UNIVERSIDADE FEDERAL DO NORTE DO TOCANTINS

CENTRO DE CIÊNCIAS INTEGRADAS

CURSO DE LICENCIATURA EM MATEMÁTICA

RAYANNE PINHEIRO DE OLIVEIRA

CÓDIGOS CORRETORES DE ERROS: DA MÉTRICA DE HAMMING AOS CÓDIGOS PERFEITOS

Araguaína (TO)
2023

RAYANNE PINHEIRO DE OLIVEIRA

CÓDIGOS CORRETORES DE ERROS: DA MÉTRICA DE HAMMING AOS CÓDIGOS PERFEITOS

Monografia apresentada ao curso de Licenciatura em Matemática do Centro de Ciências Integradas da Universidade Federal do Norte do Tocantins, como requisito parcial para obtenção do título de Licenciada em Matemática.

Orientador: Prof. Dr. José Carlos Oliveira Junior

Araguaína (TO)

2023

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

O48c Oliveira, Rayanne Pinheiro de.

Códigos Corretores de Erros: da Métrica de Hamming aos Códigos Perfeitos. / Rayanne Pinheiro de Oliveira. – Araguaína, TO, 2023.

56 f.

Monografia Graduação - Universidade Federal do Tocantins – Câmpus Universitário de Araguaína - Curso de Matemática, 2023.

Orientador: José Carlos de Oliveira Junior

1. Códigos Corretores de Erros. 2. Códigos Perfeitos. 3. Códigos Lineares. 4. Álgebra.. I. Título

CDD 510

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

RAYANNE PINHEIRO DE OLIVEIRA

CÓDIGOS CORRETORES DE ERROS: DA MÉTRICA DE HAMMING AOS CÓDIGOS PERFEITOS

Monografia apresentada ao curso de Licenciatura em Matemática do Centro de Ciências Integradas da Universidade Federal do Norte do Tocantins, como requisito parcial para obtenção do título de Licenciada em Matemática.

Orientador: Prof. Dr. José Carlos Oliveira Junior

Data de aprovação: 17/08/2023.

Banca Examinadora:

Documento assinado digitalmente
gov.br
JOSE CARLOS DE OLIVEIRA JUNIOR
Data: 20/11/2023 23:26:02-0300
Verifique em https://validar.iti.gov.br

_____

Prof. Dr. José Carlos Oliveira Junior, UFNT – Orientador

Documento assinado digitalmente
gov.br
ALVARO JULIO YUCRA HANCCO
Data: 07/11/2023 12:33:37-0300
Verifique em https://validar.iti.gov.br

_____

Prof. Dr. Alvaro Julio Yucra Hancco, UFNT – Avaliador

Documento assinado digitalmente
gov.br
SARA RAISSA SILVA RODRIGUES
Data: 06/11/2023 16:07:30-0300
Verifique em https://validar.iti.gov.br

_____

Profa. Dra. Sara Raissa Silva Rodrigues, UEPA – Avaliadora

Araguaína (TO)

2023

Dedico este trabalho à minha família, por seu amor, encorajamento e sacrifícios, que tornaram possível a realização deste sonho.

AGRADECIMENTOS

"Porque dEle, e por meio dEle, e para Ele são todas as coisas. A Ele seja a glória para sempre. Amém!" (Romanos 11.36). Quero, em primeiro lugar, agradecer ao meu bondoso e amado Deus por ser a minha força ao longo de todos esses anos. Se não fosse por Ele, afirmo que eu não teria conseguido.

Aos meus pais, Joaquim e Clarice, as pessoas que mais amo e estimo, que sempre me apoiaram e cuidaram de mim. Obrigada pela paciência e apoio nos momentos em que não pude estar por perto. Às minhas irmãs, Ana Livya e Chrislanne, por estarem sempre comigo nos momentos bons e ruins, por me divertirem e serem um ombro amigo nos momentos difíceis. À minha sobrinha, Katarina, por ser a minha alegria e por sempre me distrair nos momentos oportunos.

À minha tia Regina, por todo o apoio, carinho e companheirismo, por me suportar nos últimos dois anos. Agradeço, principalmente, pela hospedagem e por ser tão atenciosa comigo. À minha família em Araguaína, pelo carinho e cuidado que tiveram comigo. Também, à minha família em Amsterdam, por estarem orando e torcendo por mim, mesmo que de longe.

Expresso aqui a minha enorme e sincera gratidão ao meu querido orientador, professor Dr. José Carlos, por toda a paciência e dedicação ao me orientar, não apenas na monografia, mas também na iniciação científica. Obrigado por todos os momentos de risadas, conselhos e aprendizado. Levarei sempre em minhas memórias o excelente profissional que és.

Aos meus queridos amigos Heloísa, Maryana e Francisco, por todo o companheirismo e parceria ao longo desses anos, pela amizade que levarei comigo para a vida e por todos os momentos compartilhados. À minha amiga Lorena Vitória, por sua amizade sincera e por todos os momentos significativos que compartilhamos, os quais contribuíram positivamente para o meu crescimento pessoal. A todos os meus colegas de curso que, direta ou indiretamente, me apoiaram e ajudaram ao longo deste percurso acadêmico.

Agradeço aos meus amados amigos e irmãos em Cristo por todas as orações e palavras de apoio. À minha querida amiga Simara, pelo carinho recebido mesmo à distância.

Agradeço a todos os professores do colegiado de matemática por todo o conhecimento que pude adquirir com eles. Quero aqui expressar uma gratidão

especial ao professor Sinval, que nunca mediu esforços para auxiliar a comunidade acadêmica em suas dificuldades e preocupações. Sinto-me feliz e honrada por tê-lo como meu professor.

À universidade, agradeço por todo o apoio e investimento em mim. Minha gratidão.

RESUMO

Esta monografia explora os códigos corretores de erros que desempenham um papel crucial nas tecnologias, principalmente nos meios de informação e comunicação. O cerne da investigação consistiu 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 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).

Palavras-chaves: códigos corretores de erros; códigos perfeitos; códigos lineares; álgebra.

ABSTRACT

This monograph explores error-correcting codes that play a crucial role in technologies, particularly in information and communication systems. The core of the investigation aimed to answer the following guiding question: How to determine a relationship between parameters of a linear code to ascertain whether it is perfect or not? The main objective of this study is to establish a strong connection between the parameters of a linear code and its quality as a perfect code. Within this scope, the specific goals of this work encompass a deep exploration of fundamental concepts in Linear and Abstract Algebra, addressing elements such as residue classes of integers, vector spaces, fields, linear transformations, and other relevant notions. Furthermore, essential terms such as metric, metric spaces, packing radius of a code, Hamming metric, linear codes, and perfect codes are rigorously defined and examined in depth. Through a comprehensive analysis of these concepts, the focus is not only limited to the introductory presentation of error-correcting codes but also aims to build a solid theoretical foundation for determining perfect codes based on their linear code parameters, as evidenced in the (Pinheiro-Oliveira) Theorem.

Keywords: error-correcting codes; perfect codes; linear codes; algebra.

SUMÁRIO

1 INTRODUÇÃO

A Matemática, durante os séculos, tem revolucionado a sociedade e ainda o faz. Ao pensar nas inúmeras aplicações que esta ciência possui, traz um sentimento de pura satisfação. Pode-se encontrá-la ao nosso redor como em tecnologias, construções, política, remédios, mercado financeiro, economia e muito mais.

Há alguns anos, o universo da tecnologia tem sido cada vez mais ampliado e, com isso, existe por trás desses meios tecnológicos uma matemática brilhante trabalhando para que informações sejam transmitidas com mais eficiência e, se possível, sejam perfeitamente transmitidas. Como, por exemplo, ao se comunicar com pessoas que moram em outro país via ligação de voz pelo celular, é imprescindível que não haja interferências para que a comunicação ocorra de forma fluente e com boa qualidade. No entanto, existem tantos obstáculos até que os sinais cheguem ao seu local de destino (montanhas, distâncias, construções, entre outros). Com isso, pode-se questionar como é possível que a comunicação como esta, entre celulares, alcancem tamanho nível de perfeição com tantas possíveis interrupções?

É aí que nos deparamos com o principal problema da Teoria de Informações: no processo de transmitir ou armazenar uma informação pode haver erros, o que acaba comprometendo a confiabilidade da tecnologia em questão. Então, a partir daí a Teoria dos Códigos Corretores de Erros entra em cena. Segundo [1], essa teoria foi fundada pelo matemático C. E. Shannon num trabalho publicado em 1948. No início, os matemáticos eram os maiores interessados nessa teoria, os quais a desenvolveram consideravelmente nas décadas de 50 e 60. Somente a partir de 1970, com as pesquisas espaciais e o avanço da tecnologia, principalmente a popularidade dos computadores, é que essa teoria começou a interessar outro público de estudiosos, os engenheiros. Atualmente, os códigos corretores de erros são utilizados sempre que se deseja armazenar ou transmitir dados, garantindo assim a confiabilidade necessária.

Com o intuito de ilustrar os princípios dessa teoria, [1] apresenta o seguinte exemplo

> Suponhamos que temos um robô que se move sobre um tabuleiro quadriculado, de modo que, ao darmos um dos comandos (Leste, Oeste, Norte ou Sul), o robô se desloca do centro de uma casa para o centro da casa contígua indicada pelo comando. Os quatros comandos acima podem ser codificados como elementos de $\{0,1\} \times \{0,1\}$, como se segue:

$$\text{Leste} \mapsto 00 \qquad \text{Norte} \mapsto 10$$
$$\text{Oeste} \mapsto 01 \qquad \text{Sul} \mapsto 11.$$

Os códigos 00, 01, 10 e 11 (pares ordenados que não precisam necessariamente ser representados na sua forma usual, entre parentes e separados por vírgula), são chamados de *códigos da fonte*. Segundo os autores, imaginemos que esses códigos passariam a ser transmitidos via rádio. Suponha agora que o sinal durante o caminho sofra algumas interferências, por exemplo, a mensagem transmitida 00 possa, na chegada, ser recebida como 01, o que mudaria a direção que o robô andaria, ao invés de ir para Leste, ele iria para Oeste. Para corrigir esse erro, o que se faz é recodificar as palavras, de maneira a introduzir redundâncias que permitam detectar e corrigir tal erro. A modificação das palavras sugeridas pelos autores é a seguinte:

$$00 \mapsto 00000$$
$$01 \mapsto 01011$$
$$10 \mapsto 10110$$
$$11 \mapsto 11101.$$

Nessa recodificação, as duas primeiras posições reproduzem o código da fonte, enquanto que as três últimas posições são redundâncias introduzidas nesse processo. Esse novo código é chamado de *código de canal*. Agora, vamos supor que houve um erro ao transmitir, por exemplo, a palavra[1] 10110, de modo que a mensagem recebida tenha sido 11110. Ao comparar essa mensagem com as palavras do código, nota-se que ela não pertence ao código de canal e, portanto, detectou-se erro. Analisando as demais palavras, a que mais se aproxima da referida mensagem é a 10110, pois esta é a que possui menor número de componentes diferentes, isto é, entre 10110 e 11110 a única componente diferente é a segunda letra da palavra.

Embora o exemplo ilustre bem os princípios dos códigos corretores de erros, ainda assim não é suficiente para entendermos como essa teoria funciona. Portanto, para entendermos melhor como funcionam os Códigos Corretores de Erros, precisa-se que nos debrucemos em estudar conceitos algébricos, como Corpos Finitos,

[1] Na Teoria dos Códigos, os elementos de um conjunto A (denominado de Alfabeto) são chamados de letras e os códigos são palavras.

Espaços Vetoriais, Classes Residuais, Teoria de Grupos, entre outros conceitos importantes.

Após considerar as observações acima, este trabalho tem como propósito apresentar uma introdução aos códigos corretores de erros, com foco particular nos códigos perfeitos, buscando abordar a seguinte questão norteadora: *Como determinar uma relação entre parâmetros de um código linear para saber se o mesmo é ou não perfeito?* Com essa problemática delineada, o objetivo principal é definir uma conexão entre os parâmetros de um código linear com os códigos perfeitos. Para atingir essa finalidade de forma específica, pretende-se apresentar conceitos da Álgebra Linear e Abstrata, incluindo classes residuais de inteiros, espaços vetoriais, corpos, transformações lineares, bem como outros conceitos relevantes. Ademais, serão definidos termos como métrica, espaços métricos, raio de empacotamento de um código, métrica de Hamming, códigos lineares e códigos perfeitos. Esses elementos serão utilizados como base para estabelecer a relação desejada entre os parâmetros de um código linear e a propriedade de ser perfeito.

