ETSETB

Curso 2005-06 Primavera

EXAMEN DE TRANSMISIÓN DE DATOS

6 de junio de 2006

PUBLICACIÓN DE NOTAS PROVISIONALES: 9/06/2006
FECHA LÍMITE PARA LAS ALEGACIONES: 13/06/2006
PUBLICACIÓN DE NOTAS DEFINITIVAS: 16/06/2006
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. En un sistema de transmisión de datos se emplea un código binario lineal y sistemático Cod(5,2) generado por el polinomio $D^3 + D^2 + 1$. El sistema de decisión entrega al decodificador de canal el bloque con borrones (1 a b c 0). Los valores más verosímiles de a, b y c son respectivamente:

   a) a=0, b=1, c=1
   b) a=1, b=0, c=1
   c) a=1, b=1, c=0
   d) a=0, b=0, c=1

Base x	Base $X(D)$	$D^r X(D)$	$R(D)$	$Y(D)$	Y
(0,1)	1	D^3	D^2+1	D^3+D^2+1	(0 1 ; 1 0 1)
(1,0)	D	D^4	D^2+D+1	D^4+D^2+D+1	(1 0 ; 1 1 1)

$$D^3 \;\Big|\; D^3+D^2+1 \qquad \text{resto } D^2+1,\ \text{cociente } 1$$

$$D^4 \;\Big|\; D^3+D^2+1 \qquad D^4+D^3+D,\ \text{cociente } D+1;\quad D^3+D^2+1 \quad\Rightarrow\quad D^2+D+1$$

Código:

$$\left\{\begin{array}{l} 0\ 0\ 0\ 0\ 0 \\ 0\ 1\ 1\ 0\ 1 \\ 1\ 0\ 1\ 1\ 1 \\ 1\ 1\ 0\ 1\ 0 \end{array}\right.$$

$$Z = (1\ a\ b\ c\ 0)$$

$$1\ 1\ 0\ 1\ 0 \Rightarrow \hat{Y} \Rightarrow \begin{cases} a=1 \\ b=0 \\ c=1 \end{cases} \Rightarrow b)$$

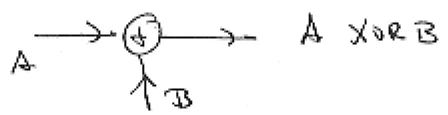
2. Sean A y B dos fuentes binarias sin memoria donde H(A) tiene entropía máxima. Se puede afirmar que:

a) $H(B/A) < H(A)$
b) $H(A \text{ XOR } B) = H(A)$
c) $I(A;B)=0$
d) Ninguna de las anteriores

$H(A) = 1$

a) $H(B/A) < H(A)$ no necesariamente

b)



$H(A \oplus B) = H(A)$ si $H(A)$ máxima.

CIERTO

c) $I(A;B) = \emptyset$ no necesariamente.

4. En Z_{35}, la inversa de 25 es:

a) 30
b) 1
c) 3
d) Ninguna de las anteriores

Z_{35} anillo conmutativo.

$\exists\, a^{-1} \in Z_{35}$ sii m.c.d$(a, 35) = 1$

En este caso

m.c.d$(25, 35) = 5 \neq 1 \Rightarrow \nexists\, a^{-1}$

3. Para un receptor con S/N=10 y una fuente ternaria sin memoria con probabilidad de emisión de los símbolos 1/2, 1/8 y 3/8 respectivamente, el ancho de banda mínimo necesario para poder transmitir 1000 símbolos por segundo de dicha fuente sin pérdidas es:

a) 406 Hz
b) 528 Hz
c) 1748 Hz
d) Ninguna de las anteriores

$$V_t \leq C = W \cdot \log_2 (1 + S/N)$$

$$\left[\frac{bits}{seg}\right] V_t = \frac{L}{T_F} \frac{\left[\frac{bits}{simb.}\right]}{\left[\frac{seg}{simb}\right]}$$

$$L \geq H$$

El mínimo será

$$\frac{H}{T_F} = W \log_2 (1 + S/N)$$

$$W = \frac{H}{T_F \cdot \log_2 (1 + S/N)} = \frac{V_F \cdot H}{\log_2 (1 + S/N)} \Rightarrow \underline{\underline{406\,Hz}}$$

$$H = \frac{1}{2} \log_2 2 + \frac{1}{8} \log_2 8 + \frac{3}{8} \log_2 8/3 = 2 - \frac{3}{8} \log_2 3$$

