10 F
7 N
3 D

ETSETB
Curso 2005-06 Primavera
EXAMEN DE TRANSMISIÓN DE DATOS
12 de enero de 2007

PUBLICACIÓN DE NOTAS PROVISIONALES: 19/01/2007
FECHA LÍMITE PARA LAS ALEGACIONES: 24/01/2007
PUBLICACIÓN DE NOTAS DEFINITIVAS: 27/01/2007
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

N

1. Un cifrador en flujo síncrono consta de un LFSR y una función de salida. La secuencia generada tiene un periodo de 2047 bits. Se puede afirmar que:

   a) El número de celdas del LFSR es < 11
   b) La función de salida es no lineal
   [✓ *c*)] El número de celdas del LFSR puede ser > 11
   d) Ninguna de las anteriores

La longitud del periodo de la salida será la del LFSR o un divisor.

$2047 = 2^{11} - 1$

Posibilidades: → LFSR primitivo de 11 celdas
→ LFSR primitivo de 22 celdas

$$L = 2^{22} - 1 = \underbrace{(2^{11}-1)}\cdot(2^{11}+1)$$

↳ esto hace que 2047 sea divisor de L.

→ ...

F

binario ✓

3. Se dispone de un código (6,3). Indíquese la respuesta correcta

   a) La capacidad correctora siempre es 1 $\qquad\qquad r = n - k = 3$

   b) La capacidad detectora siempre es 2

   [✓ c)] Nunca puede ser un código 1-perfecto

   d) Ninguna de las anteriores $\tilde{e}$

c) Cierto. Debería cumplir $\underset{\underset{2^3=8}{\|}}{2^r} = 1 + \underset{\underset{6}{\|}}{n} = 7$!

El de Hamming es el código (7,4), que recortado da un código (6,3) con $e=1$ pero no es 1-perfecto.

a) A veces puede corregir más, pues no es perfecto! $e=1$.

N

2. Un cifrador en flujo autosincronizante consta de un LFSR y una función de salida. Cuando se han obtenido 2047 bits, no se ha encontrado ningún periodo. Se puede afirmar que:

   a) La longitud del registro de desplazamiento es inferior a 11

   b) La función de salida es no lineal

   c) La longitud del registro de desplazamiento debe ser superior a 11

   [✓ d)] Ninguna de las anteriores

Autosincronizante: La salida no tiene porqué ser periódico independientemente de la longitud del LFSR

F

5. Sea un código polinómico caracterizado por $g(D) = D^7 + D^6 + D^5 + D^4 + D^3 + D^2 + D + 1$. Se puede garantizar que detecta:

   a) Todas las ráfagas de error de longitud menor o igual a 8

   b) Cualquier error doble donde las posiciones de los errores está a distancia menor o igual a 9

   [✓ c)] Cualquier error triple.

   d) Ninguna de las anteriores

$$g(D) = \overset{r=7}{D^7} + D^6 + D^5 + D^4 + D^3 + D^2 + D + 1 = (D+1)\cdot(D^6 + D^4 + D^2 + 1) =$$

$$= (D+1)\cdot(\underbrace{D^3 + D^2 + D + 1}_{\text{no es primitivo}})^2 \equiv (D+1)\cdot\underbrace{\gamma(D)}_{\text{primitivo}}$$

a) $\underset{\overset{\shortparallel}{j-i+1}}{\text{long. ráfaga}} < r+1 = 8 \rightarrow$ Se detectan todas si $\gamma(D)$ primitivo.

b) error doble, $j-i < L = 2^m - 1$ con m grado de $\gamma(D)$ primitivo

ⓒ Un error triple es un error impar.

Se detectan todos los errores $e(D)$ que no sean múltiplos de $g(D)$

- Un $e(D)$ error impar cumple $e(D=1) = 1$. $\Rightarrow$ $e(D)$ no tiene a $D+1$ como factor!
- Este $g(D)$ cumple $g(D=1) = 0$, pues tiene a $(D+1)$ como factor.