Nesse contexto, 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. Para alicerçar a metodologia empregada, a pesquisa encontra suporte em referências como [2], [3] e [4]. A seguir, a estrutura estabelecida na monografia é examinada.

No Capítulo 2, intitulado "Preliminares", busca-se apresentar um breve relato acerca da história da teoria dos códigos corretores de erros, destacando alguns de seus avanços e conquistas.

No Capítulo 3, o objetivo é fornecer noções preliminares para uma compreensão aprofundada do objeto de estudo. Para tal fim, o capítulo explora os conceitos fundamentais da Álgebra Linear e Abstrata.

No Capítulo 4, são apresentados conceitos essenciais sobre códigos corretores de erros, juntamente com exemplos elucidativos para uma melhor compreensão de como esses códigos estão intrínsecos no cotidiano. Nesse sentido, são definidos conceitos como espaços métricos, métricas de um código, disco e

esfera de um código, cardinalidade de um código, parâmetros fundamentais de um código, códigos perfeitos e, ainda, códigos lineares.

Por fim, o Capítulo 5 apresenta o teorema dos códigos perfeitos cuja distância mínima é igual a $d = 3$ ou $d = 4$. Este capítulo constitui a essência da monografia, com o propósito de demonstrar uma abordagem mais simplificada para determinar se um código com distância mínima de $d = 3$ ou $d = 4$ é perfeito ou não. Isso é alcançado sem a necessidade de recorrer a métodos demorados e, por vezes, sem sucesso.

2 PANORAMA HISTÓRICO

No presente capítulo, propõe-se apresentar uma breve abordagem histórica acerca da teoria dos códigos corretores de erros, com ênfase na identificação de eventos importantes para o desenvolvimento desta teoria. Para embasar esta investigação, as fontes consultadas abarcam as obras [1], [5] e [6], cuja contribuição foi fundamental na concepção deste capítulo.

Na década de 1940, época em que os computadores eram máquinas caríssimas e somente instituições como governos e universidades as possuíam, foi quando essa teoria iniciou-se. Em 1947, o pesquisador Richard W. Hamming trabalhava no Laboratório Bell de Tecnologia com esses computadores somente nos finais de semana. Naquela época, os programas eram gravados em cartões perfurados e ao passarem pela leitura do computador, ocorria a detecção de erros de digitação. Se o erro fosse detectado, a leitura era interrompida e o computador passava automaticamente a ler o próximo programa. Por esse motivo, Hamming perdeu duas semanas tentando fazer com que o computador lesse seus programas, mas sem sucesso, decidiu procurar uma solução para o problema que havia enfrentado.

Em 1950, uma das pesquisas de Hamming foi publicada no *"The Bell System Technical Journal"*, na qual ele desenvolveu um código capaz de detectar até dois erros e corrigir apenas um, caso fosse o único presente. Antes dessa publicação, o pesquisador compartilhava o progresso de sua pesquisa por meio de memorandos internos do Laboratório Bell, questionando-se acerca da possibilidade de desenvolver códigos mais eficientes do que aquele que ele propôs.

No ano de 1948, C. E. Shannon, colega de Hamming, publicou um artigo intitulado “A Mathematical Theory of Communication”, que deu início à Teoria de códigos (em colaboração com o trabalho de Hamming) e à Teoria da Informação, novos campos de pesquisa em matemática. E não parou por aí, depois deste artigo houve um desenvolvimento significativo e linear da Teoria dos Códigos até os dias de hoje.

Além destes dois, outro proeminente pioneiro na teoria dos códigos foi Marcel J. E. Golay, que expandiu o resultado do $(7,4)$-código de Hamming, o qual foi apresentado no artigo de Shannon em 1948, para desenvolver um código corretor de erro único de comprimento primo p. Adicionalmente, Golay foi responsável pela

criação dos códigos de Golay, dentre os quais um deles desempenhou um papel crucial na transmissão de fotografias coloridas de Júpiter e Saturno pela espaçonave Voyager. Seu trabalho abordando esses códigos foi registrado em um artigo publicado em 1949, sendo amplamente reconhecido como uma das contribuições mais significativas no campo da teoria de códigos.

Atualmente, a Teoria dos Códigos tem sido amplamente utilizada em programas espaciais da NASA (National Aeronautics and Space Administration) e do JPL (Jet Propulsion Laboratory). Por exemplo, em 1965, a nave espacial *Mariner 4* transmitiu 22 fotos em preto e branco do planeta Marte. Cada foto foi decomposta em 200×200 elementos de imagem, e a cada elemento de imagem foi atribuído um dos 64 tons de cinza pré-escolhidos, os quais foram codificados como elemento de $\mathbb{Z}_2^6$. Esses vetores eram transmitidos sem nenhuma informação adicional, isto é, sem codificação de canal, pois a transmissão era muito lenta, levando oito horas para completar a transmissão de uma foto.

Em 1972, a nave espacial *Mariner 9* transmitiu novas imagens de Marte. Desta vez as imagens foram decompostas em uma resolução de 700×832 elementos. O código de fonte foi mantido, mas com o aumento da velocidade de transmissão foi possível recodificar o código através de uma função injetora $\varphi\colon \mathbb{Z}_2^6 \longrightarrow \mathbb{Z}_2^{32}$, de modo que o código de canal resultante conseguia detectar e corrigir até sete erros. O sinal recebido era corrigido e decodificado através da transformação φ^{-1}, encontrando-se o elemento de $\mathbb{Z}_2^6$ e, posteriormente, o tom de cinza correspondente a ele. Esse código pertence a uma família de códigos chamados de *Códigos de Reed-Muller*.

No ano de 1979, foram transmitidas imagens coloridas de Júpiter pela nave espacial *Voyager*, a transmissão dessas imagens coloridas na verdade foi uma sequência de imagens em preto e branco, tiradas através de vários filtros. Cada elemento de imagem foi representado por uma tonalidade de cinza previamente escolhida, ao total eram $2^{12} = 4096$ tonalidades. O codificador da fonte usava 12 bits binários, enquanto que o codificador de canal usava 24 bits. Esse código, também chamado de código de Golay, permitia corrigir até três erros cometidos nos 24 bits de informação transmitidos.

3 PRELIMINARES

Neste capítulo, vamos estudar conceitos básicos de Álgebra necessários para compreender os códigos corretores 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. Para construir as preliminares, utilizaram-se as seguintes referências bibliográficas [7], [8], [9], [10], [11] e [12].

3.1 Corpos

Nesse primeiro momento, definiremos corpos, subcorpo e corpo finito para, posteriormente, conceituar o corpo finito mais importante para compreender o nosso objeto de estudo.

Definição 3.1. *Seja* $\mathbb{K}$ *um conjunto não vazio. Considere*

$$+: \mathbb{K} \times \mathbb{K} \to \mathbb{K} \ \ e \ \cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$

duas operações em $\mathbb{K}$ *chamadas, respectivamente, de adição e multiplicação de* $\mathbb{K}$*. Diremos que a terna* $(\mathbb{K}, +, \cdot)$ *é um corpo se as operações satisfizerem as seguintes propriedades:*

i. ***A adição é associativa:*** *quaisquer que sejam* $a, b, c \in \mathbb{K}$*, tem-se*

$$(a + b) + c = a + (b + c).$$

ii. ***A adição e comutativa:*** *quaisquer que sejam* $a, b \in \mathbb{K}$*, tem-se*

$$a + b = b + a.$$

iii. ***Existe elemento neutro para a adição:*** *existe* $0 \in \mathbb{K}$ *tal que para qualquer* $a \in \mathbb{K}$*, tem-se*

$$0 + a = a.$$

iv. ***Existência do elemento inverso para a adição:*** *para cada* $a \in \mathbb{K}$ *existe* $-a \in \mathbb{K}$ *tal que* $a + (-a) = 0$*.*

v. ***A multiplicação é associativa:*** *quaisquer que sejam* $a, b, c \in \mathbb{K}$*, tem-se*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

vi. ***A multiplicação é comutativa:*** *quaisquer que sejam* $a, b \in \mathbb{K}$*, tem-se*

$$a \cdot b = b \cdot a.$$

vii. ***Existência do elemento neutro para a multiplicação:*** *existe* $1 \in \mathbb{K}$*, com* $0 \neq 1$*, tal que para cada* $a \in \mathbb{K}$ *temos*

$$1 \cdot a = a.$$

viii. ***Existência do elemento inverso para a multiplicação:*** *para cada* $a \in \mathbb{K} - \{0\}$ *existe* $a^{-1} \in \mathbb{K}$ *tal que* $a \cdot a^{-1} = 1$*.*

ix. ***A multiplicação é distributiva com relação à adição:*** *quaisquer que sejam* $a, b, c \in \mathbb{K}$*, tem-se*

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Podemos perceber que $\mathbb{R}, \mathbb{Q}$ e $\mathbb{C}$ são exemplos particulares de corpos. Por outro lado, nota-se que o conjunto numérico $\mathbb{Z}$ não é corpo, já que seus elementos não possuem inverso multiplicativo, com exceção dos elementos 1 e -1.

Proposição 3.2. *Sejam* $\mathbb{K}$ *um corpo e* $a \in \mathbb{K}$ *tal que* $a \neq 0_{\mathbb{K}}$*, sendo* $0_{\mathbb{K}}$ *o elemento nulo do corpo* $\mathbb{K}$*. O elemento inverso de* a *é único.*
Demonstração: Veja a prova desta proposição em [8], página 29.

Definição 3.3. *Seja* $\mathbb{K}$ *um corpo. Um subconjunto* $\mathbb{K}'$ *de* $\mathbb{K}$ *é dito subcorpo de* $\mathbb{K}$ *se satisfaz as seguintes condições:*

i. *Os elementos neutros para a adição e multiplicação de* $\mathbb{K}$ *pertencem a* $\mathbb{K}'$*;*
ii. $\mathbb{K}'$ *é fechado para a adição, isto é, se* $a, b \in \mathbb{K}'$ *então* $a + b \in \mathbb{K}'$*;*
iii. $\mathbb{K}'$ *é fechado para a multiplicação, isto é, se* $a, b \in \mathbb{K}'$ *então* $a \cdot b \in \mathbb{K}'$*;*
iv. *Para cada* $a \in \mathbb{K}'$*,* $-a \in \mathbb{K}'$*;*
v. *Para cada* $a \in \mathbb{K}' - \{0\}$*,* $a^{-1} \in \mathbb{K}'$*.*

Exemplo 3.4. O conjunto numérico $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$, assim como $\mathbb{R}$ é subcorpo de $\mathbb{C}$.

A cardinalidade de um corpo $(\mathbb{K}, +, \cdot)$ é determinada pela quantidade de elementos no conjunto $\mathbb{K}$. Assim, com base no exemplo anterior, identificamos que os conjuntos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos de cardinalidade infinita, uma vez que possuem um número infinito de elementos. No entanto, também encontramos corpos cuja

cardinalidade é finita, sendo esses conhecidos como corpos finitos. Destaca-se que o corpo de maior relevância para este estudo será introduzido a seguir, através do conceito de classes residuais.

Ressaltamos que, daqui em diante, usaremos o símbolo $\mathbb{F}$ para designar um corpo.

3.2 Classes Residuais

Definição 3.5. *Sejam $a, b \in \mathbb{Z}$. Diz-se que b divide a se existe um inteiro k tal que*

$$b \cdot k = a.$$

Denota-se por $b|a$.

Exemplo 3.6. Sabe-se que $4|12$, pois existe um inteiro k, tal que $3 \cdot k = 12$. De fato, $4 \cdot 3 = 12$. Por outro lado, $4 \nmid 13$, pois não existe um inteiro k tal que $4 \cdot k = 13$.

Definição 3.7. *Um inteiro p é chamado primo se tem exatamente dois divisores positivos: 1 e $|p|$.*

Exemplo 3.8. Note que 7 é um número primo. De fato, 7 possui somente dois divisores positivos: 1 e 7. Em contrapartida, sabe-se que o número 4 não é primo, uma vez que possui os seguintes divisores positivos: 1, 2 e 4.

