

Teoria da Informação

Capítulo I - Introdução

Paulo de Carvalho, Rui Pedro Paiva

Departamento de Engenharia Informática
Faculdade de Ciências e Tecnologia da Universidade de Coimbra

Sumário

- Teoria da Informação: Porquê?
 - Compressão
 - Códigos de Recuperação de Erros
 - Segurança Informática
 - Aprendizagem Computacional (Machine Learning)
- Leitura Aconselhada:
 - Sayood Cap. I
 - MacKay Cap. I e II

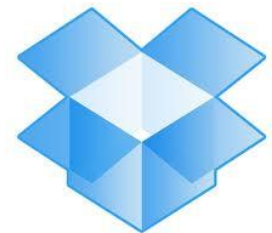
Compressão de Dados, Porquê?

- Diminuição dos requisitos de armazenamento
- Uso adequado da largura de banda disponível
- Dados Multimédia
 - Cloud data: drop-box, iCloud,...
 - Aplicações médicas
 - Web: Google, youtube, facebook,...
 - Imagens de satélite
 - Jornais on-line (público, diariodigital, IEEE, etc)
 - Bases de dados Multimédia (e.g. aplicações móveis; música)
 - Vídeo conferência

You Tube



iCloud



Compressão de Dados, Porquê?

- Armazenamento:
 - Hospital com 500 camas/160 000 estudos por ano (3.5 Tb)

Modalidade	Matriz	Bytes/pixel	MB/Estudo
CR	2048x2580	2	20
CT	512x512	2	30
MRI	256x256	2	25
US	512x512	3	10
Mamografia	4096x6144	2	192
Angiografia	1024x1024	2	30
Fluoroscopia	1024x1024	1	10

Compressão de Dados, Porquê?

- Armazenamento:
 - Televisão de baixa resolução 512x512 pixels, 3 canais de cor a 8 bits – 6.3 Mb/imagem



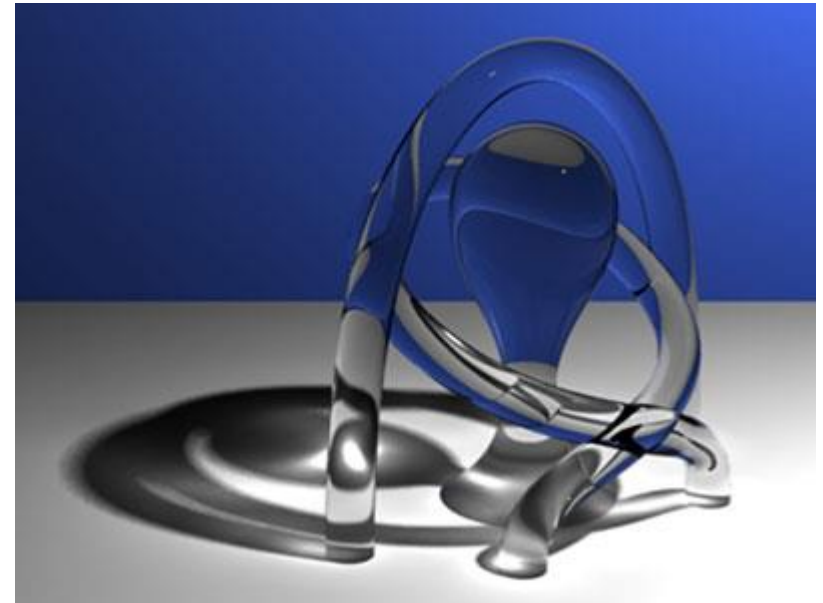
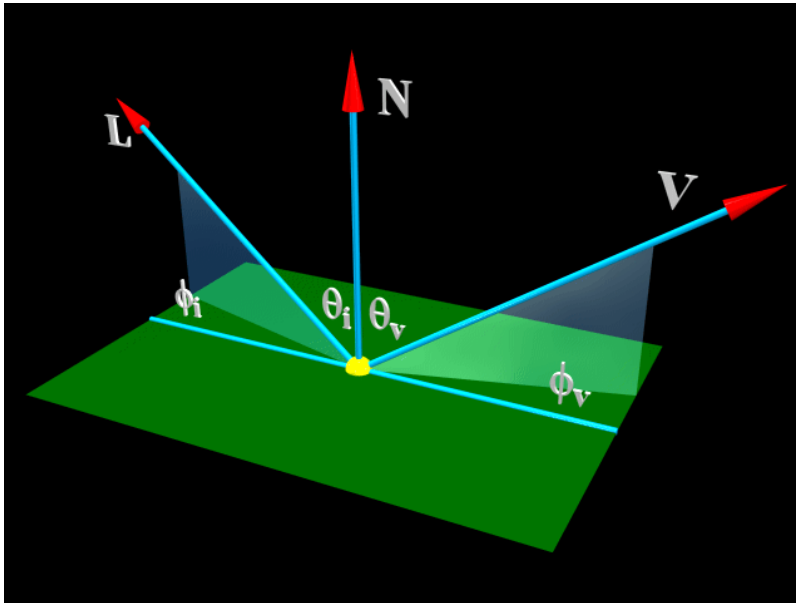
Compressão de Dados, Porquê?