F

6. El número de códigos binarios de Hamming sistemáticos distintos para r=7 vale:

   a) 7!
   b) 127!
   [✓ c) 120!]
   d) Ninguna de las anteriores

② Código binario de Hamming: $2^r = 1 + n$

$r = 7 \to n = 2^7 - 1 = 127 \Rightarrow k = n - r = 120$. Código$(\overset{\overset{n}{\shortparallel}}{127}, \overset{\overset{k}{\shortparallel}}{120})$

Sistemático ⇒

$$H^T_{\underset{127}{\overset{\shortparallel}{n}} \times \underset{7}{\overset{\shortparallel}{r}}} = \begin{pmatrix} -P \\ \hdashline I_r \end{pmatrix} = \left(\begin{array}{c} \\ \\ \\ \hdashline 1000000 \\ 01 - - - 0 \\ \vdots \\ 00 - - - 1 \end{array} \right) \begin{array}{l} \updownarrow 120 \\ \\ \updownarrow 7 \end{array}$$

$$\xleftrightarrow{\quad 7 \quad}$$

- Con 7 componentes hay $2^7 - 1 = 127$ vectores a colocar en las 127 filas de H^T
- Todas las filas de H^T deben ser diferentes
- Hay 7 vectores ya cogidos en I_7
- $127 - 7 = 120$ vectores libres en 120 filas ⇒ 120!

ⓒ

D

7. Sea M el mensaje en claro (m bits), C el criptograma (n bits) y k la clave de cifrado (r bits). Es FALSO que:

   a) H(M/C) ≤ m
   b) H(M/C) ≤ n
   c) H(M/C) ≤ r ✓
   [✓ d)] Alguna de las anteriores es falsa

c) $H(M \backslash C) \leq H(\overset{\nearrow \text{clave}}{K})$

a) $H(M) \underset{\Downarrow}{\leq} 2^m \cdot \frac{1}{2^m} \cdot \log_2 \frac{1}{1/2^m} = \log_2 2^m = m$ bits

M equiprobables → hay 2^m Ms → prob = $\frac{1}{2^m}$

M de m bits

$H(K) \leq r$ bits

c) $H(K) \leq r$ bits $\Rightarrow \#K \leq 2^r \Rightarrow \#M \backslash C \leq 2^r$

b) $M \longleftrightarrow C$ $\quad \#C \leq 2^n \Rightarrow \#M \leq 2^n \Rightarrow H(M) \leq n$

$H(C) \leq n \Rightarrow H(M) \leq n$

N

4. Dos usuarios intercambian mensajes firmados, utilizando RSA con claves de 1024 bits cada una y una función de hash de longitud 64 bits. Indíquese la respuesta correcta

   [✓ a)] La probabilidad de falsificar la firma es $\geq \frac{1}{\underset{2}{3^{64}}}$
   b) La probabilidad de falsificar la firma pertenece al intervalo $\left[\frac{1}{2^{1024}}, \frac{2^{64}}{2^{1024}}\right]$
   c) a probabilidad de falsificar la firma depende del nivel de confidencialidad requerido
   d) Ninguna de las anteriores

$\underbrace{e \| N}_{M} \| \underbrace{FD(M)}_{H(M)^d \bmod N}$

H(M) de 64 bits, hay 2^{64} H(M) ≠.

Dadas las propiedades de H(M) la prob. de dar con la H(M) acertada es $1/2^{64}$, para una f$^{\underline{\text{ón}}}$ de Hash totalmente perfecta. Para otras, será mayor.

D

10. Una fuente emite el símbolo S con una probabilidad igual a 0.0347. Con referencia a la codificación de fuente indica la correcta:

a) Se puede asegurar que la fuente tiene memoria

[✓ *b*)] La secuencia binaria 000000000000001 es una posible codificación aritmética para la secuencia extendida SSS de la fuente

c) Si la fuente emite también el símbolo T con probabilidad 0.0347, entonces la codificación binaria de S según Huffman deberá tener la misma longitud que la de T

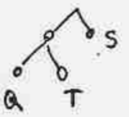
d) Ninguna de las anteriores

a) No se sabe → falsa.

b) $\underbrace{0..1}_{15 \text{ bits}} \equiv 2^{-15} = 0.000030517$ y $P_S^3 = 0.000041781$ → cierta.

c) Por ejemplo: $P_T = P_S = 0.0347$

$P_Q = 0.01$
(< 0.0347)



→ falsa.

