ETSETB
Curso 2004-05 Primavera
EXAMEN DE TRANSMISIÓN DE DATOS
23 de junio de 2005

PUBLICACIÓN DE NOTAS PROVISIONALES: 28/06/05
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. Para un código ternario sistemático de repetición Cod(3,1) es FALSO que:
   a) La matriz de generación es $G = (111)$
   b) El subespacio ortogonal al código está generado por la base $\{(1,0,2),(0,1,2)\}$
   c) El número de síndromes distintos de 0 es 8
   d) Alguna de las anteriores es falsa

a) Base espacio de mensajes $\{1\}$
Imagen del vector de la base $\{(1\,1\,1\}$ $\Rightarrow$ $G = (1\,1\,1)$
Cierta

b) Dimensión del código = 1
Dimensión del ortogonal = 2
$(1,0,2)$ y $(0,1,2)$ son linealmente independientes, y ortogonales al $(1,1,1)$ Cierta

c) síndromes $= q^r = 3^2 = 9$
Nº Distintos de $\emptyset = q^r - 1 = 8$ cierta.

d) Falsa

2. ¿Cuánto vales $\Psi(12)$ (SI)

a) 2
b) 4
c) 6
d) Ninguna de las anteriores

$\Psi(12)$ = cardinal del conjunto reducido de restos mod 12

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ $\quad 12 = 2^2 \cdot 3$

4 elementos $\Rightarrow \Psi(12) = 4$

---

3. Para un código de Hamming (15,11) el número de palabras NO código que están a distancia 2 de una palabra código cualquiera es:

a) 98
b) 105
c) 120
d) Ninguno de los anteriores

$\binom{15}{2} = \frac{15 \cdot 14}{2} = 105$

(SI) 4. Una fuente emite 3 símbolos independientes con probabilidades $\{0{,}7, 0{,}2, 0{,}1\}$. La fuente se codifica mediante un código de Huffman y luego mediante un código de Hamming (15,11). La entropía de la fuente codificada es:

a) 0.92 bits/simb
b) 1.03 bits/simb
c) 1.16 bits/simb
d) Ninguna de las anteriores

La entropía de la fuente no depende de la codificación

$H = 0'7 \log_2 \frac{1}{0'7} + 0'2 \log_2 \frac{1}{0'2} + 0'1 \cdot \log \frac{1}{0'1} = 1.16$ bits/simb

(S1) 5. Se utiliza un codigo de Hamming (15,11) para codificar un canal binario simétrico con una tasa de error $p_e = 10^{-4}$. La tasa binaria de error a la SALIDA del decodificador es:

a) $0{,}14\ 10^{-6}$

b) $0{,}21\ 10^{-6}$

c) $0{,}10\ 10^{-5}$

d) Ninguna de los anteriores

$$P_E \approx \binom{15}{2} (10^{-4})^2 (1-10^{-4})^{13} = 0'105\ 10^{-5}$$

$$p_e = \frac{3}{15} \cdot P_E = 0'21\ 10^{-6}$$

---

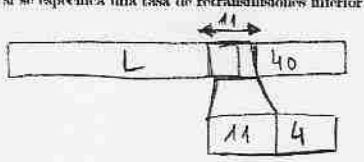
6. Para proteger la comunicación a través de un canal sin memoria con una tasa de error de bit de $0{,}6\,10^{-5}$, se emplea un código corrector (15,11) y un codigo polinómico usado como detector con polinomio generador de grado 40 ¿Cuál es el número máximo de bits de información de usuario que puede contener la trama si se especifica una tasa de retransmisiones inferior a 10^{-7}?

a) 123 bits

b) 102 bits

c) 246 bits

d) Ninguna de las anteriores.



Retransmisión = 1 ó más bloques erroneos.

Prob. bloque erróneo = $\binom{15}{2}(0'6\,10^{-5})^2(1-0'6\,10^{-5})^{13} = 0'378\,10^{-9}$

Prob trama errónea $\binom{N}{1} 0'378\,10^{-8} (1-0'378\,10^{-9})^{N-1} \approx N \cdot 0'378\,10^{-9} < 10^{-7} \Rightarrow N < 26'45$

$N \leq 26 \Rightarrow \left\lfloor \frac{L+40}{11} \right\rfloor < 26 \Rightarrow L = 26 \cdot 11 - 40 = \underline{246}$

7. Para a y b dos números naturales, ambos menores que n, puede asegurarse:

a) Si a y b son los divisores de n, entonces $\Psi(n) = (a-1)(b-1)$

b) Si a y b pertenecen al conjunto reducido de residuos de n, entonces $(a*b) mod n$ también pertenece a este conjunto

c) Si $a^b = 1 \ mod n$, entonces a^{b-2} es la inversa de $a \ mod n$

d) Ninguna de las anteriores.

8. Para una fuente binaria sin memoria es cierto que:

a) Si la eficiencia del código de fuente es 1, entonces la información media por dígito binario codificado no puede ser de 1 bit por dígito.

b) Sumar XOR la secuencia con otra perfectamente aleatoria antes de realizar la codificación de fuente mejora la longitud de codificación.

