Songklanakarin J. Sci. Technol.
47 (1), 34–39, Jan. – Feb. 2025

http://www.sjst.psu.ac.th

Original Article

On *h*-combined matrix and its applications

Supunnee Sompong, and Jirawat Kantalo*

Department of Mathematics and Statistics, Faculty of Science and Technology, Sakon Nakhon Rajabhat University, Mueang, Sakon Nakhon, 47000 Thailand

Received: 13 December 2023; Revised: 24 October 2024; Accepted: 21 November 2024

Abstract

In this paper, we introduce a new special combined matrix H(*A*), where *A* is a nonsingular square matrix and then we discuss some properties that are related to this matrix, including its sum of rows. Additionally, we also study applications of the discussed results, showing that our results can be practically applied in many situations.

Keywords: matrix, *h*-combined matrix, Hadamard product, cryptography, real solution

1. Introduction

In recent years, the combined matrices have been widely studied by many authors. Fiedler (2010) studied the special combined matrix of *A*, which was defined as $C(A) = A \circ A^{-T}$ where ∘ is the Hadamard product of matrices. The properties of combined matrices have been studied; for example, Bru, Gassó, Giménez, and Santana (2016) studied some classes of matrices such that their combined matrices are non-negative and obtained the relation with the sign pattern of *A*. Alonso and Serrano (2019) analyzed the properties of the combined matrix associated with the almost strictly sign regular matrices.

In this work, we introduce a new combined matrix as follows:

$$H(A) = A \circ A^{-h}, \qquad (1)$$

where A^{-h} is the inverse *h*-transpose of matrix *A*, introduced by Hamza and Hussein (2015), and ∘ denotes a new product of matrices, which will be presented in Section 2.

Moreover, we discuss the properties of these matrices and apply our results to practical applications, such as cryptography and the identification of real solutions for equations. In the field of cryptography, various authors have delved into this area, presenting diverse encoding and decoding algorithms. For instance, refer to Sümeyra, Nihal, and Özgr (2019), Salman and Yassein (2019), and Khompurngson and Sompong (2023). In this work, we focus on the Affine-Hill cipher and introduce new encoding and decoding algorithms for encryption.

Additionally, one of the applications of the combined matrix $C(A)$ is finding the real solution of the equation $C(A) = \frac{1}{n} J_n$, where J_n is an n x n all-one matrix, a question first posed by Johnson and Shapiro (1986). In the study conducted by Zhang, Yang, and Cao (2000), they found the real solution of the equation $C^t(A) = \frac{1}{n} J_n$ for any positive integer t, where C^t represents the map C applied t times.

In this paper, we propose this problem. Let $K_n = [K_{i,j}]$ be an n x n matrix whose entries are defined by $K_{i,j} = (1)^{j+1}$ for $1 \le i, j \le n$. When does the equation $\mathrm{H}(A) = \frac{1}{n} K_n$ have a real solution?

We organize our work into sections as follows. In Section 2, we provide new definitions and discuss their properties. Applications are studied in Section 3, and finally, conclusions are presented in Section 4.

*Corresponding author
Email address: jirawat@snru.ac.th

2. *h*-Combined Matrix and Its Properties

First, we present definitions as follows.

Definition 2.1 Let $A=[a_{i,j}]$ and $B=[b_{i,j}]$ be $n\times m$ matrices for $1\le i\le n$, $1\le j\le m$.

A new product of matrices, denoted by $A\odot B$, is a $n\times m$ matrix given by

$$A\odot B=[a_{i,j}b_{i,m-j+1}] \tag{2}$$

Definition 2.2 Let $A=[a_{i,j}]$ be a $n\times m$ nonsingular matrix. A new combined matrix, which we call h-combined matrix, denoted by $\mathrm{H}(A)$, is defined by

$$\mathrm{H}(A),\ = A\odot A^{-h}, \tag{3}$$

where $A^h=[a_{i,j}^h]=\left[a_{(n+1-j),(n+1-i)}\right]$ is *h*-transpose and A^{-h} is the inverse of matrix A^h.