- Armazenamento:
 - LANDSAT Thematic Mapper: 6000x6000 pixels/ banda espectral/8 bits por banda/ 6 bandas – 1700 Mb/imagem



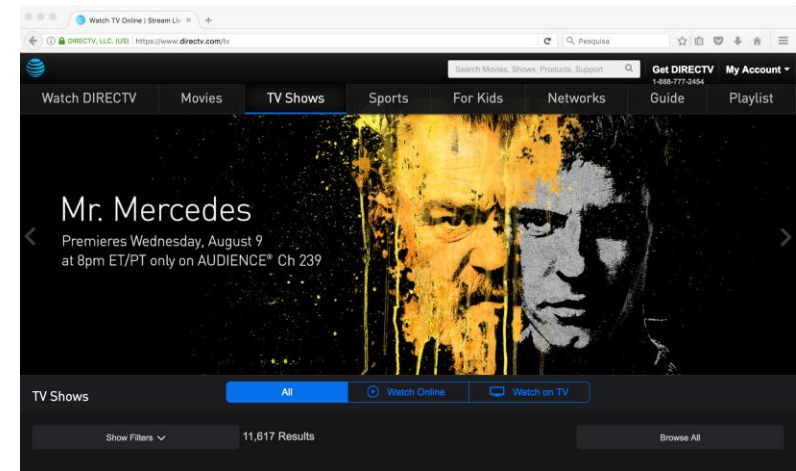
Compressão de Dados, Porquê?

- Armazenamento:
 - Computação gráfica – representação espectral de um quadro (e.g. BRDFs) – muitos Mb/imagem



Compressão de Dados, Porquê?

- Vídeo
 - 640x480 pixels (3 canais de cor a 8 bits) x 30 imagens /segundo: 221 Mb/s
 - CIF (vídeo-conferência) – 360x288 pixels - na ordem dos 70Mb/s
 - CCIR(TV: 720x576): 300 Mb/s
 - StandardHDTV (1260x720 pixels X 24 b/p X 80 imagens/s): 1.3 Gb/s (Full HD → ainda mais)



