COMUNICAÇÃO DE DADOS

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Departamento de Informática
Universidade do Minho

2012-2013

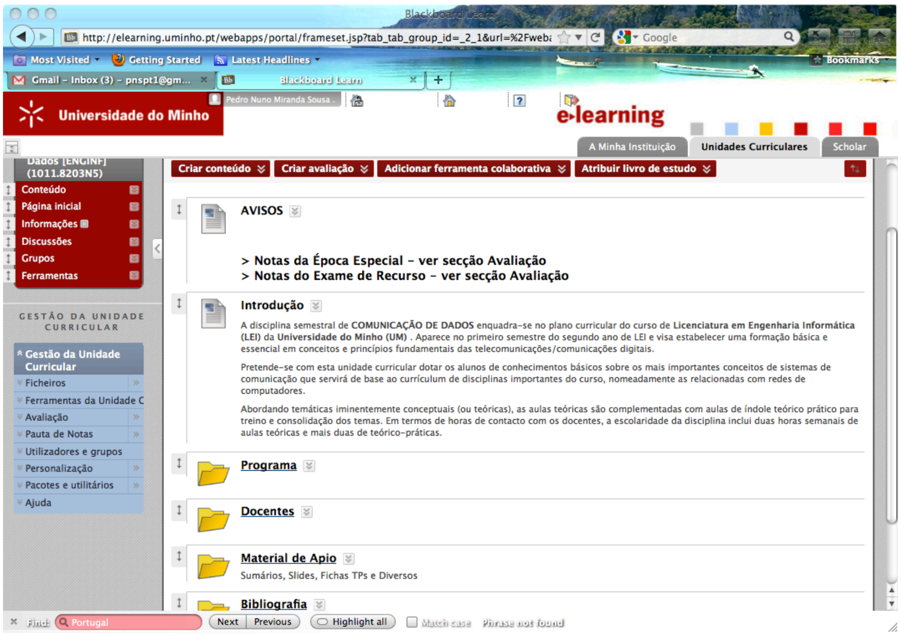
EQUIPA DOCENTE

- **Pedro Sousa**
  pns@di.uminho.pt
  253 604 436
  (Docente Responsável - Teóricas + TPs)

INFORMAÇÕES E MATERIAL DE APOIO À UNIDADE CURRICULAR

- Aceder à plataforma de e-learning da Universidade do Minho

Slides Aulas / FichasTPs / Sebenta - PASSWORD: LEI-CD-1213
Pré-inscrição BB: LEICD1213



AVALIAÇÃO

- **Regime de Avaliação**
  2 Testes de Avaliação (T1,T2)
  - » *em regime de avaliação periódica distribuídos ao longo do semestre*
  - » *mais informações sobre os testes serão posteriormente anunciadas*
  - » **Nota Final [0.5*T1 + 0.5*T2]**

- **Exame:** os alunos sem aproveitamento (i.e. nota final < 10) podem efectuar uma prova final de avaliação na data definida para o efeito pelo Conselho de Cursos.

BIBLIOGRAFIA

- ***Fundamentos das Telecomunicações***
  V. Freitas, Universidade do Minho, 2003.

- *Principles of Communications, 5th Edition*
  R. Ziemer, W. Tranter, John Wiley & Sons.

- *Communication Systems,*
  A. Bruce Carlson, McGraw-Hill Series

Comunicação de Dados
Licenciatura em Engenharia Informática
Departamento de Informática, Universidade do Minho

DATAS dos Testes de Avaliação

– 21 Nov. & 25 Jan. (a serem confirmadas pela DC-LEI)

TURNOS TEÓRICO-PRÁTICOS

– 4 turnos (TP1 .. TP4)
– **Material necessário paras as TPs**
  - **Sebenta da disciplina**
  - **Máquina calculadora**
– Início das aulas TPs - próxima semana (24 Set.)

>> Enquadramento na LEI ...

PROGRAMA RESUMIDO

I. Teoria da Informação
II. Digitalização
III. Multiplexagem
IV. Análise de Sinais (+ Cap. Introdução)
V. Análise de Sistemas de Transmissão
VI. Códigos para Controlo de Erros (+ breve introdução a ruído e erros)

I. TEORIA DA INFORMAÇÃO

Teorema Fundamental da Teoria de informação

*"Dado um **canal de comunicação** e uma **fonte de informação** cujo débito de informação não excede a capacidade do canal, existe um código tal que a informação pode ser transmitida através do canal com uma frequência de erros arbitrariamente pequena, apesar da presença de ruído no canal."*

I. TEORIA DA INFORMAÇÃO

Teoria de informação estuda 4 problemas fundamentais:

– A medida de informação produzida por uma fonte ...

