CÓDIGOS CORRETORES DE ERROS: A MÉTRICA E HAMMING COMO UMA FERRAMENTA DE DETECÇÃO E CORREÇÃO DE ERROS

OLIVEIRA, Rayanne Pinheiro de[1]; **OLIVEIRA JUNIOR**, José Carlos de[2]

RESUMO

Esta pesquisa explora os códigos corretores de erros que desempenham um papel crucial nas tecnologias, principalmente nos meios de informação e comunicação. O objetivo geral dessa pesquisa é estudar a teoria dos códigos corretores de erros de forma a compreender como os códigos corretores de erros funcionam e analisar a detecção e a correção de determinados erros. Com o tempo, houve uma particularização nas classes de códigos estudados, com isso o cerne da investigação consistiu, posteriormente, em responder à seguinte questão norteadora: Como determinar uma relação entre parâmetros de um código linear para saber se o mesmo é ou não perfeito? O objetivo principal deste estudo consiste em estabelecer uma sólida conexão entre os parâmetros de um código linear e sua qualidade de código perfeito. Dentro desse escopo, os objetivos específicos deste trabalho abrangem uma exploração aprofundada dos conceitos fundamentais da Álgebra Linear e Abstrata, abordando elementos como classes residuais de inteiros, espaços vetoriais, corpos, transformações lineares e outras noções pertinentes. Além disso, termos essenciais, como métrica, espaços métricos, raio de empacotamento de um código, métrica de Hamming, códigos lineares e códigos perfeitos, são rigorosamente definidos e examinados em profundidade. Por meio de

[1] Bolsista do Programa de Iniciação Científica (PIBIC). Universidade Federal do Norte do Tocantins (UFNT), Centro de Ciências Integradas. rayanne.pinheiro@mail.uft.edu.br.
[2] Orientador do Programa de Iniciação Científica (PIBIC). Universidade Federal do Norte do Tocantins (UFNT), Centro de Ciências Integradas. jc.oliveira@mail.uft.edu.br.

uma análise abrangente desses conceitos, o foco não se restringe somente à apresentação introdutória dos códigos corretores de erros, mas também visa estabelecer um sólido alicerce teórico para a determinação de códigos perfeitos com base em seus parâmetros de códigos lineares, conforme evidenciado no Teorema (Pinheiro-Oliveira). Além disso, os estudos nessa pesquisa não estar estrito somente a uma área de estudo da matemática, mas também a outras áreas, como Probabilidade, Álgebra Abstrata, Teoria de Números, Teoria de Grupos, Álgebra Linear e Matemática Aplicada.

Palavras-chave: Códigos Corretores de Erros. Álgebra. Códigos Lineares. Matemática Aplicada.

I. INTRODUÇÃO/JUSTIFICATIVA

A Matemática, ao longo dos séculos, tem revolucionado a sociedade em inúmeras áreas, como tecnologia, construção, política, medicina, finanças e economia. Isso despertou meu interesse em estudar sua aplicabilidade, especialmente em áreas que muitas pessoas não percebem. Ao escolher meu orientador de PIBIC, ele me introduziu aos Códigos Corretores de Erros. Sempre tive curiosidade em entender a matemática por trás das tecnologias, particularmente na comunicação e informação, e como coisas intangíveis, como ligações de voz, podem transmitir mensagens pelo mundo. Isso me fez perceber a vastidão da matemática. Portanto, desenvolvemos esta pesquisa para tornar a matemática acessível a estudantes de ensino básico e graduação, ajudando-os a compreender seu papel em situações do dia a dia, como mencionado anteriormente.

II. BASE TEÓRICA

Como a pesquisa é essencialmente de cunho bibliográfico, utilizou-se alguns livros relacionados com o tema estudado. Para compreendermos melhor essa teoria, de forma introdutória, utilizou-se o livro “Códigos Corretores de Erros - Notas de Aulas” de Marcelo Firer. Além disso, precisou-se de alguns estudos complementares obtidos a partir do livro de “Álgebra Linear” de José Luiz Boldrini e “Álgebra Moderna” de Hygino H. Domingues e Gelson Iezzi. E como fonte para estudos mais aprofundados utilizou-se o livro “Códigos Corretores de Erros” de Abramo Hefez e Maria Lúcia T. Villela.

III. OBJETIVOS

O objetivo desse trabalho de pesquisa consiste em estudar a teoria dos códigos corretores de erros de forma a compreender como os códigos corretores de erros funcionam e analisar a detecção e a correção de determinados erros. Como objetivos específicos este trabalho propõe:

- Estudar classes residuais de um inteiro;
- Definir alfabeto, letra e palavra na linguagem dos códigos;
- Compreender os códigos lineares a partir de exemplos;
- Definir a métrica de Hamming;
- Provar o Teorema Pinheiro-Oliveira;
- Aplicar os conceitos da Álgebra na Teoria dos Códigos em geral.