Definição 3.9. *Seja $m \neq 0$ um inteiro fixo. Dois inteiros a e b são congruentes módulo m se m divide a diferença $a - b$, isto é, se $m|(a - b)$.*

Exemplo 3.10. Seja $m = 3$. Os inteiros 18 e 6 são congruentes módulo 3, pois existe um inteiro k tal que 3 divide a diferença $18 - 6$. De fato, pela Definição 3.9, temos

$$3|(18 - 6) \Rightarrow 3 \cdot k = (18 - 6) \Rightarrow 3 \cdot k = 12 \Rightarrow k = 4,\ 4 \in \mathbb{Z}.$$

Definição 3.11. *Sejam $a, m \in \mathbb{Z}$ tais que $m > 1$. Chama-se classe de congruência de a módulo m o conjunto formado por todos os inteiros x que são congruentes a a módulo m. Escreve-se $x \equiv a\ (mod\ m)$ e denota-se esse conjunto por $\bar{a}$ e a é chamado de representante da classe residual. Ou seja,*

$$\bar{a} = \{x \in \mathbb{Z} |\ x \equiv a(mod\ m)\}.$$

Como $x \equiv a(mod\ m)$ se, e somente se, x é da forma $x = a + qm$, para algum $q \in \mathbb{Z}$, podemos escrever o conjunto $\bar{a}$ como

$$\bar{a} = \{a + qm |\ q \in \mathbb{Z}\}. \qquad (1)$$

A seguir, apresentamos algumas propriedades básicas da relação $\equiv$ nos inteiros.

P1. $a \equiv a\ (mod\ m)$ (reflexividade)

P2. Se $a \equiv b(mod\ m)$, então $b \equiv a(mod\ m)$. (Simetria)

P3. Se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$, então $a \equiv c(mod\ m)$. (Transitividade)

P4. Se $a \equiv b(mod\ m)$ e $0 \leq b < m$, então b é resto da divisão euclidiana de a por m. Reciprocamente, se r é o resto da divisão de a por m, então $a \equiv r(mod\ m)$.

P5. $a \equiv b(mod\ m)$ se, e somente se, a e b possuem o mesmo resto na divisão euclidiana por m.

P6. $a \equiv b(mod\ m)$ se, e somente se, $a \pm c \equiv b \pm c\ (mod\ m)$, $c \in \mathbb{Z}$.

P7. $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $a + c \equiv b + d\ (mod\ m)$, com $c, d \in \mathbb{Z}$

P8. Se $a \equiv b(mod\ m)$, então $ac \equiv bc\ (mod\ m)$, com $c \in \mathbb{Z}$.

P9. Se $a \equiv b(mod\ m)$ e $c \equiv d\ (mod\ m)$, então $ac \equiv bd\ (mod\ m)$.

P10. Se $ca \equiv cb\ (mod\ m)$ e $mdc(c, m) = d$, então $a \equiv b\ (mod\ \frac{m}{d})$.

A prova das propriedades acima pode ser consultada em [10], páginas 54 e 55.

Agora vamos construir as classes residuais dos elementos de $\mathbb{Z}$ módulo m. Antes, se os inteiros a, b possuem o mesmo resto na divisão euclidiana por m, então eles são congruentes. De fato, subtraindo membro a membro as igualdades a seguir $a = mq_1 + r$ e $b = mq_2 + r$, para $0 \leq r < m$, temos:

$$a - b = m(q_1 - q_2)$$

de onde, $a \equiv b\ (mod\ m)$.

Portanto, como vale (1), temos que as classes residuais dos inteiros $0, 1, \ldots, m - 1$ módulo m são

$$\bar{0} = \{0, \pm m, \pm 2m, \cdots\}$$
$$\bar{1} = \{1, 1 \pm m, 1 \pm 2m, \cdots\}$$
$$\bar{2} = \{2, 2 \pm m, 2 \pm 2m, \cdots\}$$
$$\vdots$$
$$\overline{m-1} = \{m-1, m-1 \pm m, m-1 \pm 2m, \cdots\}.$$

Exemplo 3.12. Se $m = 2$, temos que todas as classes possíveis módulo 2 são

$$\bar{0} = \{0, \pm 2, \pm 4, \cdots\},$$
$$\bar{1} = \{1, \pm 3, \pm 5, \cdots\}.$$

Dessa forma, qualquer inteiro par é representante da classe residual $\bar{0}$ e qualquer inteiro ímpar é representante da classe residual $\bar{1}$. Em outras palavras,

$$\bar{0} = \bar{2} = \overline{-10} = \cdots$$

e

$$\bar{1} = \bar{3} = \overline{-5} = \cdots$$

Exemplo 3.13. Se $m = 3$, temos que todas as classes possíveis módulo 3 são

$$\bar{0} = \{0, \pm 3, \pm 6, \cdots\}$$
$$\bar{1} = \{1, \pm 4, \pm 7, \cdots\}$$
$$\bar{2} = \{2, \pm 5, \pm 8, \cdots\}.$$

Definição 3.14. *O conjunto das classes de congruência módulo m, denotado por $\mathbb{Z}_m$, é chamado de conjunto dos inteiros módulo m, ou ainda,*

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}.$$

Dadas duas classes $\bar{a}, \bar{b} \in \mathbb{Z}_m$, vamos definir agora as operações de adição e multiplicação sobre $\mathbb{Z}_m$:

Definição 3.15. *Dadas duas classes $\bar{a}, \bar{b} \in \mathbb{Z}_m$, chama-se soma $\bar{a} + \bar{b}$ a classe $\overline{a+b}$.*

Definição 3.16. *Dadas duas classes* $\bar{a}, \bar{b} \in \mathbb{Z}_m$*, chama-se produto* $\bar{a} \cdot \bar{b}$ *a classe* $\overline{a \cdot b}$.

Note que, ao definirmos essas operações usando os representantes a e b para as classes residuais $\bar{a}$ e $\bar{b}$, temos que verificar que, ao mudarmos os representantes das classes $\bar{a}$ e $\bar{b}$, os conjuntos $\overline{a+b}$ e de $\overline{a \cdot b}$ não se alteram. Para isso, basta notar que, se $\bar{a} = \overline{a'} \in \mathbb{Z}_m$ e $\bar{b} = \overline{b'} \in \mathbb{Z}_m$, então $a \equiv a'(mod\ m)$ e $b \equiv b'(mod\ m)$. Portanto, pela P7 e P9, temos $a + b \equiv a' + b'(mod\ m)$ e $a \cdot b \equiv a' \cdot b'(mod\ m)$ e, consequentemente, $\overline{a+b} = \overline{a'+b'}$ e $\overline{a \cdot b} = \overline{a' \cdot b'}$. Portanto, a soma e o produto de classes não dependem dos representantes das classes. Dessa forma, fica garantido que $\overline{a+b}$ e $\overline{a \cdot b}$ são únicos.

Uma observação importante a ser feita é que nem toda definição de uma operação no conjunto $\mathbb{Z}_m$ está bem definida por causa dos diferentes representantes das classes residuais. Por exemplo, considere a operação $*: \mathbb{Z}_5 \to \mathbb{Z}_5$ definida por

$$*(\overline{a}) = \overline{3^a}.$$

Nesse caso, temos simultaneamente que

$$*\left(\overline{2}\right) = \overline{3^2} = \overline{9} = \overline{4}$$

e

$$*\left(\overline{7}\right) = \overline{3^7} = \overline{2187} = \overline{2} \neq \overline{4},$$

mas as classes $\overline{2}$ e $\overline{7}$ são classes iguais módulo 5. Isso mostra que a função * não está bem definida (bem posta) e, além disso, destaca a importância da prova contida no parágrafo anterior, que mostra que $+$ e $\cdot$ estão bem definidas em $\mathbb{Z}_m$.

Agora, vamos estudar algumas propriedades da soma e multiplicação dessas classes.

Propriedades da adição:

i. **Associativa:** para quaisquer $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$, temos:

$$\bar{a} + \left(\bar{b} + \bar{c}\right) = \bar{a} + \overline{b+c} = \overline{a+(b+c)} = \overline{(a+b)+c} = \overline{a+b} + \bar{c} = \left(\bar{a} + \bar{b}\right) + \bar{c}\,.$$

ii. **Comutativa:** Para quaisquer $\bar{a}, \bar{b} \in \mathbb{Z}_m$, temos:

   a. $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$.

iii. **Elemento neutro:** Para qualquer $\bar{a} \in \mathbb{Z}_m$, temos:

$$\bar{a} + \bar{0} = \overline{a+0} = \bar{a}.$$

   Portanto, $\bar{0}$ é o elemento neutro da adição em $\mathbb{Z}_m$.

iv. **Elementos simetrizáveis:** Dado $\bar{a} \in \mathbb{Z}_m$, procuramos seu simétrico $\overline{a'}$.

Devemos ter $\bar{a} + \overline{a'} = \overline{a + a'} = \bar{0}$ e, portanto, $a + a' \equiv 0(mod\ m)$ ou $a' \equiv -a(mod\ m)$. De onde, $\overline{a'} = \overline{m - a}$.

Isso mostra que todo elemento $\bar{a} \in \mathbb{Z}_m$ é simetrizável para a adição e seu simétrico é $\overline{m - a}$.

Propriedades da multiplicação

Analogamente, pode-se provar a associatividade e comutatividade para a multiplicação.

1) Elemento neutro: Para qualquer $\bar{a} \in \mathbb{Z}_m$, temos:

$$\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a}.$$

Portanto, $\bar{1}$ é o elemento neutro da multiplicação em $\mathbb{Z}_m$.

2) Elemento invertível:

Proposição 3.17. *Seja $\bar{a} \in \mathbb{Z}_m$, então $\bar{a}$ é simetrizável para a multiplicação se, e somente se, $mdc(a, m) = 1$.*

Demonstração: ($\Rightarrow$) Seja $\bar{a} \in \mathbb{Z}_m$ um elemento invertível. Então, existe $a' \in \mathbb{Z}$, tal que $\bar{a} \cdot \overline{a'} = \overline{a \cdot a'} = \bar{1}$. Daí, $a \cdot a' \equiv 1(mod\ m)$ ou $a \cdot a' - 1 = mq$, para algum $q \in \mathbb{Z}$. Logo, $aa' + m(-q) = 1$. Portanto, se $mdc(a, m) = d$, então $aa' + m(-q) = 1$ implica que $d\big(a_0 a' + m_0(-q)\big) = 1$, para alguns inteiros a_0, m_0. Isso mostra que $d = 1$, como queríamos.

($\Leftarrow$) Suponhamos que $mdc(a, m) = 1$. Então, pela Identidade de Bezeout (veja Proposição 2, página 43 de [10]), existem inteiros x_0 e y_0 tais que $a \cdot x_0 + m \cdot y_0 = 1$. Logo, $ax_0 \equiv 1(mod\ m)$. Consequentemente, $\bar{a} \cdot \overline{x_0} = \overline{a \cdot x_0} = \bar{1}$ e, portanto, $\bar{a}$ é invertível.

Teorema 3.18. *$\mathbb{Z}_m$ é corpo se, e somente se, m é primo.*

Demonstração: $\mathbb{Z}_m$ é um corpo se, e somente se, todos os elementos $\bar{1}, \bar{2}, \cdots, \overline{m-1}$ possuírem inversos multiplicativos, isto é, pela Proposição 3.17, equivalente ao fato de que

$$mdc(1, m) = mdc(2, m) = \cdots = mdc(m - 1, m) = 1,$$

o que , portanto, equivale a m ser primo (pois não possui divisores menores que ele). Reciprocamente, se m é primo, temos $mdc(a, m) = 1$, para todo $\bar{a} \in \mathbb{Z}_m - \{\bar{0}\}$. Logo, pela Proposição 3.17, $\bar{a}$ é invertível. Sendo os elementos de $\mathbb{Z}_m - \{\bar{0}\}$, com m primo, são invertíveis, então $\mathbb{Z}_m$ é um corpo.

Exemplo 3.19. Seja $m = 2$. Logo, $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ com as operações de soma e multiplicação dadas a seguir.

