U.P.B. Sci. Bull., Series A, Vol. 84, Iss. 1, 2022 ISSN 1223-7027

ON SOME PROPERTIES OF SINGULAR SYMMETRIC MATRICES

Marius BREBENEL [1], Mircea SULARIA [2]

In this paper, some properties of singular symmetric matrices are investigated in relation to the rectangular matrices. New theorems are proposed which show that a product of some rectangular matrices with their transposes yield always singular square matrices of the same rank. We also give some results regarding the possibility of splitting a singular symmetric square matrix into a product of a rectangular matrix with its transpose. This paper gives thus to the researchers new keys for providing solutions needed in the fields of IT, computer engineering, statistics and information security.

Keywords: singular matrix; rank; indeterminate system; linear subspace.

1. Introduction

The subject of this paper is in connection with linear algebra [1] and specially with matrix algebra [2]. The references mentioned before are recommended to any reader interested in numerical linear algebra for applications in statistics. In the above references, one can find basic elements of linear algebra along with a sound description of many important aspects regarding theory, computations and applications of matrix algebra needed by statisticians for practical problems solving.

In general, practical problems requiring solving linear systems of equations need to ensure that the main matrix of such a system is nonsingular. Once this is done, the system can be solved using one of the methods (exact or iterative) developed along the time. This is why the properties of singular matrices are less studied. Actually, no extensive literature exists dealing for example with generating of singular matrices. However, in the last years, a special attention was paid to encryption and decryption processes used in the cryptographic systems used in information security. These processes need building of singular matrices, as it is shown in [3]. In this paper, the authors use singular matrices to determine a method for a key exchange in which two users operating an insecure channel want to agree a secret key.

[1] Assist. Prof., Department of Aerospace Sciences “Elie Carafoli”, University POLITEHNICA of Bucharest, Romania, e-mail: mariusbreb@yahoo.com

[2] Assist. Prof., Department of Mathematical Methods and Models, University POLITEHNICA of Bucharest, Romania; email: m.sularia@gmail.com

A method of generating some singular matrices is presented in [4]. The authors of this paper show that forming a singular matrix manually and randomly is a difficult task. As a consequence of their research, they have simplified the process of generating a singular matrix at random, based only on the basic properties of the determinants.

The present paper is closely related to a recent paper [6] which considers the general case of the product of rectangular matrices of some kind, not only the product of a rectangular matrix with its transpose. However, in addition about [6], in the present paper new theorems are added regarding the rank of the singular matrix and the possibility of splitting a symmetric singular matrix into a product of a rectangular matrix with its transpose and the way of finding this matrix. It will be shown that such a matrix is not unique.

2. Product of some rectangular matrices with their transposes

Let's consider a matrix $A \in M_{mn}(R)$ where $m < n$ (rectangular matrix). One attaches to this matrix the linear system:

$$AX = B \text{ , where } X \in E_n \text{ , } B \in E_m. \tag{1}$$

Since $m < n$, the system will be indeterminate (more unknowns than equations). One multiplies to the left the matrix equation (1) with the transpose of matrix *A*:

$$A^t(AX) = A^t B \quad \text{where} \quad A^t \in M_{nm}(R) \tag{2}$$

Taking into account the associativity of the matrix product, we will have:

$$\left(A^t A\right)X = A^t B \quad \text{where} \quad A^t A \in M_n(R) \tag{3}$$

In addition, the square matrix $A^t A$ will be a symmetric one:

$$\left(A^t A\right)^t = A^t \left(A^t\right)^t = A^t A. \tag{4}$$

Coming back to the system (1), let $r = \text{rank}(A)$, $r \le m$. In this case, the solution of the system can be expressed as:

$$X = c_1 V_1 + c_2 V_2 + \ldots + c_{n-r} V_{n-r} + V_B. \tag{5}$$

where $\left(V_1, V, \ldots . V_{n-r}\right)$ represents the basis of the linear space of the solutions of indeterminate system, and V_B is a constant vector. What we need to keep in mind is that the solution is not unique. On the other hand, the same solution needs to satisfy the system (3) as well, whose main matrix is a square one. Since the system is consistent and indeterminate, it follows that the square matrix A^tA must be singular and the right hand term A^tB will belong to the column space of matrix A^tA.

