CÓDIGOS CORRETORES DE ERROS

Renata Yuri Yokosawa Fujisawa (PIC/CNPq/Uem), Osvaldo Germano do Rocio (Orientador), e-mail: ogrocio@gmail.com; Marcos André Verdi (Coorientador) e-mail: maverdi@uem.br.

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

Matemática/Matemática Aplicada

Palavras-chave: código de bloco, código linear, Máxima Distância Separável (MDS).

Resumo:

Neste trabalho apresentamos noções introdutórias da teoria de códigos corretores de erros. Foram estudados conceitos e definições inerentes à teoria e alguns de seus resultados. Ainda, estudamos os códigos de bloco lineares, os códigos de Máxima Distância Separável (MDS) e, em particular, provamos que não existe um *(4,2,3)-código MDS* sobre um alfabeto binário.

Introdução

A teoria de códigos intervém em nosso cotidiano sempre que alguma mensagem é transmitida ou algum dado é estocado. Isso porque, por melhor que um sistema de comunicação seja projetado, ele sempre estará sujeito a perturbações causadas por algum tipo de ruído, falha humana ou erro do próprio sistema. Com isso, mensagens transmitidas ou dados estocados podem ser diferentes dos originais e aí entra a teoria de códigos, que visa a detectar a ocorrência de algum erro e, depois, tentar corrigi-lo (OZIERANSKI, 2000).

Na prática, procura-se criar sistemas de comunicação que transmitam informações por meio de canais com a maior confiabilidade possível, isto é, sistemas que possuam uma taxa de erros suficientemente pequena. Para atingir esse objetivo, utilizam-se principalmente os códigos denominados lineares, que são aqueles que se caracterizam por estarem munidos de alguma estrutura algébrica que fornece uma maior simplicidade no processo de codificação e decodificação (MILIES, 2009).

Uma das classes refinadas dos códigos lineares é a dos códigos de Máxima Distância Separável (MDS), em que é válida a igualdade $d = n - k + 1$, onde d é a distância mínima de Hamming, n é a quantidade de dígitos das

palavras-código e *k* é a quantidade de dígitos informativos (OZIERANSKI, 2000).
O objetivo final deste trabalho é demonstrar que não existe um código binário de bloco tal que $n = 4$, $k = 2$, e $d = 3$.

Materiais e métodos

Este projeto foi realizado por meio da leitura dos trabalhos constantes nas referências, além de apresentação de seminários semanais.

Resultados e Discussão

Inicialmente, antes de adentrarmos aos resultados inerentes à teoria, apresentemos os **parâmetros fundamentais** de um código, que estudamos em Hefez (1994) e Ozieranski (2000). Os tópicos de Álgebra Linear, necessários para o desenvolvimento do trabalho foram estudados em Lima (2001).
Um código *C* sobre um alfabeto A_q *possui três parâmetros fundamentais:* o **comprimento** das palavras-código (*n*); a **quantidade de elementos** de *C* (*M*); e a **distância mínima de Hamming** (*d*), que indica a menor distância de Hamming entre elementos distintos de *C*, tomados dois a dois.
A partir desses três parâmetros, podemos extrair a quantidade de dígitos informativos de uma palavra-código, isto é, a **dimensão** (*k*) de um código finito, por meio da igualdade $k = \log_q M$.
Na prática, sabemos que a classe de códigos mais utilizada é a dos **códigos de bloco lineares**, que são códigos em que todas as palavras têm o mesmo número *n* de dígitos e os dígitos redundantes são calculados somando módulo *q* (MILIES, 2009). Nesse caso, quando o conjunto de índices *I* é finito, todos os parâmetros fundamentais são bem definidos e, assim, podemos fazer referência a um código de bloco linear com palavras-código de comprimento *n*, *k* dígitos de informação e distância mínima *d* simplesmente indicando-o como *(n,k,d)-código de bloco*.
Feitas essas considerações introdutórias, podemos avançar a um primeiro resultado importante:

Proposição 1 Num *(n,k,d)-código de bloco* de tamanho *M*, temos que:
(i) $1 \leq M \leq q^n$;
(ii) $0 \leq k \leq n$;
(iii) $d \leq n - k + 1$ (limitante de Singleton).

Trata-se de resultado relevante porque relaciona os parâmetros de um código.

