EXAMEN DE TRANSMISIÓN DE DATOS
10 de junio de 2002

NOTAS IMPORTANTES:
Toda hoja de respuestas que no esté completamente identificada será anulada.
La numeración en la hoja de respuestas es la de la *izquierda* (*correlativas*)
No se responderá a ninguna pregunta sobre el enunciado. El alumno responderá según su criterio pudiendo realizar las alegaciones que considere oportunas en la forma y plazo que se anunciará una vez se hagan públicas las calificaciones provisionales.
Úsense las expresiones:

$$F_0 = \sum_{k=0}^{M-1}\sum_{k'=0}^{M-1} a(k)a_*(k')\rho_s(k'-k) - 2\Re\{\sum_{k=0}^{M-1} a(k)\tilde{y}(k)\}$$

$$\sigma_i = 2Re\{a^*(M+i)\sum_{j=1}^{M} a(M+i-j)\rho_s(j)\} +$$

$$+|a(M+i)|^2\rho_s(0) - 2Re\{a^*(M+i)\tilde{y}(M+i)\}$$

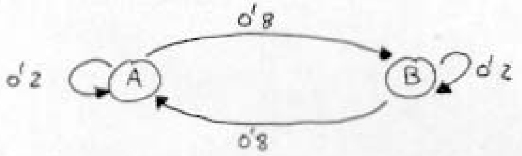
CÓDIGO DE LA PRUEBA: 230 1510 00 0

1. Una fuente emite dos símbolos, A y B, con las probabilidades

$$p(A|A) = 0.2, p(A|B) = 0.8$$

Para una extensión de fuente de orden 1 (agrupaciones de dos símbolos) ¿cuánto vale su longitud media de codificación (Huffman)?

(a) 1.8
(b) 1.3
(c) 1.1
(d) Ninguna de las anteriores



Por simetría, saldrá que $P(A) = P(B) = 0'5$.

$\Rightarrow$ $P(AA) = P(BB)$
$P(AB) = P(BA)$

$P(AA) = \underbrace{P(A \backslash A)}_{\text{ir al estado A.}} \cdot \underbrace{P(A)}_{\text{desde estado A,}} = 0'2 \cdot 0'5 = 0'1 \quad = P(BB)$

$P(AB) = P(B \backslash A) \cdot P(A) = 0'8 \cdot 0'5 = 0'4 \quad = P(BA)$

AB 0'4
BA 0'4
AA 0'1 } 0'2 F } 0'66 ⇒ 0'66 / 0'4 AB
BB 0'1

AB	0
BA	11
AA	101
BB	100

$\bar{\ell} = 1 \cdot 0'4 + 2 \cdot 0'4 + 3 \cdot 0'1 + 3 \cdot 0'1 = 1'8$ bits

2. En un juego de azar se lanzan 7 monedas y la apuesta es hacer un pronóstico sobre los resultados de dichos lanzamientos. ¿Cuál de las siguientes apuestas no forma parte del conjunto mínimo de apuestas que aseguran, al menos, 6 aciertos? (*cara*=*c* *cruz*=†)

(a) c † † † cc†

(b) ccccccc

(c) ccc † † cc

(d) Todas las anteriores forman parte del conjunto mínimo

El código (7,4) de Hamming es 1 perfecto

$\Rightarrow d_{min} = 3$

Si apostamos a todas las palabras código

Hay $\Rightarrow 2^4$:

→ Si el resultado es palabra código, acertamos 7.

→ Si no lo es, existe una palabra código que dista 1 $\Rightarrow$ acertamos 6.

Por ser 1-perfecto se garantiza que es la apuesta ÓPTIMA.

La respuesta c no constituye una palabra código del código (7,4), por lo tanto no forma parte de la apuesta mínima.

<u>Nota</u>: a) 0000000, 1111111 $\in$ Código seguro.

b) 0001100 está a distancia 2 de una de las palabras código, no pertenece al código dado que $d_{min} = 3$.

c) Observe que hay simetría con la asignación 1, 0.