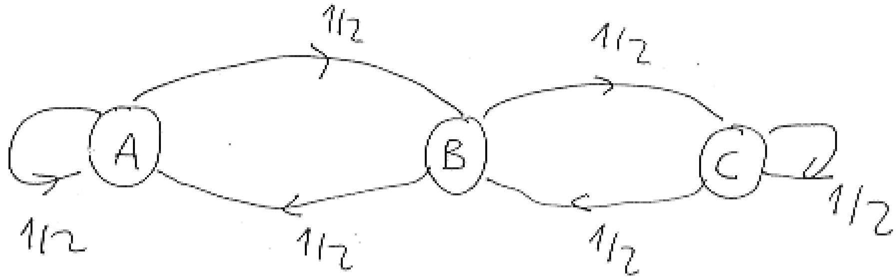
5. Sea una fuente F= {A, B, C}, con las siguientes probabilidades condicionadas
$P(A/A)=P(C/C)=0.5$;
$P(A/C)=P(C/A)=0$;
$P(A/B)=P(C/B)=0.5$.
La eficiencia de una codificación de Huffman de F vale:

a) 1

b) 0.75

c) 0.6

d) Ninguna de las anteriores



$$H(F) = P(A)\,H(F|A) + P(B)\,H(F|B) + P(C)\,H(F|C)$$

$$H(F|A) = H(F|B) = H(F|C) = H(1/2) = 1$$

$$H(F) = 1$$

Huffman $A \to 0\ ;\ B \to 10\ ;\ C = 11$

$$\bar{l} = 1 \cdot \frac{1}{3} + 2 \cdot \frac{2}{3} = \frac{5}{3}$$

$$\boxed{E = \frac{H(F)}{\bar{l}} = \frac{1}{5/3} = \frac{3}{5} = 0'6}$$

<u>Nota:</u>

$$\left.\begin{array}{l} \frac{1}{2} P_A = \frac{1}{2} P_B \\ \frac{1}{2} P_B = \frac{1}{2} P_C \end{array}\right\} P_A = P_B = P_C = 1/3$$

5. Para un código con capacidad correctora 5, puede asegurarse que:

a) La distancia mínima es al menos 12

b) La razón (k/n) es mayor que 0.1

c) La redundancia es mayor o igual que 10

d) Ninguna de las anteriores

a) $d_{min} = 11 \rightarrow$ FALSO $\quad d_{min} \geq 2e + 1 = 11$

b) NO.- POR EJEMPLO EL CÓDIGO DE REPETICIÓN (11, 1) TIENE $e = 5$ $\quad R = \frac{1}{11} < 0'1$

c) SI $\rightarrow$ <u>COTA DE SINGLETON</u>

$r \geq 2 \cdot e = 10$

$e = 5$

7. El número de códigos binarios de Hamming sistemáticos distintos para n=255 vale:

a) 8!

b) 255

c) 247!

d) Ninguna de las anteriores

$n = 255 \Rightarrow r = 8 \ , \ k = 247$

$$\underset{\left(\underset{n}{255} \times \underset{r}{8}\right)}{H^t} = \left(\begin{array}{c} \\ \\ \hline I_8 \end{array} \right) \begin{array}{l} \left.\begin{array}{c} \\ \\ \end{array}\right\} 247 \text{ FILAS} \\ \left.\begin{array}{c} \\ \end{array}\right\} 8 \text{ FILAS} \end{array}$$

$\rightarrow$ PERMUTACIONES DE 247 VECTORES DE 8 componentes: 247!

Vernam.

