UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Cristiano Isidoro da Silva

Códigos Cíclicos: uma proposta de sequência didática para o ensino de polinômios

RECIFE
2020

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Cristiano Isidoro da Silva

Códigos Cíclicos: uma proposta de sequência didática para o ensino de polinômios

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Profª. Dra. Bárbara Costa Silva

RECIFE
2020

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

S586c Silva, Cristiano Isidoro
Códigos Cíclicos: uma proposta de sequência didática para o ensino de polinômios / Cristiano Isidoro Silva. - 2020.
83 f. : il.

Orientador: Barbara Costa da Silva.
Inclui referências.

Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Mestrado Profissional em Matemática (PROFMAT), Recife, 2021.

1. Transmissão de mensagens. 2. Códigos Corretores de Erro. 3. Códigos Cíclicos. 4. Polinômios. I. Silva, Barbara Costa da, orient. II. Título

CDD 510

CRISTIANO ISIDORO DA SILVA

Códigos Cíclicos: uma proposta de sequência Didática para o ensino de polinômios.

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática – PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em ___ /___ /_____

BANCA EXAMINADORA

_____

Profª. Drª. Bárbara Costa da Silva (Orientadora)– UFRPE

_____

Prof. Dr. Éden Santana Campos Amorim – CEFET-MG

_____

Prof. Dr. Gabriel Araújo Guedes– PROFMAT/UFRPE

DECLARAÇÃO

Eu, CRISTIANO ISIDORO DA SILVA declaro, para devidos fins e efeitos, que a dissertação sob título "**Códigos Cíclicos: uma proposta de sequência didática para o ensino de polinômios"**, entregue como Trabalho de Conclusão de curso para obtenção do título de mestre, com exceção das citações diretas e indiretas claramente indicadas e referenciadas, é um trabalho original. Eu estou consciente que a utilização de material de terceiros incluindo uso de paráfrase sem a devida indicação das fontes será considerado plágio, e estará sujeito à processos administrativos da Universidade Federal Rural de Pernambuco e sanções legais. Declaro ainda que respeitei todos os requisitos dos direitos de autor e isento a Pós-graduação PROFMAT/UFRPE, bem como a professora orientadora BÁRBARA COSTA DA SILVA, de qualquer ônus ou responsabilidade sobre a sua autoria.

Recife, 7 de dezembro de 2020.

_____

Cristiano Isidoro da Silva

À minha família

Agradecimentos

Agradeço em primeiro lugar a Deus, pois sem Ele nada eu seria. À minha amada esposa Sâmela Isys que me apoiou e acreditou em mim durante todo período do mestrado. À minha filha Clarice que foi motivo de minha inspiração e força desde que chegou ao mundo. Aos meus pais Claudeny e Dulcilene pela educação que me deram e ao meu irmão Adriano por acreditar sempre em mim. À minha orientadora, Dra. Barbara Costa, pelas ricas contribuições durante toda orientação. Aos meus amigos Eliú Oliveira, Pedro Vitor, Valter Junior, Gabriel Brito, Peterson, Cícero e Luiz Manoel por tornarem o período do mestrado aprazível. Também quero agradecer a todos os professores do programa PROFMAT que contribuíram de forma efetiva com a minha formação.

"Não vos amoldeis às estruturas deste mundo,
mas transformai-vos pela renovação da mente,
a fim de distinguir qual é a vontade de Deus:
o que é bom, o que Lhe é agradável, o que é perfeito.
(Bíblia Sagrada, Romanos 12.2)

Resumo

A matemática está em toda parte. O problema é que muitas vezes não percebemos isso. Por exemplo, ao assistirmos televisão, ao enviarmos um e-mail, ao realizarmos uma ligação telefônica, ou ao utilizarmos qualquer meio de comunicação, a matemática está presente. De uma forma geral, quando uma mensagem é transmitida por qualquer meio de comunicação, existe um código numérico associado. Códigos corretores de erros são códigos utilizados no sistema de transmissão de mensagens, com o objetivo de recuperar uma informação perdida durante o processo de transmissão, na ocorrência de algum erro ou alteração na mensagem. Nesta dissertação, apresentamos os códigos cíclicos, um tipo de código corretor de erros, cuja relevância é possuir algoritmos de implementação de grande eficiência, baseados em operações com polinômios. Propomos uma sequência didática, direcionada para turma do 3º ano do Ensino Médio, que permite ao professor realizar uma aplicação com operações de polinômios em um tema relacionado ao cotidiano dos alunos.

Palavras-chave: Transmissão de mensagens, Códigos Corretores de Erros, Códigos Cíclicos, Polinômios.

Abstract

Mathematics is in everywhere. The problem is that we often don't realize this. For example, when watching television, sending an e-mail, making a phone call, or using any means of communication, mathematics is present. In general, when a message is transmitted by any means of communication there is an associated numeric code. Error correcting codes are codes used in the message transmission system, in order to recover lost information during the transmission process, in the event of an error or change in the message. In this dissertation, we present the cyclic codes, a type of error-correcting code, whose relevance is to have highly efficient implementation algorithms, based on operations with polynomials. We propose a didactic sequence, aimed at the 3rd year high school class, which allows the teacher to carry out an application with polynomial operations on a theme related to the students' daily lives.

Keywords: Transmission of messages, Error Correcting Codes, Cyclic Codes, Polynomials.

Lista de ilustrações

Sumário

Introdução

A Teoria dos Códigos Corretores de Erros, fundada pelo matemático C. E. Shannon, num trabalho publicado em 1948, foi inicialmente de interesse dos matemáticos, que deram grandes contribuições no período entre as décadas de 50 e 60. Com o passar dos anos, com o avanço nas pesquisas espaciais e a popularização dos computadores, passou também a ser do interesse dos engenheiros. Nos dias atuais, essa teoria se tornou um campo de pesquisa muito ativo em diversas áreas do conhecimento: matemática, engenharia, computação, estatística, biologia entre outras.

Recentemente, o avanço das tecnologias de comunicação vem sendo cada vez mais impressionante. É muito difícil encontrar uma pessoa que não foi influenciada pelo uso dessas novas tecnologias. Isto justifica a importância desses meios na vida da sociedade. Uma simples transmissão de mensagens escritas por correio eletrônico, de voz por telefone ou de imagens e sons da televisão, que estão presentes no nosso cotidiano, envolve uma teoria matemática, que permite ao usuário desses meios de comunicação uma transmissão de qualidade.

No processo da transmissão de informações, podem ocorrer algum tipo de interferência ou erro, que é chamado de ruído, fazendo com que a mensagem recebida seja diferente da enviada. Com o surgimento de um sistema de comunicação cada vez mais moderno, é possível fazer com que essa mensagem chegue ao receptor da forma mais confiável possível. O uso desses sistemas de comunicação torna possível o desenvolvimento de teorias matemáticas basilares às novas tecnologias, dentre elas, a Teoria dos Códigos Corretores de Erros.

Na experiência como professor, já ouvi de muitos alunos a seguinte pergunta: "Onde os polinômios serão usados na minha vida?"ou "Pra que serve esse ou aquele conteúdo de matemática e onde é aplicado?"Com base nesses tipos de pergunta, resolvemos elaborar essa dissertação que tem por objetivo principal propor uma sequência didática que possibilite ao professor do ensino básico apresentar aos seus alunos uma aplicação de polinômios em um tema relacionado com o cotidiano deles.

Vejamos a seguir as competências 3 e 4 específicas de matemática para o ensino médio, presentes no texto da BNCC [1] (11)(BRASIL, 2018, p. 531).

> 3. Utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente.

[1] Base Nacional Comum Curricular

> 4. Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas.

Nessas competências, consideramos relevante para os nossos propósitos a necessidade do uso de procedimentos matemáticos na construção de modelos e resolução de problemas em diversos contextos, e da utilização de registros algébricos e computacionais, na busca de solução e comunicação de resultados de problemas. Essas competências apoiam a ideia do estudo de aplicações matemáticas, que envolvem os diversos campos dessa ciência, entre eles a álgebra.

No primeiro capítulo, trazemos os principais resultados que servirão de material de apoio para o professor relembrar alguns conceitos das disciplinas de Anéis e Álgebra Linear. Os resultados apresentados nesse capítulo ajudarão na compreensão dos resultados posteriores encontrados principalmente no capítulo 3, no qual estudaremos os códigos cíclicos.

No segundo capítulo, além de descrever alguns fatos históricos, apresentamos os conceitos básicos da teoria, como definições de códigos corretores de erros, a métrica de Hamming, os parâmetros de um código, e finalizamos com o problema fundamental da teoria dos códigos.

No terceiro capítulo, estudamos os códigos cíclicos, numa abordagem voltada para o professor do ensino médio. No estudo desse código, utilizamos algoritmos de implementação muito eficientes baseados em operações com polinômios e multiplicação de matrizes.

No capítulo 4, produto final dessa dissertação, elaboramos uma proposta de sequência didática, voltada para alunos do Ensino Médio, turmas participantes de olimpíadas de matemática e alunos interessados. A sequência é composta por 7 aulas de 50 minutos. A primeira aula, aborda o conteúdo "Divisão euclidiana", que é ensinado no Ensino Fundamental - Anos Finais para compreensão da definição de corpos finitos. Vejamos o que diz a BNCC, com relação ao estudo dos conteúdos do Ensino Fundamental no Ensino Médio.

> A BNCC da área de Matemática e suas Tecnologias propõe a consolidação, a ampliação e o aprofundamento das aprendizagens essenciais desenvolvidas no Ensino Fundamental. Para tanto, propõe colocar em jogo, de modo mais inter-relacionado, os conhecimentos já explorados na etapa anterior, a fim de possibilitar que os estudantes construam uma visão mais integrada da Matemática, ainda na perspectiva de sua aplicação à realidade. (BRASIL, 2018, p. 527)

A BNCC prima pela aplicação dos conteúdos do Ensino Fundamental no Ensino Médio de forma mais aprofundada e integrada à realidade. As aulas 2, 3 e 4 tratam do estudo dos polinômios com coeficientes em corpos finitos. Nelas abordaremos raízes, divisão

e fatoração de polinômios com coeficientes em corpos finitos. As aulas 5, 6 e 7 dedicam-se à aplicação de códigos cíclicos no ensino médio, nos quais os alunos usarão operações de polinômios em algoritmos para codificação e decodificação de mensagens.

1 Um breve passeio pelas estruturas algébricas

Para melhor entendimento do estudo dos códigos cíclicos, trataremos nesse capítulo de alguns conceitos e resultados matemáticos fundamentais para o desenvolvimento da teoria. Para um estudo mais objetivo, alguns resultados que utilizaremos não serão demonstrados. Ao leitor interessado em um maior aprofundamento no conteúdo recomendamos uma consulta às referências (1), (2), (3) e (4).

1.1 Noções de anéis

Definição 1.1. Seja A um conjunto não vazio munido de duas operações, às quais chamaremos de *soma* e *produto* em A e denotaremos por $+$ e $\cdot$

Assim,

$$+ : \begin{array}{ccc} A \times A & \longrightarrow & A \\ (a,b) & \longmapsto & a+b \end{array} \quad \text{e} \quad \cdot : \begin{array}{ccc} A \times A & \longrightarrow & A \\ (a,b) & \longmapsto & a \cdot b \end{array}$$

Chamaremos a tripla $(A, +, \cdot)$ um anel comutativo com unidade, se as seguintes propriedades são verificadas, quaisquer que sejam $a, b, c \in A$.

(A1) $(a+b)+c = a+(b+c)$ (associatividade da soma);

(A2) Existe um elemento chamado *zero* e denotado por 0, de forma que $a+0 = 0+a = a$ (existência de elemento neutro para a soma);

(A3) Dado $a \in A$, existe um único elemento chamado *simétrico* de a e denotado por $-a$ tal que $a+(-a) = -a+a = 0$ (existência de inverso aditivo);

(A4) $a+b = b+a$ (comutatividade da soma);

(M1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatividade do produto);

(M2) Existe um elemento chamado unidade e denotado por 1 tal que $a \cdot 1 = 1 \cdot a = a$ (elemento neutro do produto);

(M3) $a \cdot b = b \cdot a$ (comutatividade do produto);

(AM) $a \cdot (b+c) = a \cdot b + a \cdot c$ (distributividade do produto em relação à soma).

Seja A um anel. Diremos que $a \neq 0$ um elemento de A é um *divisor de zero* se existir $b \in A$, com $b \neq 0$ tal que $a \cdot b = 0$. Diremos que o anel A é um *domínio de integridade* se A não possui divisores de zero.

Se A é um domínio de integridade então vale a Lei do Cancelamento, isto é, dados $a,\ b,\ c \in A$ tais que $c \neq 0$ e $a \cdot c = b \cdot c$, então $a = b$.

Exemplo 1.2. Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, juntamente com suas operações usuais de soma e produto são exemplos de domínios de integridade. Já o conjunto dos naturais $\mathbb{N}$ não é um anel, por não haver simétrico, nem elemento neutro da soma.

Um elemento a de um anel A será dito *invertível*, se existir um elemento $a^{-1} \in A$ de modo que $a \cdot a^{-1} = 1$. Assim diremos que a^{-1} é o inverso de a. Ao anel, onde todos os elementos não nulos são invertíveis, chamaremos de corpo.

Dos exemplos acima, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são exemplos de corpo, porém $\mathbb{Z}$ não é corpo, pois os únicos elementos invertíveis neste anel são 1 e -1. Assim, nem todo domínio é corpo.

Todo corpo A é um domínio de integridade, pois se $a \in A$ é um divisor de zero, então existe $b \in A$ com $b \neq 0$ tal que $a \cdot b = 0$. Sendo A corpo e $b \neq 0$ existe b^{-1} inverso de b. Daí,

$$a = a \cdot 1 = a \cdot (b \cdot b^{-1}) = (a \cdot b) \cdot b^{-1} = 0 \cdot b^{-1} = 0.$$

Definição 1.3. Seja A um anel e I um subconjunto de A. Diremos que I é um *ideal* de A se para todo $x, y \in I$ e $a \in A$ temos

i) $x + y \in I$.

ii) $a \cdot x \in I$.

Observe que $\{0\}$ e o próprio A são ideais de A. Se A é um anel e $a \in A$, então $A \cdot a$ é um ideal de A, chamado de *ideal principal* gerado por a. De formal geral, se $a_1, \cdots, a_n \in A$, então o conjunto

$$I = \{x_1 a_1 + \cdots + x_n a_n;\ \ x_1, \cdots, x_n \in A\}$$

é um ideal de A, e os elementos $a_1, \cdots, a_n$ são chamados de geradores de I.

Definição 1.4. Seja A um anel. Um ideal $\mathcal{M}$ é chamado de *ideal maximal* se $\mathcal{M} \neq A$ e se I é um ideal de A, de forma que

$$\mathcal{M} \subseteq I \subseteq A, \text{ então } I = \mathcal{M} \text{ ou } I = A.$$

Observação 1.5. Em relação ao anel dos inteiros, é possível mostrar que todo ideal de $\mathbb{Z}$ é principal. E dado $p \cdot \mathbb{Z} = I \subset \mathbb{Z}$, poderemos verificar também que p é um número primo se, e somente se I é um ideal maximal em $\mathbb{Z}$.

Seja A um anel e I um ideal de A, definiremos a relação $\equiv \mod I$ em A por:

$$x, y \in A, x \equiv y \mod I \Leftrightarrow x - y \in I.$$

A relação $\equiv \mod I$ define em A uma relação de equivalência.

A classe de equivalência do elemento $x \in A$ em relação a $\equiv \mod m$, denotada por $\overline{x}$, é o conjunto $\overline{x} = \{y \in A \mid y \equiv x \mod I\} = x + I$ e o conjunto das classes de equivalências, chamado de conjunto quociente, será denotado por $A/I = \{\overline{x} = x + I \mid x \in A\}$.

O próximo resultado nos permitirá definir as operações de adição e multiplicação no conjunto quociente A/I.

Proposição 1.6. *Seja A um anel e I um ideal em A. Se $a \equiv b \mod I$ e $c \equiv d \mod I$, então*

(i) $a + c \equiv b + d \mod I$

(ii) $a \cdot c \equiv b \cdot d \mod I$.

Observe que pela Proposição 1.6 a classe da soma não depende dos representantes das classes das parcelas, como de modo análogo ocorre com a classe do produto que não depende das classes dos fatores. Ou seja, as operações da adição e multiplicação em A/I, que serão apresentadas no próximo Teorema, estão bem definidas.

Teorema 1.7. *Seja A um anel e I um ideal de A. Se $\overline{x} = x + I$ e $A/I = \{\overline{x} \mid x \in A\}$, então*

i. *As operações de adição e multiplicação em A/I são definidas por*

$$\begin{array}{rcll} + : A/I \times A/I & \longrightarrow & A/I & \\ (\overline{x}, \overline{y}) & \longmapsto & \overline{x} + \overline{y} & = \overline{x + y} \end{array} \quad \text{e} \quad \begin{array}{rcll} \cdot : A/I \times A/I & \longrightarrow & A/I & \\ (\overline{x}, \overline{y}) & \longmapsto & \overline{x} \cdot \overline{y} & = \overline{x \cdot y} \end{array}$$

ii. *O conjunto A/I munido das operações de adição de multiplicação definidas no item acima é um anel, chamado de anel quociente de A por I;*

iii. *Se 1 é a unidade de A, então $\overline{1}$ é a unidade de A/I;*

iv. *Se A é um anel comutativo, então A/I é comutativo.*

Teorema 1.8. *Seja A um anel comutativo com unidade $1 \in A$ e seja I um ideal de A. Então I é ideal maximal de A se, e somente se, A/I é um corpo.*

Veremos agora como exemplo as operações de soma e produto em $\mathbb{Z}_m = Z/I$, em que $I = m\mathbb{Z}$, para alguns valores de m específicos.

Exemplo 1.9. Seja $m = 3$. Assim $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ e efetuando todas as operações de soma e produto possíveis com elementos de $\mathbb{Z}_3$, obteremos

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

e

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

.

