ETSETB
Curso 2007-08 Otoño
EXAMEN DE TRANSMISIÓN DE DATOS
16 de enero de 2008

PUBLICACIÓN DE NOTAS PROVISIONALES: 22/01/2008
FECHA LÍMITE PARA LAS ALEGACIONES: 24/01/2008 a las 14:00 horas
PUBLICACIÓN DE NOTAS DEFINITIVAS: 29/01/2008

NOTAS IMPORTANTES:

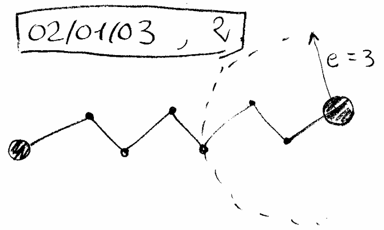
- Toda hoja de respuestas que no esté completamente identificada será anulada.
- La numeración en la hoja de respuestas es la de la *izquierda* (*correlativas*)
- No se responderá a ninguna pregunta sobre el enunciado. El alumno responderá según su criterio pudiendo realizar las alegaciones que considere 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 EXPRESÁMENTE 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. En un juego de azar se lanzan 23 monedas y la apuesta consiste en pronosticar los resultados de dichos lanzamientos (ordenados). Un jugador realiza el número mínimo de apuestas que le garantizan tener, al menos, 20 aciertos. ¿Cuál es la probabilidad que consiga al menos 22 aciertos? NOTA: Existe un código binario (23,12) que es perfecto y tiene una distancia mínima de 7

   a) 1/256
   b) 2/256
   c) 3/256
   d) Ninguna de las anteriores

$\boxed{02/01/03\ ,\ 2}$



$n = 23,\ k = 12$

$d_{min} = 7$

$e = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 3$

Apostando a TODAS las palabras código se consigue que cualquier resultado esté como mucho a distancia 3 de alguna apuesta.
$\Rightarrow$ Por tanto, 20 aciertos. Nº apuestas mínimo $= 2^k = 2^{12}$

Para acertar 22 o 23 resultados, ha de salir una n-tupla que diste 1 de una palabra código (22 aciertos) o una palabra código (23 aciertos).

Probabilidad $= \dfrac{2^{12} \cdot 23 + 2^{12}}{2^{23}} = \dfrac{3}{256}$

2. En una implementación del algoritmo RSA se tiene que C=119 (se ha cifrado para ofrecer confidencialidad). Un atacante cifra el criptograma con la clave pública del ~~emisor~~ receptor! de forma iterativa, obteniendo los siguientes valores: 6, 93, 175, 54, 123, 119. ¿Cuál es el mensaje en claro?

   a) 6
   b) 93
   c) 123
   d) Ninguno de los anteriores

Se trata de un ataque cíclico.

$$\begin{array}{ll} C & 6 \\ C^e & 93 \\ (C^e)^e & 175 \\ \vdots & 54 \\ \boxed{M} & 123 \quad \boxed{M=123} \\ M^e = C & 119 = C \end{array}$$

4. En un sistema RSA se tiene que $\Phi(n)$=75362 y se toma e=28137. Calcúlese el valor de d.

   a) 26567
   b) 35199
   c) 23185
   d) Un sistema RSA no puede tener esos parámetros.

$\phi(n) = (p-1)(q-1)$

Dado que p y q deben ser primos grandes, p y q son impares $\rightarrow$ $p-1$, $q-1$ son pares

$\Rightarrow$ $\phi(n)$ es múltiplo de 4

y 75362 no lo es.

3. Un código corrector de errores es diseñado de forma que todos los bits del mensaje aparecen en la palabra código y se añaden r bits de redundancia, siendo cada uno de ellos un bit de paridad correspondiente a un subconjunto de bits del mensaje. Indíquese que afirmación es correcta

   a) La capacidad detectora de errores siempre es r.

   b) No se puede garantizar que el código sea sistemático

   c) Para calcular la distancia mínima del código, basta calcular el peso de Hamming de todas las filas de la matriz generadora

   d) Ninguna de las anteriores

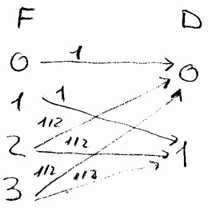
b/ No se dice nada respecto al orden de los bit de paridad, y por ello no se puede garantizar que sea sistemático

La c) es incorrecta ya que debe compararse todas las palabras código y no sólo las de la base.

