ETSETB
Curso 2003-04 Otoño
EXAMEN DE TRANSMISIÓN DE DATOS
13 de enero de 2004

PUBLICACIÓN DE NOTAS PROVISIONALES: 20/01/04
FECHA LÍMITE PARA LAS ALEGACIONES: ~~23/01/04~~ 22/01/04
PUBLICACIÓN DE NOTAS DEFINITIVAS: ~~04/02/04~~ 29/01/04

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 por escrito en la secretaría de la ETSETB a partir de la publicación de las calificaciones provisionales y hasta el plazo arriba indicado. En ellas debe consignarse OBLIGATORIAMENTE el DNI y el código de la prueba.

Queda expresamente prohibido el uso de cualquier dispositivo de comunicación. El incumplimiento de esta norma supondrá la expulsión del examen.

CÓDIGO DE LA PRUEBA: 230 11510 00 0

F 1. Sea un LFSR caracterizado por $c(D) = D^4+D^3+D^2+D+1$ y estado inicial $S(D) = D^2+D$. El estado al cabo de 17 iteraciones vale:

(a) D^2+D+1
(b) D^3+D^2
(c) $D+1$
(d) Niguna de las anteriores

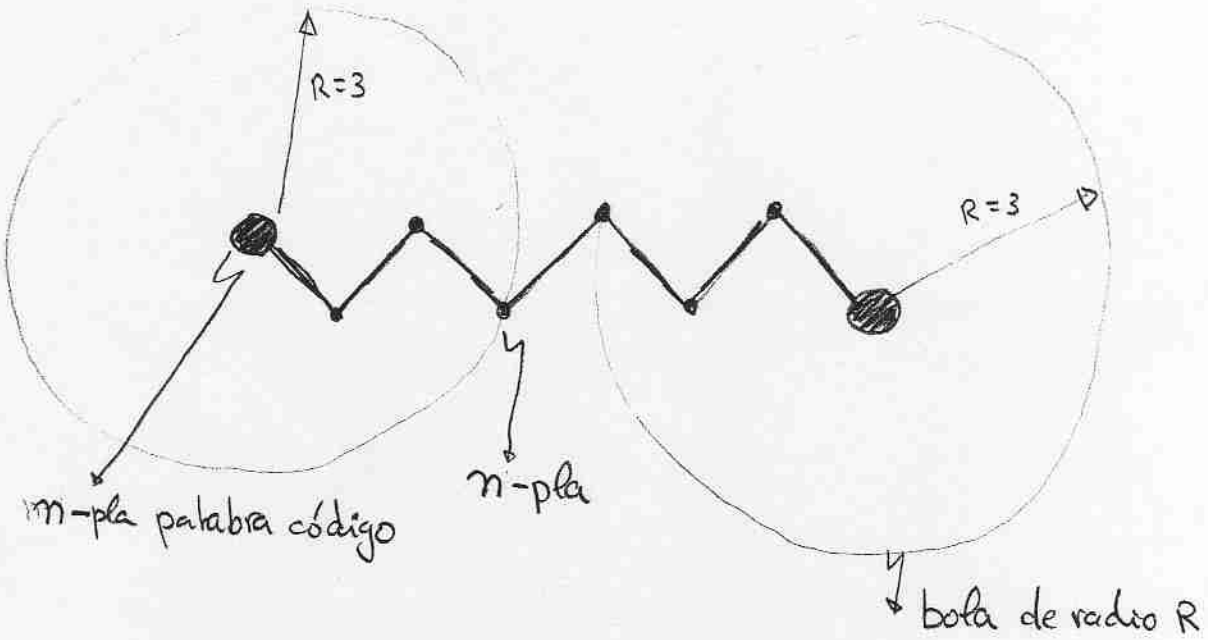
- $c(D)$ es completo de grado $m \rightarrow$ período máximo $= m+1 = 5$
- El período depende del estado inicial, ¡podría ser menor!

$p^{(0)}(D) = D^2+D$
$p^{(1)}(D) = D^3+D^2$
$p^{(2)}(D) = D^4+D^3 \mod D^4+D^3+D^2+D+1 = D^2+D+1$
$p^{(3)}(D) = D^3+D^2+D$
$p^{(4)}(D) = D^4+D^3+D^2 \mod D^4+D^3+D^2+D+1 = D+1$
$p^{(5)}(D) = D^2+D = p^{(0)}(D) \Rightarrow \boxed{L=5}$

$p^{(17)}(D) = p^{(15+2)}(D) = p^{(5\cdot 3+2)}(D) = p^{(2)}(D) = D^2+D+1$

2. Se define el radio de recubrimiento de un código como el mínimo radio que han de tener las bolas centradas en palabras código para que se recubra todo el espacio de las n-plas. ¿Cuál es el radio de recubrimiento para un código binario perfecto con distancia 7?