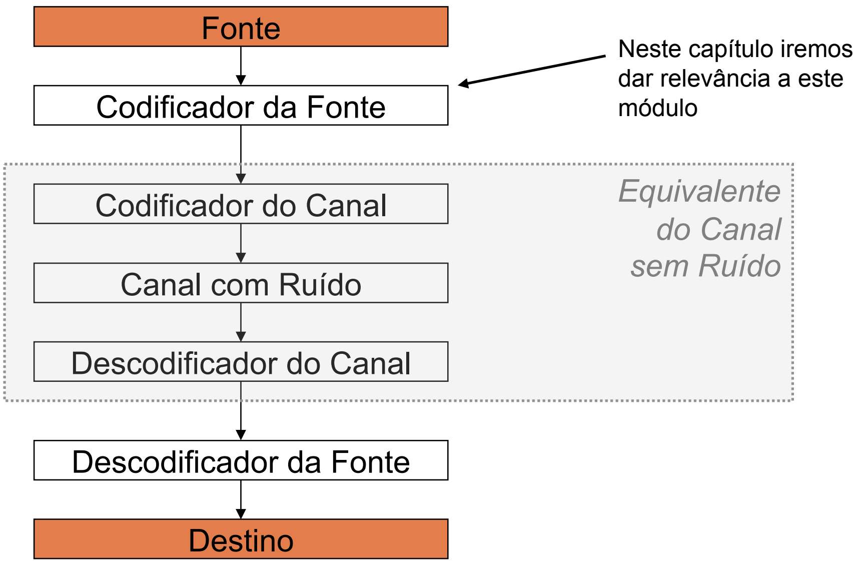
– A codificação eficiente da fonte ...

– A capacidade do canal ...

– A codificação do canal para controlo de erros ...

I. TEORIA DA INFORMAÇÃO

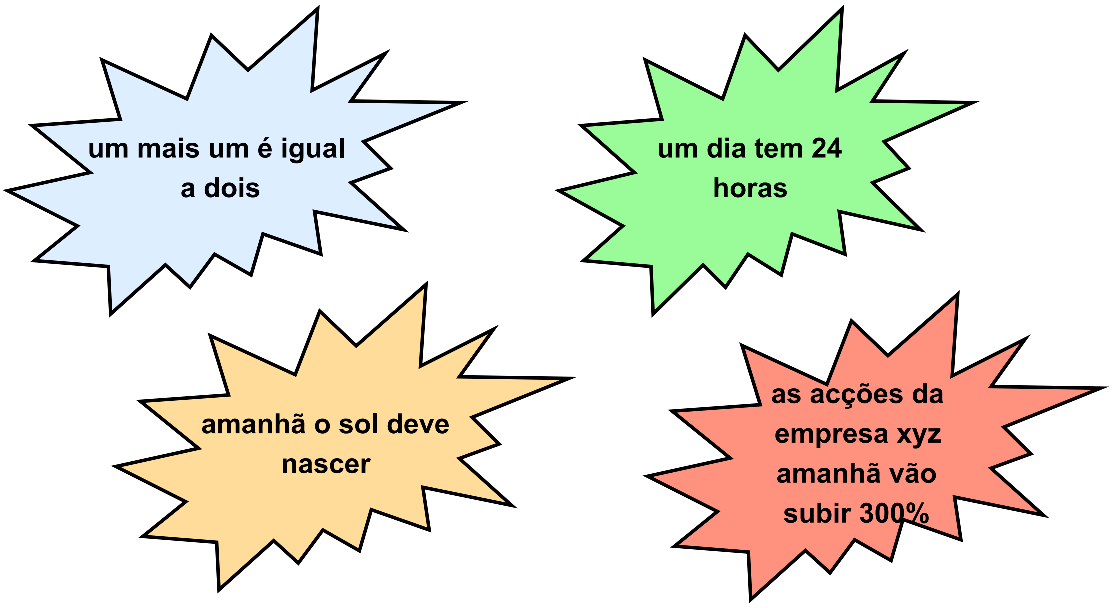
Sistema de Comunicação com codificação da fonte e do canal



I. TEORIA DA INFORMAÇÃO

- Estudo da produção e transferência de informação
- Relevância na informação da mensagem em si e não dos sinais utilizados para a transmitir
- **Informação**: (no contexto das comunicações)
  - "*objecto imaterial útil produzido por uma fonte que tem de ser transmitido para um determinado destino*"