By considering the above reasons, we can state the following theorems:

Theorem 1: For any rectangular matrix $A \in M_{mn}(R)$ where $m > n$, the product AA^t will be a symmetric and singular square matrix.

Remark: This theorem was mentioned for the first time in [6] considering the more general case of a product of a $m \times n$ matrix and a $n \times m$ one, where a nonsymmetrical singular matrix is obtained.

Theorem 2: Let's consider the rectangular matrix $A \in M_{mn}(R)$ where $m > n$ having the rank $r \le n$. Then, the rank of matrix $AA^t \in M_m$ will be also $r = \operatorname{rank}(A) < m$.

The proofs of the above theorems are suggested by the previous considerations. For a more rigor, one can use *reductio ad absurdum*: one assumes that the square matrix AA^t is nonsingular; in this case, the system (3) will be of Cramer type, so that it will have a unique solution. But the system (3) is equivalent to (1), which is indeterminate; as such, the assumption cannot be true. The equivalence between the systems (1) and (3) provides also the proof of the theorem 2.

For the case of a column matrix, checking of the above theorems is almost straightforward:

$$A = \begin{pmatrix} a_{11} \\ a_{12} \\ \dots \\ a_{1m} \end{pmatrix}, \quad A^t = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \end{pmatrix}, \quad AA^t = \begin{pmatrix} a_{11}^2 & a_{11}a_{12} & \dots & a_{11}a_{11m} \\ a_{12}a_{11} & a_{12}^2 & \dots & a_{12}a_{1m} \\ \dots & \dots & \dots & \dots \\ a_{1m}a_{11} & a_{1m}a_{12} & \dots & a_{1m}^2 \end{pmatrix}. \tag{6}$$

One can observe easily that

$$\det\left(AA^t\right) = a_{11}a_{12}\dots a_{1m} \begin{vmatrix} a_{11} & a_{11} & \dots & a_{11} \\ a_{12} & a_{12} & \dots & a_{12} \\ \dots & \dots & \dots & \dots \\ a_{1m} & a_{1m} & \dots & a_{1m} \end{vmatrix} = 0, \ \operatorname{rank}\left(AA^t\right) = 1. \tag{7}$$

Example: Let's take the matrix $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \\ 3 & 2 \end{pmatrix}$, $A^t = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 1 & 2 \end{pmatrix}$. The product matrix AA^t will be:

$$AA^t = \begin{pmatrix} 2 & 1 \\ 1 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 & 3 \\ 1 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 3 & 8 \\ 3 & 2 & 5 \\ 8 & 5 & 13 \end{pmatrix}. \qquad (8)$$

By computing the determinant expanding upon the first row (or column), one yields:

$$\begin{aligned} \det\left(AA^t\right) &= 5 \times (2 \cdot 13 - 5 \cdot 5) - 3 \times (3 \cdot 13 - 8 \cdot 5) + 8 \times (3 \cdot 5 - 8 \cdot 2) \\ &= 5 \times 1 - 3 \times (-1) + 8 \times (-1) = 0 \end{aligned} \qquad (9)$$

which confirms the validity of theorem (1). Let's attach now the linear homogeneous system

$$\begin{pmatrix} 2 & 1 & 3 \\ 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \qquad (10)$$

which can be re-written as

$$\begin{cases} 2x + y + 3z = 0 \\ x + y + 2z = 0 \end{cases} \qquad (11)$$

The rank of the main matrix of the system (equal to the rank of matrix *A*) is 2, since

$$\det\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = 1 \neq 0 \qquad (12)$$

According to the theorem (2), the rank of the product matrix AA^t will be 2 either, which can be easily seen from (8). Considering now (*x, y*) as main unknowns, the solution of system (11) will be derived as follows:

$$z = \lambda \;\Rightarrow\; \begin{cases} 2x + y = -3\lambda \\ x + y = -2\lambda \end{cases} \;\Rightarrow\; \begin{cases} \mathrm{x} = -\lambda \\ \mathrm{y} = -\lambda \\ \mathrm{z} = \lambda \end{cases} \;\Rightarrow\; \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \lambda \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix} \qquad (13)$$

It is easy to check that the same solution simple indeterminate (13) verifies the system (3) particularized in the given example.

