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

Uma Proposta de Oficina sobre Códigos para a Contextualização do Estudo de Aritmética e Matrizes no Ensino Médio

Bruno Coelho Alves

Goiânia

2015

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR ELETRONICAMENTE OS TRABALHOS DE CONCLUSÃO DE CURSO NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **Trabalho de Conclusão de Curso de Mestrado Profissional**

2. Identificação do Trabalho

Autor (a):	Bruno Coelho Alves						
E-mail:	b.coelhoalves@gmail.com						
Seu e-mail pode ser disponibilizado na página? [X]Sim [ ] Não							
Vínculo empregatício do autor	Professor da UEG – Câmpus Santa Helena						
Agência de fomento:	-				Sigla:	-	
País:	-	UF:	-	CNPJ:	-		
Título:	Uma Proposta de Oficina sobre Códigos para a Contextualização do Estudo de Aritmética e Matrizes no Ensino Médio.						
Palavras-chave:	Códigos Corretores de Erros, Álgebra, Oficina para Ensino Médio.						
Título em outra língua:	A Workshop Proposal on Codes for the contextualization of Arithmetic and Matrix Study in High School.						
Palavras-chave em outra língua:	Error-Correcting Codes, Algebra, Workshop for High School.						
Área de concentração:	Matemática do Ensino Básico.						
Data defesa: (dd/mm/aaaa)	07/08/2015						
Programa de Pós-Graduação:	PROFMAT – Mestrado Profissional em Matemática em Rede Nacional.						
Orientador (a):	Prof. Dr. Mário José de Souza.						
E-mail:	mariojsouza@gmail.com						
Co-orientador(a):*	-						
E-mail:	-						

*Necessita do CPF quando não constar no SisPG

3. Informações de acesso ao documento:

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

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC do trabalho de conclusão de curso.

O sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses, dissertações ou trabalhos de conclusão de curso, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

Bruno Coelho Alves
_____
Assinatura do (a) autor (a)

Data: 07 / 08 / 2015

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

Bruno Coelho Alves

Uma Proposta de Oficina sobre Códigos para a Contextualização do Estudo de Aritmética e Matrizes no Ensino Médio

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.
Área de Concentração: Matemática do Ensino Básico
Orientador: Prof. Dr. Mário José de Souza.

Goiânia

2015

Ficha catalográfica elaborada automaticamente
com os dados fornecidos pelo(a) autor(a), sob orientação do Sibi/UFG.

Alves, Bruno Coelho
Uma Proposta de Oficina sobre Códigos para a Contextualização do Estudo de Aritmética e Matrizes no Ensino Médio [manuscrito] / Bruno Coelho Alves. - 2015.
74 f.: il.

Orientador: Prof. Dr. Mário José de Souza.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME) , Jataí, Programa de Pós-Graduação em Matemática (PROFMAT - Profissional), Goiânia, 2015.
Bibliografia. Apêndice.
Inclui lista de figuras.

1. Códigos Corretores de Erros. 2. Álgebra. 3. Oficina para Ensino Médio. I. Souza, Mário José de, orient. II. Título.

Bruno Coelho Alves

Uma Proposta de Oficina sobre Códigos para a Contextualização dos Estudos de Aritmética e Matrizes no Ensino Médio

Trabalho de Conclusão de Curso defendido no Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG, do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática, área de concentração Matemática do Ensino Básico, aprovado no dia 07 de agosto de 2015, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Mário José de Souza
Instituto de Matemática e Estatística-UFG
Presidente da Banca

Prof. Dr. Flávio Raimundo de Souza
Membro externo IFG - GOIÂNIA

Profª. Drª. Lidiane dos Santos Monteiro Lima
Instituto de Matemática e Estatística - UFG

Bruno Coelho Alves graduou-se em Matemática pela Universidade Estadual de Goiás - Câmpus Santa Helena em 2010, foi bolsista PICjr do CNPQ entre os anos de 2007 e 2008. Foi professor substituo no Instituto Federal Goiano - Câmpus Rio Verde no ano de 2014. É Professor de Ensino Superior na Universidade Estadual de Goiás - Câmpus Santa Helena desde 2011, atuando principalmente no curso de Licenciatura em Matemática desde o ano de 2012, fazendo parte do NDE(Núcleo Docente Estruturante). Atua como professor de Ensino Médio em colégios particulares de Rio Verde desde o ano de 2014.

Dedico este trabalho à minha esposa Marianne Ferreira Gomes e aos meus futuros filhos. Que eles possam apreciar toda a beleza que a Matemática proporciona.

Agradecimentos

Agradeço à Deus por tudo que vivi em todos esses anos.

Agradeço à minha mãe Elizabeth Cunha Coelho Alves (*In Memoriam*), que compartilhou desse sonho, sendo fundamental para a conclusão deste e, infelizmente, partindo antes da conclusão.

Agradeço à minha esposa Marianne Ferreira Gomes Alves, que, por mais difícil que foi, conseguiu compreender e suportar o desenvolvimento deste trabalho.

Agradeço ao meu pai Luiz Carlos Alves, que entendeu e auxiliou financeiramente durante grande parte deste.

Agradeço à minha irmã, refúgio para toda a pressão desses pouco mais de dois anos.

Ao meu orientador Prof. Dr. Mário José de Souza, sua contribuição foi inestimável, incentivou e auxiliou neste trabalho apesar de todos os entraves ocorridos.

Aos meus colegas de PROFMAT, eles contribuíram no desenvolvimento do meu "ser professor". Aqueles sábados serão inesquecíveis.

Resumo

Este trabalho tem como objetivo apresentar o conteúdo de Códigos Corretores de Erros a professores, de modo que possam utilizá-lo em suas aulas. Um código é a representação de uma determinada palavra ou símbolo por uma outra palavra ou símbolo. Este trabalho aborda os códigos corretores de erros, principalmente os ditos lineares. Dessa forma, o conceito de código é apresentado junto a dois exemplos motivadores. Os requisitos de Álgebra e Álgebra Linear são expostos, abordando o conceito de corpos finitos, a definição de espaço linear e de transformação linear. Os códigos corretores de erros, a partir de alfabetos definidos em corpos finitos, permitem que o envio de mensagens, mesmo em canais ruidosos, possam ser interpretadas com uma menor probabilidade de erro. Esse processo é feito em códigos lineares através de transformações lineares. Os códigos de Hamming e os códigos de Reed-Solomon são exemplos de códigos lineares que são tratados neste trabalho. Após apresentada a base teórica do conteúdo, é proposta uma oficina que possui como alvo os alunos dos anos finais do Ensino Médio. Essa oficina explora alguns códigos comuns, como o uso de dígitos verificadores e a interpretação de textos por máquinas digitais através de zeros e uns. Espera-se que este trabalho possa auxiliar a divulgação de alguns tópicos atuais de pesquisa entre os professores e incentivar o uso de novas metodologias para ensinar conteúdos que são considerados "difíceis" e "inúteis" para vários alunos de Ensino Médio.

Palavras-chave

Códigos Corretores de Erros, Álgebra, Oficina para Ensino Médio

Abstract

This work aims to present the content of Error-Correcting Codes to teachers, in a way to use this content in their classes. A code representing a particular word or symbol by another word or symbol. This study handle with the error correcting codes, especially that said linears. Thus, the concept of code is disclosed along two examples. The Linear Algebra and Algebra requirements are exposed, handling the concept of finite fields, the definition of linear space and linear transformation. The error correcting codes, from alphabets defined in finite fields, allow sending messages, even in noisy channels, they can be interpreted with a lower probability of error. This process is done in linear codes through linear transformations. Hamming codes and Reed-Solomon codes are exemples of linear codes which are showed in this work. After presented the theoretical basis of content, it is proposed a workshop that has as target students from the final years of High School. This workshop explore some common feature codes, such as the use of check digits and the interpretation of texts by digital machines by zeros and ones. It is hoped that this work can assist the release of some current research topics among teachers and encourage the use of new methodologies for teaching content that is considered " difficult " and " useless " to several students of High School.

Keywords

Error-Correcting Codes, Algebra, Workshop for High School.

Sumário

Lista de Figuras

Introdução

Os códigos se apresentam de formas tão simples no cotidiano que, às vezes, nos permite ignorar seu funcionamento e usufruir de seus resultados. Dessa forma, acaba-se por não perceber a importância de dígitos verificadores em contas bancárias, a possibilidade da leitura de códigos de barra, a melhora na qualidade da recepção de imagens por correio eletrônico, entre outros.

É de conhecimento geral que, com o advento do computador e da Internet, que os dados podem ser transmitidos apenas usando zeros e uns. O processo de transmissão de informações, principalmente no contexto atual, exige que a recepção seja o mais confiável possível, isto é, com a menor quantidade de erros. Detectar erros nesse processo e conseguir corrigí-los é uma atividade estudada e desenvolvida por uma área da Matemática conhecida como Teoria dos Códigos.

A Teoria dos Códigos tem como um de seus ramos a Teoria dos Códigos Corretores de Erros, fundada em 1948 pelo Matemático C. E. Shannon. Inicialmente apenas de interesse dos matemáticos, dentro das décadas de 50 e 60, mostrou sua utilidade a partir da década de 70, devido ao desenvolvimento dos computadores e da necessidade da transmissão de dados através de grandes distâncias. Um exemplo é o envio de imagens da Lua por sinais não antes possíveis, já que a interferência de raios não permitiam clareza na recepção. Hoje, temos a transmissão de sinal digital de TV que necessita desses códigos para transmissões usando a tecnologia 4K de forma rápida, possibilitando uma maior robustez às interferências presentes no processo de envio do sinal.

Este trabalho tem como foco desenvolver parte da teoria dos códigos corretores de erros. Utilizando os resultados apresentados, é desenvolvido uma oficina, destinada aos alunos de Ensino Médio, com o intuito de motivar o ensino de diversos temas que compõem o currículo básico do Ensino Médio.

O Capítulo 1 apresenta o conceito de código e alguns códigos usados dentro de

Matemática e Informática. É apresentada a conversão de números inteiros para outras bases numéricas e o código ASCII como exemplo do uso cotidiano desse estudo. A mudança de base é fundamental nesse momento para mostrar como é possível identificar através de corpos finitos elementos diversos, como palavras e imagens.

No Capítulo 2 é apresentado conceitos preliminares de Álgebra que fundamentam os estudos de códigos lineares e códigos cíclicos. Conceitos do estudo de polinômios sobre corpos finitos e de Álgebra Linear importantes para o desenvolvimento do estudo de códigos corretores de erros são apresentados e discutidos.

Com base nos temas preliminares mostrados, o Capítulo 3 expõe o conceito de códigos corretores de erros, suas principais características, como distância mínima e existência de isometrias, e exemplos.

O Capítulo 4 traz a classe dos códigos lineares, que são os mais usados no cotidiano devido às suas características. Sua definição, algumas de suas propriedades e o processo de codificação e descodificação envolvido nesse estudo estão apresentados neste capítulo.

O Capítulo 5 apresenta os códigos de Hamming e os códigos de Reed-Solomon, exemplos de códigos lineares de fácil implementação e decodificação.

Por fim, no Capítulo 6 encontra-se o esquema de uma oficina para ilustrar de forma simples os temas desenvolvidos neste trabalho. Pretende-se também instigar os alunos a realização de pesquisas.

Apresentar a Matemática como um ser vivo em constante evolução é dever de todo professor. Esse fato norteia a existência e o desenvolvimento deste trabalho.

O professor precisa se manter atualizado e aberto aos novos conhecimentos, principalmente aqueles que se referem a temas da atualidade, uma vez que os alunos, durante o contato com a utilidade de um conhecimento obtido em sala de aula, estão mais propícios a absorver com mais qualidade um conteúdo. Alguns dos conteúdos aqui expostos, como polinômios e matrizes, são objetos de uma pergunta muito comum em sala de aula: “Para que serve isso?”. Grande parte dos professores não conseguem responder prontamente esse questionamento. Este trabalho visa possibilitar o acesso aos professores de uma forma de alterar essa realidade, além de contextualizar alguns conteúdos, necessidade exposta em diversos parâmetros curriculares propostos pelo governo.

Capítulo 1

Códigos

Um código é um sistema de palavras ou outros símbolos usados para representar um dado conjunto de palavras ou outros símbolos. É de conhecimento que esse conceito é comum aos sistemas de criptografia, muito vistos em filmes de espionagem e livros, mas ele é aplicado a códigos mais "comuns" ao cotidiano, tais como códigos de barras, qr codes e o sistema Braille. Esse capítulo expõe o tema como explorado em [2].

1.1 Bases numéricas

Um exemplo de código é a escrita de números em outras bases numéricas.

O sistema numérico mais usado no cotidiano é o sistema decimal. Esse sistema consiste em justapor algarismos, onde cada algarismo possui um valor que depende da sua posição. Um número decimal da forma

$$m = a_n a_{n-1} a_{n-2} \cdots a_1 a_0$$

pode ser representado como

$$m = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_1 \cdot 10^1 + a_0 \cdot 10^0 = \sum_{i=0}^{n} a_i 10^i.$$

Existem outras bases que apresentam grande utilidade por possuírem um número menor de algarismos, minimizando possibilidades de erros, ou por apresentarem mais algarismos, permitindo a escrita de mais informações em um menor espaço. Entre

elas é possível citar as bases binária(composta por dois algarismos, 0 e 1) e a base hexadecimal(composta pelos algarismos da base decimal, acrescidos das letras A, B, C, D, E, F). A fim de minimizar possível confusão, os números na base binária estão aqui representados na forma $(x)_2$ e na base hexadecimal na forma $(x)_{16}$.

