UNIVERSITAT POLITÈCNICA DE CATALUNYA

$P^{(n)}(D) = D^n \cdot P^{(0)}(D) \bmod G(D)$

- [ ] E.T.S. d'Enginyeria de Telecomunicació de Barcelona
- [ ] E.T.S. d'Enginyers de Camins, Canals i Ports de Barcelona
- [ ] Facultat d'Informàtica de Barcelona

Titulació

Solución Control 22-Mayo-2002

Assignatura

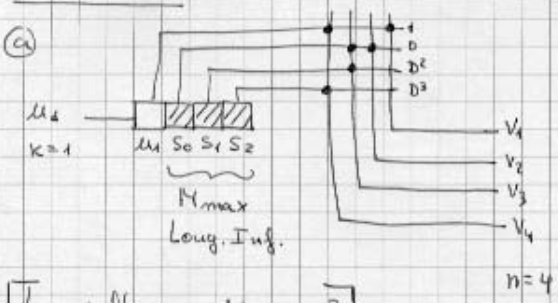
(Mónica Aguilar)

Cognoms — Nom

Pàgina 1 de 5

Problema 1

(a)



$n = k + r$

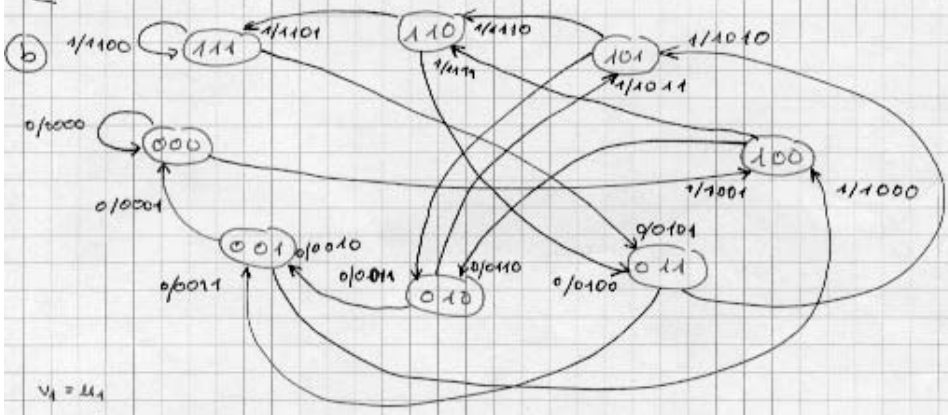
$\text{tasa} = \frac{k}{n} = \frac{k}{4} \Rightarrow k = 1$

$4 = 1 + r \Rightarrow \boxed{r = 3}$

[Long. influencia = $M_{max} = 3$]

[Nº Estados = $S = 2^M = 2^3 = 8$]

(b)



$V_1 = u_1$

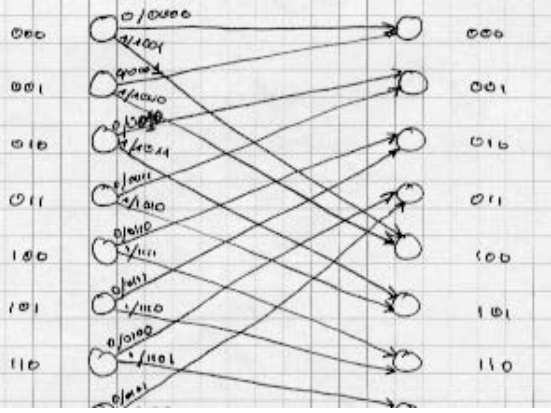
$V_2 = S_0$

$V_3 = S_0 \oplus S_1$

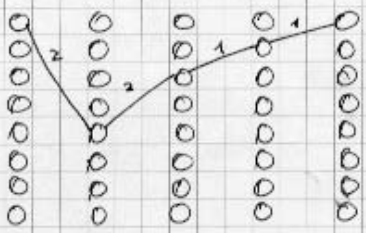
$V_4 = u_1 \oplus S_2$

Ecuaciones del Codificador.