3. Un decodificador que trabaja con bloques de 28 octetos es capaz de corregir hasta 5 octetos erróneos cualesquiera. Si se tiene una probabilidad de error de bit de 0.0003 y los errores son *independientes*, ¿cuál es la tasa de error de bloque a la salida del decodificador?

(a) 0.1 $10^{-15} \leq p_{error}(bloque) \leq 0.3 \quad 10^{-15}$

(b) 0.3 $10^{-12} \leq p_{error}(bloque) \leq 0.5 \quad 10^{-12}$

(c) 0.6 $10^{-10} \leq p_{error}(bloque) \leq 0.8 \quad 10^{-10}$

(d) Ninguna de los anteriores.

$p = 0'0003$

Probabilidad de octeto erróneo a la entrada del decodificador:

$$P_E = 1 - \underbrace{(1-p)^8}_{\text{prob. no hay ningún bit erróneo en el octeto}} = 0'0023974$$

Probabilidad de Bloque Erróneo:

$$\simeq \binom{28}{6} \cdot P_E^{6} \cdot (1-P_E)^{22} =$$

n → 28; $e+1$ → 6; $n-e-1$ → 22

$$= \frac{28 \cdot 27 \cdot 26 \cdot 25 \cdot \cancel{24} \cdot 23}{\cancel{6} \cdot 5 \cdot \cancel{4} \cdot 3 \cdot 2} \cdot 0'0023974^6 \cdot (0'9976025)^{22} =$$

$$= 376740 \cdot 1'800979 \cdot 10^{-16} = 6'785 \cdot 10^{-11}$$

$$= 0'6785 \cdot 10^{-10}$$

4. Un banco firma mensajes mediante RSA con parámetros e=67, N=2021027. El procedimiento para firmar un mensaje m es: $firma(m) = m^d mod N$. Una banda de falsificadores quiere poder falsificar la firma de cualquier mensaje menor o igual que 40. ¿Cuál es el número mínimo de parejas escogidas *mensaje-firma* que necesita?

(a) 6

(b) 12

(c) 38

(d) Ninguno de los anteriores

Por construcción (débil) de la firma:

FIRMA DEL PRODUCTO = PRODUCTO DE FIRMAS

Para factorizar un número cualquiera menor o igual que 40 => primos menores que él:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37

Hay 12 en total.

5. En el criterio de decisión MLSE si aplicamos el algoritmo de Viterbi bajo un modelo de ruido de media cero, pero no necesariamente gaussisano, es FALSO que:

(a) El valor final mínimo de F es negativo si la potencia de ruido es menor que la de señal

(b) El valor final óptimo de F coincide con su valor mínimo

(c) La diferencia de entre dos valores finales de F coincide con la diferencia entre las energías de ruido asociadas

(d) Alguna de las anteriores es falsa.

Por ser el ruido de media ϕ

$\Rightarrow$ F = energía de ruido − energía de señal

a) CIERTO, pues $\frac{F}{n\ muestras} = \frac{Energ.(R)}{n\ muestras} - \frac{Energ.(S)}{n\ muestras} =$

$= pot.(R) - pot.(S) < \phi$

b) FALSO, el valor óptimo MLSE depende de la estadística del ruido.

Coincide con su valor mínimo para ruido gaussiano.

c) $F_a - F_b = energ.(R_a) - energ.(S) - \left(energ.(R_b) - energ.(S)\right)$

CIERTO

$= energ.(R_a) - energ.(R_b)$

6. Un sistema de transmisión de datos 2-PAM {-1,1} cuya respuesta impulsional del canal es:

$$x[0] = 0.9, x[1] = 1, x[2] = 0.8$$

con ruido ~~gasiano~~ gaussiano blanco recibe seis muestras de valores:

$$y[0] = 1, y[1] = 0, y[2] = 1, y[3] = 1, y[4] = 2, y[5] = 1$$

Se aplica el algoritmo de Viterbi para la estimación de la secuencia enviada y se decide la secuencia:

$$a[0] = 1, a[1] = -1, a[2] = 1, a[3] = 1$$

Indique cuál de las siguientes afirmaciones es cierta:

