Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

Corpos de Funções Algébricas sobre Corpos Finitos e Códigos Corretores de Erros

Rayanne Auxiliadora de Oliveira Matos

Goiânia

2021

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA) PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES

E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo das Teses e Dissertações disponibilizado na BDTD/UFG é de responsabilidade exclusiva do autor. Ao encaminhar o produto final, o autor(a) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do material bibliográfico

[X] Dissertação [ ] Tese

2. Nome completo do autor

Rayanne Auxiliadora de Oliveira Matos

3. Título do trabalho

Corpos de Funções Algébricas sobre Corpos Finitos e Códigos Corretores de Erros

4. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador)

Concorda com a liberação total do documento [**X**] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante:
a) consulta ao(à) autor(a) e ao(à) orientador(a);
b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo da tese ou dissertação.
O documento não será disponibilizado durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

Obs. Este termo deverá ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Jhone Caldeira Silva**, **Professor do Magistério Superior**, em 27/04/2021, às 13:27, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **RAYANNE AUXILIADORA DE OLIVEIRA MATOS**, **Discente**, em 27/04/2021, às 14:06, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2029011** e o código CRC **27DE4945**.

Referência: Processo nº 23070.012523/2021-11 SEI nº 2029011

Rayanne Auxiliadora de Oliveira Matos

Corpos de Funções Algébricas sobre Corpos Finitos e Códigos Corretores de Erros

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.
Área de Concentração: Álgebra
Orientador: Prof. Dr. Jhone Caldeira Silva

Goiânia

2021

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Matos, Rayanne Auxiliadora de Oliveira
Corpos de Funções Algébricas sobre Corpos Finitos e Códigos Corretores de Erros [manuscrito] / Rayanne Auxiliadora de Oliveira Matos. - 2021.
163 f.: il.

Orientador: Prof. Dr. Jhone Caldeira Silva.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), PROFMAT - Programa de Pós graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RG), Goiânia, 2021.
Bibliografia. Anexos. Apêndice.

1. Corpos Finitos. 2. Códigos Corretores de Erros. 3. Códigos Lineares. 4. Corpos de Funções Algébricas. 5. Códigos de Goppa. I. Silva, Jhone Caldeira, orient. II. Título.

CDU 512.5

UNIVERSIDADE FEDERAL DE GOIÁS

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

ATA DE DEFESA DE DISSERTAÇÃO

Ata nº **22** da sessão de Defesa de Dissertação de **Rayanne Auxiliadora de Oliveira Matos**, que confere o título de Mestra em Matemática, na área de concentração em **Álgebra.**

Aos oito dias do mês abril de dois mil e vinte um, a partir da 14 **horas**, por meio de video conferência devido a pandemia covid - 19, realizou-se a sessão pública de Defesa de Dissertação intitulada **"Corpos de Funções Algébricas sobre Corpos Finitos e Códigos Corretores de Erros"**. Os trabalhos foram instalados pelo Orientador, Professor Doutor Jhone Caldeira Silva – (IME/UFG) com a participação dos demais membros da Banca Examinadora: Professora Doutora Ana Paula de Araújo Chaves – (IME/UFG) e o membro titular externo o Professor Doutor Jean Carlos de Aguiar Lelis (UFPA). Durante a arguição os membros da banca **não fizeram** sugestão de alteração do título do trabalho. A Banca Examinadora reuniu-se em sessão secreta a fim de concluir o julgamento da Dissertação, tendo sida a candidata **aprovada** pelos seus membros. Proclamados os resultados pelo Professor Doutor Jhone Caldeira Silva, Presidente da Banca Examinadora, foram encerrados os trabalhos e, para constar, lavrou-se a presente ata que é assinada pelos Membros da Banca Examinadora, aos oito dias do mês abril de dois mil e vinte um.

TÍTULO SUGERIDO PELA BANCA

Corpos de Funções Algébricas sobre Corpos Finitos e Códigos Corretores de Erros

Documento assinado eletronicamente por **Jhone Caldeira Silva**, **Professor do Magistério Superior**, em 08/04/2021, às 15:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Ana Paula De Araújo Chaves**, **Professora do Magistério Superior**, em 08/04/2021, às 15:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jean Carlos de Aguiar Lelis**, **Usuário Externo**, em 08/04/2021, às 15:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site

https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1925796** e o código CRC **D47337E0**.

Referência: Processo nº 23070.012523/2021-11 SEI nº 1925796

Rayanne Auxiliadora de Oliveira Matos graduou-se em Matemática pela Universidade Católica de Goiás em 2008, durante a graduação foi bolsista do Programa Universidade para Todos (PROUNI). Possui especialização em Matemática (2020) pelo Instituto Federal de Goiás - Câmpus Goiânia. Atua como professora efetiva de Matemática na Educação Básica na Secretaria de Estado da Educação, Cultura e Esporte de Goiás 2010, com lotação no Colégio Estadual Horácia Lobo, na cidade de Caldazinha - Goiás.

Dedico este trabalho à minha mãe, Maria, a meu esposo Celso, e aos meus filhos Oscar e Tarsila

Agradecimentos

Agradeço a Deus por me sustentar e me ajudar a seguir em frente.

Agradeço a minha família, em especial a minha mãe, Maria Izabel, por estar sempre do meu lado. Em especial também a meu marido Celso, por todo o apoio incondicional que proporcionou e continua proporcionando para que eu conseguisse manter o foco e chegar até o fim.

Agradeço ao meu orientador, Professor Dr. Jhone Caldeira Silva, pela sua disponibilidade e incentivo, desde o primeiro contato, que foram fundamentais para realizar esse estudo. Agradeço a forma interessada, extraordinária e pertinente como acompanhou a realização deste trabalho. As suas críticas construtivas, as discussões e reflexões foram fundamentais ao longo de todo o percurso.

Agradeço ao Professor Dr. Jean Carlos de Aguiar Lelis pela sugestão do tema e por toda ajuda prestada no desenvolvimento do trabalho.

Agradeço a todos os professores que tive a oportunidade de conhecer durante este curso pelo excelente trabalho desenvolvido.

Aos meus colegas da turma 2019 do PROFMAT de Goiânia agradeço por terem me mostrado a importância da união. Agradeço especialmente aos colegas Murillo Alves Macêdo e Bruno Gama, por todo apoio e companherismo que demonstraram nos momentos mais difíceis de nosso aprendizado.

Resumo

Neste trabalho serão apresentados os conceitos básicos para a construção de Códigos Corretores de Erros, em especial, a Construção de Códigos Lineares e uma breve introdução à construção dos Códigos Algébricos Geométricos. Tais códigos são utilizados para garantir a confiabilidade de mensagens enviadas por longas distâncias, por diferentes canais, sendo asssim, é necessário que existam maneiras de detectar e corrigir erros. Começamos abordando as ferramentas matemáticas necessárias para a construção dos diferentes códigos. Apresentamos os fundamentos da Teoria dos Códigos Corretores de Erros, também apresentamos como se faz a construção das matrizes geradoras e decodificadoras de um código. Apresentamos também, em particular, os Códigos Cíclicos, Códigos BCH e Códigos de Goppa Racionais, com suas matrizes geradoras e decodificadoras. Também apresentamos os Corpos de Funções Algébricas sobre Corpos Finitos, pois esses são de grande interesse para a Teoria dos Códigos, pois com essa teoria é possível construir os Códigos Algébricos Geométrico, assunto este que abordamos de maneira introdutória ao final do texto e, para o qual, indicamos algumas possibilidades de estudos futuros.

Palavras-chave Corpos Finitos, Códigos Corretores de Erros, Códigos Lineares, Corpos de Funções Algébricas, Códigos de Goppa.

Abstract

In this paper the basic concepts for the construction of Error-Correcting Codes will be presented. In particular, the construction of Linear Codes and a brief introduction to the construction of Geometric Algebraic Codes. Such codes are used to ensure the reliability of messages sent over long distances, over different channels, so it is necessary to have ways to detect and correct errors. We begin by discussing the mathematical tools needed to construct the different codes. We present the fundamentals of the Theory of Error-Correcting Codes, and present how to construct the generator and decoder matrices of a code. In particular, we also present Cyclic Codes, BCH Codes, and Rational Goppa Codes, with their generator and decoder matrices. We also present the Bodies of Algebraic Functions Fields over Finite Fields, because these are of great interest for Code Theory, since with this theory it is possible to construct Geometric Algebraic Codes, a subject that we address in an introductory way at the end of the text and, for which, we indicate some possibilities for future studies.

Keywords Finite Fields, Error-Correcting Codes, Linear Codes, Algebraic Function Fields, Goppa Codes.

Lista de Figuras

Conteúdo

Introdução

A Teoria dos Códigos Corretores de Erros teve origem na década de 1940, no Labortório Bell de Tecnologia. Nasceu dos estudos de Richard W. Hamming e Claude E. Shannon. Desde então, fazem parte do nosso cotidiano de inúmeras formas, quando estamos utilizando um meio digital para ouvir músicas, ver uma foto ou enviar mensagens, os Códigos Corretores de Erros estão presentes.

Um código corretor de erros é, em essência, um modo organizado de acrescentar dados adicionais (redundâncias) a cada informação que se deseja transmitir ou armazenar, que permita, ao recuperar a informação, detectar e corrigir erros. Isso se faz necessário, pois ao transmitir uma informação por um determinado canal (por exemplo, canal de radiofrequência, cabo, canal de micro-ondas, cabo, circuito integrado digital, disco de armazenamento, etc.) essa pode sofrer alguma interferência (ruído), fazendo com que a mensagem enviada possa não ser igual a recebida. Cabe então ao código corretor de erros, através das redundância inseridas, detectar e corrigir esses erros.

Para que possamos ter um código, precisamos de um conjuntos de símbolos (alfabeto) que serão utilizados para escrever as palavras (sequência de símbolos do alfabeto). Nesse sentido, é de fundamental importância que tenhamos uma estrutra sobre o alfabeto que nos permita utilizar ferramentas matemáticas disponíveis para que possamos desenvolver bons algoritmos de codificação e decodificação. Por isso é bastante conveniente utilizar corpos finitos. Assim, podemos verificar como um problema, a princípio "aplicado"se relaciona tão intimamente com vários tópicos da Matemática "pura".

Na História recente, temos exemplos de diferentes aplicações para a Teoria dos Códigos, em especial, nas comunicações espaciais. Imagens de Marte foram transmitidas pelas naves *Mariner 4* (1965) e *Mariner 9* (1972), nesse último foram utilizados uma família de códigos chamados *Códigos de Reed-Muller* . Os Códigos de Golay foram utilizados em 1979, pela nave espacial *Voyager* prara transmitir imagens coloridas de Júpter. Hefez e Villela (2008)

O objetivo do presente trabalho é introduzir a Teoria dos Códigos Corretores de Erros, em especial trabalhamos com uma classe específica: os Códigos Lineares. Também introduziremos a teoria dos Corpos de Funções Algébricas sobre Corpos Finitos, pois com essa teoria é possível realizar a construção dos Códigos Algébricos Geométricos. Para atingir esses objetivos, este trabalho está divido como se segue.

No Capítulo 1, abordamos alguns conceitos básicos da Álgebra Abstrata. Esses conceitos serão utilizados como ferramentas para desenvolver a Teoria dos Códigos

Corretores de Erros e a Teoria dos Corpos de Funções Algébricas sobre Corpos Finitos.

No Capítulo 2 apresentamos as extensões de corpos e diferentes representações de Corpos Finitos, a saber, a representação polinomial e a representação utilizando elementos primitivos. Esse assunto também nos ajudará a desenvolver as teorias mencionadas no parágrafo anterior.

O Capítulo 3 é dedicado aos Códigos Corretores de Erros, em especial à classe de códigos chamada Códigos Lineares. Abordamos os conceitos básicos da Teoria dos Códigos Corretores de Erros e faremos a construção das chamadas matrizes geradoras e matrizes teste de paridade que são utilizadas no processo de codificação/decodificação. São apresentados, em particular, os Códigos Cíclicos, Códigos BCH e os Códigos de Goppa Racionais.

O Capítulo 4 fornece uma introdução à teoria dos Corpos de Funções Algébricas sobre corpos finitos. O assunto é abordado do ponto de vista da teoria da valorização. A motivação para o estudo desses conceitos é a sua importância na teoria da codificação, em especial, na construção dos chamados Códigos Algébricos Geométricos. Para o desenvolvimento deste capítulo foi utilizado como referência Niederreiter (2002), e é o principal capítulo deste trabalho.

Por último, no Capítulo 5, faremos a descrição dos chamados códigos de Reed-Solomon. Tais códigos são utilizados, por exemplo, no armazenamento de som em formatos digitais. Em seguida, faremos uma generalização desses códigos para obtermos os chamados Códigos de Goppa Racionais também conhecidos como Códigos Geométricos de Goppa e fazemos alguns apontamentos sobre aprofundamentos desse estudo e aplicações.

Apresentamos também, no Apêndice, várias propostas de atividades que podem ser utilizadas para trabalhar códigos corretores de erros em sala de aula na Educação Básica.

Ressaltamos que a principal referência utilizada nesse trabalho é o artigo de Niederreiter (2002). Além disso, o aporte teórico necessário está baseado em Lidl e Niederreiter (1994), Herstein (1970), Masuda e Panario (2007) e Garcia e Lequain (2006).

1 Preliminares

Neste capítulo abordaremos importantes conceitos e resultados da Álgebra Abstrata que serão utilizados como ferramentas para o estudo da teoria dos Códigos Corretores de Erros no Capítulo 3. Também abordaremos alguns temas que serão úteis no estudo dos Corpos de Funções Algébricas sobre Corpos Finitos, assunto este que será apresentado no Capítulo 4. Para o desenvolvimento deste capítulo foram utilizadas as referências Garcia e Lequain (2006), Herstein (1970), Masuda e Panario (2007) e Lidl e Niederreiter (1994).

1.1 Anéis

A Álgebra teve um desenvolvimento tardio no que se refere à organização lógica e axiomatização. A primeira tentativa feita nesse sentido ocorreu apenas no século XIX (vale lembrar que a Geometria já recebera uma axiomatização no ano 300 a.C. com a obra *Elementos*, de Euclides). Foi Geogorge Peacok (1805-1865), que em 1830 publicou o primeiro importante trabalho escrito com a intenção de dar à Álgebra o caráter de ciência demonstrativa. Porém, Peacock renunciou suas opiniões sobre a Álgebra, pois seu trabaho trazia resultados controversos, como por exemplo, sugeria que as leis da Álgebra são as mesmas quaisquer que sejam os números ou objetos dentro dela. Em 1833, o irlândes Willian R. Hamilton (1805 - 1865) publicou um artigo onde apresentava os quarténios, onde também mostrou que as leis da Álgebra (como a comutatividade, por exemplo) podem não ser aplicadas em alguns casos. O trabalho de Hamilton e outros matemáticos colaborou, já no século XIX, para a criação de inúmeras estruturas algébricas novas, entre as quais as de corpo e de anel. Para mais detalhes, consultar Boyer e Merzbach (2019).

Vamos nos concentrar agora no conceito de anel. Na maioria dos sistemas numéricos usados na aritmética elementar, existem duas operações binárias distintas: adição e multiplicação. Temos como exemplos os números inteiros ($\mathbb{Z}$), os números racionais ($\mathbb{Q}$) e os números reais ($\mathbb{R}$). Agora vamos definir uma estrutura algébrica conhecida como **anel** que compartilha algumas das propriedades básicas desses sistemas numéricos.

Definição 1.1.1. *Um anel* $(\mathsf{A}, +, \cdot)$ *é um conjunto* A *não vazio, munido de uma operação denotada por* $+$*, chamada adição, e de uma operação denotada por* $\cdot$ *,chamada multiplicação, que satisfazem as seguintes condições:*

(A.1) *A adição é associativa, isto é,*

$$\textit{para todos } x, y, z \in A, (x + y) + z = x + (y + z).$$

(A.2) *Existe um elemento neutro com respeito à adição, isto é,*

$$\textit{existe } 0_A \in A \textit{ tal que, para todo } x \in A, 0_A + x = x + 0_A = x.$$

(A.3) *Todo elemento de* A *possui um simétrico com respeito à adição, isto é,*

$$\textit{para todo } x \in A, \textit{existe } z \in A \textit{ tal que } x + z = z + x = 0.$$

(A.4) *A adição é comutativa, isto é,*

$$\textit{para todos } x, y \in A, x + y = y + x.$$

(M.1) *A multiplicação é associativa, isto é,*

$$\textit{para todos } x, y, z \in A, (x \cdot y) \cdot z = x \cdot (y \cdot z).$$

(AM) *A adição é distributiva relativamente à multiplicação, isto é,*

$$\textit{para todos } x, y, z \in A, x \cdot (y + z) = x \cdot y + x \cdot z \textit{ e } (y + z) \cdot x = y \cdot x + z \cdot x.$$

Denotaremos simplesmente por 0 o elemento neutro da adição e por $-a$ o simétrico aditivo de a.

Com as propriedades (A.1), (A.2), (A.3) e (A.4), dizemos que $(A, +)$ é um *grupo abeliano.*

Exemplo 1.1.2. *A seguir, temos exemplos de alguns anéis.*

- *Os conjuntos* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *e* $\mathbb{C}$ *são anéis com as operações usuais de adição e multiplicação.*

- *O conjunto* $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$*, onde* $[a] = [x \in \mathbb{Z}; x \equiv a \mod n]$*. Definindo a soma* $[a] + [b]$ *e produto* $[a] \cdot [b]$ *em* $\mathbb{Z}/n\mathbb{Z}$ *da seguinte maneira:*

$$[a] + [b] = [a + b] \text{ e } [a] \cdot [b] = [a \cdot b].$$

O conjunto $\mathbb{Z}/n\mathbb{Z}$ *com as operações acima definidas é um anel. Para simplificar a notação, vamos escrever o conjunto* $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \cdots, n-1\}$ *com as operações módulo* n*.*

A definição de anel é bastante aberta no que se refere a multiplicação. Um anel pode ou não possuir elemento neutro da multiplicação. Da mesma forma, um anel poderá ou não ser comutativo, ou seus elementos podem ou não possuir inverso multiplicativo. Portanto, um anel poderá ou não possuir essas propriedades "especiais". Em caso afirmativo, esses anéis recebem nomes especias, conforme veremos na definição a seguir.

Definição 1.1.3. *Um anel* A *é chamado:*

1. ***Anel com identidade****, se existe um elemento em* A*, denotado por* 1_A*, tal que* $a \cdot 1_A = 1_A \cdot a = a$ *para todo* $a \in A$ *(nesse caso* 1_A*, o* ***elemento neutro*** *da multiplicação, é chamado de identidade, também simplesmente denotado por* 1*);*

2. ***Anel comutativo****, se a multiplicação é comutativa, isto é,* $a \cdot b = b \cdot a$ *para quaisquer* $a, b \in A$*;*

3. ***Domínio de Integridade****, se* A *é um anel comutativo com identidade e se, para quaisquer* $a, b \in A$ *tais que* $a \cdot b = 0$*, tem-se que* $a = 0$ *ou* $b = 0$*;*

4. ***Anel com Divisão****, se os elementos não nulos de* A *formam um grupo sob a multiplicação;*

5. ***Corpo****, se é um anel comutativo com divisão.*

Exemplo 1.1.4.

- *Os anéis* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *e* $\mathbb{C}$ *são comutativos.*

- *O anel* $\mathbb{Z}/n\mathbb{Z}$*, com* $n \in \mathbb{Z}$ *é um anel com unidade. De fato,*

$$[a] \cdot [1] = [a \cdot 1] = [a] = [1] \cdot [a].$$

- *Se* $n > 1$ *é um inteiro composto, então* $\mathbb{Z}/n\mathbb{Z}$ *não será um domínio de integridade. De fato, dados* $a, b \in \mathbb{Z}$ *tais que* $0 < a, b < n$ *e* $n = a \cdot b$*, temos* $[a] \cdot [b] \in \mathbb{Z}/n\mathbb{Z}$*,* $[a], [b] \neq 0$ *e* $[a] \cdot [b] = [n] = [0]$.

O próximo resultado estabelecerá uma importante relação entre um domínio de integridade e um corpo.

Teorema 1.1.1. *Todo domínio de integridade finito é um corpo.*

Demonstração: Seja A um domínio de integridade finito e a um elemento não nulo em A. Consideremos a aplicação $\phi : A \to A$ definida por $\phi(x) = ax$. Como $a(x-y) = 0$ implica que $x-y = 0$, a aplicação ϕ é injetora. Por outro lado, A é finito e, portanto, ϕ também é sobrejetora; em particular, existe $\bar{a} \in A$ tal que $a.\bar{a} = 1$. □

A recíproca deste resultado é mais geral: qualquer corpo é um domínio de integridade. Para isso, seja F um corpo e suponhamos que $a \cdot b = 0$ onde $a, b \in F$ e $a \neq 0$. Seja $\bar{a} \in F$ ta que $\bar{a}a = 1$. Então

$$b = 1 \cdot b = (\bar{a} \cdot a)b = \bar{a}(ab) = \bar{a} \cdot 0 = 0.$$

Definição 1.1.5. *Um elemento não nulo* a *num anel* A *é um divisor de zero, se existe um elemento não nulo* b *em* A *tal que* $a \cdot b = 0$.

Exemplo 1.1.6.

- *Um domínio de integridade não contém divisores de zero.*
- *Os divisores de zero em* $\mathbb{Z}/12\mathbb{Z}$ *são* $2, 3, 4, 6, 8, 9$ *e* 10.

As seguintes terminologias serão utilizadas frequentemente.

Definição 1.1.7. *Seja* A *um anel.*

1. *Um elemento* $a \in A$ *é um* ***divisor*** *de* $b \in A$*, se existe* $c \in A$ *tal que* $b = ac$*. Neste caso, escrevemos* $a|b$.
2. *Um elemento não nulo* r *é um* ***elemento invertível*** *em* A*, se existe* $s \in A$ *tal que* $rs = 1$*. Neste caso, escrevemos* $r^{-1} = s$.
3. *Os elementos* a *e* b *em* A *são* ***associados****, se existe um elemento invertível* $r \in A$ *tal que* $a = rb$.

4. *Seja* p *um elemento não nulo que não seja invertível em* A*. Dizemos que* p *é* ***irredutível*** *em* A*, se* $p = ab$ *com* $a, b \in A$ *implica que* a *ou* b *seja invertível em* A*. Caso contrário,* p *é* ***redutível*** *em* A*.*

Exemplo 1.1.8. *Num corpo, qualquer elemento não nulo é invertível.*

Um importante conceito no estudo de corpos finitos é o de característica. Mas antes de apresentá-lo, vamos enunciar a definição de múltiplo.

Definição 1.1.9. *Seja* A *um anel ,* $a \in A$ *e* n *um inteiro. Definimos o produto* na *por*

$$na = \begin{cases} 0, & \text{se } n = 0 \\ \underbrace{a + \cdots + a}_{n \text{ cópias}}, & \text{se } n > 0 \\ -((-n)a), & \text{se } n < 0 \end{cases}.$$

O elemento na é chamado de múltiplo n-ésimo de a. Essa multiplicação tem a propriedade de que $(na)(mb) = (nm)(ab)$, para todos m, n inteiros e $a, b \in A$. Usando esta operação, definimos agora a *característica* de um anel.

Definição 1.1.10. *Seja* A *um anel para o qual existe um inteiro positivo* n *tal que*

$$n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ cópias}} = 0$$

O menor tal inteiro positivo n *é chamado de* ***característica*** *de* A *e é denotado por* $car(A)$*. Neste caso, dizemos que* A *tem característica positiva, além disso, se* n *é primo, então dizemos que* A *tem característica prima. Se* A *não tem característica positiva, dizemos que* A *tem característica zero.*

Teorema 1.1.2. *Seja* A *um anel. Se* A *tem característica positiva e se* A *não contém divisores de zero, então a característica de* A *é prima.*

Demonstração: Seja $n \geq 2$ a característica de A. Escrevendo $n = ab$, onde $a, b \in \mathbb{N}$ e $1 < a, b < n$, obtemos $0 = n \cdot 1 = (ab)1 = (a \cdot 1)(b \cdot 1)$. Como A não possui divisores de zero, temos que $a \cdot 1 = 0$ ou $b \cdot 1 = 0$. Em qualquer caso, uma contradição, pois n é a característica. □

Sejam A um anel e S um subconjunto de A. Dizemos que S é um **subanel** de A se S também é um anel sob as mesmas operações de A e com o mesmo elemento neutro da multiplicação de A. Considerando as operações usuais sobre os conjuntos numéricos, $\mathbb{Z}$ é um subanel de $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, $\mathbb{Q}$ é um subanel de $\mathbb{R}$ e $\mathbb{C}$ e $\mathbb{R}$ é subanel de $\mathbb{C}$.

O próximo teorema fornece um critério muito útil para verificar que um subconjunto de um anel é de fato um subanel.

Teorema 1.1.3. *Um subconjunto S de A é um subanel se, e somente se,*

- $1_R \in S$*;*
- $s - t \in S$ *para quaiquers* $s, t \in S$*.*

Alguns anéis possuem a mesma estrutra algébrica. Esta semelhança pode ser expressa por meio de uma função que preserva os elementos neutros da multiplicação, a adição e a multiplicação.

Definição 1.1.11. *Sejam A e B anéis. Um homomorfismo de anéis é uma função $\phi : A \to B$, satisfazendo*

- $\phi(a + b) = \phi(a) + \phi(b)$ *para quaisquer* $a, b \in A$*;*
- $\phi(ab) = \phi(a)\phi(b)$ *para quaisquer* $a, b \in A$*.*

Além disso, se ϕ é bijetora, dizemos que ϕ é um isomorfismo e escrevemos $A \cong B$ para dizer que A e B são isomorfos. Como consequência dessa definição, qualquer homomorfismo também preserva zeros, negativos, multiplicação por inteiros e potências. Isso significa que se 0_A e 0_B são os zeros de A e B respectivamente, então $\phi(0_A) = 0_B$, $\phi(-a) = -\phi(a)$, $\phi(na) = n\phi(a)$ e $\phi(a^k) = \phi(a)^k$, para quaisquers $a \in A, n \in \mathbb{Z}$ e $k \in \mathbb{N}$. Se A e B forem anéis com identidade, tais que 1_A e 1_B são as unidades de A e B respectivamente, então $\phi(1_A) = 1_B$

Se $\phi : A \to B$ é um homomorfismo de anéis, a *imagem* de ϕ definida por $\phi(A) = \{b \in B; b = \phi(a) \text{para algum } a \in A\}$ é um subanel de B.

Segundo Iezzi, Dolce e Machado (1993), os isomorfismos são importantes para entender a estrutura de um corpo finito. O papel dos isomorfismos de anéis é, em essência, o de separar os anéis em classes disjuntas, de maneira tal que as propriedades pertinentes à estrutura de anel deduzidas para um dos representantes das classes possam ser estendidas para os outros anéis da mesma classe, apenas mudando conveniente as

notações (dos elementos e das operações). Reflete bem essa situação imaginar os anéis de uma mesma classe como "cópias"uns dos outros.

Outro conceito necessário para esse estudo é o de *anel quociente*, mas primeiro precisamos introduzir o conceito de ideal. Segundo Iezzi, Dolce e Machado (1993), o conceito de ideal de um anel é um dos instrumentos mais poderosos para o desenvolvimento da teoria dos anéis, e tem aplicações em diversas áreas, como por exemplo, no estudo das curvas algébricas e nos Códigos Cíclicos, conforme veremos no Capítulo 2.

Definição 1.1.12. *Um subconjunto* I *não vazio de um anel* A *é um ideal de* A *se forem verificadas as condições:*

1. $a - b \in I$ *para quaiquers* $a, b \in I$*;*
2. $r \cdot a, a \cdot r \in I$ *para quaisquers* $a \in I$ *e* $r \in A$*.*

Exemplo 1.1.13.

- *Em qualquer anel* A*, há dois ideais triviais:* $\{0\}$ *e* A*. O ideal* $\{0\}$ *é conhecido como o ideal zero. Qualquer ideal* I *de* A *é um ideal próprio se* $I \neq A$*.*
- *Dado* $a \in A$*, o conjunto* $\{ra; r \in A\}$ *é um ideal de* A *chamado o* ***ideal gerado por*** a *e denotado por* (a)*.*
- *Sejam* A *e* B *anéis. Dado um homomorfismo de anéis* $\phi : A \to B$*, o* ***núcleo de*** ϕ*, definido por* $\ker \phi = \{s \in A; \phi(s) = 0\}$*, é um ideal de* A*. De fato, suponhamos que* a *e* b *estejam no núcleo de* ϕ*. Segue que* $\phi(a - b) = \phi(a) - \phi(b) = 0$*,* $\phi(a \cdot r) = \phi(a) \cdot \phi(r) = 0 \cdot \phi(r) = 0$ *e* $\phi(r \cdot a) = \phi(r) \cdot \phi(a) = \phi(r) \cdot 0 = 0$ *para qualquer* $r \in A$*.*

A partição de um anel em conjuntos disjuntos conhecidos como *classes laterais* é bastante útil no estudo de anéis, pois dá uma maneira de construir novos anéis a partir de dados anéis.

Definição 1.1.14. *Sejam* A *um anel e* I *um ideal de* A*. O conjunto*

$$r + I = \{r + a; a \in I, r \in A\}$$

é chamado uma classe lateral de I *em* A*.*

A relação[1] em A induzida por esta definição é dada pela igualdade $r + I = s + I$, sempre que $r - s \in I$. Esta é uma **relação de equivalência**[2] e portanto as classes laterais de I em A formam uma **partição**[3] de A. Definindo as operações de adição e de multiplicação em A/I de maneira natural, não é dificil ver que A/I é um anel.

Teorema 1.1.4. *Sejam* I *um ideal de um anel* A*. Então* A/I *é um anel com a adição e a multiplicação definidas por*

$$(r + I) + (s + I) = (r + s) + I$$

e

$$(r + I)(s + I) = (rs) + I.$$

O conjunto de todas as classes laterias de I em A é conhecido como **anel quociente** de A por I e é denotado por A/I.

Definição 1.1.15.

1. *Um ideal* I *de* A *é* ***principal****, se exsite* $a \in A$ *tal que* $I = (a)$*. Neste caso,* I *também é chamado de o* ***ideal gerado por*** a*.*

2. *Um ideal* P *de* A *é* ***primo****, se* $P \neq A$ *e se* $ab \in P$ *implica que* $a \in P$ *ou* $b \in P$*.*

3. *Um ideal* M *de* A *é* ***maximal****, se* $M \neq A$ *e se os únicos ideais* I *de* A *tais que* $M \subseteq I \subseteq A$ *são* $I = M$ *e* $I = R$*.*

4. *O anel* A *é um* ***domínio de ideais principais****, se* A *é um domínio de integridade e se cada ideal* I *de* A *é principal.*

Teorema 1.1.5. *Seja* A *um anel.*

1. *Um ideal* M *de* A *é maximal se e somente se* A/M *é um corpo.*

2. *Um ideal* P *de* A *é primo se e somente se* A/P *é um domínio de integridade.*

[1] Qualquer subconjunto $S \subseteq A \times A$ é uma **relação** em A. Denotamos uma relação por $\sim$, onde $a \sim b$, se $(a, b) \in S$.

[2] A relação $\sim$ é de equivalência, se $\sim$ é reflexiva, simétrica e transitiva.

[3] Se $\sim$ é uma relação de equivalência, dizemos que a **classe de equivalência** de a é formada por todos os elementos $b \in A$ tais que $a \sim b$. Neste caso, o conjunto de todas as classes de equivalência forma uma partição de A.

3. *Todo ideal maximal é primo.*

4. *Se* A *é um domínio de ideais principais, então* $A/(p)$ *é um corpo se e somente se* p *é irredutível em* A*.*

5. *Se* A *é um domínio de ideais principais e* $p \neq 0$*, então* (p) *é um ideal primo se e somente se* (p) *é um ideal maximal.*

Um importante anel quociente utilizado na Teoria dos Códigos é o anel $\mathbb{Z}/(p)$ que é o anel quociente de $\mathbb{Z}$ pelo ideal gerado por um número primo p. Conforme veremos, esse anel é um corpo.

Teorema 1.1.6. *Seja* p *um número primo. O conjunto* $\mathbb{Z}/(p)$ *é um corpo.*

Teorema 1.1.7. *Se* $\phi : A \to B$ *é um homomorfismo de anéis, então* $A/\ker\phi$ *é isomorfo a* $\phi(A)$*.*

Demonstração: Vamos mostrar que a função $\Phi : A/\ker\phi \to \phi(A)$ com $\Phi(r + \ker\phi) = \phi(r)$ é um isomorfismo de anéis. Primeiramente, veremos que Φ está bem definida e é injetora. Sejam $r_1, r_2 \in A$. Temos que $r_1 + \ker\phi = r_2 + \ker\phi$ se, e somente se $\phi(r_1 - r_2) = 0$, o que é equivalente a $\phi(r_1) = \phi(r_2)$. Como ϕ é um homomorfismo, segue imediatamente que Φ também é um homomorfismo. Além disso, Φ é claramente sobrejetora. □

Funções podem ser usadas para transferir a estrutura de um sistema agébrico para um conjunto sem estrutura. Por exemplo, seja A um anel e φ uma função que leva cada elemento de A a um único elemento de um conjunto S, então por meio de φ pode-se definir uma estrutura de anel em S que converte φ em um homomorfismo. Em detalhe, seja $s_1, s_2 \in S$ e seja $r_1, r_2 \in A$ unicamente determinados tais que $\varphi(r_1) = s_1$ e $\varphi(r_2) = s_2$, onde definimos $s_1 + s_2$ para ser $\varphi(r_1 + r_2)$ e $s_1 s_2$ para ser $\varphi(r_1 r_2)$ e todas as propriedades desejadas são satisfeitas. Essa estrutura de S pode ser chamada de estrutura de anel *induzida por* φ. No caso de A possuir propriedades adicionais, como por exemplo, ser um domínio de integridade ou um corpo, essas propriedades são herdadas por S.

Definição 1.1.16. *Para um primo* p*, seja* $\mathbb{F}_p$ *o conjunto de inteiros* $\{0, 1, \ldots, p-1\}$ *e seja* $\varphi : \mathbb{Z}/(p) \to \mathbb{F}_p$ *a aplicação definida por* $\varphi([a]) = a$ *para todo* $a = 0, 1, \ldots, p-1$*. Então* $\mathbb{F}_p$*, com a estrutura de corpo induzida por* φ*, é um corpo finito, chamado* ***Corpo de Galois de ordem*** p*.*

Exemplo 1.1.17.

- *Considere* $\mathbb{Z}/(5)$*, isomorfo a* $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ *com o homomorfismo dado por:* $[0] \to 0$, $[1] \to 1$,$[2] \to 2$,$[3] \to 3$, $[4] \to 4$. *A seguir temos as tábuas das operações de* $+$ *e* $\cdot$ *para os elementos de* $\mathbb{F}_5$*:*

$+$	*0*	*1*	*2*	*3*	*4*
0	*0*	*1*	*2*	*3*	*4*
1	*1*	*2*	*3*	*4*	*0*
2	*2*	*3*	*4*	*0*	*1*
3	*3*	*4*	*0*	*1*	*2*
4	*4*	*0*	*1*	*2*	*3*

$\cdot$	*0*	*1*	*2*	*3*	*4*
0	*0*	*0*	*0*	*0*	*0*
1	*0*	*1*	*2*	*3*	*4*
2	*0*	*2*	*4*	*1*	*3*
3	*0*	*3*	*1*	*4*	*2*
4	*0*	*4*	*3*	*2*	*1*

- *Um exemplo simples mas importante é o corpo finito* $\mathbb{F}_2 = \{0, 1\}$*. Suas tábuas de operações são:*

$+$	*0*	*1*
0	*0*	*1*
1	*1*	*0*

$\cdot$	*0*	*1*
0	*0*	*0*
1	*0*	*1*

Nesse contexto, os elementos 0 *e* 1 *são chamados de* ***elementos binários****.*

1.2 Corpos e Extensões

Nesta seção assumiremos algumas noções básicas sobre espaços vetoriais como conhecidas.

O "embrião" da ideia de corpo apareceu em 1820, nos trabalhos sobre equações algébricas do norueguês N. H. Abel (1802-1829). Abel entendia por corpo uma coleção de números fechados para a adição, multiplicação e divisão (salvo no caso de divisor igual a 0). Para mais detalhes, consultar Iezzi, Dolce e Machado (1993).

Definição 1.2.1. *Seja* F *um corpo e* K *um subconjunto de* F*. Se* K *também é um corpo sob as operações de* F*, dizemos que* K *é um subcorpo de* F *e que* F *é uma extensão de* K*.*

Exemplo 1.2.2. $\mathbb{Q}$ *é um subcorpo de* $\mathbb{R}$ *e* $\mathbb{R}$ *é um subcorpo de* $\mathbb{C}$*.*

Teorema 1.2.1. *Um subconjunto* K *de um corpo* F *é um subcorpo se, e somente as seguintes condições são satisfeitas:*

1. K *contém pelo menos um elemento não nulo.*
2. *Se* $a, b \in K$ *então* $a - b \in K$*.*
3. *Se* $a, b \in K$ *e* $b \neq 0$ *então* $ab^{-1} \in K$*.*

Exemplo 1.2.3. *O conjunto* $L = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ *é um subcorpo do corpo* $\mathbb{R}$*. Note que* $L \neq \varnothing$*, pois* $1 = 1 + 0 \cdot \sqrt{2} \in L$*. Além disso, se* $x = a + b\sqrt{2}, y = c + d\sqrt{2} \in L$*, com* $a, b, c, d \in \mathbb{Q}$*, temos* $x - y = (a - c) + (b - d)\sqrt{2}$*. Como* $(a - c), (b - d) \in \mathbb{Q}$*, então* $x - y \in L$*. Por útimo, se* $x = a + b\sqrt{2}, y = c + d\sqrt{2} \in L$*, com* $y \neq 0$ *(com* $a, b, c, d \in \mathbb{Q}$*,* $c \neq 0$ *ou* $d \neq 0$*, temos:*

$$\begin{aligned} xy^{-1} &= \frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{(ac - 2bd)(bc - ad)\sqrt{2}}{c^2 - 2d^2} = \\ &= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - 2ad}{c^2 - 2d^2}\sqrt{2}. \end{aligned}$$

Como $c^2 - 2d^2 \neq 0$*, pois, caso contrário,* $c/d = \sqrt{2}$*, o que é impossível, já que* $c, d \in \mathbb{Q}$*, então* $\dfrac{ac - 2bd}{c^2 - 2d^2}$ *e* $\dfrac{bc - 2ad}{c^2 - 2d^2}$ *são números racionais e, portanto,* $xy^{-1} \in L$*.*

O subcorpo K é próprio, se $K \neq F$. Um corpo que não contém nenhum subcorpo próprio é chamado um *subcorpo primo.*

Teorema 1.2.2. *O subcorpo primo de um corpo* F *é isomorfo a* $\mathbb{Z}/p\mathbb{Z}$ *ou a* $\mathbb{Q}$ *de acordo com a característica de* F *ser prima ou zero.*

Demonstração: Seja $\phi : \mathbb{Z} \to F$ o homomorfismo de anéis definido por $\phi(n) = n \cdot 1_F$. O núcleo de ϕ é $(car(F))\mathbb{Z}$. Se $car(F) = p$ para algum primo p, então pelo Teorema 1.1.7, $\phi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ que é um corpo primo. Se $car(F) = 0$, então ϕ é injetora. Neste

caso, $\phi(\mathbb{Z})$ é um anel isomorfo a $\mathbb{Z}$. Definimos agora $\phi' : \mathbb{Q} \to F$ por $\phi'(m/n) = (m \cdot 1_F)(n \cdot 1_F)^{-1}$, se $n \neq 0$. Temos que ϕ' é um homomorfismo injetor. Com efeito,

$$\begin{aligned}\phi'\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) &= ((m_1n_2 + m_2n_1) \cdot 1_F)((n_1 \cdot n_2) \cdot 1_F)^{-1} \\ &= (m_1 \cdot 1_F)(n_1 \cdot 1_F)^{-1} + (m_2 \cdot 1_F)(n_2 \cdot 1_F)^{-1} \\ &= \phi'\left(\frac{m_1}{n_1}\right) + \phi'\left(\frac{m_2}{n_2}\right)\end{aligned}$$

e

$$\begin{aligned}\phi'\left(\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}\right) &= ((m_1m_2) \cdot 1_F)((n_1 \cdot n_2) \cdot 1_F)^{-1} \\ &= (m_1 \cdot 1_F)(n_1 \cdot 1_F)^{-1} \cdot (m_2 \cdot 1_F)(n_2 \cdot 1_F)^{-1} \\ &= \phi'\left(\frac{m_1}{n_1}\right) \cdot \phi'\left(\frac{m_2}{n_2}\right).\end{aligned}$$

Além disso, se $\phi'(m/n) = 0$ então $m1_F = 0$ e, portanto, $m = 0$, já que $car(F) = 0$. Concluímos que $\phi'(\mathbb{Q})$, que é o menor subcorpo de F contendo 1_F, é isomorfo ao corpo primo $\mathbb{Q}$. □

A interseção de subcorpos de um corpo é um subcorpo. Logo, corpos primos também podem ser obtidos considerando a interseção da coleção de todos os subcorpos de um dado corpo. Na verdade, a ideia de tomar interseções pode ser generalizada para obter outros subcorpos.

