TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Hoja nº 5

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

2. 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?

3. 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, <u>siempre</u> 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.

4. 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), (8,30,3).

5. 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 $A_q(3, 2) = q^2$.

6. 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.

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

8. 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 $A_2(n, d) \leq 2A_2(n - 1, d)$.

9. 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.]