INFORMAÇÕES GERAIS DO TRABALHO

Título do Trabalho: Códigos Corretores de Erros

Autores: **Letícia Aparecida de Figueiredo**[1]
Gabriel Souza de Oliveira[2]
Sávio Ribas[3]

Palavras-chave: códigos corretores de erros, detecção e correção de ruídos, matemática
Campus: Ouro Preto
Área do Conhecimento (CNPq): **1.01.00.00-8 Matemática (Grande Área)**
1.01.01.00-4 Álgebra
1.01.02.00-0 Análise
1.01.04.00-3 Matemática Aplicada

RESUMO

Com o gradativo crescimento tecnológico, a cada dia torna-se mais necessário o envio e recebimento de informações, seja para assistir televisão, para navegar na internet, para armazenar dados ou, até mesmo, para monitorar satélites e robôs em Marte. A transmissão de dados está presente no cotidiano de todos, em enorme quantidade e a todo momento. No meio dessa transmissão, é possível que haja a interferência de certos ruídos. Para garantir que a mensagem chegue sem erros ao destinatário, os aparelhos digitais usam uma técnica matemática, aplicada a um algoritmo, conhecida como Códigos Corretores de Erros. Um código corretor de erros é, essencialmente, uma forma de acrescentar ambiguidades a cada informação que se queira transmitir ou armazenar, de forma a permitir a detecção e a correção de erros ao recuperar uma informação. O objetivo da pesquisa é entender, do ponto de vista matemático, os fundamentos envolvidos nos códigos corretores de erros. Para isso faz-se necessário compreender diversos conceitos abstratos, tais como anéis e corpos, corpos finitos, fatoração de polinômios com os coeficientes em um determinado corpo, matrizes e operações elementares, relações de equivalência entre códigos (ou, de forma análoga, relações de equivalência entre matrizes) e métrica. O método de pesquisa está sendo baseado, principalmente, no estudo do livro “Códigos Corretores de Erros” [2] (HEFEZ-VILLELA, 2008), que contém toda a base matemática necessária para a compreensão dos códigos, além de diversos códigos que já foram utilizados para detecção e correção de erros. Atualmente, todo o embasamento teórico matemático necessário já foi absorvido, possibilitando o prosseguimento no estudo dos diversos códigos existentes. Os próximos temas a serem estudados são os Códigos Lineares (nos quais aplicaremos os conceitos algébricos de matrizes e operações elementares) e, em seguida, os Códigos Cíclicos (nos quais aplicaremos os conceitos de anéis, corpos finitos e polinômios irredutíveis). A partir do conhecimento consolidado, futuramente, será possível

[1] UFOP, Voluntária do programa Mentores da OBMEP, e-mail: *le.fig22@gmail.com*
[2] IFMG - Campus Ouro Preto, Bolsista do programa Mentores da OBMEP / CNPq, e-mail: *gabriel_gdi3@hotmail.com*
[3] IFMG - Campus Ouro Preto, Orientador do programa Mentores da OBMEP, e-mail: *savio.ribas@ifmg.edu.br*

implementar algoritmos eficientes capazes de detectar e corrigir erros, aperfeiçoando a transmissão de dados.

INTRODUÇÃO

Uma enorme quantidade de dados é transmitida a todo momento nos dias de hoje. Os dois principais problemas nessa transmissão são:

- ✓ Garantir que, se a mensagem for interceptada por um indivíduo diferente do destinatário, esta esteja codificada e este indivíduo não consiga compreendê-la, mas o destinatário consiga decodificá-la sem maiores problemas;
- ✓ Garantir que a mensagem chegue sem erros (ou ruídos) ao destinatário.

O primeiro problema é resolvido usando Criptografia, e não é tratato nessa pesquisa. O segundo problema é resolvido usando os Códigos Corretores de Erros. Durante a transmissão de dados às vezes ocorrem problemas (como interferências eletromagnéticas ou erros de digitação, por exemplo) que fazem com que a mensagem recebida seja diferente da mensagem enviada. Essa pesquisa visa desenvolver métodos que permitam detectar e corrigir esses ruídos. Por exemplo, na língua portuguesa, usamos um alfabeto com 23 letras e as palavras são sequências de letras (mas não todas as sequências possíveis). Certas vezes, reconhecemos que algumas palavras não fazem parte da língua, como por exemplo as palavras “teoxia” e “qato”. Observamos que houve um erro ao escrever cada uma dessas palavras. A primeira delas, sem dúvida, deveria ser a palavra “teoria” pois é a palavra do alfabeto que está *mais próxima* da palavra recebida (em certo sentido). Por outro lado, a segunda palavra pode ser “bato”, “fato”, “gato”, “jato”, “mato”, “nato”, “pato”, “rato” ou “tato”. Todas essas palavras são *igualmente próximas* a “qato”. Isso significa que em “teoxia” conseguimos detectar e corrigir o erro, mas em “qato” conseguimos apenas detectar o erro.

