5. Matrizes – Aplicações em problemas

A capacidade de interpretar e resolver problemas que podem ser modelados por matrizes é essencial em diversas áreas do conhecimento, sendo especialmente crucial na ciência da computação, no desenvolvimento de dados e na tecnologia como um todo. Matrizes são ferramentas fundamentais para representar e manipular dados estruturados, permitindo resolver problemas complexos de forma eficiente.

Uma destas aplicações é o estudo da codificação e decodificação de mensagens secretas denominado criptografia. Criptografia é a técnica de codificar informações para protegê-las contra acessos não autorizados, garantindo sigilo, autenticidade e integridade dos dados. Na linguagem de criptografia, os códigos são denominados **cifras**, as mensagens não codificadas são textos comuns e as mensagens codificadas são textos cifrados ou criptogramas. O processo de converter um texto comum num cifrado é denominado cifrar ou criptografar, e o processo inverso de converter um texto cifrado num comum é denominado decodificar ou decifrar.

As Cifras são os algoritmos utilizados para transformar mensagens legíveis (texto claro) em mensagens codificadas (texto cifrado) durante o processo de criptografia, tornando os dados seguros contra acessos não autorizados. Há inúmeras cifras conhecidas e utilizadas em processos de codificação, cada qual com uso específico, dependendo do nível de segurança desejado. Dentre elas, pode-se destacar:

- **RSA (Rivest-Shamir-Adleman)** – Criptografia assimétrica amplamente usada para segurança digital.
- **Blowfish e Twofish** – Algoritmos rápidos e seguros para criptografia de dados.
- **ChaCha20** – Alternativa moderna ao AES, usada em criptografia de rede.
- **AES (Advanced Encryption Standard)** – Padrão moderno e seguro usado em muitas aplicações.

Nosso objetivo, é compreender a aplicação de matrizes na área de criptografia. Para isso, estudaremos a **cifra de Hill**. Ela é uma cifra de substituição poligráfica baseada em álgebra linear. A **Cifra de Hill** utiliza **matrizes e operações matemáticas** para criptografar mensagens. Cada bloco de texto claro é transformado em um vetor numérico e multiplicado por uma **matriz chave**. O resultado é convertido de volta em caracteres, formando o texto cifrado.

Vamos supor que cada letra de texto comum e texto cifrado, tem um valor numérico que especifica sua posição no alfabeto padrão.

Tabela 5.1.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

No caso mais simples de cifras de Hill, transformamos pares sucessivos de texto comum em texto cifrado segundo o procedimento a seguir.

5.1 Criptografando uma mensagem (Módulo 26)

Passo 1. Escolha uma matriz $2 \ x \ 2$ com entradas inteiras para efetuar a codificação.

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Passo 2. Agrupe letras sucessivas de texto comum em pares, adicionando uma letra fictícia para complementar o último par se o texto comum tiver um número ímpar de letras e substitua cada letra do texto comum por seu valor numérico.

Passo 3. Converta cada par p_1 e $p_2$de letras comum sucessivamente numa matriz/vetor coluna, e forme a matriz P com cada vetor coluna p, em seguida determine o produto $q = A \cdot P$. (Se necessário aplique o módulo 26 para os valores maiores que 26).

$$p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

Passo 4. Converta cada matriz/vetor coluna cifrado q em seu equivalente alfabético;

Exemplo 1. Use a matriz A dada para obter a cifra de Hill (mensagem criptografada) do texto: MATRIZES

$$A = \begin{bmatrix} 3 & 2 \\ 0 & 5 \end{bmatrix}$$

p/ completar o par

$\underbrace{TE}_{p_1}\underbrace{XT}_{p_2}\underbrace{OO}_{p_3}$

$\underbrace{MA}_{p_1}\underbrace{TR}_{p_2}\underbrace{IZ}_{p_3}\underbrace{ES}_{p_4}$

①

MA TR IZ ES

13 1 20 18 9 0 5 19

$p_1 = \begin{pmatrix} 13 \\ 1 \end{pmatrix}$ $p_2 = \begin{pmatrix} 20 \\ 18 \end{pmatrix}$ $p_3 = \begin{pmatrix} 9 \\ 0 \end{pmatrix}$ $p_4 = \begin{pmatrix} 5 \\ 19 \end{pmatrix}$