Diagrama de Entrejada TCM:



(c)

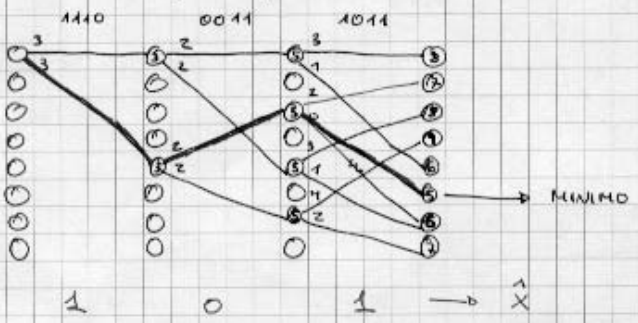


$d_{libre} = 2+2+1+1 = 6$

(d) $X = 1110$ ¿ Y?

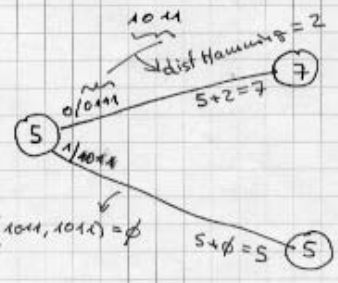
Estado	Entra	Sale	Nuevo Estado
000	1	1001	100
100	1	1111	110
110	1	1101	111
111	0	0101	011

(e) $Y = 1110 \,|\, 0011 \,|\, 1011$ ¿ $\hat{X}$?



1 0 1 → $\hat{X}$

En detalle un ejemplo:



Problema 2

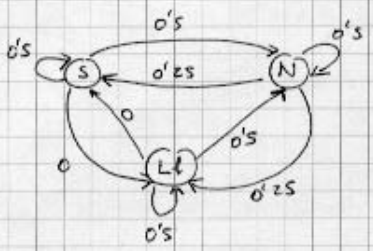
(a) Piden la entropía de la fuente "El motorista ganador es ..."

$$H(F) = P(S)\cdot H(F\backslash S) + P(N)\cdot H(F\backslash N) + P(Ll)\cdot H(F\backslash Ll)$$

$$H(F\backslash S) = 0'4\cdot \log_2 \frac{1}{0'4} + 2\cdot 0'3\cdot \log_2 \frac{1}{0'3} = 1'5709$$

$$H(F\backslash N) = 0'1\cdot \log_2 \frac{1}{0'1} + 0'35\cdot \log_2 \frac{1}{0'35} + 0'3\cdot \log_2 \frac{1}{0'3} + 0'25\cdot \log_2 \frac{1}{0'25} = 1'8834$$

$$H(F\backslash Ll) = 2\cdot 0'5\cdot \log_2 \frac{1}{0'5} = 1$$



Ecuaciones de equilibrio:

$$P(S) = P(S)\cdot 0'5 + P(N)\cdot 0'25 + P(Ll)\cdot 0$$

$$P(N) = P(S)\cdot 0'5 + P(N)\cdot 0'5 + P(Ll)\cdot 0'5$$

$$P(Ll) = P(S)\cdot 0 + P(N)\cdot 0'25 + P(Ll)\cdot 0'5$$

Y además: $P(S)+P(N)+P(Ll)=1$

$$0'5\cdot P(S) = 0'25\cdot P(N)$$

$$0'5\cdot P(N) = 0'5\cdot P(S) + 0'5\cdot P(Ll)$$

$$0'5\cdot P(Ll) = 0'25\cdot P(N)$$

$$\frac{1}{2}P(N) + P(N) + \frac{1}{2}P(N) = 1$$

$$2\cdot P(N) = 1$$

$$\boxed{P(N) = \frac{1}{2}}$$

$$\begin{cases} P(S) = \frac{1}{2}P(N) \\ P(N) = P(S) + P(Ll) \\ P(Ll) = \frac{1}{2}P(N) \end{cases}$$