La a/ es incorrecta; sería una cota.

5. Una fuente tiene un alfabeto {0, 1, 2, 3}, siendo las probabilidades de emisión de símbolos $x, y, z, 1-x-y-z$, respectivamente. Cuando se emite un 0 o un 1 el canal se comporta de forma perfecta, es decir, se recupera un 0 o un 1 respectivamente (el símbolo enviado). En cambio, cuando se emite un 2, o un 3 se recupera un 0 con probabilidad 0.5, o un 1 con probabilidad 0.5. Calcule la capacidad del canal discreto.

   a) [0, 0.5)
   b) [0.5, 0.75)
   c) [0.75, 1)
   d) Ninguna de las anteriores



$$p(D \backslash F) = \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 1 \\ 2 & 1/2 & 1/2 \\ 3 & 1/2 & 1/2 \end{array}$$

$$C = \max_{p\{F\}} \left[H(D) - H(D \backslash F) \right]$$

$$H(D\backslash F) = p(F=0)\cdot\left(1 \log_2 1 + 0\right) + p(F=1)\cdot\left(0 + 1\cdot \log_2 1\right) + \left(p(F=2) + p(F=3)\right)\cdot\left(2\cdot\frac{1}{2}\log_2 2\right) =$$
$$= z + 1 - x - y - z = 1 - x - y$$

$$H(D) = \sum_{j=1}^{2} p(D_j)\cdot \log_2 \frac{1}{p(D_j)}$$

$$P(D=0) = p(F=0) + \frac{1}{2}\cdot P(F=2) + \frac{1}{2} P(F=3) = x + \frac{1}{2}\left(z + 1 - x - y - z\right) = x + \frac{1-x-y}{2} = \frac{1+x-y}{2}$$

$$P(D=1) = P(F=1) + \frac{1}{2} P(F=2) + \frac{1}{2} P(F=3) = y + \frac{1-x-y}{2} = \frac{1+y-x}{2}$$

$$H(D) = \frac{1+x-y}{2}\cdot \log_2 \frac{2}{1+x-y} + \frac{1+y-x}{2}\cdot \log_2 \frac{2}{1+y-x}$$

$$C(x,y) = \left[\frac{1+x-y}{2} \log_2 \frac{2}{1+x-y} + \frac{1+y-x}{2}\cdot \log_2 \frac{2}{1+y-x} - 1 + x + y \right]$$

No depende de z.

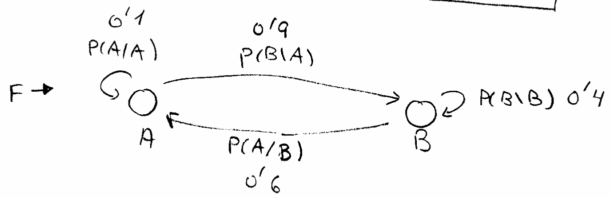
Para $x = y = \frac{1}{2}$ → $\boxed{H(D\backslash F) = 0}$; $H(D) = 1$ → $\boxed{C = 1 \text{ bit/símbolo}}$

$P(D=0) = 1/2$
$P(D=1) = 1/2$ → D es equiprobable

6. 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 $p_e = 0,134$. ¿Cuál es la entropía a la salida del canal?

