

On the Hadamard Product of the Golden Matrices

Ayşe NALLI

Department of Mathematics, Selcuk University
42070, Campus-Konya, Turkey
aysenalli@yahoo.com

Abstract. In this paper we did a generalization of Hadamard product of Fibonacci Q^n matrix and Fibonacci Q^{-n} matrix for continuous domain. We obtained Hadamard product of the golden matrices in the terms of the symmetrical hyperbolic Fibonacci functions and investigated some properties of Hadamard product of the golden matrices.

Mathematics Subject Classification: Primary 11B25, 11B37, 11B39, Secondary 11C20

Keywords: Fibonacci Q^n matrix, Fibonacci Q^{-n} matrix, Golden matrix

1. INTRODUCTION

In the last decades the theory of Fibonacci numbers [1],[3] was complemented by the theory of the so-called *Fibonacci Q - matrix* [2],[3]. The latter is a square 2×2 *matrix* of the following form,

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

In [3] the following property of the n *th power* of the Q - *matrix* was proved

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \quad (1.1)$$

$$\det(Q^n) = F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n \quad (1.2)$$

where $n = 0, \pm 1, \pm 2, \dots$, F_{n-1} , F_n , F_{n+1} are Fibonacci numbers given with the following recurrence relation :

$$F_{n+1} = F_n + F_{n-1} \quad (1.3)$$

with the initial terms $F_1 = F_2 = 1$.

Rule (1.3) can be used to extend the sequence backwards, thus

$$F_{-n} = (-1)^{n+1} F_n .$$

In [7], represent matrix (1.1) is showed in the following form

$$Q^n = \begin{pmatrix} F_n + F_{n-1} & F_{n-1} + F_{n-2} \\ F_{n-1} + F_{n-2} & F_{n-2} + F_{n-3} \end{pmatrix} = \begin{pmatrix} F_n & F_{n-1} \\ F_{n-1} & F_{n-2} \end{pmatrix} + \begin{pmatrix} F_{n-1} & F_{n-2} \\ F_{n-2} & F_{n-3} \end{pmatrix}$$

or

$$Q^n = Q^{n-1} + Q^{n-2}.$$

It is proved in [8] the following property of the Q -matrix,

$$Q^n \cdot Q^m = Q^m \cdot Q^n = Q^{n+m}.$$

Alexey Stakhov, Ivan Tkachenko and Boris Rozin developed recently a theory of the hyperbolic Fibonacci and Lucas functions [9, 10, 11].

Let us consider so-called symmetrical hyperbolic Fibonacci functions introduced in [11].

Symmetrical hyperbolic Fibonacci sine :

$$sFs(x) = \frac{\tau^x - \tau^{-x}}{\sqrt{5}} \quad (1.4)$$

Symmetrical hyperbolic Fibonacci cosine :

$$cFs(x) = \frac{\tau^x + \tau^{-x}}{\sqrt{5}} \quad (1.5)$$

where $\tau = \frac{1+\sqrt{5}}{2}$ (the Golden Proportion).

The symmetrical hyperbolic Fibonacci functions are connected to the Fibonacci numbers by the following correlations:

$$F_n = \begin{cases} sFs(n), & \text{for } n = 2k \\ cFs(n), & \text{for } n = 2k + 1 \end{cases} \quad (1.6)$$

It was proved in [11] that the following identities connect the symmetrical hyperbolic Fibonacci functions.

$$[sFs(x)]^2 - cFs(x+1)cFs(x-1) = -1 \quad (1.7)$$

$$[cFs(x)]^2 - sFs(x+1)sFs(x-1) = 1 \quad (1.8)$$

Note that the identities (1.7) and (1.8) are a generalization of the Cassini formula (1.2) for continuous domain.

Stakhov [12] developed a theory of the golden matrices that are a generalization of the matrix (1.1) for continuous domain. He defined the golden matrices in the terms of the symmetrical hyperbolic Fibonacci functions (1.4) and (1.5). The golden matrices that are the functions of the continuous variable x are the following form

$$Q^{2x} = \begin{bmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{bmatrix}, \quad (1.9)$$

$$Q^{2x+1} = \begin{bmatrix} sFs(2x+2) & cFs(2x+1) \\ cFs(2x+1) & sFs(2x) \end{bmatrix}. \quad (1.10)$$

Stakhov [12] obtained inverse matrices of (1.9) and (1.10). The inverse golden matrices that are the functions of the continuous variable x are the following form.

$$Q^{-2x} = \begin{bmatrix} cFs(2x-1) & -sFs(2x) \\ -sFs(2x) & cFs(2x+1) \end{bmatrix} \quad (1.11)$$

$$Q^{-(2x+1)} = \begin{bmatrix} -sFs(2x) & cFs(2x+1) \\ cFs(2x+1) & -sFs(2x+2) \end{bmatrix} \quad (1.12)$$

Furthermore, in [12] the golden matrices were used for creation of a new kind of cryptography called the golden cryptography.

