**CONTROL DE TRANSMISIÓN DE DATOS.** **17 de Diciembre de 2004**

MÓNICA AGUILAR

**Notas Importantes:**

1. Los resultados no justificados, no serán tenidos en cuenta.
2. Los problemas se entregan por separado, ponga su nombre y apellidos en cada hoja, enumerándolas.
3. Un error conceptual grave, puede anular todo el problema.

**Problema 1 (40%)**

Sea un canal discreto que representa a una "máquina de escribir ruidosa" en que el símbolo impreso se corresponde con la letra tecleada o con la anterior letra del alfabeto, con la misma probabilidad. Considere que el alfabeto tiene 26 letras (no incluimos la letra Ñ). El diagrama de transiciones del canal es el siguiente:

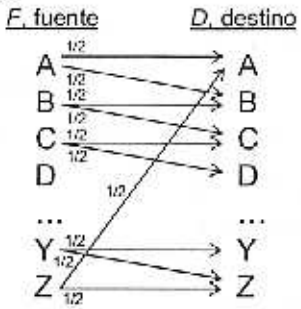



Fig. 1. Diagrama de transiciones del canal "máquina de escribir ruidosa".

0'4 a) Escriba la matriz de probabilidades condicionales de transición, P($D\backslash F$).

0'8 b) Calcule la capacidad de canal.

c) Compare la capacidad de canal obtenida con la de un canal BSC (Canal Binario Simétrico) caracterizado por una probabilidad de error en el bit $p$.

Nota: $f(x) = x \cdot \log_2 \frac{1}{x} + (1-x) \cdot \log_2 \frac{1}{1-x}$ tiene la siguiente representación gráfica:

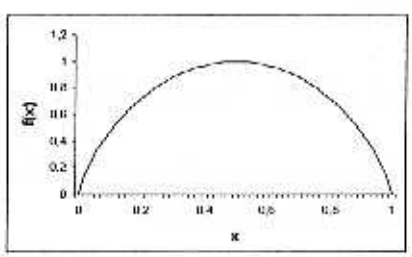



Fig. 2. Representación gráfica de $f(x)$, dato del enunciado. Nótese que $f(0.5)=1$.

0'4 c.1. ¿Con qué canal de los dos se puede transmitir más información por cada uso que se haga de él?

0'4 c.2. ¿Para qué valor de $p$ (probabilidad de error en el bit) el canal BSC será un canal sin ruido? ¿Cuál es la capacidad del canal BSC en este caso?

0'4 c.3. Para qué valor de $p$ no podemos transmitir ninguna información por el canal BSC? ¿Cuál es la capacidad del canal BSC en este caso?

0'8 d) Si mediante el canal "máquina de escribir ruidosa" de la Fig. 1, queremos transmitir símbolos de una fuente con un alfabeto de 26 símbolos equiprobables, ¿cuál será la probabilidad de error, $P_{error}$?

0'8 e) Explique cómo podría utilizarse dicho canal para distinguir a la salida del canal, con $P_{error}=0$, cuál es la entrada.

**Problema 2** (40%)

Sean X e Y dos variables aleatorias discretas con la siguiente función de distribución (**probabilidades conjuntas**):

| Y,X | $X_1$ | $X_2$ | $X_3$ | $X_4$ |
|---|---|---|---|---|
| $Y_1$ | 1/8 | 1/16 | 1/32 | 1/32 |
| $Y_2$ | 1/16 | 1/8 | 1/32 | 1/32 |
| $Y_3$ | 1/16 | 1/16 | 1/16 | 1/16 |
| $Y_4$ | 1/4 | 0 | 0 | 0 |

0'4 a) Calcule la entropía conjunta, H(X, Y).
0'8 b) Calcule la entropía de X, H(X).
0'8 c) Calcule la entropía de Y, H(Y).
0'4 d) Calcule la entropía condicionada, H(Y\X).
0'4 e) Calcule la entropía condicionada, H(X\Y).
0'8 f) Calcule $H(Y\backslash X_1)$.
0'4 g) Calcule la información mutua, I(X, Y).

