MATRICES AND ITS APPLICATIONS

ABSTRACT

This Project examines *matrices and three of its applications*. Matrix theories were used to solve economic problems, which involves methods at which goods can be produced efficiently. To encode and also to decode very sensitive information. This project work also goes further to apply matrices to solve a 3 x 3 linear system of equations using row reduction methods.

TABLE OF CONTENT

CHAPTER ONE

GENERAL INTRODUCTION

1.0 BACKGROUND OF THE STUDY

In order to unfold the history of Matrices and Its Applications, the influence of matrices in the mathematical world is spread wide because it providesan importantbaseto many of the principles and practices. It is important that we first determine what matrices is. As such, this definition is not a complete and comprehensive answer, but rather a broad definition loosely wrapping itself around thesubject.

"Matrix" is the Latin word for womb, and it retains that sense in English. It can also mean more generally any place in which something is formed or produced.

The origin of mathematical matrices lies with the study of systems of simultaneous linear equations. An important Chinese text from between 300Bc and Ad 200, nine chapters of the mathematical art, gives the first known example of the use of matrix methods to solve simultaneous equations. *(Laura Smoller (2012))[9]*

In the treatises seventh chapter “too much and not enough”, the concept of a determinant first appears, nearly two milkman before its supposed inventions by the Japanese mathematician SEKI KOWA in 1683 or his German contemporary GOTTFRIED LEIBNIZ (who is also credited with the invention of differential calculus, separately from but simultaneously with Isaac Newton).

More uses of matrix-like arrangements of numbers appears in which a method is given for solving simultaneous equations using a counting board that is mathematically identical to the modern matrix method of solution outlined by Carh Fredrich Gauss (1777-1855) also known as Gaussian Elimination. *(Vitull marie 2012)[17]*

This project seeks to give an overview of the history of matrices and its practical applications touching on the various topics used in concordance with it.

Around 4000 years ago, the people of Babylon knew how to solve a simple 2X2 system of linear equations with two unknowns. Around 200 BC, the Chinese published that “Nine Chapters of the Mathematical Art, “they displayed the ability to solve a 3X3 system of equations. *(perotti) [13]*. The power and progress in Matrices and its application did not come to fruition until the late 17th century.

The emergence of the subject came from determinants, values connected to a square matrix, studied by the founder of calculus, Leibnitz, in thelate17th century. Lagrange came out with his work regarding Lagrange multipliers, a way to “characterize the maxima and minima multivariate functions.” (Darkwing) More than fifty-year later, Cramer presented his ideas of solving systems of linear equations based on determinants more than50 years after Leibnitz (Darkwing).

Interestingly enough, Cramer provided no proof for solving an n x n system.

As mentioned before, Gauss work dealt much with solving linear equations themselves initially but did not have as much to do with matrices. In order for matrix algebra to develop, a proper notation or method of describing the process was necessary. Also vital to this process was a definition of matrix multiplication and the facets involving it. "The introduction of matrix notation and the invention of the word matrix were motivated by attempts to develop the right algebraic language for studying determinants. In 1848, J.J. Sylvester introduced the term "matrix," the Latin word for womb, as a name for an array of numbers. He used womb, because see, linear algebra has become more relevant since the emergence of calculus even though it's foundational equation of ax+ b=0 dates back centuries.

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Euler brought to light the idea that a system of equations doesn't necessarily have to have a solution. He recognized the need for conditions to be placed upon unknown variables in order to find a solution. The initial work up until this period mainly dealt with the concept of unique solutions and square matrices where the number of equations matched the number of unknowns.

With the turn intothe19th century Gauss introduced a procedure to be used for solving a system of linear equations. His work dealt mainly with the linear equations and had yet to bring in the idea of matrices or their notations. His efforts dealt with equations of differing numbers and variables as wella s thetraditionalpre-19th century works of Euler, Leibnitz, and Cramer. Gauss' work is now summed up in the term Gaussian elimination. This method uses the concepts of combining, swapping, or multiplying rows with each other in order to eliminate variables fromcertain equations.Aftervariables are determined,thestudent is thento use back substitution tohelp findthe remainingunknown variables.

Heviewed a matrixas ageneratorof determinants (Tucker, 1993).Theother part,matrix multiplication or matrixalgebracamefrom thework ofArthurCayleyin 1855.

Cayley's defined matrix multiplication as, "the matrix of coefficients for thecomposite transformationT2T1is theproductof the matrix forT2times thematrix ofT1"(Tucker, 1993). His work dealingwith Matrixmultiplicationculminatedin his theorem, the Cayley-Hamilton Theorem. Simply stated, a square matrixsatisfiesMatrices atthe end of the 19thcentury were heavily connectedwith Physics issues andfor mathematicians, moreattentionwas givento vectorsas they proved tobe basic mathematical elements.Withtheadvancementof technologyusing themethods of Cayley, Gauss, Leibnitz, Euler, andothers determinantsand linear algebra movedforwardmore quickly and more effective. Regardless of thetechnologythough Gaussian eliminationstillproves to be thebest way known to solve asystemof linear equations (Tucker,1993).

Theinfluence of matrices and it's applicationsinthe mathematicalworldis spreadwide becauseit providesan importantbaseto many of the principles and practices. Some of thethings Matrices is usedfor are tosolvesystems of linearformat, to find least-square bestfitlines topredictfuture outcomes or find trends, to encode and decode messages. Other morebroad topicsthatit is used for areto solve questionsof energy in Quantummechanics. It is also usedto create simple everyday household games likeSudoku. Itis because of these practicalapplications thatMatriceshas spread so far and advanced.Thekey, however,is to understand that thehistory of linear algebra providesthe basis for theseapplications.

Althoughlinearalgebrais a fairly new subjectwhencomparedto othermathematical practices,its uses are widespread.Withthe efforts of calculussavvy Leibnitz theconceptof using systems of linear equations tosolveunknowns was formalized. Otherefforts fromScholars like Cayley.Euler, Sylvester, and others changed matricesinto theuseof linear algebratorepresent them. Gauss broughthis theory tosolve systems of equations proving to bethe most effectivebasis for solving unknowns.

Technologycontinues to push the use furtherand further, butthe historyof matrices and its applicationcontinues toprovide thefoundation. Even thoughevery few years companiesupdate their textbooks, the fundamentals stay thesame.*(laura smoller (2001)[9].*

1.2 STATEMENT OF PROBLEM

Due to the great need of security for passing sensitive information from one person to another or from one organization to another through electronic technology, there is need for cryptography as a solution to this problem.

Also in economics this research work is going to discuss how Leontief model is used to represent the economy as a system of linear equation so as to calculate the gross domestic products and goods production efficiently.

1.3 AIMS AND OBJECTIVES

i. To apply matrices to Cryptography, Economic Models and system of Linear Equations

ii.To improve the methods at which increase in production out-put can be achieved

iii.To show ways at which sensitive information can be passed across mathematically.

iv. To disseminate this improved methods to the relevant communities and end use

CHAPTER TWO

LITERATURE REVIEW

2.0 INTRODUCTION

The study of matrix algebra first emerged in England in the mid-1800s. In 1844 Herman Grassmann published his theory of extension which include fundamental new topics of what is today called linear algebra. In 1848, James Joseph Sylvester introduced the term matrix, which is a Latin word for “womb” while studying compositions of linear transformations, Arthur Cayley was led to define matrix multiplication and universe. Crucially, Cayley used a single letter to denote a matrix, thus treating a matrix as an aggregate object. He also realized the connection between matrices and determinants, and wrote “There will be many Things to say about this theory of matrices which should (seems to me) precede the theory of determinants”. *(Calson (1993)[12]*

In 1882, Husejin Tevfik Pasha wrote a book title “Linear Algebra”.*(Tucker (1993))[19]*Linear algebra first took it modern form in the first half of the 20^{th} century, when many ideas and methods of previous centuries were generalized an abstract algebra. The use of matrices in quantum mechanics, special relatively and statistics helped spread the subject of linear algebra betics helped spread the subject of linear algebra beyond pure mathematics. The development of computers led to increased research in efficient algorithms for Gaussian elimination and matrix decompositions and linear algebra become an essential tool for modelling and stimulations. *(Tucker A. (1993))[16]*.