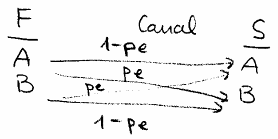
a) 0.77 bits/símbolo
b) 0.88 bits/símbolo
c) 0.93 bits/símbolo
d) Ninguna de las anteriores

$\boxed{23/01/06\ ,\ 2}$



$$P(A) = P(A\backslash A)\cdot P(A) + P(A\backslash B)\cdot P(B)$$
$$P(A) + P(B) = 1$$

$$0'9 \cdot P(A) = 0'6 \cdot P(B)$$
$$0'9 \cdot P(A) = 0'6\,(1 - P(A))$$
$$1'5 \cdot P(A) = 0'6$$
$$P(A) = 0'4 \ ; \ P(B) = 0'6$$



$$P_S(A\backslash \underline{\underline{A}}) = P(A\backslash \underline{\underline{A}}) \cdot (1-p_e) + P(B\backslash \underline{\underline{A}})\cdot p_e = 0'1\,(1-0'134) + 0'9\cdot 0'134 =$$
$$= 0'2072 \rightarrow P_S(B\backslash \underline{\underline{A}}) = 0'7928$$

$$P_S(B\backslash \underline{\underline{B}}) = P(A\backslash \underline{\underline{B}})\cdot p_e + P(B\backslash \underline{\underline{B}})\cdot(1-p_e) = 0'6\cdot 0'134 + 0'4\cdot(1-0'134) =$$
$$= 0'4268 \rightarrow P_S(A\backslash \underline{\underline{B}}) = 0'5732$$

$$H_S(S\backslash \underline{\underline{A}}) = P_S(A\backslash \underline{\underline{A}})\cdot \log_2 \frac{1}{P_S(A\backslash \underline{\underline{A}})} + P_S(B\backslash \underline{\underline{A}})\cdot \log_2 \frac{1}{P_S(B\backslash \underline{\underline{A}})} = 0'7361 \ \frac{\text{bits}}{\text{símbolo}}$$

$$H_S(S\backslash \underline{\underline{B}}) = P_S(A\backslash \underline{\underline{B}})\cdot \log_2 \frac{1}{P_S(A\backslash \underline{\underline{B}})} + P_S(B\backslash \underline{\underline{B}})\cdot \log_2 \frac{1}{P_S(B\backslash \underline{\underline{B}})} = 0'9845 \ \frac{\text{bits}}{\text{símbolo}}$$

$$H_S = H_S(S\backslash A)\cdot P(A) + H_S(S\backslash B)\cdot P(B) =$$
$$= 0'7361\cdot 0'4 + 0'9845\cdot 0'6 = 0'8851 \ \frac{\text{bits}}{\text{símbolo}}$$

7. Indíquese la respuesta correcta relativa a certificados digitales

a) Es un documento confidencial que permite la identificación de un usuario

b) Es un documento auténtico que garantiza la identidad de su poseedor

c) Es un documento confidencial que garantiza la identidad de su poseedor

d) Es un documento auténtico que permite la identificación de un usuario

a y c falsas, ya que no es confidencial.
b es falsa ya que un certificado es un documento público que puede tener cualquier usuario; sólo permite identificar al usuario o entidad cuyo nombre consta en el certificado ⇒ d) correcta.

9. Sean $F_1 = \{1, 2, 3\}$ y $F_2 = \{5, 7\}$ dos fuentes equiprobables e independientes. Sea F una fuente cuya salida es el producto de los simbolos emitidos por F_1 y F_2 ($F = F_1 * F_2$). La información mutua entre F y F_1 vale:

a) 0

b) 1

c) $log_2(3)$

d) Ninguna de las anteriores

F_1	F_2	F
1	5	5
1	7	7
2	5	10
2	7	14
3	5	15
3	7	21

$H(F) = \log_2 6$

$H(F/F_1) = 1 = \log_2 2$

$I(F, F_1) = H(F) - H(F/F_1) =$

$= \log_2 6 - \log_2 2 = \log_2 3$

8. Para codificar bloques de 7 bits de información se usa un código lineal y sistemático basado en el polinomio $g(D) = D^3 + D + 1$. Se produce un único error que afecta al primer bit recibido (el de mayor peso). El resto al dividir el bloque recibido entre $g(D)$ es:

   a) D
   b) D^2
   c) D^5
   d) Ninguna de las anteriores

Grado $g(D)$ 3 $\Rightarrow$ $r = 3$

$k = 7$, $r = 3$ $\Rightarrow$ $n = 10$

error : 1 0 0 0 0 0 0 0 0 0

$e(D) = D^9$

$$
\begin{array}{l|l}
D^9 & D^3 + D + 1 \\ \hline
D^9 + D^7 + D^6 & D^6 + D^4 + D^3 + D^2 \\ \hline
D^7 + D^6 & \\
D^7 + D^5 + D^4 & \\ \hline
D^6 + D^5 + D^4 & \\
D^6 + D^4 + D^3 & \\ \hline
D^5 + D^3 & \\
D^5 + D^3 + D^2 & \\ \hline
D^2 &
\end{array}
$$

D^2 //

10. Sea una fuente compuesta por 32 símbolos equiprobables. La eficiencia de una codificación de Huffman de esta fuente vale:

a) 0.86
b) 0.92
c) 1
d) Ninguna de las anteriores

$H(F) = \log_2 32 = 5$

HUFFMAN → CODIF LONG FIJA (5 bits/símbolo)

$$E = \frac{H(F)}{l} = \frac{5}{5} = 1$$

13. Sea un código de Hamming usado como corrector y caracterizado por el polinomio $g(D) = D^4 + D^3 + 1$. Si el canal tiene una probabilidad de error binaria $p = 10^{-3}$, la probabilidad binaria de error de usuario vale aproximadamente:

a) 1,05 10^{-4}
b) 2,1 10^{-5}
c) 9 10^{-6}
d) Ninguna de las anteriores

$r = 4 \Rightarrow n = 2^r - 1 \Rightarrow (15, 11)$

$$P_E(\text{BLOQUE}) \simeq \binom{15}{2} p^2 = \frac{15 \cdot 14}{2} 10^{-6} = 1'05 \cdot 10^{-5}$$

$$P_E(\text{BIT}) = \frac{d_{min}}{n} P_E(\text{BLOQUE}) = \frac{3}{15} \cdot 1'05 \cdot 10^{-5} = \boxed{2'1 \cdot 10^{-5}}$$

11. Sea un código polinómico basado en el polinomio $g(D) = D^4 + D^3 + D^2 + D + 1$. ¿Qué patrón de error no será detectado?

a) $e(D) = D^{12} + D^{11} + D^{10} + D^9$
b) $e(D) = D^{17} + D^2$
c) $e(D) = D^8 + D^7 + D^6 + D^5 + D^4 + D^3$
d) Ninguna de las anteriores

a) Se detecta pq la ráfaga es de grado menor que $g(D)$

b) No se detecta:
$g(D)$ divide a (D^5+1) por ser polin completo de grado 4, y por lo tanto tb divide a $e'(D) = D^{15}+1$
(3 veces el periodo del LFSR)

c) $e'(D) = D^5 + D^4 + D^3 + D^2 + D + 1$
$g(D)$ mod $e'(D) \neq 0 \Rightarrow$ SE DETECTA

12. ¿Qué condición NO debe cumplir un código binario 2-perfecto?

a) $d_{min} = 5$
b) $r \geq 4$
c) $n^2 + n + 2 = 2^{(r+1)}$
d) Ninguna de las anteriores

a) SI $\Rightarrow$ $e=2 \rightarrow d_{min}=5$

b) SINGLETON: $r \geqslant 4$ SI

c) # sindromes = # vectores 0,1,2 errores

$$2^r = 1 + n + \binom{n}{2}$$

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

$$2^r = \frac{n^2}{2} + \frac{n}{2} + 1$$

$$\boxed{2^{r+1} = n^2 + n + 2}$$ SI

d) POR LO TANTO d

14. Sea un sistema RSA en el que $\Phi(N_A) = 72$. ¿Cuál de los siguientes valores no es posible para p_A?

a) 13

b) 37

c) 19

d) Ninguna de las anteriores

$\phi(N_A) = 72 = 2^3 \cdot 3^2 = (p-1)(q-1)$

p, q pueden ser cualquier pareja de n.os primos que cumpla que $(p-1)$ y $(q-1)$ sean factores de $\phi(N)$.