**Problema 3** (20%)

Sea un sistema RSA con dos usuarios A y B. El usuario B tiene los parámetros $p_B$=7, $q_B$=11, $e_B$=17. El usuario A envía a B el criptograma $C(K_{sesión})$ = 00010001 correspondiente a la codificación RSA de la clave de sesión, $K_{sesión}$.

0'5 a) Obtenga las claves pública y privada de B.
0'5 b) Obtenga la $K_{sesión}$ que B descodifica.

El usuario B envía a A el mensaje M=110011. Considere MPI (más peso a la izquierda).

En un primer caso, suponga que el mensaje se codifica según el algoritmo de cifrado de Vernan (de 6 bits). Para ello B utiliza la $K_{sesión}$ para cifrar el mensaje.

0'5 c) Obtenga el criptograma del mensaje M=110011 que B ha de cifrar.

Suponga ahora que B realiza un cifrado de flujo utilizando un LFSR con polinomio primitivo de conexiones $C(D)=1+D+D^6$. La $K_{sesión}$ es el estado inicial del LFSR (p.ej. para $K_{sesión}$=36, $P^0(D)=100100\equiv 1+D^3$). La secuencia pseudoaleatoria generada se utiliza para cifrar el mensaje. Considere que el primer bit de salida del LFSR es el bit de mayor peso MPI (más peso a la izquierda) de la secuencia pseudoaleatoria generada.

0'5 d) Obtenga el criptograma del mensaje M=110011 que B ha de cifrar.

Cognoms: Control T.D. | Nom: MÓNICA AGUILAR

Centre:

Assignatura / especialitat: | 17/12/04

DNI | Núm. matrícula | Cicle | Grup

P1

(a)

$F$ — Canal — $D$

$A_i$, $m=26$ → $B_j$, $n=26$

$$P(D\backslash F) = \begin{array}{c|cccccccccccc} & B_1=A & B_2=B & B_3=C & \cdots & B_{25}=Y & B_{26}=Z \\ \hline A_1=A & 1/2 & 1/2 & 0 & \cdots & 0 & 0 \\ A_2=B & 0 & 1/2 & 1/2 & 0 & \cdots & 0 & 0 \\ A_3=C & 0 & 0 & 1/2 & 1/2 & 0 & \cdots & 0 & 0 \\ \vdots & & & & & & & & \vdots \\ A_{25}=Y & 0 & \cdots & & & 0 & 1/2 & 1/2 \\ A_{26}=Z & 1/2 & 0 & \cdots & & & & 0 & 1/2 \end{array}$$

(b)

$$C\left[\frac{\text{bits}}{\text{símbolo}}\right] = \max_{\{p(A_i)\}} I(F,D) = \max_{\{p(A_i)\}} \left[H(D) - H(D\backslash F)\right]$$

$$H(D\backslash F) = \sum_i p(A_i)\cdot H(D\backslash A_i) = \sum_i p(A_i) = 1 \text{ bit/símbolo}$$

(Canal simétrico)

$$H(D\backslash A_1) = 2\cdot\frac{1}{2}\cdot\log_2 2 = 1$$

$$C = \max_{\{p(A_i)\}} H(D) - 1$$

$$H(D) = \sum_j p(B_j)\cdot\log_2\frac{1}{p(B_j)}$$

$$p(B_j) = \frac{1}{2}\cdot P(A_j) + \frac{1}{2}P(A_{j-1})$$

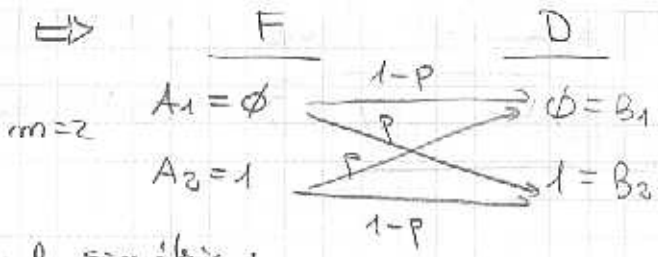
Si $p(A_i) = \frac{1}{m} = \frac{1}{26}, \forall i \Rightarrow p(B_j) = \frac{1}{2}\cdot\frac{1}{26} + \frac{1}{2}\cdot\frac{1}{26} = \frac{1}{26}, \forall j$

$$\Rightarrow \max_{\{p(A_i)\}} H(D) \leq \log_2 n \quad \text{con} = \text{si } p(B_j) = \frac{1}{n}, \forall j$$

$$C = \log_2 26 - 1 = \log_2(2\cdot 13) - 1 = \log_2 2 + \log_2 13 - 1$$

$$\boxed{C = \log_2 13 \left[\frac{\text{bits}}{\text{símbolo}}\right] = 3'7 \frac{\text{bits}}{\text{símbolo}}}$$

