Proyecciones (Antofagasta. On line) | vol. 39, n. 1 (2020) | pp. 135-153.

10.22199/issn.0717-6279-2020-01-0009

PROYECCIONES
Journal of Mathematics

ISSN 0717-6279 (On line)

A cryptography method based on hyperbolicbalancing and Lucas-balancing functions

Prasanta Kumar Ray[1] orcid.org/0000-0002-1208-8113

[1]Sambalpur University, School of Mathematical Sciences, Sambalpur, OR, India.
prasantamath@suniv.ac.in

Received: December 2018 | Accepted: December 2019

Abstract:

The goal is to study a new class of hyperbolic functions that unite the characteristics of the classical hyperbolic functions and the recurring balancing and Lucas-balancing numbers. These functions are indeed the extension of Binet formulas for both balancing and Lucas-balancing numbers in continuous domain. Some identities concerning hyperbolic balancing and Lucas-balancing functions are also established. Further, a new class of square matrices, a generalization of balancing Q_B*-matrices for continuous domain, is considered. These matrices indeed enable us to develop a cryptography method for secrecy purpose.*

Keywords: Balancing numbers; Lucas-balancing numbers; Hyperbolic balancing functions; Hyperbolic Lucas-balancing functions; Cryptography.

MSC (2010): 11B37; 11B39; 11Z05.

Cite this article as (IEEE citation style):

P. K. Ray, "A cryptography method based on hyperbolicbalancing and Lucas-balancing functionse of integrable functions with respect to a vector measure", *Proyecciones (Antofagasta, On line)*, vol. 39, no. 1, pp. 135-153, Feb. 2020, doi: 10.22199/issn.0717-6279-2020-01-0009. [Accessed dd-mm-yyyy].

1. Introduction

Balancing numbers were originally introduced by Behera and Panda [1] in connection with the Diophantine equation $1+2+\cdots+(n-1)=(n+1)+(n+2)+\cdots+(n+r)$, where, they call '$n$' a balancing number and 'r' a balancer corresponds to 'n'. The sequence of balancing numbers $\{B_n\}$ satisfies the recurrence relation

$$B_{n+1}=6B_n-B_{n-1}, \quad n\geq 1, \tag{1.1}$$

with $B_0=0, B_1=1$. A closely associate sequence $\{C_n\}$ of $\{B_n\}$ called as sequence of Lucas-balancing numbers satisfies the same recurrence relation as that of balancing numbers but with different initials, that is

$$C_{n+1}=6C_n-C_{n-1}, \quad n\geq 1, \tag{1.2}$$

with $C_0=1, C_1=3$. Both of the sequences $\{B_n\}$ and $\{C_n\}$ are obtained from the Pell equation $C_n^2-8B_n^2=1$ [8, 10]. For details about these number sequences, one can go through [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15].

In [18], Stakhov and Rozin presented the results of some new research on hyperbolic functions that unite the characteristics of the classical hyperbolic functions and the recurring Fibonacci and Lucas series. The simplicity and beauty of Fibonacci numbers have motivated to develop matrix cryptosystems, which are useful in digital communications, i.e., digital TV, digital telephony, digital measurement, etc. One of such cryptosystems, called as "golden cryptography" based on the golden matrices, a generalization of Fibonacci Q-matrices for continuous domain, was introduced by Stakhov [18]. Later, he improved the golden cryptography by using the golden G_k-matrices based on the k-Fibonacci hyperbolic functions [17].

In the present article, we introduce a new class of hyperbolic functions known as hyperbolic balancing and hyperbolic Lucas-balancing functions that also unite the characteristics of the classical hyperbolic functions and the recurring balancing and Lucas-balancing numbers. Several identities involving hyperbolic balancing and Lucas-balancing functions are also established. Further, a new class of square matrices, a generalization of balancing Q_B-matrices for continuous domain, is considered. This class of matrices enable us to develop a cryptography method for security purpose.

2. Hyperbolic balancing and hyperbolic Lucas-balancing functions

Behera and Panda [1] and later Panda and Ray [6] have connected balancing and Lucas-balancing numbers with balancing constants $\lambda = 3+\sqrt{8},\ \lambda^{-1} = 3-\sqrt{8}$ that are the roots of (1.1) and obtained the Binet formulas for both these numbers as

$$B_n = \frac{\lambda^n - \lambda^{-n}}{2\sqrt{8}} \quad \text{and} \quad C_n = \frac{\lambda^n + \lambda^{-n}}{2}. \tag{2.1}$$

Also it is observed that, both balancing and Lucas-balancing numbers may be extended backward. For instance, the sequences B_n and B_{-n} are of opposite sign, that is $B_n = -B_{-n}$ for all integers n. On the other hand, the sequences C_n and C_{-n} coincide for every integer n, that is $C_n = C_{-n}$.