(a) La energía del ruido asociada a la estimación más verosímil es 0.033

(b) El valor medio del ruido asociado a la estimación más verosímil es 0

(c) El valor máximo del ruido asociado a la estimación más verosímil es 0.2

(d) Ninguna de las anteriores

Convolucionamos: $x(n) * a(n) = \underbrace{(0'9, 0'1, 0'7, 1'1, 1'8, 0'8)}_{= y_K(n)}$

$$\eta(n) = y(n) - y_K(n) =$$

$$= (0'1, -0'1, 0'3, -0'1, 0'2, 0'2)$$

a) Energía de ruido $= \sum_{i=0}^{5} \eta^2[i] = 0'2 \neq 0'033$

b) $\bar{\eta} = \dfrac{\sum_{i=0}^{5} \eta[i]}{6} = 0'1 \neq \emptyset$

c) $\max_i \eta[i] = \eta[2] = 0'3 \neq 0'2$

0'9	1	0'8				
	-0'9	-1	-0'8			
*		0'9	1	0'8		
			0'9	1	0'8	
0'9	0'1	0'7	1'1	1'8	0'8	$= y_K(n)$

7. Indique cuál de las siguientes afirmaciones es cierta para un código de repetición binario Cod(5,1)

(a) El número de síndromes distintos no nulos es menor o igual que 15

(b) Es un código 3-perfecto

(c) La capacidad de detección de errores es 2

(d) Ninguna de las anteriores

Cód. (5,1) repetición binario:

$$0 \longrightarrow 00000$$

$$1 \longrightarrow 11111$$

$k=1 \qquad n=5 \qquad r=n-k=4$

$d_{min} = r+1 = 5$

a) El nº de síndromes distintos es $2^r = 2^4 = 16$.

" no nulos es $2^r - 1 = 15$. $\Rightarrow$ OK.

b) $2^r = 1 + \binom{n}{1} + \dots + \binom{n}{e}$

$$e = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 2$$

$$2^4 = 1 + \binom{5}{1} + \binom{5}{2} = 1 + 5 + 10 = 16$$

No puede ser 3-perfecto porque como máximo corrige $\frac{r}{2}$ errores, o sea $\frac{4}{2} = 2$.

c) $d_{min} = 5 \Longrightarrow \delta = d_{min} - 1 = 4 \neq 2$

d) La a) es cierta.

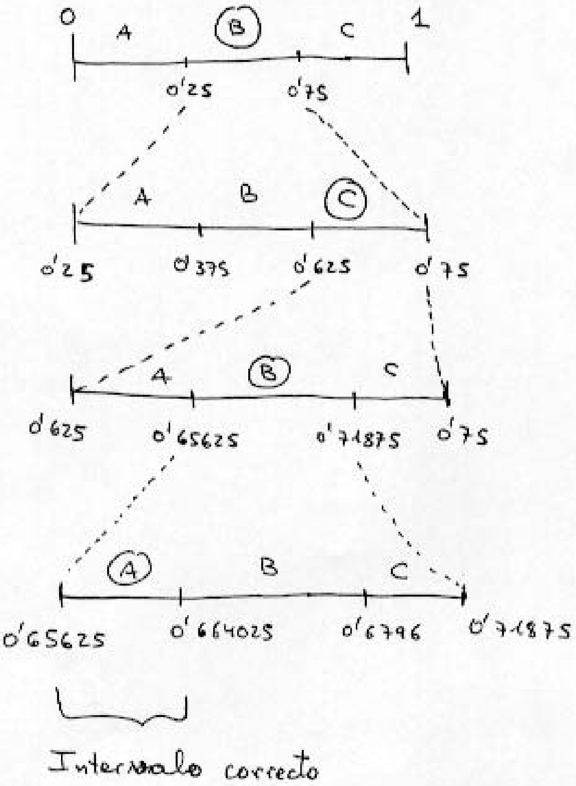
8. Se emplea un código aritmético para enviar el mensaje BCBA generado por una fuente que emite símbolos de un alfabeto {A,B,C} con probabilidades 0.25, 0.5 y 0.25 respectivamente. El valor x codificado cumple:

