TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Curso 2024-25

Hoja nº 6

1. a) Estamos llamando por teléfono utilizando (el subcódigo de las palabras que no incluyen el 10) el código sobre $\mathbb{F}_{11}$ con matriz comprobadora de paridad:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}.$$

¿Qué hará nuestro teléfono inteligente si marcamos 20617960587? [Parte del ejercicio es pensar qué es eso del "teléfono inteligente".]

b) Demuestra que, si en vez de un subcódigo de un código sobre $\mathbb{F}_{11}$, utilizásemos para llamar por teléfono el código <u>decimal</u> (esto es, sobre $\mathbb{Z}/10\mathbb{Z}$)

$$C := \left\{ (x_1, \ldots, x_{10}) \in (\mathbb{Z}/10\mathbb{Z})^{10} \ : \ \sum_{i=0}^{10} x_i \equiv 0 \,(\text{mód } 10), \ \sum_{i=0}^{10} i x_i \equiv 0 \,(\text{mód } 10) \right\},$$

no podríamos corregir todos los errores simples.

2. Cada habitante de Noruega tiene un número de identificación de 11 cifras, $x_1 \cdots x_{11}$, donde $x_1 \cdots x_6$ es la fecha de nacimiento, $x_7 x_8 x_9$ es un número personal, y x_{10} y x_{11} son dígitos de control definidos por:

$$\begin{aligned} &3x_{10} \equiv -(2x_9 + 5x_8 + 4x_7 + 9x_6 + 8x_5 + x_4 + 6x_3 + 7x_2 + 3x_1) \,(\text{mód } 11) \\ &x_{11} \equiv -(2x_{10} + 3x_9 + 4x_8 + 5x_7 + 6x_6 + 7x_5 + 2x_4 + 3x_3 + 4x_2 + 5x_1) \,(\text{mód } 11). \end{aligned}$$

Escribe una matriz comprobadora de paridad para este código sobre $\mathbb{F}_{11}$. Si el código se utiliza unicamente para detectar errores, ¿se detectarán todos los errores dobles? Si no es así, ¿cuáles no se detectan?

3. Escribe una matriz comprobadora de paridad y encuentra la dístancia mínima del código binario generado por G_1, del código sobre $\mathbb{F}_3$ generado por G_2 y del código sobre $\mathbb{F}_5$ generado por G_3, donde

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad G_2 = \begin{pmatrix} 1 & 2 & 0 & 2 & 1 & 0 \\ 2 & 0 & 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 2 & 1 & 2 \end{pmatrix} \qquad G_3 = \begin{pmatrix} 1 & 2 & 4 & 0 & 3 \\ 0 & 2 & 1 & 4 & 1 \\ 2 & 0 & 3 & 1 & 4 \end{pmatrix}$$

4. a) Construye tablas de Slepian para los códigos binarios generados por

$$G_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad G_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

b) Supón que estas utilizando el código generado por G_3 para corregir errores. Si recibes los vectores 11111 y 01011, ¿cómo los decodificarías? Da un ejemplo de un error doble en una palabra que se corrija y de un error doble que no se corrija.

5. a) Comprueba que el código ternario generado por la matriz $\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}$ es perfecto.

b) Utiliza decodificación por el síndrome para decodificar los vectores recibidos 2121, 1201 y 2222.

6. Consideramos el código lineal binario que tiene como matriz generadora

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

a) Calcula su parámetros y demuestra que se puede utilizar para corregir un error y detectar tres.
b) Empleamos este código para transmitir palabras castellanas que se pueden escribir con las siguientes ocho letras: A, B, E, I, L, M, N, S [por supuesto, esto es para simplificar el problema y no tener que utilizar códigos demasiado largos]. Para ello, hacemos corresponder a cada letra un vector de $\mathbb{F}_2^3$ como sigue, A=000, B=001, E=010, I=011, L=100, M=110, N=111, S=101, y antes de transmitir codificamos la letra que corresponde al vector $x = (x_1, x_2, x_3)$ como $xG \in \mathbb{F}_2^7$. Si estás utilizando un canal que no permite retransmitir ¿que leerías si recibes el siguiente mensaje $0011111, 0110110, 0001111, 1111000$ (las comas separan las letras)?

7. Estamos transmitiendo mensajes escritos en el alfabeto castellano de 27 letras (con Ñ y W). Como el canal tiene ruido, decidimos utilizar el siguiente código sobre $\mathbb{F}_3$: escribimos las letras como números de tres cifras en base 3, A=000, B=001, C=002, D=010,..., W=212, X=220, Y=221, Z=222, y codificamos la letra $x_1x_2x_3$ como el vector de $\mathbb{F}_3^6$ dado por

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1, x_2, x_3)G, \quad \text{donde} \quad G = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 0 & 2 & 2 \end{pmatrix}.$$

a) Escribe la matriz comprobadora de paridad H y encuentra los parámetros n, k y d del código definido por G.
b) Estás utilizando el código, y hablando de Matemáticas recibes el mensaje

$$000000, 100201, 020101, 010021, 001022, 100110, 000000$$

(las comas están sólo para que te sea más fácil separar las letras). ¿Qué te han querido decir?

8. a) Transmitimos utilizando el código $Ham(3, 2)$ y recibes el mensaje 0111001. ¿Qué harías si estás utilizando el código para corregir errores? ¿Y si estás unicamente interesado en la detección de errores?
b) Las mismas preguntas suponiendo que el vector recibido es 0110011.

9. El código $Ham(3, 2)$ tiene $d = 3$, y por tanto, si se utiliza sólo para detectar, detecta todos los errores simples y dobles y no detecta todos los errores triples. Sin embargo, ¿puede detectar algún error triple? ¿Cuáles exactamente? ¿Qué puedes decir sobre su capacidad para detectar errores de pesos superiores?

10. a) Escribe una matriz comprobadora de paridad para el $[8, 6]_7$-código de Hamming y utilízala para decodificar 35234106 y 10521360.
b) Escribe una matriz comprobadora de paridad para el $[31, 28]_5$-código de Hamming.

11. Demuestra que el dual del código $Ham(2, q)$ es un $[q + 1, 2, q]$-código.

12. Construye un código lineal sobre $\mathbb{F}_{11}$ de longitud $n = 8$ que corrija un error y detecte dos, y que tenga la mayor cantidad posible de palabras.

13. a) Construye, o demuestra que no existe, un $[6, 3, 4]_5$-código.
b) Construye, o demuestra que no existe, un $[10, 7, 5]_{11}$-código.
c) Construye un código lineal perfecto sobre $\mathbb{F}_3$ con 3^{15} palabras y $d = 3$, o demuestra que tal código no existe.