Como $\overline{1}$ e $\overline{2}$ são invertíveis, $\mathbb{Z}_3$ é um corpo.

Exemplo 1.10. Seja $m = 4$. Logo $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ e fazendo todas as operações de soma e produto possíveis com elementos de $\mathbb{Z}_4$, teremos

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

e

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

.

Como $\overline{2}$ não é invertível, $\mathbb{Z}_4$ não é um corpo. Como $\overline{2} \cdot \overline{2} = \overline{0}$, esse anel não é um domínio de integridade.

Pela Observação 1.5 e Teorema 1.8 temos que $\mathbb{Z}_m$ é um corpo se, e somente se, m é um número primo.

1.1.1 Anéis de polinômios

Nesta seção, estudaremos o conceito de polinômios com coeficientes em um anel. Observaremos que as propriedades das operações de polinômios estão intimamente ligadas às propriedades da soma e produto no conjunto de seus coeficientes.

Seja A um anel. Chamaremos de um polinômio sobre A em uma *indeterminada* $X \notin A$ a expressão do tipo

$$P(X) = a_0 + a_1X + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i,$$

onde n é um inteiro não negativo, $a_i \in A$, para $0 \leq i \leq n$. É de costume não escrever o termo a_iX^i sempre que $a_i = 0$.

Dados dois polinômios $P(X) = a_0+a_1X+\cdots+a_nX^n$ e $Q(X) = b_0+b_1+\cdots+b_mX^m$, ambos com coeficientes em A. Diremos que $P(X) = Q(X)$ se, e somente se, $m = n$ e $a_i = b_i$ para $0 \leq i \leq n$.

Denotaremos por $A[X]$ o conjunto de todos os polinômios na indeterminada X com coeficientes em A.

Definiremos as operações de soma e produto de polinômios em $A[X]$, tomando como base as operações de soma e produto sobre A.

Definição 1.11. Sejam $P(X) = \sum_{i=0}^{n} a_i X^i$ e $Q(X) = \sum_{i=0}^{m} b_i X^i$ em $A[X]$, definiremos as operações de soma e produto em $A[X]$ como segue

$$P(X) + Q(X) = \sum_{i=0}^{\max\{n,m\}} c_i X^i,$$

onde $c_i = a_i + b_i$, e

$$P(X) \cdot Q(X) = \sum_{i=0}^{n+m} c_i X^i,$$

onde

$$\begin{aligned}
&c_0 = a_0 \cdot b_0 \\
&c_1 = a_0 \cdot b_1 + a_1 \cdot b_0 \\
&\vdots \\
&c_i = \sum_{\lambda+\mu=i} a_\lambda \cdot b_\mu = a_0 \cdot b_i + a_1 \cdot b_{i-1} + \cdots + a_i \cdot b_0 \\
&\vdots \\
&c_{n+m} = a_n \cdot b_m.
\end{aligned}$$

Teorema 1.12. *Com as operações acima definidas, $A[X]$ é um anel.*

Definição 1.13. Para todo polinômio $P(X)$ não identicamente nulo em $A[X]$, algum coeficiente deve ser distinto de zero. Então existe um maior índice $n \neq 0$, o qual chamaremos de *grau* de $P(X)$ e denotaremos por $gr(P(X))$. Neste caso, chamaremos a_n de *coeficiente líder* de $P(X)$.

Observação 1.14. Note que pela definição acima $gr(P(X)) = 0$ se, e somente se, $P(X) = a_0 \in A \setminus \{0\}$, e que o grau do polinômio nulo não é definido.

Proposição 1.15. *Seja A um domínio de integridade. As seguintes condições são satisfeitas.*

(i) *Se $P(X), Q(X) \in A[X] \setminus \{0\}$, então $gr(P(X) \cdot Q(X)) = gr(P(X)) + gr(Q(X))$;*

(ii) *$A[X]$ é um domínio de integridade;*

(iii) *Os elementos invertíveis de $A[X]$ são os elementos invertíveis de A.*

De agora em diante admitiremos que A é um corpo K. Segue do resultado acima que $K[X]$ é um domínio de integridade.

Definição 1.16. Os polinômios de grau n com coeficiente líder $a_n = 1$ são chamados de *polinômios mônicos*.

Iremos enunciar alguns resultados de divisibilidade, iniciando com o algoritmo euclidiano de divisão de polinômios com coeficientes em um corpo arbitrário K.

Definição 1.17. Sejam dois polinômios $F(X)$ e $G(X)$ no anel de polinômios $K[X]$ com coeficientes num corpo K. Diremos que $F(X)$ é *múltiplo* de $G(X)$ quando existe $H(X) \in K[X]$ tal que $F(X) = G(X) \cdot H(X)$. Para o caso em que $G(X) \neq 0$, diremos que $G(X)$ *divide* $F(X)$.

Proposição 1.18. *(Divisão Euclidiana)*

Seja K um corpo e $F(X), G(X) \in K[X]$, com $G(X) \neq 0$. Então, existem $Q(X)$ e $R(X)$ em $K[X]$, unicamente determinados, de modo que

$$F(X) = Q(X)G(X) + R(X),$$

em que $R(X) = 0$ ou $gr(R(X)) < gr(G(X))$.

Definição 1.19. Seja K um corpo e $F(X) \in K[X] \backslash K$. Diremos que $F(X)$ é um *polinômio irredutível* em $K[X]$ se possuir a seguinte propriedade:

- Se $F(X) = G(X) \cdot H(X)$, com $G(X), H(X) \in K[X]$, então $G(X)$ ou $H(X)$ é um polinômio constante não nulo.

Teorema 1.20. *(Fatoração única) Todo polinômio mônico em $K[X]$, não constante e não irredutível, pode ser escrito como produto de polinômios de $K[X]$ irredutíveis e mônicos. Essa escrita é única a menos da ordem dos fatores.*

Definição 1.21. Seja $P(X) \in K[X]$ e seja $\alpha \in K$, onde K é um anel. Diremos que α é uma raiz de $P(X)$, se $P(\alpha) = 0$.

Proposição 1.22. *Sejam K um corpo, $P(X) \in K[X]$ e $\alpha \in K$. Então α é uma raiz de $P(X)$ se, e somente se, $(X - \alpha)$ divide $P(X)$.*

Teorema 1.23. *Um polinômio de grau n com coeficientes num corpo K possui, no máximo, n raízes distintas sobre K.*

Estudaremos agora os ideais de $K[X]$ que serão fundamentais para o desenvolvimento e compreensão da teoria dos códigos cíclicos.

Proposição 1.24. *Todo ideal de $K[X]$ é da forma $I(F(X))$, onde $F(X) \in K[X]$.*

Dado um ideal I de $K[X]$, se $F(X)$ é um gerador de I, para toda constante não nula $c \in K$, $cF(X)$ também é um gerador de I. Como consequência dos resultados obtidos acima, temos o seguinte corolário:

Corolário 1.25. *Seja $I \neq \{0\}$ um ideal de $K[X]$. Então, existe um único polinômio mônico $F(X)$ em I (de grau mínimo), tal que $I = I(F(X))$.*

Estudaremos os anéis quocientes $K[X]/P(X)$, onde $P(X)$ é um polinômio não constante e mônico de grau n. Observe inicialmente que

$$K[X]/P(X) = \{\overline{R(X)}; R(X) \in K[X] \text{ com } R(X) = 0, \text{ ou } gr(R(X)) < n\}$$

e que dado $R_1(X), R_2(X) \in K[X]$ com $gr(R_1(X)) < n$ e $gr(R_2(X)) < n$, sendo $R_1(X) \neq R_2(X)$, então $\overline{R_1(X)} \neq \overline{R_2(X)}$.

Teorema 1.26. *O anel $K[X]/P(X)$ é um corpo se, e somente se, o polinômio $P(X)$ é irredutível.*

O resultado acima nos fornece uma forma prática para construção de corpos finitos. Dado $K = \mathbb{Z}_p$, em que p é um número primo positivo. Se $P(X) \in K[X]$ é irredutível com grau n, então $K[X]/P(X)$ é formado pelas classes de polinômios $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ em $K[X]$, e dois polinômios distintos de graus menores do que n definem classes distintas. O corpo $K[X]/P(X)$ tem p^n elementos. Veremos $\mathbb{Z}_p$ como um subcorpo de $K[X]/P(X)$ e identificaremos o elemento $\lambda \in K = \mathbb{Z}_p$ como $\overline{\lambda} \in K[X]/P(X)$.

Exemplo 1.27. Sejam $K = \mathbb{Z}_2$ e $P(X) = X^2 + X + 1$. Observe que $P(X)$ é irredutível em $K[X]$. Construiremos um corpo $\mathbb{F}_4$, cujos elementos listamos abaixo.

$$\mathbb{F}_4 = K[X]/P(X) = \{\overline{0}, \overline{1}, \overline{X}, \overline{1+X}\}.$$

As tabelas de operações de soma e produto de $\mathbb{F}_4$ são, respectivamente:

$+$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{1+X}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{1+X}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1+X}$	$\overline{X}$
$\overline{X}$	$\overline{X}$	$\overline{1+X}$	$\overline{0}$	$\overline{1}$
$\overline{1+X}$	$\overline{1+X}$	$\overline{X}$	$\overline{1}$	$\overline{0}$

,

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{1+X}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{1+X}$
$\overline{X}$	$\overline{0}$	$\overline{X}$	$\overline{1+X}$	$\overline{1}$
$\overline{1+X}$	$\overline{0}$	$\overline{1+X}$	$\overline{1}$	$\overline{X}$

.

Exemplo 1.28. Dado $P(X) = X^2 + 1 \in \mathbb{Z}_3[X]$, um polinômio irredutível. Poderemos construir um corpo $\mathbb{F}_9$ com 9 elementos, os quais descreveremos abaixo:

$$\mathbb{F}_9 = \{\overline{0}, \overline{1}, \overline{2}, \overline{X}, \overline{2X}, \overline{1+X}, \overline{1+2X}, \overline{2+X}, \overline{2+2X}\}.$$

Exemplo 1.29. Seja $K = \mathbb{Z}_2$ e $P(X) = X^7 - 1$. Observe que $\overline{1}$ é raiz de $P(X)$. Logo poderemos escrever

$$P(X) = (X+1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1).$$

Portanto, nesse caso, como $P(X)$ é redutível, pelo teorema 1.26, o conjunto $K[X]/P(X)$ não é corpo. Poderemos continuar com a fatoração do polinômio $Q(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$. Como $Q(X)$ não tem raízes em $\mathbb{Z}_2$ e $gr(Q(X)) = 6$, então poderemos considerar que, ou $Q(X)$ é irredutível, ou é produto de dois polinômios de grau 3, ou é produto de três polinômios de grau 2. Verificando os possíveis casos, teremos que o único polinômio de grau 2 irredutível sobre $\mathbb{Z}_2[X]$ é $X^2 + X + 1$, e como $(X^2 + X + 1)^3 \neq Q(X)$, concluíremos que $Q(X)$ só pode ser produto de dois polinômios irredutíveis de grau 3. Os únicos casos de irredutíveis de grau 3 em $\mathbb{Z}_2[X]$ são os polinômios $X^3 + X + 1$ e $X^3 + X^2 + 1$. Logo poderemos verificar que

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

Proposição 1.30. *Todo ideal de $K[X]/P(X)$ é da forma $I(\overline{F(X)})$, onde $F(X)$ é um divisor de $P(X)$.*

Demonstração. Seja I um ideal de $K[X]/P(X)$. Considere o conjunto

$$J = \{G(X) \in K[X];\ \overline{G(X)} \in I\}.$$

Iremos mostrar que J é um ideal de $K[X]$. Para isso, considere $G_1(X)$ e $G_2(X)$ elementos de J, o que significa que $\overline{G_1(X)}$ e $\overline{G_2(X)}$ estão em I. Desta maneira

$$\overline{G_1(X)} + \overline{G_2(X)} = \overline{G_1(X) + G_2(X)} \in I$$

assim $G_1(X) + G_2(X) \in J$.

No entanto, se $G(X) \in J$ e $H(X) \in K[X]$, como efeito $\overline{G(X)} \in I$, e sendo assim $\overline{G(X)} \cdot \overline{H(X)} = \overline{G(X)H(X)} \in I$. Portanto, $G(X)H(X) \in J$.

Como $P(X) \in J$, logo $J \neq \{0\}$, segue da proposição 4.6. que existe $F(X) \in K[X] \setminus \{0\}$ de forma que $J = I(F(X))$.

Como $P(X) \in J = I(F(X))$, segue que $P(X)$ é um múltiplo de $F(X)$, ou $F(X)$ é um divisor de $P(X)$.

Agora observe que $I = \{\overline{G(X)};\ G(X) \in J\}$, e como $J = I(F(X))$, poderemos concluir que

$$I = \{\overline{H(X)} \cdot \overline{F(X)};\ \overline{H(X)} \in K[X]/P(X)\} = I(\overline{F(X)}).$$

□

Para finalizar essa seção, veremos um exemplo de anel quociente que, apesar de não ser um corpo, será de extrema importância para o estudo do capítulo sobre códigos cíclicos.

Exemplo 1.31. O anel quociente $R_n = K[X]/(X^n - 1)$ onde seus elementos são da forma

$$\overline{F(X)} = \{F(X) + G(X)(X^n - 1); G(X) \in K[X]\}.$$

Observe que R_n não é um corpo, pois o polinômio $X^n - 1$, para $n \in \mathbb{Z}, n \geqslant 2$, não é irredutível, pois sempre é divisível por $X - 1$.

Uma outra forma de verificar que R_n não é um corpo, é o fato de não ser um domínio de integridade, pois como contraexemplo

$$\overline{X-1} \cdot \overline{X^{n-1} + \cdots + X + 1} = \overline{X^n - 1} = \overline{0}.$$

1.2 Noções de álgebra linear sobre corpos finitos

Estudaremos nesta seção, as noções básicas de álgebra linear necessárias para o estudo de códigos cíclicos.

Definição 1.32. Seja K um corpo, cujos elementos são chamados de *escalares*. Um *espaço vetorial* sobre K, ou um K-*espaço vetorial*, é um conjunto V, não vazio, munido de duas operações, uma operação de adição

$$\begin{array}{rccc} + : & V \times V & \longrightarrow & V \\ & (\mathbf{v}, \mathbf{w}) & \longmapsto & \mathbf{v} + \mathbf{w} \end{array}$$

e uma multiplicação dos elementos de V por escalares

$$\begin{array}{rccc} \cdot : & K \times V & \longrightarrow & V \\ & (\lambda, \mathbf{v}) & \longmapsto & \lambda \cdot \mathbf{v} \end{array}$$

possuindo as seguintes propriedades para quaisquer que sejam $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ e $\lambda, \mu \in K$:

(i) associatividade: $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$ e $(\lambda\mu)\mathbf{v} = \lambda(\mu\mathbf{v})$;

(ii) comutatividade da adição: $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$;

(iii) vetor nulo: Existe $\mathbf{0} \in V$ de forma que $\mathbf{u} + \mathbf{0} = \mathbf{u}$;

(iv) inverso aditivo: Existe $-\mathbf{u} \in V$ tal que $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$;

(v) distributividade: $(\lambda + \mu)\mathbf{v} = \lambda\mathbf{v} + \mu\mathbf{v}$ e $\lambda(\mathbf{u} + \mathbf{v}) = \lambda\mathbf{u} + \lambda\mathbf{v}$;

(vi) multiplicação pela unidade de K: $1 \cdot \mathbf{v} = \mathbf{v}$.

Um subespaço vetorial de um espaço vetorial V é um subconjunto $W \subset V$ que com as mesmas operações de adição e multiplicação de V, também é um K-espaço vetorial.

Definição 1.33. Seja V um espaço vetorial, um subconjunto $W \subset V$, não vazio, será um subespaço de V, se satisfaz as seguintes condições:

1. $\mathbf{0} \in W$;

2. Para quaisquer $\mathbf{u}, \mathbf{v} \in W$, $\mathbf{u} + \mathbf{v} \in W$;

3. Se $\mathbf{v} \in W$, então para todo $\lambda \in K$, $\lambda\mathbf{v} \in W$.

Note que as condições 2 e 3 na definição 1.33 podem ser substituídas por:

4. W é um subespaço de V se for cumprida a condição:

$$\forall\, \mathbf{u}, \mathbf{v} \in W,\ \forall\, \lambda \in K,\ \mathbf{u} + \lambda\mathbf{v} \in W.$$

Os espaços vetoriais de dimensão finita possuem uma estrutura algébrica apresentada pelas ideias de base e dimensão.

Um conjunto $\mathcal{B} = \{v_1, \cdots, v_n\}$ de vetores *linearmente independentes* é um conjunto cuja única combinação linear nula de seus vetores é aquela cujos coeficientes são todos iguais a zero. Em símbolos, temos

$$\lambda_1\mathbf{v}_1 + \cdots + \lambda_n\mathbf{v}_n = 0 \Longrightarrow \lambda_1 = \cdots = \lambda_n = 0.$$

No caso em que os vetores de $\mathcal{B}$ não são linearmente independentes, eles serão chamados linearmente dependentes. Isto significa que $\mathbf{v}_1, \cdots, \mathbf{v}_n$ são linearmente dependentes quando existem escalares $\lambda_1, \cdots, \lambda_n$ não todos nulos de modo que

$$\lambda_1\mathbf{v}_1 + \cdots + \lambda_n\mathbf{v}_n = 0.$$

Definição 1.34. Seja V um espaço vetorial. Uma base de V é um subconjunto $\mathcal{B} \subset V$ linearmente independente que *gera* V. Ou seja, todo vetor $v \in V$ pode ser representado de forma única, como combinação linear dos elementos da base $\mathcal{B}$.

Se um espaço vetorial V admite uma base com n elementos, então todas as bases de V têm o mesmo número n de elementos. Este número é chamado de *dimensão* de V.

