Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, v. 6, n. 1, 2018.

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

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Caracterização e decodificação dos Códigos Cíclicos

Renata Vieira Costa[1]
Instituto de Ciências Exatas, UFF, Volta Redonda, RJ
Rosemary Miguel Pires[2]
Departamento de Matemática, Instituto de Ciências Exatas, UFF, Volta Redonda,RJ

1 Introdução

Os códigos corretores de erros são ferramentas utilizadas para transmitir ou armazenar informações de modo seguro. O seu uso ocorre quando são identificados erros durante a transmissão, devido alguma interferência no canal utilizado, fazendo com que o receptor não consiga identificar a mensagem que lhe foi enviada, ou então, quando ao armazenar uma informação não for possível recuperar a mensagem original.

Pretendemos neste trabalho fazer uma introdução aos códigos cíclicos. Para mais detalhes, consultar [1].

Para definirmos um código corretor de erros, considere um conjunto finito A chamado de alfabeto e denotemos por $|A| = q$ o número de elementos de A.

Um **código corretor de erros** é um subconjunto próprio C de A^n. Uma palavra de comprimento n é uma sequência finita de n símbolos do alfabeto.

Dados dois elementos $u, v \in A^n$, a **distância de Hamming** entre u e v é definida como sendo $d(u, v) = |\{i : u_i \neq v_i\}|$ e a **distância mínima** de um código C é o número $d = min\{d(u, v)|u, v \in C, u \neq v\}$.

Segue abaixo, um resultado que nos ajudará na detecção e correção de erros de um código.

Teorema 1. *Seja C um código com distância mínima d. Então C pode corrigir até $k = \left[\frac{d-1}{2}\right]$ erros e detectar até $d - 1$ erros.*

2 Códigos Cíclicos

Denotaremos por K um corpo finito com q elementos tomado como alfabeto. Da Álgebra Linear, sabemos que, para cada número natural n, K^n é um K-espaço vetorial de dimensão n. Um código $C \subset K^n$ será chamado de **código linear** se for um subespaço vetorial de K^n.

[1]renatac@id.uff.br
[2]rosemarypires@id.uff.br

Um código linear $C \subset K^n$ será chamado de **código cíclico** se, para todo $c = (c_0, ..., c_{n-1})$ pertencente a C, o vetor $(c_{n-1}, c_0, ..., c_{n-2})$ pertence a C.

Existem vários questões interessantes que surgem no estudo dos códigos cíclicos tais como: Como podem ser descritos todos os códigos cíclicos de K^n? Quantos são os códigos cíclicos de dimensão k em K^n? Será que todo código cíclico é da forma $< v >$ para algum v?

Nesta apresentação, mostraremos como estas questões podem ser respondidas. Com este propósito, consideramos R_n como sendo o anel das classes residuais em $K[x]$ módulo $x^n - 1$, isto é, $R_n = K[x]_{(x^n-1)}$. Um elemento de R_n é um conjunto da forma $[f(x)] = \{f(x) + g(x)(x^n - 1) \, : \, g(x) \in K[x]\}$.

R_n munido da adição e multiplicação por escalares $\lambda \in K$ usuais é um K-espaço vetorial de dimensão n com base $\{[1], [x], ..., [x^{n-1}]\}$ e, como tal é isomorfo a K^n através da transformação linear

$$\nu : K^n \longrightarrow R_n$$
$$(a_0, ..., a_n) \mapsto [a_0 + a_1 x + ... + a_{n-1} x^{n-1}]$$

No estudo da caracterização dos códigos cíclicos mostraremos os seguintes resultados:

Teorema 2. *Um subespaço $C \subset K^n$ é um código cíclico se, e somente se, $\nu(C)$ é um ideal de R_n.*

Teorema 3. *Seja $I = I([g(x)])$, onde $g(x)$ é um divisor de $x^n - 1$ de grau s. Temos que $\{[g(x)], [xg(x)], [x^2 g(x)], ..., x^{n-s-1} g(x)\}$ é uma base de I como espaço vetorial sobre K.*

Como consequência deste teorema, se prova que: Dado um código cíclico C, existe $v \in C$ tal que $C =< v >$.

Por fim, com relação ao processo de decodificação, serão dadas as definições das principais matrizes associadas a um código conhecidas como matrizes geradoras e matrizes teste de paridade e serão apresentados os resultados relacionados.

3 Conclusões

Neste trabalho, mostramos como caracterizar e decodificar códigos cíclicos, pois estes são muito utilizados em aplicações por formarem uma classe de códigos lineares que possui bons algoritmos de codificação e decodificação ([1]).

Notemos que os conceitos abordados, por mais que sejam abstratos, possuem aplicações diretas na vida real. A utilização de informações digitalizadas, como assistir televisão, falar ao telefone ou ouvir um CD mostram como os códigos corretores de erros participam do nosso cotidiano. Além disso, a Teoria de Códigos constitui hoje uma área de pesquisa ativa, tanto pelos aspectos matemáticos como pelos aspectos computacionais.

Referências

[1] A. Hefez; M. L. T. Villela, *Códigos Corretores de Erros*. Série de Computação e Matemática, IMPA,2002.