



## Sessão nº9

# Capacidade de canal e Introdução à codificação de canal

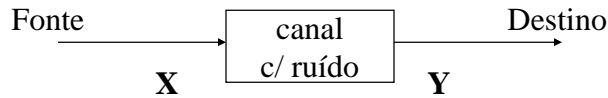


## Conceitos básicos da Teoria da Informação

- Medida de quantidade de informação (entropia).
- Capacidade de informação dum canal.
- ↙ - Codificação:
  - codificação de fonte
  - [cifra]
  - ↘ • codificação de canal



## Modelo de canal discreto sem memória



Sejam  $X$  e  $Y$  variáveis aleatórias:

- $p(x_i)$  - probabilidade da fonte produzir o símbolo  $x_i$  para transmissão
- $p(y_j)$  - probabilidade do símbolo  $y_j$  ser recebido no destino
- $p(x_i, y_j)$  - probabilidade conjunta de ser transmitido  $x_i$  e de ser recebido  $y_j$
- $p(x_i | y_j)$  - probabilidade condicionada de ter sido transmitido  $x_i$  dado que foi recebido  $y_j$
- $p(y_j | x_i)$  - probabilidade condicionada de ser recebido  $y_j$  dado que foi transmitido  $x_i$



## Informação mútua



- Define-se **informação mútua** das v.a.  $X$  e  $Y$  como

$$I(X; Y) = \sum_{x_i \in X} \sum_{y_j \in Y} p(x_i, y_j) \log_2 p(x_i, y_j) / p(x_i) p(y_j)$$

- Informação mútua é a medida da quantidade de informação que a v.a.  $X$  contém acerca da v.a.  $Y$ ; redução da incerteza de  $X$  por conhecimento de  $Y$

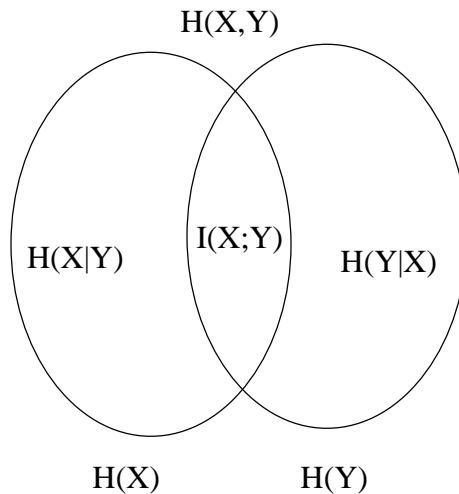
–  $I(X; Y) = H(X) - H(X|Y)$

- se  $X$  e  $Y$  são independentes então

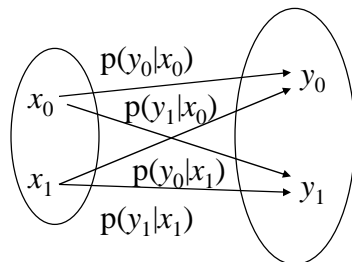
$$I(X; Y) = 0$$



## Relação entre a entropia e a informação mútua



## Análise do canal binário simétrico - exemplo



### Dados:

$$p(x_0) = 1/4, \quad p(x_1) = 3/4$$

$$p(y_1|x_0) = 1/2, \quad p(y_0|x_1) = 1/2$$

### Verifica-se que

$$H(X) \approx 0,81 \text{ [bit/símbolo]}$$

$$H(Y|X) = 1 \text{ [bit/símbolo]}$$

$$H(Y) = 1 \text{ [bit/símbolo]}$$

$$I(X;Y) = ?$$

$$I(X;Y) = 0$$

**não se “ganha” informação acerca do símbolo**

**transmitido por observação do símbolo recebido pois X e**

**Y são independentes, uma vez que  $p(x|y) = p(x) \quad \forall x \quad \forall y$**



## Capacidade de canal

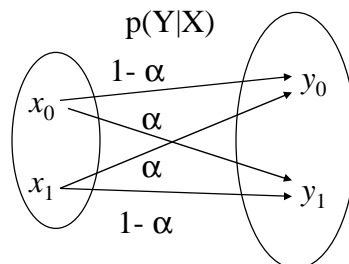


- define-se **capacidade de canal** dum canal discreto e sem memória como sendo o máximo da informação mútua média  $I(X;Y)$ , onde a maximização faz-se considerando todas as possíveis distribuições de probabilidade dos símbolos da fonte

$$C_s = \max_{\{p(x_i)\}} I(X;Y) \text{ [bit/símbolo]}$$



## Capacidade do canal binário simétrico



$$C_s = 1 - H(a) \text{ [bit/símbolo]}$$

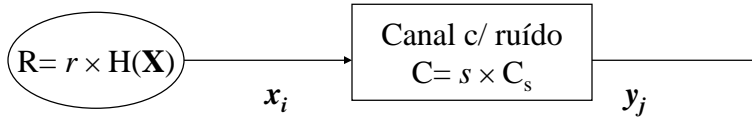
- Probabilidade de erro médio

$$P_e = p(x_0) p(y_1|x_0) + p(x_1) p(y_0|x_1) = a$$

é independente das probabilidades da fonte!



