UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIA E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
CURSO DE LICENCIATURA EM MATEMÁTICA

NIEDJA NATIELLE RODRIGUES DA SILVA

MATRIZES E APLICAÇÕES

Campina Grande – PB.
2015

NIEDJA NATIELLE RODRIGUES DA SILVA

MATRIZES E APLICAÇÕES.

Trabalho de Conclusão de Curso (TCC) apresentado à banca examinadora do curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba – UEPB, como exigência para obtenção do título de graduada.

Orientadora: Profª.Drª. Maria Isabelle Silva

Campina Grande – PB.
2015

S586m Silva, Niedja Natielle Rodrigues da.
Matrizes e aplicações [manuscrito] / Niedja Natielle Rodrigues da Silva. - 2015.
54 p. : il. color.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2015.
"Orientação: Profa. Dra. Maria Isabelle Silva, Departamento de Matemática".

1. Matemática. 2. Matrizes. 3. Grafos. 4. Criptografia. I. Título.

21. ed. CDD 512.943 4

NIEDJA NATIELLE RODRIGUES DA SILVA

MATRIZES E APLICAÇÕES

Trabalho de Conclusão de Curso (TCC) apresentado à banca examinadora do curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba – UEPB, como exigência para obtenção do título de graduada.

APROVADO EM 19 / 06 / 2015

BANCA EXAMINADORA

Maria Isabelle Silva

Profª. Drª. Maria Isabelle Silva
(Orientadora – / UEPB)

Walber Santiago Colaço

Prof. Me. Walber Santiago Colaço
(Examinador – / UEPB)

Kátia Suzana Medeiros Graciano

Prof. Ma. Kátia Suzana Medeiros Graciano
(Examinadora – / UEPB)

AGRADECIMENTOS

A Deus, primeiramente, por me conceder a graça da vida;por me dar saúde, sabedoria e capacidade de concluir meu curso;

À minha querida mãe, Joseneide, que sempre acreditou em mim, e me deu apoio em todas as minhas decisões. Obrigada por tanto carinho, dedicação e paciência! Palavras, nunca serão suficientes para mostrar o tamanho da minha gratidão;

Ao meu filho, Alisson Júniorque é uma benção na minha vida, e veio ao mundo para me incentivar cada vez mais a vencer.

Ao meu esposo, companheiro e amigo Alisson, que sempre esteve ao meu lado. Nunca me deixou desistir, principalmente em momentos difíceis.Dando-me apoio, amor e carinho;

À minha família, por estar presente em minha vida. De uma forma ou de outra está sempre me ajudando;

A todos os meus amigos de curso, em especial, Ivson, Rosilda e Deleon que sempre me ajudaram quando precisei e sei que posso contar sempre com eles.

À Professora Dra. Isabelle, pela orientação, boa vontade e responsabilidade. Agradeço imensamente por ter dedicado seu tempo para realização desse trabalho.

A todos vocês, meu MUITO OBRIGADO!

“...Dando sempre graças por tudo a nosso Deus e Pai,

em nome de nosso Senhor Jesus Cristo...”

(Efésios 5:20)

RESUMO

A matemática é uma ciência muito antiga,desde os primórdios esteve presente em nosso dia a dia. Porém muitos têm dificuldade em fazer a associação entre a matemática e as situações do cotidiano. Neste trabalho, estudamos um pouco da história das matrizes, mostrando de que forma surgiram e quem foram seus idealizadores, tratamos dos tipos de matrizes e suas propriedades, assim como operações. Por fim, fazemos duas aplicações das matrizes, a saber, Teoria de grafos e Criptografia. A primeira muito utilizada em circuitos elétricos, mapas, relações humanas e a segunda de muita valia para o envio de mensagens secretas.

PALAVRAS CHAVE: Matrizes, Grafos, Criptografia.

ABSTRACT

Mathematics is an ancient science, from the beginning was present in our daily lives. But many find it difficult to make the association between mathematics and everyday situations. In this paper, we study a little history of matrices showing how emerged and who were its founders, treat the types of matrices and their properties, as well as operations. Finally, we make two applications of arrays, namely, theory of graphs and Encryption. The first widely used in electrical circuits, maps, human relations and the second much use for sending secret messages.

KEYWORDS: Arrays, Graphs, Cryptography.

SUMÁRIO

INTRODUÇÃO

O presente trabalho trata das matrizes e algumas aplicações. Ao estudarmos sua história, suas definições e aplicações faz-se necessário considerar que tais categorias não são atemporais. Devem ser entendidas como produzidas historicamente, resultantes do tempo e do espaço vivenciado pelos matemáticos que direcionaram suas pesquisas para este aspecto da matemática. A este respeito, dois nomes se relacionam quanto à história da matriz: James Joseph Sylvester e Arthur Cayley. Estes intelectuais escreveram suas memórias acerca da matriz, no decorrer no século XIX. Ambos atuantes em academias inglesas, país que, aliás, evidenciava-se como importante potência em estudos matemáticos (BOYER, 1996). Sylvester (1814-1897) nasceu em Londres, em 1883 ocupou importante disciplina como Professor de Geometria em Oxford. Como parte dessa experiência, publicou, entre 1850 e 1851, uma série de *memórias*, cuja principal contribuição foi o recurso ao cálculo de determinantes.

Segundo Bernardes:

> Em uma memória publicada em 1859, de título *Philosophical Magazine,* o matemático inseriu o termo matriz para generalizar um resultado sobre o número de determinantes pertencentes a um sistema de menores considerando matrizes retangulares (BERNARDES, p. 4).

Sylvester deu o significado original da palavra MATRIZ, ou seja, local onde se gera ou se cria, ela surge para classificar o tipo de contato entre duas cônicas, podendo ser definida como: uma tabela retangular, geradora de vários sistemas de determinantes menores.

Cayley (1821-1895) também inglês e atuante no meio acadêmico deste país, foi contemporâneo de Sylvester, inclusive com o mesmo manteve relações estreitas de amizade, o que lhe permitiu ter conhecimento do que o amigo discorria a respeito dos conhecimentos matemáticos de matriz. A partir de 1855 Cayley demonstrou interesse pela noção de matriz, no artigo Remarques sur La notationdesfunctionsalgébriques, definindo-as como prática para representar sistemas lineares e formas quadráticas. Em A MemoirontheTheoryofMatrices no PhilosophicalTransactions, definiu matriz como “um conjunto de quantidades

organizadas em forma de quadrado” e, inicialmente, associa a noção de matriz a uma notação abreviada de um conjunto de equações lineares. (BERNARDES, p.8).

De acordo com Bernardes, assim podem ser percebidas as diferenças no modo de pensar, definir e aplicar a matriz para cada um dos matemáticos:

A noção de matriz emerge durante a pesquisa de Sylvester sobre a classificação dos tipos de contatos entre duas cônicas quando ele investiga os determinantes menores associados a um determinante completo e suas propriedades. Porém, as matrizes não são o objeto de investigação, elas desempenharam o papel de uma representação para a fonte geradora de sistemas de determinantes menores. Elas não foram um objeto epistêmico e nem uma técnica epistêmica neste episódio da pesquisa de Sylvester. No episódio da pesquisa de Cayley, as matrizes constituem o principal objeto epistêmico. A*memória* de 1858 foi intencionalmente dedicada a estudar este objeto. As matrizes são associadas as leis de um cálculo simbólico, a um teorema notável e à prática de fatoração de polinômios de matrizes. Elas ofereceram uma nova linguagem, na quais problemas já conhecidos puderam ser tratados de outra forma e novos problemas puderam ser colocados (BERNARDES, p.13).

Objetivo deste trabalho é tratar de algumas aplicações das matrizes que estão presentes em diversas situações do nosso cotidiano. O interesse em fazer esse estudo surgiu da minha curiosidade a respeito das utilidades das matrizes em nossas vidas. O trabalho está organizado em dois capítulos. No capítulo 1 (primeiro), serão apresentadas as definições, tipos e exemplos das matrizes, e no capítulo 2 (segundo) iremos explorar duas aplicações, quais sejam Teoria de grafos e criptografia. A metodologia utilizada foi a pesquisa bibliográfica.

CAPÍTULO 1

1.1 MATRIZES E SUAS E PROPRIEDADES

Este primeiro capítulo tem como objetivo dar uma ideia geral sobre matriz do tipo mxn, podendo ser representada por $A_{mxn}(\mathbb{R})$, bem como especificar seus tipos e propriedades. As matrizes são frequentemente utilizadas para organizar dados. Ocorrem principalmente como quadros dos coeficientes de sistemas de equações lineares, mas também surgem com os vetores. Neste trabalho adotaremos a notação simplificada A_{mxn}, já que trabalharemos apenas com matrizes com entradas reais.

Definição 1*:* Sejam m e n números inteiros positivos. Uma matriz do tipo mxn é uma tabela de $m.n$elementos (números, polinômios, funções, expressões algébricas etc.) dispostos em m linhas (filas horizontais) e n colunas (filas verticais). Uma matriz é representada com seus elementos entre parênteses, colchetes ou duas barras verticais.

