# Teoria da Informação (#4)

Classes de códigos, desigualdade de Kraft, código óptimo, Shannon-Fano, Huffman, Huffman adaptativo

Miguel Barão



### O que é um código?

# Código

Singular e não singular Univocamente descodificável Instantaneo

# Classes de códigos

### Códigos instantaneos

Desigualdade de Kraft Códigos óptimos Shannon-Fano Grupos de símbolos Penalização em L(C)

#### Huffman

# O que é um código?

# Definição (Código)

Um código é uma aplicação  $\mathcal{C}:\mathcal{X}\to\mathcal{D}^*$ , em que

- $\blacksquare$   $\mathcal{X}$  é um alfabeto
- lacksquare  $\mathcal{D}^*$  é o conjunto das strings finitas de símbolos de um alfabeto  $\mathcal{D}$

### O que é um código?

# Definição (Código)

Um código é uma aplicação  $\mathcal{C}:\mathcal{X}\to\mathcal{D}^*$ , em que

- $\mathbf{Z}$  é um alfabeto
- lacksquare é o conjunto das strings finitas de símbolos de um alfabeto  $\mathcal D$
- $\mathbf{C}(x)$  é a palavra de código correspondente a x
- I(x) é o comprimento da palavra de código C(x)
- *L*(*C*) é o comprimento médio do código *C*

# Definição (Código)

Um código é uma aplicação  $\mathcal{C}:\mathcal{X}\to\mathcal{D}^*$ , em que

- $\blacksquare$   $\mathcal{X}$  é um alfabeto
- lacksquare  $\mathcal{D}^*$  é o conjunto das strings finitas de símbolos de um alfabeto  $\mathcal{D}$
- C(x) é a palavra de código correspondente a x
- I(x) é o comprimento da palavra de código C(x)
- *L*(*C*) é o comprimento médio do código *C*

# Exemplo

X	p(x)	C(x)	I(x)	$L(C) = \sum p(x)I(x)$
Α	0.4	00	2	
В	0.3	101	3	x∈X
C	0.3	110	3	= 2.6 bits

# Que propriedades deve um código satisfazer?

# Definição (Código não singular)

Um código é n $\tilde{\text{no}}$  singular se símbolos diferentes têm palavras de código diferentes, i.e.

$$x_i \neq x_j \quad \Rightarrow \quad C(x_i) \neq C(x_j)$$

### Definição (Código não singular)

Um código é não singular se símbolos diferentes têm palavras de código diferentes, *i.e.* 

$$x_i \neq x_j \Rightarrow C(x_i) \neq C(x_j)$$

Só garante a descodificação de símbolos isolados.

### Exemplo

O código

$$\begin{array}{c|c} x & C(x) \\ \hline A & 0 \\ B & 00 \end{array}$$

é um código não singular. No entanto a string "ABBA", codificada como "000000", não é descodificável univocamente.

### Código univocamente descodificável

### Definição (Extensão de um código)

A extensão  $C^*$  de um código C é um novo código que codifica uma sequência de símbolos usando a sequência das respectivas palavras de código:

$$C^*(x_1x_2\cdots x_n)=C(x_1)C(x_2)\cdots C(x_n)$$

### Definição (Extensão de um código)

A extensão  $C^*$  de um código C é um novo código que codifica uma sequência de símbolos usando a sequência das respectivas palavras de código:

$$C^*(x_1x_2\cdots x_n)=C(x_1)C(x_2)\cdots C(x_n)$$

### Definição (Código univocamente descodificável)

Um código é univocamente descodificável se a sua extensão é não singular.

I.e., cada string pode apenas ter sido gerada por uma única mensagem.

# Código univocamente descodificável

### Exemplo

$$\begin{array}{c|cccc} x & C(x) \\ \hline A & 001 \\ B & 00 \\ C & 11 \\ D & 110 \\ \end{array}$$

- É univocamente descodificável.
- Pode ser necessário analisar toda a sequência para descodificar o primeiro símbolo.
- Não é praticável quando a string é grande ou quando não termina (ex: streaming de radio pela internet).

#### Exemplo

Descodifique a string:

001111111111111100000001

# Código instantaneo (ou de prefixo)

# Definição (Código instantaneo)

Diz-se que um código C é um código instantaneo ou código de prefixo se nenhuma palavra de código é prefixo de outra.