Definição 1.35. Sejam V e W dois K-espaços vetoriais. Uma *transformação linear* $T : V \longrightarrow W$ é uma aplicação que associa a cada vetor $\mathbf{v} \in V$ um vetor $T(\mathbf{v}) \in W$ de forma que sejam verificadas para quaisquer $\mathbf{u}, \mathbf{v} \in V$ e $\lambda \in K$ as seguintes condições:

(i) $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$;

(ii) $T(\lambda \cdot \mathbf{v}) = \lambda \cdot T(\mathbf{v})$.

Dada a transformação linear $T : V \longrightarrow W$, existem dois subespaços essenciais para o estudo do comportamento de T: o núcleo de T, que é subespaço de V, e a imagem de T, que é um subespaço de W.

Definição 1.36. A *imagem* de T é o subconjunto $\mathcal{I}m(T) \subset W$ formado por todos os vetores $\mathbf{w} = T(\mathbf{v}) \in W$ que são imagens de elementos de V por T.

Diremos que a transformação T é *sobrejetora* se $\mathcal{I}m(T) = W$. Ou seja, para todo $\mathbf{w} \in W$, existe $\mathbf{v} \in V$ tal que $T(\mathbf{v}) = \mathbf{w}$.

Seja $X = \{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$ um conjunto de vetores que geram V. A transformação $T : V \longrightarrow W$ é sobrejetora se, e somente se, transforma X num conjunto de geradores de W. Isto significa que, se $\mathbf{v}_1, \cdots, \mathbf{v}_n$ geram V, os vetores $T(\mathbf{v}_1), \cdots, T(\mathbf{v}_n)$ geram W.

Definição 1.37. O *núcleo* da transformação linear $T : V \longrightarrow W$ é o conjunto dos vetores $\mathbf{v} \in V$ tais que $T(\mathbf{v}) = \mathbf{0}$. Denotaremos o núcleo de T por $\mathcal{N}(T)$.

Teorema 1.38. *Uma transformação linear $T : V \longrightarrow W$ é injetora se, e somente se, $\mathcal{N}(T) = \{\mathbf{0}\}$.*

Teorema 1.39. *Uma transformação linear é injetiva se, e somente se, leva vetores* **L.I.** *em vetores* **L.I.**

Definição 1.40. Diremos que uma transformação linear $T : V \longrightarrow W$ é *invertível* quando existe $T^{-1} : W \longrightarrow V$ linear de forma que $T^{-1}T = I_V$ e $TT^{-1} = I_W$.

Uma transformação linear T é invertível se, e somente se, ela é injetiva e sobrejetiva. Diremos então que T é uma *bijeção linear* entre V e W ou, mais precisamente, que $T : V \longrightarrow W$ é um *isomorfismo* e que os espaços vetoriais V e W são *isomorfos*.

Teorema 1.41. *(**Teorema do Núcleo e da Imagem**) Sejam V e W espaços vetoriais de dimensão finita. Se $T : V \longrightarrow W$ é uma transformação linear sobre um corpo K, então $dim_K \mathcal{N}(T) + dim_K \mathcal{I}m(T) = dim_K V$.*

Como consequência do teorema do núcleo e da imagem, segue o resultado abaixo.

Corolário 1.42. *Dados V e W espaços vetoriais de mesma dimensão finita n. Uma transformação linear $T : V \longrightarrow W$ é injetora se, e somente se, é sobrejetora e portanto é um isomorfismo.*

Demonstração. De fato, sendo $n = dim\mathcal{N}(T) + dim\mathcal{I}m(T)$. Logo $\mathcal{N}(T) = \mathbf{0}$ se, e somente se, $dim\mathcal{I}m(T) = n$, isto significa que, $\mathcal{I}m(T) = W$. □

Exemplo 1.43. O anel quociente $R_n = K[X]/(X^n - 1)$ do exemplo 1.31, com as operações de soma definida por

$$\overline{f_1(X)} + \overline{f_2(X)} = \overline{f_1(X) + f_2(X)}$$

e multiplicação por escalares $\lambda \in K$, definida por

$$\lambda\overline{f(X)} = \overline{\lambda f(X)},$$

é um k-espaço vetorial de dimensão n com base $1, \overline{X}, \cdots, \overline{X^{n-1}}$.

De fato, a soma e a multiplicação por escalar é bem definida, satisfazendo as propriedades da definição 1.32, e o conjunto $\{1, \overline{X}, \cdots, \overline{X^{n-1}}\}$ é **L.I.** dado que $\lambda_0 + \lambda_1\overline{X} + \cdots + \lambda_{n-1}\overline{X^{n-1}}$ se anula somente quando é multiplo de $X^n - 1$. E nesse caso, isso ocorre apenas quando $\lambda_0 = \lambda_1 = \ldots = \lambda_{n-1} = 0$.

Exemplo 1.44. Considere a aplicação

$$\begin{array}{ccc} \sigma : K^n & \longrightarrow & R_n \\ (a_0, ..., a_{n-1}) & \longmapsto & \overline{a_0 + a_1X + ... + a_{n-1}X^{n-1}}. \end{array}$$

Seja $u, v \in K^n$ e $\lambda \in K$ com $u = (u_0, ..., u_{n-1})$ e $v = (v_0, ..., v_{n-1})$. Assim,

$$\sigma(u + \lambda v) = \overline{(u_0 + \lambda v_0) + (u_1 + \lambda v_1)X + ... + (u_{n-1} + \lambda v_{n-1})X^{n-1}}$$

$$= \overline{u_0 + u_1X + ... + u_{n-1}X^{n-1} + \lambda(v_0 + v_1X + ... + v_{n-1}X^{n-1})}$$

$$= \overline{u_0 + u_1X + ... + u_{n-1}X^{n-1}} + \lambda\overline{v_0 + v_1X + ... + v_{n-1}X^{n-1}}$$

$$= \sigma(u) + \lambda\sigma(v).$$

Logo σ é uma transformação linear e, pelo corolário 1.42 R_n é isomorfo a K^n através de σ.

A ideia de isomorfismo entre espaços vetoriais é imprescindível, pois nos permite relacionar, sob a perspectiva algébrica, espaços que se apresentam de formas distintas aparentemente, mas que são indistinguíveis algebricamente. Por exemplo, a correspondência $(a_0, \cdots, a_{n-1}) \longleftrightarrow a_0X + \cdots + a_{n-1}X^{n-1}$, é um isomorfismo natural entre K^n e $\mathcal{P}_{n-1}$, onde $\mathcal{P}_{n-1}$ é o espaço dos polinômios de grau menor ou igual a $n - 1$, que possui dimensão n.

2 Códigos que corrigem erros

A Teoria dos códigos corretores de erros, hoje em dia, é muito aplicada nos campos da engenharia, computação, matemática, entre outros. O objetivo principal dessa teoria é de garantir com precisão e eficácia, sempre que possível, a transferência, do remetente ao receptor, da informação desejada. Para elaboração deste capítulo foram estudados (1), (6) e (8).

Fundada pelo matemático Claude E. Shannon, num artigo publicado em 1948, intitulado "*A Mathematical Theory of Communications*", a Teoria dos Códigos Corretores de Erros foi inicialmente de interesse dos matemáticos, que foram responsáveis por grande parte do desenvolvimento da Teoria nas décadas de 50 e 60. Nesse período se destacam a construção dos códigos de Hamming, para simples correção de erros, e a construção dos poderosos códigos de Reed-Solomon. Na década de 70, com as pesquisas avançadas nas explorações espaciais e o advento da popularização dos computadores, houve também o interesse dos engenheiros no estudo dos códigos corretores de erros.

Para um bom esclarecimento da ideia dessa teoria, usaremos um exemplo. Suponhamos que uma máquina de impressão utiliza as cores Ciano, Magenta, Amarelo e Preto, para desenvolver o seu trabalho. E que ao darmos o comando de impressão ela receba a informação das cores que serão usadas para realizar a impressão.

Poderemos codificar as quatro cores acima como elementos de $\{0,1\} \times \{0,1\}$, da seguinte forma:

Ciano	$\longmapsto$	00	Amarelo	$\longmapsto$	10
Magenta	$\longmapsto$	01	Preto	$\longmapsto$	11

Admitiremos agora que essas mensagens sejam transmitidas de um computador via cabo para nossa máquina de impressão e que durante a transmissão ocorra alguma interferência. Imagine que no lugar da mensagem 10 transmitida, recebamos a mensagem 11. Isto nos traria um problema, pois onde seria usado a cor Amarelo, agora, com o erro de transmissão, será usado a cor Preto. Dessa forma se faz necessário recodificar as mensagens inserindo dígitos de redundância, que permitam detectar e corrigir erros.

Assim, por exemplo, poderemos modificar o nosso código de acordo com a tabela abaixo:

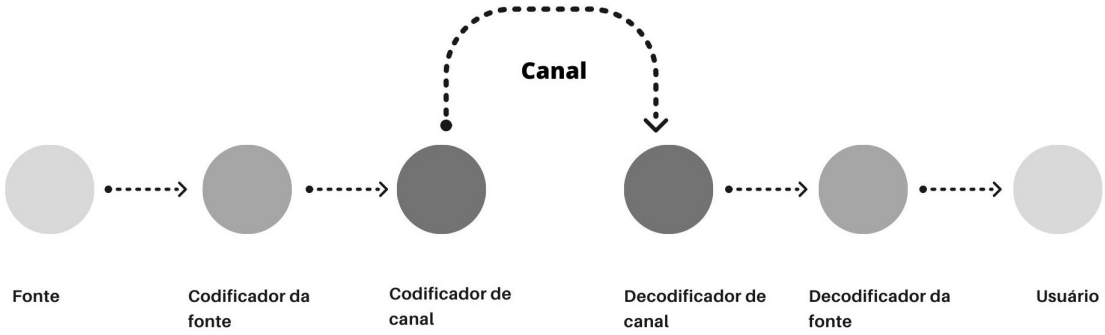
Fonte	Código da fonte	Código de canal
Ciano	00	00000
Magenta	01	01011
Amarelo	10	10110
Preto	11	11101

Nessa nova recodificação, a primeira coluna da tabela, chamada de *fonte*, representa a mensagem original. Na segunda coluna temos o *código da fonte*; e na terceira coluna o *código de canal*, que nos permite detectar e corrigir possíveis erros na transmissão.

Imagine agora que durante uma transmissão da palavra 10110 ocorra um erro e a palavra recebida seja 10010. Realizando uma comparação dessa mensagem recebida, com as mensagens do código, perceberemos que ela não pertence ao código, assim saberemos que existe um erro e, portanto verificaremos que a palavra do código que tem o menor número de componentes distintos da palavra recebida é 10110, que é corretamente a palavra transmitida.

A figura 1 abaixo representa bem o procedimento de transmissão da informação.

Figura 1 – Esquema de Transmissão da Informação



Fonte: Elaborada pelo autor

O canal é o meio pelo qual a mensagem é transmitida. Por exemplo, pode ser um cabo, um canal de radiofrequência, canal de micro-ondas, disco de armazenamento, ou qualquer outro meio que represente uma rede de comunicação.

Nesse trabalho, abordaremos bem todo processo do esquema da figura 1, enfatizando a detecção e correção de erros, sempre que possível.

2.1 A métrica de Hamming

Para entender como construir um código corretor de erros, inicialmente definiremos alguns conceitos básicos e notações que utilizaremos a partir daqui.

Um *alfabeto* é um conjunto finito $A_q = \{a_1, a_2, \cdots, a_q\}$.

Usaremos $|A|$ para denotar a quantidade de elementos do conjunto A, e o símbolo q para representar essa quantidade.

Uma *palavra* é uma sequência finita de símbolos do alfabeto. Ao número de símbolos de uma palavra chamamos de *seu comprimento*.

Um *código corretor de erros* é um subconjunto de A_q^n, para n natural, onde n é o comprimento das palavras do código.

Definição 2.1. Seja $\mathbf{u}$ e $\mathbf{v}$ elementos de A_q^n, a *distância de Hamming* entre $\mathbf{u}$ e $\mathbf{v}$ é definida como

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

Exemplo 2.2. Considere o exemplo da máquina de impressão apresentado no início deste capítulo. Assim teremos

$$\begin{array}{rcl} d(01011, 10110) & = & 4 \\ d(00000, 01011) & = & 3 \end{array}$$

Proposição 2.3. *Dados* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in A_q^n$*, valem as seguintes propriedades:*

1. *Positividade:* $d(\mathbf{u}, \mathbf{v}) \geqslant 0$*, valendo a igualdade se, e somente se,* $\mathbf{u} = \mathbf{v}$*.*

2. *Simetria:* $d(\mathbf{u}, \mathbf{v}) = d(\mathbf{v}, \mathbf{u})$*.*

3. *Desigualdade Triangular:* $d(\mathbf{u}, \mathbf{v}) \leqslant d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$*.*

Demonstração. Para primeira propriedade, como $d(\mathbf{u}, \mathbf{v})$ é por definição a quantidade de elementos de um conjunto, não pode ser negativa. Para segunda propriedade, basta verificar que comparar as coordenadas entre duas palavras $\mathbf{u}$ e $\mathbf{v}$ independe da ordem das palavras. Na terceira propriedade, temos dois casos:

i) Se $u_i = v_i$, para todo i, então por definição $d(\mathbf{u}, \mathbf{v}) = 0$. E por (**1**.) segue que

$$d(\mathbf{u}, \mathbf{v}) \leqslant d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v}).$$

ii) Se $u_i \neq v_i$, não podemos ter $u_i = w_i$ e $w_i = v_i$, logo segue que

$$d(\mathbf{u}, \mathbf{v}) \leqslant d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v}).$$

□

Definição 2.4. Dado um conjunto $\mathcal{X}$, uma *métrica* sobre $\mathcal{X}$ é uma função

$$d : \mathcal{X} \times \mathcal{X} \longrightarrow \mathbb{R}$$

que goza das propriedades da proposição 2.3. Por isso, a distância de Hamming entre elementos de A_q^n é também chamada de *métrica de Hamming*.

Definição 2.5. Dados $\mathbf{a} \in A_q^n$ e $t \in \mathbb{R}$, com $t \geqslant 0$, definimos a *bola* e a *esfera* de centro $\mathbf{a}$ e raio t, como sendo, respectivamente, os conjuntos finitos

$$B(\mathbf{a}, t) = \{\mathbf{u} \in A_q^n;\ d(\mathbf{u}, \mathbf{a}) \leqslant t\},$$

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

O próximo lema nos fornecerá as cardinalidades desses conjuntos.

Lema 2.6. *Quaisquer que sejam* $\mathbf{a} \in A_q^n$ *e* $r > 0$*, com* $r \in \mathbb{N}$*, tem-se que*

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

Demonstração. Primeiro vamos mostrar que

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

Como $\mathbf{a} \in A_q^n$, logo precisaremos escolher i componentes dentre as n possibilidades. Essa escolha pode ser feita de $\binom{n}{i}$ maneiras. Agora basta trocar o símbolo de cada uma das i componentes escolhidas, onde para cada uma teremos $q-1$ possibilidades, daí segue o resultado.

Observe que $S(\mathbf{a}, i) \cap S(\mathbf{a}, j) = \emptyset$ sempre que $i \neq j$. Assim segue que

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

Assim, obteremos que

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

□

Definição 2.7. Seja C um código. A *distância mínima* de C é o número

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

Observe, na tabela a seguir, que no exemplo do código da máquina de impressão, dado no início desse capítulo, a distância mínima é $d = 3$.

$\mathbf{u}$	$\mathbf{v}$	$\mathbf{d}(\mathbf{u}, \mathbf{v})$
00000	01011	3
00000	10110	3
00000	11101	4
01011	10110	4
01011	11101	3
10110	11101	3

Definição 2.8. Sejam $a, b \in \mathbb{Z}$. Chamaremos de *parte inteira* de $\frac{a}{b}$ o maior inteiro menor ou igual a $\frac{a}{b}$. Denotaremos por $\lfloor \frac{a}{b} \rfloor$.

Por exemplo, considerando $a = 3$ e $b = 2$, a parte inteira de $\frac{3}{2}$ é o maior inteiro na reta real que aparece a esquerda do número $\frac{3}{2}$. E portanto, $\lfloor \frac{3}{2} \rfloor = 1$.

Observação 2.9. Escrevendo a divisão euclidiana de a por b, obteremos

$$a = bq + r, \quad \text{com } 0 \leqslant r < b,$$

temos

$$bq \leqslant bq + r < bq + b,$$

e, portanto

$$bq \leqslant a < b(q + 1)$$

dividindo a desigualdade por b, segue que

$$q \leqslant \frac{a}{b} < q + 1.$$

Logo o quociente q da divisão euclidiana é o maior inteiro menor ou igual a $\frac{a}{b}$.

Definição 2.10. Dado um código C, com distância mínima d, define-se $k = \lfloor \frac{d-1}{2} \rfloor$.

Lema 2.11. *Dado C um código com distância mínima d. Se $\mathbf{c}$ e $\mathbf{c}'$ são palavras distintas de C, então*

$$B(\mathbf{c}, k) \cap B(\mathbf{c}', k) = \emptyset.$$

Demonstração. Se $\mathbf{x} \in B(\mathbf{c}, k) \cap B(\mathbf{c}', k)$, então $d(\mathbf{x}, \mathbf{c}) \leqslant k$ e $d(\mathbf{x}, \mathbf{c}') \leqslant k$, e, pela simetria, pela desigualdade triangular e pela Observação 2.9,

$$d(\mathbf{c}, \mathbf{c}') \leqslant d(\mathbf{c}, \mathbf{x}) + d(\mathbf{x}, \mathbf{c}') \leqslant 2k \leqslant d - 1,$$

que é um absurdo, pois $d(\mathbf{c}, \mathbf{c}') \geqslant d$. □

O resultado a seguir, mostrará a importância da distância mínima d de um código.