Compressão destrutiva e não destrutiva

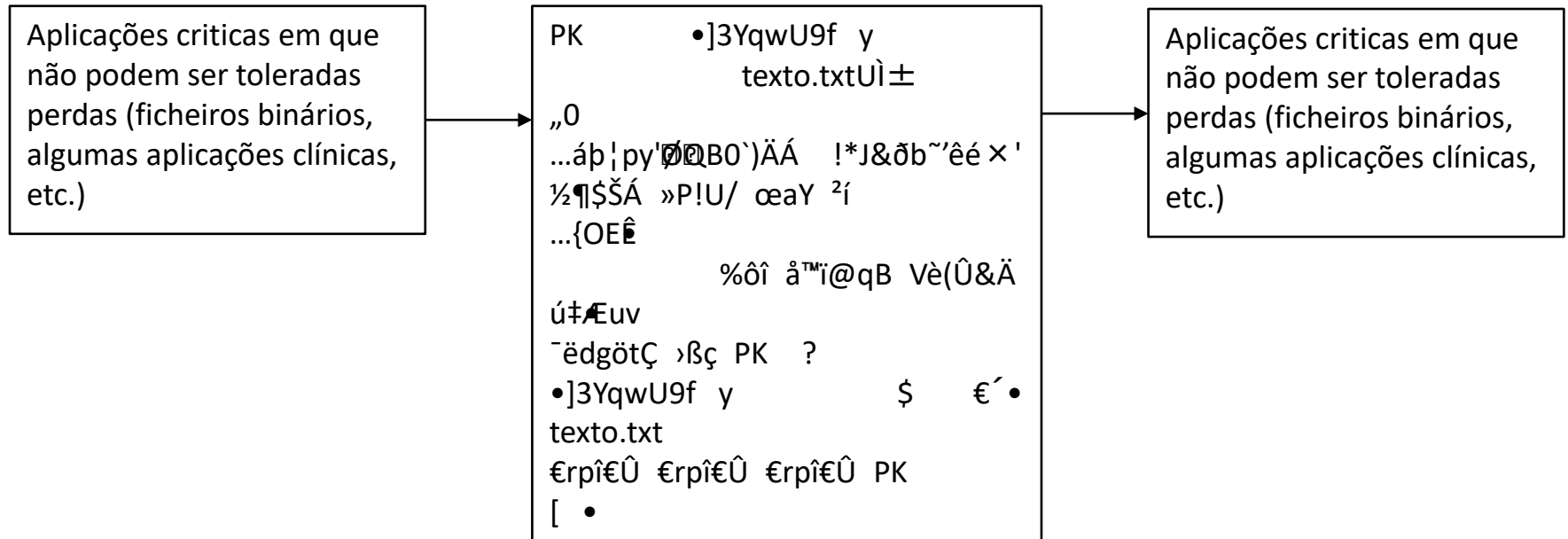
- A ideia: Identificação e remoção da **redundância**/irrelevância (destrutiva) da fonte.
- Tipos de compressão:
 - Não destrutiva: a reconstrução é exacta
 - Destrutiva: a reconstrução é aproximada (exploração das limitações dos sistemas perceptuais)

Original → Comprimido → Descomprimido
110101101 → 10101 → 110101101

Original → Comprimido → Descomprimido
110101101 → 101 → 110110101

Compressão destrutiva e não destrutiva

- Texto, ficheiros binários, etc
 - Tipicamente compressão não destrutiva



Compressão destrutiva e não destrutiva

- Imagem fotográfica
 - Tipicamente compressão destrutiva (e.g., JPEG)



(a) Imagem original

(b) $Q = 75$ (factor de qualidade típico)




(c) $Q = 25$

(d) $Q = 5$

© Ze-Nian Li 2014, p. 34

Compressão Não Destrutiva

- Codificação de eventos de elevada probabilidade com poucos bits.
- Codificação de eventos improváveis com um número superior de bits

A		
	50%	00
	9%	10
	40%	11

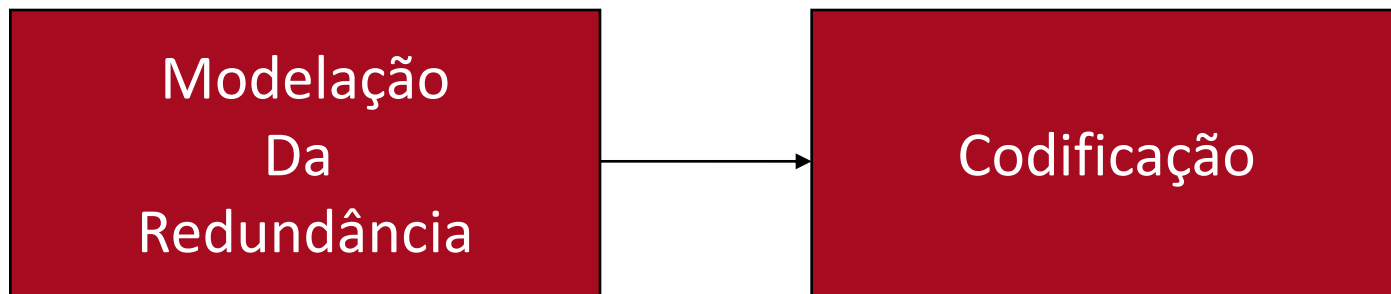
Necessários Códigos Variáveis
VLC (Variable Length Code)