Exemplo 1:

i) $A = \begin{pmatrix} 3 & -1 \\ 0 & 4 \end{pmatrix}$

ii) $B = \begin{bmatrix} 4 & 2 \\ -2 & 5 \end{bmatrix}$

iii) $C = \begin{Vmatrix} 1 & 7 \\ 4 & 3 \end{Vmatrix}$

1.1.1 Representação de uma matriz

A matriz A pode ser representada por $A_{mxn}(\mathbb{R})$, podendo ser escrita abreviadamente por $A = [a_{ij}]$, onde $i\epsilon\{1, \dots, m\}$ é o índice linha e $j\epsilon\{1, \dots, n\}$ é o índice coluna da matriz. O elemento a_{ij} chama-se o ij-ésimo elemento da matriz. A matriz é representada por um quadro numérico contendo m linhas e n colunas, segue o exemplo:

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

1.2 TIPOS DE MATRIZES

Abaixo descreveremos alguns tipos de matrizes:

1.2.1 Matriz Linha

Chama-se matriz linha ou vetor-linha toda matriz de ordem 1 por n.

Exemplo 2:

$$A = [a_{11} \quad a_{12} \quad a_{13} \quad \dots \quad a_n]$$

1.2.2 Matriz Coluna

Chama-se matriz coluna ou vetor-coluna toda matriz de ordem m por 1.

Exemplo 3:

$$A = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_m \end{bmatrix}$$

1.2.3 Matriz Retangular

Dizemos que uma matriz é retangular quando o número de linhas é diferente do número de colunas, ou seja,$m \neq n$.

Exemplo 4:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{33} \end{bmatrix}$$

1.2.4 Matriz quadrada

Seja A uma matriz $m \times n$, dizemos que A é quadrada quando o número de linhas é igual ao número de colunas, ou seja, $m = n$. A ordem da matriz quadrada é$n \times n$, ou simplesmente n.

Exemplo 5:

i) $A_2 = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$

ii) $A_3 = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$

Observação:

1. Numa matriz quadrada $A = (a_{ij})$, os elementos a_{ij}, em que $i = j$, constituem a diagonal principal. Logo, a diagonal principal é formada pelos elementos: $a_{11}, a_{22}, a_{33}, \dots, a_{nn}$.

2. Numa matriz quadrada $A = (a_{ij})$, os elementos a_{ij}, em que $i + j = n + 1$, constituem a diagonal secundária. Logo, a diagonal secundária é formada pelos elementos:$a_{1\,n}, a_{2\,n-1,} \dots, a_{n1}$

1.2.5 Triangular superior

Chama-se matriz triangular superior a matriz quadrada $A = \left(a_{ij}\right) \in M_n(\mathbb{R})$tal que$a_{ij} = 0$, se $i > j$ (isto é, possui todos os elementos, abaixo da diagonal principal, nulos).

Exemplo 6:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{bmatrix}$$

1.2.6 Triangular inferior

Chama-se matriz triangular superior a matriz quadrada $A = (a_{ij}) \in M_n(\mathbb{R})$ tal que$a_{ij} = 0\ sei < j$(isto é, todos os elementos, acima da diagonal principal, nulos).

Exemplo 7:

A= $\begin{bmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$

1.2.7 Diagonal

É a matriz quadrada em que todos os elementos fora da diagonal principal são nulos, ou seja, $a_{ij} = 0\ sei\ \neq j$.

Exemplo 8:

A = $\begin{bmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{bmatrix}$

1.2.8 Identidade

Denomina-se matriz identidade toda matriz de ordem n, em que todos os elementos da diagonal principal são iguais a 1 e os demais iguais a 0, isto é, $a_{ij} = 0$ para $i \neq j$ e $a_{ij} = 1$ para $i = j$. Indica-se a matriz identidade por I_n, ou simplesmente I.

Exemplo 9:

i)$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

ii) $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

1.2.9 Matriz nula

Uma matriz nula é a matriz cujos elementos a_{ij} são todos iguais a zero.

Exemplo 10:

$0 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

1.3 OPERAÇÕES COM MATRIZES:

Apresentaremos abaixo algumas operações entre matrizes como adição, igualdade, multiplicação de uma matriz por um número real e multiplicação entre matrizes.

1.3.1 Adição

Dadas duas matrizes $A = (a_{ij})$, $B = (b_{ij}) \epsilon M_{mxn}(\mathbb{R})$, a matriz soma de Ae B é a matriz $C = (c_{ij}) \epsilon M_{mxn}(\mathbb{R})$ tal que:

$$c_{ij} = a_{ij} + b_{ij}, \forall\, i \,\epsilon\, \{1, \dots, m\}, \quad \forall\, j \,\epsilon\, \{1, \dots, n\}$$

Observação: A diferença $A - B$ de duas matrizes de ordem $m \times n$ é uma matriz C tal que: $C_{ij} = a_{ij} - b_{ij}$

Exemplo 11:

i) $\begin{bmatrix} 0 & 2 & 1 \\ 1 & -4 & 3 \end{bmatrix} + \begin{bmatrix} 2 & 3 & 0 \\ 1 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 5 & 1 \\ 2 & -6 & 4 \end{bmatrix}$

ii) $\begin{bmatrix} 0 & 2 & 1 \\ 6 & 4 & -3 \\ 2 & 8 & 9 \end{bmatrix} - \begin{bmatrix} 1 & 0 & 2 \\ 1 & 3 & 8 \\ 2 & 7 & 4 \end{bmatrix} = \begin{bmatrix} -1 & 2 & -1 \\ 5 & 1 & -11 \\ 0 & 1 & 5 \end{bmatrix}$

Propriedades:

Sejam $A = (a_{ij}), B = \left(b_{ij}\right) e C = \left(c_{ij}\right)$ matrizes quaisquer em $M_{mxn}(\mathbb{R})$. Valem as seguintes propriedades.

i) Comutativa: $A + B = B + A$

ii) Associativa: $(A + B) + C = A + (B + C)$

iii) Existência do elemento neutro: Para toda matriz $A \in M_{mxn}(\mathbb{R})$ existe$O \in M_{m\times n}$ tal que $A + 0 = 0 + A = A$.

iv) Existência do elemento oposto: Existe $(-A) \in M_{m\times n}(\mathbb{R})$, tal que $A + (-A) = O$.

1.3.2 Igualdade de matrizes

Dadas as matrizes A e B, dizemos que essas matrizes são iguais se, e somente se, elas possuem a mesma ordem e os mesmos elementos que ocupam a mesma posição. De maneira simbólica, temos:

$$A_{mxn} = B_{mxn} \Leftrightarrow a_{ij} = b_{ij}, 1 \leq i \leq m \; e \; 1 \leq j \leq n$$

Se existir pelo menos um elemento a_{ij}, tal que $a_{ij} \neq b_{ij}$. Com $1 \leq i \leq me \; 1 \leq j \leq n$, então $A \neq B$.

1.3.3 Multiplicação de uma matriz por um número real

Seja α um número real, o produto de uma matriz $A = [a_{ij}] \epsilon M_{mxn}(\mathbb{R})$ por α é uma matriz $B = [b_{ij}] \epsilon M_{mxn}(\mathbb{R})$ tal que $b_{ij} = \alpha a_{ij}$, ou seja, basta multiplicar cada elemento da matriz por α.

Exemplo 12:

Seja $A = \begin{bmatrix} -3 & 6 \\ 2 & 5 \end{bmatrix}$ e $\alpha = 2$, temos:

$$\alpha . \begin{bmatrix} -3 & 6 \\ 2 & 5 \end{bmatrix} = 2 . \begin{bmatrix} -3 & 6 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} -6 & 12 \\ 4 & 10 \end{bmatrix}$$

Propriedades:

Sejam $A = (a_{ij}),\ B = (b_{ij}) \epsilon M_{mxn}(\mathbb{R}), \alpha, \beta, \gamma \epsilon\ \mathbb{R}$. Valem as seguintes propriedades:

i) $(\alpha\beta)A = \ \alpha(\beta A)$

ii) $(\alpha + \beta)A = \alpha A + \beta A$

iii) $\alpha(A + B) = \ \alpha A + \alpha B$

iv) $1 . A = A$

1.3.4 Multiplicação entre matrizes

Em álgebra linear, as matrizes surgem principalmente associadas a transformações lineares e o produto de duas matrizes é definido como a matriz associada à composta de duas transformações lineares.

Sejam $A = (a_{ij}) \epsilon M_{mxp}(\mathbb{R})$ e $B = (b_{ij}) \in\ M_{pxn}(\mathbb{R})$. A matriz produto de A por B é matriz $AB = (c_{ij}) \in\ M_{mxn}\ (\mathbb{R})$ tal que:

$$c_{ij} = \sum_{k=1}^{p} a_{ik} \,.\, b_{kj}, i = 1, \dots, m; j = 1, \dots, n$$

Exemplo 13:

Sejam $A = \begin{bmatrix} 2 & 3 \\ -1 & 5 \end{bmatrix}$ e $B = \begin{bmatrix} 0 & 1 \\ -1 & 2 \end{bmatrix}$

Então, $A.B = \begin{bmatrix} 2.0 + 3.(-1) & 2.1 + 3.2 \\ -1.0 + 5.(-1) & -1.1 + 5.2 \end{bmatrix} = \begin{bmatrix} -3 & 8 \\ -5 & 9 \end{bmatrix}$

Propriedades:

i) Associativa: $(AB)C = A(BC). \forall\, A \in M_{nxp}(\mathbb{R}), B \in M_{nxp}(\mathbb{R}), C \in M_{pxq}(\mathbb{R})$.

ii) Distributiva em relação a adição: $A(B + C) = AB + AC, \forall\, A \in M_{nxp}(\mathbb{R}), B, C \in M_{nxp}(\mathbb{R})$.

iii) $\lambda(AB) = (\lambda A)B = A(\lambda B), \forall\, \lambda \in \mathbb{R}, \forall\, A \in M_{mxn}(\mathbb{R}), B \in M_{nxp}(\mathbb{R})$

iv) Dada $A \in M_{mxn}(\mathbb{R}), I_n A = A I_n = A$.