(a) 7
(b) 5
(c) 3
(d) Ninguna de las anteriores



Así quedan todas las n-plas cubiertas.
Si el código no fuera perfecto, las bolas no serían disjuntas, tendrían intersecciones.

3. El número medio de mensajes aleatorios que son necesarios para que, con una probabilidad de 0.5, al menos dos de ellos generen el mismo hash de 160 bits es, aproximadamente:

D

(a) 2^{160}

(b) 2^{159}

(c) 2^{80}

(d) Ninguno de los anteriores

Nº de mensajes	Prob. de coincidir el hash de 2 mensajes
1	$\emptyset / 2^{160}$ → nº de hashes totales
2	$1/2^{160}$
3	$2/2^{160}$ → casos favorables: que para el 3er mensaje su hash coincida con algún otro hash de los dos mensajes primeros.
⋮	
i	$\frac{i-1}{2^{160}}$ → prob. de que haya 1 sola coincidencia, al generar 3 hash (es decir, que 2 mensajes generen el mismo hash).

Hay que sumar todos los casos:

$$\text{Prob.} = \sum_{i=1}^{N} \frac{i-1}{2^{160}} = \frac{1}{2^{160}} \cdot \sum_{i=1}^{N} (i-1)$$

$$0+1+2+3+\dots+N = \text{Suma de los } N \text{ 1ºs términos de una progr. aritmética de razón 1.}$$

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

$$0\text{'s} = \frac{N(N+1)}{2} \cdot \frac{1}{2^{160}}$$

$$2^{160} = N^2 + N$$

$$N \simeq \sqrt{2^{160}} = 2^{80}$$

N

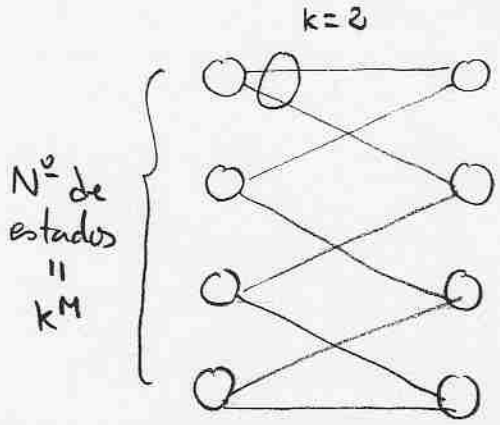
5. Indique la respuesta FALSA:

(a) Si la memoria de un codificador convolucional se dobla, la complejidad computacional de la decodificación se eleva al cuadrado.

(b) Si la longitud de la secuencia codificada mediante un código convolucional se dobla, la complejidad computacional de la decodificación también se dobla.

(c) El número de estados de un codificador convolucional crece exponencialmente con la tasa de codificación.

(d) Alguna de las anteriores es falsa.



M=2

Nº de estados = $k^M = 4$

El nº de operaciones a hacer (sumar, comparar) es lineal con el número de estados.

a) Si $M' = 2M$, nº de estados = $k^{2M} = (k^M)^2 = 4^2 = 16$

cierta

El nº de estados se eleva al cuadrado

⇩

El nº de operaciones se eleva al cuadrado

b) cierta. Para una secuencia dada hago x operaciones. Para una secuencia el doble de larga, pues el doble de operaciones se harán.

c) Nº de estados = k^M

tasa codif. = $\frac{k}{n}$

} no se observa tal relación!

