

Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Ejemplos de Pruebas de Autoevaluación

Mayo de 2017

Prueba de autoevaluación: Modelo A**Curso OCW: Introducción a la Teoría de Códigos**

Teoría

1. **(2 ptos.)** Probar que el código dual C^\perp de un (n, k) -código cíclico $C \subseteq \mathbb{F}_q^n$ es cíclico y tiene dimensión $n - k$.

Problemas

1. Se considera el código lineal $C \subseteq \mathbb{F}_3^8$, cuya matriz generadora es

$$G = \begin{pmatrix} 1 & 2 & 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 & 2 & 0 & 1 \end{pmatrix}.$$

- a) **(1,5 ptos.)** Localiza, si es posible, una matriz generadora de C que esté dada en forma estándar y una matriz de control de C .
 - b) **(1 pto.)** Demuestra que la distancia mínima de C es 4.
 - c) **(1 pto.)** ¿Es C cíclico?. En caso de que lo sea, calcula su polinomio generador.
2. Se considera el código lineal $C_1 \subseteq \mathbb{F}_3^8$, dado por

$$C_1 = \langle 00111201, 01220211, 12121212, 10122021 \rangle.$$

- a) **(1.5 ptos.)** Demuestra que C_1 es cíclico y calcula su polinomio de control. ¿Cuál es la dimensión de C_1 ?
- b) **(1 pto.)** Calcula una matriz generadora y un polinomio generador de C_1^\perp .
- c) **(1 pto.)** ¿Es C_1 autoortogonal?
- d) **(1 pto.)** Decodifica la palabra 01001110. ¿Es única su decodificación? Razona la respuesta.

Ayuda: La descomposición en factores irreducibles sobre \mathbb{F}_3 de $x^8 - 1$ es

$$(1 + x)(2 + x)(1 + x^2)(2 + x + x^2)(2 + 2x + x^2).$$

Prueba de autoevaluación: Modelo B**Curso OCW: Introducción a la Teoría de Códigos**

Teoría

1. **(2 ptos.)** Probar la existencia y unicidad del polinomio generador de un código cíclico $C \subseteq \mathbb{F}_q^n$ y que éste es un divisor de $x^n - 1$.

Problemas

1. Se considera el código lineal $C \subseteq \mathbb{F}_5^5$, cuya matriz de control viene dada por

$$H = \begin{pmatrix} 0 & 4 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & 0 \end{pmatrix}.$$

- a) **(1 pto.)** Hallar su distancia mínima.
- b) **(1,5 ptos.)** Decodificar la palabra 12031. ¿Tiene decodificación única?
- c) **(1 pto.)** ¿Existe alguna palabra de C que no tenga decodificación única? Razona tu respuesta.
- d) **(2 ptos.)** ¿Es C cíclico? En caso de respuesta afirmativa, calcula su polinomio generador y una matriz generadora.

Ayuda: La descomposición en factores irreducibles sobre \mathbb{F}_5 de $x^5 - 1$ es $(4+x)^5$

2. **(2,5 puntos)** Sea $C \subseteq \mathbb{F}_q^n$ un código lineal de dimensión k que corrige errores $\mathbf{e} \in \mathbb{F}_q^n$ tales que $w(\mathbf{e}) \leq t$. Probar que $2t + k \leq n$.

Prueba de autoevaluación: Modelo C**Curso OCW: Introducción a la Teoría de Códigos**

Teoría:

1. **(2 ptos.)** Definir distancia de Hamming y código perfecto. Enunciar y probar la Cota de Hamming.

Problemas:

1. Se considera el código binario C cuya matriz de control es:

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

- a) **(1,5 ptos.)** Hallar una matriz generadora de C .
 - b) **(0,5 ptos.)** Probar que 11101000 pertenece a C .
 - c) **(1,5 pto.)** ¿Es C un código autodual?
 - d) **(1,5 ptos.)** Calcular un código cíclico C_1 de menor dimensión posible que contenga a 11101000.
 - e) **(1,5 pto.)** ¿Es $\dim(C_1 \cap C) > 1$?
2. **(1,5 pto.)** Sea $C \subseteq \mathbb{F}_q^n$ un código lineal de dimensión k y distancia mínima d . Si $n = 15$ y $k = 6$, probar que C no corrige 5 errores o más.