ETSETB
Curso 2005-06 Otoño
EXAMEN DE TRANSMISIÓN DE DATOS
23 de enero de 2006

PUBLICACIÓN DE NOTAS PROVISIONALES: 26/01/2006
FECHA LÍMITE PARA LAS ALEGACIONES: 29/06/05
PUBLICACIÓN DE NOTAS DEFINITIVAS: 30/06/05
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

1. Sabiendo que la información mutua entre dos variables aleatorias A y B NO es nula, es FALSO que:
   a) $H(B|A) < H(B)$
   b) $H(B,A) < H(A) + H(B)$
   c) $H(A|B) \geq H(A) - H(B)$
   d) Alguna de las anteriores es falsa

a) $I(A;B) = H(B) - H(B/A) > 0 \Rightarrow H(B) > H(B/A)$

b) $I(A;B) = H(A) + H(B) - H(A;B) > 0$

$H(A) + H(B) > H(A;B)$

c) $I(A;B) = H(A) - H(A/B) > 0$

$I(A;B) = H(B) - H(B/A) > 0$

$H(A) - H(A/B) = H(B) - H(B/A)$

$H(A/B) = H(A) - H(B) + H(B/A)$

$H(B/A) \geq 0 \Rightarrow H(A/B) \geq H(A) - H(B)$

d) FALSO

2. Una fuente binaria queda caracterizada por las probabilidades $p(A|A) = 0{,}1$ y $p(B|B) = 0{,}4$. Los símbolos emitidos atraviesan un canal binario con $p_e = 0{,}13$ ¿Cuál es la entropía a la salida del canal?

a) 0,77 bits/símbolo
b) 0,88 bits/símbolo
c) 0,93 bits/símbolo
d) Ninguna de las anteriores

$$\left.\begin{matrix} p(A|A) = 0'1 \\ p(B|B) = 0'4 \end{matrix}\right\} \quad \left.\begin{matrix} p(A) = p(A|A)p(A) + p(A|B)p(B) \\ p(A)+p(B) = 1 \end{matrix}\right\} \quad \left.\begin{matrix} p(A) = 0'4 \\ p(B) = 0'6 \end{matrix}\right.$$

$$p_S(A|A) = p(A|A)(1-p_e) + p(B|A)\,p_e = 0'204$$

$$p_S(B|B) = p(A|B)\,p_e + p(B|B)(1-p_e) = 0'426$$

$$H_S(X|A) = p_S(A|A)\log_2 \frac{1}{p_S(A|A)} + p_S(B|A)\log_2 \frac{1}{p_S(B|A)} = 0'73$$

$$H_S(X|B) = p_S(A|B)\log_2 \frac{1}{p_S(A|B)} + p_S(B|B)\log \frac{1}{p_S(B|B)} = 0'984$$

$$H_S = H_S(X|A)\,p(A) + H_S(X|B)\,p(B) = \underline{0'882 \text{ bits/sím}}$$

3. Sean $F_1 = \{1,2,3\}$ y $F_2 = \{2,4,6,8\}$ dos fuentes equiprobables independientes. Sea una fuente (F) cuya salida es el mínimo común múltiplo de la salida de las fuentes anteriores $F = mcm(F_1, F_2)$. La entropía de F condicionada al valor 6 de F_2 $H(F|F_2 = 6))$ vale:

[a] 0 bits/símbolo

b) 0,9 bits/símbolo

c) 1 bit/símbolo

d) Ninguna de las anteriores

F_1	F_2	F
1	6	6
2	6	6
3	6	6

PARA $F_2 = 6$ F siempre vale 6 (debido a que todos los elementos de F_1 son factores de 6).

POR LO TANTO $H(F|F_2 = 6) = 0$

6. Sea una fuente de 2 símbolos A y B con las siguientes probabilidades: $P(B) = 1/3, P(B/B) = 0{,}2$. Calcule la entropía de la fuente.

