TWMS J. App. Eng. Math. V.5, N.2, 2015, pp. 201-207.

ON THE HADAMARD PRODUCT OF BALANCING Q_B^n MATRIX AND BALANCING Q_B^{-n} MATRIX

PRASANTA KUMAR RAY[1], SUJATA SWAIN[2], §

Abstract. In this paper, the matrix $Q_B^n \circ Q_B^{-n}$ which is the Hadamard product of both balancing Q_B^n matrix and balancing Q_B^{-n} matrix is introduced. Some properties of the Hadamard product of these matrices are investigated. A different coding and decoding method based on the application of the Hadamard product of balancing Q_B^n matrix and balancing Q_B^{-n} matrix is also considered

Keywords: Balancing numbers, Balancers, Balancing Q-matrix, Cryptography

AMS Subject Classification: 11B 39, 11B 83, 11T 71

1. Introduction

The balancing numbers are the terms of the sequence $\{0, 1, 6, 35, 204, \ldots\}$ and their recurrence relation is given by

$$B_{n+1} = 6B_n - B_{n-1},\ n \geq 1, \tag{1}$$

with initials $B_0 = 0$ and $B_1 = 1$ [1]. Many important and useful results of these numbers and their related sequences are available in the literature. Interested reader can go through [2, 4–24]. There is another way to generate balancing numbers using powers of a matrix called as balancing Q-matrix introduced by Ray in [13]. The balancing matrix is a second order matrix whose entries are the first three balancing numbers 0, 1 and 6, and is in the form

$$Q_B = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix}.$$

In [13], he has also shown that the n^{th} power of the balancing Q-matrix is in the form

$$Q_B^n = \begin{pmatrix} B_{n+1} & -B_n \\ B_n & -B_{n-1} \end{pmatrix}, \tag{2}$$

with the determinant value 1, i.e. by Cassini formula for balancing numbers,

$$\det(Q_B^n) = B_n^2 - B_{n-1}B_{n+1} = 1. \tag{3}$$

The recurrence relation (1) can be used to extend the balancing numbers backward to get

$$B_{-n} = -B_n. \tag{4}$$

---

[1] Veer Surendra Sai University of Technology, Odisha, Burla, India.
e-mail: rayprasanta2008@gmail.com;
[2] DAV Unit-8 Bhubaneswar, India.
e-mail: sujataswn@gmail.com;
§ Manuscript received: March 11, 2014.
TWMS Journal of Applied and Engineering Mathematics, Vol.5, No.2;

We now present some basic results relating to the n^{th} power of the balancing Q-matrix, Q_B^n.

Lemma 1.1. *The balancing matrix Q_B^n is also satisfy the recurrence relation (1) of the balancing numbers, that is $Q_B^n = 6Q_B^{n-1} - Q_B^{n-2}$.*

Proof. The proof is easy. By (1), we obtain

$$\begin{aligned} Q_B^n = \begin{pmatrix} B_{n+1} & -B_n \\ B_n & -B_{n-1} \end{pmatrix} &= \begin{pmatrix} 6B_n - B_{n-1} & -6B_{n-1} + B_{n-2} \\ 6B_{n-1} - B_{n-2} & -6B_{n-2} + B_{n-3} \end{pmatrix} \\ &= 6 \begin{pmatrix} B_n & -B_{n-1} \\ B_{n-1} & -B_{n-2} \end{pmatrix} - \begin{pmatrix} B_{n-1} & -B_{n-2} \\ B_{n-2} & -B_{n-3} \end{pmatrix} \\ &= 6Q_B^{n-1} - Q_B^{n-2}, \end{aligned}$$

which completes the proof. □

Lemma 1.2. *The following property for Q_B^n is valid: $Q_B^n \cdot Q_B^m = Q_B^m \cdot Q_B^n = Q_B^{n+m}$.*

Proof. Since $B_{n+1}B_m - B_nB_{m-1} = B_{m+1}B_n - B_mB_{n-1} = B_{m+n}$ [11], we have

$$\begin{aligned} Q_B^n \cdot Q_B^m &= \begin{pmatrix} B_{n+1} & -B_n \\ B_n & -B_{n-1} \end{pmatrix} \begin{pmatrix} B_{m+1} & -B_m \\ B_m & -B_{m-1} \end{pmatrix} \\ &= \begin{pmatrix} B_{n+1}B_{m+1} - B_nB_m & -B_{n+1}B_m + B_nB_{m-1} \\ B_{m+1}B_n - B_mB_{n-1} & -B_nB_m + B_{n-1}B_{m-1} \end{pmatrix} \\ &= \begin{pmatrix} B_{n+m+1} & -B_{n+m} \\ B_{n+m} & -B_{n+m-1} \end{pmatrix} \\ &= Q_B^{n+m}. \end{aligned}$$

