Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Solución a los problemas de la Prueba de Autoevaluación: Modelo C

Mayo de 2017

Prueba de autoevaluación: Modelo C

Solución a los problemas

Curso OCW: Introducción a la Teoría de Códigos

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 $\dim(C_1 \cap C) > 1$?*

Solución

a) Sumando a la cuarta fila las otras tres filas, obtenemos otra matriz de control de H que es

$$H_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

y, reordenando las filas de H_1, obtenemos otra matriz de control de C que viene dada por

$$H_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Como H_2 está dada en forma estándar, podemos deducir que una matriz generadora de C es

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

b) La palabra 11101000 está en C ya que es la primera fila de la matriz G (recordemos que en una matriz generadora van los vectores de una base de C). Otra forma de demostrar que 11101000 está en C es comprobar que su síndrome es (0 0 0 0), esto es,

$$S(11101000) = (1\ 1\ 1\ 0\ 1\ 0\ 0\ 0)H^t = (0\ 0\ 0\ 0).$$

c) C es autodual si $C = C^\perp$. Ahora, dado $\mathbf{c} \in C$ sabemos que $\mathbf{c}$ pertenece a $C^\perp$ si

$$\mathbf{c}G^t = (0\ 0\ 0\ 0).$$

Por ello, para estudiar si $C \subseteq C^\perp$, es suficiente con estudiar si $GG^t = 0$ y como esto se cumple, deducimos que $C \subseteq C^\perp$ y al ser la dimensión de ambos códigos 4, deducimos que C es autodual.

d) Tenemos que a 11101000 le corresponde el polinomio $1 + x + x^2 + x^4$, que se escribe como producto de irreducibles sobre $\mathbb{F}_2$ de la manera siguiente:

$$1 + x + x^2 + x^4 = (1 + x)(1 + x^2 + x^3).$$

Por otro lado, la descomposición en factores irreducibles sobre $\mathbb{F}_2$ de $x^8 - 1$ es $(1 + x)^8$. Por tanto,

$$\text{mcd}\{1 + x + x^2 + x^4, x^8 - 1\} = 1 + x$$

y el código cíclico de menor dimensión que contiene a 11101000 es el que tiene por polinomio generador a $1 + x$.

e) $\dim(C_1 \cap C)$ es mayor que 1 ya que la palabra 11010100 de C (y en general cualquiera de peso par de C) también pertenece a C_1 porque

$$1 + x + x^3 + x^5 = (1 + x)(1 + x^3 + x^4)$$

y, como $\{11010100, 11101000\}$ es un conjunto libre, se sigue que $\dim(C_1 \cap C)$, que contiene a $< 11010100, 11101000 >$, es mayor o igual que 2.

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 corrije 5 errores o más.*

Solución

Supongamos, por reducción al absurdo, que C corrije al menos 5 errores. Entonces, la distancia mínima de C es al menos 11. Entonces, por la Cota de Singleton se debe verificar

$$11 \leq 15 - 6 + 1 = 10,$$

lo cual es absurdo. Por tanto, C no corrije 5 errores o más.