Definition 2.3 Let $P=[p_{i,j}]$ be unitary $n\times m$ matrix whose entries are defined by

$$p_{i,j}=\begin{cases}1, & \text{if } i+j=n+1;\\ 0, & \text{otherwise.}\end{cases} \tag{4}$$

By the definitions, we have the following:

1. Let $h_{i,j}$ be the entries of $\mathrm{H}(A)$, then we have

$$h_{i,j}=\frac{(-1)^{i+j}a_{i,j}M_{n-i+1,j}}{\det A}, \tag{5}$$

where $M_{i,j}$ is the minor of the entry in the i^{th} row and j^{th} column.

2. Let $A=[a_{i,j}]$ be $n\times n$ matrix. Then $AP=[a_{i,n-j+1}]$ and $PA=[a_{n-i+1,j}]$.

3. The *h*-combined matrix can be written as $\mathrm{H}(A)=A\circ A^{-h}P$.

Now, let's provide the following examples:

Example 2.4 Let *Q* be the Fibonacci matrix defined by $\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}$.

Then $Q^n=\begin{bmatrix}F_{n+1} & F_n\\ F_n & F_{n-1}\end{bmatrix}$, where F_n is the classical Fibonacci sequence.

Then, we have $\mathrm{H}(Q^n)=(-1)^n\begin{bmatrix}-F_{n+1}F_n & F_{n+1}F_n\\ F_nF_{n-1} & -F_nF_{n-1}\end{bmatrix}$.

Example 2.5 Let *A* be the nonsingular 3x3 matrix defined by $A=\begin{bmatrix}7 & 2 & 1\\ 0 & 3 & -1\\ -3 & 4 & -2\end{bmatrix}$. Then, we have $\mathrm{H}(A)=\begin{bmatrix}-35 & 14 & 21\\ 0 & -33 & 34\\ 6 & 12 & -18\end{bmatrix}$.

Next, we will present lemmas and theorems.

Lemma 2.6 Let $A=[a_{i,j}]$ and $B=[b_{i,j}]$ be $n\times n$ nonsingular matrices and $D=[d_{i,j}]$ be a $n\times n$ nonsingular diagonal matrix. We have

1. $(A\circ B)P=AP\circ BP$
2. $A^h=PA^tP$
3. $A^{-1}P=P(A^t)^{-h}$
4. $PD=D^hP$

Proof. Now, we will prove 1. – 4. by using Definitions 2.1–2.3. Then, we have

1. $(A\circ B)P=[a_{i,j}b_{i,j}]P=[a_{i,n-j+1}b_{i,n-j+1}]=[a_{i,j}]P\circ[b_{i,j}]P=AP\circ BP.$
2. We have $PA^t=[a_{n-j+1,i}]$, then $PA^tP=[a_{n-j+1,n-i+1}]=A^h.$
3. We have $(A^h)^t=(PA^tP)^t=P^tAP^t=PAP$, then $P(A^t)^{-h}=P(PAP)^{-1}=PP^{-1}A^{-1}P^{-1}=A^{-1}P.$
4. $D^hP=[d_{n-i+1,n-j+1}]P=[d_{n-i+1,j}]=PD.$

Theorem 2.7 Let $A=[a_{i,j}]$ be an $n\times n$ nonsingular matrix and $\mathrm{H}(A)=[h_{i,j}]$. The rwo sums of $\mathrm{H}(A)$ satisfy these relations.

1. If *n* is an odd integer, then the row sums of the *h*-combined matrix are

$$\sum_{j=1}^{n} h_{i,j}=\begin{cases}1, & \text{where } i=\dfrac{n+1}{2};\\ 0, & \text{otherwise.}\end{cases} \tag{6}$$

2. If *n* is an even integer, then the row sums of the *h*-combined matrix are zero, namely $\sum_{j=1}^{n} h_{i,j}=0.$

Proof. First, we calculate the sum for row $i=\dfrac{n+1}{2}$, when *n* is an odd integer. Then, we have $n=2k+1$, where *k* is a nonnegative integer. So,

$$\begin{aligned}\sum_{j=1}^{n} h_{k+1,j} &= \frac{1}{\det A}\sum_{j=1}^{n}(-1)^{k+1+j}a_{k+1,j}M_{(2k+1)-(k+1)+1,j}\\ &= \frac{1}{\det A}\sum_{j=1}^{n}(-1)^{k+1+j}a_{k+1,j}M_{k+1,j}\\ &= 1.\end{aligned}$$

We next consider the sum of elements in row i, excluding the case proven above. Since the sum by rows of H(*A*) is computed as the sum of the products of each entry in that row with the corresponding cofactors of some other rows, it is obvious that the sum by rows is zero.