Um número binário possui representação decimal se escrito da forma

$$(b_n b_{n-1} \cdots b_2 b_1 b_0)_2 = b_n \cdot 2^n + b_{n-1} \cdot 2^{n-1} + \cdots + b_2 \cdot 2^2 + b_1 \cdot 2^1 + b_0 \cdot 2^0 = \sum_{i=0}^{n} b_i 2^i.$$

Um número hexadecimal pode ser representado na forma decimal caso seja escrito como

$$(h_n h_{n-1} \cdots h_2 h_1 h_0)_{16} = h_n \cdot 16^n + h_{n-1} \cdot 16^{n-1} + \cdots + h_2 \cdot 16^2 + h_1 \cdot 16^1 + h_0 \cdot 16^0 = \sum_{i=0}^{n} h_i 16^i,$$

onde os algarismos A, B, C, D, E, F devem ser substituídos por 10, 11, 12, 13, 14, 15, respectivamente.

É possível representar números em uma base inteira positiva qualquer, seja o número inteiro ou não. Esse processo é feito utilizando um processo de divisões sucessivas.

Exemplo 1. *Converter o número* $(2102)_3$ *para a base binária.*

Resolução: Sabe-se que $(2102)_3 = 2 \cdot 3^3 + 1 \cdot 3^2 + 0 \cdot 3^1 + 2 \cdot 3^0 = 65$ em decimais. Fazendo divisões sucessivas, tem-se

$$\begin{aligned} 65 &= 2 \cdot 32 + 1 \\ 32 &= 2 \cdot 16 + 0 \\ 16 &= 2 \cdot 8 + 0 \\ 8 &= 2 \cdot 4 + 0 \\ 4 &= 2 \cdot 2 + 0 \\ 2 &= 2 \cdot 1 + 0 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

Dessa forma, tomando os restos como coeficientes das potências, tem-se que $(2102)_3 = 65 = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = (1000001)_2$.

Pode ser mencionado que o principal motivador do uso de números binários e hexadecimais no cotidiano se refere ao advento da informática. Computadores digitais

trabalham internamente com números binários e permitem entradas usando códigos hexadecimais para facilitar a referência. Códigos antigos, como o código morse, apresentam representação em base ternária, isto é, utilizando três algarismos.

1.2 O código ASCII

O código ASCII(American Standart Code for Information Interchange - Código Padrão Americano para Intercâmbio de Informação) é um código binário que possibilita a conversão de números para letras maiúsculas e minúsculas, além de alguns símbolos e caracteres de controle que alteram o processamento do texto inserido.

A Tabela 1.1, extraída de [2], apresenta os valores do código ASCII dada entrada hexadecimal, isto é, deve ser realizada a operação de adição entre os valores das linhas e das colunas seguindo a numeração hexadecimal.Os símbolos presentes no intevalo entre 00 e 1F, isto é, as quatro primeiras linhas da Tabela 1.1, são conhecidos como caracteres de controle, eles alteram propriedades do documento e não são impressos no resultado. A partir desse código, é possível codificar palavras através de comando hexadecimais e, consequentemente, em valores binários, que permitem a compreensão de um texto por uma máquina digital.

Exemplo 2. *Converter a palavra "Aluno" para hexadecimal e, em seguida, em binário, usando a tabela ASCII.*

Resolução: Usando a Tabela 1.1, obtém-se A:41 L:6C U:75 N:6E O:6F, que possui representação binária 01000001 01101100 01110101 01101110 01101111, onde os zeros à esquerda foram adicionados para que cada representação tenha 8 algarismos (ditos *bits* em linguagem informacional e cada um desses conjuntos de 8 *bits* é conhecido como *byte*).

O exemplo anterior mostra como é possível o processo de codificação de palavras. Existem outros códigos que possuem propriedades semelhantes à tabela ASCII, como os códigos de barras e os qr codes, que são representantes bidimensionais do processo de codificação de informações.

Meios usados para transportar informações entre o emissário e o receptor são denominados canais de comunicação. Esse processo envolve o uso de codificações e decodificações de mensagens, além de se tentar evitar o máximo possível de ruídos. O estudo desse processo é abordado no capítulo seguinte.

	0	1	2	3	4	5	6	7
00	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL
08	BS	HT	LF	VT	FF	CR	SO	SI
10	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB
18	CAN	EM	SUB	ESC	FS	GS	RS	US
20		!	”	#	$	%	&	’
28	(	)	*	+	,	-	.	/
30	0	1	2	3	4	5	6	7
38	8	9	:	;	<	=	>	?
40	@	A	B	C	D	E	F	G
48	H	I	J	K	L	M	N	O
50	P	Q	R	S	T	U	V	W
58	X	Y	Z	[	\	]	^	_
60	‘	a	b	c	d	e	f	g
68	h	i	j	k	l	m	n	o
70	p	q	r	s	t	u	v	w
78	x	y	z	{	|	}	~	DEL

Tabela 1.1: código ASCII

Capítulo 2

Corpos Finitos e Espaços Vetoriais

Os corpos finitos e as transformações lineares são fundamentais para o desenvolvimento do estudo de códigos lineares. A base teórica deste capítulo fundamenta-se em [4], [6], [7] e [10].

2.1 Corpos Finitos

Um anel comutativo é um conjunto R munido de duas operações:

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

chamadas de adição e multiplicação, respectivamente, possuindo as seguintes propriedades:

Dados $a, b, c, 0, 1 \in R$,

1. (associatividade da adição) $a + (b + c) = (a + b) + c$;
2. (elemento neutro da adição) $a + 0 = 0 + a = a$;
3. (elemento inverso da adição) $a + (-a) = (-a) + a = 0$;
4. (comutatividade da adição) $a + b = b + a$;
5. (associatividade da multiplicação) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
6. (elemento neutro da multiplicação) $a \cdot 1 = 1 \cdot a = a$;

7. (comutatividade da multiplicação) $a \cdot b = b \cdot a$;

8. (distributividade da multiplicação em relação à adição) $a \cdot (b + c) = a \cdot b + a \cdot c$.

O elemento $a + b$ é dito soma e o elemento $a \cdot b$, também escrito como ab, é dito produto.

Definição 2.1.1. *Um anel R é dito domínio de integridade, se for válido*

$$\forall a, b \in A, a \neq 0 \text{ e } b \neq 0 \Rightarrow a \cdot b \neq 0.$$

Exemplos de domínios de integridade são os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. Em um domínio de integridade é válida a lei de cancelamento para igualdades de produtos.

Definição 2.1.2. *Um elemento de um anel R é chamado invertível se $a \cdot a^{-1} = 1$, onde o inverso de a é o elemento a^{-1}.*

Um anel em que todo elemento, diferente do 0, seja invertível, é denominado corpo.

Definição 2.1.3. *Um elemento não nulo e não invertível a de um anel R é dito primo se*

$$\forall b, c \in R, a|b \cdot c \Rightarrow a|b \text{ ou } a|c.$$

Onde $a|b$ significa que existe um elemento $x \in R$ tal que $ax = b$.

Definição 2.1.4. *Seja R um anel e $m \in R$. Dados elementos $a, b \in R$, diremos que a é congruente a b módulo m, e se escreve*

$$a \equiv b \bmod m$$

caso $m|(a - b)$.

As seguintes propriedades envolvendo congruências são válidas:
Dados $a, b, c, a', b' \in R$, então

1. $a \equiv a \bmod m$;

2. se $a \equiv b \bmod m$, então $b \equiv a \bmod m$;

3. se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$;

4. se $a \equiv a' \bmod m$ e $b \equiv b' \bmod m$, então $a + b \equiv a' + b' \bmod m$ e $a \cdot b \equiv a' \cdot b' \bmod m$.

As três primeiras propriedades caracterizam a congruência como uma relação de equivalência.

Definição 2.1.5. *A classe residual de um elemento $a \in R$, módulo m, é o conjunto*

$$[a] = \{x \in R; x \equiv a \bmod m\} = \{a + m \cdot \lambda; \lambda \in R\}$$

O anel R_m, formado pelas classes residuais módulo m, é conhecido como anel dos inteiros módulo m. Caso m seja um elemento primo p, o anel R_p é um corpo, comumente denominado corpo de Galois, representado por $GF(p)$. Como o conjunto R_p é finito, esse corpo é denominado como corpo finito. Os corpos finitos estão representados nesse trabalho por $\mathbb{F}_p$.

Polinômios podem ser construídos a partir de corpos finitos. Um polinômio é um elemento do conjunto $\mathbb{F}[x]$, onde os coeficientes são elementos do corpo finito $\mathbb{F}$ sobre uma variável x. Assim, esse conjunto é descrito como:

$$\mathbb{F}[x] = \left\{ \sum_{i=0}^{n} c_i \cdot x^i = c_0 x^0 + c_1 x^1 + c_2 x^2 + c_3 x^3 + \cdots + c_n x^n \right\}$$

onde $c_i \in \mathbb{F},\ i = 1, 2, \ldots, n$.

As operações entre os polinômios são as usuais, com a soma e produto entre os coeficientes realizadas dentro de $\mathbb{F}$.

2.2 Espaços Vetoriais

Definição 2.2.1. *Dado um corpo $\mathbb{F}$, V é um espaço vetorial sobre um corpo $\mathbb{F}$ se possui uma adição entre elementos $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$, munida das propriedades:*

- *é associativa, isto é, $(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w})$;*
- *é comutativa, isto é, $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$;*
- *possui elemento neutro, isto é, $\boldsymbol{v} + \boldsymbol{0} = \boldsymbol{0} + \boldsymbol{v} = \boldsymbol{v}$;*
- *possui simétricos, isto é, $\boldsymbol{v} + (\text{-}\boldsymbol{v}) = \boldsymbol{0}$.*

E, além disso, existe uma operação denominada multiplicação por escalar, que associa um elemento $a \in \mathbb{F}$ a um elemento $\boldsymbol{v} \in V$, um elemento $a\boldsymbol{v} \in V$, tal que

- *é distributiva, isto é,* $a(\boldsymbol{u}+\boldsymbol{v}) = a\boldsymbol{u}+a\boldsymbol{v}$ *e* $(a+b)\boldsymbol{v} = a\boldsymbol{v}+b\boldsymbol{v}$*;*
- *associativa em relação ao produto escalar, isto é,* $(ab)\boldsymbol{v} = a(b\boldsymbol{v})$*;*
- *possui elemento neutro, isto é,* $1\boldsymbol{v} = \boldsymbol{v}$*.*

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

Exemplo 3. *Os polinômios com coeficientes no corpo finito* $\mathbb{F}$*, conhecidos como* $\mathbb{F}[x]$*, com as operações usuais, estabelece uma estrutura de espaço vetorial.*

Um subespaço vetorial é um subconjunto de um espaço vetorial que mantém as mesmas propriedades de um espaço vetorial.

Definição 2.2.2. *Sejam* $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n$ *vetores de um espaço vetorial* V*. Diz-se que esses vetores são linearmente independentes caso a equação*

$$a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n = 0$$

é satisfeita apenas quando $a_1 = a_2 = \cdots = a_n = 0$*. Caso contrário, esses vetores são ditos linearmente dependentes.*

O conceito de vetores linearmente independentes é útil na definição de base e dimensão de um espaço vetorial.

Definição 2.2.3. *Seja* α *um conjunto composto exclusivamente por vetores linearmente independentes. Dizemos que* α *é uma base de um espaço vetorial* V *se todo vetor* $\boldsymbol{v}$ *de* V *pode ser escrito como combinação linear dos vetores do conjunto* α*, isto é,*

$$\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n,$$

onde $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n \in V$*.*

O número de elementos de uma base é dito dimensão de V e denotado por $dim\, V$.

No Exemplo 3, uma base para o espaço dos polinômios é o conjunto dos vetores $1, x, x^2, \cdots, x^n$, cuja dimensão é $n+1$.

Algumas funções entre espaços lineares possuem propriedades específicas, o que exige uma definição própria.

Definição 2.2.4. *Sejam* V *e* W *espaços vetoriais. Uma transformação linear de* V *em* W *é uma função* $T : V \to W$ *que possui as seguintes propriedades:*

1. $T(\boldsymbol{v}_1 + \boldsymbol{v}_2) = T(\boldsymbol{v}_1) + T(\boldsymbol{v}_2)$, *para quaisquer* $\boldsymbol{v}_1$ *e* $\boldsymbol{v}_2$ *em* V*;*

2. $T(a\boldsymbol{v}) = aT(\boldsymbol{v})$, *para quaisquer* $\boldsymbol{v}$ *em* V *e* a *em* $\mathbb{F}$.

Exemplo 4. *A aplicação* $T(x, y) = (x + y, x - y, 2x, 2y)$ *é uma transformação linear do espaço vetorial* $\mathbb{R}^2$ *no espaço vetorial* $\mathbb{R}^4$*, pois, dados* $\boldsymbol{u} = (x_1, y_1)$ *e* $\boldsymbol{v} = (x_2, y_2)$ *vetores de* $\mathbb{R}^2$ *e um escalar* $\alpha \in \mathbb{R}$*:*

- $T(\boldsymbol{u}+\boldsymbol{v}) = T(x_1+x_2, y_1+y_2) = (x_1+x_2+y_1+y_2, x_1+x_2-y_1-y_2, 2x_1+2x_2, 2y_1+2y_2) = (x_1 + y_1, x_1 - y_1, 2x_1, 2y_1) + (x_2 + y_2, x_2 - y_2, 2x_2, 2y_2) = T(\boldsymbol{u}) + T(\boldsymbol{v})$;
- $T(\alpha\,\boldsymbol{u}) = T(\alpha x_1, \alpha y_1) = (\alpha x_1 + \alpha y_1, \alpha x_1 - \alpha y_1, 2\alpha x_1, 2\alpha x_2) = \alpha(x_1 + y_1, x_1 - y_1, 2x_1, 2x_2) = \alpha T(\boldsymbol{u})$

O conceito de núcleo e imagem de uma transformação linear é de grande importância nos próximos capítulos.