F

8. Sea $c(D) = D^6 + D + 1$ un polinomio primitivo de grado 6. Calcule $D^195 modc(D)$

D^{195}

a) 1

b) D^2

[✓ *c*)] $D + 1$

d) Ninguna de las anteriores

19| 23 Junio 2005

$L = 2^6 - 1 = 63$;; $195 = 3 \cdot 63 + 6$

$D^{195} \bmod C(D) = D^6 \bmod C(D) = D + 1$

N

11. La variable aleatoria de una fuente Y es Y = $\underset{X^2}{\boxed{X2}}$+3 donde X es la variable aleatoria de otra fuente X con entropía no nula. Puede decirse que:

   a) $H(X,Y) > H(X)$
   b) $H(X) < H(Y)$
   c) $I(X;Y) = 0$
   [✓ d)] Ninguna de las anteriores

$Y = f(X)$; $H(Y|X) = 0$

$$\left.\begin{array}{l} H(X;Y) = H(X) + H(Y|X) = H(X), \text{ a) falsa} \\ \quad = H(Y) + H(X|Y) \geq H(Y), \text{ b) falsa} \\ I(X;Y) = H(Y) - H(Y|X) = H(Y) \neq 0, \text{ c) falsa} \end{array}\right\} \rightarrow \text{d) cierta.}$$

F

9. En un sistema RSA todos los valores de n contienen siempre un mismo factor $\overset{\overset{59}{\shortparallel}}{\text{primo}}$. En dicho sistema, indique qué valor de n no es apropiado si $e = 11$

   a) 413 = 59 · 7
   b) 649 = 59 · 11
   c) 1003 = 59 · 17
   [✓ d)] 1357 = 59 · 23

Euclides $\mathrm{mcd}(\underset{59\cdot 7}{\underset{\shortparallel}{413}}, \underset{59\cdot 11}{\underset{\shortparallel}{649}}) = 59$ → Me ayuda a factorizar los n.

$\phi(413) = 58 \cdot 6 = 348 = 29 \cdot 3 \cdot 2^2$

$\phi(649) = 58 \cdot 10 = 580 = 29 \cdot 5 \cdot 2^2$

$\phi(1003) = 58 \cdot 16 = 928 = 29 \cdot 2^5$

$d(1357) = 58 \cdot 22 = 1276 = 29\,\boxed{11}\,2^2 \Rightarrow$ este $n = 1357$ no es válido.

e válido debe ser coprimo con $\phi(n)$.

D

12. Un LFSR tiene un polinomio de conexiones $c(D)$ de grado r con término independiente. Indica la FALSA:

- *a)* Para algún estado inicial $S_0(D)$ genera una secuencia con un periodo mayor o igual a r
- *b)* Si $S_0(D) = 1$ y $D^r modc(D) = 1$ la secuencia tiene un periodo igual a r
- [✓ *c)*] Si genera una secuencia con un periodo igual a 31 entonces c(D) divide a $D^{342} + 1$
- *d)* Alguna de las anteriores es falsa

a) y b) ciertas :

$$\left.\begin{array}{l} S_0(D) = 1 \bmod c(D) = 1 \\ S_1(D) = D \bmod c(D) = D \\ \quad\vdots \\ S_{r-1}(D) = D^{r-1} \bmod c(D) = D^{r-1} \end{array}\right\} \text{puesto que D no es factor de } c(D).$$

Si $S_r(D) = D^r \bmod c(D)$ repite algún estado $\rightarrow T = r$, en otro caso $T > r$

c) falsa :

Si $c(D) \mid (D^{31}+1) \rightarrow c(D) \mid (D^{K31}+1)$ y $342 \bmod 31 \neq 0$.

F

16. Sea el canal binario discreto representado en la Figura 1. ¿Qué afirmación es correcta?

- *a)* Es un canal simétrico respecto de la entrada
- *b)* Es un canal determinista
- [✓ *c)*] La capacidad de canal es 1 bit/símbolo
- *d)* Ninguna de las anteriores

$$P(D|F) = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ 0 & 1/4 & 1/2 & 1/4 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array}$$

a) No es simétrico respecto entrada.

b) Vemos que: conocida la salida, la entrada queda determinada:

$H(F|D) = 0$, es un canal SIN PÉRDIDA .

c) Por ello, $C = \max\limits_{\substack{P\{A_i\} \\ F}} \left[H(F) - \underbrace{\cancel{H(F|D)}}_{0}\right] = \max\limits_{P\{A_i\}} H(F) = 2 \cdot \frac{1}{2} \cdot \log_2 2$