N

6. Dado un código convolucional de tasa 1/3, memoria L=2 y conexiones según la Figura A, indicar cuál es la respuesta correcta:

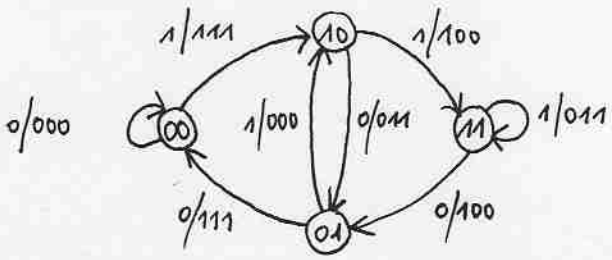
(a) La distancia libre del código es 6

(b) Es una codificación sistemática

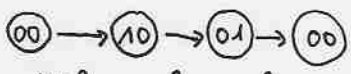
(c) La secuencia de salida del codificador para la entrada (1101) es 111100100000

(d) Ninguna de las anteriores

DIAGRAMA DE ESTADOS :

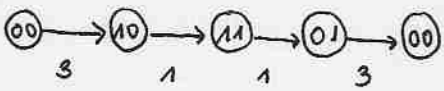


a) DISTANCIA LIBRE (df):



$d = 3+2+3 = 8$

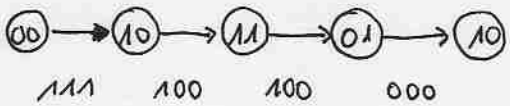
$\Rightarrow df = 8$



$d = 3+1+1+3 = 8$

b) POR INSPECCIÓN DE LAS TRANSICIONES DE LOS ESTADOS (11) y (01) SE TIENE UNA CODIFICACIÓN NO-SISTEMÁTICA. (*)

c) $x = (1101)$



CORRECTA

(*) Sería $v_1 = u_1$ en caso de ser sistemático.

Y es $v_1 = u_1 + m_2$.

D

7. Sea el polinomio $D^5 + D^4 + D^2 + 1$, ¿qué afirmación es correcta?

(a) Genera un código polinómico (15,10)
(b) Es apropiado para un LFSR de máximo período (MLSR)
(c) El código polinómico que genera es capaz de corregir 2 errores
(d) Ninguna de las anteriores

$g(D) = D^5 + D^4 + D^2 + 1$ tiene un número par de términos → $(D+1)$ es un factor

$D^5 + D^4 + D^2 + 1 \;\big|\; D+1$ ⋱ ☺ $\quad D^4 + D + 1$ → $g(D) = (D+1)(D^4 + D + 1)$

$(D^4 + D + 1)$ p. primitivo ya conocido

a) $(D+1)$ divide a $D^{15}+1$

(D^4+D+1) divide a $D^{15}+1$ con 15 el más pequeño } → $g(D)$ divide a $D^{15}+1$ y por tanto genera un código polinómico cíclico. (*)

CORRECTA

b) No es apropiado puesto que $g(D)$ no es primitivo

c) Como $g(D)$ tiene peso 4 la $d_{min} \leq 4$ → no puede corregir 2 errores (Se necesitaría una $d_{min} \geq 5$).

(*) Condición para que $g(D)$ genere código polinómico (Código(n,k)) CÍCLICO

$g(D)$ divida a $D^n + 1$.

F

4. Para un código binario lineal NO se puede afirmar que:

(a) Si el producto escalar de dos palabras código es cero, entonces son ortogonales → Cierta
(b) Si el producto escalar de dos palabras código es cero, entonces son linealmente independientes
(c) Una palabra código NO NULA puede ser ortogonal a ella misma. → Cierta
(d) Alguna de las anteriores es falsa

b) No se puede afirmar.

Ej $\quad z_2 : (0101) \cdot (0101) = \emptyset$

D

8. Lamentablemente en un sistema RSA se ha filtrado cierta información, los números $x1 = 11710301 = pq$ y $x2 = 11700000$ primos entre sí. Con respecto estos números:

(a) Si el módulo es $x1$ entonces $\phi(x1) = x2$

(b) $x2$ podría utilizarse como el módulo del RSA

(c) Se puede comprobar que la inversa de $x2$ mod $x1$ es -320299

(d) Ninguna de las anteriores

a) $n = 11710301$

$\varphi(n) = 11700000$?

- Sabemos que $\varphi(n) = (p-1)(q-1) = n - (p+q) + 1 \rightarrow (p+q) = n - \varphi(n) + 1$.
- Como $(p+q)^2 = p^2 + 2pq + q^2 = p^2 - 2pq + q^2 + 4pq = (p-q)^2 + 4n$, se tiene $(p-q)^2 = (p+q)^2 - 4n$
- Sustituyendo en las 2 ecuaciones: $(p+q) = 10302$

$(p-q)^2 = 59290000 \rightarrow (p-q) = 7700$

CORRECTA

$\rightarrow p = 9001$

$q = 1301$. 2 valores enteros que satisfacen las ecuaciones $n = pq = 11710301$

$\varphi(n) = 11700000$

b) x2 es divisible por números no primos

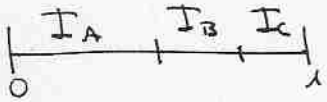
c) $(-320299) \cdot x_2 \bmod x_1 = (-320299)(-10301) \bmod 11710301 = 8805418 \neq 1$

↓ congruente con $11700000 \bmod x_1$.