Definição 2.2.5. *O núcleo de uma transformação linear* T*, definida por* $T : V \to W$*, denotado por* $Ker\,T$*, é o conjunto de vetores de* V *que possuem o vetor nulo de* W *como imagem, isto é,*

$$Ker\,T = \{\boldsymbol{v} \in V; T(\boldsymbol{v}) = 0\}.$$

A imagem de uma transformação linear T *é o conjunto*

$$Im\,T = T(V) = \{\boldsymbol{w} \in W; \exists \boldsymbol{v} \in V \Rightarrow T(\boldsymbol{v}) = \boldsymbol{w}\}.$$

É importante observar que o núcleo e a imagem de uma transformação linear são subespaços vetoriais de V e W, respectivamente. Um resultado decorrente dessa definição, de uso no estudo de códigos lineares, é mostrado a seguir.

Teorema 2.2.1. *Seja* $T : V \to W$ *uma transformação linear, onde* V *tem dimensão finita. Então*

$$dim\,Ker\,T + dim\,Im\,T = dim\,V$$

Demonstração: Considere $dim\,V = n$, e uma base $\mathfrak{B}$ de $Ker\,T$ com m vetores. É claro que $m \leq n$, pois existem no máximo n vetores linearmente independentes em V. Assume-se dois casos:

i) $m = n$: Nesse caso, $dim\,Ker\,T = dim\,V$. Dessa maneira, a base de $Ker\,T$ também é uma base de V, implicando a igualdade entre esses conjuntos. Daí,

$$Im\,T = \{0\} \Rightarrow dim\,Im\,T = 0,$$

mostrando a validade da fórmula.

ii) $m < n$: Nesse caso, podemos completar a base $\mathfrak{B}$ de $Ker\, T$ até obter uma base para V, inserindo $n - m$ vetores linearmente independentes aos já existentes em $\mathfrak{B}$. Seja $\mathfrak{B}' = \{\mathbf{v}_{m+1}, \mathbf{v}_{m+2}, \ldots, \mathbf{v}_n\}$ os vetores adicionados. Uma vez que $\mathfrak{B}'$ é um conjunto de geradores de V, pois é formado por vetores linearmente independentes, então $\{T(\mathbf{v}_{m+1}), T(\mathbf{v}_{m+2}), \ldots, T(\mathbf{v}_n)\}$ é um conjunto de geradores de $Im\, T$. Daí, $dim\, Im\, T = n - m$, satisfazendo o Teorema. ■

Maiores detalhes dessa demonstração podem ser obtidos em [4].

Capítulo 3

Códigos Corretores de Erros

Este capítulo apresenta o processo de transmissão de mensagens codificadas, tendo como foco a detecção e a possível correção de erros. A base teórica deste capítulo segue o exposto em [1], [2], [3], [5] e [8].

3.1 Canais de comunicação e codificação

Um canal de comunicação é um processo que envolve o envio de uma informação entre dois entes, denominados emissor(aquele que envia a informação) e receptor(aquele que recebe a informação). Durante o processo de transmissão da mensagem em canais ruidosos existe a possibilidade da alteração da mesma. Ruído é qualquer meio que altere a mensagem durante o envio. Ele pode ocorrer devido uma fonte térmica, elétrica, humana, imperfeições no equipamento, etc. Assim, nesses casos existe uma probabilidade de que a mensagem recebida difira da mensagem enviada.

O objetivo de um código corretor de erros é codificar a mensagem de forma a evitar a alteração da mensagem por ruídos, de forma a corrigir prováveis erros, desde que em número não além ao poder de correção do código utilizado.

Para exemplificar, como apresentado em [3], pode-se pensar no envio de uma mensagem à um robô que determina sua direção. Os comando norte, sul, leste e oeste como apresentado abaixo.

$$norte \longmapsto 10 \quad sul \longmapsto 11$$

$$leste \longmapsto 00 \quad oeste \longmapsto 01$$

O código à direita é chamado de código fonte. Supondo que o canal por onde é enviado o código fonte exista a possibilidade de ruído, é feita uma nova codificação, adicionando ao código fonte uma sequência redundante de valores que permitam realizar a detecção e correção de erros. É chamado de código de canal esse novo código gerado. O código fonte apresentado acima pode ser recodificado como:

$$norte \longmapsto 10110 \quad sul \longmapsto 11101$$

$$leste \longmapsto 00000 \quad oeste \longmapsto 01011$$

Assim, uma mensagem recebida como 01010 pelo robô na verdade deveria ser 01011, uma vez que essa é a mais próxima da mensagem recebida, e o robô deverá realizar o comando "oeste".

O processo exposto pode ser esquematizado como na Figura 3.1.

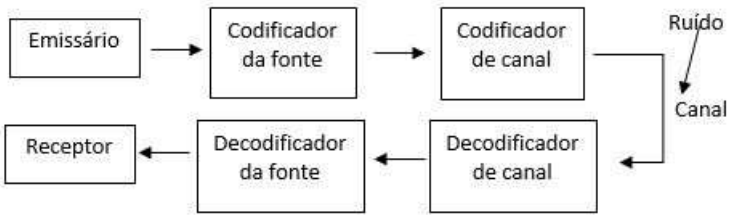

Figura 3.1: Esquema de um canal codificado

Este trabalho aborda apenas canais simétricos, isto é, aqueles cuja a probabilidade de recebimento de símbolos errados é equiprovável e, dentre os símbolos errados a serem recebidos, a probabilidade de receber qualquer um também é a mesma.

Um código corretor de erros é um subconjunto qualquer de A^n, onde A é um conjunto finito, denominado alfabeto, que contém $|A| = q$ elementos, dito $q-$ário, e n é um número natural. Uma palavra é o nome dado a um elemento de um código corretor de erros. No exemplo do robô, o conjunto $A = \{0, 1\}$ é o alfabeto, com $q = 2$, e cada palavra possui $n = 5$ dígitos.

Para que se possa criar o conceito de proximidade entre palavras é necessário o desenvolvimento de uma métrica, cuja definição se encontra abaixo.

Definição 3.1.1. *Dadas duas palavras* $\boldsymbol{u}$, $\boldsymbol{v} \in A^n$, *a métrica de Hamming, ou distância de Hamming entre* $\boldsymbol{u}$ *e* $\boldsymbol{v}$ *é definida como*

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

Por exemplo, a distância entre as palavras "norte" e "sul" do código do robô é

$$d(10110, 11101) = 3.$$

Proposição 3.1.1. *Dados* $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in A^n$, *valem as seguintes propriedades:*

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

ii) Simetria: $d(\boldsymbol{u}, \boldsymbol{v}) = d(\boldsymbol{v}, \boldsymbol{u})$;

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

Demonstração: i) É imediata da definição, pois se a igualdade ocorrer, não existe componentes distintas, logo a distância é nula e, caso haja alguma componente diferente, a distância é positiva.

ii) Como $u_i \neq v_i \Leftrightarrow v_i \neq u_i$, segue o resultado

iii) Considera-se dois casos: no primeiro, se $\mathbf{u} = \mathbf{v}$, a distância é nula, dessa forma, a distância dentre essas palavras com $\mathbf{w}$ é não-negativa, devido à i); no segundo, considere $\mathbf{u} \neq \mathbf{v}$, a contribuição das i-ésimas coordenadas à soma das distâncias é igual a 0, 1 ou 2, igual ou maior que a contribuição entre $\mathbf{u}$ e $\mathbf{v}$, que são valores entre 0 e 1 para cada coordenada. ■

Definição 3.1.2. *Dado um elemento* $\boldsymbol{a} \in A^n$ *e um número real* $t \geq 0$, *defini-se o disco e a esfera de raio* t *e centro* $\boldsymbol{a}$, *respectivamente, os conjuntos*

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

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

Esses conjuntos são finitos, com cardinalidades dadas por

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

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

Definição 3.1.3. *Seja C um código, a distância mínima de C é*

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

Dessa forma, é necessário um uso de $\binom{M}{2}$, onde $M = |C|$, cálculos computacionais para determinar a distância mínima, um custo computacional muito alto se o valor de M for grande.

Lema 3.1.1. *Seja C um código de distância mínima d. Se $\boldsymbol{c}, \boldsymbol{c'} \in C$, com $c \neq c'$, então $D(\boldsymbol{c}, \kappa) \cap D(\boldsymbol{c'}, \kappa) = \emptyset$.*

Demonstração: Suponha por absurdo que a intersecção dos discos seja não vazia, ou seja, que exista $\mathbf{v}$ tal que $\mathbf{v} \in D(\mathbf{c}, \kappa) \cap D(\mathbf{c'}, \kappa)$, daí

$$d(\mathbf{c}, \mathbf{c'}) \leq d(\mathbf{c}, \mathbf{v}) + d(\mathbf{c'}, \mathbf{v}) \leq \kappa + \kappa \leq d - 1 \leq d$$

o que é um absurdo, pois d é a distância mínima. ■

A importância de determinar a distância mínima de um código é exemplificada no Teorema 3.1.1.

Teorema 3.1.1. *Seja C um código com distância mínima d. Então C pode corrigir até $\kappa = \left[\frac{d-1}{2}\right]$ erros e detectar até $d-1$ erros.*

Demonstração: Se durante a transmissão de uma palavra $\mathbf{c}$ do código for cometido t erros, com $t \leq \kappa$, recebendo a palavra $\mathbf{r}$, então $d(\mathbf{r}, \mathbf{c}) = t \leq \kappa$; se a distância entre $\mathbf{r}$ a qualquer outra palavra do código é maior do que κ, pois $D(\mathbf{c}, \kappa) \cap D(\mathbf{c'}, \kappa) = \emptyset$, onde $\mathbf{c} \neq \mathbf{c'}$. Isso determina $\mathbf{c}$ univocamente a partir de $\mathbf{r}$. ■

Dessa forma, é possível a detecção de erros caso a quantidade seja de até $d-1$ erros, mas é possível corrigir apenas κ desses erros.

Definição 3.1.4. *Um código $C \subset A^n$ é dito perfeito, com distância mínima d, e possibilidade de correção κ se*

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

A Definição 3.1.4 garante que um código perfeito permite a correção de qualquer erro cometido.

Esse processo permite estabelecer uma estratégia para correção da mensagem recebida pelo receptor:

1. Se a palavra $\mathbf{r}$ se encontra em um disco de raio κ, substitui-se $\mathbf{r}$ por $\mathbf{c}$, onde $\mathbf{c}$ é o centro do disco.

2. Se a palavra $\mathbf{r}$ não se encontra em nenhum disco de raio κ, é improvável a decodificação correta de $\mathbf{r}$.

Um código C sobre um alfabeto A possui três parâmetros fundamentais $[n, M, d]$, que são, respectivamente, o seu comprimento, o seu número de elementos e a sua distância mínima. Nem sempre existe um código com parâmetros $[n, M, d]$ definidos inicialmente, pois existe uma interdependência entre esses parâmetros.

3.2 Isometrias

Definição 3.2.1. *Seja A um alfabeto e $n \in \mathbb{N}$. Diz-se que uma função $F : A^n \longrightarrow A^n$ é uma isometria se ela preserva distâncias de Hamming, isto é,*

$$d(F(\boldsymbol{x}), F(\boldsymbol{y})) = d(\boldsymbol{x}, \boldsymbol{y}) \quad \forall \boldsymbol{x}, \boldsymbol{y} \in A^n.$$

É claro que toda isometria é uma bijeção, pois, seja F uma isometria, dados $\mathbf{x}, \mathbf{y} \in A^n$, se $F(\mathbf{x}) = F(\mathbf{y}) \Leftrightarrow d(F(\mathbf{x}), F(\mathbf{y})) = 0$, como $d(F(\mathbf{x}), F(\mathbf{y})) = d(\mathbf{x}, \mathbf{y}) = 0$, segue que $\mathbf{x} = \mathbf{y}$, mostrando que F é injetora; como toda aplicação injetora de um conjunto finito nele próprio é sobrejetora, o resultado segue.

Proposição 3.2.1. *É válido afirmar:*

1. *A função identidade de A^n é uma isometria;*

2. *Se F é uma isometria de A^n, então F^{-1} é uma isometria de A^n;*

3. *Se F e G são isometrias de A^n, então $F \circ G$ é uma isometria de A^n.*

Demonstração:
1. É imediata, pois gera a definição;
2. Como F é uma isometria, logo bijetora, existe uma função F^{-1} tal que $(F \circ F^{-1})(x) = (F^{-1} \circ F)(x) = x$. Daí,

$$d(\mathbf{x}, \mathbf{y}) = d(F(F^{-1})(\mathbf{x}), F(F^{-1})(\mathbf{y})) = d(F^{-1}(\mathbf{x}), F^{-1}(\mathbf{y}))$$

o que prova que F^{-1} é uma isometria;
3. Como F e G são isometrias, tem-se

$$d((F \circ G)(\mathbf{x}), (F \circ G)(\mathbf{y})) = d(F(G(\mathbf{x})), F(G(\mathbf{y}))) = d(G(\mathbf{x}), G(\mathbf{y})) = d(\mathbf{x}, \mathbf{y}).$$

■

Definição 3.2.2. *Se C e C' são códigos de A^n, diz-se que C' é equivalente à C se existir uma isometria F de A^n tal que $F(C) = C'$.*

A equivalência de códigos é uma relação de equivalência, devido à Proposição 3.2.1.

Exemplo 5. *Seja $f : A \longrightarrow A$ uma bijeção, i um número inteiro tal que $1 \leq i \leq n$, a transformação linear*

$$\begin{array}{rccc} T_f^i: & A^n & \longrightarrow & A^n \\ & (x_1, x_2, \cdots, x_n) & \longmapsto & (x_1, x_2, \cdots, f(x_i), \cdots, x_n). \end{array}$$

é uma isometria.

Pode-se verificar o exemplo. Uma vez que todas as coordenadas distintas de i possuem a mesma contribuição no cálculo da distância, a única alteração possível no valor da distância esta relacionada à coordenada i. Como f é bijetora, caso as i cordenadas sejam distintas, suas imagens também são distintas, caso sejam iguais, suas imagens são iguais. Assim, a distância é preservada e, portanto, o exemplo trata de uma isometria.