$\downarrow$ $P\{A_i\} = \frac{1}{2}$ F equiprobable

$C = 1$ bit/símbolo $\rightarrow$ c)

P

13. Un código ternario utiliza las longitudes ($l_1 = 3, l_2 = 2, l_3 = 3, l_4 = 3, l_5 = 3, l_6 = 3$) para unos símbolos con probabilidades de ocurrencia ($p_1 = 1/4, p_2 = 1/6, p_3 = 1/12, p_4 = 1/6, p_5 = 1/4, p_6 = 1/12$) respectivamente. Sin extender la fuente, puede decirse que:

   a) La longitud media es inferior a H+1
   b) Cumple la desigualdad de Kraft, por lo que es instantáneo
   c) No existe otro código con longitud media menor
   [✓ d)] Ninguna de las anteriores

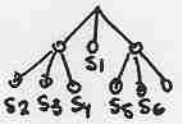
$\bar{L} = 2/6 + 3 \cdot 5/6 = 2.833$ dígitos ternarios/símbolo

$H+1 = -\sum_{\forall i} p_i \log_3 p_i + 1 = \dots = 1.551 + 1 = 2.55$ dígitos ternarios/símbolo

→ a) falsa

b) Que el código cumpla la desigualdad de Kraft no garantiza que éste sea instantáneo.

c) Por inspección en el árbol



→ $\bar{L} = 2\frac{3}{4} + 1\frac{1}{4} = 1.75$ dígitos ternarios/símbolo

---

F

18. Sea un código (n, k) codificador de canal 2-perfecto de alfabeto ternario. ¿Cuántos vectores de error corregibles hay? *Nota: el vector nulo no lo considere*

   [✓ a)] Hay 3(n-k)-1 → 3^{n-k}
   b) Hay 2*n-1 errores corregibles
   c) Hay n2 errores corregibles → n^2
   d) Ninguna de las anteriores

$q = 3$;; 2-perfecto ⇒ $\underbrace{q^r = \binom{n}{0}} + \binom{n}{1} \cdot (q-1) + \binom{n}{2} \cdot (q-1)^2 + \dots + \binom{n}{e} \cdot (q-1)^e$

Sin incluir al error nulo, hay $q^r - \binom{n}{0} = q^r - 1$ errores $\vec{e}$ corregibles. ⇒ $3^{n-k} - 1$ ⓐ

N

14. Sea un sistema RSA y dos usuarios A y B con la misma N=4141, y con $e_A = 7$ y $e_B = 11$. Los usuarios A y B se intercambian un saludo de inicio idéntico M con criptogramas $C_{A\to B} = 3384$ y $C_{B\to a} = 3625$. Indique qué afirmación es correcta. Nota: (3384*1012) mod 4141=1 mod 4141.

   a) El mensaje que se intercambian A y B es M=11.
   b) El mensaje que se intercambian A y B es M=5.
   [✓ c)] El mensaje que se intercambian A y B es M=7.
   d) Ninguna de las anteriores

Ataque por módulo común.

$$C_{AB} = M^{e_B} \bmod N = 3384$$

$$C_{BA} = M^{e_B} \bmod N = 3625$$

Si $\text{mcd}(\underset{7}{\overset{\shortparallel}{e_A}}, \underset{11}{\overset{\shortparallel}{e_B}}) = 1$, como es el caso, $\exists\, r,s \mid \underset{8}{\underset{\downarrow}{r}} \cdot \underset{7}{\underset{\shortparallel}{e_A}} + \underset{-5}{\underset{\downarrow}{s}} \cdot \underset{11}{\underset{\shortparallel}{e_B}} = 1$

$$C_{AB}^{s} \cdot C_{BA}^{r} \bmod N = M^{e_B s + e_A \cdot r} \bmod N = M \bmod N$$

$$M = (3384^{-5} \cdot 3625^{8}) \bmod 4141 = ((3384^{-1})^{5} \cdot 3625^{8}) \bmod 4141$$

$$3384^{-1} \cdot 3384 = 1 + K \cdot N \Rightarrow \exists\ 3384^{-1} \bmod N$$

$\text{mcd}(3384, 4141) = 1$, Alg. Euclides

4141 ⌊3384
757 1

757 ⌊356
45 2

45 ⌊41
4 1

4 ⌊1
0 4

3384 ⌊757
356 4

356 ⌊45
41

41 ⌊4
① 10
↓
mcd

$$\boxed{3384^{-1}} = \frac{1 + k\cdot 4141}{3384} = \frac{1 + K\cdot(1\cdot 3384 + 757)}{3384} =$$