In 1801, 23 year old Carl Fredrick Gauss (1777-1855) become instantly famous when he was able to compute the orbit of the newly discovered planetoid career from just a few observations. The Italian astronomer Piazzi, discovered this new planetoid at the beginning of 1801, and then lost sight of it using Gauss computed orbit, the planetoid was rediscovered at the end of the year in almost exactly the position forecast by Gauss. Later in 1801, Gauss become interested in discovering the orbit of Pallas, the second-largest asteroid of the solar system. This work led him to a system of six linear equations in six unknowns. In order to solve this system, Gauss invented the method of Gaussian elimination which are still use today. The method consists of performing row-operation on the co-efficient matrix to obtain an equivalent system of equations whose co-efficient matrix is upper triangular. This means that the last equation will involve only one unknown and can be easily solved substituting that solution into the second to last equations, one can then solve for another unknown.

The set of points with coordinates that satisfy a linear equation from a hyper plane is an in-dimensional space. The conditions under which a set of in hyper planes intersects in a single point is an important focus of study in linear algebra. Such an investigation is initially motivated by a system of linear equations containing several unknowns, such equations are naturally represented using the formalism of matrices and vectors. Techniques from linear algebra are also used in analytic geometry, engineering, physics, natural science, computer science and social sciences (particularly in economics). Because linear algebra is such a well-developed theory, non-linear mathematical models are sometimes approximated by linear models. *(Calson D. (1993))[5]*

CHAPTER THREE (3);

3.0 THEORY OF MATRICES

3.1 DEFINATION OF MATRIX AND TYPES OF MATRICE

A matrix (Plural Matrices) is a two dimensional array of numbers or expressions arranged in a dimensional array of numbers or expressions arranged in a set of rows and columns (*Weisstein (1995)) [18]*. An M X N matrix A has m rows and n columns and is written

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

Where the element aij, located in the ith row and the ith column is a **scalar quantity;** a numerical constant, or a single valued expression. If m=n, that is there are the same number of rows as columns, the matrix is square, otherwise it is a rectangular matrix.

A matrix having either a single row (m=1) or a single column (n=1) is defined to be a vector because it is often used to define the coordinates of a point in a multi-dimensional space.

A vector having a single row, for example

X= [xii x12 … x1n] Is define to be a row vector, while a vector having a single column is define to be a **column vector**

$$Y=\begin{bmatrix} y_{11} \\ y_{22} \\ \vdots \\ y_{m1} \end{bmatrix}$$

Two special matrices are the square identity matrix, I, which is defined to have all of its elements equal to zero except those on the main diagonal (where i=j) which have a value of one.

$$I=\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

And the null matrix 0, which has the value of zero for all of its elements.

$$0=\begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

MATRIX ADDITION

The operation of addition of two matrices is only defined when both matrices have the same dimensions. If A and B are both (mxn), then the sum

$$C= A+B$$

Is also (mxn) and is defined to have each element the sum of the correpending elements of A and B, thus $C_{ij}=a_{ij} + b_{ij}$

Matrix addition is both associative that is **A+(B+C) = (A+B)+C** and commutative **A+B = B+A**

MATRIX SUBTRACTION

The subtraction of two matrices is simlarly defined if A and B have the same dimensions then the different **C = A - B** implies that the element of C are $\mathbf{C_{ij} = a_{ij} - b_{ij}}$

MULTIPLICATION OF A MATRIX By A Scalar Quantity

If A is a matrix and K is a scalar quantity, the product B=kA is defined to be the matrix of the same dimensions as A whose elements are simply all scaled by the constant K.

$$B_{ij} = Kxa_{ij}$$

MATRIX MULTIPLICATION

Two matrices may be multiplied together only if they meet conditions on there dimensions that allow them to conform. Let A have dimensions mxn, and B be n x p, that is A has the same number as columns as the number of rows in B, then the product

C = AB

is defined to be an mxp matrix with elements

$$C_{ij} = \sum_{k=1}^{n} aikbkj$$

The element in position ij is the sum of the products of elements in the ith row of the first matrix (A) and the corresponding element in the ith column of the second matrix (B). the product AB is not defined unless the above condition is satisfied, that is the number of columns of the first matrix must equal the number of rowa in the second.

Matrix multiplication is associative, that is

$$A (BC) = (AB) C$$

But is not commutative in general

$$AB \neq BA$$

infact unless the two matrices are square, reversing the other in the product will cause the matrices to be nonconformed. The order of the terms in the product is

therefore very important. In the product C = AB. A is said to pre-multiply B, while B is said to post multiply A.

It is interesting to note in passing that unlike the scalar case, the fact that AB=0 does not imply that either A = 0 or that B = 0

REPRESENTING SYSTEM OF EQUATIONS IN MATRIX FORM LINEAR ALGEBRAIC EQUATIONS

The rules given above for matrix arithemetic allow a set of Linear algebraic equations to be written compactly in matrix form.

Considering this set of n independent linear equations in the variables x for i=1….n

$$\begin{bmatrix} a_{11}x1 & + & a_{12}\,x2 & + & \cdots & + & a_{1n}x\,n \\ a_{21}x1 & + & a_{22}\,x2 & + & \cdots & + & a_{2n}x\,n \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n1}x1 & + & a_{n2}\,x2 & + & \cdots & + & a_{nn}\,x\,n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Writing out the coefficients a_{ij} in a square matrix ***A*** of dimension ***n***

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

The unknowns x_{ij} in a column vector of x length N

$$X = \begin{bmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{bmatrix}$$

And the constant on the right-hand side in a column vector.

$$B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Then equations may be written as the product.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Which may be written compactly as

$$Ax = b$$

TYPES OF MATRICES

UNIT OR IDENTITY MATRIX

- A unit matrix (identity) matrix is a diagonal matrix with all the elements in the principal diagonal equal to one.
- The identity or unit matrix, designated by *I* is worthy of special consideration.
- For any arbitrary matrix A, the following relationships hold true:

$AI=A$ and $IA = A$

Examples: 3.1.1

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

If the matrix $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}$ then

$$AI = IA = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}$$

NULL OR ZERO MATRIX

- A null (zero) matrix is any matrix in which all the elements have zero values. It is usually denoted as 0.

- Examples:
- $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

SYMMETRIC MATRIX

Symmetric matrix In linear algebra, a symmetric matrix is a square matrix that is equal to its transpose. Formally, matrix A is symmetric if Because equal matrices have equal dimensions, only square matrices can be symmetric.

The entries of a symmetric matrix are symmetric with respect to the main diagonal. So if the entries are written as

A = (a_{IJ}), then $a_{ij} = a_{ji}$, for all indices i and j. The following 3×3 matrix is symmetric:

$$A_{13} = A_{31}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix} \qquad a_{23} = a_{32}\begin{bmatrix} 1 & 3 & 7 & 9 \\ 3 & 4 & 2 & 10 \\ 7 & 2 & 7 & 8 \\ 9 & 10 & 8 & 11 \end{bmatrix}$$

SKEW SYMMETRIC

- A skew-symmetric matrix is square matrix with all values on the principal diagonal equal to zero and with off-diagonal values given such that $a_{ij} = -a_{ji}$

Examples

$$\begin{bmatrix} 1 & 3 & 7 & 9 \\ 3 & 4 & 2 & 10 \\ 7 & 2 & 7 & 8 \\ 9 & 10 & 8 & 11 \end{bmatrix}$$

TRANSPOSED MATRIX

- Given a matrix A, the transpose of A, denoted by A^T and read A-transpose, is obtained by changing all the rows of A into the columns of A^T while preserving the order.

- Hence, the first row of A becomes the first column of A^T, while the second row of A becomes the second column of A^T, and the last row of A becomes the last column of A^T.
- In terms of the elements, $a_{ij}^T = a_{ij}$

- If matrix A has *r* rows and *c* columns, then A^T will have *c* rows and *r* columns
- Noting that $(A^T)^T = A$

Examples 3.1.2

-thus if $A=\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{bmatrix}$ then $A^T=\begin{bmatrix}1 & 4 & 7\\ 2 & 5 & 8\\ 3 & 6 & 9\end{bmatrix}$

- and if $A=\begin{bmatrix}1 & 2 & 3 & 4\\ 5 & 6 & 7 & 8\end{bmatrix}$ then $A^T=\begin{bmatrix}1 & 5\\ 2 & 6\\ 3 & 7\\ 4 & 8\end{bmatrix}$

3.2 ADDITION AND SUBTRACTION OF MATRICES

Matrix algebra has operations called addition, subtraction, and multiplications, no division in matrix algebra, instead there is matrix inversion.