   a) 0,677 bits/símbolo
   b) 0,715 bits/símbolo
   c) 0,888 bits/símbolo
   d) Ninguna de las anteriores

$$p(B) = p(B/A)p(A) + p(B/B)p(B)$$

$$p(B) + p(A) = 1$$

$$p(A) = 2/3$$
$$p(A/B) = 0'8 \quad p(B/B) = 0'2$$
$$p(B/A) = 0'4 \quad p(A/A) = 0'6$$

$$H(X|A) = p(A/A)\log_2 \frac{1}{p(A/A)} + p(B/A)\log_2 \frac{1}{p(B/A)} = 0'971$$

$$H(X|B) = p(A/B)\log_2 \frac{1}{p(A/B)} + p(B/B)\log_2 \frac{1}{p(B/B)} = 0'722$$

$$H = H(X/A)p(A) + H(X|B)p(B) = 0'888$$

5. Para el código ISBN 846*310592 en el que se ha borrado la cuarta posición, puede afirmarse que

a) No puede calcularse el valor del dígito borrado
b) El valor del dígito borrado es 9
c) El valor del dígito borrado es 6
d) Ninguna de las anteriores

b,c)

$$ISBN \rightarrow H^T_{nxr} = \begin{pmatrix} 10 \\ 9 \\ 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ \hline 1 \end{pmatrix} = \begin{pmatrix} -P \\ \hline I_r \end{pmatrix}$$

a) ISBN:
$\rho = 1$ → corrige 1 borrón
$\delta = 1$ → detecta 1 error
$e = 0$ → no corrige errores

$$S = z \cdot H^T = \emptyset \Rightarrow 846a310592 \cdot \begin{pmatrix} 10 \\ 9 \\ 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{pmatrix} = 80 + 36 + 48 + 7a + 18 +$$

$$+ 5 + 15 + 18 + 2 = 222 + 7a$$

$$(222 + 7a) \bmod 11 = \emptyset$$

$222 \;|\; 11$
20

$11 \cdot 21 = 231$
$231 - 222 = 9$

$11 \cdot 22 = 242$
$242 - 222 = 20$

$11 \cdot 23 = 253$
-222
31

$11 \cdot 24 = 264$
-222
$42 \;|\; 7$
(6)

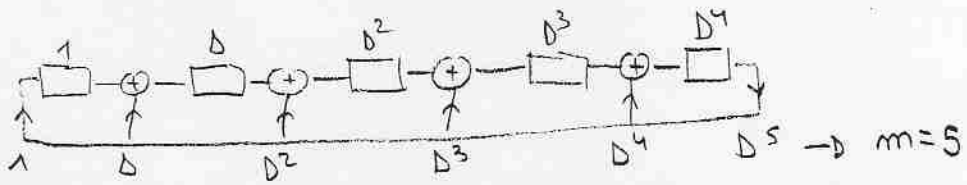
7. Para un LFSR con polinomio de conexiones $D^5 + D^4 + D^3 + D^2 + D + 1$

a) Si el estado inicial es $D^4 + D^3 + D^2 + D + 1$ al cabo de 11 iteraciones el polinomio de estado no tiene término independiente

b) Si el estado inicial es $D + 1$ al cabo de 12 iteraciones el estado es $D + 1$

c) Si el estado inicial es D al cabo de 4 iteraciones el estado es 1

d) Ninguna de las anteriores



- $C(D)$ es un polinomio completo → $L \leq L_{max} = m+1$
- L depende del $p^{(0)}(D)$. Hay ciertos $p^{(0)}(D)$ que llevan a L_{max},

POR EJEMPLO CUALQUIER $p^{(0)}(D)$ DEL CONJUNTO:

$\{1, D, D^2, D^3, D^4, 1+D+D^2+D^3+D^4\} \Rightarrow L = L_{max} = m+1 = 6$

¡ PERO PUEDE HABER OTROS CONJUNTOS DE $p^{(0)}(D)$ EN QUE $L = L_{max}$ TAMBIÉN!

a) $D \cdot p^{(11)}(D) \mid C(D)$ → $p^{(12)}(D)$ | $\{0, 1\}$ → Estado último registro al cabo de 11 iteraciones.

con este $p^{(0)}(D)$, $L = m+1 = 6$.

$p^{(12)}(D) = p^{(6)}(D) = p^{(0)}(D) = D^4 + D^3 + D^2 + D + 1$

$D \cdot p^{(11)}(D) = C(D) \cdot \{0, 1\} + p^{(12)}(D) = (D^5 + D^4 + D^3 + D^2 + D + 1) \cdot \{0, (1)\} + D^4 + D^3 + D^2 + D + 1 =$

(1) ES UN 1

$= D^5 \Rightarrow p^{(11)}(D) = D^4 \equiv 0\,0\,0\,0\,\underline{1}$

b) $p^{(m)}(D) = D^m \cdot p^{(0)}(D) \bmod C(D)$

$p^{(12)}(D) = D^{12} \cdot (D+1) \bmod C(D) = D+1$

$D^{13} + D^{12} \mid D^5 + D^4 + D^3 + D^2 + D + 1$

$D^{13} + D^{12} + D^{11} + D^{10} + D^9 + D^8 \quad | \quad D^8 + D^6 + D^2 + 1$