$$= k + \underbrace{\frac{757k+1}{3384}}_{k_1} \underset{k=827}{\overset{\uparrow}{=}} \boxed{1012}$$

$$k = \frac{3384k_1 - 1}{757} = \frac{k_1\cdot(4\cdot 757 + 356) - 1}{757} = 4k_1 + \underbrace{\frac{356\cdot k_1 - 1}{757}}_{k_2} \underset{k_1=185}{\overset{\uparrow}{=}} 827$$

$$k_1 = \frac{757k_2 + 1}{356} = \frac{(2\cdot 356 + 45)k_2 + 1}{356} = 2k_2 + \underbrace{\frac{45k_2 + 1}{356}}_{k_3} \underset{k_2=87}{\overset{\uparrow}{=}} 185$$

$$k_2 = \frac{356k_3 - 1}{45} = \frac{(7\cdot 45 + 41)k_3 - 1}{45} = 7k_3 + \underbrace{\frac{41\cdot k_3 - 1}{45}}_{k_4} \underset{k_3=11}{\overset{\uparrow}{=}} 87$$

$$k_3 = \frac{45k_4 + 1}{41} = \frac{(41\cdot 1 + 4)k_4 + 1}{41} = k_4 + \frac{4k_4 + 1}{41} \underset{k_4=10}{\overset{\downarrow}{=}} 11$$

→ Ver Nota: $(3384 \cdot \underbrace{1012}_{3384^{-1} \bmod 4141}) \bmod 4141 = 1 \bmod 4141$

$$\boxed{M = (1012)^{5} \cdot 3625^{8} \bmod 4141 = (3365 \cdot 16) \bmod 4141 = 7}$$

N

15. Sea F_1 el resultado de lanzar una moneda. Sea F_2 el resultado de lanzar un dado. Sea F otra fuente que si F_1 es cruz, emite el resultado de F_2; y si F_1 es cara, emite el resultado de (F_2 módulo 4). Qué afirmación es correcta:

- *a)* $I(F;F_1) < 0{,}3$
- [✓ *b)*] $0{,}3 \le I(F;F_1) < 0{,}5$
- *c)* $0{,}5 \le I(F;F_1) < 0{,}8$
- *d)* $0{,}8 \le I(F;F_1)$

$$\left.\begin{array}{l} F_1 = \{C, X\} \\ F_2 = \{1,2,3,4,5,6\} \end{array}\right\} \quad \begin{array}{l} F_1 = X \Rightarrow F = F_2 \\ F_1 = C \Rightarrow F = F_2 \bmod 4 \end{array}$$

F_1	F_2	F
C	1	$1 \to 2/6$
	2	$2 \to 2/6$
	3	$3 \to 1/6$
	4	$0 \to 1/6$
	5	1
	6	2
X	1	$1 \to 1/6$
	2	$2 \to 1/6$
	3	$3 \to 1/6$
	4	$4 \to 1/6$
	5	$5 \to 1/6$
	6	$6 \to 1/6$

≡

F		P(F)
0	⟶	1/12
1	⟶	3/12
2	⟶	3/12
3	⟶	2/12
4	⟶	1/12
5	⟶	1/12
6	⟶	1/12

$$H(F) = 4 \cdot \frac{1}{12} \cdot \log_2 12 +$$

$$+ 2 \cdot \frac{3}{12} \cdot \log_2 \frac{12}{3} + \frac{2}{12} \cdot \log_2 \frac{12}{2} =$$

$$= \frac{1}{3} \log_2 (6 \cdot 2) + \frac{1}{2} \log_2 2^2 +$$

$$+ \frac{1}{6} \cdot \log_2 6 =$$

$$= \left(\frac{1}{3} + \frac{1}{6}\right) \log_2 6 + \frac{1}{3} + 1 =$$

$$= \frac{1}{2} \log_2 6 + \frac{4}{3} = 2'6258 \frac{\text{bits}}{\text{símbol}}$$