Definição 1.2.4. *Sejam K um subcorpo do corpo F e M um subconjunto de F. O corpo $K(M)$ é definido como sendo a interseção de todos os subcorpos de F contendo ambos K e M e é chamado o* ***corpo de extensão de*** *K obtido pela* ***adjunção*** *dos elementos de M. Quando $M = \{\theta_1, \theta_2, \ldots, \theta_n\}$, escrevemos $K(M) = K(\theta_1, \theta_2, \ldots, \theta_n)$. Quando $M = \{\theta\}$, dizemos que $L = K(\theta)$ é uma* ***extensão simples*** *de K.*

Se L é um corpo de extensão de K, então L pode ser visto como um espaço vetorial sobre K. Primeiramente, isto deve-se ao fato de que os elementos de L formam um grupo abeliano sob a adição. Além disso, a multiplicação de um elemento $\alpha \in L$ por um escalar $r \in K$ dá $r\alpha \in L$ satisfazendo

$$r(\alpha + \beta) = r\alpha + r\beta$$

$$(r+s)\alpha = r\alpha + s\alpha$$

$$(rs)\alpha = r(s\alpha)$$

$$1_K \cdot \alpha = \alpha,$$

para quaisquer $r, s \in K$ e $\alpha, \beta \in L$. Quando L é um espaço vetorial de dimensão finita sobre K, a dimensão é o *grau* de L sobre K e é denotada por $[L : K]$. Neste caso, dizemos que L é uma extensão finita de K.

Teorema 1.2.3. *Se M é uma extensão finita de L e L é uma extensão finita de K, então M é uma extensão finita de K com $[M : K] = [M : L][L : K]$.*

Demonstração: Suponhamos que $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ e $\{\beta_1, \beta_2, \ldots, \beta_n\}$ sejam bases de M sobre L e de L sobre K, respectivamente. Então $[M : L] = m$ e $[L : K] = n$ e queremos provar que $[M : K] = mn$. Qualquer elemento $\alpha \in M$ pode ser escrito como

$$\alpha = \gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_m\alpha_m,$$

onde $\gamma_1, \gamma_2, \ldots, \gamma_m \in L$. Agora, para cada i tal que $1 \leq i \leq m$, temos

$$\gamma_i = r_{i1}\beta_1 + r_{i2}\beta_2 + \cdots + r_{in}\beta_n,$$

onde $r_{i1}, \ldots, r_{in} \in K$. Logo, combinamos as duas expressões acima dá que

$$\alpha = \sum_{i=1}^{m} \gamma_i\alpha_1 = \sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\beta_j\alpha_i,$$

onde cada $r_{ij} \in K$. A seguir mostraremos que o conjunto $\{\beta_j\alpha_i; 1 \leq j \leq n, 1 \leq i \leq m$ é linearmente independente e assim é uma base de M sobre K. Seja $\sum_{i=1}^{m}\sum_{j=1}^{n} s_{ij}\beta_j\alpha_i = 0$ onde cada $s_{ij} \in K$. Como $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ forma uma base de M sobre L, obtemos $\sum_{j=1}^{n} s_{ij}\beta_j = 0$ para qualquer i. Finalmente, como $\{\beta_1, \beta_2, \ldots, \beta_n\}$ é uma base de L sobre K concluímos que cada s_{ij} é zero. □

1.3 Alguns Resultados em Anéis de Polinômios

Nesta seção abordaremos os polinômios como elementos de um certo anel e estaremos preocupados com as propriedades algébricas desse anel.

Definição 1.3.1. *Seja* A *um anel. Dados os polinômios* $f = \sum_{i=0}^{n} a_i x^i$ *e* $g = \sum_{i=0}^{m} b_i x^i$*, tais que cada* $a_i, b_i \in A$ *e* $m \leq n$*, definimos a soma* $f + g$ *e o produto* fg *da seguinte maneira:*

$$f + g = \sum_{k=0}^{n} (a_k + b_k)x^k \text{ e } fg = \sum_{k=0}^{m+n} (a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0)x^k,$$

onde $a_i = b_i = 0$ *para quaisquer* i, j *com* $i > n, j > m$*. O conjunto de todos os polinômios sobre* A *com essas duas operações é um anel conhecido como o* ***anel dos polinômios sobre*** A *e é denotado por* $A[x]$*.*

Exemplo 1.3.2.

- *Seja* A *um anel. Se* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *é um polinômo sobre* A*, com* $a_n \neq 0$ *dizemos que cada* a_i *é um coeficiente de* f*,* a_n*, é o coeficiente do termo dominante de* f *e o grau de* f *é* n *(*$gr(f) = n$*). O polinômio nulo tem todos os coeficientes iguais a zero. Se* A *é um domínio de integridade, então, em* $A[x]$*, temos que* $gr(fg) = gr(f) + gr(g)$*. Em particular, se* f *e* g *são polinômios não nulos em* $A[x]$*, então* fg *também é não nulo. Isto mostra que, quando* A *é um domínio de integridade,* $A[x]$ *também é um domínio de integridade.*

- *Seja* F *um corpo. Qualquer polinômio linear* $ax + b$*, com* $a \neq 0$ *é irredutível em* $F[x]$*.*

- *Dizemos que* α *é uma* ***raiz*** *de f, se* $f(\alpha) = 0$*. Sejam* F *um corpo,* $f \in F[x]$ *e* $\alpha \in F$*. Neste caso, o polinômio* $x - \alpha$ *divide* f *em* $F[x]$*. Além disso, se* $gr(f) > 1$*, então* f *é redutível sobre* F*. Isto dá um critério de irretubilidade: se* $gr(f) = 2$ *ou* 3 *então* f *é irredutível sobre* F *se, e somente se* f *não tem raízes em* F*. A restrição no grau do polinômio se deve ao fato de que o polinômios redutíveis de grau maior que* 3 *não necessariamente possuem fatores lineares. Por exemplo, em* $\mathbb{R}[x]$*, o polinômio* $x^4 + 4x^2 + 3 = (x^2 + 1)(x^2 + 3)$ *é redutível, mas não tem raízes em* $\mathbb{R}$**.**

É bastante conhecido o algoritmo para efetuar divisões com resto de polinômios com coeficientes reais. Podemos efetuar, de maneira análoga, a divisão entre polinômios com coeficientes num corpo F arbitrário, o que será mostrado no resultado a seguir.

Teorema 1.3.1 (Algoritmo da Divisão)**.** *Sejam* F *um corpo e* $f, g \in F[x]$ *com* $g \neq 0$*. Existem únicos polinômios* $h, r \in F[x]$*, tais que* $f = gh + r$ *e* $gr(r) < gr(g)$*.*

Demonstração: Seja $S = \{f - gh; h \in F[x]\}$. Digamos que $r = f - gh \in F[x]$ é um polinômio em S de menor grau e que $gr(r) = m$, $gr(g) = n$. Mostraremos que $m < n$.

Suponhamos, por contradição, que $m \geq n$. Seja $a \in F$ tal que o produto de a e o coeficiente do termo dominante de g dá o coeficiente do termo dominate de r. Subtraindo $ax^{m-n}g$ de ambos os lados de $r = f - gh$ dá que

$$r - ax^{m-n}g = f - gh - ax^{m-n}g,$$

onde o polinômio do lado esquerdo tem grau menor que m. O lado direito é igual a $f - g(h + ax^{m-n}) \in S$. Isto contradiz o fato de que r é o polinômio de menor grau em S. Assim, existem polinômios $h, r \in F[x]$ tais que $f = gh + r$ e $m < n$.

Suponhamos que existam polinômios h_1, h_2, r_1, r_2 em $F[x]$ tais que $f = gh_1 + r_1$, $f = gh_2 + r_2$, $gr(r_1) < gr(g)$ e $gr(r_2) < gr(g)$. Assim $gh_1 + r_1 = gh_2 + r_2$ implica que $g(h_1 - h_2) = r_2 - r_1$. Como $gr(r_2 - r_1) < gr(g)$, temos que $h_1 - h_2 = 0$ e assim $r_2 - r_1 = 0$. Logo $h_1 = h_2$ e $r_1 = r_2$.

□

Seja A um anel. Para que o algoritmo da divisão seja válido em $A[x]$, é necessário que o coeficiente do termo dominante de g seja invertível em A.

Exemplo 1.3.3. *Sejam os polinômios* $f(x) = 2x^5 + x^4 + 4x + 3, g(x) = 3x^2 + 1 \in \mathbb{F}_5$. *Calculando os polinômios* $h, r \in \mathbb{F}_5$ *pelo algoritmo da divisão, temos*

$$
\begin{array}{l|l}
2x^5 + x^4 + 4x + 3 & 3x^2 + 1 \\
\cline{2-2}
-2x^5 - 4x^3 & 4x^3 + 2x^2 + 2x + 1 \\
\cline{1-1}
x^4 + x^3 + 4x + 3 & \\
-x^4 + 3x^2 & \\
\cline{1-1}
x^3 + 3x^2 + 4x + 3 & \\
-x^3 + 3x & \\
\cline{1-1}
3x^2 + 2x + 3 & \\
-3x^2 + 4 & \\
\cline{1-1}
2x + 2 &
\end{array}
$$

Assim, $h(x) = 4x^3 + 2x^2 + 2x + 1, r(x) = 2x + 2$ *e* $1 = gr(r) < gr(h) = 3$. *Logo,* $2x^5 + x^4 + 4x + 3 = (3x^2 + 1)(4x^3 + 2x^2 + 2x + 1) + (2x + 2)$

Definição 1.3.4. *Seja* F *um corpo. Dados* $f, g \in F[x]$, *existe um único polinômio mônico* $d \in F[x]$ *tal que*

1. d *divide* f *e* g,
2. *qualquer polinômio* $h \in F[x]$ *dividindo ambos* f *e* g *divide também* d.

Este polinômio d *é o* ***máximo divisor comum de*** f ***e*** g, *denotado por* $\mathrm{mdc}(f, g)$.

Observação 1. *O máximo divisor comum entre dois polinômios pode não ser único, sendo assim, utiliza-se o polinômio mônico na definição de* mdc *para garantir a unicidade. A existência do máximo divisor comum, é consequência simples do fato que todo ideal de* $F[x]$ *é principal, isto é, gerado por um único elemento, (ver teorema 1.3.3, para mais detalhes, consultar Masuda e Panario (2007)). Por exemplo, dados* $f(x) = x^3 + 3$ *e* $g(x) = 2x^2 + 2$, *onde* $f, g \in \mathbb{Z}_5$. *Temos que* $4x + 3$ *é um* $\mathrm{mdc}(f, g)$, *porém* $4x + 3 = (4^{-1})(4x + 3) = 4(4x + 3) = x + 2$ *é o único polinômio mônico que satisfaz a definição 1.3.4.*

Observamos que o $mdc(f, g)$ é o polinômio mônico de maior grau dentre os polinômios que dividem ambos f e g em $F[x]$.

Quando $mdc(f, g) = 1$, dizemos que f e g são polinômios *coprimos* ou *relativamente primos* .

Dados $f, g \in F[x]$, F corpo, com $g \neq 0$, podemos aplicar sucessivamente o algoritmo da divisão com resto, obtendo

$$\begin{aligned}
f(x) &= g(x)q_1(x) + r_1(x), gr(r_1) < gr(g) \qquad (1)\\
g(x) &= r_1(x)q_2(x) + r_2(x), gr(r_2) < gr(r_1)\\
r_1(x) &= r_2(x)q_3(x) + r_3(x), gr(r_3) < gr(r_2)\\
&\vdots\\
r_{s-3}(x) &= r_{s-2}(x)q_{s-1}(x) + r_{s-1}(x), gr(r_{s-1}) < gr(r_{s-2})\\
r_{s-2}(x) &= r_{s-1}(x)q_s(x) + r_s(x), gr(r_s) < gr(r_{s-1})\\
r_{s-1}(x) &= r_s(x)q_{s+1}(x) + 0,
\end{aligned}$$

onde $q_1, ..., q_{s+1}, r_1, ..., r_s$ são polinômios sobre F. Como o $gr(g)$ é finito, este processo termina com uma divisão exata. Quando isso acontece, temos que $mdc(f, g) = a^{-1}r_s$ onde a é o coeficiente do termo dominante do último resto não nulo r_s. Essa multiplicação de r_S por a^{-1} é realizada para que tenhamos um polinômio mônico. Tem-se assim o seguinte algoritmo de Euclides para polinômios:

Algoritmo de Euclides para Polinômios

1. Faça $n = 0$.
2. Faça $r_{-1}(x) = f(x)$ e $r_0(x) = g(x)$
3. Determine $r_{n+1}(x)$ e $q_{n+1}(x)$ tais que $r_{n-1}(x) = r_n(x)q_{n+1} + r_{n+1}$, onde $gr(r_{n+1}) < gr(r_n)$.
4. Se $r_{n+1} \neq 0$, então faça $n = n + 1$ e vá para 3.
5. Se $r_{n+1} = 0$, então r_n é o $mdc(f, g)$. Pare.

É possível escrever o $mdc(f, g)$ como uma combinação linear de f e g, no sentido de que $mdc(f, g) = af + bg$, para certos polinômios $a, b \in F[x]$. Para isso, escrevemos o

resto de cada divisão, em termos dos outros polinômios envolvidos em cada expressão de (1).

Exemplo 1.3.5. *Sejam* $f(x) = 2x^{10} + x^7 + x^2 + 1, g(x) = x^7 + 1 \in \mathbb{Z}/3\mathbb{Z}$. *Vamos escrever o* $\mathrm{mdc}(f, g)$ *como combinação linear de* f *e* g. *Pelo algoritmo euclideano, temos as seguintes expressões:*

$$\begin{aligned} 2x^{10} + x^7 + x^2 + 1 &= (2x^3 + 1)(x^7 + 1) + (x^3 + x^2) \\ x^7 + 1 &= (x^4 + 2x^3 + x^2 + 2x + 1)(x^3 + x^2) + (2x^2 + 1) \\ x^3 + x^2 &= (2x + 2)(2x^2 + 1) + (x + 1) \\ 2x^2 + 1 &= (2x + 1)(x + 1) + 0. \end{aligned}$$

Logo, $\mathrm{mdc}(f, g) = x + 1$. *Além disso, temos:*

$$\begin{aligned} x + 1 &= (x^3 + x^2) - (2x + 2)(2x^2 + 1) \\ &= (x^3 + x^2) - (2x + 2)((x^7 + 1) - ((x^4 + 2x^3 + x^2 + 2x + 1)) \\ &= (2x^5)(x^3 + x^2) + (x + 1)(x^7 + 1) \\ &= (2x^5)((2x^{10} + x^7 + x^2 + 1) - (2x^3 + 1)(x^7 + 1)) + (x + 1)(x^7 + 1) \\ &= (2x^5)(2x^{10} + x^7 + x^2 + 1) + (2x^8 + x^5 + x + 1)(x^7 + 1). \end{aligned}$$

Assim, obtemos $\mathrm{mdc}(f, g) = (2x^5)f + (2x^8 + x^5 + x + 1)g$.

Os elementos primos do anel $F[x]$ são chamados de *polinômios irredutíveis*. Para enfatizar a importância desses conceito, damos a seguinte definição.

Definição 1.3.6. *Um polinômio* $p \in F[x]$ *é dito um polinômo irredutível sobre* F *(ou irredutível sobre* $F[x]$*, ou primo em* $F[x]$*), se* p *possui grau positivo e* $p = bc$ *com* $b, c \in F[x]$ *implica que* b *ou* c *é um polinômio constante.*

Polinômios irredutíveis são de fundamental importância para a estrutura do anel $F[x]$. Consideramos umas das propriedade mais importantes de $F[x]$: a fatoração única de polinômios.

Teorema 1.3.2 (Fatoração Única de Polinômios)**.** *Seja* F *um corpo. Então todo polinômio* $f \in F[x] \setminus \{0\}$ *de grau positivo pode ser escrito na forma*

$$f = u \cdot p_1 \cdot p_2 \cdots p_m, \tag{2}$$

onde $u \in F \setminus \{0\}, p_1, p_2, \ldots, p_m$ *são polinômios irredutíveis sobre* F *(não necessariamente distintos). Mais ainda, essa expressão é única a menos da constante* u *e da ordem dos polinômios* $p_1, p_2, \ldots, p_m$.

Demonstração: Seja $f \in F[x] \setminus \{0\}$. Vamos provar por indução sobre o grau de f, $gr(f) = n$. Se $n = 0$, $f = u$ é um polinômio constante não nulo, portanto, podemos assumir $gr(f) = n \geq 1$. Vamos supor, por hipótese de indução, que todo polinômio não nulo de grau menor que n pode ser escrito na expressão desejada, e vamos demonstrar que f também pode ser escrito naquela expressão.

Suponhamos, por absurdo, que f não pode ser escrito como produto de irredutíveis. Então f é um polinômio redutível sobre F. Assim, existem $g, h \in F[x], 1 \leq gr(g) < n, 1 \leq gr(f) < n$ tais que $f = gh$.

Agora, por indução, temos

$$g = a \cdot p_1 \cdot p_2 \cdots p_r,$$

com $a \in F \setminus \{0\}$ e $p_1, \ldots, p_r$ polinômios irredutíveis sobre F.

Analogamente,

$$h = b \cdot p_{r+1} \cdot p_{r+2} \cdots p_m,$$

com $b \in F \setminus \{0\}$ e $p_{r+1}, \ldots, p_m$ são polinômios irredutíveis sobre F.

Assim $f = a \cdot u \cdot p_1 \cdots p_m$, onde $u = ab \in F \setminus \{0\}$ e $p_1, \ldots, p_m$ são polinômios irredutíveis sobre F.

Vamos agora demonstrar a unicidade da expressão.

Suponhamos

$$f = u \cdot p_1 \cdots p_m = u' \cdot p_1 \cdots p'_s$$

onde $u, u' \in F \setminus \{0\}$ e $p_1, \ldots, p_m, p'_1, \ldots, p'_s$ são polinômios irredutíveis sobre F.

Assim, temos,

$$p_1 | p'_1 \cdots p'_s$$

e daí segue que existe $u'_i \in F[x] \setminus \{0\}$ tal que $p'_i = u'_i p_1$ (p'_i e p_1 são associados em $F[x]$. Agora o teorema segue por indução sobre m. Se $m = 1$ e p_1 irredutível, temos necessariamente que $s = 1$ e p_1 e p'_i são associados em $F[x]$. Suponhamos $m > 1$. De

$p_i' = u_i' p_1$ e sendo $F[x]$ um domínio temos que:

$$u \cdot p_2 \cdots p_m = u' \cdot u_i p_1' \cdots p_{i-1} \cdot p_{i+1} \cdots p_s$$

e daí segue pela hipótese de indução qie $m - 1 = s - 1$ (isto é, $m = s$) e mais cada p_j' está associado com algum p_i através de uma constante, e isto termina a demonstração do teorema.

□

O próximo teorema mostra que qualquer ideal em $F[x]$ é principal. A fatoração única de polinômios e a existência do máximo divisor comum são consequências dele.

Teorema 1.3.3. *Seja* F *um corpo. Então* $F[x]$ *é um domínio de ideais principais. Mais precisamente, para qualquer ideal não nulo* I *de* $F[x]$*, existe um único polinômio mônico* $f \in F[x]$ *tal que* $I = (f)$*, onde* $(f) = \{f \cdot g; g \in F[x]\}$.

A seguir, discutiremos os quocientes $F[x]/(f)$ do anel dos polinômios $F[x]$ pelo ideal gerado pelo polinômio f. O teorema a seguir nos fornece um método prático para construir corpos finitos.

Teorema 1.3.4. *Seja* F *um corpo e* f *um polinômio mônico de grau positivo sobre* F*. Então* $F[x]/(f)$ *é um corpo se, e somente se,* f *é irredutível sobre* F*.*

Demonstração: Basta combinarmos o item 4 do Teorema 1.1.5 e o Teorema 1.3.3 para demonstrar o resultado.

□

Teorema 1.3.5. *Sejam* F *um corpo e* f *um polinômio mônico de grau positivo* n *sobre* F*. Então o anel quociente* $F[x]/(f)$ *pode ser descrito como*

$$\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}; a_0, a_1, \ldots, a_{n-1} \in F \text{ e } f(\alpha) = 0\}.$$

Demonstração: Seja $f \in F[x]$ com $gr(f) = n$, se f é irredutível sobre F, então $F[x]/(f)$ é um corpo. Um elemento típico de $F[x]/(f)$ é $[g] = g + f$, onde $g \in F[x]$. Se $gr(g) > n$, pelo algoritmo da divisão existem polinômios $q, r \in F[x]$ univocamente determinados pelas condições

$$g = fq + r, \text{ com } gr(r) = 0 \text{ ou } gr(r) < n.$$

Assim $[g] = g + f = fq + r + f = r + (q + 1)f$. Como $(q + 1)f \in (f)$, segue que $[(q + 1)f] = [0]$ em $F[x]/(f)$. Logo $[g] = r$, como $gr(r) = 0$ ou $gr(r) < n$, temos que r é um polinômio de grau menor que ou igual a $n - 1$. Portanto

$$r(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1},$$

com $a_0, a_1, \ldots, a_{n-1} \in F$.

Se $\alpha \in F$ é uma raiz de f, temos que $[g(\alpha)] = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$. Portanto, todo elemento de $F[x]/(f)$ é da forma $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ com $a_0, a_1, \ldots, a_{n-1} \in F$ e $f(\alpha) = 0$, o que demonstra o resultado.

□

Veremos um tipo especial de extensão de corpos.

Definição 1.3.7. *Seja K uma extensão do corpo F. Um elemento $\theta \in K$ é **algébrico sobre** F, se existe um polinômio $f \in F[x]$ tal que $f(\theta) = 0$. Caso contrário, dizemos que θ é **transcedente** sobre F. Se todos os elementos de K são algébricos sobre F, dizemos que a extensão de K de F é **algébrica**.*

Definição 1.3.8. *Seja $\theta \in K$ um elemento algébrico sobre F. O único polinômio mônico $M \in F[x]$ que gera o ideal*

$$I = \{f \in F[x]; f(\theta) = 0)\}$$

*é chamado de **polinômio minimal** de θ sobre F.*

Polinômios minimais desempenham um papel fundamental na teoria dos códigos, em especial, os códigos BCH, que serão apresentados no Capítulo 3. *Corpos de decomposição* são usados para descrever corpos finitos, como veremos no Capítulo 2.

Definição 1.3.9. *Sejam F e K corpos, onde K é uma extensão de F. O corpo K é um **corpo de decomposição** do polinômio $f \in F[x]$, se f é um produto de fatores lineares em $K[x]$ e se f não é um produto de fatores lineares sobre qualquer subcorpo próprio de K contendo F.*

Em outras palavras, o corpo de decomposição de um polinômio f sobre F é o menor corpo que contém F e as raízes de f. Na verdade, existe apenas um único corpo de decomposição de um polinômio, a menos de isomorfismos.

Teorema 1.3.6. *Sejam* F *um corpo e* f *um polinômio sobre* F. *Existe uma extensão* K *de* F *que é um corpo de decomposição de* f. *Além disso, quaisquer dois corpos de decomposição de* f *sobre* F *são isomorfos.*

Exemplo 1.3.10.

- *O corpo de decomposição de* $x^2 - 2$ *sobre* $\mathbb{Q}$ *é* $\mathbb{Q}(\sqrt{2})$.
- *O corpo de decomposição de* $x^4 - 5x^2 + 6$ *sobre* $\mathbb{Q}$ *é* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- *Considere o polinômio* $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. *As suas quatro raízes em* $\mathbb{C}$ *são:*

$$\theta_1 = \sqrt[4]{2},\ \theta_2 = \sqrt[4]{2}i,\ \theta_3 = -\sqrt[4]{2} \ \text{ e } \ \theta_4 = -\sqrt[4]{2}i,$$

  e $\mathbb{Q}(\sqrt[4]{2}, i)$ *é o seu corpo de decomposição.*

2 Corpos Finitos e suas Representações

Neste capítulo abordaremos vários fundamentos e propriedades de corpos finitos além de métodos para a construção de corpos finitos. Entender a estrutura, propriedadades e construções de corpos finitos será de fundamental importância para desenvolvermos a Teoria dos Códigos Corretores de Erros, apresentada no Capítulo 3, e também para compreendermos a teoria dos Corpos de Funções Algébricas sobre Corpos Finitos no Capítulo 4. Aqui, utilizamos como referência Masuda e Panario (2007) e Lidl e Niederreiter (1994).

2.1 Extensão de Corpos Finitos

Seja F um corpo com q elementos, onde $q < \infty$. Neste caso, dizemos que F é um *corpo finito* e q é a *ordem* de F.

Proposição 2.1.1. *A característica de qualquer corpo finito é prima.*

Demonstração: Seja F um corpo finito com identidade 1_F. Existem inteiros positivos m e n com $1 \leq m < n$ e $n \cdot 1_F = m \cdot 1_F$, já que F é finito. Portanto,$(n - m) \cdot 1_F = 0$ e logo F tem característica positiva. Pelo Teorema 1.1.2, a característica de F é prima.

□

Teorema 2.1.1. *Sejam K um corpo finito de ordem q e F uma extensão finita de K de grau n. Então, a ordem de F é q^n. Em particular, se F é um corpo finito de ordem q e característica p, então $q = p^n$ onde n é o grau de extensão de F sobre $\mathbb{F}_p$.*

Demonstração: Seja $\{\beta_1, \beta_2, \ldots, \beta_n\}$ uma base para o espaço vetorial F sobre K. Qualquer elemento de F tem uma expressão única da forma

$$a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n$$

com $a_1, a_2, \cdots, a_n \in K$. Ha q valores possíveis para cada a_i, logo o número total de elementos em F é q^n. Pelo Teorema 1.2.2, o corpo F contém o corpo primo $\mathbb{F}_p$ e assim concluímos a prova.

□

Lema 2.1.2. *Num corpo finito F de ordem q, qualquer $a \in F$ satisfaz $a^q = a$.*

Lema 2.1.3. *Seja* F *um corpo finito de ordem* q*. Se* r *e* s *são inteiros tais que* $r \equiv s \mod (q-1)$*, então* $a^r = a^s$ *para todo* $a \in F$*.*

Lema 2.1.4. *Seja* F *um corpo de ordem* q *e característica* p*. Então o polinômio* $x^q - x$ *fatora-se em* $F[x]$ *como*

$$x^q - x = \prod_{a \in F} (x - a).$$

Além disso, F *é o corpo de decomposição de* $x^q - x$ *sobre* $\mathbb{F}_p$*.*

Lema 2.1.5. *Seja* F *um corpo de característica* p*. Então, para qualquer inteiro* $n \geq 0$*, temos que*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Proposição 2.1.6. *Seja* F *um corpo de característica* p*. A função* $\theta : F \to F$ *dada por* $\theta(a) = a^p$ *é um isomorfismo de anéis tal que* $\theta(a) = a$ *para todo* $a \in \mathbb{F}_p$*.*

Agora vamos demonstrar a existência e unicidade de corpos finitos.

Teorema 2.1.2 (Existência e unicidade de corpos finitos)**.** *Para qualquer primo* p *e qualquer inteiro positivo* n*, existe um corpo finito com* p^n *elementos. Além disso, qualquer corpo com* p^n *elementos é isomorfo ao corpo de decomposição de* $x^{p^n} - x$ *sobre* $\mathbb{F}_p$*.*

Demonstração: Suponhamos $q = p^n$. Seja F o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Todas as raízes de $x^q - x$ em F são distintas. De fatos, se um polinômio f tem fatores repetidos, então $mdc(f, f') \neq 1$. No nosso caso,

$$mdc(x^q - x, (x^q - x)') = mdc(x^q - x, qx^{q-1} - 1) = mdc(x^q - x, -1) = 1.$$

Assim $S = \{a \in F; a^q = a\}$ tem q elementos. A seguir, mostraremos que S é um corpo. Vamos verificar as condições do Teorema 1.2.1. Claramente, S é um subconjunto de F que contém 0 e 1. Além disso, usando a Proposição 2.1.5, se $a, b \in S$ então

$$(a-b)^q = a^q + (-b)^q = a^q - b^q = a - b$$

implica que $a - b \in S$. Para $b \neq 0$, temos

$$(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1},$$

isto é, $ab^{-1} \in S$. Logo S é um corpo e contém todas as raízes de $x^q - x$, ou seja $x^q - x$ fatora-se completamente em S. Portanto, $S = F$ é um corpo finito e F é um corpo com q elementos.

Para mostrar a unicidade, seja F um corpo finito com $q = p^n$ elementos. Então F tem característica p e contém $\mathbb{F}_p$ como um subcorpo primo. O Lema 2.1.4 implica que F seja um corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. O Teorema 1.3.6 completa a prova. □

Teorema 2.1.3. *Seja $q = p^n$. Se f é um polinômio irredutível sobre $\mathbb{F}_p$ de grau n então $\mathbb{F}_q \cong \mathbb{F}_p/(f)$.*

Demonstração: Consequência do Teorema 1.3.4. □

Este isomorfismo fornece uma maneira de representar os elementos de um corpo finito como veremos na subseção 2.2.1. O seguinte resultado também sera usado mais tarde.

Teorema 2.1.4. *Seja $f \in \mathbb{F}_q[x]$ irredutível sobre $\mathbb{F}_q$. Então existe uma extensão simples de $\mathbb{F}_q$ sendo definida por uma raiz de f. Além disso, se θ é uma raiz de f, então $\mathbb{F}_q(\theta) \cong \mathbb{F}_q[x]/(f)$.*

Lema 2.1.7. *Seja A uma anel e $a \in A$. Suponhamos que m e n sejam inteiros positivos tais que $m|n$. Então $(a^m - 1)|(a^n - 1)$.*

Teorema 2.1.5. *Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos. Então todo subcorpo de $\mathbb{F}_q$ tem ordem p^m, onde m é um divisor positivo de n. Reciprocamente, se m é um divisor positivo de n, então existe um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Demonstração: Se $q = p^n$, então qualquer subcorpo F de $\mathbb{F}_q$ tem ordem p^m com $0 < m \leq n$. Se $[\mathbb{F}_q : F] = \ell$, então $p^n = (p^m)^\ell = p^{m\ell}$, pelo Teorema 2.1.1, e assim, $m|n$.

Reciprocamente, se m é um divisor positivo de n, pelo Lema 2.1.7, obtemos que $(p^m - 1)|(p^n - 1)$ e assim

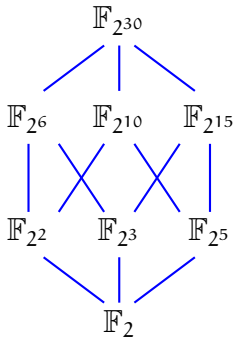
$$(x^{p^m-1} - 1)|(x^{p^n-1} - 1),$$

por uma outra aplicação do Lema 2.1.7, desta vez no anel $\mathbb{F}_p[x]$. Deduzimos que toda raiz de $x^{p^m} - x$ é uma raiz de $x^{p^n} - x = x^q - x$ e portanto toda raiz de $x^{p^m} - x$ pertence a $\mathbb{F}_q$. Segue que $\mathbb{F}_q$ deve conter um corpo de decomposição de $x^{p^m} - x$ sobre $\mathbb{F}_q$. O Teorema 2.1.2 implica que tal corpo de decomposição contenha p^m elementos.

Portanto, existe exatamente um subcorpo com p^m elementos, caracterizado pelas raízes do polinômio $x^{p^m} - x$ em $\mathbb{F}_q$. □

Exemplo 2.1.8. *Os subcorpos do corpo finito* $\mathbb{F}_{2^{30}}$ *são determinados por todos os divisores positivos de* 30. *Como os divisores positivos de* 30 *são* $1, 2, 3, 5, 6, 10, 15$ *e* 30 *os subcorpos de* $\mathbb{F}_{2^{30}}$ *são* $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^5}$, $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^{10}}$ $\mathbb{F}_{2^{15}}$ *e* $\mathbb{F}_{2^{30}}$. *O diagrama abaixo lista essas subcorpos.*

Figura 1: Subcorpos de $\mathbb{F}_{2^{30}}$



Fonte: Lidl e Niederreiter (1994),p. 47.

2.2 Aritmética em Corpos Finitos

Corpos finitos oferecem a flexibilidade de que seus elementos podem ser representados de maneiras diferentes. Dependendo da operação aritmética (adição, multiplicação, exponenciação e cálculo de inversos), uma representação pode ser mais conveniente que outra. Veremos duas formas de representar um corpo finito: através de um polinômio e através de um elemento primitivo. Independente da representação em questão, a aritmética em $\mathbb{F}_q$ dependerá da aritmética em $\mathbb{F}_p$, onde p é a característica de $\mathbb{F}_q$.

2.2.1 Representação Polinomial

Pelo Teorema 2.1.3, temos que $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(f)$, onde f é um polinômio irredutível de grau n sobre $\mathbb{F}_q$. Assim, pelo Teorema 1.3.5, temos que qualquer elemento em $\mathbb{F}_{q^n}$ pode ser representado por um polinômio em $\mathbb{F}_q[x]$ de grau menor que n e que o próprio f é o zero do corpo.

Ao operamos com dois polinômios, se o grau do polinômio resultante ultrapassar n, devemos fazer uma redução para que tenhamos uma representação em termos de um polinômio de grau menor que n. Para isso, seja r o resto da divisão de g por f. Então

r tem grau menor que n e os polinômios r e g representam o mesmo elemento em $\mathbb{F}_{q^n}$. Neste caso, escrevemos $g \equiv r \mod f$.

Exemplo 2.2.1. *Seja* $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. *Temos que* f *tem grau* 2 *e não possui raízes em* $\mathbb{F}_2$. *Logo, pelo Exemplo 1.3.2 (3), o polinômio* f *é irredutível sobre* $\mathbb{F}_2$. *Temos que* $\mathbb{F}_2[x]/(f)$ *possui* $p^n = 2^2 = 4$ *elementos:* $[0], [1], [x], [x+1]$ *e assim, pelo Teorema 2.1.3,* $\mathbb{F}_4$ *é isomorfo a* $\mathbb{F}_2[x]/(f)$. *Portanto, os elementos de* $\mathbb{F}_4$, *representado em termos de polinômios, são*

$$\mathbb{F}_4 = \{[0], [1], [x], [x+1]\}.$$

Abaixo, apresentamos a tabela de operações

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x]$	$[x+1]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

A título de justificativa de parte da tabela acima, note que:

$$[0] = [1 + x + x^2] = [1] + [x + x^2] = [1] + [x(1 + x)] = [1] + [x] \cdot [1 + x],$$

donde

$$[x] \cdot [1 + x] = -[1] = [1].$$

De modo semelhante, mostra-se que $[x]^2 = [1 + x]$ *e* $[1 + x]^2 = [x]$.

Essa representação será utilizada no Capítulo 3, no desenvolvimentos dos Códigos Cíclicos.

2.2.2 Elementos Primitivos

Uma propriedade importante de corpos finitos é que qualquer elemento não nulo é uma potência de um certo elemento fixo.

Teorema 2.2.1. *O grupo multiplicativo de qualquer corpo finito é cíclico.*

Demonstração: Podemos supor $q \geq 3$. Seja $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ a decomposição em fatores primos de ordem $h = q - 1$ do grupo $\mathbb{F}_q^*$. Para todo i, $1 \leq i \leq m$, o polinômio $x^{\frac{h}{p_i}} - 1$ possui no máximo $\frac{h}{p_i}$ raízes em $\mathbb{F}_q$. Desde que $\frac{h}{p_i} < h$, segue que existem elementos diferentes de zero em $\mathbb{F}_q$ que não são raízes deste polinômio. Seja a_i esse elemento e defina $b_i = a_i^{\frac{h}{p_i^{r_i}}}$. Temos que $b_i^{p_i^{r_i}} = 1$, desde que a ordem de b_i seja um divisor de $p_i^{r_i}$ e é, portanto, da forma $p_i^{s_i}$ com $0 \leq s_i \leq r_i$. Por outro lado,

$$b_i^{p_i^{r_i-1}} = a_i^{\frac{h}{p_1}} \neq 1,$$

e então a ordem de b_i é $p_i^{r_i}$. Afirmamos que o elemento $b = b_1 b_2 \cdots b_m$ tem ordem h. Suponha, por absurdo, que a ordem de b é um divisor próprio de h e é, portanto, um divisor de pelo menos um dos inteiros $\frac{h}{p_i}$, $1 \leq i \leq m$, digamos de $\frac{h}{p_1}$. Então, temos

$$1 = b^{\frac{h}{p_1}} = b_1^{\frac{h}{p_1}} b_2^{\frac{h}{p_1}} \cdots b_m^{\frac{h}{p_1}}.$$

Agora, se $2 \leq i \leq m$, então $p_i^{r_i}$ divide $\frac{h}{p_1}$ e, portanto, $b_i^{\frac{h}{p_1}} = 1$. Portanto, $b_1^{\frac{h}{p_1}} = 1$. Isso implica que a ordem de b_1 deve dividir $\frac{h}{p_1}$, o que impossível, pois a ordem de b_1 é $p_1^{r_1}$. Portanto, $\mathbb{F}_q^*$ é um grupo cíclico com gerador b. □

Definição 2.2.2. *Um gerador de $\mathbb{F}_q^*$ é chamado um* ***elemento primitivo****.*

O Teorema 2.2.1 fornece uma maneira bastante conveniente de representar os elementos não nulos de um corpo finito. Suponhamos que α seja um elemento primitivo de $\mathbb{F}_q$. Então $\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$, porém o teorema não fornece uma maneira eficaz de se encontrar o elemento primitivo. O método mais ingênuo é por tentativa e eliminação de erros, que consiste na busca de um elemento $\alpha \in \mathbb{F}_q$ cuja ordem é $q-1$, isto é, $q-1 = \min_{i \in \mathbb{N}}\{i; \alpha^i = 1\}$. Uma vez que encontramos tal α, então teremos encontrado todos os elementos primitivos , a saber, qualquer α^i, onde i e $q-1$ são relativamente primos. Assim, há $\phi(q-1)$ elementos primitivos onde $\phi : \mathbb{N} \to \mathbb{N}$, onde $\phi(n)$ é definido como sendo o número de inteiros m, $1 \leq m \leq n$ com a propriedade de que $mdc(m, n) = 1$. Tal ϕ é conhecida como a *função de Euler*.