$D^{11} + D^{10} + D^9 + D^8$

$D^{11} + D^{10} + D^9 + D^8 + D^7 + D^6$

$D^7 + D^6$

$D^7 + D^6 + D^5 + D^4 + D^3 + D^2$

$D^5 + D^4 + D^3 + D^2$

$D^5 + D^4 + D^3 + D^2 + D + 1$

$D + 1$

c) $D = p^{(0)}(D)$

D^2

D^3

D^4

$1 + D + D^2 + D^3 + D^4 = p^{(4)}(D)$

1

D

D^2

$\vdots$

8. La distancia mínima y la distancia máxima de un código corrector de errores es 4. Indique la respuesta correcta

a) Si hay 2 errores y se intenta corregir, la tasa de acierto del decodificador siempre es 0,5
b) Si hay 3 errores y se intenta corregir, la tasa de acierto del decodificador siempre es 0
c) Se trata de un código 1-perfecto
(d) Ninguna de las anteriores

La distancia entre cualquier pareja de palabras es 4, pero al no ser un código perfecto, dada una palabra código, no todas las palabras a distancia 4 son también palabra código.

Asimismo, si hay 2 errores puede ser que la palabra resultante sea equidistante entre varias palabras código.

Ej: (7, 3)

0000000
0010111
0101011
1001101
0111100
1011001
1110001
1100110

→ Y: 0000000 → 2 errores → Z = 1100000

↓

Decodificación equiprobable entre
0000000, 1110001 y 1100110
prob acierto = 1/3 ≠ 1/2

b) No. Ejemplo código con 2 palabras código < 0000000 / 1111000

Si los 3 errores se dan en las últimas posiciones → 0000111 se puede corregir.

c) No es perfecto ⇒ (d) Ninguna anteriores

9. Un sistema RSA utiliza los valores $p = 29$ y $q = 43$. Un usuario quiere cifrar el mensaje (en binario con el mayor peso a la izquierda) 1011110111ρ10110110101, usando exclusivamente dicho algoritmo. Indíquese la longitud máxima del texto cifrado

a) 11 bits
b) 22 bits
c) 33 bits
d) 40 bits

$N = p \cdot q = 1247$ ⇒ Los bloques a cifrar no pueden superar los 10 bits y el resultado de cada bloque puede ser un número entre 0 y 1246 ⇒ pueden llegar a ser necesario 11 bits.

El mensaje es de 22 bits ⇒ 3 bloques

⇓

33 bits de salida

4. Sea $f(\vec{u})$ el codificador de un código de Hamming (7,4) y sea $g(\vec{v})$ su decodificador. Se puede asegurar que:

a) $g(\vec{v})$ es biyectiva
b) Existen 8 valores distintos de $\vec{v}$ que tienen la misma imagen $g(\vec{v})$
c) Pueden existir más de 8 valores distintos de $\vec{v}$ que tienen la misma imagen $g(\vec{v})$
d) Nada de lo anterior puede afirmarse.

Todas las n-plas que difieren en un solo error y la propia palabra código, generan el mismo valor de información $7+1=8$

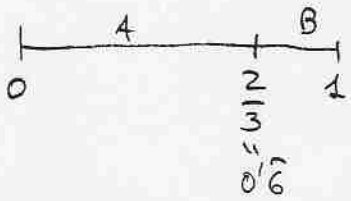
10. Una fuente emite dos símbolos con las probabilidades $p(A) = 2/3$ y $p(B) = 1/3$. Si se utiliza un código aritmético asignando el primer segmento al símbolo A, se puede afirmar que:

   a) El mensaje de 3 símbolos codificado como 0.75 es BAB

   b) El mensaje BA puede codificarse como 0.5

   c) Los mensajes AB y ABA pueden codificarse como 0.5

   d) Ninguna de las anteriores



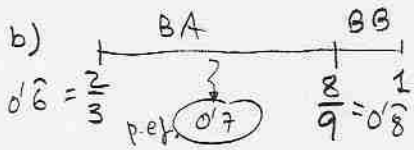
a) $0'75 \longrightarrow B$

$\frac{0'75 - 2/3}{2/3} = 0'125 \longrightarrow A$

$\frac{0'125 - 0}{2/3} = 0'1875 \longrightarrow A$

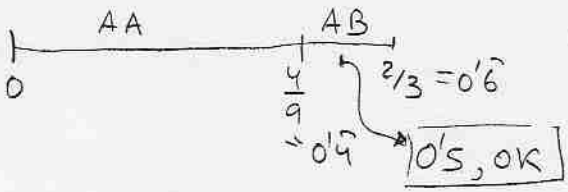
BAA

b)