MATRIX ADDITION:

If $A=[a_{ij}]_{rxc}$ are both of order (size) r x c, then A + B is a r x c matrix $[c_{ij}]_{r\,x\,c}$ where

$$C_{ij} = a_{ij} + b_{ij}$$

Examples:3.2.1

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

Example 3.2.2

$$:2\ \begin{bmatrix}t2 & 5\\ 3t & 0\end{bmatrix}+\begin{bmatrix}1 & -6\\ t & -t\end{bmatrix}=\begin{bmatrix}t2+1 & -1\\ 4t & -t\end{bmatrix}$$

MATRIX SUBTRACTION

- If $A = [a_{ij}]_{rxc}$ and $B = [b_{ij}]_{rxc}$ are both of order (size) r x c, then A – B is a r x c matrix $[c_{ij}]_{rxc}$

$$C_{ij} = a_{ij} - b_{ij}$$

Example:3.2.3

$$\begin{bmatrix} 1 & 9 & -2 \\ 3 & 6 & 0 \end{bmatrix} - \begin{bmatrix} 8 & -4 & 3 \\ 7 & 1 & 6 \end{bmatrix} = \begin{bmatrix} -7 & 12 & -5 \\ -4 & 5 & -6 \end{bmatrix}$$

3.3 PROPERTIES OF MATRIX ADDITION

The basic properties of addition for real numbers also hold true for matrices.

Let A, B and c be m x n matrices

1. A+B=B+A Commutative
2. A+(B+C)=(A+B)+C ASSOCIATIVE
3. There is a Unique m x n Zero Matrix, with A + 0 =A additive identity

3.4 SCALAR MULTIPLICATION

Let $A = a_{ij}$ be an mxn matrix, and K be a scalar (any number). Then the product kA of the matrix A and scalar k is the matrix $B=b_{ij}$ obtained by multiplying each elements a_{ij} of A by k, i.e $kA - ka_{ij}= (b_{ij}) = B$

3.5 MULTIPLICATION OF MATRICES

Let A and B be two matrices, the two matrices can only be multiplied if the number of columns in B is equal to the number of rows in A then the two matrix are said to be confortable for multiplications.

Suppose A is an mxn matrix, and B an nxn matrix then the AB=C of A and B is an mxu matrix whose $(i.j)^{th}$ elements are obtained by multipliyng elements of the i^{th} row of A with the corresponding elements of j^{th} column of B beginning at the left hand end of the row and the top of the column respectively and then summing the products i.e

$$C_{ij} = a_{ij}b_{ij} + a_{i2}b_{2j}+\ldots+a_{in}b_{ni}$$

For any matrix, if A = $\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix}$ and B = $\begin{bmatrix} p_1 & q_1 \\ p_2 & q_2 \\ p_3 & q_3 \end{bmatrix}$ then C = AB

Then C = AB = $\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix}\begin{bmatrix} p_1 & q_1 \\ p_2 & q_2 \\ p_3 & q_3 \end{bmatrix}$

$$\begin{bmatrix} a_1p_1 & + & b_1p_2 & + & c_1p_2 & + & a_1q_1 & + & b_1q_2 & + & c_1q_3 \\ a_2p_1 & + & b_2p_2 & + & c_2p_2 & + & a_2q_1 & + & b_2q_2 & + & c_2q_3 \end{bmatrix}$$

Therefore, the product will have equal number of rows of the first matrix A and columns equal to the number of column of the second matrix B. that is why matrix multiplication can also simply be called multiplication of rows into columns.

3.6 PROPERTIES OF MATRIX MULTIPLICATION

1. multiplication of matrices is not generally commutative AB $\neq$ BA

2. matrix multiplication is associative, A(BC) = (AB)C

3. matrix multiplication is distribute with respect to additive A(B+C) = AB + AC

4. multiplication of matrix A by unit matrix AI = IA =A

5. multiplication inverse of a matrix exists if A $\neq$P and $AA^{-1} = A^{-1}A=I$

3.7 ELEMENTARY ROW OPERATION

An elementry row operation on my mxn matrix is any of the following

a. Interchanging of any two rows (or columns)
b. Multiplication of any row (or column) by non-zero scalar
c. Addition of the multiple of one row (or column) to another row (or column)

ROW OPERATIONS

The following notations shall be used to indicate the three elementary row operations.

1. The interchange of rows (column) will be denoted by R_i <------> R_j

2. The multiplication of row I by S_i where S is not=0 will be denoted by SR_i ----->R_i
3. The addition of S times row I to row j will be denoted by Sri + Rj ----->Rj

COLUMN OPERATIONS

1. Interchanging columns I and j Ci ←--------> Cj
2. The multiplication of column I by Si where S is not= 0 will be denoted by sCi --------→ Ci
3. The addition of S times column I to column J will be denoted by sCi + Cj --------→Cj

3.8 ECHELON AND ROW-REDUCED ECHELON FORMS OF MATRIX

ECHELON FORM OF A MATRIX

A matrix is in row echelon form (REF) when it satisfies the following conditions

The first non-zero element in each row, called the leading entry, is 1

Each leading entry is in a column to the right of the leading entry in the previous row.

Rows with all zero elements, if any are below rows having a non-zero element.

Each of the matrices shown below are examples of matrices in row echelon form.

A-REF = $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ B-REF = $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ C-REF = $\begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$

In linear algebra, a matrix is in echelon form if it has the shape resulting of a Gaussian elimination. Row echelon form means that Gaussian elimination has operated on the rows and column echelon on the columns. In other words, a

matrix is in column echelon form of its transpose is in row echelon form. Therefore only row echelon forms are considered in the remainder of this article.

The similar properties of column echelon form are easily deduced by transposing all the matrices.

ROW-REDUCED ECHELON FORMS OF MATRIX.

If A matrix in echelon form satisfies the following additional conditions, then it is in reduced row echelon form (RREF)

1. The matrix is in row-echelon form

2. Each leading 1 is the only non-zero entry in its column, this matrix is in reduced row echelon form:

$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and also we have $\begin{bmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

how to proceed from a matrix to a reduced row form is explained below.

CHANGING A MATRIX INTO A ROW ECHELON FORM OR ROW REDUCED ECHELON FORM.

A system of linear equations can be solved by reducing its augmented matrix into reduced echelon form.

A matrix can be changed to its reduced row echelon form using the elementary row operations. These are:

1. Interchanging one row of the matrix with another of the matrix.

2. Multiply one row of the matrix by a non-zero scalar constant

3. Replace the one row with the one row plus a constant times another row of the matrix.

Example 3.8.1

given the following linear system with corresponding augmented matrix.

$3x_2 - 6x_3 + 6x_4 + 4x_5 = -5$

$3x_1 - 7x_2 + 8x_3 - 5x_4 + 8x_5 = 9$

$3x_1 - 9x_2 + 12x_3 - 9x_4 + 6x_5 = 15$

Solution

$$\begin{bmatrix} 0 & 3 & -6 & 6 & 4 & -5 \\ 3 & -7 & 8 & -5 & 8 & 9 \\ 3 & -9 & 12 & -9 & 6 & 15 \end{bmatrix}$$

To solve this system, the matrix has to be reduced into reduced echelon form.

> **STEP1**: switch row 1 and row 3. All leading zeros are row below non-zero leading entries

$$\begin{bmatrix} 3 & -9 & 12 & -9 & 6 & 15 \\ 3 & -7 & 8 & -5 & 8 & 9 \\ 0 & 3 & -6 & 6 & 4 & -5 \end{bmatrix}$$

>STEP2: Set row 2 to row 2 plus -1 (R2+(-1)) X Row 1 (R1). In other words, subtract row 1 from row2 (R2-R1). This will eliminate the first entry of zero 2

R1 $[3 \quad -9 \quad 12 \quad -9 \quad 6 \quad 15]$

R2 $[0 \quad 2 \quad -4 \quad 4 \quad 2 \quad -6]$ $R_2 = R_2 - R_1$

R3 $[0 \quad 3 \quad -6 \quad 6 \quad 4 \quad -5]$

> STEP 3: Multiply row 2 by 3 (3R2) and row 3 by 2 (2R3) this will eliminate the first entry of row 3

$$\begin{bmatrix} 3 & -9 & 12 & -9 & 6 & 15 \\ 0 & 6 & -12 & 12 & 6 & -18 \\ 0 & 6 & -12 & 12 & 8 & -10 \end{bmatrix} \quad R_2 = 3R_2 \; \& \; R_3 = 2R_3$$

>STEP4: set row 3 to row 3 plus (-1) times row 2. In other words, subtract row 2 from 3. This will eliminate the second entry of low 3.

$$\begin{bmatrix} 3 & -9 & 12 & -9 & 6 & 15 \\ 0 & 6 & -12 & 12 & 6 & -18 \\ 0 & 0 & 0 & 0 & 2 & 8 \end{bmatrix} R_3 = R_3 + (-1) \times R_2$$

>STEP 5: multiply each row by the reciprocal of its first non-zero value. This will make every row start with a 1.

$$\begin{bmatrix} 1 & -3 & 4 & -3 & 2 & 5 \\ 0 & 1 & -2 & 2 & 1 & -3 \\ 0 & 0 & 0 & 0 & 1 & 4 \end{bmatrix}$$

The matrix is now in row echelon form: all non-zero rows are above any rows of all zeros (there are no zero rows), each leading entry of a row is in a column to

the right of the leading entry of the row above it and it and all entries in a column below a leading entry are zeros.As can and will be shown later, from this form one can observe that the system has infinitely many solutions. To get those solutions the matrix is further reduced into reduced echelon form.