Remark: The product AA^t is not commutative. It is known that the matrix $A^t A \in M_n$ is nonsingular and it is used to determine the pseudo-solution of an overdetermined system. For instance, if we start from the previous matrix and consider the system

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \tag{14}$$

we can see that $\operatorname{rank}(A) = 2 \neq \operatorname{rank}(\overline{A}) = 3$ where $\overline{A} =$ augmented matrix of the system, since

$$\det\begin{pmatrix} 2 & 1 & 1 \\ 1 & 1 & 1 \\ 3 & 2 & 1 \end{pmatrix} = -1. \tag{15}$$

It follows that the system is inconsistent and we can consider only an optimum solution in the sense of least squares, which can be obtained by multiplying the system (14) at the left with the transpose of the main matrix:

$$\begin{pmatrix} 2 & 1 & 3 \\ 1 & 1 & 2 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 1 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \Rightarrow \quad \begin{pmatrix} 14 & 9 \\ 9 & 6 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 6 \\ 4 \end{pmatrix} \tag{16}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 14 & 9 \\ 9 & 6 \end{pmatrix}^{-1}\begin{pmatrix} 6 \\ 4 \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 6 & -9 \\ -9 & 14 \end{pmatrix}\begin{pmatrix} 6 \\ 4 \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 2/3 \end{pmatrix}. \tag{17}$$

3. Splitting of a symmetric singular matrix into a product of a rectangular matrix and its transpose

Theorem 3: For any square matrix $S \in M_m(R)$ symmetric and singular, there exist always factorizations of type $S = AA^t$ where *A* is a rectangular matrix of form $A \in M_{mn}(R)$ where $m > n$ and $\operatorname{rank}(A) = \operatorname{rank}(S)$.

In order to prove that, let's consider a symmetric and singular matrix $S \in M_m(R)$. In this case, it is obvious that

$$r = \operatorname{rank}(S) < m \tag{18}$$

We assume (without restricting the generality) that, by eliminating the last *m-r* rows, the square submatrix $\left(s_{ij}\right)_{i,j=\overline{1,r}}$ is nonsingular. One attaches the algebraic linear and homogeneous system

$$\begin{cases} s_{11}x_1 + s_{12}x_2 + \ldots + s_{1m}x_m = 0 \\ s_{21}x_1 + s_{22}x_2 + \ldots + s_{2m}x_m = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{r1}x_1 + s_{r2}x_2 + \ldots + s_{r,m}x_m = 0 \end{cases} \tag{19}$$

Taking $\left(x_1, x_2, \ldots, x_r\right)$ as main unknowns and denoting $x_{r+i} = \lambda_i \left(i = \overline{1, m-r}\right)$, the solution of the above homogeneous system will be:

$$\left(x_1, x_2, \ldots, x_m\right) = \sum_{i=1}^{m-r} \lambda_i V_i = \mathrm{Sp}\left\{V_1, V_2, \ldots, V_{m-r}\right\}. \tag{20}$$

The same solution needs to satisfy the following homogeneous system as well:

$$A^t X = 0_r \quad \text{where} \quad AA^t = S \quad \text{and} \quad A^t \in M_{rm}(R),\ r < m. \tag{21}$$

The problem reduces at the beginning to determine the general form of the linear and homogeneous system which admits the solution (20). The matrix of this system will be the transpose of rectangular matrix *A* that we are looking for.

Let's consider $\left(W_1, W_2, \ldots, W_r\right)$ as a basis for the orthogonal linear subspace of that one defined by (20):

$$\mathrm{Sp}\left\{W_1, W_2, \ldots, W_r\right\} = \mathrm{Sp}^{\perp}\left\{V_1, V_2, \ldots, V_{m-r}\right\} \tag{22}$$

Using these notations, the general system which admits the solution (20) can be written as:

$$\begin{cases} \left(\sum_{j=1}^{r} \lambda_{1j} W_{j1}\right) x_1 + \left(\sum_{j=1}^{r} \lambda_{1j} W_{j2}\right) x_2 + \ldots + \left(\sum_{j=1}^{r} \lambda_{1j} W_{jm}\right) x_m = 0 \\ \left(\sum_{j=1}^{r} \lambda_{2j} W_{j1}\right) x_1 + \left(\sum_{j=1}^{r} \lambda_{2j} W_{j2}\right) x_2 + \ldots + \left(\sum_{j=1}^{r} \lambda_{2j} W_{jm}\right) x_m = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \left(\sum_{j=1}^{r} \lambda_{rj} W_{j1}\right) x_1 + \left(\sum_{j=1}^{r} \lambda_{rj} W_{j2}\right) x_2 + \ldots + \left(\sum_{j=1}^{r} \lambda_{rj} W_{mj}\right) x_m = 0 \end{cases}. \tag{23}$$

