CÓDIGOS CORRETORES DE ERROS

Priscila Cunha Vazquez[1], Samir Assuena[2]
[2] Departamento de Matemática, FEI
uniepvazquez@fei.edu.br e samir.assuena@fei.edu.br

Resumo: A Teoria de Códigos Corretores de Erros tem como objetivo transmitir mensagens através de um canal de maneira segura, de forma que o código seja capaz de detectar e corrigir o maior número de erros que possam ocorrer durante essa transmissão. Por conta da importância disso na atualidade, este projeto busca estudar os códigos corretores de erros e suas caracterizações algébricas utilizando-se das teorias de anéis e grupos.

1. Introdução

A Teoria dos Códigos Corretores de Erros se iniciou com o trabalho de Richard Hamming que, frustrado pela capacidade das máquinas de detectar erros, mas não de localizá-los e corrigi-los, publicou o artigo intitulado *Error Detecting and Error Correcting Codes* [1]. Desde então se desenvolveu, consolidando-se como uma área de pesquisa de grande relevância. Seu objetivo é a transmissão de mensagens de forma segura e com a menor quantidade de erros possíveis, corrigindo os que surgirem durante o envio.

Para isso, são necessários algoritmos de codificação e decodificação desses códigos, muitos feitos com base nas teorias de grupos e anéis.

Como exemplo simples, podemos citar o idioma. O alfabeto, com as vogais acentuadas e c cedilha, é o conjunto A, enquanto as palavras são elementos de A^{27}, onde 27 é o comprimento da palavra mais longa da língua portuguesa. Suponhamos que seja escrita a sequência de letras “cathorro”; percebe-se facilmente o erro, e a correção para “cachorro” pode ser feita, por ser a palavra que mais se assemelha à sequência apresentada. Porém, este código não é eficiente, visto que caso a palavra desejada seja “pato”, mas seja escrita como “pano”, não será possível detectar o erro por ambas existirem.

Além deste caso, códigos corretores de erros são utilizados sempre que há a transmissão ou armazenamento de dados, desde comunicações via satélite, até a movimentação de robôs.

2. Funcionamento de um código

Para ilustrar o funcionamento de um código podemos pensar em um robô que se move dentro de um mapa quadriculado. Ele aceita comandos do tipo Norte, Sul, Leste e Oeste, se deslocando para a casa adjacente indicada. Esses comandos podem ser codificados em números binários de dois dígitos da seguinte forma:

$$\begin{array}{rr} \text{Norte} \mapsto 00 & \text{Leste} \mapsto 10 \\ \text{Sul} \mapsto 01 & \text{Oeste} \mapsto 11 \end{array}$$

Esse código tem o nome de “código da fonte”. Porém, neste ponto, existe o mesmo problema do alfabeto citado anteriormente: no caso de haver um erro durante a transmissão, não será possível detectá-lo porque todas as combinações de 0 e 1 correspondem a comandos existentes. Assim, é feita uma recodificação em cima disso, adicionando redundâncias que permitem detectar e corrigir os erros, como por exemplo:

$$\begin{array}{rr} \text{Norte} \mapsto 00 \mapsto 00000 & \text{Leste} \mapsto 10 \mapsto 10110 \\ \text{Sul} \mapsto 01 \mapsto 01011 & \text{Oeste} \mapsto 11 \mapsto 11101 \end{array}$$

Esse segundo código é chamado de “código de canal”, e ele serve justamente para que caso ocorra um erro, seja possível corrigi-lo. Esse procedimento pode ser esquematizado da seguinte forma:

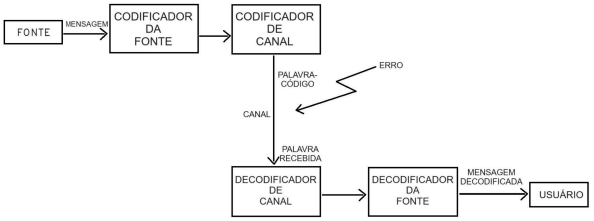

Figura 1 – Sistema de comunicação digital

Com isso, fica claro que é da responsabilidade do código corretor de erros desenvolvido conseguir transformar o código fonte em código de canal, além de detectar e corrigir os erros na recepção da mensagem.

3. Metodologia

Após a exposição da visão geral do funcionamento e objetivos dos códigos corretores de erros, vale destacar que a metodologia utilizada para chegar no nível de entendimento e aplicação deles é a revisão sistemática da bibliografia e discussão dos tópicos em seminários.

Para isso, deve ser feito o levantamento bibliográfico dos temas relativos ao estudo; temos que o funcionamento dos códigos corretores de erros depende de uma série de assuntos matemáticos, então primeiramente estudamos teoria de grupos, álgebra linear e teoria de anéis.

Uma vez que os fundamentos e principais resultados e definições foram compreendidos, foi possível avançar para a parte principal do projeto, que são as diferentes caracterizações algébricas dos principais tipos de códigos corretores de erros, sua estrutura e funcionamento.