Compressão Não Destrutiva

- Qual é o menor comprimento médio do melhor código?
- Como obter o melhor código possível?
 - A primeira pergunta a que iremos responder na cadeira!

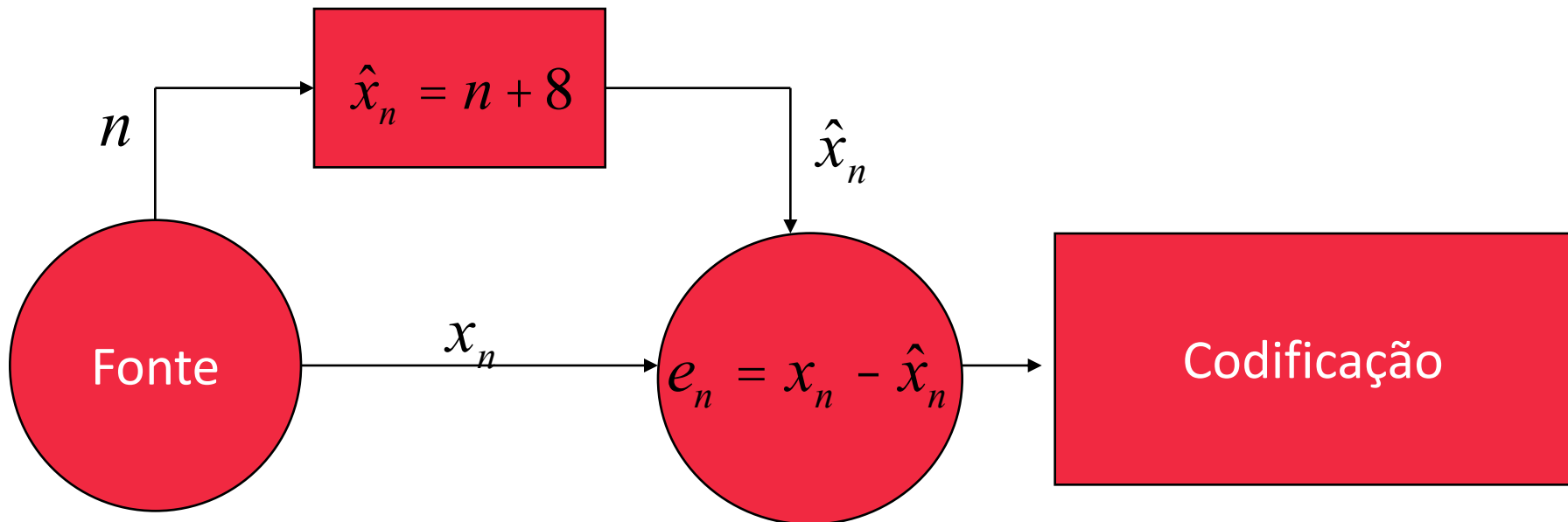
Modelo de Compressão

- Codificação da fonte
 - A redundância, normalmente, não é imediatamente evidente/disponível



- Tipos de modelos (mais frequentes)
 - Modelação do Processo (ou Física)
 - Modelação Preditiva
 - Modelação Estatística

Exemplo 1 (Modelação Física)



9	11	11	11	14	13	15	17	16	17	20	21
---	----	----	----	----	----	----	----	----	----	----	----