$$I(F;F_1) = H(F) - H(F \backslash F_1)$$

$$H(F \backslash F_1) = \underset{1/2}{P(F_1 = C)} \cdot \underset{\downarrow}{H(F \backslash F_1 = C)} + \underset{1/2}{P(F_1 = X)} \cdot \underset{\downarrow}{H(F \backslash F_1 = X)} = 2'2516 \frac{\text{bits}}{\text{símbol}}$$

$$2 \cdot \frac{1}{6} \log_2 6 + 2 \cdot \frac{2}{6} \cdot \log_2 \frac{6}{2} = 1'9183 \qquad 6 \cdot \frac{1}{6} \cdot \log_2 6 = 2'5849$$

$$\boxed{I(F;F_1)} = \frac{1}{2} \cdot \log_2 6 + \frac{4}{3} - \frac{1}{2} \cdot \left(\frac{1}{3} \log_2 6 + \frac{2}{3} \log_2 3\right) - \frac{1}{2} \cdot \log_2 6 =$$

$$= \frac{4}{3} - \frac{1}{6} \cdot \log_2 6 - \frac{1}{3} \log_2 3 = \boxed{0'3742 \text{ bits/seg}} \to \text{b)}$$

F

16. Sea el canal binario discreto representado en la Figura 1. ¿Qué afirmación es correcta?

- *a*) Es un canal simétrico respecto de la entrada
- *b*) Es un canal determinista
- [✓ c)] La capacidad de canal es 1 bit/símbolo
- *d*) Ninguna de las anteriores

$$P(D\backslash F) = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ 0 & 1/4 & 1/2 & 1/4 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array}$$

a) No es simétrico respecto entrada.

b) Vemos que: conocida la salida, la entrada queda determinada:

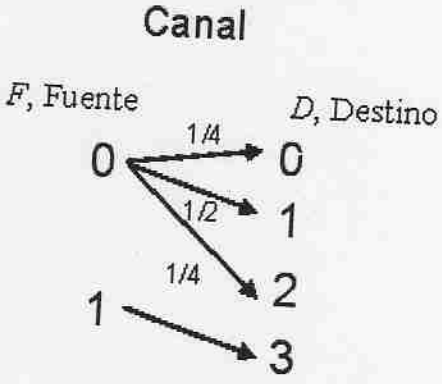
$H(F\backslash D) = 0$, es un canal SIN PÉRDIDA.

c) Por ello, $C' = \max_{\substack{p\{A_i\} \\ F}} [H(F) - \underbrace{H(F\backslash D)}_{0}] = \max_{p\{A_i\}} H(F) = 2 \cdot \frac{1}{2} \cdot \log_2 2$

$\downarrow$ $p\{A_i\} = \frac{1}{2}$

F equiprobable

$C' = 1$ bit/símbolo $\rightarrow$ c)



F

17. Sea un código polinómico sistemático (7, 4) con polinomio generador $g(D) = 1 + D + D^3$. Hallar la matriz generadora.

[✓ *a)*] $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

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

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

d) **Ninguna de las anteriores**

Código cíclico sistemático $(\underset{n}{\overset{}{7}}, \underset{k}{4}) \rightarrow r = n - k = 3$

$$G_{\underset{4}{k} \times \underset{7}{n}} = (I_K \mid P_{K\times r}) = \left(\begin{array}{c|c} \underbrace{\begin{matrix}1000\\0100\\0010\\0001\end{matrix}}_{X} & \begin{matrix}---\\---\\---\\---\end{matrix}\end{array}\right)$$

Código Cíclico:
SISTEMÁTICO
$R(D) = D^r \cdot X(D) \bmod C(D)$
$Y(D) = D^r \cdot X(D) + R(D)$

$X = \overset{D^3\,D^2\,D\,1}{1000} \equiv D^3 = X(D)$;; $D^r \cdot X(D) = D^6$;;

$D^6 \;\big\lfloor\; D^3 + D + 1$
$D^6 + D^4 + D^3 \quad D^3 + D + 1$
$D^4 + D^3$
$D^4 + D^2 + D$
$D^3 + D^2 + D$
$D^3 + D + 1$
$D^2 + 1 = R(D)$

$Y(D) = D^6 + D^2 + 1 \equiv 1000|101$

$X = 0100 \equiv D^2 = X(D)$
$D^r \cdot X(D) = D^5$
$Y(D) = D^5 + D^2 + D + 1 \equiv$
$\equiv 0100|111$