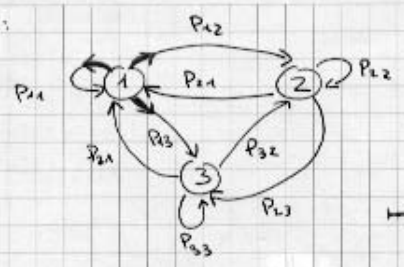
$$\boxed{P(S) = \frac{1}{4}}$$

$$\boxed{P(Ll) = \frac{1}{4}}$$

bits necesarios para comunicar el ganador.

$$\boxed{H(F) = \frac{1}{4}\cdot 1'5709 + \frac{1}{2}\cdot 1'8834 + \frac{1}{4}\cdot 1 = 1'5844 \text{ bits}}$$

En general:



* Ec. equilibrio: prob salen = prob entran

$\mapsto P(1)\cdot(P_{12}+P_{13}) = P(2)\cdot P_{21} + P(3)\cdot P_{31}$

* Cadena Markov $\rightarrow \mu_0 \cdot P = \mu_1 \xrightarrow{\infty} \bar{\mu}\cdot P = \bar{\mu}$

$$\begin{pmatrix} p(1) & p(2) & p(3) \end{pmatrix} = \begin{pmatrix} p(1) & p(2) & p(3) \end{pmatrix} \cdot \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{pmatrix}$$

· matriz de transiciones.
· las filas suman 1.

$$p(1) = p(1)\cdot p_{11} + p(2)\cdot p_{21} + p(3)\cdot p_{31}$$

$$\mapsto p(1)\cdot \underbrace{(1-p_{11})}_{p_{12}+p_{13}} = p(2)\cdot p_{21} + p(3)\cdot p_{31}$$

Es decir, que es lo mismo. Se puede resolver de las dos formas.

(b) Como ya se sabe qué tiempo hace en el ámbito local del circuito, sólo hay que usar un código Huffman diferente para cada posible tiempo.

Sol:

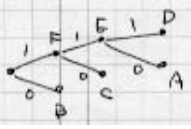
A	0
B	10
C	11
D	—

Llueve:

A	—
B	0
C	—
D	1

Nubes:

B	0'35		B	0'35	F 0'65
C	0'3		E	0'35	B 0'35
D	0'25		C	0'3	
A	0'1	E 0'35			F 0'65



A	110
B	0
C	10
D	111

Codificación del ganador de la carrera, para cada tiempo que puede hacer hoy:

	A	B	C	D
sol	0	10	11	–
lluvia	–	0	–	1
nubes	110	0	10	111

(c) Nº de bits necesarios para comunicar el tiempo que hace hoy.

Suponemos que ayer ya les comunicamos el tiempo, ya saben qué tiempo hizo ayer en el Circuito.

t_a = tiempo que hizo ayer
t_h = " que hace hoy
$\Big\}$ $t_a, t_h \in \{S, N, Ll\}$

Nos piden la $\overline{I} = H$ [bits] de la fuente con memoria "Qué tiempo hace hoy, conocido el de ayer?"

$$H(t_h \mid t_a) = \sum p(t_h, t_a) \cdot \log_2 \frac{1}{p(t_h \mid t_a)}$$

Prob. conjunta: $p(t_h, t_a) = p(t_a, t_h) = p(t_a) \cdot p(t_h \mid t_a)$

$P(S,S) = P(S) \cdot P(S \mid S) = \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}$

$P(S,N) = P(S) \cdot P(N \mid S) = \frac{1}{4} \cdot \frac{1}{2} = 1/8$

$P(S,Ll) = P(S) \cdot P(Ll \mid S) = \frac{1}{4} \cdot 0 = 0$

$P(N,S) = P(N) \cdot P(S \mid N) = \frac{1}{2} \cdot \frac{1}{4} = 1/8$

$P(N,N) = P(N) \cdot P(N \mid N) = \frac{1}{2} \cdot \frac{1}{2} = 1/4$

$P(N,Ll) = P(N) \cdot P(Ll \mid N) = \frac{1}{2} \cdot \frac{1}{4} = 1/8$

$P(Ll,S) = P(Ll) \cdot P(S \mid Ll) = \frac{1}{4} \cdot 0 = 0$

$P(Ll,N) = P(Ll) \cdot P(N \mid Ll) = \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}$

