Nome: **Nº:**

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

16 de Janeiro de 2025
Exame Normal

Teoria da Informação

Duração: 2h

Notas prévias:

1) *Consulta permitida: uma página A4 de apontamentos.*
2) *Não são permitidos meios electrónicos (computador, telemóveis, etc.), excepto calculadoras. (não programáveis).*
3) *Qualquer tentativa de fraude conduzirá à anulação da prova para todos os intervenientes e activação do procedimento disciplinar da Universidade de Coimbra.*
4) *Escolha múltipla:* ***só uma das opções é a correcta****; as respostas* ***erradas subtraem 25%*** *da cotação da pergunta.*
5) *As cotações das questões poderão sofrer alterações ligeiras para beneficiar a maioria dos alunos.*
6) Respostas na folha de prova

1. Seja a variável estocástica X = "humidade relativa média em Coimbra num dado dia", com **alfabeto A_x = {B, b, m, a, A}** (B=muito baixa, b=baixa, m=média, a=alta, A=muito alta). De 1 a 16 de Abril de 2024, X variou segundo a **sequência** seguinte: **mmAaAamAambBbBbm**. Assuma que a distribuição probabilística da sequência representa a distribuição probabilística de X. Seleccione uma e uma só resposta correcta nas alíneas abaixo (valores arredondados à milésima).

   a) (5%) Assumindo independência dos símbolos na sequência, o limite mínimo teórico para o número médio de bits por símbolo é:
   ☐ 2.258 ☐ 3.907 ☐ 3 ☐ 2.322 ☐ 4

   b) (2.5%) Na sequência referida acima, o agrupamento de 2 símbolos permitirá codificar X com:
   ☐ 2.322 ☐ 2.5 ☐ 4.644 ☐ 1.25 ☐ 0.625

   c) (7.5%) A modelação da sequência referida acima como um modelo de Markov de 1ª ordem permitirá codificar X com:
   ☐ 0.258 ☐ 1.626 ☐ 4.644 ☐ 1.37 ☐ 0.813

   d) (2.5%) Aplicando um código de Huffman para codificar X, é possível garantir-se que o pior desempenho será:
   ☐ 3.122 ☐ 4.231 ☐ 3.258 ☐ 2.5 ☐ 4.807

   e) (5%) Aplicando um código de Huffman para codificar X, o comprimento médio das palavras binárias obtidas será:
   ☐ 2.322 ☐ 4.231 ☐ 2.258 ☐ 3.258 ☐ 2.313

f) (7.5%) Considere que uma dada sequência de alfabeto especificado acima foi codificada usando o algoritmo de Huffman adaptativo, gerando o código **0010010101000010010**. Assumindo a ordem do alfabeto especificada acima, i. e., **B, b, m, a, A**, a sequência original de símbolos é:

☐ b, m, b, a, B ☐ b, m, m, b, B ☐ b, m, m, b, B, m
☐ b, m, m, b, B, a ☐ b, m, b, a, B, a

g) (7.5%) Indique a sequência de códigos transmitidos codificando a sequência acima com o algoritmo LZW. Assuma a ordem do alfabeto especificada acima, i.e., **B, b, m, a, A**.

☐ 3, 3, 5, 4, 5, 7, 4, 3, 2, 1, 14, 2, 16 ☐ 3, 3, 5, 4, 8, 7, 4, 3, 2, 1, 14, 2, 3
☐ 3, 3, 5, 4, 8, 7, 4, 3, 2, 1, 14, 2, 16, 3 ☐ 3, 3, 5, 4, 8, 7, 4, 3, 2, 1, 14, 2, 16
☐ 3, 3, 5, 4, 5, 4, 4, 3, 2, 1, 14, 2, 3

h) (7.5%) Considere que uma dada sequência de **3 símbolos** do alfabeto especificado acima foi codificada usando o algoritmo aritmético, gerando o código binário **110000000**. Assumindo a ordem do alfabeto especificada acima, i. e., **B, b, m, a, A**, a sequência original de símbolos é:

☐ a, b, m ☐ a, a, b ☐ b, m, a ☐ a, m, b ☐ a, A, a

2. Seja X uma variável aleatória definida como "humidade relativa diária em Coimbra, entre os anos de 2000 e 2024", com alfabeto A_x = {0, 1, 2, …, 100}. Seja $Y = \left\lfloor \frac{X}{20} \right\rfloor$. Seja $Z = Y^2$.

a) (5%) Assinale uma e uma só opção correcta:

☐ H(Y,Z) = H(Y) + H(Z) ☐ H(Y,Z) = H(Z) – H(Y) ☐ H(Z|Y) = H(Y)
☐ I(Y;Z) = H(Y,Z) ☐ I(Y;Z) = H(Y|Z) + H(Z|Y)

b) (5%) Assinale uma e uma só opção correcta:

☐ H(X,Z) = H(X) + H(Z) ☐ H(X,Z) = H(Z) ☐ H(Z|X) = H(X)
☐ I(X;Z) = H(X,Z) ☐ I(X;Z) = H(Z) + H(Z|X)

c) (5%) Assinale uma e uma só opção correcta:

☐ H(X) ≤ 1.573 ☐ H(X) = 0, em qualquer caso ☐ H(X) = H(Y)
☐ H(X) = H(Z) ☐ H(X) ≤ 6.658

3. (7.5%) Das funções abaixo, apenas uma pode servir como uma **medida da redundância**, $R(X, Y)$, entre duas variáveis aleatórias X e Y. Qual delas é?