Exemplo 6. *Seja π uma bijeção do conjunto $\{1, 2, \ldots, n\}$ nele próprio, chamada de permutação, a transformação linear*

$$\begin{array}{rccc} T_\pi: & A^n & \longrightarrow & A^n \\ & (x_1, x_2, \cdots, x_n) & \longmapsto & (x_{\pi(1)}, x_{\pi(2)}, \cdots, x_{\pi(n)}). \end{array}$$

é uma isometria.

Esse exemplo pode ser verificado ao notar que a i-ésima coordenada é trocada pela $\pi(i)$-ésima coordenada. As i-ésimas coordenadas contribuem para o cálculo da distância como a coordenada $\pi(k) = i$. Como a função π é uma bijeção, todas as coordenadas continuam a contribuir da mesma forma, preservando a distância de Hamming.

A importância desses dois exemplos é o Teorema 3.2.1, que permite caracterizar todas as isometrias a partir dos exemplos apresentados. Para demonstrá-lo, é apresentado dois lemas que ajudam sua compreensão.

Lema 3.2.1. *Dada uma isometria F de A^n com $n \geq 2$, e dados elementos $a_1, \ldots, a_{n-1} \in A$, existem $a'_1, \ldots, a'_{n-1} \in A$, uma bijeção $f_n : A \longrightarrow A$ e uma permutação σ de $\{1, \ldots, n\}$ tais que*

$$(T_\sigma \circ F)(a_1, \ldots, a_{n-1}, x) = (a'_1, \ldots, a'_{n-1}, f_n(x)), \quad \forall x \in A.$$

Demonstração: Se $q = 1$, então $A^n = \{a, \ldots, a\}$ e $F(a, \ldots, a) = (a, \ldots, a)$, onde resultado segue trivialmente.

Considere agora $q \geq 2$. Sejam $a_n, b_n \in A$ tais que $a_n \neq b_n$ e ponhamos

$$\mathbf{u} = (a_1, \ldots, a_{n-1}, a_n) \quad \text{e} \quad \mathbf{v} = (a_1, \ldots, a_{n-1}, b_n),$$

tem-se que

$$d(F(\mathbf{u}), F(\mathbf{v})) = d(\mathbf{u}, \mathbf{v}) = 1.$$

Daí, pode se afirmar que $F(\mathbf{u})$ e $F(\mathbf{v})$ diferem em apenas uma componente. Escolhendo convenientemente a permutação σ de $\{1, \ldots, n\}$ - que depende em princípio de $\mathbf{u}$ e $\mathbf{v}$ - pode-se supor que

$$(T_\sigma \circ F)(\mathbf{u}) = (a'_1, \ldots, a'_{n-1}, a'_n)$$

$$(T_\sigma \circ F)(\mathbf{v}) = (a'_1, \ldots, a'_{n-1}, b'_n)$$

com $a'_n \neq b'_n$.

Se $q = 2$, o lema está provado, pois, nesse caso, a bijeção f_n procurada é definida por $a_n \longmapsto a'_n$ e $b_n \longmapsto b'_n$.

Se $q > 2$, ponhamos

$$\mathbf{w} = (a_1, \ldots, a_{n-1}, x),$$

e como $T_\sigma \circ F$ é uma isometria, temos, para $x \neq a_n$, que

$$d((T_\sigma \circ F)(\mathbf{w}), (T_\sigma \circ F)(\mathbf{u})) = d(\mathbf{w}, \mathbf{u}) = 1.$$

Existe um único $y \in A$ tal que

$$(T_\sigma \circ F)(\mathbf{w}) = (a'_1, \ldots, a'_{i-1}, y, a'_{i+1}, \ldots, a'_n)$$

com $y = a'_i$. Mostrando que $i = n$, pode-se afirmar que σ não depende de $\mathbf{u}$ nem de $\mathbf{v}$. De fato, se $x = b_n$, teríamos $\mathbf{w} = \mathbf{v}$ e, consequentemente,
$(T_\sigma \circ F)(\mathbf{w}) = (a'_1, \ldots, a'_{n-1}, b'_n)$ e $i = n$. Se $x \neq b_n$ e $i < n$, teríamos

$$1 = d(\mathbf{v}, \mathbf{w}) = d((T_\sigma \circ F)(\mathbf{v}), (T_\sigma \circ F)(\mathbf{w})) = 2,$$

um absurdo, logo $i = n$. Consequentemente,

$$(T_\sigma \circ F)(\mathbf{w}) = (a'_1, \ldots, a'_{n-1}, y),$$

e, portanto, esta bem definida uma função $f_n : A \longrightarrow A$ tal que

$$(T_\sigma \circ F)(a_1, \ldots, a_{n-1}, x) = (a'_1, \ldots, a'_{n-1}, f_n(x)).$$

Como $(T_\sigma \circ F)$ é bijetora, segue que f_n é injetora e, como A é finito, temos que f_n é bijetora. ■

Lema 3.2.2. *Seja dada uma isometria G de A^n e sejam $a_1, \ldots, a_{n-1}, a'_1, \ldots, a'_{n-1}$ elementos fixos de A. Suponhamos que exista uma bijeção $f : A \longrightarrow A$ tal que*

$$G(a_1, \ldots, a_{n-1}, x) = (a'_1, \ldots, a'_{n-1}, f(x)), \quad \forall x \in A.$$

Então, existe uma isometria H de A^{n-1} tal que

$$G(x_1, \ldots, x_{n-1}, x_n) = (H(x_1, \ldots, x_{n-1}), f(x_n)), \quad (x_1, \ldots, x_n) \in A^n.$$

Demonstração: Seja $(b_1, \ldots, b_{n-1}) \in A^{n-1}$ tal que

$$(b_1, \ldots, b_{n-1}) \neq (a_1, \ldots, a_{n-1}),$$

e seja $a_n \in A$. Ponhamos

$$\mathbf{u} = (a_1, \ldots, a_n) \quad \text{e} \quad \mathbf{v} = (b_1, \ldots, b_{n-1}, a_n).$$

Tem-se, por hipótese, que

$$G(\mathbf{u}) = (a'_1, \ldots, a'_{n-1}, f(a_n)).$$

Agora, tomando $G(\mathbf{v}) = (c_1, \ldots, c_n)$, pode ser provado que $c_n = f(a_n)$. De fato, suponha por absurdo que $c_n \neq f(a_n)$. Como f é uma bijeção, existe $b_n \in A$, com $b_n \neq a_n$ tal que $c_n = f(b_n)$. Considere

$$\mathbf{w} = (a_1, \ldots, a_{n-1}, b_n);$$

logo,

$$G(\mathbf{w}) = (a'_1, \ldots, a'_{n-1}, f(b_n)).$$

Seja $r = d(\mathbf{u}, \mathbf{v})$. Logo,

$$d((a_1, \ldots, a_{n-1}), (b_1, \ldots, b_{n-1})) = d(\mathbf{u}, \mathbf{v}) = r.$$

Por outro lado,

$$d((a'_1, \ldots, a'_{n-1}), (c_1, \ldots, c_{n-1})) = d(G(\mathbf{u}), G(\mathbf{v})) - 1 = d(\mathbf{u}, \mathbf{v}) - 1 = r - 1.$$

Como $a_n \neq b_n$, tem-se

$$d(\mathbf{w}, \mathbf{v}) = d((a_1, \ldots, a_{n-1}), (b_1, \ldots, b_{n-1})) + 1 = r + 1.$$

Por outro lado,

$$d(G(\mathbf{w}), G(\mathbf{v})) = d((a'_1, \ldots, a'_{n-1}), (c_1, \ldots, c_{n-1})) = r - 1.$$

Como G é uma isometria, as duas últimas equações deveriam gerar o mesmo resultado, consequentemente, existe uma contradição e pode ser afirmado que $c_n = f(a_n)$.

Provou-se então que, dado $(x_1, \ldots, x_n) \in A^n$ qualquer, existe $(y_1, \ldots, y_{n-1}) \in A^{n-1}$ tal que

$$G(x_1, \ldots, x_n) = (y_1, \ldots, y_{n-1}, f(x_n)),$$

logo, $y_1, \ldots, y_{n-1}$ são univocamente determinados por $x_1, \ldots, x_n$; e, para provar a existência da função H, é preciso mostrar que $y_1, \ldots, y_{n-1}$ dependem de $x_1, \ldots, x_{n-1}$ e não de x_n. Para isso, considere $z_n \in A$ tal que $z_n \neq x_n$ e suponha que

$$G(x_1, \ldots, x_{n-1}, z_n) = (y'_1, \ldots, y'_{n-1}, f(z_n)),$$

de onde resulta,

$$d(G(x_1, \ldots, x_{n-1}, x_n), G(x_1, \ldots, x_{n-1}, z_n)) = d((x_1, \ldots, x_{n-1}, x_n), (x_1, \ldots, x_{n-1}, z_n)) = 1;$$

e como $f(x_n) \neq f(z_n)$, tem-se $y'_i = y_i$, $\forall i = 1, \ldots, n-1$, o que prova que esta bem definida a função $H : A^{n-1} \longrightarrow A^{n-1}$ tal que

$$G(x_1, \ldots, x_n) = (H(x_1, \ldots, x_{n-1}), f(x_n)).$$

Agora, resta mostrar que H é uma isometria. Sejam $(x_1, \ldots, x_{n-1})$ e $(x'_1, \ldots, x'_{n-1})$ em A^{n-1} e seja $x_n \in A$, logo, tem-se

$$d((x'_1, \ldots, x'_{n-1}), (x_1, \ldots, x_{n-1})) =$$

$$d((x'_1,\ldots,x'_{n-1},x_n),(x_1,\ldots,x_{n-1},x_n)) =$$
$$d(G(x'_1,\ldots,x'_{n-1},x_n),G(x_1,\ldots,x_{n-1},x_n)) =$$
$$d((H(x'_1,\ldots,x'_{n-1}),f(x_n)),(H(x_1,\ldots,x_{n-1}),f(x_n)) =$$
$$d(H(x'_1,\ldots,x'_{n-1}),H(x_1,\ldots,x_{n-1})),$$

mostrando que H é uma isometria. ■

Teorema 3.2.1. *Seja $F : A^n \longrightarrow A^n$ uma isometria, então existe uma permutação π de $\{1,2,\ldots,n\}$ e bijeções f_i de A, $i = 1,\ldots,n$, tais que*

$$F = T_\pi \circ T^1_{f_1} \circ T^2_{f_2} \circ \cdots \circ T^n_{f_n}.$$

Demonstração: É feita por indução sobre n. Se $n = 1$, o resultado segue trivialmente. Suponha $n > 1$ e que o resultado vale para $n-1$. Seja $a_1,\ldots,a_{n-1} \in A$. Pelo Lema 3.2.1, existem $a'_1,\ldots,a'_{n-1} \in A$, uma bijeção $f_n : A \longrightarrow A$ e uma permutação σ de $\{1,2,\ldots,n\}$ tais que

$$(T_\sigma \circ F)(a_1,\ldots,a_{n-1},x) = (a'_1,\ldots,a'_{n-1},f_n(x)), \quad \forall x \in A.$$

Pelo Lema 3.2.2, existe uma isometria H de A^{n-1} tal que

$$(T_\sigma \circ F)(x_1,\ldots,x_n) = (H(x_1,\ldots,x_{n-1}),f_n(x_n)).$$

Pela hipótese de indução, temos que existe uma permutação τ' de $\{1,\ldots,n-1\}$ e bijeções $f_1,\ldots,f_{n-1}$ de A tais que

$$H = (T_{\tau'})' \circ (T^1_{f_1})' \circ \cdots \circ (T^{n-1}_{f_{n-1}})',$$

onde

$$\begin{array}{lccc} (T_{\tau'})': & A^{n-1} & \longrightarrow & A^{n-1} \\ & (x_1,x_2,\cdots,x_{n-1}) & \longmapsto & (x_{\tau'(1)},\cdots,x_{\tau'(n-1)}). \end{array}$$

e, para $i = 1,\ldots,n-1$,

$$\begin{array}{lccc} (T^i_{f_i})': & A^{n-1} & \longrightarrow & A^{n-1} \\ & (x_1,x_2,\cdots,x_{n-1}) & \longmapsto & (x_1,\cdots,f_i(x_i),\cdots,x_{n-1}). \end{array}$$

Defina a permutação τ de $\{1, \ldots, n\}$ como se segue:

$$\tau(i) = \begin{cases} \tau'(i) & se \quad 1 \leq i \leq n-1 \\ n & se \quad i = n \end{cases}$$

e ponha

$$\begin{array}{rccc} T_\sigma: & A^n & \longrightarrow & A^n \\ & (x_1, x_2, \cdots, x_n) & \longmapsto & (x_{\tau(1)}, \cdots, x_{\tau(n)}). \end{array}$$

Para $i = 1, \ldots, n$, ponha

$$\begin{array}{rccc} T^i_{f_i}: & A^n & \longrightarrow & A^n \\ & (x_1, x_2, \cdots, x_n) & \longmapsto & (x_1, \cdots, f_i(x_i), \cdots, x_n). \end{array}$$

Segue, das definições de $T_\sigma \circ F$ e H, que

$$T_\sigma \circ F = T_\tau \circ T^1_{f_1} \circ \cdots \circ T^n_{f_n}.$$

Usando o fato de que $T^{-1}_\sigma = T_{\sigma^{-1}}$ e que $T_\sigma \circ T_{\sigma'} = T_{\sigma \circ \sigma'}$, e pondo $\pi = \sigma^{-1} \circ \tau$, resulta em

$$F = T_\pi \circ T^1_{f_1} \circ \cdots \circ T^n_{f_n},$$

como proposto pelo enunciado. ■

3.3 Mudança de Alfabeto

Dados dois conjuntos A e B finitos e $f : A \to B$ uma bijeção. Assuma φ como

$$\begin{array}{rccc} \varphi: & A^n & \longrightarrow & B^n \\ & (x_1, x_2, \cdots, x_n) & \longmapsto & (f(x_1), f(x_2), \cdots, f(x_n)). \end{array}$$

Essa função é bijetora, uma vez que cada coordenada é levada à uma imagem de uma função bijetora, e preserva a métrica de Hamming, caracterizando essa função como uma isometria.