>STEP 6: set row 2 to row 2 +(-1) times row 3 and row 1 to row 1+(-2) times row 3. Thia will eliminate the entries above the leading entry of row 3. This will eliminate the entries above the leading entry of row 3.

$$\begin{bmatrix} 1 & -3 & 4 & -3 & 0 & -3 \\ 0 & 1 & -2 & 2 & 0 & -7 \\ 0 & 0 & 0 & 0 & 1 & 4 \end{bmatrix}$$

>STEP 7: set row 1 to row 1 + 3 x row 2. This eliminated the entry above the leading entry of row 2.

$$\begin{bmatrix} 1 & 0 & -2 & 3 & 0 & 24 \\ 0 & 1 & -2 & 2 & 0 & -7 \\ 0 & 0 & 0 & 0 & 1 & 4 \end{bmatrix}$$

This is a reduced echelon form, since the leading entry in each non zero row is 1 and each leading 1 is the only non zero entry in its column.

From this the solution of the system can be read:

$X_1 + 0x_2 - 2x_3 + 3x_4 + 0x_5 = -24$

$0X_1 + x_2 - 2x_3 + 2x_4 + 0x_5 = -7$

$0X_1 + 0x_2 + 0x_3 + 0x_4 + x_5 = 4$

This can be re-written as

$X_1 - 2x_3 + 3x_4 = -24$

$X_2 - 2x_3 + 2x_4 = -7$

$X_5 = 4$

This equations can be solved for x_1, x_2 and x_5:

$X_1 = 2x_3 - 3x_4 - 24$

$X_2 = -2x_3 + 2x_4 - 7$

$X_5 = 4$

This is the solution of the system. The variables X_3 and X_4 can take any value and are so called free variables. The solution is valid for any X_3 and X_4.

3.9 DETERMINANT OF MATRICES

The determinant of a square matrix $A=[a_{ij}]$ is a number denoted by $|A|$ or det(A) through which important properties such as singularity can be briefly characterized. *(Determinant inverses pdf)[12]*

This number is defined as the following function of the matrix elements.

$|A| = \det(A) = \pm a_{1j}, a_{2j} \ldots . a_{njn}$

Where the column indices $j_1, j_2 \ldots j_n$ are taken from the set {1,2,...n}, with no repetitions allowed. The plus(minus) sign is taken if the permutation $(j_1 j_2 \ldots j_n)$ is even (odd) [12]

Example: 3.9.1

For a 2x2 matrix

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

Example: 3.9.2

For a 3x3 matrix

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$$

the concept of determinant is not applicable to rectangular matrices or to vectors. Thus the notation |x| for a vector X can be reserved for its magnitude (as in appendix A) without risk of confusion.

In as much as the product (example 1) contains n! Terms, the calculation of |A| from the definition is inpractical from general matrices whose order exceeds 3 or 4.

3.10 PROPERTIES OF DETERMINANTS

1. Rows and columns can be interchanged without affecting the value of a determinant consequently $|A| = |A^T|$.

2. If two rows, or two columns, are interchanged the sign of the determinant is reserved

for example $\begin{bmatrix} 3 & 4 \\ 1 & -2 \end{bmatrix} = - \begin{bmatrix} 1 & -2 \\ 3 & 4 \end{bmatrix}$

3. If a row (or column) is changed by adding to or subtracting for its corresponding elements of any other row (or column) the determinant remains unaltered.

For example $\begin{bmatrix} 3 & 4 \\ 1 & -2 \end{bmatrix} = \begin{bmatrix} 3+1 & 4-2 \\ 1 & -2 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 1 & -2 \end{bmatrix} = -10$

4. If the elements in any row (or column) have a common factor $\propto$ then the determinant equals the determinants of the corresponding matrix N which $\propto$=1,

5. multiplied by $\propto$

for example $\begin{bmatrix} 6 & 8 \\ 1 & -2 \end{bmatrix} = 2\begin{bmatrix} 3 & 4 \\ 1 & -2 \end{bmatrix} = 2$ x (-10) =-20

6. When at least one row (or column) of a matrix is a linear combination of the other rows (or column) the determinant is zero. Conversely, if the determinant is zero, then at least one row and one column are linearly dependent on the other rows and column respectively. For example,

we consider

$$\begin{bmatrix} 3 & 2 & 1 \\ 1 & 2 & -1 \\ 2 & -1 & 3 \end{bmatrix}$$

This determinant is zero because the first column is a linear combination of the second and third columns. i.e column1=column2 + column3

Similarly, there is a linear dependence between the rows which is given by the relation

$$\text{row } 1 = \frac{7}{8}\text{row2} + \frac{4}{5}\text{row } 3$$

7. The determinant of an upper triangle or lower triangle matrix is the product of the main diagonal entries

for example

$$\begin{bmatrix} 3 & 2 & 1 \\ 0 & 2 & -1 \\ 0 & 0 & 4 \end{bmatrix} = 3x2x4 = 24$$

This rule is easily verified from the definition (1) because all terms vanish except $J_1 = 1$, $J_2 = 2, \ldots J_n = n$, which is the product of the main diagonal entries. Diagonal matrices are particular case of this rule.

8. The determinant of the product of two square matrices is the product of the individual determinants $|AB| = |A||B|$. The proof requires the concept of triangular decomposition, which is covered in the remark below. This rule can be generalized to any number of factors. One immediate application is to matrix powers: $|A^2| = |A||A| = |A|^2$, and more generally $|A^n| = |A|^n$ for integers n.

9. The determinant of the transpose of a matrix is the same as that of the original matrix $|A^T|=|A|$ this rule can be directly verified from the definition of determinant, and also as direct consequence of rule 1.*(Linear algebra rank.pdf)[12]*

3.11 INVERSE OF MATRIX

The inverse of a square non-singular matrix A is represented by the symbol A^{-1} and is defined by the relation $AA^{-1} = I$

The most important application of the concept of inverse is the solution of linear systems. Suppose that, in the usual notation we have A_x=y

Pre-multiplying both sides by A^{-1} we get the inverse relationship $X=A^{-1}y$.

More generally consider the matrix equation for multiple (M) right hand side A_{nxn} X_{nxm} =Y_{nxm} which reduces to for m=1. The inverse relation that gives X as function of Y is $X=A^{-1}$. In particilar, the solution of A_x = I, is $X=A^{-1}$.Practical methods for computing inverses are based on directly solving this equation.

3.13 PROPERTIES OF INVERSE MATRICES

If A is non-singular, then so is A^{-1} and $(A^{-1})^{-1}$ =A

If A and B are non-singular matrices, then AB is non-singular and

$(AB)^{-1} = B^{-1}A^{-1}$

If A is non-singular then $(A^T)^{-1} = (A^{-1})^T$

If A and B are matrices with AB = I_n then A and B are inverse of each other.

Notice that the fourth property implies that if AB = I then BA =I

Let A,A_1 and A_2 be n x n matrices, the following statements are true:

1. If A^{-1} = B, then A (col k of B) = e_k
2. If A has an inverse matrix, then there is only one inverse matrix
3. If A_1 and A_2 have inverses, then A_1A_2 has an inverse and $(A_1A_2)^{-1} = A_1^{-1}A_2^{-1}$
4. If A has an inverse then $X = A^{-1}$ d is the solution of Ax = d and this is the

only solution.