Exemplo 2.2.3. *Em* $\mathbb{F}_{13}$*, temos*

$$3^1 = 3, 3^2 = 9, 3^3 = 1,$$

logo 3 não é um elemento primitivo de $\mathbb{F}_{13}$*. Por outro lado, temos*

$$2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 3, 2^5 = 6, 2^6 = 12,$$

$$2^7 = 11, 2^8 = 9, 2^9 = 5, 2^{10} = 10, 2^{11} = 7, 2^{12} = 1,$$

ou seja, 2 é um elemento primitivo de $\mathbb{F}_{13}$*. Como* $\phi(12) = 4$ *há três outros elementos primitivos de* $\mathbb{F}_{13}$*, a saber* $2^5 = 6, 2^2 = 11, 2^{11} = 7$*.*

Ao representarmos um elemento num corpo finito como uma potência de um elemento primitivo, as operações de multiplicação, exponenciação e cálculo de inversos são facilmente realizadas. Primeiramente, lembramos que pelo Lema 2.1.3, se $a > q - 1$ então podemos tomar r tal que $r \equiv a \mod (q-1)$ e $0 \leq r < q - 1$ para obtermos $\gamma^a = \gamma^r$, para todo $\gamma \in \mathbb{F}_q$. Suponhamos que γ seja um elemento primitivo de $\mathbb{F}_q$. Para a multiplicação, temos $\gamma^a\gamma^b = \gamma^{a+b}$. Para a exponenciação, temos $(\gamma^a)^k = \gamma^{ak}$ para todo $k \in \mathbb{Z}$. Em particular, para o cálculo de inversos, temos $(\gamma^a)^{-1} = \gamma^{-a}$. Sempre que o expoente for maior que $q - 1$ podemos obter a redução módulo $q - 1$ discutida acima.

Exemplo 2.2.4. *O elemento* γ *correspondente ao polinômio* $1 + x$ *é um elemento primitivo em* $\mathbb{F}_{16} \cong \mathbb{F}_2[x]/(x^4 + x + 1)$*. De fato,na próxima página apresentamos a tabela das potências de* γ *juntamente com suas representações polinomiais.*

Para ilustramos as operações aritméticas usando o elemento primitivo γ*, calculamos:*

1. $\gamma^7\gamma^{14} = \gamma^{21} = \gamma^6$*;*
2. $(\gamma^{13})^{-1} = \gamma^{-13} = \gamma^2$*;*
3. $\gamma^i = \gamma^3$ *para todo* i *tal que* $i \equiv 3 \mod 15$*.*

potência de γ	*polinômio*
1	1
γ	$x+1$
γ^2	x^2+1
γ^3	x^3+x^2+x+1
γ^4	x
γ^5	x^2+x
γ^6	x^3+x
γ^7	x^3+x^2+1
γ^8	x^2
γ^9	x^3+x^2
γ^{10}	x^2+x+1
γ^{11}	x^3+1
γ^{12}	x^3
γ^{13}	x^3+x+1
γ^{14}	x^3+x^2+x

2.3 Polinômios Irredutíveis

A aritmética usando a representação polinomial depende da redução módulo um polinômio irredutível. Para essa tarefa, polinômios irredutíveis com muitos coeficientes iguais a zero são desejados. Um tipo importante de polinômio irredutível é o polinômio primitivo. Esse tipo de polinômio tem a propriedade de que todas suas raízes são elementos primitivos. Tais elementos por sua vez, conforme vimos, determinam uma outra maneira de representar elementos num corpo finito.

Começaremos com um resultado fundamental sobre polinômios irredutíveis.

Teorema 2.3.1. *O produto de todos os polinômios mônicos irredutíveis sobre* $\mathbb{F}_q$ *cujos graus dividem* n *é igual a* $x^{q^n}-x$.

Teorema 2.3.2. *O número de polinômios mônicos e irredutíveis de grau* n *sobre* $\mathbb{F}_q$ *é*

$$I_n = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d},$$

onde μ *é a função de Mobius.*[4]

Falaremos agora sobre polinômios primitivos, pois estes formam uma classe particular de polinômios irredutíveis.

Definição 2.3.1. *Um polinômio* $f \in \mathbb{F}_q[x]$ *de grau* m *é primitivo, se* f *é o polinômio minimal sobre* $\mathbb{F}_q$ *de algum elemento primitivo de* $\mathbb{F}_{q^m}$.

Em outras palavras, um polinômio primitivo de grau m é um polinômio mônico e irredutível com a propriedade adicional de que se $\alpha \in \mathbb{F}_{q^m}$ é uma raiz de f então a ordem de α é $q^m - 1$.

Seja $\alpha \in \mathbb{F}_q$. Pelo Lema 2.1.2, temos que $\alpha^q = \alpha$, ou seja, α satisfaz a equação $x^q - x = 0$. Assim, α é algébrico sobre $\mathbb{F}_p$ e portanto tem um polinômio minimal $M \in \mathbb{F}_p[x]$. Esses polinômios tem uma profunda relação com códigos cíclicos, conforme veremos no Capítulo 3.

Proposição 2.3.2. *Seja* $\alpha \in \mathbb{F}_{p^m}$ *com polinômio minimal* M *sobre* $\mathbb{F}_p$. *Então, temos que*

1. M *é irredutível;*
2. *Se* $f \in \mathbb{F}_p[x]$ *com* $f(\alpha) = 0$, *então* $M|f$;
3. $M|(x^{p^m} - x)$;
4. $gr(M) \leq m$;
5. *Se* α *é um elemento primitivo de* $\mathbb{F}_{p^m}$, *então* $gr(M) = m$ *e* M *é um polinômio primitivo.*

[4] A função μ de Mobius é a função $\mu : \mathbb{N} \longrightarrow \mathbb{N}$ definida por

$$\mu(n) = \begin{cases} 1, & \text{se } n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \\ (-1)^r, & \text{se } a_1 = a_2 = \cdots = a_r = 1 \\ 0, & \text{caso contrário} \end{cases}$$

onde a_i, com $1 \leq i \leq r$ é um inteiro não negativo.

A seguir, provamos um lema básico na teoria de Galois que será necessário para mostrar um resultado sobre polinômios minimais.

Lema 2.3.3. *Sejam* K *uma extensão de um corpo* F, $\theta : K \to K$ *um isomorfismo de anéis fixando* F *e* $f \in F[x]$. *Suponhamos que* $\alpha \in K$ *seja uma raiz de* f. *Então* $\theta(\alpha)$ *também é uma raíz de* f.

Demonstração: Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ com $a_i \in F$ para $i = 1, \ldots, n$. Como $f(\alpha) = 0$ e $\theta(0) = 0$, temos que

$$\begin{aligned} 0 &= \theta(f(\alpha)) \\ &= \theta(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0) \\ &= \theta(a_n)\theta(\alpha)^n + \theta(a_{n-1})\theta(\alpha)^{n-1} + \ldots + \theta(a_0) \\ &= f(\theta(\alpha)), \end{aligned}$$

de onde obtemos que $\theta(\alpha)$ é uma raiz de f.

□

Caracterizamos agora os elementos de $\mathbb{F}_q$ com o mesmo polinômio minimal.

Proposição 2.3.4. *Sejam* $\alpha \in \mathbb{F}_q$ *e* $p = car(\mathbb{F}_p)$. *Então,* α *e* α^p *têm o mesmo polinômio minimal sobre* $\mathbb{F}_p$.

Exemplo 2.3.5. *Considere* $\alpha \in \mathbb{F}_{2^4}$. *Assim,*

$$\alpha, \alpha^2, (\alpha^2)^2 = \alpha^4, (\alpha^4)^2 = \alpha^8, (\alpha^8)^2 = \alpha^{16} = \alpha.$$

Todos esses elementos têm o mesmo polinômio minimal. O mesmo acontece com os elementos

$$\alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^6)^2 = \alpha^{12}, (\alpha^{12})^2 = \alpha^{24} = \alpha^9, (\alpha^9)^2 = \alpha^{18} = \alpha^3.$$

Estudaremos agora as raízes da unidade. Uma raíz n-ésima da unidade num corpo F é uma raíz em F do polinômio $x^n - 1$. Nem sempre é possível fatorar o polinômio $x^n - 1$ como produto de fatores lineares em $F[x]$. O próximo resultado nos dirá quando isso é possível.

Teorema 2.3.3. *Seja* F *um corpo finito e,* n*, um inteiro positivo que divide* $|F| - 1$*. Então, existe um elemento* $\gamma \in F$ *tal que*

$$x^n - 1 = (x - \gamma^0)(x - \gamma^1)(x - \gamma^2) \cdots (x - \gamma^{n-1}), \tag{3}$$

com $1, \gamma, \gamma^2, \cdots, \gamma^{n-1}$ *dois a dois distintos.*

Demonstraçã: Seja α um elemento primitivo de F. Logo $a^{|F|-1} = 1$ e

$$a^m \neq 1, \text{ se } 0 < m < |F| - 1.$$

Se $n = 1$, nada temos a provar. Suponhamos $n \geq 2$. Definamos $\gamma = \alpha^{\frac{|F|-1}{n}} \in F$. Temos então que $1, \gamma, \gamma^2, \cdots, \gamma^{n-1}$ são raízes de $x^n - 1$, e são duas a duas distintas; pois, caso contrário, se $\gamma^i = \gamma^j$ para algum par (i, j) tais que $0 \leq i < j \leq n - 1$, então

$$a^{(j-i)\frac{|F|-1}{n}} = \gamma^{j-1} = 1,$$

o que contradiz 3 pelo fato de $(j - i)\frac{|F|-1}{n}$ ser um inteiro positivo menor do que $|F| - 1$. Isso estabelece o teorema. □

Corolário 2.3.3.1. *Seja* K *um corpo finito com* q *elementos e,* n*, um inteiro primo com* q*. Então, existem uma estensão* F *de* K *e um elemento* $\gamma \in F$ *tais que*

$$x^n - 1 = (x - \gamma^0)(x - \gamma^1)(x - \gamma^2) \cdots (x - \gamma^{n-1}), \tag{4}$$

com $1, \gamma, \gamma^2, \cdots, \gamma^{n-1}$ *dois a dois distintos.*

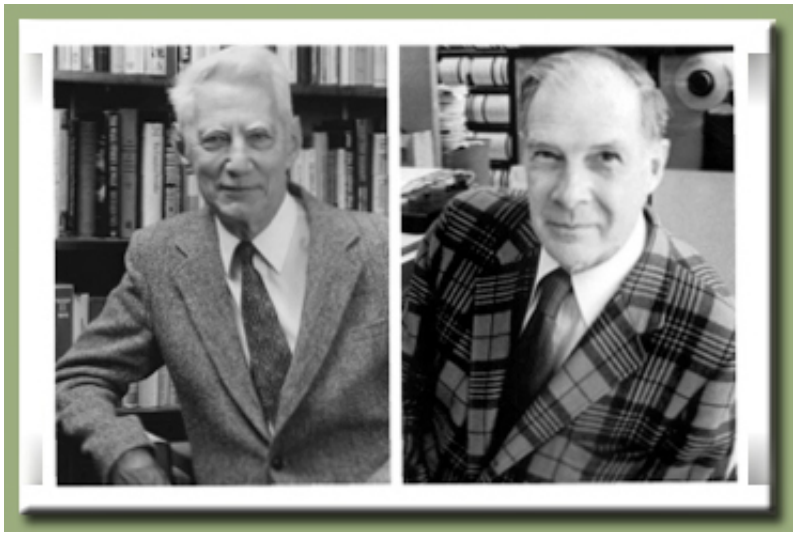
3 Códigos Corretores de Erros

Nesta seção apresentamos as ideias básicas para a construção de um código, bem como os principais códigos utilizados: códigos lineares, códigos cíclicos, códigos BCH e códigos de Goppa clássicos.As referêcias utilizadas nessa seção foram Hefez e Villela (2008), Masuda e Panario (2007), Milies (2009) e Voloch (2020).

3.1 Um Pouco de História

A Teoria dos Códigos teve início da década de 1940, no Laboratório Bell de Tecnologia. Lá, Richard W. Hamming e Claude E. Shannon trabalhavam com computadores, que nessa época, apenas instituições de grande porte tinham condições de mantê-los. Na época, os programas eram gravados em cartões perfurados cuja leitura pelo computador permitia detectar erros de digitação. Caso um erro fosse detectado, a leitura era interrompida e o computador passava automaticamente a ler o programa do próximo usuário. Hamming, que havia passado por essa situação, começou a se questionar se além de detectar os erros, os computadores também seriam capazes de corrigi-los. Esta questão foi crucial para o desenvolvimento dos códigos corretores de erros.

Figura 2: Claude E. Shannon e Richard W. Hamming



Fonte: http://www1.spms.ntu.edu.sg/ ccrg/About_us.html.

Hamming desenvolveu então um código capaz de detectar até dois erros e corrigir um erro se ele for único. Seu trabalho foi publicado em abril de 1950 no *"The Bell*

System Technical Journal" (A publicação tardia deste artigo ocorreu devido ao pedido de patente destes códigos, feita pelo *Laboratório Bell*). Durante três anos transcorridos da elaboração desses códigos, Hamming publicou diversos memorandos conforme sua pesquisa evoluia. Nesses artigos, se questionava sobre a possibilidade de criar códigos mais eficientes que os propostos inicialmente. A questão foi respondida em outubro de 1948 por Shannon num artigo intitulado *"A Mathematical Theory of Communication"*, também publicado no *"The Bell System Technical Journal"*.

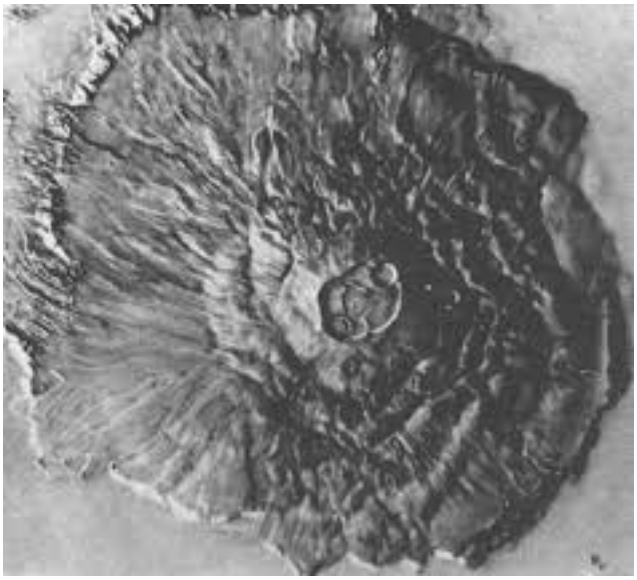
Mais adiante, Marce J. Golay, que trabalhava no *Signal Corps Enginneering Laboratories ar Fort Monmouth*, em Nova Jersey, leu a descrição do chamado $(7,4)$-código de Hamming dada no artigo de Shannom em 1948, e estendeu o resultado para um código corretor de erro úncio de comprimento primo $\mathtt{p}$. Seu trabalho foi publicado em julho de 1949 no *"Proceedings of the I.R.E"*, o artigo foi intitulado *"Notes on Digital Coding"*.

O artigo de Shannon deu início a dois novos campos de pesquisa em matemática: a Teoria dos Códigos (em conjunto com o trabalho de Hamming) e a Teoria da Informação. Desde então, pode-se dizer, que houve um desenvolvimento contínuo e significativo na Teoria dos Códigos até hoje.

O código de Golay foi o responsável pelo código usado pela espaçonave Voyager para transmitir fotos coloridas de Júpiter e Saturno, no final da década de 1970. Códigos de Reed-Solomom são utilizados no armazenamento em CDs de sons digitalizados. Os Códigos de Reed-Muller foram utilizados pela nave espacial Mariner 9, que entrou na órbita de Marte em 13 de novembro de 1971, 167 dias após o lançamento, e foi responsável pela transmissão para a Terra 7.329 fotografias, em preto e branco, que cobriram mais de 80% da superfície do planeta Marte.

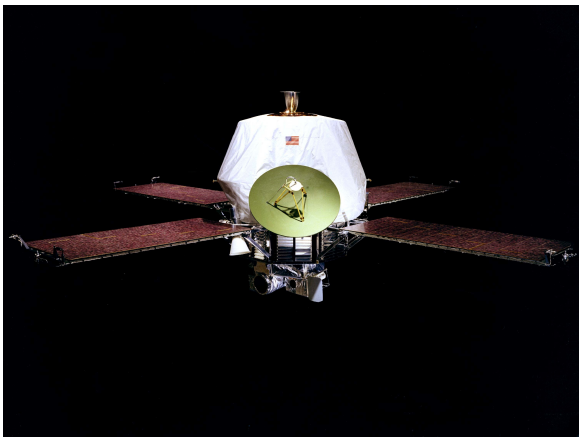
Golay, Hamming e Shannon foram os grandes pioneiros que iniciaram o trabalho com este assunto e desenvolveram ideias que são usadas até hoje no nosso dia a dia, como por exemplo, a comunicação de telefonia móvel, aparelhos de armazenamento de dados, comunicações via satélite, processamento de imagens digitais, internet, rádio, entre outras. Atualmente esses códigos são amplamente utilizados em programas espaciais da *National Aeronautics and Space Administration* (NASA) e do *Jet Propulsion Laboratory* (JPL).

Figura 3: Monte Olimpo, maior vulcão conhecido do Sistema Solar localizado em Marte



Fonte: NASA

Figura 4: Nave espacial Mariner 9.



Fonte: NASA.

3.2 Conceitos Básicos sobre Códigos Corretores de Erros

Na transmissão de dados, na vida real, às vezes ocorrem problemas como interferências eletromagnéticas ou erros humanos (por exemplo, erros de digitação) que chamamos de *ruído* e que podem fazer com que a mensagem recebida seja diferente daquela enviada. O objetivo da Teoria dos Códigos é desenvolver métodos que permitam detectar e corrigir esses erros. Um exemplo de código é o idioma, e a construção de códigos é

inspirada neles. Na língua portuguesa, por exemplo, usamos um alfabeto de 26 letras e as palavras nada mais são do que sequências de letras. É claro que existem sequências de letras (palavras) que não fazem parte do nosso idioma. Para um código estar bem estruturado, devemos definir quais são os elementos necessários para construi-ló. Os elementos básicos para se construir um código são os seguintes:

- Um conjunto finito, A que chamaremos *alfabeto*. Denotaremos por $q = |A|$ o número de elementos de A. Neste caso, dizemos que o código composto pelos elementos de A é um código q-*ário*.

- *Palavra* é uma sequência finita de símbolos do alfabeto. O número de letras de uma palavra chama-se *comprimento*. Para termos um código com o qual seja fácil trabalhar com certo rigor, faremos a convenção de que todas as palavras que iremos considerar tem o mesmo comprimento n. Por essa razão, esses códigos dizem-se em *blocos*.

- Um *código* q-*ário de comprimento* n será um subconjunto qualquer (a nossa escolha) de palavras de comprimento n, isto é, um código C é um subconjunto

$$C \subset A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ cópias}}.$$

Exemplo 3.2.1. *Quando o alfabeto utilizado é o conjunto* $\mathbb{F}_2 = \{0, 1\}$*, o código diz-se binário. O conjunto*

$$C_1 = \{0000, 0001, 0011, 0111, 1111\}$$

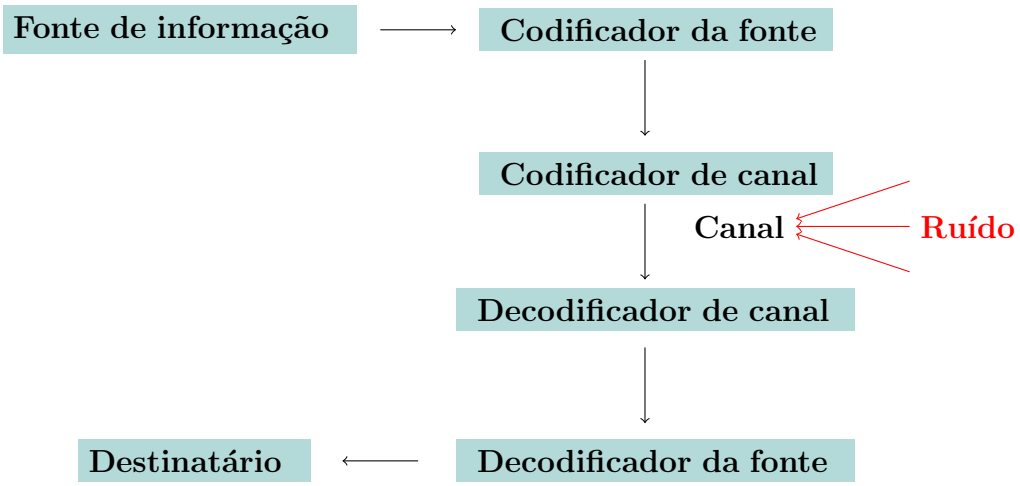
é um código binário de comprimento 4.

Segundo Firer (2007), um dos principais problemas em Teoria de Códigos (e em Teoria de Informação de modo mais geral) é a existência de erros: ao se transmitir ou armazenar informações, ocorrem erros que podem comprometer a confiabilidade dos dados. Em outras palavras, assim como na brincadeira de "telefone sem fio", a mensagem recebida pode não ser igual aquela transmitida. São diversas as fontes de erros, mas estes estão quase sempre presentes e o problema se resume em duas etapas: detectar a existência de erros e tentar corrigi-los. A confiabilidade é adquirida através de algum tipo de redundância (como por exemplo repetir cada palavra), mas a redundância tem sempre um custo, o que nos leva a um dos grandes desafios da Teoria

de Códigos: adquirir a confiabilidade desejada ao menor custo (taxa de redundância) possível.

A fonte de informação, ou código da fonte, é a mensagem que deve ser enviada. A ideia básica da teoria dos códigos é codificar essa informação inicial, adicionando infomação redundante, aqui temos o código de canal, de forma que ao receber o sinal modificado pelo ruído, de alguma forma, seja possível recuperar a mensagem original. Esse procedimento pode ser esquematizado conforme mostra a Figura 5.

Figura 5: Esquema de codificação/decodificação



Fonte: Lidl e Niederreiter (1994), p. 306.

Votando ao exemplo da Língua Portuguesa, uma situação em que utilizamos o esquema acima são os editores de texto com correção ortográfica. Imagine que recebemos uma mensagem com a palavra "gilafa". Imediatamente verificamos que a mensagem contém um erro, pois não reconhecemos essa palavra como pertencente à língua, mais ainda, achamos que a mensagem correta deve ser "girafa", pois é a palavra mais próxima da palavra recebida. Vale observar que este não é um código muito eficiente, pois se tivéssemos recebido a mensagem "zato", reconhecemos que ela está errada, mas percebemos que há várias palavras igualmente próximas, como por exemplo "mato", "gato, "pato", rato, fato, etc. A fim de tornar precisa essa noção intuitiva de proximidade de palavras, apresentamos a seguir um modo de medir a distância entre as palavras em A^n.

Definição 3.2.2. *Dados dois elementos* $u, v \in A^n$*, a distância de Hamming entre* u *e*

v *é definida como*

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

Por exemplo, em $\{0,1\}^4$, isto é, um código cujo alfabeto são os elementos do conjunto $\{0,1\}$ e as palavras possuem comprimento 4, temos

$$d(0000, 0010) = 1;$$

$$d(1110, 0010) = 2;$$

$$d(1111, 0000) = 4.$$

Proposição 3.2.3. *Dados* $u, v, w \in A^n$*, valem as seguintes propriedades*

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

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

iii) Desigualdade triangular: $d(u,v) \leq (u,w) + d(w,v)$*.*

Demonstração: A única propriedade cuja demonstração não é totalmente trivial é a terceira que passamos a desmonstrar.

A contribuição das i-ésimas coordenadas de u e v para $d(u,v)$ é igual a zero se $u_i = v_i$, e igual a um se $u_i \neq v_i$, $1 \leq i \leq n$.

No caso em que a contribuição é zero, certamente a contribuição das i-ésimas coordenadas a $d(u,v)$ é menor ou igual a das i-ésimas coordenadas a $d(u,w) + d(w,v) (= 0, 1, \text{ ou } 2)$. No outro caso, temos que $u_i \neq v_i$ e, portanto, não podemos ter $u_i = w_i$ e $w_i = v_i$. Consequentemente, a contribuição das i-ésimas coordenadas a $d(u,w) + d(w,v)$ é maior ou igual a 1, que é a contribuição das i-ésimas coordenadas a $d(u,v)$. □

As propriedades contidas na Proposição 3.2.3 caracterizam o que se costuma, em matemática, chamar *métrica* [5]. Por isso, a distância de Hamming entre elementos de A^n é também chamada de *métrica de Hamming*.

[5] Uma métrica num conjunto M é uma função $d : M \times M \to \mathbb{R}$, que associa a cada para ordenado de elementos $x, y \in M$ um número real $d(x,y)$, chamado a distância de x a y, de modo que sejam satisfeitas as seguintes condições para quaisquers $x, y, z \in M$:

d1) $d(x,x) = 0$;

d2) Se $x \neq y$, então $d(x,y) > 0$;

d3) $d(x,y) = d(y,x)$;

Pode-se definir agora os conceitos de disco e esfera em A^n, tal como é feito em qualquer espaço métrico.

Definição 3.2.4. *Dado um elemento* $a \in A^n$ *e um número real* $t \geq 0$*, chamamos de* ***disco de centro*** a ***e raio*** t*, ao conjunto*

$$D(a,t) = \{u \in A^n; d(u,a) \leq t\}$$

e ***esfera de centro*** a ***e raio*** t*, ao conjunto*

$$S(a,t) = \{u \in A^n; d(u,a) = t\}.$$

Note que como as distâncias são sempre inteiros positivos, dentro de um disco de centro a e raio t estão contidas todas as esferas do mesmo centro cujos raios são os inteiros menores ou iguais a t. Logo, temos que:

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

Esses conjuntos, $D(a,t)$ e $S(a,t)$ são finitos e o próximo lema nos fornecerá a cardinalidade de $D(a,t)$.

Lema 3.2.5. *Para todo* $a \in A^n$*, e todo número natural* $r > 0$*, temos que*

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

Demonstração: Dado um ponto a, um outro ponto b estará a distância t de a se diferir dele em t posições. Digamos que escolhemos t posições fixas entre as que compõe a. Como em cada uma destas posições podemos ter $q-1$ letras do alfabeto, diferentes da letra correspondente em a, existem $(q-1)^t$ palavras de A^n que diferem de a nas t posições fixadas. Ainda podemos escolher t posições entre as n posições do elemento a de $\binom{n}{t}$ maneiras distintas. Portanto, existem exatamente $\binom{n}{t}(q-1)^t$ pontos na esfera

d4) $d(x,z) \leq d(x,y) + d(y,z)$.

Lima (1983)

$S(a,t)$. Podemos então calcular o número de pontos no disco de centro a e raio t:

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

□

Definição 3.2.6. *Seja* C *um código. A* ***distância mínima*** *de* C *é o número*

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

No próximo resultado, $\lfloor x \rfloor$ representa a parte inteira do número real x.

Teorema 3.2.1. *Seja* C *um código com distância mínima* d *e seja*

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Então, é possível detectar até $d-1$ *erros e corrigir até* κ *erros.*

Demontração: Seja c um elemento de C e suponhamos que ele foi recebido como outro elemento r, com $t \leq d-1$ erros. Como o número t de erros conhecidos é precisamente a distância de Hamming de c a r, temos que $d(c,r) = t \leq d-1 \leq d$. Isto implica que $r \notin C$ e, portanto, o erro pode ser detectado. Suponhamos ainda que o número de erros cometidos é menor que κ. Consideremos o disco $D(r,\kappa)$. Como $d(c,r) = t \leq \kappa$, temos que $c \in D(c,\kappa)$. Afirmamos que r é o único elemento de C pertencente a este disco. De fato, se existisse $r' \in C$ em $D(r,\kappa)$, ter-se-ia que

$$d(r,r') \leq d(r,c) + d(c,r') \leq \kappa + \kappa = 2\kappa < d,$$

uma contradição. Consequentemente r é o único elemento de C mais próximo de c e é possível corrigir o erro. □

Corolário 3.2.1.1. *Um código* C *pode corrigir até* κ *erros se, e somente se, sua distância mínima* $d(C)$ *satisfaz a desigualdade*

$$d(C) \geq 2\kappa + 1.$$

Demonstração: Do teorema anterior sabemos que

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

onde $d = d(C)$ é a distância mínima do código. Assim,

$$\kappa = \left\lfloor \frac{d(C)-1}{2} \right\rfloor \leq \frac{d(C)-1}{2},$$

o que prova o resultado. □

Definição 3.2.7. *Dado um código* C *com distância miníma* d*, o número*

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$$

chama-se ***capacidade*** *do código* C*.*

Na Figura 6[6], mostramos como atua a capacidade de correção de um código.

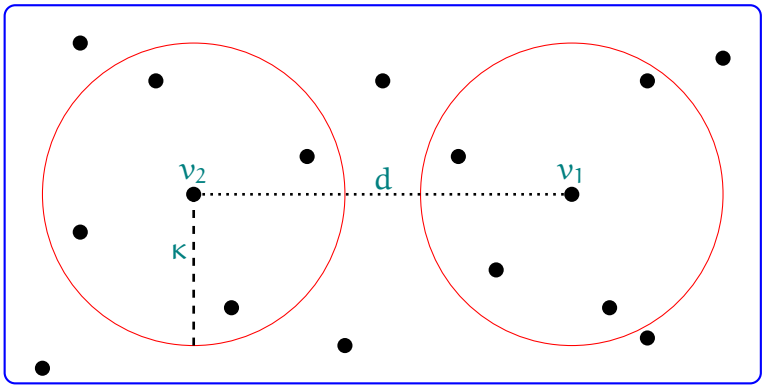


Figura 6: Capacidade de correção de um código.

Sejam dadas duas palavras $v_1, v_2 \in C$, onde C é um código cuja distância mínima é d e capacidade de correção κ. Qualquer palavra (na figura, as palavras são representadas por pontos) que pertença ao $D(v_1, \kappa)$, será corrigida pelo código como sendo v_1. De modo análogo, toda palavra que pertença ao $D(v_2, \kappa)$, será corrigida pelo código como

[6]A Figura 6 foi elaborada tendo por referência o seminário "Representações de Corpos Finitos com aplicações em Criptografia e Códigos Corretores de Erros", disponível em https://www.youtube.com/watch?v=L_Up4wNiTJIt=3357s.

sendo ν_2. As palavras que estão fora dos discos anteriormente mencionado, não podem ser corrigidas, pois estão fora da capacidade de correção do código.

Definição 3.2.8. *Seja* $C \subset A^n$ *um código com distância mínima* d *e seja* $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$. *O código C será dito perfeito se*

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

Note que em virtude do teorema 3.2.1, um código terá maior capacidade de correção de erros quanto maior for sua distância mínima. Portanto, é fundamental, para a Teoria dos Códigos, poder calcular d ou pelo menos determinar uma cota inferior para ele.

Um código C sobre um alfabeto A possui três parâmetos fundamentas $[n, M, d]$, que são respectivamente, o seu comprimento, o seu número de elementos e sua distância mínima. Neste caso, dizemos que C é um $[n, M, d]$-código. Existe uma interdependência complexa entre esses três números, e um dos problemas fundamentais da Teoria dos Códigos é o de estudá-la.

Interessa-nos estabelecer quando dois códigos têm os mesmos parâmetros. Para isso, definimos o seguinte:

Definição 3.2.9. *Seja* A *um conjunto finito e* n *um número inteiro. Uma função* $\varphi : A^n \to A^n$ *diz se uma* ***isometria*** *de* A^n *se* φ *preserva a distância de Hamming, isto é, se*

$$d(\varphi(x), \varphi(y)) = d(x, y),$$

para todos $x, y \in A^n$.

Como $d(x, y) = 0$ se, e somente se, $x = y$, é fácil ver que uma isometria é necessariamente, uma função injetora. Ainda, como A^n é finito, segue imediatamente que φ também é sobrejetora. Logo, toda isometria de A^n é uma função bijetora.

Proposição 3.2.10.

i) A função identidade é uma isometria.

ii) Se φ *é uma isometria de* A^n*, então* φ^{-1} *é uma isometria de* A^n.

iii) Se φ *e* γ *são duas isometrias de* A^n*, então* $\varphi \circ \gamma$ *é uma isometria de* A^n.

Definição 3.2.11. *Dados dois códigos* C *e* C' *em* A^n*, diremos que o código* C *é equivalente a* C'*, escrevemos* $C \cong C'$*, se existe uma isometria* $\varphi : A^n \to A^n$ *tal que* $\varphi(C) = \varphi(C')$*.*

Segue da Proposição 3.2.10 que a equivalência de códigos é uma relação de equivalência.

Decorre da Definição 3.2.11 que dois códigos equivalentes possuem mesmos parâmetros, porém existem códigos com os mesmos parâmetros que não são equivalentes.

Exemplo 3.2.12. *Sejam* $C = \{0000, 0100, 0101\}$ *e* $C' = \{0000, 0010, 0111\}$ *dois códigos de* $\mathbb{Z}_2^4$*. Ambos possuem parâmetros* $n = 4, M = 3$ *e* $d = 1$*. Porém não existe uma isometria* $\varphi : \mathbb{Z}_2^4 \to \mathbb{Z}_2^4$*, tal que* $\varphi(C) = \varphi(C')$*.*

Damos, abaixo, exemplos de duas famílias importantes de isometrias.

Exemplo 3.2.13. *Se* $f : A \to A$ *é uma bijeção, e* i *é um número inteiro tal que* $1 \leq i \leq n$*, a função*

$$\begin{aligned} \varphi_f^i : A^n &\longrightarrow A^n \\ (a_1, \ldots, a_n) &\longmapsto (a_1, \ldots, f(a_i), \ldots, a_n) \end{aligned}$$

é uma isometria.

Exemplo 3.2.14. *Se* π *é uma bijeção do conjunto* $\{1, \ldots, n\}$ *nele próprio, também chamada de permutação de* $\{1, \ldots, n\}$*, então a função permutação de coordenadas*

$$\begin{aligned} \varphi_\pi : A^n &\longrightarrow A^n \\ (a_1, \ldots, a_n) &\longmapsto (a_{\pi(1)}, \ldots, a_{\pi(n)}) \end{aligned}$$

é uma isometria.

Pode-se demonstrar que toda isometria é um dos dois tipos acima ou uma composição de isometrias desse tipo. Mais precisamente, vale o seguinte.

Teorema 3.2.2. *Dada uma isometria* $\varphi : A^n \to A^n$ *existe uma permutação* π *do conjunto* $\{1, \ldots, n\}$ *e bijeções* $f_i : A \to A, 1 \leq i \leq n$ *tais que*

$$\varphi = \varphi_\pi \circ \varphi_F,$$

onde $F = \{f_1, f_2, \ldots, f_n\}$ φ_F *e* φ_π *e estão definidas nos Exemplos 3.2.13 e 3.2.14 respectivamente.*

Com esse resultado, dizemos que dois códigos de comprimento n sobre um alfabeto A, cujos elementos são chamados de letras, são equivalentes se, e somente se, um deles pode ser obtido do outro mediante uma sequência de operações do tipo:

(i) Substituição de letras numa dada posição fixa em todas as palavras do código por meio de uma bijeção de A.

(ii) Permutação das posições das letras em todas as palavras do código, mediante uma permutação fixa de $\{1, \ldots, n\}$.

3.3 Mudança de Alfabeto

É possível trocar o alfabeto de um código por outro alfabeto qualquer com o mesmo número de elementos sem alterar os parâmetros do código.

Sejam A e B dois conjuntos finitos e seja

$$f : A \to B$$

uma bijeção. A partir de f podemos definir a função

$$\begin{aligned} \phi : A^n &\longrightarrow B^n \\ (x_1, \ldots, x_n) &\longmapsto (f(x_1), \ldots, f(x_n)). \end{aligned}$$

Essa função é claramente bijetora e preserva a distância de Hamming.

Seja $C \subset A^n$ um código com M elementos e distância mínima d, a sua imagem $C' = \phi(C) \subset B^n$ é um código sobre o alfabeto B com parâmetros iguais aos de C. Assim, dado um código C sobre um alfabeto qualquer A com m elementos, podemos, mediante uma bijeção dada $f : A \to \mathbb{Z}_m$, obter um código C' sobre o anel $\mathbb{Z}_m$ com os mesmos parâmetros de C. Uma das vantagens disso é que temos mais estrutura sobre o afabeto, o que nos permite usar mais ferramentas matemáticas. Em particular, tem-se a noção de peso $\omega(u)$ de um elemento $u \in \mathbb{Z}_m$ definido como

$$\omega(u) = |\{i; u_i \neq 0\}|,$$

isto é, o número de coordenadas não nulas de u. E se o código C' é fechado para a subtração, isto é, se

$$\forall u, v \in C', u - v \in C',$$

então vale a seguinte igualdade para a distância mínima d de C'

$$d = \min\{\omega(u); u \in C', u \neq 0\}.$$

3.4 Códigos Lineares

Segundo Hefez e Villela (2008), a classe de códigos mais utilizada na prática é chamada classe dos códigos lineares. Devido a sua estrutura algébrica, eles são mais fáceis de descrever do que os códigos não lineares.

Seja K um corpo finito com q elementos tomado como alfabeto. Temos, portanto, para cada número natural n, um K-espaço vetorial K^n de dimensão n.

Definição 3.4.1. *Um código $C \subset K^n$ será chamado de **código linear** se for um subespaço vetorial de K^n.*

Se a dimensão de C é k e $|K| = q$, segue facilmente que o número de palavras do código é $M = q^k$. Se a distância mínima d é conhecida, o código C diz-se um $[n, k, d]$-código linear.

Segundo Milies (2009), uma primeira vantagem dos códigos lineares é aparentemente quando queremos calcular sua distância mínima. Como um código linear é um subespaço vetorial, se denotarmos por 0 o elemento neutro da adição no espaço vetorial, temos que $0 \in C$. Podemos então introduzir o seguinte.

Definição 3.4.2. *Dado um elemento $x \in C$, chama-se peso de x ao número*

$$\omega(x) := d(x, 0) = |\{i; x_i \neq 0\}.$$

Chama-se peso do código C ao número

$$\omega(C) = \min\{\omega(x); x \in C \text{ e } x \neq 0\}.$$

Note que dados $x = (x_1, x_2, \cdots, x_k), y = (y_1, y_2, \cdots, y_k) \in C$, temos

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

Esta observação mostra que toda distância entre elementos do código C é também o peso de algum elemento. Consequentemente

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

Falaremos agora do processo de codificação. Suponhamos que desejamos enviar mensagens com k dígitos de informação e $n-k$ dígitos de redundância. Podemos considerar que o vetor de infomação é um elemento do espaço vetorial K^k e que o vetor já codificado é um elemento de K^n. Nosso código será então um subespaço vetorial $C \subset K^n$ de dimensão k.