A partir de um código $C \subset A^n$, com M elementos e distância mínima d, ao aplicar a função $\varphi(C) = C' \subset B^n$, tem-se que a imagem é um código sobre o alfabeto B com parâmetros iguais à C. Dessa forma, é possível mudar o alfabeto de qualquer código para um alfabeto sobre um corpo finito através de uma função bijetora $f : A \to \mathbb{F}$.

A vantagem desse método é poder realizar os estudos de códigos sempre sobre corpos finitos, uma vez que sempre é possível construir uma bijeção que leve esse alfabeto ao desejado.

Capítulo 4

Códigos Lineares

Os códigos mais utilizados na prática, devido à maior facilidade de construção e implementação, é a classe dos códigos lineares, cuja introdução é abordada neste capítulo. As fontes bibliográficas em que se baseia este capítulo são [3], [5], [12].

4.1 Conceito

Definição 4.1.1. *Um código $C \subset \mathbb{F}^n$ é chamado de código linear se for um subespaço vetorial de $\mathbb{F}^n$, ou seja, dados $\boldsymbol{u}$ e $\boldsymbol{v}$ elementos de C, é válido*

1. $\boldsymbol{u} + \boldsymbol{v} \in C$;
2. $a\boldsymbol{u} \in C$, *para todo* $a \in \mathbb{F}$.

O código do robô, apresentado no Capítulo 3, é um exemplo de código linear, pois é uma transformação linear T definida como

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

sobre o espaço vetorial formado por produtos cartesianos do corpo $\mathbb{F}_2$.

Por definição, todo código linear é um espaço vetorial finito. Assim, é possível estabelecer uma base para todo código linear e, através de combinação linear, obter todos os vetores de um código C.

Definição 4.1.2. *Dado um vetor $\boldsymbol{u} \in \mathbb{F}^n$, define-se o peso de $\boldsymbol{u}$ como sendo o número inteiro*

$$\omega(\boldsymbol{u}) := |\{i; x_i \neq 0\}|.$$

O peso de um código C é definido como

$$\omega(C) := min\{\omega(\boldsymbol{u}); \boldsymbol{u} \in C \backslash \{\boldsymbol{0}\}\}$$

O conceito de peso esta relacionado ao conceito de distância na métrica de Hamming, na forma

$$\omega(\mathbf{u}) = d(\mathbf{u}, \mathbf{0}),$$

assim, é possível definir uma nova forma de determinar a distância mínima de um código.

Proposição 4.1.1. *Seja $C \subset \mathbb{F}^n$ um código linear de distância mínima d. É válido afirmar:*

a) $d(\boldsymbol{x}, \boldsymbol{y}) = \omega(\boldsymbol{x} - \boldsymbol{y})$ *onde* $\boldsymbol{x}, \boldsymbol{y} \in C$*;*

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

Demonstração: O item *a)* decorre da definição, pois as componentes que diferem entre os vetores tem valor não-nulo, gerando o mesmo resultado. Para o item *b)*, é possível assumir a existência de um vetor $\mathbf{z} = \mathbf{x} - \mathbf{y}$ pertencente ao código C, fazendo que $d(\mathbf{x}, \mathbf{y}) = \omega(\mathbf{z})$, logo a distância mínima é o menor dos pesos, que por sua vez é a definição de $\omega(C)$. ■

A Proposição 4.1.1 e o fato de se trabalhar em um espaço vetorial permite enunciar algumas vantagens do uso de códigos lineares:

• Ao invés de ser necessário computar $\binom{|C|}{2}$ cálculos de distância para determinar a distância mínima, é necessário apenas calcular $|C| - 1$ pesos, o que é considerável principalmente se $|C|$ é grande;

• É possível conhecer todos os vetores de um código sem necessidade de listá-los, apenas mostrando sua base.

Descrever a base é a forma mais comum de indicar um código linear.

4.2 Matriz Geradora de um Código

Dada uma base ordenada $\mathfrak{B} = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k\}$ de um código linear, a matriz G cujas linhas são os vetores da base é dita matriz geradora de C associada à base $\mathfrak{B}$, assim,

$$G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix} = \begin{pmatrix} \mathbf{v}_{11} & \mathbf{v}_{12} & \cdots & \mathbf{v}_{1n} \\ \vdots & \vdots & & \vdots \\ \mathbf{v}_{k1} & \mathbf{v}_{k2} & \cdots & \mathbf{v}_{kn} \end{pmatrix}.$$

No código do robô, presente no Capítulo 3, a partir da transformação linear que gera esse código, $T(\mathbf{x}_1, \mathbf{x}_2) = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_1, \mathbf{x}_1 + \mathbf{x}_2, \mathbf{x}_2)$, obtém-se a base
$\mathfrak{B} = \{(1,0,1,1,0), (0,1,0,1,1)\}$, então uma matriz geradora desse código é

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

Observe que a transformação T leva o código da fonte, dada por vetores $(x_1, x_2) \in \mathbb{F}_2^2$, no código de canal $T(\mathbb{F}_2^2) = C \subset \mathbb{F}_2^5$. Diz-se então que T é uma codificação.

A matriz geradora não é determinada de forma única, pois o sistema linear $T(\mathbf{x}) = \mathbf{x}G$ permite a existência de outros sistemas equivalentes. Dessa forma, duas matrizes geradoras de um mesmo código linear podem ser obtidas através de uma sequência de operações do tipo:

- permutação de linhas;
- multiplicação de uma linha por um escalar não-nulo;
- adição de um múltiplo escalar de uma linha em outra;
- permutação de colunas;
- multiplicação de qualquer coluna por um escalar não-nulo.

Definição 4.2.1. *Diz-se que uma matriz geradora G de um código esta na forma padrão se*

$$G = (Id_k | A)$$

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

É sempre possível reescrever uma matriz geradora de um código na forma padrão através de um código equivalente. Um código equivalente é uma isometria linear T tal que $T(C) = C'$, onde C' é o complemento de C em relação ao espaço vetorial $\mathbb{F}^n$, isto é,

$$C \oplus C' = \mathbb{F}^n$$

onde $\oplus$ representa a soma direta entre os conjuntos.

Exemplo 7. *Considere o código linear $C \subset \mathbb{F}_3^6$ de matriz geradora*

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 1 & 0 & 2 & 0 & 1 & 1 \end{pmatrix}$$

é possível encontrar uma matriz geradora na forma padrão através da permutação das colunas para um código equivalente de matriz

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 2 & 1 & 1 \end{pmatrix}.$$

4.3 Códigos Duais

Seja $C \subset \mathbb{F}^n$ um código linear, define-se

$$C^{\perp} = \{\mathbf{v} \in \mathbb{F}^n; \langle \mathbf{v}, \mathbf{u} \rangle = 0, \quad \forall \mathbf{u} \in C\},$$

onde $\langle \mathbf{u}, \mathbf{v} \rangle$ é o produto interno entre os vetores $\mathbf{u}$ e $\mathbf{v}$. Quando o produto interno de dois vetores é nulo, diz-se que esses vetores são ortogonais.

Lema 4.3.1. *Se $C \subset \mathbb{F}^n$ é um código linear, com matriz geradora G, então:*

1. *$C^{\perp}$ é um subespaço vetorial de $\mathbb{F}^n$;*
2. *$\boldsymbol{x} \in C^{\perp} \iff G\boldsymbol{x}^t = \boldsymbol{0}$.*

Demonstração: *1.* Dados dois vetores $\mathbf{u}, \mathbf{v} \in C^{\perp}$ e um escalar $\alpha \in \mathbb{F}$, a partir das propriedades do produto interno, obtém-se:

$$\langle \mathbf{u} + \alpha\mathbf{v}, \mathbf{x} \rangle = \langle \mathbf{u}, \mathbf{x} \rangle + \alpha \langle \mathbf{v}, \mathbf{x} \rangle = 0,$$

para todo $\mathbf{x} \in C$, assim, $\mathbf{u} + \alpha\mathbf{v} \in C^{\perp}$. Logo, um subespaço vetorial de $\mathbb{F}^n$.

2. As linhas l_i da matriz G são vetores da base de C, assim, o produto pode ser escrito como $\langle l_i, \mathbf{x} \rangle$ para todas as i linhas da matriz G. Como $\mathbf{x} \in C^{\perp}$, as coordenadas da matriz resultante são todas nulas. ■

O subespaço $C^{\perp}$ é um código linear, chamado de código dual de C ou ortogonal à C.

Proposição 4.3.1. *Dado $C \subset \mathbb{F}^n$ com dimensão k e matriz geradora na forma padrão $G = (Id_k|A)$, é válido afirmar:*

i) $dim\ C^{\perp} = n - k$;

ii) $H = (-A^t|Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.

Demonstração: *i)* Como $G\mathbf{x}^t = \mathbf{0}$, devido ao Lema 4.3.1, para todo vetor $\mathbf{x} \in C^{\perp}$, pode-se usar o fato de G estar na forma padrão para reescrever essa equação como

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} + A \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Dessa forma, as $n - k$ componentes que estão multiplicando a matriz A, cada um com $q = |\mathbb{F}^n|$ possibilidades. Então, tem-se $|C^{\perp}| = q^{n-k}$ e a dimensão de $C^{\perp}$ é $n - k$.

No item *ii)*, pode-se observar que as linhas de H são linearmente independentes, então podem ser consideradas a base de um subespaço vetorial de dimensão $n - k$. Como essa base possui vetores ortogonais à base de C, tem-se que esse subespaço gerado por essa base é ortogonal à C. Uma vez que a dimensão dos dois é idêntica, conclui-se que essa base é uma base de $C^{\perp}$, assim, a matriz H é uma matriz geradora de $C^{\perp}$. ■

Um código dual é importante pois auxilia na determinação dos vetores de um código. A matriz H, matriz geradora de $C^{\perp}$ é conhecida como matriz teste de paridade de C. A Proposição 4.3.2 apresenta como utilizá-la para verificar a existência de um vetor do código C.

Proposição 4.3.2. *Seja C um código linear. Se H é uma matriz teste de paridade de C, tem-se*

$$\boldsymbol{v} \in C \iff H\boldsymbol{v}^t = \boldsymbol{0}$$

Uma demonstração dessa proposição pode ser obtida em [3]. O vetor $H\mathbf{v}^t$ é dito *síndrome* de $\mathbf{v}$.

Assim, determinar se um vetor pertence ou não à um código pode ser feito calculando a síndrome desse vetor, caso o resultado seja o vetor nulo, a afirmação é positiva.

Exemplo 8. *A partir do código do robô, apresentado no Capítulo 3, é possível verificar se os vetores $\boldsymbol{a} = 11101$ e $\boldsymbol{b} = 10111$ pertencem ao código. Como*

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

a matriz teste de paridade é dada por

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

pois $-1 \equiv 1(mod 2)$. Calculando a síndrome de cada um dos vetores pedidos,

$$H\boldsymbol{a}^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \qquad e \qquad H\boldsymbol{b}^t = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Assim, o vetor $\boldsymbol{a}$ pertence ao código e o vetor $\boldsymbol{b}$ não pertence.

De posse dessas informações, é possível detectar e corrigir qualquer possível erro em um código linear.

4.4 Codificação e decodificação com um código linear

Um código C pode ser codificado através da transformação linear relacionada, uma vez que a transformação leva o espaço vetorial $\mathbb{F}^k$ em um subespaço de dimensão k

denominado C. Assim, seja G a matriz geradora de um código e $\mathbf{x} = (x_1, x_2, \ldots, x_k) \in \mathbb{F}^k$ a mensagem a ser enviada, a codificação é realizada por

$$\mathbf{x}G = \sum_{i=1}^{k} x_i l_i,$$

onde l_i é a i-ésima linha da matriz G.

Na forma padrão, o processo é simplificado. Como $G = (Id_k|A)$, sendo a matriz A definida como $A = (a_{ij})$, a codificação pode ser feita calculando

$$\mathbf{x}G = x_1 x_2 \cdots x_k x_{k+1} \cdots x_n,$$

onde os primeiros k dígitos são os dígitos de mensagem e os dígitos x_{k+i}, com $1 \leq i \leq n-k$ são ditos dígitos verificadores, calculados como

$$x_{k+i} = \sum_{j=1}^{k} a_{ji} x_j.$$

Os dígitos verificadores atuam de forma a acrescentar uma proteção contra possíveis ruídos.

A decodificação é o processo de detecção e correção de possíveis erros em um código. Para realizar esse processo, considere $\mathbf{e}$ o vetor erro, resultado da diferença entre os vetores $\mathbf{r}$(vetor recebido) e $\mathbf{c}$(vetor transmitido), isto é, $\mathbf{e} = \mathbf{r} - \mathbf{c}$.

Observe que todas as componentes do vetor $\mathbf{e}$ não-nulas ocorrem quando existe um erro na transmissão, assim, o valor de $\omega(\mathbf{e})$ indica o número de erros cometidos em uma transmissão. Daí, caso $\omega(\mathbf{e}) = 0$, não foi cometido nenhum erro e o vetor recebido é igual ao vetor transmitido.

Como $\mathbf{c} \in C$, onde C é um código linear, tome H como a matriz teste de paridade de C. Pelo Teorema 4.3.2, é válido que $H\mathbf{c}^t = 0$, e, consequentemente,

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

ou seja, a síndrome do vetor erro é igual à síndrome do vetor recebido.

