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

Teoria da Informação
3, Fevereiro 2015
Exame Época Normal
Duração: 2:30h

Nome: **Número de 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. Suponha que X={1,2,3,....,32} é uma variável aleatória. equiparável. Nestas condições assinale as opções verdadeiras:

a) ☐ H(X) = 5 ☐ H(X) < 5
☐ H(X) ≥ 0 ☐ nenhuma das anteriores

b) ☐ H(X,X) = H(X) ☐ H(X,X) =H(X)+H(X)
☐ H(X,X) = H(X)+H(X|X) ☐ nenhuma das anteriores

c) ☐ I(X;X) = 0 ☐ I(X;X) = H(X|X)
☐ I(X;X) = 5 ☐ nenhuma das anteriores

d) Suponha agora que Y=2X+E e que E é uma variável aleatória. Nestas circunstâncias, assinale as opções verdadeiras:

i. ☐ H(X|Y)= 0 ☐ H(X|Y)=H(Y)
☐ H(X|Y)=H(X,Y) ☐ nenhuma das anteriores

ii. ☐ H(X,Y)=H(X)+H(Y) ☐ H(X,Y)=H(Y)
☐ H(X,Y)=H(X)+H(Y|X) ☐ nenhuma das anteriores

iii. ☐ I(X;Y) = 0 ☐ I(X;Y) = H(X)-H(X|Y)
☐ I(X;Y) = H(X) ☐ nenhuma das anteriores

iv. ☐ H(X)>H(Y) ☐ H(Y)=0
☐ H(X,Y)=H(X) ☐ nenhuma das anteriores

2. Assinale as afirmações correctas:

☐ A diferença entre um código aritmético e um código de dicionário é que o primeiro é mais eficiente qualquer que seja o contexto.

☐ Um código de Huffman pode na prática ser menos eficiente que um código de Fano-Elias.

☐ O agrupamento de um número elevado de símbolos é uma boa estratégia prática de codificação quando se usa um código de Huffman.

☐ O agrupamento de um número elevado de símbolos é uma boa estratégia de codificação quando se usa um código de Aritmético.

☐ Comparativamente com um esquema de codificação LZW, um código LZ78 é sempre vantajoso dado não requerer um dicionário pré-preenchido.

☐ O código aritmético e o código Fano-Elias têm o mesmo princípio.

☐ A relação entre o LZW e o LZ77 é que o segundo não consegue capturar os padrões locais.

3. Num RSA observa-se que o expoente de encriptação verifica $e^2 \bmod \Phi(n) = 1$ (assuma que a função $\Phi()$ representa a função de Euler). Assinale a(s) resposta(s) certa(s).

☐ O esquema de codificação é seguro.

☐ O esquema de codificação não é utilizável devido à sua insegurança.

☐ A codificação da mensagem m=e revela a chave de desencriptação.

☐ Nenhuma das anteriores está correcta

4. Considere um sistema de cifra com chave privada que produz mensagens de comprimento 7 compostas por símbolos do alfabeto {1,2,3,4,5,6,7,8}. Sabendo que a entropia da chave é 3600, que o alfabeto de entrada tem cardinalidade 8 e que as mensagem encriptadas têm um comprimento de 7 caracteres, para aplicar este esquema num banco que garantias pode dar relativamente à segurança do esquema.

5. Considere uma fonte X={1,2,3,4,5} tal que P(X=1)=0.2, P(X=2)=0.2, P(X=3)=0.4, P(X=4)=0.1 e P(X=5)=0.1.

   a) Nestas condições, determine o número de bits a usar na codificação por recurso a um código aritmético de mensagens agrupadas com 4 símbolos.

   b) Dada a mensagem "1223", determine a TAG necessária à transmissão desta mensagem por recurso a um código aritmético.

c) Dada a mensagem “123312331233”, codifique-a usando LZW. Para o efeito apresente a sequência de índices e o estado final do dicionário.

6. Demonstre, com recurso ao princípio da máxima entropia, que a entropia de uma dada variável aleatória X é máxima quando os acontecimentos são equiprováveis.

7. Considere um código linear (8,4) em que as equações de verificação de paridade são as seguintes (os bits u são bits da mensagem e os bits v são bits resultantes da verificação da paridade) :

$$v_0 = u_1 + u_2 + u_3$$
$$v_1 = u_0 + u_1 + u_2$$
$$v_2 = u_0 + u_1 + u_3$$
$$v_3 = u_0 + u_2 + u_3$$

   a. Construa um codificador para este código.

b. Construrua um descodificador para este código.

8. Comente a seguinte afirmação: “num esquema de pesquisa não basta analisar o valor absoluto da informação mútua”.

9. Comente a seguinte afirmação: “No GIF é obrigatório existir uma palete de cores no *image header*”?