Se $\{e_1, \ldots, e_k\}$ é base canônica de K^k e $\{c_1, \ldots, c_k\}$ é uma base de C, a função linear

$$\begin{array}{rcl} \nu : K^k & \longrightarrow & K^n \\ e_i & \longmapsto & \nu(e_i) = c_i, , \end{array}$$

onde $1 \leq i \leq k$, é bijetora e $\mathrm{Im}(\nu) = C$.

Esta aplicação pode ser visualizada no seguinte diagrama:

$$\begin{array}{ccc} K^k & \xrightarrow{\nu} & K^n \\ | & & | \\ K^k & \xrightarrow{\nu|_{K^k}} & \mathrm{Im}(\nu) = C \end{array}$$

Vamos representar a matriz G que representa a transformação linear ν nas bases canônicas de K^k e K^n, respectivamente. Para isso, escrevemos os elementos da base de

C na base canônica de K^n, que denotaremos por $\mathfrak{B} = \{v_1, \ldots, v_k\}$:

$$\begin{cases} c_1 = b_{11}v_1 + b_{21}v_2 + \cdots + b_{n1}v_n \\ c_2 = b_{12}v_1 + b_{22}v_2 + \cdots + b_{n2}v_n \\ \vdots \\ c_k = b_{1k}v_1 + b_{2k}v_2 + \cdots + b_{nk}v_n \end{cases}$$

onde os coefeicientes $b_{ij} \in K$, com $1 \leq i \leq n$ e $1 \leq j \leq k$. Então, a matriz procurada é

$$G = \begin{pmatrix} b_{11} & b_{21} & \ldots & b_{k1} \\ b_{12} & b_{22} & \ldots & b_{k2} \\ \vdots & \vdots & & \vdots \\ b_{1n} & b_{2n} & \ldots & b_{kn} \end{pmatrix}.$$

Note que cada linha da matriz G corresponde a um vetor que pertence ao código C, ou seja, pode-se dizer que C é o subespaço de K^n gerado pelas linhas da matriz G (que formam na realidade, uma base de C). Os elementos de C são então todos os vetores $y \in K^n$ da forma $x \cdot G = y$, para todo $x \in K^k$.

Definição 3.4.3. *Uma matriz* $G \in \mathbb{M}_{n\times k}(K)$ *cujas linhas formam uma base para* C *diz-se uma* ***matriz de codificação*** *de* C.

Note que, para cada escolha de uma base para C obtemos uma matriz de codificação G diferente, de modo que esta matriz não é único. Pensando K^k como o conjunto de palavras a ser transmitida, a transformação v nos diz como codificar as palavras. Em outras palavras, K^k é o código da fonte, $C = v(K^k) \subset K^n$ é o código de canal e a transformação v é a codificação.

Duas matrizes geradoras de um mesmo código C podem ser obtidas uma da outra por meio de operações do tipo:

(L1) Permutação de duas linhas.

(L2) Multiplicação de uma linha por um escalar não nulo.

(L3) Adição de um múltiplo escalar de uma linha a outra.

Exemplo 3.4.4. *Tome* $K = \mathbb{F}_2$. *Considere a tranformação linear injetora*

$$\begin{aligned} \nu : \mathbb{F}^3 &\longrightarrow \mathbb{F}^5 \\ (x_1, x_2, x_3) &\longmapsto (x_1, x_3, x_1 + x_2, x_2 + x_3, x_2). \end{aligned}$$

Seja $C = \mathrm{Im}(\nu)$. *Sejam* (e_1, e_2, e_3) *a base canônica de* $\mathbb{F}^3$ *e* $(\nu_1, \nu_2, \nu_3, \nu_4, \nu_5)$ *a base canônica de* $\mathbb{F}^5$. *Vamos encontrar uma matriz* G *que representa a transformação linear* ν.

Assim,

$$\begin{aligned} \nu(e_1) &= (1,0,1,0,0) = 1\nu_1 + 0\nu_2 + 1\nu_3 + 0\nu_4 + 0\nu_5 \\ \nu(e_2) &= (0,0,1,1,1) = 0\nu_1 + 0\nu_2 + 1\nu_3 + 1\nu_4 + 1\nu_5 \\ \nu(e_3) &= (0,1,0,1,0) = 0\nu_1 + 1\nu_2 + 0\nu_3 + 1\nu_4 + 0\nu_5. \end{aligned}$$

Portanto, uma matriz de codificação G *é da forma*

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Assim, as palavras código $(1,1,1)$ *e* $(0,1,0)$ *serão codificados respectivamente como* $(1,1,0,0,1)$ *e* $(0,0,1,1,1)$.

Podemos ainda escrever uma matriz geradora na forma padrão, confome definição a seguir.

Definição 3.4.5. *Dizemos que a matriz geradora de um código* C *está na forma padrão se tivermos*

$$G = (\mathrm{Id}_k | A),$$

onde Id_k *é a matriz identidade de ordem* k *e* A *uma matriz* $k \times (n - k)$.

Efetuando operações do tipo $(L1), (L2)$ e $(L3)$ sobre as linhas de uma matriz geradora G, ela poderá ser colocada na forma padrão. Por exemplo, a matriz G do Exemplo

3.4.4, pode ser colocada na forma

$$G' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

assim, por exemplo, a palavra $(1,1,1)$ do código da fonte é codificada como $(1,1,1,1,0)$. A vantagem da representação de uma matriz geradora na forma padrão é que ao codificar a palavra, conseguimos identificar qual é a mensagem original e quais redundâncias foram inseridas.

Dado um código C, nem sempre é possível achar uma matriz geradora de C na forma padrão. Por exemplo, o código em $\mathbb{F}_2^5$ de matriz geradora

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

No entanto, efetuando também permutações nas colunas de G, podemos obeter a matriz

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

que é a matriz geradora na forma padrão de um código C' equivalente a C.

De modo mais geral, efetuando também sequências de operações sobre a matriz geradora G de um código linear C, do tipo:

(C1) permutação de duas colunas;

(C2) Multiplicação de uma coluna por um escalar não nulo,

obtemos uma matriz G' de um código C' equivalente a C.

Note que dado o código linear C, como ele é um subespaço de K^n de dimensão k, pode-se determinar uma transformação linear sobrejetora $\pi : K^n \longrightarrow K^{n-k}$ tal que $\ker(\pi) = C$, por exemplo como descrevemos a seguir.

Dada uma base $\{c_1, \ldots, c_k\}$ de C, ela pode ser extendida a uma base

$$\{c_1, \ldots, c_k, v_1, \ldots, v_{n-k}\}$$

de K^n. Dado um vetor $v \in K^n$, ele pode ser escrito na forma

$$v = \lambda_1 c_1 + \lambda_2 c_2 + \cdots + \lambda_k c_k + \lambda_{k+1} v_1 + \cdots + \lambda_n v_{n-k},$$

onde $\lambda_i \in K$, $1 \leq i \leq n$.
Definimos então

$$\begin{aligned} \pi : K^n &\longrightarrow K^{n-k} \\ v &\longmapsto v' = \lambda_{k+1} v_1 + \cdots + \lambda_n v_{n-k}, \end{aligned}$$

e é fácil verificar que $\ker(\pi) = C$

Podemos representar essa transformação pelo diagrama:

$$\begin{array}{ccc} K^n & \xrightarrow{\pi} & K^{n-k} \\ | & & | \\ \ker(\pi) = C & \longrightarrow & 0 \end{array}$$

Denotaremos por $H = (h_{ij}) \in \mathbb{M}_{n\times(n-k)}$ a matriz de posto $n-k$ que representa a transformação linear π nas bases canônicas de K^n e K^{n-k}.

Definição 3.4.6. *A matriz* H *construída acima diz-se uma* ***matriz de verificação*** *ou* ***matriz teste de paridade*** *do código linear* C*.*

Se uma matriz geradora G está na forma padrão, fica fácil encontrar a matriz teste de paridade.

Proposição 3.4.7. *Seja* $C \subset K^n$ *um código de dimensão* k *com matriz geradora* $G = (Id_k|A)$*, na forma padrão. Então a matriz* $H = (-A^t|Id_{n-k})$ *é uma matriz teste de paridade de* C*.*

Exemplo 3.4.8. *Seja* $\mathbb{F}_2$ *o corpo finito com dois elementos. Considere a transformação linear sobrejetora*

$$\begin{aligned} \pi : \mathbb{F}^3 &\longrightarrow \mathbb{F}^2 \\ (x_1, x_2, x_3) &\longmapsto (x_1 + x_2, x_3) \end{aligned}$$

cujo núcleo e $C = \ker(\pi) = \{(x_1, x_1, 0); x_1 \in \mathbb{F}_2\}$. *Agora, considere as bases canônicas* (e_1, e_2, e_3) *e* (f_1, f_2) *de* $\mathbb{F}^3$ *e* $\mathbb{F}^2$ *respectivamente.*

Vamos achar a matriz H *que representa a transformação linear* π *nessas bases.*

Temos que

$$\pi(e_1) = \pi(1,0,0) = 1f_1 + 0f_2$$
$$\pi(e_2) = \pi(0,1,0) = 1f_1 + 0f_2$$
$$\pi(e_3) = \pi(0,0,1) = 0f_1 + 1f_2$$

Portanto, a matriz é:

$$H = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

A matriz teste de paridade é bastante eficiente quando queremos determinar se uma palvavra pertence ou não ao código, e será utilizada também no processo de decodificação, conforme veremos mais a diante.

Proposição 3.4.9. *Seja* C *um código linear e suponhamos que* H *seja uma matriz teste de paridade. Temos então que*

$$v \in C \text{ } \textit{se, e somente se,} \text{ } Hv^t = 0.$$

Dados um código C com matriz teste de paridade H e um vetor $v \in K^n$, o vetor Hv^t é chamado de *síndrome* de v.

Exemplo 3.4.10. *Seja dado um código* C *sobre* $\mathbb{F}_2$ *com matriz geradora*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Como G *está na forma padrão é fácil calcular uma matriz teste de paridade* H. *Pela Proposição 3.4.7, temos que*

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Dados $v = (100111)$ *e* $v' = (010101)$, *como*

$$Hv^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ e } H(v')^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \neq 0,$$

temos que $v \in C$ *e* $v' \notin C$.

Um resultado útil para determinar $\omega(C)$ é o seguinte:

Proposição 3.4.11. *Seja* C *um código com matriz teste de paridade* H *e peso* $\omega(C)$. *Então quaisquer* $\omega(C)-1$ *colunas de* H *são linearmente independentes e existem* $\omega(C)$ *colunas de* H *linearmente dependentes.*

Corolário 3.4.0.1. ***(Cota de Singleton)*** *Os parâmetros* (n, k, d) *de um código linear satisfazem à desigualdade*

$$d \geq n - k + 1.$$

Portanto, a cota de Singleton relaciona os três parâmetros de um código linear. Um código será chamado MDS (Maximum Distance Separable) se valer a igualdade $d = n - k + 1$.

Exemplo 3.4.12. ***Códigos de Hamming*** *Um código de Hamming de ordem* m *sobre* $\mathbb{F}_2$ *é um código com matriz teste de paridade* H_m *de ordem* $m \times n$, *cujas colunas são os elementos de* $\mathbb{F}_2^m \setminus \{0\}$ *numa ordem qualquer. A determinação de* H_m *determina o código* C *a menos de equivalência.*

Temos, portanto, que o comprimento de um código de Hammimg de ordem m *é* $2^m - 1$ *e, portanto, sua dimensão é* $k = n - m = 2^m - 1$. *Verificamos que* $d = 3$, *pois, em* H_m, *é fácil achar três colunas linearmente dependentes. Para* $m = 3$, *temos*

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

é uma matriz de um código de Hamming. Pode ser demonstrado que todo código de Hamming é perfeito. Além disso, um código de Hamming de ordem m *é* MDS *se, e somente se,* $m = 2$.

Decodificação

Chama-se *decodificação* ao procedimento de detecção e correção de erros num determinado código. Para isso, define-se inicialmente o vetor erro e como sendo a diferença entre o vetor recebido r e o vetor transmitido c, isto é

$$e = r - c$$

Note que o peso do vetor erro corresponde ao número de erros cometidos numa palavra entre a transmissão e a recepção.

Seja H a matriz teste de paridade do código. Como $Hc^t = 0$, temos que

$$He^t = H(r^t - c^t) = Hr^t - Hc^t = Hr^t.$$

Portanto, a palavra recebida e o vetor erro têm mesma síndrome.

Denotemos por h^i a i-ésima coluna de H. Se $e = (\alpha_1, \ldots, \alpha_n)$, então

$$\sum_{i=1}^{n} \alpha_i h^i = He^t = Hr^t.$$

Lema 3.4.13. *Seja* C *um código linear em* K^n *com capacidade de correção* κ. *Se* $r \in K^n$ *e* $c \in C$ *são tais que* $d(c, r) \leq \kappa$, *então existe um único vetor* e *com* $\omega(e) \leq \kappa$,

cuja síndrome é igual a síndrome de r *e ta que* $c = r - e$.

Seja $C \subset K^n$ um código corretor de erros com matriz de teste de paridade H. Sejam d a distância mínima de C e $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$. Seja $v \in K^n$. Defina

$$v + C = \{v + c; c \in C\}.$$

Cada conjunto da forma $v + C$ é chamado de *classe lateral segundo C*. Note que $v + C = C$ se, e somente se, $v \in C$

Lema 3.4.14. *Os vetores* $u, v \in K^n$ *têm a mesma síndrome se, e somente se,* $u \in v+C$.

Demonstração: $Hu^t = 0 \iff H(u-v)^t = 0 \iff u - v \in C \iff u \in v + C$. □

Definição 3.4.15. *Um vetor de peso mínimo numa classe lateral é chamado* ***elemento líder*** *dessa classe.*

Proposição 3.4.16. *Seja* C *um código linear em* K^n *com distância mínima* d. *Se* $u \in K^n$ *é tal que*

$$\omega(u) \leq \left\lfloor \frac{d-1}{2} \right\rfloor = \kappa,$$

então u *é o único elemento líder de sua classe.*

Vamos discutir um algoritmo de correção de mensagens que tenha sofrido um número de erros menor ou igual à capacidade de correção do código (κ).

Preparação: Determine todos os elementos $u \in K^n$, tais que $\omega(u) \leq \kappa$. Em seguida, calcule as síndromes desses elementos e coloque esses dados numa tabela. Seja r uma palavra recebida.

O Algoritmo de Decodificação

1. Calcule a síndrome $s^t = Hr^t$.
2. Se s está na tabela, seja ℓ o elemento líder da classe determinada por s; troque r por $r - \ell$.
3. Se s não está na tabela, então na mesagem recebida foram cometidos mais de κ erros.

Justificativa: Dado r, sejam c e e, respectivamente, a mensagem transmitida e o vetor erro. Como $He^t = Hr^t$, temos que a classe lateral onde e se encontra está determinada pela síndrome de r. Se $\omega(e) \leq \kappa$, temos que e é o único elemento líder ℓ de suas classe e, portanto, é conhecido e se encontra na tabela. Consequentemente, pelo Lema 3.4.13, $c = r - e = r - \ell$ é determinado.

Exemplo 3.4.17. *Considere o* $(6,3)$*-código linear sobre* $\mathbb{F}_2$ *com matriz teste de paridade*

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Nesse caso $d = 3$ *e, portanto,* $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor = 1$. *Os vetores de peso* ≤ 1 *com as suas respectivas síndromes estão relacionados na tabela abaixo*

líder	***síndrome***
000000	*000*
000001	*101*
000010	*011*
000100	*110*
001000	*001*
010000	*010*
100000	*100*

Suponhamos, agora, que a palavra recebida seja

(a) $r = (100011)$. *Logo,* $Hr^t = (010)^t$ *e, portanto,* $e = (010000)$. *Consequentemente,* $c = r - e = (110011)$.

(b) $r = (111111)$. *Logo* $Hr^t = (111)^t$, *que não se encontra na tabela. Sendo assim foi cometido mais do que* 1 *erro na mensagem* r.

Todos os códigos que apresentaremos nas próximas seções fazem parte da classe

dos códigos lineares, portanto, nosso estudo consiste em determinar a matriz geradora, matriz teste de paridade e, quando possível, a distância mínima. E para isso, utilizaremos os conceitos até agora estudados. Para que tenhamos bons algoritmos de codificação/decodificação, é importante enriquecermos a estrutura de espaço vetorial ja existente nesses códigos com outras estruturas algébricas.

3.5 Códigos Cíclicos

A seguir, vamos descrever os códigos cíclicos. Segundo Voloch (2020), o interesse fundamental dos códigos cícilos é que eles admitem uma representação interessante em termos de polinômios sobre um corpo K que permite a descrição de um algoritmo de decodificação muito simples. Outro ponto interessante, é que um código cíclico, possui além da estrutura de espaço vetorial, a estrutura adicional de um **ideal**, conceito esse apresentado no Capítulo 1.

Seja K um corpo finito. No que se segue, representaremos as coordenadas de um elemento em K^n por $(x_0, x_1, \ldots, x_{n-1})$.

Definição 3.5.1. *Um código linear* $C \subset K^n$ *será chamado de código cíclico se, para todo* $c = (c_0, c_1, \ldots, c_{n-1}) \in C$*, o vetor* $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$*.*

Equivalentemente, o código linear C será um código cíclico se, dada a permutação π de $\{0, \ldots, n-1\}$ definida por

$$\pi(i) = \begin{cases} i-1 & , \text{se} \quad i \geq 1 \\ n-1 & , \text{se} \quad i = 0 \end{cases}$$

e sendo

$$T_\pi(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_o, \ldots, c_{n-2}),$$

temos que $T_\pi(c) \in C$ para todo $c \in C$; ou seja $T_\pi(C) \subset C$.

$$R_n = K[x]_{(x^n-1)} = K[x]/(x^n - 1).$$

odifcação muito simples.

Vamos agora enriquecer a estrutura de um código cíclico como se segue.

Um elemento de R_n é, portanto, um conjunto da forma

$$[f(x)] = \{f(x) + g(x)(x^n - 1); g(x) \in K[x]\};$$

e a adição e a multiplicação em R_n são respectivamente definidas por

$$[f_1(x)] + [f_2(x)] = [f_1(x) + f_2(x)],$$

e por

$$[f_1(x)] \cdot [f_2(x)] = [f_1(x) \cdot f_2(x)].$$

R_n, munido da multiplicação por escalares $\lambda \in K$, definida por

$$\lambda[f(x)] = [\lambda f(x)],$$

é um K-espaço vetorial de dimensão n com base $1, [x], \ldots, [x^{n-1}]$. Assim, é isomorfo a K^n através da transformação linear

$$\begin{array}{rcl} v : K^n & \longrightarrow & R_n \\ (a_0, \ldots, a_{n-1}) & \longmapsto & [a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}]. \end{array}$$

Temos então, que todo código linear $C \subset K^n$ pode ser transportado para R_n mediante o isomorfismo v e aí estudado. A vantagem de R_n sobre K^n é que, no primeiro, temos, além da estrutura de espaço vetorial, uma estrutura de anel. A imagem por v de um código cíclico de K^n possui a estrutura algébrica de um ideal.

Sobre os ideais de R_n, enunciamos os seguintes resultados:

Proposição 3.5.2. *Um ideal de* $K[x]$ *é da forma* $I(f(x))$*, onde* $f(x) \in K[x]$*.*

Corolário 3.5.0.1. *Seja* $I \neq \{0\}$ *um ideal de* $K[x]$*. Então existe um único polinômio mônico* $f(x)$ *em* I *(de grau mínimo), tal que* $I = I(f(x))$*.*

Proposição 3.5.3. *Todo ideal de* $K[x]_{p(x)}$ *é da forma* $I([f(x)])$*, onde* $f(x)$ *é um divisor de* $p(x)$*.*

Demonstração. Seja I um ideal de $K[x]_{p(x)}$. Considere o conjunto

$$J = \{g(x) \in K[x]; [g(x)] \in I\}.$$

Vamos inicialmente, provar que J é um ideal de $K[x]$. De fato, se $g_1(X)$ e $g_2(x)$ estão em J, então $[g_1(X)]$ e $[g_2(x)]$ estão em I. E, portanto,

$$[g_1(x) + g_2(x)] = [g_1(x)] + [g_2(x)] \in I,$$

e consequentemente, $g_1(x) + g_2(x) \in J$.

Por outro lado, se $g(x) \in J$ e $h(x) \in K[x]$, temos que $[g(x)] \in I$, e portanto, $[g(x)h(x)] = [g(x)][h(x)] \in I$. Logo, $g(x)h(x) \in J$.

Sendo $J \neq \{0\}$, pois $p(x) \in J$, segue da Proposição 3.5.2 que existe $f(x) \in K[x] \setminus \{0\}$ tal que $J = I(f(x))$. Como $p(x) \in J = I(f(x))$, segue que $p(x)$ é um múltiplo de $f(x)$, ou seja $f(x)$ é um divisor de $p(x)$.

Note agora que $I = \{[g(x)]; g(x) \in J\}$, e como $J = I(f(x))$, temos que

$$I = \{[h(x)][f(x)]; [h(x)] \in K[x]_{p(X)} = I([f(x)])\}.$$

□

Os resultados anteriores nos ajudarão a determinar as matrizes geradora e teste de paridade de códigos cíclicos. Inicialmente, vamos caracterizar os códigos cíclicos em R_n.

Note qe a ação de T_π em K^n traduz-se, por meio de ν, na mutiplicação por $[x]$ em R_n.

De fato, tomando $c = (c_o, \ldots, c_{n-1})$, temos:

$$T_\pi(c) = (c_{n-1}, c_0, \ldots, c_{n-2})$$

e

$$\nu(T_\pi)(c) = [c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1}] = [x][c_0 + c_1x + \cdots + c_{n-1}x^{n-1}] = [x]\nu(c).$$

A demonstração do próximo resultado encontra-se em Hefez e Villela (2008).

Proposição 3.5.4. *Todo ideal* I *de* R_n *é da forma* $I = I([g(x)])$*, onde* $g(x)$ *é um divisor mônico de* $x^n - 1$*. Além disso,tal* $g(x)$ *é unicamente determinado pelo ideal.*

Definição 3.5.5. *Seja* $C = (g)$ *um código cíclico. Dizemos que* g *é um polinômio gerador de* C *e* $h = \dfrac{x^n - 1}{g}$ *é o polinômio verificador de* C*.*

No próximo teorema, reunimos algumas propriedades do polinômio gerador e também nos diz como obter a matriz geradora e a matriz teste de paridade de um código cíclico.

Teorema 3.5.1. *Seja* C *um ideal não nulo em* R_n*, isto é,* C *é um código cíclico de comprimento* n*.*

1. *O código* C *é gerado por um único polinômio mônico* g *de grau mínimo em* C*.*

2. *O polinômio gerador* g *de* C *é um fator de* $x^n - 1$*.*

3. *Em* $K[x]$*, qualquer* $c \in C$ *pode ser escrito unicamente como* $c = fg$*, onde* $gr(f) < n - r$ *e* $gr(g) = r$*. Além disso, a dimensão de* C *é* $n - r$*.*

4. *Se* $g(x) = g_0 + g_1x + \cdots + g_rx^r$*. Se* $I = I([g(x)])$*, então o código* $C = v^{-1}(I)$ *tem matriz geradora*

$$G = \begin{pmatrix} v^{-1}([g(x)]) \\ v^{-1}([xg(x)]) \\ \vdots \\ v^{-1}([x^{n-r-1}g(x)]) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & g_0 & \dots & \dots & g_r \end{pmatrix}.$$

5. *A matriz teste de paridade de* C *gerado por* G *é dada por*

$$H = \begin{pmatrix} h_{n-s} & h_{n-s-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \dots & h_0 \dots & 0 & \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \\ 0 & \dots & 0 & h_{n-s} & \dots & \dots & h_0 \end{pmatrix},$$

onde

$$\frac{x^n - 1}{g(x)} = h_0 + h_1x + \ldots + h_{n-s}x^{n-s}.$$

Demonstração: A afirmação (1) segue da prova do Teorema 1.3.3. Para mostrar (2), escrevemos $x^n - 1 = hg + r$, onde $r, g \in K[x]$ e $gr(r) < gr(g)$. Em $K[x]_{p(x)} = k[x]/(x^n - 1) = R_n$, isto implica que $r = -hg$. Como $gr(r) < gr(g)$, temos que $r = 0$ e assim $g|x^n - 1$.

Seja $c \in C$ onde $gr(c) < n$. Por (2), existe um polinômio q tal que $c = gq$ em R_n. Por (3), suponhamos que $x^n - 1 = gh$. Em $K[x]$, temos que $c = qg + l(x^n - 1)$ para algun $l \in K[x]$, isto é, $c = (q + lh)g$. Seja $f = q + lh$. Então $c = fg$ e $gr(f) < n - r - 1$. Assim, o código é formado por múltiplos de g, que são polinômios de grau máximo $n - r - 1$ avaliado em $K[x]$ e não em R_n.

Há $n - r$ múltiplos de g linearmente independentes, a saber, $g, xg, x^2g, \cdots, x^{n-r-1}g$. Os vetores correspondentes são as linhas da matriz geradora G. Portanto, o código tem dimensão $n - r$.

Para demonstrar (5), seja h o polinômio verificador de C. Seja f uma mensagem codificada pela multiplicação por g:

$$c = fg = \sum_{i=0}^{n-1} c_i x^i.$$

Então $ch = fgh = f(x^n - 1)$, isto é, $ch = 0$ em R_n. Digamos que

$$ch = \left(\sum_{i=0}^{n-1} c_i x^i \right) \left(\sum_{l=0}^{k} h_l x^l \right),$$

onde $h_k \neq 0$. O coeficiente de x^j neste produto é

$$\sum_{i=0}^{n-1} c_i h_{j-i} = 0, \tag{5}$$

para $j = 0, 1, \ldots, n-1$, onde os subíndices são tomados módulo n. Se $c \in C$, a Equação 5 implica que $Hc^t = 0$, sendo a matriz H a matriz teste de paridade de C. □

Decodificação

Seja $C \subset K^n$ um código cíclico. Apresentaremos agora, uma maneira de determinar a matriz gerador G na forma padrão e discutiremos um algoritmo de decodificação.

As demonstrações dos teoremas aqui apresentados podem ser encontrados em Hefez e Villela (2008).

Seja

$$\begin{aligned} \mu : K^s &\longrightarrow K[x]_{s-1} \subset K[x] \\ (a_0, \ldots, a_{s-1}) &\longmapsto \sum_{i=0}^{s-1} a_i x^i. \end{aligned}$$

o isomorfismo de K-espaços vetoriais, onde $K[x]_{s-1}$ é o espaço vetorial dos polinômios de grau menor ou igual a $s-1$. Esse isomorfismo será de grande utilidade no que se segue.

Teorema 3.5.2. *Seja $C \subset K^n$ um código cíclico. Suponhamos que $C = v^{-1}(I)$, onde $I = I([g(x)])$, com $g(x)$ divisor de $x^n - 1$ de grau s. Seja R a matriz $(n-s) \times s$ cuja i-ésima linha é*

$$R_i = -\mu^{-1}(r_i(x)), 1 \leq i \leq n-s,$$

onde $r_i(x)$ é o resto da divisão de x^{s-1+i} por $g(x)$. Então, $(R|Id_{n-s})$ é uma matriz geradora de C.

Teorema 3.5.3. *Seja $C \subset K^n$ um código linear gerado por um polinômio mônico $g(x)$ de grau s com matriz geradora na forma padrão $(R|Id_{n-s})$ e matriz teste de paridade $(Id_s|-R^t)$. Se $v = (v_0, \ldots, v_{n-1}) \in K^n$, então a síndrome de v com relação a matriz H é dada por*

$$\mu^{-1}(r(x))$$

onde $r(x)$ é o resto da divisão de $v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$ por $g(x)$.

Exemplo 3.5.6. *Considere o polinõmio $x^7 - 1$ sobre $\mathbb{F}_2$. A fatoração de $x^7 - 1$ é dada por*

$$x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3).$$

Vamos considerar o código $C \subset \mathbb{F}_2^7$ gerado pelo polinômio $g(x) = 1+x+x^3$. A dimensão

de C *é 4. Agora determinaremos uma matriz geradora desse código na forma padrão.*

$$\begin{aligned} x^3 &= (x^3+x+1)+(x+1) \\ x^4 &= (x^3+x+1)x+(x^2+x) \\ x^5 &= (x^3+x+1)(x^2+1)+(x^2+x+1) \\ x^6 &= (x^3+x+1)(x^3+x+1)+(x^2+1). \end{aligned}$$

Logo, pelo Teorema 3.5.2, temos que uma matriz geradora de C *é dada por*

$$G' = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Suponhamos que seja dado o vetor $(a_1, a_2, a_3, a_4) \in \mathbb{F}_2^4$*, do código da fonte, então de acordo com a discussão acima, a codificação desse vetor é dada por*

$$(b_0, b_1, b_2, a_1, a_2, a_3, a_4),$$

onde b_0, b_1 *e* b_2 *são os coeficientes do polinômio*

$$\begin{aligned} a_1(x+1)+a_2(x^2+x)+a_3(x^2+x+1)+a_4(x^2+1) = \\ a_1+a_3+a_4+(a_1+a_2+a_3)x+(a_2+a_3+a_4)x^2. \end{aligned}$$

Portanto a codificação de (a_1, a_2, a_3, a_4) *é*

$$(a_1+a_3+a_4, a_1+a_2+a_3, a_2+a_3+a_4, a_1, a_2, a_3, a_4).$$

A matriz teste de paridade associada a G' *é a matriz*

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Dado o vetor $(1101001) \in \mathbb{F}_2^8$*, a sua síndrome relativa a* H *é dada por* $\mu^{-1}(r(x))$*, onde* $r(x)$ *é o resto da divisão de* $1 + x + x^3 + x^6$ *por* $g(x) = 1 + x + x^3$*. Portanto* $r(x) = x^2 + 1$*, e consequentemente, a síndrome é* (101)*.*

3.6 Códigos BCH

Os Códigos BCH são uma família especial de código cíclicos. Eles possuem bons algoritmos de codificação e decodificação por admitir uma representação em termos de polinômios sobre um corpo K. A vantagem em se trabalhar com códigos BCH é que podemos determinar, a priori, cotas inferiores para suas distâncias mínimas.

A próxima proposição será utilizado na determinação do polinômio gerador de um código BCH. A demonstração pode ser encontrada em Hefez e Villela (2008).

Proposição 3.6.1. *Sejam* F *um corpo finito,* K *um subcorpo de* F *e* $\beta \in F$*. Se* $q = |K|$*, então* $\beta^{q^m} = \beta$ *e* $\beta^{q^i} \neq \beta^{q^j}$ *para* $i \neq j$*,* $i, j = 0, 1, \ldots m - 1$*. Além disso,*

$$m_\beta(x) = (x - \beta)(x - \beta^q) \cdots (x - \beta^{q^{m-1}}).$$

No próximo resultado, veremos que, construindo um código cíclico com um conjunto conveniente de raízes n-ésimas da unidade, temos uma cota inferior para sua distancia mínima. A demonstração do resultado pode ser encontrado em Hefez e Villela (2008).

Teorema 3.6.1. ***(Bose-Chaudhuri-Hocquenghem)***[7] *Seja* $K = \mathbb{F}_q$ *e,* n *um inteiro maior do que* 1 *e primo com* q*. Seja* F *um corpo onde* $x^n - 1$ *se decompõe em fatores lineares, e seja* $\gamma \in F$ *uma raiz* n*-ésima primitiva da unidade. Seja* C *o código cíclico com polinômio gerador*

$$g(x) = mmc(m_{\gamma^a}(x), \ldots, m_{\gamma^{a+\delta-2}}(x)),$$

com $a \geq 0$ *e* $\delta \leq n$*. Então a distância mínima de* C *é pelo menos* δ *e a sua dimensão é pelo menos* $n - m(\delta - 1)$*, onde* $m = \dim_K F$*.*

O número δ que aparece no enunciado do teorema acima, é chamado de *peso estimado* do código BCH, pois representa uma estimativa para a distãncia mínima do código.

Definição 3.6.2. *Fixados um corpo* K *e uma extensão* F *com uma raiz* n*-ésima primitiva da unidade* $\gamma \in F$*, definimos*

$$C_K(n, \delta) = \left\{ (a_0, \ldots, a_{n-1}) \in K^n; \sum_{i=0}^{n-1} a_i \gamma^{ij} = 0, j = 1, \ldots, \delta - 1 \right\},$$

como sendo o código BCH *definido pelo polinômio gerador*

$$g(x) = mmc(m_\gamma(x), \ldots, m_{\gamma^{\delta-1}}(x)).$$

A seguir, daremos outra maneira de descrever um código BCH que nos permitirá, na próxima seção, generalizar esses códigos.

Teorema 3.6.2. *Temos que*

$$(a_0, \ldots, a_{n-1}) \in C_K(n, \delta) \textit{se, e somente se,} \sum_{j=0}^{n-1} a_j \gamma^{j(\delta-1)} \frac{x^{\delta-1} - \gamma^{-j(\delta-1)}}{x - \gamma^{-j}} = 0.$$

[7] Códigos BCH foram inventados em 1959 por Alexis Hocquenghem, e de forma independente em 1960 por Raj Chandra Bose e Ray-Chaudhuri. A abreviação BCH compreende as iniciais dos nomes desses inventores.

Demonstração. Por definição, segue que $(a_0, \ldots, a_{n-1}) \in C_K(n, \delta)$ se, e somente se,

$$\sum_{i=1}^{\delta-1} \left(\sum_{j=0}^{n-1} a_j \gamma^{ij} \right) x^i = 0.$$

Reescrevendo a identidade acima, obtemos

$$0 = \sum_{i=1}^{\delta-1} \left(\sum_{j=0}^{n-1} a_j \gamma^{ij} \right) x^i = \sum_{j=0}^{n-1} a_j \gamma^{\delta-1} \sum_{i=0}^{\delta-2} \gamma^{-j(\delta-2-i)} x^i = \sum_{j=0}^{n-1} a_j \delta^{j(\delta-1)} \frac{x^{\delta-1} - \gamma^{-j(\delta-1)}}{x - \gamma^{-j}}.$$

□

O resultado seguinte nos dá uma estimativa para o peso C e justifica o nome de peso estimado. A demonstração do resultado pode ser encontrada em Voloch (2020).

Teorema 3.6.3. *Seja* $C \subset K^n$ *um código* BCH*, temos que*

$$\omega(C) \geq \delta.$$

Estudaremos agora como obter o polinômio gerador de um código BCH, e assim determinar sua matriz geradora. Seja dado um código BCH sobre um corpo finito K, definido por raízes da unidade, $\gamma^a, \ldots, \gamma^{a+\delta-2}$ numa extensão F de K. Para determinar

$$g(x) = mmc(m_{\gamma^a}(x), \ldots, m_{\gamma^{a+\delta-2}}(x)),$$

é preciso determinar os polinômios $m_{\gamma^j}(x)$ para qualquer valor de j.

Pela Proposição 3.6.1, temos que

$$m_{\gamma^j}(x) = (x - \gamma^j)(x - (\gamma^j)^q) \cdots (x - (\gamma^j)^{q^{d_j - 1}}),$$

onde d_jé o menor inteiro positivo tal que $(\gamma^j)^{q^{d_j}} = \gamma^j$, ou seja, d_j é o menor inteiro positivo tal que

$$jq^{d_j} \equiv j \mod n.$$

Portanto, a determinação do polinômio mínimo de γ^j passa pela determinação do

conjunto

$$C_j = \{[jq^t] \in \mathbb{Z}_n; t \in \mathbb{Z}, t \geq 0\},$$

cujos elementos são os expoentes a que devemos elevar γ para achar todas as raízes do polinômio mínimo de γ^j. Esses conjuntos possuem propriedades importantes como podemos verificar no resultado subsequente.

Proposição 3.6.3. *Os conjuntos* C_i *possuem as seguintes propriedades:*

i) Se $C_i \cap C_j \neq \emptyset$*, então* $C_i = C_j$*.*

ii) A união de todos os C_j *é igual a* $\mathbb{Z}_n$*.*

O conjunto C_i é chamado de *classe de ciclotomia* de i, módulo n.

Exemplo 3.6.4. *Seja* $n = 21$ *e* $q = 2$*. Ponha* $K = \mathbb{F}_2$*. O menor inteiro* m *tal que* $2^m \equiv 1 \mod 21$ *é* $m = 6$*. Seja* α *um elemento primitivo de* $F = \mathbb{F}_{64}$*. Logo,* $\gamma = \alpha^3$ *é uma raiz* 21*-ésima primitiva da unidade em* F*. As classes de ciclotomia módulo* 21 *são as seguintes:*

$$\begin{aligned}
C_0 &= \{[0]\} \\
C_1 &= \{[1], [2], [4], [8], [16], [11]\} \\
C_3 &= \{[3], [6], [12]\} \\
C_5 &= \{[5], [10], [20], [19], [17], [13]\} \\
C_7 &= \{[7], [14]\} \\
C_9 &= \{[9], [18], [15]\}.
\end{aligned}$$

Podemos, então, determinar os polinômios mínimos de todas as potências de γ*:*
$m_\gamma(x) = m_{\gamma^2}(x) = m_{\gamma^4}(x) = m_{\gamma^8}(x) = m_{\gamma^{16}}(x) = m_{\gamma^{11}}(x) = (x-\gamma)(x-\gamma^2)(x-\gamma^4)(x-\gamma^8)(x-\gamma^{16})(x-\gamma^{11}) = 1 + x + x^2 + x^4 + x^6$.

$m_{\gamma^3}(x) = m_{\gamma^6}(x) = m_{\gamma^{12}}(x) = (x-\gamma^3)(x-\gamma^6)(x-\gamma^{12}) = 1 + x^2 + x^3$.

$m_{\gamma^5}(x) = m_{\gamma^{10}}(x) = m_{\gamma^{13}}(x) = m_{\gamma^{17}}(x) = m_{\gamma^{19}}(x) = m_{\gamma^{20}}(x) = (x-\gamma^5)(x-\gamma^{10})(x-\gamma^{13})(x-\gamma^{17})(x-\gamma^{19})(x-\gamma^{20}) = 1 + x^2 + x^4 + x^5 + x^6$.

$m_{\gamma^7}(x) = m_{\gamma^{14}}(x) = (x - \gamma^7)(x - \gamma^{14}) = 1 + x + x^2$.

$m_{\gamma^9}(x) = m_{\gamma^{15}}(x) = m_{\gamma^{18}}(x) = (x - \gamma^9)(x - \gamma^{18})(x - \gamma^{15}) = 1 + x + x^3$.

Pelo Teorema 3.6.1, o código BCH *gerado pelo polinômio*

$$g(x) = mmc\{m_\gamma(x), m_{\gamma^2}(x), m_{\gamma^3}(x), m_{\gamma^4}(x)\} = m_\gamma(x)m_{\gamma^3}(x),$$

que é o código $C_K(n, 5)$*, tem distância mínima* $d \geq 5$.

Decodificação

Suponha que escolhemos um código BCH com peso estimado $\delta = 2t + 1$. O que torna os códigos BCH muito interessantes é que há um algoritmo de decodificação eficiente, devido a Berlekamp [8], que passamos a expor. Surgido em 1967-68, trata-se de um eficiente procedimento iterativo para determinar o polinômio localizador de erros.

Seja $C \in R_n$ então um código BCH de peso estimado $\delta = 2t+1$ e β a raiz primitiva n-ésima da unidade usada para definir C.