I. TEORIA DA INFORMAÇÃO



I. TEORIA DA INFORMAÇÃO

- Como definir uma **medida de informação** ?
  - relacionada com o grau de incerteza do destinatário relativamente à mensagem que vai receber
  - relacionada com a probabilidade da ocorrência da mensagem
  - vai ser definida como uma função que leva em conta essa probabilidade f(Pi)

I. TEORIA DA INFORMAÇÃO

- Informação própria de uma mensagem X_i :

$$\boxed{I_i = f(P_i)}$$

- Propriedades:

?

$$\text{(i)}\ \ f(P_i) \geq 0 \quad \text{para} \quad 0 \leq P_i \leq 1$$

$$\text{(ii)}\ \ \lim_{P_i \to 1} f(P_i) = 0$$

$$\text{(iii)}\ \ f(P_i) > f(P_j) \quad \text{para} \quad P_i < P_j$$

$$\text{(iv)}\ \ f(P_i P_j) = f(P_i) + f(P_j)$$

I. TEORIA DA INFORMAÇÃO

- Adoptar uma função que satisfaz estas propriedades: $\boxed{-\log_b()}$
- A base adoptada define a unidade de medida de informação
- base=2 na teoria de informação
- logo a unidade correspondente é o *bit*

I. TEORIA DA INFORMAÇÃO

Bit como unidade de medida de informação

O bit é a quantidade de informação necessária para escolher uma entre duas alternativas igualmente prováveis ou, a quantidade de informação contida numa mensagem emitida por uma fonte capaz de emitir apenas duas mensagens distintas e equiprováveis.

Portanto, e por definição, a quantidade de informação, ou informação própria, I_i numa mensagem x_i é dada por:

$$\boxed{I_i \stackrel{def}{=} \log_2 \frac{1}{P_i} \quad bits}$$

I. TEORIA DA INFORMAÇÃO

- Assumir uma fonte que emite uma série de símbolos $X = \{x_1, ..., x_m\}$ com probabilidades $\{P_1.....P_m\}$

- **Entropia**: informação média (por símbolo) gerada pela fonte

$$\boxed{\mathcal{H}(X) \stackrel{def}{=} \sum_{i=1}^{m} P_i\, I_i = \sum_{i=1}^{m} P_i \log_2 \frac{1}{P_i} \quad bits/símbolo}$$

Comunicação de Dados
Licenciatura em Engenharia Informática
Departamento de Informática, Universidade do Minho

I. TEORIA DA INFORMAÇÃO

- Quais os **limites para a entropia** de uma fonte?

- Valor que depende:
  - das probabilidades dos símbolos da fonte e
  - da cardinalidade (m)

$$\boxed{0 \leq \mathcal{H}(X) \leq \log_2 m}$$

I. TEORIA DA INFORMAÇÃO

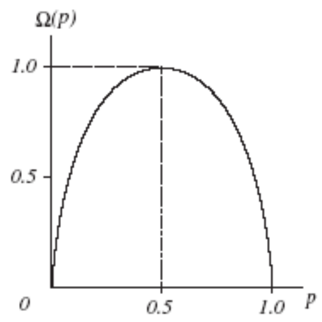
- **Débito de Informação**
  - indica o débito médio de informação por segundo
  - assumindo que a fonte produz r_s símbolos por segundo:

$$\boxed{\mathcal{R} \stackrel{def}{=} r_s \mathcal{H}(X) \quad bits/seg}$$

I. TEORIA DA INFORMAÇÃO

- **Exemplo 1**: Fonte binária (m=2); P_1=p e P_2=1 -p ; entropia?

$$\mathcal{H}(X) = \Omega(p) \stackrel{def}{=} p \log_2 \frac{1}{p} + (1-p) \log_2 \frac{1}{1-p}$$

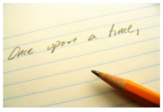


I. TEORIA DA INFORMAÇÃO

- **Exemplo 2**: Fonte emite 2000 símbolos/seg de um alfabeto de 4 símbolos (m=4) com probabilidades:

x_i	P_i	I_i
A	$1/2$	1
B	$1/4$	2
C	$1/8$	3
D	$1/8$	3

- Entropia?
- Débito de informação?