Um código instantaneo pode ser descodificado sem referência às palavras de código futuras.

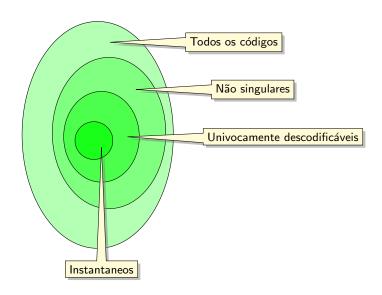
# Código instantaneo (ou de prefixo)

# Definição (Código instantaneo)

Diz-se que um código C é um código instantaneo ou código de prefixo se nenhuma palavra de código é prefixo de outra.

Um código instantaneo pode ser descodificado sem referência às palavras de código futuras.

Exemplo		
		A string
	C(x)	0100110111001
Α	01	/ :
В	001	é imediatamente reconhecida como
C	111	01,001,10,111,001
D	10	02,002,20,222,002
		ou seja ABDCB

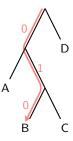


# Exemplos de códigos

E	Exemplo				
	X	Singular	Não singular	Univ. descod.	Instantaneo
	Α	0	0	10	00
	В	0	00	00	10
	C	1	000	11	111
	D	1	0000	110	110

# Como construir um código instantaneo?

Um código instantaneo pode ser construído desenhando uma árvore e seleccionando como palavras de código o caminho desde a raiz até às folhas.



X	C(x)
Α	00
В	010
C	011
D	1

#### Os símbolos estão nas folhas da árvore

Repare que a restrição "nenhuma palavra de código é prefixo de outra" obriga a que nenhum símbolo possa ser definido num nó da árvore.

### Construção de códigos instantaneos

Dados os comprimentos I(x) das palavras de código, será que existe um código instantaneo que satisfaz esses comprimentos?

# Teorema (Desigualdade de Kraft)

 $\acute{E}$  possível construir um código instantaneo com palavras de código de comprimento I(x) se e só se

$$\sum_{x \in \mathcal{X}} 2^{-l(x)} \le 1.$$

# Desigualdade de Kraft

# Demonstração.

■ Seja I<sub>max</sub> o tamanho da maior palavra de código.

### Demonstração.

- lacksquare Seja  $I_{\max}$  o tamanho da maior palavra de código.
- Qualquer palavra de código de comprimento I(x) é prefixo de  $2^{l_{\max}-I(x)}$  palavras (não usadas) no nível  $l_{\max}$ .



### Demonstração.

- Seja I<sub>max</sub> o tamanho da maior palavra de código.
- Qualquer palavra de código de comprimento I(x) é prefixo de  $2^{l_{max}-I(x)}$  palavras (não usadas) no nível  $l_{max}$ .



■ Podem existir até 2<sup>l</sup>max palavras de código no nível l<sub>max</sub>. Então

$$\sum_{x \in \mathcal{X}} 2^{l_{\mathsf{max}} - l(x)} \leq 2^{l_{\mathsf{max}}} \qquad \Leftrightarrow \qquad \sum_{x \in \mathcal{X}} 2^{-l(x)} \leq 1.$$

12/ 27

### Códigos óptimos

- Considera-se o conjunto de todos os códigos instantaneos (i.e., satisfazem a desigualdade de Kraft).
- Códigos diferentes têm comprimentos médios diferentes.

### **Problema**

Qual o código C que tem o menor comprimento médio L(C)?

### Códigos óptimos

- Considera-se o conjunto de todos os códigos instantaneos (i.e., satisfazem a desigualdade de Kraft).
- Códigos diferentes têm comprimentos médios diferentes.

#### **Problema**

Qual o código C que tem o menor comprimento médio L(C)?

- Sabemos construir um código instantaneo desenhando uma árvore.
- Falta saber que posição cada símbolo ocupa na árvore.
- Um código óptimo pode ser obtido calculando os comprimentos óptimos I(x) das palavras de código.
  - Os símbolos mais frequentes devem ter comprimentos menores.
  - **E**xistem vários códigos possíveis para os mesmos comprimentos I(x).

