Centro Federal de Educação Tecnológica-MG
Departamento de Matemática

# 1 Aula sobre aplicação de Matrizes

## 1.1 Determinante e inversa de uma matriz 2x2

Considere a matriz

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

O determinante da matriz $A$ é definido por

$$\det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

Uma matriz $A$ é dita invertível se existe uma matriz $B$, tal que $A.B = B.A = I$. E para verificar se uma matriz possui inversa, basta verificar se seu determinante é diferente de Zero.

Supondo que a matriz $A$ de ordem 2 possui inversa, podemos encontrar a inversa de

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

usando a fórmula

$$A^{-1} = \frac{1}{detA} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Observe nessa fórmula a importância de $det(A)$ ser diferente de Zero.

## 1.2 O que é Criptografia?

Criptografia é a ciência de proteger informações, tornando-as ilegíveis para quem não tem a chave de acesso. Ela é utilizada em muitas situações do nosso dia a dia, como em mensagens de e-mail, transações bancárias e comunicações online. Para criptografar uma mensagem, usamos um algoritmo e uma chave. O objetivo é embaralhar as informações para que apenas a pessoa que conhece a chave consiga "desembaralhar" a mensagem e entender o conteúdo.

Existem dois tipos de criptografia que são mais usadas, os de chave simétrica e os de chave assimétrica.

Matrizes são estruturas matemáticas que podem ser usadas para transformar uma mensagem em um código. As matrizes funcionam como uma espécie de "chave" para embaralhar e reorganizar os dados da mensagem, tornando-a ilegível para quem não souber o procedimento correto.

## 1.3 Cifra de Hill

Cifra de Hill é um tipo de cifra de substituição baseado em álgebra linear usado para codificação de mensagens. Foi inventada pelo matemático norte americano Lester S. Hill em 1929. Uma mensagem codificada com uma matriz $N \times N$ é chamada de N-Cifra de Hill.

Um sistema poligráfico é um sistema de criptografia no qual o texto é separado em conjuntos de n letras, cada qual é substituído por um conjunto de n letras cifradas. As cifras de Hill são uma classe de sistemas poligráficos, baseados em transformações matriciais.

**Codificação e decodificação**

- Transformamos a mensagem em uma matriz, convertendo as letras em números usando va tabela de letras e números abaixo:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |

| N | 0 | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

- Codificação: Multiplicar uma matriz associada à mensagem por uma matriz-chave $A$ para obter o código de modo que $det(A) \neq 0(mod 26)$ e diferente de 2 e 13, além disso, $mdc(det\ A, 26) = 1$.

- Decodificação: A recuperação da mensagem original ocorre por meio da multiplicação pela matriz inversa da matriz chave. No caso de uma matrix $2 \times 2$,

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{1}$$

sua inversa módulo 26 é dada por

$$A^{-1} \equiv (\det A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \pmod{26}, \tag{2}$$

em que $(\det A)^{-1}$ representa o inverso multiplicativo do determinante módulo 26.

A chave para Criptografar será uma matriz A invertível. E a chave para descriptografar será a inversa de A.

## 1.4 Exemplo

Considere a matriz,

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

vamos verificar se $A$ é invertível.
Para uma matriz ser invertível, seu determinante precisa ser diferente de zero. Como $detA = 10 - 9 = 1 \neq 0$, segue que $A$ possui inversa.

Utilizando a matriz $A$, vamos criptografar a frase:

CIFRAR É UMA ARTE

Primeiramente vamos substituir cada letra da frase pelo número correspondente da Tabela dada anteriormente e montar uma matriz B do tipo 2x7

$$B = \begin{bmatrix} c & i & f & r & a & r & e \\ u & m & a & a & r & t & e \end{bmatrix} = \begin{bmatrix} 3 & 9 & 6 & 18 & 1 & 18 & 5 \\ 21 & 13 & 1 & 1 & 18 & 20 & 5 \end{bmatrix}$$

A Matriz criptografada será dada por

$$AB \equiv C \ mod(26)$$

Observe que

$$A.B = \begin{bmatrix} 69 & 57 & 15 & 39 & 56 & 96 & 25 \\ 114 & 92 & 23 & 59 & 93 & 154 & 40 \end{bmatrix} = \begin{bmatrix} 17 & 5 & 15 & 13 & 4 & 18 & 25 \\ 10 & 14 & 23 & 7 & 15 & 24 & 14 \end{bmatrix} mod(26)$$

Convertendo a última matriz para letras teremos

$$\begin{bmatrix} 17 & 5 & 15 & 13 & 4 & 18 & 25 \\ 10 & 14 & 23 & 7 & 15 & 24 & 14 \end{bmatrix} = \begin{bmatrix} Q & E & O & M & D & R & Y \\ J & N & W & G & O & X & N \end{bmatrix}$$

Portanto a mensagem criptografada é

QEOMDRYJNWGOXN

Para voltar a frase original precisamos fazer $A^{-1}.C$.

Podemos encontrar a inversa de $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ usando a fórmula $A^{-1} = \frac{1}{detA} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

Dessa forma, como $A = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$, teremos $A^{-1} = \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix}$, pois $det(A) = 1$.

Fazendo

$$A^{-1}.C = \begin{bmatrix} 55 & -17 & 6 & 44 & -25 & 18 & 83 \\ -31 & 13 & 1 & -25 & 18 & -6 & -47 \end{bmatrix} = \begin{bmatrix} 3 & 9 & 6 & 18 & 1 & 18 & 5 \\ 21 & 13 & 1 & 1 & 18 & 20 & 5 \end{bmatrix} mod(26)$$

E retornamos a mensagem original "CIFRAR É UMA ARTE".

