Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Estrutura Algébrica de um Código Corretor de Erros

Juliana Gavinho Sanção [1]
Universidade Federal do Espírito Santo
Victor do Nascimento Martins [2]
Universidade Federal do Espírito Santo

1 Introdução

A construção de códigos inspira-se bem através dos mais comuns códigos utilizados pelos seres humanos: os idiomas. Na língua portuguesa, por exemplo, usamos um alfabeto de 23 letras e as palavras nada mais são do que sequências de letras. Se, por exemplo, ao escrevermos uma palavra, produzimos a sequência de letras "gadanhoto", como esta não é uma palavra da língua portuguesa, percebe-se imediatamente que houve um erro, e, nesse caso, a correção é possível, pois a palavra que mais se assemelha a "gadanhoto" é "gafanhoto".

Em essência, um código corretor de erros é um modo organizado de se acrescentar algum dado adicional a cada informação que se queira transmitir ou armazenar, que permita, ao recuperar a informação, detectar e corrigir erros.

Em 1965, a nave espacial Mariner 4 enviou 22 fotos em preto e branco de Marte. Foram utilizados 64 tons de cinza codificados como elementos de $\{0,1\}^6$ para transmitir cada um dos 200×200 pontos das fotos. Em 1972, a nave espacial Mariner 9 transmitiu imagens de Marte com uma resolução de 700 x 832 pontos. Como a velocidade da transmissão era maior, o código foi recodificado através de uma função injetora φ de $\{0,1\}^6$ em $\{0,1\}^{32}$ para acrescentar o código de canal que permite detectar e corrigir até sete erros. Esse código pertence à família de códigos chamados de Códigos de Reed-Muller.

Sabe-se atualmente que a utilização de mais estruturas algébricas sobre um código nos dá mais informações a respeito do mesmo, bem como algoritmos de codificação e decodificação mais eficientes. Neste sentido, procuramos estudar neste trabalho a classe de códigos que talvez seja a mais utilizada na prática: os códigos lineares. Estes utilizam como base a estrutura matemática dos espaços vetoriais, sendo, portanto, um exemplo da aplicação de técnicas de Álgebra Linear em algo do cotidiano.

[1] julianagavinho@hotmail.com
[2] victor.n.martins@ufes.br

2 Códigos Lineares

Considere um conjunto finito **A** qualquer, que será chamado de **alfabeto** e os elementos deste conjunto de **letras** ou **dígitos**. Uma **palavra** é uma sequência de elementos de **A** e o **comprimento** dessa palavra é o número de letras que a compõe. Iremos considerar o conjunto $\mathbf{A}^n$. Um **código corretor de erros** é um subconjunto próprio C de $\mathbf{A}^n$, para algum número natural n.

Dados dois elementos $x = (x_1, x_2, ..., x_n)$ e $y = (y_1, y_2, ..., y_n)$ de $\mathbf{A}^n$, chama-se **distância de Hamming** de x a y ao número de coordenadas em que estes elementos são diferentes. Em um código C a menor distância entre dois elementos quaisquer do código é chamada **distância mínima** do código C. Esse conceito de distância mínima está diretamente ligado a capacidade de correção de um código. Como nota-se no resultado a seguir, quanto mais distantes entre si são as palavras de um código, maior é a capacidade de correção.

Teorema 2.1. *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.*

Uma classe de códigos muito utilizada é a dos códigos lineares. Um código C será um código linear se for um subespaço vetorial próprio do espaço vetorial $\mathbb{K}^n$, onde $\mathbb{K}$ é um corpo finito. Se considerarmos uma base ordenada do espaço vetorial C, podemos gerar uma matriz de linhas linearmente independentes chamada **matriz geradora** do código C e a partir daí podemos estudar melhor o código.

Se C tem dimensão k sobre $\mathbb{K}$ dizemos que C é um (n, k) - código linear e se C tem distância mínima d, dizemos que C é um (n, k, d) - código linear.

No estudo de códigos a busca por "bons códigos" pode ser traduzida, de certa forma, como a busca por bons parâmetros que vão melhorar a capacidade de detecção e correção de erros. Portanto resultados que relacionam os parâmetros de um código são sempre interessantes. Um destes resultados que pode ser demonstrado usando a teoria da matriz geradora do código é o que segue.

Teorema 2.2. *(Cota de Singleton) Os parâmetros $[n; k; d]$ de um código linear satisfazem à desigualdade*

$$d \leq n - k + 1.$$

Quando tivermos um código em que $d = n - k + 1$, chamaremos esse código de MDS (Maximum Distance Separable) e como já mencionado teríamos um código "bom", já que as palavras estão distanciadas o máximo possível.

Referências

[1] A. Hefez, M. L. T. Vilela. *Códigos Corretores de Erros*. Rio de Janeiro, IMPA, 2002.

[2] R. Lidl, H. Niederreiter. *Finite Fields, second edition*. Cambridge University Press, 1997.

[3] J. H. Van Lint. *An Introduction to Coding Theory*. Springer-Verlang New York Inc., 1982.