É importante observar que:

1. A multiplicação de matrizes não é comutativa, isto é, em geral, $A.B \neq B.A$.

Exemplo 14:

Sejam $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 4 \\ 1 & 4 & 5 \end{bmatrix}$

Temos então que o produto $A.B$ é,

$$\begin{bmatrix}1 & 2 & 3\\4 & 5 & 6\\7 & 8 & 9\end{bmatrix}.\begin{bmatrix}1 & 2 & 3\\1 & 3 & 4\\1 & 4 & 5\end{bmatrix}=\begin{bmatrix}6 & 20 & 26\\15 & 47 & 62\\24 & 74 & 98\end{bmatrix}$$

Agora fazendo $B.A$, temos:

$$\begin{bmatrix}1 & 2 & 3\\1 & 3 & 4\\1 & 4 & 5\end{bmatrix}.\begin{bmatrix}1 & 2 & 3\\4 & 5 & 6\\7 & 8 & 9\end{bmatrix}=\begin{bmatrix}30 & 36 & 42\\41 & 49 & 57\\52 & 62 & 73\end{bmatrix}$$

Logo, $A.B \neq B.A$.

2. Se o produto entre duas matrizes A e B for nulo, não é necessário, que A ou B sejam matrizes nulas.

Exemplo 15:

Sejam $A=\begin{bmatrix}2 & 0\\1 & 0\end{bmatrix}.\begin{bmatrix}0 & 0\\4 & 6\end{bmatrix}=\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$

Ou seja, Para $A \neq 0 e B \neq 0$, obtemos $A.B = 0$.

1.3.6 Potência de uma matriz

Dada uma matriz quadrada $A = [a_{ij}]$e um número $n \in \mathbb{Z}_+^*$. A matriz A pode ser multiplicada $n$vezes por si mesma, resultando em uma matriz representada por A^n, chamada potência de n da matriz A.

Exemplo 16:

Se $A=\begin{bmatrix}2 & 0\\1 & 3\end{bmatrix}$

i) $A^2=\begin{bmatrix}2 & 0\\1 & 3\end{bmatrix}.\begin{bmatrix}2 & 0\\1 & 3\end{bmatrix}=\begin{bmatrix}4 & 0\\5 & 9\end{bmatrix}$

ii)$A^3=\begin{bmatrix}2 & 0\\1 & 3\end{bmatrix}.\begin{bmatrix}2 & 0\\1 & 3\end{bmatrix}.\begin{bmatrix}2 & 0\\1 & 3\end{bmatrix}=\begin{bmatrix}8 & 0\\19 & 27\end{bmatrix}$

1.4 OUTROS TIPOS DE MATRIZES

1.4.1 Matriz Transposta

A transposta da matriz $A \epsilon M_{m\times n}(\mathbb{R})$, é a matriz denotada por $A^T \epsilon M_{n\times m}(\mathbb{R})$, que se obtém da matriz A permutando as linhas pelas colunas de mesmo índice. Quando A é uma matriz quadrada, os elementos da diagonal principal da sua transposta não se alteram.

Exemplo 17:

$$A = \begin{bmatrix} 1 & 3 & -4 \\ 5 & 7 & 2 \end{bmatrix} A^T = \begin{bmatrix} 1 & 5 \\ 3 & 7 \\ -4 & 2 \end{bmatrix}$$

Propriedades:

i) $(A + B)^T = A^T + B^T$

ii) $(\alpha A)^T = \alpha A^T$

iii) $(A^T)^T = A$

iv) $(AB)^T = B^T A^T$

1.4.2 Matriz Simétrica e Matriz Anti-simétrica

Uma matriz quadrada A é:

i) Simétrica, se $A^T = A$

Exemplo 18: Seja a matriz A,

$$A = \begin{bmatrix} 1 & 2 & 8 \\ 2 & 5 & 6 \\ 8 & 6 & 4 \end{bmatrix}$$

Sua transposta é,

$$A^T = \begin{bmatrix} 1 & 2 & 8 \\ 2 & 5 & 6 \\ 8 & 6 & 4 \end{bmatrix}$$

Isto é, $A = A^T$

Observação: O produto de uma matriz quadrada A pela sua transposta A^T é uma matriz simétrica.

Exemplo 19: Seja A uma matriz quadrada de ordem n, temos:

$$A = \begin{bmatrix} 0 & 1 \\ 3 & 2 \end{bmatrix} e A^T = \begin{bmatrix} 0 & 3 \\ 1 & 2 \end{bmatrix}$$

Logo,

$$S = A.A^T = \begin{bmatrix} 0 & 1 \\ 3 & 2 \end{bmatrix} . \begin{bmatrix} 0 & 3 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 2 & 13 \end{bmatrix}$$

E, $S = S^T$

ii) Anti-simétrica, se $A^T = -A$

Exemplo 20:

Seja a matriz $A = \begin{bmatrix} 0 & 6 & -3 \\ -6 & 0 & 2 \\ 3 & -2 & 0 \end{bmatrix}$

Fazendo a transposta obtemos:

$$A^T = \begin{bmatrix} 0 & -6 & 3 \\ 6 & 0 & -2 \\ -3 & 2 & 0 \end{bmatrix}$$

Isto é, $A = -A^T$

Teorema1: Se A é uma matriz de ordem n, então A pode ser escrita como a soma de uma matriz simétrica com uma anti-simétrica, da seguinte forma:

$$A = \frac{1}{2}(A + A^T) + \frac{1}{2}(A - A^T)$$

Prova:

Observe que $\frac{1}{2}(A + A^T)$ é simétrica, pois:

$$(\frac{1}{2}(A + A^T))^T = \frac{1}{2}(A^T + (A^T)^T) = \frac{1}{2}(A^T + A) = \frac{1}{2}(A^T + A) = \frac{1}{2}(A + A^T)$$

e,$\frac{1}{2}(A - A^T)$ é anti-simétrica, pois:

$$(\frac{1}{2}(A - A^T))^T = \frac{1}{2}(A^T - (A^T)^T) = \frac{1}{2}(A^T - A) = \frac{1}{2}(A^T - A) = \frac{1}{2}(A - A^T)$$

1.4.3 Matriz Inversa

Seja A uma matriz quadrada de ordem n. A matriz A é dita inversível ou não-singular se existe uma matriz B quadrada de mesma ordem, tal que: $A.B = B.A = I_n$. Nesse caso, B é a inversa de A e é indicada por A^{-1}.

Exemplo21:

Seja $A = \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix} e B = \begin{bmatrix} 3 & -4 \\ -2 & 3 \end{bmatrix}$.

Verifiquemos se $A.B = B.A = I_n$

$$\begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & -4 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 3 & -4 \\ -2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Logo A e B são inversíveis e B é a inversa de A.

Transformações Elementares

Seja A uma matriz de ordem$m \times n$. Para cada $1 \leq i \leq m$, denotamos por L_i a $i - ésima$ linha de A. Definimos as transformações elementares nas linhas da matriz A como segue:

1) Permutação das linhas L_i e L_j, indicada por $L_i \leftrightarrow L_j$.
2) Substituição de uma linha L_i pela adição desta mesma linha com c vezes uma outra linha L_j, indicada por $L_i \rightarrow L_i + cL_j$.
3) Multiplicação de uma linha L_i por um elemento não nulo, indicada por $L_i \rightarrow cL_i$.

Observação: Dizemos que uma matriz $B \in M_{mxn}(\mathbb{R})$ é equivalente a matriz $A \in M_{mxn}(\mathbb{R})$, se pudermos obter B aplicando-se uma sequência de operações elementares a uma matriz A, indicamos por $B \sim A$, e dizemos que A e B são equivalentes.

Exemplo22:

Dadas as matrizes $A = \begin{bmatrix} 1 & 3 & 7 \\ 4 & 2 & 5 \\ 0 & 1 & 3 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 3 & 7 \\ 4 & 3 & 8 \\ 0 & 1 & 3 \end{bmatrix}$.Vamos aplicar algumas Operações elementares às linhas da matriz A para obtermos a matriz$B$.

$$\begin{bmatrix} 1 & 3 & 7 \\ 4 & 2 & 5 \\ 0 & 1 & 3 \end{bmatrix} L_1 \leftrightarrow L_2 \Rightarrow \begin{bmatrix} 4 & 2 & 5 \\ 1 & 3 & 7 \\ 0 & 1 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 3 & 7 \\ 4 & 2 & 5 \\ 0 & 1 & 3 \end{bmatrix} L_1 \leftarrow 2L_1 \Rightarrow \begin{bmatrix} 2 & 6 & 14 \\ 4 & 2 & 5 \\ 0 & 1 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 3 & 7 \\ 4 & 2 & 5 \\ 0 & 1 & 3 \end{bmatrix} L_2 \leftarrow L_2 + L_3 \Rightarrow \begin{bmatrix} 1 & 3 & 7 \\ 4 & 3 & 8 \\ 0 & 1 & 3 \end{bmatrix}$$

Assim em $M_{mxn}(\mathbb{R})$, temos:

1. Reflexiva: $A \sim A$
2. Simétrica: Se $A \sim B$ então $B \sim A$

3. Transitiva: Se $A \sim B$ e $B \sim C$ então $A \sim C$

Teorema2: Se uma matriz é inversível, sua inversa é única.