Other part can be shown similarly. □

In this study, we will consider the Hadamard product of balancing Q_B^n matrix and balancing Q_B^{-n} matrix denoted by $Q_B^n \circ Q_B^{-n}$, where Q_B^{-n} is the inverse of the matrix Q_B^n. We will also investigate some important properties of this product.

2. Some identities of $Q_B^n \circ Q_B^{-n}$ matrix

By virtue of (2), the Hadamard product $Q_B^n \circ Q_B^{-n}$ can be written as

$$Q_B^n \circ Q_B^{-n} = Q_B^n \circ adjQ_B^n = \begin{pmatrix} -B_{n+1}B_{n-1} & -B_n^2 \\ -B_n^2 & -B_{n+1}B_{n-1} \end{pmatrix},$$

where $adjQ_B^n$ is the adjoint of the matrix Q_B^n.

The following definition is given in [3, 12].

Definition 2.1. *Let $A = (a_{ij})$ be $n \times n$ matrix over any commutative ring. The permanent of A denoted by $per(A)$ is defined by*

$$per(A) = \sum_{\sigma} a_{1\sigma_1} a_{2\sigma_2} \dots a_{n\sigma_n},$$

where the summation extends over all one-to-one functions from $\{1, 2, ..., n\}$ to $\{1, 2, ..., n\}$.

The following are some important results on the Hadamard product $Q_B^n \circ Q_B^{-n}$.

Theorem 2.1. *For all integers n,* $\det\left(Q_B^n \circ Q_B^{-n}\right) = 1 - 2B_n^2$.

Proof. Using Definition 2.1 and the identity (3), we get

$$\begin{aligned}\det\left(Q_B^n \circ Q_B^{-n}\right) &= B_{n+1}^2 B_{n-1}^2 - B_n^4 \\ &= (B_{n+1}B_{n-1} - B_n^2)(B_{n+1}B_{n-1} + B_n^2) \\ &= -per(Q_B^n) \\ &= 1 - 2B_n^2,\end{aligned}$$

which ends the proof. □

The following corollary is an immediate consequence of Theorem 2.1.

Corollary 2.1. *The trace of the matrix $Q_B^n \circ Q_B^{-n}$ is, trace* $\left(Q_B^n \circ Q_B^{-n}\right) = 2(1 - B_n^2)$.

Theorem 2.2. *If λ_1 and λ_2 are the eigenvalues of the matrix $Q_B^n \circ Q_B^{-n}$, then*
$\lambda_1 = 1,\ \lambda_2 = -per(Q_B^n)$.

Proof. Let I is the identity matrix of order 2. By (3), the characteristic equation of the matrix $Q_B^n \circ Q_B^{-n}$ is given by

$$\begin{aligned}0 &= det\left(Q_B^n \circ Q_B^{-n} - \lambda I\right) \\ &= (B_{n+1}B_{n-1} + \lambda)^2 - B_n^4 \\ &= (B_{n+1}B_{n-1} + B_n^2 + \lambda)(B_{n+1}B_{n-1} - B_n^2 + \lambda) \\ &= (\lambda + per(Q_B^n))(\lambda - 1).\end{aligned}$$

It follows that $\lambda_1 = 1$ and $\lambda_2 = -per(Q_B^n)$. □

Theorem 2.3. *The linearly independent eigenvectors corresponding to the eigenvalues $\lambda_1 = 1$ and $\lambda_2 = -per(Q_B^n)$ of the matrix $Q_B^n \circ Q_B^{-n}$ are* $X_{\lambda_1} = \begin{pmatrix}-1\\1\end{pmatrix}$ and $\mathrm{X}_{\lambda_2} = \begin{pmatrix}1\\1\end{pmatrix}$.

