Examen 7 de junio 2013, preguntas y respuestas

Informació i Seguretat (Universitat Autònoma de Barcelona)

INFORMACIÓ I SEGURETAT
7 de juny de 2013

Nom i cognoms: ______________________________ Grup: ________

- **Cal que justifiqueu convenientment totes les respostes**
- $\log 3 = 1.58$, $\log 5 = 2.32$, $\log 7 = 2.8$
- $13^{-1} \bmod 161 = 62$, $13^{-1} \bmod 132 = 61$, $15^{61} \bmod 161 = 148$, $15^{61} \bmod 132 = 15$, $15^{13} \bmod 132 = 72$, $15^{13} \bmod 161 = 120$.
- Equivalència entre lletres i números:

$$\begin{bmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \end{bmatrix}$$

1. (25%=5%+10%+10%) Hem codificat una font d'informació $S = \{A, B, C, D\}$ amb probabilitats $\{\frac{1}{3}, \frac{1}{3}, \frac{1}{6}, \frac{1}{6}\}$ fent servir el codi $C = \{01, 11, 100, 101\}$.

   (a) Definiu codi instantani i digueu si C ho és.

   (b) Digueu si l'eficiència de C és menor o igual a 1 i justifiqueu si és òptim.

   (c) Pot existir un codi binari instantani que codifiqui S amb longituds $L_1 = L_2 = L_3 = 2$, $L_4 = 3$?

   Solució:

   (a) Un codi és instantani si cap paraula-codi és prefix d'una altra. C és un codi instantani.

   (b) $\eta = \frac{H(S)}{\bar{L}\log(D)}$. Tenim que $\log(D) = 1$, $H(S) = 2\frac{1}{3}\log(3) + 2\frac{1}{6}\log(6) = \frac{2}{3}\log(3) + \frac{1}{3}(\log(3)+\log(2)) = \log(3)+\frac{1}{3} = 1.58+0.33 = 1.91$ bits i $\bar{L} = \frac{2}{3}+\frac{2}{3}+\frac{3}{6}+\frac{3}{6} = \frac{7}{3} = 2.33$. Per tant, $\eta = \frac{1.91}{2.33}$ és menor que 1. Per saber si el codi és o no òptim, apliquem l'algoritme de Huffman per trobar un codi òptim. Si apliquem l'algoritme, obtenim $C_H = \{0, 10, 110, 111\}$ que té longitud mitjana $\bar{L}_H = \frac{1}{3} + \frac{2}{3} + 2\frac{1}{6} = \frac{6}{3} = 2$. Com $\bar{L}_H < \bar{L}$, podem concloure que C no és òptim.

   (c) Apliquem la desigualtat de Kraft; existeix si i només si $(2^{-2} + 2^{-2} + 2^{-2} + 2^{-3}) \leq 1$. Tenim que $(2^{-2} + 2^{-2} + 2^{-2} + 2^{-3}) = 3\frac{1}{4} + \frac{1}{8} = \frac{7}{8} \leq 1$; per tant, sí que pot existir.

2. (25%=10%+10%+5%) Considereu el canal amb entrada $A = \{a_1, a_2, a_3\}$, sortida $B = \{b_1, b_2, b_3, b_4\}$ i determinat per la matriu de transicions:

$$\Pi = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ \frac{1}{4} & \frac{1}{2} & 0 & \frac{1}{4} \\ 0 & \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \end{pmatrix}.$$

   (a) Considereu les probabilitats inicials $\{p(a_1) = 0, p(a_2) = 1, p(a_3) = 0\}$. Calculeu $H(A)$, $H(B)$, $H(B|A)$ i doneu la informació mútua de la entrada i la sortida.

   (b) Doneu la capacitat del canal. Amb quina distribució d'entrada i de sortida s'assoleix la capacitat?

(c) Si la distribució de probabilitats inicial és $\{\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\}$, calculeu la regla MPE i digueu quina és la probabilitat mitjana d'error.

Solució:

(a) Considerem les taules:

$p(b_i, a_j)$	b_1	b_2	b_3	b_4
a_1	0	0	0	0
a_2	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$
a_3	0	0	0	0

$p(a_j\|b_i)$	b_1	b_2	b_3	b_4
a_1	0	0	0	0
a_2	1	1	0	1
a_3	0	0	0	0

Tenim que $H(A) = H(0, 1, 0) = 0$ bits i $H(B) = H(\frac{1}{4}, \frac{1}{2}, \frac{1}{4}) = \frac{1}{2}\log(2) + 2\frac{1}{4}\log(2) = \frac{1}{2} + 1 = 1,5$ bits. D'altra banda, $H(B|A) = \frac{1}{4}\log(4) + \frac{1}{2}\log(2) + \frac{1}{4}\log(4) = 1,5$ bits. Finalment, $I(A, B) = H(B) - H(B|A) = 1.5 - 1.5 = 0$ bits.