5. The following are equivalent

   i. A has an inverse.

   ii. Det (A) is not zero

   iii. A_x = implies x=0

If C is any non-zero scalar then cA is invertible and $(cA)^{-1} = A^{-1}/c$. for n = 0,1,2…A^n is invertible and $(A^n)^{-1} = A^{-n} = (n^{-I})^{n.}$ $A^{-n} = (A^{-1})^n$

3.13 A METHOD OF COMPUTING THE INVERSE OF A MATRIX

Example 3.13.1: compute A^{-3} for the matrix

$$A= \begin{bmatrix} 2 & -3 \\ 4 & -7 \end{bmatrix}$$

Solution

First of all, we need to find the inverse of the given matrix. The method to find the inverse is only applicable for 2x2 matrices.

STEP AS FOLLOWS

1. Interchanging leading diagonal elements

-7 → 2

2 → -7

$$\begin{bmatrix} -7 & -3 \\ 4 & 2 \end{bmatrix}$$

2. Change signs of the other 2 elements

-3 → 3

4 → 4

$$\begin{bmatrix} -7 & 3 \\ -4 & 2 \end{bmatrix}$$

3. Find the determinant |A|

$\begin{bmatrix} 2 & -3 \\ 4 & 7 \end{bmatrix}$ = -14 + 12

= -2

4. Multiply result of [2] by 1|A|

5.

$A^{-1} = 1/|A| \begin{bmatrix} -7 & 3 \\ -4 & 2 \end{bmatrix} = 1/-2 \begin{bmatrix} -7 & 3 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} 35 & -1.5 \\ 2 & -1 \end{bmatrix}$

Now

$A^{-3} = (A^{-1})^3 = \begin{bmatrix} 3.5 & -15 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} 3.5 & -1.5 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} 3.5 & -1.5 \\ 2 & -1 \end{bmatrix} = \begin{bmatrix} 24.875 & -10.125 \\ 13.5 & -5.5 \end{bmatrix}$

Example 3.13.2:

let A be the 2x2 matrix $A = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix}$ show that A has no inverse.

Solution :

An inverse for A must be a 2x2 matrix

B=$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that AB =BA =I. if such a matrix B exists, it must satisfy the following equation

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+2c & b+2d \\ 3a+6c & 3b+6d \end{bmatrix}$$

The proceeding equation requires that.

A+ 2c = 1 and 3a +6c = 0

Which is clearly impossible, so we can conclude that A has no inverse.

CHAPTER FOUR

4.0 INTRODUCTION:

Matrices are used in many areas. In this chapter we will be considering its application to Cryptography, Economics and System of Linear Equations.

4.1 APPLICATIONS OF MATRICES TOCRYPTOGRAPHY

Cryptography is concerned with keeping communications private. Indeed, the protection of sensitive communications has been the emphasis of cryptography throughout much of its history. **Encryption** is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data.

Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form.

Encryption and decryption require the use of some secret information, usually referred to as a **key**. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different.

Today governments use sophisticated methods of coding and decoding messages. One type of code, which is extremely difficult to break, makes use of a large matrix to encode a message. The receiver of the message decodes it using the inverse of the matrix. This first matrix is called the encoding matrix and its inverse is called the decoding matrix. *(Abraham S (1996)) [1].*

Cipher - A procedure that will render a message unintelligible to the recipient. Used to also recreate the original message

Plaintext - The message or information that is being encrypted.

Ciphertext - The message or information that is created after the cipher has been used. *(Alan G.(1981))[2]*

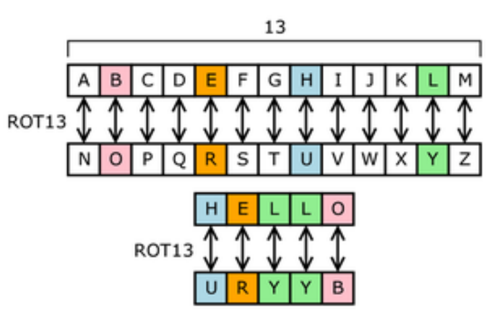
Example 4.1.1

Substitution: in cryptography a substitution cipher is a method of encoding by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution.

Substitution ciphers can be compared with transposition ciphers. In a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged. By contrast, in a substitution cipher, the units of the plaintext are retained in the same sequence in the ciphertext, but the units themselves are altered.

There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice versa.

SIMPLE SUBSTITUTION



ROT13 is a Caesar cipher, a type of substitution cipher. In ROT13, the alphabet is rotated 13 steps. Substitution of single letters separately—simple substitution—can be demonstrated by writing out the alphabet in some order to represent the substitution. This is termed a substitution

Alphabet. The cipher alphabet may be shifted or reversed (creating the Caesar and at bash ciphers, respectively) or scrambled in a more complex fashion, in which case it is called a mixed alphabet or deranged alphabet. Traditionally, mixed alphabets may be created by first writing out a keyword, removing repeated letters in it, then writing all the remaining letters in the alphabet in the usual order.

A matrix can be used as a cipher to encrypt a message. The matrix must be invertible for use in decrypting. Cipher matrix can be as simple as a 3x3 matrix composed of random integers. In order to encrypt plaintext, each character in the plaintext must be denoted with a numerical value and placed into a matrix.

These numbers can range in value, but an example is using 1-26 to represent A to Z and 27 to represent a space. This matrix is then multiplied with the cipher matrix to form a new matrix containing the cipher text message.

ENCRYPTING A MESSAGE

- Each character of the plaintext is given a numerical value as stated before.

- These values are then separated into vectors, S.T. the number of rows of each vector is equivalent to the number of rows of the cipher matrix.

Values are placed into each vector one at a time, going down a row for each value.

Once a vector is filled the next vector is created. If the last vector does not get filled by the plaintext then the remaining entries will hold the

Value for a space.

- The vectors are then augmented to form a matrix that contains the plaintext.

- The plaintext matrix is then multiplied with the cipher matrix to create the ciphertext matrix. *(Alan G. (1981))[2]*

DECRYPTING A MESSAGE

- To decrypt a ciphertext matrix the original cipher matrix must be used. The cipher matrix must be inverted in order to decrypt the ciphertext.
- This inverted cipher matrix is then multiplied with the ciphertext matrix.
- The product produces the original plaintext matrix.
- The plaintext can be found again by taking this product and splitting it back up into its separate vectors, and then converting the numbers back into their letter forms.

EXAMPLE 4.1.2

To encode the plain text

PIGUINS ARE ONE TO ONE

Step 1.

First obtain a cipher text. Taking

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

Step 2.

Now we will replace each letter with its numerical representation using 1-26 for A-Z and 27 for a space

We have, 16, 5, 14, 7, 21, 9, 14, 19 , 27, 1, 18, 5, 27, 15, 14, 5, 27, 20, 15, 27, 15, 14, 5

Step 3.

Now separating one plaintext into 3x1 vectors until the whole plain text is used

$$\begin{bmatrix}16\\5\\14\end{bmatrix}\begin{bmatrix}7\\21\\9\end{bmatrix}\begin{bmatrix}14\\19\\27\end{bmatrix}\begin{bmatrix}1\\18\\5\end{bmatrix}\begin{bmatrix}27\\15\\14\end{bmatrix}\begin{bmatrix}5\\27\\20\end{bmatrix}\begin{bmatrix}15\\27\\15\end{bmatrix}\begin{bmatrix}14\\5\\27\end{bmatrix}$$

Step 4.

Augmenting these vectors into a plaintext matrix

$$\begin{bmatrix}16 & 7 & 14 & 1 & 27 & 5 & 15 & 14\\5 & 21 & 19 & 18 & 15 & 27 & 27 & 5\\14 & 9 & 27 & 5 & 14 & 20 & 15 & 27\end{bmatrix}$$

Step 5

Multiplying the plain text with the cipher matrix to form the encrypted matrix

$$\begin{bmatrix}-3 & -3 & -4\\0 & 1 & 1\\4 & 3 & 4\end{bmatrix} \text{x} \begin{bmatrix}16 & 7 & 14 & 1 & 27 & 5 & 15 & 14\\5 & 21 & 19 & 18 & 15 & 27 & 27 & 5\\14 & 9 & 27 & 5 & 14 & 20 & 15 & 27\end{bmatrix}$$

Step 6

The newly formed matrix contains the ciphertext

$$\begin{bmatrix} -119 & -120 & -207 & -77 & -82 & -176 & -186 & -165 \\ 19 & 30 & 46 & 23 & 29 & 47 & 42 & 32 \\ 135 & 127 & 221 & 78 & 209 & 181 & 201 & 179 \end{bmatrix}$$

DECRYPTION TECHNIQUE

To decrypt the matrix back into plaintext, multiply it by the inverse of the cipher

$$A^{-1} = \begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix} \text{x} \begin{bmatrix} -119 & -120 & -207 & -77 & -82 & -176 & -186 & -165 \\ 19 & 30 & 46 & 23 & 29 & 47 & 42 & 32 \\ 135 & 127 & 221 & 78 & 209 & 181 & 201 & 179 \end{bmatrix}$$

$$= \begin{bmatrix} 16 & 7 & 14 & 1 & 27 & 5 & 15 & 14 \\ 5 & 21 & 19 & 18 & 15 & 27 & 27 & 5 \\ 14 & 9 & 27 & 5 & 14 & 20 & 15 & 27 \end{bmatrix} \Rightarrow \begin{bmatrix} P & G & N & A & - & E & O & N \\ E & U & S & R & O & - & - & E \\ N & I & - & E & N & T & O & - \end{bmatrix}$$

Which contains the plaintext

PENGUINS ARE ONE TO ONE.