6. Dos usuarios A y B ofrecen confidencialidad a sus comunicaciones mediante un cifrado de Vernan. La clave de cifrado k es generada por A y enviada a B utilizando un cifrado RSA (la clave pública de B vale N_B=187=11*17; e_B=7), generándose el criptograma C1. Posteriormente B obtiene k y cifra el mensaje M2, obteniendo el criptograma C2. Conocidos C1=00000011 y C2=11110000 (mayor peso a la izquierda), calcule el valor de M2.

a) 00110011

b) 01000101

c) 11100011

d) Ninguna de las anteriores

$\boxed{A}$ $\boxed{B}$

Genera k $\xrightarrow{E_{AB}(k) = C_1}$ OBTIENE k

$\xleftarrow{C_2 = E_K(m_2)}$ TX m_2 CIFRADO CON k

- CLAVE PRIVADA DE B

$\phi(N_B) = 160$ $\underbrace{7}_{e_B} \cdot d_B = k \cdot 160 + 1$ $\boxed{d_B = 23}$

$k = C_1^{d_B} \bmod N_B = 3^{23} \bmod 187 = 181$

$k = 1\,0\,1\,1\,0\,1\,0\,1$

<u>VERNAN</u> - $m_i = c_i \oplus k_i$

$\boxed{m_2} = C_2 \oplus k = 1111\,0000 \oplus 1\,0\,1\,1\,0\,1\,0\,1$

$= \boxed{0\,1\,0\,0\,0\,1\,0\,1}$

9. Alicia envía un mensaje m a Bob con la clave e_1=4807 y $n = pq$=360671 y también a Berta con la clave e_2=9889 y n=360671. Se consigue descifrar:

a) con la inversa de $(e_1 + e_2) mod \Phi(n)$

b) con la inversa del $mcd(e_1, e_2) mod \Phi(n)$

c) únicamente con las inversas de e_1 y de $e_2 mod \Phi(n)$

d) Ninguna de las anteriores

Ataque de módulo común:

$$c_1^x c_2^y = m^{xe_1 + ye_2} \bmod n = m \bmod n \quad \text{si } mcd(e_1, e_2) = 1 = xe_1 + ye_2$$

pero:

$$\begin{array}{cccccc} & 2 & 17 & 2 & 12 & \\ 9889 & 4807 & 275 & 132 & \boxed{11} & 0 \end{array}$$

→ Si $x=1, y=1$ se necesita la inversa de $(e_1+e_2) = 14696$, un número par y $\phi(n) = (p-1)(q-1)$ también es par → no existe la inversa.

→ Como e_1 y e_2 son primos con $\phi(n)$, el $mcd(e_1, e_2) = 11$ es primo con $\phi(n)$ → existe la inversa y se consigue descifrar

→ b

10. Dados a, p, q coprimos, entonces $((a * b) \bmod p) * q * (a^{-1} \bmod p)$ es:

a) $q * (b \bmod p)$ si se calcula el $\bmod (p * q)$

b) 1 si se calcula el $(\bmod q)$

c) $b * (q \bmod p)$ si se calcula el $(\bmod p)$ y $b < p$

d) Ninguna de las anteriores

$$((ab) \bmod p)(a^{-1} \bmod p)\, q = ((a a^{-1} b) \bmod p + Kp)\, q \quad \text{, algún } K.$$

$$= (b \bmod p)\, q + Kpq.$$

- Si se calcula el mod q: $((b \bmod p) q + Kpq) \bmod q = 0$.

- Si se calcula el mod p: $((b \bmod p) q + Kpq) \bmod p = (bq) \bmod p$

$$= (\underbrace{b (q \bmod p)}_{\text{podría ser } > p}) \bmod p.$$

- Si se calcula el mod pq: $((b \bmod p) q + Kpq) \bmod pq = ((\underbrace{b \bmod p}_{\text{inferior a } p}) q) \bmod pq$

inferior a pq

$$= (b \bmod p)\, q$$

$\Rightarrow$ a.

11. Si n tiene k factores primos impares f_i con multiplicidad l_i, la función $\lambda(n)$ se define como el $mcm(\Phi(f_1^{l_1}), \Phi(f_2^{l_2}), \cdots, \Phi(f_k^{l_k}))$ y se cumple que $m^{\lambda(n)} mod\, n = 1$ si el $mcd(m, n) = 1$. Para $n = 19 * 43 * 43$ se calcula el criptograma 127 como $m^e \bmod n$ con $e = 9851$, entonces:

a) $m = 18033$ y $d = 11$

b) $e = 9851$ no es un valor válido

c) El número de e distintas tal que $mcd(e, \Phi(n)) = 1$ reducidas $mod\, \lambda(n)$ no coincide con las e tal que $mcd(e, \lambda(n)) = 1$

d) Ninguna de las anteriores

$$\lambda(n) = mcm(18, 43 \cdot 42) = 3 \cdot 43 \cdot 42 = 5418$$

$$\phi(n) = \phi(f_1^{l_1}) \cdot \phi(f_2^{l_2}) \cdots \phi(f_k^{l_k}) = \underbrace{mcm(\phi(f_1^{l_1}), \ldots, \phi(f_k^{l_k}))}_{\lambda(n) = 5418} \underbrace{mcd(\phi(f_1^{l_1}), \ldots, \phi(f_k^{l_k}))}_{K}$$

