CÓDIGOS LINEARES

Tainara Bernardo Colombo (PIBIC/CNPq/FA/UEM), Fernanda Diniz de Melo Hernandez (Orientador). E-mail: 115486@uem.br.

Universidade Estadual de Maringá, Centro de Ciências Exatas, Maringá, PR.

Matemática, Álgebra /Teoria dos Códigos Corretores de Erros

Palavras-chave: Códigos, Transformações Lineares, Distância Mínima.

RESUMO

O projeto consiste em estudar a Teoria dos Códigos Corretores de Erros, estudando seus conceitos básicos, como a distância mínima de um código, e conceitos um pouco mais específicos envolvendo Códigos Lineares, como a matriz geradora, a matriz de teste de paridade de um código e a Cota de Singleton.

INTRODUÇÃO

Os códigos estão presentes na nossa vida desde sempre, não só nos meios de comunicação tecnológicos atuais, mas também como uma forma de linguagem, como por exemplo a nossa língua portuguesa. Quando estamos conversando dentro de uma sala muito barulhenta, geralmente, precisamos repetir algumas frases para que uma outra pessoa possa nos compreender melhor. Nos meios de comunicação acontece algo similar, onde, ao transmitirmos uma mensagem pode ocorrer alguma interferência externa que acaba deixando a mensagem final ilegível.

Nas transmissões via satélite ou nas comunicações internas de um computador, são utilizados códigos que detectam e corrigem erros, a chamada Teoria dos Códigos Corretores de Erros. Esta teoria teve seu início num trabalho publicado em 1948 por Claude E. Shannon. Nas décadas de 50 e 60 muitos matemáticos se interessaram por ela e foram os responsáveis pelo seu desenvolvimento, como Richard W. Hamming, que desenvolveu a classe de códigos conhecida como Códigos de Hamming. Outras classes bem conhecidas são os códigos BCH, Mariner-9 e Reed Solomon. Atualmente essa teoria ainda é um tema atual de pesquisa e continua despertando o interesse de vários cientistas, inclusive o nosso.

MATERIAIS E MÉTODOS

Foram feitas pesquisas bibliográficas e seminários semanais entre orientadora e aluna para a realização deste trabalho.

RESULTADOS E DISCUSSÃO

Neste trabalho, estudamos como construir um código corretor de erros e alguns conceitos importantes envolvendo essa teoria. Primeiramente, para construirmos um código corretor de erros, tomamos um conjunto finito $\square$, o qual chamaremos de alfabeto. Um código corretor de erros, $\square$, será um subconjunto próprio de $\square^{\square} = \{(\square_1, \ldots, \square_{\square}); \square_{\square} \in \square\}$ para um número natural $\square$, onde chamamos cada elemento de $\square^{\square}$ de palavra. Assim, dizemos que $\square$ é o comprimento das palavras do código.

Na Teoria dos Códigos utilizamos a Métrica de Hamming para calcular a distância entre duas palavras, a qual é dada por

$$\square(\square, \square) = |\{\square; \square_{\square} \neq \square_{\square}, 1 \leq \square \leq \square\}|, \text{ onde } \square, \square \in \square^{\square}.$$

O mínimo das distâncias entre quaisquer duas palavras de $\square$ é dito distância mínima do código $\square$. Um resultado muito importante que estudamos é que um código $\square$, com a distância mínima $\square$, pode corrigir até $\kappa = \left[\frac{\square - 1}{2}\right]$ erros e detectar até $\square - 1$ erros.

Esses conceitos apresentados aqui são fundamentais para trabalharmos com essa teoria, pois nos fornecem os parâmetros de um código que são $[\square, \square, \square]$, onde $\square$ é o comprimento do código, $\square$ é a quantidade de elementos que o código possui e $\square$ é a distância mínima do código.

Quando consideramos o alfabeto representado anteriormente por $\square$ como sendo um corpo finito $\square$, temos uma classe de códigos corretores de erros que são os códigos lineares, os quais são subespaços vetoriais do espaço vetorial $\square^{\square}$, onde $\square$ é um número natural. Nesse caso, os parâmetros podem ser reestruturados como $[\square, \square, \square]$, onde $\square$ é a dimensão do código como subespaço vetorial de $\square^{\square}$, e $\square$ é a distância mínima do código. Nos Códigos Lineares, a distância mínima é equivalente ao peso de um código $\square$ o qual dado por

$$\omega(\square) = \square\square\square\{\square(\square, 0); \square \in \square \backslash \{0\}\},$$

ou seja, $\square = \square(\square)$.

Sabendo que o código linear é um subespaço vetorial então ele pode ser obtido a partir de uma transformação linear de $\square^{\square}$ em $\square^{\square}$, ou seja, código $\square$ é gerado por uma uma matriz de transformação linear $\square$ de ordem $\square \times \square$, chamamos $\square$ de matriz geradora de $\square$. Além da matriz geradora, existe uma matriz $\square$ de ordem, com $\square - \square$ linhas linearmente independentes que satisfaz $\square = \{\square \in \square^{\square}; \square\square^{\square} = 0\}$, ela é denominada matriz de teste de paridade de $\square$. Assim, para saber se uma palavra $\square$ pertence ao código devemos verificar apenas se $\square\square^{\square} = 0$.

Com uma análise aprofundada na quantidade de colunas linearmente independentes e linearmente dependentes de $\square$, chegamos em dois resultados importantes. O primeiro nos fornece que o peso de $\square$ é maior ou igual a um natural $\square$ se, e somente se, quaisquer $\square - 1$ colunas de $\square$ forem linearmente independentes. Particularmente, o peso de $\square$ é igual a $\square$ se, e somente se, quaisquer $\square - 1$ colunas de $\square$ são linearmente independentes e existem $\square$ colunas de $\square$ linearmente dependentes. Essas informações nos levam a um dos resultados

mais importantes sobre Códigos Lineares, pois nos fornece uma relação entre os parâmetros de um código. Chamado de Cota de Singleton a desigualdade $\square \leq \square - \square + 1$ permite que estimamos um valor máximo para a distância mínima no momento de construir um código linear.

CONCLUSÕES

Os Códigos Lineares, formam uma importante classe de códigos corretores de erros, pois ao colocarmos uma estrutura de espaço vetorial em um código corretor de erros, adquirimos diversas ferramentas matemáticas que facilitam o trabalho dos pesquisadores da área. Sendo que, suas matrizes geradoras tornam o processo de codificação mais rápido e barato com relação a memória de um sistema operacional, já as matrizes de teste de paridade nos ajudam a identificar, com certa facilidade, se uma palavra pertence ou não ao código, ou seja, nos permite detectar os erros para em seguida corrigi-los.

Entre os anos 1971 e 1972 a NASA utilizou os Códigos de Reed-Muller de Primeira Ordem para transmissão dos dados coletados pela sonda Mariner 9, em uma missão de mapeamento do planeta Marte. Este é só um de muitos dos exemplos onde esse tipo de código foi utilizado.

AGRADECIMENTOS

Agradeço ao CNPq pelo apoio financeiro.

REFERÊNCIAS

[1] HEFEZ, A. & VILLELA, M. L. T. **Códigos corretores de erros**. Instituto de Matemática Pura e Aplicada, 2008.

[2] LOURENÇO, M. L. & COELHO, F. U. **Um Curso de Álgebra Linear**. 2001.

[3] TRAPPE, W et al. **Introduction to cryptography with coding theory**. Pearson Education India, 2006.