# ETSETB
## Curso 2007-08 Primavera
## EXAMEN DE TRANSMISIÓN DE DATOS
## 26 de junio 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 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 el código de ~~Golay~~ **ternario** (11,6) es 2-perfecto ¿cuántos vectores ternarios de 11 componentes se decodifican en la misma palabra código?

   *a*) Depende de la palabra código
   *b*) 67
   *c*) 243
   *d*) Ninguna de las anteriores

2-perfecto ⇒ distancia 5 ⇒ 

Todas las n-plas que distan 0, 1, ó 2 de palabra código, al decodificarse, llegan a la misma palabra código:

$$\binom{11}{0}2^0 + \binom{11}{1}2^1 + \binom{11}{2}2^2 = \underline{\underline{243}}$$

2. Sabiendo que en un sistema RSA el valor de $ed = 22236001$, ¿cuál de los siguientes puede ser un valor válido para $n$?

   a) $n = 1009 * 1103 = 1112927$
   b) $n = 1013 * 1097 = 1111261$
   c) $n = 1019 * 1093 = 1113767$
   d) Ninguno de los anteriores

$e \cdot d = k \cdot \varphi(n) + 1 \Rightarrow \frac{ed - 1}{\varphi(n)}$ . entero

a) $\frac{22236001 - 1}{1008 \cdot 1102}$ = no es entero

b) $\frac{22236000}{1012 \cdot 1098}$ = no es entero

c) $\frac{22236000}{1018 \cdot 1092}$ = no es entero

d) Ninguno de los anteriores

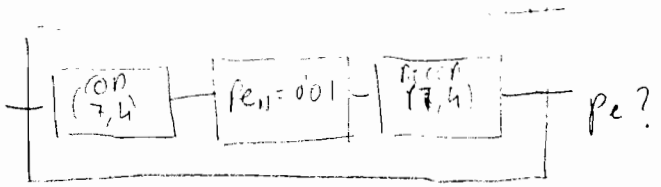
3. A un canal binario simétrico con tasa de error $p_e = 0.01$ se le añade a la entrada un codificador de Hamming (7,1) y a la salida el correspondiente decodificador. ¿Cuál es la capacidad del canal resultante? *NOTA.- Ajuste el resultado final a dos decimales*

   *a*) 0.95 bits/simb

   *b*) 0.96 bits/simb

   *c*) 0.99 bits/simb

   *d*) Ninguna de las anteriores




$$P_{E\,\text{bl}} = \binom{7}{2} p_e^2 (1-p_e)^5 = 0'19971\ 10^{-2}$$

$$P_e = \frac{3}{7} P_E = 0'8559\ 10^{-3}$$

$$C = 1 - \left[p_e \log_2 \frac{1}{p_e} + (1-p_e) \log_2 \left(\frac{1}{1-p_e}\right)\right] = 0'99 \text{ bits/simb}$$

4. Un código cíclico con polinomio generador $g(D) = x^4 + x^3 + 1$ se usa como detector de ráfagas. ¿Cuál de los siguientes errores será detectado? ~~Calcular el valor de d.~~

a) $e(D) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$ $\quad x^6 + x^5 + x^4 + x^3 + x^2 + 1$

b) $e(D) = x^{12} + x^{11} + x^9 + x^5$ $\quad x^{12} + x^{11} + x^9 + x^5$

c) $e(D) = x^{10} + x^8 + x^9 + x^1 + x^3$ $\quad x^{12} + x^{11} + x^8 + x^7 + x^6 + x^3$

(d) Ninguno de los errores anteriores será detectado.