$\Rightarrow mcd(e, \phi(n)) = 1 = xe + y\phi(n) = xe + yK\lambda(n)$, las mismas e reducidas $mod\, \lambda(n)$.

$\Rightarrow mcd(e, \lambda(n)) = 1$, e es primo con los factores no comunes y con los comunes con mayor exponente de $\phi(n)$ $\Rightarrow$ es primo con $\phi(n)$.

$\Rightarrow$ c) falsa

			x	y
9851	5418	1	$\boxed{11}$	-20
5418	4433	1	-9	11
4433	985	4	2	-9
985	493	1	-1	2
493	492	1	1	-1
492	$\boxed{1}$	492	0	1

$d = 11$, e primo con $\phi(n)$ y $\lambda(n)$

$$127^{11} \bmod 35131 = (34717)^2 \cdot 127^3 \bmod 35131$$
$$= 30872 \cdot 10785 \bmod 35131$$
$$= 18033$$

$\Rightarrow$ a

la inversa de e mod $\phi(n)$ es $d_2 = 10847$ y $d_2 \bmod \lambda(n) = 11 = d$

12. La secuencia de punteros (4,6)D (2,3)A (3,3)C en dígitos decimales ha sido generada por un compresor LZ77 con un buffer inicializado con BCBCBDC (más antiguo a la izquierda). La posición del buffer más próxima a los datos por codificar es la número 1. La secuencia que se ha comprimido contiene la cadena:

a) BDCD
b) DBAD
c) BADC
d) Ninguna de las anteriores

... 7 6 5 4 3 2 1
... BCBCBDC (4,6) D
... BCBCBDCC
... BCBCBDCCB
... CBDCCBD
... BDCCBDC
... DCCBDCC
... CCBDCCB
... $\boxed{\text{CBDCCBD}}$

... CBDCCBD (2,3) A
CBDB
CBDBD
BDBDB
D$\boxed{\text{BDBA}}$ (3,3) C
DBAD
BADB
ADBA
$\boxed{\text{DBAC}}$

CBDCCBDB$\boxed{\text{DBAD}}$BAC → (b)

13. Un código de Hamming (7,4) se ha extendido con 1 bit de paridad global para utilizarlo en un canal con una probabilidad de error de bit de 10^{-3} y una probabilidad de borrón de 10^{-3}. La probabilidad p de recibir 1 error y 1 borrón es:

a) $p \geq 0{,}044\ 10^{-3}$
b) $0{,}044\ 10^{-3} > p \geq 0{,}033\ 10^{-3}$
c) $0{,}033\ 10^{-3} > p \geq 0{,}022\ 10^{-3}$
d) $0{,}022\ 10^{-3} > p$

$$2 \cdot \binom{n}{2} P_e \cdot P_b \left(1-(P_e+P_b)\right)^6 = 2 \binom{8}{2} P_e^2 (1-2P_e)^6 \quad \text{con} \quad P_b = P_e = 10^{-3}$$

$$= 0.055 \cdot 10^{-3} \rightarrow (a)$$

14. A partir de un LFSR de 3 registros se ha generado la secuencia 001110100111010011101, entonces el polinomio de conexiones:

a) tiene el término D^2 no nulo

b) tiene el término D no nulo

c) no existe para esta secuencia

d) Ninguna de las anteriores

0011101 ¦ 0011101 ¦ 0011101 periodo 7. Como el LFSR tiene 3 registros, el polinomio de conexiones es de grado 3 y primitivo. Sólo pueden ser: D^3+D+1 ó D^3+D^2+1

$1 \bmod (D^3+D+1) = 1 \to 0$

D " $= D \to 0$

D^2 " $= D^2 \to 1$

D^3 " $= D+1 \to 0$, b) falsa.

