eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

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 B

Mayo de 2017

Prueba de autoevaluación: Modelo B

Solución a los problemas

Curso OCW: Introducción a la Teoría de Códigos

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.)** *¿Es C perfecto? Razona tu respuesta.*

d) **(2 ptos.)** *¿Es C cíclico? En caso de respuesta afirmativa, calcula su polinomio generador y una matriz generadora.*

Solución

a) Para calcular la distancia mínima aplicamos la Proposición 3.5 del Tema 3. Observamos que dos columnas cualesquiera de H son linealmente independientes y que las columnas primera, segunda y quinta son linealmente dependientes, por lo que la distancia mínima es 3.

b) Empleamos el método de decodificación mediante síndromes. Tenemos que:

$$\begin{aligned} S(12031) &= (1\ 2\ 0\ 3\ 1)H^t \\ &= (1\ 2\ 0\ 3\ 1)\begin{pmatrix} 0 & 4 \\ 4 & 3 \\ 3 & 2 \\ 2 & 1 \\ 1 & 0 \end{pmatrix} \\ &= (0\ 3). \end{aligned}$$

Entonces, 12031 no es una palabra del código C. Pero $S(12031)$ coincide con $S(20000)$, así que ambas palabras tienen el mismo síndrome. Además, 20000 es la única palabra de peso 1 que tiene ese síndrome, por lo que es líder en su clase de equivalencia. Por tanto, la decodificación de 12031, que es única, viene dada por

$$\mathbf{c} = 12031 - 20000 = 42031.$$

c) Para que C sea perfecto, debemos comprobar si C alcanza la cota de Hamming. Ahora, C es un código de dimensión 3 porque la matriz de control H es de tamaño 2×5, luego

$$|C| \sum_{i=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{i} (m-1)^i = 5^3 \sum_{i=0}^{1} \binom{5}{i} (5-1)^i = 5^3(1+20) < 5^5.$$

Por consiguiente, C no es perfecto.

d) Sabemos que C es cíclico si y, solo si, $C^\perp$ es cíclico. Por ello, vamos a estudiar si $C^\perp$ es cíclico. Sabemos que $C^\perp$ tiene por matriz generadora a $H = \begin{pmatrix} 0 & 4 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & 0 \end{pmatrix}$, por lo que una base de $C^\perp$ es $\{04321, 43210\}$. Pero $C^\perp$ es cíclico si las traslaciones cíclicas de una base son elementos de $C^\perp$. Ahora, la traslación cíclica de 04321 es 10432 y pertenece a $C^\perp$ ya que podemos encontrar $\alpha, \beta \in \mathbb{F}_5$ tales que

$$10432 = \alpha 04321 + \beta 43210 \Rightarrow \begin{cases} 1 = 4\beta \\ 0 = 4\alpha + 3\beta \\ 4 = 3\alpha + 2\beta \\ 3 = 2\alpha + \beta \\ 2 = \alpha \end{cases} \Rightarrow \alpha = 2,\ \beta = 4.$$

Por otro lado, la traslación cíclica de 43210 es 04321, que también pertenece a $C^\perp$. Por tanto, $C^\perp$ es cíclico y también lo es C. Finalmente, como C es cíclico de dimensión 3 y solo hay un código cíclico en $\mathbb{F}_5^5$ de dimensión 3, que es el que está generado por el polinomio $(x+4)^2 = x^2 + 3x + 1$, una matriz generadora de C es

$$G = \begin{pmatrix} 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 3 & 1 \end{pmatrix}.$$

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 $2t + k \leq n$.*

Solución

Como C corrije errores de peso hasta t, significa que si d es la distancia mínima de C, entonces

$$t = \left[\frac{d-1}{2}\right] \leq \frac{d-1}{2} \Rightarrow 2t \leq d-1$$

Pero sabemos que $d-1$ es menor o igual que el rango de H matriz de control de C, luego

$$2t \leq d - 1 \leq \operatorname{rg} H = n - k \Rightarrow 2t + k \leq n.$$