OCW
OpenCourseWare

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

Resumen Teórico
Apartado 3 del Tema 3:
Matriz de control de un código lineal. Código dual de un código lineal

Mayo de 2017

3 Matriz de control de un código lineal. Código dual de un código lineal

En el espacio vectorial $\mathbb{F}_q^n$ disponemos del producto escalar siguiente:

$$\forall \mathbf{x} = x_1 \dots x_n, \mathbf{y} = y_1 \dots y_n \in \mathbb{F}_q^n,\ \mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i$$

y dado $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal sobre $\mathbb{F}_q$, definimos

$$C^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n \,|\, \mathbf{x} \cdot \mathbf{y} = 0, \forall \mathbf{y} \in C\}.$$

Empleando las propiedades de los subespacios vectoriales, se demuestra:

Proposición 3.1 *Si $C \subseteq \mathbb{F}_q^n$ es un (n,k)-código lineal, entonces $C^{\perp}$ es un código lineal de $\mathbb{F}_q^n$.*

Si $C \subseteq \mathbb{F}_q^n$ es un (n,k)-código lineal, entonces a $C^{\perp}$ se le conoce como el **código dual** de C. Se pueden caracterizar de forma sencilla los elementos de $C^{\perp}$, si conocemos una matriz generadora de C. En efecto, se puede demostrar el siguiente lema

Lema 3.2 *Sea $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal con matriz generadora G y $C^{\perp}$ su código dual. Entonces, $\boldsymbol{x} \in C^{\perp}$ si y sólo si $\boldsymbol{x}G^t = 0$.*

Esta caracterización de los elementos del código dual nos va a servir para calcular la dimensión de $C^{\perp}$:

Proposición 3.3 *Si $C \subseteq \mathbb{F}_q^n$ es un (n,k)-código lineal, entonces $C^{\perp}$ es un código lineal de dimensión $n-k$.*

En resumen, si $C \subseteq \mathbb{F}_q^n$ es un (n,k)-código lineal, sabemos que $C^{\perp}$ es otro código lineal de longitud n y dimensión $n-k$. Por otro lado, $C^{\perp}$ admite una matriz generadora $H \in \mathrm{Mat}_{(n-k)\times n}(\mathbb{F}_q)$, por ser $C^{\perp}$ un código lineal. A esta matriz H, generadora de $C^{\perp}$, se le llama **matriz de control (de paridad)** de C.

Además, de la definición y de las propiedades del código dual, se deduce que si C es un (n,k)-código lineal y $C^{\perp}$ su código dual, entonces $(C^{\perp})^{\perp} = C$. Entonces, si H es la matriz de control de C, podemos caracterizar C, vía H, de la siguiente manera:

$$C = \{\mathbf{z} \in \mathbb{F}_q^n \,|\, \mathbf{z}H^t = 0\}.$$

Por otro lado, también se cumple que si G y H son matrices generadoras y de control de un (n,k)-código lineal, entonces $GH^t = 0$.

Esta última propiedad nos servirá para localizar una matriz de control cuando la matriz generadora de un código lineal está dada en forma estándar, tal y como enunciamos en el siguiente resultado:

Proposición 3.4 *Sea $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal con matriz generadora $G = (I_k|B)$. Entonces, una matriz de control para C es $H = (-B^t|I_{n-k})$.*

Ejemplo Consideremos el código $C = \{(x_1, ..., x_n) \in \mathbb{F}_q^n \mid x_1 + \cdots + x_n = 0\}$, que es un $(n, n-1)$-código lineal sobre $\mathbb{F}_q$. Si tomamos el conjunto

$$\{(1,0,0,\ldots,0,0,-1),(0,1,0,\ldots,0,-1),\ldots,(0,0,0,\ldots,0,1,-1)\},$$

resulta que es una base de C, por lo que la matriz

$$G = \begin{pmatrix} 1 & 0 & \ldots & 0 & -1 \\ 0 & 1 & \ldots & 0 & -1 \\ & & \ddots & & \\ 0 & 0 & \ldots & 1 & -1 \end{pmatrix}$$

es una matriz generadora de C que además está dada en forma estándar. Entonces, si aplicamos la Proposición 3.4, la matriz de control de C será

$$H = (1\ 1\ \ldots\ 1\ 1).$$

Esto implica que $C^\perp$ va a ser de dimensión 1 y, obviamente, la condición que debe cumplir un elemento $(x_1, ..., x_n)$ de $\mathbb{F}_q^n$ para estar en C es

$$(x_1, ..., x_n)H^t = 0 \ \Rightarrow\ x_1 + \cdots + x_n = 0.$$

Finalmente, la matriz de control de un (n,k)-código lineal también nos sirve para determinar la distancia mínima de un código lineal:

Proposición 3.5 *Sea $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal con matriz de control H. Entonces, la distancia mínima de C es d si y, solo si, cualesquiera $d-1$ columnas de H son linealmente independientes y existen d columnas de H linealmente dependientes*

De la proposición anterior podemos deducir que el rango de H es al menos $d-1$. Luego si $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal con distancia mínima d, se tiene la siguiente desigualdad, conocida como **Cota de Singleton**:

$$d - 1 \leq \mathrm{rg}(H) = n - k \ \Rightarrow\ d \leq n - k + 1.$$

Ejemplo Si consideremos el código $C = \{(x_1, ..., x_n) \in \mathbb{F}_q^n \mid x_1 + \cdots + x_n = 0\}$, que es un $(n, n-1)$-código lineal sobre $\mathbb{F}_q$, sabemos que $H = (1\ 1\ \ldots\ 1\ 1)$ es una matriz de control de C, luego por la Proposición 3.5 deducimos que la distancia mínima de C es 2. Observamos que en este caso se da la igualdad en la Cota de Singleton.