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Percebe-se que o único elemento não nulo de $\mathbb{Z}_2$ é invertível, isto é, o elemento $\bar{1}$. Logo, $\mathbb{Z}_2$ é um corpo.

Exemplo 3.20. Seja $m = 3$. Logo, $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ com as operações de soma e multiplicação dadas a seguir.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Note que os elementos $\bar{1}$ e $\bar{2}$ são invertíveis (com inversos respectivamente $\bar{1}$ e $\bar{2}$), logo $\mathbb{Z}_3$ é corpo.

Exemplo 3.21. Seja $m = 4$. Logo, $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ com as operações de soma e multiplicação dadas a seguir.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Note que um dos elementos não nulos de $\mathbb{Z}_4$ não é invertível, isto é, o elemento $\bar{2} \neq \bar{0}$, no entanto, $\bar{2} \cdot \bar{2} = \bar{0}$. Portanto, $\mathbb{Z}_4$ não é um corpo.

Exemplo 3.22. Seja $m = 5$. Logo, $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ com as operações de soma e multiplicação dadas a seguir.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Observe que todos os elementos não nulos de $\mathbb{Z}_5$ são invertíveis, isto é, todos os quatro elementos $\bar{1}, \bar{2}, \bar{3}$ e $\bar{4}$ de $\mathbb{Z}_5$ possuem simétricos multiplicativos, são eles, respectivamente, $\bar{1}, \bar{3}, \bar{2}$ e $\bar{4}$. Portanto, $\mathbb{Z}_5$ é corpo.

Exemplo 3.23. Seja $m = 7$. Logo, $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ com as operações de soma e multiplicação dadas a seguir.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{5}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Perceba que todos os elementos não nulos de $\mathbb{Z}_7$ são invertíveis, portanto $\mathbb{Z}_7$ é corpo.

3.3 Grupos e subgrupos

Definição 3.24. *Um sistema matemático constituído de um conjunto não vazio G e uma operação $(x, y) \mapsto x * y$ sobre G é chamado grupo se essa operação se sujeita aos seguinte axiomas:*

i. ***Associatividade:*** $(a * b) * c = a * (b * c)$*, quaisquer que sejam* $a, b, c \in G$*;*

ii. ***Comutatividade:*** $a * b = b * a$*, quaisquer que sejam* $a, b \in G$*, o grupo recebe o nome de grupo comutativo ou abeliano;*

iii. ***Existência de elemento neutro:*** *Existe um elemento* $e \in G$ *tal que* $a * e = e * a = a$*, qualquer que seja* $a \in G$*;*

iv. ***Existência de simétricos:*** *Para todo* $a \in G$ *existe um elemento* $a' \in G$ *tal que* $a * a' = a' * a = e$*.*

Definição 3.25. *Seja* $(G, *)$ *um grupo. Diz-se que um subconjunto não vazio* $H \subset G$ *é um subgrupo de* G *se:*

i. H *é fechado para a operação* $*$ *(isto é, se* $a, b \in H$ *então* $a * b \in H$*);*

ii. $(H, *)$ *também é um grupo (aqui o símbolo* $*$ *indica a restrição da operação de* G *aos elementos de* H*).*

3.3 Espaço Vetorial

Definição 3.26. *Sejam* $\mathbb{F}$ *um corpo e* V *um conjunto não vazio no qual estão definidas as operações de adição e multiplicação por escalar:*

$$+\colon V \times V \longrightarrow V \qquad (u, v) \mapsto u + v \qquad \text{e} \qquad \cdot\colon \mathbb{F} \times V \longrightarrow V \qquad (\alpha, v) \mapsto \alpha \cdot v$$

O conjunto V é chamado de espaço vetorial sobre $\mathbb{F}$*, se forem satisfeitas as seguintes propriedades, para todo* $u, v, w \in V$ *e* $\alpha, \beta \in \mathbb{F}$*:*

i. ***A adição é associativa****:* $(u + v) + w = u + (v + w)$*, para todo* $u, v, w \in V$*;*

ii. ***A adição é comutativa****:* $u + v = v + u$*, para todo* $u, v \in V$*;*

iii. ***Existência do elemento neutro da adição (elemento zero)****: existe* $0 \in V$*, tal que* $v + 0 = v$*, para todo* $v \in V$*;*

iv. ***Existência do simétrico aditivo:*** *para todo* $v \in V$*, existe* $-v \in V$ *tal que* $v + (-v) = 0$*;*

v. ***Distributiva I:*** $\alpha \cdot (u + v) = \alpha u + \alpha v$*, para todo* $\alpha \in \mathbb{F}$ *e* $u, v \in V$*;*

vi. ***Distributiva II:*** $(\alpha + \beta) \cdot v = \alpha v + \beta v$*, para todo* $\alpha, \beta \in \mathbb{F}$ *e* $v \in V$*;*

vii. ***Associatividade da multiplicação:*** $(\alpha \cdot \beta) \cdot v = \alpha \cdot (\beta \cdot v)$*, para todo* $\alpha, \beta \in \mathbb{F}$ *e* $v \in V$*;*

viii. ***Existência do elemento neutro multiplicativo:*** *Existe* $1_{\mathbb{F}} \in \mathbb{F}$ *tal que* $1_{\mathbb{F}} \cdot v = v \cdot 1_{\mathbb{F}} = v$*, para todo* $v \in V$*.*

Os elementos de V são chamados de vetores e os elementos de $\mathbb{F}$ de escalares.

3.4 Subespaço Vetorial

Definição 3.27. *Sejam* V *um espaço vetorial e* W *um subconjunto não vazio de* V*. Diz-se que* W *é subespaço vetorial de* V *se, e somente se, as seguintes condições são satisfeitas:*

i. *Se* $u, v \in W$*, então* $u + v \in W$ *;*

ii. *Se* $\alpha \in \mathbb{F}$ *e* $u \in W$*, então* $\alpha \cdot u \in W$*.*

Exemplo 3.28. O conjunto $W = \{(x, y) \in \mathbb{R}^2 \mid x + y = 0\}$ é um subespaço vetorial de $\mathbb{R}^2$, pois

i. O vetor nulo $(0,0) \in W$, se tomarmos $x = y = 0$, teremos $0 + 0 = 0$;

ii. Sejam $(a, b), (c, d) \in W$, temos por definição que $a + b = 0$ e $c + d = 0$. Daí, ao somarmos $(a, b) + (c, d)$, obtemos o par $(a + c, b + d)$, logo

$$(a + c) + (b + d) = (a + b) + (c + d) = 0 + 0 = 0$$

e, portanto, $(a + b) + (c + d) \in W$;

iii. Se $\alpha \in \mathbb{R}$ e $(a, b) \in W$, então $\alpha \cdot (a, b) = (\alpha a, \alpha b) \in W$, já que

$$\alpha a + \alpha b = \alpha \cdot (a + b) = \alpha \cdot 0 = 0,$$

(por definição $a + b = 0$).

Contraexemplo 3.29. O conjunto $W = \{(x, y) \in \mathbb{R}^2 | \, x + y = 2\}$ não é subespaço vetorial de $\mathbb{R}^2$, já que o vetor nulo $(0,0) \notin W$, pois se tomarmos $x = y = 0$, teremos $0 + 0 = 2$, absurdo!

Definição 3.30. *Seja V um espaço vetorial sobre $\mathbb{F}$. Dizemos que um conjunto $L = \{v_1, v_2, \dots, v_n\} \subset V$ é linearmente independente (L.I.) se, e somente se, a igualdade a seguir se verifica*

$$\alpha_1 \cdot v_1 + \cdots + \alpha_n \cdot v_n = 0_{\mathbb{F}}$$

com $\alpha_i \in \mathbb{F}$, somente para $\alpha_1 = \cdots = \alpha_n = 0_{\mathbb{F}}$. Caso o conjunto L não seja L.I. dizemos que L é linearmente dependente (L.D.).

3.5 Base e Dimensão

Definição 3.31. *Um conjunto $B = \{v_1, \cdots, v_n\}$ de vetores de V será uma base de V se:*

i. $B = \{v_1, \cdots, v_n\}$ *é L.I.;*

ii. $B = \{v_1, \cdots, v_n\} = V$.

Dessa forma, B será uma base de V se for linearmente independente e se gerar o espaço vetorial V. Quando isso ocorre, é possível expressar cada vetor de V de maneira única como uma combinação linear dos vetores da base B.

O número de elementos de uma base de um espaço vetorial V é chamado de dimensão de V, denotado por $dim V$.

Exemplo 3.32. O conjunto $B = \{(1,0), (0,1)\}$ é linearmente independente e gera o $\mathbb{R}^2$. Portanto, o conjunto B é uma base de $\mathbb{R}^2$, e a sua dimensão é dois, isto é, $dim\mathbb{R}^2 = 2$.

Exemplo 3.33. O conjunto $B = \{(1,0,0), (0,1,0), (0,0,1)\}$ é linearmente independente e gera o $\mathbb{R}^3$. Portanto, o conjunto B é uma base de $\mathbb{R}^3$ e a sua dimensão é três, isto é, $dim\mathbb{R}^3 = 3$.

3.6 Transformações Lineares

Definição 3.34. *Sejam V e W dois espaços vetoriais sobre um corpo $\mathbb{F}$. Uma transformação Linear (aplicação linear) é uma função $T: V \to W$, que satisfaz as seguintes condições:*

i. *Quaisquer que sejam u e v em V,*

$$T(u+v) = T(u) + T(v);$$

ii. *Quaisquer que sejam $\alpha \in \mathbb{F}$ e $v \in V$,*

$$T(\alpha v) = \alpha \cdot T(v).$$

Exemplo 3.35. A função $T: \mathbb{R}^3 \to \mathbb{R}^2$ dada por $T(x,y,z) = (x-y, y-z)$ é uma transformação linear e para verificarmos isso ela precisa satisfazer as condições (i) e (ii) dadas acima.

Vamos tomar $v_1 = (x_1, y_1, z_1)$, $v_2 = (x_2, y_2, z_2) \in \mathbb{R}^3$ e $\alpha \in \mathbb{R}$, vejamos que

i) $T(v_1 + v_2) = T(v_1) + T(v_2)$. De fato, temos que $T(v_1) = (x_1 - y_1, y_1 - z_1)$ e $T(v_2) = (x_2 - y_2, y_2 - z_2)$, assim

$$\begin{aligned} T(v_1 + v_2) &= T(x_1 + x_2, y_1 + y_2, z_1 + z_2) \\ &= \big(x_1 + x_2 - (y_1 + y_2), y_1 + y_2 - (z_1 + z_2)\big) \\ &= (x_1 + x_2 - y_1 - y_2, y_1 + y_2 - z_1 - z_2) \\ &= ((x_1 - y_1) + (x_2 - y_2), (y_1 - z_1) + (y_2 - z_2)) \\ &= (x_1 - y_1, y_1 - z_1) + (x_2 - y_2, y_2 - z_2) \\ &= T(v_1) + T(v_2). \end{aligned}$$

ii) $T(\alpha v_1) = \alpha T(v_1)$.

De fato, temos

$$\begin{aligned} T(\alpha v_1) &= T\big(\alpha(x_1, y_1, z_1)\big) \\ &= T(\alpha x_1, \alpha y_1, \alpha z_1) \\ &= (\alpha x_1 - \alpha y_1, \alpha y_1 - \alpha z_1) \\ &= \big(\alpha(x_1 - y_1), \alpha(y_1 - z_1)\big) \end{aligned}$$

$$= \alpha(x_1 - y_1, y_1 - z_1)$$
$$= \alpha T(v_1).$$

Portanto, T é uma transformação linear.

3.7 Núcleo e Imagem de uma transformação linear

Definição 3.36. *Seja $T: V \to W$ uma transformação linear. O conjunto de todos os vetores $v \in V$ tais que $T(v) = 0$ é chamado núcleo de T, sendo denotado por $ker(T)$. Isto é,*

$$ker(T) = \{v \in V |\, T(v) = 0\}.$$

O núcleo de V é um subespaço desse espaço vetorial. Se o núcleo de uma transformação linear for apenas o vetor nulo, a transformação é chamada de injetora.

