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

Teoria da Informação

8, Fevereiro 2022
Exame Época Recurso
Duração: 2:00h

Nome: Nº Estudante:

Observe que:
Exame com consulta condicionada (uma página A4 de apontamentos)
Não são permitidos meios electrónicos (computador, telemóveis, etc.), excepto calculadoras.
Qualquer tentativa de fraude conduzirá à anulação da prova para todos os intervenientes.
Respostas na folha de prova
Nas respostas múltiplas, as respostas erradas subtraem cotação.

1 – Considere que X é uma variável estocástica equi-provável com 16 estados possíveis e que f(X) é uma função linear dessa variável.

a) Indique a(s) opção(ões) verdadeira(s)

☐ H(X) < 2 bits/símb. ☐ H(X) ≥ H(f(X))

☐ H(X|f(X)) = H(X) bits/símb. ☐ Nenhuma das anteriores

b) Nas condições da alínea a) observa-se que:

☐ H(X,f(X)) = H(X)+H(f(X)) ☐ H(X|f(X))=H(f(X))

☐ H(X,f(X)) ≤ 4 bits/símb. composto ☐ Nenhuma das anteriores

2 - Seja a variável estocástica X = "*sequência de resultados de 10 jogos da equipa de futebol da AAC na Liga de Honra*", em que o alfabeto de resultados possíveis em cada jogo é $A=\{v,e,d\}$ (*v=vitória, e=empate, d=derrota*). Assuma que todas as equipas do campeonato são equiparáveis e que os resultados de todos os jogos são independentes. Seja Y = "total de pontos da AAC nos 10 jogos" (vitória = 3 pontos, empate = 1 ponto, derrota = 0 pontos).

a) Nestas condições observa-se que I(X;Y) é igual a:

☐ 0 ☐ H(Y)
☐ H(X) ☐ Nenhuma das anteriores

b) Nas condições da alínea a) observa-se que H(X|Y) é igual a:

☐ H(X,Y) ☐ H(X)
☐ H(X)-H(Y) ☐ Nenhuma das anteriores

c) Nas condições da alínea a) observa-se que H(Y|X) é igual a:

☐ H(Y) ☐ 0
☐ H(X,Y) ☐ Nenhuma das anteriores

3 – Considere uma fonte de informação descrita pelo alfabeto A={*A, B, C, D, E, F, G, H, I, J, K*}. Pretende-se codificar a fonte usando uma árvore de Huffman adaptativa.

a) O código pré-acordado para o símbolo **G** é:

☐ 0101 ☐ 011
☐ 010 ☐ 0011

b) Indique o bitstream resultante da codificação da seguinte mensagem: **GGFHGF**

☐ 10010010100011001 ☐ 10010010100011101
☐ 10010001010111000101 ☐ Nenhum dos anteriores

4 – Assinale as afirmações verdadeiras e falsas:

☐ A utilização de preditores na codificação de imagens tem como objetivo diminuir a redundância das cores da imagem

☐ Na codificação GIF, o dicionário é inicializado com um número de entradas igual ao dobro do número de cores na paleta de cores da imagem.

☐ A utilização do método Burrows Wheeler reduz a entropia da fonte de informação.

☐ A utilização do método Move to Front tem o objetivo de aumentar a redundância da fonte de informação.

☐ A codificação BZip2 combina vários métodos, entre eles o Burrows Wheeler, RLE, Move to Front e Delta encoding.

☐ No deflate a unidade a codificar é a informação contida em menos de 8 bits.

☐ No deflate a codificação LZ77 implica sempre o envio de 3 valores.

☐ No GIF o LZW pode fazer reset ao dicionário.

☐ No RLE assume-se que os símbolos são dependentes.

☐ O objectivo do Move-to-Front é tornar a fonte mais dependente.

☐ Regra geral o RLE e o Burrows Wheeler estão associados.

☐ O Move-to-Front tende a aumentar a entropia.

☐ Contextos grandes no método PPM aumenta a probabilidade de se obter sequências grandes de ESC

☐ Na codificação GIF, o dicionário duplica de tamanho sempre que enche, até um máximo de 4098 entradas.

☐ Nos métodos de codificação com preditores, a informação codificada é a diferença entre o resultado da predição e a informação real.

☐ As funções de hashing não permitem ser usadas em funções de autenticação.

☐ As funções de hashing garantem sempre a produção de saídas (outputs) distintas para entradas (inputs) distintos.

☐ Numa assinatura digital a propriedade de não repúdio é obtida por recurso à chave privada.

☐ O Cipher Block Chain está sujeito a ataques de Meet-in-the-middle.

☐ Num esquema de cifra, assumindo que a entropia da mensagem é de 125, então para garantir segurança máxima temos que ter uma chave que apresente uma entropia de pelo menos 250 bits.

☐ Assumindo que H(z)=325 bits, em que z é a chave e y representa a cifra, então garante-se segredo perfeito se H(x)<=125 bits, sendo x a mensagem.

☐ Seja X a mensagem a ser encriptada com a chave Z e seja Y a respetiva cifra. Assumindo que o número de símbolos nos alfabetos de entrada e de saída são iguais, pretende-se que H(X)=H(Y|Z).

5 – Considere uma fonte de informação com alfabeto A={0,1,2}. Seja X a variável estocástica correspondente ao símbolo e Y a variável estocástica correspondente ao símbolo anterior numa cadeia de símbolos. Assuma que a distribuição conjunta P(X,Y) é a que se apresenta na tabela seguinte:

P(X,Y)	X=0	X=1	X=2
Y=0	1/9	2/9	0
Y=1	0	0	1/9
Y=2	1/3	2/9	0

c) É possível afirmar-se que existe um código que permite codificar X com
☐ 1.1021 bits/símb. ☐ 1.3921 bits/símb.
☐ 1.4921 bits/símb. ☐ Nenhuma das anteriores

d) Aplicando um código de Huffman para codificar X, é possível garantir-se que o pior desempenho será:
☐ 1.4921 bits/símb. ☐ 1.3921 bits/símb.
☐ 1.5921 bits/símb. ☐ Nenhuma das anteriores

e) Na pior das hipóteses um código aritmético dimensionado para a transmissão de agrupamentos de 10 símbolos terá um desempenho de:
☐ 1.4921 bits/símb. ☐ 1.3921 bits/símb.
☐ 1.5921 bits/símb. ☐ Nenhuma das anteriores

f) Considere a sequencia “001”. A codificação da sequencia usando um algoritmo aritmético poderá resultar na transmissão do seguinte código:
☐ 0.1000 ☐ 0.1756
☐ 0.5000 ☐ Nenhuma das anteriores

6 - Num sistema iCloud para armazenamento distribuído de informação em que um ficheiro é armazenado de forma distribuída por diversos servidores (cada um somente com uma fracção do ficheiro inicial), determine qual deverá ser a informação mútua ideal entre o ficheiro original e o ficheiro recuperado do sistema.

7 - Considere uma fonte de informação pertencente ao dicionário S={1,2,3,4,5}.

a) Assumindo que os símbolos são todos equiprováveis, indique a sequência de bits resultante da codificação da sequencia “1233554424” usando um código artimético inteiro.

b) Assumindo um algoritmo PPM com contexto de ordem 1, indique a codificação dos 3 primeiros símbolos da sequência referida em a).

9 - No trabalho 1, foi implementada uma solução de codificação de fontes de informação usando agrupamento de 2 símbolos contíguos. Qual o impacto (positivo e negativo) desta solução, em comparação com a codificação de Huffman de símbolos individuais.