0	1	0	-1	1	-1	0	1	-1	-1	1	1
---	---	---	----	---	----	---	---	----	----	---	---

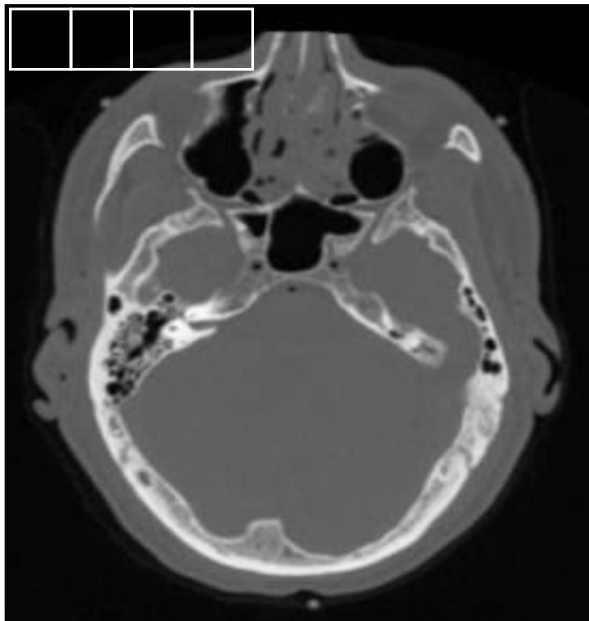
Número de símbolos distintos do alfabeto: 3 \Rightarrow 2

bits/símbolo

$12 \cdot 2 = 24$ bits (mensagem)

Exemplo 2 (Modelação Preditiva - Aplicações à Imagem)

- Redundância Espacial
 - Exemplo: Pixels vizinhos são semelhantes



Exemplo 2 (Modelação Preditiva - Aplicações à Imagem)

- PNG: Método de Compressão

- Modelos de previsão


- Em cada linha, cada **byte** é previsto com base nos valores de bytes anteriores (explora correlação espacial entre amostras consecutivas)

Bytes

c	b
a	x

- Tipo de modelo de previsão

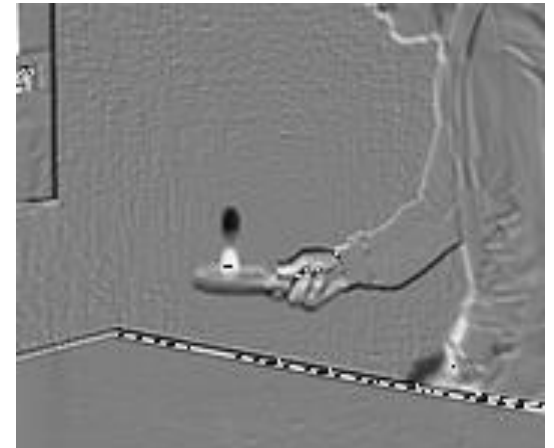
Type	Name	Filter Function
0	None	$\text{Filt}(x) = \text{Orig}(x)$
1	Sub	$\text{Filt}(x) = \text{Orig}(x) - \text{Orig}(a)$
2	Up	$\text{Filt}(x) = \text{Orig}(x) - \text{Orig}(b)$
3	Average	$\text{Filt}(x) = \text{Orig}(x) - \text{floor}((\text{Orig}(a) + \text{Orig}(b)) / 2)$
4	Paeth	$\text{Filt}(x) = \text{Orig}(x) - \text{PaethPredictor}(\text{Orig}(a), \text{Orig}(b), \text{Orig}(c))$



```
p = a + b - c
pa = abs(p - a)
pb = abs(p - b)
pc = abs(p - c)
if pa <= pb and pa <= pc then Pr = a
else if pb <= pc then Pr = b
else Pr = c
return Pr
```

Exemplo 3 (Modelação Preditiva - Aplicações ao Vídeo)

- Redundância Temporal
 - Exemplo: Frames adjacentes são semelhantes
 - Diferença entre duas frames consecutivas → gama de valores reduzida → menos bits