Definição 3.37. *Seja $T: V \to W$ uma aplicação linear. A imagem de T é o conjunto dos vetores $w \in W$ tais que existe um vetor $v \in V$, que satisfaz $T(v) = w$. Ou seja,*

$$Im(T) = \{w \in W | T(v) = w, para\ algum\ v \in V\}.$$

Note que $Im(T)$ é um subconjunto de W e, além disso, é um subespaço vetorial de W.

Teorema 3.38: Seja $T: V \to W$ uma transformação linear. O conjunto $Im(T)$, imagem da transformação linear T, é um subespaço vetorial de W.

Demonstração: Vamos mostrar que a $Im(T)$ satisfaz as condições para ser subespaço vetorial de W, conforme definido em Definição 3.36 e Definição 3.37. Então,

i. Como T é uma transformação linear, sabemos que $\ker(T)$ contém pelo menos o elemento neutro de V, ou seja, $T(0) = 0$. Dessa forma, existe pelo menos um elemento em V que é levado no elemento neutro de W pela transformação linear T, o que implica que $0 \in Im(T)$;

ii. Considerando $w_1, w_2 \in Im(T)$, temos que existem $v_1, v_2 \in V$ tais que

$$T(v_1) = w_1$$

e

$$T(v_2) = w_2.$$

Assim, como T é transformação linear, temos:

$$T(v_1 + v_2) = T(v_1) + T(v_2)$$
$$= w_1 + w_2$$

Logo, existe o elemento $v_1 + v_2 \in V$ tal que $T(v_1 + v_2) = w_1 + w_2$ e, portanto, $w_1 + w_2 \in Im(T)$;

iii. Considerando $w \in Im(T)$ e $\alpha \in \mathbb{F}$, temos que existe um $v \in V$ tal que

$$T(v) = w.$$

Como T é transformação linear, temos:

$$T(\alpha v) = \alpha T(v)$$
$$= \alpha w.$$

Assim, existe o elemento $\alpha v \in V$ tal que $T(\alpha v) = \alpha w$, logo $\alpha w \in Im(T)$.

Dessa forma, podemos concluir que $Im(T)$ é um subespaço vetorial de W.

Exemplo 3.39. Seja $T: \mathbb{R}^2 \to \mathbb{R}$, definida por $T(x, y) = x + y$. Para calcular o núcleo dessa transformação linear devemos obter o conjunto de vetores (x, y) em $\mathbb{R}^2$ tais que $T(x, y) = x + y = 0$, ou seja, devemos obter a solução de

$$x + y = 0 \Rightarrow y = -x.$$

Dessa forma,

$$\text{Ker}(T) = \{(x, -x) \in \mathbb{R}^2 | \, x \in \mathbb{R}\}$$
$$= \{x(1, -1) | x \in \mathbb{R}\}$$
$$= [(1, -1)].$$

A imagem dessa transformação linear é o conjunto dos números reais, isto é, $Im(T) = \mathbb{R}$, pois para $w \in \mathbb{R}$, tem-se $w = T(w, 0)$.

4 CÓDIGOS CORRETORES DE ERROS

Neste capítulo, será realizado um exame aprofundado de conceitos relacionados aos códigos corretores de erros. No tópico "Conceitos Iniciais", serão fornecidas as definições essenciais de espaços métricos, métrica, métrica de Hamming, disco e esfera de um código, menor inteiro, distância mínima, código perfeito e parâmetros fundamentais de um código. No subsequente tópico "Códigos Lineares", serão apresentadas definições cruciais referentes a esses códigos, incluindo o peso de um código linear e a relação entre o peso e a distância mínima de um código linear. Ademais, será abordada a probabilidade de correção e detecção de um código linear.

A construção desse capítulo é embasada nas seguintes referências bibliográficas: [1], [6], [13], [14], [15].

4.1 Conceitos iniciais

Antes de adentrar aos códigos corretores de erros, seguem alguns exemplos.

Exemplo 4.1. O português, idioma falado no Brasil, serve como exemplo de um sistema de correção de erros. Considerando o alfabeto P da língua portuguesa, composto por 26 letras, além do espaço em branco e das letras acentuadas, incluindo o "c" cedilha, temos um total de 39 elementos. Uma palavra em português pode ser vista como um elemento de P^{46}, uma vez que a palavra mais longa registrada no dicionário possui 46 letras, como no caso de "pneumoultramicroscopicossilicovulcanoconiótico". Palavras com menos de 46 letras são completadas com espaços em branco à direita, que são omitidos na escrita. Assim, o conjunto C, contendo todas as palavras da língua portuguesa, é um subconjunto de P^{46} e, portanto, um sistema de correção de erros. Por exemplo, suponhamos que, ao escrever uma palavra, cometemos um erro e produzimos a sequência de letras "corrito". Como essa palavra não pertence a C, percebemos que ocorreu um erro, e podemos corrigi-lo, identificando que a palavra correta seria "correto". No entanto, é importante observar que esse sistema de correção não é muito eficiente, pois se a palavra "sem" for escrita erroneamente como "som" ou "sim", o erro não seria detectado nem corrigido.

Exemplo 4.2. Os códigos de barras presentes nos produtos que adquirimos e o número do nosso CPF (Cadastro de Pessoas Físicas) representam exemplos de códigos corretores de erros, cujo alfabeto é $A = \{0,1,2,3,4,5,6,7,8,9\}$. No caso dos códigos de barras, os símbolos estão no conjunto A^{13}, enquanto para o CPF, estão no conjunto A^{11}.

Exemplo 4.3. (Código da Nave) Vamos considerar um cenário em que há um protótipo de uma nave espacial que está voando a uma altitude de 20 metros acima do solo. Neste cenário, quando são dados comandos, como Para Cima, Leste, Sudeste, Sul, Oeste, Noroeste, Norte ou Para Baixo, a nave se move na direção correspondente a esses comandos. Estes oito comandos podem ser codificados como elementos de $\mathbb{F}_2^3$, conjunto de palavras formado por duas letras, cujo comprimento das palavras é três, conforme tabela abaixo.

$Para\ Cima \rightarrow 000$
$Leste \rightarrow 001$
$Sudeste \rightarrow 010$
$Sul \rightarrow 011$
$Oeste \rightarrow 100$
$Noroeste \rightarrow 101$
$Norte \rightarrow 110$
$Para\ Baixo \rightarrow 111$

Os códigos apresentados acima são chamados de código da fonte. Suponhamos que esses ternos ordenados devam ser transmitidos via rádio e que, durante o percurso, o sinal sofra interferências. Imaginemos que a mensagem 110 (Norte) possa ser recebida como 111 (Para Baixo), levando o protótipo ir Para Baixo em vez de ir para o Norte. Para tentar corrigir tais erros, pode-se recodificar as palavras, adicionando redundâncias nos códigos da fonte, de forma a permitir a detecção e correção dos erros. Podemos, por exemplo, modificar o nosso código como demonstrado na tabela abaixo:

$Para\ Cima \rightarrow 000 \rightarrow 0000000$
$Leste \rightarrow 001 \rightarrow 0010111$
$Sudeste \rightarrow 010 \rightarrow 0101010$
$Sul \rightarrow 011 \rightarrow 0111101$
$Oeste \rightarrow 100 \rightarrow 1001100$
$Noroeste \rightarrow 101 \rightarrow 1011011$
$Norte \rightarrow 110 \rightarrow 1100110$
$Para\ Baixo \rightarrow 111 \rightarrow 1110001$

Nessa recodificação, as três primeiras posições reproduzem o código da fonte, enquanto as demais posições são redundâncias introduzidas adequadas. O novo código inserido na recodificação é chamado de código de canal.

Vamos supor que ocorra um erro durante a transmissão de uma das palavras, por exemplo, a palavra 1110001 (Para Baixo), e a mensagem recebida seja 1110000. Ao comparar essa mensagem com as palavras do código de canal, percebe-se que ela não pertence ao conjunto do código de canal, o que permite detectar a presença de erros. A palavra do código de canal mais próxima da referida mensagem (ou seja, aquela que possui o menor número de elementos diferentes) é 1110001, que é, portanto, a palavra que foi originalmente transmitida.

Para construirmos de forma eficiente um código corretor de erros, é necessário definir alguns de seus elementos básicos, que são os seguintes:

- Um conjunto finito e não vazio A, denominado alfabeto. Denota-se por $|A| = q$ o número de elementos desse conjunto;
- Um código corretor de erros C é um subconjunto próprio de A^n, para algum $n \in \mathbb{N}$, em que n representa o comprimento dos elementos do código. Os elementos do código são chamados de “palavras” e consistem em sequências finitas formadas pelos elementos do alfabeto A, todas com o mesmo comprimento n. Por exemplo, podemos representar um elemento de um código como um vetor $v = (v_1, v_2, \cdots, v_n) \in A^n$, onde $v_1, v_2, \cdots, v_n \in A$, e o comprimento do vetor é n.

Para compreendermos melhor os códigos corretores de erros, precisamos, primeiramente, definir o conceito de métrica e espaços métricos.

Definição 4.4. *(Métrica) Uma métrica em um conjunto não vazio X é uma função $d: X \times X \to \mathbb{R}$ satisfazendo as seguintes propriedades:*

i. $d(x,y) > 0$ *se* $x \neq y$ *e* $d(x,x) = 0$*, para quaisquer* $x, y \in X$*;*

ii. $d(x,y) = d(y,x)$*, para quaisquer* $x, y \in X$*;*

iii. $d(x,z) \leq d(x,y) + d(y,z)$*, para quaisquer* $x, y, z \in X$*.*

Definição 4.5. *(Espaços Métricos) Um Espaço Métrico é um conjunto não vazio munido de uma métrica. Em outras palavras, é um par ordenado (M,d), em que M é um conjunto não vazio e d é uma métrica em M.*

Exemplo 4.6. Consideremos um conjunto M formado por três objetos aleatórios, como um dado, um cubo e uma tesoura, denotados por d, c e t, respectivamente. Agora, definimos a função $d: M \times M \to \mathbb{R}$ sendo a distância entre os elementos do conjunto. Se um elemento é comparado consigo mesmo, a distância é zero, ou seja, $d(x,x) = 0$ para qualquer $x \in M$. Por outro lado, a distância entre qualquer objeto e um objeto diferente é igual a um, ou seja, $d(x,y) = 1$ para quaisquer $x, y \in M$, com $x \neq y$.

Vamos mostrar que (M,d) é um espaço métrico. Para isto, devemos verificar que as propriedades da Definição 4.4. são válidas. De fato, pela forma que definimos a função, temos que $d(x,x) = 0$, para qualquer $x \in M$ e $d(x,y) = 1 > 0$ para quaisquer $x, y \in M$, com $x \neq y$, satisfazendo assim a propriedade (i). Além disso, a condição (ii) também é satisfeita, pois $d(x,y) = 1 = d(y,x)$ para quaisquer $x, y \in M$, com $x \neq y$. Agora, para verificar a condição (iii), isto é, $d(x,z) \leq d(x,y) + d(y,z)$ para quaisquer $x, y, z \in M$, separaremos em dois casos:

- Caso (1): Se $x = z$, então é óbvio que $d(x,z) \leq d(x,y) + d(y,z)$, independentemente de quem seja y, pois 0 é menor ou igual à soma de quaisquer números positivos, inclusive o próprio zero.
- Caso (2): Se $x \neq z$, então certamente temos que ou $x \neq y$ ou $z \neq y$ (pois, se $x = y$ e $y = z$, então $x = z$, o que contradiz a hipótese). Portanto,

$$d(x,y) + d(y,z) \geq 1 = d(x,z).$$

Dessa forma, podemos concluir que (M,d) é um espaço métrico, pois satisfaz todas as propriedades da Definição 4.4.

Exemplo 4.7. (A reta real $\mathbb{R}$) A métrica neste caso é $d(x,y) = |x-y|$.