The matrix of the above homogeneous system can be written symbolically:

$$A^t = \left(\sum_{j=1}^{r} \lambda_{ij} W_{jk} \right)_{\substack{i=\overline{1,r} \\ k=\overline{1,m}}} . \tag{24}$$

Applying the condition that $AA^t = S$ (where S = given), one obtains a nonlinear (quadratic) system in the coefficients λ_{ij} $(i, j = \overline{1, r})$, but which is indeterminate, as it can be observed in the following example. As such, a multitude of decompositions of type (21) can be obtained.

Example: Let's consider the matrix of the previous example:

$$S = \begin{pmatrix} 5 & 3 & 8 \\ 3 & 2 & 5 \\ 8 & 5 & 13 \end{pmatrix}, \quad S = S^t \text{ and } \det(S) = 0 . \tag{25}$$

Since $r = \operatorname{rank}(S) = 2$, one seeks a matrix $A \in M_{32}$ such that $AA^t = S$.

We are going to determine the non-trivial solution of the homogeneous system $SX = 0_3$:

$$\begin{pmatrix} 5 & 3 & 8 \\ 3 & 2 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \Rightarrow \quad \begin{cases} 5x + 3y + 8z = 0 \\ 3x + 2y + 5z = 0 \end{cases} \tag{26}$$

$$z = \lambda \quad \Rightarrow \quad \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = -\lambda \begin{pmatrix} 8 \\ 5 \end{pmatrix} \quad \Rightarrow \quad \begin{pmatrix} x \\ y \end{pmatrix} = -\lambda \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 8 \\ 5 \end{pmatrix} . \tag{27}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = -\lambda \begin{pmatrix} 2 & -3 \\ -3 & 5 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} = -\lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \lambda \begin{pmatrix} -1 \\ -1 \end{pmatrix} \tag{28}$$

whose general solution can be written as

$$(x, y, z) = \lambda(-1, -1, 1) = \operatorname{Sp}\{(-1, -1, 1)\} . \tag{29}$$

One determines further the homogeneous system which generates the orthogonal subspace of the latter one:

$$-\xi - \eta + \zeta = 0 \quad \Leftrightarrow \quad \xi + \eta - \zeta = 0 . \tag{30}$$

$$\eta = \lambda, \ \zeta = \mu \quad \Rightarrow \quad \xi = -\lambda + \mu \quad \Rightarrow \quad (\xi, \eta, \zeta) = \lambda(-1, 1, 0) + \mu(1, 0, 1) \tag{31}$$

The wanted system will be of form:

$$\begin{cases} (-\lambda_1+\mu_1)x+\lambda_1 y+\mu_1 z=0 \\ (-\lambda_2+\mu_2)x+\lambda_2 y+\mu_2 z=0 \end{cases} \Rightarrow \begin{pmatrix} -\lambda_1+\mu_1 & \lambda_1 & \mu_1 \\ -\lambda_2+\mu_2 & \lambda_2 & \mu_2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \end{pmatrix} \qquad (32)$$

The matrix A will be the transpose of the matrix of the above system:

$$A=\begin{pmatrix} -\lambda_1+\mu_1 & -\lambda_2+\mu_2 \\ \lambda_1 & \lambda_2 \\ \mu_1 & \mu_2 \end{pmatrix} \Rightarrow A^t=\begin{pmatrix} -\lambda_1+\mu_1 & \lambda_1 & \mu_1 \\ -\lambda_2+\mu_2 & \lambda_2 & \mu_2 \end{pmatrix} \qquad (33)$$