p.e $\quad p_A = 19 \,;\; q_A = 5$

$p_A = 13 \,;\; q_A = 7$

$p_A = 37 \,;\; q_A = 3$

es decir, la correcta es d

16. Dos jugadores de tenis S1 y S2 juegan dos partidos consecutivos semanalmente. Sea X la variable aleatoria que indica al vencedor del primer partido e Y la variable aleatoria que indica al vencedor del segundo partido. Cada partido lo gana un jugador. Estadísticamente sucede que si el primer partido lo gana S1, el segundo lo gana siempre S2. Y si el primer partido lo gana S2, el segundo lo gana S2 con probabilidad 1/3. El primer partido lo gana S1 con probabilidad 1/3. Calcule I(X; Y).

   a) I(X; Y) ≤ 0,05 bits/símbolo
   b) 0,05 bits/símbolo < I(X; Y) ≤ 0,1 bits/símbolo
   c) 0,1 bits/símbolo < I(X; Y) ≤ 0,2 bits/símbolo
   d) 0,2 bits/símbolo < I(X; Y)

16

$Y \backslash X$	S_1	S_2
S_1	0	2/3
S_2	1	1/3

$P(X=S_1) = 1/3 \rightarrow P(X=S_2) = 2/3$

$I(X;Y) = H(Y) - H(Y \backslash X)$

$H(Y) = \sum_i p(y_i) \cdot \log_2 \frac{1}{p(y_i)}$

$P(y_i \backslash x_i) \cdot P(x_i) = p(y_i, x_i) \longrightarrow$

Y, X	S_1	S_2
S_1	0	4/9
S_2	1/3	2/9

$P(y_i) = \sum_i p(x_i, y_i) \longrightarrow P(y=S_1) = 0 + 4/9 = 4/9$

$P(y=S_2) = 1/3 + 2/9 = 5/9$

$H(Y) = \frac{4}{9}\log_2\frac{9}{4} + \frac{5}{9}\log_2\frac{9}{5} = 0'9911$ bits/símbolo

$H(Y \backslash X) = \underbrace{H(Y \backslash X=S_1)}_{0 + 1 \cdot \log_2 1 = 0} \cdot \underbrace{P(X=S_1)}_{1/3} + \underbrace{H(Y \backslash X=S_2)}_{\frac{2}{3}\log_2\frac{3}{2} + \frac{1}{3}\log_2 3 = 0'9183 \text{ b/símb.}} \cdot \underbrace{P(X=S_2)}_{2/3} = \cancel{0'9183}$ bits/símbolo

$0'6122$

$0'6122 \quad\quad 0'3789$

$I(X;Y) = 0'9911 - \cancel{0'9183} = \cancel{0'07277}$ bits/símbolo $\rightarrow$ b

17. Sea el código cíclico (7, 3) generado por $g(D) = 1 + D + D^2 + D^4$. ¿Qué afirmación es correcta?

a) La matriz generadora es G= $\begin{pmatrix} 1001011 \\ 0101110 \\ 0010101 \end{pmatrix}$

b) La d_{min} es 4

c) La capacidad correctora de errores es 1 y la detectora de errores es 2.

d) Ninguna de las anteriores

17) $R(D) = D^r \cdot X(D) \bmod g(D)$

$r = 4$ grado $g(D)$

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

a) $x(D) = D^2 \quad (x = 100)$

$$\begin{array}{l|l} D^6 & D^4 + D^2 + D + 1 \\ \hline D^6 + D^4 + D^3 + D^2 & D^2 + 1 \\ \hline D^4 + D^3 + D^2 & \\ D^4 + D^2 + D + 1 & \\ \hline D^3 + D + 1 & \end{array}$$

$D^6 + D^3 + D + 1$

$Y = 1001011$

$x(D) = D \quad (x = 010)$

$$\begin{array}{l|l} D^5 & D^4 + D^2 + D + 1 \\ \hline D^5 + D^3 + D^2 + D & D \\ \hline D^3 + D^2 + D & \end{array}$$