$P(Ll,Ll) = P(Ll) \cdot P(Ll \mid Ll) = \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}$

$$H(t_h \setminus t_a) = \frac{1}{8}\cdot\log_2\frac{1}{1/2} + \frac{1}{8}\cdot\log_2\frac{1}{1/2} + \phi + \phi + \frac{1}{8}\cdot\log_2\frac{1}{1/2} +$$

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

$$= \frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{2}{8}+\frac{1}{4}+\frac{2}{8} =$$

$= 1'25$ bits (*)

Nº bits necesarios para comunicar el tiempo de hoy, sabido el de ayer.

(d)

		Tiempo que hizo ayer, t_a		
		S	N	Ll
Tiempo que hace hoy, t_h	S	0'5	0'25	0
	N	0'5	0'5	0'5
	Ll	0	0'25	0'5

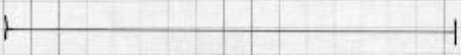
Codificación del tiempo que hace hoy, para cada caso del tiempo que hizo ayer:

	ayer hizo sol	ayer nubes	ayer llovió
S	1	10	—
N	0	0	1
Ll	—	11	0

(e) Mensajes para comunicar lejos que:

ayer hizo nublado y hoy sol ⇒ 10

Ha ganado G ⇒ 11 (hoy hace sol)



(*) De otra forma:

$$H(F) = \overset{1/4}{P(S)}\cdot H(F \setminus S)^{\text{ayer}} + \overset{1/2}{P(N)}\cdot H(F \setminus N) + \overset{1/4}{P(Ll)}\cdot H(F \setminus Ll) = \frac{1}{4}\cdot 1 + \frac{1}{2}\cdot\frac{3}{2} + \frac{1}{4}\cdot 1 = 1'25$$

$$\downarrow$$

$$P(S \setminus S)\cdot\log_2\frac{1}{P(S \setminus S)} + P(Ll \setminus S)\cdot\log_2\frac{1}{P(Ll \setminus S)} + P(N \setminus S)\cdot\log_2\frac{1}{P(N \setminus S)}$$

$$\overset{1/2}{P(S \setminus S)}\cdot\log_2\frac{1}{P(S \setminus S)} \quad \overset{\text{hoy ayer}}{\phi} \quad \overset{1/2}{P(N \setminus S)}\cdot\log_2\frac{1}{P(N \setminus S)}$$

$$P(S \setminus N)\cdot\log_2\frac{1}{P(S \setminus N)} + P(N \setminus N)\cdot\log_2\frac{1}{P(N \setminus N)} + P(Ll \setminus N)\cdot\log_2\frac{1}{P(Ll \setminus N)}$$

$$\overset{1/4}{P(S \setminus N)} \quad \overset{1/2}{P(N \setminus N)} \quad \overset{1/4}{P(Ll \setminus N)}$$

$$P(S \setminus Ll)\cdot\log_2\frac{1}{P(S \setminus Ll)} + P(N \setminus Ll)\cdot\log_2\frac{1}{P(N \setminus Ll)} + P(Ll \setminus Ll)\cdot\log_2\frac{1}{P(Ll \setminus Ll)}$$

$$\overset{\phi}{P(S \setminus Ll)} \quad \overset{1/2}{P(N \setminus Ll)} \quad \overset{1/2}{P(Ll \setminus Ll)}$$

(c)

De otra forma:

$$H(F) = P(S)\cdot H(F|S) + P(N)\cdot H(F|N) + P(Ll)\cdot H(F|Ll)$$

$H(F)$: qué tiempo hace hoy, conocido el que hizo ayer?

$P(S)$: prob. ayer hizo sol

$H(F|S)$: Entropía Fuente, si ayer hizo sol.