$1 \bmod (D^3+D^2+1) = 1 \to 0$

D " $= D \to 0$

D^2 " $= D^2 \to 1$

D^3 " $= D^2+1 \to 1$

D^4 " $= D^2+D+1 \to 1$

D^5 " $= D+1 \to 0$

D^6 " $= D^2+D \to 1$ $\to$ a

D^7 " $= 1$ (se repite)

15. El polinomio de conexiones de un LFSR es $D^4 + D + 1$. Indica la FALSA:

   a) La secuencia generada es $D^{11} + D^8 + D^7 + D^5 + D^3 + D^2 + D + 1$
   b) La probabilidad de emitir un 0 es de 7/15
   c) La secuencia generada tiene ráfagas de cuatro 1's y tres 0's
   d) Alguna de las anteriores es falsa

D^4+D+1 es primitivo $\rightarrow$ periodo $2^4-1=15$ y $p(0)=7/15$ y $p(1)=8/15$

b) cierta.

$$D^{15}+1 \;\; \underline{| D^4+D+1}$$

$$\smile \quad D^{11}+D^8+D^7+D^5+D^3+D^2+D+1 \rightarrow \text{a) cierta}$$

$\underbrace{000}1001101 0\underbrace{1111} \rightarrow$ c) cierta

d es falsa.

16. Una fuente X emite los símbolos 0 y 1 y se sabe que la P(0/1)=0.3 y P(1/0)=0.7. Una segunda fuente Y independiente de la primera también emite los símbolos 0 y 1 pero la P(0/1)=0.4 y la P(1/0)=0.6. La entropía conjunta H es:

   a) $H \geq 1.95$
   b) $1,95 > H \geq 1,9$
   c) $1,9 > H \geq 1.85$
   d) $1,85 > H$

En ambas fuentes se cumple $P(0/1) = 1 - P(1/0)$ y como $p(0/0) = 1 - p(1/0)$ entonces $p(0/1) = p(0/0) = p_0$. Son fuentes sin memoria e independientes:

$p(00) = 0.3 \times 0.4 = 0.12$
$p(01) = 0.18$
$p(10) = 0.28$
$p(11) = 0.42$

$$H(X,Y) = -(0.12\log_2 0.12 + 0.18\log_2 0.18 + 0.28\log_2 0.28 + 0.42\log_2 0.42) = 1.8522 \text{ bits/símbolo}.$$

17. Un mensaje de 50 bits se envía por un canal BSC (Binary Symmetric Channel) con probabilidad de error en el bit $p = 10^{-3}$. Se utiliza un código corrector de errores 2-perfecto. Comparando la $p_{e_{sin}}$(mensaje) sin protegerlo con la $p_{e_{res}}$(mensaje) residual de usuario, se ha reducido *aproximadamente* en:

a) 50 veces
b) 505 veces
c) 2550 veces
d) Ninguna de las anteriores

$e = 2$

Sin código canal $\rightarrow$ $P_{E\_bit} = 10^{-3}$

Con código canal:

$$P_{E\_bloque} = \sum_{i=e+1}^{50} \binom{n}{i} \cdot p^i \cdot (1-p)^{n-i} \simeq \binom{50}{3} \cdot p^3 + \binom{50}{4} \cdot p^4 =$$

$$= 19600 \cdot 10^{-9} + 2'3 \cdot 10^{-7} = 1'98 \cdot 10^{-5}$$

$$P_{E\_bit} = \frac{5}{50} \cdot P_{E\_bloque} = 1'98 \cdot 10^{-6}$$

$\underbrace{e+1}_{\text{se excedió la capacidad correctora}} + \underbrace{2}_{\text{el código intenta corregir 2 errores y se equivoca.}} = 5$ bits erróneos

$$\frac{10^{-3}}{1'98 \cdot 10^{-6}} = \frac{10^{3}}{1'98} = \boxed{505'05 \text{ veces}}$$

~~error:~~ $\dfrac{10^{-3} \rightarrow P_{E\_bit}\ (SIN)}{1'98 \cdot 10^{-5} \rightarrow P_{E\_bloque}\ (CON)} = 50'50$

~~error:~~ $\displaystyle\sum_{i=1}^{50} \binom{n}{i} p^i (1-p)^{n-i} \simeq \binom{50}{1} \cdot p^1 = 50 \cdot p = 0'05 = P_{E\_bloque}$ sin código