EXAMPLE 4.1.3

Encode and the message TEXT MESSAGE

SOLUTION:

Using $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ as the key

The message is then encoded using the numbers above.

T	***E***	***S***	***T***		***M***	***E***	***S***	***S***	***A***	***G***	***E***
20	**5**	**19**	**20**	**27**	**13**	**5**	**19**	**19**	**1**	**7**	**5**

The message is split up into3x1 vectors as such:

$$\begin{bmatrix}20\\5\\19\end{bmatrix}\begin{bmatrix}20\\27\\19\end{bmatrix}\begin{bmatrix}5\\19\\19\end{bmatrix}\begin{bmatrix}1\\7\\5\end{bmatrix}$$

All of the vectors can then be augmented into one matrix and multiplied by the encoding matrix,

The resulting matrix is the encoded message

$$\begin{bmatrix}-3 & -3 & -4\\0 & 1 & 1\\4 & 3 & 4\end{bmatrix}\begin{bmatrix}20 & 20 & 5 & 1\\5 & 27 & 19 & 7\\19 & 13 & 19 & 5\end{bmatrix}=\begin{bmatrix}-157 & -193 & -148 & -44\\24 & 40 & 38 & 12\\171 & 213 & 153 & 45\end{bmatrix}$$

In order to decode this message, the receiver must multiply the decoding matrix, which is simply the inverse of the encoding matrix, by the encoded matrix. The resulting matrix, when formed back into
a continuous string and returned to the original characters, represents the original message.

$$\begin{bmatrix}1 & 0 & 1\\4 & 4 & 3\\-4 & -3 & -3\end{bmatrix}\begin{bmatrix}-151 & -193 & -148 & -44\\24 & 40 & 38 & 12\\171 & 213 & 153 & 45\end{bmatrix}=\begin{bmatrix}20 & 20 & 5 & 1\\5 & 27 & 19 & 7\\19 & 13 & 19 & 5\end{bmatrix}\Rightarrow\begin{bmatrix}T & T & E & A\\E & - & S & G\\S & M & S & E\end{bmatrix}$$

Which is translated to ***TEXT MESSAGE***

4.2 APPLICATION TO ECONOMICS.

In order to understand and be able to manipulate the economy of a country or a region, one needs to come up with a certain model based on the various sectors of this economy. The Leontief model is an attempt in this direction based on the assumption that each industry in the economy has two types of demands. External demand (from outside the system) and internal demand (demand placed on one industry by another in the same system). The Leontief model represents the economy as a system of linear equations. The Leontief model was invented in the 30's by professor Wassily Leontief who developed an economic model of the united states economy by dividing into 500 economic sectors. On October 18, 1973, professor Leontief was awarded the model prize to economy for his effort. *(Leontief (2006)[11]*

4.2.1 OPEN AND CLOSE ECONOMIC SYSTEM

Close Economic system.

An economy in which no activity is conducted with outside economies. A closed economy is self-sufficient, meaning that no imports are brought in and no exports are sent out. The goal is to provide consumers with everything that they need from within the economy's borders.[11]

A closed economy is the opposite of an open economy, in which a country will conduct trade with outside regions. A closed economy does not enter into any one of the following activities;

i. It neither exports goods and services to the foreign countries nor imports goods and services from the foreign countries.
ii. It neither buy shares, debentures, bonds etc. from foreign countries nor sells shares, debenture, bonds etc. from

foreign countries nor sells shares, debentures, bonds etc.

to foreign countries

iii. It neither borrows from the foreign countries nor

The Leontief Closed Model: Consider an economy consisting of *n* independent industries (or sector) $S_1 \ldots\ldots S_n$. That means that each industry consumes some of the goods produced by the other

industries, including itself (for example; a power generating plant uses some of its own power for production) we say that such an economy is **CLOSED** if it satisfies its own needs, that is no goods leave or enter these systems.

Let M_{ij} be the number of units produced by industry S_i and necessary to produce one unit of industry S_j. If P_k is the production level of industry S_k. Then M_{ij} P_j represents the number of units produced by industry S_i and consumed by industry S_j. Then the total number of units produced by industry S_i is given by

$P_1M + P_2M_{i2} + \ldots + P_nM_{in}$

In order to have a balanced economy the total production of each industry must be equal to its total consumption. This gives the linear system.

$$\begin{bmatrix} m_{11}p_1 & + & m_{12}p_2 & + & \ldots & + & m_{1n}p_n & = & p_1 \\ m_{21}p_1 & + & m_{22}p_2 & + & \ldots & + & m_{2n}p_n & = & p_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & = & \vdots \\ m_{n1}p_1 & + & m_{n2}p_2 & + & \ldots & + & m_{nn}p_n & = & p_n \end{bmatrix}$$

If

$$A = \begin{bmatrix} m_{11} & m_{12} & \ldots & m_{1n} \\ m_{21} & m_{22} & \ldots & m_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ m_{n1} & m_{n2} & \ldots & m_{nn} \end{bmatrix}$$

Then the above system can be written as *AP* = *P,* where

$$P = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}$$

A is called the **input-output matrix.**

We are then looking for a vector *P* satisfying *AP*=*P* and with non-negative components, at least one of which is positive.

EXAMPLE 4.2.1.

Suppose that the economy of a certain region depends on three industries: services, electricity and oil production.

Monitoring the operations of these three industries over a period of one year, we were able to come up with the following observations.

1. To produce 1-unit worth of service, the service industry must consume 0.3 units of its own production 0.3 units of electricity and 0.3 units of oil to run its operations.

2. To produce 1 unit of electricity, the power-generating plant must buy 0.4 units of service, 0.1 units of its own production, and 0.5 units of oil.

3. Finally, the oil production company requires 0.3 units of service, 0.6 units of electricity and 0.2 units of it own production to production to produce 1 unit of oil.

Find the production level of each of these industries in order to satisfy the external and the internal demands assuming that the above model is closed. That is, no goods leave or enter the system.

Solution;

Consider the following variables

1. P_1= production level for the service industry
2. P_2= production level for the power-generating plant (electricity)
3. P_3=production level for the oil production company

Since the model is closed, the total consumption of each industry must equal its total production. This gives the following linear system.

$$\begin{array}{ccccccc} 0.3p_1 & + & 0.3p_2 & + & 0.3p_3 & = & p_1 \\ 0.4p_1 & + & 0.1p_2 & + & 0.5p_3 & = & p_2 \\ 0.3p_1 & + & 0.6p_3 & + & 0.2p_3 & = & p_3 \end{array}$$

The input-output matrix is

$$A = \begin{bmatrix} 0.3 & 0.3 & 0.3 \\ 0.4 & 0.1 & 0.5 \\ 0.3 & 0.6 & 0.2 \end{bmatrix}$$

And the above system can be written as *(A-I) P=0.* Note that this homogeneous system has infinitely many solutions (and consequently a nontrivial solution) since each column in the coefficient matrix sums to 1. The augmented matrix of this homogeneous system is

$$\begin{bmatrix} -0.7 & 0.3 & 0.3 & 0 \\ 0.4 & -0.9 & 0.5 & 0 \\ 0.3 & 0.6 & -0.8 & 0 \end{bmatrix}$$

Which can be reduced to

$$\begin{bmatrix} 1 & 0 & -0.82 & 0 \\ 0 & 1 & -0.92 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

To solve the system, we let $P_3 = t$ (a parameter), then the general solution is

$$\begin{cases} p_1 = 0.82t \\ p_2 = 0.92t \\ p_3 = t \end{cases}$$

And as we mentioned above, the values of the variables in this system must be nonnegative in order for the model to make sense; in other words, t >-0. Taking t=100 for example would give the solution

$$\begin{cases} p_1 = 82units \\ p_2 = 92units \\ p_3 = 100units \end{cases}$$

OPEN ECONOMIC SYSTEM

Market –economy mostly free from trade barriers and where exports and imports form a large percentage of the GDP. No economy is totally open or closed in terms of trade restrictions, and all governments have varying degrees of control over movements of capital and labor. Degree of openness of an economy determines a government's freedom to pursue economic policies of its choice, and the susceptibility of the country to international economic cycles. In terms of the percentage of the GDP dependent on foreign trade, the UK is a more open economy than the US.