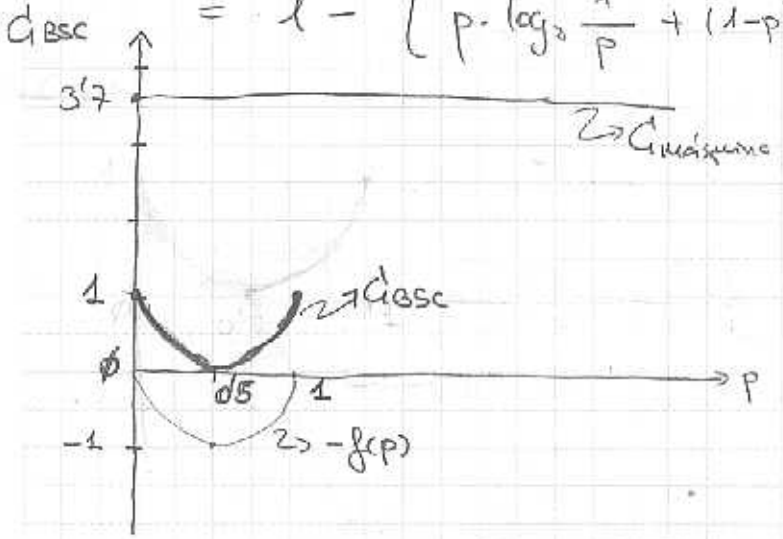
(c) BSC ⇒




$$P(D|F) = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix} \begin{matrix} A_1 \\ A_2 \end{matrix} \qquad \begin{matrix} B_1 & B_2 \end{matrix}$$

Es un canal simétrico:

$$C_{BSC} = \log_2 n - \left[ p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{1-p} \right] \overset{n=2}{=} 1 - \left[ p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{1-p} \right] = 1 - f(p)$$




c1) $C_{BSC} \leq 1$ bit/símbolo

$C_{máquina} = 3'7$ bit/símbolo

Con la "máquina ruidosa".

c2) Para $p = \emptyset$ ó $p = 1$. En ambos casos, el canal queda determinado, es un canal sin ruido:

$H(F|D) = \emptyset$ → sin pérdida: conocida la salida, la entrada queda determinada.

$H(D|F) = \emptyset$ → determinista: " entrada, " salida "

En ambos casos, $C_{BSC} = 1$ bit/símbolo

c3) Para $p = 0'5$. En este caso es un canal aleatorio.

$C_{BSC} = \emptyset$ bit/símbolo

(d) Si recibimos $B_j$, puede ser que se transmitiera $A_j$ o $A_{j-1}$ con la misma probabilidad.

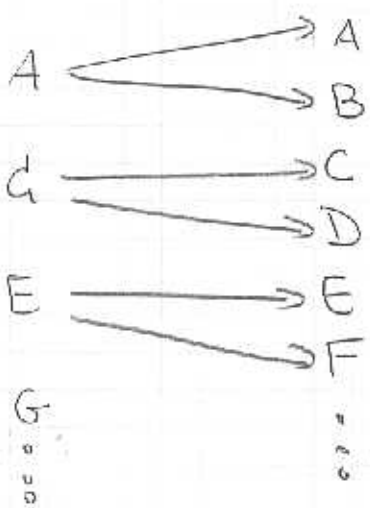
$$P_{error} = 1/2$$

(e)

Sí que podría utilizarse codificando esa fuente en 13 símbolos de canal bien elegidos:

A, a, E, G, I, ....., Y

Así, cada entrada nos da un conjunto de salidas DISJUNTO con los demás conjuntos:




Así puedo distinguir a la salida, cuál fue la entrada sin ninguna duda.