10. Un codificador aritmético de una fuente cuyo alfabeto es $\{A, B, C\}$ envía el valor 0.34 correspondiente a la codificación de un mensaje de 4 caracteres. Sabiendo que la codificación aritmética emplea valores crecientes según el orden $\{A, B, C\}$ y que las probabilidades de estos símbolos son respectivamente 0.5, 0.3 y 0.2, indique el valor del mensaje descodificado:

(a) ABBB
(b) ACBA
(c) CBBA
(d) Ninguno de los anteriores

Definimos los intervalos



$I_A = [0, 0'5)$; $I_B = [0'5; 0'8)$; $I_C = [0'8, 1)$

Los puntos de inicio de cada intervalo son: $i_A = 0$, $i_B = 0'5$, $i_C = 0'8$

y la longitud de los segmentos es: $\Delta_A = 0'5$, $\Delta_B = 0'3$, $\Delta_C = 0'2$.

Aplicando recursivamente:

$$x_0 = 0'34$$

$$x_{n+1} = \frac{x_n - i_j}{\Delta_j} \quad \text{donde } x_n \in I_j$$

$x_0 = 0'34 \in I_A \Rightarrow A$

$$x_1 = \frac{x_0 - i_A}{\Delta_A} = \frac{0'34 - 0}{0'5} = 0'68 \in I_B \Rightarrow B$$

$$x_2 = \frac{x_1 - i_B}{\Delta_B} = \frac{0'68 - 0'5}{0'3} = 0'6 \in I_B \Rightarrow B$$

$$x_3 = \frac{x_2 - i_B}{\Delta_B} = \frac{0'6 - 0'5}{0'3} = 0'\widehat{3} \in I_A \Rightarrow A$$

Descodificación ABBA $\Rightarrow$ d)

F

12. Un código polinómico emplea el polinomio generador $g(D) = D^2 + D + 1$. Es FALSO que:

(a) La palabra $D^3 + D^2 + D$ es palabra código

(b) Si los mensajes de usuario son de 1 bit, la capacidad correctora del código es 1

(c) Si los mensajes de usuario son de 2 bits, se detectan todos los errores dobles

(d) Alguna de las anteriores es falsa

$r = 2$

a) $D^3 + D^2 + D \mod g(D) = \phi \rightarrow$ Es palabra código

b) $\left.\begin{matrix} k=1 \\ r=2 \end{matrix}\right\} n=3 \rightarrow cod(3,1)$

Palabras código $\begin{cases} 000 \\ 111 \end{cases} \Rightarrow d_{min}=3 \Rightarrow e=1$, cierto.

c) Caso $k=2 \rightarrow$ Palabras código $\begin{cases} 00\,00 \\ 01\,11 \\ 10\,01 \\ 11\,10 \end{cases} \rightarrow d_{min}=2$

No se detectan todos los errores dobles.

$Y(D) = D^r \cdot X(D) + D^r \cdot X(D) \mod g(D)$

$X(D)=1 \Rightarrow Y(D) = D^2 + D + 1 \equiv 0111$

$X(D)=D \Rightarrow Y(D) = D^3 + 1 \equiv 1001$

11. Se codifica el mensaje AABBABBCBBCDA generado por una fuente cuyo alfabeto es $\{A, B, C, D\}$ utilizando la técnica LZ-77. La codificación aplicada es binaria con una capacidad en el búfer de almacenamiento de 3 posiciones. Para referenciar cadenas de símbolos se emplean 2 bits para la longitud y 2 bits para la posición relativa. Teniendo en cuenta que los símbolos de la fuente se codifican con dos bits según la asignación: A=00, B=01, C=10, D=11, indique cuál es el valor hexadecimal de la secuencia binaria enviada (mayor peso a la izquierda):