Demonstração: Suponha que as matrizes B e C são inversas de A, isto é:

$$AB = BA = I \text{ (1)}$$

e

$$AC = CA = I \text{ (2)}$$

De (1) obtemos,

$$AB = I \ (*)$$

Multiplicando C em ambos os lados de $(*)$ à direita, teremos:

$$C(AB) = CI$$
$$(CA)B = CI$$
$$IB = CI$$
$$B = C$$

Logo, se existe inversa de A, fica provado que esta é única.

Teorema 3: Seja $A \in M_n(\mathbb{R})$. Então A é inversível se, e somente se, $A \sim I_n$. Se A é inversível, a mesma sucessão de operações elementares que transformam A em I_n, transformamI_n na inversa de A.

Propriedades:

1. Se $A \in M_n(\mathbb{R})$ é inversível, então $(A^{-1})^{-1} = A$

2. Se $A, B \in M_n(\mathbb{R})$ são inversíveis, então AB é inversível e $(AB)^{-1} = B^{-1}A^{-1}$.

3. Se $A \in M_n(\mathbb{R})$ é inversível, então $(A^T)^{-1} = (A^{-1})^T$

1.4.4 Matrizes Ortogonais

Dizemos que uma matriz $A \in M_n(\mathbb{R})$, inversível, é ortogonal, quando $A^{-1} = A^T$. Ou seja, $A^{-1}.A^T = I_n$.

Proposição:

i)O produto de duas matrizes ortogonais é uma matriz ortogonal.

Suponhamos que A e B sejam matrizes ortogonais, então $A^T = A^{-1}$ e $B^T = B^{-1}$, agora sabemos que se A e B são inversíveis então AB também o é $(AB)^{-1} = B^{-1}A^{-1} = B^TA^T = (AB)^T$.

ii) O determinante de uma matriz ortogonal é +1 ou -1
De fato, se $A^T = A^{-1} \Rightarrow Det(A^T) = Det(A^{-1}) \Rightarrow Det(A) = [Det(A)]^{-1} \Rightarrow [Det(A)]^2 = 1 \Rightarrow Det(A) = 1\ ou Det(A) = -1$.

Exemplo23: A matriz $A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ é ortogonal.

De fato,
Se $A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$, temos $A^T = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$

Façamos$A^T.A$,

$$\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}.\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} =$$

$$= \begin{bmatrix} \cos^2\theta + \sin^2\theta & -\sin\theta\cos\theta + \sin\theta\cos\theta \\ -\cos\theta\sin\theta + \cos\theta\sin\theta & \sin^2\theta + \cos^2\theta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Logo $A^T.A = I_n$, da mesma forma $A.A^T = I_n$. Isto é, $A^T = A^{-1}$. Fica provado assim que a matriz A é ortogonal.

CAPÍTULO 2

2. APLICAÇÕES DE MATRIZES

Neste capítulo, temos como objetivo mostrar algumas aplicações das matrizes no nosso cotidiano. As matrizes são utilizadas em diversas áreas tais como economia, engenharia, biologia entre outras. Uma dessas aplicações que iremos abordar é a teoria de grafos, que pode ser utilizada em diversas situações como as interações humanas, os problemas de comunicação,circuitos elétricos,sistemas de transporte,mapas de estradas etc. Outra aplicação também muito interessante é a criptografia, que é muito utilizada para o envio de mensagens secretas.

2.1 TEORIA DE GRAFOS

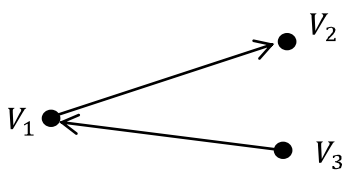
Um grafo (finito), também chamado digrafo, consiste em um conjunto finito de pontos chamados de vértices ou nós, juntamente com um número finito de arestas ou arcos, cada um dos quais envolvendo um par de vértices distintos. Formalmente temos:

Definição 2: Um grafo simples G é formado por um par (V(G), A(G)) onde V(G) é um conjunto não vazio e A(G) um conjunto de pares distintos não ordenados de elementos distintos de V(G).

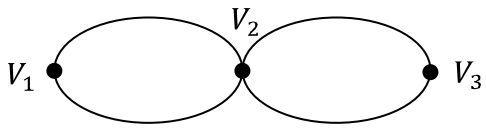
Os elementos de V(G) são chamados vértices $(V_1, V_2, \dots, V_n)$ e os de A(G) as arestas, que são uma coleção finita de pares ordenados (V_i, V_j), neste trabalho iremos denotá-los apenas por V e A. Usamos a notação $V_i \rightarrow V_j$ (que lemos "V_i tem acesso a V_j") para indicar que a aresta dirigida (V_i, V_j) pertence ao grafo dirigido.

Exemplo 24: As figuras a seguir representam exemplos de grafos:

i)



ii)



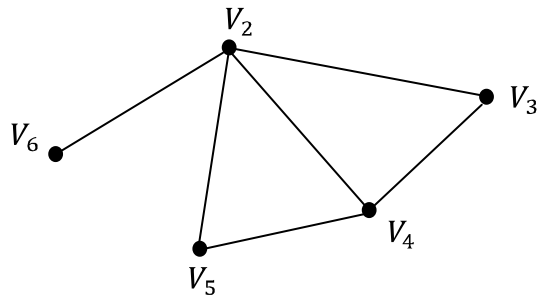
Os grafos podem ser orientados ou não. No exemplo 24i), temos um grafo orientado que possui três vértices $V_1, V_2 e V_3$ e duas arestas, que ligam os vértices V_3 a V_1 e V_1 a V_2. Assim, observamos que "V_3 tem acesso a V_1" e "V_1 tem acesso a V_2". Em ii) temos um exemplo de um grafo não orientado, ou seja, existem dois caminhos que ligam V_1 a V_2 e outros dois que ligam V_2 a V_3, mas não indica o sentido desse caminho (não há setas). Observe que existem quatro caminhos que ligam V_1 a V_3 e consequentemente também ligam V_3 a V_1.

Os grafos podem ser representados através de matrizes, as representações usuais são: Matriz de adjacência e Matriz de Incidência.

2.1.1 Matriz de Adjacência

Definição 3: A matriz adjacência de um digráfico G contendo n vértices é uma matriz $n \times n$, cujo ij-ésimo elemento é igual a 1 se houver aresta de V_i a V_j e zero caso contrário. Observe que A(G) não precisa ser uma matriz simétrica.

Exemplo 25: Observe o grafo a seguir



Sua matriz de adjacência é:

$$A(G) = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{array} \begin{array}{c} \begin{array}{ccccc} V_1 & V_2 & V_3 & V_4 & V_5 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

Por definição, as matrizes de adjacência têm as seguintes propriedades:

i) Todas as entradas são 0 ou 1

ii) Todas as entradas na diagonal principal são 0

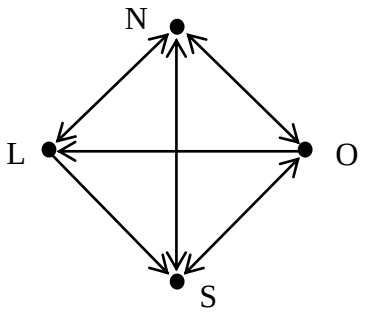
Observe que os elementos de número 1 indicam que há uma aresta que liga V_i a V_j. Ou seja, V_i tem acesso a V_j. Consequentemente, os de número 0 indicamquando não existe aresta ligando os vértices.

Teorema 4: Seja $A(G)$ a matriz de adjacência de um digrafo$G$ e seja B, a potência n-ésima de $A(G)$:

$$[A(G)]^k = B_k = \left[b_{ij}{}^{(k)}\right].$$

Então, o elemento ij-ésimo de $B_n, b_{ij}{}^{(k)}$ é o número de maneiras por meio das quais V_i tem acesso a V_j em k estágios.

Exemplo 26: A figura abaixo representa o mapa das rotas de uma empresa de ônibus. Essa empresa atende quatro bairros da cidade, são eles N, S, L e O.