Teorema 2.12. *Seja C um código de distância mínima d e $k = \lfloor \frac{d-1}{2} \rfloor$. Então C pode detectar até $d - 1$ erros e corrigir até k erros.*

Demonstração. Se durante a transmissão de uma palavra $\mathbf{c}$ do código ocorre i erros, com $i \leqslant k$, e receberemos a palavra $\mathbf{r}$, então $d(\mathbf{r}, \mathbf{c}) = i \leqslant k$. Mas pelo Lema 2.11, como $B(\mathbf{c}, k) \cap B(\mathbf{c}', k) = \emptyset$ e $\mathbf{r} \in B(\mathbf{c}, k)$, então $\mathbf{r} \notin B(\mathbf{c}', k)$, ou seja, a distância de $\mathbf{r}$ a qualquer

outra palavra do código diferente de c é maior de que k. Assim, temos que a palavra c está univocamente determinada a partir de r.

Para detecção de erros, dada uma palavra do código, é possível inserir nela até $d-1$ erros, sem encontrar outra palavra do código, possibilitando assim a detecção do erro. □

Observe que pelo Teorema 2.12 acima, quanto maior for a distância mínima d maior a capacidade de correção do código, porém aumentar a distância mínima siginifica aumentar o comprimento das palavras do código, então para obtermos bons códigos de correção de erros, é fundamental encontrar um equilíbrio entre esses parâmetros. Isso torna a distância mínima fundamental na Teoria dos Códigos. O teorema ainda nos diz que, se uma palavra recebida $\mathbf{r}$ encontra-se numa bola de raio k cujo centro é uma palavra $\mathbf{c}$ do código, essa palavra $\mathbf{c}$ é única, sendo $\mathbf{c}$ a palavra do código enviada.

Definição 2.13. Dado $C \subset A_q^n$ um código com distância mínima d e seja $k = \lfloor \frac{d-1}{2} \rfloor$. Se

$$\bigcup_{\mathbf{c} \in C} B(\mathbf{c}, k) = A_q^n,$$

então o código C será chamado de *código perfeito*.

Definição 2.14. Seja $\mathbf{a} \in A_q^n$, o peso de $\mathbf{a}$ é definido como

$$\omega(\mathbf{a}) := |\{i; a_i \neq 0\}|,$$

ou seja, é o número de coordenadas não nulas de $\mathbf{a}$.

Em particular, o peso de um código $C \subset A_q^n$ é o inteiro

$$\omega(C) := \min\{\omega(\mathbf{a});\ \mathbf{a} \in C \backslash \{\mathbf{0}\}\}.$$

Proposição 2.15. *Seja $C \subset A_q^n$ um código com distância mínima d. Se C é fechado para a subtração, então vale a seguinte igualdade:*

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

Demonstração. Sejam $\mathbf{a}, \mathbf{a}' \in C$. Como C é fechado para subtração, $(\mathbf{a} - \mathbf{a}') \in C$. Assim a contribuição das i-ésimas coordenadas de $\mathbf{a}$ e $\mathbf{a}'$ para $d(\mathbf{a}, \mathbf{a}')$ é zero se $a_i - a_i' = 0$.

No caso em que a contribuição das i-ésimas coordenadas de $\mathbf{a}$ e $\mathbf{a}'$ para $d(\mathbf{a}, \mathbf{a}')$ é igual a um, teremos que $a_i - a_i' \neq 0$. Portanto $d(\mathbf{a}, \mathbf{a}') = \omega(\mathbf{a} - \mathbf{a}')$. Concluíremos dessa forma que

$$d = \min\{d(\mathbf{a}, \mathbf{a}');\ \mathbf{a}, \mathbf{a}' \in C \text{ e } \mathbf{a} \neq \mathbf{a}'\} = \min\{\omega(\mathbf{b});\ \mathbf{b} \in C, \mathbf{b} \neq 0\}.$$

onde $\mathbf{b} = \mathbf{a} - \mathbf{a}'$. □

Assim a proposição acima nos fornece uma forma mais simples de encontrar a distância mínima, em que basta verificar a palavra que mais se aproxima do vetor nulo.

2.2 O problema fundamental da teoria dos códigos

Um código C sobre um alfabeto A_q é bem determinado por três parâmetros fundamentais $[n, M, d]$, onde n é o seu comprimento, M o número de palavras do código, e d a sua distância mínima. Para um código ter uma boa eficiência, é desejável que M e d sejam grandes em relação a n. Mas construir códigos que satisfazem essa relação é o **problema principal da teoria dos códigos**.

No que se refere a essa interdependência entre os parâmetros de um código, existem alguns resultados desenvolvidos para análise do problema. O leitor interessado nas demonstrações dos resultados abaixo deve consultar (1).

Teorema 2.16. *(Cota de Singleton) Seja C um código com parâmetros $[n, M, d]$, definido sobre um alfabeto A_q. A seguinte relação é verificada.*

$$M \leqslant q^{n-d+1}.$$

Teorema 2.17. *(Cota de Hamming) Seja C um código com parâmetros $[n, M, d]$. Se $k = \lfloor \frac{d-1}{2} \rfloor$, então*

$$M \leqslant \frac{q^n}{\sum_{i=0}^{r} \binom{n}{i}(q-1)^i},$$

valendo a igualdade se, e só se, C é um código perfeito.

Analisando o problema de um outro ponto de vista, considere a função:

$$A_q(n, d) = \max\{M;\ \text{existe um código com parâmetros } [n, M, d]\}.$$

Definição 2.18. Um código A_q com os parâmetros $[n, M, d]$ se diz *ótimo* se $M = A_q(n, d)$.

Pouco se sabe ainda sobre $A_q(n, d)$. Porém, segue abaixo um dos resultados obtidos, em relação à cota de Hamming, que limita esses valores.

Corolário 2.19. *Para todos os números naturais n e d, segue que*

$$A_q(n, d) \leqslant \frac{q^n}{\sum_{i=0}^{r} \binom{n}{i}(q-1)^i}.$$

O próximo resultado nos dará uma cota inferior para $A_q(n, d)$, descoberta independentemente por Gilbert em 1952 e por Varshamov em 1957.

Teorema 2.20. *(Cota de Gilbert-Varshamov) Para todos os números naturais n e d com $n \geqslant d$, segue que*

$$A_q(n, d) = \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}.$$

3 Códigos cíclicos

Os códigos cíclicos se tornam atraentes por terem uma estrutura algébrica de fácil implementação, que nos possibilita encontrar vários métodos práticos para codificação e decodificação. Para o desenvolvimento deste capítulo foram estudados (1), (5), (7) e (9).

3.1 Caracterização dos códigos cíclicos

Seja K um corpo finito e seja $v = (v_0, v_1, ..., v_{n-1}) \in K^n$. Ao deslocarmos cada coordenada de v uma vez para a direita, e a última coordenada para a posição da primeira, obtemos um novo vetor $v^{(1)} = (v_{n-1}, v_0, ..., v_{n-2}) \in K^n$. Esse procedimento é o que chamamos de deslocamento cíclico de v à direita, cuja ordem é 1. Analogamente, podemos realizar um deslocamento cíclico de v à esquerda.

Se as coordenadas de v forem deslocados ciclicamente i vezes para a direita, o vetor resultante seria $v^{(i)} = (v_{n-i}, v_{n-i+1}, ..., v_{n-1}, v_0, ..., v_{n-i-1})$. Observe que deslocar ciclicamente v i vezes para a direita é equivalente a deslocar ciclicamente v $n - i$ vezes para a esquerda.

Definição 3.1. Seja K um corpo finito e seja $C \subset K^n$. Dizemos que C é um código cíclico se:

i. C é um subespaço de K^n;

ii. se para todo $v \in C$ temos $v^{(1)} \in C$.

Da definição de códigos cíclicos dada acima, concluímos que $C \subset K^n$ é um espaço vetorial de dimensão finita. Seja k a dimensão de C e $b_1, \cdots, b_k$ uma base de C, todos os elementos de C podem ser escritos da forma

$$\lambda_1 b_1 + \cdots + \lambda_k b_k,$$

em que $\lambda_i \in K$ com $i = 1, \cdots, k$. Assim denotaremos por $C(n, k)$ um código cíclico $C \subset K^n$ de comprimento n e dimensão k.

Exemplo 3.2. São exemplos de códigos cíclicos "não interessantes", os códigos $C = \mathbf{0}$, onde $\mathbf{0}$ é o vetor nulo, e $C = K^n$.

Sabemos que uma forma de obter subespaços de K^n é considerar os espaços gerados por um conjunto finito de vetores de K^n. Mostramos, no próximo exemplo, que dado $v \in K^n$ o subespaço $C = \langle v, v^{(1)}, \ldots, v^{(n-1)} \rangle$ é um código cíclico. Além disso, no corolário

3.8, mostramos que dado um código cíclico C de comprimento n, existe um vetor $v \in K^n$ tal que $C = \langle v, v^{(1)}, \ldots, v^{(n-1)} \rangle$. Para simplificar a notação usamos $C = \langle v \rangle$ para representar $C = \langle v, v^{(1)}, \ldots, v^{(n-1)} \rangle$.

Exemplo 3.3. Seja K um corpo finito e seja $v \in K^n$. Então $C = \langle v \rangle$ é um código cíclico.

Basta mostrar que, se dado um vetor arbitrário $u \in C = \langle v, v^{(1)}, \ldots, v^{(n-1)} \rangle$, então $u^{(1)} \in C$.

Então dada a matriz

$$V = \begin{pmatrix} v \\ v^{(1)} \\ \vdots \\ v^{(n-1)} \end{pmatrix} = \begin{pmatrix} v_0 & v_1 & \ldots & v_{n-1} \\ v_{n-1} & v_0 & \ldots & v_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ v_1 & v_2 & \ldots & v_0 \end{pmatrix}.$$

E seja

$$\Lambda = \begin{pmatrix} \lambda_0 & \lambda_1 & \ldots & \lambda_{n-1} \end{pmatrix}$$

em que $\lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in K$. Considerando

$$u = \lambda_0 v + \lambda_1 v^{(1)} + \ldots + \lambda_{n-1} v^{(n-1)} = \Lambda V.$$

Observe que $\Lambda V = u$ e $u^{(1)} = \Lambda^{(1)} V$.

$$\underbrace{\begin{pmatrix} \lambda_0 v_0 + \lambda_1 v_{n-1} + \ldots + \lambda_{n-1} v_1 \\ \lambda_0 v_1 + \lambda_1 v_0 + \ldots + \lambda_{n-1} v_2 \\ \vdots \\ \lambda_0 v_{n-1} + \lambda_1 v_{n-2} + \ldots + \lambda_{n-1} v_0 \end{pmatrix}}_{u^t} \quad \underbrace{\begin{pmatrix} \lambda_0 v_{n-1} + \lambda_1 v_{n-2} + \ldots + \lambda_{n-1} v_0 \\ \lambda_0 v_0 + \lambda_1 v_{n-1} + \ldots + \lambda_{n-1} v_1 \\ \vdots \\ \lambda_0 v_{n-2} + \lambda_1 v_{n-3} + \ldots + \lambda_{n-1} v_{n-1} \end{pmatrix}}_{(u^{(1)})^t}.$$

Deslocar cíclicamente para direita as coordenadas do vetor u é o mesmo que deslocar ciclicamente as constantes na combinação linear dos vetores $v, v^{(1)}, \ldots, v^{(n-1)}$. Assim

$$u^{(1)} = \lambda_{n-1} v + \lambda_0 v^{(1)} + \ldots + \lambda_{n-2} v^{(n-1)} \in C = \langle v \rangle.$$

Em particular, considere $K = \mathbb{F}_2$ e seja $\mathbf{v} = (10011001) \in K^8$. Como $v^{(4)} = v$ segue que

$$C = \langle \mathbf{v} \rangle = K(10011001) + K(11001100) + K(01100110) + K(00110011) \tag{3.1}$$

Como $K = \mathbb{F}_2$ é um corpo com dois elementos então C é um código em exatamente 8 palavras, mais especificamente,

$$C = \{(10011001), (01010101), (00110011), (00000000),$$

$$(11001100), (10101010), (01100110), (11111111)\}.$$

A partir de agora vamos mostrar alguns resultados que relacionam cada código cíclico com um polinômio irredutível no anel $R_n = K[X]/(X^n - 1)$, definido no exemplo 1.31. Lembre-se que no exemplo 1.43 mostramos que R_n também é um espaço vetorial.

Considerando a aplicação

$$\begin{array}{rcl} \sigma : K^n & \longrightarrow & R_n \\ (a_0, ..., a_{n-1}) & \longmapsto & \overline{a_0 + a_1X + ... + a_{n-1}X^{n-1}} \end{array}$$

temos, pelo Corolário 1.42, R_n é isomorfo a K^n através de σ.

Dessa forma, todo código $C \subset K^n$ pode ser transportado para R_n mediante o isomorfismo σ. A vantagem de estudar os códigos em R_n é que, além de uma estrutura de espaço vetorial, R_n tem também uma estrutura de anel.

Dado v um vetor de K^n, chamaremos de $v^{(i)}(X)$ o polinômio associado ao vetor $v^{(i)} = (v_{n-i}, v_{n-i+1}, \ldots, v_{n-1}, v_0, \ldots, v_{n-i-1})$ dado por

$$v_{n-i} + v_{n-i+1}X + \ldots + v_{n-i-1}X^{n-1}.$$

Existe uma relação algébrica interessante entre $v(X)$ e $v^{(i)}(X)$.

Lema 3.4. *Em R_n, $\overline{X^i v(X)} = \overline{v^{(i)}(X)}$.*

Demonstração. Multiplicando $v(X)$ por X^i, obtemos

$$X^i v(X) = v_0X^i + v_1X^{i+1} + ... + v_{n-i-1}X^{n-1} + ... + v_{n-1}X^{n+i-1}.$$

A equação acima pode ser manipulada da seguinte forma:

$$X^i v(X) = v_{n-i} + v_{n-i+1}X + ... + v_{n-1}X^{i-1} + v_0X^i + ... + v_{n-i-1}X^{n-1} +$$

$$+v_{n-i}(X^n - 1) + v_{n-i+1}X(X^n - 1) + ... + v_{n-1}X^{i-1}(X^n - 1)$$

$$= q(X)(X^n - 1) + v^{(i)}(X),$$

onde $q(X) = v_{n-i} + v_{n-1+1}X + ... + v_{n-1}X^{i-1}$. Vemos que o polinômio do código $v^{(i)}(X)$ é simplesmente o resto da divisão do polinômio $X^i v(X)$ por $X^n - 1$. □

Lema 3.5. *Seja V um subespaço vetorial de R_n. Então, V é um ideal de R_n se, e somente se, V é fechado pela multiplicação por $\overline{X}$.*

Demonstração. Observe que se V é um ideal de R_n, então pela definição de ideal, segue que $\overline{X} \cdot \overline{f(X)} \in V$, qualquer que seja $f(X) \in V$.

Reciprocamente, V é um subespaço vetorial, logo é fechado pela soma e multiplicação por escalar. Suponha que V seja fechado pela multiplicação por $\overline{X}$. Vamos verificar que qualquer que seja $\overline{g(X)} \in R_n$, e para todo $\overline{f(X)} \in V$, obtemos $\overline{g(X)} \cdot \overline{f(X)} \in V$.

Seja $\overline{f(X)} \in V$. Temos que para todo $a \in K$, $a \cdot \overline{f(X)} \in V$. Como

$$\overline{X} \cdot \overline{f(X)} = \overline{Xf(X)} \in V,$$

então

$$\overline{X} \cdot \overline{Xf(X)} = \overline{X^2} \cdot \overline{f(X)} = \overline{X^2 f(X)} \in V.$$

De modo indutivo, obtemos, para todo $m \in \mathbb{N}$, que

$$\overline{X^m} \cdot \overline{f(X)} = \overline{X^m f(X)} \in V.$$

Assim, escrevendo $\overline{g(X)} = \overline{a_0 + a_1 X + ... + a_{n-1} X^{n-1}}$ temos que

$$\overline{g(X)} \cdot \overline{f(X)} = \overline{g(X) f(X)} = \overline{(a_0 + a_1 X + ... + a_{n-1} X^{n-1}) f(X)} =$$

$$a_0 \overline{f(X)} + a_1 \overline{X} \cdot \overline{f(X)} + ... + a_{n-1} \overline{X^{n-1}} \cdot \overline{f(X)} \in V,$$

pois V é subespaço e cada termo da última expressão pertence a V. □

A discussão acima, juntamente com o Lema 3.5, provam o seguinte teorema:

Teorema 3.6. *Um subespaço C de K^n é um código cíclico se, e somente se, $\sigma(C)$ é um ideal de R_n.*

Assim, pela Proposição 1.30, podemos concluir que um código C em K^n é cíclico se, e somente se, $\sigma(C) = I(\overline{g(X)})$, onde $g(X) \in K[X]$ é um divisor de $X^n - 1$. Isto significa que, ao realizarmos a decomposição de $X^n - 1$ em fatores irredutíveis, obtemos todos os possíveis códigos cíclicos $C \subset K^n$.

Teorema 3.7. *Seja $I = I(\overline{g(X)})$, onde $g(X)$ é um divisor de $X^n - 1$ de grau r. Temos que $\overline{g(X)}, \overline{Xg(X)}, \overline{X^2 g(X)}, ..., \overline{X^{n-r-1} g(X)}$ é uma base de I como espaço vetorial sobre K.*

Demonstração. Admitimos que

$$a_0 \overline{g(X)} + a_1 \overline{Xg(X)} + ... + a_{n-k-1} \overline{X^{n-r-1} g(X)} = \overline{0}.$$

Assim,

$$\overline{g(X)} \cdot \overline{a_0 + a_1 X + ... + a_{n-r-1} X^{n-r-1}} = \overline{0}.$$

Desse modo, existe $d(X) \in K[X]$, tal que

$$g(X)(a_0 + a_1 X + ... + a_{n-r-1} X^{n-r-1}) = d(X) \cdot (X^n - 1).$$

Dividindo ambos os membros da última equação por $g(X)$, obtemos

$$a_0 + a_1X + ... + a_{n-r-1}X^{n-r-1} = d(X) \cdot h(X).$$

Como o grau de $h(X)$ é $n-r > n-r-1$, devemos ter $a_0 + a_1X + ... + a_{n-r-1}X^{n-r-1} = 0$, e consequentemente, $a_0 = a_1 = a_{n-r-1} = 0$.