Exemplo 4.8. (O plano Euclidiano $\mathbb{R}^2$): Sejam $x = (x_1, x_2)$ e $y = (y_1, y_2)$ elementos de $\mathbb{R}^2$. Definimos a métrica d neste caso como:

$$d(x,y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}.$$

Definição 4.9. *Dados dois elementos $u, v \in \mathbb{F}^n$, a distância de Hamming entre u e v é definida como*

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

Proposição 4.10. *Dados $u, v, w \in \mathbb{F}^n$, valem as seguintes propriedades:*

i. *Positividade: $d_H(u,v) \geq 0$, valendo a igualdade se, e somente se, $u = v$.*

ii. *Simetria: $d_H(u,v) = d_H(v,u)$.*

iii. *Desigualdade Triangular: $d_H(u,v) \leq d_H(u,w) + d_H(w,v)$.*

Demonstração:

i. Temos por definição que

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

Para $u \neq v$, existe $1 \leq i \leq n$, tal que $u_i \neq v_i$. Então, $d_H(u,v) > 0$.

Agora, para a igualdade teremos: (Ida) Se $d(u,v) = 0$, temos que $u_i = v_i$ para $i = 1, \ldots, n$ e daí $u = v$. (Volta) Se $u = v$, temos $u_j = v_j$, para todo $1 \leq j \leq n$ e, consequentemente, $d(u,v) = 0$.

ii. Pela definição de distância de Hamming temos que

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

iii. A contribuição das i-ésimas coordenadas de u e v para $d_H(u,v)$ é igual a zero se $u_i = v_i$ e igual a um se $u_i \neq v_i$. No caso em que a contribuição é igual a zero, certamente a contribuição das i-ésimas coordenadas a $d_H(u,v)$ é menor ou igual a das i-ésimas coordenadas a $d_H(u,w) + d_H(v,w)$, que podem

resultar em 0, 1 ou 2. No outro caso, temos que $u_i \neq v_i$ e, portanto, não podemos ter $u_i = w_i$ e $w_i = v_i$ (pois $d_H(u,v)$ seria maior que $d_H(u,w) + d_H(v,w)$). Consequentemente, a contribuição das i-ésimas coordenadas a $d_H(u,w) + d_H(v,w)$ é maior ou igual a 1, que é a contribuição das i-ésimas coordenadas a $d(u,v)$. Portanto, a desigualdade triangular vale.

Exemplo 4.11. Seja $u = (0000)$ e $v = (1011)$, com $u, v \in \mathbb{F}_2^4$, então a distância de Hamming entre u e v é

$$d_H(u,v) = d_H(0000,1011) = |\{1,3,4\}| = 3.$$

Ao provar as três propriedades da proposição, mostramos que 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 4.12. *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:*

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

Exemplo 4.13. Considere o conjunto $C = \{0000, 0111, 1010, 1101\} \subset \mathbb{F}_2^4$. Para identificar as palavras em $\mathbb{F}_2^4$ que estão a uma distância de 3 da palavra 0000 no código, procedemos da seguinte maneira:

- Para encontrar as palavras que estão exatamente a uma distância de 3 de 0000, ou seja, $S(0000,3) = \{u \in \mathbb{F}_2^4 | d(u,0000) = 3\}$, selecionamos aquelas palavras que diferem em três componentes de 0000. Nesse contexto, as palavras 0111, 1110, 1011 e 1101 atendem a essa condição.
- Agora, para determinar as palavras que estão a uma distância máxima de 3 de 0000, ou seja, $D(0000,3) = \{u \in \mathbb{F}_2^4 | d(u,0000) \leq 3\}$, precisamos considerar todas as palavras que possuem distância 0, 1, 2 e 3 em relação à palavra 0000 do código. Isso envolve encontrar as palavras que pertencem às esferas $S(0000,0)$, $S(0000,1)$, $S(0000,2)$ e $S(0000,3)$. Nesse caso, as palavras que distam no máximo 3 de 0000 serão todas as palavras de $\mathbb{F}_2^4$,

exceto a palavra 1111, pois esta é a única que difere em quatro componentes de 0000.

Assim, resumidamente, temos

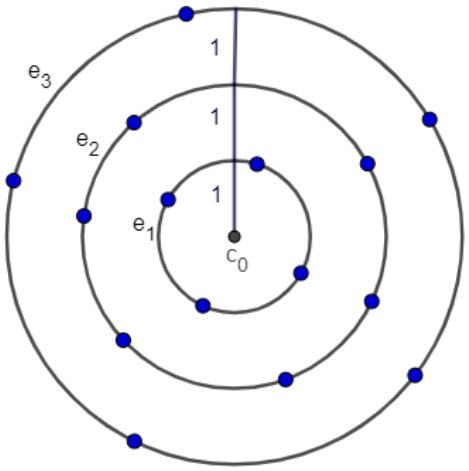
$$S(0000, 3) = \{0111, 1110, 1011, 1101\}$$

e

$$D(0000, 3) = Todas\ as\ palavras\ de\ \mathbb{F}_2^4, exceto\ 1111.$$

Geometricamente, podemos pensar no disco como sendo formado por camadas como de cebola, onde seu centro é c_0. A figura abaixo exemplifica a cardinalidade do disco $D(0000,3)$.

Figura 1: Representação do disco $D(0000,3)$.



Fonte: Arquivo da autora.

Esses são conjuntos finitos e o próximo lema fornece as suas cardinalidades.

Lema 4.14. *Para todo $a \in \mathbb{F}^n$ e todo número natural $r > 0$, temos que*

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

com q sendo o número de letras de um código.

Demonstração: Pela Definição 4.12, sabemos que $S(a,i) = \{u \in \mathbb{F}^n | d(u,a) = i\}$ e $S(a,j) = \{v \in \mathbb{F}^n | d(v,a) = j\}$, dessa forma temos que se $i \neq j$, , pode-se concluir que $S(a,i) \cap S(a,j) = \emptyset$. Dessa forma, vamos ter

$$\bigcup_{i=0}^{r} S(a,i) = D(a,r).$$

Daí temos

$$|S(a,i)| = \binom{n}{i}(q-1)^i.$$

Já que o número de palavras que diferem i componentes de a em $\mathbb{F}^n$ é $\binom{n}{i}$ e temos $q-1$ escolhas possíveis de elementos de $\mathbb{F}-\{0\}$ para cada componente de a. Assim, temos $(q-1)^i$ escolhas de componentes não nulas e diferentes das componentes de a. Note que o número de palavras que coincidem com a é $\binom{n}{0}$.

De forma geral,

$$|S(a,0)| = |\{u \in \mathbb{F}^n; d(u,a) = 0\}| = \binom{n}{0}(q-1)^0 = 1;$$

$$|S(a,1)| = |\{u \in \mathbb{F}^n; d(u,a) = 1\}| = \binom{n}{1}(q-1)^1 = n(q-1);$$

$$|S(a,2)| = |\{u \in \mathbb{F}^n; d(u,a) = 2\}| = \binom{n}{2}(q-1)^2$$

$$\vdots$$

$$|S(a,r)| = |\{u \in \mathbb{F}^n; d(u,a) = r\}| = \binom{n}{r}(q-1)^r.$$

Portanto, ao somar todas as cardinalidades das superfícies esféricas obtemos a cardinalidade do disco:

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

Note que o somatório acima não depende da palavra a.

Exemplo 4.15. No código do Robô, temos o conjunto

$$C = \{(00000), (01011), (10110), (11101)\} \subset \mathbb{F}_2^5.$$

Suponhamos que c_1 represente a palavra 00000 nesse código. Nosso objetivo consiste em calcular o número de palavras no espaço $\mathbb{F}_2^5$ que estão a uma distância máxima de 2 do centro c_1, ou seja, determinar $|D(c_1,2)|$.

Nesse cenário, é importante ressaltar que a única palavra que se encontra a uma distância de zero de c_1 é o próprio centro, ou seja, 00000.

Em relação às palavras que estão a uma distância de 1 do centro c_1, elas se diferem em apenas uma componente em relação à palavra 00000. Exemplos disso são $10000, 01000, 00100, \cdots, 00001$. Para identificar essas palavras, existem $\binom{5}{1} = 5$ maneiras de escolher a posição do dígito distinto.

Além disso, as palavras que estão a uma distância de 2 de c_1 são aquelas que diferem em duas componentes em relação a 00000, como por exemplo, $11000, 01100, 10100, \cdots, 00011$ e assim sucessivamente. Para encontrá-las, basta realizar $\binom{5}{2} = 10$, visto que há 10 maneiras possíveis para as posições dos dígitos distintos.

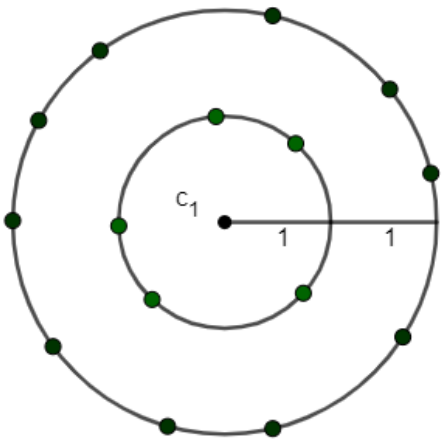
Dessa forma, pelo Lema 4.14, vamos ter:

$$|D(00000,1)| = \sum_{i=0}^{2} \binom{5}{i} (q-1)^i = 1 \cdot 1 + 5 \cdot 1 + 10 \cdot 1 = 16.$$

A cardinalidade do disco é determinada pela quantidade total de palavras que estão a uma distância de 0, 1 e 2 do seu centro.

Geometricamente, podemos pensar no disco como sendo formado por camadas como de cebola, onde seu centro é c_1. A figura abaixo exemplifica a cardinalidade do disco $D(00000,2)$.

Figura 2: Representação do disco $D(00000,2)$.



Fonte: Arquivo da autora.

Definição 4.16. *(Distância mínima) Seja C um código. A distância mínima de C é o número*

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

Exemplo 4.17. Seja C o código do Robô, calculemos as distâncias entre as palavras de C:

$$d_H(00000, 01011) = 3$$
$$d_H(00000, 10110) = 3$$
$$d_H(00000, 11101) = 4$$
$$d_H(01011, 10110) = 4$$
$$d_H(01011, 11101) = 3$$
$$d_H(10110, 11101) = 3$$

Portanto, temos que $d = 3$.

Definição 4.18. *(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 4.19. Seja C um código com distância mínima d. Se $u, v \in C$ e $u \neq v$, então

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

Demonstração: Sejam $u, v \in C$. Vamos supor por absurdo que existe

$$x \in D(u,\kappa) \cap D(v,\kappa),$$

teríamos $x \in D(u,\kappa)$ e $x \in D(v,\kappa)$, disto $d(u,x) \leq \kappa$ e $d(v,x) \leq \kappa$ e, portanto, pela desigualdade triangular, pela simetria e pela definição de κ,

$$d(u,v) \leq d(u,x) + d(v,x) \leq 2\kappa \leq d - 1,$$

o que é absurdo, pois, pela definição de distância mínima, $d(u,v) \geq d$, ou seja, a distância $d(u,v)$ não pode ser menor que a distância mínima d.

A importância dos números κ e d de um código é destacada no resultado a seguir e está inteiramente relacionada com a detecção e correção de erros.

Teorema 4.20. 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.

Demonstração:

(i) Suponha que, ao transmitirmos uma palavra w_1 do código, ela sofra interferência de t erros, tal que $t \leq d-1$, formando a palavra w_2. Dessa forma, a palavra w_2 não pode pertencer ao código, uma vez que, do contrário, teríamos $d_H(w_1, w_2) = t \leq d-1 < d$, um absurdo. Logo, w_2 não pertence ao código e, assim, é possível detectar o erro.

(ii) Se ao transmitirmos uma palavra u de C e ocorrer t erros, com $t \leq \kappa$, recebendo a palavra r, então $d_H(r,u) = t \leq \kappa$, logo $r \in D(u,k)$. Portanto, temos que $D(u,\kappa) \cap D(r,\kappa) \neq \emptyset$, então pelo Lema 4.19, $r \notin C$. Isso determina u univocamente a partir de r e nos garante a correção de até κ erros.