#### **Problema**

Minimizar L(C) com a restrição do código resultante ser um código instantaneo.

■ Funcional a optimizar:

$$L(C) = \sum_{x} p(x) I(x).$$

■ Restrição:

$$\sum_{x} 2^{-I(x)} \leq 1.$$

Usando o método dos multiplicadores de Lagrange obtém-se o funcional modificado:

$$J = \sum_{x} p(x)I(x) + \lambda \left( \underbrace{\sum_{x} 2^{-I(x)} - 1}_{\text{restricão}} \right).$$

Derivando J em ordem aos comprimentos I(x) e ao multiplicador de Lagrange  $\lambda$ , e igualando a zero, obtêm-se os pontos de estacionariedade

$$\frac{\partial J}{\partial I(x_j)} = p(x_j) - \lambda 2^{-I(x_j)} \log_e 2 = 0 \tag{1}$$

$$\frac{\partial J}{\partial \lambda} = \sum_{x} 2^{-l(x)} - 1 = 0 \tag{2}$$

Da equação (1) resulta que

$$I(x_j) = -\log_2 p(x_j) + \log_2(\lambda \log_e 2)$$
(3)

Substituindo (3) em (2), e resolvendo em ordem a  $\lambda$ , obtém-se  $\lambda=1/\log 2$ . Substituindo este  $\lambda$  em (3) obtém-se finalmente

$$I(x_j) = -\log_2 p(x_j). \tag{4}$$

■ Se p(x) é uma potência negativa de 2, então

$$L(C) = \sum_{x} p(x)I(x) = \sum_{x} p(x)(-\log p(x)) = H(X).$$

- Se as probabilidades p(x) não são potências negativas de 2, então os comprimentos  $I(x) = -\log_2(p(x))$  não são números inteiros.
  - ▶ Nesse caso podem usar-se comprimentos imediatamente superiores

$$I(x) = \lceil -\log_2 p(x) \rceil.$$

- Estes novos comprimentos satisfazem a desigualdade de Kraft.
- O comprimento médio satisfaz

$$H(X) \le L(C) < H(X) + 1.$$

O código obtido chama-se código de Shannon-Fano e é subóptimo.

### Exemplo

Uma fonte sem memória gera símbolos do alfabeto  $\mathcal{X} = \{A, B, C\}$  com probabilidadades  $\{0.25, 0.25, 0.5\}$ , respectivamente.

O código Shannon-Fano é:

$$L(C) = 1.5 \text{ bits}$$
  
 $H(X) = 1.5 \text{ bits}$   
 $1.5 \le L(C) < 2.5$ 

O código é óptimo.

### Exemplos de códigos Shannon-Fano

### Exemplo

Uma fonte sem memória gera símbolos do alfabeto  $\mathcal{X} = \{A, B, C, D\}$  com probabilidadades  $\{0.1, 0.2, 0.3, 0.4\}$ , respectivamente.

O código Shannon-Fano é:

X	p(x)	$-\log p(x)$	I(x)	C(x)
Α	0.1	3.3219	4	0000
В	0.2	2.3219	3	001
C	0.3	1.7370	2	01
D	0.4	1.3219	2	10

$$L(C) = 2.4 \text{ bits}$$
  
 $H(X) = 1.8464 \text{ bits}$   
 $1.8464 \le L(C) < 2.8464$ 

O código não é óptimo.

#### Exemplo

Uma fonte sem memória gera símbolos do alfabeto  $\mathcal{X} = \{A, B, C, D\}$  com probabilidadades  $\{0.1, 0.2, 0.3, 0.4\}$ .

É possível construir um código de Shannon-Fano com comprimento médio mais perto de H(X) do que o obtido no exemplo anterior.

