Os Códigos Corretores de Erros

Pedro Leonardo Pinto de Souza [42]
Edney Augusto Jesus de Oliveira[43]
Vinícius Vivaldino Pires de Almeida[44]

Resumo: Neste trabalho abordaremos os códigos corretores de erros lineares e uma classe específica de códigos lineares, os códigos cíclicos. Nosso principal objetivo é apresentar a construção desses códigos com um viés matemático, buscando evidenciar e comprovar alguns de seus importantes aspectos, tais como o comprimento de um código, sua capacidade de detecção de erros e a sua efetiva capacidade de corrigi-los. Durante os estudos dos fundamentos teóricos, percebemos que a estrutura de um código linear é substancialmente mais simples do que a de um código cíclico, no entanto percebemos que em contrapartida, os algoritmos de codificação e decodificação se tornam mais efetivos e elegantes.

Mas afinal, o que é um código corretor de erros? Em essência, um código corretor de erros é um modo de acrescentar um dado adicional a cada informação que se queira transmitir ou armazenar, que permita ao destinatário recuperar a informação e, na ocorrência de erros durante a transmissão, detecta-los e corrigi-los.

Durante uma transmissão de dados alguns fatores como a interferência nos canais de transmissão podem alterar a integridade da informação recebida impossibilitando a comunicação. Sendo assim, é de interesse a criação de uma ferramenta que consiga reverter essa situação, motivando assim o nascimento dos códigos corretores de erros.

O ponto de partida para isso, é a criação de um código corretor de erros, para tanto, definimos um conjunto de símbolos denominado alfabeto, que serão utilizados para escrever as palavras desse código. Matematicamente, a melhor estrutura para o alfabeto é um corpo finito K^n com q elementos. Além disso, por padronização, estipulamos que todas as palavras do código tenham sempre a mesma quantidade de símbolos (diferentemente do nosso vocabulário que apresenta palavras com a quantidade de letras variando entre um e quarenta e três). Portanto, o conjunto de todas as palavras de um código será um subconjunto próprio qualquer de K^n. Desta forma, temos que o código está contido dentro de um K-espaço vetorial n-dimensional,mas além disso, precisamos de um modo de medir a distância entre as palavras, para isso é necessário definir a métrica de Hamming e uma vez que possuímos uma métrica, podemos definir conceitos como disco e esfera. Agora, para que o código herde as propriedades vetoriais de K^n, ele próprio deve ser um K-espaço vetorial. Motivados por isso, definimos um código corretor de erros linear da seguinte maneira.

Definição 1. Um código $\mathcal{C} \subset K^n$ é chamado de código linear se $\mathcal{C}$ for um subespaço vetorial de K^n.

[42]Universidade Federal de Ouro Preto -Instituto de Ciências Exatas e Biológicas, pedro.leonardo@aluno.ufop.edu.br,
[43]Universidade Federal de Ouro Preto -Instituto de Ciências Exatas e Biológicas, edney@ufop.edu.br
[44]Universidade Federal de Ouro Preto -Instituto de Ciências Exatas e Biológicas, viniciusalmeida@iceb.ufop.br

A partir desta definição, estabeleceremos os conceitos de peso de um código, matrizes geradoras de um código, códigos duais, codificação e decodificação. Para realizar essa aplicação, codificamos a palavra a ser transmitida, chamada de código da fonte, adicionando redundâcias a mesma através de uma transformação linear injetiva, a partir da qual definimos matriz geradora do código. Deste modo, teremos uma nova palavra chamada de código de canal pronta para ser transmitida. A palavra recebida será decodificada e, através do algoritmo da decodificação que é baseado em operações matriciais, corrigida caso tenha ocorrido até uma certa quantidade de erros.

Em contrapartida, enquanto os códigos lineares correspondem a um subespaço vetorial de um espaço adequado, os códigos cíclicos possuem uma estrutura de um ideal de um anel quociente oportuno. Entretanto a complexidade teórica dos códigos cíclicos é superior aos lineares e apesar disso, quando utilizamos os códigos cíclicos conseguimos algoritmos de codificação e decodificação mais rápidos e eficientes. Deste modo a definição de um código cíclico é dada por

Definição 2. Seja K um corpo e K^n um espaço vetorial sobre K. Dizemos que o subespaço vetorial $\mathcal{C} \subset K^n$ é um código cíclico quando para todo $c = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$, $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.

A partir dessa definição, estabeleceremos os mesmos conceitos de matrizes geradoras de um código, codificação e decodificação dos códigos lineares, no entanto essas definições serão adaptadas para a estrutura de anéis de polinômios. Além disso, essa estrutura nos permite calcular de maneira mais eficiente a matriz geradora de um código cíclico e, posteriormente, codificar uma palavra do código $\mathcal{C}$ através da matriz geradora. Conhecendo tal matriz, conseguimos determinar uma maneira mais simples do que os códigos lineares, para decodificar as palavras recebidas.

Os resultados obtidos neste trabalho evidenciam a estreita relação entre a matemática e a teoria da informação, tendo em vista a eficiêcia dessas aplicações ao gerar precisão e segurança nas mais variadas formas de comunicação e, principalmente, entender como a Álgebra Linear e a Álgebra Abstrata podem ser utilizadas em diversas aplicações práticas ao enxergar por exemplo, um código corretor de erros linear $\mathcal{C}$ como um subespaço vetorial de K^n e descrevê-lo como uma transformação linear cujos elementos do núcleo são as palavras do código e por outro lado, o quanto o algoritmo de codificação e decodificação de um código cíclico pode ser superior ao de um código linear, uma vez que via um isomorfismo linear, conseguimos propriedades importantes do código C quando enxergamos seus elementos como elementos de um anel quociente, possibilitando desenvolver um algoritmo de codificação e decodificação tão mais simples na prática quando nos embasamos em uma teoria mais sofisticada.

Referências

[1] A. Gonçalves, *Introdução à Álgebra*, IMPA - Instituto de Matematica Pura e Aplicada, 1979.

[2] A. Hefez, M. L. Villela, *Códigos corretores de erros*, IMPA - Instituto de Matematica Pura e Aplicada, 2008.

[3] P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul *Basic Abstract Algebra*, Cambridge University Press, 1994.

[4] S. Lang *Graduate Texts in Mathematics: Algebra*, Springer, 2002.