Como o grafo é dirigido, a matriz de adjacência é:

$$A(G) = \begin{array}{c} \\ \text{L} \\ \text{N} \\ \text{O} \\ \text{S} \end{array} \begin{array}{c} \begin{array}{cccc} \text{LN} & \text{O} & \text{S} & \end{array} \\ \begin{vmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{vmatrix} \end{array}$$

E portanto,

$$[A(G)]^2 = \begin{array}{c} \\ \text{L} \\ \text{N} \\ \text{O} \\ \text{S} \end{array} \begin{array}{c} \begin{array}{cccc} \text{LN} & \text{O} & \text{S} & \end{array} \\ \begin{bmatrix} 1 & 1 & 2 & 1 \\ 1 & 3 & 1 & 2 \\ 1 & 2 & 2 & 2 \\ 2 & 1 & 1 & 2 \end{bmatrix} \end{array}$$

$$[A(G)]^3 = \begin{array}{c} \\ \text{L} \\ \text{N} \\ \text{O} \\ \text{S} \end{array} \begin{array}{c} \begin{array}{cccc} \text{LN} & \text{O} & \text{S} & \end{array} \\ \begin{vmatrix} 3 & 1 & 2 & 1 \\ 1 & 3 & 1 & 1 \\ 1 & 1 & 3 & 2 \\ 2 & 1 & 0 & 4 \end{vmatrix} \end{array}$$

Se uma pessoa tem interesse de se deslocar de um bairro para outro, ela pode ter vários caminhos para chegar no seu destino. Por exemplo, nosso interesse é fazer um deslocamento do bairro O para o bairro S. Teremos as seguintes opções:

i) De O a S por um estágio: O → S
ii) De O a S por dois estágios: O → L → S e O → N → S
iii) De O a S por três estágios: O → N → L → S e O → L → N → S

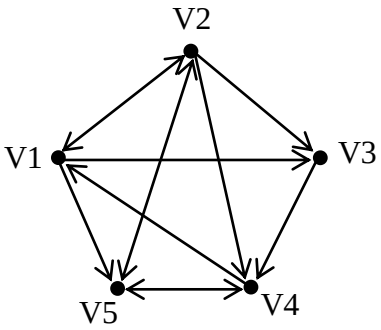
Logo, existem cinco maneiras diferentes para se deslocar do bairro O para o bairro S.

A partir deste exemplo podemos dizer que: A soma dos elementos da j-ésima coluna de $[A(G)]^n$ fornece o número de maneiras por meio das quais P_j é alcançado por todos os outros indivíduos em n estágios. Temos:

$$A(G) + [A(G)]^2 + \cdots + [A(G)]^n = C = [c_{ij}].$$

Logo, c_{ij} é o número de maneiras por meio das quais P_i tem acesso a P_j em um, dois ou n estágios.

Exemplo 27: Considere o digráfico G e sua matriz de Adjacência A(G) a seguir:



$$A(G) = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Daí pode-se encontrar $[A(G)]^2$.

$$[A(G)]^2 = \begin{bmatrix} 1 & 1 & 1 & 3 & 1 \\ 1 & 2 & 1 & 2 & 2 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 \end{bmatrix}$$

Logo,

$$A(G) + [A(G)]^2 = C = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 & 3 & 1 \\ 1 & 2 & 1 & 2 & 2 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 2 & 3 & 2 \\ 2 & 2 & 2 & 3 & 3 \\ 1 & 0 & 0 & 1 & 1 \\ 2 & 1 & 1 & 1 & 2 \\ 2 & 1 & 1 & 2 & 2 \end{bmatrix}$$

Um aspecto importante na estrutura de um grafo é a sua formação a partir de grafos menores, chamados de subgrafos. Os subgrafos são subconjuntos de indivíduos que se relacionam entre si. Chamamos de subgrafo maximal bidirecional completo, os subconjuntos cuja definição formal, é a seguinte:

Definição 4: Um subgrafo maximal bidirecional completo em um digrafo é um subconjunto S dos vértices que satisfazem as seguintes propriedades:

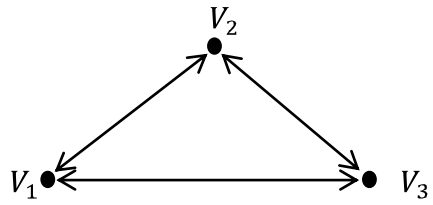
(a) Scontém três ou mais vértices.

(b) Se V_i e V_j estão em S, então há um aresta orientada de V_i a V_j e uma aresta orientada de V_j a V_i.

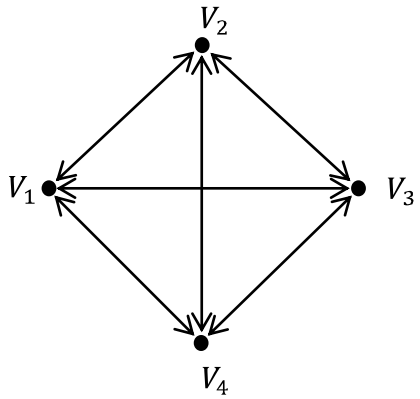
(c) O subconjunto é tão grande quanto possível, ou seja, não existe um subconjunto que seja maior que T dos vértices que satisfazem propriedade (b) e contem S [isto é, S é um subconjunto maximal que satisfaz (b)].

Exemplo 28: Considere os digrafos abaixo:

i)



ii)



Em i) temos o conjunto $\{V_1, V_2, V_3\}$que satisfazem as condições (a), (b) e (c), logo ele é um subgrafo maximal bidirecional completo.

Em ii) note que ao tomarmos o conjunto $\{V_1, V_2, V_3\}$, verificamos que ele não é um subgrafo maximal bidirecional completo, uma vez que ele satisfaz (a) e (b), mas não satisfaz (c), ou seja, $\{V_1, V_2, V_3\}$ está contido em $\{V_1, V_2, V_3, V_4\}$. Sendo assim o único subgrafo maximal completo em ii) é $\{V_1, V_2, V_3, V_4\}$

Nestes exemplos, foi fácil determinar os subgrafos maximais bidirecionais completos. Porém na medida em que tomamos subgrafos maiores o nível de dificuldade para determiná-los aumenta. A seguir mostraremos um método útil para encontrar subgrafo maximais bidirecionais completos que podem ser facilmente implementados em um computador.

Se $A(G) = [a_{ij}]$ é a matriz de adjacência dada de um digrafo, podemos formar uma nova matriz $S = [s_{ij}]$. Tal que: $S_{ij} = S_{ji} = 1$ se $a_{ij} = a_{ji} = 1$. Caso contrário, teremos: $S_{ij} = S_{ji} = 0$. Ou seja, $S_{ij} = 1$ se V_i e V_j tiverem acesso um ao outro, caso contrário $S_{ij} = 0$. Observe que S é uma matriz simétrica ($S = S^T$)

Exemplo 29: Considere um digrafo com matriz de adjacência:

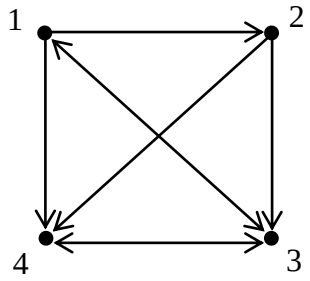
$$A(G) = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{array} \begin{array}{c} \begin{array}{ccccc} V_1 & V_2 & V_3 & V_4 & V_5 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

A partir de $A(G)$, podemos encontrar a Matriz S,

$$S = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{array} \begin{array}{c} \begin{array}{ccccc} V_1 & V_2 & V_3 & V_4 & V_5 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

Teorema5: Seja$A(G)$ a Matriz de adjacência de um grafo e $S = [s_{ij}]$ a matriz simétrica definida anteriormente, com $S^3 = [S_{ij}^{(3)}]$ é o i,j-ésimo elemento em S^3. Então, um vértice V_i pertence a um subgrafo maximal bidirecional completo se, e somente se, o elemento $s_{ii}^{(3)} \neq 0$.

Exemplo 30: Considere o grafo abaixo. Verifique se ele possui algum subgrafo maximal bidirecional completo.



$$A(G) = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},\ S = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Logo,

$$S^3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} . \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} . \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{bmatrix}$$

Como todo elemento da diagonal principal de S^3 é nulo, segue do teorema 5,que o grafo não possui nenhum subgrafo maximal bidirecional completo.

Observe o próximo exemplo:

Exemplo 31: Suponha um digrafo, com matriz de adjacência:

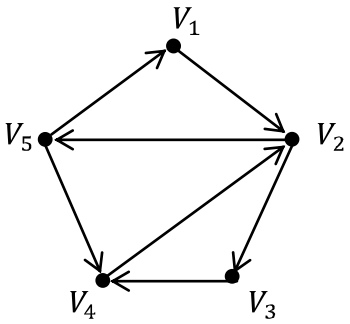
$$A(G) = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \text{ntão,} S = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

E, $S^3 = \begin{bmatrix} 2 & 4 & 0 & 4 & 3 \\ 4 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 0 & 2 & 1 \\ 3 & 1 & 0 & 1 & 0 \end{bmatrix}$

As entradas diagonais não nulas de S^3 são $s_{11}^{(3)}, s_{22}^{(3)} e s_{44}^{(3)}$. Consequentemente, o grafo tem apenas um subgrafo maximal bidirecional completo, a saber, $\{V_1, V_2, V_4\}$.

Definição 5: Um caminho que une dois indivíduos V_i e V_k em um digrafo é uma sequência de vértices distintos $V_i, V_a, V_b, \ldots, V_n, V_k$ e arestas orientadas $V_iV_a, V_aV_b, \ldots, V_nV_k$.

Exemplo 32:

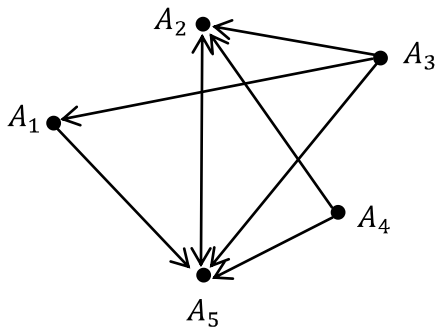


A sequência $V_1V_2V_3V_4$ é ~~um~~ caminho.
Já a sequência $V_1V_2V_3V_4V_2V_5$ não é ~~um~~ caminho, já ~~que~~ V_2 se repete.