Para o efeito, agrupam-se vários símbolos e constrói-se um código para esses grupos (que são os "novos" símbolos).

y	p(y)	I(y)
AA	0.01	7
AB	0.02	6
AC	0.03	6
AD	0.04	5
BA	0.02	6
BB	0.04	5
:	:	
DD	0.16	3

$$L(C) = \frac{\sum_{y} p(y)I(y)}{2} = 2.155 \text{ bits}$$

Agrupando 2 símbolos obtém-se um comprimento médio

$$H(X) \leq L(C) < H(X) + \frac{1}{2}$$

### Código de Shannon-Fano sobre grupos de símbolos

Agrupando n símbolos para formar "novos" símbolos, obtém-se um comprimento médio no intervalo

$$H(X_1, \dots, X_n) \leq \underbrace{E[I(X_1, \dots, X_n)]}_{\text{comprimento médio}} < H(X_1, \dots, X_n) + 1$$

### Código de Shannon-Fano sobre grupos de símbolos

Agrupando n símbolos para formar "novos" símbolos, obtém-se um comprimento médio no intervalo

$$H(X_1, \dots, X_n) \leq \underbrace{E[I(X_1, \dots, X_n)]}_{\text{comprimento médio}} < H(X_1, \dots, X_n) + 1$$

Como os símbolos são i.i.d. (fonte sem memória):

$$H(X_1,\ldots,X_n)=nH(X).$$

Agrupando n símbolos para formar "novos" símbolos, obtém-se um comprimento médio no intervalo

$$H(X_1, \dots, X_n) \leq \underbrace{E[I(X_1, \dots, X_n)]}_{\text{comprimento médio}} < H(X_1, \dots, X_n) + 1$$

Como os símbolos são i.i.d. (fonte sem memória):

$$H(X_1,\ldots,X_n)=nH(X).$$

Substituindo em cima obtém-se

$$nH(X) \leq E[I(X_1,\ldots,X_n)] < nH(X) + 1.$$

Agrupando n símbolos para formar "novos" símbolos, obtém-se um comprimento médio no intervalo

$$H(X_1, \dots, X_n) \leq \underbrace{E[I(X_1, \dots, X_n)]}_{\text{comprimento médio}} < H(X_1, \dots, X_n) + 1$$

Como os símbolos são i.i.d. (fonte sem memória):

$$H(X_1,\ldots,X_n)=nH(X).$$

Substituindo em cima obtém-se

$$nH(X) \leq E[I(X_1, \ldots, X_n)] < nH(X) + 1.$$

Dividindo por n obtém-se

o comprimento médio por símbolo individual

$$H(X) \leq \frac{E[I(X_1,\ldots,X_n)]}{n} < H(X) + \frac{1}{n}.$$

### Aplicação do código numa fonte diferente

#### **Problema**

- Uma fonte sem memória gera símbolos com probabilidades p(x).
- Constrói-se um código Shannon-Fano usando probabilidades q(x) de uma fonte diferente.
- Ao aplicar o código à fonte p(x), qual vai ser a penalização no comprimento médio L(C)?

#### **Problema**

- Uma fonte sem memória gera símbolos com probabilidades p(x).
- Constrói-se um código Shannon-Fano usando probabilidades q(x) de uma fonte diferente.
- Ao aplicar o código à fonte p(x), qual vai ser a penalização no comprimento médio L(C)?

A penalização será a diferença entre o comprimento médio e a entropia da fonte. Isto é,

$$\begin{split} L(C) - H(X) &= \sum_{x} p(x) \lceil -\log_2 q(x) \rceil + \sum_{x} p(x) \log_2 p(x) \\ &\geq \sum_{x} p(x) \big( -\log_2 q(x) \big) + \sum_{x} p(x) \log_2 p(x) \\ &= \sum_{x} p(x) \log \frac{p(x)}{q(x)} \quad \text{(Kullback-Leibler)}. \end{split}$$

# Código de Huffman

- Requesitos:
  - ▶ Conhecer a priori as probabilidades p(x)

### Código de Huffman

- Requesitos:
  - ightharpoonup Conhecer a priori as probabilidades p(x)
- Algoritmo:
  - ► Todos os símbolos são folhas de uma árvore a construir.
  - Em cada passo seleccionam-se os dois nós de menor probabilidade para formar o novo nó pai.
  - ► As palavras de código correspondem ao caminho da raiz até às folhas.

### Código de Huffman

- Requesitos:
  - ▶ Conhecer a priori as probabilidades p(x)
- Algoritmo:
  - ► Todos os símbolos são folhas de uma árvore a construir.
  - Em cada passo seleccionam-se os dois nós de menor probabilidade para formar o novo nó pai.
  - As palavras de código correspondem ao caminho da raiz até às folhas.
- Optimalidade:
  - ▶ O código de Huffman satisfaz

$$H(X) \le L(C) < H(X) + 1$$

▶ É o melhor código instantaneo que se pode construir para um dado alfabeto.