We defined the matrix $Q^n \circ Q^{-n}$, Hadamard product of Fibonacci Q^n matrix and Fibonacci Q^{-n} matrix and investigated some properties of Hadamard product of Fibonacci Q^n matrix and Fibonacci Q^{-n} matrix in [14]

In this paper we did a generalization of Hadamard product of Fibonacci Q^n matrix and Fibonacci Q^{-n} matrix for continuous domain. We obtained Hadamard product of the golden matrices in the terms of the symmetrical hyperbolic Fibonacci functions (1.4) and (1.5) and investigated some properties of Hadamard product of the golden matrices.

2. THE HADAMARD PRODUCT OF GOLDEN MATRICES

Let us represent the Hadamard product of golden matrices that are the functions of the continuous variable x in following form :

$$Q^{2x} \circ Q^{-2x} = \begin{bmatrix} cFs(2x+1)cFs(2x-1) & -[sFs(2x)]^2 \\ -[sFs(2x)]^2 & cFs(2x+1)cFs(2x-1) \end{bmatrix} \quad (2.1)$$

$$Q^{2x+1} \circ Q^{-(2x+1)} = \begin{bmatrix} -sFs(2x+2)sFs(2x) & [cFs(2x+1)]^2 \\ [cFs(2x+1)]^2 & -sFs(2x+2)sFs(2x) \end{bmatrix}. \quad (2.2)$$

Let us calculate now the determinants of the matrices (2.1) and (2.2).

Theorem 1.

$$\begin{aligned} \det(Q^{2x} \circ Q^{-2x}) &= 1 + 2 [sFs(2x)]^2 \\ \det(Q^{2x+1} \circ Q^{-(2x+1)}) &= 1 - 2 [cFs(2x+1)]^2 \end{aligned}$$

Proof.

$$\begin{aligned} \det(Q^{2x} \circ Q^{-2x}) &= (cFs(2x+1)cFs(2x-1))^2 - (sFs(2x))^4 \\ &= (cFs(2x+1)cFs(2x-1) + [sFs(2x)]^2) \\ &= 1 + 2 [sFs(2x)]^2 \end{aligned}$$

and

$$\begin{aligned} \det(Q^{2x+1} \circ Q^{-(2x+1)}) &= (sFs(2x+2)sFs(2x))^2 - (cFs(2x+1))^4 \\ &= (-1) (2 [cFs(2x+1)]^2 - 1) \\ &= 1 - 2 [cFs(2x+1)]^2 \end{aligned}$$

■

Let us calculate now the inverses of the matrices (2.1) and (2.2).

Theorem 2.

$$\begin{aligned} (Q^{2x} \circ Q^{-2x})^{-1} &= \begin{bmatrix} \frac{1+[sFs(2x)]^2}{1+2[sFs(2x)]^2} & \frac{[sFs(2x)]^2}{1+2[sFs(2x)]^2} \\ \frac{[sFs(2x)]^2}{1+2[sFs(2x)]^2} & \frac{1+[sFs(2x)]^2}{1+2[sFs(2x)]^2} \end{bmatrix}, \\ (Q^{2x+1} \circ Q^{-(2x+1)})^{-1} &= \begin{bmatrix} \frac{1-[cFs(2x+1)]^2}{1-2[cFs(2x+1)]^2} & \frac{-[cFs(2x+1)]^2}{1-2[cFs(2x+1)]^2} \\ \frac{-[cFs(2x+1)]^2}{1-2[cFs(2x+1)]^2} & \frac{1-[cFs(2x+1)]^2}{1-2[cFs(2x+1)]^2} \end{bmatrix}. \end{aligned}$$

Proof.

$$adjoint(Q^{2x} \circ Q^{-2x}) = \begin{bmatrix} cFs(2x+1)cFs(2x-1) & [sFs(2x)]^2 \\ [sFs(2x)]^2 & cFs(2x+1)cFs(2x-1) \end{bmatrix}$$

By using (1.7) and Theorem 1,

$$(Q^{2x} \circ Q^{-2x})^{-1} = \begin{bmatrix} \frac{1+[sFs(2x)]^2}{1+2[sFs(2x)]^2} & \frac{[sFs(2x)]^2}{1+2[sFs(2x)]^2} \\ \frac{[sFs(2x)]^2}{1+2[sFs(2x)]^2} & \frac{1+[sFs(2x)]^2}{1+2[sFs(2x)]^2} \end{bmatrix} \tag{2.3}$$

and

$$adjoint(Q^{2x+1} \circ Q^{-(2x+1)}) = \begin{bmatrix} -sFs(2x+2).sFs(2x) & -[cFs(2x+1)]^2 \\ -[cFs(2x+1)]^2 & -sFs(2x+2).sFs(2x) \end{bmatrix}$$

