Utilizando matrices circulantes para la construcción de nuevos códigos

José Noé Gutiérrez Herrera
ngh@xanum.uam.mx

1. Planteamiento del problema

1.1. Definición de código y de matriz circulante

Supongamos que q es una potencia de un número primo, que $\mathbb{F}_q$ es un campo con q elementos. Para un entero positivo n se define función distancia $d(\mathbf{u},\mathbf{v})$ sobre $\mathbb{F}_q^n$ como el número de coordenadas en las que $\mathbf{u},\mathbf{v}$ difieren. Un código de longitud n y dimesión k y distancia mínima d es un subespacio vectorial de $\mathbb{F}_q^n$ con dimensión k, donde $d = \min\left\{d(\mathbf{u},\mathbf{v}) : \mathbf{u},\mathbf{v} \in \mathbb{F}_q^n,\ \mathbf{u} \neq \mathbf{v}\right\}$. Si $\sigma(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ es el corrimiento cíclico, un código se dice casi-cíclico si es invariante bajo σ^r, la composición de σ consigo misma r veces, para un entero fijo r.

Una matriz se dice circulante si tiene la forma

$$circ\begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \end{pmatrix} := \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{pmatrix}$$

Considere la función $circ\begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \end{pmatrix} \mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ del conjunto de matrices circulantes de $n \times n$ (sobre $\mathbb{F}_q$) en el anillo cociente $\mathbb{F}_q[x] / (x^n - 1)$. Es bien conocido que esta función es un isomorfismo de álgebras.

Si $n = c\ell$ entonces para cualesquiera $e, k \in \mathbb{Z}_n$, gcd $(k,n) = 1$, al aplicar la permutación de $\mathbb{Z}_n$ dada por $\pi(ac + j) = e + k(a + j\ell) \pmod{n}$, con $0 \leq a < \ell,\ 0 \leq j < c$, a las columnas y después a los renglones de una matriz circulante se obtiene una matriz de la forma

$$\mathcal{A} = \begin{pmatrix} A_0 & A_1 & \cdots & A_{\ell-2} & A_{\ell-1} \\ \Gamma A_{\ell-1} & A_0 & & A_{\ell-3} & A_{\ell-2} \\ \Gamma A_{\ell-2} & \Gamma A_{\ell-1} & \cdots & A_{\ell-4} & A_{\ell-3} \\ \vdots & & \ddots & & \vdots \\ \Gamma A_1 & \Gamma A_2 & \cdots & \Gamma A_{\ell-1} & A_0 \end{pmatrix}$$

donde $\Gamma = circ\,(0,1,0,0,\ldots,0)$, y tanto Γ como las A_i son matrices circulantes de tamaño $c \times c$ (cf. [5]).

Estamos considerando los problemas de analizar códigos generados por los renglones de matrices de la forma:

- $\begin{pmatrix} \Gamma A_{\ell-r} & \Gamma A_{\ell-(r-1)} & \cdots & \Gamma A_{\ell-1} & A_0 & \cdots & A_{\ell-(r+1)} \end{pmatrix}$, o algunas de sus columnas

- $(I|\mathcal{A})$, que son iguales a sus espacio ortogonal. Hemos obtenido que es suficiente con que se cumpla

$$\delta_{0j} I + \Gamma^t \sum_{k=0}^{j-1} A_k A_{k-j}^t + \sum_{k=j}^{\ell-1} A_k A_{k-j}^t = 0, \quad 0 \leq j \leq \ell - 1.$$

  Por ejemplo con $A_0 = circ\,(0,0,1,1)$, $A_1 = circ\,(0,1,1,1)$ y $A_2 = circ\,(1,1,0,0)$ la matriz $(I|\mathcal{A})$ genera un $[24,12,8]$ código binario, conocido como código de Golay.

- códigos $\mathcal{C}$, llamados θ-cíclicos, invariantes bajo automorfismos θ de $\mathbb{F}_q$:

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \Rightarrow (\theta\,(c_{n-1})\,, \theta\,(c_0)\,, \theta\,(c_1)\,, \ldots, \theta\,(c_{n-2})) \in \mathcal{C}$$

  que pueden describirse polinomialmente, y son generados por matrices de la forma $\mathcal{A}$.

Los códigos casi-cíclicos se han estudiado ampliamente por su eficiencia en implementación. Se utilizan actualmente en el diseño de los llamados códigos LDPC (cf. [6]), que presentan un mejor desempeño en tiempo de codificación y decodificación que muchas otras familias de códigos.

Los códigos casi-cíclicos se han empleado recientemente en el criptosistema de McEliece (cf. [1]), para reducir la longitud de la llave que utilizan. Pero se han encontrado debilidades cuando se emplean códigos casi-cíclicos alternantes, que son los recomendados. Por esto un problema importante es encontrar familias de códigos casi-cíclicos, con sus respectivo métodos de decodificación.

En [3, 4] el principal objetivo es obtener códigos con mejor distancia mínima que códigos ya conocidos, de la misma longitud y dimensión.

Referencias

[1] Augot, D., Barbier, M., Couvreur, A. *List-decoding of binary Goppa codes up to binary Johnson bound.* Inform. Theory Workshop (ITW) (2011), 229-233.

[2] Barbier, M. et al. *On Quasi-Cyclic Codes as a Generalization of Cyclic Codes.* Finite Fields and Their Appl. 18 (2012), 904-919.

[3] Georgious, S.D., Lappas, E. *Self-dual codes from circulant matrices.* Des. Codes Cryptogr. **64** (2012), 129-141.

[4] Grassl, M., Gulliver, T.A. *On circulant self-dual codes over small fields.* Des. Codes Cryptogr. **52** (2009), 57-81.

[5] Huang, Q. et. al. *Cyclic and Quasi-Cyclic LDPC Codes: New Devolopments.* Proc. of Information Theory and App. Workshop (ITA), 2011.

[6] Huffman, W.C., Pless, V. Fundamentals of Error-Correcting Codes. Cambridge Univ. Press, 2003.

[7] Wu, B., Liu, Z. *Linearized Polynomials over finite fields revisited.* Finite Fields and Their Applications **22** (2013), 79-100.