No se detectan aquellos polinomios multiplo de $g(x)$

a) $e(D) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$ | $x^4 + x^3 + 1$

$x^6 + x^5 + x^2$ | $x^2 + 1$

$x^4 + x^3 + 1$

0

No se detecta

b) $e(D) = x^{12} + x^{11} + x^9 + x^5 \Rightarrow e'(D) = x^7 + x^6 + x^4 + 1$ | $x^4 + x^3 + 1$

$x^7 + x^6 + x^3$ | $x^3 + 1$

$x^4 + x^3 + 1$

0 No se detecta

c) $e(D) = x^{12} + x^{11} + x^8 + x^7 + x^6 + x^3 \Rightarrow e'(D) = x^9 + x^8 + x^5 + x^4 + x^3 + 1$ | $x^4 + x^3 + 1$

$x^9 + x^8 + x^3$ | $x^5 + 1$

$x^4 + x^3 + 1$

0 No se detecta

(d)

5. En la matriz G sistemática calculada a partir de $g(D) = D^3 + D + 1$ se ha eliminado la 4 fila y la 4 columna, entonces:

   *a*) $g(D) = D^3 + D^2 + D$ genera el código

   *b*) 010110 es palabra código

   *c*) No existe $g(D)$ que genere el código

   *d*) Ninguna de las anteriores

El recorte es válido (se mantiene la linealidad) pero no es polinómico:

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 1\,0\,1 \\ 0 & 1 & 0 & 1\,1\,1 \\ 0 & 0 & 1 & 1\,1\,0 \\ \hline 0 & 0 & 0 & 1\,1\,1 \end{array}\right) \begin{array}{l} \to D^4+D^2+D+1 = (D+1)(D^3+D^2+1) \\ \to D^3+D^2+D \end{array}$$

la palabra 010110 no es palabra código, la redundancia debería ser 111 → b) falsa

El polinomio de menor grado no divide a la palabra código

$D^4+D^2+D+1 \Rightarrow$ a) falsa

c) cierta

6. El código (512,502) se genera con el polinomio $D^{10} + D^9 + D^5 + D^4 + D + 1$(uno de sus 2 factores es primitivo), ¿cuál es cierta?

   *a*) Detecta todos los errores dobles

   *b*) Detecta todos las ráfagas con 11 bits erróneos

   *c*) Es cíclico

   *d*) Ninguna de las anteriores

$D^{10}+D^9+D^5+D^4+D+1 \quad \lfloor D+1$

☺ $D^9+D^4+1$, primitivo. Detecta todas las ráfagas dobles $< 2^9-1 = 511$

→ la ráfaga $D^{511}+1$ no la detecta ($D^9+D^4+1$ la divide) → a) falsa.

Como es $(D+1)p(D)$ detecta todos los impares → b) cierta

Es un código recortado → c) falsa.

7. Se quiere construir un código con 57 bits de usuario y 7 bits de redundancia, ¿qué polinomio generador encuentras más adecuado?

   a) $D^5 + D^2 + 1$ (primitivo)
   b) $D^6 + D + 1$ (primitivo)
   c) $D^7 + D^3 + 1$ (primitivo)
   d) $D^7 + D^6 + D^2 + 1$

Debe ser de grado 7 por la redundancia

$D^7+D^3+1$ tiene pero 3 por lo que la dmin = 3

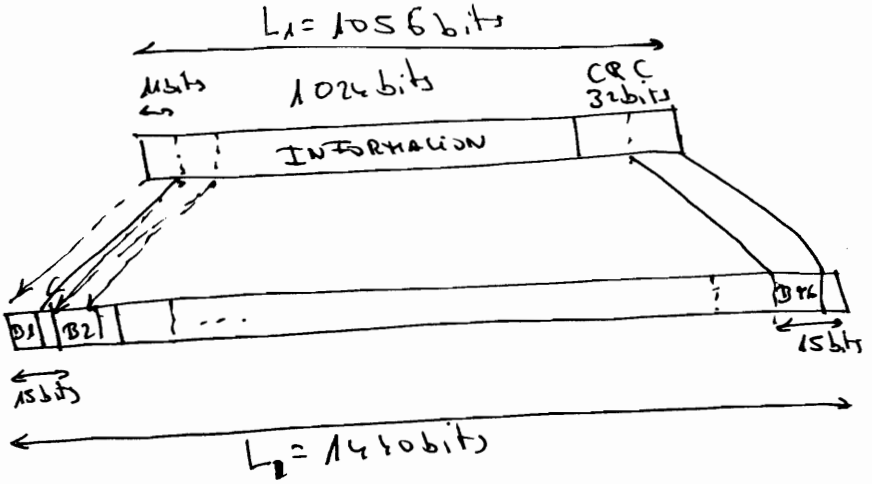
$D^7+D^6+D^2+1 = (D+1)(D^6+D+1) = (D+1)\,p(D)$