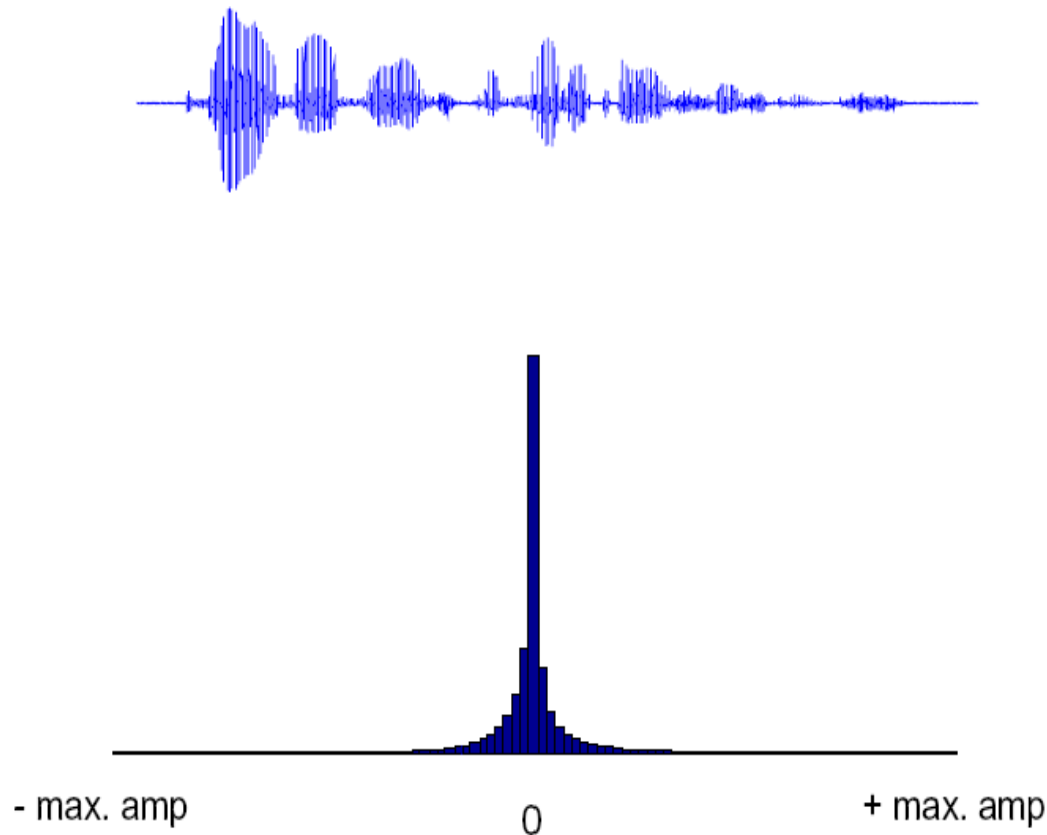
Exemplo 4 (Modelação Estatística)

- Fonte:
“akbarayarankarraykankfarkfaarkfaaarkaway”
- Análise estatística
 - **Histograma** de símbolos (número de ocorrências)
 - Símbolos mais frequentes → menos bits (e vice-versa)

Símbolo	Ocorrência	Código
A	16	1
K	7	001
B	1	01100
F	3	0100
N	2	0111
R	7	000
W	1	01101
Y	1	0101

Exemplo 4 (Modelação Estatística – Aplicações ao Áudio)

- Redundância Estatística (na voz)



Criptografia

- **Confidencialidade - Manter os dados secretos**
 - Encriptação de dados - garantia de que os dados só podem ser decodificados pelo receptor autorizado
 - Exemplo: dados financeiros, documentos confidenciais, etc.
- **Integridade**
 - Garantia de que os dados não sofreram alteração
 - Exemplo: dados forenses
- **Autenticação**
 - Saber origem dos dados / emissor
 - Exemplo: transferência bancária
- **Não repúdio**
 - Garantia de origem dos dados
 - Exemplo: evitar que alguém não assuma a origem dos dados

Criptografia

- Tipos de algoritmos
 - Chave simétrica (privada)
 - Chave assimétrica (pública e privada)
 - Funções de Hashing
- Como?
 - É a segunda pergunta a que iremos responder!