By using (1.8) and Theorem 1,

$$(Q^{2x+1} \circ Q^{-(2x+1)})^{-1} = \begin{bmatrix} \frac{1-[cFs(2x+1)]^2}{1-2[cFs(2x+1)]^2} & \frac{-[cFs(2x+1)]^2}{1-2[cFs(2x+1)]^2} \\ \frac{-[cFs(2x+1)]^2}{1-2[cFs(2x+1)]^2} & \frac{1-[cFs(2x+1)]^2}{1-2[cFs(2x+1)]^2} \end{bmatrix} \tag{2.4}$$

■

3. THE GOLDEN CRYPTOGRAPHIC METHOD WITH HADAMARD PRODUCT OF THE GOLDEN MATRICES

This method is done by similar to in [12].

What we have introduced above, that is (2.1), (2.2), (2.3) and (2.4), allow us to develop the following application to cryptography.

[12] Let the initial message be a digital signal, which is any sequence of real numbers

$$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, \dots \tag{3.1}$$

Separate real numbers of the sequence (3.1) are called readings. There are many examples of the digital signals (3.1). The problem of protecting the digital signal (3.1) from the hackers is solved usually with application of cryptographic methods.[12].

Consider a new cryptographic method based on the Hadamard product of golden matrices.

To this end let us choose the first four readings a_1, a_2, a_3, a_4 of (3.1) and form from them a square 2×2 matrix M :

$$M = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}. \quad (3.2)$$

Note that the initial matrix M can be considered as plaintext [13].

There are $4!$ variants (permutations) to form the matrix (3.2) from the four readings a_1, a_2, a_3, a_4 . Let us designate the i th permutation by P_i ($i = 1, 2, \dots, 24$) [12].

Then we choose the Hadamard product of golden matrices (2.1) or (2.2) as *enciphering matrices* and their inverse matrices (2.3) and (2.4) *deciphering matrices*.

Let us consider now the following encryption / decryption algorithms based on matrix multiplication by similar to in [12].

Here M is the plaintext (3.2) that is formed according to the permutation P_i ; $E_1(x), E_2(x)$ are ciphertexts; $Q^{2x} \circ Q^{-2x}$ and $Q^{2x+1} \circ Q^{-(2x+1)}$ are the *enciphering matrices* (2.1) and (2.2); $(Q^{2x} \circ Q^{-2x})^{-1}$ and $(Q^{2x+1} \circ Q^{-(2x+1)})^{-1}$ are the *deciphering matrices* (2.3) and (2.4). We can use the variable x as a cryptographic key or simply a key. This means that in dependence on the value of the key x there is an infinite number of transformation of the plaintext M into the ciphertext $E(x)$.

In general the key K consists of two parts : permutation P_i and the variable x , that is, $K = \{P, x\}$.

Encryption

$$\begin{aligned} M \times (Q^{2x} \circ Q^{-2x}) &= E_1(x) \\ M \times (Q^{2x+1} \circ Q^{-(2x+1)}) &= E_2(x) \end{aligned}$$

Description

$$\begin{aligned} E_1(x) \times (Q^{2x} \circ Q^{-2x})^{-1} &= M \\ E_2(x) \times (Q^{2x+1} \circ Q^{-(2x+1)})^{-1} &= M \end{aligned} \quad (3.3)$$

Let us prove that the cryptographic method given with (3.3) ensures one-valued transformation of the plaintext into the ciphertext E and then the ciphertext E into the plaintext M . Let us consider this transformation for the case when we choose the Hadamard product of golden matrix (2.1) as the enciphering matrix. For the given value of the cryptographic key $x = x_1$ the golden encryption with Hadamard product of golden matrices can be represented as follows:

$$M \times (Q^{2x} \circ Q^{-2x}) = \begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix} = E(x_1) \quad (3.4)$$

where

$$e_{11} = a_1 (1 + [sFs(2x_1)]^2) - a_2 [sFs(2x_1)]^2, \quad (3.5)$$

$$e_{12} = -a_1 [sFs(2x_1)]^2 + a_2 (1 + [sFs(2x_1)]^2), \tag{3.6}$$

$$e_{21} = a_3 (1 + [sFs(2x_1)]^2) - a_4 [sFs(2x_1)]^2, \tag{3.7}$$

$$e_{22} = -a_3 [sFs(2x_1)]^2 + a_4 (1 + [sFs(2x_1)]^2). \tag{3.8}$$

Let us consider the golden decryption for this case ,

$$E(x_1) \times (Q^{2x} \circ Q^{-2x})^{-1} = \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix} = D \tag{3.9}$$

