1. Información Clásica

EJERCICIOS

1.1 Un mensaje ordinario S se ha llevado a forma binaria asignando a cada símbolo del teclado su código ASCII escrito como número binario de siete bits (el primero de los cuales puede ser un 0), seguido de un bit de comprobación de paridad. Se ha obtenido así una larga cadena binaria M_2 representativa de S. Con el fin de acortar su expresión, damos a continuación la expresión hexadecimal M_{16} de M_2:

$M_{16} =$

9cc3e8ebe4ca41d2e7dd4ee841c6d8c3e7e7d2c6c3d85941c9
c3dbdbd2e85941c3ddc941d2cc41f3deeb41eec3dde841e8de
41dbc3d7ca41c341e7d2dbebd8c3e8d2dedd41decc41ddc3e8
ebe4ca5941f3deeb4ec941c5cae8e8cae441dbc3d7ca41d2e8
41e2ebc3dde8ebdb41dbcac6d1c3ddd2c6c3d85941c3ddc941
c5f341cfded8d8f341d2e84ee741c341eededdc9cae4ccebd8
41e1e4dec5d8cadb5941c5cac6c3ebe7ca41d2e841c9decae7
dd4ee841d8deded741e7de41cac3e7f35c4150a55c418dcaf3
dddbc3dd53

Hallar S.

1.2 Sean X, Y, Z tres variables aleatorias discretas, con resultados respectivos

$$\{x_1, x_2, ..., x_m\}, \quad \{y_1, y_2, ..., y_n\}, \quad \{z_1, z_2, ..., z_r\},$$

siendo $m = 5, n = 10, r = 15$.

Si las probabilidades conjuntas $p_{i,j,k} := \text{prob}(X = x_i, Y = y_j, Z = z_k)$ son proporcionales a $1/(i+j+k)^2$, calcular:

$$H(X,Y,Z), H(X,Y), H(Y,Z), H(X,Z), H(X), H(Y), H(Z),$$
$$H(X,Y|Z), H(X,Z|Y), H(Y,Z|X), H(X|Y,Z), H(Y|X,Z), H(Z|X,Y),$$
$$H(X,Y:Z), H(X,Z:Y), H(Y,Z:X),$$
$$H(X:Y), H(X:Z), H(Y:Z).$$

A la vista de los resultados, comentar qué propiedades sugieren estos resultados sobre la entropía y sus derivados.

1.3 Sea la variable aleatoria $\Sigma_{\text{español}} = \{-,A,B,C,...,Ñ,...X,Y,Z\}$ con la distribución de probabilidad contenida en esta relación:

```
{{0.1864,  -}, {0.0974, A}, {0.0075, B}, {0.0238, C},
{0.056, D}, {0.1367, E}, {0.0042, F}, {0.0059, G},
{0.0072, H}, {0.0338, I}, {0.0024, J}, {0., K},
{0.0682, L}, {0.0173, M}, {0.0571, N}, {0.0024, Ñ},
{0.0708, O}, {0.0226, P}, {0.0125, Q}, {0.0402, R},
{0.0642, S}, {0.027, T}, {0.0391, U}, {0.0032, V},
{0., W}, {0.0004, X}, {0.0125, Y}, {0.0012, Z}}
```

donde – denota el espacio vacío.

1/ Hallar, con los convenios normativos comentados en clase, el código Huffman ternario de $\Sigma_{\text{español}}$, y su longitud media L. Atención: no incluir en la obtención del código las letras K y W, de probabilidades nulas. (Comprobación: Z $\rightarrow$ 100112)

2/ Codificar con este código el siguiente texto:

EL-SECRETO–DE–UNA-BUENA–VEJEZ–NO–ES–OTRA–
COSA–QUE–UN–PACTO–HONRADO–CON–LA–SOLEDAD

Llamemos c al resultado obtenido. Es una cadena de trits (0,1,2).

3/ Interpretada la cadena anterior c como la forma ternaria de un entero $n(c)$, escribir $n(c)$ en base 10.

4/ Descodificar la siguiente cadena ternaria de palabras código Huffman concatenadas:

```
12020001202101121211201200010021011212112101012112
00120220011010110012101022101100002012000111012112
00102021000111112101111101200110120001101010210110
10212021011201000100200110012022001101011110110101
12012022001101201101011111010020120 22
```

y comprobar que la afirmación que expresa es cierta.