**P2**

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y) =$$
$$= \sum_i \sum_j p(x_i, y_j) \cdot \log_2 \frac{1}{p(x_i, y_j)}$$

$$H(Y|X) = \sum_i \sum_j p(x_i, y_j) \cdot \log_2 \frac{1}{p(y_j|x_i)}$$

$H(X,Y) \leq H(X) + H(Y)$

$H(X,Y) = H(X) + H(Y)$ si son v.a. independientes.

$H(X|Y) \leq H(X)$

$H(Y|X) \leq H(Y)$

$I(X,Y) = H(X) - H(X|Y) = I(Y,X) = H(Y) - H(Y|X)$

$I(X,Y) \leq \min\{H(X), H(Y)\}$

(a) $H(X,Y) = \sum_i \sum_j p(x_i, y_j) \cdot \log_2 \frac{1}{p(x_i, y_j)} =$

$= p(x_1,y_1)\cdot\log_2\frac{1}{p(x_1,y_1)} + p(x_1,y_2)\cdot\log_2\frac{1}{p(x_1,y_2)} + \dots + p(x_1,y_4)\cdot\log_2\frac{1}{p(x_1,y_4)}$

$+ p(x_2,y_1)\cdot\log_2\frac{1}{p(x_2,y_1)} + \dots + p(x_2,y_4)\cdot\log_2\frac{1}{p(x_2,y_4)} +$

$+ p(x_3,y_1)\cdot\log_2\frac{1}{p(x_3,y_1)} + \dots + p(x_3,y_4)\cdot\log_2\frac{1}{p(x_3,y_4)} +$

$+ p(x_4,y_1)\cdot\log_2\frac{1}{p(x_4,y_1)} + \dots + p(x_4,y_4)\cdot\log_2\frac{1}{p(x_4,y_4)} =$

$= \frac{1}{8}\cdot\log_2 8 + \frac{2}{16}\cdot\log_2 16 + \frac{1}{4}\cdot\log_2 4 + \frac{2}{16}\cdot\log_2 16 + \frac{1}{8}\log_2 8 +$

$+ \frac{2}{32}\cdot\log_2 32 + \frac{1}{16}\log_2 16 + \frac{2}{32}\cdot\log_2 32 + \frac{1}{16}\cdot\log_2 16 =$

$= \frac{1}{4}\cdot 3 + \frac{3}{8}\cdot 4 + \frac{1}{2} + \frac{1}{8}\cdot 5 = \frac{17}{8} + \frac{10}{8} = \frac{27}{8} = \underline{3'375 \ \frac{\text{bits}}{\text{símbolo}}}$

(b) $p(x_1) = \sum_{j=1}^{4} p(x_1, y_j) = \frac{1}{8} + \frac{2}{16} + \frac{1}{4} = 1/2$

$p(x_2) = \sum_{j=1}^{4} p(x_2, y_j) = \frac{2}{16} + \frac{1}{8} = 1/4$

$p(x_3) = \sum_{j=1}^{4} p(x_3, y_j) = \frac{2}{32} + \frac{1}{16} = 1/8$

$p(x_4) = \sum_{j=1}^{4} p(x_4, y_j) = 1/8$

$\begin{cases} p(x_1, y_j) = p(x_1)\cdot p(y_j \mid x_1) \\ \sum_j p(x_1, y_j) = p(x_1)\cdot \underbrace{\sum_j p(y_j \mid x_1)}_{1} \\ \quad = p(x_1) \end{cases}$

$H(X) = \sum_{i=1}^{4} p(x_i)\cdot\log_2\frac{1}{p(x_i)} = \frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 + \frac{2}{8}\log_2 8 = \frac{7}{4} = 1'75 \ \frac{\text{bits}}{\text{símbolo}}$

(c) $p(Y_j) = \sum_{i=1}^{4} p(y_j \mid x_i)$

$p(Y_1) = \frac{1}{8} + \frac{1}{16} + \frac{2}{32} = 1/4 = p(Y_2) = p(Y_3) = p(Y_4)$

$H(Y) = 4\cdot\frac{1}{4}\cdot\log_2 4 = \underline{2 \ \text{bits/símbolo}}$

(d) $\boxed{H(Y\backslash X) = H(X,Y) - H(X) = \frac{27}{8} - \frac{7}{4} = \frac{13}{8} = 1'625 \frac{\text{bits}}{\text{símbolo}}}$

