Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 5, N. 1, 2017.

Trabalho apresentado no CNMAC, Gramado - RS, 2016.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Aplicação da Teoria de Grupos para Construção de Códigos Lineares com o Uso do GAP

João Vitor M. Domingos[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

Ultimamente a Teoria de Códigos Corretores de Erros vem ganhando espaço nas grandes pesquisas da atualidade com ampla aplicações na Matemática, Computação, Estatística entre outras, conforme [2]. Como esta teoria é bastante extensa, nos focaremos em códigos lineares.

Uma mensagem enviada através da internet e outros meios está sujeita a interferências externas, isto torna a mensagem recebida diferente da original. Por conta disso, em [1], foram desenvolvidos estudos para corrigir esses erros. Com base nesta referência, apresentaremos um método para produzir códigos lineares utilizando matrizes geradoras e aplicando a teoria elementar de grupos.

Utilizaremos para ilustrações e simulações das correções o sistema computational GAP (Groups, Algorithms and Programming), disponível no endereço http://www.gap-system.org/. Este sistema foi criado para programar e/ou computar estruturas algébricas, tais como: Grupos, Espaços Vetoriais, Teoria de Códigos, Teoria de Números, etc.

2 Método para Construção de Códigos Lineares

Inicialmente vejamos algumas definições e resultados elementares para a teoria de códigos. Sejam $B = \{0, 1\}$ o corpo com dois elementos e B^n o produto cartesiano de n cópias do conjunto binário B considerado como um grupo abeliano sobre a adição. Uma palavra de comprimento n é uma *string* de n dígitos binários. Consideremos $f : B^m \to B^n$ uma função código que associa uma palavra w de comprimento m a uma palavra $f(w)$ de comprimento n. Uma palavra código é qualquer palavra de comprimento n na imagem de f. O peso de uma palavra binária w, denotado por $|w|$, é definido como a quantidade de números 1 na sua expressão binária. Também definimos a distância entre códigos binários v, w de mesmo comprimento como sendo $d(v, w) = |v - w|$.

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

© 2017 SBMAC

Teorema 1. *Seja $f : B^m \to B^n$ uma função código. Então f permite a detecção de k ou menos erros se, e somente se, a menor distância entre palavras códigos distintas é $k + 1$.*

Teorema 2. *Seja $f : B^m \to B^n$ uma função código. Então f permite a correção de k ou menos erros se, e somente se, a menor distância entre palavras códigos distintas é pelo menos $2k + 1$*

Definição 1. *Seja $f : B^m \to B^n$ uma função código, se f produz um código linear, a imagem de f forma um subgrupo de B^n.*

Uma das vantagens para se usar códigos lineares é que facilita o cálculo da distância mínima entre palavras código. Assim apresentaremos um método para produzir códigos lineares. Para isso vejamos o que venha ser uma matriz geradora.

Definição 2. *Sejam m, n números inteiros, com $m < n$. Uma matriz geradora G é uma matriz $m \times n$ com entradas em B. As primeiras m colunas formam a matriz identidade $m \times m$ denotada por I_m. Podemos escrever tal matriz como uma matriz particionada: $G = (I_m A)$, onde A é uma matriz $m \times (n - m)$.*

Dada uma matriz geradora G $m \times n$ podemos encontrar uma função código correnpondente da seguinte maneira: $f = f_G : B^m \to B^n$ onde $f_G(w) = wG$ para $w \in B^m$. Para finalizar mostraremos que o conjunto de palavras código formam um grupo com respeito a operação de adição.

Teorema 3. *Seja G uma matriz geradora. Então f_G é um código linear é, de fato, $f_G(v, w) = f_G(v) + f_G(w)$ para todas as palavras v, w.*

3 Conclusões

Vemos neste trabalho uma aplicação da teoria de grupos na teoria de códigos lineares através de matrizes geradoras. Também implementamos a teoria de códigos lineares com auxílio do GAP para podermos trabalhar com matrizes geradoras de ordem elevada, assim podendo corrigir erros de mensagens com grande número de palavras.

Referências

[1] J. F. Humphreys, M. Y. Prest. *Numbers, Groups and Codes*. Cambridge University Press, New York, 2004.

[2] C. P. Milies, *Breve Introdução à Teoria de Códigos Corretores de Erros*, Colóquio de Matemática da Região Centro-Oeste, 2009.

© 2017 SBMAC