Portanto os elementos acima são linearmente independentes.

Para finalizarmos, mostramos que $\overline{g(X)}, \overline{Xg(X)}, \overline{X^2g(X)}, ..., \overline{X^{n-r-1}g(X)}$ geram I sobre K. Se $\overline{f(X)} \in I$, temos que

$$f(X) \equiv d(X) \cdot g(X)\ mod\ (X^n - 1).$$

Pelo algoritmo da divisão, temos que $d(X) = c(X) \cdot h(X) + r(X)$, com $r(X) = a_0 + a_1X + ... + a_{n-r-1}X^{n-r-1}$. Assim

$$f(X) \equiv d(X) \cdot g(X) \equiv c(X) \cdot h(X) \cdot g(X) + r(X) \cdot g(X)\ mod\ (X^n - 1),$$

Logo

$$f(X) \equiv c(X) \cdot (X^n - 1) + r(X) \cdot g(X) \equiv r(X) \cdot g(X)\ mod\ (X^n - 1).$$

Portanto

$$\overline{f(X)} = a_0\overline{g(X)} + a_1\overline{Xg(X)} + ... + a_{n-r-1}\overline{X^{n-r-1}g(X)}.$$

□

Corolário 3.8. *Dado um código cíclico C, existe $\boldsymbol{v} \in C$ tal que $C = \langle \boldsymbol{v} \rangle$.*

Demonstração. Seja $I = \sigma(C)$. Logo I é gerado como K-espaço vetorial por

$$\overline{g(X)}, \overline{Xg(X)}, ..., \overline{X^{n-r-1}g(X)},$$

onde $g(X)$ é um divisor de $X^n - 1$ de grau r. Assim colocando v $= \sigma^{-1}(\overline{g(X)})$, temos que C é gerado por $v, v^{(1)}, ..., v^{(n-r-1)}$ e, portanto, $C = \langle v \rangle$. □

Observe que pela demonstração do corolário acima e pelo Teorema 3.7 a dimensão de C é $n-r$ onde r é o grau de $g(X)$.

Exemplo 3.9. Considere o polinômio $X^3 - 1$ sobre $\mathbb{F}_2$ e sua fatoração dada por

$$X^3 - 1 = (X + 1)(X^2 + X + 1).$$

Note que o código cíclico $C(3, 2)$ é determinado pelo polinômio $X + 1$, divisor de $X^3 - 1$, de grau $r = 1$.

Dessa forma, sendo $v = \sigma^{-1}(\overline{X + 1}) = 110$, segue do Corolário 3.8 que $C(3, 2) = \langle 110 \rangle$.

Analogamente, o código cíclico $C(3, 1)$ determinado por $X^2 + X + 1$, divisor de $X^3 - 1$ é gerado por 111, ou seja $C(3, 1) = \langle 111 \rangle$.

3.2 Matriz geradora

A matriz geradora de um código cíclico tem um papel fundamental na codificação de uma palavra do código fonte para o código de canal, ou seja, com ela inserimos os dígitos de redundância na mensagem.

Definição 3.10. Sejam K um corpo finito e $C \subset K^n$ um código cíclico. Dada $\mathcal{B} = \{\mathbf{v_1}, ..., \mathbf{v_k}\}$ uma base ordenada de C, a *matriz geradora* de C associada à base $\mathcal{B}$ é a matriz G, cujas linhas são os vetores $\mathbf{v_i} = (v_{i1}, ..., v_{in})$, $i = 1, ..., k$, isto é,

$$G = \begin{pmatrix} \mathbf{v_1} \\ \vdots \\ \mathbf{v_k} \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

Para entender melhor a função da matriz geradora, considere a transformação linear definida por

$$\begin{array}{rccc} T\colon & K^k & \longrightarrow & K^n \\ & \mathbf{x} & \longmapsto & \mathbf{x}G \end{array}.$$

Note que para $x = (x_1, ..., x_k)$, temos

$$T(x) = xG = x_1\mathbf{v_1} + \cdots + x_k\mathbf{v_k},$$

logo $T(K^k) = C$. Assim consideramos K^k como sendo o código da fonte, C o código do canal e a transformação T uma codificação.

Como para cada base β temos uma matriz geradora de C, podemos escolher β de modo conveniente. Uma outra base de C pode ser obtida de β através de uma sequência de operações do tipo:

(V1) Permutação de vetores.

(V2) Multiplicação de um vetor por um escalar não nulo.

(V3) Adição de um múltiplo escalar de um vetor a outro vetor.

Estas operações estão intrinsecamente ligadas a operações com as linhas da matriz G. Assim uma matriz geradora de C pode ser obtida de G por uma sequência 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.

Definição 3.11. Uma matriz geradora G de um código C está na *forma padrão* se tivermos

$$G = \begin{pmatrix} A & | & Id_k \end{pmatrix},$$

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

Da definição de matriz geradora e dos resultados anteriores em relação ao estudo dos códigos cíclicos, segue corolário abaixo:

Corolário 3.12. *Seja $g(X) = g_0 + g_1X + \cdots + g_rX^r$ um divisor de $X^n - 1$ de grau r. Se $I = I(\overline{g(X)})$, então*

$$dim_K I = n - r,$$

e o código $C = \sigma^{-1}(I)$ tem matriz geradora

$$G = \begin{pmatrix} \sigma^{-1}(\overline{g(X)}) \\ \sigma^{-1}(\overline{Xg(X)}) \\ \vdots \\ \sigma^{-1}(\overline{X^{n-r-1}g(X)}) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_r & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & g_0 & \cdots & \cdots & g_r \end{pmatrix}$$

Analisamos a seguir uma outra forma de determinar uma matriz geradora de C na forma padrão $\begin{pmatrix} R & | & Id_k \end{pmatrix}$.

Para o que se segue, denotamos por $K[X]_{r-1}$ o espaço vetorial dos polinômios de grau menor ou igual a $r-1$.

Considere o isomorfismo θ abaixo que será de fundamental importância para o resultado em seguida.

$$\begin{array}{ccc} \theta : K^r & \longrightarrow & K[X]_{r-1} \subset K[X] \\ (a_0, ..., a_{r-1}) & \longmapsto & [a_0 + a_1X + ... + a_{r-1}X^{r-1}] \end{array}$$

Teorema 3.13. *Seja $C \subset K^n$ um código cíclico. Suponhamos que $C = \sigma^{-1}(I)$, em que $I = I(\overline{g(X)})$, com $g(X)$ um divisor de $X^n - 1$ de grau r. Seja R a matriz $(n-r) \times r$ cuja i-ésima linha é*

$$R_i = -\theta^{-1}(s_i(X)), \qquad 1 \leq i \leq n - r,$$

onde $s_i(X)$ é o resto da divisão de X^{r-1+i} por $g(X)$. Então $(R \mid Id_{n-r})$ é uma matriz geradora de C.

Demonstração. Sejam $q_i(X)$ e $s_i(X)$ o quociente e o resto da divisão de X^{r-1+i} por $g(X)$. Assim teremos

$$X^{r-1+i} = g(X)q_i(X) + s_i(X), \quad com \quad s_i(X) = 0 \quad ou \quad gr(s_i(X)) \leq r - 1.$$

Logo $X^{r-1+i} - s_i(X) = g(X)q_i(X)$. Portanto $\overline{X^{r-1+i} - s_i(X)}$ pertence a I e evidentemente esses vetores para $i = 1, ..., n-r$ são linearmente independentes sobre K. Como $\sigma^{-1}(\overline{X^{r-1+i} - s_i(X)}) = \mathbf{e}_{r-1+i} - \theta^{-1}(s_i(X))$, temos que a matriz

$$\begin{pmatrix} -\theta^{-1}(s_1(X)) & 1 & 0 & \cdots & 0 \\ -\theta^{-1}(s_2(X)) & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ -\theta^{-1}(s_{n-r}(X)) & 0 & 0 & \cdots & 1 \end{pmatrix}$$

é uma matriz geradora de C. □

Exemplo 3.14. Considere o exemplo $C(7,4)$, onde $g(X) = 1 + X + X^3$. Temos que $n = 7$, $k = 4$ e $r = 3$. Vamos determinar a matriz geradora desse código na forma padrão, de acordo com o Teorema 3.13. Assim

$$X^3 = (X^3 + X + 1) + (X + 1)$$

$$X^4 = (X^3 + X + 1)X + (X^2 + X)$$

$$X^5 = (X^3 + X + 1)(X^2 + 1) + (X^2 + X + 1)$$

$$X^6 = (X^3 + X + 1)(X^3 + X + 1) + (X^2 + 1)$$

Portanto basta observar os restos das divisões acima, que nos fornece a matriz geradora $(R \mid Id_4)$ de C, dada por

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

Para o estudo da codificação, essa segunda forma de construir a matriz geradora de C é mais interessante. Vemos essa relação na Seção 3.4, na qual abordamos a codificação de códigos cíclicos.

3.3 Códigos duais - matriz teste de paridade

Seja $\langle \mathbf{u}, \mathbf{v} \rangle$ o produto interno usual de vetores em K^n. O complemento ortogonal de um código cíclico $C \subset K^n$ é o conjunto

$$C^{\perp} = \{\mathbf{v} \in K^n; \langle \mathbf{v}, \mathbf{u} \rangle = 0, \ \forall\, \mathbf{u} \in C\}.$$

Lema 3.15. *Se $C \subset K^n$ é um código cíclico, com matriz geradora G, então*

i) *$C^{\perp}$ é um subespaço de K^n;*

ii) $\mathbf{v} \in C^{\perp} \iff G\mathbf{v}^t = 0$.

Demonstração. **(i)** Sejam $\mathbf{u}, \mathbf{v} \in C^{\perp}$ e $\lambda \in K$. Para todo $\mathbf{w} \in C$, tem-se:

$$\langle \mathbf{u} + \lambda\mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \lambda \langle \mathbf{v}, \mathbf{w} \rangle = 0,$$

portanto $\langle \mathbf{u} + \lambda\mathbf{v}, \mathbf{w} \rangle \in C^{\perp}$, mostrando que $C^{\perp}$ é um subespaço vetorial de K^n.

(ii) $\mathbf{v} \in C^{\perp}$ se, e somente se, $\mathbf{v}$ é ortogonal a todos os vetores de C e portanto ortogonal à base de C. Como as linhas de G formam uma base de C, logo $G\mathbf{v}^t = 0$.

□

Da definição acima e do Lema 3.15 segue que $C^{\perp}$ é um subespaço de K^n, ortogonal a C, e também um código cíclico ao qual chamamos de *código dual* de C.

Vamos agora estudar uma matriz fundamental no processo de decodificação de uma palavra recebida. Ela nos permite identificar erro na palavra recebida e corrigir quando possível, o que minimiza os erros no processo de transmissão.

Como consequência do Lema 3.15 , $\mathbf{x} = (x_1, \cdots, x_n)$ pertence a $C^{\perp}$ se, e somente se, $G\mathbf{x}^t = 0$. Como G está na forma padrão, isso equivale a ter

$$G\mathbf{x}^t = \begin{pmatrix} s_{11} & \cdots & s_{1r} & 1 & 0 & \cdots & 0 \\ s_{21} & \cdots & a_{2r} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{(n-r)1} & \cdots & s_{(n-r)r} & 0 & 0 & \cdots & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{r+1} \\ x_{r+2} \\ \vdots \\ x_n \end{pmatrix} + R \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} = 0$$

que equivale a

$$\begin{pmatrix} x_{r+1} \\ x_{r+2} \\ \vdots \\ x_n \end{pmatrix} = -R \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix}.$$

Portanto $C^{\perp}$ possui q^{n-k} elementos, que são justamente as possíveis escolhas arbitrárias de $x_{k+1}, \cdots, x_n$. Logo $C^{\perp}$ tem dimensão $n-k$. Devido ao bloco Id_{n-k}, podemos perceber que as linhas da matriz H são linearmente independentes e, portanto geram um subespaço vetorial de dimensão $n-k$.

Observação 3.16. Como as linhas de H são ortogonais às linhas de G, temos que o espaço gerado pelas linhas de H está contido em $C^{\perp}$; e como esses dois espaços têm mesma dimensão, eles coincidem, provando assim que H é uma matriz geradora de $C^{\perp}$.

A matriz geradora H de $C^{\perp}$ é chamada de *matriz teste de paridade* de C.

Teorema 3.17. *A matriz teste de paridade de C é da forma* $H = (Id_r \mid -R^t) = \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_r \end{pmatrix}$.

Demonstração. Dado

$$R = \begin{pmatrix} R_1 \\ R_2 \\ \vdots \\ R_{n-r} \end{pmatrix},$$

onde $R_i = -\theta^{-1}(s_i(X))$ e $s_i(X) \equiv X^{n-1+i} \mod G(X)$, queremos provar que

(i) as linhas de H são ortogonais a todo vetor de C;

(ii) as linhas de H são linearmente independentes.

(i) Lembre que a matriz geradora de C é da forma $(R \mid Id_{n-r})$ e as linhas dessa matriz é base de C.

Seja a_{ij} os elementos da matriz H e b_{ij} os elementos de G, em que G é a matriz geradora de C. Observe que $a_{i(r+j)} = -b_{ji}$ pela definição de H. Assim, sendo L_i, L'_j respectivamente as linhas das matrizes H e G, em que $1 \leqslant i \leqslant r$ e $1 \leqslant j \leqslant n-r$, temos que

$$H \cdot G^t = \langle L_i, L'_j \rangle = b_{ji} + a_{i(r+j)} = b_{ji} - b_{ji} = 0.$$

(ii) Sejam $\lambda_1, \cdots, \lambda_r \in K$ tais que

$$\lambda_1 L_1 + \cdots + \lambda_r L_r = 0,$$

e suponha que $\lambda_i \neq 0$ para algum $i = 1, \cdots, r$. Daí

$$L_i = -\frac{\lambda_1}{\lambda_i} L_1 - \cdots - \frac{\lambda_{i-1}}{\lambda_i} L_{i-1} - \frac{\lambda_{i+1}}{\lambda_i} L_{i+1} - \cdots - \frac{\lambda_r}{\lambda_i} L_r.$$

Como a i-ésima coordenada de L_i é 1 e as coordenadas dos L_j $(j \neq i)$ são 0, temos um absurdo. Logo $\lambda_i = 0$ para todo $i = 1, \cdots, r$.

□

Definição 3.18. Seja C um código cíclico com matriz teste de paridade H e um vetor $\mathbf{v} \in K^n$, chamamos o vetor $H\mathbf{v}^t$ de *síndrome* de $\mathbf{v}$.

O resultado a seguir nos permite utilizar a matriz H para caracterizar os elementos de um código cíclico C por uma condição de anulamento.

Proposição 3.19. *Seja C um código cíclico e suponhamos que H seja uma matriz geradora de $C^{\perp}$. Temos então que*

$$v \in C \iff Hv^t = 0.$$

Demonstração. Seja G a matriz geradora de C. Logo $G \cdot H^t = 0$. Tomando as transpostas nessa última igualdade, temos que $H \cdot G^t = 0$, logo, G é matriz geradora de $(C^{\perp})^{\perp}$. Assim, $v \in (C^{\perp})^{\perp}$ se, e somente se, $Hv^t = 0$. □

Para verificar se um determinado vetor $\mathbf{v}$ pertence ou não a um código C com matriz geradora G, é necessário verificar se o sistema de n equações com k incógnitas $\mathbf{x} = (x_1, ..., x_k)$, dado por

$$\mathbf{x}G = \mathbf{v},$$

admite solução. Em geral, resolver esse sistema requer um custo computacional elevado, especialmente quando se tem um código de comprimento n grande. Porém, utilizando a matriz teste de paridade H, basta verificar se o vetor Hv^t é nulo, que é bem mais simples.

Exemplo 3.20. Seja o código cíclico C sobre $\mathbb{F}_2$ com matriz geradora

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

Como G está na forma padrão, a matriz teste de paridade H, como já vimos na observação 3.16, é expressa por

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

Dados $\mathbf{v} = (010101)$ e $\mathbf{v}' = (100111)$, como

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

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

O resultado a seguir nos fornece uma forma de calcular algebricamente a síndrome de um vetor $\mathbf{v}$ em relação a uma matriz teste de paridade num código cíclico, sem que seja necessário efetuarmos o produto matricial $H\mathbf{v}^t$.

Teorema 3.21. *Seja $C \subset K^n$ um código cíclico gerado por um polinômio mônico de grau r com matriz geradora na forma padrão $(R \mid Id_{n-r})$ e matriz teste de paridade $H = (Id_r \mid -R^T)$. Se $\boldsymbol{v} = (v_0, ..., v_{n-1}) \in K^n$, então a síndrome de $\boldsymbol{v}$ com relação à matriz H é dada por*

$$\theta^{-1}(s(X)),$$

onde $s(X)$ é o resto da divisão de $v_0 + v_1X + \cdots + v_{n-1}X^{n-1}$ por $g(X)$.

Demonstração. A síndrome de $\mathbf{v}$ é o vetor

$$(Id_r| - R^t)v^t =$$

$$(\theta^{-1}(1), \theta^{-1}(X), \cdots, \theta^{-1}(X^{r-1}), \theta^{-1}(s_1(X)), \cdots, \theta^{-1}(s_{n-r}(X)))v^t =$$

$$\theta^{-1}(v_0 + v_1X + \cdots + v_{r-1}X^{r-1} + v_rs_1(X) + \cdots + v_{n-1}s_{n-r}(X)),$$

de onde segue o resultado, pelo fato de

$$s(X) = v_0 + v_1X + \cdots + v_{r-1}X^{r-1} + v_rs_1(X) + \cdots + v_{n-1}s_{n-1}(X)$$

ser o resto da divisão de $v_0 + v_1X + \cdots + v_{n-1}X^{n-1}$ por $g(X)$. □

Considere o código $C(7, 4)$. A matriz teste de paridade associada 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 $(1101001) \in \mathbb{F}_2^7$, para calcular a síndrome, extraímos o resto da divisão do polinômio $1 + X + X^3 + X^6$ por $g(X) = 1 + X + X^3$ que é $s(X) = X^2 + 1$. De acordo com o Teorema 3.21, a síndrome é dada por

$$\theta^{-1}(s(X)) = (101).$$

3.4 Codificação e decodificação

A ideia de codificação de códigos corretores de erros se baseia em codificar uma informação (mensagem), adicionando informação redundante, de forma que, ao receber a mensagem modificada (com algum erro), seja possível recuperar a informação na sua forma original.