Proof. If λ is an eigenvalue of the matrix $Q_B^n \circ Q_B^{-n}$, then the corresponding eigenvectors $X_\lambda = \begin{pmatrix}x_1\\x_2\end{pmatrix}$ are the solution of the equation

$$\left(Q_B^n \circ Q_B^{-n} - \lambda I\right) X_\lambda = 0. \tag{5}$$

For $\lambda_1 = 1$, (5) reduces to

$$\begin{pmatrix}-B_{n+1}B_{n-1} - 1 & -B_n^2 \\ -B_n^2 & -B_{n+1}B_{n-1} - 1\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}.$$

Using (3) again, we obtain

$$\begin{pmatrix}-B_n^2 & -B_n^2 \\ -B_n^2 & -B_n^2\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix},$$

which is a system of homogenous equations. Therefore by elementary row operation, we get

$$\begin{pmatrix}-1 & -1 \\ 0 & 0\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}.$$

Since the rank of the coefficient matrix of this system is 1, there exists infinitely many solutions depending on one parameter. Therefore, the solutions of the system are $x_1 =$

$-k$, $x_2 = k$, where k is arbitrary. Hence, the linearly independent eigenvector corresponding to the eigenvalue $\lambda_1 = 1$ is equal to $[-1, 1]^T$. Similarly, For $\lambda_2 = -per(Q_B^n)$ and by (3) again, (5) reduces to

$$\begin{pmatrix} B_n^2 & -B_n^2 \\ -B_n^2 & B_n^2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

One can proceed similarly to get $x_1 = x_2 = k$, where k is arbitrary. Thus, the linearly independent eigenvector corresponding to the eigenvalue $\lambda_2 = -per(Q_B^n)$ is equal to $[1, 1]^T$. Which completes the proof. □

Remark 2.1. *Since the matrix $Q_B^n \circ Q_B^{-n}$ is symmetric, it can be diagonalize. Therefore by virtue of Theorem 2.2 and Theorem 2.3, we can write the matrix P in the form $P = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$ and notice that, $P^{-1}(Q_B^n \circ Q_B^{-n})P = diag(1, -per(Q_B^n))$.*

It is well known that, if M_n denote the class of complex $n \times n$ matrices, then the maximum column sum matrix norm on M_n is defined by

$$|||A|||_1 = \max_{1 \le j \le n} \sum_{i=1}^{n} |a_{ij}|$$

and the maximum row sum matrix norm on M_n is defined by

$$|||A|||_\infty = \max_{1 \le i \le n} \sum_{j=1}^{n} |a_{ij}|.$$

Also, the l_1 norm and the Euclidean norm or l_2 norm on M_n are respectively given by

$$||A||_1 = \sum_{1,j=1}^{n} |a_{ij}|$$

and

$$||A||_2 = \sqrt{\sum_{1,j=1}^{n} |a_{ij}|^2}.$$

The following identities are easily deduced from the definition of norms.

Theorem 2.4. *For all integers n, we have*

$$a)\ |||Q_B^n \circ Q_B^{-n}|||_1 = |||Q_B^n \circ Q_B^{-n}|||_\infty = 2B_n^2 - 1,$$
$$b)\ ||Q_B^n \circ Q_B^{-n}||_1 = 4B_n^2 - 2,$$
$$c)\ ||Q_B^n \circ Q_B^{-n}||_2 = \sqrt{4B_n^4 - 4B_n^2 + 2}.$$

Theorem 2.5. *The matrix $Q_B^n \circ Q_B^{-n}$ is invertible, and* $\left(Q_B^n \circ Q_B^{-n}\right)^{-1} = \begin{pmatrix} \frac{1-B_n^2}{1-2B_n^2} & \frac{B_n^2}{1-2B_n^2} \\ \frac{B_n^2}{1-2B_n^2} & \frac{1-B_n^2}{1-2B_n^2} \end{pmatrix}$.

Proof. By virtue of Theorem 2.2, $det\left(Q_B^n \circ Q_B^{-n}\right) = -per(Q_B^n) = 1 - 2B_n^2 \neq 0$. Therefore it is invertible, and its inverse can be easily deduced as $\left(Q_B^n \circ Q_B^{-n}\right)^{-1} = \begin{pmatrix} \frac{1-B_n^2}{1-2B_n^2} & \frac{B_n^2}{1-2B_n^2} \\ \frac{B_n^2}{1-2B_n^2} & \frac{1-B_n^2}{1-2B_n^2} \end{pmatrix}$.