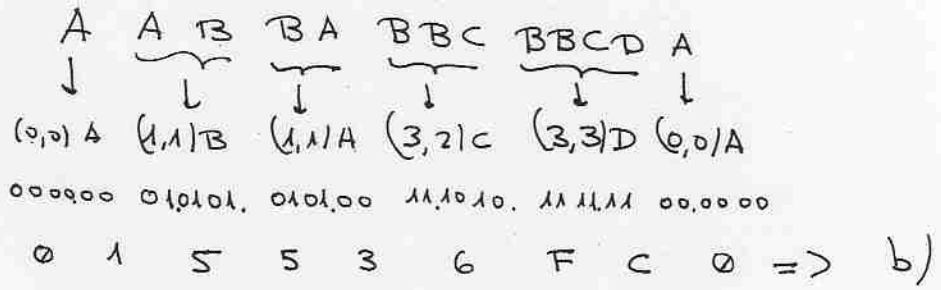
F

(a) 0025246AC6F0

(b) 015536FC0

(c) 515D5697B

(d) Ninguno de los anteriores



⇒ Substituido por pregunta 9 del test 7-enero-2003

F

14. Sea un código codificador de canal de *Hamming* sistemático caracterizado por la matriz generadora G. Si se recibe la palabra 1011101, ¿qué afirmación es correcta?. Nota: Las posiciones de la palabra recibida se empiezan a numerar desde la izquierda, empezando por la posición 1.

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

a) Si el código se usa como corrector, se estima el mensaje de usuario 1001.
b) Si el código se usa como detector, no se detecta error en la palabra recibida.
c) Si el código se usa como corrector, suponiendo que hubo error en las posiciones 1 y 4 se confunde con un error simple en la posición 5.
d) Ninguna de las anteriores frases es correcta.

Solución:

$$G_{kxn} = \begin{pmatrix} * & * & * & * & 0 & 1 & 1 \\ * & * & * & * & 1 & 1 & 0 \\ * & * & * & * & * & * & * \\ * & * & * & * & 1 & 1 & 1 \end{pmatrix} = G_{4x7} = \left(I_k \middle| P\right) \qquad \text{k} = 4, \text{n} = 7, \text{r} = \text{n} - \text{k} = 3$$

$$\text{H}_{\text{rxn}} = \text{H}_{3x7} = \left(-P^T \middle| I_r\right) = \begin{pmatrix} 0 & 1 & * & 1 & 1 & 0 & 0 \\ 1 & 1 & * & 1 & 0 & 1 & 0 \\ 1 & 0 & * & 1 & 0 & 0 & 1 \end{pmatrix} \rightarrow \text{H}_{3x7} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

a) $$s = Z \cdot H^T = (1011101) \cdot \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (100) \rightarrow \vec{e} = (0000100) \rightarrow \hat{Y} = Z + \vec{e} = \underbrace{1011}_{\hat{x}}001$$

b) Si sólo detecta errores, como $s=Z\cdot H^T \neq 0$ sí que se detecta que ha habido error.

c) Es cierto, Z=**1**011**1**101, Y=0010101, $s=Z\cdot H^T=100=5^a$ fila de H^T, por lo que se confunde con un error simple en la 5^a posición.

F

13. Calcule la probabilidad de detección de error (p_d) para el código codificador de canal ternario 2-perfecto de menor redundancia posible cuando la probabilidad de error en el bit que introduce un canal binario simétrico es $p=10^{-4}$.
    a) $p_d \leq 10^{-5}$
    b) $10^{-5} < p_d \leq 10^{-2}$
    c) $10^{-2} < p_d \leq 10^{-1}$
    (d) $10^{-1} < p_d \leq 1$

Solución:

$$q^r = \binom{n}{0} + \binom{n}{1}\cdot(q-1) + \binom{n}{2}\cdot(q-1)^2 + \ldots + \binom{n}{e}\cdot(q-1)^e$$

ternario : q = 3; 2 - perfecto : e = 2

$$3^r = 1 + n\cdot 2 + n\cdot(n-1)\cdot\frac{4}{2} = 1 + 2n + 2(n^2 - n) = 2n^2 + 1$$

$r = 1 \rightarrow n = \sqrt{(3-1)/2} = 1 \rightarrow$ No tiene sentido pues k = n - r = 0

$r = 2 \rightarrow n = \sqrt{(9-1)/2} = 2 \rightarrow$ No tiene sentido pues k = n - r = 0

$r = 3 \rightarrow n = \sqrt{(27-1)/2} = \sqrt{13} \rightarrow$ No tiene sentido

$r = 4 \rightarrow n = \sqrt{(81-1)/2} = \sqrt{40} \rightarrow$ No tiene sentido

$r = 5 \rightarrow n = \sqrt{(243-1)/2} = 11 \rightarrow OK! \rightarrow k = n - r = 6$

