Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 11, n. 1, 2025.

Trabalho apresentado no XLIII CNMAC, Centro de Convenções do Armação Resort - Porto de Galinhas - PE, 2024

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Introdução a Códigos Lineares

Analisse M. Alves[1], Gabriel A. A. Bezzera[2], Clarice D. de Albuquerque[3]
UFCA, Juazeiro do Norte, CE

A teoria de Códigos Corretores de Erros (CCE) tem origem na década de quarenta, quando o matemático e engenheiro C. E. Shannon, do Laboratório Bell, percebeu a necessidade de transmitir informações minimizando a perda de dados ou adição de ruídos. Com esse objetivo, Shannon desenvolveu uma teoria visando a criação de métodos que detectam e corrigem parte dos erros ocasionados na transmissão de informação de um sistema de comunicação.

A teoria de interesse, inicialmente matemática, avançou para diversos campos de estudo, como engenharia, física, computação e estatística. Na atualidade, está presente em diversos setores tecnológicos, entre eles, comunicação móvel, armazenamento de dados e, também, computação quântica. Desse modo, a vasta importância de CCE na transmissão de informações é uma das razões que os leva a ser uma área de amplo desenvolvimento na comunicação clássica e quântica.

O aprimoramento da transmissão de informação não a isenta de falhas, interferências externas podem modificar a mensagem e ocasionar a perda do significado original. Para minimizar esses danos, a teoria propõe adicionar redundâncias à informação original no processo de codificação, de forma que, se a mensagem sofrer alteração durante a transmissão, ainda seja possível recuperar a informação original após a decodificação.

Na evolução da teoria de CCE, diversas classes de códigos foram desenvolvidas e disseminadas para diferentes propósitos. Destaca-se a classe de códigos lineares por ser a de maior utilização prática, devido, em grande parte, a sua estrutura algébrica de espaço vetorial bem definida.

Os códigos lineares estão presentes nas codificações clássica e quântica. São exemplos desses códigos na codificação clássica o código de Hamming, BCH, Reed-Solomon e Reed-Muller, e na quântica, os códigos de Shor e CSS. As características algébricas gerais apresentadas nos códigos lineares são comuns a ambas as codificações e podem ser estudadas em diversos livros e trabalhos, destacamos aqui as referências [1–4].

Para construir um código linear C é preciso determinar alguns parâmetros essenciais: o comprimento do código n, o número de bits codificados k, e a distância mínima do código d. O código será denotado por $C(n, k, d)$. Para compreender esses parâmetros, considere um corpo finito K de q elementos chamado alfabeto, as sequências finitas de elementos do alfabeto com comprimento n, formam o espaço vetorial K^n de dimensão n. O código C pertence a um subespaço vetorial de K^n com dimensão finita k, em que cada elemento é denominado palavra-código. Por fim, a distância mínima d de um código é definida como a menor distância entre duas palavras-código, ou seja, o menor número de bits distintos entre essas palavras.

A estrutura algébrica do código linear permite determinar algumas informações a partir da definição do código $C(n, k, d)$. Primeiramente, o código C é capaz de detectar até w erros, onde w é dado pela equação (1)

$$w = (d - 1)\,. \tag{1}$$

[1]analisse.magalhaes@aluno.ufca.edu.br
[2]gabriel.bezerra@aluno.ufca.edu.br
[3]clarice.albuquerque@ufca.edu.br

O código também será capaz de corrigir até t erros, onde t é dado na equação (2)

$$t = \left[\frac{(d-1)}{2}\right]. \tag{2}$$

Além disso, podemos calcular a taxa de codificação de C, expressa pela equação (3)

$$R_c = \frac{k}{n}. \tag{3}$$

Os cálculos realizados em (1), (2) e (3) têm como objetivo determinar se um código é de boa utilização, observando-se se o código é capaz de detectar e corrigir o maior número de erros e possuir taxa de codificação próxima a um.

Outra característica da estrutura de subespaço vetorial permite que todas as palavras-códigos de C sejam escritas como combinação linear de uma base ordenada de C. Dessa forma, podemos escrever os vetores da base como linhas de uma matriz G, denominada matriz geradora de C. Assim, se o vetor u for a informação a ser codificada e v a palavra-código correspondente, podemos definir o processo de codificação descrito na equação (4)

$$v = u \times G. \tag{4}$$

Por fim, a estrutura algébrica também permite determinar se a mensagem recebida após o ruído pertence ao código. Para determinar se a mensagem corresponde a uma palavra-código, utiliza-se a matriz teste de paridade H, determinada pela equação (5)

$$H^t \times G = 0, \tag{5}$$

em que, H^t é a matriz transposta de H. Assim, a mensagem recebida v será uma palavra-código se satisfizer a equação (6)

$$H \times v^t = 0. \tag{6}$$

Neste trabalho, foi realizado um estudo introdutório da classe de códigos lineares, em que buscou-se ressaltar a estrutura algébrica que dá suporte para a determinação desses códigos. Além disso, ressaltou-se a importância e aplicabilidade dessa classe de CCE.

Agradecimentos

Agradeço à Universidade Federal do Cariri pelo suporte no desenvolvimento do projeto de pesquisa, por meio da bolsa PIBIC.

Referências

[1] A. Hefez e M. L. T. Villela. **Códigos Corretores de Erros**. 1ª.ed. Rio de Janeiro: IMPA, 2002. ISBN: 8524401699.

[2] C. C. Lavor, M. M. S. Alves, R. M. Siqueira e S. I. R. Costa. **Uma introdução á teoria de códigos**. 1ª.ed. São Paulo: SBMAC, 2012. ISBN: 9788586883866.

[3] C. P. Milies. **Breve introdução à Teoria dos Códigos Corretores de Erros**. Colóquio de Matemática da Região Centro-Oeste, Campo Grande, MS, 2009.

[4] R. Palazzo, J. C. Interlando, J. R. Geronimo, M. C. Araújo, Neto T. P. N. e G. O. dos Santos. **Fundamento Algébricos e Geométricos dos Códigos Corretores de Erros**. Manuscrito não publicado. UNICAMP, 2006.