Tome h^i a i-ésima coluna da matriz H. Se $\mathbf{e} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$, então

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

Lema 4.4.1. *Dado um código linear $C \subset \mathbb{F}^n$ com capacidade de correção κ. Se o vetor recebido $\boldsymbol{r} \in \mathbb{F}^n$ e o vetor $\boldsymbol{c} \in C$ são tais que $d(\boldsymbol{c}, \boldsymbol{r}) \leq \kappa$, então existe um único vetor $\boldsymbol{e}$, com $\omega(\boldsymbol{e}) \leq \kappa$, cuja síndrome é igual à síndrome de $\boldsymbol{r}$.*

Demonstração: É claro que $\omega(\mathbf{e}) \leq \kappa$, pois $\omega(\mathbf{e}) = \omega(\mathbf{r} - \mathbf{c}) = d(\mathbf{c}, \mathbf{r})$. Suponha que exista dois vetores erros $\mathbf{e} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ e $\mathbf{e'} = (\alpha'_1, \alpha'_2, \cdots, \alpha'_n)$ que satisfaçam as condições do Lema. Então, como H é uma matriz teste de paridade, pode-se concluir que

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

gerando uma dependência linear entre $2\kappa(\leq d-1)$ colunas de H. Como existem pelo menos $d-1$ colunas linearmente independentes, então não existe colunas linearmente dependentes em H, então $\alpha_i = \alpha'_i$ para todo i e $\mathbf{e} = \mathbf{e'}$. ■

É possível estabelecer um algoritmo a partir das definições até aqui expostas para o caso onde $\omega(e) \leq 1$.

Seja H uma matriz teste de paridade de um código linear C com distância mínima $d \geq 3$, seja $\mathbf{c}$ o vetor transmitido e $\mathbf{r}$ um vetor recebido.

1. Calcule $H\mathbf{r}^t$.
2. Se $H\mathbf{r}^t = \mathbf{0}$, assuma $\mathbf{r} = \mathbf{c}$ e conclua a decodificação.
3. Se $H\mathbf{r}^t = \mathbf{s}^t \neq \mathbf{0}$, compare $\mathbf{s}^t$ com as colunas de H.
4. Caso exista i e α tais que $\mathbf{s}^t = \alpha h^i$, para $\alpha \in \mathbb{F}$, então $\mathbf{e}$ é a n-upla com α na posição i e zeros nas outras posições. Corrija $\mathbf{r}$ pondo $\mathbf{c} = \mathbf{r} - \mathbf{e}$.
5. Caso não exista as condições do item anterior, foram cometidos mais de um erro e $\omega(e) \geq 1$.

Exemplo 9. *Admitindo que uma mensagem* $\boldsymbol{w} = (101010101010101)$ *recebida de um código linear* $C \subset \mathbb{F}_2^{15}$ *contenha no máximo um erro e seja*

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

a matriz de teste de paridade de C*, pode se afirmar que ocorreu um erro de transmissão?*

Como $H\boldsymbol{w}^t = (1111)^t$*, ocorreu um erro na transmissão. Como a síndrome é a primeira coluna de* H*, o vetor erro é dado por* $\boldsymbol{e} = (100000000000000)$*. Assim, a mensagem original transmitida era* $\boldsymbol{w'} = (001010101010101)$.

Para o caso geral, será utilizada a decodificação pela síndrome.

A classe lateral de $\mathbf{v}$ segundo C é dada pelo conjunto

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

Lema 4.4.2. *Dois vetores* $\boldsymbol{u}$ *e* $\boldsymbol{v}$ *estão na mesma classe lateral de* C *se, e somente se, eles tem a mesma síndrome.*

Demonstração: Se $\mathbf{u}$ e $\mathbf{v}$ estão na mesma classe lateral, então

$$\mathbf{u} + C = \mathbf{v} + C \Longleftrightarrow \mathbf{u} - \mathbf{v} \in C \Longleftrightarrow H(\mathbf{u} - \mathbf{v})^t = \mathbf{0} \Longleftrightarrow H\mathbf{u}^t = H\mathbf{v}^t.$$

■

O Lema 4.4.2 afirma a existência de uma correspondência biunívoca entre classes laterais e síndromes. Dessa forma, elementos de uma mesma classe lateral devem ter a mesma síndrome.

Definição 4.4.1. *Os líderes de uma classe lateral são os vetores de menor peso nesse conjunto.*

A importância dos líderes de cada classe esta relacionada ao algoritmo de decodificação através das síndromes. Antes do algoritmo, é necessário a Proposição 4.4.1 para reduzir o custo computacional utilizado para determinar os líderes de cada classe.

Proposição 4.4.1. *Seja* $C \subset \mathbb{F}^n$ *um código linear com distância mínima* d*. Se* $\boldsymbol{u} \in \mathbb{F}^n$ *tal que*

$$\omega(\boldsymbol{u}) \leq \kappa = \left[\frac{d-1}{2}\right],$$

então $\boldsymbol{u}$ *é o único elemento líder de sua classe.*

Demonstração: Seja $\mathbf{u}, \mathbf{v} \in \mathbb{F}^n$, com $\omega(\mathbf{u}) \leq \kappa$ e $\omega(\mathbf{v}) \leq \kappa$. Se $\mathbf{u} - \mathbf{v} \in C$, tem-se

$$\omega(\mathbf{u} - \mathbf{v}) \leq \kappa + \kappa \leq d - 1;$$

então,

$$\mathbf{u} - \mathbf{v} = \mathbf{0} \Longleftrightarrow \mathbf{u} = \mathbf{v},$$

mostrando a unicidade. ■

O procedimento de decodificação pelas síndromes é dado pelo algoritmo abaixo:

1. Calcule a síndrome $\mathbf{s}$ do vetor recebido $\mathbf{r}$, indicada por $H\mathbf{r}^t = \mathbf{s}^t$.

2. Faça uma tabela com a síndrome de todos os elementos líderes $\mathbf{l}$ das classes do código.

3. Se $\mathbf{s}$ está na tabela, com vetor líder $\mathbf{l}$, decodifique $\mathbf{c} = \mathbf{r} - \mathbf{l}$.

4. Caso $\mathbf{s}$ não esteja na tabela, foram cometidos mais que κ erros e a decodificação não é possível.

Exemplo 10. *Seja $C \subset \mathbb{F}_2^4$ um código linear com matriz geradora*

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

Os elementos de C, obtidos por combinação linear dos elementos da base, são 0000, 1011, 0101, 1110.

As classes laterais de C são

$$\begin{aligned} 0000 + C &= C = \{0000, 1011, 0101, 1110\}, \\ 1000 + C &= \{1000, 0011, 1101, 0110\}, \\ 0100 + C &= \{0100, 1111, 0001, 1010\}, \\ 0010 + C &= \{0010, 1001, 0111, 1100\}. \end{aligned}$$

Note que todas as outras classes laterais sobre C devem coincidir com uma das quatro já apresentadas, pois a união dela é igual ao conjunto $\mathbb{F}_2^4$.

A matriz teste de paridade de C é

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

Como os líderes devem ter peso menor ou igual a 1, é possível criar a seguinte tabela relacionando os líderes com suas síndromes

Lideres	Sindromes
0000	00
1000	11
0100	01
0010	10

Dessa forma, caso a palavra recebida seja $\boldsymbol{r} = 1111$*, sua síndrome é o vetor* $\boldsymbol{s} = 01$*. Pela tabela, o vetor lider de síndrome* 01 *é* 0100*. Então o vetor* $\boldsymbol{c} = 1111 - 0100 = 1011$*.*

Capítulo 5

Exemplos de Códigos Lineares

Este capítulo apresenta dois exemplos de códigos lineares, ambos de grande uso atualmente. As principais referências desse capítulo são [3] e [5].

5.1 Códigos de Hamming

Os códigos de Hamming possuem como característica uma grande facilidade em codificação e decodificação.

Definição 5.1.1. *Um código de Hamming de ordem r sobre $\mathbb{F}_2$ é um código linear, com matriz teste de paridade H_r, de ordem $r \times n$ cujas colunas são os elementos de $\mathbb{F}_2^r \backslash \{0\}$ em uma ordem qualquer.*

De forma geral, o comprimento de um código de Hamming de ordem r é dado por $n = 2^r - 1$ e sua dimensão é $k = n - r = 2^r - r - 1$. Por exemplo, a matriz

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

é a matriz teste de paridade de um código de Hamming (15, 4), uma vez que suas colunas são todos os $2^4 - 1$ vetores não-nulos possíveis nesse espaço vetorial. A dimensão

desse código é 11. A partir de H é possível determinar a matriz geradora desse código.

A distância mínima de um código de Hamming é 3, portanto, $\kappa = 1$. Então é possível corrigir $\kappa = 1$ erro em códigos de Hamming e verificar a existência de até $d - 1 = 2$ erros.

Uma propriedade importante dos códigos de Hamming é o fato de serem sempre perfeitos.

Proposição 5.1.1. *Todo código de Hamming é perfeito.*

Demonstração: Dado $\mathbf{c} \in \mathbb{F}_2^n$, tem-se

$$|D(\mathbf{c}, \kappa)| = |D(\mathbf{c}, 1)| = 1 + n.$$

Como

$$|\bigcup_{\mathbf{c} \in C} D(\mathbf{c}, 1)| = [1 + n]\, 2^k = [1 + 2^r - 1]\, 2^{n-r} = 2^n,$$

mas $|\mathbb{F}_2^n| = 2^n$, o resultado segue. ■

5.2 Códigos de Reed-Solomon

Seja $\mathbb{F}$ um corpo finito. Considere o espaço vetorial dos polinômios de grau menor ou igual à $k - 1$ com coeficientes em $\mathbb{F}$, incluindo o polinômio nulo, ou seja,

$$\mathbb{F}[X]_{k-1} = \{P \in \mathbb{F}[X]\,; gr(P) \leq k - 1\} \cup \{0\}.$$

Esse espaço vetorial tem base definida por

$$\mathrm{B} = \{1, X, X^2, \ldots, X^{k-1}\}.$$

Considere

$$\begin{array}{rccc} T\colon & \mathbb{F}[X]_{k-1} & \longrightarrow & \mathbb{F}^n \\ & P & \longmapsto & (P(\alpha_1), P(\alpha_2), \cdots, P(\alpha_n)) \end{array}$$

uma aplicação, onde $\alpha_1, \cdots, \alpha_n$ são elementos distintos de $\mathbb{F}$. É claro que essa aplicação é uma transformação linear, pois

$$Ker\ T = \{P \in \mathbb{F}[X]\,; P(\alpha_1) = P(\alpha_2) = \cdots = P(\alpha_n) = 0\} = \{0\},$$

uma vez que é impossível que um polinômio de grau menor que k tenha n raízes distintas.

Daí, pode-se dizer que $C = Im(T)$ é um código linear de comprimento n e dimensão k.

Códigos com as propriedades apresentadas são conhecidos como códigos de Reed-Solomon.

Uma matriz geradora G de C é dada por

$$G = \begin{pmatrix} T(1) \\ T(X) \\ T(X^2) \\ \vdots \\ T(X^{k-1}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}.$$

Exemplo 11. *Considere o corpo finito* $\mathbb{F}_7$, $k = 4$ *e* $n = 6$ *e* $\alpha_1 = 3^0 = 1$, $\alpha_2 = 3^1 = 3$, $\alpha_3 = 3^2 = 2$, $\alpha_4 = 3^3 = 6$, $\alpha_5 = 3^4 = 4$, $\alpha_6 = 3^5 = 5$. *Assim a matriz geradora desse (6,4)Código de Reed-Solomon é*

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 3^0 & 3^1 & 3^2 & 3^3 & 3^4 & 3^5 \\ 3^0 & 3^2 & 3^4 & 3^6 & 3^8 & 3^{10} \\ 3^0 & 3^3 & 3^6 & 3^9 & 3^{12} & 3^{15} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \end{pmatrix}.$$

Capítulo 6

Oficina - Introdução aos códigos

O professor de Matemática deve estar ciente de sua responsabilidade em estar sempre atento aos avanços da Matemática, principalmente àqueles que estão presentes diretamente no cotidiano de seus alunos. Dessa forma, além da busca por uma constante atualização, é dever de todo professor encontrar formas de apresentar sempre que possível a contextualização dos conteúdos ensinados. A oficina surge como metodologia apropriada a desenvolver essa relação entre teoria e prática, dando um aspecto mais concreto a diversos conteúdos. Aqui se propõe uma oficina tendo como eixo temático a Teoria dos Códigos e algumas de suas aplicações no cotidiano. A teoria que embasa este capítulo segue o exposto em [2], [9] e [11].

6.1 Importância de uma oficina

Uma oficina pedagógica é uma atividade que visa a apropriação do conhecimento a partir do tripé: sentir, pensar e agir. É uma metodologia que difere da expositiva, uma vez que o principal foco da expositiva é cognitivo, enquanto a oficina pedagógica permite desenvolver também a ação e a reflexão sobre o tema proposto.

Uma característica importante em uma oficina é o papel do professor. Ele atua como mediador no processo de aprendizagem, não sendo o único motivador. Assim, as atividades propostas atuam como meio para o desenvolvimento do conhecimento. É necessário que o professor tenha algum conhecimento sobre os objetivos da oficina, mas o foco de aprendizagem deve ser centrado nas experiências vividas durante a execução.

O planejamento é necessário para uma execução adequada. Ademais, é importante ressaltar que o planejamento nunca consegue prever os resultados de forma perfeita, já que as oficinas tem como particularidade o meio como gerador do conhecimento, partindo de cada participante o saber desenvolvido na mesma.

A escolha pela execução de uma oficina se deve as suas características já apresentadas, atuando de forma a motivar a busca pelo conhecimento e possibilitando a interação em grupos, além de permitir uma avaliação distinta da formal.

O fato de ser um tópico não abordado nos currículos propostos para o Ensino Médio não impedem a realização da oficina, pois ela lida com outros temas comuns aos diversos currículos, como funções e matrizes.

A ideia para a execução da oficina é que ela possa ser realizada de forma concomitante com as aulas já previstas em calendário, a título de aplicação de tópicos já anteriormente explanados, como forma de contextualização e aplicação dos saberes teóricos obtidos.