$$AA^t=\begin{pmatrix} (\lambda_1-\mu_1)^2+(\lambda_1-\mu_1)^2 & -\lambda_1^2-\lambda_2^2+\lambda_1\mu_1+\lambda_2\mu_2 & \mu_1^2+\mu_2^2-\lambda_1\mu_1-\lambda_2\mu_2 \\ -\lambda_1^2-\lambda_2^2+\lambda_1\mu_1+\lambda_2\mu_2 & \lambda_1^2+\lambda_2^2 & \lambda_1\mu_1+\lambda_2\mu_2 \\ \mu_1^2+\mu_2^2-\lambda_1\mu_1-\lambda_2\mu_2 & \lambda_1\mu_1+\lambda_2\mu_2 & \mu_1^2+\mu_2^2 \end{pmatrix}= \\ =S=\begin{pmatrix} 5 & 3 & 8 \\ 3 & 2 & 5 \\ 8 & 5 & 13 \end{pmatrix} \qquad (34)$$

Finally, the nonlinear (quadratic) algebraic system is obtained:

$$\begin{cases} \lambda_1^2+\lambda_2^2=2 \\ \mu_1^2+\mu_2^2=13 \\ \lambda_1\mu_1+\lambda_2\mu_2=5 \end{cases} \qquad (35)$$

(the other equations are equivalent).

The system thus obtained is indeterminate, since it has 3 equations with 4 unknowns.

For the particular case $(\lambda_1,\lambda_2,\mu_1,\mu_2)=(1,1,3,2)$ one finds the matrix A from (8). Another solution can be obtained if we take, for example, $\lambda_2=0$, which yields:

$$\lambda_1=\sqrt{2}\,,\ \mu_1=\frac{5}{\sqrt{2}}\,,\ \mu_2=\sqrt{13-\frac{25}{2}}=\frac{1}{\sqrt{2}}\,. \qquad (36)$$

A new factorization is found:

$$AA^t = \begin{pmatrix} \frac{3}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \sqrt{2} & 0 \\ \frac{5}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{3}{\sqrt{2}} & \sqrt{2} & \frac{5}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 5 & 3 & 8 \\ 3 & 2 & 5 \\ 8 & 5 & 13 \end{pmatrix} \tag{37}$$

Remark: If the matrix $S \in M_m(R)$ were symmetric, nonsingular and positively defined, then it would admit the well-known Choleski factorization:

$$S = LL^t . \tag{38}$$

where *L* is a lower triangular square matrix.

4. Conclusions

In this paper it was proved that a symmetric singular square matrix can be built by multiplying a rectangular matrix of form $m \times n$ where $m > n$ with its transpose and more than that, the obtained matrix has the same rank as the rectangular matrix used in the product. This result can be useful in several fields of mathematics, computer engineering and information security.

Another interesting result in this paper consists of proving the possibility of splitting a symmetric singular matrix into a product of a rectangular matrix of form $m \times n$ ($m > n$) with its transpose, which is not unique. In this case, we have the possibility to choose the appropriate product satisfying the conditions imposed by the specific application.

A forthcoming paper showing the usefulness of presented theorems is intended to be prepared by the authors, wherein applications like optimal control of discrete-time linear systems will be analyzed.

REFERENCES

[1]. *G. Strang,* Introduction to Linear Algebra (5th Edition), Wellesley – Cambridge Press, 2016.

[2]. *J. E. Gentle*, Matrix Algebra – Theory, Computations and Applications in Statistics, (2nd Edition), Springer International Publishing AG, 2017.

[3]. *D. S. Yadav, R. K. Sharma, W. Shukla,* On Applications of Singular Matrices over Finite Fields in Cryptography, InfoSecHiComNet, Security Aspects in Information Technology, (2011), pp 181–185.

[4]. *K. Arulmani, K. Chadrasekhara Rao,* New perspective on a singular matrix formation, Journal of Theoretical and Applied Information Technology, Vol. 38 No.2, pp 163-169, 2012.

[5]. *K. Arulmani, K. Chadrasekhara Rao,* Reduction Theorem on Singular Matrix with Special Properties, Int. Journal of Math. Analysis, Vol. 6, 2012, no. 36, 1791 – 1795

[6]. *M. Miteva, L. K. Lazarova, N. Stojkovik, A. Stojanova*, A way to generate singular matrix, Advances in Mathematics: Scientific Journal 9 (2020), no.7, pp 4329–4344.

[7]. *J. Araujo, J.D. Mitchell,* An elementary proof that every singular matrix is a product of idempotent matrices, Amer. Math. Monthly, 112 (7) (2005) 641-645