(a) $0 < x < 0.5$

(b) $0.5 \leq x \leq 0.65$

(c) $0.65 < x < 0.72$

(d) $0.72 \leq x$



c) $0'65 \leq x < 0'75$ cubre el conjunto de valores que puede tomar x.

9. Para el algoritmo RSA con p=7, q=17 y n= p·q =119, indique cuál de las siguientes afirmaciones es FALSA

(a) La clave pública puede ser (e,n)=(49,119)

(b) La clave privada puede ser (d,n)=(17,119)

(c) Si la clave pública es (e,n)=(11,119) el mensaje m=35 tiene por criptograma c=35

(d) Alguna de las anteriores es falsa

$$\Phi(n) = (p-1)\cdot(q-1) = 6\cdot 16 = 96$$

a) cierta, pues mcd (49, 96) = 1

b) Cierta, pues RSA es simétrico y, por tanto, lo que aplica a la clave pública también es válido para la privada :

$$\text{mcd}\,(17, 96) = 1$$

c) $C = M^e \bmod N$

$C = 35^{11} \bmod 119 = 35$, cierto.

d) las 3 anteriores son ciertas.

10. Sea M=1011011011 un mensaje que produce un resumen H(M)=0011. Sea un sistema RSA con p=7, q=13 y la clave privada d=11. Para ofrecer autenticidad de origen y contenido debemos transmitir (considérese que la firma de un mensaje ocupa un byte):

(a) 1011011011|00000011
(b) 1011011011|00111101
(c) 1011011011|00011011
(d) Ninguna de las anteriores

Se transmite $\Rightarrow$ M | Firma

$$\downarrow$$

$$[H(M)]^d \mod N$$

$N = p \cdot q = 7 \cdot 13 = 91$

$H(M) = 3 \equiv 0011$

$\text{Firma} = 3^{11} \mod 91 = 61$

$$\downarrow$$

$$\underset{32\ 16\ 8\ 4\ 2\ 1}{00\ 111101} \Longrightarrow b)$$

Se transmite $\Rightarrow$ M | 00111101

11. Para una función de hash se cumple:

   (a) Un mismo mensaje puede generar distintos resúmenes
   (b) No existen dos mensajes diferentes que generen el mismo resumen
   (c) Dado el resumen H(M), sólo puede encontrarse un mensaje que lo genera si se conoce una clave privada
   (d) Ninguna de las anteriores

12. Para un mismo nivel de seguridad puede afirmarse que:

   (a) Los algoritmos de clave pública utilizan claves más largas que los simétricos y requieren mayor coste computacional
   (b) Los algoritmos simétricos utilizan claves más largas que los de clave pública y requieren mayor coste computacional
   (c) Los algoritmos simétricos utilizan claves más cortas que los de clave pública y requieren mayor coste computacional
   (d) Ninguna de las anteriores

13. Respecto a la modulación codificada (TCM) ¿cual de las siguientes afirmaciones es FALSA?

   (a) Secuencias código próximas se asignan a puntos distantes en la constelación
   (b) La codificación no varía la velocidad de modulación del canal
   (c) La codificación no varía la velocidad de transmisión efectiva de usuario
   (d) Alguna de las anteriores es falsa

