Teoría de Códigos y criptografía
Curso 2009-2010

Hoja 6 (Teoría de Códigos. Introducción)

1. a) Encuentra el dígito de control (c) de los siguientes EAN: 5-449000-00099c,8-410240-32700c.

b) ¿Cuáles de los siguientes EAN puedes asegurar que son incorrectos?: 6-39844-06292-3, 9-780198-538095, 8-410420-327003.

c) Al leer un UPC se ha borrado un número (que representamos por una a) y hemos recibido 3-03a65-00879-5. ¿Cuánto vale a?

2. a) Encuentra el dígito de control (c) de los siguientes ISBN: 3-540-96311-c, 84-8310-055-c.

b) ¿Cuáles de los siguientes ISBN puedes asegurar que son incorrectos?: 84-293-5922-8, 0-19-853803-0, 84-230-5921-X, 12-345-678X-5.

c) Al recibir un ISBN se ha borrado un número (que representamos por una a) y hemos recibido 0-13-1a9139-9. ¿Cuánto vale a?

d) Al recibir un ISBN se han borrado parcialmente dos números (que representamos por a y b) y hemos recibido 0-02-32ab80-0. Somos capaces de ver la parte superior de a y b, y de ello deducimos que $a, b \in \{0, 8, 9\}$. ¿Cuánto valen a y b?

3. El NIF tiene la estructura $x_7x_6x_5x_4x_3x_2x_1x_0 - r$ con $x_i \in \{0, \ldots, 9\}$ y $r \equiv \sum_{i=0}^{7} 10^i x_i$ mód 23. Cada resto módulo 23 se representa por una letra de acuerdo con la tabla que se adjunta [no se utilizan I, Ñ,O, U].

a) Encuentra la letra de control de los siguientes NIF: $2631173 - r$, $841241 - r$.

b) ¿Cuáles de los siguientes NIF puedes asegurar que son incorrectos?: 2516344-A, 76105-Q, 2516344-Y.

c) Demuestra que esta estructura permite: detectar un error; detectar el intercambio de dos dígitos; recuperar un dígito (o la letra) borrado si se sabe qué posición ocupa.

d) Comprueba que el apartado c) seguiría siendo cierto si r se calculase módulo 17, pero no si se calculase modulo m con $m < 17$.

e) Al recibir un NIF se ha borrado un número (que representamos por una a) y hemos recibido $0330a082 - Q$. ¿Cuánto vale a?

4. Si al escribir un ISBN se olvida una cifra se detecta inmediatamente: el ISBN 12-345-678-9 es forzosamente incorrecto, porque un ISBN correcto tiene 10 cifras. Esto sucedería también con el NIF si siempre se escribiesen 8 cifras y una letra. Sin embargo es costumbre escribir el NIF 02516341-A simplemente como 2516341-A. Tomando esto en consideración, ¿hay NIFs en los que no se detecte el olvido de una cifra? ¿y de dos cifras consecutivas? ¿y de dos cifras no consecutivas?

5. El *Código de las Tarjetas de Crédito (CODABAR)*: El número de las tarjetas de crédito esta compuesto por 16 cifras a las que se exige que:

$2(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + a_{13} + a_{15}) + a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12} + a_{14} + a_{16}+$ número de dígitos en posición impar que son mayores que $4 \equiv 0 \mod 10$.

a) Comprueba que 4599-8834-3278-8311 y 4605-0521-5847-2052 son CODABARs correctos.

b) Estudia la capacidad de este código para: detectar un error; detectar dos errores; detectar una permutación de dos cifras; detectar una permutación de dos cifras consecutivas; corregir un error; recuperar un número borrado (sabiendo qué lugar ocupa).

6. El *Código de los Cheques*: Esta es una lista de números de cheques bancarios: 7.425.090.1, 7.425.091.2, 7.425.092.3, 7.425.093.4, 7.425.094.5, 7.425.095.6, 7.425.096.0, 7.425.097.1, 7.425.098.2, 7.425.099.3, 7.425.100.4, 7.425.101.5, 7.425.102.6, 7.425.103.0, 7.425.104.1.

a) Como puedes ver, si te olvidas de las últimas cifras son números consecutivos. De hecho corresponden a cheques consecutivos, y el último dígito es un dígito de control, es decir, estamos ante un código. ¿Puedes averiguar cómo se calcula el dígito de control de un número de cheque?

b) Estudia la capacidad de este código para: detectar un error; detectar dos errores; detectar una permutación de dos cifras; detectar una permutación de dos cifras consecutivas; corregir un error; recuperar un número borrado (sabiendo qué lugar ocupa).

