Ma31a Elementos de Álgebra **2 de Diciembre, 2005**

Examen

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: H. Castro, J. Soto*

Tiempo 4.5 hrs.

Un código lineal $C \subseteq \mathbb{F}_q^n$ se dice cíclico si $(c_0, c_1, \ldots, c_{n-1}) \in C$ implica que $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. Para trabajar algebráicamente con C, identificamos el vector $c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ con el polinomio $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]$.

(i).- (0.5 pts) Pruebe que $C \subseteq \mathbb{F}_q^n$ es cíclico si y sólo si C es un ideal (potencialmente degenerado) de $\mathbb{F}_q[x]/(x^n - 1)$.

En lo que sigue, sea $C \subseteq \mathbb{F}_q^n$, $\emptyset \subsetneq C \subsetneq \mathbb{F}_q^n$, un código cíclico.

(ii).- (0.5 pts) Pruebe que existe un único polinomio mónico $g(x)$, denominado *polinomio generador*, tal que $C = (g)$ y que dicho polinomio es el polinomio mónico en C de menor grado.

(iii).- (1.5 pts) Sea g el polinomio generador de C. Pruebe que:

- g divide a $x^n - 1$.
- $c(x) \in C$ se escribe de manera única como $c(x) = f(x)g(x)$ donde $f \in \mathbb{F}_q[x]$ tiene grado menor que $n - \mathrm{grd}(g)$. La dimensión de C es $n - \mathrm{grd}(g)$ (a c se le llama la codificación del mensaje f).
- Si $d = \mathrm{grd}(g)$, una matríz generadora de C es

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_d & \cdots & & 0 \\ & g_0 & g_1 & g_2 & \cdots & g_d & & \\ & & & \cdots & \cdots & \cdots & & \\ 0 & \cdots & & g_0 & g_1 & g_2 & \cdots & g_d \end{pmatrix}$$

(iv).- (0.5 pts) ¿Cuantos códigos cíclicos no–vacios distintos hay en $\mathbb{F}_2^7$?

(v).- Sea $q = 2$, $n = 2^m - 1$, $g(x) \in \mathbb{F}_2[x]$ el polinomio minimal de un elemento primitivo $\alpha \in \mathbb{F}_{2^m}$, y C el código cíclico generado por g.

- (1.0 pts) Pruebe que $g(x) = \prod_{i=0}^{m-1} \left(x - \alpha^{2^i} \right)$ es el polinomio minimal de α.
- (0.5 pts) Sea H la matriz cuya j–ésima columna es $(h_{0,j}, h_{1,j}, \ldots, h_{m-1,j})^T$, $j = 1, \ldots, 2^m - 1$, donde
$$\alpha^{j-1} = \sum_{i=0}^{m-1} h_{i,j} \alpha^i \, .$$
Pruebe que H existe y esta bien definida y que $c \in C$ si y sólo si $Hc^T = 0$. Equivalentemente, pruebe que
$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \end{pmatrix}$$
y que $c(x) \in C$ si y sólo si $c(\alpha) = 0$.
- (0.5 pts) Para $m = 3$ y salvo por permutaciones de sus columnas, determine H y una matriz generadora G de C.
<u>Nota</u>: Para determinar H use un argumento básico de conteo ¿cuantas posibilidades hay para una columna de H?

En general, si $C = (g)$ y g tiene raíces $\alpha_1, \ldots, \alpha_{n-d}$, entonces $c(x) \in C$ si y sólo si $(c_0, \ldots, c_{n-1})^T$ está en el núcleo de
$$H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ \vdots & \vdots & & & \vdots \\ 1 & \alpha_{n-d} & \alpha_{n-d}^2 & \ldots & \alpha_{n-d}^{n-1} \end{pmatrix} .$$
En lo que sigue consideraremos el caso particular de (v) en que $n = 15$, $n - d = 2$, $\alpha_1 = \alpha$ y $\alpha_2 = \alpha^3$, donde $\alpha \in \mathbb{F}_{16}$ es una raíz de $x^4 + x + 1 \in \mathbb{F}_2[x]$. Supondremos que se recibe $w = c + e \in \mathbb{F}_2^n$, donde $c \in C$ es desconocido y definimos el síndrome de w por
$$S = \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = He^T = Hw^T \, .$$

(vi).- (1.0 pts) Verifique que si $e(x) = x^{a_1}$, entonces α^{-a_1} es raíz de $1 + S_1 x$, y si $e(x) = x^{a_1} + x^{a_2}$, $a_1 \neq a_2$, entonces α^{-a_1} y α^{-a_2} son raíces de $1 + S_1 x + (S_1^2 + S_2 S_1^{-1}) x^2$.

La anterior discusión sugiere una forma de construir y utilizar códigos cíclicos capaces de corregir hasta dos errores de transmisión.