Os pré-requisitos para a oficina são conceitos básicos de aritmética, o conhecimento das principais características de funções e o domínio de operações entre matrizes. Dessa forma, é esperado que todos os alunos do Segundo Ano do Ensino Médio já possuam a base para realizar essa oficina.

6.2 A oficina

A ideia é que a oficina seja executada em 10 aulas, cada uma com 50 minutos de duração. As atividades podem ser organizadas de forma a utilizarem um período menor de tempo, de acordo com as necessidades observadas pelos professores.

1ª aula

- Tema: O conceito de códigos.
- Tempo estimado: 50 minutos.
- Conteúdo: conceito de códigos; exemplos de códigos.
- Objetivos:

- Apresentar o conceito de códigos e exemplificá-los;
- Propor a construção de códigos.

• Estratégias de ensino:

- Explicar inicialmente os objetivos propostos a serem obtidos ao final da oficina, como compreender a importância de dígitos verificadores e a ideia por trás do envio de informações pela Internet.
- Conceituar códigos. Nesse momento devem ser expostos vários exemplos como motivação, como os códigos binários e hexadecimais (que são os temas da próxima aula), os diferentes tipos de alfabetos (o grego e o cirílico russo moderno), a LIBRAS (linguagem brasileira de sinais), o Braile (alfabeto usado para leitura por deficientes visuais).
- Abrir espaço para que os alunos possam indicar códigos presentes no cotidiano.
- Em grupos com cerca de 5 alunos, propor que eles criem um código próprio. Esse código deve possuir algumas características, como possuir menos de 20 caracteres diferentes e permitir a escrita de qualquer palavra em nosso idioma.
- Pedir para que cada grupo explique o funcionamento de seu código e utilize-o para codificar uma mesma frase. Comparar as diferentes formas apresentadas da frase, obtidas após as codificações.

• Recursos didáticos:

- Quadro e pincel;
- Apostila contendo um resumo das informações apresentadas na aula.

• Avaliação:

- Participação dos alunos durante a explanação;
- Análise dos códigos criados pelos alunos e a apresentação dos mesmos.

2ª aula

• Tema: Mudanças de bases numéricas.

• Tempo estimado: 50 minutos (pode ser ampliado em cerca de 30 minutos caso o

professor queira trabalhar as atividades da 3ª aula nesse momento e ignorar o primeiro momento de *feedback* da oficina).

• Conteúdo: sistema decimal; os sistemas binário e hexadecimal.

• Objetivos:

- Reconhecer o sistema decimal como um sistema posicional;
- Utilizar da representação decimal para expor as representações em bases diversas;
- Mostrar as bases binárias e hexadecimais.

• Estratégias de ensino:

- Incentivar os alunos a buscarem respostas para o motivo de contarmos utilizando dez algarismos distintos. Uma resposta é o fato de possuirmos dez dedos nas mãos. Mostrar como é importante a posição de um algarismo para a composição de cada número.

- Expor, a partir do conceito de valor absoluto e valor relativo, como todo número inteiro $n = a_n a_{n-1} \dots a_1 a_0$ pode ser representado na forma $n = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10^1 + a_0 \cdot 10^0$. Ilustrar esse processo com muitos exemplos, alguns deles propostos pelos próprios alunos.

- A partir da base 10, questionar qual seria a base a ser colocada no lugar do 10 para que seja possível uma representação binária, isto é, apenas com os algarismos 1 e 0, de forma a continuar representando todos os números. É possível neste ponto mostrar o porquê do uso de apenas zeros e uns, uma vez que todo algarismo maior que esses permitiria uma dupla representação nesse sistema.

- Generalizar o sistema de bases numéricas para qualquer base. Aqui é possível justificar o uso de letras para representação de valores maiores que 10.

- Mostrar o código hexadecimal, comparando-o com o binário. Mostrar que é possível uma codificação direta entre esses dois códigos.

• Recursos didáticos:

- Quadro e pincel;
- Apostila contendo um resumo das informações apresentadas na aula, pode ser utilizada a Seção 1.1 deste trabalho como referencial teórico.

• Avaliação:

- Participação dos alunos durante a explanação;
- Resolução dos questionamentos propostos.

3ª aula

• Tema: Resolução de exercícios envolvendo mudanças de bases.

• Tempo estimado: 50 minutos (30 minutos para execução das atividades e 20 minutos para obter um *feedback* sobre os temas até aqui desenvolvidos).

• Conteúdo: mudanças de bases numéricas; operações em bases distintas de 10.

• Objetivos:

- Resolver exercícios sobre os conteúdos abordados na aula anterior;
- Reservar um espaço para um primeiro intercâmbio de experiências obtidas até aqui.

• Estratégias de ensino:

- Aplicar a atividade proposta no Apêndice A, presentes em [2].
- A atividade deve ser realizada em grupos. Após cada grupo concluir suas respostas, o professor deve recolhê-las e entregar a grupos diferentes para que efetuem uma correção com base em suas respostas. Ao final, o professor deve disponibilizar as respostas corretas.
- Após as atividades, o professor deve se dirigir a um dos integrantes de cada grupo e pedir para que relatem o que aprenderam de novo com a oficina até este momento. O professor pode aproveitar este momento e expor os ganhos que ele obteve durante a mediação dessa oficina.

• Recursos didáticos:

- Quadro e pincel;
- Questionários com base no modelo proposto.

• Avaliação:

- Observação durante o desenvolvimento das atividades;
- Participação de cada grupo nas correções e durante o momento de troca de experiências.

4ª aula

• Tema: O código ASCII.

• Tempo estimado: 50 minutos

• Conteúdo: o código ASCII .

• Objetivos:

- Apresentar o código ASCII, seu uso e sua importância.
- Fazer a codificação e a decodificação de uma frase em ASCII

• Estratégias de ensino:

- Mostrar o código ASCII aos alunos. Apresentar a Tabela 1.1 como forma de relacionar o código hexadecimal e o código ASCII.
- Enfatizar a importância dele em codificar informações, como letras e outros caracteres, apenas com o uso de números. Lembrar que os computadores, por exemplo, interpretam cada comando enviado por teclados através de um sinal digital. Então a possibilidade de escrever letras e outros símbolos através de números facilita a conversão para um sistema binário.
- Pedir para os alunos converterem a frase

41 20 4D 61 74 65 6D

61 74 69 63 61 20 6D

20 61 20 72 61 69 6E

68 61 20 64 61 73 20

63 69 65 6E 63 69 61 73

ignorando a ausência de acentos. A frase é: “A Matematica e a rainha das ciencias”.

- Organizar os alunos em grupo. Em seguida, que cada grupo elabore uma pequena frase e converta para o código ASCII. Pedir para que os alunos troquem as frases codificadas com outros grupos e decodifiquem as frases recebidas.

• Recursos didáticos:

- Quadro e pincel;
- A tabela ASCII com entradas em hexadecimais, como a Tabela 1.1.

• Avaliação:

- Participação dos alunos durante a explanação do conteúdo;
- Realização da atividade de codificação e descodificação em ASCII.

5ª aula

• Tema: Códigos de controle de erros - preliminares.

• Tempo estimado: 50 minutos

• Conteúdo: canais de comunicação; distâncias de Hamming.

• Objetivos:

- Identificar o processo de transmissão de mensagens;
- Conceituar as distâncias de Hamming como métrica.

• Estratégias de ensino:

- Reunir os alunos em semicírculo. Em seguida, execute a brincadeira “telefone sem fio”. Essa brincadeira consiste em falar secretamente no ouvido da primeira pessoa uma frase, em seguida essa pessoa repete a frase da forma que ele compreendeu para quem estiver ao seu lado, esse processo se repete até que a frase tenha sido repassada para todos. O último deve dizer a frase como chegou até ele, normalmente distorcida.

- Através da brincadeira, iniciar um comentário sobre os canais de comunicação. Apresentar o vídeo disponível em

https://youtu.be/SniI_9PW_UE

Conceituar seus elementos principais, como emissor, receptor e ruído. Enfatizar o ruído, uma vez que seu conceito difere do uso comum, que apenas compreende os ruídos sonoros.

- Expor o problema da certificação da recepção correta, nem sempre possível. Utilizar este fato para indicar a necessidade de medir a distância entre as palavras recebidas. Isto pode ser feito indicando que palavras como Paula e pauta são mais próximas que feijão e arroz.

- Conceituar a distância de Hamming como métrica para códigos. Dar exemplos com os códigos já utilizados.

• Recursos didáticos:

- Quadro e pincel;
- Vídeo do *YouTube*;
- Apostila contendo um resumo da parte teórica da aula.

• Avaliação:

- Comentários durante a execução das atividades;
- Execução da brincadeira proposta.

6ª aula

• Tema: Códigos de controle de erros - primeiros exemplos

• Tempo estimado: 50 minutos (pode ser ampliado em cerca de 30 minutos caso o professor queira trabalhar as atividades da 7ª aula nesse momento e ignorar o segundo momento de *feedback* da oficina).)

• Conteúdo: operações modulares; dígitos verificadores.

• Objetivos:

- Compreender a aritmética modular como ferramenta para determinar restos;

- Identificar e executar o processo de cálculo do dígito verificador de contas do Banco do Brasil;

- Entender o processo de verificação da validade de CPFs.

• Estratégias de ensino:

- Iniciar apresentando a aritmética modular como uma relação entre números e seus restos. Indicar que cálculos modulares são comuns no cotidiano, por exemplo, ao indicar a adição entre 15 horas e 12 horas e resultar em 3 horas do dia seguinte, ao invés de 27 horas.

- Explicar a notação $a \ (mod\ p)$ como sendo o resto da divisão de a por p.

- Após uma maior familiaridade com o conceito de módulo, mostrar como funciona o cálculo do dígito verificador de agência e da conta bancária de um cliente do Banco do Brasil como exemplo.

Para obter o DV (dígito verificador) da agência, multiplica-se o primeiro dígito por 5, o segundo por 4, o terceiro por 3, o quarto por 2 e soma-se os resultados obtidos, obtendo uma soma s. O DV será o número d resultado de $d = 11 - \{s \ (mod\ 11)\}$. O DV da conta é obtido multiplicando o último algarismo por 2, o penúltimo por 3, o antepenúltimo por 4 e assim por diante. Soma-se os resultados obtidos, chegando a um valor s e calculando o DV como no caso da agência.

- Mostrar a imagem 6.1 e verificar a validade dos dados presentes no cheque.

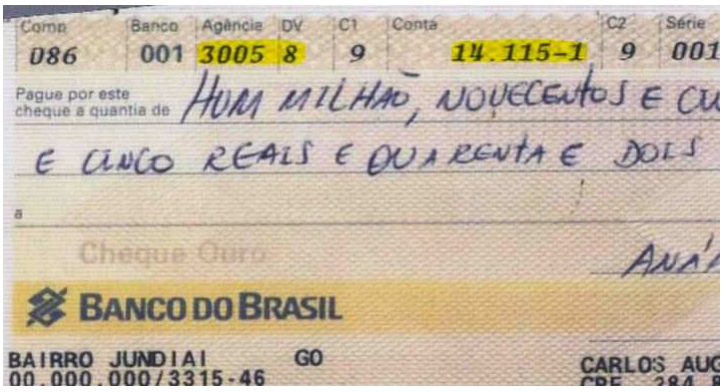

Figura 6.1: Cheque do Banco do Brasil com agência e conta destacados

- Apresentar a forma de calcular os dígitos verificadores do CPF

Para encontrar o primeiro dígito verificador, multiplica-se o primeiro dígito por 10, o segundo por 9 e assim por diante, até multiplicar o último por 2. Soma-se os valores

obtidos e, com o valor s obtido determina-se d_1 *através da equação* $d_1 = 11 - \{s \ (mod \ 11)\}$. *O segundo dígito é obtido multiplicando por 10 o segundo dígito, por 9 o terceiro dígito e assim por diante até multiplicar por 2 o primeiro dígito verificador. É calculada a soma s dos valores obtidos e determina* d_2 *pela equação* $d_2 = 11 - \{s \ (mod \ 11)\}$.

- Mostrar a imagem 6.2 e verificar a validade dos dados presentes no CPF.

Figura 6.2: Cadastro de Pessoa Física (CPF)

• Recursos didáticos:

- Quadro e pincel;
- Dados de agência e contas bancárias;
- CPFs para exemplos;
- Apostila com os métodos de cálculo dos DVs.

• Avaliação:

- Participação durante a explanação;
- Desenvolvimento durante as verificações requisitadas.

7ª aula

• Tema: Resolução de exercícios envolvendo dígitos verificadores.

• Tempo estimado: 50 minutos (30 minutos para resolução de atividades e 20 minutos para obter um *feedback* sobre os temas até aqui desenvolvidos).

• Conteúdo: Dígitos verificadores.

• Objetivos:

- Resolver exercícios sobre os conteúdos abordados nas duas aulas anteriores;

- Reservar um espaço para um segundo intercâmbio de experiências obtidas até aqui. Verificar se algumas das expectativas já foram atingidas e se existem outras expectativas a serem alcançadas.

• Estratégias de ensino:

- Aplicar as atividades propostas no Apêndice B, presentes em [2] ou criadas pelo autor.

- A atividade deve ser realizada em grupos. Após cada grupo concluir suas respostas, o professor deve recolhê-las e entregar a grupos diferentes para que efetuem uma correção com base em suas respostas. Ao final, o professor deve disponibilizar as respostas corretas.

- Após as atividades, o professor deve se dirigir a um dos integrantes de cada grupo e pedir para que relatem o que aprenderam de novo com a oficina até este momento, quais objetivos já foram alcançados e quais ainda se almeja desenvolver. O professor pode aproveitar este momento e expor os ganhos que ele obteve durante a mediação dessa oficina.

• Recursos didáticos:

- Quadro e pincel;

- Questionários com base no modelo proposto.