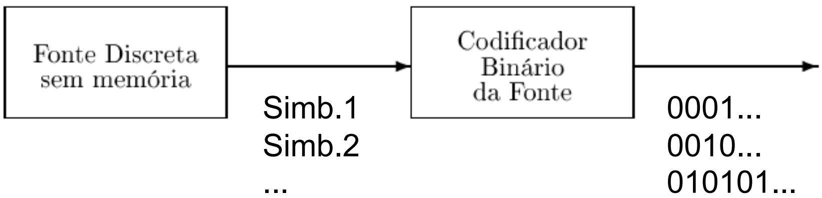


$$\mathcal{H}(X) \;=\; \frac{1}{2}\times 1+\frac{1}{4}\times 2+\frac{1}{8}\times 3+\frac{1}{8}\times 3 \;=\; 1.75 \quad \text{bits/símb}$$

$$\mathcal{R} \;=\; 2000 \times 1.75 \;=\; 3500 \quad \text{bits/seg}$$

$$\mathcal{H}(X) \stackrel{def}{=} \sum_{i=1}^{m} P_i\, I_i \;=\; \sum_{i=1}^{m} P_i \log_2 \frac{1}{P_i} \quad \textit{bits/símbolo}$$

I. TEORIA DA INFORMAÇÃO



- N_i - comprimento da palavra de código correspondente ao símbolo i
- **Comprimento médio do código**:

$$\overline{N} \;=\; \sum_{i=1}^{m} P_i\, N_i \quad \text{dig bin/símbolo}$$

I. TEORIA DA INFORMAÇÃO

- **Rendimento do código**

$$\boxed{\rho = \frac{\mathcal{H}(X)}{\overline{N}} \leq 1}$$

- **Compressão obtida numa codificação**

$$\boxed{c = \frac{N_f - \overline{N}}{N_f} \times 100\ \%}$$

codificação com um **código de comprimento fixo mínimo**

I. TEORIA DA INFORMAÇÃO

- **Como obter códigos?**
  - existem várias alternativas com diferentes desempenhos
  - os códigos necessitam de ser decifráveis (e.g. desigualdade de kraft apresentada na secção códigos óptimos)

$$\boxed{\mathrm{Kr} = \sum_{i=1}^{m} 2^{-N_i} \leq 1}$$

  - melhores códigos -> melhores rendimentos

I. TEORIA DA INFORMAÇÃO

- **Exemplo**: diferentes codificações para a uma fonte que gera quatro símbolos (entropia 1.75 bits/símbolo) – Comprimentos médios e rendimentos dos códigos?

x_i	P_i	Código I	Código II	Código III	Código IV
A	$1/2$	00	0	0	0
B	$1/4$	01	1	01	10
C	$1/8$	10	10	011	110
D	$1/8$	11	11	0111	111
$\overline{N}$		2.0	1.25	1.875	1.75

rendimento 88%

menor que a entropia!!
mas código não decifrável

código em vírgula
melhor que código I

código em árvore
que neste caso
tem rendimento =
100%

I. TEORIA DA INFORMAÇÃO

- **Códigos de Shannon-Fano / *Huffman e outras variantes***
  - Podem ser usados para construir <u>códigos decifráveis</u>
  - Geram códigos de comprimento variável
  - Geram códigos com "*bom*" rendimento
  - Algoritmos para geração de códigos? – vamos analisar unicamente um dos algoritmos mais simples para construção de códigos deste tipo
    - » Códigos de *Shannon-Fano*

I. TEORIA DA INFORMAÇÃO

- **Códigos de Shannon-Fano** (nota: em alguma bibliografia estes códigos são também por vezes associados aos Códigos de Huffman, mas na realidade estes últimos são uma evolução dos primeiros, e usam uma técnica distinta – corrigir na pp. 208 -)

(1) Ordenar os símbolos por ordem decrescente de probabilidade;

(2) Dividir o conjunto assim ordenado em dois subconjuntos tais que a soma das probabilidades em cada um deles seja o mais aproximadamente possível igual a metade da soma das probabilidades no conjunto anterior. Manter a ordenação.

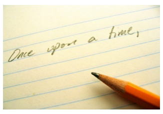
(3) O dígito seguinte do código binário dos símbolos do primeiro dos sub-conjuntos é o **0** e o dos do outro é o **1**;

(4) Se os sub-conjuntos contêm um só elemento, a codificação terminou para esses sub-conjuntos;

(5) Repetir para cada um dos restantes sub-conjuntos (passo 2.)

I. TEORIA DA INFORMAÇÃO

Códificação da fonte - **Exemplo**: aplicar o algoritmo anterior para codificar a fonte com oito símbolos (m=8)



x_i	A	B	C	D	E	F	G	H
P_i	0.50	0.15	0.15	0.08	0.08	0.02	0.01	0.01

Entropia?