Ainda considerando o isomorfismo 3.2 e sendo $C \subset K^n$ um código cíclico, de matriz geradora na forma padrão G', para codificar um vetor do código fonte como elemento de C, basta multiplicar o vetor do código por G'. Assim

$$(a_1, ..., a_{n-r}) \cdot (R \mid Id_{n-r}) = (b_0, ..., b_{r-1}, a_1, ..., a_{n-r}) \in C,$$

no qual são inseridos os dígitos (símbolos) de redundância

$$(b_0, ..., b_{r-1}) = -a_1\theta^{-1}(s_1(X)) - ... - a_{n-r}\theta^{-1}(s_{n-r}(X)) =$$

$$-\theta^{-1}(a_1s_1(X) + ... + a_{n-r}s_{n-r}(X)).$$

A partir de agora, vamos estudar o procedimento de detecção e correção de erros num determinado código. Tal procedimento é chamado de *decodificação*.

Definição 3.22. O peso de um código cíclico C é o inteiro

$$\omega(C) := \min\{\omega(\mathbf{x}); \mathbf{x} \in C \setminus \{\mathbf{0}\}.$$

Observação 3.23. Encontrar uma forma para calcular o peso de um código cíclico é um problema muito difícil de ser resolvido e é, em parte, uma questão em aberto.

Definição 3.24. Definimos o vetor erro $\mathbf{e}$ como sendo a diferença entre o vetor recebido $\mathbf{r}$ e o vetor transmitido $\mathbf{c}$, isto é,

$$\mathbf{e} = \mathbf{r} - \mathbf{c}.$$

Para exemplificar, suponhamos que num determinado código sobre $\mathbb{F}_2$ na transmissão da mensagem (010011) ocorreu um erro e a palavra recebida tenha sido (101011). Então

$$\mathbf{e} = (101011) - (010011) = (111000).$$

Observe que o peso do vetor erro corresponde ao número de erros cometidos durante a transmissão.

Seja H a matriz teste de paridade do código. Como $H\mathbf{c}^t = 0$, temos que

$$H\mathbf{e}^t = H(\mathbf{r}^t - \mathbf{c}^t) = H\mathbf{r}^t - H\mathbf{c}^t = H\mathbf{r}^t.$$

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

Denotamos por h^i a i-ésima coluna da matriz H. Se $\mathbf{e} = (\alpha_1, \cdots, \alpha_n)$, então

$$\sum_{i=1}^{n} \alpha_i h^i = H\mathbf{e}^t = H\mathbf{r}^t.$$

Lema 3.25. *Seja C um código cíclico em K^n com capacidade de correção κ. Se $\mathbf{r} \in K^n$ e $\mathbf{c} \in C$ são tais que $d(\mathbf{c}, \mathbf{r}) \leqslant \kappa$, então existe um único vetor $\mathbf{e}$ com $\omega(\mathbf{e}) \leqslant \kappa$, cuja síndrome é igual à síndrome de $\mathbf{r}$ e tal que $\mathbf{c} = \mathbf{r} - \mathbf{e}$.*

Demonstração. De fato, $\mathbf{e} = \mathbf{r} - \mathbf{c}$ satisfaz as condições do Lema, já que $\omega(\mathbf{e}) = d(\mathbf{c}, \mathbf{r}) \leqslant \kappa$. Para provar a unicidade, suponhamos que $\mathbf{e} = (\alpha_1 \cdots \alpha_n)$ e $\mathbf{e}' = (\alpha'_1 \cdots \alpha'_n)$ sejam tais que $\omega(\mathbf{e}) \leqslant \kappa$ e $\omega(\mathbf{e}') \leqslant \kappa$ e tenham mesma síndrome que $\mathbf{r}$. Então, se H é uma matriz teste de paridade de C, temos

$$H\mathbf{e}^t = H\mathbf{e}'^t \Longrightarrow \sum_{i=1}^{n} \alpha_i h^i = \sum_{i=1}^{n} \alpha'_i h^i,$$

o que nos dá uma relação de dependência linear entre $2\kappa (\leqslant d-1)$ colunas de H. Como quaisquer $d-1$ colunas de H são linearmente independentes, temos que $\alpha_i = \alpha'_i$ para todo i, logo $\mathbf{e} = \mathbf{e}'$. □

Como determinar o vetor $\mathbf{e}$ a partir de Hr^t?

Exemplo 3.26. Determinação de $\mathbf{e}$ quando $\omega(\mathbf{e}) \leqslant 1$.

Seja C um código de distância mínima $d \geqslant 3$ e o vetor erro $\mathbf{e}$ inserido durante uma transmissão da mensagem $\mathbf{c}$ seja tal que $\omega(\mathbf{e}) \leqslant 1$. Isto significa que o canal introduziu no máximo um erro.

Se $H\mathbf{e}^t = 0$, então $\mathbf{r}$ (palavra recebida) pertence a C e temos $\mathbf{c} = \mathbf{r}$.

Considere $H\mathbf{e}^t \neq 0$, então $\omega(\mathbf{e}) = 1$ e, portanto $\mathbf{e}$ tem apenas uma coordenada não nula. Assim, consideramos que $\mathbf{e} = (0, \cdots, \alpha, \cdots, 0)$ com $\alpha \neq 0$ na i-ésima posição. Logo,

$$H\mathbf{e}^t = \alpha h^i,$$

onde h^i é a i-ésima coluna de H. Portanto, não conhecendo $\mathbf{e}$, mas conhecendo

$$H\mathbf{e}^t = H\mathbf{r}^t = \alpha h^i,$$

podemos determinar $\mathbf{e}$ como sendo o vetor com todas as componentes nulas exceto a i-ésima componente que é α.

Agora vamos ver com o exemplo abaixo como construir um código cíclico, suas matrizes geradora e teste de paridade, e decodificar algumas mensagens.

Exemplo 3.27. Considere o polinômio $X^8 - 1$ sobre $\mathbb{F}_3$.

a) Vamos determinar a fatoração desse polinômio em polinômios irredutíveis e mônicos em $\mathbb{F}_3[X]$.

Como 1 e 2 são raízes, tem-se

$$X^8 - 1 = (X + 1)(X + 2)(X^6 + X^4 + X^2 + 1),$$

temos ainda que

$$(X^6 + X^4 + X^2 + 1) = X^4(X^2 + 1) + X^2 + 1 = (X^2 + 1)(X^4 + 1).$$

Note que $X^2 + 1$ é irredutível, pois esse polinômio não possui raízes em $\mathbb{F}_3[X]$.

Observe também que $0, 1$ e 2 não são raízes de $X^4 + 1$, e como seus possíveis fatores ou têm graus 1 e 3 ou dois fatores de grau 2, então a segunda opção é a única possível. Portanto

$$X^4 + 1 = (X^2 + b_1X + c_1)(X^2 + b_2X + c_2) =$$
$$= X^4 + (b_1 + b_2)X^3 + (b_1b_2 + c_1 + c_2)X^2 + (b_1c_2 + c_1b_2)X + c_1c_2.$$

Resolvendo o sistema

$$\begin{cases} b_1 + b_2 = 0 \\ b_1b_2 + c_1 + c_2 = 0 \\ b_1c_2 + b_2c_1 = 0 \\ c_1c_2 = 1 \end{cases}$$

temos $b_1 = 1, b_2 = c_1 = c_2 = 2$. Assim

$$X^8 - 1 = (X+1)(X+2)(X^2+1)(X^2+X+2)(X^2+2X+2).$$

b) Seja $C \subset \mathbb{F}_3^8$ o código cíclico gerado por $g(X) = X^2 + 2X + 2$. Vamos construir a matriz geradora de C na forma padrão $(R|Id)$ e sua correspondente matriz teste de paridade $(Id| - R^t)$.

Observe que com a escolha do polinômio $g(X)$, temos a construção de um código $C(8,6)$, isto significa que, pra esse código, são acrescentados 2 dígitos de redundância na codificação. Assim, aplicando o teorema 3.13, e realizando as divisões

$$X^2 = (X^2+2X+2) + (X+1)$$

$$X^3 = (X^2+2X+2)(X+1) + (2X+1)$$

$$X^4 = (X^2+2X+2)(X^2+X+2) + 2$$

$$X^5 = (X^2+2X+2)(X^3+X^2+2X) + 2X$$

$$X^6 = (X^2+2X+2)(X^4+X^3+2X^2+2) + (2X+2)$$

$$X^7 = (X^2+2X+2)(X^5+X^4+2X^3+2X+2) + (X+2)$$

obtemos a matriz geradora $(R|Id_6)$ e a matriz teste de paridade $(Id_2| - R^t)$ de C, dadas por

$$G' = \begin{pmatrix} 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad H' = \begin{pmatrix} 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \end{pmatrix}.$$

c) Agora iremos decodificar as mensagens $X^6 + X^4 + X^2 + 1$, $X^7 + X^5 + 2X + 1$ e $X^7 + 2X^6 + X^5 + X^3 + X^2 + 2X + 1$.

Para isto, encontramos a síndrome das mensagens recebidas dividindo o polinômio que caracteriza cada mensagem por $g(X)$, e se o resto for 0, então a mensagem pertence ao código, caso contrário, corrigimos o erro aplicando o algoritmo da decodificação.

Como,

$$X^6 + X^4 + X^2 + 1 = (X^2+2X+2)(X^4+X^3+X+2),$$

logo

$$\sigma^{-1}(X^6 + X^4 + X^2 + 1) = 10101010 \in C.$$

Assim, como a decodificação é dada pela matriz geradora na forma padrão, a mensagem transmitida é dada pelas seis componentes finais do vetor 10101010 que é 101010.

Analogamente, para a mensagem $X^7 + X^5 + 2X + 1$, tem-se

$$X^7 + X^5 + 2X + 1 = (X^2 + 2X + 2)(X^5 + X^4 + X^2 + X + 2) + 2X,$$

onde $s(X) = 2X$ é o resto da divisão de $X^7 + X^5 + 2X + 1$ por $g(X)$, e consequentemente, a síndrome é o vetor (02). Comparando com as colunas de H' temos que o vetor da síndrome é igual à sexta coluna de H', pelo algoritmo da decodificação o vetor $\mathbf{e} = (00000200)$. A relação $\mathbf{c} = \mathbf{r} + \mathbf{e}$, nos permite corrigir a mensagem. Logo

$$\mathbf{c} = \sigma^{-1}(X^7+X^5+2X+1)+(00000200) = (12000101)+(00000200) = (12000001) \in C.$$

E a mensagem decodificada é 000001.

Para finalizar temos

$$X^7 + 2X^6 + X^5 + X^3 + X^2 + 2X + 1 = (X^2 + 2X + 2)(X^5 + 2X^3 + 2X^2 + 2X + 2)$$

isso significa que $\sigma^{-1}(1 + 2X + X^2 + X^3 + X^5 + 2X^6 + X^7) = 12110121 \in C$. E a mensagem transmitida é 110121.

4 Uma proposta para o ensino de polinômios

Neste capítulo, desenvolvemos uma proposta de sequência didática para a construção do conhecimento sobre polinômios, aplicada aos códigos cíclicos, no processo de codificação e decodificação. Realizamos nosso estudo, inicialmente abordando conteúdos fundamentais da matemática que estão diretamente relacionados com a aplicação dos códigos cíclicos.

Nosso intuito inicial era mostrar, nesta dissertação, os resultados da aplicação dessa proposta porém, devido ao período pandêmico vivenciado durante a produção dessa sequência didática, não foi possível realizar tal aplicação. Mesmo assim nos dedicamos ao máximo na elaboração desse trabalho com o propósito de construir um matérial de qualidade para uma aplicação futura.

Recomendamos que esta sequência didática seja aplicada, como projeto extracurricular, para um grupo de alunos pré-selecionados do Ensino Médio. De preferência alunos que têm mais afinidade com a matemática. Como exemplo, a formação de uma sala de alunos que estudam para participarem de olimpíadas de matemática (OBMEP, OBM, OPEMAT, entre outras).

Sugerimos, com a finalidade de motivar os alunos pra essa sequência didática, que o professor construa uma aula 0, com as atividades 1 e 2, de Lira (10) (2018, p. 95), que foram atividades que nos inspiraram na construção das aulas 6 e 7 da sequência didática.

O objetivo dessa sequência didática é mostrar ao aluno que a matemática está intimamente presente no dia a dia deles. Em uma simples mensagem de e-mail, em uma ligação telefônica, na utilização de smartphones, computadores, entre outros meios de comunicação, a matemática está diretamente relacionada.

Nas próximas seções vamos apresentar a estrutura e organização de cada aula dessa sequência.

Da aula 1 até a aula 4, abordamos os conteúdos matemáticos necessários para aplicação nos códigos cíclicos. Na aula 5, introduzimos a teoria dos códigos com um texto de fácil compreensão. Nas aulas 6 e 7, apresentamos o algoritmo da codificação e decodificação, que utiliza a operação de polinômios como principal conteúdo abordado.

As aulas apresentadas a seguir estão estruturadas com os seguintes tópicos:

- Objetivos - O que desejamos que os alunos compreendam;
- Recursos didáticos - Materiais sugeridos para utilização na aula;

- Conteúdos abordados - O conhecimento matemático abordado na aula;
- Tempo de duração - tempo sugerido para duração da aula/atividade;
- Metodologia - A forma como o professor conduzirá a aula;
- Texto para o aluno - Texto para aprendizagem construtiva dos alunos;
- Atividades[1] - Conjunto de exercícios relacionados à aula;
- Avaliação - Propostas ou instrumentos de avaliação para acompanhar o progresso dos alunos com relação aos conteúdos das aulas;
- Orientação para o professor - Sugestões para uma boa condução e aproveitamento da sequência didática.

4.1 Aula 1: Corpos finitos

Objetivos: Compreender os conjuntos da forma $\mathbb{Z}_n$ como anel, com n inteiro; Realizar as operações de adição e multiplicação nesses conjuntos; Identificar quando $\mathbb{Z}_n$ é um corpo finito.

Recursos didáticos: Data show, computador, quadro branco e pincel.

Conteúdos abordados: Divisão euclidiana.

Tempo de duração: Sugerimos um período de 50 minutos, que é o tempo definido para uma aula nas escolas públicas no estado de Pernambuco.

Metodologia: O professor entregará aos alunos o texto abaixo onde será apresentado ou relembrado os conteúdos necessários para a execução da atividade. Este material também poderá ser apresentado pelo professor utilizando o data show.

Corpos Finitos

Dado um inteiro $n > 1$, o Teorema da Divisão Euclidiana garante que para todo número inteiro a existem inteiros q e r tais que $a = q \cdot n + r$, com $0 \leqslant r < n$, ou seja, é sempre possível dividir o número inteiro a por n com quociente q e resto r.

[1] As atividades precedidas de * são atividades fundamentais, pois obedecem uma ordem na construção do conhecimento, dando uma ideia de continuidade.

Como consequência deste Teorema temos o que chamamos de Lema dos restos, enunciado a seguir:

Lema dos Restos A soma e o produto de quaisquer dois números inteiros deixa o mesmo resto que a soma e o produto dos seus restos, respectivamente, na divisão por um inteiro n, $n \neq 0$.

De fato, se $a = q_1 \cdot n + r_1$ e $b = q_2 \cdot n + r_2$ então

$$a + b = (q_1 + q_2) \cdot n + (r_1 + r_2) \text{ e}$$

$$a \cdot b = (q_1 \cdot q_2 \cdot n + q_1 \cdot r_2 + q_2 \cdot r_1) \cdot n + (r_1 \cdot r_2).$$

Como a primeira parcela de $a + b$ e $a \cdot b$ já é múltiplo de n resta dividir $r_1 + r_2$ e $r_1 \cdot r_2$ por n.

Dado $n > 0$ um número inteiro vamos considerar o conjunto

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

onde $\overline{r}$, $0 \leq r \leq n-1$, representa todos os números inteiros que têm resto r quando dividido por n. Por exemplo, no conjunto $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, $\overline{0}$ representa todos os números pares e $\overline{1}$ representa todos os números ímpares.

Utilizando o Lema dos restos podemos concluir que $\overline{a} + \overline{b} = \overline{a+b}$ e $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. Por exemplo, em $\mathbb{Z}_5$ somar $\overline{3}$ e $\overline{4}$ significa somar um número da forma $a = 5 \cdot q + 3$ com outro da forma $b = 5 \cdot k + 4$, portanto $a + b = 5 \cdot (q + k) + 7 = 5 \cdot (q + k + 1) + 2$. A maneira simplificada de escrever isso é $\overline{3} + \overline{4} = \overline{3+4} = \overline{2}$, pois dividindo 7 por 5 obtemos resto 2.

Segue abaixo a tabela de multiplicação e adição de $\mathbb{Z}_3$

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

e

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

Quando $\mathbb{Z}_n$ é corpo finito? Diremos que $\mathbb{Z}_n$ é um corpo finito se todo elemento $\overline{a} \neq \overline{0}$ tem inverso multiplicativo, ou seja, existe $\overline{b}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$.

Olhando a tabela de multiplicação do $\mathbb{Z}_3$ notamos que os elementos $\overline{1}$ e $\overline{2}$ têm inverso multiplicativo pois $\overline{1} \cdot \overline{1} = \overline{1}$ e $\overline{2} \cdot \overline{2} = \overline{1}$, logo $\mathbb{Z}_3$ é um corpo finito.