$P(S) = \frac{1}{4} = P(Ll)$

$P(N) = 1/2$

$$H(F|S) = P(\text{hoy ayer sol}|\text{ayer sol})\cdot \log_2 \frac{1}{P(\text{hoy ayer sol}|\text{ayer sol})} + P(\text{hoy ayer llueve}|\text{ayer sol})\cdot \log_2 \frac{1}{P(\text{hoy ayer llueve}|\text{ayer sol})} + P(N|S)\cdot \log_2 \frac{1}{P(N|S)} =$$

$$= \frac{1}{2}\cdot \log_2 \frac{1}{1/2} + 0 + 1/2 \cdot \log_2 \frac{1}{1/2} = \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot 1 = 1$$

$$H(F|N) = P(\text{hoy ayer sol}|\text{ayer nubes})\cdot \log_2 \frac{1}{P(\text{hoy ayer sol}|\text{ayer nubes})} + P(\text{hoy ayer nubes}|\text{ayer nubes})\cdot \log_2 \frac{1}{P(\text{hoy ayer nubes}|\text{ayer nubes})} + P(\text{hoy ayer llueve}|\text{ayer nubes})\cdot \log_2 \frac{1}{P(\text{hoy ayer llueve}|\text{ayer nubes})} =$$

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

$$= \frac{1}{4}\cdot 2 + \frac{1}{2}\cdot 1 + \frac{1}{4}\cdot 2 = \frac{3}{2}$$

$$H(F|Ll) = P(S|Ll)\cdot \log_2 \frac{1}{P(S|Ll)} + P(N|Ll)\cdot \log_2 \frac{1}{P(N|Ll)} + P(Ll|Ll)\cdot \log_2 \frac{1}{P(Ll|Ll)}$$

$$= 0 + \frac{1}{2}\cdot \log_2 \frac{1}{1/2} + \frac{1}{2}\cdot \log_2 \frac{1}{1/2} = \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot 1 = 1$$

$$H(F) = \frac{1}{4}\cdot 1 + \frac{1}{2}\cdot \frac{3}{2} + \frac{1}{4}\cdot 1 = \frac{1}{4} + \frac{3}{4} + \frac{1}{4} = \frac{1}{4} + 1 = 1'25 \text{ bits}$$

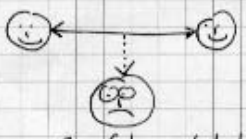
Problema 3

(a) Confidencialidad: Protección de la información frente al atacante pasivo. Se consigue PRIVACIDAD, que nadie más entienda la información.

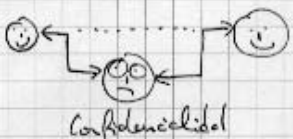
Autenticación de origen: El comunicante sea quien dice ser.

Autenticación de Contenido: Que nadie haya modificado el contenido del mensaje. Protección de la información frente al atacante activo.

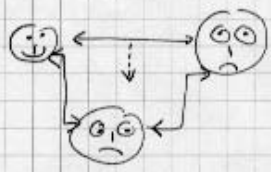
Verificabilidad: Firma Digital. Servicio que protege de un comunicante falso, que se haya aliado con el atacante.



Confidencialidad



Confidencialidad
Autenticidad



Confidencialidad
Verificabilidad

(b) Mediante la Firma Digital con Función Resumen (Hash).