$P = \begin{pmatrix} p_1 & p_2 & p_3 & p_4 \end{pmatrix}$

$P = \begin{pmatrix} 13 & 20 & 9 & 5 \\ 1 & 18 & 0 & 19 \end{pmatrix}$

②

$Q = A \cdot P$

$Q = \begin{pmatrix} 3 & 2 \\ 0 & 5 \end{pmatrix} \cdot \begin{pmatrix} 13 & 20 & 9 & 5 \\ 1 & 18 & 0 & 19 \end{pmatrix}$

$Q = \begin{pmatrix} \boxed{41} & \boxed{96} & \boxed{27} & \boxed{53} \\ 5 & \boxed{90} & 0 & \boxed{95} \end{pmatrix}$

$41 \div 26 = 1$, $41 - 26 = 15$

resto

$$\begin{array}{cccc} p_1 & p_2 & p_3 & p_4 \end{array}$$

$Q = \begin{pmatrix} 15 & 18 & 1 & 1 \\ 5 & 12 & 0 & 17 \end{pmatrix}$

$\boxed{\text{OERLAZAQ}}$

msg. criptografada

IMPORTANTE: Os números, 41, 96, 27, 53, 90 e 95 não possuem equivalente alfabético. Nestes casos, sempre que ocorrer um inteiro maior que 25, ele será substituído pelo resto da divisão desse número inteiro por 26. A **operação módulo 26** na Cifra de Hill é um cálculo matemático essencial para garantir que os valores numéricos das letras permaneçam dentro do intervalo de 0 a 25 (correspondente ao alfabeto). Se aparecerem números **negativos** em $A \cdot P$ ao cifrar ou decifrar, **basta somar 26 até obter um número positivo dentro do intervalo de 0 a 25**. Isso mantém a correspondência correta com as letras do alfabeto.

5.2. Decodificando (decifrando) uma mensagem (Módulo 26)

Para conseguir decodificar uma cifra de Hill, iremos usar a **inversa módulo 26 da matriz A codificadora**. Usamos o número 26 pois estamos trabalhando apenas com as 26 letras do alfabeto, caso se queira utilizar acentuações e pontuação, por exemplo, seria necessário trabalhar com outro módulo e seguir os mesmos passos. Se m for um número inteiro positivo, dizemos que uma matriz A é invertível módulo m se existir uma matriz B, tal que,

$$AB = BA = I \quad (mod\ m)$$

sendo B a matriz **inversa módulo 26 de A**, a qual denotamos por $A^{-1}(mod\ 26)$.

1º Passo: Determinar a matriz $A^{-1}(mod\ 26)$. Se A for quadrada de ordem 2, dada por $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$$A^{-1}(mod\ 26) = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$\det(A) \cdot I = 1 \ (mod\ 26)$

onde, $(ad - bc)^{-1}$ é o inverso multiplicativo módulo 26 do determinante de A.

IMPORTANTE: Uma matriz quadrada A com entradas em módulo 26, é invertível módulo 26 se, e somente se, o inverso multiplicativo de $\boldsymbol{det}\ (\boldsymbol{A})$ não é divisível por 2 e 13.

2º Passo: Divida o texto cifrado que conhecemos em pares de letras, e substituindo por seus correspondentes numéricos, escreva cada vetor/matriz coluna q, e por fim obtenha os correspondentes vetores p da forma,

$$p = A^{-1}q$$

substituindo cada número dos vetores p por suas letras correspondentes. Assim, conseguimos decifrar a mensagem.

Definição: Dado um número a em módulo 26, dizemos que a^{-1} em módulo 26 é um inverso multiplicativo de a módulo 26, se $a \cdot a^{-1} = a^{-1} \cdot a = 1 \ (mod\ 26)$.