$p(D) = D^6+D+1$ genera un código con dmin = 3 y ahora las p. código tienen un número par de "1" $\Rightarrow$ dmin = 4. Notar que este polinomio divide a $D^{2^6-1}+1 = D^{63}+1$ por lo que el resto a 57 bits mantiene las propiedades de distancia

$\Rightarrow$ d) cierta, como mejor generador de la lista.

8. Un sistema de transmisión de datos envía tramas de longitud L = ~~1425~~ 1440 bits sobre un canal sin memoria con probabilidad de error de bit $10^{-6}$. La trama se construye añadiendo a la información de usuario una redundancia para la detección de errores obtenida a través de un código polinómico de grado 32 y, a continuación, se realiza una codificación para la corrección de errores con un código de Hamming Cod(15,11). ¿Cuál es la probabilidad de solicitar la retransmisión de una trama?. Ajuste el resultado final a una sola cifra significativa

*a*) $10^{-6}$
*b*) $10^{-4}$
(c) $10^{-8}$
*d*) $10^{-10}$




$L_1$ = 1024 bits información + 32 bits CRC = 1056 bits

$L = \frac{1056 \text{ bits}}{11 \text{ bits/bloque}} \cdot 15 = 96 \text{ bloques} \cdot 15 \frac{\text{bits}}{\text{bloque}} = 1440 \text{ bits}.$

$N \triangleq$ nº de bloques = 96

$n \triangleq$ nº bits por bloque = 15.

$P_{\text{error bloque}} \triangleq P_B \simeq \binom{n}{2} \cdot p^2 (1-p)^{n-2} = 1'05 \cdot 10^{-10}$

$P_{\text{error en } L_1} = \text{Prob}\left[ 1 \text{ o más bloque erróneos} \right] \simeq \binom{N}{1} \cdot P_B (1-P_B)^{N-1}$

$P_{\text{error en } L_1} = 1'008 \cdot 10^{-8}$.

Cualquier ráfaga de longitud inferior a 32 bits es detectada por el CRC. Por lo tanto, siempre que 1 bloque es erróneo se detecta.

$P_{\text{retransmisión}} = P_{\text{error en } L_1} \cdot \text{Prob}[\text{detección de ráfaga}]$

$= 1'008 \cdot 10^{-8} \cdot 1 = 1 \cdot 10^{-8}$

9. Para un código lineal binario, si dos palabras distintas recibidas, $z_1$ y $z_2$, tienen el mismo síndrome, podemos afirmar que:

*a*) $z_1$ es ortogonal a $z_2$

*b*) el código no puede ser utilizado como corrector de errores

*c*) la distancia de Hamming entre $z_1$ y $z_2$ es como mínimo la distancia mínima del código

*d*) ninguna de las anteriores

$z_1 \neq z_2$ , $z_1, z_2 \in \{ z \in Z_2^n \,/\, z \cdot H^T = S_i \}$

a) No necesariamente

b) No necesariamente

c) $H^T z_1 = S_1$
$H^T z_2 = S_1$
$\Rightarrow$ $H^T (z_1 - z_2) = \emptyset \Rightarrow z_1 = z_2 + y$
con $y \in Cod. - \{0$
Luego $dis(z_1, z_2) \leq d_{min}$

d) c) es cierto.