14. Sea una fuente que emite dos símbolos A y B, con

$$P(A|A) = 0.4, P(B|B) = 0.8$$

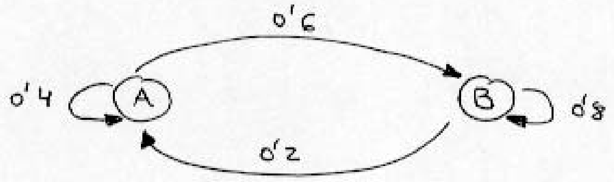
La entropía de la fuente vale

(a) $H \leq 0.6$

(b) $0.6 < H \leq 0.7$

(c) $0.7 < H \leq 0.8$

(d) Ninguna de las anteriores



$$\left.\begin{array}{r} 0'6 \cdot P(A) = 0'2 \cdot P(B) \\ P(A) + P(B) = 1 \end{array}\right\} \qquad \begin{array}{l} P(A) = 0'25 \\ P(B) = 0'75 \end{array}$$

$$H(F \backslash A) = 0'97 = 0'4 \cdot \log_2 \frac{1}{0'4} + 0'6 \cdot \log_2 \frac{1}{0'6}$$

$$H(F \backslash B) = 0'72 = 0'8 \cdot \log_2 \frac{1}{0'8} + 0'2 \cdot \log_2 \frac{1}{0'2}$$

$$H(F) = P(A) \cdot H(F \backslash A) + P(B) \cdot H(F \backslash B) =$$

$$= 0'25 \cdot 0'97 + 0'75 \cdot 0'72 =$$

$$= 0'78$$

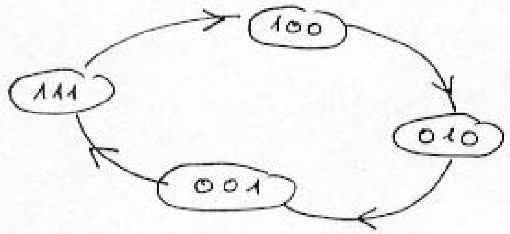
15. Sea un LFSR caracterizado por el polinomio de conexiones $C(D) = D^3 + D^2 + D + 1$ y el estado inicial $S^0(D) = 1$. El estado al cabo de 75 iteraciones vale:

(a) D

(b) 1

(c) $D^2 + D + 1$

(d) Ninguna de las anteriores



- Periodo = 4
- $C(D)$ es completo, $L = L_{max} = m + 1 = 3 + 1 = 4$
- 100 ∈ al subconjunto de periodo máximo.

75 mod 4 = 3

$$S^{75}(D) = S^{(3)}(D) \equiv 111 = D^2 + D + 1$$

16. En un sistema de criptografía de clave simétrica, la distribución de claves más apropiada de las que se enumeran a continuación, para un grupo de trabajo con sus terminales distribuidos en una red de área extendida, sería (para cada par de comunicantes A y B del grupo y suponiendo que previamente no comparten ningún secreto):

(a) Un comunicante A selecciona la clave y físicamente la entrega al comunicanse B

(b) Una tercera entidad C selecciona la clave y físicamente la entrega a los comunicante A y B

(c) A y B se transmiten la clave en claro por la red

(d) Si A y B tienen una conexión segura con la entidad C, C puede enviar la clave a A y B

a, b → Sería lo más seguro, pero no es escalable para una red grande y un equipo de trabajo en que todos los terminales deben estar conectados dos a dos.

c → No es seguro!

d → Sí, es adecuado.

17. La respuesta impulsional global de un módem es:

$$x(-2) = x(2) = 0.1, x(-1) = x(1) = 0.2, x(0) = 0.9$$

El módem receptor obtiene la secuencia

$$y[n] = (0.2, -1.2, 0.4, 0.8, -0.6, 0.6, 1.2, 0.1, 0.2, 0.2, 0.2, -0.4, 0.12, -0.3)$$

Se transmite una señal PAM-2 y el ruido es gaussiano de media nula. Se desea determinar la secuencia enviada más verosímil. ¿Qué afirmación es cierta?