Theorem 2.8 Let $A=[a_{i,j}]$ be an $n\times n$ nonsingular matrix, *D* be a nonsingular diagonal matrix, and *P* be the unitary matrix defined in (4). Then we have

1. $\mathrm{H}(A)=\mathrm{H}(AD)=\mathrm{H}(AD^{h})=\mathrm{H}(AD^{-1})=P\mathrm{H}(PA)$
2. $\mathrm{H}(AP)=\mathrm{H}(A^{-h})=\mathrm{H}(A)P$
3. $\mathrm{H}(A^{h})=P\mathrm{H}(A^{t})P=\mathrm{H}(A^{-1})P$.

Proof. We prove 1. by the following:

i. $\mathrm{H}(AD)=AD\circ(AD)^{-h}P=AD\circ A^{-h}D^{-h}P=A\circ A^{-h}D^{-h}PD=A\circ A^{-h}D^{-h}D^{h}P$
$=A\circ A^{-h}P=\mathrm{H}(A)$

ii. $\mathrm{H}(AD^{h})=AD^{h}\circ(AD^{h})^{-h}P=AD^{h}\circ A^{-h}D^{-1}P=AD^{h}\circ A^{-h}PD^{-h}=A\circ A^{-h}PD^{-h}D^{h}$
$=A\circ A^{-h}P=\mathrm{H}(A)$

iii. $\mathrm{H}(AD^{-1})=AD^{-1}\circ(AD^{-1})^{-h}P=AD^{-1}\circ A^{-h}D^{h}P=AD^{-1}\circ A^{-h}PD=A\circ A^{-h}PDD^{-1}$
$=A\circ A^{-h}P=\mathrm{H}(A)$

iv. $P\mathrm{H}(PA)=P(PA\circ(PA)^{-h}P)=A\circ PP^{-h}A^{-h}P=A\circ A^{-h}P=\mathrm{H}(A)$

Hence, $\mathrm{H}(A)=\mathrm{H}(AD)=\mathrm{H}(AD^{h})=\mathrm{H}(AD^{-1})=P\mathrm{H}(PA),$ and we prove this similarly in both 2. and 3.

Theorem 2.9 Let $A=[a_{i,j}]$ be a $n\times n$ nonsingular matrix and *D* be a nonsingular diagonal matrix. We have

1. $AD\odot A^{-h}=A\odot A^{-h}D^{h}$
2. $DA\odot A^{-h}=A\odot DA^{-h}$

Proof. We will prove 1. and 2., respectively, as follows:

1. $AD\odot A^{-h}=AD\circ A^{-h}P=A\circ A^{-h}PD=A\circ A^{-h}D^{h}P=A\odot A^{-h}D^{h}$
2. $DA\odot A^{-h}=DA\circ A^{-h}P=A\circ DA^{-h}P=A\odot DA^{-h}$.

We note that *D* is a nonsingular diagonal matrix, and consequently, D^{-1}, D^{h}, and D^{-h} are also nonsingular diagonal matrices. Therefore, it holds for D^{-1}, D^{h}, and D^{-h} in Theorem 2.9.

3. Applications

3.1 Cryptography

In this section, we focus on the Affine-Hill cipher, introducing novel encoding and decoding algorithms for encryption.

Firstly, let m be the smallest positive integer greater than the length of plain text divided by 9, and let P_i be the i^{-th} message matrix of size 3 x 3 for $1 \le i \le m$. If P_i is not suitable, zero will be added to complete message matrix. Now, we will present algorithms for encryption and decryption.

Encryption:

$$C_i \equiv P_i \mathrm{H}(A) + A \pmod{p}, \tag{7}$$

Decryption:

$$P_i \equiv (C_i - A)\mathrm{H}^{-1}(A) \pmod{p}, \tag{8}$$

where p is a prime number that is not less than the length of the plaintext, C_i is the 3 x 3 cipher text matrix, H(A) is the 3 x 3 nonsingular key matrix, and A is the shifting matrix.

3.1.1 Numerical example

Let us consider the 37-alphabet, in which A-Z correspond to the numbers 1–26, the digits 0–9 corresponds to the numbers 27–36, and the blank character is zero.