where

$$d_{11} = e_{11} \left(\frac{1 + [sFs(2x_1)]^2}{1 + 2[sFs(2x_1)]^2} \right) + e_{12} \left(\frac{[sFs(2x_1)]^2}{1 + 2[sFs(2x_1)]^2} \right) \tag{3.10}$$

$$d_{12} = e_{11} \left(\frac{[sFs(2x_1)]^2}{1 + 2[sFs(2x_1)]^2} \right) + e_{12} \left(\frac{1 + [sFs(2x_1)]^2}{1 + 2[sFs(2x_1)]^2} \right) \tag{3.11}$$

$$d_{21} = e_{21} \left(\frac{1 + [sFs(2x_1)]^2}{1 + 2[sFs(2x_1)]^2} \right) + e_{22} \left(\frac{[sFs(2x_1)]^2}{1 + 2[sFs(2x_1)]^2} \right) \tag{3.12}$$

$$d_{22} = e_{21} \left(\frac{[sFs(2x_1)]^2}{1 + 2[sFs(2x_1)]^2} \right) + e_{22} \left(\frac{1 + [sFs(2x_1)]^2}{1 + 2[sFs(2x_1)]^2} \right) \tag{3.13}$$

For calculation of the matrix elements given by (3.10)-(3.13) we can use the expressions (3.5)-(3.8). Then we have

$$d_{11} = a_1, \quad d_{12} = a_2, \quad d_{21} = a_3, \quad d_{22} = a_4. \tag{3.14}$$

Thus

$$D = \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = M. \tag{3.15}$$

This means that a cryptographic method given by (3.3) ensures one-valued transformation of the initial plaintext M at the entrance of the coder into the same plaintext M at the exit of the decoder.

Let us calculate now the determinant of the cipherttexts, that is, the matrices $E_1(x)$, $E_2(x)$.

Theorem 3.

$$\det E_1(x) = \det M \cdot (1 + 2 [sFs(2x)]^2)$$

$$\det E_2(x) = \det M \cdot (1 - 2 [cFs(2x+1)]^2)$$

REFERENCES

- [1] El Naschie MS., Statistical geometry of a cantor diocretum and semiconductors, Comput. Math. Appl., 1995, 29(12),103-10.
- [2] Gould HW., A History of the Fibonacci Q-matrix and a higher-dimensional problem, The Fibonacci Quart. 1981(19),250-7.
- [3] Hoggat VE., Fibonacci and Lucas numbers, Palo Alto, CA : Houghton-Mifflin, 1969.
- [4] Horn R.A., Johnson C.A., Matrix Analysis, Cambridge University Press, New York, 1985.
- [5] Minc H., Permanents, In Encyclopaedia of Mathematics and Its Applications, Vol.6, Addison-Wesley (1978).
- [6] Stakhov A., Massingue V., Sluchenkova A., Introduction into Fibonacci coding and cryptography, Kharkov, Osnova, 1999.
- [7] Stakhov A.P., Fibonacci matrices, a generalization of the Cassini formula and a new coding theory, Chaos, Solitons and Fractals, 2006.
- [8] Stakhov OP. , A generalization of the Fibonacci Q-matrix, Rep. Nat. Acad. Sci., Ukraine, 1999(9),46-9.
- [9] Stakhov A.P., Tkachenko IS. Hyperbolic Fibonacci trigonometry, Rep. Ukr. Acad. Sci., 1993, 208(7), 9-14 [in Russian].
- [10] Stakhov A.P. , Hyperbolic Fibonacci and Lucas functions, a new mathematics for the living nature, Vinnitsa, ITI, 2003.
- [11] Stakhov A., Rozin B. , On a new class of Hyperbolic function, Chaos, Solitons and Fractals, 2004, 23, 379-89.
- [12] Stakhov A.P. , The golden matrices and a new kind of cryptography, Chaos, Solitons and Fractals, 2006.
- [13] Seberry J. , Pieprzyk J. , Cryptography, an introduction to computer security, Prentice Hall, 1989.
- [14] Nalli A. , On the Hadamard Product of Fibonacci Q^n matrix and Fibonacci Q^{-n} matrix , International Journal of Contemporary Mathematical Sciences, Vol.1, no. 13-16, 2006.
- [15] Taşı D., On the Hadamard Products of its Adjoint matrix with a square matrix, Selcuk University Journal of Science, 2000(17),43-9.

Received: October 3, 2006