Código (11, 6) ternario, 2-perfecto (además, es un código de Golay)

$$\Pr ob\_error\_bloque = \sum_{i=e+1}^{n} \binom{n}{i}\cdot p^i \cdot (1-p)^{n-i}$$

e=2 → Capacidad detectora de errores = d =2·e = 4 errores

Error:

Prob_detección_error=Prob(#errores≤4)= Prob(#errores=1) + Prob(#errores=2) + Prob(#errores=3) + Prob(#errores=4) ≈ Prob(#errores=1) ≈ n·p=11·10^{-4}=1'1·10^{-3}

Error: Decir que Prob_detección_error ≈ Prob(#errores=4) = $\binom{11}{4}\cdot p^4 \cdot (1-p)^7 \approx 330\cdot p^4 =$

= 330*(10^{-4})^4=3.3*10^{-14}

Bien: Prob_detección_error=Prob(#errores≤4)= Prob(#errores=0) + Prob(#errores=1) + Prob(#errores=2) + Prob(#errores=3) + Prob(#errores=4) ≈ Prob(#errores=0) + Prob(#errores=1) = $\binom{11}{0}\cdot p^0 \cdot (1-p)^{11}$ +1'1·10^{-3}= (1-10^{-4})^{11}+1'1·10^{-3}=0.9989+1'1·10^{-3}≈ 1

Bien: Prob_detección_error=1- Prob_no_detección_error ≈ 1-Prob(#errores=5)=1- $\binom{11}{5}\cdot p^5 \cdot (1-p)^6$ =1-462*10^{-20}=1-4.62*10^{-18} ≈ 1

15. Se dispone de dos fuentes A y B cada una con un alfabeto de 4 símbolos. ¿Qué afirmación es correcta?

a) Es imposible un valor de H(A, B) = 2,4 bits/símbolo
b) Si H(A\B) = 2 bits/símbolo, entonces H(B) ≤ H(A)
c) Se puede afirmar que H(A, B) = 4 bits/símbolo
d) Ninguna de las anteriores frases es correcta

Solución:

$H(A) = \sum_{i=1}^{F} p_i \cdot \log_q \frac{1}{p_i}$ unidades de información q - arias/símbolo

Alfabeto fuente de $F = 4$ símbolos, alfabeto del código de $q = 3$ símbolos.

$H(A) = \sum_{i=1}^{F} p_i \cdot \log_2 \frac{1}{p_i}$ bits/símbolo

$H(A) \leq \log_q F$, cota que se alcanza cuando los símbolos son equiprobables, $p_i = 1/F$.

$H(A) \leq \log_2 F = \log_2 4 = 2$ bits/símbolo

H(A, B) = H(B) + H(A\B)

H(A\B) ≤ H(A), pues disminuye la información media de la fuente A al conocer datos de la fuente B.

H(A, B) ≤ H(B) + H(A) = 2· H(A) = 2*$\log_2 F$ = 2*2= 4 bits/símbolo.

a) H(A, B) ≤ 4 bits/símbolo, por lo que ese valor sí que es posible. Es falso.

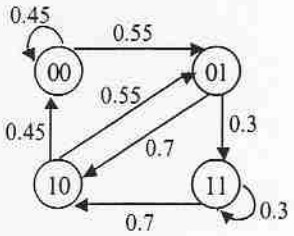
b) Como $H(A) \leq \log_a F$ bits/símbolo=$\log_2 4$=2 bits/símbolo. Entonces:

- Como H(A\B) ≤ H(A),
- Si H(A\B)=2=$\log_2 4$, como H(A\B)=2≤H(A) y H(A)≤2=$\log_2 4$ → H(A)=2 bits/símbolo
- Como H(B) ≤ $\log_2 4$=2 bits/símbolo → H(B) ≤ H(A)

c) No, lo que se puede afirmar es que H(A, B) ≤ 4 bits/símbolo. Se cumpliría la igualdad si ambas fuentes fueran independientes y emitieran símbolos equiprobables.

