Journal of Theoretical and Applied Information Technology
30th April 2012. Vol. 38 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NEW PERSPECTIVE ON A SINGULAR MATRIX FORMATION

[1] K. ARULMANI, [2] K.CHADRASEKHARA RAO

[1]Assistant Professor, Department of Computer Science Engineering, Srinivasa Ramanujan Centre,
SASTRA University, Kumbakonam - 612 001, India

[2]Professor, Department of Mathematics, Srinivasa Ramanujan Centre,
SASTRA University, Kumbakonam – 612 001, India

E-mail: [1]arulmani_k@src.sastra.edu , [2]kcrao@src.sastra.edu

ABSTRACT

Determinants play an important role to decide whether matrix is singular or not. It is known that when determinant of matrix is zero, the matrix is noninvertible or singular matrix. This paper presents special properties for forming singular matrix. When square matrix is formed using those properties, the resultant matrix is degenerate i.e singular matrix. Determinant of the matrix thus formed is zero except matrix of order 1 X 1 and 2 X 2 and the matrix satisfies the most of the properties of the determinant. In this paper, we have shown how matrix of order n X n can be constructed by using special properties. We subject the new matrix thus formed to various arithmetic operations (addition, subtraction and multiplication), the resultant matrices are all singular. The results of these operations show that all resultant matrices produced as result of these operations except the multiplication satisfies the special properties. Any matrix that obeys the special properties is singular and the determinant value is equal to the difference between the sums of main diagonal and off diagonal elements. This paper will help researchers construct singular matrices that can be used for providing information security solutions.

Keywords: *Singular Matrix, Determinants, Special Properties, Noninvertible, Arithmetic Operations*

1. INTRODUCTION

Most of the cryptographic system consists of encryption and decryption processes. The encryption process consists of many rounds involving transposition and substitution techniques that cause confusion and diffusion in the original text. In order to complicate intermediate rounds of encryption, we realized a need for generating a matrix at random and subject it to some intermediate processes that include transposition and substitution. It is very easy to generate an invertible matrix whose determinant value is nonzero. Instead, we wanted to construct a singular matrix of any order at random. Forming a singular matrix manually at random is a difficult process. In consequence of our research, we have simplified the process of generating a singular matrix at random.

So far as we know, no literature has dealt with generation of a singular matrix. The main idea of this work is to present special properties identified for forming a singular matrix so as to use it in the proposed research related to information security. The singular matrix formed is subject to various properties of determinant just to verify whether it has violated any of the determinant properties (see section 1.1) and basic matrix arithmetic operations (see section 3) to see whether the resultant matrix satisfies the special properties.

1.1 Definition of Determinant

For any square matrix of order 2, there is a necessary and sufficient condition for invertibility.

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

The matrix A is invertible if and only if $ad - bc \neq 0$

Journal of Theoretical and Applied Information Technology
30th April 2012. Vol. 38 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

We called this number the determinant of A. It is clear from this that we would like to have similar result for bigger matrices (meaning higher orders). There is similar notion of determinant for any square matrix, which determines whether square matrix is invertible or not. In order to generalize such notion to higher orders, it is required to study the determinant and see what kind of properties it satisfies.

Notation

The following notation is used for the determinant:

$$\text{determinant of}\begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} = \det\begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - cb$$

1.2 Properties of the Determinant

(1) Any matrix A and its transpose have the same determinant, meaning

$$\det(\mathrm{A}) = \det(\mathrm{A}^{\mathrm{T}})$$

(2) The determinant of a triangular matrix is the product of the entries on the diagonal, that is

$$\begin{vmatrix} a & b \\ 0 & d \end{vmatrix} = \begin{vmatrix} a & 0 \\ c & d \end{vmatrix} = ad$$

(3) If we interchange two rows, the determinant of the new matrix is the opposite of the old one, that is

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

(4) If we multiply one row with a constant, the determinant of the new matrix is the determinant of the old one multiplied by the constant, that is

$$\begin{vmatrix} ka & kb \\ c & d \end{vmatrix} = k\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} a & b \\ kc & kd \end{vmatrix}$$

In particular, if all the entries in one row are zero, then the determinant is zero.