Em muitos grupos de indivíduos, existe sempre uma ordem de dominação, um domina e o outro é dominado. Isto é, dados quaisquer dois indivíduos A e B, ou A domina B ou B domina A, mas não ambos. Em geral temos a seguinte definição.

Definição 6: Um grafo dirigido por dominância é um grafo dirigido tal que, para qualquer par de vértices distintos P_i e P_j, ou P_iP_j ou P_jP_i, ~~mas~~ não ambos.

Exemplo 33: Imagine um grupo de cinco amigos que estudam juntos há quatro anos consecutivos. O professor traçou o digráfico abaixo para representar a influência das relações entre esses alunos.



Logo, a matriz de adjacência é:

$$A(G) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Observe que o A_3 (3ª linha) tem três uns em sua linha, dessa forma A_3 (aluno 3) influência três pessoas, mais do que qualquer outro componente do grupo. Dessa maneira A_3 seria declarado o líder do grupo.

Definição 7: O digrafo é dito fortemente conexo se para quaisquer dois vértices distintos V_i e V_j há um caminho de V_i a V_j e um caminho de V_j a V_i. Caso contrário, G não é fortemente conexo.

Teorema 6: Um digrafo com n vértices é fortemente conexo se e somente se sua matriz de adjacência $A(G)$ tem a seguinte propriedade:

$$[A(G)] + [A(G)]^2 + \cdots + [A(G)]^{n-1} = E$$

Sem elementos nulos.

Exemplo 34: Dado o digrafo com matriz de adjacência abaixo, verifiquemos se ele é fortemente conexo.

$$A(G) = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Solução:

Para que o digráfico seja fortemente conexo devemos ter: $[A(G)] + [A(G)]^2 + \cdots + [A(G)]^{n-1} = E$, com a condição que E não tenha elementos nulos. Então temos,$[A(G)] + [A(G)]^2 + [A(G)]^3 + [A(G)]^4 = E$

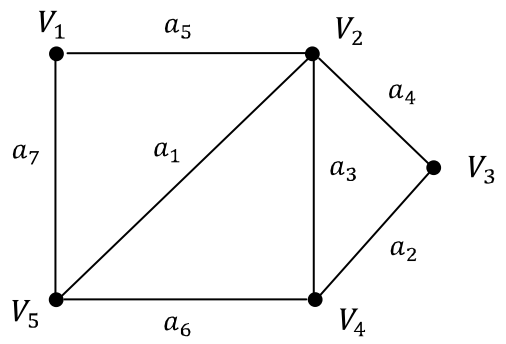
$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 3 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 2 \\ 1 & 0 & 1 & 1 & 0 \\ 2 & 1 & 1 & 1 & 0 \\ 1 & 0 & 2 & 2 & 1 \end{bmatrix} + \begin{bmatrix} 4 & 1 & 2 & 2 & 0 \\ 1 & 3 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 3 & 2 & 1 \\ 0 & 2 & 0 & 1 & 3 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 4 & 4 & 3 & 3 \\ 2 & 6 & 3 & 2 & 3 \\ 2 & 1 & 2 & 2 & 1 \\ 3 & 3 & 5 & 4 & 2 \\ 2 & 3 & 3 & 4 & 5 \end{bmatrix}$$

Observe que E não possui nenhum elemento nulo, logo o digráfico é fortemente conexo.

2.1.3 Matriz de Incidência

Seja G um grafo não direcionado de n vértices $V_1, V_2, \ldots, V_n$, e m arestas $a_1, a_2, \ldots, a_m$. A matriz de incidência é uma matriz $B = [b_{ij}]$ de ordem $n \times m$, onde o valor de cada elemento b_{ij} da matriz é $b_{ij} = 1$, se a aresta j é incidente ao vértice i, caso contrário $b_{ij} = 0$.



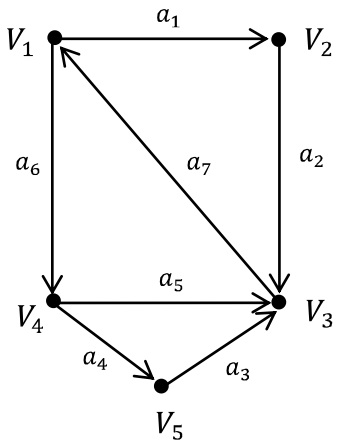
A matriz de incidência do grafo é a seguinte:

$$B = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{array} \begin{array}{c} \begin{matrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

Propriedades:

1. Como cada aresta é incidente a exatamente dois vértices, então cada coluna da matriz contém exatamente dois 1.
2. O número 1 em cada linha é igual ao grau do vértice correspondente.
3. Uma linha que contém somente 0 representa um vértice isolado.
4. Arestas paralelas resultam em colunas idênticas.

Quando o grafo é direcionado,é preciso distinguir as arestas convergentes das arestas divergentes. Em outras palavras, para cada aresta, temos que especificar de qual vértice ela vem e em qual ela chega. Podemos simplesmente utilizar 1 no primeiro caso e -1 no segundo. Observe a figura a seguir:



Sua matriz de incidência é:

$$B = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{array} \begin{array}{c} \begin{array}{ccccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & -1 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

2.2 CRIPTOGRAFIA

Criptografia é o nome dado ao estudo de codificação e decodificação de mensagens secretas. Ela é considerada ciência há mais ou menos 25 anos. Antes, era tida como “arte”. A criptografia é tão antiga quanto à escrita, ela já fazia parte da escrita hieroglífica dos egípcios e os romanos utilizavam-na como códigos (ou cifras) secretos para comunicar planos de guerra, e ainda hoje é bastante utilizada devido à necessidade de manter a privacidade de certas informações transmitidas por linhas publicas de comunicação. Na linguagem da 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 em cifrado é chamado cifrar ou criptografar e o processo inverso de converter um texto cifrado é chamado em comum é chamado *decifrar*.

2.2.1 Cifras de Substituição

As cifras de substituição são as que substituem cada letra do alfabeto por outra letra, há uma troca de três posições no alfabeto. Observe a tabela abaixo:

Tabela1:

Comum:	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
Cifra:	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

A partir daí podemos criptografar um texto apenas substituindo as letras comuns pelas suas respectivas letras cifradas.

Por exemplo: Dada a mensagem de texto comum: EU AMO MATRIZES

Criptografando essa mensagem obtemos: HX DPR PDWULCHV

A desvantagem de cifras de substituição é que elas preservam a sequência das letras individuais, tornando fácil quebrar os códigos por meios estatísticos. Uma solução para esse problema é a utilização de um sistema de criptografia no qual o

texto comum é dividido em conjuntos de n letras, cada um dos quais é substituído por um conjunto de n letras cifradas, a esse sistema damos o nome de sistema poligráfico, uma classe desse sistema poligráfico é dada a seguir.

2.2.2 Cifras de Hill

Muitas técnicas usadas para codificar e decodificar mensagens secretasutilizam a Álgebra Linear. Um bom exemplo são as cifras de Hill.

Cifras de Hill é uma classe de sistemas poligráficos baseados em transformações matriciais.

Considere a tabela abaixo:

Tabela 2:

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

Nos casos mais simples de cifras de Hill, transformamos pares sucessivos de texto comum em texto cifrado, pelas seguintes etapas:

1) Escolha uma matriz 2×2, $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, com entradas inteiras para efetuar a codificação.

2) Agrupe as letras sucessivas de texto comum em pares. Caso, o texto tenha um número impar de letras, deve-se adicionar uma letra fictícia para completar o ultimo par do texto. Logo após deve-se substituir cada letra de texto comum por seu valor numérico inteiro. Cada letra, exceto o Z, tem um valor numérico de acordo com sua posição, damos a Z o valor 0.

3) Converta cada par sucessivo P_1P_2 de letras de texto comum em um vetor-coluna. $p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$, e forme o produto Ap. Chamamos p de vetor comum e Ap o correspondente vetor cifrado.

4) Converta cada vetor cifrado em seu equivalente alfabético. Caso o número inteiro seja maior que 25, ele será substituído pelo resto de sua divisão com o número 26.

Exemplo 35: Utilizando a matriz $A = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$, obtenha a cifra de Hill da mensagem: DARK NIGHT

Primeiramente, agrupamos o texto comum em pares de letras e adicionamos uma letra fictícia T para completar o ultimo par:
DA RK NI GH TT

Pela tabela 2, obtemos os pares de números:
4 1 18 11 14 9 7 8 20 20

Para codificá-los, efetuaremos o produto matricial.
Inicialmente, codificaremos o par DA:

Dada a matriz $A = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$, e o vetor-coluna $p = \begin{bmatrix} 4 \\ 1 \end{bmatrix}$, temos:

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 1 \end{bmatrix} = \begin{bmatrix} 7 \\ 9 \end{bmatrix}$$

Pela tabela 2, temos que o par 7 9 equivale à GI. Encontramos então nosso primeiro par cifrado, da mesma forma devemos proceder com os demais pares.

