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 4:
Polinomio de control y matriz de control de un código cíclico. Código dual de un código cíclico

Mayo de 2017

3 Polinomio de control y matriz de control de un código cíclico

Si C es un código cíclico de longitud n y dimensión k con polinomio generador $g(x)$, que será de grado $n-k$, sabemos que $g(x)$ es un divisor de x^n-1 y que existe $h(x) \in \mathbb{F}_q[x]$, de grado precisamente k, tal que $g(x)h(x) = x^n - 1$. A este polinomio $h(x)$, que también es mónico y que verifica $g(x)h(x) = x^n - 1$, se le denomina **polinomio de control del código cíclico** C.

Justificamos en la siguiente proposición el denominar a $h(x)$ polinomio de control:

Proposición 3.1 ***(Matriz de control)*** *Sea $C \subset \mathbb{F}_q^n$ un código cíclico con polinomio de control $h(x) = \sum_{i=0}^{k} h_i x^i$ de grado k. Entonces, una matriz de control de C es*

$$\begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ & & & & & & & \\ & & & & & & & \\ 0 & \dots & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 \end{pmatrix}.$$

Observamos que si $C \subset \mathbb{F}_q^n$ es un código cíclico con polinomio de control $h(x) = \sum_{i=0}^{k} h_i x^i$, la matriz H que figura en la proposición anterior nos permite deducir que $C^\perp$ es otro código cíclico puesto que una base de él es la formada por las filas de H y esta base verifica la Proposición 1.1. También lo podríamos verificar estudiando si $h_0^{-1} \sum_{i=0}^{k} h_i x^{k-i}$, que lo obtenemos de la expresión de H, es un divisor de $x^n - 1$ y comprobando que este polinomio genera el ideal de $C^\perp(x)$. En cualquier caso, deducimos que un polinomio generador para $C^\perp$ es $h_0^{-1} \sum_{i=0}^{k} h_i x^{k-i}$. Obviamente, $C^\perp$, que tiene dimensión $n-k$ si C es de dimensión k por ser su dual, tiene un polinomio generador de grado k.

Ejemplo Si consideramos C_3 el código binario cíclico de longitud 7 con polinomio generador $g_3(x) = x^3 + x + 1$, sabemos que su polinomio de control viene dado por $h_3(x) = x^4 + x^2 + x + 1$. Entonces, aplicando la Proposición 3.1 una matriz de control de C_3 viene dada por

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Vemos que la matriz de control H_3 es de tamaño 3×7 y con rango 3, pues C es de dimensión 4. Además, esta matriz genera a $C_3^\perp$, que es también cíclico, y el polinomio generador de $C_3^\perp$ viene dado por $1 + x^2 + x^3 + x^4$, que es precisamente el polinomio $g_6(x)$ del ejemplo de la sección anterior, en el que se calculaban todos los polinomios generadores de códigos cíclicos binarios de longitud 7. Observamos con este ejemplo que el polinomio de control $h(x)$ de un código cíclico C no tiene que ser necesariamente el polinomio generador de $C^\perp$, aunque $h(x)$ tenga el grado adecuado para generar $C^\perp$, sea mónico y divisor de $x^n - 1$.