Example 3.1 We consider the plain text "CONGRATULATIONS", the matrix $A = \begin{bmatrix} 0 & -1 & 1 \\ 2 & 1 & 0 \\ 1 & 2 & -1 \end{bmatrix}$ and $P = 37$.

So, the plain text matrices P_1 and P_2 are given by

$$P_1 = \begin{bmatrix} 3 & 15 & 14 \\ 7 & 18 & 1 \\ 20 & 21 & 12 \end{bmatrix} \text{ and } \mathrm{P}_2 = \begin{bmatrix} 1 & 20 & 9 \\ 15 & 14 & 19 \\ 0 & 0 & 0 \end{bmatrix}.$$

Encryption: Firstly, we construct the key matrix H(A). So, we have $\mathrm{H}(A) = \begin{bmatrix} 0 & -2 & 2 \\ 2 & -1 & 0 \\ -1 & 4 & -3 \end{bmatrix}$. Then, we have C_1 and C_2, which are

$$C_1 \equiv P_1\mathrm{H}(A) + A \equiv \begin{bmatrix} 16 & 34 & -35 \\ 37 & -27 & 11 \\ 31 & -11 & 3 \end{bmatrix} \equiv \begin{bmatrix} 16 & 34 & 2 \\ 0 & 10 & 11 \\ 31 & 26 & 3 \end{bmatrix} \pmod{37},$$

$$C_2 \equiv P_2\mathrm{H}(A) + A \equiv \begin{bmatrix} 31 & 13 & -24 \\ 11 & 33 & -27 \\ 1 & 2 & -1 \end{bmatrix} \equiv \begin{bmatrix} 31 & 13 & 13 \\ 11 & 33 & 10 \\ 1 & 2 & 36 \end{bmatrix} \pmod{37}.$$

The cipher text is "P7B JK4ZC4MMK6JAB9" corresponding to the plain text "CONGRATULATIONS".

Decryption: We have to calculate the inverse of H(A), denoted by $\mathrm{H}^{-1}(A)$.

Then, $\mathrm{H}^{-1}(A) = \frac{1}{2}\begin{bmatrix} 3 & 2 & 2 \\ 6 & 2 & 4 \\ 7 & 2 & 4 \end{bmatrix}$. So, we have decrypted P_1 and P_2, which are

$$2P_1 \equiv 2(C_1 - A)\mathrm{H}^{-1}(A) \equiv \begin{bmatrix} 265 & 104 & 176 \\ 125 & 36 & 76 \\ 262 & 116 & 172 \end{bmatrix} \equiv \begin{bmatrix} 6 & 30 & 28 \\ 14 & 36 & 2 \\ 3 & 5 & 24 \end{bmatrix} \pmod{37}.$$

Hence, $P_1 \equiv \begin{bmatrix} 3 & 15 & 14 \\ 7 & 18 & 1 \\ 20 & 21 & 12 \end{bmatrix} \pmod{37}$. Similarly, $P_2 \equiv \begin{bmatrix} 1 & 20 & 9 \\ 15 & 14 & 19 \\ 0 & 0 & 0 \end{bmatrix} \pmod{37}$.

After decryption, the plain text is "CONGRATULATIONS".

3.2 Real solutions of $\mathrm{H}(A) = \frac{1}{n}K_n$

In this application, we have the following theorems.

Theorem 3.2 Let $A=[a_{i,j}]$ be a 2 x 2 nonsingular matrix. Then *A* is a real solution of $\mathrm{H}(A)=\frac{1}{n}K_n$ if and only if the condition holds: $-2a_{1,1}a_{1,2}=\det(A)=2a_{2,1}a_{2,2}$.

Proof. Let $A=[a_{i,j}]$ be a real solution of $\mathrm{H}(A)=\frac{1}{n}K_n$.

Then, $\mathrm{H}(A)=\frac{1}{2}K_2$, i.e., $\frac{1}{\det(A)}\begin{bmatrix}-a_{1,1}a_{1,2} & a_{1,1}a_{1,2}\\ a_{2,1}a_{2,2} & -a_{2,1}a_{2,2}\end{bmatrix}=\frac{1}{2}\begin{bmatrix}1 & -1\\ 1 & -1\end{bmatrix}$.

It follows that $-2a_{1,1}a_{1,2}=\det(A)=2a_{2,1}a_{2,2}$.

Conversely, if *A* satisfies the condition, then *A* is a real solution of $\mathrm{H}(A)=\frac{1}{n}K_n$.