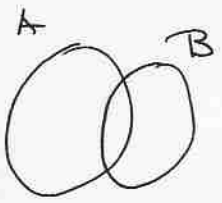
c) Si es perfectamente aleatoria la entropía es de 1 bit por símbolo, sea cual sea la extensión de la fuente.

d) Ninguna de las anteriores.

10. 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) $H(A,B) < H(A) + H(B)$
c) $H(A/B) < H(A) - H(B)$
d) Alguna de las anteriores es falsa

$I(A;B) \neq 0$



a) Siempre se cumplirá

$H(B/A) < H(B)$ si $I(A;B) \neq 0$ Cierto

b) Siempre se cumplirá

$H(A,B) < H(A) + H(B)$ si $I(A;B) \neq \emptyset$

Cierto

c) $I(A;B) = H(A) - H(A/B) \neq \emptyset$

$I(A;B) \leq H(B)$

$H(A) - H(A/B) \leq H(B)$

$H(A) - H(B) \leq H(A/B)$

Es falso que $H(A) - H(B) > H(A/B)$

d) Cierto.

12. En un sistema RSA todos los valores de n contienen siempre un mismo factor primo. Para un valor de $e = 11$, indique qué valor de n no es apropiado en dicho sistema:

a) 413
b) 649
c) 1003
d) 1357

Euclides $m.c.d(413, 649) = 59$.

$413 = 59 \cdot 7 \Rightarrow \varphi(413) = 58 \cdot 22 = 2 \cdot 29 \cdot 2 \cdot 11$

$649 = 59 \cdot 11 \Rightarrow \varphi(649) = 58 \cdot 10 = 2 \cdot 29 \cdot 2 \cdot 5$ ✓

$1003 = 59 \cdot 17 \Rightarrow \varphi(1003) = 58 \cdot 16 = 2 \cdot 29 \cdot 2^4$ ✓

$1357 = 59 \cdot 23 \Rightarrow \varphi(1357) = 58 \cdot 22 = 2 \cdot 29 \cdot 2 \cdot 11$ ✓

$m.c.d(\varphi(413), 11) \neq 0 \Rightarrow$ a)

---

9. Para una fuente binaria es FALSO que:

a) La entropía de la fuente es como máximo 1 bit/símbolo
b) La entropía de la fuente, cuando los símbolos son equiprobables, es mayor cuando no tiene memoria
c) Aumenta la eficiencia de la codificación al utilizar una extensión de fuente cuando los símbolos no son equiprobables
d) Alguna de las anteriores es falsa

---

13. Para un código binario polinómico cuyo generador es $D^3 + D^2 + 1$, ¿cuál de las siguientes palabras no pertenece al código?

a) $D^4 + D^3 + D$
b) $D^5 + D^4 + D^3 + D^2 + 1$
c) 0
d) ~~$D^3 + D^2 + 1$~~ $D^4 + D^2 + D + 1$

a) $D^4 + D^3 + D \mod D^3 + D^2 + 1 = \emptyset$

b) $D^5 + D^4 + D^3 + D^2 + 1 \mod D^3 + D^2 + 1 = D^2 \neq 0 \Rightarrow$ No pertenece

c) $0 \mod D^3 + D^2 + 1 = \emptyset$

d) $D^4 + D^2 + D + 1 \mod D^3 + D^2 + 1 = \emptyset$

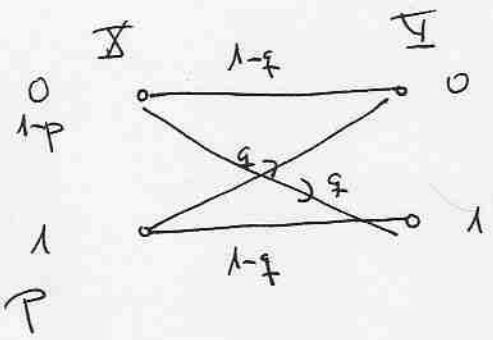
11. En un canal binario simétrico con probabilidad de error 1/8 y para una fuente binaria cuya probabilidad de emisión del símbolo 1 es 3/4, la entropía a la salida del canal, H(Y), cumple:

a) $0{,}00 \leq H(Y) < 0{,}50$

b) $0{,}50 \leq H(Y) < 0{,}75$

c) $0{,}75 \leq H(Y) < 0{,}85$

(*d*) $0{,}85 \leq H(Y) < 1{,}00$



$p = 3/4$

$q = 1/8$

$Prob[Y=0] = (1-p)(1-q) + p \cdot q = 0'3125 \triangleq (1-\alpha)$

$Prob[Y=1] = p(1-q) + (1-p) \cdot q = 0'6875 \triangleq \alpha$

$H(Y) = \alpha \log_2 \frac{1}{\alpha} + (1-\alpha) \log_2 \frac{1}{1-\alpha} = 0'896 \text{ bits/simb} \Rightarrow d)$

16. ¿Qué afirmación es FALSA?

a) Una clave será buena para cifrar si, entre otras cosas, su entropía es muy alta.

b) El cifrado de Vigènere consiste en una sustitución polialfabética.

c) El algoritmo DES simple no es recomendable porque el espacio de claves es muy bajo.