4. Métrica de Hamming

Inicialmente, dado um conjunto finito A chamado de alfabeto, temos que um *código corretor de erros* é um subconjunto próprio qualquer do produto cartesiano A^n, para algum n natural. Dados dois elementos u=(u_1, u_2, ..., u_n), v=(v_1, v_2, ..., v_n) ∈ A^n, define-se como *distância de Hamming* entre u e v:

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

Essa distância é utilizada posteriormente para determinar a distância mínima de um código, que é a menor distância entre todas as palavras do código.

Além disto, sendo C um código com distância mínima d, C pode corrigir até κ erros, sendo κ o menor inteiro positivo maior que $[\frac{d-1}{2}]$, e detectar até *d - 1* erros, ou seja, é possível corrigir a palavra que possuir até *d - 1* sem encontrar outra palavra do código.

5. Códigos Lineares

A classe mais utilizada de códigos são os códigos lineares, que por definição são espaços vetoriais de dimensão finita. Assim, sendo F_q um corpo finito com q elementos, $q = p^m$ e p primo, os *códigos lineares* são subespaços vetoriais do espaço F_q^n.

Dado um código linear C de F_q^n, definimos o peso de C como sendo o número $w(C) = min\{w(c), c \in C, c \neq 0\}$.

O peso ganha maior importância uma vez que se é provado e demonstrado que $d(C) = w(C)$, ou seja, que o peso de um código linear é igual à sua distância de Hamming.

Além dessas definições, uma das vantagens dos códigos lineares é a matriz geradora. Assim, vale destacar qual sua definição: sendo C um (n,k,d)-código linear e (v_1, v_2, · · · , v_k) uma base de C sobre F_q, a matriz geradora de C é a k × n matriz cujas linhas são as coordenadas dos vetores desta base (v_1, v_2, · · · , v_k). De forma mais explícita:

$$G = \begin{bmatrix} v_{1_1} & v_{1_2} & \cdots & v_{1_n} \\ v_{2_1} & v_{2_2} & \cdots & v_{2_n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k_1} & v_{k_2} & \cdots & v_{k_n} \end{bmatrix}$$

A matriz também pode ser escrita em sua forma padrão G = $(I_k|A_{k\times(n-k)})$. Dadas duas palavras u=(u_1, u_2, ..., u_n), v=(v_1, v_2, ..., v_n) ∈ A^n, definimos

$$\langle u,v\rangle = u_1v_1 + u_2v_2 + u_3v_3 + \ldots\ldots u_nv_n.$$

É importante definir que dado um (n,k)-código linear C, o código linear $C^{\perp} = \{x \in F_q^n \mid \langle x,c\rangle = 0, \forall c \in C\}$ chama-se código dual de C. Assim, é possível entender o que é uma *matriz teste de paridade.*

Sendo C um código linear com matriz geradora G = $(I_k|A)$, a matriz H = $(A_t|I_{n-k})$ geradora de $C^{\perp}$ é chamada de matriz de teste de paridade do código C. A razão para o nome da matriz H é que c ∈ C se e somente se $cH^t = Hc^t = 0$. Dessa forma, as linhas de H são os coeficientes de um sistema linear homogêneo cujas soluções são as palavras do código C. Estas equações lineares recebem o nome de *equações de teste de paridade*.

Outra classe de códigos de grande importância são os códigos cíclicos, que serão estudados durante a próxima parte da pesquisa.

6. Decodificação

A decodificação de um código é o processo de detecção e correção de erros num determinado código. O principal método utilizado hoje é um aperfeiçoamento do método criado por D. Slepian, chamado de decodificação por síndrome, cujos detalhes serão estudados posteriormente.

7. Conclusões

Num primeiro momento, como a pesquisa ainda não foi finalizada, estamos compreendendo melhor as teorias algébricas por trás dos códigos corretores de erros, como a teoria de grupos e de anéis, além das noções iniciais dos códigos lineares,, para posteriormente sermos capazes de caracterizar algebricamente os códigos cíclicos e usufruir das vantagens que essa caracterização possui.

Dessa forma, os principais resultados são conhecimento e compreensão maior das áreas da matemática, além da habilidade de caracterização algébrica dos códigos corretores de erros.

8. Referências

[1] HAMMING, R. W. Error Detecting and Error Correcting Codes. The Bell Systemm Technical Joural, 1948.

[2] HEFEZ, Abramo; VILLELA, Maria Lúcia T. Códigos Corretores de Erros. Série Computação e Matemática. IMPA, 2008. ISBN 9788524401695.

.

Agradecimentos

À instituição FEI pela oportunidade de pesquisa em teorias algébricas e suas aplicações.

[1] Aluno de IC do Centro Universitário FEI. Projeto com vigência de 02/2024 a 01/2025.