10. Un cifrado de sustitución obtiene los criptogramas $c$ a partir de los mensajes $m$ realizando la operación: $c = (am + b) mod n$. Una elección de valores $a, b$ y $n$ correcta sería:

*a*) $a = 22, b = 3, n = 561$

*b*) $a = 2, b = 17, n = 561$

*c*) $a = 12, b = 3, n = 561$

*d*) ninguna de las anteriores

$$c = (am + b) \bmod n$$

Para que la codificación sea única dos mensajes $m_1$ y $m_2$ distintos tienen que tener dos criptogramas distintos $C_1$ y $C_2$. ~~Estos~~ Esto no ocurre si:

$$m_1 \neq m_2 \qquad C_1 = C_2 = C$$

$$C = (a m_1 + b) \bmod n$$

$$- \quad C = (a m_2 + b) \bmod n$$

$$0 = a(m_1 - m_2) \bmod n \Rightarrow a(m_1 - m_2) = kn$$

Si: m.c.d $(a, n) \neq 1$ entonces $m_1$ y $m_2$ pueden ser distintos

Condición: m.c.d $(a, n) = 1$ y $b$ cualquiera.

a) m.c.d $(27, 561) = 11$

b) m.c.d $(2, 561) = 1$

c) m.c.d $(12, 561) = 3$

d) b) es cierta

11. Un cifrado de sustitución monoalfabético, para una fuente de 10 símbolos, puede tener un número de claves distintas:

(a) superior a $3\ 10^6$

*b*) inferior a 22

*c*) igual a 10

*d*) ninguna de las anteriores

nº claves distintas = nº permutaciones del alfabeto. $= 10! > 3 \cdot 10^6$

⇓

a)

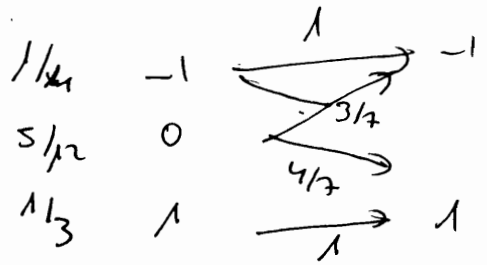
12. Una fuente ternaria emite símbolos del alfabeto {-1, 0, 1} con probabilidades 1/4, 5/12 y 1/3, respectivamente, sobre un canal cuya matriz estocástica de probabilidades de transición es: [ 1 0 , 3/7 4/7, 0 1]. Denominando la salida del canal Y, ¿ cuál de las siguientes afirmaciones es falsa?

*a*) H(Y)=H(3/7)

*b*) La fuente X emplea toda la capacidad del canal

*c*) H(Y/X)=5/12 H(Y)

*d*) Alguna de las anteriores es falsa




a) $P[Y=-1] = \frac{1}{4} + \frac{5}{12}\cdot\frac{3}{7} = \frac{3}{7}$

$P[Y=1] = 1 - P[Y=-1] = \frac{4}{7}$

$H(Y) = H(3/7) = H(4/7)$

b) $H(Y/X) = \sum_i P(X=i) \cdot \sum_j P(Y=j/X=i) \log_2 \frac{1}{P(Y=j/X=i)}$

$H(Y/X) = \frac{5}{12} H(Y/X=0) = \frac{5}{12}\cdot H(3/7)$

S/b depende del cond.

b)

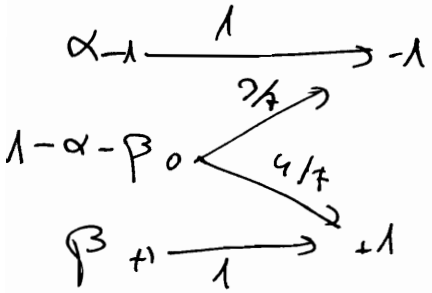
$C = \max_{p(\alpha)} I(X;Y) = \max_{p(\alpha)} H(Y) - H(Y/X)$

Ctte.