• Avaliação:

- Observação durante o desenvolvimento das atividades;

- Participação de cada grupo nas correções e durante o momento de troca de experiências.

8ª aula

• Tema: Códigos Lineares - os Códigos de Hamming

• Tempo estimado: 50 minutos

• Conteúdo: Conceito de códigos lineares; códigos de Hamming

• Objetivos:

- Apresentar os códigos lineares, suas propriedades e alguns exemplos;
- Introduzir os códigos de Hamming, especialmente os códigos $C(7,4)$

• Estratégias de ensino:

- Iniciar apresentando o conceito de códigos lineares. Expor a relação entre distâncias de Hamming e o conceito de peso de um vetor.

- Mostrar como encontrar a base de uma transformação linear e, a partir dela, a construção de uma matriz geradora de um código linear e mostrar a forma padrão das matrizes geradoras. Fazer isso através de exemplos.

- Introduzir os códigos de Hamming, através de exemplos, focando neste momento nos códigos da forma $(7,4)$, ou seja, aqueles com palavras codificadas de comprimento 7 que transmitem mensagens de comprimento 4.

- Pedir para os alunos construírem matrizes geradoras para $(7,4)$-Códigos de Hamming. É uma oportunidade para mostrar a equivalência entre os códigos construídos, pois apenas são distintos pela ordem de suas colunas.

- Conceituar código perfeito. Induzir o pensamento, através de operações, de que os $(7,4)$-Códigos de Hamming são perfeitos e mostrar uma demonstração.

- Definir matriz teste de paridade. Fazer exemplos com as matrizes geradoras obtidas.

• Recursos didáticos:

- Quadro e pincel;
- Apostila contendo um resumo dos temas abordados.

• Avaliação:

- Participação durante a explanação;
- Desenvolvimento das matrizes geradores conforme requisitado.

9ª aula

• Tema: Códigos Lineares - Codificação e Decodificação

• Tempo estimado: 50 minutos

• Conteúdo: síndrome de um código; codificação e decodificação de códigos lineares.

• Objetivos:

- Definir síndrome de um código;
- Apresentar o processo de codificação, através da multiplicação do código da fonte pela matriz geradora na forma padrão;
- Mostrar o processo de decodificação, iniciando com o caso onde o peso é menor ou igual a um e seguindo para o caso geral.

• Estratégias de ensino:

- Começar definindo síndrome de um vetor. Nesse momento, pode ser inserido o conceito de classe lateral de um código, fazendo isso através de exemplos, evitando o uma apresentação formal ao tópico.
- Pedir para os participantes calcularem a síndrome de alguns vetores para determinar se eles pertencem ou não a um determinado código linear proposto.
- Mostrar o processo de codificação através da multiplicação pela matriz geradora, fazer vários exemplos.
- Em seguida, apresentar os dois algoritmos indicados na Seção 4.4, mostrar um exemplo de uso de cada um, podendo ser os mesmos apresentados na seção.

• Recursos didáticos:

- Quadro e pincel;
- Apostila contendo os algoritmos propostos.

• Avaliação:

- Participação durante a exposição do conteúdo;
- Realização da atividade envolvendo o cálculo de síndromes.

10ª aula

• Tema: Resolução de atividades envolvendo códigos lineares.

• Tempo estimado: 50 minutos

• Conteúdo: códigos de Hamming; codificação e decodificação de códigos lineares.

• Objetivos:

- Resolver exercícios que abordam a aplicação de alguns códigos lineares;
- Realizar uma troca de experiências sobre o que foi desenvolvido ao longo da oficina.

• Estratégias de ensino:

- Aplicar a atividade proposta no Apêndice C, baseada em [11].
- A atividade deve ser realizada em grupos. Após cada grupo concluir suas respostas, o professor deve recolhê-las e entregar a grupos diferentes para que efetuem uma correção com base em suas respostas. Ao final, o professor deve disponibilizar as respostas corretas.
- Após as atividades, deve ser feito um momento de troca de experiências vividas ao longo de todas as aulas. É importante que todos possam ter a oportunidade de expressar os ganhos que foram obtidos e o que espera levar da oficina.

• Recursos didáticos:

- Quadro e pincel;
- Questionários com base no modelo proposto.

• Avaliação:

- Observação durante o desenvolvimento das atividades;
- Participação de cada grupo nas correções e durante o momento de troca de experiências.

Considerações finais

O presente trabalho foi elaborado de forma a divulgar aos professores a Teoria dos Códigos. É claro que, devido a vastidão do campo e sua constante evolução, só é possível introduzir seus principais conceitos e algumas aplicações.

O motivador deste trabalho é a situação do ensino de Matemática no país. Apesar da constante cobrança em alterar a metodologia de ensino, majoritariamente expositiva, não é fornecido meios que permitam aos professores conhecerem e utilizarem de outras metodologias. A oficina exposta neste trabalho possui uma ideia. Mesmo que diversos professores conheçam o funcionamento de uma oficina, existem aqueles que não compreendem todo o potencial em se trabalhar com essa metodologia.

A apresentação do conceito de códigos, feito no Capítulo 1, é colocada de forma a motivar o estudo, tendo como foco códigos bem presentes no cotidiano. Essa presença muitas vezes é imperceptível, como no caso da codificação de caracteres para compreensão digital. Mesmo assim, sua importância é inegável. Os alunos escutam muito a frase "A Matemática esta presente em todo lugar!", aceitam isso como fato indiscutível, mas muito se perguntam sobre a utilidade de diversos conteúdos apresentados no currículo escolar, principalmente aqueles presente no Ensino Médio. Os códigos foram escolhidos visando a influência da informática no comportamento atual dos alunos, de forma a criar uma identificação que permita ao professor introduzir conteúdos mais complexos, como os corpos finitos e espaços vetoriais.

Mesmo não sendo componente curricular do Ensino Médio, os tópicos de corpos finitos e espaços vetoriais tem importância para o aluno nesta etapa da educação. Eles são desenvolvidos com base no estudo de aritmética e álgebra matricial. Muitas vezes estes tópicos são encarados como inúteis pelos alunos. Muitos professores não conseguem apresentar exemplos de aplicação que envolvam esses conhecimentos, contribuindo ainda mais para perpetuar essa ideia. O desenvolvimento do Capítulo 2 apresenta definições e proposições de grande importância na Matemática, o que por

si só já justifica o estudo desses tópicos. O professor deve levar em consideração essa importância na hora de explanar sobre esses assuntos.

O Capítulo 3 foi inserido como introdução aos códigos corretores de erros. A relevância desse assunto se deve ao fato de ser recente, já que iniciou seu desenvolvimento a partir de 1960, além de explorar tópicos antes vistos apenas como importantes para a Matemática. Compreender que diversos avanços, tais como a obtenção de imagens de Marte, só foram possíveis devido ao desenvolvimento desses códigos. O professor pode utilizar o fato dos alunos terem conhecimento de diferentes códigos, aqui pode ser citado os códigos verificadores e o código de barras, para mostrar a presença da Matemática. É possível instigar uma pesquisa através de fatos corriqueiros, como a possibilidade da leitura de códigos de barras mesmo rotacionados, a identificação da validade de CPFs mesmo sem o registro de todos os valores possíveis, entre outros. Cabe ressaltar que é dever de todo professor incentivar a pesquisa por seus alunos, assim, é necessário "concretizar" a Matemática ensinada a eles.

Os códigos lineares aqui aparecem como uma forma de explanar o uso da teoria dos códigos. Como exposto nos Capítulos 4 e 5, seu uso é importante para garantir a precisão das informações recebidas. É de grande divulgação como os aparelhos digitais trabalham apenas com "zeros" e "uns", mas poucos conhecem como isso pode ser feito com qualidade.

O modelo de oficina, presente no Capítulo 6, é a contribuição deste trabalho para a comunidade. Como dito anteriormente, algumas metodologias de ensino são pouco utilizadas ou exploradas. A oficina é uma delas. O grande ganho de uma oficina é a possibilidade de executar o que é proposto, dessa forma, não é necessário um domínio absoluto pelo regente da oficina. As trocas de experiência durante o desenvolvimento geram o conhecimento almejado. Permitir ao professor o acesso a uma proposta como essa é uma tentativa de contribuir com a modificação da realidade.

A oficina não foi executada, apesar de planos para sua execução ainda neste ano.

Propõe-se que este trabalho possa ter continuidade. Ou na forma da execução da oficina aqui proposta e exposição dos resultados obtidos, ou na forma de continuidade do estudo sobre a Teoria dos Códigos, explorando outros códigos algébricos ou os códigos convolucionais.

Espera-se que, através da divulgação deste trabalho, muitos professores se sintam motivados a buscar as novas contribuições que a Matemática fornece à sociedade. Busquem incitar os alunos a buscarem o conhecimento propiciado por elas. Que possam sentir mais seguros quanto a importância do seu trabalho para a formação profissional e

social de seus alunos. Que os professores se sintam incentivados a proporem atividades, novas ou atuais, que busquem a melhoria do ensino, sempre almejando o desenvolvimento acadêmico de nossos alunos. Que a frase, tão temida pelos professores, "Para que serve isso professor?", seja motivo para mostrar a grandeza e a importância que a Matemática representa no desenvolvimento da sociedade.

Apêndice A

Atividades para a 3ª aula

Atividades Propostas

Questão 1. Converta o número $(5AB92)_{16}$ para binário e para decimal.

Questão 2. Converta $(10101011100001110101001101010100)_2$ para a hexadecimal e para decimal.

Questão 3. Compute $(2B)_{16} \times (C1F)_{16}$ e expresse o resultado em hexadecimal.

Questão 4. Compute $(101101)_2 \times (1101)$ e expresse o resultado em binário.

Questão 5. Como seria uma tabuada de adição e de multiplicação para números binários? E para números hexadecimais?

Questão 6. Para estender o conceito de base para números racionais, isto é, aqueles que podem ser expressos em forma de frações, qual seria um modelo para executar esse processo?

Questão 7. A partir do item anterior, converta os números $10,5$ e $10,3$ para binário. As duas representações são finitas? Elabore uma justificativa para o que ocorre.

Apêndice B

Atividades para a 7ª aula

Atividades Propostas

Questão 1. O ISBN (International Standart Book Number) é um código utilizado para identificação de livros e outras publicações não-seriadas. Atualmente, conta com 13 dígitos, sendo o último um dígito verificador. Sendo x_i o i-ésimo dígito desse código, o cálculo do dígito verificador é realizado através da equação

$$x_{13} = 10 - (x_1 + 3x_2 + x_3 + 3x_4 + \cdots + x_{11} + 3x_{12})(mod\ 10).$$

Qual o dígito verificador de um ISBN iniciado por 978-142007142?

Questão 2. Verifique a validade de seu CPF, conferindo os dígitos verificadores. Caso não possua, utilize algum *site* que gere aleatoriamente um número válido de CPF. Um *site* que permite gerar CPFs válidos é o

`http://www.geradordecpf.org/`

Questão 3. Determinado CPF apresenta os seguintes valores

$$025.\square 76.601 - 75,$$

onde o símbolo $\square$ esta representando um número ilegível. Qual é esse número?

Questão 4. Na imagem esta representada parte de um cartão do Banco do Brasil, contendo a agência e o número da conta em destaques, mas sem apresentar os dígitos verificadores. Determine-os.

Figura B.1: Imagem para Questão 2

Apêndice C

Atividades para a 10ª aula

Atividades Propostas

Questão 1. No código de Hamming $C(7,4)$, quais vetores deverão ser enviados se deseja transmitir as palavras:

1. (0000)
2. (0010)
3. (0111)

Questão 2. Um receptor recebeu as palavras (1111111), (1011111), (0000111) e (1111000) de um código de Hamming $C(7,4)$. Quais foram as palavras transmitidas originalmente?

Questão 3. Admitindo que uma mensagem $\vec{w} = (101010101010101)$ recebida de um código linear $C \subset \mathbb{F}_2^{15}$ contenha no máximo um erro e seja

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

a matriz de teste de paridade de C, pode se afirmar que ocorreu um erro de transmissão? Qual a mensagem original transmitida?

Referências Bibliográficas

[1] BERLEKAMP, E., *Algebraic Coding Theory.* London: World Scientific Publishing, 2015.

[2] HARDY, D. W.; RICHMAN, F.; WALKER, C. L., *Applied algebra: codes, ciphers and discrete algorithms.* Florida: CRC Press, 2011.

[3] HEFEZ, A.; VILLELA, M. L. T., *Códigos Corretores de Erros.* Rio de Janeiro: Instituto de Matematica Pura e Aplicada, 2008.

[4] HEFEZ, A.; VILLELA, M. L. T., *Introdução à Álgebra Linear.* Coleção PROFMAT. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

[5] HILL, R., *A First Course in Coding Theory.* Oxford University Press, 1986.

[6] LIDL R., NIEDERREITER H., *Introduction to Finite Fields and their Applications.* Cambridge: Cambridge Univ. Press, 1987.

[7] MENEGHESSO, Carla et al. *Códigos Corretores de Erros.* Monografia (Especialização) - Universidade Federal de São Carlos, 2012.

[8] MILIES, C. P., *Introdução à Teoria dos Códigos Corretores de Erros.* I Colóquio de Matemática da Região Centro-Oeste, 2009.

[9] PAVIANI, N. M. S.; FONTANA, N. M., *Oficinas pedagógicas: relato de uma experiência.* in Conjectura: filosofia e educação, v. 14, n. 2, p. 77-88, 2009.

[10] PINZ, C. R. F., *Dígitos Verificadores e Detecção de Erros.* Dissertação(Mestrado) - Universidade Federal do Rio Grande, 2013.

[11] ROUSSEAU, C. et al., *Mathematics and technology.* New York: Springer, 2008, pp. 173-206.

[12] SOUZA, M. J. *Minicurso -Códigos Corretores de Erros*. XXIII Semana do IME - Universidade Federal de Goiás, 07 - 10 de Outubro de 2008, Goiânia, GO.