## 1.5 Exercício

**1) (Puc-GO 2020)** A utilização de matrizes pode ser útil na Criptografia, ciência que estuda maneiras eficientes para troca de mensagens de modo mais seguro. Uma das formas de se criptografar uma mensagem de texto é estabelecer uma relação biunívoca entre as letras do alfabeto e os números naturais. Por exemplo, a = 1, b = 2 e, assim, sucessivamente. Em seguida, a mensagem é colocada numa matriz quadrada $X$ e multiplicada por uma matriz invertível $C$, chamada matriz Chave, resultando em $X \cdot C = Y$, em que a matriz $Y$ é a mensagem criptografada. Ao receber a mensagem criptografada $Y$, multiplica-se pela inversa de $C$: $(X \cdot C) \cdot C^{-1} = X \cdot (C \cdot C^{-1}) = X$, obtendo-se a mensagem original.

Supondo que tenha sido enviada a seguinte mensagem criptografada com base na relação biunívoca entre as letras do alfabeto e os números naturais, tal como no exemplo mencionado e que essa mensagem criptografada tenha sido enviada na forma da matriz

$$Y = \begin{pmatrix} 12 & 8 \\ 6 & 5 \end{pmatrix}$$

e sabendo que a matriz de Chave é a matriz

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

assinale a alternativa correta que apresenta a mensagem transmitida, armazenada em forma de matriz, linha a linha:

a) Fato.

b) Dado.

c) Casa.

d) Faca.

**2**) **(Anton-Algebra Linear)** Em cada parte, obtenha a cifra de Hill da mensagem

DARK NIGHTT

com matriz codificadora dada.

(a)
$$\begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix}$$

**3**) **(Anton-Algebra Linear)**

Decodifique a mensagem

SAKNOXAOJX

sabendo que ela foi cifrada utilizando a **cifra de Hill** com matriz codificadora

$$K = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}.$$

Considere a seguinte correspondência entre letras e números:

$$A = 1,\ B = 2,\ \ldots,\ Y = 25,\ Z = 0.$$

Trabalhe no conjunto dos inteiros módulo 26.

**4**) **(Uff 2005)** Um dispositivo eletrônico, usado em segurança, modifica a senha escolhida por um usuário, de acordo com o procedimento descrito a seguir.

A senha escolhida $S_1S_2S_3S_4$ deve conter quatro dígitos, representados por $S_1$, $S_2$, $S_3$ e $S_4$. Esses dígitos são, então, transformados nos dígitos $M_1$, $M_2$, $M_3$ e $M_4$, da seguinte forma:

$$\begin{pmatrix} M_1 \\ M_2 \end{pmatrix} = P \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} \qquad \text{e} \qquad \begin{pmatrix} M_3 \\ M_4 \end{pmatrix} = P \begin{pmatrix} S_3 \\ S_4 \end{pmatrix}$$

em que $P$ é a matriz

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

Se a senha de um usuário, já modificada, é 0110, isto é, $M_1 = 0$, $M_2 = 1$, $M_3 = 1$ e $M_4 = 0$, pode-se afirmar que a senha escolhida pelo usuário foi:

a) 0011

b) 0101

c) 1001

d) 1010

e) 1100

**5) (Fuvest 2019)** A multiplicação de matrizes permite codificar mensagens. Para tanto, cria-se uma numeração das letras do alfabeto, como na tabela abaixo. (O símbolo * corresponde a um espaço).

| *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 | 26 | 27 |

Como exemplo, suponha que a mensagem a ser transferida seja **FUVEST**, e que as matrizes codificadora e decodificadora sejam

$$A = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \qquad \text{e} \qquad B = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix}.$$

respectivamente. A matriz em que se escreve a mensagem é

$$M = \begin{pmatrix} F & U & V \\ E & S & T \end{pmatrix},$$

que, numericamente, corresponde a

$$M = \begin{pmatrix} 6 & 21 & 22 \\ 5 & 19 & 20 \end{pmatrix}.$$

Para fazer a codificação da mensagem, é feito o produto de matrizes

$$N = A \cdot M = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 6 & 21 & 22 \\ 5 & 19 & 20 \end{pmatrix} = \begin{pmatrix} 28 & 101 & 106 \\ 11 & 40 & 42 \end{pmatrix}.$$

O destinatário, para decifrar a mensagem, deve fazer o produto da matriz decodificadora com a matriz codificada recebida:

$$M = B \cdot N = \begin{pmatrix} 6 & 21 & 22 \\ 5 & 19 & 20 \end{pmatrix}.$$

a) Se a matriz codificadora é

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

e a mensagem a ser transmitida é **ESCOLA**, qual é a mensagem codificada que o destinatário recebe?

b) Se a matriz codificadora é

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

e o destinatário recebe a matriz codificada

$$N = \begin{pmatrix} 33 & 9 & 8 & 48 \\ 47 & 13 & 9 & 75 \end{pmatrix},$$

qual foi a mensagem enviada?

c) Nem toda matriz $A$ é eficaz para enviar mensagens. Por exemplo, se

$$A = \begin{pmatrix} 2 & -7 \\ 4 & -14 \end{pmatrix},$$

encontre 4 sequências de 4 letras de forma que as respectivas matrizes codificadas sejam sempre iguais a

$$B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Dica: considere $M = \begin{pmatrix} \alpha & \beta \\ \lambda & \gamma \end{pmatrix}$ e faça $A.M = B$ para encontrar a sequência de letras.

# 2 Referências


1. H. Anton e C. Rorres. Álgebra Linear com Aplicações. 10a. ed. Porto Alegre: Bookman, 2012. isbn: 978-85-407-0170-0.