Quanto ao item (iii), ressalte-se que, quando um código satisfaz o limitante de Singleton com igualdade, ele é denominado **código de Máxima Distância Separável**, ou código MDS. Trata-se de um código considerado refinado justamente por atingir o limitante de Singleton. Por conta disso, para se comparar duas classe de códigos diferentes, uma forma viável é através dos códigos MDS (OZIERANSKI, 2000).
Outro resultado importante envolvendo os parâmetros de um *(n,k,d)-código de bloco* é o seguinte:

Proposição 2 Num *(n,k,d)-código de bloco*, todos os subconjuntos J do conjunto de índices I, cuja cardindalidade é k, são conjuntos de informação.

Inicialmente, esclarecemos que, dado um *(n,k,d)-código de bloco*, um **conjunto de informação** do código é qualquer subconjunto J de um conjunto de índices I, com $|J| = k$, tal que a função projeção de A_q^I sobre A_q^J definida por $P_J((a_k)_{k\in I}) = (a_k)_{k\in J}$ é injetora.
Este resultado mostra que, num *(n,k,d)-código de bloco*, para quaisquer $J \subseteq I$, tal que $|J| = k$, $P_J(a) \neq P_J(b)$ sempre que $a \neq b$, com $a,b \in C$.
Como corolário, podemos mostrar que não existe um *(4,2,3)-código de bloco* sobre um alfabeto binário *{0,1}*. Para isso, verificamos todas as possibilidade de combinações para o código C que satisfaçam a hipótese de que os subconjuntos J contendo $k = 2$ elementos é conjunto de informação. Ao final, no entanto, observamos que não existem combinações desse tipo possíveis.
Portanto, não obstante o limitante de Singleton tenha sido atingido, não existe um código de bloco sobre um alfabeto binário *{0,1}* tal que $n = 4$, $k = 2$ e $d = 3$.

Conclusões

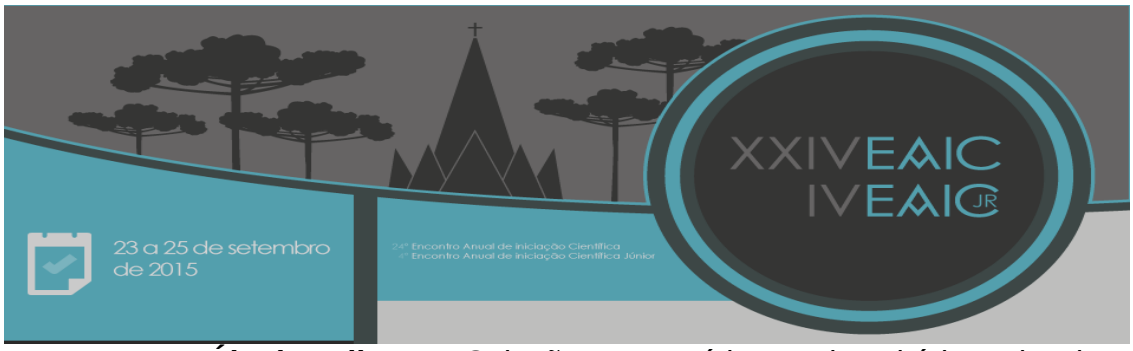
O trabalho conclui que não existe um código de bloco sobre um alfabeto binário *{0,1}* tal que $n = 4$, $k = 2$ e $d = 3$, não obstante o limitante de Singleton tenha sido atingido.

Agradecimentos

Agradeço ao meu orientador, Dr. Osvaldo Germano do Rocio, por sua paciência e motivação ao longo deste trabalho.

Referências

HEFEZ, A. **Teoria dos Códigos**. Campinas, UNICAMP, 1994.



LIMA, E. J. **Álgebra linear**. Coleção Matemática Universitária. Rio de Janeiro: SBM, 2001.

MILIES, C. P. Sociedade Brasileira de Matemática, Colóquio de Matemática da Região Centro-Oeste, 2009. **Breve introdução à Teoria dos Códigos Corretores de Erros**. Campo Grande, MS: Departamento de Matemática, Universidade Federal do Mato Grosso do Sul, 2009.

OZIERANSKI, M. **Introdução à Teoria de Códigos Corretores de Erros**. 2000. 57f. Monografia (Especialização)-Departamento de Matemática, Universidade Estadual de Maringá, Maringá, 2000.