Trabalho apresentado no XXXVII CNMAC, S.J. dos Campos - SP, 2017.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Códigos Cíclicos Definidos por Anulamento

Conrado Jensen Teixeira[1]
Departamento de Ciências Exatas, UFLA, Lavras, MG
Osnel Broche Cristo[2]
Departamento de Ciências Exatas, UFLA, Lavras, MG

1 Introdução

A classe de códigos corretores de erros mais utilizada na prática é a classe denominada de códigos lineares. Dentre os códigos lineares, a classe mais importante é a classe dos códigos cíclicos.

No aspecto teórico, a importância dos códigos cíclicos vem do fato de que vários resultados da álgebra abstrata, em particular corpos finitos, constatam-se bastante úteis para caracterizar as propriedades algébricas dessa classe de códigos. Na visão prática, a importância vem do fato desses códigos apresentarem bons algoritmos de codificação e decodificação, o que possibilita a construção de circuitos, que codificam e decodificam, menos complexos do que aqueles para códigos lineares em geral.

Neste trabalho apresenta-se os códigos cíclicos definidos por condição de anulamento.

2 Elementos Principais

Um código linear $C \in K^n$ é dito ser um código cíclico se, para todo $c = (c_0, \ldots, c_{n-1})$ pertencente a C, o vetor $(c_{n-1}, c_0 \ldots, c_{n-2})$ pertence a C. Similarmente, dado um código linear C, uma permutacão π de $\{0, \ldots, n-1\}$ definida por

$$\pi(i) = \begin{cases} i-1, \text{ se } i \geq 1 \\ n-1, \text{ se } i = 0, \end{cases}$$

e $T_\pi(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0 \ldots, c_{n-2})$, então C será um código cíclico se $T_\pi(c) \in C$ para todo $c \in C$.

Tem-se que $R_n = K[x]/(x^n - 1)$ é isomorfo a K^n por meio da transformação linear $\nu(a_0, a_1, \ldots, a_{n-1}) = a_0 + a_1 x + \ldots a_{n-1} x^{n-1}$, tal que $(a_0, a_1, \ldots, a_{n-1}) \in R_n$.

Todo ideal de R_n é da forma $I([f(x)])$, em que $f(x)$ é um divisor de $x^n - 1$. Determina-se $\nu(C)$ como um ideal de R_n se, e somente se, C é um código cíclico .

[1]conrado.jensen@gmail.com
[2]osnel@dex.ufla.br

Seja $I = I([g(x)])$, em que $g(x)$ é um divisor de $x^n - 1$ de grau s. Caracteriza-se $[g(x)], [xg(x)], \ldots, [x^{n-s-1}g(x)]$ uma base de I como espaço vetorial sobre K.

Para todo código cíclico C, existe $v \in C$ tal que $C =< v >$.

3 Códigos Cíclicos por Anulamento

Seja dado um código cíclico $C \subset \mathbb{K}^n$, em que $K = \mathbb{F}_q$ e n e q são primos entre si. Seja F uma extensão do corpo K, sobre o qual o polinômio $x^n - 1$ se fatora em fatores lineares mônicos distintos. Sejam $\alpha_1, \cdots, \alpha_r$ as raízes de $g(x)$ em F, que são portanto duas a duas distintas. Assim, segue que $\nu(C) = I([g(x)]) = \{[f(x)] \in R_n; f(\alpha_1) = \cdots = f(\alpha_r) = 0\}$.

Seja $f(x) = \sum_{j=0}^{n-1} a_j x^j \in K[x]$. Tem-se que $[f(x)]$ é um elemento de $I([g(x)])$ se, e somente, se, $f(\alpha_i) = \sum_{j=0}^{n-1} a_j \alpha_i^j = 0$, para $i = 1, \cdots, r$. Pode-se então definir C pelo polinômio $g(x)$, a partir da matriz formada por α_i^j e o conjunto $a = (a_1, a_2, \cdots, a_{n-1}) \in K^n$. Assim, $\tilde{H}a^t = 0$, em que $\tilde{H}$ é a seguinte matriz com entradas em F

$$\tilde{H} = \begin{pmatrix} \alpha_1^0 & \alpha_1^1 & \cdots & \alpha_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_r^0 & \alpha_r^1 & \cdots & \alpha_r^{n-1} \end{pmatrix}$$

Como os α_i são as raízes de $g(x)$ em F, tem-se que $\tilde{H}$ não é a matriz teste de paridade de C. Para se determinar a matriz teste de paridade de C, olha-se para F como espaço vetorial sobre $\mathbb{F}_q$ de dimensão finita d. Logo, pode-se representar os elementos $\alpha_i^j \in F$ como vetores colunas $\langle \alpha_i^j \rangle \in (\mathbb{F}_{||})^d$. De modo que $f(\alpha_i) = \langle \sum_{j=0}^{n-1} a_j \alpha_1^j \rangle = \sum_{j=0}^{n-1} a_j \langle \alpha_1^j \rangle$.

Definindo a matriz H' como sendo

$$H' = \begin{pmatrix} \langle \alpha_1^0 \rangle & \langle \alpha_1^1 \rangle & \cdots & \langle \alpha_1^{n-1} \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \alpha_r^0 \rangle & \langle \alpha_r^1 \rangle & \cdots & \langle \alpha_r^{n-1} \rangle \end{pmatrix}.$$

Portanto, $a \in C$ se, e somente se, $H'a^t = 0$.

4 Conclusões

Em geral, para conferir se um vetor $v \in K^n$ é um elemento de C com matriz geradora G, deve-se solucionar um sistema com n equações e k incógnitas x, dado por $xG = v$. No entanto, quanto maior o sistema mais custos computacionais se têm. De forma a minimizar esse custo, desenvolve-se uma matriz teste de paridade H. A matriz teste de paridade permite caracterizar os elementos do código C por condição de anulamento. Assim basta verificar se $Hv^t = 0$.

Referências

[1] A. Hefez, and M. L. T. Villela. *Códigos Corretores de Erros.* Rio de Janeiro, IMPA, 2008. 216 pg. (Série Computação e Matemática).