IV. METODOLOGIA

A pesquisa realizada é categorizada como exploratória, delineada para a obtenção de informações sobre a temática selecionada e sua delimitação. No tocante à coleta de dados, é adotada a abordagem de pesquisa bibliográfica, ancorando-se na análise de materiais previamente publicados. Quanto à abordagem, é adotada uma perspectiva qualitativa, focando-se não em dados estatísticos, mas sim na captação direta de informações do objeto de estudo.

O bolsista se encontrava uma vez por semana com o professor para discutir os resultados encontrados a partir da revisão bibliográfica dos textos base. O professor, ao final de cada encontro, deixava uma tarefa relacionada ao que tinham estudado, para que o bolsista continuasse seus estudos durante a semana.

V. RESULTADOS E DISCUSSÃO

Primeiramente, estudamos conceitos básicos de Álgebra necessários para compreender os códigos corretos de erros. Entre eles, estão as definições de corpos, corpos finitos, classes residuais, espaços vetoriais, subespaços vetoriais, base e dimensão de um espaço vetorial, transformações lineares, núcleo e imagem de uma transformação linear. Posteriormente, estudamos os conceitos iniciais sobre códigos corretos de erros e códigos lineares, cujas definições mais pertinentes estão apresentadas a seguir. A construção dessa sessão é embasada nas seguintes referências bibliográficas: (BOLDRINI, 2022), (DOMINGUES, 2003), (FIRER, 2007) e (HEFEZ; VILLELA, 2017).

Definição 1 *(Métrica de Hamming) Dados dois elementos* $u, v \in \mathbb{F}^n$*, a distância de Hamming entre* u *e* v *é definida como*

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

A distância de Hamming entre os elementos de $\mathbb{F}^n$ é também chamada de métrica de Hamming, pois caracteriza-se como uma métrica.

Definição 2 *(Discos e esferas) Dados* $a \in \mathbb{F}^n$ *e* $t \geq 0$*, tal que* $t \in \mathbb{R}$*, definimos o* ***disco*** *e a* ***esfera*** *de centro em* a *e raio* t *como sendo os respectivos conjuntos:*

$$D(a,t) = \{u \in \mathbb{F}^n | d_H(u,a) \leq t\}$$

$$S(a,t) = \{u \in \mathbb{F}^n | d_H(u,a) = t\}.$$

Lema 3 *Para todo* $a \in \mathbb{F}^n$ *e todo número natural* $r > 0$*, temos que*

$$|D(a,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

Definição 4 *(Distância mínima) Seja* C *um código. A distância mínima de* C *é o número*

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

Definição 5 *(Menor inteiro) Seja* C *um código com distância mínima* d*, define-se*

$$\kappa = \left[\frac{d-1}{2}\right],$$

onde $[t]$ *representa a parte inteira de qualquer número real* t*.*

Lema 6 Seja C um código com distância mínima d. Se $u, v \in C$ e $u \neq v$, então

$$D(u,\kappa) \cap D(v,\kappa) = \emptyset.$$

Teorema 7 Seja $C \subset A^n$ com distância mínima d. Então:

(i) C detecta até $d-1$ erros;

(ii) C corrige até $\kappa = \left[\frac{d-1}{2}\right]$ erros.

Definição 8 (Códigos Perfeitos*) Seja* $C \subset \mathbb{F}_q^n$ *um código com distância mínima* d *e seja* $\kappa = \left[\frac{d-1}{2}\right]$*. O código* C *será dito perfeito se*

$$\left|\bigcup_{c\in C} D(c,\kappa)\right| = \mathbb{F}_q^n.$$

Vamos fazer uma observação particular aqui. Por que o nome do código é *perfeito?* A definição de códigos perfeitos nos mostra que: para qualquer palavra pertencente ao espaço $\mathbb{F}_q^n$, a distância em relação às palavras do código jamais excede κ. Essa propriedade intrínseca assegura a possibilidade de detectar e corrigir eficazmente quaisquer erros introduzidos, visto que a palavra recebida se encontrará contida em um dos discos com raio κ e centro c, que não possui interseção com qualquer outro disco dessa natureza.

Definição 9 *(Códigos Lineares) Um código $C \subset \mathbb{F}^n$ será chamado de código linear se for um subespaço vetorial de $\mathbb{F}^n$.*

Códigos Perfeitos e seus Parâmetros

Neste tópico, delinearemos a essência de nosso trabalho: empregar os conceitos previamente estudados para determinar uma condição necessária e suficiente para que alguns códigos lineares sejam códigos perfeitos.

Esse resultado, que é o principal deste trabalho, foi desenvolvido pela autora desta monografia e pelo seu orientador. Após muitas pesquisas em várias bibliografias e artigos na internet, entendemos que seja um resultado novo. Sua demonstração é relativamente acessível, porém requer todo aparato trazido até aqui no trabalho além de teoremas importantes da álgebra.

Aqui, considere $\mathbb{Z}_q$ um corpo (e, portanto, q é primo).