(b) En aquest canal, tenim $C = \log 3 - H$, on $H = H(\frac{1}{2}, \frac{1}{4}, \frac{1}{4}) = 1.5$ Per tant, $C = 1.58 - 1.5 = 0.08$ bits. Així, la informació màxima del canal és 0.08 que es dóna quan la probabilitat d'entrada és equiprobable, i les probabilitats de sortida són també equiprobables, $\{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\}$.

(c) La Regla MPE és aquella que assigna a cada b_j el valor a_i tal que $p(a_i|b_j)$ sigui màxima. Si considerem la taula les probabilitats inicials $\{\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\}$. En aques cas, tenim

$p(b_i, a_j)$	b_1	b_2	b_3	b_4
a_1	$\frac{1}{6}$	0	$\frac{1}{6}$	0
a_2	$\frac{1}{12}$	$\frac{1}{6}$	0	$\frac{1}{12}$
a_3	0	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{6}$

una possible funció MPE seria $f(b_1) = a_1, f(b_2) = a_2, f(b_3) = a_1, f(b_4) = a_3$. Aleshores la probabilitat mitjana d'error és $1 - (\frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6}) = 1 - \frac{4}{6} = \frac{1}{3}$.

3. (25%) Considereu el codi binari i lineal de matriu generadora:

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(a) Calculeu totes les seves paraules-codi i la seva matriu de control, H. Trobeu la distància mínima d del codi C a partir de la matriu de control H.

(b) Utilitzem aquest codi per codificar el missatge 'HOLA' amb la següent equivalència: $H \to 100$, $O \to 101$, $L \to 001$ i $A \to 011$. Una vegada codificat, enviarem el missatge per una canal binari i simètric. Quina és la seqüència de bits que enviarem pel canal?

(c) Suposem que la seqüència rebuda es 100100101101010101110111. Utilitzant la taula de síndromes, descodifiqueu, si és possible, la seqüència rebuda.

(d) Quina seria la matriu de control i la distància mínima del codi estès C'?

(e) Tot codi 2-corrector té distància mínima 4?

Solució:

(a) Paraules-codi:

$$C = \{110100, 101010, 011001, 011110, 101101, 110011, 000111, 000000\}$$

Matriu de control:

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Com que totes les columnes de H són diferents de zero i diferents dues a dues, la distància mínima serà $d = 3$.

(b) La codificació serà: $H \to 110100$, $O \to 101101$, $L \to 011001$, $A \to 110011$. La seqüència de bits que enviarem serà: 110100101101011001110011.

(c) La seqüència rebuda correspon a $w_1 = 100100$, $w_2 = 101101$, $w_3 = 010101$ i $w_4 = 110111$. Construim la taula estàndard:

Líders	Síndrome
000000	000
100000	100
010000	010
001000	001
000100	110
000010	101
000001	011

$H(w_1) = 010$. Hi ha un error en la segona posició, $e = 010000$. $v_1 = w_1 - e = 110100$.
$H(w_2) = 000$. No hi ha hagut error.
$H(w_3) = 111$. No és a la taula. Hi ha hagut més d'un error. No el podem descodificar.
$H(w_4) = 110$. Hi ha un error en la quarta posició, $e = 000100$. $v_1 = w_1 - e = 110011$.

(d) La matriu de control de C' és:

$$H' = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Com la distància mínima de C és 3, aleshores la distància mínima de C' és 4.

(e) Si un codi és 2-corrector aleshores tenim $\lfloor \frac{d-1}{2} \rfloor = 2$; per tant, d ha de ser 5 o 6.

4. (25%) Justifiqueu si són certes o falses les afirmacions següents:

(a) Diem que un mètode xifratge té el secret perfecte si $H(M|C) < H(M)$, on M representa el text en clar i C el text xifrat.

(b) $d = 169$ es la clau privada d'un sistema RSA de clau pública $(n, e) = (299 = 13 \cdot 23, 25)$.

(c) La signatura digital del missatge $m = 15$ amb un sistema RSA de claus $(n, e) = (161 = 7 \cdot 23, 13)$ és 148.

(d) El sobre digital s'utilitza per xifrar i signar conjuntament un missatge.

(e) Amb el Doble DES fem servir dues claus k_1 i k_2 de 56 bits cadascuna i, per tant, la longitud efectiva de la clau és 112 bits.

Solució:

(a) Falsa. El secret és perfecte si $H(M|C) = H(M)$.

(b) Certa. $\phi = 12 \cdot 22 = 264$ i $de \bmod \phi = 169 \cdot 25 \bmod 264 = 1$.

(c) Certa. $\phi = 6 \cdot 22 = 132$ i $d = e^{-1} \bmod \phi = 13^{-1} \bmod 132 = 61$. Finalment, $s = m^d \bmod n = 15^{61} \bmod 161 = 148$.

(d) Falsa. El sobre digital permet enviar un missatge xifrat amb una clau compartida k i la clau k utilitzant un sistema de clau pública.

(e) Falsa. Encara que el nombre de claus teòric és 2^{112}, amb un atac "Meet in the Middle" podem reduir les possibilitats a 2^{57}.