Debemos buscar la distribución de probabilidades para que

$P(Y=1) = P(Y=-1) \Rightarrow$

$\alpha + (1-\alpha-\beta)\frac{3}{7} = \beta + (1-\alpha-\beta)\frac{4}{7}$




Se debe cumplir $\alpha = \frac{1+6\beta}{8}$

En esta fuente:

$\frac{1+6\beta}{8} = \frac{1+6\cdot 1/3}{8} = \frac{3}{8} \neq \frac{1}{4} = \alpha$

Falsa

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

14. ¿Cuál de los siguientes polinomios es primitivo?

a) $D^{16} + D^{12} + D^{10} + D^8 + D^2 + 1$

b) $D^{16} + D^{15} + D^{12} + D^{11} + D$ ← Bien

c) $D^{16} + D^{12} + D^5 + 1$

d) $D^{15} + D^{14} + D^{13} + D^{12} + D^4 + D^3 + D^2 + D + 1$

a) No, por potencias pares y nº par de términos

b) No, tiene término independiente

c) No, nº par de términos

d) Es primitivo, utilizado en HDLC

%respuesta 3

\item %pregunta 6.

Una fuente ternaria sin memoria, F, tiene unas probabilidades de transición de símbolos: p_A = 3/8, p_B = 7/24 y p_C = 1/3. Si se realiza una extensión de la fuente, F^2, concatenando dos símbolos de F, es falso que (ajuste con 3 decimales)

\alt

\item La entropía de la fuente extendida es menor que la de una fuente con nueve símbolos equiprobables

\item La entropía de la fuente extendida es 3.155 bits/simb_F^2

\item La longitud media de la codificación de ~~Hamming~~ de la fuente extendida mayor que 4 dig/simb_F^2

\item Alguna de las anteriores es falsa

\ealt

a) Cierto.
La fuente extendida tiene por alfabeto $\{AA, AB, AC, BA, BB, BC, CA, CB, CC\}$

y estos símbolos no son equiprobables. $\Rightarrow H(F^2) < \log_2 9 = 3'1$

b) $H(F^2) = 2 \cdot H(F) = -2 \cdot \left[ \frac{3}{8} \log_2 \frac{3}{8} + \frac{7}{24} \log_2 \frac{7}{24} + \frac{1}{3} \log_2 \frac{1}{3} \right]$

$H(F^2) = 3'1548 \approx 3'155$. Cierto.

c) Falso, la longitud media de la codificación de H estará próxima a $H(F^2)$ porque los símbolos no presentan mucha dispersión en sus probabilidades. Y, por lo tanto, no superará el valor de 4 dig/simb$_{F^2}$

15. Si p y q son números primos diferentes a 1, entonces la expresión $p^{(q-1)} + q^{(p-1)} mod pq$ es:

*a*) 1

*b*) La solución es un número entero y depende de los valores de p y q

*c*) No puede garantizarse que la solución sea un número entero

*d*) Ninguna de las anteriores

$p^{q-1} + q^{p-1} \equiv_{pq} m \rightarrow m \equiv_p 1 \rightarrow mqq^{-1} = k_1 pqq^{-1} + qq^{-1}$

$pq$ primos $\rightarrow m \equiv_q 1 \rightarrow + \; mpp^{-1} = k_2 qpp^{-1} + pp^{-1}$

$m \cdot 1 = k_3 \cdot pq + 1$

$\rightarrow m \equiv_{pq} 1$ a) cierta.

16. Un cifrado RSA con parámetros $(e, n)$ se ha multiplicado por $e$ y se ha reducido $mod n$ para obtener $c$. En el caso particular de $e = 907$ y $n = 37 \cdot 127$ se puede asegurar:

   a) $m = 4694c^{4531} mod n$

   b) $m = (3295c)^{(-5)} mod n$

   c) Que existen 2 mensajes con el mismo criptograma

   d) Ninguna de las anteriores

$c = (e(m^e \bmod n)) \bmod n = e m^e \bmod n$

$m = (d_2 c)^{d_1} \bmod n$ con $d_1$ la inversa de $e$ mod $\varphi(n)$

$d_2$ " " " " mod $n$ .