Os códigos corretores de erros aparecem no nosso dia-a-dia de inúmeras formas, como por exemplo quando assistimos televisão, falamos ao telefone, ouvimos um CD de música, assistimos um filme em DVD ou navegamos pela internet. Um código corretor de erros é, essencialmente, uma forma de acrescentar ambiguidades a cada informação que se queira transmitir ou armazenar, de forma a permitir detectar e corrigir erros ao recuperar a informação. Por exemplo, é notória a diferença de qualidade entre a TV analógica e a TV digital, mas como o conversor digital faz a TV exibir a imagem e o som quase perfeitos, ante a resolução analógica? Ao final dessa pesquisa, seremos capazes de responder essa pergunta.

Essa teoria surgiu na década de 40, no Laboratório Bell de Tecnologia, com os trabalhos de Hamming [1] e de Shannon [4]. Os computadores da época eram capazes de detectar erros nas perfurações dos cartões, e Hamming teve a ideia de fazer com que os computadores também localizassem a posição do erro e corrigissem-o. Shannon conseguiu criar códigos mais eficientes que aqueles propostos por Hamming. Para mais detalhes sobre a história dos códigos corretores de erros, consulte [3].

Um dos objetivos de um código é que ele possua uma quantidade grande de palavras para poder transmitir muita informação, mas que consiga detectar e corrigir muitos erros. Além disso, espera-se que possua algoritmos de codificação e decodificação simples e rápidos. Infelizmente, esses objetivos conflitam entre si. A questão de encontrar valores satisfatórios para essas variáveis é o principal problema da teoria de códigos.

METODOLOGIA

O método de pesquisa está sendo baseado, principalmente, no estudo do livro “Códigos Corretores de Erros” [2], que contém toda a base matemática necessária para a compreensão dos códigos, além de diversos códigos que já foram utilizados para detecção e correção de erros. Ademais, o grupo de pesquisa se reúne periodicamente para discussão, esclarecimento de dúvidas e resolução de exercícios, além das orientações virtuais essenciais para superar a incompatibilidade de horários disponíveis.

RESULTADOS E DISCUSSÕES

Foram estudados objetos matemáticos tais como anéis e corpos, corpos finitos, fatoração de polinômios com os coeficientes em um determinado corpo, matrizes e operações elementares e métrica. Dessa forma, todo o embasamento teórico matemático necessário já foi absorvido, possibilitando o prosseguimento no estudo dos diversos códigos existentes. Os próximos temas a serem estudados são os Códigos Lineares (nos quais aplicaremos os conceitos algébricos de matrizes e operações elementares) e, em seguida, os Códigos Cíclicos (nos quais aplicaremos os conceitos de anéis, corpos finitos e polinômios irredutíveis). A partir do conhecimento consolidado, futuramente, será possível implementar algoritmos eficientes capazes de detectar e corrigir erros, aperfeiçoando a transmissão de dados.

CONCLUSÕES

A Teoria de Códigos Corretores de Erros é uma sub-área da Matemática que une Álgebra Linear, Álgebra Abstrata, Corpos Finitos e Topologia, e é muito ativo e atual dos pontos de vista científico e tecnológico. Uma de suas virtudes é mesclar conceitos e técnicas matemática importantes com aplicações imediatas na vida real, além de ser intrinsecamente interessante. Isso tudo mostra como a sofisticação tecnológica torna cada vez mais interessante a associação entre a Matemática Pura e a Aplicada.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] HAMMING, R. W., *Error Detecting and Error Correcting Codes*, The Bell System Technical Journal, vol. XXVI, 1948, p. 379 – 423, 623 – 656.
[2] HEFEZ, A., VILLELA, M. L. T., *Códigos Corretores de Erros*, Rio de Janeiro, IMPA, 2008.
[3] MILIES, C. P., *Introdução à Teoria dos Códigos Corretores de Erros*, Colóquio de Matemática da Região Centro-Oeste. Campo Grande, SBM, 2009.
[4] SHANNON, C. E., *A Mathematical Theory of communication*, The Bell System Technical Journal, vol. XXVIII, 1950.

Participação em Congressos, publicações e/ou pedidos de proteção intelectual: Não se aplica.