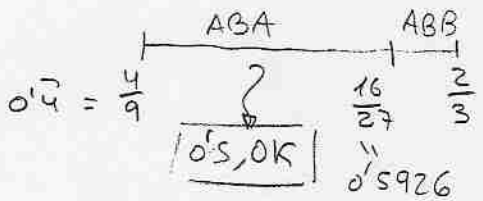


$\frac{2}{3} + \left(1 - \frac{2}{3}\right) \cdot \frac{2}{3} = \frac{8}{9} = 0'8$

c)



$0 + \left(\frac{2}{3} - 0\right) \cdot \frac{2}{3} = \frac{4}{9} = 0'4$



$\frac{4}{9} + \left(\frac{2}{3} - \frac{4}{9}\right) \cdot \frac{2}{3} = \frac{16}{27} = 0'5926$

añadir 1 espacio

12. En un sistema RSA, al cifrar el mensaje $M = 247400 (< N)$ se obtiene el criptograma C, cumpliéndose que $mcd(C, N) \neq 1$. Sabiendo que N no tiene factores primos menores que 1000 y que los números 1231, 1237 y 1249 son primos, se puede afirmar que:

   a) N es múltiplo de 1231
   b) N es múltiplo de 1237
   c) N es múltiplo de 1234
   d) Ninguna de las anteriores

$M = 247400 = 2^3 \cdot 5^2 \cdot 1237$

$M^e = C + kN$ (↑ $p \cdot q$) $\quad mcd(C,N) = \begin{cases} 1 \\ p \\ q \end{cases} \neq 1 \Rightarrow$ (p)

los divisores de C y N también han de serlo de M $\Rightarrow$

$p = 1237$

11. Un sistema binario de transmisión de datos presenta una probabilidad de error de bit de $Pe = 0{,}13\ 10^{-4}$. Se desea una probabilidad de error de bit al usuario $Pe_u < 10^{-12}$. Para ello se decide incorporar un código binario de longitud $n = 15$. ¿Cuál ha de ser la capacidad correctora mínima del código para satisfacer las especificaciones?

   a) 1
   b) 2
   c) 3
   d) Ninguna de las anteriores

$P_E \simeq \binom{15}{3} pe^3 (1-pe)^{12} = 10^{-13} \Rightarrow peus = \left(\frac{3+2}{15}\right) 10^{-13} = 3'3\ 10^{-13}$

13. Sabiendo que D^{510} mod $C(D)$ vale D^2, entonces:

a) $C(D)$ puede ser un polinomio primitivo de grado 6
b) $C(D)$ puede ser un polinomio primitivo de grado 7
c) $C(D)$ puede ser un polinomio primitivo de grado 8
d) Ninguna de las anteriores

$D^L \bmod C(D) = 1$ para L: longitud de la secuencia que contenga el estado 1

Si $C(D)$ primitivo $\Rightarrow L = L_{max} = 2^n - 1$

n: grado de $C(D)$

SIMPLEMENTE HAY VER QUE

Si $D^{510} \bmod C(D) = D^2 \Rightarrow D^{508} \bmod C(D) = 1$

HAY QUE COMPROBAR ENTONCES SI 508 ES MÚLTIPLO DE ALGUNO DE LOS PERIODOS PROPUESTOS

a] $n = 6 \Rightarrow L_{max} = 63$ $\quad 508 \bmod 63 = 4$

b] $n = 7 \Rightarrow L_{max} = 127$ $\quad 508 \bmod 127 = 0$

c] $n = 8 \Rightarrow L_{max} = 255$ $\quad 508 \bmod 255 = 253$

POR LO TANTO $C(D)$ PUEDE SER UN POL PRIMITIVO DE GRADO 7

16. Sobre un certificado digital, es FALSO que:

a) Vincula un identificador de entidad con una clave pública
b) Garantiza que la parte que lo envía es el poseedor legítimo del certificado
c) Lo genera una tercera parte de confianza
d) Es un documento firmado digitalmente