(5) If we add one row to another one multiplied by a constant, the determinant of the new matrix is the same as the old one, that is

$$\begin{vmatrix} a+kc & b+kd \\ c & d \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} a & b \\ c+ka & d+kb \end{vmatrix}$$

(6) We have

$$\det(AB) = \det(A) . \det(B)$$

If A and B are similar, then

$$\det(A) = \det(B)$$

2. FORMING SINGULAR MATRIX

2.1 Special Properties

Let us consider following special properties

$a_{11} + a_{22} - a_{21} = a_{12}$
$a_{21} + a_{32} - a_{31} = a_{22}$
$a_{12} + a_{23} - a_{22} = a_{13}$
$a_{22} + a_{33} - a_{32} = a_{33}$

The determinant of any matrix constructed using above properties is zero except matrix of order (2 X 2) and (1 X 1) and the sum of elements in the two diagonals is also equal.

2.2 Theorem

Theorem *Any Matrix formed using the above special properties is singular*

Proof: Let us consider the 3 X 3matrix.

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

From special properties (see Section. 2.1), we derive

$$a_{11} - a_{12} = a_{21} - a_{22} = a_{31} - a_{32} \quad (1)$$
$$a_{12} - a_{13} = a_{22} - a_{23} = a_{32} - a_{33} \quad (2)$$

Subtracting second column from the first column

We get

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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$A=\begin{pmatrix} a_{11}-a_{12} & a_{12} & a_{13} \\ a_{11}-a_{12} & a_{22} & a_{23} \\ a_{11}-a_{12} & a_{32} & a_{33} \end{pmatrix}$$

$$\because a_{11}-a_{12}=a_{21}-a_{22}=a_{31}-a_{32}$$

Subtracting third column from the second

$$A=\begin{pmatrix} a_{11}-a_{12} & a_{12}-a_{13} & a_{13} \\ a_{11}-a_{12} & a_{22}-a_{23} & a_{23} \\ a_{11}-a_{12} & a_{32}-a_{33} & a_{33} \end{pmatrix}$$

$$A=\begin{pmatrix} a_{11}-a_{12} & a_{12}-a_{13} & a_{13} \\ a_{11}-a_{12} & a_{22}-a_{23} & a_{23} \\ a_{11}-a_{12} & a_{32}-a_{33} & a_{33} \end{pmatrix}$$

$$A=\begin{pmatrix} a_{11}-a_{12} & a_{12}-a_{13} & a_{13} \\ a_{11}-a_{12} & a_{12}-a_{13} & a_{23} \\ a_{11}-a_{12} & a_{12}-a_{13} & a_{33} \end{pmatrix}$$

$$\because a_{12}-a_{13}=a_{22}-a_{23}=a_{32}-a_{33}$$

$$A=\begin{pmatrix} 1 & 1 & a_{13} \\ 1 & 1 & a_{23} \\ 1 & 1 & a_{33} \end{pmatrix}$$

$$\det(A)=1.\begin{vmatrix} 1 & a_{23} \\ 1 & a_{33} \end{vmatrix}-1.\begin{vmatrix} 1 & a_{23} \\ 1 & a_{33} \end{vmatrix}+a_{13}.\begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix}$$

$\det(A) = a_{33} - a_{23} - (a_{33} - a_{23}) + a_{13}(1-1)$

$\det(A) = a_{33} - a_{23} - a_{33} + a_{23} + a_{13}(0)$

$\det(A) = 0$

2.3 Example matrices

The following are the simple matrices constructed by applying special properties shown under Section. 2.1

i) $\begin{pmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{pmatrix}$

ii) $\begin{pmatrix} 10 & 3 & 12 \\ 12 & 5 & 14 \\ 8 & 1 & 10 \end{pmatrix}$

iii) $\begin{pmatrix} 5 & 10 & 15 & 20 \\ 25 & 30 & 35 & 40 \\ 45 & 50 & 55 & 60 \\ 65 & 70 & 75 & 80 \end{pmatrix}$

iv) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{pmatrix}$

3. ARITHMETIC OPERATIONS

The matrices formed from the properties (see Section. 2.1) are subject to various arithmetic operations such as addition, subtraction and multiplication. Let S be a resultant matrix and A, B,. . .,N are the matrices.

3.1 Addition

$$S = A+B+C+\cdots+N$$

Then,

$$\det(S) = \det(A) + \det(B) + \cdots + \det(N) = 0.$$

S is a matrix inheriting the special properties and its determinant is zero.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1.1 Example

Let

A= $\begin{pmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{pmatrix}$ B= $\begin{pmatrix} 10 & 3 & 12 \\ 12 & 5 & 14 \\ 8 & 1 & 10 \end{pmatrix}$

S = A + B

$$S = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{pmatrix} + \begin{pmatrix} 10 & 3 & 12 \\ 12 & 5 & 14 \\ 8 & 1 & 10 \end{pmatrix}$$

$$S= \begin{pmatrix} 11 & 6 & 16 \\ 15 & 10 & 20 \\ 15 & 10 & 20 \end{pmatrix}$$ then,

det(S) = 0

3.2 Subtraction

S = A-B-C-· · ·-N

then ,

det(S) = det(A) - det(B) - det(C) -· · ·- det(N) =0.