Nótese que $H(Y\backslash X) \leq H(Y) = 2$

* Otro modo de hacerlo:

$\Rightarrow H(Y\backslash X) = \sum_i \sum_j p(x_i, y_j) \cdot \log_2 \frac{1}{p(y_j \backslash x_i)}$

$P(Y\backslash x_i) = \frac{P(x_i, y)}{P(x_i)}$

| $Y\backslash X$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ |
|---|---|---|---|---|
| $y_1$ | 1/4 | 1/4 | 1/4 | 1/4 |
| $y_2$ | 1/8 | 1/2 | 1/4 | 1/4 |
| $y_3$ | 1/8 | 1/4 | 1/2 | 1/2 |
| $y_4$ | 1/2 | $\phi$ | $\phi$ | $\phi$ |

P.ej. $\Rightarrow P(y_2\backslash x_1) = \frac{P(x_1, y_2)}{P(x_1)} = \frac{1/16}{1/2} = 1/8$

(b) $\boxed{H(Y\backslash x_1) = \frac{1}{4}\cdot\log_2 4 + \frac{2}{8}\cdot\log_2 8 + \frac{1}{2}\log_2 2 = \frac{1}{2} + \frac{3}{4} + \frac{1}{2} = \frac{7}{4} \text{ bits/símbolo} = 1'75 \text{ b/s}}$

$H(Y\backslash x_2) = \frac{2}{4}\cdot\log_2 4 + \frac{1}{2}\log_2 2 = 1 + \frac{1}{2} = 3/2$

$H(Y\backslash x_3) = H(Y\backslash x_4) = \frac{2}{4}\log_2 4 + \frac{1}{2}\log_2 2 = 3/2$

$\Rightarrow H(Y\backslash X) = H(Y\backslash x_1)\cdot p(x_1) + H(Y\backslash x_2)\cdot p(x_2) + H(Y\backslash x_3)\cdot p(x_3) + H(Y\backslash x_4)\cdot P(x_4) = \frac{7}{4}\cdot\frac{1}{2} + \frac{3}{2}\cdot\frac{1}{4} + \frac{3}{2}\cdot\frac{2}{8} = \frac{13}{8} = 1'625 \frac{\text{bits}}{\text{símbolo}}$

(c) $\boxed{H(X\backslash Y) = H(X,Y) - H(Y) = \frac{27}{8} - 2 = \frac{11}{8} = 1'375 \text{ bits/símbolo}}$

(q) $\boxed{I(X,Y) = H(X) - H(X\backslash Y) = \frac{7}{4} - \frac{11}{8} = \frac{3}{8} = 0'375 \text{ bits/símbolo}}$

$I(X,Y) = H(Y) - H(Y\backslash X) = 2 - \frac{13}{8} = \frac{3}{8}$ $\boxed{I(X,Y) = H(X) + H(Y) - H(X,Y)}$

**P3** ⓐ **Clave pública (B) = $(e_B, N_B) = (17, 77)$**

$N_B = p_B \cdot q_B = 7 \cdot 11 = 77$

$\phi(N_B) = (p_B - 1)\cdot(q_B - 1) = 6 \cdot 10 = 60$

¿ $mcd(e_B, \phi(N_B)) = 1$ ? ($e_B = 17$, $\phi(N_B) = 60$)

| 60 \| 17 | 17 \| 9 | 9 \| 8 | 8 \| 1 |
|---|---|---|---|
| 9 3 | 8 1 | (1) 1 | ϕ \| 8 |

mcd

OK! $e_B$ válido. $\exists\ d_B = e_B^{-1} \bmod \phi(N_B)$ :

$d_B \cdot e_B = 1 + k \cdot \phi(N_B)$ // $d_B = \frac{1 + k\cdot 60}{17} = \frac{(17\cdot 3 + 9)k + 1}{17} = 3k + \underbrace{\frac{9k+1}{17}}_{k_1}$

$k_1 = \frac{9k+1}{17}$ // $k = \frac{17\cdot k_1 - 1}{9} = \frac{(9+8)k_1 - 1}{9} = k_1 + \underbrace{\frac{8k_1 - 1}{9}}_{k_2}$