Replacing the discrete variable n by the continuous variable x (x is any real number) in (3) and based on an analogy between (3) and the classical hyperbolic functions

$$sh(x) = \frac{e^x - e^{-x}}{2}, \qquad ch(x) = \frac{e^x + e^{-x}}{2},$$

we now define the hyperbolic balancing and hyperbolic Lucas-balancing functions as follows:

Definition 2.1. *Sine hyperbolic balancing and cosine hyperbolic balancing functions are respectively defined by*

$$shB(x) = \frac{\lambda^x - \lambda^{-x}}{2\sqrt{8}} \quad \text{and} \quad chB(x) = \frac{\lambda^x + \lambda^{-x}}{2\sqrt{8}}, \tag{2.2}$$

where $\lambda = 3+\sqrt{8}$ *and* $\lambda^{-1} = 3-\sqrt{8}$.

Definition 2.2. *Sine hyperbolic Lucas-balancing and cosine hyperbolic Lucas-balancing are defined by*

$$shC(x) = \frac{\lambda^x - \lambda^{-x}}{2} \quad \text{and} \quad chC(x) = \frac{\lambda^x + \lambda^{-x}}{2}. \tag{2.3}$$

Balancing numbers and Lucas-balancing numbers are related with sine hyperbolic balancing and cosine hyperbolic Lucas-balancing functions given by (2.1) and (2.2) in the following way.

$$shB(n) = B_n, \quad chC(n) = C_n, \tag{2.4}$$

where $n \in \mathbf{Z}$. It can also be observed that the hyperbolic balancing and Lucas-balancing functions are connected with classical hyperbolic functions by

$$\begin{aligned} shB(x) &= \frac{1}{\sqrt{8}}\, sh(\ln\lambda \cdot x);\ chB(x) = \frac{1}{\sqrt{8}}\, ch(\ln\lambda \cdot x), \\ shC(x) &= sh(\ln\lambda \cdot x);\ chC(x) = ch(\ln\lambda \cdot x). \end{aligned} \tag{2.5}$$

Further, the hyperbolic balancing and Lucas-balancing functions are connected among themselves by the relation:

$$shB(x) = \frac{1}{\sqrt{8}}\, shC(x), \quad chB(x) = \frac{1}{\sqrt{8}}\, chC(x). \tag{2.6}$$

The graphs of hyperbolic balancing and Lucas-balancing functions are shown in Fig. 1 and Fig. 2. Their graphs have a symmetrical form and are similar to the graphs of the classical hyperbolic functions. Noting that, for the point $x = 0$, the hyperbolic balancing cosine $chB(x)$ takes the value $chB(0) = \frac{1}{\sqrt{8}}$ whereas the hyperbolic Lucas-balancing cosine $chC(x)$ has the value $chC(0) = 1$.

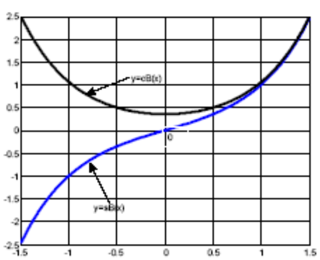

Figure 1: Balancing Function

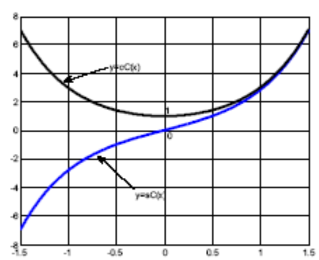

Figure 2: Lucas-Balancing Function

3. Identities involving hyperbolic balancing and hyperbolic Lucas-balancing functions

In this section, we find some mathematical properties of the hyperbolic balancing and Lucas-balancing functions resemble with that of balancing and Lucas-balancing numbers.

Theorem 3.1. *The following identities that are analogous to the recurrence relation for balancing numbers are valid for hyperbolic balancing functions too. That is,*

$$shB(x+2) = 6shB(x+1) - shB(x) \text{ and } chB(x+2) = 6chB(x+1) - chB(x).$$

Proof. By virtue of Definition 2.1 and the recurrence relation (1.1), we have

$$\begin{aligned} 6shB(x+1) - shB(x) &= 6\frac{\lambda^{x+1}-\lambda^{-x-1}}{2\sqrt{8}} - \frac{\lambda^{x}-\lambda^{-x}}{2\sqrt{8}} \\ &= \frac{\lambda^{x}(6\lambda-1)-\lambda^{-x}(6\lambda^{-1}-1)}{2\sqrt{8}} \\ &= \frac{\lambda^{x}\lambda^{2}-\lambda^{-x}\lambda^{-2}}{2\sqrt{8}} = \frac{\lambda^{x+2}-\lambda^{-x-2}}{2\sqrt{8}} = shB(x+2). \end{aligned}$$

The other identity can be shown similarly.