$\dfrac{0'05 \rightarrow P_{E\_bloque}\ (SIN)}{1'98 \cdot 10^{-5} \rightarrow P_{E\_bloque}\ (CON)} = 2551'02$ veces

15. El alfabeto de una fuente consta de 4 símbolos con probabilidades p(A)=0.2, p(B)=0.4, p(C)=0.3, p(D)=0.1 y se utiliza un código Huffman binario. La fuente emite un mensaje de 10 símbolos. Se desea aleatorizar el mensaje utilizando un LFSR. El grado mínimo del polinomio de conexiones a utilizar es:

a) 6

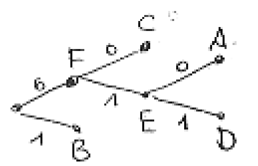
b) 5

c) 4

d) Ninguna de las anteriores

Hay que calcular la longitud (media) en bits de los mensajes emitidos por la fuente que van a ser aleatorizados por el LFSR:

B 0'4		B 0'4		F 0'6	
C 0'3		C 0'3	F 0'6	B 0'4	
A 0'2	E 0'3	E 0'3			
D 0'1					



A 010
B 1
C 00
D 011

L_{MAX} = 3 bits/símbolo

Nota
No considerar $\bar{L}$ (2'5 bits/símbolo)
sino el caso peor ~~no~~ es emitir A

$\text{Mensaje}_{MAX} = 10 \cdot L_{MAX} = 30 \ \frac{\text{bits}}{\text{mensaje}}$

Se elegirá un C(D) primitivo, y así $L_{MAX} = 2^n - 1$

$$2^n - 1 \geq 30 \rightarrow [n = 5]$$

$$n \geq \log_2 31 = 4'95$$

19. ¿Qué diagrama de enrejado puede corresponder con un codificador convolucional de tasa 2/3 y memoria 2?

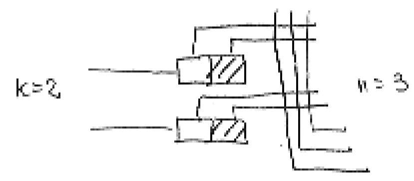
a) Figura A

b) Figura B

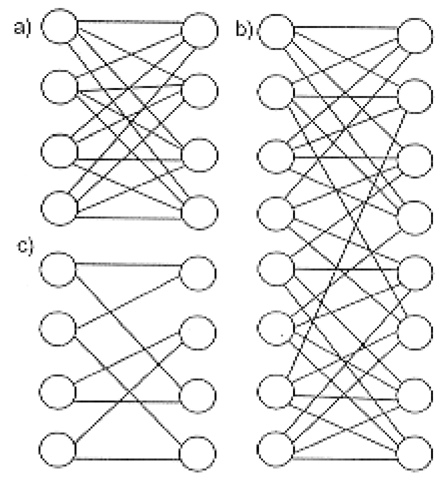
c) Figura C

d) Ninguna de las anteriores.

$G(3,2)$
$\quad n \; k$



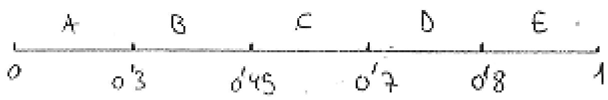
- $2^{\text{memoria}} = 2^2 = 4$ Estados //
- $2^k = 4$ salidas desde cada estado



d) Ninguno de los anteriores

20. Una fuente emite 5 símbolos con las siguientes probabilidades: p(A)=0.3, p(B)=0.15, p(C)=0.25, p(D)=0.1, p(E)=0.2. Descodifique la secuencia de longitud 3 cuya palabra código es 0.20, si se ha utilizado un codificador aritmético.

a) ACE
b) AAE
c) ACC
d) Ninguna de las anteriores



$$0'2 \in [0, 0'3) \Rightarrow A$$

$$\frac{0'2 - 0}{0'3} = 0'67 \in [0'45, 0'7) \Rightarrow C$$

ACE

$$\frac{0'67 - 0'45}{0'7 - 0'45} = 0'88 \in [0'8, 1] \Rightarrow E$$

<u>error</u> $\Rightarrow \frac{0'67 - 0'45}{0'45} = 0'48 \Rightarrow C \rightarrow$ ACC