

INTRODUÇÃO AOS CÓDIGOS CORRETORES DE ERROS

Gabriel Vinícius Brandão (PIBIC/CNPq/FA/UEM), Eduardo Brandani da Silva
(Orientador), e-mail: ebsilva@uem.br

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

Ciências Exatas e da Terra - Matemática

Palavras-chave: códigos corretores de erros, códigos lineares, corpos finitos

Resumo:

Através do estudo da fundamentação necessária para construção de códigos corretores de erros, o projeto teve como foco compreender a definição e estruturação de um código em geral, bem como estudar os diversos tipos de códigos corretores existentes.

Introdução

A existência de erros em sistemas de comunicações são inerentes à obtenção de dados e também são devidos a fatores aleatórios e completamente naturais. Tanto que existem estudos voltados para minimizar e corrigir os erros dentro de um ambiente de pesquisa ou de obtenção de quaisquer tipos de dados. E assim, o interesse do ser humano na correção de erros faz parte do cotidiano. Desde a linguística, até as atividades mais ordinárias no cotidiano apresentam erros que podem ser corrigidos de forma mais ou menos precisa. Navegando pela internet, assistindo televisão ou ouvindo músicas, os meios que utilizados para obter informação passam por um tratamento de dados que envolvem algoritmos que corrigem erros quando os encontram.

Um código corretor de erros, portanto, trata-se de um modo bem estruturado de recuperar informações, detectar erros e corrigi-los. Assim, o objetivo de um código é acrescentar ou substituir dados que em alguma etapa foram captados/transmitidos errados. A Teoria dos Códigos Corretores de Erros então, apresenta uma investigação moderna e tecnológica, de problemas que não são necessariamente advindos do avanço da pesquisa e da tecnologia. Muitos dos problemas que tinham-se anteriormente a esse estudo agora podem ser resolvidos. A Teoria tem uma forte fundamentação matemática, que serve de base para a própria construção dos códigos.

Neste trabalho, estudou-se toda a fundamentação matemática necessária para a construção de um código, para, posteriormente, estudarem-se os códigos em si e suas construções.

Materiais e métodos

O estudo deu-se por meio da leitura de livros e artigos relacionados ao assunto, bem como a apresentação de seminários semanais com o orientador, e leituras aprofundadas em encontros. A metodologia do projeto foi a típica da área da Matemática, estudando as estruturas básicas não anteriormente conhecidas.

Resultados e Discussão

Abaixo vamos relacionar as principais definições e conceitos estudados, bem como os resultados mais importantes que foram estudados. Maiores detalhes podem ser encontrados nas referências listadas ao fim do resumo.

Antes de explicarmos as definições formais de um código, vamos dar uma ideia geral. De forma simples, um código corretor de erros é um código que transforma o sinal de uma fonte, detecta e corrige erros no momento da recepção e decodifica novamente em informações úteis, como arquivos, comandos, instruções, dentre outros. Da fonte do sinal, parte um código, que é traduzido como as informações que queremos no fim da recepção, e este é chamado de código da fonte. Entretanto, para aumentar a eficiência de um código, introduzimos o chamado código de canal, que acrescenta redundâncias neste. A figura 1 mostra um esquema do caminho pelo qual é passada a informação até que chegue ao usuário com a quantidade mínima de erros possíveis.

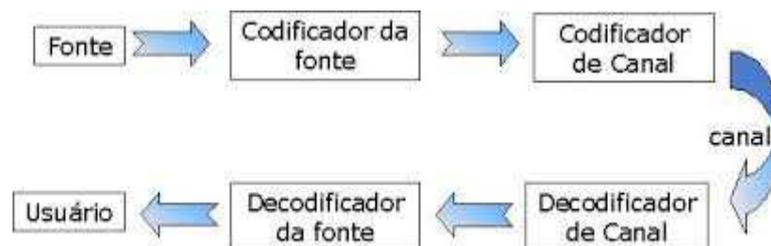


Figura 1 – Funcionamento simplificado de um código da fonte até o que é mostrado ao usuário

Formalmente, dado um conjunto A finito qualquer chamado de alfabeto, com q elementos, e um natural n , um código corretor de erros é um subconjunto qualquer de A^n . Com isso em mente, podemos definir uma importante noção, de proximidade entre palavras de um código, através da métrica e da distância de *Hamming*. Em símbolos, a distância entre dois elementos $u, v \in A^n$, é definida como:

$$d(u, v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|.$$

Uma outra noção pertinente é introduzida: a de distância mínima. Em símbolos, a distância mínima d de um código C é:

$$d = \min\{d(u, v); u, v \in C \text{ e } u \neq v\}.$$

A definição de distância mínima de um código é muito importante, pois, podemos assim analisar a capacidade de correção de erros de um código. Conseguimos obter o resultado de que um código qualquer é capaz de detectar até $d - 1$ erros. Este resultado é muito importante pois indica de forma direta a eficiência de um código e observamos que quanto maior a distância mínima, maior a capacidade de correção e de detecção.

Estes fundamentos são muito importantes para a discussão de códigos em geral. Contudo, os códigos mais complexos e de fato funcionais, são apresentados com uma forte fundamentação matemática. Como o objetivo principal deste trabalho não é estudar a fundamentação, não iremos nos alongar nesta direção. Contudo, é importante ressaltar que diversos resultados foram obtidos com o estudo de: Anéis e Corpos, Polinômios e Corpos Finitos, que são base para construção de todos os códigos estudados posteriormente.

Finalizaremos então por introduzir e comentar os principais resultados do estudo dos códigos lineares, por este ser um dos maiores objetivos do projeto como um todo.

Assim sendo, dado um corpo finito denotado por K , com q elementos tomado como alfabeto, temos para cada natural n um K -espaço vetorial K^n de dimensão n . Definimos então um código linear como sendo um subespaço vetorial de K^n . A partir desta definição, constroem-se diversas noções para a construção de um código linear. Tais como: um código como uma transformação linear, a matriz geradora de um código, a matriz teste de paridade, que são todas ferramentas que tornam este tipo de códigos (os lineares) muito importantes e de fácil aplicação, uma vez que são todos baseados em fundamentos de álgebra linear.

Ainda, estudou-se diversas aplicações de famosos códigos corretores. Um código que se destaca foi utilizado pela NASA, na nave *Mariner 9*, para obtenção das imagens do planeta Marte. O código utilizado por eles é um código de uma família chamada de *Códigos de Reed-Muller de Primeira Ordem*, que também são lineares.

Assim, os resultados foram obtidos através do contato por parte do acadêmico a aspectos da Matemática que não se tinham conhecimento, possibilitando o estudo de técnicas para construções de diversos tipos de códigos corretores de erros.

Conclusões

Os tópicos estudados sobre os códigos corretores de erros, e seus diversos tipos, bem como toda a estrutura matemática aprendida, foram de muita utilidade para uma aproximação com a aplicação de uma teoria matemática dentro de um contexto tecnológico, e aplicável. Levantaram-se discussões sobre diversas demonstrações matemáticas, possibilitando a introdução ao meio da pesquisa científica em uma área não abordada na grade curricular do seu curso.



Agradecimentos

Agradecimentos ao CNPq, à Fundação Araucária e à UEM pelo apoio financeiro.

Referências

HEFEZ, Abramo; VILLELA, Maria Lúcia. **Códigos corretores de erros**. 2. Ed. Rio de Janeiro: IMPA, 2008. 216 p.

S. A. Vanstone; P. C. van Oorschot. **An Introduction to Error Correcting Codes with Applications**. Kluwer Academic Publishers, 1989.