Example 3.3 Let $A=\begin{bmatrix}2 & -6\\ 2 & 6\end{bmatrix}$, then we have $\mathrm{H}(A)=\frac{1}{2}\begin{bmatrix}1 & -1\\ 1 & -1\end{bmatrix}=\frac{1}{2}K_2$. So, *A* is a real solution to the equation $\mathrm{H}(A)=\frac{1}{n}K_n$.

Theorem 3.4 Let *n* be an odd integer with $n\geq 3$, and let $A=[a_{i,j}]$ be a $n\times n$ nonsingular matrix. Then, the equation $\mathrm{H}(A)=\frac{1}{n}K_n$ has no solution.

Proof. We assume that matrix *A* is the real solution of $\mathrm{H}(A)=\frac{1}{n}K_n$. According to Theorem 2.7, for *n* an odd integer, the row sums of $\mathrm{H}(A)$ are zero, except for the $\left(\frac{n+1}{2}\right)^{\text{th}}$ row. This contradicts the condition $\frac{1}{n}K_n$, where the sum of rows is nonzero for *n* as an odd integer. Therefore, the equation $\mathrm{H}(A)=\frac{1}{n}K_n$ has no solution.

3.3 Open problems

Lastly, we propose the following two open problems. First, we inquire about the existence of real solutions to the equation $\mathrm{H}(A)=\frac{1}{n}K_n$ for $n \geq 4$ when *n* is an even integer. Second, if we define a new matrix K_n, when does the equation $\mathrm{H}(A)=\frac{1}{n}K_n$ have a real solution for $n\geq 2$?

4. Conclusions

A new combined matrix, namely the *h*-combined matrix, has been proposed in this study. Moreover, some of its properties are given, such as the sum by rows and columns, as well as the relationship between the *h*-combined matrix, the diagonal matrix, and the unitary matrix.

In addition, applications are studied in various fields. First, we applied the proposed combined matrix to construct a method for encryption and decryption based on the Affine-Hill cipher. The proposed method appears to be effective and secure, but caution should be exercised because the key matrix should be a nonsingular matrix. And then, we investigated the real solution matrix of $\mathrm{H}(A)=\frac{1}{n}K_n$ for *n* a positive integer. We found the general solution of these equations for *n* = 2 and proved that there is no solution for *n* an odd integer with $n \geq 3$.

Acknowledgements

This work was supported by Sakon Nakhon Rajabhat University, Thailand Science Research and Innovation and National Science, Research and Innovation Fund (FF: Grant no.11/2566).

References

Alonso, P., & Serrano, M. L. (2019). Combined matrices of almost strictly sign regular matrices. *Journal of Computational and Applied Mathematics*, *354*, 144–151.

Bru, R., Gasśo, M. T., Gimńez, I., & Santana, M. (2016). Combined matrices of sign regular matrices. *Linear Algebra and Its Applications*, *498*, 88–98.

Fiedler, M. (2010). Notes on hilbert and cauchy matrices. *Linear Algebra and Its Applications*, *432*, 351–356.

Hamza, A. H. M., & Hussein, H. A. (2015). Construction of new types of matrices. *International Journal of Mathematics Trends and Technology*, *24*, 84–91.

Johnson, C. R., & Shapiro, H. M. (1986). Mathematical aspects of the relative gain array $A \circ A^{-T}$. *SIAM Journal on Algebraic Discrete Methods*, *7*, 627–644.

Khompurngson, K., & Sompong, S. (2023). On matrix sequences represented by negative indices pell and pell–lucas number with the decoding of lucas blocking error-correcting codes. *Discrete Mathematics, Algorithms and Applications*, *15*, 2250154.

Salman, H. S., & Yassein, H. R. (2023). TRUFT: A new public key cryptosystem based on novel FTH algebra. *International Journal of Mathematics and Computer Science*, *18*, 589–593.

Sümeyra, U. Ç. A. R., Nihal, T. A. Ş., & Özgr, N. Y. (2019). A new application to coding theory via fibonacci and lucas numbers. *Mathematical Sciences and Applications E-Notes*, *7*, 62–70.

Zhang, X., Yang, Z., & Cao, C. (2000). Real solutions of the equation $\Phi^t(A) = \frac{1}{n} J_n$. *SIAM Journal on Matrix Analysis and Applications*, *21*, 642–645.