S is a matrix obeying the special properties and its determinant is zero.

3.2.1 Example

Let

A= $\begin{pmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{pmatrix}$ B= $\begin{pmatrix} 10 & 3 & 12 \\ 12 & 5 & 14 \\ 8 & 1 & 10 \end{pmatrix}$

S = A - B

$$S = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{pmatrix} - \begin{pmatrix} 10 & 3 & 12 \\ 12 & 5 & 14 \\ 8 & 1 & 10 \end{pmatrix}$$

$$S= \begin{pmatrix} -9 & 0 & -8 \\ -9 & 0 & -8 \\ -1 & 8 & 0 \end{pmatrix}$$ then,

det(S) = 0

3.3 Multiplication

S = A x B x C x· · ·× N

then ,

det(S) =det(A)×det(B)×det(C)×· · ·×det(N) = 0

S is a singular matrix but it does not have special properties.

3.3.1 Example

Let

A= $\begin{pmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{pmatrix}$ B= $\begin{pmatrix} 10 & 3 & 12 \\ 12 & 5 & 14 \\ 8 & 1 & 10 \end{pmatrix}$

S = A X B

$$S = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{pmatrix} \text{ X } \begin{pmatrix} 10 & 3 & 12 \\ 12 & 5 & 14 \\ 8 & 1 & 10 \end{pmatrix}$$

$$S = \begin{pmatrix} 78 & 22 & 94 \\ 138 & 40 & 166 \\ 258 & 76 & 310 \end{pmatrix}$$ then,

det(S) = 0

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. APPLYING DETERMINANT PROPERTIES

This section shows the results when determinant's properties (see Section 1.1) are subject to singular matrices formed from special properties.

4.1 Property 1

Let $A = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{pmatrix}$ and $A^T = \begin{pmatrix} 1 & 3 & 7 \\ 3 & 5 & 9 \\ 4 & 6 & 10 \end{pmatrix}$

$$\begin{vmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{vmatrix} = \begin{vmatrix} 1 & 3 & 7 \\ 3 & 5 & 9 \\ 4 & 6 & 10 \end{vmatrix} = 0$$

i.e. $\det(A) = \det(A^T) = 0$

A^T preserves the special properties.

4.2 Property 3

By interchanging first and third columns of the matrix A, we get the following matrix:

$B = \begin{pmatrix} 4 & 3 & 1 \\ 6 & 5 & 3 \\ 10 & 9 & 7 \end{pmatrix}$ then,

$$|A| = |B| = 0$$

By interchanging first and third rows of the matrix A, we get the following matrix:

$C = \begin{pmatrix} 10 & 9 & 7 \\ 6 & 5 & 3 \\ 4 & 3 & 1 \end{pmatrix}$ then,

$$|A| = |C| = 0$$

4.3 Property 4

Multiplying anyone row/column or all rows/columns with a constant in the matrix A results in a singular matrix satisfying special properties.

$$\begin{vmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{vmatrix} = \begin{vmatrix} 1*2 & 3*2 & 4*2 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{vmatrix} = \begin{vmatrix} 1*2 & 3 & 4 \\ 3*2 & 5 & 6 \\ 7*2 & 9 & 10 \end{vmatrix} = 0$$

4.4 Property 5

Adding a row to another row multiplied with a constant in the matrix A yields also a singular matrix with special properties.

$$\begin{vmatrix} 1 & 3 & 4 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{vmatrix} = \begin{vmatrix} 1+3*2 & 3+5*2 & 4+6*2 \\ 3 & 5 & 6 \\ 7 & 9 & 10 \end{vmatrix} = 0$$

5. CONCLUSION

It has been observed that a matrix S of order n X n constructed from the special properties is always singular. The determinant value is zero which is equal to the difference between sums of main diagonal and off diagonal elements in the matrix S. It applies to all matrices of order greater than or equal to 3X3.

$$|S| = (a_{1,1} + a_{2,2} + ... + a_{n,n}) - (a_{1,n} + a_{2,n-1} + ... + a_{n,1}) \tag{3}$$

All matrices in the examples were tested using MAT LAB and found that all were singular. If special properties are not satisfied by a matrix, then equation (3) is not valid. See annexure-A in case of 10 ×10 matrix and 15×15 matrix. This work can be used to explore the possibilities of special properties' matrices to be used at intermediate stages in cryptographic system.