A

$M \rightarrow R(M)$

$FD(M) = D_{S_A}(R(M))$ ⟶

$C_{AB} = E_{P_B}(M)$ ⟶

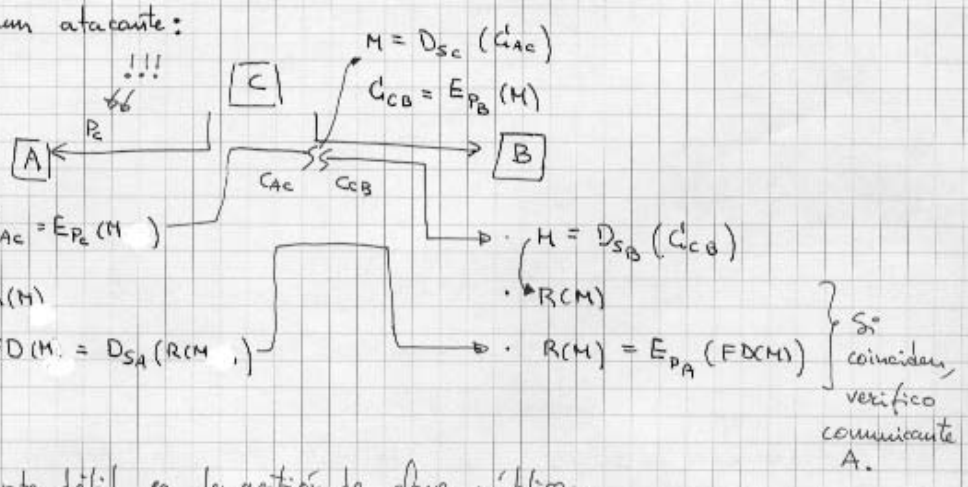
B

$E_{P(A)}(FD(M)) = R(M)$ ⟵

$M_{AB} = D_{S_B}(C_{AB})$

$M_{AB} \rightarrow R(M)$ ⟵

Ante un atacante:



El pto. débil es la gestión de claves públicas.
Debo confiar en una entidad certificadora de claves públicas, "notario".

(c)

1.- Elegir p, q primos
2.- $N = p \cdot q$
3.- $\phi(N) = (p-1)\cdot(q-1)$
4.- $e \mid mcd(e, \phi(N)) = 1$
clave pública $= (e, N)$

5.- $d = e^{-1} \bmod \phi(N)$
$d \cdot e = k \cdot \phi(N) + 1$
clave privada $= (d, N)$
6.- $M < N$
$C = M^e \bmod N$
7.- $M = C'^d \bmod N$

(d)

$p = 7$, $q = 13$
$N = p \cdot q = 91$
$\phi(N) = (p-1)\cdot(q-1) = 72$
$e = 3, 5, 7, ll \ldots$ tal que $mcd(e, \phi(N)) = 1$.
$72 = 24 \cdot 3 \rightarrow e \neq 3$
$e = 5 \Rightarrow mcd(5, 72) = 1$ $\qquad 72 = 3^2 \cdot 2^3$
clave pública $= (5, 91)$

$d = e^{-1} \bmod \phi(N) = 5^{-1} \bmod 72$

$d \cdot e = k \cdot \phi(N) + 1 \Rightarrow d = \frac{k \cdot 72 + 1}{5}$

$d = \frac{k \cdot 14 \cdot 5 + 1 + 2k}{5} = \frac{k \cdot 14 \cdot 5}{5} + \frac{1+2k}{5}$

$d = 14 \cdot k + \frac{1+2k}{5}$

entero entero $\Rightarrow \frac{1+2k}{5} =$ entero

$1 + 2k = 5$

$k = 2$

$72 \mid 5$
$2 \quad 14$

$72 = 14 \cdot 5 + 2$

$d = 14 \cdot 2 + 1 = 29$

clave privada = (29, 91)

$M = 37$

$C = M^e \bmod N = 37^5 \bmod 91$

$5 \equiv 101$
$4\,2\,1$

$M^5 = (M^2)^2 \cdot M$

$M^2 = 1369 \xrightarrow{\bmod 91} 4$

$4^2 = 16 \longrightarrow 16$

$16 \cdot M = 592 \longrightarrow [46 = C]$

$C = 46$

$M = C^d \bmod N = 46^{29} \bmod 91$

$29 \equiv 1\,1\,1\,0\,1$
$2^4\,2^3\,2^2\,2^1\,2^0$

$C^{29} = \left(\left((C^2 \cdot C)^2 \cdot C\right)^2\right)^2 \cdot C$

$C^2 = 2116 \xrightarrow{\bmod 91} 23$

$23 \cdot 46 = 1058 \longrightarrow 57$

$57^2 = 3249 \longrightarrow 64$

$64 \cdot C = 2944 \longrightarrow 32$

$32^2 = 23 \longrightarrow 23$

$23^2 = 529 \longrightarrow 74$

$74 \cdot C = 3404 \longrightarrow [37 = M]$