An open economy does enter into any one of the following activities;

i. It exports goods and services to the foreign countries and imports goods and services from the foreign countries.
ii. It buys shares, debentures, bonds etc. from foreign countries or sells shares, debenture, bonds etc. from foreign countries nor sells shares, debentures, bonds etc. to foreign countries
iii. It borrows from the foreign countries and lend to other countries

The Leontief open model: The first Leontief model treats the case where no goods leave or enter the economy, but in reality, this does not happen very often. Usually, a certain economy has to satisfy an outside demand, for example, from bodies like the government agencies. In this case, let d_i be the demand from the i^{th} outside industry, P_i and M_{ij} be as in the closed model above, then

$$P_i = m_{ij} + m_{12}p_2 + \ldots. + m_{in}p_n + d_i$$

For each I, this gives the following linear system (written in a matrix form):

$$P = AP + d$$

Where *P* and *A* are as above and

$$d = \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{bmatrix}$$

Is d ***demand vector.***

One way to solve this linear system is

$$P = AP + d \rightarrow (I\text{-}A)\, P = d \rightarrow P = (I\text{-}A)^{-1} d \qquad (*)$$

Of course, we require here that the matrix *I-A* be invertible, which might not be always the case. If, in addition, $(I\text{-}A)^{-1}$ has nonnegative entries, then the components of the vector *P* are nonnegative and therefore they are acceptable as solutions for this model. We say in this case that the matrix *A* is **Productive.**

Example 4.2.2.

Consider an open economy with three industries: coal-mining operation, electricity-generating plant and an auto-manufacturing plant. To produce $1 of coal, the mining operation must purchase $0.1 of its own production. $0.30 of electricity and $0.1 worth of automobile. Finally, to produce $1 worth of automobile, the auto manufacturing plant must purchase $0.2 of coal, $0.5 of electricity and consume $0.1 of automobile. Assume also that during a period of one week, the economy has an exterior demand of $50,000 worth of coal, $75,000 worth of electricity, and $125,000 worth of autos. Find the production level of each of the three industries in that period of one week in order to exactly satisfy both the internal and the external demands.

Solution:

The input-output matrix of this economy is

$$A = \begin{bmatrix} 0.1 & 0.25 & 0.2 \\ 0.3 & 0.4 & 0.5 \\ 0.1 & 0.15 & 0.1 \end{bmatrix}$$

and the demand vector is

$$d = \begin{bmatrix} 50{,}000 \\ 75{,}000 \\ 125{,}000 \end{bmatrix}$$

By equation (*) above

$$P = (I\text{-}A)^{-1}d$$

Where

$$I\text{-}A = \begin{bmatrix} 0.9 & -0.25 & -0.2 \\ -0.3 & 0.6 & -0.5 \\ -0.1 & -0.15 & 0.9 \end{bmatrix}$$

Using the Gaussian-elimination technique (or the formula B^{-1}= *(1/det (B)) adj (B)),* we find that

$$(I\text{-}A)^{-1} = \begin{bmatrix} 1.464 & 0.803 & 0.771 \\ 1.007 & 2.488 & 1.606 \\ 0.330 & 0.503 & 1.464 \end{bmatrix}$$

Which gives

$$P = \begin{bmatrix} 1.464 & 0.803 & 0.711 \\ 1.007 & 2.488 & 1.606 \\ 0.330 & 0.503 & 1.464 \end{bmatrix} \begin{bmatrix} 50{,}000 \\ 75{,}000 \\ 125{,}000 \end{bmatrix} = \begin{bmatrix} 229921.59 \\ 437795.27 \\ 237401.57 \end{bmatrix}$$

So, the total output of the coal-mining operation must be \$229921.59, the total output for the electricity-generating plant is \$437795.27 and the total output for the auto-manufacturing plant is \$237401.57.

4.3 APPLICATION OF MATRICES TO SYSTEM OF LINEAR EQUATION

A linear system is called inconsistent or over determined if it does not have a solution. In other words, the set of solutions is empty. Otherwise the linear system is called consistent. If we perform elementary row operations on the augmented matrix of the system and get a matrix with one of its rows equal to (0, 0,…..0) where $C \neq 0$, then the system is inconsistent.

A linear system in three variables determines a collection of planes. The intersection point is the solution. In mathematics a system of linear equations (or linear system) is a collection of linear equations involving the same set of variables [8]

Example 4.3.1

$$3x + 2y - z = 1$$

$$2x - 2y + 4z = -2$$

$$-x + 1/2y - z = 0$$

Is a system of three equations in the three variables x, y, z.

A solution to a linear system is an assignment of numbers to the variables such that all the equations are simultaneously satisfied. A solution to the system above is given by

$$x = 1$$

$$y = 2$$

$$z = -2$$

Since it makes all three equations valid. The word “system” indicates that the equations are to be considered collectively, rather than individuals.

A solution of a linear is an assignment of values to the variables X_1, X_2, X_n such that each of the equations is satisfied. This set of all possible solution is called the solution set.

A linear system may behave in any one of three possible ways

1. The system has infinitely many solutions
2. The system has a single unique solution
3. The system has no solution.

4.4 SOLVING A LINEAR SYSTEM USING (ROW REDUCTION) METHOD

Example 4.4.1

Find the solution to the following system of equations

$$3x + 4y = -2$$

$$5x + 3y = 4$$

Solution

The first step is to express the above system of equations as an augmented matrix.

$$\left[\begin{array}{cc|c} 3 & 4 & -2 \\ 5 & 3 & 4 \end{array}\right]$$

Next we label the rows

$$\left[\begin{array}{cc|c} 3 & 4 & -2 \\ 5 & 3 & 4 \end{array}\right] \qquad \begin{array}{l} R_1 \\ R_2 \end{array}$$

Now we start actually reducing the matrix to row echelon form. First, we change the leading coefficient of the first row to 1.

We achieve this by multiplying R_1 by -1/3

$$\left[\begin{array}{cc|c} 1 & 4/3 & -2/3 \\ 5 & 3 & 4 \end{array}\right] \quad 1/3R_1 \qquad \begin{array}{l} R' \\ R_2 \end{array}$$

Next, we change the coefficient in the second row that lies below the leading coefficient in first row.

This is achieved by multiplying the R_2 by -1/5 and then adding the result to R_1

$$\begin{bmatrix} 1 & 4/3 & | & -2/3 \\ -1 & -3/5 & | & -4/5 \end{bmatrix}$$ -1/5 R_2

R'_1

R_2

Adding the result to R'_1

$$\begin{bmatrix} 1 & \frac{4}{3} & | & \frac{-2}{3} \\ 0 & \frac{11}{15} & | & \frac{-22}{15} \end{bmatrix}$$

R'_1

$-1/5R_2 + R'_1$ R'_2

So now our new matrix looks like this

$$\begin{bmatrix} 1 & \frac{4}{3} & | & \frac{-2}{3} \\ 0 & \frac{11}{15} & | & \frac{-22}{15} \end{bmatrix}$$

R'_1

R'_2

At this point, we re-introduce the variables into row 2 since we will now have a one variable equations

$$0x + \frac{11}{15}y = \frac{-22}{15}$$

We can solve for y from the equation above

$$Y = \frac{-22}{15}\ x\ \frac{11}{15}$$

Now that we have y, we can use back substitution to solve for x by substituting to Y in two variables equation formed from R_1'

$$x + \frac{4}{3}y = -\frac{2}{3}$$

$$X = -\frac{2}{3} - \frac{4}{3}(-2)$$

Therefore, the solution to the system of equation is

$$x = 2$$

$$y = -2$$

Example 4.4.2

Solve for x, y and z in the system of equations below

$$3x + 3y + 4z = 1$$

$$3x + 5y + 9z = 2$$

$$5x + 9y + 17z = 4$$

Solution:

Step 1: the 1st step is to turn three variables system or equations into a 3 x 4 augmented matrix.

$$\begin{bmatrix} 3 & 3 & 4 \\ 3 & 5 & 9 \\ 5 & 9 & 17 \end{bmatrix}\begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}$$

Next we label the rows of the matrix

$$\begin{bmatrix} 3 & 3 & 4 \\ 3 & 5 & 9 \\ 5 & 9 & 17 \end{bmatrix}\begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}\begin{matrix} R_1 \\ R'_1 \\ R_3 \end{matrix}$$

Since the above augmented matrix, we can't find any rows with one as the leading coefficients, we don't need to perform a row switching operation.

