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

Teoria da Informação
6, Janeiro 2014
Exame Época Normal
Duração: 2:30h

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,....,16} é uma variável aleatória.. Nestas condições assinale as opções verdadeiras:

   a) ☐ H(X) = 4 ☐ H(X) ≤ 4
   ☐ 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) = H(X) ☐ nenhuma das anteriores

   d) Suponha agora que Y(X) é um processo que para cada X produz duas cópias de X. 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. A fonte num canal de comunicação ruidoso é uma variável aleatória X pertencente ao dicionário $\{a,b,c,d\}$. A saída deste canal é a variável aleatória Y pertencente ao mesmo dicionário. A distribuição de probabilidades conjunta é a que se apresenta na tabela seguinte:

	$x=a$	$x=b$	$x=c$	$x=d$
$y=a$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$
$y=b$	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{16}$	0
$y=c$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{16}$	0
$y=d$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{16}$	0

Nestas circunstâncias assinale as opções verdadeiras:

a) ☐ H(X)=2.275 bits ☐ H(X)=3.375 bits
☐ H(X)=1.750 bits ☐ nenhuma das anteriores

b) ☐ H(Y)=2 bits ☐ H(Y)=3.375 bits
☐ H(Y)=2.750 bits ☐ nenhuma das anteriores

c) ☐ H(Y|X)= 2 bits ☐ H(Y|X)= 1.625 bits
☐ H(Y|X)= 0 bits ☐ nenhuma das anteriores

d) ☐ I(X;Y) = 0.375 ☐ I(X;Y) = 1.750
☐ I(X;Y) = 1.625 ☐ nenhuma das anteriores

3. Para cada uma das alíneas indique se o código de prefixo apresentado é óptimo para a distribuição de probabilidades apresentada. Justifique a sua resposta.

i.

X	*p(x)*	*C(x)*
1	0.25	0110
2	0.5	00
3	0.1	010
4	0.1	0111

ii.

X	*p(x)*	*C(x)*
1	0.25	00
2	0.25	0
3	0.25	10
4	0.25	111

iii.

X	*p(x)*	*C(x)*
1	0.25	110
2	0.25	10
3	0.25	110
4	0.25	111

iv.

x	*p(x)*	*C(x)*
1	0.3	00
2	0.3	01
3	0.2	10
4	0.2	11

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

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 "1133", determine a TAG necessária à transmissão desta mensagem por recurso a um código aritmético. Apresente a sua codificação binária.

c) Dada a mensagem “1133”, determine a sequência de bits por recurso a um código de Huffman estático. Apresente a árvore de Huffman.

d) Assumindo independência estatística dos símbolos, quantos nós deverá ter a árvore de Huffman estática para codificar agrupamentos de 4 símbolos?

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

6. Seja p = 7919 e q = 17389. Seja e = 66909025. Observa-se que e^2 mod (p-1)(q-1) = 1. Considerando que a mensagem é m = 12345, qual será o resultado da cifra se houver duas encriptações consecutivas com a chave (n, e)?

7. No esquema de encriptação DES não é necessário implementar de forma explícita o algoritmo de desencriptação. Indique como é que o algoritmo de desencriptação pode ser realizado à custa do algoritmo de encriptação?

8. Comente a seguinte afirmação: "No GIF o código de RESET deverá existir pelo menos uma vez, podendo ocorrer o número ($\geq$1) de vezes que se quiser "?