Código?

Comprimento médio?

x_i	P_i	Passos de codificação 1	2	3	4	5	6	Código
A	0.50	0						0
B	0.15	1	0	0				100
C	0.15	1	0	1				101
D	0.08	1	1	0				110
E	0.08	1	1	1	0			1110
F	0.02	1	1	1	1	0		11110
G	0.01	1	1	1	1	1	0	111110
H	0.01	1	1	1	1	1	1	111111
$\mathcal{H}(X) = 2.15$								$\overline{N} = 2.18$

I. TEORIA DA INFORMAÇÃO

– Codificação por blocos

- agrupar símbolos da fonte e proceder à sua codificação
- daí a noção de "bloco"
- blocos de K símbolos
- normalmente leva a melhorias no rendimento do código...
- ... e na compressão obtida

Comunicação de Dados
Licenciatura em Engenharia Informática
Departamento de Informática, Universidade do Minho

I. TEORIA DA INFORMAÇÃO

– Exemplo:

- Fonte que emite símbolos de um alfabeto X com apenas dois símbolos X={A,B}; $P_A = 0.8$ e $P_B = 0.2$. (entropia = 0.722 bits/símbolo)
- Se se codificarem dois símbolos de cada vez temos um novo alfabeto Y={AA,AB,BA,BB}
- $P_{ij} = P_i * P_j$
  - por se tratar de uma fonte sem memória
  - ou seja, símbolos estatisticamente independentes
- código de *Shannon-Fano* para Y (blocos de K=2)?

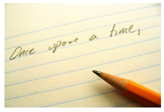
I. TEORIA DA INFORMAÇÃO

- Tabela das probabilidades/palavras de código

Código?

Comprimento médio?

y_i	P_{y_i}	Código
AA	0.64	0
AB	0.16	11
BA	0.16	100
BB	0.04	101
$\overline{N}_2$		1.56



- para uma codificação K=1 comprimento médio do código era?
- logo ....

I. TEORIA DA INFORMAÇÃO

$$\overline{N}_2 = 1.560 \ \ dígitos \ binários/símbolo_Y$$

$$\overline{N} = \frac{\overline{N}_2}{2} = 0.780 \quad dígitos \ binários/símbolo_X$$

y_i	P_{y_i}	Código
AA	0.64	0
AB	0.16	11
BA	0.16	100
BB	0.04	101
$\overline{N}_2$		1.56

Rendimento e compressão obtidos com (K=2) ?

$$\boxed{\rho = \frac{\mathcal{H}(X)}{\overline{N}} = \frac{0.722}{0.780} = 0.926} \qquad \boxed{c = \frac{N_f - \overline{N}}{N_f} \times 100 = \frac{1-0.780}{1} = 22 \ \%}$$

Rendimento e compressão obtidos com (K=1) (sem blocos) ?

0.722 **0%**

I. TEORIA DA INFORMAÇÃO

- **Rendimento e compressão obtidos com (K=3) ?**
  - experimentar.... melhor rendimento e compressão?

- **O que está a acontecer aos comprimentos médios dos códigos?**
  - à medida que K aumenta $\overline{N}$ tem tendência a diminuir; matematicamente isto é expresso na seguinte expressão:

$$\boxed{\mathcal{H}(X) \leq \overline{N} < \mathcal{H}(X) + \frac{1}{K}}$$

I. TEORIA DA INFORMAÇÃO

Um dos teoremas fundamentais da Teoria da Informação

Toda a fonte de informação caracterizada por um valor da entropia $\mathcal{H}(X)$ bits/símbolo, pode ser codificada em binário de tal forma que o comprimento médio do código, $\overline{N}$, é limitado por

$$\mathcal{H}(X) \leq \overline{N} \leq \mathcal{H}(X) + \epsilon$$

Na codificação por blocos está-se a fazer $\epsilon = \frac{1}{K}$.