Theorem 3.2. *The following identities that are analogous to the recurrence relation for Lucas-balancing numbers is also valid for hyperbolic Lucas-balancing functions:*

$$shC(x+2) = 6shC(x+1) - shC(x) \text{ and } chC(x+2) = 6chC(x+1) - chC(x).$$

Proof. The proof is analogous to Theorem 3.1.

Theorem 3.3. *The identities that are similar to the Cassini identity $B_n^2 - B_{n+1}B_{n-1} = 1$ [3] is valid for hyperbolic balancing functions too. That is*

$$shB(x)^2 - shB(x+1)shB(x-1) = 1 \text{ and } chB(x)^2 - chB(x+1)chB(x-1) = -1.$$

Proof. Using Definition 2.1 and as $\lambda - \lambda^{-1} = 2\sqrt{8}$, we obtain

$$\begin{aligned} shB(x)^2 - shB(x+1)shB(x-1) &= \left(\frac{\lambda^{x}-\lambda^{-x}}{2\sqrt{8}}\right)^2 - \frac{\lambda^{x+1}-\lambda^{-x-1}}{2\sqrt{8}}\frac{\lambda^{x-1}-\lambda^{-x+1}}{2\sqrt{8}} \\ &= \frac{\lambda^{2}+\lambda^{-2}-2}{(2\sqrt{8})^2} = \frac{\left(\lambda-\lambda^{-1}\right)^2}{(2\sqrt{8})^2} = 1. \end{aligned}$$

The second identity can be proved similarly.

Theorem 3.4. *The following identity that is similar to the identity $2C_n^2 - C_{2n} = 1$ is valid for the hyperbolic Lucas-balancing functions.*

$$2[shC(x)]^2 - shC(2x) = -1 \text{ and } 2[chC(x)]^2 - chC(2x) = 1.$$

Proof. The proof is similar to Theorem 3.3.

Theorem 3.5. *The following result that is similar to the identity* $B_{n+1} - B_{n-1} = 2C_n$ *is valid for the hyperbolic balancing and Lucas-balancing functions.*

$$shB(x+1) - shB(x-1) = 2chC(x) \text{ and } chB(x+1) - chB(x-1) = 2shC(x).$$

Proof. Using Binet's formula and as $\lambda^x - \lambda^{-x} = 2\sqrt{8}$, we get the desired result.

Theorem 3.6. *The following identity that is similar to the identity* $3B_n + C_n = B_{n+1}$ *is valid for the hyperbolic balancing and Lucas-balancing functions.*

$$3shB(x) + chC(x) = shB(x+1) \text{ and } 3chB(x) + shC(x) = chB(x+1).$$

Proof. The proof is analogous to Theorem 3.5.

In Table 1 and Table 2, we indicate some known properties of balancing and Lucas-balancing numbers and the appropriate properties of the hyperbolic balancing and Lucas-balancing functions for comparison.

Table 3.1:

Identities for balancing and Lucas-balancing numbers	**Identities for hyperbolic balancing**
$B_{n+2} = 6B_{n+1} - B_n$	$sB(x+2) = 6sB(x+1) - sB(x)$
$B_n = -B_{-n}$	$sB(x) = -sB(-x)$
$B_{n+3} + 6B_n = 35B_{n+1}$	$shB(x+3) + 6shB(x) = 35shB(x+1)$
$B_n^2 - B_{n+1}B_{n-1} = 1$	$[shB(x)]^2 - shB(x+1)shB(x-1) = 1$
$B_{2n+1} = B_{n+1}^2 - B_n^2$	$chB(2x+1) = [chB(x+1)]^2 - [chB(x)]^2$
$6B_{3n} = B_{n+1}^3 - 6B_n^3 + B_{n-1}^3$	$6shB(3x) = [chB(x+1)]^3 - 6[shB(x)]^3 + [chB(x-1)]^3$
$C_{n+2} = 6C_{n+1} - C_n$	$shC(x+2) = 6shC(x+1) - shC(x)$
$C_n = C_{-n}$	$shC(x) = -shC(-x)$
$2C_n^2 - 1 = C_{2n}$	$2[shC(x)]^2 + 1 = shC(2x)$
$C_{n+1}C_{n-1} - C_n^2 = 8$	$shC(x+1)shC(x-1) - [chC(x)]^2 = -8$
$C_{n+1} - C_{n-1} = 16B_n$	$shC(x+1) - shC(x-1) = 16chB(x)$
$3C_n + 8B_n = C_{n+1}$	$3shC(x) + 8shB(x) = shC(x+1)$
$C_{n+1}^2 - C_n^2 = 8B_{2n+1}$	$[shC(x+1)]^2 - [shC(x)]^2 = 8shB(2x+1)$