$D^5 \;\big\lfloor\; D^3 + D + 1$
$D^5 + D^3 + D^2 \quad D^2 + 1$
$D^3 + D^2$
$D^3 + D + 1$
$D^2 + D + 1 = R(D)$

$X = 0010 \equiv D = X(D)$;; $D^r \cdot X(D) = D^4$;; $D^4 \;\big\lfloor\; D^3 + D + 1$;; $Y(D) = D^4 + D^2 + D \equiv 0010|110$
$D^4 + D^2 + D \quad D$
$D^2 + D = R(D)$

$X = 0001 \equiv 1 = X(D)$;; $D^r \cdot X(D) = D^3$;; $D^3 \;\big\lfloor\; D^3 + D + 1$;; $Y(D) = D^3 + D + 1 \equiv 0001|011$
$D^3 + D + 1 \quad 1$
$D + 1 = R(D)$

$$\Rightarrow G_{4\times 7} = \left(\begin{array}{c|c} 1000 & 101 \\ 0100 & 111 \\ 0010 & 110 \\ 0001 & 011 \end{array}\right) \Rightarrow \text{ⓐ}$$

N

19. Sean X e Y dos variables aleatorias discretas cuyas probabilidades condicionadas se detallan en la siguiente tabla. Se sabe que p(X1)=p(X2)=1/4. Se puede afirmar que:

$$\begin{pmatrix} Y|X & X1 & X2 & X3 \\ Y1 & 1/2 & 1/4 & 3/4 \\ Y2 & 1/2 & 3/4 & 1/4 \end{pmatrix}$$

- a) $0 bits/simb \leq H(Y) \leq 0{,}5 bits/simb$
- b) $0{,}8 bits/simb < H(X,Y) \leq 1{,}5 bits/simb$
- [✓ c)] $I(X;Y) \leq 0{,}5 bits/simb$
- d) Ninguna de las anteriores.

$$P(x_1) = P(x_2) = \frac{1}{4} \Rightarrow P(x_3) = 1 - \frac{1}{4} \cdot 2 = \frac{1}{2}$$

Y\X	x_1	x_2	x_3
Y_1	1/2	1/4	3/4
Y_2	1/2	3/4	1/4

$$\xrightarrow{P(X,Y) = P(Y\backslash X) \cdot P(X)}$$

X, Y	x_1	x_2	x_3
Y_1	1/8	1/16	3/8
Y_2	1/8	3/16	1/8

$$P(Y_i) = \sum_{j=1}^{3} P(x_j, Y_i) \Rightarrow P(Y_1) = \frac{1}{8} + \frac{1}{16} + \frac{3}{8} = \frac{9}{16}$$

$$P(Y_2) = \frac{1}{8} + \frac{3}{16} + \frac{1}{8} = \frac{7}{16}$$

a) $\boxed{H(Y)} = \frac{9}{16} \cdot \log_2 \frac{16}{9} + \frac{7}{16} \cdot \log_2 \frac{16}{7} = \boxed{0'9887 \frac{bit}{simb}}$ a) NO

b) $H(Y,X) = \sum_i \sum_j p(x_i, y_j) \cdot \log_2 \frac{1}{p(x_i, y_j)}$

$$\boxed{H(Y,X)} = 3 \cdot \frac{1}{8} \log_2 8 + \frac{3}{8} \cdot \log_2 \frac{8}{3} + \frac{1}{16} \log_2 16 + \frac{3}{16} \log_2 \frac{16}{3} =$$

$$= \frac{3}{8} \cdot 3 + \frac{4}{16} + \frac{3}{8} \cdot \log_2 \frac{8}{3} + \frac{3}{16} \cdot \log_2 \frac{16}{3} = \boxed{2'3584 \frac{bit}{seg}} \rightarrow \text{b) NO}$$

c) $\boxed{I(X;Y)} = H(Y) - H(Y\backslash X) = 0'9887 - 0'8584 = \boxed{0'1302 \frac{bits}{simb}}$

$$H(Y\backslash X) = H(X,Y) - H(X) = 2'3584 - 1'5 = 0'8584 \frac{bit}{sim.}$$

$$H(X) = 2 \cdot \frac{1}{4} \log_2 4 + \frac{1}{2} \cdot \log_2 2 = 1 + \frac{1}{2} = \frac{3}{2} \frac{bits}{simb.}$$