15. ¿ Cuál de las siguientes afirmaciones sobre las funciones de hash es FALSA?

a) La salida es de longitud fija
b) La entrada es de longitud variable
c) Múltiples mensajes tienen la misma función de hash
d) Alguna de las anteriores es falsa

14. ¿Cuál de los siguientes ataques NO es un ataque activo?:

a) Modificación de la información
b) Suplantación
c) Escucha
d) Todos los anteriores son ataques activos

17. Indique cuál de las siguientes afirmaciones es FALSA:

a) $27^{30} mod_{31} = 1$

b) Siendo $135529 = 433 \bullet 313$, se verifica que ~~$2009^{134783} mod_{135529} = 101$~~ $42059^{134783} \bmod 135529 = 2710$

c) El número de elementos que tienen inversa, respecto a la operación producto, en el anillo Z_{77} es 60

d) Alguna de las anteriores es falsa

a) Teorema Fermat $a^{p-1} \bmod p = 1 \quad (n = p)$

$n = p = 31 \quad \varphi(31) = 30$

$a^{\varphi(n)} \bmod n = 1 \;,\; mcd(a,n) = 1$

$27^{30} \bmod 31 = 1 \;,\; mcd(27,31) = 1$

b) $n = 135529 = 433 \cdot 313$

$\varphi(n) = 432 \cdot 312 = 134784$

$a^{\varphi(n)-1} \bmod n = a^{-1}$

a^{-1} inverso de a en Z_n

Se verifica la relación si

$a \cdot a^{-1} = 1 + kn$

$42059 \cdot 2710 = 1 + 841 \cdot 135529$

c) $n = 77 = 7 \cdot 11$

$\varphi(n) = 6 \cdot 10 = 60 \Rightarrow$ Cardinal del conjunto reducido de residuos

$\varphi(n)$
$\parallel$
77

d) FALSO

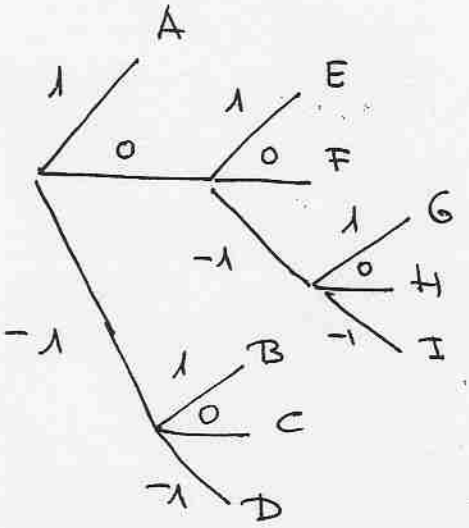
18. Se aplica una codificación ternaria de Huffman sobre una fuente sin memoria cuyas probabilidades de símbolo son: $P(A) = 1/3; P(B) = P(C) = P(D) = P(E) = P(F) = 1/9; P(G) = P(H) = P(I) = 1/27$. Indique cuál de las siguientes afirmaciones es cierta

a) La longitud media de la codificación es 1,77 dígitos ternarios por símbolo

b) La entropía de la fuente es 1,1167 bits/símbolo

c) Extendiendo la fuente se podría mejorar la eficiencia de codificación

d) Ninguna de las anteriores



Simbl Codificación

A → 1

B → -1 1

C → -1 0

D → -1 -1

E → 0 1

F → 0 0

G → 0 -1 1

H → 0 -1 0

I → 0 -1 -1

a) $L = 1'77 = \frac{1}{3}\cdot 1 + \frac{1}{9}\cdot(2+2+2+2) + \frac{1}{27}(3+3+3)$ CIERTO

b) $H = \sum_{k=1}^{9} P_k \log_2 \frac{1}{P_k} = L \cdot \log_2 3 = 2'81 \text{ bits/simb} \neq 1'77$

FALSO

c) $E = \frac{H}{L} = \frac{L_{\text{tribits/simb}}}{L_{\text{dig ternarios/simb}}} = 1$