Atividades: (Identificando corpos finitos)

4.1.1. Preencha as tabelas de adição e multiplicação dos conjuntos abaixo.

$\mathbb{Z}_2$:

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$		
$\overline{1}$		

e

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$		
$\overline{1}$		

$\mathbb{Z}_5$:

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

e

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

$\mathbb{Z}_6$:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$						
$\overline{1}$						
$\overline{2}$						
$\overline{3}$						
$\overline{4}$						
$\overline{5}$						

e

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$						
$\overline{1}$						
$\overline{2}$						
$\overline{3}$						
$\overline{4}$						
$\overline{5}$						

$\mathbb{Z}_7$:

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

e

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

$\mathbb{Z}_8$:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$								
$\overline{1}$								
$\overline{2}$								
$\overline{3}$								
$\overline{4}$								
$\overline{5}$								
$\overline{6}$								
$\overline{7}$								

e

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$								
$\overline{1}$								
$\overline{2}$								
$\overline{3}$								
$\overline{4}$								
$\overline{5}$								
$\overline{6}$								
$\overline{7}$								

$\mathbb{Z}_9$:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$									
$\overline{1}$									
$\overline{2}$									
$\overline{3}$									
$\overline{4}$									
$\overline{5}$									
$\overline{6}$									
$\overline{7}$									
$\overline{8}$									

e

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$									
$\overline{1}$									
$\overline{2}$									
$\overline{3}$									
$\overline{4}$									
$\overline{5}$									
$\overline{6}$									
$\overline{7}$									
$\overline{8}$									

4.1.2. Verifique para quais valores de n dos conjuntos $\mathbb{Z}_n$, do item anterior, $\mathbb{Z}_n$ é um corpo finito.

4.1.3. Qual a condição que classifica um conjunto $\mathbb{Z}_n$ como um corpo finito?

4.1.4. Se num conjunto, existem elementos a e b diferentes de zero, de forma que $a \times b = 0$, dizemos que este conjunto possui divisores de zero. Identifique quais conjuntos do exercício 1 admitem divisores de zero. Esses conjuntos são corpos finitos?

Avaliação: A avaliação do aprendizado dos alunos será feita a partir das observações do professor durante a execução das atividades.

Orientações para o professor: Para essa atividade, o professor poderá dividir a turma em equipes de quatro ou três alunos, em seguida entregar o texto **Corpos Finitos** para que as equipes realizem a leitura. Sugerimos que seja definido o tempo de 10 minutos para leitura do texto.

Após a leitura, o professor poderá relembrar e esclarecer alguns conceitos descritos no texto, utilizando exemplos numéricos. Também sugerimos que seja realizado algumas mediações sobre o texto. Por exemplo:

- O que diz o lema dos restos?
- Quem são os elementos de $\mathbb{Z}_5$?
- Quando $\mathbb{Z}_n$ é um corpo?
- Quem são os elementos invertíveis de $\mathbb{Z}_4$?

As perguntas devem orientar o aluno na construção do conhecimento proposto no texto.

Para finalizar a aula, o professor entrega aos alunos as tabelas de adição e multiplicação dos conjuntos $\mathbb{Z}_4$ e $\mathbb{Z}_5$ para eles preencherem juntamente com a lista de exercícios.

4.2 Aula 2: Polinômios com coeficientes em um corpo finito

Objetivos: Identificar o grau de um polinômio; efetuar a adição e multiplicação de polinômios; determinar as raízes de um polinômio com coeficientes em um corpo finito.

Recursos didáticos: Data Show, computador, quadro branco e pincel.

Conteúdos abordados: Grua de um polinômio; adição e multiplicação de polinômios; raiz de um polinômio.

Tempo de duração: Para essa atividade sugerimos que seja aplicada no tempo de uma aula 50 minutos.

Metodologia: O professor entregará aos alunos o texto abaixo, onde será apresentado ou relembrado os conteúdos necessários para a execução da atividade. Este material também poderá ser apresentado pelo professor utilizando o data show.

Polinômios com coeficientes em um corpo finito

Sejam $K = \mathbb{Z}_p$ (com p um número primo) um corpo finito, e X uma variável. Um polinômio $P(X)$ com coeficientes em K é uma expressão da seguinte forma

$$P(X) = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_1 X + a_0,$$

em que m é um número inteiro não negativo, e $a_0, a_1, \cdots, a_m$ são elementos de K, tal que $a_m \neq 0$. Chamamos m de grau do polinômio $P(X)$.

Dados $F(X) = a_m X^m + \cdots + a_1 X + a_0$ e $G(X) = b_n X^n + \cdots + b_1 X + b_0$ polinômios com coeficientes em K, podemos definir as operações de adição e multiplicação de polinômios da seguinte forma:

(i) $F(X) + G(X) = c_n X^n + \cdots + c_1 X + c_0$ onde $c_i = a_i + b_i$, com $i = 0, 1, \cdots, n$;

(ii) $F(X) \cdot G(X) = c_{m+n} X^{m+n} + \cdots + c_1 X + c_0$, onde $c_i = a_0 \cdot b_i + a_1 \cdot b_{i-1} + \cdots + a_i \cdot b_0$, com $i = 0, 1, \cdots m + n$.

O resultado da adição entre dois polinômios é chamado de soma, já o resultado da multiplicação chamamos de produto.

Por exemplo, sejam $F(X) = X^3 + X + 1, G(X) = X^3 + X^2 + 1$ em $\mathbb{Z}_2$. Então

$$F(X) + G(X) = (1+1)X^3 + (0+1)X^2 + (1+0)X + (1+1) = X^2 + X$$

e

$$F(X) \cdot G(X) = (X^3 + X + 1) \cdot (X^3 + X^2 + 1)$$
$$= X^3 \cdot (X^3 + X^2 + 1) + X \cdot (X^3 + X^2 + 1) + 1 \cdot (X^3 + X^2 + 1)$$
$$= (X^6 + X^5 + X^3) + (X^4 + X^3 + X) + (X^3 + X^2 + 1)$$
$$= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1.$$

Dizemos que $\alpha \in K$ é uma raiz de $P(X)$ se $P(\alpha) = 0$, ou seja,

$$a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0.$$

Como exemplo, considerando $K = \mathbb{Z}_5$ e $P(X) = X^2 + \overline{2}X + \overline{1}$ temos que $\overline{4}$ é uma raiz do polinômio, pois

$$\overline{4}^2 + \overline{2} \times \overline{4} + \overline{1} = \overline{0}.$$

Para encontrar as raízes de um polinômio $P(X)$ em $K = \mathbb{Z}_p$, onde $\mathbb{Z}_p$ é um corpo finito, basta avaliar $P(X)$ para os p elementos de $\mathbb{Z}_p$. Isto é um problema simples quando p é um número relativamente pequeno.

Por exemplo, para encontrar todas as raízes do polinômio $P(X) = X^3+X^2+\overline{2}X+\overline{2}$ em $\mathbb{Z}_5$, vamos avaliar em todos os elementos de $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Assim temos

$$P(\overline{0}) = \overline{0}^3 + \overline{0}^2 + \overline{2} \cdot \overline{0} + \overline{2} = \overline{2}$$
$$P(\overline{1}) = \overline{1}^3 + \overline{1}^2 + \overline{2} \cdot \overline{1} + \overline{2} = \overline{1}$$
$$P(\overline{2}) = \overline{2}^3 + \overline{2}^2 + \overline{2} \cdot \overline{2} + \overline{2} = \overline{3}$$
$$P(\overline{3}) = \overline{3}^3 + \overline{3}^2 + \overline{2} \cdot \overline{3} + \overline{2} = \overline{4}$$
$$P(\overline{4}) = \overline{4}^3 + \overline{4}^2 + \overline{2} \cdot \overline{4} + \overline{2} = \overline{0},$$

e, portanto $\overline{4}$ é a única raiz do polinômio $P(X)$ sobre $\mathbb{Z}_5$.

Atividades: (Polinômios)

4.2.1 Complete a tabela abaixo, realizando as operações e verificando os graus dos polinômios.

K	$P(X)$ $Q(X)$	$P(X)+Q(X)$ $P(X)\cdot Q(X)$	grau de $P(X)$ e $Q(X)$	grau de $P(X)+Q(X)$ e $P(X)\cdot Q(X)$
$\mathbb{Z}_2$	$P(X)=X^3+X^2+\overline{1}$ $Q(X)=X^3+X$			
$\mathbb{Z}_3$	$P(X)=X^3+\overline{2}X+\overline{1}$ $Q(X)=X^2+\overline{2}$			
$\mathbb{Z}_5$	$P(X)=X^4+\overline{1}$ $Q(X)=X^2+X+\overline{1}$			

4.2.2. Encontre todas as raízes dos polinômios $X^3+\overline{2}X+\overline{1}$, $X^3+\overline{2}X^2+X+\overline{2}$, $X^2+\overline{2}$ e $X^5+\overline{2}X$ em $\mathbb{Z}_3$.

4.2.3. Calcule todas as raízes do polinômio $F(X)=X^5+\overline{3}X^3+X^2+\overline{2}X$ com coeficientes em:

(a) $\mathbb{Z}_5$;

(b) $\mathbb{Z}_7$.

Avaliação: A avaliação do aprendizado dos alunos será feita a partir das observações do professor durante a execução das atividades.

Orientações para o professor: Nos primeiros 15 minutos, o professor poderá entregar aos alunos o texto **Polinômios com coeficientes em um corpo finito** para uma primeira leitura. Em seguida realizar algumas mediações com relação à leitura do texto. Por exemplo:

- De acordo com os exemplos do texto (ou da atividade) qual a relação entre o grau da soma $P(X)+Q(X)$, e o grau dos polinômios $P(X)$ e $Q(X)$?.
- E o que podemos concluir do grau do produto?
- O que é uma raiz de um polinômio?

Lembrando que as perguntas, aqui servem para direcionar o aluno, contribuindo para construção do conhecimento proposto no texto.

Para finalizar, o professor poderá entregar as atividades propostas (Polinômios).

4.3 Aula 3: Divisão de polinômios em $K[X]$

Objetivos: Compreender e aplicar o Algoritmo da Divisão de Polinômios em um corpo finito.

Recursos Didáticos: Data show, computador, quadro branco e pincel.

Conteúdos Abordados: Divisão de polinômios.

Tempo de duração: Para essa atividade, sugerimos empregar o tempo de uma aula de 50 minutos.

Metodologia: O professor entregará aos alunos o texto abaixo, onde será apresentado ou relembrado os conteúdos necessários para a execução da atividade. Este material também poderá ser apresentado pelo professor utilizando o data show.

Algoritmo da Divisão de Polinômios em $K[X]$

Sejam $K = \mathbb{Z}_p$ (com p um número primo) um corpo finito, e X uma variável. Assim como nos inteiros, o Teorema da Divisão Euclidiana também se aplica aos polinômios em $K[X]$, assegurando que dados $F(X)$ e $G(X) \in K[X]$, com $F(X) \neq 0$ existem únicos polinômios $Q(X)$ e $R(X)$, tais que $G(X) = Q(X) \cdot F(X) + R(X)$, **com o grau de $R(X)$ menor do que o grau de $F(X)$ ou $R(X) = 0$.**

Como efetuar na prática esta divisão?

Primeiro precisamos entender que, se o grau de $G(X)$ for menor do que o grau de $F(X)$, então

$$G(X) = 0 \cdot F(X) + G(X),$$

ou seja, $Q(X) = 0$ e $R(X) = G(X)$.

Porém, se o grau de $G(X) = a_m X^m + \ldots + a_1 X + a_0$ $(a_m \neq 0)$ for maior do que ou igual ao grau de $F(X) = b_n X^n + \ldots + b_1 X + b_0$ $(b_n \neq 0)$, ou seja, $m \geq n$ então escreveremos $Q_1(X) = a_m b_n^{-1} X^{m-n}$ e $R_1(X) = G(X) - Q_1(X) \cdot F(X)$, sendo b_n^{-1} o inverso multiplicativo de b_n. Se o grau de $R_1(X)$ for menor do que o grau de $F(X)$ ou $R_1(X) = 0$ acabamos a divisão e $G(X) = Q_1(X) \cdot F(X) + R_1(X)$, caso contrário repetimos o processo anterior agora com $R_1(X)$ e $F(X)$.

Vejamos no exemplo abaixo a divisão do polinômio $G(X) = X^4 + X^3 + X + \overline{1}$ pelo polinômio $F(X) = \overline{2}X^3 + X + \overline{1}$ em $\mathbb{Z}_3[X]$.

Passo 1 O inverso multiplicativo de $\overline{2}$ em $\mathbb{Z}_3$ é $\overline{2}$, logo $Q_1(X) = \overline{2} \cdot \overline{1} \cdot X^{4-3}$ e

$$R_1(X) = G(X) - Q_1(X) \cdot F(X) = X^4 + X^3 + X + \overline{1} - \overline{2} \cdot X \cdot (\overline{2}X^3 + X + \overline{1})$$

$$R_1(X) = X^3 - \overline{2}X^2 - X + \overline{1}$$

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

Passo 2 Veja que o grau de $R_1(X)$ é igual ao grau de $F(X)$, então devemos repetir o processo anterior agora com $R_1(X)$ e $F(X)$. Assim $Q_2(X) = \overline{2} \cdot \overline{1} \cdot X^{3-3}$ e

$$R_2(X) = R_1(X) - Q_2(X) \cdot F(X) = X^3 - \overline{2}X^2 - X + \overline{1} - \overline{2} \cdot (\overline{2}X^3 + X + \overline{1})$$

$$R_2(X) = -\overline{2}X^2 - \overline{1}$$

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

Como o grau de $R_2(X)$ é menor que o grau de $F(X)$, não continuamos com a divisão. E Obtemos $Q(X) = Q_1(X) + Q_2(X) = \overline{2}X + \overline{2}$ e $R(X) = R_2(X) = -\overline{2}X^2 - \overline{1}$.

Uma consequência direta do Teorema da Divisão Euclidiana para polinômios é o Lema a seguir.

Lema α é uma raiz do polinômio $P(X)$ se, e somente se, $P(X)$ é divisível por $(X - \alpha)$, ou seja, $P(X) = (X - \alpha) \cdot Q(X)$.

Mais ainda, se $\alpha_1, \cdots, \alpha_i$ são as raízes distintas de $P(X)$, então podemos escrever

$$P(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_i) \cdot Q(X).$$

Atividades: (Divisão de polinômios)

4.3.1. Escreva cada polinômio da questão **4.2.2** da forma $P(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_i) \cdot Q(X)$.

4.3.2. *Efetue a divisão em $\mathbb{Z}_2$ do polinômio $X^3 + X + 1$ por X^3, X^4, X^5, X^6. Complete a tabela preenchendo com o quociente e o resto.

Divisão	Quociente	Resto
$X^3 \div X^3 + X + \overline{1}$		
$X^4 \div X^3 + X + \overline{1}$		
$X^5 \div X^3 + X + \overline{1}$		
$X^6 \div X^3 + X + \overline{1}$		

Avaliação: A avaliação do aprendizado dos alunos será feita a partir das observações do professor durante a execução das atividades.

Orientações para o professor: Sugerimos ao professor que disponibilize o texto para os alunos, e desenvolva, junto com eles, o algoritmo da divisão de polinômios. Em seguida poderá abordar o Lema da divisão por $X - \alpha$, e concluir mostrando que α é uma raíz de $P(X)$ se, e somente se, $P(X)$ é divisível por $(X - \alpha)$.

Para concluir, entregar a ficha de atividades (Divisão de polinômios) sugerida.

4.4 Aula 4: Fatorando polinômios em $K[X]$

Objetivos: Desenvolver técnicas de fatoração de um polinômio em polinômios irredutíveis.

Recursos Didáticos: Data show, computador, quadro branco e pincel.

Conteúdos Abordados: Fatoração de polinômios.

Tempo de duração: Para essa atividade sugerimos que seja empregado o tempo de uma aula de 50 minutos.

Metodologia: O professor entregará aos alunos o texto abaixo, onde será apresentado ou relembrado os conteúdos necessários para a execução da atividade. Este material também poderá ser apresentado pelo professor utilizando o data show.

Fatoração de Polinômios

Sejam $K = \mathbb{Z}_p$ (com p um número primo) um corpo finito, e X uma variável. Agora estudaremos como fatorar um polinômio em $K[X]$ em fatores irredutíveis, ou polinômios irredutíveis sobre K.

Mas o que são polinômios irredutíveis?

Um polinômio $P(X)$ é chamado de ***irredutível***, quando dada qualquer fatoração da forma $P(X) = F(X)G(X)$, pelo menos um dos fatores ($F(X)$ ou $G(X)$) é um polinômio constante não nulo.

Por exemplo, o polinômio $P(X) = X^3 + X^2 + 2$ é irredutível sobre $\mathbb{Z}_3$, pois para ser redutível ele deveria ser escrito como produto de um polinômio de grau 1 com um polinômio de grau 2, ou seria produto de três polinômios de grau 1. Mas não existem raízes em $\mathbb{Z}_3$. Logo $P(X)$ é irredutível sobre $\mathbb{Z}_3$.

Todo polinômio de grau 1 em $K[X]$ é irredutível (Por quê?).

Para fatorar um polinômio $P(X) \in K[X]$ em polinômios irredutíveis, seguimos os seguintes passos:

Passo 1: Encontramos todas as raízes do polinômio em K;

Passo 2: Escrevemos $P(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_i) \cdot Q(X)$;

Passo 3: Encontramos todos os polinômios irredutíveis de grau maior ou igual a 2 e verificar quais deles dividem $Q(X)$.

Por exemplo, vamos fatorar o polinômio $P(X) = X^3 + X + \overline{2}$ em $K = \mathbb{Z}_5$, em polinômios irredutíveis.