However, we do need to modify row 1 such that is leading coefficient is 1.

We can achieve this by multiplying row 1 by 1/3.

$$\begin{bmatrix} 1 & 1 & 4/3 \\ 3 & 5 & 9 \\ 5 & 9 & 17 \end{bmatrix} \begin{bmatrix} 1/3 \\ 2 \\ 4 \end{bmatrix} \begin{matrix} R_1 \\ R_2 \\ R \end{matrix}$$

Next we need to change all the entries below the leading coefficient of the first row to zeros.

For the second row, we can achieve this by first multiplying through by -1/3 and then adding the result to row 1

$$-\frac{1}{3} \text{x } R_2 \begin{bmatrix} 1 & 1 & 4/3 & | & 1/3 \\ -1 & -5/3 & -3 & | & -2/3 \\ 5 & 9 & 17 & | & 4 \end{bmatrix} \begin{matrix} R'_1 \\ R'_2 \\ R_3 \end{matrix}$$

Adding the result to row 1.

$$-\frac{1}{3} R_2 + R_1 \begin{bmatrix} 1 & 1 & 4/3 & | & 1/3 \\ 0 & -2/3 & -5/3 & | & -1/3 \\ 5 & 9 & 17 & | & 4 \end{bmatrix} \begin{matrix} R'_1 \\ R'_2 \\ R_3 \end{matrix}$$

We then move on to 3; here we multiply the row by -1/5 and then add the result to row 1 in order to zero out the first element.

$$-\frac{1}{5} \text{x } R_3 \begin{bmatrix} 1 & 1 & 4/3 & | & 1/3 \\ 0 & -2/3 & -5/3 & | & -1/3 \\ -1 & -9/5 & -17/5 & | & -4/5 \end{bmatrix} \begin{matrix} R'_1 \\ R'_2 \\ R_3 \end{matrix}$$

Adding the result to row 1

$$-\frac{1}{3} R_3 + R'_1 \begin{bmatrix} 1 & 1 & 4/3 & | & 1/3 \\ 0 & -2/3 & -5/3 & | & -1/3 \\ 0 & -4/5 & -31/15 & | & -7/15 \end{bmatrix} \begin{matrix} R'_1 \\ R'_2 \\ R'_3 \end{matrix}$$

We need the leading element in the second row to also be one. We obtain this result by multiplying the second row by -3/2

$$-\frac{3}{2} \text{x } R'_2 \begin{bmatrix} 1 & 1 & 4/3 & | & 1/3 \\ 0 & 1 & 5/2 & | & 1/2 \\ 0 & -4/5 & -31/15 & | & -7/15 \end{bmatrix} \begin{matrix} R'_1 \\ R''_2 \\ R'_3 \end{matrix}$$

Next we zero out the element in row three beneath the leading coefficient in row two. To achieve this, we multiply the 3rd row by 5/4.

$$\frac{5}{4} \text{x } R'_3 \begin{bmatrix} 1 & 1 & 4/3 & | & 1/3 \\ 0 & 1 & 5/2 & | & 1/2 \\ 0 & -1 & -31/12 & | & -7/12 \end{bmatrix} \begin{matrix} R''_2 \\ R'_1 \\ R'_3 \end{matrix}$$

Adding the result to row 2.

$$\frac{5}{4} R'_3 + R''_2 \begin{bmatrix} 1 & 1 & 4/3 & | & 1/3 \\ 0 & 1 & 5/2 & | & 1/2 \\ 0 & 0 & -1/12 & | & -1/12 \end{bmatrix} \begin{matrix} R'_1 \\ R''_2 \\ R''_3 \end{matrix}$$

Finally, we multiply row 3 by -12 in order to have the leading entry of the third row as one

$$-12 \text{ x } R''_3 \begin{bmatrix} 1 & 1 & 4/3 & | & 1/3 \\ 0 & 1 & 5/2 & | & 1/2 \\ 0 & 0 & 1 & | & 1 \end{bmatrix} \begin{matrix} R''_3 \\ R''_2 \\ R'_1 \end{matrix}$$

From the above matrix we solve for the variables starting with Z in the last row

$$z=1$$

Next we solve for y by substituting for z in the equation formed by the second row.

$$y + 5/2 = ½$$

$$y = ½ - 5/2$$

$$y = -2$$

Finally, we solve for x by substituting the variables of Y and Z in the equation formed by the first row

$$x + y + 4/3x = 1/3$$

$$x = 1/3 + 2 – 4/3$$

$$x = 1$$

Therefore, the solution to the system of equations is

$$x = 1$$

$$y = -2$$

$$z = 1$$

CHAPTER FIVE

5.0 SUMMARY, CONCLUSION, RECOMMENDATION

5.1 SUMMARY

Matrices are nothing but the rectangular arrangement of numbers, expressions, symbols which are arranged in columns and rows.

The numbers present in the matrix are called as entries or entities. A matrix is said to be having ‘m’ number of rows and ‘n’ number of columns.

Matrices find many applications in scientific fields and apply to practical real-life problems as well, thus making an indispensable concept for solving many practical problems.

However, this study focuses on matrices application to cryptography, Economics and system of linear equation.

In cryptography, this study has shown how matrices and its inverse can be used by a programmer to encode or encrypt a message and also to decode a message.

A message is made as a sequence of numbers in a binary format for communication and it follows code theory for solving.

Hence with the help of matrices, those equations are solved. With these encryptions only, internet functions can work, and even banks could work with transmission of sensitive and private data.

Similarly, matrices were applied to Economics in this study, which have shown how to calculate the gross domestic products in economics which eventually helps in calculating the goods production efficiently.

And lastly, its application to system of linear equations has made it easy to solve for 3 unknowns or more accurately.

5.2 CONCLUSIONS

In conclusion, this study covers focus on the application of matrices and its application to real life. Which involves Cryptography, Economics and system of linear equation. The study has shown the importance of application of matrices to these areas and also the way or step on how to apply matrices to these areas.

REFERENCES

1. Abraham S. (1966.) Elementary cryptanalysis a, a mathematical approach. Mathematical association of America, mathematical library,

2. Alan G. Konhem, (1981) cryptography: a primer New York: Wiley inheritance,

3. Anton, H and C. Rorres. (1994) Elementary linear algebra applications version, 11th edition. 4. John Wilky and sons, int.

4. Budiman Johannes, (2001) New York: springer,

5. Carlson David: Johnson, Charles R; Lay, David C; porter A. Duane (1993). The linear algebra Curriculum study Group Recommendations for the first course in linear Algebra. The college mathematics journal 24(1):41-46

6. Froelich, freeman. (1992) Contemporary precalculus through applications, NCSSM, everyday learning.

7. Jelf Christensen April (2012) find project math 2270 Grant Gustafson University of Utah.

8. Kolman, B. (1999) introductory linear algebra with applications

9. Laura Smoller, (April (2001)) UALR Department of History

10.Lay, David, C. (2006.) linear algebra and its applications, third Edition. New York: Pearson,

11. Leontief, Wassily. (2006) Input-output economics, second edition New York Oxford University press,

12. Linear Algebra: (2000) Determinant, inverses, Rank.pdf

13.Perotti (N.D) (2001) history of linear algebra. Retrieved from http//www.science.unitnith/perotti/history of linear algebra.pdf

14. Sohn, Ira, Eds. (1986) Reading input-output analysis theory and application. New York, oxford university press

15. Strang G. (1993). The fundamental theorem of linear algebra. The America mathematical monthly, 100(9), 848-855

16. Tucker A. (1993). The growing importance of linear algebra in undergraduate mathematics. The college mathematics journal.

17. Vitull:, Marie. (2012) “a brief History of linear Algebra and matrix theory” Department of mathematics. University of Oregon. Archived from the original retrieved 2014-07-08

18. Weinstein, E.W. (1995) linear algebra, from math world, a wolfram web resource http//mathworld.com/linear algebra.html.