Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Resumen Teórico
Apartado 1 del Tema 4:
Definición y construcción de códigos cíclicos

Mayo de 2017

1 Definición y construcción de códigos cíclicos

Sea $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal. Se dice que C es **cíclico** si se satisface la siguiente propiedad:

$$\forall c_0 \dots c_{n-1} \in C,\ c_{n-1}c_0 \dots c_{n-2} \in C.$$

Observamos que si C es un código cíclico, entonces dada $c_0 \dots c_{n-1} \in C$, se tiene que las palabras $c_{n-1}c_0 \dots c_{n-2}$, $c_{n-2}c_{n-1}c_0 \dots c_{n-3}$, $\dots$, y $c_1 \dots c_{n-1}c_0$ están también en C.

Por otro lado, también podemos caracterizar los códigos cíclicos fijandonos solamente en lo que sucede en una base del código, tal y como se indica en el siguiente resultado:

Proposición 1.1 (Caracterización de los códigos cíclicos) *Sea $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal con base $\mathcal{B} = \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_k\}$. Entonces, C es cíclico si y, solo si, para todo $\boldsymbol{x}_i \in \mathcal{B}$, con $i = 1, \dots, k$, se tiene $x_{in-1}x_{i0} \dots x_{in-2} \in C$, siendo $\boldsymbol{x}_i = x_{i0} \dots x_{in-2}x_{in-1}$.*

Si dada una palabra $\mathbf{x} = x_0 \dots x_{n-1} \in \mathbb{F}_q^n$ llamamos a $x_{n-1}x_0 \dots x_{n-2}$ la **traslación cíclica** de $\mathbf{x}$, la proposición anterior nos indica que un código lineal es cíclico si y, solo si, la traslación cíclica de las palabras de una base están también en C. Esta caracterización nos simplificará el estudio de si un código es cíclico, cuando conozcamos una base del mismo.

Ejemplo Sea $C \subseteq \mathbb{F}_2^7$ el código lineal cuya matriz generadora viene dada por: $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$. Entonces, una base de C es

$$\mathcal{B} = \{1101000, 0110100, 0011010, 0001101\}$$

y para las tres primeras palabras de esta base se cumple que sus traslaciones cíclicas son otra palabra de la misma base, por lo que también son palabras de C. Por tanto, solo nos queda estudiar lo que sucede con la traslación cíclica de la última palabra de la base, que es 0001101. Ahora, como estamos trabajando en $\mathbb{F}_2$, se cumple que

$$1000110 = 1101000 + 0110100 + 0011010,$$

así que la traslación cíclica de la última palabra de la base es también otra palabra de C. Por consiguiente, aplicando la Proposición 1.1, podemos afirmar que C es un código cíclico.

Además de la caracterización que hemos visto de los códigos cíclicos estudiando únicamente lo que sucede en un base, vamos a encontrar otra fijandonos en una

estructura subyacente de los códigos cíclicos. Para ello, necesitamos recordar cómo se contruye el anillo cociente $\mathbb{F}_q[x]/(x^n-1)$, donde $\mathbb{F}_q[x]$ el anillo de los polinomios en la variable x, y se puede relacionar con $\mathbb{F}_q^n$. En $\mathbb{F}_q[x]$ definimos la relación de equivalencia

$$\forall f(x), g(x) \in \mathbb{F}_q[x], \quad f(x)\mathfrak{R}g(x) \Leftrightarrow (x^n-1)|f(x)-g(x),$$

esto es, $f(x)-g(x)$ es múltiplo de x^n-1. Entonces el conjunto cociente, denotado por $\mathbb{F}_q[x]/(x^n-1)$, está definido por

$$\mathbb{F}_q[x]/(x^n-1) = \{\overline{f(x)} \mid f(x) \in \mathbb{F}_q[x]\}$$

y en cada clase de equivalencia $\overline{f(x)}$ podemos elegir como representante el polinomio de grado a lo sumo $n-1$ que esté en ella, que será el resto de dividir $f(x)$ por x^n-1.

Por tanto,

$$\mathbb{F}_q[x]/(x^n-1) = \{\overline{a_0+a_1x+\cdots+a_{n-1}x^{n-1}} \,|\, a_i \in \mathbb{F}_q,\ i=0,\ldots,n-1\}.$$

Observamos que hay tantas clases de equivalencia como polinomios de grado menor que n en $\mathbb{F}_q[x]$.

Podemos establecer un isomorfismo de espacios vectoriales entre $\mathbb{F}_q^n$ y $\mathbb{F}_q[x]/(x^n-1)$ mediante $\psi(a_0\ldots a_{n-1}) = \overline{a_0+a_1x+\cdots+a_{n-1}x^{n-1}}$.

Si $C \subseteq \mathbb{F}_q^n$ es un código, denotamos por $C(x)$ a $\psi(C)$, esto es,

$$C(x) = \{\overline{a_0+a_1x+\cdots+a_{n-1}x^{n-1}} \in \mathbb{F}_q[x]/(x^n-1) | a_0a_1\ldots a_{n-1} \in C\}.$$

Observamos que si C es un código cíclico, entonces dada $c_0\ldots c_{n-1} \in C$, se tiene que $\overline{c_{n-1}c_0\ldots c_{n-2}}$, $\overline{c_{n-2}c_{n-1}c_0\ldots c_{n-3}}, \ldots, \overline{c_1\ldots c_{n-1}c_0} \in C$ y esto implica que si $\overline{\mathbf{c}(x)} = \overline{\sum_{i=0}^{n-1} c_ix^i}$, se sigue que $x\overline{\mathbf{c}(x)} = \overline{c_{n-1}+\sum_{i=0}^{n-2} c_ix^{i+1}} \in C(x)$ y en general $x^k\overline{c(x)} = \overline{\sum_{i=1}^{k} c_{n-i}x^{k-i}+\sum_{i=0}^{n-k-1} c_ix^{i+k}} \in C(x)$ para $k<n$. Utilizamos esta propiedad de los códigos cíclicos para caracterizarlos:

Proposición 1.2 (Caracterización de los códigos cíclicos) *Sea $C \subseteq \mathbb{F}_q^n$ un código lineal. Entonces, C es cíclico si y, solo si, $C(x)$ es un ideal de $\mathbb{F}_q[x]/(x^n-1)$.*

La importancia de la proposición anterior quedará de manifiesto en el siguiente apartado, donde explotaremos esta característica de los códigos cíclicos.