OCW
OpenCourseWare

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 2 del Tema 4:
Polinomio generador y matriz generadora de un código cíclico

Mayo de 2017

2 Polinomio generador y matriz generadora de un código cíclico

Como hemos indicado, usando Teoría de Anillos, vamos a poder conocer más sobre la estructura de $C(x)$, cuando C es un código cíclico:

Proposición 2.1 *Sea $C \subseteq \mathbb{F}_q^n$ un código cíclico. Entonces, existe un único polinomio mónico $g(x)$ de grado mínimo tal que*

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

Además, $g(x)$ es un factor de $x^n - 1$ en $\mathbb{F}_q[x]$.

Cuando $C \subseteq \mathbb{F}_q^n$ es un código cíclico, al polinomio mónico $g(x)$ de grado mínimo tal que $C(x) = (\overline{g(x)})$ se le llama **polinomio generador de** C. Por tanto, es fácil determinar todos los códigos cíclicos de una longitud determinada n sobre $\mathbb{F}_q$: basta con hallar los polinomios mónicos que dividen a $x^n - 1$ y tomar cada uno de ellos como polinomio generador del código cíclico buscado.

Ejemplo Para calcular los códigos cíclicos de longitud 7 en $\mathbb{F}_2$, debemos determinar los factores irreducibles sobre $\mathbb{F}_2$ de $x^7 - 1$. Ahora,

$$x^7 - 1 = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1)$$

Entonces, hay 2^3 códigos distintos $C_i(x) = (\overline{g_i(x)})$, con $i = 1, \ldots, 8$, donde

$$\begin{array}{ll} g_1(x) = 1, & g_2(x) = x+1 \\ g_3(x) = x^3+x+1 & g_4(x) = x^3+x^2+1 \\ g_5(x) = x^4+x^2+x+1 & g_6(x) = x^4+x^3+x^2+1 \\ g_7(x) = x^6+x^5+x^4+x^3+x^2+x+1 & g_8(x) = x^7-1 \end{array}$$

Observamos que $C_1(x) = \mathbb{F}_2[x]/(x^7 - 1)$ y, por tanto, $C_1 = \mathbb{F}_2^7$ y $C_8(x) = 0$, luego $C_8 = \{0000000\}$.

Este polinomio generador de un código cíclico nos sirve para determinar una matriz generadora del mismo, tal y como nos indica el siguiente resultado:

Proposición 2.2 (Matriz generadora) *Sea $C \subset \mathbb{F}_q^n$ un código cíclico con polinomio generador $g(x) = \sum_{i=0}^{n-k} g_i x^i$ de grado $n - k$. Entonces, C es un código de dimensión k y una matriz generadora es*

$$\begin{pmatrix} g_0 & g_1 & \ldots & g_{n-k} & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & 0 \\ & & & & & & & \\ & & & & & & & \\ 0 & \ldots & 0 & g_0 & g_1 & g_2 & \ldots & g_{n-k} \end{pmatrix}.$$

Ejemplo Si consideramos C_3 el código binario cíclico de longitud 7 con polinomio generador $g_3(x) = x^3 + x + 1$, entonces aplicando la Proposición 2.2 una matriz generadora de C_3 viene dada por

$$G_3 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Obviamente, la matriz generadora G_3 es de tamaño 4×7 y con rango 4, pues C es dimensión 4.

En cambio, si tomasemos el código cíclico binario C_1 de longitud 7 con polinomio generador $g_1(x) = 1$, entonces de la Proposición 2.2 deducimos que una matriz generadora de C_1 es la matriz identidad I_7.