Seja $a(x) \in R_n$ uma palavra recebida com no máximo t erros. Suponhamos inicialmente que conhecemos a palavra enviada $c(x)$ e seja $e(x) = a(x) - c(x)$ o erro. Definimos então, se $e(x) = e_0 + e_1x + \ldots + e_{n-1}x^{n-1}$,

$$\begin{aligned} M &= \{i | e_i \neq 0\}, \\ r &= |M|, \\ l(x) &= \prod_{i \in M} (1 - \beta^i x), \\ s(x) &= \left(\sum_{i \in M} e_i \beta^i \right) \left(\sum_{j \in M \setminus \{i\}} (1 - \beta^j x) \right). \end{aligned}$$

M é o conjunto das posições onde os erros ocorrem e r é o número de erros, que estamos supondo ser no máximo t. $l(x)$ é chamado o *polinômio localizador de erros*. De fatos, $i \in M$ se, e somente se, $l(\beta^{-i}) = 0$, logo conhecendo $l(x)$ saberemos onde os

[8] Elwyn Ralph Berlekamp foi um matemático americano conhecido por seu trabalho em ciência da computação, teoria da codificação e teoria dos jogos combinatórios.

erros estão. O polinômio $s(x)$ servirá para nos dizer qual foi o erro. De fato, se $i \in M$ temos

$$s(\beta^{-i}) = e_i \sum_{j \in M \setminus \{i\}} (1 - \beta^j \beta^{-i}) = -e_i l'(\beta^{-i})$$

onde l' é a derivada de l. Desta equação podemos, podemos calcular e_i a partir de l e s. Resumindo, se conhecemos l e s saberemos onde os erros ocorreram e quais foram os erros. O algoritmo consistirá então de se obter $l(x)$ e $s(x)$ somente a partir de $a(x)$. Se pudermos fazer isso, então obtemos o processo de correção como foi feito acima.

A observação crucial é a seguinte (para mais detalhes, consultar Voloch (2020)):

$$\frac{s(x)}{l(x)} = \sum_{j=1}^{\infty} e(\beta^j) x^j . (*)$$

Por outro lado, $e(\beta^j) = a(\beta^j) - c(\beta^j) = a(\beta^j)$, para $j = 1, \ldots, \delta - 1$. Logo conhecemos os valores $e(\beta^j)$ para $1 \leq j \leq 2t$ a partir de $a(x)$ somente.

O ponto crucial agora, é que, por hipótese, $r \geq t$ e como o $gr(l), gr(s) \geq r$, temos $gr(l), gr(s) \geq t$.

Seja $f(x) = \sum_{j=1}^{2t} a(\beta^j) x^j$, a equação $(*)$ se reescreve como

$$\frac{s(x)}{l(x)} \equiv f(x) \mod x^{2t+1}.$$

Como $f(x)$ é conhecido, isso nos permite determinar l e s. De fato,

$$s(x) - l(x) f(x) \equiv 0 \mod x^{2t+1},$$

como $mdc(l, s) = 1$ e $l(0) = 1$, obtemos o resultado.

3.7 Códigos de Goppa Clássicos

Os códigos de Goppa Clássicos foram introduzido por V. D. Goppa em 1970. Os códigos de Goppa Clássicos são uma generalização dos códigos BCH conforme definidos no

Teorema 3.6.2.

Definição 3.7.1. *Seja* F *um corpo finito, extensão de um corpo* K. *Seja* $\varphi(x) \in F[x]$ *e* $L = \{\alpha_0, \ldots, \alpha_{n-1}\} \subset F$, *onde os* α_i *são dois a dois distintos e tais que* $\varphi(\alpha_i) \neq 0$ *para* $i = 0, \ldots, n-1$. *Define-se*

$$\Gamma_K(L, \varphi) = \left\{ (c_0, \ldots, c_{n-1}) \in K^n; \sum_{i=0}^{n-1} c_i \varphi(\alpha_i)^{-1} \frac{\varphi(x) - \varphi(\alpha_i)}{x - \alpha_i} = 0 \right\}.$$

É claro que $\Gamma_K(L, \varphi)$ é um subespaço vetorial de K^n, pois dados dois vetores $a = (a_0, \ldots, a_{n-1}), b = (b_0, \ldots, b_{n-1}) \in \Gamma_K(L, \varphi)$ e $\lambda \in K$, temos

$$a + \lambda b = \sum_{i=0}^{n-1} a_i \varphi(\alpha_i)^{-1} \frac{\varphi(x) - \varphi(\alpha_i)}{x - \alpha_i} + \lambda \sum_{i=0}^{n-1} b_i \varphi(\alpha_i)^{-1} \frac{\varphi(x) - \varphi(\alpha_i)}{x - \alpha_i} = 0 + \lambda 0 = 0,$$

Logo, $a + \lambda b \in \Gamma_K(L, \varphi)$ e $\Gamma_K(L, \varphi)$ é um subespaço vetorial de K^n. Portanto,$\Gamma_K(L, \varphi)$ é um código linear, chamado *código de Goppa clássico* sobre K associado ao conjunto L e ao polinômio φ.

Segundo Hefez e Villela (2008), os códigos de Goppa $\Gamma_K(L, \varphi)$ possuem bons algoritmos de decodificação, além de terem cotas inferiores para a sua distância mínima, obtidas a priori, como ocorre para os códigos BCH.

Teorema 3.7.1. *Sejam* K *e* F *corpos finitos, com* F *uma extensão de* K, *tais que* $\dim_K F = m$. *Sejam* $\varphi(x) \in F[x]$, *com* $gr(\varphi) = \delta$ *e* $L = \{\alpha_0, \ldots, \alpha_{n-1}\} \subset F$, *onde os* α_i *são dois a dois distintos e tais que* $\varphi(\alpha_i) \neq 0$, $i = 0, \ldots, n-1$. *Então* $\Gamma_K(L, \varphi)$ *é um código de dimensão* $k \geq n - m\delta$ *e com distância mínima* $d \geq \delta + 1$.

Demonstração: Vamos, inicialmente, encontrar uma matriz $\widetilde{H}$ que caracterize, mediante condições de anulamento, o código $\Gamma_K(L, \varphi)$. Seja

$$\varphi(x) = \sum_{j=0}^{\delta} \varphi_j x^j, \text{ com } \varphi_\delta \neq 0.$$

Então

$$\frac{\varphi(x) - \varphi(\alpha)}{x - \alpha} = \sum_{j=0}^{\delta} \varphi_j \frac{x^j - \alpha^j}{x - \alpha} = \sum_{t=0}^{\delta-1} \left(\sum_{j=t+1}^{\delta} \varphi_j \alpha^{j-1-t} \right) x^t.$$

Portanto, $(c_0, \ldots, c_{n-1}) \in \Gamma_K(L, \varphi)$ se, e somente se,

$$0 = \sum_{i=0}^{n-1} c_i \varphi(\alpha_i)^{-1} \frac{\varphi(x) - \varphi(\alpha_i)}{x - \alpha_i} = \sum_{i=0}^{n-1} c_i \varphi(\alpha_i)^{-1} \sum_{t=0}^{\delta-1} \left(\sum_{j=t+1}^{\delta} \varphi_j \alpha_i^{j-1-t} \right) x^t =$$

$$\sum_{t=0}^{\delta-1} \left(\sum_{i=0}^{n-1} \left(\varphi(\alpha_i)^{-1} \sum_{j=t+1}^{\delta} \varphi_j \alpha_i^{j-1-t} \right) c_i \right) x^t,$$

e isso ocorre se, e somente se,

$$\sum_{i=0}^{n-1} \left(\varphi(\alpha_i)^{-1} \sum_{j=t+1}^{\delta} \varphi_j \alpha_i^{j-1-t} \right) c_i = 0, 0 \leq t \leq \delta - 1.$$

Portanto, pondo

$$B = \begin{pmatrix} \varphi(\alpha_0)^{-1}\varphi_\delta & \ldots & \varphi(\alpha_{n-1})^{-1}\varphi_\delta \\ \varphi(\alpha_0)^{-1}(\varphi_{\delta-1} + \varphi_\delta \alpha_0) & \ldots & \varphi(\alpha_{n-1})^{-1}(\varphi_{\delta-1} + \varphi_\delta \alpha_{n-1}) \\ \vdots & & \vdots \\ \varphi(\alpha_0)^{-1} \sum_{j=1}^{\delta} \varphi_j \alpha_0^{j-1} & \ldots & \varphi(\alpha_{n-1})^{-1} \sum_{j=1}^{\delta} \varphi_j \alpha_{n-1}^{j-1} \end{pmatrix}$$

temos que

$$c \in \Gamma_K(L, \varphi) \text{ se, e somente se, } Bc^t = 0.$$

Como $\varphi_\delta \neq 0$, após realizar as operações elementares sobre as linhas de B, obtemos a matriz

$$\widetilde{H} = \begin{pmatrix} \varphi(\alpha_0)^{-1} & \cdots & \varphi(\alpha_{n-1})^{-1} \\ \varphi(\alpha_0)^{-1}\alpha_0 & \cdots & \varphi(\alpha_{n-1})^{-1}\alpha n - 1 \\ \vdots & & \vdots \\ \varphi(\alpha_0)^{-1}\alpha_0^{\delta-1} & \cdots & \varphi(\alpha_{n-1})^{-1}\alpha_{n-1}^{\delta-1} \end{pmatrix} \tag{6}$$

e, portanto,

$$c \in \Gamma_K(L, \varphi) \text{ se, e somente se, } \widetilde{H}c^t = 0.$$

Se $K = F$, a matriz $\widetilde{H}$ é uma matriz teste de paridade de $\Gamma_K(L, \varphi)$ e, portanto, sendo $\Lambda(L, \varphi)$ o código gerado pela matriz $\widetilde{H}$, temos que

$$\Lambda(L, \varphi) = \Gamma_K(L, \varphi)^{\perp},$$

onde $\Gamma_K(L, \varphi)^{\perp} = \{v \in K^n; \langle v, u\rangle = 0, \forall u \in C\}$. Se, ao contrário, $K \neq F$, então a matriz $\widetilde{H}$ não é uma matriz teste de paridade de $\Gamma_K(L, \varphi)$, pois seus coeficientes não pertencem ao corpo K. Olhando para F como K-espaço vetorial, com $\dim_K F = m$, podemos escrever cade entrada de $\widetilde{H}$ como vetor coluna com coeficientes de K de comprimento m. Dessa maneira, obtemos uma matriz H' com coeficientes em K tal que

$$c \in \Gamma_K(L, \varphi) \text{ se, e somente se, } H'c^t = 0.$$

Como as linhas de H' não são necessariamente linearmente independentes sobre K, a matriz H' não é necessariamente a matriz teste de paridade de $\Gamma_K(L, \varphi)$. Como a matriz teste de paridade H de $\Gamma_K(L, \varphi)$ é a matriz obtida de H' suprimindo linhas linearmente dependentes, temos que um conjunto de colunas de H é linearmente independente sobre K se, e somente se, o conjunto correspondente de colunad de H' é linearmente dependente sobre K □

O próximo resultado nos dará uma outra maneira equivalente de definir um código de Goppa, que nos permitirá determinar, matrizes geradoras para esse código. Utilizamos como referência para os próximos resultados Hefez e Villela (2008) e Voloch (2020).

Proposição 3.7.2. *Seja K e F corpos finitos com F sendo uma extensão de K. Sejam $\varphi(x) \in F[x]$, com $gr(\varphi) = \delta$ e $L = \{\alpha_0, \ldots, \alpha_{n-1}\} \subset F$, onde os α_i são dois a dois distintos e tais que $\varphi(\alpha_i) \neq 0$, $i = 0, \ldots, n-1$. Temos que*

$$\left\{(c_o, \ldots, c_{n-1}) \in K^n; \sum_{i=0}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \mod \varphi(x)\right\} = \Gamma_K(L, \varphi). \tag{7}$$

9

Demonstração: Observe inicialmente que

$$\frac{1}{x-\alpha_i}+\frac{1}{\varphi(\alpha_i)}\left(\frac{\varphi(x)-\varphi(\alpha_i)}{x-\alpha_i}\right)=\frac{\varphi(\alpha_i)+\varphi(x)-\varphi(\alpha_i)}{(x-\alpha_i)\varphi(\alpha_i)}=\frac{\varphi(x)}{(x-\alpha_i)\varphi(\alpha_i)}.$$

Logo,

$$\frac{1}{x-\alpha_i}\equiv\frac{-1}{\varphi(\alpha_i)}\left(\frac{\varphi(x)-\varphi(\alpha_i}{x-\alpha_i}\right)\mod\varphi(x).$$

Chamando de C o conjunto no primeiro membro de (7), e pondo $c=(c_0,\ldots,c_{n-1})$, temos

$$\begin{aligned}
c\in C &\iff \sum_{i=0}^{n-1}\frac{c_i}{x-\alpha_i}\equiv 0 \mod\varphi(x)\\
&\iff \sum_{i=0}^{n-1}\frac{-c_i}{\varphi(\alpha_i)}\left(\frac{\varphi(x)-\varphi(\alpha_i)}{x-\alpha_i}\right)\equiv 0 \mod\varphi(x)\\
&\iff \sum_{i=0}^{n-1}c_i\varphi(\alpha_i)^{-1}\left(\frac{\varphi(x)-\varphi(\alpha_i)}{x-\alpha_i}\right)=0\\
&\iff c\in\Gamma_K(L,\varphi),
\end{aligned}$$

onde a penúltima equivalência decorre do fato de

$$f(x)=\sum_{i=0}^{n-1}c_i\varphi(\alpha_i)^{-1}\left(\frac{\varphi(x)-\varphi(\alpha_i)}{x-\alpha_i}\right)$$

ser um polinômio de grau menor que o grau de $\varphi(x)$. Portanto,

$$f(x)\equiv 0 \mod\varphi(x),$$

se, e somente se, $\varphi(x)$ divide $f(x)$, o que equivale a ter $f(x)=0$. □

[9] $\sum_{i=0}^{n}\frac{c_i}{x-\alpha_i}\equiv 0 \mod\varphi$ significa que existem $a(x)$ e $b(x)$ primos entre si com $a(x)$ divisível por $\varphi(x$ e $\sum_{i=0}^{n}\frac{c_i}{x-c_i}=\frac{a(x)}{b(x)}$.

Proposição 3.7.3. *Uma matriz geradora do código* $\Gamma_K(L,\varphi)$ *é*

$$\begin{pmatrix} \frac{\varphi(\alpha_0)}{h'(\alpha_0)} & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})} \\ \frac{\varphi(\alpha_0)}{h'(\alpha_0)}\alpha_0 & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})}\alpha_{n-1} \\ \vdots & & \vdots \\ \frac{\varphi(\alpha_0)}{h'(\alpha_0)}\alpha_0^{n-1-\delta} & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})}\alpha_{n-1}^{n-1-\delta} \end{pmatrix},$$

onde $h(x) = \prod_{j=0}^{n-1}(x-\alpha_j)$.

Demonstração: Note que $c = (c_0,\ldots,c_{n-1}) \in \Gamma_F(L,\varphi)$ se, e somente se, existe $b(X) \in F[x]$ tal que

$$\sum_{i=0}^{n-1} \frac{c_i}{x-\alpha_i} = \frac{b(x)\varphi(x)}{h(x)}. \tag{8}$$

Portanto, para determinar um elemento $c \in \Gamma_F(L,\varphi)$, basta determinar $b(x) \in F[x]$ satisfazendo a igualdade (8). Desta mesma igualdade, segue que

$$b(x)\varphi(x) = h(x)\sum_{i=0}^{n-1}\frac{c_i}{x-\alpha_i} = \sum_{i=0}^{n-1} c_i \prod_{k\neq i}(x-\alpha_k). \tag{9}$$

Observando que $h'(x) = \sum_{i=0}^{n-1}\prod_{k\neq i}(x-\alpha_k)$ temos

$$h'(\alpha_j) = \sum_{i=0}^{n-1}\prod_{k\neq i}(\alpha_j-\alpha_k) = \prod(\alpha_j-\alpha_k).$$

Logo, de (9), obtemos, para $0 \leq j \leq n-1$,

$$b(\alpha_j)\varphi(\alpha_j) = \sum_{i=0}^{n-i} c_i \prod_{k\neq i}(\alpha_j-\alpha_k) = c_j\prod_{k\neq j}(\alpha_j-\alpha_k) = c_j h'(\alpha_j). \tag{10}$$

Como $gr(b(x)) \leq n-1-\delta$, podemos escrever

$$b(x) = \sum_{i=0}^{n-1-\delta} b_i x^i.$$

Portanto, de 10, segue, para $0 \leq j \leq n-1$, que

$$\frac{c_j h'(\alpha_j)}{\varphi(\alpha_j)} = b(\alpha_j) = \sum_{i=0}^{n-1-\delta} b_i \alpha_j^i.$$

Assim, para $0 \leq j \leq n-1$,

$$c_j = \frac{\varphi(\alpha_j)}{h'(\alpha_j)} \sum_{i=0}^{n-1-\delta} b_i \frac{\varphi(\alpha_j)\alpha_j^i}{h'(\alpha_j)}.$$

Logo, $c \in \Gamma_F(L, \varphi)$ se, e somente se, existe $(b_0, \ldots, b_{n-1-\delta}) \in F^{n-\delta}$ tal que

$$c = (b_0, \ldots, b_{n-1-\delta}) \begin{pmatrix} \frac{\varphi(\alpha_0)}{h'(\alpha_0)} & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})} \\ \frac{\varphi(\alpha_0)}{h'(\alpha_0)}\alpha_0 & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})}\alpha_{n-1} \\ \vdots & & \vdots \\ \frac{\varphi(\alpha_0)}{h'(\alpha_0)}\alpha_0^{n-1-\delta} & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})}\alpha_{n-1}^{n-1-\delta} \end{pmatrix},$$

o que prova o resultado. □

Códigos de Goppa têm também um algoritmo de decodificação similar aos códigos BCH.

Sejam dados um corpo finito K, uma extensão finita F de K, um polinômio $\varphi(x) \in F[x]$ de grau δ e $L = \{\alpha_0, \ldots, \alpha_{n-1}\} \subset F^*$, tais que $\varphi(\alpha_i) \neq 0$ para $i = 0, \ldots, n-1$. Seja $r = (r_0, \ldots, r_{n-1})$ a mensagem recebida e $c = (c_0, \ldots, c_{n-1})$ a mensagem enviada.

Suponha que $|c - r| \leq \frac{\delta}{2}$. Seja $e = (e_0, \ldots, e_{n-1}) = r - c$. Definimos:

$$\begin{aligned} M &= \{i | e_i \neq 0\}, \\ e &= |M|, \\ l(x) &= \prod_{i \in M} (x - \alpha_i), \\ s(x) &= \sum_{i \in M} e_i \prod_{j \in M \setminus \{i\}} (x - \alpha_j). \end{aligned}$$

Exatamente como no caso dos códigos BCH o nosso problema é calcular l e s conhecendo apenas r.

Seja

$$S(x) = \sum_{i=0}^{n-1} r_i \frac{-1}{\varphi(\alpha_i)} \frac{\varphi(x) - \varphi(\alpha_i)}{x - \alpha_i}.$$

Então

$$S(x) \equiv \sum_{i=0}^{n-1} \frac{r_i}{x - \alpha_i} \equiv \sum_{i=0}^{n-1} \frac{e_i}{x - \alpha_i} \mod \varphi(x).$$

Temos :

$$\begin{aligned} S(x)l(x) &\equiv \sum_{i=0}^{n-1} \frac{e_i}{x - \alpha_i} \prod_{j \in M} (x - \alpha_j) \\ &\equiv \sum_{i=0}^{n-1} e_i \prod_{j \in M \setminus \{i\}} (x - \alpha_j) \\ &\equiv s(x) \mod \varphi(x). \end{aligned}$$

$S(x)$ é conhecido, $\varphi(x)$ também, e temos que determinar l e s de grau $< \frac{\delta}{2}$ tais que

$$S(x)l(x) \equiv s(x) \mod \varphi(x),$$

e lembramos que o grau de $\varphi(x)$ é δ. Isso é uma generalização do problema tratado no caso dos códigos BCH onde tínhamos $\varphi(x) = x^{2n+1}$. A solução neste caso é uma generalização direta do que fizemos anteriormente.

4 Corpos de Funções Algébricas sobre Corpos Finitos

Neste capítulo vamos introduzir as definições e os conceitos básicos da Teoria dos Corpos de Funções Algébricas: corpos com valorizações, valorizações de corpos de funções algébricas, divisores, teorema de Riemana-Roch, função Zeta de um corpo de funções algébricas e o limite de Hasse-Weil. A principal motivação para o estudo dos Corpos de Funções Algébricas sobre Corpos Finitos nesse trabalho é a sua importância na teoria dos Códigos Corretores de Erros, em particular, na construção dos Códigos Algébrico Geométricos. As referências utilizadas nessa capítulo foram Niederreiter (2002), Stichtenoth (2009), Weiss (1998).

4.1 Corpos com Valorização

Para introduzir o conceito de valorização, começaremos com os dois exemplos a seguir.

Exemplo 4.1.1. *Seja* $\mathbb{Q}$ *o corpo dos números racionais. Para todo* $r \in \mathbb{Q}$ *não nulo e* p *número primo, podemos escrever*

$$r = p^m \frac{a}{b},$$

com $m \in \mathbb{Z}$ *único,* a, b *inteiros não nulos e tais que* $mdc(a, p) = mdc(p, b) = 1$. *Considere a função* $|\,.\,|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$, *definida por*

$$|r|_p = \begin{cases} 0 & , se\ r = 0 \\ p^{-m} & , se\ r \neq 0 \end{cases}.$$

A função $|\,.\,|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ *é chamada valorização absoluta* p*-ádica sobre* $\mathbb{Q}$ *e satisfaz as seguintes propriedades:*

i) $|r|_p = 0$ *se, e somente se,* $r = 0$*;*

ii) $|r.s|_p = |r|_p.|s|_p$ *para todos* $r, s \in \mathbb{Q}$*;*

iii) $|r + s|_p \leq \max(|r|_p, |r|_s) \leq |r|_p + |r|_s$ *para todos* $r, s \in \mathbb{Q}$.

De fato. Para mostrar i), note que se $r = 0$*, segue imediatamente da definição que* $|r|_p = 0$*. Se* $|r|_p = 0$ *e* $r = p^m \frac{a}{b}$*, então* $p^{-m} = 0$ *se, e somente se,* $p = 0$*, portanto,* $r = 0$*. Para mostrar ii) e iii) , sejam* $r, s \in \mathbb{Q}$ *e escrevamos:*

$$r = p^m \frac{a}{b}, \ s = p^n \frac{c}{d},$$

com $m, n \in \mathbb{Z}$ *únicos,* $a, b, c, d \in \mathbb{Z}$ *não nulos tais que* p *não os divida. Sem perda de generalidade, suponha* $m \leq n$*. Temos:*

$$r \cdot s = p^m \frac{a}{b} \cdot p^n \frac{c}{d} = p^{m+n} \cdot \left(\frac{ac}{bd}\right).$$

Portanto $|r \cdot s|_p = p^{-(m+n)} = p^{-m} \cdot p^{-n} = |r|_p \cdot |s|_p$*, e assim, a propriedade ii) está demonstrada. Para iii), note que:*

$$r + s = p^m \frac{a}{b} + p^n \frac{c}{d} = p^m \left(\frac{a}{b} + p^{n-m} \frac{c}{d}\right) = p^m \left(\frac{ad + p^{n-m} bc}{bd}\right),$$

e então

$$|r + s|_p \leq p^{-m} = \max(|r|_p, |s|_p).$$

Como queríamos demonstrar.

Qualquer função sobre $\mathbb{Q}$ satisfazendo as propriedades *i), (ii)* e *iii)* do Exemplo 4.1.1, com pelo menos um valor diferente de 1 em $\mathbb{Q}^*$ é chamada de *valorização absoluta* em $\mathbb{Q}$.

Outra função sobre $\mathbb{Q}$ satisfazendo as propriedades *i), ii)* e *iii)* do Exemplo 4.1.1 é a função $|\ .\ | : \mathbb{Q} \to \mathbb{R}_{\geq 0}$, chamada *valorização absoluta ordinária* em $\mathbb{Q}$, definida por

$$|r| = \max\{r, -r\}.$$

Exemplo 4.1.2. *Para todo* $r \in \mathbb{Q}^*$*, temos*

$$|r| . \prod_p |r|_p = 1. \tag{11}$$

onde o produto anterior vale para todo números primo p.

De fato, considere $r \in \mathbb{Q}^*$. *Utilizando a decomposição em fatores primos, podemos escrever* r *na forma*

$$r = \pm p_1^{m_1} ... p_k^{m_k},$$

onde os p_i *são primos distintos e* $m_i \in \mathbb{Z}_+$, *com* $1 \leq i \leq k$. *Assim,* $|r|_{p_i} = p_i^{-m_i}$ *para* $1 \leq i \leq k$ *e* $|r|_p = 1$ *para os outros primos* p. *Logo:*

$$|r|. \prod_p |r|_p = p_1^{m_1} ... p_k^{m_k} p_1^{-m_1} ... p_k^{-m_k} = 1.$$

Portanto

$$|r|. \prod_p |r|_p = 1. \tag{12}$$

Vamos nos concentrar agora em $|\ .\ |_p$. Considere a função $\nu_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$, definida por

$$\nu_p(r) = \begin{cases} \infty & , \text{se } r = 0 \\ -\log_p |r|_p = m, & \text{se } r \neq 0 \end{cases}.$$

A função ν_p possui as seguintes propriedades:

i) $\nu_p(r) = \infty$ se, e somente se $r = 0$;

ii) $\nu_p(r.s) = \nu_p(r) + \nu_p(s)$ para todos $r, s \in \mathbb{Q}$;

iii) $\nu_p(r + s) \geq \min(\nu_p(r), \nu_p(s))$ para todos $r, s \in \mathbb{Q}$.

iv) $\nu_p(\mathbb{Q}^*) \neq \{0\}$.

De fato, note que pela definição, se $r = 0$, então $\nu_p(r) = \infty$ e, se $\nu_p(r) = \infty$, temos que $r = 0$. Portanto, a propriedade *i)* está provada. Para mostra *ii)*, sejam $r = ap^m$ e $s = bp^n$, com $mdc(a, p) = mdc(b, p) = 1$. Assim

$$r \cdot s = (ap^m)(bp^n) = (ab)p^{m+n}.$$

Logo, $\nu_p(r \cdot s) = m + n = \nu_p(r) + \nu_p(s)$. Para determinar $\nu_p(r + s)$, sejam $r = ap^m$ e $s = bp^n$, com $mdc(a, p) = mdc(b, p) = 1$, suponha, sem perda de generalidade, que

$n > m$. Temos

$$r + s = (ap^m) + (bp^n) = p^m(a + b^{n-m}) \Rightarrow \nu_p(r + s) = m \geq \min(\nu_p(r), \nu_p(s)).$$

Este exemplo dá origem à seguinte definição:

Definição 4.1.3. *Seja* K *um corpo arbitrário. Uma valorização (não arquimediana) de* K *é uma função* $\nu : K \longrightarrow \mathbb{R} \cup \{\infty\}$ *satisfazendo:*

i) $\nu(x) = \infty$ *se, e somente se,* $x = 0$*;*

ii) $\nu(x.y) = \nu(x) + \nu(y)$ *para todos* $x, y \in K$*;*

iii) $\nu(x + y) \geq \min(\nu(x), \nu(y))$ *para todos* $x, y \in K$.

iv) $\nu(K^*) \neq \{0\}$.

Se a imagem $\nu(K^*)$ é um conjunto discreto[10] em $\mathbb{R}$, então ν é chamada *valorização discreta*. Se $\nu(K^*) = \mathbb{Z}$, então ν é chamada *valorização normalizada*. O par ordenado (K, ν) é chamado de *corpo valorizado*. A propriedade *iv)* exclui o que é chamado de valorização trivial de K. A valorização ν_p é uma valorização normalizada de $\mathbb{Q}$.

Estaremos interessados apenas em valorizações discretas.

O próximo resultado mostra que qualquer valorização absoluta em $\mathbb{Q}$ é equivalente (no sentido de ser uma potência da ordem) à valorização absoluta ordinária ($|\ .\ |$) ou à valorização absoluta p-ádica ($|\ .\ |_p$), para algum primo p. A demonstração pode ser encontrada em Weiss (1998).

Teorema 4.1.1. *Toda valorização absoluta em* $\mathbb{Q}$ *é equivalente a exatamente uma das seguintes:*

i) a valorização absoluta ordinária;

ii) a valorização absoluta p*-ádica, com* p *primo.*

[10] Diz se que um ponto $a \in \mathbb{R}$ é um ponto de acumulação do conjunto $X \subset \mathbb{R}$ se para todo real $\epsilon > 0$ tem-se $(a - \epsilon, a + \epsilon) \cap (X - \{a\}) \neq \varnothing$. Se $a \in X$ não é um ponto de acumulação de X, diz-se que a é um **ponto isolado** de X. Quando todos os pontos de X são isolados, X chama-se um **conjunto discreto**. Lima (2004)

Lema 4.1.4. *Seja* (K, ν) *um corpo valorizado. Temos:*

i) $\nu(1) = \nu(-1) = 0$*;*

ii) $\nu(-x) = \nu(x)$ *para todo* $x \in K$*;*

iii) $\nu(xy^{-1}) = \nu(x) - \nu(y)$ *para todos* $x, y \in K$

Demonstração:

i) $1^2 = 1 \Rightarrow \nu(1^2) = \nu(1) \Rightarrow \nu(1 \cdot 1) = \nu(1) \Rightarrow \nu(1) + \nu(1) = \nu(1) \Rightarrow 2\nu(1) = \nu(1) \Rightarrow \nu(1) = 0$.

E $(-1)^2 = 1 \Rightarrow \nu((-1)^2) = \nu(1) \Rightarrow \nu((-1) \cdot (-1)) = \nu(1) \Rightarrow \nu(-1) + \nu(-1) = \nu(1) \Rightarrow 2\nu(-1) = \nu(1) \Rightarrow \nu(-1) = 0$.

Nos dois casos usamos a propriedade *ii)* da Definição 4.1.3.

ii) $\nu(-x) = \nu((-1)x) = \nu(-1)\nu(x) = 0 + \nu(x) = \nu(x)$.

Usamos novamente a propriedade *ii)* da Definição 4.1.3 e o resultado anterior.

iii) $0 = \nu(1) = \nu(yy^{-1}) = \nu(y) + \nu(y^{-1}) \Rightarrow \nu(y^{-1}) = -\nu(y)$. Portanto, $\nu(xy^{-1}) = \nu(x) + \nu(y^{-1}) = \nu(x) - \nu(y)$.

Usamos novamente a propriedade *ii)*da Definição 4.1.3 e o resultado do item *i)*.

□

Proposição 4.1.5. ***(Desigualdade Triangular Estrita)*** *Seja* (K, ν) *um corpo valorizado. Se* $x, y \in K$ *com* $\nu(x) \neq \nu(y)$*, então*

$$\nu(x + y) = \min(\nu(x), \nu(y)).$$

Demonstração. Suponha, sem perda de generalidade, que $\nu(x) < \nu(y)$. Então, pela Propriedade (iii) da Definição 4.1.3 temos $\nu(x + y) \geq \min(\nu(x), \nu(y)) = \nu(x)$. Se tivéssemos $\nu(x + y) > \nu(x)$, então pela mesma propriedade e pelo Lema 4.1.4 (ii),

$$\nu(x) = \nu((x + y) - y) \geq \min(\nu(x + y), \nu(-y)) = \min(\nu(x + y), \nu(y)) > \nu(x),$$

o que é uma contradição. □

O próximo exemplo ilustra a Proposição 4.1.5.

Exemplo 4.1.6. *Seja* $K = \mathbb{Q}$ *e* ν *a valorização p-ádica de* $\mathbb{Q}$. *Tome* $x, y \in \mathbb{Z}$ *não nulos. Então podemos escrever* $x = p^m a$ *e* $y = p^n c$, *onde* a *e* b *não são divisíveis por* p. *Suponha que* $\nu(x) = m < \nu(y) = n$. *Então:*

$$x + y = p^m a + p^n c = p^m(a + p^{n-m}c),$$

com $a + p^{n-m}c \equiv a \not\equiv 0 \mod p$. *Portanto,* $\nu(x + y) = m = \min(\nu(x), \nu(y))$.

4.2 Lugares e Anéis de Valorização

Todas as valorizações apresentadas nesta seção são discretas.

Definição 4.2.1. *Duas valorizações* ν *e* μ *de um corpo* K *são chamadas equivalentes se existe uma constante* $c > 0$ *tal que:*

$$\nu(x) = c\mu(x), \text{ para todo } x \in K.$$

A equivalência entre duas valorizações apresentada na Definição 4.2.1 gera uma relação de equivalência entre as valorizações de K. Uma classe de equivalência de valorizações de K é chamada de ***lugar*** de K.

Se $\nu(K^*)$ é um subgrupo discreto[11] diferente de zero de $(\mathbb{R}, +)$, temos que $\nu(K^*) = \alpha\mathbb{Z} = \{\alpha \cdot n; n \in \mathbb{Z}\}$ para algum $\alpha \in \mathbb{R}$ positivo. Portanto, existe uma valorização normalizada de K que é equivalente a valorização ν. Todo lugar $\mathbb{P}$ de K contém uma única valorização normalizada de K que é indicada por $\nu_{\mathbb{P}}$. Assim, podemos identificar os lugares de K e as valorizações normalizadas (discretas) de K.

Definição 4.2.2. *Seja* $\mathbb{P}$ *um lugar de* K. *Então, o conjunto*

$$O_{\mathbb{P}} := \{x \in K; \nu_{\mathbb{P}}(x) \geq 0\}$$

é chamado de anel das valorizações de $\mathbb{P}$.

[11] Seja $(G, +)$ um grupo. Diz-se que um conjunto $H \subset G$ é um subgrupo de G se, com relação a operação $+$ em G, o próprio H é um grupo. Se H é um conjunto discreto, então $(H, +)$ será um subgrupo discreto

Usando as propriedades das valorizações da Seção 4.1, podemos mostrar que $O_{\mathbb{P}}$ é um domínio de integridade com $1 \in O_{\mathbb{P}}$. De fato, do item *i)* do Lema 4.1.1, temos que $\nu(1) = 0$, portanto $1 \in O_{\mathbb{P}}$. Tome agora $x, y \in O_{\mathbb{P}}$. Note que $\nu(x \cdot y) = \nu(x) + \nu(y) \geq 0$. Portanto $x \cdot y \in O_{\mathbb{P}}$. Como $x \cdot y \in K$ e K é um corpo, se$x \cdot y = 0$, então $x = 0$ ou $y = 0$, e assim $O_{\mathbb{P}}$ é um domínio de integridade.

Proposição 4.2.3. *O grupo multiplicativo das unidades de* $O_{\mathbb{P}}$ *é dado por*

$$U_{\mathbb{P}} := \{x \in K; \nu_{\mathbb{P}}(x) = 0\}.$$

Demonstração: Considere $x \in O_{\mathbb{P}}$. Temos que x é uma unidade de $O_{\mathbb{P}}$ se, e somente se, $x^{-1} \in O_{\mathbb{P}}$ se, e somente se, $\nu_{\mathbb{P}}(x^{-1}) \geq 0$ se, e somente se, $\nu_{\mathbb{P}}(x) \geq 0$ se, e somente se, $\nu_{\mathbb{P}}(x) \leq 0$ se, e somente se, $\nu_{\mathbb{P}}(x) = 0$. □

Proposição 4.2.4. $O_{\mathbb{P}}$ *possui um único ideal maximal dado por*

$$M_{\mathbb{P}} := \{x \in K; \nu_{\mathbb{P}}(x) > 0\}.$$

Demonstração: $M_{\mathbb{P}}$ é um ideal de $O_{\mathbb{P}}$. De fato, dados $x, y \in M_{\mathbb{P}}$, temos que $\nu_{\mathbb{P}}(x - y) = \nu_{\mathbb{P}}(x + (-y)) = \nu_{\mathbb{P}}(x) + \nu_{\mathbb{P}}(-y) = \nu_{\mathbb{P}}(x) + \nu_{\mathbb{P}}(y) \geq \min(\nu_{\mathbb{P}}(x), \nu_{\mathbb{P}}(y)) > 0$. Portanto, $x - y \in M_{\mathbb{P}}$. Além disso, dados $r \in O_{\mathbb{P}}$ e $x \in M_{\mathbb{P}}$, temos $\nu_{\mathbb{P}}(r \cdot x) = \nu_{\mathbb{P}}(r) + \nu_{\mathbb{P}}(x) > 0$ e $\nu_{\mathbb{P}}(x \cdot r) = \nu_{\mathbb{P}}(x) + \nu_{\mathbb{P}}(r) > 0$. Logo, $r \cdot x, x \cdot r \in M_{\mathbb{P}}$. Portanto, $M_{\mathbb{P}}$ é um ideal de $O_{\mathbb{P}}$.

Vamos mostrar agora que $M_{\mathbb{P}}$ é maximal. Considere o conjunto J com $M_{\mathbb{P}} \subset J \subseteq O_{\mathbb{P}}$, um ideal de $O_{\mathbb{P}}$. Tome $x \in J \setminus M_{\mathbb{P}}$, então $\nu_{\mathbb{P}}(x) = 0$ e x é uma unidade de $O_{\mathbb{P}}$ pela Proposição 4.2.3. Portanto, $1 = x.x^{-1} \in J$, e consequentemente $J = O_{\mathbb{P}}$, e então $M_{\mathbb{P}}$ é um ideal maximal. Finalmente, seja $M \subset O_{\mathbb{P}}$ um ideal maximal arbitrário de $O_{\mathbb{P}}$. Como M não pode conter a unidade de $O_{\mathbb{P}}$, devemos ter $M \subseteq M_{\mathbb{P}}$, e então $M = M_{\mathbb{P}}$.

$M_{\mathbb{P}}$ é de fato um ideal principal: tome $t \in O_{\mathbb{P}}$ com $\nu_{\mathbb{P}}(t) = 1$, então é fácil verificar que $M_{\mathbb{P}} = tO_{\mathbb{P}}$. O número t é chamado de *parâmetro local* de $\mathbb{P}$. □

Definição 4.2.5. *O corpo* $O_{\mathbb{P}}/M_{\mathbb{P}}$ *é chamado de corpo das classes residuais de* $\mathbb{P}$. *O homomorfismo de anéis dado por*

$$\begin{aligned} O_{\mathbb{P}} &\to O_{\mathbb{P}}/M_{\mathbb{P}} \\ x &\mapsto x + M_{\mathbb{P}} \end{aligned}$$

é chamado de função das classes residuais de $\mathbb{P}$.

Exemplo 4.2.6. *Seja* ν_p *a valorização p-ádica de* $\mathbb{Q}$*, que é uma valorização normalizada de* $\mathbb{Q}$*(ver seção 4.1). Escrevendo todos os números racionais na forma* $\frac{a}{b}$*, com* $mdc(a,b) = 1$*. Verificamos que:*

$$\begin{aligned} O_p &= \left\{\frac{a}{b} \in \mathbb{Q}; mdc(b,p) = 1\right\}, \\ U_p &= \left\{\frac{a}{b} \in \mathbb{Q}; mdc(a,p) = mdc(b,p) = 1\right\}, \\ M_p &= \left\{\frac{a}{b} \in \mathbb{Q}; p|a\right\}. \end{aligned}$$

Para qualquer $b \in \mathbb{Z}$, podemos escrever a classe residual módulo b. Se $mdc(b,p) = 1$, então $b \in \mathbb{Z}/p\mathbb{Z}$ possui inverso multiplicativo $b^{-1} \in \mathbb{Z}/p\mathbb{Z}$. A função $\psi : O_P \to \mathbb{Z}/p\mathbb{Z}$ dada por

$$\psi\left(\frac{a}{b}\right) = \bar{a}.\bar{b}^{-1} \in \mathbb{Z}_p \text{ para todo } \frac{a}{b} \in O_p$$

está bem definida. Claramente, ψ é um homomorfismo de anel sobrejetivo cujo núcleo é M_p, e assim, o corpo das classes residuais O_p/M_p é isomorfo ao corpo finito $\mathbb{Z}/p\mathbb{Z}$.