Para codificar o par RK:

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 18 \\ 11 \end{bmatrix} = \begin{bmatrix} 51 \\ 47 \end{bmatrix}$$

Como os números inteiros 51 e 47 são ambos maiores que 25, ou seja, não estão presentes na tabela 2, devemos substituí-los pelo resto de sua divisão pelo número 26. Logo,

51÷26 = 1, resta 25

47÷26 = 1, resta 21

Pela tabela 2, os números 25 e 21 correspondem a YU.

Para codificar o par NI:

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\cdot\begin{bmatrix}14\\9\end{bmatrix}=\begin{bmatrix}41\\37\end{bmatrix}$$

41÷26 = 1, resta 15

37÷26 = 1, resta 11

Pela tabela 2, os números 15 e 11 correspondem a OK

Para codificar o par GH:

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\cdot\begin{bmatrix}7\\8\end{bmatrix}=\begin{bmatrix}31\\22\end{bmatrix}$$

31÷26 = 1, resta 5

Os números 5 e 22, correspondem a EV.

E por ultimo o par TT:

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\cdot\begin{bmatrix}20\\20\end{bmatrix}=\begin{bmatrix}80\\60\end{bmatrix}$$

80÷26 = 3, resta 2

60÷26 = 2, resta 8

De 2 e 8, obtemos BH.

Organizando os pares de texto cifrado, obtemos a seguinte mensagem:

GI YU OK EV BH

Que seria transmitida como uma única cadeia sem espaços:

GIYUOKEVBH

Como o texto comum foi agrupado em pares e criptografado por uma matriz 2×2, dizemos que essa cifra de Hill é uma 2-cifra de Hill. Da mesma forma, também

é possível fazer o agrupamento em ternos e criptografar com uma matriz 3×3 com entradas inteiras, assim chamamos de 3-cifra de Hill. Em geral para uma n-cifra de Hill agrupamos o texto comum em conjuntos de n letras e codificamos com uma matriz codificadora n×n de entradas inteiras.

2.2.2.1 Aritmética Modular

No exemplo 35, todos os números maiores que 25 foram substituídos pelo resto de sua divisão por 26. Esta técnica de trabalhar com restos é a base de uma parte da Matemática chamada aritmética modular.

Definição8: Dados um número inteiro positivo m e dois inteiros a e b quaisquer, dizemos que a é equivalente a b módulo m, e escrevemos $a \equiv b\ (mod m)$ se a−b é um múltiplo inteiro de m.

Exemplo 36:

i) $7 \equiv 3\ (mod\ 4)$
ii) $14 \equiv 2\ (mod\ 6)$

Observe que a é equivalente, módulo m, a exatamente um dos inteiros: $0,1,2 \ldots, m-1$.Este inteiro é chamado de resíduo de$a$ módulo m e escrevemos:$Z_m = \{0,1,2, \ldots, m-1\}$, para denotar o conjunto dos resíduos de a módulo m.

Teorema 7: Dados um inteiro a e um módulo m quaisquer, seja $R = restode\frac{|a|}{m}$. Então o resíduo r de a módulo m é dado por:

$$r = \begin{cases} R & se\ a \geq 0 \\ m - R\ se\ a < 0\ e\ R \neq 0 \\ 0 & se\ a < 0\ e\ R = 0 \end{cases}$$

Exemplo 37: Encontre os resíduos, módulo 14, de 36, -75 e -42.

1) Seja $a = 36$, temos:

$|36| = 36$, $\frac{36}{14} = 9$, e tem resto $R = 8$. Pelo teorema 7, obtemos $r = 8$, ou seja:

$$36 \equiv 8\ (mod\ 14)$$

2) Seja $a = -75$,temos:

$|-75| = 75$, $\frac{75}{14} = 5$, e tem resto $R = 5$, ou seja, $r = m - R = 9$.

Assim,

$$-75 \equiv 9\ (mod\ 14)$$

3) Seja$a = -42$, temos:

$|-42| = 42$, $\frac{42}{14} = 3$, e tem resto $R = 0$. Logo,

$$-42 \equiv 0\ (mod\ 14)$$

Na aritmética usual, cada número inteiro não nulo a tem um recíproco ou inverso multiplicativo denotado por a^{-1}, tal que $aa^{-1} = a^{-1}a = 1$. Já na aritmética modular temos o seguinte conceito:

Definição 9: Dado um número a em Z_m, dizemos que um número a^{-1} em Z_m é um recíproco, ou inverso multiplicativo de a módulo m se $aa^{-1} = a^{-1}a \equiv 1(modm)$.

Exemplo 38: Recíproco de 5mod 26

Observe que 5 e 26 não possuem fatores primos em comum, ou seja, podemos encontrar um inverso multiplicativo módulo m, que pode ser obtido encontrando um número x em Z_{26} que satisfaça a equação modular:

$$5x \equiv 1(mod\ 26)$$

Experimentando uma a uma cada solução possível de 0 a 25, encontramos que x=21 é a solução, pois:

$$5\,.\,21 = 105 \equiv 1\ (mod\ 26)$$

Assim,

$$5^{-1} \equiv 21(mod\ 26)$$

Para agilizar questões posteriores, apresentaremos a seguinte tabela de inversos multiplicativos módulo 26:

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

2.2.2.2 Decifrar

Cada cifra útil possui um procedimento para decifrar. Para decifrar a cifra de Hill, usamos a inversa modulo 26 da matriz codificadora. Isso acontece da seguinte forma:

Seja a matriz A de ordem 2×2 e seja B sua inversa. Suponha que $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, é invertível módulo 26 e que esta matriz é usada para uma 2-cifra de Hill. Se $p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ é um vetor comum, então $c = Ap$ é o correspondente vetor cifrado e $p = A^{-1}c$.
Assim, cada vetor comum pode ser recuperado do correspondente vetor cifrado pela multiplicação à esquerda por $A^{-1}(mod 26)$.

Teorema 8: Uma matriz quadrada A com entradas em Z_m é invertível módulo m, se e somente se, o resíduo de $\det(A)$ módulo m tem inverso multiplicativo módulo m.

Corolário 1: Uma matriz quadrada A com entradas em Z_m é invertível módulo m, se e somente se, o resíduo de $\det(A)$ módulo m tem fatores primos comuns.
Como os únicos fatores primos de $m = 26$ são 2 e 13, temos o seguinte corolário:

Corolário 2: Uma matriz quadrada A com entradas em Z_{26} é invertível módulo 26 se, e somente se, o resíduo de $\det(A)$, módulo 26, não é divisível por 2 ou 13.

Prova:

Dada a matriz $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, com entradas em Z_{26} e se o resíduo de $\det(A) = ad - bc$ módulo 26 não é divisível por 2 ou por 13, então a inversa de $\det(A)\ (mod 26)$ é dada por:

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

Onde $(ad - bc)^{-1}$ é o recíproco $ad - bc\ (mod 26)$.

Exemplo 39: Decodifique a mensagem: SAKNOXAOJX. Sabendo que é uma cifra de Hill com matriz codificadora $A = \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$.

Pela tabela 2, o equivalente numérico do texto cifrado é:

19 1 11 14 15 24 115 1024

Encontremos então a inversa de A,

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

$$A^{-1} \equiv (8 - 3)^{-1} \begin{bmatrix} 2 & -1 \\ -3 & 4 \end{bmatrix} (mod 26)$$

$$A^{-1} \equiv (5)^{-1} \begin{bmatrix} 2 & -1 \\ -3 & 4 \end{bmatrix} (mod 26)$$

Pela tabela 2, obtemos $(5)^{-1} = 21$, logo

$$A^{-1} \equiv 21 \begin{bmatrix} 2 & -1 \\ -3 & 4 \end{bmatrix} = \begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix} (mod 26)$$

$$\begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 1 \end{bmatrix} = \begin{bmatrix} 309 \\ 291 \end{bmatrix} = \begin{bmatrix} 23 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix} \begin{bmatrix} 11 \\ 14 \end{bmatrix} = \begin{bmatrix} 246 \\ 249 \end{bmatrix} = \begin{bmatrix} 12 \\ 15 \end{bmatrix}$$

$$\begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix} \begin{bmatrix} 15 \\ 24 \end{bmatrix} = \begin{bmatrix} 360 \\ 369 \end{bmatrix} = \begin{bmatrix} 22 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix} \begin{bmatrix} 1 \\ 15 \end{bmatrix} = \begin{bmatrix} 91 \\ 105 \end{bmatrix} = \begin{bmatrix} 13 \\ 27 \end{bmatrix}$$

$$\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}10\\24\end{bmatrix}=\begin{bmatrix}280\\294\end{bmatrix}=\begin{bmatrix}20\\8\end{bmatrix}$$

Pela tabela 1, os equivalentes alfabéticos desses vetores são:

WE LO VE MA TH

Que fornecem a mensagem:

WE LOVE MATH

2.2.2.3 Quebrando uma cifra

O objetivo de criptografar mensagens é impedir que pessoas não autorizadas descubram o conteúdo das mensagens. Porém é possível decifra-las mesmo não tendo acesso a matriz codificadora. Iremos agora discutir um pouco a respeito.

Suponha que se tenha um texto comum e o cifrado correspondente de uma mensagem. Examinando a mensagem talvez sejamos capazes de deduzir que a mensagem é uma carta que começa com CARO SENHOR. Mostraremos que com apenas poucos destes dados é possível determinar a matriz decodificadora de uma cifra de Hill e consequentemente obter acesso ao restante da mensagem.