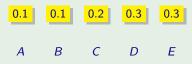
- Requesitos:
  - ightharpoonup Conhecer a priori as probabilidades p(x)
- Algoritmo:
  - ► Todos os símbolos são folhas de uma árvore a construir.
  - Em cada passo seleccionam-se os dois nós de menor probabilidade para formar o novo nó pai.
  - As palavras de código correspondem ao caminho da raiz até às folhas.
- Optimalidade:
  - ▶ O código de Huffman satisfaz

$$H(X) \leq L(C) < H(X) + 1$$

- ▶ É o melhor código instantaneo que se pode construir para um dado alfabeto.
- Desvantagens:
  - Assume que os símbolos são v.a. independentes.
  - Assume que as probabilidades não variam no tempo.
  - O compressor e o descompressor têm de conhecer a mesma árvore (necessário enviar a árvore para o descompressor descodificar a mensagem).

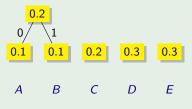
### Exemplo

Considere um alfabeto  $\{A,B,C,D,E\}$  com probabilidades  $\{0.1,0.1,0.2,0.3,0.3\}$ . O código de Huffman constrói-se do seguinte modo:



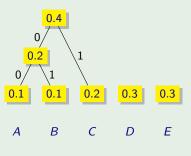
## Exemplo

Considere um alfabeto  $\{A, B, C, D, E\}$  com probabilidades  $\{0.1, 0.1, 0.2, 0.3, 0.3\}$ . O código de Huffman constrói-se do seguinte modo:



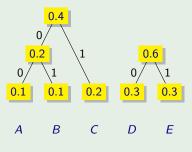
## Exemplo

Considere um alfabeto  $\{A, B, C, D, E\}$  com probabilidades  $\{0.1, 0.1, 0.2, 0.3, 0.3\}$ . O código de Huffman constrói-se do seguinte modo:



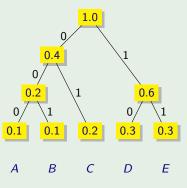
# Exemplo

Considere um alfabeto  $\{A, B, C, D, E\}$  com probabilidades  $\{0.1, 0.1, 0.2, 0.3, 0.3\}$ . O código de Huffman constrói-se do seguinte modo:

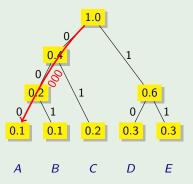


# Exemplo

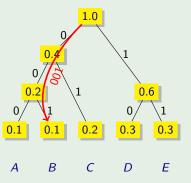
Considere um alfabeto  $\{A,B,C,D,E\}$  com probabilidades  $\{0.1,0.1,0.2,0.3,0.3\}$ . O código de Huffman constrói-se do seguinte modo:



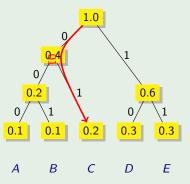
Considere um alfabeto  $\{A, B, C, D, E\}$  com probabilidades  $\{0.1, 0.1, 0.2, 0.3, 0.3\}$ . O código de Huffman constrói-se do seguinte modo:



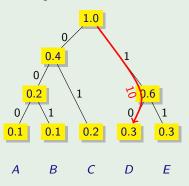
Considere um alfabeto  $\{A, B, C, D, E\}$  com probabilidades  $\{0.1, 0.1, 0.2, 0.3, 0.3\}$ . O código de Huffman constrói-se do seguinte modo:



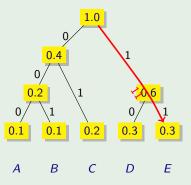
Considere um alfabeto  $\{A, B, C, D, E\}$  com probabilidades  $\{0.1, 0.1, 0.2, 0.3, 0.3\}$ . O código de Huffman constrói-se do seguinte modo:



Considere um alfabeto  $\{A, B, C, D, E\}$  com probabilidades  $\{0.1, 0.1, 0.2, 0.3, 0.3\}$ . O código de Huffman constrói-se do seguinte modo:



Considere um alfabeto  $\{A, B, C, D, E\}$  com probabilidades  $\{0.1, 0.1, 0.2, 0.3, 0.3\}$ . O código de Huffman constrói-se do seguinte modo:



 O código de Huffman anterior só pode ser construído depois de conhecer as probabilidades da fonte.