$k_2 = \frac{8k_1 - 1}{9}$ // $k_1 = \frac{9k_2 + 1}{8} = \frac{(8+1)k_2 + 1}{8} = k_2 + \frac{k_2 + 1}{8} \Rightarrow k_2 = 7$

$k_1 = 8 \longrightarrow k = 15 \longrightarrow$ **$d_B = 53$ = Clave Secreta (B)**

ⓑ $K_{sesión} = C_1^{d_B} \bmod N_B$, con $C_1 = 10001 \equiv 17$ ($2^4$, $2^0$)

$K_{sesión} = 17^{53} \bmod 77 = ((((17^2 \cdot 17)^2)^2 \cdot 17)^2)^2 \cdot 17 \bmod 77$

$53 \equiv 110101$

$17^2 = 289 \xrightarrow{mod\,77} 58 \cdot 17 = 986 \xrightarrow{mod\,77} 62^2 = 3844 \xrightarrow{mod\,77} 71$

$71^2 = 5041 \cdot 17 = 85697 \xrightarrow{mod\,77} 73^2 = 5329 \longrightarrow 16^2 = 256$

$256 \longrightarrow 25 \cdot 17 = 425 \xrightarrow{mod\,77} 40$ // **$K_{sesión} = 40$**

ⓒ $K_{sesión} = 40 \equiv 101000$ ($2^5$, $2^3$)

$H = 110011$

$C_1 = H \oplus K_{sesión}$

$110011 \oplus 101000 = 011011$

**Criptograma (Vernam) = 011011**

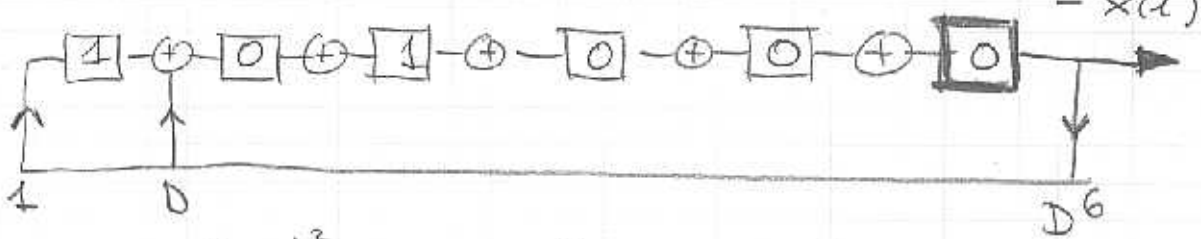
Cognoms | Nom

Centre

Assignatura / especialitat

DNI | Núm. matrícula | Curs | Grup | Data

d) secuencia pseudoaleatoria = $x(i^0)$




Ksesión = 40 $\equiv$ $1\,0\,1\,\overset{D^2}{1}\,0\,0\,0 = p^{(0)}(D) = 1 + D^2$

$p^{(0)}(D) = 1\,0\,1\,0\,0\,\boxed{0} \rightarrow 1^{er}$ bit

$p^{(1)}(D) = 0\,1\,0\,1\,0\,\boxed{0}$

$p^{(2)}(D) = 0\,0\,1\,0\,1\,\boxed{0}$

$p^{(3)}(D) = 0\,0\,0\,\overset{D^3}{1}\,0\,\boxed{\overset{D^5}{1}}$ · $D \cdot p^{(3)}(D)$

$p^{(4)}(D) = \overset{1}{1}\,\overset{D}{1}\,0\,0\,\overset{D^4}{1}\,\boxed{0} \longrightarrow D^6 + D^4$ | $D^6 + D + 1$

$D^6 + D + 1$ | 1

$D^4 + D + 1 = p^{(4)}(D)$

$p^{(5)}(D) = 0\,1\,1\,0\,0\,\boxed{1}$

$x(i^0) = 0\,0\,0\,1\,0\,1$

$1^{er}$ bit ↑

$C_i = M \oplus x(i)$

$1\,1\,0\,0\,1\,1$

$\oplus\ 0\,0\,0\,1\,0\,1$

$1\,1\,0\,1\,1\,0$

**Criptograma (LFSR) = 110110**