REFRENCES:

[1] David C.Lay, "Linear Algebra & its applications", Pearson Education, 2004.
[2] K.B.Datta, "Matrix and Linear Algebra", PHI, New Delhi, 2003.
[3] I.N.Herstein, "Topics in Algebra", John Wiley and Sons ,2003
[4] Derek J.S. Robinson, "A Course in Linear Algebra with Applications", Allied Publishers Ltd, 2003
[5] G.Hadley, "Linear Algebra", Narosa Publishing House, 2002

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[6] Gilbert Strang, "Linear Algebra and its applications", Thomson Learning Inc,1998
[7] David W.Lewis, "Matrix Theory", Allied Publishers Ltd, Kolkatta,1995
[8] Seymour Liprehutz,"Linear Algebra", McGraw Hill- Metric Editions, Schaum's outline series,1987
[9] Frank Ayres,JR,"Theory and Problems of Matrices", McGraw Hill- Metric Editions, Schaum's outline series,(1974)

Journal of Theoretical and Applied Information Technology
30th April 2012. Vol. 38 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ANNEXURE -A

Sample 10×10 matrix

$$\begin{pmatrix}
1 & 3 & 6 & 10 & 15 & 21 & 28 & 36 & 45 & 55 \\
4 & 6 & 9 & 13 & 18 & 24 & 31 & 39 & 48 & 58 \\
8 & 10 & 13 & 17 & 22 & 28 & 35 & 43 & 52 & 62 \\
5 & 7 & 10 & 14 & 19 & 25 & 32 & 40 & 49 & 59 \\
7 & 9 & 12 & 16 & 21 & 27 & 34 & 42 & 51 & 61 \\
3 & 5 & 8 & 12 & 17 & 23 & 30 & 38 & 47 & 57 \\
2 & 4 & 7 & 11 & 16 & 22 & 29 & 37 & 46 & 56 \\
9 & 11 & 14 & 18 & 23 & 29 & 36 & 44 & 53 & 63 \\
13 & 15 & 18 & 22 & 27 & 33 & 40 & 48 & 57 & 67 \\
21 & 23 & 26 & 30 & 35 & 41 & 48 & 56 & 65 & 75
\end{pmatrix}$$

Sample 15×15 matrix

$$\begin{pmatrix}
15 & 17 & 20 & 25 & 26 & 28 & 38 & 50 & 54 & 62 & 73 & 86 & 93 & 102 & 108 \\
3 & 5 & 8 & 13 & 14 & 16 & 26 & 38 & 42 & 50 & 61 & 74 & 81 & 90 & 96 \\
7 & 9 & 12 & 17 & 18 & 20 & 30 & 42 & 46 & 54 & 65 & 78 & 85 & 94 & 100 \\
2 & 4 & 7 & 12 & 13 & 15 & 25 & 37 & 41 & 49 & 60 & 73 & 80 & 89 & 95 \\
6 & 8 & 11 & 16 & 17 & 19 & 29 & 41 & 45 & 53 & 64 & 77 & 84 & 93 & 99 \\
9 & 11 & 14 & 19 & 20 & 22 & 32 & 44 & 48 & 56 & 67 & 80 & 87 & 96 & 102 \\
5 & 7 & 10 & 15 & 16 & 18 & 28 & 40 & 44 & 52 & 63 & 76 & 83 & 89 & 95 \\
1 & 3 & 6 & 11 & 12 & 14 & 24 & 36 & 40 & 48 & 59 & 72 & 79 & 88 & 94 \\
4 & 6 & 9 & 14 & 15 & 17 & 27 & 39 & 43 & 51 & 62 & 75 & 82 & 91 & 97 \\
11 & 13 & 16 & 21 & 22 & 24 & 34 & 46 & 50 & 58 & 69 & 82 & 89 & 98 & 104 \\
13 & 15 & 18 & 23 & 24 & 26 & 36 & 48 & 52 & 60 & 71 & 84 & 91 & 100 & 106 \\
12 & 14 & 17 & 22 & 23 & 25 & 35 & 47 & 51 & 59 & 70 & 83 & 90 & 99 & 105 \\
17 & 19 & 22 & 27 & 28 & 30 & 40 & 52 & 56 & 64 & 75 & 88 & 95 & 104 & 110 \\
21 & 23 & 26 & 31 & 32 & 34 & 44 & 56 & 60 & 68 & 79 & 92 & 99 & 108 & 114 \\
8 & 10 & 13 & 18 & 19 & 21 & 31 & 43 & 47 & 55 & 66 & 79 & 86 & 95 & 101
\end{pmatrix}$$