Teorema 4.2.1. *(Teorema da Aproximação Fraca) Sejam* $P_1, \ldots, P_n$ *lugares de* K *dois a dois distintos,* $x_1, \ldots, x_n \in K$ *e* $m_1, \ldots, m_n \in \mathbb{Z}$*. Então existe* $x \in K$ *tal que*

$$\nu_{P_i}(x - x_i) \geq m_i$$

para $i = 1, \ldots, n$*.*

No próximo exemplo, ilustraremos a utilização do Teorema da Aproximação Fraca.

Exemplo 4.2.7. *Seja* $K = \mathbb{Q}$. *Escolher* n *lugares distintos de* K *significa escolher* n *números primos distintos* $p_1, \ldots, p_n$. *Sejam* $x_1, \ldots, x_n \in \mathbb{Z}$ *e tome os inteiros positivos* $m_1, \ldots, m_n$. *Pelo Teorema Chinês dos Restos*[12], *existe* $x \in \mathbb{Z}$ *tal que*

$$x \equiv x_i \mod p_i^{m_i} \Rightarrow p_i^{m_i} = (x - x_i) \cdot k, \text{ com } k \in \mathbb{Z}.$$

Isso significa que

$$\nu_{p_i}(x - x_i) \geq m_i.$$

Assim, o Teorema da Aproximação Fraca pode ser visto como um análogo do Teorema Chinês dos Restos para um corpo K.

4.3 Corpo das Funções Racionais

Nesta seção, abordaremos os conceitos de valorização e lugares no corpo das funções racionais, o que nos ajudará a compreender esses mesmos conceitos em corpos de funções arbitrários.

Seja K um corpo arbitrário e tome $K(x)$ o corpo das funções racionais sobre K na variável x (em termos algébricos rigorosos, x é transcendente sobre K). Nesse contexto, K é chamado de *corpo das constantes de* $K(x)$. Podemos representar os elementos de $K(x)$ pelo conjunto

$$K(x) = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], g(x) \neq 0, \text{ e } mdc(g(x), f(x)) = 1 \right\}.$$

As valorizações de $K(x)$ podem ser construídas de maneira análogas às de $\mathbb{Q}$. O papel dos números primos agora é desempenhado pelos polinômios mônicos irredutíveis. Fixando um polinômio mônico irredutível $p(x) \in K[x]$ e utilizando a decomposição em

[12](Teorema Chinês dos Restos) Seja r um inteiro positivo, sejam $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_r \in \mathbb{Z}$ e $m_1, m_2, \ldots, m_r$ inteiros maiores que 1. Suponhamos que $mdc(a_i, m_i) = 1$ para todo $1 \leq i \leq r$, e $mdc(m_i, m_j) = 1$ para todos $i \leq i, j \leq r, i \neq j$. Então o sistema de conguências

$$\begin{cases} a_1 x \equiv b_1 \mod m_1 \\ a_2 x \equiv b_2 \mod m_2 \\ \vdots \\ a_r x \equiv b_r \mod m_r \end{cases}$$

possui uma única solção módulo m, onde $m = m_1 m_2 \ldots m_r$. Silva e Gomes (2018)

fatores primos em $K[x]$, podemos escrever todo $r(x) \in K[x]$ não nulo na forma

$$r(x) = p(x)^m \frac{f(x)}{g(x)},$$

com $m \in \mathbb{Z}$ único, $p(x) \neq 0$ e $mdc(p(x), g(x)) = mdc(p(x), f(x)) = 1$. A função $\nu_{p(x)} : K(x) \to \mathbb{Z} \cup \{\infty\}$, definida por

$$\nu_{p(x)}(r(x)) = \begin{cases} \infty, & \text{se } r = 0 \\ m, & \text{se } r \neq 0 \end{cases},$$

é uma valorização normalizada (discreta) de $K(x)$.

Existe outra valorização normalizada de $K(x)$ definida através do grau do polinômio $r(x) \in K(x)$. Se $r(x) = \dfrac{f(x)}{g(x)} \neq 0$, definimos

$$\nu_\infty(r(x)) = gr(g(x)) - gr(f(x)).$$

Definimos também que $\nu_\infty(0) = \infty$.

Proposição 4.3.1. *Considere a função* $\nu_\infty : K(x) \to \mathbb{Z} \cup \{\infty\}$*, definida por:*

$$\nu_\infty(r(x)) = \begin{cases} \infty & , \textit{se } r(x) = 0 \\ gr(g(x)) - gr(f(x)) & , \textit{se } r(x) \neq 0 \end{cases}.$$

Temos que ν_∞ *é uma valorização normalizada de* $K(x)$.

Demonstração: De fato, as propriedades *i)* e *iv)* da Definição 4.1.3 são triviais. A propriedade *ii)* segue do fato que $gr(gh) = gr(g) + gr(h)$ para todos $g, h \in K[x]$. Para

provar *iii)* , temos

$$\begin{aligned}
\nu_\infty\left(\frac{f}{g}+\frac{e}{h}\right) &= \nu_\infty\left(\frac{fh+eg}{gh}\right) \\
&= gr(gh)-gr(fh+eg) \\
&\geq gr(gh)-\max(gr(fh),gr(eg)) \\
&= \min(gr(gh)-gr(fh),gr(gh)-gr(eg)) \\
&= \min(gr(g)-gr(f),gr(h)-gr(e)) \\
&= \min\left(\nu_\infty\left(\frac{f}{g}\right),\nu_\infty\left(\frac{e}{h}\right)\right).
\end{aligned} \tag{13}$$

Portanto, ν_∞ é uma valorização normalizada de $K(x)$ □

As valorizações $\nu_{p(x)}$, com $p(x) \in K[x]$ mônico e irredutível, e ν_∞ serão pares não equivalentes desde que $\nu_{p(x)}(p(x)) = 1$, e $\nu_{q(x)}(p(x)) = 0$, sendo $q(x) \neq p(x)$ um polinômio mônico irredutível e $\nu_\infty(p(x)) < 0$. Assim, o conjunto

$$\{p(x) \in K[x]; p(x) \text{é mônico irredutível}\} \cup \{\infty\}$$

é o conjunto de lugares de $K(x)$.

Observação 2. *Se o corpo K é algebricamente fechado, então os polinômios mônicos e irredutíveis sobre K são exatamente os polinômios lineares $x-a$ com $a \in K$. Assim, o conjunto dos lugares descritos acima pode ser identificado como $K \cup \{\infty\}$. Se $K = \mathbb{C}$, então isso produz o plano complexo com pontos em ∞, ou seja, a esfera de Riemann. Portanto, o conjunto dos lugares $\mathbb{C}(x)$ acima está em correspondência biunívoca com ou pontos (ou lugares) da esfera de Riemann* [13]*. Isso explica a origem histórica do termo "lugar".*

Assumiremos, a partir de agora, que o corpo das constantes K é **finito**, embora alguns resultados sejam válidos para K arbitrário.

Lema 4.3.2. *Se K é finito, então para qualquer valorização ν de $K(x)$, temos $\nu(a) = 0$ para todo $a \in K^*$.*

[13] Seja o pano complexo completado, definido por $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. A função $P : S^2 \to \widehat{\mathbb{C}}$, onde $S^2 = \{(x,y,z); x^2+y^2+z^2 = 1\}$ é tal que $P(v) = P(x,y,x) = \frac{x}{1-z} + \frac{y}{1-z}i$ para todo $v \in S^2 \setminus (0,0,1)$, permite identificar $\widehat{\mathbb{C}}$ como a esfera unitária, também conhecido como *esfera de Riemann.* Hefez e Villela (2012).

Demonstração: Se $K = \mathbb{F}_q$, com q primo, temos $a^{q-1} = 1$ para todo $a \in \mathbb{F}_q$. Utilizando o Lema 4.1.4, temos

$$0 = \nu(1) = \nu(a^{q-1}) = (q-1)\nu(a).$$

Portanto, $\nu(a) = 0$. □

Teorema 4.3.1. *Se K é finito, então o conjunto de lugares de $K(x)$ é dado por*

$$\{p(x) \in K[x]; p(x) \textit{é mônico irredutível}\} \cup \{\infty\}.$$

Demonstração: Precisamos mostrar que se $\mathbb{P}$ é um lugar de $K(x)$ e $\nu \in \mathbb{P}$, então ν é equivalente a $\nu_{p(x)}$ ou a ν_∞. Vamos considerar dois casos.

Caso 1: $\nu(x) \geq 0$. Pelo Lema 4.3.2, $K[x] \subseteq O_P$. Se $\nu(K(x))^* \neq \{0\}$, então pela definição, existe $h(x) \in K[x]$ com $\nu(h(x)) > 0$. Seja $J := K[x] \cap M_P$ é um ideal primo de $K[x]$ diferente de zero. Se $1 \notin J$, temos $J \neq K[x]$. Se $M_{\mathbb{P}}$ é um ideal primo de $O_{\mathbb{P}}$, então J é um ideal primo de $K[x]$. Consequentemente, existe um polinômio mônico irredutível $p(x) \in K[x]$ de tal modo que $J = (p(x))$. Seja $c := \nu(p(x)) > 0$. Se $g(x) \in K[x]$ não é divisível por $p(x)$, então $g(x) \notin M_{\mathbb{P}}$ e então $\nu(g(x)) = 0$. Assim, escrevendo $r(x) \in K[x]$ não nulo na forma

$$r(x) = p(x)^m \frac{f(x)}{g(x)}$$

com $f(x)$ e $g(x)$ não divisíveis por $p(x)$. Então

$$\nu(r(x)) = m\nu(p(x)) = mc = c\nu_{p(x)}(r(x))$$

e, assim, ν é equivalente a $\nu_{p(x)}$.

Caso 2: $\nu(x) < 0$. Seja $c := \nu(x^{-1}) > 0$ e $x^{-1} \in M_P$. Tome qualquer $f(x) \in K[x]$

não nulo de grau $d \neq 0$. Então

$$\begin{aligned} f(x) &= \sum_{i=0}^{d} a_i x^i \\ &= x^d \sum_{i=0}^{d} a_i x^{i-d} \\ &= x^d \sum_{i=0}^{d} a_{d-i} x^{-i} \end{aligned}$$

com $a_i \in K$. Além disso,

$$\sum_{i=0}^{d} a_{d-i} x^{-i} = a_d + \sum_{i=1}^{d} a_{d-i} x^{-i} = a_d + s(x)$$

com $s(x) \in M_{\mathbb{P}}$. Se $a_d \neq 0$, temos $\nu(a_d) = 0$, e então

$$\nu\left(\sum_{i=0}^{d} a_{d-i} x^{-i}\right) = 0,$$

pela Proposição 4.1.5. Segue que

$$\nu(f(x)) = \nu(x^d) = -d\nu(x^{-1}) = c\nu_\infty(f(x))$$

e, assim, ν é equivalente a ν_∞. □

Observação 3. *Note que na prova do Teorema 4.3.1 não usamos o fato de que ν é discreto. Portanto, a prova mostra que toda valorização de $K(x)$ é automaticamente discreta.*

Os lugares $p(x)$ são chamados de *lugares finitos* de $K(x)$ e os lugares ∞ são chamados de *lugares infinitos* de $K(x)$.

Exemplo 4.3.3. *No Exemplo 4.2.6 mostramos que o anel das classes residuais dos*

lugares $p(x)$ *são isomorfos a* $K[x]/p(x)$. *Para o lugar* ∞, *temos:*

$$\begin{aligned} O_\infty &= \left\{ \frac{f(x)}{g(x)} \in K(x); gr(f(x)) \leq gr(g(x)) \right\}, \\ U_\infty &= \left\{ \frac{f(x)}{g(x)} \in K(x); gr(f(x)) = gr(g(x)) \right\}, \\ M_\infty &= \left\{ \frac{f(x)}{g(x)} \in K(x); gr(f(x)) < gr(g(x)) \right\}. \end{aligned}$$

De fato, considere $r(x) = \dfrac{f(x)}{g(x)} \neq 0$,

- $r(x) = \dfrac{f(x)}{g(x)} \in O_\infty \Leftrightarrow \nu_\infty(r(x)) \geq 0 \Leftrightarrow gr(g(x)) - gr(f(x)) \geq 0 \Leftrightarrow gr(f(x)) \leq gr(g(x))$.
- $r(x) = \dfrac{f(x)}{g(x)} \in U_\infty \Leftrightarrow \nu_\infty(r(x)) = 0 \Leftrightarrow gr(g(x)) - gr(f(x)) = 0 \Leftrightarrow gr(f(x)) = gr(g(x))$.
- $r(x) = \dfrac{f(x)}{g(x)} \in M_\infty \Leftrightarrow \nu_\infty(r(x)) > 0 \Leftrightarrow gr(g(x)) - gr(f(x)) > 0 \Leftrightarrow gr(f(x)) < gr(g(x))$.

Todo $r(x) \in O_\infty$ pode ser escrito na forma

$$r(x) = \frac{a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0}{x^d + b_{d-1} x^{d-1} + \cdots + b_0}$$

com $a_i, b_i \in K$. A função $\psi : O_\infty \to K$ dada por

$$\psi(r(x)) = a_d \in K, \text{para todo } r(x) \in O_\infty$$

está bem definida. É fácil ver que ψ é um homomorfismo de anel sobrejetivo com núcleo M_∞, e portanto o corpo das classes residuais dos lugares ∞ é isomorfo a K.

Observação 4. *Para todo* $r(x) \in K(x)$ *não nulo, temos:*

$$\nu_\infty(r(x)) + \sum_{p(x)} \nu_{p(x)}(r(x)) gr(p(x)) = 0,$$

onde a soma é dada sobre todos os polinômios mônicos irredutíveis $p(x) \in K[x]$. *Observe que a soma faz sentido pois* $\nu_{p(x)}(r(x)) = 0$ *para um número finito de* $p(x)$. *Devido às propriedades das valorizações, basta verificar a fórmula para os polinômios mônicos* $f(x) \in K[x]$ *não nulos. Se*

$$f(x) = \prod_{i}^{n} p_i(x)^{m_i}$$

é a fatoração canônica de $f(x) \in K[x]$, *então*

$$\sum_{p(x)} \nu_{p(x)}(f(x))gr(p(x)) = \sum_{i=1}^{n} m_i gr(p_i(x)) = gr(f(X)) = -\nu_\infty(f(x)).$$

Essa fórmula é um análogo aditivo da equação (12) para $\mathbb{Q}$. *(Ver início da Seção 4.1).*

4.4 Corpo das Funções Algébricas e suas Valorizações

A seguir, definiremos o corpo das funções algébricas sobre um corpo K (finito).

Definição 4.4.1. *Um corpo* F *é um* ***corpo de funções algébricas*** *sobre o corpo finito* K *se existe um elemento transcendente* $z \in F$ *sobre* K, *de modo que* F *é uma extensão finita sobre o corpo das funções racionais* $K(z)$.

O exemplo mais simples de um corpo de funções algébricas é o corpo das funções racionais sobre um corpo finito.

Proposição 4.4.2. *Toda valorização de um corpo de funções algébricas é discreta.*

Demonstração: Seja F um corpo de funções algébricas. Com a notação da Definição 4.4.1, coloque $K(z) = K$. Seja ν uma valorização arbitrária de F e μ a restrição de ν a K. É suficiente mostrar que o índice $[\nu(F^*) : \mu(K^*)]$ é finito. Já que $\nu(F^*)$ é um subgrupo finito de $(\mathbb{R}, +)$, basta mostra que $\mu(K^*) = \{0\}$ não é possível. Como μ é uma valorização de K, então, pela Observação 3 será discreto e, então, ν será discreta.

Tome $x_1, ..., x_n \in F^*$ tais que $\nu(x_1), ..., \nu(x_n)$ sejam conjuntos distintos módulo $\nu(K^*)$. Afirmamos que $x_1, ..., x_n$ são linearmente independentes sobre K. Isso irá monstra que

$$[\nu(F^*) : \mu(K^*)] \leq [F : K] < \infty.$$

Então, suponhamos que

$$\sum_{i}^{n} b_i x_i = 0,$$

sem perda de generalidade, suponhamos que $b_i \in K^*$. Se tivéssemos $v(b_i x_i) = v(b_j x_j)$ para algum $i \neq j$, então

$$\begin{aligned} 0 &= v(b_i x_i) - v(b_j x_j) \Rightarrow \\ 0 &= v(b_i) + v(x_i) - v(b_j) - v(x_j) \Rightarrow \\ v(x_i) - v(x_j) &= v(b_j) - v(b_i) = v(b_j b_i^{-1}) \in \mu(K^*), \end{aligned}$$

uma contradição com a escolha de $x_1, ..., x_n$. Portanto, $v(b_1 x_1), ..., v(b_n x_n)$ são todos distintos e pela Proposição 4.1.5 produz

$$\infty = v\left(\sum_{i=1}^{n} b_i x_i\right) = \min_{1 \leq i \leq n} v(b_i x_i).$$

Isso mostra que $b_i x_i = 0$ para $1 \leq i \leq n$, novamente uma contradição. □

Na prova acima, mostramos em particular, que a restrição de uma valorização de F a $K(z)$ produz uma valorização de $K(z)$. Para valorizações equivalentes de F, as restrições também serão equivalentes. Assim, um lugar Q de F corresponde de uma única restrição P de $K(z)$. Dizemos que Q *está sobre* P ou que P *está abaixo* Q. Portanto, todo lugar de F está sobre um lugar de $K(z)$ correspondente a um polinômio mônico irredutível em $K[z]$ ou sobre un lugar infinito de $K(z)$.

Proposição 4.4.3. *Seja F um corpo de funções algébricas sobre K. Então o corpo das classes residuais de todo lugar de F é uma extensão finita (uma cópia isomorfa) de K.*

Demonstração: Seja Q um lugar de F que se encontra sobre o lugar P de $K := K(z)$(com z como na Definição 4.4.1). Sejam $R_Q := O_Q/M_Q$ e $R_P := O_P/M_P$ os corpos das classes residuais correspondente e note que $O_P \subseteq O_Q$. A função $\rho : R_P \to R_Q$ dada por

$$\rho(b + M_P) = b + M_Q \text{ para todo } b \in O_P$$

está bem definida, desde que $M_P \subseteq M_Q$. É claro que ρ é um homomorfismo de anéis injetor, e então R_Q contém a cópia isomorfa $\rho(R_P)$ de R_P como um subcorpo.

Tome $x_1, \ldots, x_n \in O_Q$ tais que $x_1 + M_Q, \ldots, x_n + M_Q$ são linearmente independentes sobre $\rho(R_P)$. Afirmamos que $x_1, ..., x_n$ são linearmente independentes sobre K, isso irá mostrar que

$$[R_Q : \rho(R_P)] \leq [F : K] < \infty.$$

Desde que R_P seja uma extensão finita (de uma cópia isomorfa) de K (ver Exemplo 4.3.3), isso prova a proposição. Então, suponha que tenhamos

$$\sum_{i=1}^{n} b_i x_i = 0,$$

com $b_1, \ldots, b_n \in K$ não todos nulos. Sem perda de generalidade, suponha

$$\nu_P(b_1) = \min_{1 \leq i \leq n} \nu_P(b_i).$$

Então $b_1 \neq 0$ e

$$x_1 + \sum_{i=2}^{n} b_i b_1^{-1} x_i = 0.$$

Pela condição em $\nu_P(b_1)$ temos $b_i b_1^{-1} \in O_P$ para $2 \leq i \leq n$. Passando para a classe residual módulo M_Q temos

$$(x_1 + M_Q) + \sum_{i=2}^{n} \rho(b_i b_1^{-1} + M_P)(x_i + M_Q) = 0 + M_Q,$$

uma contradição para as escolha de $x_1, ..., x_n$. □

O resultado a seguir, mostra que toda valorização de um corpo de funções racionais sobre K pode ser estendida a uma valorização sobre um corpo de funções algébricas sobre K.

Teorema 4.4.1. *Seja F uma extensão finita do corpo de funções racionais $K(z)$. Então todo lugar de $K(z)$ fica abaixo de pelo menos um e no máximo $[F : K(z)]$ lugares de F.*

Seja F novamente um corpo de funções algébricas sobre o corpo finito K. Seja $\tilde{K}$ é

o fecho algébrico de K em F, ou seja,

$$\tilde{K} = \{x \in F; x \text{ é algébrico sobre } K\}.$$

Claramente $\tilde{K}$ é um corpo com $K \subseteqq \tilde{K} \subseteqq F$. O espaço $\tilde{K}$ é chamado de *corpo completo das constantes* de F. O seguinte resultado mostra que $\tilde{K}$ é novamente um corpo finito.

Proposição 4.4.4. *O corpo $\tilde{K}$ é uma extensão finita de K.*

Demonstração: Pelo Teorema 4.4.1 existe um lugar Q de F. Tome um $x \in \tilde{K}^*$. Por meio de seu polinômio minimal sobre K obtemos

$$x^d + c_{d-1}x^{d-1} + \cdots + c_0 = 0$$

com $c_0, \ldots, c_{d-1} \in K$ e $c_0 \neq 0$. Se tivéssemos $\nu_Q(x) < 0$, então

$$\nu_Q(x^d + c_{d-1}x^{d-1} + \cdots + c_0) = \nu_Q(x_d) < 0$$

pela Proposição 4.1.5, uma contradição. Se tivéssemos $\nu_Q(x) > 0$, então

$$\nu_Q(x^d + c_{d-1}x^{d-1} + \cdots + c_0) = \nu_Q(c_0) = 0$$

pela Proposição 4.1.5, novamente uma contradição. Assim, devemos ter $\nu_Q(x) = 0$. Considerando agora a função $\psi : \tilde{K} \to R_Q := O_Q/M_Q$ dada por

$$\psi(x) = x + M_Q, \text{ para todo} x \in \tilde{K}.$$

As considerações acima, mostram que ψ é injetiva, e pela Proposição 4.4.3, temos $|\tilde{K}| \leq |R_Q| < \infty$. □

Observe que $K(z) \subseteq \tilde{K}(z) \subseteq F$, e então F é uma extensão finita de $\tilde{K}(z)$. Além disso, z é transcendente sobre $\tilde{K}(z)$ pela Proposição 4.4.4, e então F também é um corpo de funções algébricas sobre K. Na sequência, assumiremos que K é o corpo completo de constantes de F. Se quisermos enfatizar isso, usamos a notação F/K para um corpo de funções algébricas com corpo completo de constantes K.

Em vista da Proposição 4.4.3, a seguinte definição faz sentido.

Definição 4.4.5. *O grau* $\deg(\mathbb{P})$ *do lugar* $\mathbb{P}$ *de* F/K *é definido como o grau das classes residuais de* P *sobre* K. *O lugar de* F/K *de grau* 1 *e comumente chamado de lugar racional de* F/K.

Exemplo 4.4.6. *Tome* $F = K(x)$ *o corpo das funções racionais sobre* K. *Para quaisquer funções racionais não constantes* $r(x) \in F$, *existe um lugar finito* P *de* F *tal que* $v_P(r(x)) \neq 0$. *Portanto, pela demonstração da Proposição 4.4.4, o corpo completo de constantes de* F *é* K. *Pelo Exemplo 4.3.3 o grau de um lugar finito* $p(x)$ *de* F *é igual ao grau do polinômio* $p(x)$ *e o grau do lugar* ∞ *de* F *é igual a* 1. *Se* $K = \mathbb{F}_q$, *então* F *tem exatamente* $q + 1$ *lugares racionais.*

Para um corpo de funções algébricas F/K, denotamos por $\mathbb{P}_F$ o conjunto de todos os lugares de F. Note que $\mathbb{P}_F$ é um conjunto enumerável. O resultado a seguir é um fortalecimento do Teorema 4.2.1, O Teorema da Aproximação Forte (também conhecido como Teorema da Independência), é o mais importante desta seção, e diz o seguinte: se $v_1, \ldots, v_n$ são valorizações duas a duas disntintas de um corpo K e $z \in K$, e se conhecemos as valorizações $v_1(z), \ldots, v_{n-1}(z)$, então nada podemos concluir sobre $v_n(z)$

Teorema 4.4.2 (Teorema da Aproximação Forte)**.** *Sejam* $S \subsetneq \mathbb{P}_F$ *subconjunto próprio de* $\mathbb{P}_F$ *e* $P_1, \ldots, P_r \in S$. *Suponha dados os elementos* $x_1, \ldots, x_r \in F$ *e inteiros* $n_1, \ldots, n_r$. *Então, existe um elemento* $x \in F$ *tal que:*

1. $v_{P_i}(x - x_i) = n_i, i = 1, \ldots r$;
2. $v_P(x) \geq 0$, *para todo* $P \in S \backslash \{P_1, \ldots, P_n\}$.

Demonstração: A demonstração desse resultado será feita em algumas etapas. Com o intuito de simplificar a notação, escrevamos $v_i = v_{P_i}$.

Etapa 1. Existe $u \in K$ tal que $v_1(u) > 0$ e $v_i(u) < 0$, para $i = 2, \cdots, n$.

Prova da Etapa 1.

Façamos a demonstração por indução. Para $n = 2$, observemos que $O_{P_1} \nsubseteq O_{P_2}$ e $O_{P_2} \nsubseteq O_{P_1}$, já que anéis de valorização são subanéis próprios maximais de K, pela Proposição 4.2.4. Deste modo, podemos encontrar $y_1 \in O_{P_1} \setminus O_{P_2}$ e $y_2 \in O_{P_2} \setminus O_{P_1}$, de modo que $v_1(y_1) \geq 0$, $v_2(y_1) < 0$, $v_1(y_2) < 0$ e $v_2(y_2) \geq 0$.

O elemento $u = y_1/y_2$ possui a propriedade que desejamos, pois

$$v_1(u) = v_1(y_1) + v_1(y_2^{-1}) = v_1(y_1) - v_1(y_2) > 0$$

e

$$v_2(u) = v_2(y_1) + v_2(y_2^{-1}) = v_2(y_1) - v_2(y_2) < 0.$$

Para $n > 2$, temos pela hipótese de indução, que existe um elemento y com $v_1(y) > 0, v_2(y) < 0, \ldots, v_{n-1}(y) < 0$. Se $v_n(y) < 0$, então a demonstração termina considerando $u = y$. Caso contrário, isto é, se $v_n(y) \geq 0$, escolhemos z tal que $v_1(z) > 0$ e $v_n(z) < 0$ e escrevemos $u = y + z^r$, onde $r \geq 1$ é escolhido de modo que $rv_i(z) \neq v_i(y)$, para $i = 1, \ldots, n-1$. Daí, $v_1(u) \geq \min\{v_1(y), r \cdot v_1(z)\} > 0$ e $v_i(u) \geq \min\{v_i(y), r \cdot v_i(z)\} < 0$, para $i = 2, \ldots, n$.

Etapa 2. Existe $w \in K$ tal que $v_1(w-1) > r_1$ e $v_i(w) > r_i$, para $i = 2, \ldots, n$.

Prova da Etapa 2.

Escolhamos u como na **Etapa 1** e escrevamos $w = (1+u^s)^{-1}$. Temos, para $s \in \mathbb{N}$ suficientemente grande, que

$$\begin{aligned}
v_1(w-1) &= v_1((1+u^s))^{-1} - 1 \\
&= v_1\left(\frac{1-1-u^s}{1+u^s}\right) \\
&= v_1(-u^s(1+u^s)^{-1}) \\
&= s \cdot v_1(u) - v_1(1+u^s) \\
&= s \cdot v_1(u) - \min\{v_1(1), s \cdot v_1(u)\} \ (*) \\
&= s \cdot v_1(u) - 0 \\
&= s \cdot v_1(u) > r_1
\end{aligned}$$

e

$$\begin{aligned}\nu_1(w) &= -\nu_i(w^{-1}) \\ &= -\nu_i(1+u^s) \\ &= -s\cdot\nu_i(u) > r_i.\ (*)\end{aligned}$$

$(*)$ Temos que $\nu_1(1) = 0 < \nu_1(u^s)$, para qualquer $s \in \mathbb{N}$, donde, pelo Lema 4.1.5, temos que $\nu_1(1+u^s) = \min\{\nu_1(1), \nu_1(u^s)$. Um resultado análogo vale para ν_i, $i = 2, \ldots, n$.

Etapa 3. Dados $y_1, \ldots, y_n \in K$, existe um elemento $z \in K$ com $\nu_i(z - y_i) > r_i$, para $i = 1, \ldots, n$.

Prova da Etapa 3.

Escolhamos $s \in \mathbb{Z}$ tal que $\nu_i(y_j) \geq s$, para todos $i, j \in \{1, \ldots, n\}$. Pela **Etapa 3**, temos que existem $w_1, \ldots, w_n$ tais que

$$\begin{array}{cccc}
\nu_1(w_1-1) > r_1 - s & \nu_1(w_2) > r_1 - s & \ldots & \nu_1(w_n) > r_1 - s \\
\nu_2(w_1) > r_2 - s & \nu_(w_2 - 1) > r_2 - s & \ldots & \nu_2(w_n) > r_2 - s \\
\vdots & \nu_3(w_2) > r_3 - s & \ldots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\ldots & \ldots & \ldots & \nu_{n-1}(w_n) > r_{n-1} - s \\
\nu_n(w_1) > r_n - s & \nu_n(w_2) > r_n - s & \ldots & \nu_n(w_n - 1) > r_n - s.
\end{array}$$

Considerando $\sum_{j=1}^{n} y_j w_j$, temos

$$\begin{aligned}\nu_i(z - y_i) &= \nu_i(y_i(w_i - 1) + \sum_{j\neq 1} y_j w_j) \\ &\geq \min\{\nu_i(y_i(w_i-1)), \nu_i(y_1 w_1), \ldots, \nu_i(y_{i-1}w_{i-1}), \nu_i(y_{i+1}w_{i+1}), \ldots, \nu_i(y_n w_n))\} \\ &> r_i.\end{aligned}$$

Conclusão da Demonstração

Pela **Etapa 3**, podemos encontrar $z \in K$ tal que $\nu_i(z - x_i) > r_i$, para $i = 1, \ldots, n$. A seguir, escolhemos z_i ta que $\nu_i(z_i) = r_i$ (isso pode sempre ser feito, pois ν_i é sobrejetora para todo i). Novamente, pela **Etapa 3**, existe z', tal que $\nu_i(z' - z_i) > r_i$, para $i = 1, \ldots, n$. Daí temos que

$$\nu_i(z') = \nu_i((z' - z_i) + z_i) = \min\{\nu_i(z' - z_i), \nu_i(z_i)\} = r_i.$$

Escrevendo $x = z + z'$, temos que

$$\nu_i(x - x_i) = \nu_i((z - x_i) + z') = \min\{\nu_i(z - x_i), \nu_i(z')\} = r_i.$$

□

4.5 Divisores

Consideremos ao longo dessa seção F/K um corpo de funções algébricas em uma variável com corpo das constantes K (K finito).

Definição 4.5.1. *Um divisor* D *de* F *é uma soma formal*

$$\sum_{P \in \mathbb{P}_F} m_P P,$$

com $m_P \in \mathbb{Z}$*, e quase todo* $m_P = 0$*.*

Um lugar $P \in \mathbb{P}_F$ é também um divisor (coloque $m_P = 1, m_Q = 0$ para todo $Q \in \mathbb{P}_F$ com $Q \neq F$). Nesse contexto, o lugar P é chamado de *divisor primo*.

Os divisores de F formam um grupo aditivo, donde definimos a adição:

$$D + E = \sum_{P \in \mathbb{P}_F} m_P P + \sum_{P \in \mathbb{P}_F} n_P P = \sum_{P \in \mathbb{P}_F} (m_P + n_P) P,$$

onde D e E são divisores de F, que é claramente associativa e comutativa.

O elemento zero do grupo dos divisores é o divisor

$$0 := \sum_{P \in \mathbb{P}_F} m_P P,$$

onde $m_P = 0$, para todo $P \in \mathbb{P}_F$.

O inverso aditivo de $\sum_{P \in \mathbb{P}_F} m_P P$ é

$$-D = \sum_{P \in \mathbb{P}_F} (-m_P) P.$$

Definição 4.5.2. *O grupo abeliano de todos os divisores de* F *é chamado grupo dos divisores de* F *e é denotado por* $\mathrm{Div}(F)$ *também pode ser descrito como o grupo abeliano gerado pelos lugares (divisores primos) de* F.

Observação 5. *Façamos uma simples analogia entre polinômios e divisores. Um polinômio é uma atribuição que associa cada monômio* x^i *a um coeficiente* a_i *,* $i = 0, 1, 2, \ldots$*, onde existe um número finito de* $a_i = 0$*. Um divisor é uma atribuição que associa cada lugar* $P \in \mathbb{P}_F$ *a um coeficiente inteiro* m_P*, com um número finito de* $m_P = 0$*. A adição de divisores opera da mesma maneira que a adição de polinômios.*

Definição 4.5.3. *O suporte* $\mathrm{supp}(D)$ *do divisor* $D = \sum_{P \in \mathbb{P}_F} m_P P$ *é dado por*

$$\mathrm{supp}(D) = \{P \in \mathbb{P}_F; m_P \neq 0\}.$$

Pela definição de divisores, o $\mathrm{supp}(D)$ é um subconjunto finito de $\mathbb{P}_F$. Se $D = \sum_{P \in \mathbb{P}_F} m_P P$, muitas vezes é conveniente escrever $m_P = \nu_P(D)$. Portanto, um divisor D pode ser representado na forma

$$D = \sum_{P \in \mathrm{supp}(D)} \nu_P(D) P.$$

Definição 4.5.4. *Se* $D \in \mathrm{Div}(F)$ *é como na definição acima, então o grau de um divisor é definido como*

$$\deg(D) = \sum_{P \in \mathrm{supp}(D)} \nu_P(D) \deg(P).$$

Proposição 4.5.5. *A função*

$$\begin{aligned} \deg : \mathrm{Div}(F) &\to \mathbb{Z} \\ D &\mapsto \deg(D) \end{aligned}$$

é um homomorfismo de grupos.

Demonstração: Esta é uma verificação imediata □

Consequentemente, os divisores de F de grau 0 formam um subgrupo de $\mathrm{Div}(F)$. Uma relação de ordem parcial em $\mathrm{Div}(F)$ pode ser definida por

$$D_1 \leq D_2 \text{ se, e somente se, } \nu_P(D_1) \leq \nu_P(D_2),$$

para todo $P \in \mathbb{P}_F$. Se $D_1 \geq D_2$ e $D_1 \neq D_2$, escrevemos $D_1 > D_2$. Ainda, se $D \geq 0$, então D é chamado um divisor positivo.

Se F é um corpo de funções racionais e $f \in F^*$, então é óbvio que $\nu_P(f) \neq 0$ para quase todos $P \in \mathbb{P}_F$. O mesmo vale para um corpo de funções algébricas arbitrário F/K. Portanto, a seguinte definição faz sentido.

Definição 4.5.6. *Seja F um corpo de funções algébricas e $f \in F^*$. O divisor principal de f, denotado por $\mathrm{div}(f)$, é definido como*

$$\mathrm{div}(f) = \sum_{P \in \mathbb{P}_F} \nu_P(f) P.$$

Observação 6. *Se f pertence ao corpo das constantes K de F e $f \neq 0$, segue como prova do Lema 4.3.2 que $\nu_P(f) = 0$ para todo $P \in \mathbb{P}_F$. Portanto, concluímos que $\mathrm{div}(f) = 0$. O inverso também vale já que pode ser demonstrado que para qualquer $f \in F/K$, ou seja, para qualquer transcendente f sobre K, existe pelo menos um $P \in \mathbb{P}_F$ com $\nu_P(f) \neq 0$.*

Se F é o corpo das funções racionais e $f \in F^*$, então segue pela Observação 4 e a informação sobre o grau de $P \in \mathbb{P}_F$ do exemplo 4.4.6 que

$$\deg(\mathrm{div}(f)) = \sum_{P \in \mathbb{P}_F} \nu_P(f) \deg(P) = 0.$$

A mesma fórmula também vale para corpos de funções algébricas arbitrários.

Proposição 4.5.7. *O grau de todo divisor principal é* 0.

Verifica-se facilmente que o conjunto $\mathtt{Princ}(F)$ dos divisores principais de F formam um subgrupo de $\mathtt{Div}^0(F)$;observe, por exemplo, que

$$\mathtt{div}(fg) = \mathtt{div}(f) + \mathtt{div}(g)$$

para todos $f, g \in F^*$.

O grupo quociente

$$\mathtt{Cl}(F) := \mathtt{Div}^0(F)/\mathtt{Princ}(F)$$

é chamado grupo das classes de divisores de F/K. Esse conjunto é finito (a demonstração deste fato pode ser encontrada em Stichtenoth (2009) e sua cardinalidade $h(f) := |\mathtt{Cl}(F)|$ é chamada de *número de classes de divisores* de F.

4.6 O Teorema de Riemann-Roch

Consideremos novamente F/K um corpo de funções algébricas em uma variável com corpo das constantes K (K finito). O principal resultado desse seção é o Teorema de Reimann-Roch. Segundo Stichtenoth (2009), este é o mais importante teorema da teoria Corpos de Funções Algébricas, desempenhando um importante papel no cálculo da dimensão de um Código Algébrico Geométrico, que será apresentado no Capítulo 5.

Definição 4.6.1. *Para qualquer divisor* $D \in \mathtt{Div}(F)$*, definimos o espaço de Riemann-Roch associado a* D *por*

$$\mathcal{L}(D) := \{f \in F^*; \mathtt{div}(f) + D \geq 0\} \cup \{0\}.$$

Explicitamente, isso significa que $\mathcal{L}(D)$ consiste em todos $f \in F$ com

$$\nu_P(f) \geq -\nu_P(D).$$

para todo $P \in \mathbb{P}_F$.

Proposição 4.6.2. $\mathcal{L}(D)$ *é um espaço vetorial sobre* K.

Demonstração: Em primeiro lugar, notemos que $\mathcal{L}(D)$ é não vazio pois $0 \in \mathcal{L}(D)$. Sejam agora $f_1, f_2 \in \mathcal{L}(D)$ e $a \in K$. Então, para todo $P \in \mathbb{P}_F$

$$\nu_P(f_1 + f_2) \geq \min\{\nu_P(f_1), \nu_P(f_2)\} \geq -\nu_P(D)$$

e

$$\nu_P(af_1) = \nu_P(a) + \nu_P(f_1) \geq -\nu_P(D).$$

Portanto, $f_1 + f_2 \in \mathcal{L}(D)$ e $af_1 \in \mathcal{L}(D)$. Sendo assim, $\mathcal{L}(D)$ é um espaço vetorial sobre K. □

Exemplo 4.6.3. *Para os divisores de zero, temos* $\mathcal{L}(0) = K$. *Observe que para* $f \in F^*$, *temos* $f \in \mathcal{L}(0) \Leftrightarrow \nu_P(f) \geq 0$, *para todo* $P \in \mathbb{P}_F$. *Mas*

$$\deg(\mathrm{div}(f)) = \sum_{P \in \mathbb{P}_F} \nu_P(f) \deg(P) = 0$$

pela Proposição 4.5.7. Então, $f \in \mathcal{L}(0) \Leftrightarrow \nu_P(f) = 0$ *para todo* $p \in \mathbb{P}_F$ *se, e somente se,* $f \in K^*$, *sendo essa última equivalência obtida pela Observação 6.*

Observação 7. *Se* $\deg(D) < 0$, *então necessariamente* $\mathcal{L}(D) = \{0\}$. *Pois se tivéssemos* $f \in \mathcal{L}(D)$ *não nulo, aplicando a função grau para*

$$\mathrm{div}(f) + D \geq 0$$

teríamos $0 + \deg(D) \geq 0$, *uma contradição.*

O espaço vetorial $\mathcal{L}(D)$ tem, de fato, uma dimensão finita sobre K, que é denotada por $\ell(D)$. Assim, pelo mostrado acima, temos $\ell(0) = 1$ e $\ell(D) = 0$ se $\deg(D) < 0$.