- código ideal será aquele em que ϵ=0; na prática nem sempre é possível sendo satisfatório um código que possua bom rendimento

I. TEORIA DA INFORMAÇÃO

Fontes com memória

- Por vezes a probabilidade de emissão de um determinado símbolo depende dos símbolos anteriormente emitidos
- Fontes com memória de primeira ordem
    - fonte só se *lembra* do símbolo precedente
    - noção de probabilidade condicional
    - probabilidade de um símbolo ter ocorrido depois de um outro símbolo da fonte

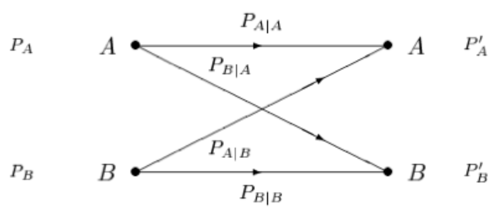
Comunicação de Dados
Licenciatura em Engenharia Informática
Departamento de Informática, Universidade do Minho

I. TEORIA DA INFORMAÇÃO

Fontes com memória de primeira ordem

- **P (x_i | x_j)** - probabilidade de o símbolo x_i ser escolhido depois do símbolo x_j
- **P (x_i x_j)** - se for interpretado como a probabilidade da ocorrência de x_j e posteriormente x_i **:**

$$P(x_i\, x_j) = P(x_j) * P(x_i \mid x_j)$$ ← ...para a construção da tabela de blocos de símbolos



$$P'_A = P_A \cdot P_{A|A} + P_B \cdot P_{A|B}$$
$$P'_B = P_A \cdot P_{B|A} + P_B \cdot P_{B|B}$$

I. TEORIA DA INFORMAÇÃO

Fontes com memória

Como se calcula a entropia para fontes com memória de primeira ordem?

- Entropia condicional relativamente ao símbolo x_j

$$\boxed{\mathcal{H}(X|x_j) \stackrel{def}{=} \sum_{i=1}^{m} P(x_i|x_j)\, \log_2 \frac{1}{P(x_i|x_j)}}$$

- Entropia real de uma fonte de primeira ordem

$$\boxed{\mathcal{H}(X) = \sum_{j=1}^{m} P(x_j)\, \mathcal{H}(X|x_j)}$$

I. TEORIA DA INFORMAÇÃO

Fontes com memória

- Quando as probabilidades condicionais de uma fonte com memória reduzem significativamente o valor da entropia face ao seu valor máximo:
  - ***a fonte diz-se redundante***

- possibilidade de codificar a fonte com códigos mais eficientes (i.e. comprimento médio do código próximo da entropia real da fonte)

I. TEORIA DA INFORMAÇÃO

- Processos de **codificação da fonte** estudados no contexto da Teoria da Informação levam em conta o grau de incerteza da fonte para tentar:
  - **retirar a redundância** produzida pela fonte
  - daí se designarem por mecanismos de **compressão da fonte**

- ... Além da codificação da fonte a Teoria da Informação também aborda questões relacionadas com o **canal de comunicação**.... e.g. Capacidade do canal e Codificação do Canal

Comunicação de Dados
Licenciatura em Engenharia Informática
Departamento de Informática, Universidade do Minho

I. TEORIA DA INFORMAÇÃO

Transmissão de Informação: o canal

(secção 8.4 da sebenta)

- aborda a transmissão de informação em canais de comunicação
- *não iremos abordar esta parte da matéria em detalhe...*
- .... mas iremos *mais tarde* utilizar a fórmula da Capacidade do Canal que é demonstrada nessa secção

I. TEORIA DA INFORMAÇÃO

Transmissão de Informação: o canal

- Capacidade do Canal

$$\boxed{C = B_T \log_2\left(1 + \frac{S}{N}\right) \quad bits/s}$$

Correcção - p. 210:

A codificação por blocos conduz tendencialmente a um código óptimo, isto é, com $K \to \infty$ tem-se $\boxed{\overline{N}} \to \mathcal{H}(X)$, $\rho \to 1$ e $c \to c_{max}$. De facto, para a codificação por blocos, a desigualdade 8.13 escreve-se

$$\boxed{K * \mathcal{H}(X) \leq \overline{N}_K < K * \mathcal{H}(X) + 1}$$

donde, dividindo por K e tendo em atenção que a entropia da fonte não se altera com a codificação, se obtém

$$\mathcal{H}(X) \leq \frac{\overline{N}_K}{K} < \mathcal{H}(X) + \frac{1}{K}$$

ou, visto que $\overline{N} = \frac{\overline{N}_K}{K}$,

$$\mathcal{H}(X) \leq \overline{N} < \mathcal{H}(X) + \frac{1}{K}$$

Podemos agora enunciar um dos teoremas fundamentais da Teoria da Informação embora não procedamos à sua demonstração geral:

Correcção - p. 208:

Corrigir títulos da secção e exemplo:

Secção 8.2.3 – Códigos de *Shannon-Fano*

Exemplo 8.4 – Codificação de *Shannon-Fano*