Teorema 10: (Pinheiro-Oliveira) Um código linear $C \subset \mathbb{Z}_q^n$, com distância mínima $d = 3$ ou $d = 4$, é perfeito se, e somente se, $n = 1 + q + q^2 + \cdots + q^{n-\frac{\ln|C|}{\ln q}-1}$.

Demonstração: Se $d = 3$ ou $d = 4$, temos $\kappa = 1$. Nessas condições, pela Definição 8, temos que C é perfeito se, e somente se,

$$\left|\bigcup_{c\in C} D(c,1)\right| = \mathbb{Z}_q^n.$$

Como pelo Lema 6, $D(c_1,\kappa) \cap D(c_2,\kappa) = \emptyset$, para todo $c_1, c_2 \in C$, tem-se:

$$C \text{ é perfeito} \Leftrightarrow \sum_{c\in C} |D(c,1)| = \left|\mathbb{Z}_q^n\right| = q^n.$$

Já pelo Lema 3 $|D(a,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$, para todo $a \in C$, segue que

$$C \text{ é perfeito} \Leftrightarrow |C| \cdot |D(c_0, 1)| = q^n,$$

com $c_o \in C$ um elemento fixo qualquer. Assim, C é perfeito se, e somente se,

$$|C| \cdot \sum_{i=0}^{1} \binom{n}{i} (q-1)^i = q^n.$$

O espaço vetorial $\mathbb{Z}_q^n$ é um grupo aditivo e $C \subset \mathbb{Z}_q^n$ é um subgrupo aditivo. Logo, pelo Teorema de Lagrange (ver páginas 189 e 190 de [3]) o número $|C|$ divide $\left|\mathbb{Z}_q^n\right| = q^n$. Como $\mathbb{Z}_q$ é corpo, temos que q é primo. Assim, $|C|$ divide q^n implica que $|C| = q^m$ para algum $m \leq n$. Logo,

$$C \text{ é perfeito} \Leftrightarrow q^m \cdot \sum_{i=0}^{1} \binom{n}{i} (q-1)^i = q^n$$

$$C \text{ é perfeito} \Leftrightarrow 1 + n \cdot (q-1) = q^{n-m}$$

$$C \text{ é perfeito} \Leftrightarrow n = \frac{q^{n-m} - 1}{q-1}$$

$$C \text{ é perfeito} \Leftrightarrow n = 1 + q + q^2 + \cdots + q^{n-m-1}.$$

Note que

$$|C| = q^m \Leftrightarrow ln|C| = m \cdot ln\, q \Leftrightarrow m = \frac{\ln|C|}{\ln q}.$$

Logo,

$$C \text{ é perfeito} \Leftrightarrow n = 1 + q + q^2 + \cdots + q^{n - \frac{\ln|C|}{\ln q} - 1}$$

VI. CONCLUSÃO/CONSIDERAÇÕES FINAIS

Nesta investigação, empenhamo-nos no estudo dos códigos corretores de erros com o propósito de relacionar conceitos matemáticos, buscando uma compreensão mais profunda desta teoria que desempenha um papel significativo na sociedade contemporânea. O cerne da nossa pesquisa concentrou-se na análise de uma classe específica de códigos conhecida como códigos perfeitos. Para alcançar

esse objetivo, apresentamos e discutimos conceitos fundamentais de Álgebra, cujo entendimento é essencial para a construção do objeto de estudo abordado.

É relevante enfatizar que a jornada de investigação na iniciação científica resultou na elaboração do meu Trabalho de Conclusão de Curso (TCC), que foi apresentado e aprovado em 17 de agosto de 2023.

Por último, é notável salientar que a escolha deste tema proporcionou uma série de desafios gratificantes, permitindo-nos adquirir novos conhecimentos e aprofundar conceitos previamente explorados durante nossa trajetória acadêmica. Além disso, essa pesquisa ofereceu uma oportunidade valiosa para uma investigação mais profunda nos campos da Matemática Pura e Aplicada.

VII. REFERÊNCIAS

BOLDRINI, José Luiz et al. **Álgebra Linear**. 3. ed. São Paulo: Harper & Row do Brasil, 1980. 411 p. Disponível em: https://cin.ufpe.br/~brgccf/archive/. Acesso em: 04 dez. 2022.

DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra Moderna**. 4. ed. São Paulo: Atual, 2003. 368 p.

FIRER, Marcelo. **Códigos Corretores de Erros – Notas de Aula**. UNICAMP, Campinas, v. 5, 2007. Recuperado de https://www.ime.unicamp.br/~mfirer/3NotasFoz2006.pdf. Acesso em: 27 maio 2022.

HEFEZ, Abramo; VILLELA, Maria Lúcia T. **Códigos Corretores de Erros**. 2. ed. Rio de Janeiro: IMPA, 2017. 216 p.

VIII. AGRADECIMENTOS

O presente trabalho foi realizado com o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq – Brasil e da Universidade Federal do Norte do Tocantins – UFNT.