Teorema 4.6.1 (Riemann-Roch)**.** *Seja* F/K *um corpo de funções algébricas. Existe uma constante* c *tal que para todo divisor* D *de* F, *temos*

$$\ell(D) \geq \deg(D) + 1 - c.$$

Como consequência do Teorema de Riemann-Roch, podemos definir o número

$$g = \max_{D \in Div(F)} (\deg(D) - \ell(D) + 1).$$

O inteiro $g = g(F)$ é chamado de *gênero* de F, e é o invariante mais importante de um corpo de funções algébricas. Mas colocando $D = 0$ na definição, vemos que $g \geq 0$. Observe que pela definição, temos

$$\ell(D) \geq \deg(D) + 1 - g,$$

para todo $D \in Div(F)$

Pelo resultado a seguir, teremos a igualdade se $\deg(D)$ for suficientemente grande.

Teorema 4.6.2. *Se* $\deg(D) \geq 2g - 1$*, então*

$$\ell(D) = \deg(D) + 1 - g.$$

Exemplo 4.6.4. *Se* F *é o corpo das funções racionais, então é fácil verificar que*

$$\ell(D) \geq \deg(D) + 1,$$

para todo $D \in Div(F)$*. Portanto,* $g(F) = 0$*. De fato, o corpo das funções racionais sobre corpos finitos pode ser caracterizado pela propriedade de ter gênero zero.*

Um corpo de funções algébricas de gênero 1 é também chamado de *corpo de função elíptica*. Corpos de funções elípticas F/K com $K = \mathbb{F}_q$ podem ser caracterizados. Em todos os casos, F é uma extensão quadrática de $K := K(x)$. Se q é ímpar, então $F = K(y)$ para algum $y \in F$ com

$$y^2 = f(x),$$

onde $f \in K[x]$ é quadrado de grau 3. Se q é par, então $F = K(y)$ para algum $y \in F$ com

$$y^2 + y = f(x)$$

com $f \in K[x]$ de grau 3 ou

$$y^2 + y = x + \frac{1}{ax + b},$$

com $a, b \in K$ e $a \neq 0$.

Não existe uma fórmula explícita geral para o gênero de um corpo de funções algébricas. No entanto, para certas famílias de corpos de funções algébricas, como no exemplo abaixo, existe essa fórmula. Em geral, o cálculo do gênero de um corpo de funções algébricas é um problema não trivial.

Uma importante ferramenta para o cálculo de gênero é a fórmula do gênero de Hurwitz (ver Stichtenoth (2009)).

Exemplo 4.6.5. *Seja* $K = \mathbb{F}_q$ *com* q *ímpar e deixe* $K = K(x)$ *o corpo das funções racionais. Se* $F = K(y)$ *é a extensão quadrática definida por*

$$y^2 = f(x),$$

onde $f \in K[x]$ *é quadrado de grau* $d \geq 1$*. Então.*

$$g(F) = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

A demonstração pode ser encontrada em Stichtenoth (2009).

4.7 Função Zeta e Limite de Hasse-Weil

Como sempre F/K é um corpo de funções algébrica com corpo completo de constantes K (K finito).

Proposição 4.7.1. *Um corpo de funções algébricas* F/K *possui um número finito de lugares racionais.*

Demonstração: Pela Definição 4.4.1, existe $z \in F/K$ de tal modo que $[F : K(z)] < \infty$. Todos os lugares racionais de F estão sobre os lugares racionais de $K(z)$(usamos a primeira parte da Proposição 4.4.3). Pelo Teorema 4.4.1, para cada lugar racional P de $K(z)$, existem no máximo $[F : K(z)]$ lugares racionais de F sobre P. Além disso, se $K = \mathbb{F}_q$, então, pelo Exemplo 4.4.6, existem apenas $q + 1$ lugares racionais sobre $K(z)$. Portanto o número de lugares racionais de F é no máximo $(q + 1)[F : K(z)]$. □

Podemos agora definir a Função Zeta de um corpo de funções algébricas $F/\mathbb{F}_q$. Para cada inteiro $n \geq 1$, considere a composição de corpos

$$F_n := \mathbb{F}_{q^n} \circ F.$$

Isto é um corpo de funções algébricas sobre $\mathbb{F}_{q^n}$ (chamado de extensão do corpo das constantes de F). Denotando por N_n o número de lugares racionais de $F_n/\mathbb{F}_{q^n}$, que pela Proposição 4.7.1, será um número finito .

Definição 4.7.2. *A série de potências*

$$Z(F,t) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} t^n\right) \in \mathbb{C}[[t]]$$

é chamada de função Zeta de $F/\mathbb{F}_q$

Observe que consideramos t como uma variável complexa, e $Z(F,t)$ é uma série de potências sobre o corpo dos números complexos.

Exemplo 4.7.3. *Calculando a função Zeta do corpo das funções racionais* F *sobre* $\mathbb{F}_q$*, pelo Exemplo 4.4.6, temos* $N_n = q^n + 1$ *para todo* $n \geq 1$*. Daí chegamos que*

$$\begin{aligned}
\log Z(F,t) &= \sum_{n=1}^{\infty} \frac{q^n + 1}{n} t^n \\
&= \sum_{n=1}^{\infty} \frac{(qt)^n}{n} + \sum_{n=1}^{\infty} \frac{t^n}{n} \\
&= -\log(1-qt) - \log(1-t) \\
&= \log \frac{1}{(1-t)(1-qt)},
\end{aligned}$$

Isto é,

$$Z(F,t) = \frac{1}{(1-t)(1-qt)}$$

Teorema 4.7.1 (Teorema Weil)**.** *Seja* $F/\mathbb{F}_q$ *um corpo de funções algébricas de gênero* g*. Então.*

1. $Z(F,t)$ *é uma função racional da forma*

$$Z(F,t) = \frac{L(F,t)}{(1-t)(1-qt)}$$

onde $L(F,t) \in \mathbb{Z}[t]$ *é um polinômio de grau* $2g$ *com* $L(F,0) = 1$ *e coeficiente principal* q^g. *Além disso,* $L(F,1)$ *é igual ao número de classes de divisores* $h(F)$ *de* F.

2. *O fator* $L(F,t)$ *é da forma*

$$L(F,t) = \prod_{j=1}^{2g}(1 - w_j t) \in \mathbb{C}[t].$$

Onde $|w_j| = q^{1/2}$ *para* $1 \leq j \leq 2g$.

Teorema 4.7.2 (Limite de Hasse-Weil)**.** *Seja* $F/\mathbb{F}_q$ *um corpo de funções algébricas de gênero* g. *Então o número* $N(F)$ *de lugares racionais de* $F/\mathbb{F}_q$ *satisfaz*

$$|N(F) - (q+1)| \leq 2gq^{1/2}$$

Demonstração. Pela definição de $Z(F,t)$ obtemos

$$N(F) = N_1 = \left.\frac{d(\log Z(F,t))}{dt}\right|_{t=0} = Z'(F,0)$$

por outro lado, pelo Teorema 4.7.1, temos

$$Z'(F,0) = \left.\left(\frac{L'(F,t)}{L(F,t)} + \frac{1}{1-t} + \frac{q}{1-qt}\right)\right|_{t=0} = a_1 + 1 + q$$

onde a_1 é o coeficiente de t em $L(F,t)$. Comparando os coeficientes com a identidade do Teorema 4.7.1, obtemos

$$a_1 = -\sum_{j=1}^{2g} w_j.$$

A combinação das três identidades acima produz

$$N(F) = q + 1 - \sum_{j=1}^{2g} w_j.$$

Portanto,

$$|N(F) - (q+1)| = \left| \sum_{j=1}^{2g} w_j \right| \leq \sum_{j=1}^{2g} |w_j| = 2gq^{1/2}$$

pelo item (ii) do Teorema 4.7.1. □

Observação 8. *Uma abordanagem refinada produz o limite de Serre*

$$|N(F) - (q+1)| \leq g\lfloor 2q^{1/2} \rfloor.$$

Para a prova desse limite, ver Niederreiter (2002) e Stichtenoth (2009).

Em particular, obtemos um limite superior em $N(F)$ que depende apenas de g e q. Portanto, a seguinte definição faz sentido.

Definição 4.7.4. *Seja q uma potência prima fixa e $g \geq 0$ um inteiro, temos*

$$N_q(g) := \max N(F),$$

onde o máximo está definido sobre os corpos de funções algébricas $F/\mathbb{F}_q$ de gênero g.

É trivial que $N_q(0) = q + 1$. Do limite de Serre, temos

$$N_q(g) \leq q + 1 + g\lfloor 2q^{1/2} \rfloor$$

Se colocarmos

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}$$

concluímos que $A(q) \leq \lfloor 2q^{1/2} \rfloor$ para todo q. Vladut e Drinfeld [14] melhoram isso para

$$A(q) \geq q^{1/2} - 1$$

para todo q, e de um resultado de Ihara [15], segue que

$$A(q) = q^{1/2} - 1$$

para todos os quadrados de q. A quantidade $A(q)$ é de muita importância na aplicação para os códigos Algébricos Geométrico.

[14] S. G. Vladut, V. G. Drinfeld, "Number of points of an algebraic curve", Funktsional. Anal. i Prilozhen., 17:1 (1983), 68–69; Funct. Anal. Appl., 17:1 (1983), 53–54

[15] Y. Ihara, Some remarks on the number of rational points of algebratic curves over finite fields, 1982, Mathematics Journal of the Faculty of Science, the University of Tokyo. Sect. 1 A, Mathematics

5 Códigos de Goppa Racionais

Neste capítulo, apresentaremos uma introdução ao Códigos Algébricos Geométricos, também conhecidos como Códigos de Goppa Racionais, sendo estes uma generalização dos Códigos de Reed-Solomon, também aqui apresentados. As referências utilizadas foram Stichtenoth (2009) e Rousseau e Saint-Aubin (2015).

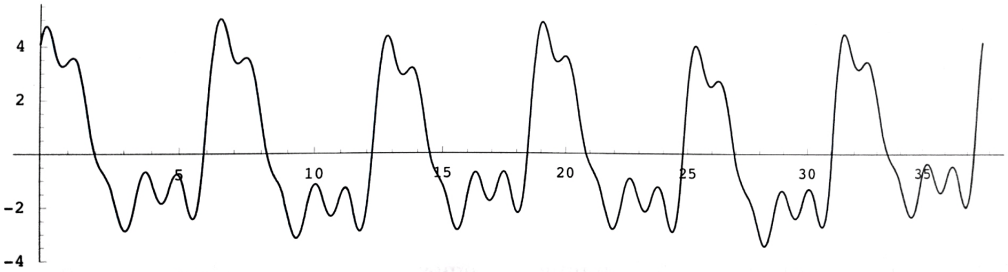
5.1 Códigos de Reed-Solomon

Os Códigos Algébrico Geométricos foram introduzidos pelo matemático russo V. D. Goppa sendo às vezes chamados de *Códigos Geométricos de Goppa*. Como uma motivação para a construção desses códigos, primeiro consideraremos os códigos de Reed-Solomon sobre $\mathbb{F}_q$. Segundo Stichtenoth (2009), esta importante classe de códigos é bem conhecida na teoria da codificação e os Códigos Algébrico Geométricos são uma generalização muito natural dos Códigos Reed-Solomon.

Os Códigos de Reed-Solomon foram desenvolvidos em 1959 pelos matemáticos Irving Reed e Gustave Solomon. Segundo Abrantes (2003), atualmente os códigos de Reed-Solomon são, provavelmente, os mais usados de todos os códigos corretores de erros, pois têm encontrado aplicações em produtos eletrônicos de grande consumo, como os CDs e os CD-ROM, além de serem usados numa multiplicidade de outras situações, como as comunicações espaciais. Por exemplo, os disco compactos (CDs) não guardam caracteres latinos, mas som digitalizados. Som, música em particular, é frequentemente guardada em formato digital. Som é uma onda na densidade do ar. Se medirmos a densidade do ar num local fixo perto de um piano (bem afinado), veríamos que a densidade aumenta e decai 440 vezes por segundo quando o Lá médio é tocado. A Figura 7 mostra a representação desta onda de pressão. (O eixo horizontal indica o tempo e o vertical a amplitude da onda).

Quando o valor é positivo, isto indica que a densidade do ar é mais alta que que a normal (ar em repouso), enquanto valores negativos indicam uma densidade do ar diminuída. Cada curto período de tempo de Δ segundos é aproximado pelo valor médio daquela onda naquele intervalo de tempo. Se Δ é pequeno o bastante, a aproximação da onda pela função degrau será indistinguível da original ao ser ouvida pelo ouvido humano. Feita essa digitalização, a onda pode agora ser representada como uma sequência de números inteiros identificando as alturas dos degraus numa escala pré definida. Em CDs, a onda sonora é particionada em 44100 amos-

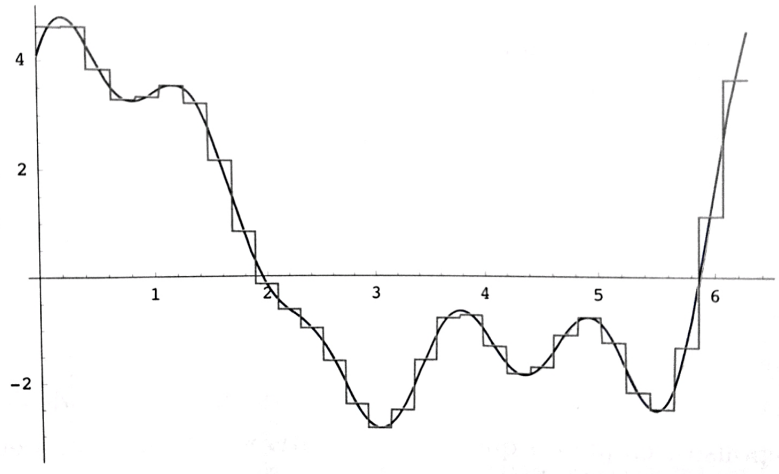
Figura 7: Uma onda sonora medida numa fração de segundo.



Fonte: Rousseau e Saint-Aubin (2015), p. 187.

tras por segundo, e intensidade de cada amostra é representada por um inteiro de 16 bits($2^{16} = 65.536$). Recordando que discos compactos guardam som estéreo, vemos que um segundo de música requer $44.100 \times 16 \times 2 = 1.411.200$ bits e 70 minutos de áudio requer $1.411.200 \times 60 \times 70 = 5.927.040.000$ bits= $740.880.000$B ≈ 740MB. Dada tamanha quantidade de dados, é desejável sermos capazes de detectar e corrigir erros, e para isso, são utilizados os Códigos de Reed-Solomon.

Figura 8: Uma onda sonora e uma função degrau aproximando-a.



Fonte: Rousseau e Saint-Aubin (2015), p. 187.

Para definir os Códigos de Reed-Solomon, considere $n = q - 1$ e $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^\times$, ou seja, $\mathbb{F}_q^\times = \{\beta, \beta^2, \ldots, \beta^n = 1\}$. Para um inteiro k com $1 \leq k \leq n$ consideremos o seguinte espaço vetorial de dimensão k:

$$\mathcal{L}_k := \{f \in \mathbb{F}_q[x]; gr(f) \leq k-1\},$$

e a função avaliação $ev : \mathcal{L}_k \to \mathbb{F}_q^n$ dada por

$$ev(f) := (f(\beta), f(\beta^2), \ldots, f(\beta^n)) \in \mathbb{F}_q^n.$$

A função ev é $\mathbb{F}_q$-linear, e é injetiva, pois todo polinômio não nulo $f \in \mathbb{F}_q[x]$ de grau $< n$ possui menos de n zeros. Portanto

$$C_k := \{f(\beta), f(\beta^2), \ldots, f(\beta^n)), f \in \mathcal{L}_k\}$$

é um $[n, k]$ código sobre $\mathbb{F}_q$, e é chamado *Código de Reed-Solomon.*

O peso de uma palavra código $0 \neq c = ev(f) \in C_k$ é dado por

$$\begin{aligned} w(c) &= n - |\{i \in \{1, \cdots, n\}; f(\beta^i) = 0\}| \\ &\geq n - gr(f) \\ &\geq n - (k-1). \end{aligned}$$

Consequentemente, a distância mínima d de C_k satifaz a desigualdade $d \geq n+1-k$. Por outro lado, pela Cota de Singleton, $d \leq n+1-k$. Logo, $d = n+1-k$. Portanto, os Códigos de Reed-solomon sobre $\mathbb{F}_q$ são MDS (Maximum Distance Separabel). Observe, no entanto, que os Códigos de Reed-Solomon são curtos quanto comparados ao tamanho do alfabeto $\mathbb{F}_q$, já que $n = q - 1$.

Para exemplificar, considere $\mathbb{F}_{2^m}$ o corpo com 2^m elementos e seja α uma raiz primitiva. Os $2^m - 1$ elementos de $\mathbb{F}_{2^m}$ são da forma

$$\{\alpha, \alpha^2, \ldots, \alpha^{2^m-1} = 1\},$$

e, portanto, para todos os elementos $x \in \mathbb{F}_{2^m}$ não nulos temos que $x^{2^m-1} = 1$. As palavaras a serem codificadas serão aquelas de k, cada letra sendo um elemento de $\mathbb{F}_{2^m}$ e onde $k < 2^m - 2$. (Como escolher este inteiro k será explicado em breve). Desta forma, serão elementos $(u_0, u_1, u_2, \ldots, u_{k-1}) \in \mathbb{F}_{2^m}^k$. A cada uma dessas palavras será

associado um polinômio

$$p(x) = u_0 + u_1 x + u_2 x^2 + \cdots + u_{k-1} x^{k-1} \in \mathbb{F}_{2^m}[x].$$

Tais palavras serão codificadas num vetor $v = (v_0, v_1, v_2, \ldots, v_{2^m-2}) \in \mathbb{F}_{2^m}^{2^m-1}$, cujas entradas serão dadas por

$$v_i = p(\alpha^i), i = 0, 1, 2, \ldots, 2^m - 2,$$

onde α é a raíz primitiva que havíamos escolhido a príncipio. Desse modo, **codificar** consiste em calcular:

$$\begin{array}{rcccl} v_0 & = & p(1) & = & u_o + u_1 + u_2 + \cdots + u_{k-1}, \\ v_1 & = & p(\alpha) & = & u_o + u_1\alpha + u_2\alpha^2 + \cdots + u_{k-1}\alpha^{k-1}, \\ v_2 & = & p(\alpha^2) & = & u_o + u_1\alpha^2 + u_2\alpha^4 + \cdots + u_{k-1}\alpha^{2(k-1)}, \\ \vdots & = & \vdots & = & \vdots \\ v_{2^m-2} & = & p(\alpha^{2^m-2}) & = & u_o + u_1\alpha^{2^m-2} + u_2\alpha^{2(2^m-2)} + \cdots + u_{k-1}\alpha^{(2^m-2)(k-1)}. \end{array} \quad (*)$$

Os códigos de Reed-Solomon, $C(2^m - 1, k)$, são os conjuntos de vetores $v \in \mathbb{F}_{2^m}^{2^m-1}$ obtidos desta maneira.

Um requisito básico de toda codificação é que palavras diferentes não sejam codificadas da mesma maneira. Isso é o que nos diz a próxima proposição.

Proposição 5.1.1. *A codificação* $u \to v$*, onde* $u \in \mathbb{F}_{2^m}^k$ *e* $v \in \mathbb{F}_{2^m}^{2^m-1}$*, é uma transformação linear com núcleo* $\ker = \{0\} \subset \mathbb{F}_{2^m}^k$*.*

A transmissão pode introduzir alguns erros na mensagem codificada v. A mensagem recebida $w \in \mathbb{F}_{2^m}^{2^m-1}$ pode diferir de v em uma ou mais posições. A decodificação consiste em, primeiramente, substituir em (*), os v_i pelos componentes w_i de w e, então, extrair desse novo sistema linear a informação original u, apesar dos possíveis erros em w. Cada uma destas equações (com v_i substituído pelo w_i correspondente) representa um plano no espaço $\mathbb{F}_2^k$ com coordenadas $(u_0, u_1, \ldots, u_{k-1})$. Existem $2^m - 1$ planos, o que são mais que k, o número de incógnitas u_j. Para o sistema (*) precisamos de k planos (ou seja, k equações) para obter uma determinação de u. Podemos pensar que cada escolha de k planos esteja "votando"para o valor de u onde eles se intersectam. Se alguns dos w_i estão incorretos, podemos perguntar se o u correto consguirá o maior

número de votos. Esta é a questão que trataremos agora.

Suponha que, uma vez que a mensagem seja transmitida, nós recebamos os $2^m - 1$ símbolos $w = (w_0, w_1, w_2, \ldots, w_{2^m-1}) \in \mathbb{F}_{2^m}^{2^m-1}$. Se todos esses símbolos estiverem exatos, podemos recuperar a mensagem original escolhendo de (*) qualquer subconjunto de k linhas e resolvendo o sistema linear resultante. Suponha que escolhamos as linhas $i_0, i_1, \ldots, i_{k-1}$ com $0 \leq i_0 < i_1 < \cdots < i_{k-1} \leq 2^m - 2$, e que α_j denote α^{i_j}. O sistema linear resultante fica

$$\begin{pmatrix} w_{i_0} \\ w_{i_1} \\ w_{i_2} \\ \vdots \\ w_{i_{k-1}} \end{pmatrix} = \begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \alpha_0^3 & \cdots & \alpha_0^{k-1} \\ 1 & \alpha_1 & \alpha_1^2 & \alpha_1^3 & \cdots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_2^3 & \cdots & \alpha_2^{k-1} \\ \vdots & & & & & \\ 1 & \alpha_{k-1} & \alpha_{k-1}^2 & \alpha_{k-1}^3 & \cdots & \alpha_{k-1}^{k-1} \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{k-1} \end{pmatrix}, (**)$$

e podemos obter a mensagem original invertendo a matriz $\{\alpha_i^j\}_{0 \leq i,j \leq k-1}$, assumindo que ela seja invertível.

Proposição 5.1.2. *Para todas as escolhas $i_0, i_1, \ldots, i_{k-1}$ com $0 \leq i_0 < i_1 < \cdots < i_{k-1} \leq 2^m - 2$, a matriz $\{\alpha_i^j\}$ descrita acima é invertível.*

Assim, assumindo que a mensagem recebida não contém erros, existem tantas maneiras de recuperar a mensagem original quanto as maneiras de escolher k equações das $2^m - 1$ em (*):

$$\binom{2^m - 1}{k} = \frac{(2^m - 1)!}{k!(2^m - 1 - k)!}.$$

agora, suponha que s dos $2^m - 1$ coeficientes de w estejam incorretos. Então, somente $(2^m - s - 1)$ das equações de (**) estarão corretas, e somente $\binom{2^m - s - 1}{k}$ dos $\binom{2^m - 1}{k}$ possíveis cálculos de u estarão corretos, com apenas um deles corretos. Seja $\overline{u}$ um dos candidatos incorretos, obtidos por escolher equações falsas em (*). Quantas vezes podemos obter $\overline{u}$ mudando as equações que usamos? A solução $\overline{u}$ é obtida como intersecção de k planos representados pelas k equações escolhidas de (*). No máximo $s + k - 1$ destes planos intersectarão em $\overline{u}$, porque, se fossem mais, haveria entre eles k planos descritos por equações verdadeiras, e $\overline{u} = u$. Logo, há no máximo $\binom{s+k-1}{k}$ modos de chegar a $\overline{u}$. O valor correto u receberá a maioria dos "votos"(calculados pela

maioria das escolhas de equações) se

$$\binom{2^m - s - s}{k} > \binom{s + k - 1}{k}$$

ou, equivalentemente,

$$2^m - s - 1 > s + k - 1.$$

Assim, deduzimos que

$$2^m - k > 2s.$$

Por estarmos interessados apenas nos valores inteiros de s, esta última desigualdade equivale a

$$2^m - k - 1 \geq 2s.$$

Em outras palavras, enquanto o número de erros for menor ou igual a $\frac{2^m-k-1}{2}$, teremos que o valor correto de u receberá o maior número de votos, provando a próxima proposição.

Proposição 5.1.3. *Os códigos de Reed-Solomon podem corrigir* $\left\lfloor \frac{2^m - k - 1}{2} \right\rfloor$ *erros.*

A **decodificação** de w consiste em escolher, entre todas as determinações de u, a que recebe mais votos. As demonstrações das Proposições 5.1.1 e 5.1.2 podem ser encontradas em Rousseau e Saint-Aubin (2015).

5.2 Códigos Geométricos de Goppa

Para introduzir a noção de um código Algébrico Geométrico, fixaremos a seguinte notação nesta seção.

- $F/\mathbb{F}_q$ é um corpo de função algébrica de gênero g,
- $P_1, \cdots, P_n$ são lugares, dois a dois distintos de $F/\mathbb{F}_q$ de grau 1,
- $D = P_1 + \cdots + P_n$,
- G é um divisor de $F/\mathbb{F}_q$ tal que $\mathrm{supp}G \cap \mathrm{supp}D = \emptyset$.

Definição 5.2.1. *Um código Algébrico Geométrico* $C_{\mathcal{L}}(D, G)$ *associado aos divisores* D *e* G *é definido como*

$$C_{\mathcal{L}}(D, G) := \{x(P_1), \ldots, x(P_n); x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Note que a definição faz sentido: para $x \in \mathcal{L}(G)$, temos $v_{P_i} \geq 0, (i = 1, \ldots, n)$, pois $\mathrm{supp}G \cap \mathrm{supp}D = \emptyset$. A classe residual $x(P_i)$ de x módulo P_i é um elemento do corpo das classes residuais de P_i. Como $\deg P_i = 1$, o corpo da classe residual é $\mathbb{F}_q$, então $x(P_i) \in \mathbb{F}_q$.

Considere novamente a função avaliação $ev_D : \mathcal{L}(G) \to \mathbb{F}_q^n$ dada por

$$ev_D := (x(P_i), \ldots, x(P_n)) \in \mathbb{F}_q^n.$$

A função avaliação é $\mathbb{F}_q$ linear, e $C_{\mathcal{L}}(D, G)$ é a imagem de $\mathcal{L}(G)$. Podemos observar a analogia existente com a definição dos códigos de Reed-Solomon. De fato, escolhendo a corpo de funções $F/\mathbb{F}_q$ e os divisores D e G de uma maneira apropriada, os códigos de Reed-Solomon são facilmente vistos como um caso especial dos códigos Algébrico Geométricos.

A Definição 5.2.1 parece uma maneira muito artificial de definir certos códigos sobre $\mathbb{F}_q$. Mostraremos no próximo teorema o porquê de esses códigos serem de fato interessantes: pode-se calcular (ou pelo menos estimar) os parâmtros n, k e d por meio do Teorema de Riemann-Roch, e obtém-se um limite inferior não trivial para a distância mínima para o caso geral. A demonstração do próximo teorema pode ser encontrada em Stichtenoth (2009).

Teorema 5.2.1. *Seja* $C_{\mathcal{L}}(D, G)$ *um código com parâmetros* $[n, k, d]$*, temos*

$$k = \ell(G) - \ell(G - D) \text{ e } d \geq n - \deg G.$$

Corolário 5.2.1.1. *Suponha que o grau de* G *é estritamente menor que* n*. Então a função avaliação* $ev_D : \mathcal{L}(G) \to C_{\mathcal{L}}(D, G)$ *é injetiva, e:*

(a) $C_{\mathcal{L}}(D, G)$ *é um* $[n, k, d]$ *código com*

$$d \geq n - \deg G \text{ e } k = \ell(G) \geq \deg G + 1 - g.$$

Consequentemente,

$$k + d \geq n + 1 - g. \tag{14}$$

(b) Se $2g - 2 < \deg G < n$*, então* $k = \deg G + 1 - g$.

(c) Se $\{x_1, \ldots, x_k\}$ *é uma base de* $\mathcal{L}(G)$*, então a matriz*

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ \vdots & \vdots & & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{pmatrix}$$

é uma matriz geradora de $C_{\mathcal{L}}(D, G)$.

Demonstração: Suponha que tenhamos $\deg(G - D) = \deg G - n < 0$, então $\mathcal{L}(G - D) = 0$. Desde que $\mathcal{L}(G-D) = 0$ seja o núcleo da função avaliação, ela será uma função injetiva. Os demais itens, são consequências triviais do Teorema 5.2.1 e o Teorema de Riemman - Roch (4.6.1). □

Ressaltamos que o limite inferior (14) para a distância mínima é muito semelhante a Cota de Singleton. Juntando os dois limites vemos que para $\deg G < n$,

$$n + 1 - g \leq k + d \leq n + 1. \tag{15}$$

Observe que $k + d = n + 1$ se F é um corpo de função de gênero $g = 0$. Consequentemente, os códigos Algébrico Geométricos construídos através do corpo de função racional $\mathbb{F}_q(z)$ são códigos MDS.

A fim de obter um limite significativo para a distância mínima de $C_{\mathcal{L}}$, pelo Teorema 5.2.1, assumimos frequentemente que $\deg G < n$.

Definição 5.2.2. *O inteiro* $d^* := n - \deg G$ *é chamado de distância projetada do código* $C_{\mathcal{L}}(D, G)$.

O Teorema 5.2.1 afirma que a distância mínima d de um código Algébrico Geométrico não pode ser menor que a distância projetada. A questão se $d^* = d$ ou $d^* < d$ pode ser respondida pela seguinte observação.

Observação 9. *Suponha que* $\ell(G) > 0$ *e* $d^* = n - \deg G > 0$*. Então* $d^* = d$ *se, e somente se, existe um divisor* D' *com* $0 \leq D' \leq D$*,* $\deg D' = \deg G$ *e* $\ell(G - D') > 0$.

Demonstração: Primeiramente, vamos assumir que $d^* = d$. Então, existe um elemento $0 \neq x \in \mathcal{L}(G)$ tal que a palavra código $(x(P_1), \ldots, x(P_n)) \in C_{\mathcal{L}}(D, G)$ possui precisamente $n - d = n - d^* = \deg G$ componentes zeros, digamos $x(P_{i_j}) = 0$ para $j = 1, \ldots, \deg G$. Mas

$$D' := \sum_{j=1}^{\deg G} P_{i_j}.$$

Então, $0 \leq D' \leq D$, $\deg D' = \deg G$ e $\ell(G - D') > 0$ (como $x \in \mathcal{L}(G - D')$).

Inversamente, se D' possui as propriedades acima, escolhemos um elemento $0 \neq y \in \mathcal{L}(G - D')$. O peso da palavra código correspondente $(y(P_1), \ldots, y(P_n))$ é $n - \deg G = d^*$, consequentemente, $d = d^*$. □

Com tudo isso, foi possível introduzir a Teoria dos Códigos Algébricos Geométricos. Esses códigos exigem a abordagem de diversos conceitos das teorias de corpos de corpos finitos e corpos de funções, necessitando de uma gama de resultados e prosseguir esse estudo, requer conhecimentos sobre curvas algébricas que transcedem os métodos e os objetivos do trabalho proposto.

Do ponto de vista que abordamos, a questão principal da Teoria dos Códigos é a busca de subespaços vetoriais de dimensão finita, das quais sejamos capazes de calcular sua distância mínima. Os Códigos Algébricos Geométricos são construídos por meio de curvas algébricas sobre um corpo finito $\mathbb{F}_q$, sendo assim, seus parâmetros podem ser interpretados de maneira mais fácil, pois possuem um significado geométrico. Tais curvas são geradas por polinômios irredutíves em duas variáveis sobre um corpo algebricamente fechado. Mudando o enfoque, esse mesmo polinômio define um corpo de funções, e assim, de um estudo puramente algébrico, podemos construir códigos. Para isso, é necessário um conhecimento sobre Extensões de Corpos e Teoria de Galois. Uma excelente referência para quem deseja aprofundar estudos sobre os códigos Algébricos Geométricos é Stichtenoth (2009).

Considerações Finais

Os Códigos Corretores de Erros, enquanto teoria, surgiu nos laboratórios de telefonia, e posteriomente transformou-se em uma teoria matemática, podendo ser aplicada em várias áreas da matemática, como por exemplo, na Geometria Algébrica. Desde seu surgimentos, nos anos 1940, tem motivado diversas pesquisas, tanto pelo aspecto computacional como matemático. Agora, as comunicações digitais não fazem parte só das missões espaciais, mas fazem parte do nosso cotidiano, do cotidiano de empresas e nações. O computadore digital agora é uma ferramenta essencial em nossa sociedade tecnológica. Portanto, garantir a confiabilidade das mensagens transmitidas faz-se mais necessário do que nunca, assim, os Códigos Corretores de Erros vem conquistado uma posição proeminente.

No presente trabalho, buscamos desenvolvemos as ferramentas e parte das técnicas aplicadas na Teoria da Codificação, passando por conceitos de Álgebra Abstrata, Álgebra Linear e Teoria dos Números, vendo assim, que áreas abstratas da Matemática podem sim ser aplicada a problemas "reais". Utilizando bases de subespaços vetoriais, é possível codificar e decodificar informação. Enriquecendo as estruturas dessas bases com outras estrutras algébricas, é possível obter algoritmos de codificação e decodificação mais eficientes.

Referências

ABRANTES, S. A. Notas históricas da codificação para controlo de erros. 2003.

BELL, T.; WITTEN, I. H.; FELLOWS, M.; ADAMS, R.; MCKENZIE, J. Ensinando ciência da computação sem o uso do computador. **Computer Science Unplugged ORG**, 2011.

BOYER, C. B.; MERZBACH, U. C. **História da matemática**. [S.l.]: Editora Blucher, 2019.

FIRER, M. Códigos corretores de erros-notas de aula. UNICAMP, 2007.

GARCIA, A.; LEQUAIN, Y. **Elementos de álgebra**. [S.l.]: Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2006.

HEFEZ, A.; VILLELA, M. L. T. **Códigos corretores de erros**. [S.l.]: Instituto de Matematica Pura e Aplicada, 2008.

_____. **Polinômios e equações algébricas**. [S.l.]: Sociedade Brasileira de Matemática, 2012.

HERSTEIN, I. **Tópicos de ágebra**. [S.l.]: Editora Polígono, 1970.

IEZZI, G.; DOLCE, O.; MACHADO, A. dos S. **Matemática e realidade**. [S.l.]: Atual, 1993.

LIDL, R.; NIEDERREITER, H. **Introduction to finite fields and their applications**. [S.l.]: Cambridge university press, 1994.

LIMA, E. L. **Espaços métricos**. [S.l.]: Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1983. v. 4.

_____. **Análise Real**. [S.l.]: Instituto de Matemática Pura e Aplicada,Rio de Janeiro, 2004.

MASUDA, A. M.; PANARIO, D. **Topicos de corpos finitos com aplicacoes em criptografia e teoria de codigos**. [S.l.]: Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2007.

MILIES, C. P. Breve introduçao teoria dos códigos corretores de erros. **Colóquio de Matemática da Região Centro-Oeste, SBM**, 2009.

MONTEIRO, M. A. Sistemas não decimais de numeração posicional. **Revista do Professor de Matemática, Ediçã0 63, SBM**, 2009.

NIEDERREITER, H. Algebraic function fields over finite fields. In: **Coding Theory and Cryptology**. [S.l.]: World Scientific, 2002.

ROUSSEAU, C.; SAINT-AUBIN, Y. **Matemática e Atualidade**. [S.l.]: Sociedade Brasileira de Matemática, Rio de Janeiro, 2015.

SILVA, J. C.; GOMES, O. R. **Estruturas Algébricas para Licenciatura: Elementos de Aritmética Superior**. [S.l.]: Blucher, São Paulo, 2018. v. 2.

STICHTENOTH, H. **Algebraic function fields and codes**. [S.l.]: Springer Science & Business Media, 2009. v. 254.

VOLOCH, J. F. **Códigos corretores de erros**. [S.l.]: Livraria da Física, São Paulo, 2020. v. 16.

WEISS, E. **Algebraic number theory**. [S.l.]: Courier Corporation, 1998.

A Apêndice

A.1 Proposta de Atividades

A seguir, sugerimos algumas propostas de ativades que podem ser desenvolvidas com os alunos da Educação Básica utilizando códigos corretores de erros. As referidas atividades, buscam além de desenvolver as habilidades previstas na Base Nacional Curricular Comum (BNCC), mostrar aos alunos como conhecimentos matemáticos até então tidos como abstratos ou até mesmo irrelevantes, são aplicados em situações do cotidiano. As atividades podem ser realizadas seguindo a ordem apresentada ou independente.

A.2 Atividade 01 - O Sistema Binário

O sistema universalmente utilizado pelas pessoas comuns para representar os números inteiros é o sitema decimal posicional ou de base 10. O que isso significa? Que 10 unidades de uma ordem representam 1 unidade de ordem imediatamente superior. Com isso, precisamos de apenas 10 símbolos, que chamamos de algarismos, para escrever qualquer numeral

No sitema decimal, todo número inteiro é representado por uma sequência formada pelos algarismos

$$1, 2, 3, 4, 5, 6, 7, 8, 9,$$

acrescido do símbolo 0 (zero), que representa a ausência de algarismo. Por serem dez algarismos, o sistema é chamado decimal.

O sistema também é chamado posicional, pois cada algarismo, além do seu valor intrínseco, possui um peso que lhe é atribuído em função da posição que ele ocupa no número. Esse peso, é sempre uma potência de dez.

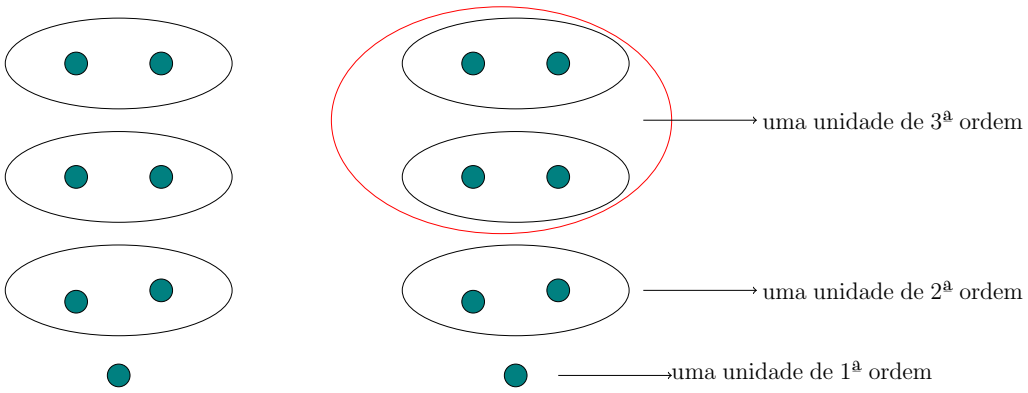
Segundo Monteiro (2009), Usar sistemas de numeração posicional não decimal com os alunos do ensino básico é útil para provocar questionamentos e testar a compreensão sobre procedimentos já automatizados na base 10, uma vez que devem ser reproduzidos em outra base.