Exemplo 4.21. Considere o código $C = \{(000000), (010111), (101110), (111001)\} \subset \mathbb{F}_2^6$. Temos que a distância mínima d é igual a 4, logo é possível corrigir

$$\kappa = \left[\frac{d-1}{2}\right] = \left[\frac{4-1}{2}\right] = \left[\frac{3}{2}\right] = [1{,}5] = 1 \text{ erro}$$

e detectar

$$d - 1 = 4 - 1 = 3 \text{ erros}$$

sem encontrar outra palavra que pertence ao código. Por exemplo, ao transmitirmos uma palavra e por alguma interferência ocorra erro, e a palavra recebida seja 001000, podemos detectar seu erro, pois ela não pertence ao código, e ainda corrigi-lo para a palavra 000000, que é a palavra com menor número de caracteres diferentes. Já se nesse caso a palavra recebida fosse 011000, conseguiríamos detectar seus erros já que ela não pertence ao código, no entanto, não conseguiríamos corrigi-los, pois

$$d_H(011000, 000000) = d_H(011000, 111001) = 2.$$

Exemplo 4.22. Considere o código

$$C = \{(0000000000), (01011101101), (1011010110), (1110111011)\} \subset \mathbb{F}_2^{10}.$$

Temos que a distância mínima d é igual a 6, logo é possível corrigir

$$\kappa = \left[\frac{d-1}{2}\right] = \left[\frac{6-1}{2}\right] = \left[\frac{5}{2}\right] = [2{,}5] = 2 \text{ erros}$$

e detectar

$$d - 1 = 6 - 1 = 5 \text{ erros}$$

sem encontrar outra palavra que pertence ao código. Por exemplo, ao transmitirmos uma palavra e por alguma interferência ocorra erro, e a palavra recebida seja 0110101101, podemos detectar seu erro, pois ela não pertence ao código, e ainda corrigi-lo para a palavra 01011101101, que é a palavra com menor número de caracteres diferentes. Já se nesse caso a palavra recebida fosse 0110111101, conseguiríamos detectar seus erros já que ela não pertence ao código, no entanto, não conseguiríamos corrigi-los, pois

$$d_H(0110111101, 01011101101) = d_H(0110111101, 1110111011) = 3.$$

Definição 4.23. *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*

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

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.

Exemplo 4.24. O código do Robô não é um código perfeito. Podemos verificar isso calculando $|D(c,1)|$. Consideremos $c = 00000$. Vamos calcular $|D(00000,1)|$, ou seja,

$$|D(00000,1)| = \sum_{i=0}^{1} \binom{5}{i} (q-1)^i = 1 \cdot 1 + 5 \cdot 1 = 6.$$

Dessa forma, temos que o disco $D(00000,1)$ possui 6 elementos, o mesmo acontece com todos os discos em torno das demais palavras do código. Assim, teremos:

$$\left| \bigcup_{c \in C} D(00000,1) \right| = 6 \cdot 4 = 24 \neq |\mathbb{F}_2^5| = 2^5 = 32.$$

Logo, como a união dos discos com centro em c, palavras do código, e raio $\kappa = 1$ não cobre $\mathbb{F}_2^5$, concluímos que o Código do Robô não é perfeito.

Exemplo 4.25. O código da Nave também não é um código perfeito. Podemos verificar isso seguindo o mesmo raciocínio usado no Exemplo 4.23. Primeiramente, vamos calcular $|D(0000000,1)|$. Então,

$$|D(0000000,1)| = \sum_{i=0}^{1} \binom{7}{i} (q-1)^i = 1 \cdot 1 + 7 \cdot 1 = 8.$$

Dessa forma, temos que o disco $D(0000000,1)$ possui 8 elementos. Diante disto, podemos afirmar que todos os discos em torno das demais palavras do código também terão 8 elementos. Assim, teremos:

$$\left| \bigcup_{c \in C} D(0000000,1) \right| = 8 \cdot 8 = 64 \neq |\mathbb{F}_2^7| = 2^7 = 128.$$

Logo, como a união dos discos com centro em c e raio $\kappa = 1$ não cobre $\mathbb{F}_2^7$, concluímos que o Código da Nave também não é perfeito.

Exemplo 4.26. O código $C = \{000,111\} = \{c_0, c_7\} \subset \mathbb{F}_2^3$ é um código perfeito. A distância mínima de C é $d = 3$, logo $\kappa = 1$. Sabendo disso, vamos calcular a cardinalidade do disco de centro 000, daí

$$|D(000,1)| = \sum_{i=0}^{1} \binom{3}{i} (q-1)^i = 1 \cdot 1 + 3 \cdot 1 = 4.$$

Dessa forma, temos que ambos os discos com centros 000 e 111 possuem 4 elementos. Assim, teremos:

$$\left|\bigcup_{c\in C} D(000,1)\right| = 4 \cdot 2 = 8 = |\mathbb{F}_2^3| = 2^3 = 8.$$

Portanto, como o código C cobre todo $\mathbb{F}_2^3$, o código C é perfeito.

4.2 Códigos Lineares

Na prática, a classe de códigos mais utilizada é a chamada classe dos códigos lineares.

Denotaremos por $\mathbb{F}$ um corpo finito com q elementos tomados como alfabeto. Dessa forma, temos para cada número natural n, um $\mathbb{F}$-espaço vetorial $\mathbb{F}^n$ de dimensão n.

Definição 4.27. *Um código $C \subset \mathbb{F}^n$ será chamado de código linear se for um subespaço vetorial de $\mathbb{F}^n$.*

Em outras palavras, um $(n; M)$ código C sobre $\mathbb{F}_q$ é um subconjunto de $\mathbb{F}_q^n$ com M elementos. É possível enriquecer C através da estrutura de espaço vetorial. Assim sendo, dizemos que $C \subset \mathbb{F}_q^n$ é um $[n; k]$ código linear sobre $\mathbb{F}_q$ se C for um subespaço vetorial de dimensão k de $\mathbb{F}_q^n$.

A própria estrutura de espaço vetorial possibilita, em determinadas circunstâncias, a detecção de erros. Consideremos um código linear C com parâmetros $[n; k]$, onde $k < n$, e $v \in C$ seja uma palavra. Suponha que, ao transmitirmos a palavra v, a palavra recebida seja w (podendo eventualmente ser $v = w$). Ao recebermos a mensagem w, procedemos, antes de qualquer outra ação, com a verificação de que essa mensagem é uma palavra válida em nosso vocabulário, ou seja, verificamos se $w \in C$. Essa verificação é facilitada se nos lembrarmos que um subespaço vetorial é definido por um sistema de equações lineares homogêneas. Podemos representar esse sistema matricialmente pela equação, considerando a matriz H com os coeficientes do sistema linear

$$H\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

e temos que C é o conjunto de soluções deste sistema. Uma matriz H satisfazendo esta propriedade é chamada de matriz de verificação de paridade. Observemos que sendo C um código de dimensão k, o posto de H é $n-k$. Assim, a matriz H deve ter ao menos $n-k$ linhas linearmente independentes.

A seguir, vamos explorar como detectarmos a presença de erros. Se tivermos uma palavra $w = (w_1, \cdots, w_n)$ recebida e representarmos a matriz transposta por w^t (na realidade um vetor coluna), podemos efetuar o produto Hw^t para determinar se w pertence ao código C. Se $w \notin C$, sabemos que a mensagem recebida é equivocada, ou seja, conseguimos detectar a ocorrência de erro.

Perceba, no entanto, que é possível termos $w \neq v$, mas, ainda assim, com $w \in C$. Observemos que C possui q^k elementos, enquanto $\mathbb{F}_q^n$ possui q^n elementos, dos quais exatamente $q^n - q^k = q^k(q^{n-k} - 1)$ elementos não pertencem a C. Se considerarmos a suposição de que o ruído causa interferência na palavra transmitida v, de maneira que possamos receber qualquer elemento de $\mathbb{F}_q^n$, resultará na probabilidade de detecção de erro, a qual é expressa por:

$$P = \frac{\#(elementos\ de\ \mathbb{F}_q^n\ não\ pertencentes\ a\ C)}{\#(elementos\ de\ \mathbb{F}_q^n)}$$

$$P = \frac{q^n - q^k}{q^n}$$

$$P = 1 - \frac{1}{q^{n-k}}.$$

Como $q \geq 2$ e $n - k \geq 1$, temos que $P < 1$ e esta cresce conforme q ou $n-k$ crescem.

Assim, se quisermos detectar em média 999 erros a cada 1000 ocorrências se tivermos $q = 2$, basta termos $n - k \geq 10$. Como

$$\lim_{q \to +\infty} \frac{1}{q^{n-k}} = \lim_{n-k \to +\infty} \frac{1}{q^{n-k}} = 0,$$

podemos detectar erros com a confiança tão grande quanto desejarmos.

Observação 4.28. Por definição, todo código linear é um espaço vetorial de dimensão finita. Seja k a dimensão do código C e seja $v_1, v_2, \cdots, v_k$ uma de suas bases, dessa forma, todo elemento de C se escreve de maneira única na forma

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k,$$

onde os escalares λ_i, $i = 1, \cdots, k$, são elementos de $\mathbb{F}$. Logo, um código linear $C \subset \mathbb{F}^n$ de dimensão k possui 2^k elementos.

Exemplo 4.29. O código do Robô é um código linear. O seu alfabeto é $A = \mathbb{F}_2$ e o código é o subespaço vetorial de $\mathbb{F}_2^5$, sendo a imagem da transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_2^2 & \to & \mathbb{F}_2^5 \\ & (x_1, x_2) & \mapsto & (x_1, x_2, x_1, x_1 + x_2, x_2). \end{array}$$

Para encontrar a imagem da transformação linear fez-se o seguinte:
Sabendo que o código do Robô é dado pela transformação linear acima, definida por

$$T(0,0) = (0,0,0,0,0)$$
$$T(1,0) = (1,0,1,1,0)$$
$$T(0,1) = (0,1,0,1,1)$$
$$T(1,1) = (1,1,1,0,1).$$

Seja $\beta = \{(1,0), (0,1)\}$ uma base de $\mathbb{F}_2^2$ e seja $v = (x_1, x_2)$ um vetor qualquer de $\mathbb{F}_2^2$. Sendo assim, podemos escrever o vetor v como combinação linear dos elementos da base β. Isto é, existem escalares a e b, tais que

$$(x_1, x_2) = a(1,0) + b(0,1)$$
$$(x_1, x_2) = (a, 0) + (0, b)$$
$$(x_1, x_2) = (a, b).$$

Daí teremos $x_1 = a$ e $x_2 = b$. Logo,

$$(x_1, x_2) = x_1(1,0) + x_2(0,1).$$

Aplicando, agora, T em ambos os membros dessa igualdade vamos ter:

$$T(x_1, x_2) = x_1 T(1,0) + x_2 T(0,1). \quad (*)$$

Substituindo $T(1,0) = (1,0,1,1,0)$ e $T(0,1) = (0,1,0,1,1)$ em $(*)$, teremos:

$$\begin{aligned} T(x_1, x_2) &= x_1(1,0,1,1,0) + x_2(0,1,0,1,1) \\ T(x_1, x_2) &= (x_1, 0, x_1, x_1, 0) + (0, x_2, 0, x_2, x_2) \\ T(x_1, x_2) &= (x_1, x_2, x_1, x_1 + x_2, x_2). \end{aligned}$$

É importante ressaltar que o conjunto C é um subespaço vetorial de $\mathbb{F}_2^5$, pois ele é fechado em relação à soma, ou seja, a soma de quaisquer duas palavras pertencentes a C resulta em outra palavra desse conjunto. Além disso, ele também é fechado em relação à multiplicação por escalares de $\mathbb{F}_2$ e contém o vetor nulo (representado por (0, 0, 0, 0, 0) nesse caso).

Exemplo 4.30. O código da Nave também é um código linear. O seu alfabeto é o mesmo $A = \mathbb{F}_2$ e o código é um subespaço vetorial de $\mathbb{F}_2^7$, sendo a imagem da transformação linear

$$\begin{aligned} T: \quad \mathbb{F}_2^3 &\to \mathbb{F}_2^7 \\ (x_1, x_2, x_3) &\mapsto (x_1, x_2, x_3, x_1 + x_2, x_1 + x_3, x_2 + x_3, x_3). \end{aligned}$$

A seguir, vamos ver que a distância mínima de um código linear pode ser calculada utilizando o seu peso.

Definição 4.31. *Dado $x \in \mathbb{F}^n$, define-se o peso de x como sendo o número inteiro*

$$\omega(x) \coloneqq |\{i; x_i \neq 0\}|$$

Isto é,

$$\omega(x) = d(x, 0),$$

onde d representa a métrica de Hamming.

