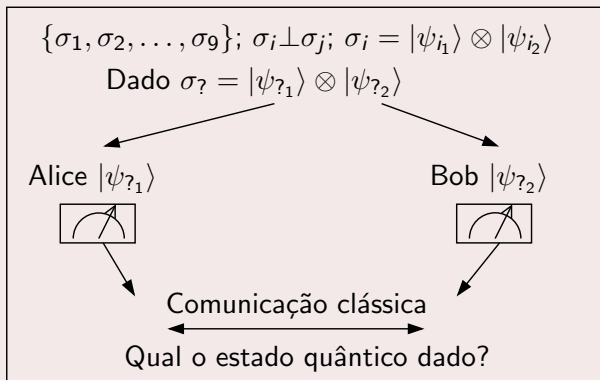
Dois estados quânticos  $\rho_1$  e  $\rho_2$  são ditos distinguíveis se o resultados de suas medições pelo POVM da saída do canal são distinguíveis.

Notação:

$$\mathcal{E}(\rho_1) \perp \mathcal{E}(\rho_2) \quad \text{ou} \quad \rho_1 \perp_{\mathcal{E}} \rho_2$$

# Capacidade de canais quânticos com entradas emaranhadas

## Indistinguibilidade de estados quânticos



- Nem sempre é possível distinguir estados ortogonais com medições coletivas! (Bennett et. al.)

## Função de Lovász quântica

Winter et al., *Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovász  $\vartheta$  function*, arXiv:1002.2514[quant-ph], Mar 2010

Andreas Winter et al., *Improving zero-error classical communication with entanglement*, arXiv:0911.5300[quant-ph], Nov 2009

Andreas Winter et al., *Zero-error channel capacity and simulation assisted by non-local correlations*, arXiv:1003.3195[quant-ph], Mar 2010

- Propõe uma generalização quântica da matriz de confusão (adjacência) no espaço dos operadores com a qual redefine as capacidades erro-zero clássica, quântica e quântica com auxílio de emaranhamento
- Define a versão quântica da função  $\vartheta$  de Lovász que é um limite superior para o número de mensagens erro-zero que podem ser transmitidas com auxílio de emaranhamento
- Propõe o estudo de espaços de operadores associados aos canais como *grafos não-comutativos*

## Emaranhamento e transmissão erro-zero

Shi and Duan, *Entanglement between Two Uses of a Noisy Multipartite Quantum Channel Enables Perfect Transmission of Classical Information*, PRL 101, 020501 (2008)

- Para um sistema com  $m$  fontes e  $n$  destinatários com transmissão erro-zero através de um canal ruidoso
- Entre as fontes é permitido a troca de mensagens clássicas (cooperação clássica) e também entre os destinatários
- Se o canal é clássico uma única transmissão erro-zero é possível se e somente se múltiplas transmissões erro-zero são possíveis
- Descubrem que para canais quânticos que não permitem transmissão erro-zero com uma transmissão podem permitir para duas transmissões em sistemas com  $m \geq 2$  ou  $n \geq 2$

## Superativação de capacidade erro-zero de canais quânticos

Toby S. Cubbit et al., *Superactivation of the Asymptotic Zero-Error Classical Capacity of a Quantum Channel*, arXiv:0906.2547[quant-ph]v2, Sept 2009 Chen, Cubbit, Harrow and Smith, *Super-duper-activation of the Zero-Error Quantum Capacity*, International Symposium on Information Theory (ISIT), Austin, Texas, June, 2010

Apresentam o teorema:

Sejam  $d_A = 16$ ,  $d_E = 124$  e  $d_B = 1984$ . Então existem canais  $\mathcal{E}_1$ ,  $\mathcal{E}_2$ , tais que:

- 1 Cada canal  $\mathcal{E}_{1,2}$  mapeia  $\mathbb{C}^{d_A}$  em  $\mathbb{C}^{d_B}$  e têm  $d_E$  operadores de Kraus
- 2 Cada canal  $\mathcal{E}_{1,2}$  tem capacidade erro-zero nula
- 3 O canal conjunto  $\mathcal{E}_1 \otimes \mathcal{E}_2$  tem capacidade erro-zero maior que zero.

Note que individualmente os canais **não** podem transmitir qualquer informação livre de erros ainda que um número ilimitado de usos de canal seja permitido. Entretanto se os dois canais são combinados mesmo um **único uso** de cada um dos dois canais permite a transmissão de informação livre de erros!



Salman Beigi and Peter W. Shor, *On the Complexity of Computing Zero-Error and Holevo Capacity of Quantum Channels*, arXiv:07092090[quant-ph], Oct 2008

Partindo do problema NP da determinação do número de clique em grafos define o análogo quântico: dado um canal quântico decida se existem  $k$  estados distinguíveis. O que coincide com o problema da determinação da capacidade erro-zero de um canal quântico definida com uso de grafos. **É demonstrado que o problema em foco é da classe QMA-completo.**

Hui Khoon Ng et al., *Information preserving structures: A general framework for quantum zero-error information*, arXiv:1006.1358v1[quant-ph], Jun 2010

Promessas dos autores:

- 1 Introduzir um referencial geral usando *estruturas preservadoras de informação* para classificar os tipos de informação que podem ser transmitidas livres de erro em sistemas quânticos.
- 2 Provar que todo código para transmissão livre de erros possui a mesma estrutura algébrica matricial.
- 3 Dar critérios distintos para preservação da informação e algoritmos para encontrar todas as estruturas preservadoras de informação de um canal.



Rex A. C. Medeiros, Francisco M. de Assis , *Quantum Zero-Error Capacity*, International Journal of Quantum Information, Vol. 3, No. 1, pp. 135-139, May, 2005.



C. E. Shannon *The Zero Error Capacity of a Noisy Channel* , IRE Transactions on Information Theory, Vol. 2, N0. 3, pp. 8-19, 1956.



Lászlo Lovász, *On the Shannon Capacity of a Graph*, IEEE Transactions on Information Theory, Vol. 25, No. 1, pp. 1-7, May 1979.



Runyiao Duan, *Super-Activation of Zero-Error Capacity of Noisy Quantum Channels*, arXiv 0906.02527v1, [quant-ph], 15 Jun 2009



G. Brassard and L. Salvail, *Secret-key reconciliation by public discussion*, in Proc. EUROCRYPT'93: Workshop on the Theory and Applications of Cryptographic Technics on Advances in Cryptology. New York: Springer-Verlag, 1994, pp. 410-423.



C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, *Generalized privacy amplification* IEEE Transactions Information Theory, vol. 41, no. 6, pp. 1915-1923, Nov. 1995.



Toby S. Cubbit et al., *Superactivation of the Asymptotic Zero-Error Classical Capacity of a Quantum Channel*, arXiv:0906.2547[quant-ph]v2, Sept 2009



Shi and Duan, *Entanglement between Two Uses of a Noisy Multipartite Quantum Channel Enables Perfect Transmission of Classical Information* , PRL 101, 020501 (2008)



Salman Beigi and Peter W. Shor, *On the Complexity of Computing Zero-Error and Holevo Capacity of Quantum Channels*, arXiv:07092090[quant-ph], Oct 2008



Chen, Cubbit, Harrow and Smith, *Super-duper-activation of the Zero-Error Quantum Capacity*, International Symposium on Information Theory (ISIT), Austin, Texas, June, 2010



Andreas Winter et al., *Improving zero-error classical communication with entanglement*, arXiv:0911.5300[quant-ph], Nov 2009



Andreas Winter et al., *Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovász  $\vartheta$  function*, arXiv:1002.2514[quant-ph], Mar 2010