- O código de Huffman anterior só pode ser construído depois de conhecer as probabilidades da fonte.
- No caso de se pretender comprimir uma string gerada por uma fonte desconhecida (e.g. um ficheiro), é necessário determinar a frequência com que os símbolos ocorrem.

- O código de Huffman anterior só pode ser construído depois de conhecer as probabilidades da fonte.
- No caso de se pretender comprimir uma string gerada por uma fonte desconhecida (e.g. um ficheiro), é necessário determinar a frequência com que os símbolos ocorrem.
- São necessárias duas passagens sobre o ficheiro:
  - 1 Contar o número de ocorrências de cada símbolo;
  - 2 Desenhar código e comprimir ficheiro.

- O código de Huffman anterior só pode ser construído depois de conhecer as probabilidades da fonte.
- No caso de se pretender comprimir uma string gerada por uma fonte desconhecida (e.g. um ficheiro), é necessário determinar a frequência com que os símbolos ocorrem.
- São necessárias duas passagens sobre o ficheiro:
  - 1 Contar o número de ocorrências de cada símbolo;
  - 2 Desenhar código e comprimir ficheiro.

O código de Huffman adaptativo permite fazer compressão nas seguintes condições:

- não necessita de conhecer as probabilidades dos símbolos.
- faz apenas uma passagem sobre o ficheiro.
- não é necessário transmitir o código. O receptor consegue reconstruir a árvore à medida que faz a descodificação.

O algoritmo foi desenvolvido independentemente por Faller (1973) e Galager (1978) e melhorado por Knuth (1985), ficando conhecido como algoritmo FGK. Existe ainda outro melhoramento devido a Vitter (1987), conhecido como algoritmo V, que não é apresentado aqui.

O código de Huffman adaptativo é usado no comando compact do UNIX.

# Código de Huffman adaptativo: ideias chave

■ Construir uma árvore binária à medida que são lidos novos símbolos.

## Código de Huffman adaptativo: ideias chave

- Construir uma árvore binária à medida que são lidos novos símbolos.
- Reserva um símbolo de ESCAPE para representar todos os símbolos que ainda não ocorreram até ao momento actual.

### Código de Huffman adaptativo: ideias chave

- Construir uma árvore binária à medida que são lidos novos símbolos.
- Reserva um símbolo de ESCAPE para representar todos os símbolos que ainda não ocorreram até ao momento actual.
- Manipular a árvore de modo a aproximar-se de uma árvore de Huffman:
  - Cada nível da árvore não pode conter nós com número de ocorrências superior aos níveis de cima: ordenar nós de baixo para cima de modo a que os símbolos mais frequentes estejam mais acima.
  - As ocorrências devem estar ordenadas da esquerda para a direita em cada nível da árvore.

- Construir uma árvore binária à medida que são lidos novos símbolos.
- Reserva um símbolo de ESCAPE para representar todos os símbolos que ainda não ocorreram até ao momento actual.
- Manipular a árvore de modo a aproximar-se de uma árvore de Huffman:
  - Cada nível da árvore não pode conter nós com número de ocorrências superior aos níveis de cima: ordenar nós de baixo para cima de modo a que os símbolos mais frequentes estejam mais acima.
  - As ocorrências devem estar ordenadas da esquerda para a direita em cada nível da árvore.
- Para codificar um símbolo, verifica-se se este já existe na árvore e:
  - Se já existe, usa-se o código correspondente e incrementam-se as ocorrências desse símbolo e dos seus ascendentes.
  - Se não existe, usa-se o código de "escape" seguido do símbolo sem ser codificado, acrescenta-se o símbolo à árvore por baixo de onde antes estava o "escape", e actualizam-se as ocorrências dos nós ascendentes.

Em qualquer um dos casos anteriores, modifica-se a árvore de modo a que as ocorrências estejam ordenadas de baixo para cima e depois da esquerda para a direita.

"ABRACADABRA"  $\longrightarrow$  A

"ABRACADABRA"  $\longrightarrow$  A