$$H(Y\backslash X) = p(X=x_1) \cdot H(Y|X=x_1) + p(X=x_2) \cdot H(Y\backslash X=x_2) + p(X=x_3) \cdot H(Y\backslash X=x_3) =$$

$$= \frac{1}{4} \cdot 2 \cdot \frac{1}{2} \log_2 2 + \frac{1}{4} \cdot \left(\frac{1}{4} \log_2 4 + \frac{3}{4} \log_2 \frac{4}{3} \right) + \frac{1}{2} \cdot \left(\frac{3}{4} \log_2 \frac{4}{3} + \frac{1}{4} \log_2 4 \right) =$$

$$= \frac{1}{4} + \frac{1}{8} + \frac{1}{4} + \underbrace{\left(\frac{3}{16} + \frac{3}{8} \right)}_{\frac{9}{16}} \cdot \log_2 \frac{4}{3} = 0'8584 \frac{bits}{simb.}$$

F

20. Sea un código polinómico con polinomio generador $g(D) = \overset{\to r=4}{D^4} + D^3 + D^2 + 1$. Puede afirmarse que:

- *a*) El error $e(D) = D^7 + D^4 + D^2$ NO se detecta
- *b*) El error $e(D) = D^{15} + D^7$ NO se detecta
- c) El error $e(D) = D^{12} + D^{10} + D^9 + D^8$ se detecta con probabilidad 87.5 %
- [✓ *d*)] Ninguna de las anteriores

$$g(D) = \overset{\nearrow r=4}{D^4} + D^3 + D^2 + 1 = (D+1)\cdot\underbrace{(D^3+D+1)}$$

$$\begin{array}{l|l} D^4+D^3+D^2+1 & D+1 \\ \cline{2-2} D^4+D^3 & D^3+D+1 \\ \hline D^2+1 & \\ D^2+D & \\ \hline D+1 & \\ D+1 & \\ \hline 0 & \end{array}$$

$\left\{\begin{array}{l} \text{polinomio primitivo } m=3 \\ L = 2^m - 1 = 7 \\ \text{Divide a } D^L+1 \text{ , } L=7 \\ \text{No divide a ningún } D^\lambda+1 \text{ , } 3 \leq \lambda < 7 \end{array}\right.$

Se detectan todos los errores cuyo $e(D)$ no sea múltiplo de $g(D)$.

$S(D) = Z(D) \bmod g(D) = e(D) \bmod g(D) \neq 0 \to e(D)$ se detecta.

a) Error impar. $e(D=1) = 1$, pero $g(D=1) = 0$, por el factor $D+1$.

$\Rightarrow e(D)$ y $g(D)$ no tienen los mismos factores: $e(D)$ no es múltiplo de $g(D)$. <u>Se detecta.</u>

no puede tener al $D+1$ — tiene al $D+1$

b) Error par. Sabemos que se detectan si $\overbrace{\text{long.(paquete)}}^{¿?} < L = 7\ldots$

Pero aquí nos dan <u>UN ERROR EN PARTICULAR</u> $\Rightarrow$ Se detecta si NO ES MULTIPLO DE $g(D)$!!

$\underset{D^{15}+D^7}{e(D)} \bmod \underset{D^4+D^3+D^2+1}{g(D)} = \cdots = D \neq 0 \Rightarrow$ Este $e(D)$ se detecta.

c) OJO... Long. Ráfaga error $= j - i + 1 = 12 - 8 + 1 = 5$.

Grado $g(D) = r = 4$.

Si long. ráfaga $= r+1 = 5 \Rightarrow$ prob. detección $= 1 - \dfrac{1}{2^{r-1}} = 1 - \dfrac{1}{2^3} =$

EN GENERAL PARA ERRORES $= 0'875 \equiv 87'5\%$

$e(D)$ de RAFAGAS de LONGITUD 5... Pero aquí nos dan <u>UN ERROR EN PARTICULAR</u> $\Rightarrow$ Se detecta si NO es múltiplo de $g(D)$, <u>al 100%</u>!!

$e(D) \bmod g(D) = D^{12} + D^{10} + D^9 + D^8 \bmod D^4 + D^3 + D^2 + 1 = \cdots = D^3 + 1 \neq 0$