Teoría de Códigos y criptografía
Curso 2009-2010

Hoja 7 (Códigos Lineales.)

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

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

¿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 $\mathbb{Z}/10\mathbb{Z}$)

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

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:

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

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. Sea $C := \{x \in \mathbb{F}_2^n \mid w(x) \text{ es par}\}$.

a) Demuestra que C es un código lineal. Sin buscar la matriz comprobadora de paridad H, ¿cuánto vale $d(C)$?

b) Encuentra H, calcula la dimensión de C y deduce que es un código MDS (un código lineal que satisface la cota de Singleton).

c) ¿Cuántos elementos tiene C? ¿Cuántos elementos tiene el conjunto $\{x \in \mathbb{F}_2^n \mid w(x) \text{ es impar}\}$?

4. 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 $G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$, $G_2 = \begin{bmatrix} 1 & 2 & 0 & 2 & 1 & 0 \\ 2 & 0 & 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 2 & 1 & 2 \end{bmatrix}$, $G_3 = \begin{bmatrix} 1 & 2 & 4 & 0 & 3 \\ 0 & 2 & 1 & 4 & 1 \\ 2 & 0 & 3 & 1 & 4 \end{bmatrix}$.

5. a) Construye tablas de Slepian para los códigos binarios generados por $G_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, G_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, G_3 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$.

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.

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

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

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

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

a) Calcula su parámetros y demuestra que se puede utilizar simultaneamente para corregir un error y detectar dos.

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, 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)?

8. Estamos transmitiendo mensajes escritos en el alfabeto castellano de 27 letras (con $\tilde{\text{N}}$ 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

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

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?

9. 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.

10. 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?

11. a) Escribe una matriz comprobadora de paridad para el $[8, 6]$-código de Hamming sobre $\mathbb{F}_7$ (recuerda, en $[n, k]$, n =longitud y k =dimensión) y utilízala para decodificar 35234106 y 10521360.

b) Escribe una matriz comprobadora de paridad para el $[31, 28]$-código de Hamming sobre $\mathbb{F}_5$.

12. Estamos utilizando el código de Hamming extendido $\widehat{Ham}(3, 2)$ y un algoritmo de decodificación incompleta. Si recibes los vectores 11100000, 01110000, 11000000 y 00110011, ¿cómo los decodificarías?

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

14. a) Demuestra que $A_2(6, 3) = 8$. [SUGERENCIA: para la construcción de un $(6, 8, 3)$-código binario utiliza algo parecido a la construcción de $Ham(3, 2)$.]

b) ¿Cuánto vale $A_2(7, 4)$? Construye, si es posible, un $(7, 8, 4)$- código binario.

c) ¿Cuánto vale $A_2(8, 4)$? Construye, si es posible, un $(8, 16, 4)$- código binario.

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

16. a) Construye, o demuestra que no existe, un $[6, 3, 4]$-código sobre $\mathbb{F}_5$.

b) Construye, o demuestra que no existe, un $[10, 7, 5]$-código sobre $\mathbb{F}_{11}$.

c) Construye un código lineal perfecto sobre $\mathbb{F}_3$ con 3^{15} palabras y $d = 3$, o demuestra que tal código no existe.

17. Supón que un cierto canal binario simétrico acepta palabras de longitud 7, y que sólo se observan los 8 típos de errores siguientes: 0000000, 0000001, 0000011, 0000111, 0001111, 0011111, 0111111, 1111111. Diseña un $[7, k]$-código lineal binario que corrija todos estos errores y que tenga una tasa de transmisión lo más alta posible.

18. Trabajamos con el código lineal sobre $\mathbb{F}_{11}$ definido por

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

Encuentra, o explica por qué no lo puedes encontrar, el vector de error correspondiente a cada uno de estos tres síndromes: $(2, 0, 2, 2), (3, 4, 9, 1), (6, 5, 0, 3)$.

19. Sea $C \subset \mathbb{F}_{13}^6$ el código lineal definido por la matriz $H = [h_{ij}]$ de dimensión 4×6 con $h_{ij} = (2j - 1)^{i-1}$ mód 13.

a) Escribe explícitamente la matriz H y calcula los parámetros d, k y M para el código C. Comprueba que C es un código MDS.

b) Recibes el mensaje $y = (4, 0, 0, 3, 0, 1)$. ¿Cuál crees que fue el mensaje x enviado? (Comprueba que, efectivamente, $x \in C$.)

c) Recibes el mensaje $y = (1, 9, 0, 9, 1, 0)$. ¿Cuál crees que fue el mensaje x enviado? (Comprueba que, efectivamente, $x \in C$.)

d) Recibes el mensaje $y = (1, 1, 1, 1, 1, 1)$. Explica por qué puedes asegurar que en la transmisión se han producido al menos tres errores.

20. *(El problema de la "quiniela con n partidos")*Apostamos sobre los posibles resultados de n partidos (de futbol normalmente): gana el equipo que juega en casa (1), empatan (X),

o gana el equipo que juega fuera de su campo (2). Tanto los resultados de los partidos como las posibles apuestas se pueden ver como vectores en $\mathbb{F}_3^n$ (basta con sustituir la X por un 0). Si hacemos una apuesta A y tras jugarse los partidos se produce un vector de resultados R, ganamos un premio de primera categoría si $A = R$, un premio de segunda categoría si A y R se diferencian en el resultado de un partido, y en general un premio de i-ésima categoría si $d(A, R) = i - 1$. (En España, olvidandose del llamado "pleno al 15"que tiene reglas especiales, se juega con $n = 14$ y sólo se pagan premios si $d(A, R) \leq 4$.)

El llamado problema de la "quiniela con n partidos.$^{\text{es}}$: ¿Cúal es el número mínimo de apuestas que hay que hacer para asegurarse un premio de segunda categoría? Llamemos a este número $f(n)$.

a) Interpreta el problema de la quiniela con n partidos en términos de recubrimientos por esferas.

b) Utiliza los códigos de Hamming ternarios para calcular $f(n)$ en el caso de que exista r tal que $n = (3^r - 1)/2$, esto es, para $n = 4, 13, 40, \ldots$.

c) Demuestra que $23 \leq f(5) \leq 27$. (De hecho se sabe que $f(5) = 27$, pero la prueba no es fácil.)

d) Podemos generalizar el problema y definir $f_i(n)$ cómo el mínimo número de apuestas necesario para garantizar un premio de i-ésima categoría. Interpreta la busqueda de este número como un problema de recubrimientos por esferas. Por supuesto, con la notación anterior, $f_2(n) = f(n)$. ¿Puedes explicar por qué el problema "clásico.$^{\text{es}}$ encontrar $f_2(n)$ y no $f_1(n)$? Explica cómo usar un código de Golay para demostrar que $f_3(11) = 3^6 = 729$.

e) Escribe un boleto de quinielas con el mínimo número de columnas (= apuestas) que te garantice acertar el resultado de al menos tres de los cuatro partidos siguientes:

ATLETICO DE MADRID - REAL MADRID
ESPANYOL - BARCELONA
SEVILLA - BETIS
LEVANTE - VALENCIA