$\varphi(n) = 36 \cdot 126 = 4536$

| | | | | |
|---|---|---|---|---|
| $e=907$ | 5 | 1 | $-5 = d_1 \equiv_{\varphi(m)}$ | 4531 |
| 907 | 1 | 907 | 0 | 1 $\equiv_n$ 4694 |

a) falsa

$n = 37 \cdot 127 = 4699$

| | | | | |
|---|---|---|---|---|
| $e=907$ | 5 | 271 | $-1404 = d_2 \equiv_n$ | 3295 |
| 907 | 164 | 5 | -49 | 271 |
| 164 | 87 | 1 | 26 | -49 |
| 87 | 77 | 1 | -23 | 26 |
| 77 | 10 | 7 | 3 | -23 |
| 10 | 7 | 1 | -2 | 3 |
| 7 | 3 | 2 | 1 | -2 |
| 3 | 1 | 3 | 0 | 1 |

$\rightarrow mcd(e, n) = 1$ → c) falsa .

→ $m = (3295c)^{-5} \bmod n$ , b) cierta .

17. Una fuente de bits X se modela con el lanzamiento alternado de 2 dados de 6 caras cada uno. Uno de los dados tiene en una de sus caras el 00, en 2 el 01 y en 3 el 10. El otro dado tiene el 01 en 2 de sus caras así como el 10 y el 11, ¿cuál es la H(X) en bits por símbolo?

   a) $H(X) < 0{,}8$
   b) $0{,}8 \leq H(X) < 1{,}5$
   c) $1{,}5 \leq H(X) < 3$
   d) $3 \leq H(X)$

| Dado 1: | | Pi |
|---|---|---|
| | 00 | 1/6 |
| | 01 | 2/6 |
| | 01 | |
| | 10 | 3/6 |
| | 10 | |
| | 10 | |

| Dado 2: | | Pi |
|---|---|---|
| | 01 | 2/6 |
| | 01 | |
| | 10 | 2/6 |
| | 10 | |
| | 11 | 2/6 |
| | 11 | |

| Dado 1: | | PROB. |
|---|---|---|
| | 00 | 1/6 |
| | 01 | 2/6 |
| | 01 | |
| | 10 | 3/6 |
| | 10 | |
| | 10 | |

| Dado 2: | | PROB. |
|---|---|---|
| | 01 | 2/6 |
| | 01 | |
| | 10 | 2/6 |
| | 10 | |
| | 11 | 2/6 |
| | 11 | |

Sea $\mathcal{X}_1$ la fuente de bits del dado 1 y $\mathcal{X}_2$ la del dado 2

$H(X_1) = H(1/6, 2/6, 3/6)/2 = \frac{1.459148}{2} = 0.729574$ bpm

$H(X_2) = H(1/3, 1/3, 1/3)/2 = \log_2 3/2 = 0.792481$ bpm

$H(X) = 1/2\,(H(X_1) + H(X_2)) = 0.761027$ bpm → a) cierta

18. Un código (9,4) tiene la siguiente matriz de comprobación, indica la cierta:

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

*a*) Corrige 1 error y además detecta 2 adicionales

*b*) Corrige 4 borrones

*c*) Corrige 2 errores y además detecta 1 adicional

*d*) Ninguna de las anteriores

En H no hay 2 columnas iguales $\Rightarrow d_{min} > 2$

Sumar cualquier par de columnas de H da como resultado una columna con al menos dos "1" y no existe ninguna columna con dos "1" que las cancele $\Rightarrow d_{min} \geq 4$. Pero sí existen dos columnas, cada una con un "1", que las cancela $\Rightarrow d_{min} = 4$

a) $2 \cdot 1 + 2 = 4 \leq d_{min}$, CIERTA

b,c) ciertas si $d_{min} \geq 5$ → FALSAS.

19. Un código de Hamming (n,k) se extiende con un bit de paridad impar, puede asegurarse que:

*a*) El código es no lineal

*b*) El código es cíclico

*c*) La dmin se incrementa en 1

*d*) Ninguna de las anteriores

Para ser lineal la palabra todo "0" debe ser palabra código.
Si se añade un bit de paridad impar no puede serlo!
⇒ a) cierta, el código es no lineal
Obviamente no puede ser cíclico ⇒ b) falsa
Si la dmin es impar añadir el bit no la cambiará ⇒ c) falsa

20. 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 código de Huffmann

    *d*) Ninguna de las anteriores