(*d*) Alguna de las anteriores es falsa.

a) ok!

b) ok!

c) 56 bits es poco...

14. ¿Qué afirmación es correcta?

a) El llamado Código Telefónico funciona así: A cada tecla del teléfono se le asignan tres letras en el siguiente orden: 2-ABC, 3-DEF, 4-GHI, 5-JKL, 6-MNO, 7-PRS, 8-TUV, 9-WXY, 1-ÑQZ. Cada letra se sustituye por el número al que está asignada + la posición que ocupa (que puede ser 1, 2 ó 3); así la letra E se codifica como 32. El mensaje "HOLA" tiene como criptograma "42635322".

b) El sistema RSA utiliza como módulo el valor $N = pq$, con p y q primos grandes. La clave privada d deberá ser inversa de la clave pública e módulo (N). Su robustez está basada en el problema de la factorización de números primos.

c) En el sistema DES, la clave original de 64 bits se convierte en una clave real de 56 bits al eliminarse el bit de paridad de cada octeto. El algoritmo tiene 12 rondas.

d) Ninguna de las anteriores.

a) HOLA → 42635321

b) Su robustez se base en problema factorización de números GRANDES!

c) Son 16 rondas de Feistel.

15. Sobre las propiedades detectoras del código polinómico con polinomio generador $g(D) = 1 + D^3 = (1 + D)(1 + D + D^2)$, ¿qué afirmación es correcta?

a) Se detectan todos los errores simples, impares y dobles.

b) Se detectan todos los errores simples, impares y los errores dobles con posiciones de bit erróneos que disten menos de 7 posiciones.

c) Se detectan todas las ráfagas de error de longitud menor que 4, aquellas ráfagas de error de longitud 4 con probabilidad del 75 % y aquellas ráfagas de error de longitudes mayores que 4 con probabilidad del 87.5 %

d) Ninguna de las anteriores.

a)

b) - simples sí se detectan
- impares "
- dobles se detectan si están a distancia $< L = 2^2 - 1 = 3$, no 7!

c) · Si longitud ráfaga $< r+1 = 4 \rightarrow$ se detectan 100%

· " $= r+1 = 4 \rightarrow$ " con prob. $1 - \frac{1}{2^{r-1}} =$

$= 1 - \frac{1}{4} = 0'75 \equiv 75\%$

· Si " $> r+1 = 4 \rightarrow$ Se detectan con

prob $= 1 - \frac{1}{2^r} = 1 - \frac{1}{8} =$

$= 0'875 \equiv 87'5\%$

Nota:
$1 + D + D^2$ es primitivo!

equiprobables

17. Sean F1 y F2 dos fuentes equiprobales cuyos elementos pertenecen al conjunto {1,2,3}. Sea F una fuente cuya salida es el máximo común divisor de los símbolos emitidos simultaneamente por F1 y F2. Calcule H(F).

   a) 0 bits/símb
   b) 0.9864 bits/símb
   c) 1.58 bits/símb
   d) Ninguna de las anteriores

F_1	F_2	F
1	1	1
1	2	1
1	3	1
2	1	1
2	2	**2**
2	3	1
3	1	1
3	2	1
3	3	**3**

$F = \{1, 2, 3\}$

$P(1) = 7/9$

$P(2) = P(3) = 1/9$

$$H(F) = \frac{7}{9} \log_2 \frac{9}{7} + 2 \cdot \frac{1}{9} \log_2 9 = 0'9864$$

18. Sea M el mensaje en claro, C el criptograma y k la clave de cifrado. Para un criptosistema incodicionalmente seguro es FALSO que:

   a) $H(M/C) > H(M)$
   b) $longitud(k) \geq longitud(M)$
   c) Son de poca utilidad práctica
   d) Ninguna de las anteriores

6^4

20. ¿Para elegir una clave numérica, lanzamos repetidas veces un dado no trucado. Si la clave tiene 4 dígitos, la entropía es de:

a) $log_2(6)$ bits/símbolo
b) $log_2(1/64)$ bits/símbolo
c) $log_2(6^4)$ bits/símbolo
d) Ninguna de las anteriores.

de la clave

m n

6 nºs (dado) cogidos de 4 en 4

— — — — }

sí importa orden
sí puede haber repetición

$\Rightarrow VR^m_n = m^n = 6^4$

$P(\text{cada clave posible}) = \frac{1}{6^4}$, son equiprobables. (dado OK)

$H = \overline{I} = \sum P(i) \cdot \log_2 \frac{1}{P(i)} = 6^4 \cdot \frac{1}{6^4} \cdot \log_2 6^4 =$

$= \log_2 6^4$ bits/símbolo

---

19. Sea $c(D) = D^6 + D + 1$ un polinomio primitivo de grado 6. Calcule $D^{195} \bmod C(D)$.

a) 1
b) D^3
c) $D + 1$
d) Ninguna de las anteriores

periodo $2^6 - 1 = 63$

$195 = 3 \cdot 63 + 6$

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