This ends the proof. □

3. Balancing coding/decoding method

In this section, we consider a simple coding/decoding method based on application of the Hadamard product $Q_B^n \circ Q_B^{-n}$. Let the initial massage M is represented by a 2×2 matrix of the form

$$M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}.$$

Based on matrix multiplication, we now consider the following encryption/decryption algorithms.

Encryption:	Decryption:
$M \times (Q_B^n \circ Q_B^{-n}) = E$	$E(x) \times \left(Q_B^n \circ Q_B^{-n}\right)^{-1} = M$

We assume that the entries of M are all positive integers, i.e.
$m_1 > 0, m_2 > 0, m_3 > 0, m_4 > 0$. To describe the method, for example we select the matrix $Q_B^3 \circ Q_B^{-3}$ as the coding matrix. Then

$$Q_B^3 \circ Q_B^{-3} = \begin{pmatrix} -B_4B_2 & -B_3^2 \\ -B_3^2 & -B_4B_2 \end{pmatrix} = \begin{pmatrix} -1224 & -1225 \\ -1225 & -1224 \end{pmatrix} \tag{6}$$

and

$$\left(Q_B^3 \circ Q_B^{-3}\right)^{-1} = \begin{pmatrix} \frac{1-B_3^2}{1-2B_3^2} & \frac{B_3^2}{1-2B_3^2} \\ \frac{B_3^2}{1-2B_3^2} & \frac{1-B_3^2}{1-2B_3^2} \end{pmatrix} = \begin{pmatrix} \frac{1224}{2449} & -\frac{1225}{2449} \\ -\frac{1225}{2449} & \frac{1224}{2449} \end{pmatrix}. \tag{7}$$

Thus the balancing coding of the massage M consists in its multiplication by the direct coding matrix (6), that is

$$\begin{aligned} M \times (Q_B^3 \circ Q_B^{-3}) &= \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \begin{pmatrix} -1224 & -1225 \\ -1225 & -1224 \end{pmatrix} \\ &= \begin{pmatrix} -1224m_1 - 1225m_2 & -1225m_1 - 1224m_2 \\ -1224m_3 - 1225m_4 & -1225m_3 - 1224m_4 \end{pmatrix} \\ &= \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix} = E, \end{aligned}$$

where

$$\begin{aligned} e_1 &= -1224m_1 - 1225m_2, \\ e_2 &= -1225m_1 - 1224m_2, \\ e_3 &= -1224m_3 - 1225m_4, \\ e_4 &= -1225m_3 - 1224m_4. \end{aligned}$$

Thus, the sent code massage $E = \{e_1, e_2, e_3, e_4\}$ is now decoded by multiplying it with the inverse matrix (7) in the following way:

$$\begin{aligned} \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix} \begin{pmatrix} \frac{1224}{2449} & -\frac{1225}{2449} \\ -\frac{1225}{2449} & \frac{1224}{2449} \end{pmatrix} &= \begin{pmatrix} \frac{1224}{2449}e_1 - \frac{1225}{2449}e_2 & \frac{1224}{2449}e_3 - \frac{1225}{2449}e_4 \\ -\frac{1225}{2449}e_1 + \frac{1224}{2449}e_2 & -\frac{1225}{2449}e_3 + \frac{1224}{2449}e_4 \end{pmatrix} \\ &= \begin{pmatrix} e_1' & e_2' \\ e_3' & e_4' \end{pmatrix}. \end{aligned}$$

By simple algebraic manipulation with the help of the identities e_1, e_2, e_3 and e_4, one can easily obtain

$$\begin{pmatrix} e_1' & e_2' \\ e_3' & e_4' \end{pmatrix} = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} = M.$$

We notice that, the determinant of the code matrix E which is obtained from the multiplication of initial matrix M with the coding matrix $Q_B^n \circ Q_B^{-n}$ is given by

$$\det E = \det \left(M \times (Q_B^n \circ Q_B^{-n}) \right) = 1 - 2B_n^2,$$

for all integers n.

References

[1] Behera, A. and Panda, G.K., (1999), On the square roots of triangular numbers, 37(2), Fibonacci Quart., pp. 98-105.

[2] Bèrczes, A., Liptai, K. and Pink, I., (2010), On generalized balancing numbers, Fibonacci Quart., 48(2), pp. 121-128.

[3] Horn, R.A. and Johnson, C.A., (1985), Matrix Analysis, Cambridge University Press, New York.