7. Sea C el código binario de longitud n obtenido añadiendo a las palabras de longitud $n-1$ un comprobador de paridad global, o sea $C = \{x_1 \dots x_n \in \mathbf{F}_2^n \mid \sum_{i=1}^n x_i \equiv 0 \mod 2\}$. Demuestra que C es un $(n, 2^{n-1}, 2)$-código binario, y en particular que C siempre detecta un error. Encuentra todos los errores que pueden ser detectados por C.

8. Consideramos el código C de repetición de longitud 4 sobre el alfabeto de 29 letras $\mathbb{F}_{29} = \mathbb{Z}/29\mathbb{Z}$.

a) Demuestra que C permite, simultaneamente, corregir un error y detectar 2 en cada mensaje emitido.

b) Si hacemos corresponder los números 0 - 26 a las letras A - Z (incluyendo la Ñ y también la W) y además 27=¡, 28=!, y recibimos el siguiente mensaje (los guiones están solo para separar los números), 27 - 27 - 15 - 27 - 5 - 5 - 5 - 5 - 5 - 4 - 4 - 5 - 4 - 11 - 11 - 11 - 8 - 8 - 8 - 26 - 26 - 8 - 26 - 26 - 13 - 6 - 13 - 13 - 13 - 13 - 0 - 13 - 13 - 22 - 22 - 22 - 8 - 8 - 8 - 8 - 8 - 3 - 3 - 3 - 3 - 0 - 0 - 0 - 0 - 0 - 3 - 3 - 28 - 3 - 28 - 28, ¿qué interpretarias que nos quieren decir?

9. Utilizamos el código binario de repetición de longitud 5 para transmitir a traves de un canal binario simétrico con probabilidad de error en un símbolo p. Recibido un mensaje, siempre intentamos leerlo (es decir, lo usamos como código corrector). Demuestra que la probabilidad de decodificar erroneamente una palabra es $P_{err} = 10p^3 - 15p^4 + 6p^5$. ¿Aproximadamente con que frecuencia decodificaremos incorrectamente si $p = 0{,}1$? ¿Y si $p = 0{,}01$? Compara con lo que sucedería si utilizasemos el código binario de repetición de longitud 3, o si no codificásemos en absoluto.

10. Construye, o demuestra la no existencia, de (n, M, d)-códigos binarios con los siguientes parámetros: (6,2,6), (3,8,1), (4,8,2), (5,3,4), (8,30,3).

11. a) Demuestra que todo $(3, M, 2)$-código ternario debe tener $M \leq 9$.

b) Construye un $(3, M, 2)$-código ternario con $M = 9$ y concluye que $A_3(3, 2) = 9$.

c) Generaliza lo anterior y demuestra que para cualquier $q \geq 2$ se tiene $A_q(3, 2) = q^2$.

12. a) Demuestra que $A_2(4, 3) = 2$ y que, salvo equivalencia, existe un único (4,2,3)-código binario.

b) Demuestra que $A_2(8, 5) = 4$ y que, salvo equivalencia, existe un único (8,4,5)-código binario.

13. Demuestra que todo $(q+1, M, 3)$-código q-nario satisface $M \leq q^{q-1}$.

14. a) Demuestra que, si existe un (n, M, d)-código binario, entonces existe un $(n-1, M', d)$-código binario con $M' \geq M/2$. [Sugerencia: Clasifica las palabras según que la última letra sea 0 ó 1.]

b) Deduce de esto que $A_2(n, d) \leq 2A_2(n-1, d)$.

15. Demuestra que, si existe un (n, M, d)-código binario con d par, entonces existe un

(n, M, d)-código binario en el que todas las palabras tienen peso par. [Sugerencia: Primero acortar el código y luego alargarlo.]

16. a) Demuestra que si C es un código binario perfecto de longitud n con $d = 7$, entonces $n = 7$ o $n = 23$.

b) Construye un código binario perfecto de longitud $n = 7$ con $d = 7$. [Se puede también construir un código binario perfecto de longitud $n = 23$ con $d = 7$, pero es más difícil. Es uno de los llamados Códigos de Golay.]