Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Resumen Teórico
Apartado 4 del Tema 4:
Ejemplo de códigos cíclicos:
Códigos BCH

Mayo de 2017

5 Ejemplo de códigos cíclicos: Códigos BCH

Por Teoría de Anillos, si n y q son coprimos entre sí, sabemos que $x^n - 1$ se puede expresar como producto de polinomios mónicos $f_i(x)$ irreducibles sobre $\mathbb{F}_q$, esto es, $x^n - 1 = \prod f_i(x)$ y que si α_i es una raíz de f_i, entonces $t(\alpha_i) = 0$ si y, solo si, $t(x) = f_i(x)a(x)$ para algún polinomio $a(x)$. Esto nos sirve para caracterizar a los códigos cíclicos, usando las raíces de su polinomio generador de la forma siguiente:

Proposición 5.1 *Sea $C \subset \mathbb{F}_q^n$ un código cíclico con polinomio generador $g(x) = \prod_{i=1}^{s} f_i(x)$, siendo f_i polinomio irreducible sobre $\mathbb{F}_q$, y sea α_i una raíz de $f_i(x)$ en una extensión apropiada de $\mathbb{F}_q$. Entonces,*

$$C(x) = \{\overline{t(x)} \in \mathbb{F}_q[x]/(x^n - 1) \,|\, t(\alpha_1) = \cdots = t(\alpha_s) = 0\}.$$

A las raíces del polimonio generador de un código cíclico se les llaman **ceros** del código. Observamos que los ceros siempre son raíces n-ésimas de la unidad. Estos ceros nos sirven para dar otra construcción de los códigos cíclicos: si partimos de un subconjunto de raíces n-ésimas de la unidad, para cada una de ellas le localizamos el polinomio irreducible del que es raíz y construimos el código C cuyo polinomio generador sea el mínimo común múltiplo de de estos polinomios irreducibles. Además, si $\alpha_1, \ldots, \alpha_r$ son los ceros del código cíclico que buscamos, la matriz

$$H_1 = \begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_r & \ldots & \alpha_r^{n-1} \end{pmatrix}$$

funciona como una "matriz de control" en el sentido que $c \in C$ si y, solo si, $cH_1^t = 0$.

Un tipo de códigos que se contruyen de esta manera son los códigos BCH: Sean n, $q = p^r$ dos números naturales coprimos entre sí. Sea m el orden multiplicativo de q módulo n, es decir, el número natural más pequeño tal que $q^m \equiv 1 \bmod n$. Sea δ un número natural tal que $2 \leq \delta \leq n$ y sea $\alpha \in \mathbb{F}_{q^m}$ una raíz primitiva n-ésima de la unidad. Se llama **código BCH en sentido estricto sobre $\mathbb{F}_q$ de longitud n y distancia mínima prevista** δ al código cíclico cuyo polinomio generador tiene por raíces a $\{\alpha, \alpha^2, \ldots, \alpha^{\delta-1}\}$. Se puede demostrar que la distancia mínima del código así construido es, al menos, δ.

Ejemplo Consideramos $q = 2$, $n = 2^3 - 1 = 7$ y $\delta = 3$. Entonces, debemos considerar un código cíclico cuyo polinomio generador tenga por raíces a α, y α^2, siendo α una raíz primitiva séptima de la unidad. Ahora, si $f(x) \in \mathbb{F}_2[x]$, entonces $f(\alpha^2) = f(\alpha)^2$, luego α y α^2 tienen el mismo polinomio irreducible. Además, $m = 3$, luego el polinomio irreducible que tiene a α como raíz es de grado 3. Pero $x^7 - 1 = (x-1)(x^3 + x^2 + 1)(x^3 + x + 1)$ en $\mathbb{F}_2[x]$, así que α es raíz de $(x^3 + x^2 + 1)$ ó de $(x^3 + x^2 + 1)$. Supongamos que α es raíz de $(x^3 + x^2 + 1)$. Entonces, este polinomio

será el polinomio generador del código BCH buscado. Si aumentaramos en una unidad la distancia prevista, esto es, pidieramos $\delta = 4$, entonces para hallar el código BCH C_1 que tiene también por cero a α, raíz primitiva séptima de la unidad con polinomio irreducible (x^3+x^2+1), debemos incluir en el polinomio generador de C_1 al polinomio irreducible que tenga a α^3, como raíz. Pero el polinomio irreducible de α^3 es, en este caso, $(x^3 + x + 1)$, con lo que C_1 tendrá por polinomio generador a $(x^3 + x^2 + 1)(x^3 + x + 1)$.