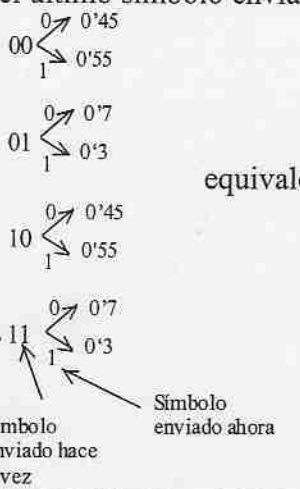
16. Una fuente F que emite dos símbolos según el diagrama de estados de la figura B (bit más antiguo a la izquierda) atraviesa un canal binario simétrico caracterizado por una probabilidad de error en el bit p=0.3. Sea F' la fuente resultante a la salida del canal. ¿Qué afirmación es FALSA?

a) La fuente F tiene memoria 1.
b) $0.93 \leq H(F) \leq 0.95$ bits/símbolo
c) $0.9906 \leq H(F') \leq 0.9918$ bits/símbolo
d) Alguna de las anteriores es falsa.

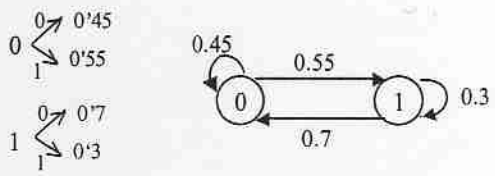


Solución:

a) Es cierta. Se observa que no hay dependencia con el símbolo emitido hace 2 veces, y sí que depende del último símbolo enviado. La memoria es 1:



equivale a:



b) Es cierta. $H(F)=H(F\backslash 0)*P(0)+H(F\backslash 1)*P(1)$

$P(0)=P(0\backslash 0)*P(0)+P(0\backslash 1)*P(1)=0'45*P(0)+0'7*P(1)$
$P(0)+P(1)=1 \rightarrow 0'55*P(0)=0'7*P(1)=0'7*(1-P(0))$
$1'25*P(0)=0'7 \rightarrow P(0)=0'56, P(1)=0'44$

$H(F\backslash 0) = P(0\backslash 0)*\log_2(1/P(0\backslash 0)) + P(1\backslash 0)*\log_2(1/P(1\backslash 0)) = 0.45*\log_2(1/0.45) + 0.55*\log_2(1/0.55) = 0.5184+0.4744 = 0.9928$ bits/símbolo
$H(F\backslash 1) = P(0\backslash 1)*\log_2(1/P(0\backslash 1)) + P(1\backslash 1)*\log_2(1/P(1\backslash 1)) = 0.7*\log_2(1/0.7) + 0.3*\log_2(1/0.3) = 0.3602+0.5211 = 0.8813$ bits/símbolo

$H(F)=H(F\backslash 0)*P(0)+H(F\backslash 1)*P(1)= 0.9928*0.56+0.8813*0'44=0.9437$ bits/símbolo

c) Es cierta. (F_0=0 indica que la fuente F parte del estado 0. F_1=1 indica que ahora F emite 1)
$H(F')= H(F'\backslash F_0=0)*P(F_0=0)+ H(F'\backslash F_0=1)*P(F_0=1)= H(F'\backslash F_0=0)*0'56+ H(F'\backslash F_0=1)*0'44$

$H(F'\backslash F_0=0) = P(F'=0\backslash F_0=0)*\log_2(1/P(F'=0\backslash F_0=0))+ P(F'=1\backslash F_0=0)*\log_2(1/P(F'=1\backslash F_0=0))=0'9989$
$H(F'\backslash F_0=1) = P(F'=0\backslash F_0=1)*\log_2(1/P(F'=0\backslash F_0=1))+ P(F'=1\backslash F_0=1)*\log_2(1/P(F'=1\backslash F_0=1))=0'9815$

$P(F'=0\backslash F_0=0) = P(F_1=0\backslash F_0=0)*(1-p) + P(F_1=1\backslash F_0=0)*p \quad = 0'45*0'7 + 0'55*0'3 = 0'48$
$P(F'=1\backslash F_0=0) = P(F_1=0\backslash F_0=0)*p \quad + P(F_1=1\backslash F_0=0)*(1-p) = 0'45*0'3 + 0'55*0'7 = 0'52$
$P(F'=0\backslash F_0=1) = P(F_1=0\backslash F_0=1)*(1-p) + P(F_1=1\backslash F_0=1)*p \quad = 0'7*0'7 + 0'3*0'3 = 0'58$
$P(F'=1\backslash F_0=1) = P(F_1=0\backslash F_0=1)*p \quad + P(F_1=1\backslash F_0=1)*(1-p) = 0'7*0'3 + 0'3*0'7 = 0'42$