Tabela 5.2. Inversos multiplicativos de números em módulo 26.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

▷ continuando o Exemplo 1: decodificando a mensagem OERLAZAQ

$$Q = \begin{pmatrix} 15 & 18 & 1 & 1 \\ 5 & 12 & 0 & 17 \end{pmatrix} \quad A = \begin{pmatrix} 3 & 2 \\ 0 & 5 \end{pmatrix}$$ do exemplo 1

① $\det(A) = \begin{vmatrix} \overset{a}{3} & \overset{b}{2} \\ \underset{c}{0} & \underset{d}{5} \end{vmatrix}$

$\det(A) = 15$

• calc. o inverso multiplicativo do $\det(A)$

$15 \rightarrow 7$

② $A^{-1}(mod\ 26) = 7 \cdot \begin{pmatrix} \overset{d}{5} & \overset{-b}{-2} \\ \underset{-c}{0} & \underset{a}{3} \end{pmatrix}$

$A^{-1}(mod\ 26) = \begin{pmatrix} 35 & -14 \\ 0 & 21 \end{pmatrix}$

$A^{-1}(mod\ 26) = \begin{pmatrix} 9 & 12 \\ 0 & 21 \end{pmatrix}$

③ $P = A^{-1}(mod\ 26) \cdot Q$

$P = \begin{pmatrix} 9 & 12 \\ 0 & 21 \end{pmatrix} \cdot \begin{pmatrix} 15 & 18 & 1 & 1 \\ 5 & 12 & 0 & 17 \end{pmatrix}$

$P = \begin{pmatrix} 195 & 306 & 9 & 213 \\ 105 & 252 & 0 & 357 \end{pmatrix} \xrightarrow{mod\ 26} \begin{pmatrix} 13 & 20 & 9 & 5 \\ 1 & 18 & 0 & 19 \end{pmatrix}$

▷ matriz P do ex. 1

13 → M
1 → A
20 → T
18 → R
9 → I
0 → Z
5 → E
19 → S

Lista 4. Criptografia – (Utilize em todos os exercícios a tabela de Hill do exemplo da aula).

1. Obtenha a cifra de Hill da mensagem MATEMÁTICA com cada matriz codificadora dada.

a) $\begin{bmatrix} 7 & 4 \\ 1 & 1 \end{bmatrix}$ b) $\begin{bmatrix} 8 & 1 \\ 5 & 2 \end{bmatrix}$ c) $\begin{bmatrix} 5 & 1 \\ 4 & 5 \end{bmatrix}$ d) $\begin{bmatrix} 5 & 8 \\ 0 & -1 \end{bmatrix}$

2. Obtenha a cifra de Hill da mensagem DARK NIGTH com cada matriz codificadora dada.

a) $\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$ b) $\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$ c) $\begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix}$ d) $\begin{bmatrix} 5 & 2 \\ 4 & 3 \end{bmatrix}$

3. Decodifique a mensagem SAKNOXAOJX sabendo que é uma cifra de Hill com matriz codificadora $\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$

4. Decodifique a mensagem JAJKYIWYTCYIOQUQ, sabendo que é uma cifra de Hill com matriz codificadora $\begin{bmatrix} 3 & 1 \\ 3 & 8 \end{bmatrix}$.

5. Obtenha a cifra de Hill para a mensagem CRIPTOGRAFIA IFRS com a matriz codificadora $\begin{bmatrix} 1 & 4 \\ -1 & 3 \end{bmatrix}$. Em seguida, faça o processo de decodificação para retornar a mensagem original.

OBS: Caso o determinante da matriz A, seja negativo, primeiro converte-se o número negativo para o seu equivalente positivo no módulo 26. Depois, calcula-se o inverso multiplicativo desse número. Em seguida, se necessário, retorna-se o resultado para o intervalo de 0 a 25. Resumindo, o inverso módulo 26 de um número negativo é o mesmo que o inverso módulo 26 do seu equivalente positivo (no intervalo de 0 a 25).

Exemplo:

$A = \begin{bmatrix} 5 & 5 \\ 0 & -3 \end{bmatrix}$ $\det(A) = -15$ $\quad conversão\ para\ positivo: -15 + 26 = 11;$

Inverso multiplicativo de 11 é 19 de acordo com a tabela 5.2. Logo, o inverso módulo 26 de -15 é igual a 19.

Respostas:

Número 1: a) QNDYQNTCYD b) AOIFAOMNYQ c) NEAANEEUPQ d) UYJUUYPQWY

Número 2: a) GIYUOKOHFX b) SFANEFJUDX c) ENCXWHAIP c) VSHAJEWJDD

Número 3: We love math Número 4: Eu gosto de estudar

Número 5: WYUMBYAUYQMTGIPM