La eficiencia es máxima, la extensión de fuente no puede mejorar E

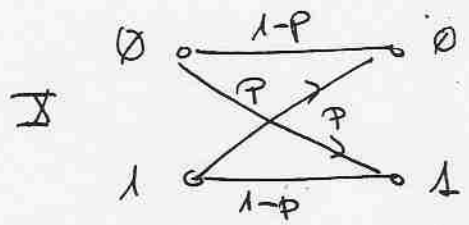
FALSO

d) FALSO

19. Un canal binario simétrico tiene por valores de entropía $H(X)$, $H(E)$ y $H(Y)$ correspondientes a la entrada, el ruido y la salida del canal, respectivamente. Teniendo en cuenta que ninguno de los tres valores es nulo, indique cuál de las siguientes afirmaciones es FALSA:

a) $H(Y) \geq H(X)$
b) $H(Y|X) = H(Y) - I(X;Y)$
c) $H(X|Y) > H(X) - H(Y) + H(E)$
d) Alguna de las anteriores es falsa

a)



$H(X) > 0$
$H(Y) > 0$
$H(E) = H(p) > 0$

a) $H(Y)$ siempre es mayor que $H(X)$ y $H(E)$ salvo cuando $H(X)$ o $H(E)$ es 1 bit/simb. En este caso $H(Y) = H(X)$ o $H(Y) = H(E)$. Por lo tanto $H(Y) \geq H(X)$ siempre se verifica

b) En general $I(X;Y) = H(Y) - H(Y/X)$

c) $I(X;Y) = H(X) - H(X/Y)$

$I(X;Y) = H(Y) - H(Y/X)$

Se verifica que $H(Y/X) = H(E)$

Por lo tanto:

$$H(X) - H(X/Y) = H(Y) - H(E)$$

$$H(X/Y) = H(X) - H(Y) + H(E)$$

La relación es de igualdad no de mayor.

FALSA

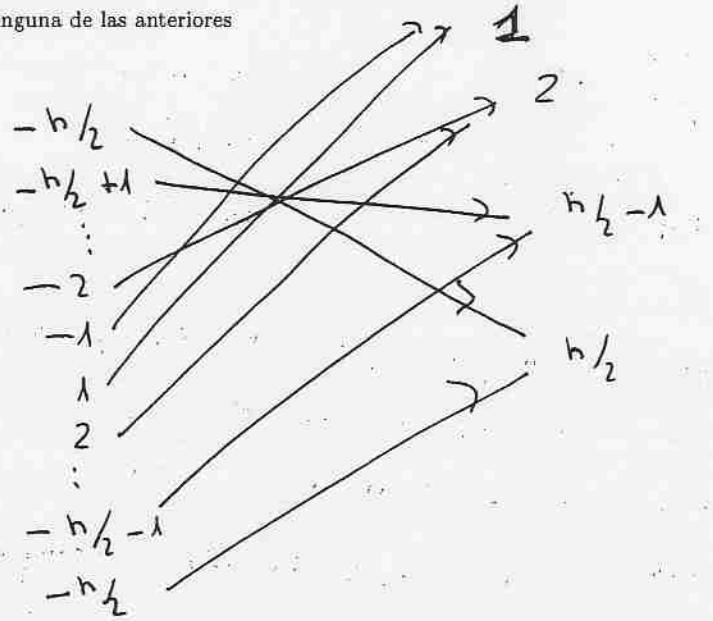
d) CIERTA

20. Un canal tiene a la entrada una fuente con alfabeto:

$$\{-n/2, -n/2+1, ..., -2, -1, 1, 2, ..., n/2-1, n/2\},\ n\ par$$

La salida del canal es el valor absoluto del símbolo a la entrada. Indique cuál de las siguientes afirmaciones es CIERTA:

a) La entropía a la salida del canal es siempre la mitad que a la entrada
b) La entropía a la entrada depende exclusivamente de n
c) La capacidad del canal es igual a la máxima entropía de una fuente de $n/2$ símbolos
d) Ninguna de las anteriores



a) No tiene porqué producirse esta relación.
Ejemplo. Si los símbolos a la entrada son equiprobables la relación entrada a salida es:

FALSO $\quad \frac{H(Y)}{H(X)} = \frac{\log_2 n/2}{\log_2 n} = \frac{\log_2 n - 1}{\log_2 n} \neq 1/2 \quad n>4$

b) La entropía siempre depende de la estadística de la fuente y no del ~~no~~ número de símbolos de la fuente.
FALSO

c) $C = \max_{p(x)} \left(H(Y) - H(Y/X) \right) = \max_{p(x)} H(Y) = \log_2 n/2$ ($H(Y/X) \to \emptyset$)

La entropía máxima de una fuente de $n/2$ símbolos será también $\log_2 n/2$. CIERTA

d) FALSO