Definição 4.32. *O peso de um código linear C é o inteiro*

$$\omega(C) \coloneqq min\{\omega(x); x \in C - \{0\}\}.$$

Proposição 4.33. *Seja $C \subset \mathbb{F}_2^n$ um código linear com distância mínima d. Tem-se que*

(i) $d(x,y) = \omega(x-y), \forall x, y \in \mathbb{F}_2^n$;

(ii) $d = \omega(C)$.

Demonstração:

i. Segue que para todo $x, y \in \mathbb{F}_2^n$, com $x = (x_1, x_2, \cdots, x_n)$ e $y = (y_1, y_2, \cdots, y_n)$ temos

$$d(x,y) = |\{i; x_i \neq y_i, 1 \leq i \leq n\}|$$
$$d(x,y) = |\{i; x_i - y_i \neq 0, 1 \leq i \leq n\}|$$
$$d(x,y) = \omega(x-y).$$

ii. Para todo par de elementos x, y em C, com $x \neq y$, tem-se $z = x - y \in C - \{0\}$. Dessa forma, temos

$$d = \min\{i; x_i \neq y_i, 1 \leq i \leq n\}$$
$$d = \min\{i; x_i - y_i \neq 0, 1 \leq i \leq n\}$$
$$d = \min\{i; z_i \neq 0, 1 \leq i \leq n\}$$
$$d = \min\{\omega(z); z \in C - \{0\}\}$$
$$d = \omega(C).$$

Perceba que, conforme mostra a Proposição 4.33., em códigos lineares o peso de um código é exatamente a distância mínima das palavras do código, ou seja, $d = \omega(C)$. Partindo desse pressuposto, podemos calcular a distância mínima d de um código linear com M elementos a partir do seu peso com $M - 1$ cálculos de distâncias, ao invés de $\binom{M}{2}$ cálculos requeridos anteriormente.

5 CÓDIGOS PERFEITOS E SEUS PARÂMETROS

Neste capítulo, 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 5.1: (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 4.23, 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 4.19, $D(c_1,\kappa) \cap D(c_2,\kappa) = \emptyset$, 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 4.14 $|D(a,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$, 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 [10]) 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,

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

Exemplo 5.2. Seja $C \subset \mathbb{Z}_2^5$ um código linear com $\kappa = 1$. O código C não é perfeito, pois não existe valor para m que satisfaça

$$5 = 1 + 2 + \cdots + 2^{5-m-1}.$$

De fato, se tomarmos $m = 1$, $m = 2$, $m = 3$ e $m = 4$, teremos, respectivamente:

$$5 = 1 + 2 + \cdots + 2^{5-1-1} \Rightarrow 5 = 1 + 2 + \cdots + 2^3 \Rightarrow 5 = 1 + 2 + 2^2 + 2^3 \Rightarrow 5 \neq 15.$$

$$5 = 1 + 2 + \cdots + 2^{5-2-1} \Rightarrow 5 = 1 + 2 + \cdots + 2^2 \Rightarrow 5 = 1 + 2 + 2^2 \Rightarrow 5 \neq 7.$$

$$5 = 1 + 2^{5-3-1} \Rightarrow 5 = 1 + 2 \Rightarrow 5 \neq 3.$$

$$5 = 2^{5-4-1} \Rightarrow 5 = 1 \Rightarrow 5 \neq 1.$$

Exemplo 5.3. Seja $C = \{0000000000, 0010010110, 0101001100, 0111011010\}$ um código linear em $\mathbb{Z}_2^{10}$. O peso de C é $\omega(C) = 4$, logo $\kappa = 1$. Sendo assim, podemos verificar se C é ou não um código perfeito, tendo em vista que $|C| = 4 = 2^2$, então $m = 2$. Assim,

$$10 = 1 + 2 + \cdots + 2^{10-2-1} \Rightarrow 10 = 1 + 2 + \cdots + 2^7 \Rightarrow 10 \neq 1 + 2 + \cdots + 1024.$$

Portanto, C não é perfeito.

Exemplo 5.4. O código linear $C \subset \mathbb{Z}_2^7$ com $|C| = 2^4$ elementos e $\kappa = 1$ é um código perfeito. De fato, como $|C| = q^m = 2^4$, então $m = 4$. Dessa forma, pelo teorema acima, temos

$$1 + 2 + 2^{7-4-1} = 3 + 4 = 7.$$

Exemplo 5.5. O código linear $C \subset \mathbb{Z}_2^{15}$ com $|C| = 2^{11}$ elementos e $\kappa = 1$ é, também, um código perfeito. De fato, como $|C| = q^m = 2^{11}$, então $m = 11$. Dessa forma, pelo Teorema, temos

$$1 + 2 + \cdots + 2^{15-11-1} = 1 + 2 + \cdots + 2^3 = 1 + 2 + 2^2 + 2^3 = 15.$$

6 CONSIDERAÇÕES FINAIS

Nesta investigação, buscou-se estudar os códigos corretores de erros a fim de relacionar conceitos matemáticos, visando compreender o funcionamento dessa teoria que possui uma presença significativa na sociedade contemporânea. Dessa forma, o principal objetivo da pesquisa foi o estudo de uma classe de códigos conhecida como códigos perfeitos. Para isso, foram apresentados conceitos fundamentais de Álgebra, necessários para a construção do objeto de estudo abordado.

É relevante destacar que este trabalho é produto do PIBIC (Programa Institucional de Bolsas de Iniciação Científica), iniciado em 01 de setembro de 2022. Enquanto o período de pesquisa de iniciação científica permanece em curso, seu objetivo primordial reside na validação da perfeição do Código de Hamming. É oportuno salientar, no entanto, que uma exploração minuciosa deste tópico não foi possível dentro do escopo deste trabalho, em virtude da necessidade de um prazo mais amplo para a explanação de todos os conceitos requeridos pelo assunto em análise.

Não obstante, a pesquisa cumpriu efetivamente seu propósito, uma vez que o resultado fundamental da investigação, que, por sinal, não encontramos em nenhum material pesquisado, emergiu como resultado direto dos estudos conduzidos durante o período de iniciação científica.

Em relação aos procedimentos, a pesquisa é de cunho bibliográfica e exploratória. Destaca-se ainda que se utilizou a abordagem qualitativa para responder à seguinte problemática: Como determinar uma relação entre parâmetros de um código linear para saber se o mesmo é ou não perfeito?

Inicialmente, para compreendermos o que são os códigos perfeitos, foi necessário revisitar conceitos prévios essenciais para sua definição. Dentre estes, destacam-se as noções de métricas, fundamentais para compreender a Métrica de Hamming, bem como as definições de esfera e disco em um código. Além disso, a consideração de que os códigos estudados possuem uma estrutura linear em espaços vetoriais permitiu a exploração de diversas possibilidades, culminando no teorema central demonstrado neste trabalho. A análise destes aspectos contribuiu significativamente para a aprimorada compreensão dos códigos perfeitos.

Durante a realização desta pesquisa, foi evidente que existem muitos estudos publicados que abordam os códigos corretores de erros e suas diversas aplicações. No entanto, grande parte desses trabalhos consiste em dissertações de mestrado. Consequentemente, esta monografia se posiciona como um recurso de pesquisa valioso para aqueles que desejam iniciar sua jornada de estudo nos códigos corretores de erros.

Por fim, é notável que a escolha deste tema apresentou diversos desafios gratificantes, o que permitiu a obtenção de novos conhecimentos e aprofundamento nos conceitos previamente abordados durante a graduação. Adicionalmente, proporcionou uma oportunidade para uma exploração mais profunda nos estudos na área de Matemática Pura e Aplicada.

REFERÊNCIAS

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

[2] MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003. 311 p. Disponível em: https://docente.ifrn.edu.br/olivianeta/disciplinas/copy_of_historia-i/historia-ii/china-e-india. Acesso em: 16 nov. 2022.

[3] PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013. 276 p. Disponível em: https://www.feevale.br/institucional/editora-feevale/metodologia-do-trabalho-cientifico---2-edicao. Acesso em: 16 nov. 2022.

[4] SILVEIRA, Denise Tolfo; CÓRDOVA, Fernanda Peixoto. A pesquisa científica. In: GERHARD, Tatiana Engel; SILVEIRA, Denise Tolfo (org.). **Métodos de pesquisa**. Porto Alegre: Editora da UFRGS, 2009. Cap. 2. p. 31-42. Disponível em: https://lume.ufrgs.br/handle/10183/52806. Acesso em: 16 nov. 2022.

[5] SILVEIRA, Raphael Bruno Rodrigues da. **Códigos Corretores de Erros**: exemplos da matemática aplicada em situações do cotidiano. 2015. 99 f. Dissertação (Mestrado) - Curso de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional, Instituto de Ciências Exatas, Universidade Federal Rural do Rio de Janeiro, Seropédica, 2015. Disponível em: https://tede.ufrrj.br/jspui/handle/jspui/2883. Acesso em: 12 abr. 2023.

[6] MILIES, César Polcino. **Breve introdução à teoria dos códigos corretores de erros**. In: 1º Colóquio de Matemática da Região Centro-Oeste, 2009. UFMS, Campo Grande. **Anais...** São Paulo: Instituto de Matemática e Estatística da Universidade de São Paulo, 2009. Disponível em: http://www.mat.ufrgs.br/~backes/AnexosPDF/FArit-2019/introducao%20aos%20codigos%20corretores%20de%20erros.pdf. Acesso em: 15 nov. 2022.

[7] SANTOS, Jefson dos. **Congruências modulares, corpos finitos e aplicações**. 2015. 54 f. Dissertação (Mestrado) - Curso de Mestrado Profissional em Matemática, Universidade Federal de Sergipe, São Cristóvão, 2015. Disponível em: https://ri.ufs.br/handle/riufs/6527. Acesso em: 03 out. 2022.

[8] TARCHA, Alexsander Andrey Gomes. **Um estudo dos três problemas clássicos da Geometria**. 2019. 88 f. TCC (Graduação) - Curso de Licenciatura em Matemática, Instituto Federal de Educação, Ciência e Tecnologia de São Paulo-IFSP, São Paulo, 2019. Disponível em: https://eadcampus.spo.ifsp.edu.br/pluginfile.php/261871/mod_resource/content/0/TCC%20Tarcha%20Alexsander.%20A.G%20Vers%C3%A3o%20Final%20.pdf. Acesso em: 02 jun. 2023

[9] SILVA, Valter Félix Pereira da. **Aplicações dos Códigos Corretores de Erros com fundamentação teórica em Álgebra**. 2020. 125 f. TCC (Graduação) - Curso de Licenciatura em Matemática, Instituto Federal de Educação, Ciências e Tecnologia de São Paulo, São Paulo, 2020. Disponível em: https://app.uff.br/riuff/bitstream/handle/1/4176/Jo%C3%A3oVitorMedeiros%202016-2.PDF?sequence=1&isAllowed=y. Acesso em: 12 maio 2023.

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

[11] RITTER, Donizete. **Um estudo sobre Códigos Corretores de Erros em espaços sobre posets**. 2009. 74 f. Dissertação (Mestrado) - Curso de Mestrado Profissional em Matemática, Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas, 2009. Disponível em: http://repositorio.unicamp.br/Acervo/Detalhe/436921. Acesso em: 12 abr. 2023.

[12] 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.

[13] DIAS, José Silvino. **O Código da Mariner 9**. 2017. 23 f. Dissertação (Mestrado) - Curso de Mestrado Profissional em Matemática-PROFMAT, Departamento de Física e Matemática, Universidade Federal de São João Del-Rei, Ouro Branco, 2017. Disponível em: https://www.sje.ifmg.edu.br/portal/images/artigos/biblioteca/teses-dissertacoes-docentes/jose-silvino-dias-diss.pdf. Acesso em: 28 abr. 2023.

[14] 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.

[15] ENDO, Daniela Hiromi Cavamura. **Espaços Métricos**: uma introdução. 2015. 63 f. TCC (Graduação) - Curso de Licenciatura em Matemática, Centro de Ciências Exatas e de Tecnologia, Universidade Federal de São Carlos, São Carlos, 2015. Disponível em: https://www.dm.ufscar.br/profs/franciscobraun/Arquivo/teses/DanielaEndo.pdf. Acesso em: 20 jul. 2023.