Seguindo os passos acima, primeiro vamos encontrar as raízes de $P(X)$, então temos

$$P(\overline{0}) = \overline{0}^3 + \overline{0} + \overline{2} = \overline{2},$$
$$P(\overline{1}) = \overline{1}^3 + \overline{1} + \overline{2} = \overline{4},$$
$$P(\overline{2}) = \overline{2}^3 + \overline{2} + \overline{2} = \overline{2},$$
$$P(\overline{3}) = \overline{3}^3 + \overline{3} + \overline{2} = \overline{2},$$
$$P(\overline{4}) = \overline{4}^3 + \overline{4} + \overline{2} = \overline{0},$$

logo $\overline{4}$ é a única raiz de $P(X)$.

Agora, escrevemos $P(X) = (X - \overline{4})(X^2 + \overline{4}X + 2)$. Como $\overline{4}$ é a única raiz de $P(X)$, segue que $(X^2 + \overline{4}X + 2)$ é irredutível.

Atividades: (Fatorando polinômios)

4.4.1. *Marque na tabela os polinômios irredutíveis em $\mathbb{Z}_2$ de grau menor do que ou igual a 3.

$P(X)$	$K = \mathbb{Z}_2$	$P(X)$	$K = \mathbb{Z}_2$	$P(X)$	$K = \mathbb{Z}_2$
X		$X + \overline{1}$		X^2	
$X^2 + \overline{1}$		$X^2 + X$		$X^2 + X + \overline{1}$	
X^3		$X^3 + \overline{1}$		$X^3 + X$	
$X^3 + X + \overline{1}$		$X^3 + X^2$		$X^3 + X^2 + \overline{1}$	
$X^3 + X^2 + X$		$X^3 + X^2 + X + \overline{1}$			

4.4.2. Fatore em polinômios irredutíveis os seguintes polinômios:

*a) $X^7 - 1$ em $\mathbb{Z}_2$;

b) $X^6 - 1$ em $\mathbb{Z}_5$.

c) $X^4 + X^3 + X + \overline{1}$ em $\mathbb{Z}_3$.

Avaliação: A avaliação do aprendizado dos alunos será feita a partir das observações do professor durante a execução das atividades.

Orientações para o professor: O professor poderá iniciar discutindo a quantidade de raízes de um polinômio $P(X)$. Explicar o que é um polinômio irredutível. Abordar cada passo da fatoração de polinômios descritos no exemplo do texto.

Para concluir, entregar a ficha de atividades (Fatorando polinômios) sugerida.

4.5 Aula 5: Códigos corretores de erros

Objetivos: Compreender a importância da matemática na aplicação de códigos corretores de erros. Estudar os códigos cíclicos, utilizando a divisão de polinômios com coeficientes em um corpo finito como ferramenta para codificação e decodificação.

Recursos didáticos: Data show, computador, quadro branco e pincel.

Conteúdos abordados: Códigos cíclicos; operações com polinômios.

Metodologia: O professor entregará aos alunos o texto abaixo, onde será apresentado ou relembrado os conteúdos necessários para a execução da atividade. Este material também poderá ser apresentado pelo professor utilizando o data show.

Códigos corretores de erros

A Teoria dos códigos corretores de erros, hoje em dia, é muito aplicada nos campos da engenharia, computação, matemática, entre outros. O objetivo principal dessa teoria é de garantir com precisão e eficácia, sempre que possível, a transferência, do remetente ao receptor, da informação desejada.

Todos os meios de comunicação (como comunicação entre computadores, telefones, smartphones, televisores, entre outros), são suscetíveis a erros durante uma transmissão.

Como é feita a transmissão das mensagens? Para transmitir uma mensagem, cada palavra é pré-codificada com um código chamado *código da fonte*. O código da fonte é formado por elementos de um conjunto chamado de *alfabeto*.

Uma *palavra do código* é uma sequência finita de símbolos do alfabeto. O número de letras de uma palavra do código chama-se o seu comprimento.

Quando o alfabeto utilizado é o conjunto $\mathbb{Z}_2 = \{0, 1\}$ o código diz-se binário.

Por exemplo, suponha que numa sorveteria uma máquina para pedidos de sorvete, possa fazer até quatro pedidos de sabores distintos de sorvete. Sejam eles baunilha, doce de leite, chocolate e morango. Ao escolher um sabor, essa máquina envia um código, referente ao sabor do sorvete, de acordo com a tabela abaixo.

Baunilha	$\longmapsto$	00	Doce de Leite	$\longmapsto$	10
Chocolate	$\longmapsto$	01	Morango	$\longmapsto$	11

Suponha então, que ao enviar um pedido de um sorvete sabor Baunilha, por alguma interferência, no lugar de enviar o código 00, a máquina envia o código 10, trocando o valor do primeiro dígito do código. Nesse caso, ao receber o código 10 será feito o sorvete sabor Doce de Leite. Considere que a cada interferência de transmissão a máquina comete no máximo um erro. **Como evitar o problema da máquina de pedir sorvete?**

A ideia da construção de códigos corretores de erros é de inserir dígitos de redundância para evitar esse tipo de problema.

Assim, por exemplo podemos modificar o nosso código da fonte acrescentando alguns dígitos, de acordo com a tabela abaixo:

Fonte	**Código da fonte**	**Código de canal**
Baunilha	00	00000
Chocolate	01	01011
Doce de Leite	10	10110
Morango	11	11101

Suponha agora que durante uma transmissão da mensagem 11101, ocorre um erro, e a mensagem recebida seja 10101. Realizando uma comparação dessa mensagem recebida, com as mensagens do código, percebemos que ela não pertence ao código, assim sabemos que existe um erro, e portanto verificamos que a mensagem do código que tem o menor número de componentes distintos da mensagem recebida é 11101, que é corretamente a mensagem transmitida.

Atividades: Não sugerimos atividades para essa aula.

Avaliação: A avaliação do aprendizado dos alunos será feita a partir das observações do professor durante a execução das atividades.

Orientações para o professor: Sugerimos que essa atividade seja aplicada em uma aula com duração de 50 minutos.

Nesta aula o professor irá mostrar a importância dos códigos corretores na transmissão da informação. O texto explica a ideia desse processo, com um exemplo ilustrativo, para que os alunos desenvolvam o conhecimento proposto pela atividade.

4.6 Aula 6: Codificação

Objetivos: Estudar os códigos cíclicos, utilizando a divisão de polinômios com coeficientes em um corpo finito como ferramenta para codificação.

Recursos didáticos: Data show, computador, quadro branco e pincel.

Conteúdos abordados: Multiplicação de matrizes; operações com polinômios.

Tempo de duração: Sugerimos que essa atividade seja aplicada em uma aula com duração de 50 minutos.

Metodologia: O professor entregará aos alunos o texto abaixo, onde será apresentado ou relembrado os conteúdos necessários para a execução da atividade. Este material também poderá ser apresentado pelo professor utilizando o data show.

Codificação

Estudaremos agora um tipo especial de códigos, que são chamados códigos cíclicos. Para definirmos esses códigos vamos considerar toda teoria que estudamos até aqui. E o interessante é que ele se torna simples quando trabalhamos com polinômios.

Escolhendo um código

Para definir um código cíclico precisaremos de um corpo finito $K = \mathbb{Z}_p$ (sendo p um número primo) e de um número natural n. Depois precisaremos fatorar $X^n - \overline{1}$ em K em fatores irredutíveis e escolheremos um desses fatores para gerar o código. Chamaremos o gerador do código de $G(X) = a_r X^r + \ldots + a_1 X + a_0$.

Por exemplo, sejam $K = \mathbb{Z}_2$ e $n = 9$. A fatoração de $X^9 - 1$ é dada por

$$X^9 - 1 = (X + 1)(X^2 + X + 1)(X^6 + X^3 + 1).$$

Agora, vamos considerar o código C gerado pelo polinômio $G(X) = X^6 + X^3 + 1$.

Preparando-se para a codificação Divida $X^r, X^{r+1}, \ldots, X^{n-1}$ por $G(X)$ e guarde cada um de seus restos. Chamaremos esses restos de $R_1(X), \ldots, R_{n-r}(X)$.

Prosseguindo com o exemplo dado acima temos:

$$X^6 = (X^6 + X^3 + 1) + (X^3 + 1)$$

$$X^7 = (X^6 + X^3 + 1)X + (X^4 + X)$$

$$X^8 = (X^6 + X^3 + 1)X^2 + (X^5 + X^2).$$

Assim, $R_1(X) = X^3 + 1$, $R_2(X) = X^4 + X$ e $R_3(X) = X^5 + X^2$.
Antes de continuarmos, vamos estabelecer uma relação entre um polinômio em $K[X]$ de grau menor do que n e uma sequência de n números em K. Para o polinômio $P(X) = b_m X^m + \ldots + b_1 X + b_0$, $m < n$, considere a sequência $(b_0, b_1, \ldots, b_m, \underbrace{0, 0, \ldots, 0}_{n-m \text{ vezes}})$.

Codificando uma mensagem Para codificar a palavra $(c_1, \ldots, c_{n-r})$, calculamos o polinômio

$$C(X) = -c_1 R_1(X) - \ldots - c_{n-k} R_{n-k}(X)$$

que tem grau menor do que k (Por quê?). Digamos que $C(X) = b_{r-1}X^{r-1} + \ldots + b_1 X + b_0$. Então a palavra codificada será $(b_0, b_1, \ldots, b_{r-1}, c_1, \ldots, c_{n-r})$.
Usando o exemplo dado no texto, codifique a palavra $(1, 1, 0)$. Temos

$$C(X) = 1 \cdot (X^3 + 1) + 1 \cdot (X^4 + X) + 0 \cdot (X^5 + X^2)$$

$$C(X) = X^4 + X^3 + X + 1,$$

logo a palavra codificada será $C = (1, 1, 0, 1, 1, 0, 1, 1, 0)$

Atividade: (Codificando uma mensagem)

4.6.1. *Considere $K = \mathbb{Z}_2$, $n = 7$ e o código cíclico C gerado pelo polinômio $G(X) = X^3 + X + 1$. Observe a tabela abaixo.

Palavra	**Pré-codificação**	**Palavra**	**Pré-codificação**
MATEMÁTICA	1100	COMER	1001
ROBÓTICA	0110	BRINCAR	1110
FAMÍLIA	0011	NAMORAR	0111
CONVERSAR	1010	COMPUTADOR	1011
VÍDEO GAME	0101	MÚSICA	1101

Dentre as palavras pré-codificadas acima escolha uma que seja importante para você e a codifique.

Avaliação: A avaliação do aprendizado dos alunos será feita a partir das observações do professor durante a execução das atividades.

Orientações para o professor: Nesta atividade, a turma será dividida em três grupos, e cada grupo irá simular uma função no sistema de comunicação (codificação, canal de transmissão e decodificação). Os grupos deverão ser mantidos na próxima aula.

Para esta aula, o professor poderá desenvolver o algoritmo da codificação com a participação dos alunos. Permitindo que eles realizem cada passo do algoritmo, utilizando o conhecimento desenvolvido nas aulas anteriores.

Para uma maior familiaridade com o algoritmo, solicite aos alunos que respondam a atividade (Codificando) proposta.

4.7 Aula 7: Decodificação

Objetivos: Estudar os códigos cíclicos, utilizando a divisão de polinômios com coeficientes em um corpo finito como ferramenta para decodificação.

Recursos didáticos: Data show, computador, quadro branco e pincel.

Conteúdos abordados: Códigos cíclicos; operações com polinômios.

Metodologia: O professor entregará aos alunos o texto abaixo onde serão apresentados ou relembrados os conteúdos necessários para a execução da atividade. Este material também poderá ser apresentado pelo professor utilizando o data show.

Decodificação

A decodificação é o método para detectar e corrigir erros num determinado código. Nem sempre um código é capaz de corrigir erros nas mensagens, e quando temos um determinado código corretor de erros, é possível corrigir apenas uma quantidade limitada de erros. Isto significa que, ao utilizarmos um código corretor de erros, estamos apenas minimizando os erros na transmissão das mensagens, o que traz maior qualidade e eficiência na comunicação.

Vamos primeiramente discutir como detectar erros nas mensagens recebidas em um código cíclico.

Detectando Erros Suponha que, depois de enviada a mensagem codificada, recebemos a palavra $M = (m_0, m_2, \ldots, m_{n-1})$.

Passo 1: Escrevemos o polinômio associado à palavra M, que é $M(X) = m_{n-1}X^{n-1} + \ldots + m_1X + m_0$;

Passo 2: Dividimos $M(X)$ por $G(X)$ (o polinômio gerador do código);

Se o resto da divisão for zero então a mensagem recebida está correta, caso contrário houve erro na transmissão e teremos que tentar corrigir o erro.

Corrigindo um erro O que iremos estudar agora permite corrigir no máximo um erro de transmissão.
Antes da continuar vamos lembrar algumas notações da aula anterior.

- Chamamos o grau de $G(X)$ de r;
- Chamamos o resto da divisão de X^{r+i-1} por $G(X)$ de $R_i(X)$, sendo o i qualquer valor entre 1 e $n - r$.

Para descobrir em qual posição da palavra M está o erro, basta observar o resto da divisão $R(X)$ de $M(X)$ por $G(X)$ de acordo com os itens descritos abaixo:

1. se $R(X) = a \cdot X^l$, com $0 \leq l \leq r - 1$ então o erro está na posição l;

2. se $R(X) = a \cdot R_i(X)$, com $1 \leq i \leq n - r$ então o erro está na posição $r - 1 + i$.

Supondo que o erro ocorreu na posição l, corrija M pondo $C = (m_0, \ldots, m_l - a, \ldots, m_{n-1})$.
Exemplo: Vamos considerar o exemplo da aula anterior, onde $K = \mathbb{Z}_2$, $n = 9$ e $G(X) = X^6 + X^3 + 1$ é o polinômio gerador do código. Suponha que recebemos a palavra $M = (1, 1, 0, 1, 0, 0, 1, 1, 0)$.
O polinômio associado a M é $M(X) = X^7 + X^6 + X^3 + X + 1$. Ao dividirmos $M(X)$ por $G(X)$ obtemos

$$M(X) = G(X)(X + 1) + X^4.$$

Como o resto não é zero temos um erro de transmissão. Além disso, sendo o resto da divisão acima $R(X) = X^4$ e este tem grau menor do que o grau de $G(X)$, segue que o erro da mensagem está em m_4. Logo

$$C = (1, 1, 0, 1, 0 - 1, 0, 1, 1, 0) = (1, 1, 0, 1, 1, 0, 1, 1, 0)$$

(lembre-se que em $\mathbb{Z}_2$ temos $1 = -1$).
Volte à aula passada e observe quem é C.

Atividade 1: (Detectando e Corrigindo Erros)

4.7.1. *Nesta atividade, os grupos da aula anterior serão mantidos. As palavras codificadas pelo primeiro grupo serão passadas para o segundo grupo e as do segundo para o terceiro, e as do terceiro para o primeiro (Chamaremos este processo de *giro de palavras*). Após passarem as palavras, cada grupo irá decidir se insere ou não um erro na palavra. Então farão um novo giro de palavras, de forma que o primeiro grupo fique com as palavras do segundo, o segundo com as do terceiro e o terceiro com as do primeiro. Depois cada grupo irá realizar o processo de decodificação das palavras.

Avaliação: A avaliação do aprendizado dos alunos será feita a partir das observações do professor durante a execução das atividades.

Orientações para o professor: Nesta aula o professor colocará em prática o processo de transmissão e decodificação das mensagens.

Para isso, sugerimos que inicialmente, realize em grupos o estudo do texto do aluno. E em seguida faça mediações abordando o conteúdo do texto. Por exemplo:

- Qual é o processo da decodificação?
- Como sabemos se uma palavra tem ou não erro?

Sugerimos para realização da atividade (Detectando e Corrigindo Erros) proposta.

Conclusão

Nesta dissertação, mostramos, de uma forma simplificada, a matemática presente nos meios de comunicação, utilizando os códigos cíclicos, como ferramenta de codificação e decodificação. Apesar da pouca utilização desses códigos na prática, consideramos uma boa ferramenta didática, por ser um código de implementação simples envolvendo operações com polinômios, e que não exige muito além do que é visto no ensino básico. Como produto final desta dissertação desenvolvemos uma proposta de sequência didática, voltada para alunos do Ensino Médio, participantes de olimpíadas de matemática, entre outros interessados. Por questões do isolamento, devido a pandemia, fomos impossibilitados de aplicar essa sequência com os alunos, mas esperamos com este trabalho estimular os professores em sua prática docente no ensino da matemática (especialmente no ensino de polinômios) e seus alunos a desenvolverem um maior interesse pelo estudo de polinômios, e incentivá-los na busca pelo conhecimento e relações da matemática presente no meio em que vivemos.

Referências

1 HEFEZ, Abramo; VILLELA, Maria Lúcia T. **Códigos corretores de erros**. Instituto de Matematica Pura e Aplicada, 2008.

2 HEFEZ, Abramo. **Curso de Algebra**, vol. 1. Coleção Matemática Universitária, IMPA/CNPq, RJ, 1993.

3 HEFEZ, ABRAMO; **ARITMÉTICA**, Coleção PROFMAT. Sociedade Brasileira de Matemática. 2009.

4 LIMA, Elon Lages. Álgebra linear. 2006.

5 BERLEKAMP, Elwyn. **Algebraic coding theory**. 1968.

6 SHANNON, Claude Elwood. **The Mathematical Theory of Communication**, by CE Shannon (and Recent Contributions to the Mathematical Theory of Communication), W. Weaver. University of illinois Press, 1949.

7 MACWILLIAMS, Florence Jessie; SLOANE, Neil James Alexander. **The theory of error-correcting codes**. Elsevier, 1977.

8 ROUSSEAU, Christiane, et al. **Mathematics and technology**. New York: Springer, 2008.

9 LIN, Shu; COSTELLO, Daniel J.**Error control coding**. Prentice hall, 2001.

10 LIRA, Everton Henrique Cardoso de. **Códigos Corretores de Erros no Ensino Médio: um estudo sobre o Código de Hamming**. Dissertação de Mestrado - PROFMAT. Universidade Federal Rural de Pernambuco, 2018.

11 BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Brasília, 2018.