Há outros sistemas de numeração em uso, aqui destacamos os **sistemas binário** ou em **bases de potência 2**, que são correntemente usados em computação. Os computadores descrevem dados em termo de 0's e 1's (que podem ser interpretados

como desligado/ligado, fechado/aberto, falso/verdadeiro ou não/sim).

Vejamos, inicialmente, como escreveríamos alguns numerais no sistema de base 2. No sistema decimal, ao juntarmos 10 unidades simples, temos uma dezena, ao juntarmos 10 dezenas, temos uma centena e assim por diante. No sistema de base 2, a cada duas unidades de 1ª ordem, formaremos uma unidade de 2ª ordem, 2 unidades de 2ª ordem formarão uma unidade de 3ª ordem e assim por diante. Considerando, por exemplo, 7 unidades (ver Figura 9 a seguir), no sistema de numeração de base 2, temos uma unidade de 1 ordem, uma unidade de 2 ordem e uma unidade de 3 ordem. Como o sistema de numeração é posicional, a representação será $(111)_2$, onde o índice 2 indica o sistema de numeração.

Figura 9: Representando o número 7 no sitema binário



$$7 = (111)_2$$

Fonte: Monteiro (2009)

Podemos utilizar também o algoritmo conhecido e tradicional de conversão de base:

$$\begin{array}{r|l} 7 & 2 \\ 1 & 3 \quad 2 \\ & 1 \quad 1 \quad 2 \\ & \quad 1 \quad 0 \end{array}$$

$$7 = (111)_2 = 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$$

Os computadores atualmente utilizam o sistema binário para representar informações. Chama-se binário porque utiliza dois dígitos distintos - 0 e 1. Também é conhecido como base dois (as pessoas utilizam no dia-a-dia a base 10). Cada zero ou um é chamado de bit (dígito binário). Um bit é normalmente representado na memória principal do computador por um transistor, que pode estar ligado ou desligado, ou um capacitor, que pode estar carregado ou descarregado.

Quando os dados devem ser transmitidos por uma linha telefônica ou enlace de rádio, tons de alta e baixa freqüência são utilizados para os zeros e uns. Em discos magnéticos (disquetes e discos rígidos) e fitas, os bits são representados pela direção de um campo magnético sobre uma superfície revestida, podendo ser norte-sul ou sul-norte.

Um único bit não consegue representar muito. Por isso, os bits são utilizados geralmente em grupos de oito, podendo representar números de 0 a 255. Um grupo de oito bits é chamado de byte. A velocidade de um computador depende do número de bits que este pode processar de uma só vez. Por exemplo, um computador de 32 bits pode processar números de 32 bits em uma única operação, ao passo que um computador de 16 bits divide os números de 32 bits em partes menores, o que o torna mais lento. Em suma, bits e bytes são tudo que um computador utiliza para armazenar e transmitir números, texto e todas as outras informações. Em algumas das atividades seguintes veremos como outros tipos de informações podem ser representados em um computador.

A aritmética no sitema binário é como se segue:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

A Atividade a seguir foi adaptada de Bell et al. (2011).

Contando os Pontos—Números Binários

Sumário

Os dados são armazenados em computadores e transmitidos como uma série de zeros e uns. Como podemos representar palavras e números usando apenas estes dois

símbolos ?

Série

- 6° e 7° anos.

Unidade Temática

- Números.

Objetos de Conhecimento

- Sistema de numeração decimal: características, leitura, escrita e comparação de números naturais e de números racionais representados na forma decimal.
- Divisão euclidiana.
- Fluxograma para determinar a paridade de um número natural

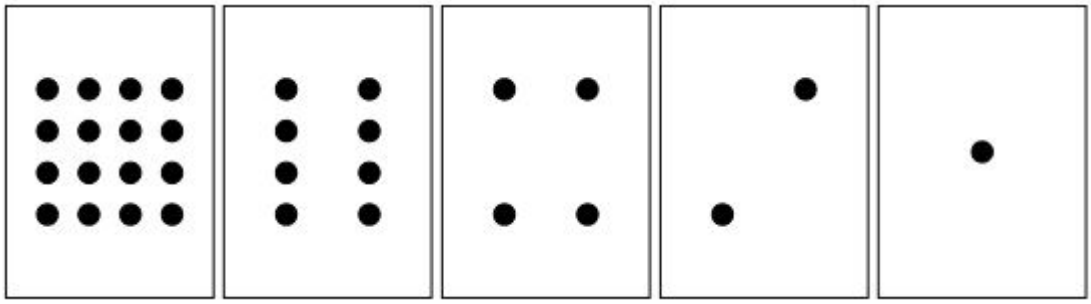
Habilidades - BNCC

- Comparar, ordenar, ler e escrever números naturais e números racionais cuja representação decimal é finita, fazendo uso da reta numérica.
- Reconhecer o sistema de numeração decimal, como o que prevaleceu no mundo ocidental, e destacar semelhanças e diferenças com outros sistemas, de modo a sistematizar suas principais características (base, valor posicional e função do zero), utilizando, inclusive, a composição e decomposição de números naturais e números racionais em sua representação decimal
- Resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora.
- Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par).

Material

- Será necessário confeccionar um conjunto de cinco cartões com números binários conforme Figura 10

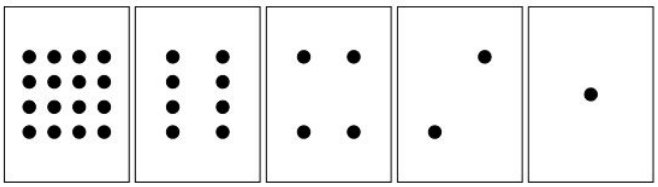
Figura 10: Cartões para formar números binários



Fonte: Bell et al. (2011), p. 6.

Desenvolvimento

Antes de iniciar a atividade "Trabalhando com números binários", pode ser útil demonstrar os fundamentos ao grupo. Para esta atividade, são necessários cinco cartões, conforme mostrado abaixo, com pontos marcados de um lado e nada sobre o verso. Escolha cinco crianças para segurar os cartões de demonstração na frente da turma. Os cartões devem estar na seguinte ordem:



Discussão

- O que você percebeu sobre o número de pontos nos cartões ?

  (Cada cartão tem duas vezes mais pontos que o cartão à sua direita.)

- O que você percebeu sobre o número de pontos nos cartões ?

  (Cada cartão tem duas vezes mais pontos que o cartão à sua direita.)

- Quantos pontos teria o próximo cartão colocado à esquerda ? E o próximo ...?

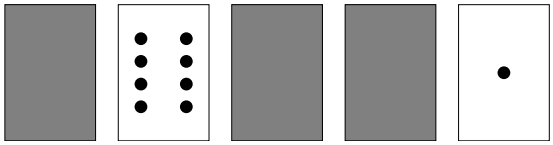
  $(32, 64, 128, \cdots$.

Podemos usar estes cartões para representar números virando alguns deles para baixo e adicionando os pontos dos cartões com a face para cima. Peça às crianças para representarem os números 6 (cartões com 4 e 2 pontos), 15 (cartões com 8, 4, 2 e 1 pontos e, em seguida, 21 (cartões com 16, 4 e 1 ponto) ...

Agora tente contar de zero em diante.

O resto da turma deve prestar atenção sobre como os cartões são virados para tentar reconhecer um padrão (cada cartão é virado metade das vezes do que as vezes do cartão a sua direita).

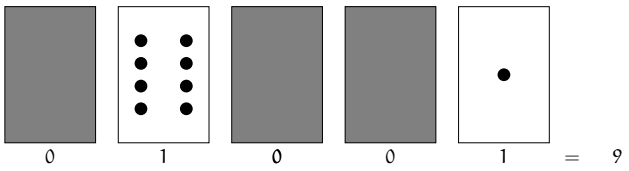
Talvez você queira experimentar isso com mais de um grupo. Quando um cartão está com a face para baixo, sem mostrar os pontos, este cartão é representado por um zero. Quando os pontos são exibidos, o cartão é representado por um. Este é o sistema numérico binário.



Peça aos alunos para formarem o número 01001. Qual o seu número equivalente em decimal ? (9) Como seria o número 17 em binário ? (10001) Faça alguns exemplos até que os alunos compreendam o conceito.

Folha de Atividade: Trabalhando com números binários

O sistema binário utiliza o zero e o um para representar se um cartão está virado para cima ou não. O 0 indica que os pontos do cartão estão escondidos, e o 1 significa que os pontos do cartão são visíveis. Por exemplo:



1. Descubra os números representados pelas seguintes sequências:

   (a) 10101: 21

   (b) 11111: 31

   (c) 00110: 6

   (d) 01010: 10

2. Em qual dia do mês você nasceu ? Escreva-o em formato binário. Descubra os aniversários dos seus amigos em formato binário.

   Resposta pessoal.

3. Agora, vamos utilizar o algoritmo da divisão para representar um número escrito no sistema decimal no sistema binário.

   (a) 45: $1 \cdot 2^5 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1$

   (b) 56: $1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3$

   (c) 72: $1 \cdot 2^6 + 1 \cdot 2^3$

4. Outra situação interessante dos números binários acontece quando um zero é colocado ao lado direito de um número. Se estivermos trabalhando na base 10 (decimal), ao colocarmos um zero ao lado direito de um número, este é multiplicado por 10. Por exemplo, 9 torna-se 90, 30 torna-se 300. Mas o que acontece quando você coloca um 0 à direita de um número binário ? Tente isto:

$$1001 \longrightarrow 10010$$
$$(9) \longrightarrow (?)$$

Tente com outros números para testar sua hipótese. Qual é a regra ? Por que você acha que isso acontece ?

Quando você coloca um zero à direita de um número binário, esse número é dobrado. Todos os locais contendo um "'1" valem agora duas vezes seu valor anterior, e assim o número total é duplicado. (Na base 10, acrescentando um zero à direita do número multiplica-o por 10.)

Referências

HEFEZ, Abramo; **ARITMÉTICA, Coleçao PROFMAT**. Sociedade Brasileira de Matemática. Rio de Janeiro, 2009.

MONTEIRO, Marcio Andrade. **Sistemas não decimais de numeração posicional**. Revista do Professor de Matemática, n. 63, Rio de Janeiro 2009. Disponível em: https://www.rpm.org.br/cdrpm/63/4.html. Acesso em: 10 de abril de 2021.

A.3 Atividade 02 - Códigos Detectores e Corretores de Erros

A Mágica de virar as cartas—Detecção e Correção de Erros

Sumário

Quando os dados são armazenados num disco ou transmitidos de um computador para outro, costumamos supor que estes não tenham sofrido alterações no processo. Mas, às vezes, problemas acontecem e os dados são alterados acidentalmente. Esta atividade utiliza um truque de mágica para mostrar como detectar quando os dados foram corrompidos e como podemos corrigi-los.

Série

- 6° e 7° anos.

Unidade Temática

- Números.

Objetos de conhecimento

- Fluxograma para determinar a paridade de um número natural.

Habilidades BNCC

- Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par).

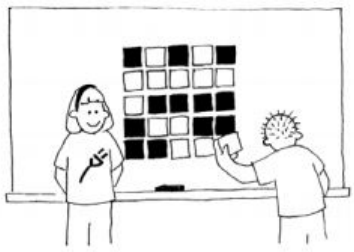
Material

- Um conjunto de 36 cartas do tipo "ímã de geladeira", coloridas em um dos lados.
- Um quadro de metal (um quadro branco funciona bem) para a demonstração.
- Cada par de crianças vai precisar de: 36 cartas idênticas, coloridas em apenas um lado.

Desenvolvimento

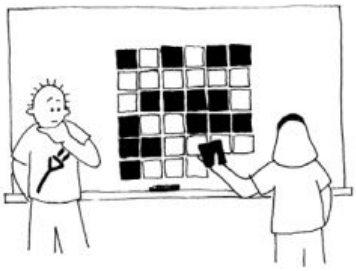
Esta é a sua chance de se tornar um mágico ! Você precisará de um conjunto de cartas iguais de duas faces. (Para fazer suas próprias cartas, corte uma folha grande e colorida apenas de um lado). Para a demonstração, é mais fácil usar cartas magnéticas e planas com uma cor diferente em cada lado—ímãs de geladeira são ideais.

1. Escolha um aluno para dispor as cartas aleatoriamente em um quadrado de dimensões 5×5.



Fonte: Bell et al. (2011), p.32.

Casualmente adicione outra linha e coluna, "apenas para dificultar o truque".



Fonte: Bell et al. (2011), p.32.

Essas cartas são a chave para o truque. Você deve escolher as cartas adicionais para assegurar que haja um número par de cartas coloridas em cada linha e coluna.

2. Peça a um aluno para virar apenas uma carta enquanto você cobre seus olhos. A linha e coluna que contém a carta modificada agora terão um número ímpar de cartas coloridas, e isto identificará a carta modificada.

Os alunos conseguem adivinhar como o truque é feito ?

Ensine o truque para os alunos:

1. Trabalhando em pares, os alunos distribuem suas cartas em um quadrado 5×5.

2. Quantas cartas coloridas estão em cada linha e coluna ? Trata-se de um número par ou ímpar ? Lembre-se, 0 é um número par.

3. Agora, adicione uma sexta carta a cada linha, certificando-se de que o número de cartas coloridas seja sempre ímpar. Esta carta extra é chamada de carta de "paridade".

4. Adicione uma sexta linha de cartas na parte de baixo, fazendo com que o número de cartas em cada coluna seja um número par.

5. Agora, vire uma carta. O que você nota sobre a linha e coluna dessa carta ? (Elas terão um número ímpar de cartas coloridas.) Cartas de paridade são usadas para lhe mostrar a ocorrência de um erro.

6. Agora, faça revezamentos para realizar o "truque".

Atividades de Extensão:

1. Tente usar outros objetos. Tudo o que tem dois "estados" é apropriado. Por exemplo, você poderia utilizar cartas de baralho, moedas (cara ou coroa) ou cartões impressos com 0 ou 1 (para referir-se ao sistema binário).

2. O que acontece quando duas ou mais cartas são viradas ? (Nem sempre é possível saber exatamente quais duas cartas foram viradas, embora seja possível dizer que alguma coisa foi modificada. Normalmente, é possível restringir a um dos dois pares de cartas. Após 4 viradas, é possível que todos os bits de paridade estejam corretos e, por isso, o erro poderia passar despercebido.)

3. Outro exercício interessante é considerar a carta do lado inferior direito. Se você a escolhe como correta para a coluna logo acima, então ela estará correta para a fila à sua esquerda? (A resposta é sim, sempre.)

4. Neste exercício de cartas empregamos a paridade par—usando um número par de cartas coloridas. Podemos fazê-lo com paridade ímpar ? (Isso é possível, porém a carta do lado direito somente funciona para a sua linha e coluna se os números de linhas e colunas são ambos pares ou ímpares. Por exemplo, isso funciona bem para um quadrado 5×9 ou 4×6, mas não para um quadrado 3×4.)

Referências

BELL, Tim; WITTEN, Ian H.; FELOWS, Fellows. **Ensinando Ciência da Computação sem o uso do computador**. Computer Science Unplugged ORG, 2011.

A.4 Atividade 03 - O código do robô

Sumário

Durante a transmissão ou armazenamento de , podem ocorrer interferências que podem modificar os dados recebidos. Para aumentar a confiabiliade são inseridas informações adicionais (redundânicas) a mensagem que se deseja enviar para que seja possível detectar e corrigir possíveis erros.

Série

- 6° e 7° anos.

Unidade Temática

- Números.
- Geometria.

Objetos de Conhecimento

- Fluxograma para determinar a paridade de um número natural.
- Sistema de numeração binário.
- Localização e movimentação de objeto em mapas, croquis e outras representações gráficas.
- Plano cartesiano

Habilidades BNCC

- Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par).
- Associar pares ordenados de números a pontos do plano cartesiano do 1º quadrante.

Material

- Cópia da atividade “O caminho do robô”.

Desenvolvimento

Comece a atividade com a seguinte questão:

Suponhamos que temos um robô que se move sobre um tabuleiro quadriculado, de modo, que ao darmos um dos comandos (Leste (L) , Oeste (O), Norte (N), Sul (S)), o robô se desloca do centro de uma casa para o centro da casa contígua indicada pelo comando. O quadro de comandos pode ser codificado como segue:

Comando	Codificação
Leste	00
Oeste	01
Norte	10
Sul	11

Suponhamos, agora, que esses pares ordenados devam ser transmitidos via rádio e que o sinal no caminho sofra interferências.

Se enviarmos os comandos (S)-(S)-(L)-(L)-(N)-(0), qual codificação será enviada?

(11-11-00-00-10-01)

Se durante o envio correu uma interferência e a codifação enviada foi (10-11-00-00-10-01), o robô fará o mesmo caminho do item anterior? Nesse caso, é possível ifentificar que houve erro?

(Espera-se que os alunos percebem que o caminho percorrido pelo robô não será o que foi enviado, além disso, espera-se também que elas percebem que apenas dois dígitos não são suficientes para que haja a detecção de erros.)

Vamos agora adicionar mais um dígito a nossa codificação, de forma que a soma dos dígitos seja zero (no sistema binário).

Comando	Codificação
Leste	000
Oeste	011
Norte	101
Sul	110

Se a codificação do comando Norte (101), for enviada como (100), é possivel identificar que houve erro, pois (100) não está entre os códigos que podem ser enviados. Mas será que é possível corrigir esse erro?

(Espera-se que os alunos concluam que não é possível corrigir, pois o código 100 difere em apenas um dígito dos códigos $000, 101, 110$, portanto o camando enviado pode ter sido oeste, norte ou sul).

Agora, modificando nosso código como se segue:

Comando	Codificação
Leste	00000
Oeste	01011
Norte	10110
Sul	11101

Nessa recodificação, as duas primeiras posições produzem os códigos originais, chamados de *códigos da fonte*, enquanto as três posisções restantes são as redundâncias inseridas. O novo código introduzido na recodificação é chamado *código de canal*.

Imagine agora que a mensagem recebida seja 11110. É possível identifcar o erro? E corrigi-lo?

(Espera-se que os alunos identifiquem o erro, pois 11110 não pertence a codificação. Comparando-o com cada palavra do código, temos:

- $00000 - 11110$ - possui quatro dígitos diferentes.
- $010101 - 11110$ - possui três dígitos diferentes.
- $10110 - 11110$ - possui um dígito diferente.

- 11101 – 11110 - possui dois dígitos diferentes.

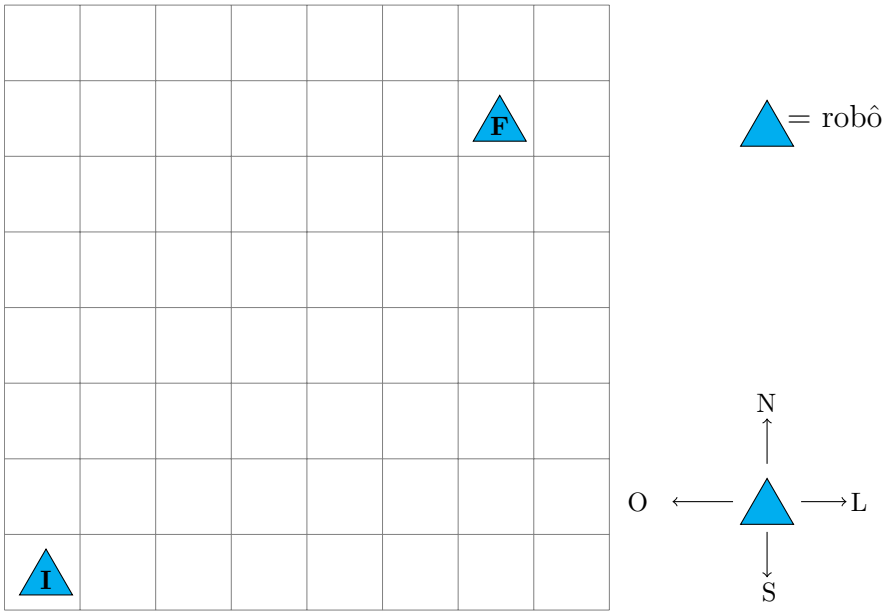
A palavra do código mais próxima da referida mensagem (a que tem menor número de componentes diferentes) é 10110, comando norte. Sendo assim com 5 dígitos será possível identificar e corrigir o erro)

Folha de Atividade - O caminho do robô

1. Considere a tabela de comandos e suas codificações abaixo:

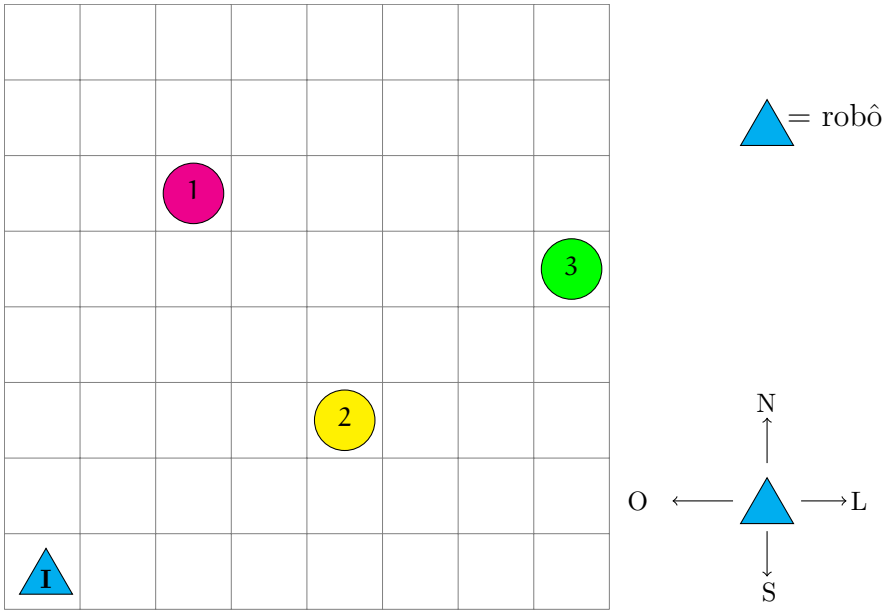
Comando	Codificação
Leste	00000
Oeste	01011
Norte	10110
Sul	11101

Observe as posições inicial (I) e final (F) do robô. Indique quais comandos foram enviados e suas respectivas codificações para que o robô percorresse esse caminho.



Possível resposta: 10110 – 10110 – 10110 – 10110 – 10110 – 10110 – 00000 – 00000 – 00000 – 00000 – 00000 – 00000.

2. Determine uma possível codificação o robô receberá (sabendo que não haverá erros) para percorrer o caminho indicado pelos círculos $1, 2$ e 3?



Possível resposta: $10110 - 10110 - 10110 - 10110 - 10110 - 00000 - 00000 - 11101 - 11101 - 11101 - 00000 - 00000 - 10110 - 10110 - 00000 - 00000 - 00000$.

3. Considere a posição inicial do robô (I). Se o robô recebe a mensagem:

$$00000 \longrightarrow 01000 \longrightarrow 00000 \longrightarrow 10000 \longrightarrow 10010 \longrightarrow$$

$$\longrightarrow 10110 \longrightarrow 10110 \longrightarrow 00011 \longrightarrow 01011 \longrightarrow 11100$$

   (a) Houve erro no envio dessa mensagem? Justifique.

   Sim, pois há mensagens que não pertencem à codificação.

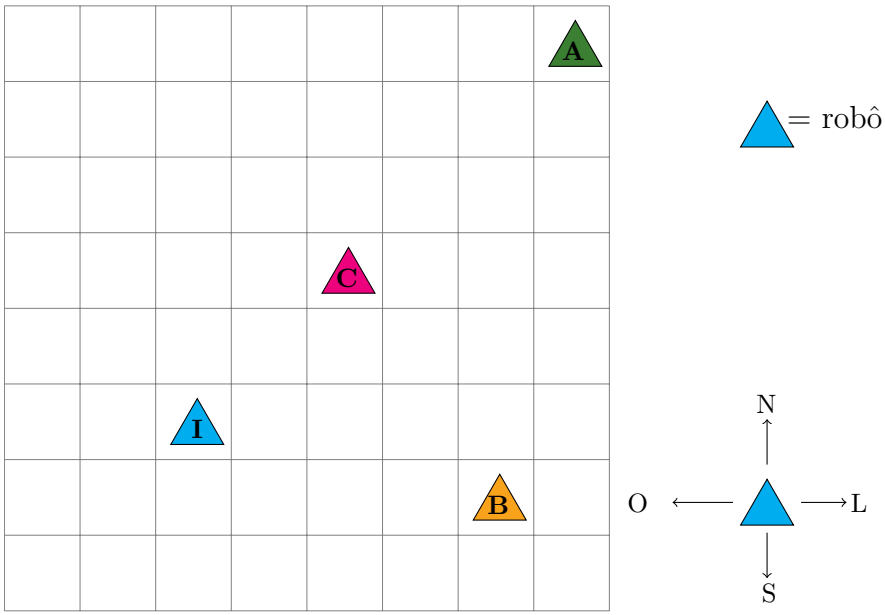
   (b) Qual é a mesagem correta que foi enviada?

$$00000 \longrightarrow 00000 \longrightarrow 00000 \longrightarrow 00000 \longrightarrow 10110 \longrightarrow$$

$$\longrightarrow 10110 \longrightarrow 10110 \longrightarrow 01011 \longrightarrow 01011 \longrightarrow 11101$$

(c) Sabendo que a posição inicia do robô é (I), em quais das posições abaixo ele deverá parar?

C



Referências

HEFEZ, Abramo; VILLELA, Maria Lúcia T. **Códigos corretores de erros**. Instituto de Matematica Pura e Aplicada, 2008.

A.5 Atividade 04 - Códigos Corretores de erros no dia-a-dia

O código de barras

Sumário

Hoje em dia, muitos produtos são identificados como códigos numéricos. Um exemplo são os produtos que compramos no supermercado. Esses são identificados por um código de barras barras, como o que mostramos na Figura 11 : não é mais do que um número, associado ao produto para sua identificação, escrito de forma a permitir uma leitura rápida no caixa. Note que, imediatamente abaixo das barras, aparece o mesmo número escrito em algarismos correntes, de forma que o leitor humano também possa ler o número

Figura 11: Código de barras

Fonte: http://www.ime.unicamp.br/ apmat/a-matematica-do-codigo-de-barras/

Algumas vezes acontece que, ao passar um produto pela leitora ótica (por exemplo, quando a embalagem está úmida ou enrugada), esta não consegue realizar a leitura. O que vemos então é que a pessoa que está na caixa tenta passar o produto em sentido contrário, ou inverte o produto, de modo que o código de barras fique de cabeça para baixo, e tenta passá-lo mais uma vez. Se nem assim dá certo, então ela lê e digita o código. Algumas perguntas então podem surgir:

- Em primeiro lugar, uma vez que o desenho das barras é totalmente simétrico para a máquina, que o lê usando um feixe de luz transversal, ao passá-lo "de ponta cabeça" ela não deveria ler o número na ordem contrária?

- O operador do caixa, ao digitar o número rapidamente, não poderia cometer um erro e nós acabarmos pagando por um produto muito mais caro que aquele que

estamos comprando?

Na prática isso não ocorre. O que ocorre é que mesmo lido ao contrário, o código sempre é interpretado de forma correta e se por acaso o operador do caixa cometa um erro de digitação, a máquina emite um aviso.

O objetivo dessa atividade é mostrar o aluno o funcionamento desses códigos e como os códigos corretores de erros são utilizados para isso.

Série

- 6° e 7° anos.

Unidade Temática

- Números

Objetos de conhecimento

- Operações (adição, subtração, multiplicação, divisão) com números naturais
- Divisão euclidiana
- Múltiplos e divisores de um número natural

Habilidades BNCC

- Resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora.
- Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000.
- Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.

Material

- Cópia da folha de atividade “Os códigos corretores de erros no cotidiano”.

Desenvolvimento

Inicie a atividade contando a história da criação dos códigos de barras.

A primeira patente de um código de barras foi atribuída em 1952 a Joseph Woodland e Bernard Silver.

O código consistia em um padrão de circunferências concêntricas de espessura variável. Ao dar entrada ao pedido de patentes, os dois cientistas descreviam sua nova invenção como uma classificação de artigos através de identificação de padrões.

Em torno de 1970, uma firma de assessoria, a McKinsey & Co., junto com a Uniform Grocery Product Code Council, definiu um formato numérico para identificar produtos e pediu a diversas companhias que elaborassem um código adequado para isso. Dentre as firmas contatadas, a que acabou apresentando a proposta vencedora foi a IBM, e o código foi criado por George J. Laurer.

Figura 12: Norman Joseph Woodland, George Laurer e Bernard Silve

Fonte: http://www.ime.unicamp.br/ apmat/a-matematica-do-codigo-de-barras/

O código proposto foi formalmente aceito em maio de 1973, e passou a ser conhecido como código UPC (Universal Product Code) e foi adotado nos Estados Unidos e no Canadá. Ele consistia em uma seqüência de 12 dígitos, traduzidos para barras.

Existem várias versões sucessivas do UPC, com pequenas modificações. Posteriormente foi solicitado a Laurer que ampliasse o código, para permitir uma maior difusão do sistema, de modo a identificar também o país de origem de cada produto classifi-

cado. assim, baseado no UPC-A, ele acabou criando um novo código, com 13 dígitos, que foi adotado em dezembro de 1976 com o nome EAN (European Article Numbering system). Alguns países adotam esse mesmo sistema, dando-lhe outro nome. Por exemplo, no Japão o sistema é conhecido como JAN (Japanese Article Numbering system).

A detecção de erros

Para compreender como funciona o processo de detecção de erros, precisamos entender, inicialmente, como se atribui a cada produto um dígito que permite essa detecção. Suponhamos que um determinado produto está identificado, no sistema EAN-13, por uma dada sequência de dígitos $a_1 a_2 \cdots a_{12} a_{13}$. Os primeiros doze dígitos identificam o país de origem, o fabricante e o produto específico, e são determinados naturalmente, por um método padrão, a cargo de uma autoridade classificadora em cada país. O décimo terceiro dígito, chamado dígito de verificação, é justamente o dado utilizado para a detecção de erros, e o denotaremos por x.

Para facilitar nossa exposição, vamos escrever essa sequência como um vetor

$$\alpha = (a_1, a_2, . \cdots , a_{11}, a_{12}, x).$$

O sistema EAN-13 se utiliza de um vetor fixo, que chamaremos vetor de pesos:

$$w = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1).$$

Calcula-se, então, o produto escalar de ambos os vetores multiplicando cada dígito do vetor de informação pelo número que ocupa a mesma posição no vetor de pesos:

$$\begin{aligned} \alpha \cdot w &= (a_1, a_2, . \cdots , a_{11}, a_{12}, x) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1) \\ &= a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + x \end{aligned}$$

Agora, o dígito de verificação x se escolhe de forma tal que a soma acima seja múltiplo de 10. O número 3 foi escolhido por ser o menor número diferente de 1 tal que $mdc(3, 10) = 1$.

Por exemplo, no caso do código da figura abaixo, os números que indicam o país de origem, o fabricante e o produto são 789883571789. Vamos ver como foi determinado

o dígito de verificação. Chamando esse dígito de x e fazendo o "produto escalar"com o vetor de pesos, temos:

Figura 13: Código EAN-13

Fonte: http://www.jrbarcode.com.br/blog/codigo-de-barras-ean-13/

$$7+(3\times 8)+9+(3\times 8)+3+(3\times 5)+7+(3\times 4)+1+(3\times 7)+8+(3\times 9)+x = 158+x$$

Consequentementes, escolhe-se $x = 2$.

O código UPC é muito semelhante. Como utiliza apenas 12 dígitos (pois usa apenas um para identificar o país de origem do artigo, enquanto o EAN utiliza-se de dois), e o vetor de pesos utilizado pelo UPC também tem um dígito a menos, ele é: $w = (3,1,3,1,3,1,3,1,3,1,3,1)$

Considerando o código de barras a seguir:

Temos:

$$(3\times 0)+1+(3\times 2)+3+(3\times 4)+5+(3\times 6)+7+(3\times 8)+9+(3\times 0)+x = 85+x$$

Consequentementes, escolhe-se $x = 5$.

Figura 14: Código UPC

Fonte: https://guelcos.com.br/

Folha de Atividade - Os códigos corretores de erros no cotidiano

1. Observe o código de barras a seguir.

   Suponha que por um erro de digitação, o código de barras 9414942010910 é transmitido como $\beta = 9414942010912$. Fazendo o produto escalar $\beta \cdot w$, onde $w = (1,3,1,3,1,3,1,3,1,3,1,3,1)$, como é possível identificar o erro?

   Efetuando o produto escalar $\beta \cdot w$, obtemos como resultado 78 que não é um múltiplo de 10, portanto, um erro foi cometido.

2. Qual é o dígito verificador x do produto identificado por $977100723720 - x$?

   Efetuando o produto escalar de $(9,7,7,1,0,0,7,2,3,7,2,0,x)$

por $w = (1,3,1,3,1,3,1,3,1,3,1,3,1)$, obtemos:

$$(9,7,7,1,0,0,7,2,3,7,2,0,x) \cdot (1,3,1,3,1,3,1,3,1,3,1,3,1) =$$

$$9+21+7+3+0+0+7+6+3+21+2+0+x = 79+x,$$

logo para termos um múltiplo de 10, devemos ter $x = 1$.

3. Esta mesma técnica de verificação é utilizada em códigos de livro. Livros publicados possuem um código de dez dígitos normalmente encontrados na contracapa. O décimo dígito é um dígito verificador. Isto significa que se você encomendar um livro usando o seu ISBN (International Standard Book Number – Padrão Internacional de Número de Livro), o editor pode verificar se você cometeu um erro. Eles simplesmente testam a soma verificadora. Assim, você não acaba esperando o livro errado !

   Veja como calcular a soma verificadora: multiplique por dez o primeiro dígito, o segundo por nove, o terceiro por oito, e assim por diante, até o nono dígito multiplicado por dois. Some esses valores.

   Por exemplo, o ISBN $0-13-911991-4$ fornece o seguinte valor

   $(0\times10)+(1\times9)+(3\times8)+(9\times7)+(1\times6)+(1\times5)+(9\times4)+(9\times3)+(1\times2) = 172$

   Em seguida, divida o resultado por onze. Qual é o resto ?

   $172 = 15 \times 11 + 7$, portanto o resto é 7.

   Se o resto for igual a zero, então a soma verificadora é zero. Caso contrário, subtraia 11 do resto para obter a soma verificadora.

   $11–7 = 4$.

   Portanto, 4 é o dígitor verificador.

   Agora é com você. Qual é o dígito verificador x do livro identificado por ISBN $85-7312-135-x$?

   Multiplicando os dígitos do código conforme o esquema, temos:

$$8\times10+5\times9+7\times8+3\times7+1\times6+2\times5+1\times4+3\times3+5\times2 = 241.$$

Efetuando a divisão por 11, obtemos: $241 = 11 \times 21 + 10$. Portanto, o resto é diferente de zero, logo o dígito verificador deverá ser $11 - 10 = 1$.

4. Toda pessoa que se inscreve no Cadastro de Pessoas Físicas da Receita Federal do Brasil recebe um número de inscrição de onze dígitos decimais com a seguinte configuração: ABC.DEF.GHI-JK.

   - Os primeiros oito dígitos, ABCDEFGH, formam o número-base definido pela Receita Federal no momento da inscrição.
   - O nono dígito, I, define a Região Fiscal responsável pela inscrição.
   - O penúltimo, J, é o dígito verificador dos nove primeiros.
   - O último, K, é o dígito verificador dos noves anteriores a ele.

Fonte: http://clubes.obmep.org.br/blog/a-matematica-nos-documentos-cpf/

A Região Fiscal onde é emitido o CPF (definida pelo nono dígito) tem as seguintes identificações:

No caso da 10ª Região Fiscal (Rio Grande do Sul), o algarismo zero é utilizado como nono dígito. Podem existir casos específicos em que esse nono dígito não esteja de acordo com os determinados acima.

Particularmente, no caso do CPF, os dois Dígitos Verificadores são calculados, a partir da esquerda, da seguinte maneira:

- Os nove primeiros algarismos são ordenadamente multiplicados pela sequência $10, 9, 8, 7, 6, 5, 4, 3, 2$ (o primeiro por 10, o segundo por 9, e assim sucessivamente). Em seguida, calcula-se o resto r da divisão da soma dos resultados das multiplicações por 11:
  - se esse resto for 0 ou 1, o primeiro dígito verificador é zero ($d_1 = 0$); caso contrário, $d_1 = 11 - r$.

Figura 15: Regiões fiscais

1 – DF, GO, MS, MT e TO
2 – AC, AM, AP, PA, RO e RR
3 – CE, MA e PI
4 – AL, PB, PE, RN
5 – BA e SE
6 – MG
7 – ES e RJ
8 – SP
9 – PR e SC
0 – RS

Fonte: http://clubes.obmep.org.br/blog/a-matematica-nos-documentos-cpf/

- O segundo Dígito Verificador (d_2) é calculado pela mesma regra, na qual os números a serem multiplicados pela sequência $10, 9, 8, 7, 6, 5, 4, 3, 2$ são contados a partir do segundo algarismo, sendo d_1 o último algarismo. Se s é o resto da divisão por 11 das somas das multiplicações, então:
  - d_2 é zero, se s for 0 ou 1; caso contrário, $d_2 = 11 - s$.

Considere o CPF que tem $093.412.856$ como seus nove primeiros dígitos.

(a) Determine seus dois dígitos verificadores.

Efetuando os produtos e as somas conforme o enunciado, temos:

$$0 \times 10 + 9 \times 9 + 3 \times 8 + 4 \times 7 + 1 \times 6 + 2 \times 5 + 8 \times 4 + 5 \times 3 + 6 \times 2 = 208.$$

$208 = 11 \times 18 + 10$, assim $d_1 = 11 - 10 = 1$. Assim, o CPF com o primeiro dígito verificador fica $093.412.856 - 1d_2$. Determinando d_2, temos:

$$9 \times 10 + 3 \times 9 + 4 \times 8 + 1 \times 7 + 2 \times 6 + 8 \times 5 + 5 \times 4 + 6 \times 3 + 1 \times 2 = 248.$$

$248 = 11 \times 22 + 6$, logo $d_2 = 11 - 6 = 5$. O CPF completo será $093.412.856-$

15.

(b) Qual o Estado Brasileiro responsável pela emissão do CPF?
Minas Gerais.

5. (ENEM – Adaptado) Suponha que João tenha perdido seus documentos, inclusive o cartão de CPF e, ao dar queixa da perda na delegacia, não conseguisse lembrar quais eram os Dígitos Verificadores, recordando-se apenas que os nove primeiros algarismos eram 123.456.789 Neste caso, os Dígitos Verificadores d_1 e d_2 esquecidos são, respectivamente:

   (a) 0 e 9.
   (b) 1 e 4.
   (c) 1 e 7.
   (d) 9 e 1.
   (e) 0 e 1.

Referências

MILIES, César Polcino.**A Matemática e o código de barras**. Revista do Professor de Matemática, n. 65, Rio de Janeiro 2009. Disponível em: https://www.rpm.org.br/cdrpm/65/9. Acesso em: 10 de abril de 2021.

_____ **A Matemática dos códigos de barras: detectando erros**. Revista do Professor de Matemática, n. 68, Rio de Janeiro 2009. Disponível em: https://www.rpm.org.br/cdrpm/65/9. Acesso em: 10 de abril de 2021.

OBMEP. **Clubes de Matemática da OBMEP - Disseminando o estudo da Matemática**. Disponível em:http://clubes.obmep.org.br/blog/a-matematica-nos-documentos-cpf/. Acesso em: 10 de abril de 2021.