Teorema 9: Sejam $p_1, p_2, \dots, p_n$ vetores comuns linearmente independentes sejam $c_1, c_2, \dots, c_n$ os correspondentes vetores cifrados de uma n-cifra de Hill. Se

$$P=\begin{bmatrix}p_1^T\\p_2^T\\\vdots\\p_3^T\end{bmatrix}$$

É a matriz $n \times n$ de vetores-coluna $p_1^T, p_2^T, \dots, p_n^T$ e se

$$C=\begin{bmatrix}c_1^T\\c_2^T\\\vdots\\c_3^T\end{bmatrix}$$

É a matriz $n \times n$ de vetores-linha $c_1^T, c_2^T, \dots, c_n^T$, então a sequência de operações elementares sobre linhas que reduz C a I transforma P em $(A^{-1})^T$.

Observação: A demonstração deste teorema vai além do objetivo deste trabalho.

Exemplo 40: Decodifique a 2-cifra de Hill: GFYKEJDGYZIVUJBTCD

Sabendo que ela inicia com a palavra CARO.

Pela tabela 2, o equivalente do texto comum conhecido é:

CA RO

3 1 18 15

E o equivalente numérico do texto cifrado correspondente é

G F Y K

7 6 25 11

De modo que os vetores comuns e correspondentes vetores cifrados são:

$$p_1 = \begin{bmatrix} 3 \\ 1 \end{bmatrix} \Leftrightarrow c_1 = \begin{bmatrix} 7 \\ 6 \end{bmatrix}$$

$$p_2 = \begin{bmatrix} 18 \\ 15 \end{bmatrix} \Leftrightarrow c_2 = \begin{bmatrix} 25 \\ 11 \end{bmatrix}$$

Nós queremos reduzir

$$C = \begin{bmatrix} c_1^T \\ c_2^T \end{bmatrix} = \begin{bmatrix} 7 & 6 \\ 25 & 11 \end{bmatrix}$$

aI por operações elementares sobre linhas e simultaneamente aplicar estas operações a

$$P = \begin{bmatrix} p_1^T \\ p_2^T \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 18 & 15 \end{bmatrix}$$

Para obter $(A^{-1})^T$. Isto pode ser obtido adjuntando P à direita de C e aplicando as operações sobre linhas à matriz resultante $[C|P]$ até que o lado esquerdo esteja reduzido a I.

$\left[\begin{matrix} 7 & 6 \\ 25 & 11 \end{matrix}\middle|\begin{matrix} 3 & 1 \\ 18 & 15 \end{matrix}\right]$ → Matriz $[C|P]$ formada

$\left[\begin{matrix} 1 & 90 \\ 25 & 11 \end{matrix}\middle|\begin{matrix} 45 & 15 \\ 18 & 15 \end{matrix}\right]$ → $L_1 \to 7^{-1}.L_1$,

$\left[\begin{matrix} 1 & 12 \\ 25 & 11 \end{matrix}\middle|\begin{matrix} 19 & 15 \\ 18 & 15 \end{matrix}\right]$ → Substituímos 90 e 45 pelo seu resíduo módulo 26

$$\left[\begin{array}{cc|cc} 1 & 12 & 19 & 15 \\ 0 & -289 & -457 & -360 \end{array}\right] \rightarrow L_2 \rightarrow -25.L_1 + L_2$$

$\left[\begin{array}{cc|cc} 1 & 12 & 19 & 15 \\ 0 & 23 & 11 & 4 \end{array}\right]$ → Substituímos o -289, -457, -360 pelos seus resíduos módulo 26.

$$\left[\begin{array}{cc|cc} 1 & 12 & 19 & 15 \\ 0 & 1 & 187 & 68 \end{array}\right] \rightarrow L_2 \rightarrow 23^{-1}.L_2$$

$\left[\begin{array}{cc|cc} 1 & 12 & 19 & 15 \\ 0 & 1 & 5 & 16 \end{array}\right]$ → Substituímos 187 e 68 pelos seus resíduos módulo 26.

$$\left[\begin{array}{cc|cc} 1 & 0 & 11 & 5 \\ 0 & 1 & 5 & 16 \end{array}\right] \rightarrow L_1 = -12.L_2 + L_1$$

Assim,

$$(A^{-1})^T = \begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix}$$

E, portanto a matriz decodificadora é: $A^{-1} = \begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix}$

Por fim, agrupamos o texto cifrado em pares e encontramos os equivalentes numéricos de cada letra.

$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 7 \\ 6 \end{bmatrix} = \begin{bmatrix} 107 \\ 131 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$ C A

$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 25 \\ 11 \end{bmatrix} = \begin{bmatrix} 330 \\ 301 \end{bmatrix} = \begin{bmatrix} 18 \\ 15 \end{bmatrix}$ R O

$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} 105 \\ 185 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$ A C

$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 4 \\ 7 \end{bmatrix} = \begin{bmatrix} 79 \\ 132 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ A B

$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 25 \\ 0 \end{bmatrix} = \begin{bmatrix} 275 \\ 125 \end{bmatrix} = \begin{bmatrix} 15 \\ 21 \end{bmatrix}$ O U

$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 9 \\ 22 \end{bmatrix} = \begin{bmatrix} 209 \\ 397 \end{bmatrix} = \begin{bmatrix} 1 \\ 7 \end{bmatrix}$ A G

$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 21 \\ 10 \end{bmatrix} = \begin{bmatrix} 281 \\ 265 \end{bmatrix} = \begin{bmatrix} 21 \\ 5 \end{bmatrix}$ U E

$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 2 \\ 20 \end{bmatrix} = \begin{bmatrix} 122 \\ 330 \end{bmatrix} = \begin{bmatrix} 18 \\ 18 \end{bmatrix}$ R R

$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 53 \\ 79 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ A A

CARO ACABOU A GUERRA.

CONCLUSÃO

Neste trabalho foi abordado o assunto: Matrizes e duas aplicações. Tratamos primeiramente um pouco da história da matriz na introdução, citando dois nomes, James Joseph Sylvester e Arthur Cayley, que deram sua contribuição o cálculo das matrizes. No capítulo 1 mostramos seus tipos, definições, operações e exemplos. No capítulo 2 discutimos as duas aplicações. A primeira delas foi a Teoria dos grafos e a segunda criptografia. Tais aplicações estão presentes no nosso cotidiano, sem que possamos perceber. Quando fazemos uma viagem e precisamos usar um mapa para ver qual o melhor caminho, estamos utilizando grafos. Ou quando um agente da policia utiliza códigos na comunicação, por telefone ou pelo rádio comunicador da viatura, temos então o uso da criptografia. E não só isso, podemos encontrar inúmeros casos em que faremos uso destas.

Sempre admirei as matrizes, de uma forma geral. Acho interessante a forma como elas são organizadas. Já conhecia outras aplicações das matrizes, mas não estas que expus neste trabalho, conhecê-las foi de extrema valia para mim, como futura professora de matemática.

Este trabalho foi de grande relevância, haja vista, ter tido a oportunidade de conhecer e admirar cada vez mais os matemáticos que fizeram estudos tão belos e tão importantes para a sociedade.

REFERÊNCIAS

BOYER, C. B. **História da matemática**. 2. Ed. São Paulo: Edgard Blucher, 1996.

CAJORI, F.**Uma história da matemática**. Rio de Janeiro. Editora ciência moderna Ltda, 2007.

CONTADOR, P. R. M. **Matemática, uma breve história**. Vol. 3. 2.ed. Caderno de práticas. São Paulo: Editora livraria da física, 2007.

HOWARD, A.; RORRES, C. **Álgebra Linear com aplicações**, 8.ed. Porto Alegre:bookman, 2001.

KOLMAN, B.; HILL, D. R.**Introdução à Álgebra Linear com aplicações**. 8.ed. Rio de Janeiro: LTC, 2006.

LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C.**A matemática do ensino médio**. Vol. 3. 6. ed. Rio de Janeiro: SBM, 2006.

LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C., **A matemática do Ensino médio**, vol. 4. Rio de Janeiro, SBM, 2010.

Meio eletrônico:

BERNARDES, A. C. S., Objetos epistêmicos, técnicas epistêmicas e dois episódios da historias das matrizes. Disponível em: <http://www.sbhc.org.br/resources/anais/10/1345074112_ARQUIVO_artigocompleto13SNHCT.pdf>. Acesso em: 16/05/2014

FERREIRA, S. R. I. Aplicações de matriz no ensino médio. USP, São Paulo, 2013. Disponível em <http://www.teses.usp.br/teses/disponiveis/55/55136/tde-07062013-100316/es.php>. Acesso em: 09/06/2014

GAGNON, Michel. Algoritmos e teoria dos grafos. 2000. Disponível em: <http://www.professeurs.polymtl.ca/michel.gagnon/Disciplinas/Bac/Grafos/RepImpl/rep_impl.html>. Acesso em: 09/06/2014

ZATTI, S. B.; BELTRAME, A. M., A presença da álgebra linear e teoria dos números na criptografia. Disponível em: <http://www.unifra.br/eventos/jornadaeducacao2006/2006/pdf/artigos/matem%C3%A1tica/A%20PRESEN%C3%83A%20DA%20-ALGEBRA%20LINEAR%20E%20TEORIA%20DOS%20N+MEROS%20NA%20CRIPT%C3%A0.pdf>. Acesso em: 15/07/2014