1.4 Sea Q un canal con la siguiente matriz 15×15 de probabilidades de transición:

$$Q = \frac{1}{33} \begin{pmatrix} 4&4&4&4&6&4&6&4&4&4&3&4&4&4&6 \\ 2&3&2&3&3&3&2&1&2&1&1&1&1&2&3 \\ 3&1&2&3&1&3&2&1&2&2&3&3&1&2&1 \\ 1&3&1&1&3&2&3&2&3&1&2&1&2&3&2 \\ 6&6&6&3&3&6&4&6&3&3&4&3&6&3&3 \\ 3&3&3&6&4&3&3&3&6&6&6&6&3&6&4 \\ 1&0&0&0&2&2&0&1&2&2&0&1&2&2&0 \\ 3&1&1&2&1&1&3&2&3&2&3&2&2&3&1 \\ 2&1&1&1&1&1&2&2&1&0&1&0&1&0&1 \\ 1&2&2&2&1&2&2&2&2&2&1&2&2&1&1 \\ 1&2&3&1&2&2&1&3&1&3&2&3&3&1&2 \\ 2&2&2&1&2&2&1&1&2&1&2&2&1&2&2 \\ 2&1&1&2&2&1&2&2&1&2&2&1&2&2&2 \\ 2&2&3&2&2&1&1&3&1&3&1&2&3&1&3 \\ 0&2&2&2&0&0&1&0&0&1&2&2&0&1&2 \end{pmatrix}$$

Se pide:

1/ La capacity $C(Q)$ de este canal Q.
(Ayuda: usar, si se desea, el algoritmo de Arimoto-Blahut (ver, por ejemplo, www.rle.mit.edu/rgallager/documents/notes4.pdf).)

2/ Una distribución óptima p^* de entrada. ¿Era de esperar?

3/ Mostrar, mediante sendos ejemplos, que con este canal concreto la entropía del alfabeto $p := Q.q$ saliente puede ser unas veces mayor, y otras veces menor, que la entropía del alfabeto entrante q.

4/ Argumentar que esto no ocurre cuando la matriz de canal es doblemente estocástica.

1.5 Sea $H_3(3) \subset \mathbb{F}_3^{13}$ el código Hamming ternario (es decir, sobre el cuerpo $\mathbb{F}_q$, con $q = 3$. Es un código lineal $[n = 1 + q + ... + q^{r-1} = 13, k = n - r = 10, d = 3]_q$, con $r = 3$. Su matriz de control de paridad H es $r \times n$, cuyas columnas pueden tomarse como las ternas de coordenadas de un elemento representativo de cada subespacio unidimensional del espacio lineal F_q^r, esto es, F_3^3. Una elección simple para el caso $q = 3$ consiste en tomar todas las ternas no nulas de elementos 0,1,2 tales que el de más arriba (en H) no nulo sea 1. Se pide:

1/ Escribir la matriz H, ordenando sus columnas de modo que los enteros representados en forma ternaria por esas columnas formen una sucesión creciente.

2/ Escribir una matriz generatriz G, de dimensiones $k \times n$, cuyas filas son las coordenadas de una base cualquiera del F_3^{10} ortogonal a todas las filas de H. Para ello seguir este procedimiento: permutar las columnas de H de modo que H pasa a ser $\bar{H}$ de la forma $\bar{H} = (A, \mathbf{1}_{n-k})$, donde A es una matriz $(n-k) \times k$; hecho eso, una posible matriz $\bar{G}$ es $\bar{G} = (\mathbf{1}_k, -A^{\mathrm{t}})$, y deshaciendo sobre $\bar{G}$ las permutaciones efectuadas para ir de H a $\bar{H}$, obtenemos una G.

3/ Con esa G así conseguida, definir como palabras código base $c_j, j = 1, ..., 10$, las 10 filas de G. Para codificar un mensaje ternario, descomponerlo en bloques de longitud 10 (anteponiendo al principio los ceros precisos); codificar cada bloque $(b_1, ..., b_{10})$ de estos asignándole la suma vectorial $\sum_j b_j c_j$ en F_3^{13}.

4/ Un cierto entero n se lleva a base 3, y la cadena ternaria se codifica con $H_3(3)$ en la forma indicada, obteniéndose un resultado que, al ser transmitido por el canal, llega como

```
2001122212211101012021212121022200010012012201 1
2210020122210222012222201121010100022110101210112 1
2021
```

La transmisión ha corrompido alguno de los trits en los diversos bloques de codificación. Supóngase que en cada bloque ha cambiado a lo sumo uno de sus 13 trits. Detectarlos, corregirlos, y averiguar qué entero n se codificó.

1.6 Sea $f : \mathbb{Z}_2^4 \to \mathbb{Z}_2^4$ la siguiente aplicación booleana:

$$\begin{aligned} f: \quad & (x,y,z,t) \to \\ & (x+tyz, y+txz+tyz, z+txy+txz, t+txy+xyz). \end{aligned}$$

Se pide:

1. ¿Es reversible?

2. Probar que si C_{ijk}CNOT es la puerta de $\mathbb{Z}_2^4 \to \mathbb{Z}_2^4$ en que los bits i, j, k, terna ordenada de 1,2,3,4, son bits de control mientras el restante l hace de bit diana (por ejemplo, C_{134}CNOT: $(x_1, x_2, x_3, x_4) \mapsto (x_1, x_1x_3x_4 + x_2, x_3, x_4)$), entonces

$$f = \mathrm{C}_{123}\mathrm{CNOT} \circ \mathrm{C}_{124}\mathrm{CNOT} \circ \mathrm{C}_{134}\mathrm{CNOT} \circ \mathrm{C}_{234}\mathrm{CNOT}$$

3. Diseñar un circuito lógico que implemente f, y que solo use en su construcción las puertas primitivas del conjunto básico {AND, NOT, OR, COPY}.