## Teorema fundamental para um canal c/ ruído



- **R** representa a velocidade de informação da fonte
- **s** representa o ritmo médio de símbolos binários transmitidos pelo canal em cada segundo
- **C** representa a capacidade do canal; expressa em [bit/s]

Se **R**  $\leq$  **C** então existe uma técnica de codificação tal que os símbolos produzidos pela fonte podem ser transmitidos sobre o canal com uma probabilidade de erros arbitrariamente pequena.



## Capacidade do canal telefónico - exemplo



- Considere-se

$$B = 3 \text{ KHz e } S/N = 35 \text{ dB (garantidos pela PT)}$$

- A capacidade dum canal contínuo com ruído aditivo branco e gaussiano (AWGN) é determinada pela lei de Hartley-Shannon, por

$$C = B \log_2(1 + S/N)$$

- então temos

$$C = 34,88 \text{ Kbit/s}$$



## Codificação de canal



- Com a codificação de fonte **eliminou-se a redundância**, pelo que idealmente todos os símbolos binários “contêm” um bit de informação.
- Mas estes símbolos vão ser transmitidos sobre um **canal com ruído**, logo vai haver **perda de informação** sempre que existir erro num símbolo.
- A solução deste problema consiste em **adicionar redundância** de tal forma que apesar dos erros do canal ainda é possível transferir a quantidade de informação associada à mensagem; faz-se com a **codificação de canal**.



## Como adicionar redundância?



- forma simples:
  - código de repetição
  - código de bit de paridade
- forma mais elaborada:
  - códigos de bloco lineares
    - Ex. Código de Hamming
    - códigos cíclicos
      - Ex. CRC, BCH, ...
  - códigos convolucionais (orientados ao símbolo)



## Probabilidade de erros numa palavra de código



- Se os erros de transmissão são aleatórios e independentes, então a probabilidade de existirem  $i$  erros numa palavra com  $n$  bits é dada pela função distribuição binomial

$$P(i,n) = \binom{n}{i} \alpha^i (1-\alpha)^{n-i}$$

onde

- $\alpha$  é a probabilidade de erro de 1 bit
- $\binom{n}{i} = n! / i! (n-i)!$



## Conceitos básicos na codificação de canal



- Define-se **distância de Hamming** entre duas palavras  $\mathbf{X}$  e  $\mathbf{Y}$ ,  $\mathbf{d}(\mathbf{X},\mathbf{Y})$ , como sendo o número de símbolos em que diferem as duas palavras.
- Define-se **peso de Hamming** de uma palavra  $\mathbf{X}$ ,  $\mathbf{W}(\mathbf{X})$ , como sendo o número de símbolos diferentes de zero que integram essa palavra.
- A **distância mínima** de um código é determinada pela palavra, diferente de zero, com menor peso de Hamming .
- Um código com palavras de  $n$  bits onde  $k$  bits são de dados e os restantes são redundantes, designa-se por **código de bloco linear**  $(n,k)$  sendo o limite superior da distância mínima dado por  $\mathbf{d}_{\min} \leq n - k$ 
  - para detectar até  $l$  erros  $\mathbf{d}_{\min} \geq l + 1$
  - para corrigir até  $t$  erros  $\mathbf{d}_{\min} \geq 2t + 1$
  - para detectar até  $l$  erros e corrigir até  $t$  erros  $\mathbf{d}_{\min} \geq l + t + 1$



## Códigos de bloco lineares



- Seja  $\mathbf{X}$  uma palavra do código tal que  $\mathbf{X} = [ \mathbf{0} \ \mathbf{0} \ \mathbf{0} ]$ , por exemplo.
- Um código diz-se linear se for gerado com base numa **matriz geradora**  $\mathbf{G}$ . Sendo  $\mathbf{M}$  a matriz que representa a mensagem a codificar, então as palavras do código obtêm-se por

$$\mathbf{X} = \mathbf{M} \cdot \mathbf{G}$$

- Para garantir que o código seja **sistemático**, ou seja no bloco encontram-se primeiro os *bits* de dados e depois os redundantes (ou vice versa), então deve-se fazer  $\mathbf{G} = [ \mathbf{I}_k \ | \ \mathbf{P} ]$  sendo  $\mathbf{P}$  a sub-matriz geradora de paridade.
- A **matriz de controlo de paridade**  $\mathbf{H}$  definida por  $\mathbf{H} = [ \mathbf{P} \ | \ \mathbf{I}_{n-k} ]$  permite verificar se existem erros na palavra recebida  $\mathbf{Y}$ , através do cálculo do **síndrome**  $\mathbf{S} = \mathbf{Y} \cdot \mathbf{H}^T$



## Códigos de Hamming