Con ello, $H(F')= 0'9912$ bits/símbolo

F

9. Indique cuál de las siguientes afirmaciones es FALSA:

   (a) La entropía de una fuente sin memoria sólo depende de la estadística de sus símbolos

   (b) La entropía de una fuente es siempre menor o igual a la de otra fuente sin memoria con el mismo alfabeto y con símbolos equiprobables

   (c) La entropía de una fuente es siempre menor o igual que la longitud media de la codificación, sin pérdidas, de la fuente

   (d) Alguna de las anteriores es falsa

c) $\bar{L} \geq H \qquad E = \frac{H}{\bar{L}} \leq 1$ OK

b) $0 \leq H(F) \leq \underbrace{\log_2 F}_{\text{entropía con símbolos equipr.}}$

Fuente sin memoria → + incertidumbre
+ entropía

D

17. Sean a, k, p números naturales, con p primo y sea $mcd(a, p) = 1, a < p$. El valor de $C = (a^{kp}) mod p$ es:

   (a) 1

   (b) $a^k mod p$

   (c) $a^{(p-k)} mod p$

   (d) Ninguna de las anteriores

$$a^{kp} \bmod p = \underbrace{a^{k(p-1)}}_{1} \cdot a^k \bmod p = a^k \bmod p$$

p primo $\Rightarrow \phi(p) = p-1$

FERMAT → $a^{k\,\phi(p)} \bmod p = 1$

N

18. Sea un código polinómico caracterizado por $g(D) = (D+1)p(D)$, con $p(D)$ un polinomio primitivo de grado 17. No puede asegurarase la detección de:

(a) $e(D) = D^{25} + D^{17} + D^{15} + D^8$

(b) $e(D) = D^{127} + D^{23} + D^2 + D + 1$

(c) $e(D) = D^{1024} + 1$

(d) Ninguna de las anteriores

b] # impar errores $\Rightarrow (D+1)$ lo detecta

a] Long ráfaga $= 25 - 8 = 17$

grado $(g(D)) = 18$

Long ráfaga $<$ grado $(g(D)) \Rightarrow$ lo detecta

c] $p(D)$ primitivo $\Rightarrow D^\lambda + 1 \neq 0 \quad \forall \lambda < 2^{17} - 1$

$\Rightarrow D^{1024} + 1 \mod p(D) \neq 0$

lo detecta

N

19. Sea una fuente sin memoria con 3 símbolos $\{A, B, C\}$. Se sabe que $p(A) = 0.5$. La entropía máxima de una fuente extendida de orden 2 es:

(a) 2 bits

(b) 2.5 bits

[(c)] 3 bits

(d) Ninguna de las anteriores

ENTROPIA MAX : B, C equiprob

$p(A) = \frac{1}{2}$ $p(B) = \frac{1}{4}$ $p(c) = \frac{1}{4}$

$H(F)_{max} = \frac{1}{2} \log_2 2 + \frac{1}{4} \log_2 4 + \frac{1}{4} \log_2 4 = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} = 1'5$

$H(F^2) = 2\, H(F) = 3$ bits

F

20. Sea un usuario A de un sistema RSA con los siguientes parámetros: $e = 723; \phi(N) = 1012$. Decodifique $C = 45$, enviado por un usuario B de forma confidencial al usuario A.

(a) $M = 436$
(b) $M = 234$
(c) $M = 45$
(d) Ninguna de las anteriores

$\Phi(N) = 2^2 \cdot 11 \cdot 23 = (p-1)\cdot(q-1) = 22 \cdot 46 = 1012$

$p = 23$, $q = 47$ $\Big\}$ $N = 1081$

$e \cdot d = 1 + k \cdot \phi(N)$

$d = \dfrac{1 + k \cdot 1012}{723} = \dfrac{1 + k \cdot (723 \cdot 1 + 289)}{723} = 1 \cdot k + \underbrace{\dfrac{289k + 1}{723}}_{k_1}$

$1012 = 1 \cdot 723 + 289$

$723 k_1 = 289k + 1$

$k = \dfrac{723k_1 - 1}{289} = \dfrac{(2 \cdot 289 + 145)k_1 - 1}{289}$

$= 2k_1 + \dfrac{145k_1 - 1}{289}$

$k_1 = 2 \Rightarrow k = 5 \Rightarrow \boxed{d = 7}$

$M = C^d \bmod N = 45^7 \bmod 1081 = 436$