[4] Keskin R. and Karaatly O., (2012), Some new properties of balancing numbers and square triangular numbers, J.Integer Seq., 15(1), pp. 12.1.4.

[5] Liptai, K., Fibonacci balancing numbers, (2004), Fibonacci Quart., 42(4), pp. 330-340.

[6] Liptai, K., Lucas balancing numbers, (2006), Acta Math. Univ. Ostrav., 14(1), pp. 43-47.

[7] Liptai, K., Luca, F., Pinter A. and Szalay L. , (2009), Generalized balancing numbers, Indag. Math.(N. S.), 20, pp. 87-100.

[8] Olajos, P., (2010), Properties of balancing, cobalancing and generalized balancing numbers, Ann. Math. Inform. , 37, pp. 125-138.

[9] Panda, G.K. and Ray P.K., (2011), Some links of balancing and cobalancing numbers with Pell and associated Pell numbers, Bull. Inst. Math. Acad. Sin. (N. S.), 6(1), pp. 41-72.

[10] Panda, G.K. and Ray P.K., (2005), Cobalancing numbers and cobalancers, Int. J. of Math. Math. Sci., 8, pp. 1189-1200.

[11] Panda, G.K. (2009), Some fascinating properties of balancing numbers, Proceeding of the Eleventh International Conference on Fibonacci Numbers and Their Applications, Congr. Numer. , 194, pp. 185-189.

[12] Patel, B.K. and Ray, P.K. (2015), The Period, rank and order of the sequence of balancing numbers modulo m, accepted in Mathematical Reports.

[13] Ray P.K., (2012), Application of Chybeshev polynomials in factorization of balancing and Lucas-balancing numbers, Bol, Soc. Parana. Mat. , 30 (2), pp. 49-56.

[14] Ray P.K., (2012), Certain matrices associated with balancing and Lucas-balancing numbers, Matematika, 28 (1), pp. 15-22.

[15] Ray P.K., (2013), Factorization of negatively subscripted balancing and Lucas-balancing numbers, Bol, Soc. Parana. Mat. , 31 (2), pp. 161-173.

[16] Ray P.K., (2012), Curious congruences for balancing numbers, Int. J. of Contemp. Math. Sci., 7 (18), pp. 881-889.

[17] Ray P.K., (2013), New identities for the common factors for balancing and Lucas-balancing numbers, Int. J. Pure Appl. Math., 85, pp. 487-494.

[18] Ray P.K., (2014), Some congruences for balancing and Lucas-balancing numbers and their applications, Integers, 14, #A8.

[19] Ray P.K., (2014), On the properties of Lucas-balancing numbers by matrix method, Sigmae, Alfenas, 3(1), pp. 1-6.

[20] Ray P.K., Parida K., (2014), Generalization of Cassini formula for balancing and Lucas-balancing numbers, Matematychni Studii., 42(1), pp. 9-14.

[21] Ray P.K., Dila G.K., Patel B.K., (2014), Application of some recurrence relations to cryptography using finite state machine *International Journal of Computer Science and Electronics Engineering (IJCSEE)*, 2 (4), pp. 220-223.

[22] Ray P.K., (2014), Identities involving the terms of a balancing-like sequence via matrices, Caspian Journal of Applied Mathematics, Ecology and Economics, 2(1), pp. 94-100.

[23] Ray P.K., (2015), Balancing and Lucas balancing sums by matrix methods, Mathematical Reports, 17(67), 2, pp. 225-233.

[24] Ray, P.K. and Patel, B.K. (2015), Uniform distribution of the sequence of balancing numbers modulo m, accepted in Uniform Distribution Theory.

Sujata Swain received her MCA degree from Biju Pattnaik University and Technology , Roukela, India and M Tech. From Berhampur University, India. She is currently working as a computer teacher in the Department of Computer Science at D.A.V. Public School, Unit-8, Bhubaneswar, India. Her research interests are in the areas of Number Theory and Cryptography, Parallel Algorithm, Artificial Intelligence and Neural Networking. She has more than two papers in her credit.

Prasanta Kumar Ray received his Ph.D. from NIT Rourkela, India and is currently working as an Associate Professor in the Department of Mathematics at Veer Surendra Sai University of Technology, Odisha, Burla, India. His research interests includes Number Theory and Cryptography. He has published more than 25 conference/journal articles.