☐ $R(X, Y) = H(X, Y) \,/\, [H(X) + H(Y)]$ ☐ $R(X, Y) = [H(X) + H(Y)] \,/\, H(X, Y)$
☐ $R(X, Y) = I(X; Y) \,/\, H(X, Y)$ ☐ $R(X, Y) = H(X, Y) \,/\, I(X; Y)$
☐ $R(X, Y) = H(X \mid Y) + H(Y \mid X)$

4. (2.5%) Na codificação de Huffman, **que característica** deve satisfazer a distribuição de probabilidade de uma variável aleatória X, $p(X)$, para o que o **comprimento médio dos símbolos** usando codificação de **Huffman** seja **exactamente igual à entropia estimada**, assumindo independência de símbolos numa sequência? (assinale uma e uma só opção correcta)

☐ O comprimento médio dos símbolos nunca pode ser igual à entropia estimada.
☐ O comprimento médio dos símbolos é sempre igual à entropia estimada.
☐ Todas as probabilidades devem ser potências negativas de 2.
☐ As probabilidades devem seguir uma distribuição normal.
☐ Nenhuma das anteriores.

5. (2.5%) No algoritmo DEFLATE, o **cabeçalho do ficheiro gzip** (assinale uma e uma só opção correcta):
   - ☐ guarda informação sobre o número de blocos contidos no ficheiro.
   - ☐ não guarda informação sobre o número de blocos, dado que esse número é fixo.
   - ☐ não guarda informação sobre o número de blocos, dado que todos os blocos têm a mesma dimensão.
   - ☐ não guarda informação sobre o número de blocos, dado que o cabeçalho de cada bloco usa 2 bits para identificar se se trata ou não do último bloco.
   - ☐ não guarda informação sobre o número de blocos, dado que o cabeçalho de cada bloco usa 1 bit para identificar se se trata ou não do último bloco.

6. (2.5%) No algoritmo DEFLATE, a **dimensão do *search buffer*** é (assinale uma e uma só opção correcta):
   - ☐ igual à dimensão do bloco
   - ☐ igual à dimensão do *look-ahead buffer*
   - ☐ igual a 2^{12} (i.e., 4096)
   - ☐ igual a 2^{15} (i.e., 32768)
   - ☐ sem limite

7. Suponha que, num esquema RSA, n = 18871, e = 2479 e o resultado da função de Euler é 18592.

   a) (7.5%) Sabendo que se obteve a cifra 136, determine a mensagem (assinale uma e uma só opção correcta):
   - ☐ 12352
   - ☐ 21394
   - ☐ 17025
   - ☐ 8432
   - ☐ 1398

   b) (7.5%) Identifique e apresente os valores da chave privada (p, q, d). Assinale uma e uma só opção correcta.
   - ☐ p=89, q=101, d=15
   - ☐ p=89, q=113, d=11
   - ☐ p=167, q=113, d=15
   - ☐ p=167, q=113, d=11
   - ☐ p=74, q=59, d=15

8. (5%) Num esquema de encriptação, seja *X* a mensagem original, *Y* a mensagem encriptada a partir da mensagem *X,* e *Z* a chave que deu origem à encriptação. Nestas circunstâncias, idealmente deve-se obter (assinale uma e uma só opção correcta):
   - ☐ $H(X)=H(X|Y)$
   - ☐ $H(X)=H(Y)$
   - ☐ $H(Y)=H(Y|X,Z)$
   - ☐ $H(Y)= 0$
   - ☐ nenhuma das anteriores

9. (2.5%) Num esquema de encriptação usando o algoritmo RSA, os número secretos ***p* e *q*** devem obedecer aos seguintes requisitos (assinale uma e uma só opção correcta):
   - ☐ devem ser números inteiros de grande dimensão
   - ☐ podem ser números inteiros em qualquer gama de valores
   - ☐ devem ser números primos com mais de 100 bits
   - ☐ devem ser números primos com mais de 1024 bits
   - ☐ um deles deve ser primo, com mais de 100 bits

10. (2.5%) A encriptação com o algoritmo RSA adequa-se particularmente a (assinale uma e uma só opção correcta):
   - ☐ quaisquer ficheiros de utilizadores
   - ☐ transmissão de chaves públicas de algoritmos de chave simétrica
   - ☐ transmissão de chaves privadas de algoritmos de chave simétrica
   - ☐ ficheiros gzip, dado que complementam a codificação do algoritmo Deflate
   - ☐ nenhuma das anteriores