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

$Y = 0101110$

$x(D) = 1 \quad (X = 001)$

$$\begin{array}{l|l} D^4 & D^4 + D^2 + D + 1 \\ \hline D^4 + D^2 + D + 1 & 1 \\ \hline D^2 + D + 1 & \end{array}$$

$D^4 + D^2 + D + 1$

$Y = 0010111$

$$\underset{3 \quad 7}{G_{k \times n}} = \begin{pmatrix} 100 & 1011 \\ 010 & 1110 \\ 001 & 0111 \end{pmatrix} \quad \text{No!}$$

X	Y
000	000 0 000
→ 001	001 0 111
→ 010	010 1110
011	0111001
→ 100	1001011
101	1011100
110	1100101
111	1110010
D^2 D 1	$D^6 D^5 D^4 D^3 D^2 D$ 1

El resto de palabras código se obtienen del mismo modo, o bien sumando las palabras ya obtenidas.

P. ej.:

$x(D) = 1 + D \quad (X = 011)$

$$\begin{array}{l|l} D^5 + D^4 & D^4 + D^2 + D + 1 \\ \hline D^5 + D^3 + D^2 + D & D + 1 \\ \hline D^4 + D^3 + D^2 + D & \\ D^4 + D^2 + D + 1 & \\ \hline D^3 + 1 & \end{array}$$

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

$Y = 0111001$

p. ej.: $X = 110 = 100 + 010$

$Y = 1001011 + 0101110 =$
$= 1100101$

b) $W_{min} (Y \neq 0) = 4 \rightarrow d_{min} = 4$

c) $\ell = d_{min} - 1 = 3 \qquad e = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = 1$

18. Sea una fuente que emite 6 símbolos con estadísticas 0.3, 0.2, 0.2, 0.1, 0.1, 0.1. Se utiliza un código con alfabeto del código de 4 símbolos y cuyas longitudes de palabras código son {1, 1, 2, 3, 3, 3}. ¿Qué afirmación es correcta?

a) NO existe ningún código unívocamente decodificable en este caso.

b) El código tiene eficiencia 1.3591 aproximadamente.

c) Se trata de un codigo de Huffmann

d) Ninguna de las anteriores

18

a) Desigualdad de Kraft $\sum_{i=1}^{F} d^{-l_i} \le 1$ d = # símbolos del código, F = # símbolos fuente

S_i		P_i
S_1	$\longrightarrow$	P_1
$\vdots$		$\vdots$
S_F	$\longrightarrow$	P_F

l_i = longitud de la Palabra código P_i asociada al símbolo fuente S_i.

$$\sum_{i=1}^{6} 4^{-l_i} = 4^{-1} + 4^{-1} + 4^{-2} + 3\cdot 4^{-3} = 0'6093 \le 1$$

Sí que existe algún código instantáneo.

b) $H(F) = 0'3 \log_2 \frac{1}{0'3} + 2\cdot 0'2 \cdot \log_2 \frac{1}{0'2} + 3\cdot 0'1 \cdot \log_2 \frac{1}{0'1} = 2'4464 \ \frac{\text{bits}}{\text{símbolo}}$

$= 0'3 \log_4 \frac{1}{0'3} + 2\cdot 0'2 \cdot \log_4 \frac{1}{0'2} + 3\cdot 0'1 \cdot \log_4 \frac{1}{0'1} = 1'2232 \ \frac{\text{dígitos fuente}}{\text{símbolo}}$

$\bar{L} = 1\cdot 0'3 + 1\cdot 0'2 + 2\cdot 0'2 + 3\cdot 3\cdot 0'1 = 1'8 \ \frac{\text{dígitos fuente}}{\text{símbolo}} \cdot \log_2 4 = 3'6 \ \frac{\text{bits}}{\text{símbolo}}$

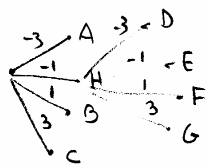
$E = \frac{H}{\bar{L}} = \frac{1'2232}{1'8} = \frac{2'4464}{3'6} = \underline{\underline{0'6795}} \equiv 67'95\%$

c) Sería un Huffman "cuaternario"

A 0'3
B 0'2
C 0'2
$\left.\begin{array}{l} \text{D } 0'1 \\ \text{E } 0'1 \\ \text{F } 0'1 \\ \text{G } 0 \end{array}\right\}$ H 0'3

G 0 → lo necesito para cuadrar.