(a) F_0 puede tomar 32 valores distintos

(b) Una vez obtenido F_4, el cálculo de F_5 depende de los valores de los símbolos emitidos a(0), a(1), a(2), a(3) y a(4)

(c) Será necesario aplicar la fórmula iterativa de Viterbi para el cómputo del parámetro F, hasta la iteración F_9

(d) Ninguna de las anteriores

a) $\#F_0 = A^M = 2^4 = 16$

$M_1 = 2,\ M_2 = 2 \rightarrow M = M_1 + M_2 = 4$

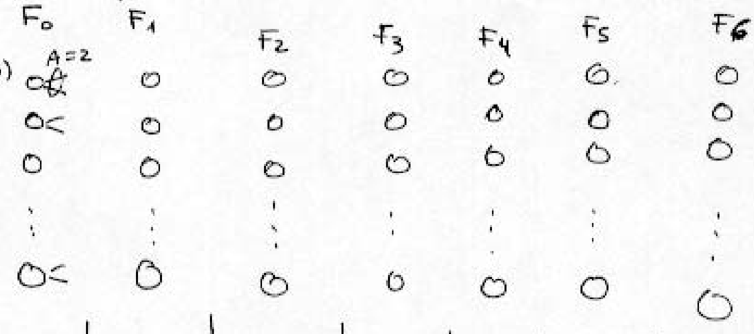
b) $F_5 = F_4 + \sigma_4$

$\sigma_4(a(4), a(5), a(6), a(7), a(8))$

$i=4$ $\quad i \quad\quad i+M = 4+4 = 8$

$\left.\begin{array}{l} L+M = 14 \\ M = 4 \end{array}\right\} L = 10 \rightarrow a(0), a(1), \ldots\ a(9)$ Secuencia de símbolos enviados

c) $F_0 \xrightarrow{\sigma_0(a(0), a(1), a(2), a(3), a(4))} F_1$



a(0) a(1) a(2) a(3)

¡Hay 16 valores de F0!!

Se deciden aquí a(0), a(1), a(2), a(3)

Se decide a(4)

a(5) a(6) a(7) a(8) a(9)

$\boxed{F = F_6}$

18. Sea un Sistema de Transmisión de Datos con velocidad de transmisión $v_t = 8400$ bps, una velocidad de modulación $v_m = 2800$ baudios y se utiliza una modulación PAM. ¿Qué afirmación es FALSA?

(a) El modulador realiza un mapeo con 3 bits/símbolo

(b) Si utilizamos un código de Hamming con redundancia 2 y queremos mantener v_u y la misma v_t efectiva al usuario, debemos doblar el número de puntos de la constelación, aunque disminuirá la SNR

(c) Si deseamos proteger al sistema frente a degradaciones del canal, sin disminuir la v_t efectiva al usuario ni deteriorar la tasa de error, podemos emplear modulación codificada de enrejado (TCM)

(d) Alguna de las anteriores es falsa

v_m

a) OK.

$$\left.\begin{array}{l} v_t = 8400 \ \frac{bits}{seg} \\ v_m = 2800 \ \frac{simb}{seg} \end{array}\right\} \quad v_t \left[\frac{bits}{seg}\right] = q\left[\frac{bits}{simb}\right] \cdot v_m \left[\frac{simb.}{seg}\right]$$

$$8400 = q \cdot 2800$$

$$q = 3 \ \text{bits}/\text{simb}$$

b) Falso.

$$2^r = 1 + \binom{n}{1} = 1 + n \quad \rightarrow \text{Hamming, 1-perfecto, } e = 1.$$

$$r = 2 \Rightarrow n = 3 \Rightarrow k = 1 \Rightarrow \text{Código}(3,1)$$

$$v_t' = v_t \cdot \frac{n}{k} = 8400 \cdot \frac{3}{1} = 25200 \text{ bps}$$

$v_t' = q' \cdot v_m$ ya se se mantiene la v_m.

$$25200 = q' \cdot 2800$$

$q' = 9 \ \frac{bits}{símbolo}$, se triplica.

c) cierto.

d) sentencia cierta.

19. Sea $C(D) = 1 + D^2 + D^5$ un polinomio primitivo, que sirve como polinomio de conexiones a un LFSR que se inicia al estado D ¿Qué afirmación es FALSA?

(a) El polinomio $C(D) = 1 + D^3 + D^5$ es irreducible

(b) $C(D)$ es divisor de $1 + D^{124}$

(c) El estado al cabo de 122 iteraciones es $D + D^4$

(d) Alguna de las anteriores es falsa → Todas son ciertas! Esta frase es falsa.

a) ok

Recíproco de $C(D) = C^*(D) = D^5 \cdot (1 + D^{-2} + D^{-5}) = D^5 + D^3 + 1$

También es primitivo → Por lo que es irreducible.

b) ok

Al ser primitivo, $L = 2^m - 1 = 31$

$$P^{(0)}(D) = D = P^{(31)}(D) = P^{(93)}(D)$$

$$\boxed{P^{(n)}(D) = D^n \cdot P^{(0)}(D) \mod C(D)} \rightarrow P^{(31)}(D) = D^{31} \cdot D \mod C(D)$$

$$D = D^{32} \mod C(D) \Rightarrow \begin{array}{l|l} D^{32} & C(D) \\ \hline D & Q(D) \end{array} \Rightarrow D^{32} = C(D) \cdot Q(D) + D$$

$$\Rightarrow D^{32} + D = C(D) \cdot Q(D)$$

$$D \cdot (D^{31} + 1) = C(D) \cdot Q(D)$$

$$D^4 \cdot (D^{31} + 1)^4 = C^4(D) \cdot Q^4(D)$$

$$D^4 \cdot (D^{124} + 1) = C^4(D) \cdot Q^4(D)$$

$C(D)$ es divisor de $D^{124} + 1$.

c) ok

$$\boxed{D \cdot P^{(n)}(D) = P^{(n+1)}(D) + \underbrace{\begin{Bmatrix} 1 \\ 0 \end{Bmatrix}}_{b_{m-1}} \cdot C(D)} \begin{cases} \xrightarrow{1} P^{(n+1)}(D) + C(D) \\ \xrightarrow{0} P^{(n+1)}(D) \end{cases}$$

$$D \cdot P^{(123)}(D) = C(D) \cdot \phi + P^{(124)}(D) = D \Rightarrow P^{(123)}(D) = 1$$

$$D \cdot P^{(122)}(D) = C(D) \cdot 1 + P^{(123)}(D) = 1 + D^2 + D^5 + 1 = D^2 + D^5$$

$$P^{(122)}(D) = D + D^4$$

20. Sea una fuente F con memoria en la que la probabilidad de emisión de cada símbolo depende del anterior símbolo enviado (es decir, caracterizable por una cadena de Markov) que emite 4 símbolos A, B, C y D. ¿Qué afirmación es cierta?

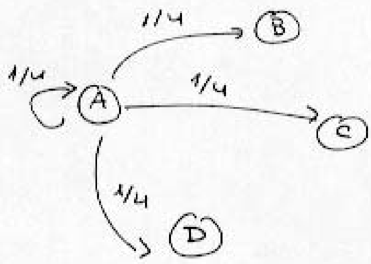
(a) Si $p(x_i|y_j) = 0.25, \forall x_i, y_j \in \{A, B, C, D\}$, entonces la entropía de la fuente es $H = 2$

(b) La codificación Huffman tiene en cuenta la memoria de la fuente

(c) Puede ocurrir que $H/L > 1$, siendo L la longitud media del código utilizado y H la entropía de la fuente

(d) Ninguna de las anteriores

a)



Es una fuente con memoria, que equiprobablemente va a cualquiera de los 4 estados!!

$\Rightarrow$ Es un fuente SIN memoria!

$\Rightarrow$ Los 4 estados son equiprobables, como se aprecia en la simetría que hay.

$0 \leq H(F) \leq \log_2 F$

En este caso, $H(F) = \log_2 F = 2$

b) No, Huffman no contempla la memoria de la fuente.

c) $\text{Eficiencia} = \frac{H}{\bar{L}} < 1$ siempre, tenga o no memoria la fuente.