A 0'3
H 0'3
B 0'2
C 0'2



A -3
B 1
C 3
D -1 -3
E -1 -1
F -1 1
G -1 3

Las longitudes serían {1, 1, 1, 2, 2, 2} ~~2~~ y NO
no se usa

En este caso, $\bar{L} = 1\cdot 0'3 + 1\cdot 0'2 + 1\cdot 0'2 + 0'1\cdot 3\cdot 2 + \underline{\underline{2\cdot 0}} = 1'3 \ \frac{\text{díg. fuente}}{\text{símbolo}}$

$E = \frac{H}{\bar{L}} = \frac{1'2232}{1'3} = 0'9409$ d

19. Un código está formado por todas las palabras de 8 bits que tienen 4 unos y 4 ceros. ¿Qué afirmación es correcta?

a) El tamaño del código es de 12 palabras

b) El código NO es lineal

c) La d_{min} del código es 4

d) Ninguna de las anteriores

19

a) $PR_8^{4,4} = \frac{8!}{4!\,4!} = 70$ palabras

b) No es LINEAL, pues no forma un subespacio vectorial, ya que no contiene al elemento neutro 00000000.

Además, la suma de dos palabras código no es otra palabra código.

$00001111 \oplus 11110000 = 11111111 \notin$ Código

c) d_{min} = menor nº de bits discrepantes entre cada dos palabras código.

No podemos usar que $d_{min} = \underset{\forall \neq 0}{W_{min}}$ pues el código no es lineal.

$d_{min} = 2$

$d\{0000\underline{0}111\underline{1},\ 000\underline{1}111\underline{0}\} = 2$

20. Sean A y B dos usuarios de un sistema de cifrado de bloque donde los mensajes se colocan como estado inicial de un LFSR con polinomio de conexiones $C(D) = D^2 + D + 1$. El criptograma se obtiene como el estado del LFSR al cabo del número de iteraciones que indique la clave de sesión, que es 11. A desea enviar el mensaje M=1011000111 a B codificado. ¿Cuál es el criptograma?

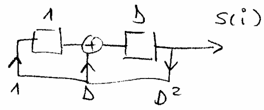
a) 1101011001

b) 0111011001

c) 1101001001

d) Ninguna de las anteriores

20



$K_{sesion} = 11 = 3 \cdot L_{max} + 2$

$L_{max} = 2^m - 1 = 3$, pues C(D) es PRIMITIVO.

1	D
1	0
0	1
1	1
1	0
0	1
1	1
s(i)	

L=3

$p^{K_{sesion}}(D) = p^{11}(D) = p^{(2)}(D)$

Codificar es avanzar DOS estados el LFSR.

M = 10 | 11 | 00 | 01 | 11

C = 11 | 01 | 00 | 10 | 01 → c

estado absorvente

15. Sea un LFSR caracterizado por el polinomio de conexiones completo de grado 23. Puede asegurarse que:

a) Si el estado inicial es D^4 el período es 24

b) El período no depende del estado inicial

c) El período es 8388607

d) Ninguna de las anteriores.

15 C(D) completo grado 23 = m.

a) Para $p^{(0)}(D) = \{1, D, D^2 \ldots, D^{22}, 1 + D + D^2 + \cdots + D^{22}\} \rightarrow L = L_{max} = m + 1$

$L = 24$

b) Sí que depende. No depende solo si C(D) primitivo

c) $2^m - 1 = 2^{23} - 1 = 8388607 = L_{max}$ para C(D) primitivo