Table 3.2:

Identities for balancing and Lucas-balancing numbers	**Identities for Lucas-balancing functions**
$B_{n+2} = 6B_{n+1} - B_n$	$cB(x+2) = 6cB(x+1) - cB(x)$
$B_n = -B_{-n}$	$cB(x) = -cB(-x)$
$B_{n+3} + 6B_n = 35B_{n+1}$	$chB(x+3) + 6chB(x) = 35chB(x+1)$
$B_n^2 - B_{n+1}B_{n-1} = 1$	$[chB(x)]^2 - chB(x+1)chB(x-1) = -1$
$B_{2n+1} = B_{n+1}^2 - B_n^2$	$chB(2x+1) = [shB(x+1)]^2 - [shB(x)]^2$
$6B_{3n} = B_{n+1}^3 - 6B_n^3 + B_{n-1}^3$	$6chB(3x) = [shB(x+1)]^3 - 6[chB(x)]^3 + [shB(x-1)]^3$
$C_{n+2} = 6C_{n+1} - C_n$	$chC(x+2) = 6chC(x+1) - chC(x)$
$C_n = C_{-n}$	$chC(x) = chC(-x)$
$2C_n^2 - 1 = C_{2n}$	$2[chC(x)]^2 - 1 = chC(2x)$
$C_{n+1}C_{n-1} - C_n^2 = 8$	$chC(x+1)chC(x-1) - [shC(x)]^2 = 8$
$C_{n+1} - C_{n-1} = 16B_n$	$chC(x+1) - chC(x-1) = 16shB(x)$
$3C_n + 8B_n = C_{n+1}$	$3chC(x) + 8chB(x) = chC(x+1)$
$C_{n+1}^2 - C_n^2 = 8B_{2n+1}$	$[chC(x+1)]^2 - [chC(x)]^2 = 8shB(2x+1)$

4. Some hyperbolic properties of the hyperbolic balancing and Lucas-balancing functions

The hyperbolic balancing and Lucas-balancing functions have properties that are similar to the classical hyperbolic functions.

Theorem 4.1. *The following result that is similar to the identity* $[ch(x)]^2 - [sh(x)]^2 = 1$ *is valid for the hyperbolic balancing and Lucas-balancing functions.*

$$[chC(x)]^2 - 8[shB(x)]^2 = 1 \quad \text{and} \quad [shC(x)]^2 - 8[chB(x)]^2 = -1.$$

Proof. Since $\lambda^x \lambda^{-x} = 1$, we have

$$\begin{aligned}[chC(x)]^2 - 8[shB(x)]^2 &= \left(\frac{\lambda^x+\lambda^{-x}}{2}\right)^2 - 8\left(\frac{\lambda^x-\lambda^{-x}}{2\sqrt{8}}\right)^2 \\ &= \frac{(\lambda^x+\lambda^{-x})^2-(\lambda^x-\lambda^{-x})^2}{4} = \lambda^x\lambda^{-x} = 1.\end{aligned}$$

Other identity can be shown similarly.

Theorem 4.2. *The following identity that is similar to the result* $ch(x+y) = ch(x)ch(y) + sh(x)sh(y)$ *is valid for the hyperbolic balancing and Lucas-balancing functions.*

$$chC(x+y) = chC(x)chC(y) + 8shB(x)shB(y).$$

Proof. By (2.1) and (2.2), we obtain

$$\begin{aligned}chC(x)chC(y) + 8shB(x)shB(y) &= \frac{\lambda^x+\lambda^{-x}}{2}\frac{\lambda^y+\lambda^{-y}}{2} + 8\frac{\lambda^x+\lambda^{-x}}{2\sqrt{8}}\frac{\lambda^y+\lambda^{-y}}{2\sqrt{8}} \\ &= \frac{\lambda^{x+y}+\lambda^{x-y}+\lambda^{-x+y}+\lambda^{-(x+y)}+\lambda^{x+y}-\lambda^{x-y}-\lambda^{-x+y}+\lambda^{-(x+y)}}{4} \\ &= \frac{\lambda^{x+y}+\lambda^{-(x+y)}}{2} = chC(x+y).\end{aligned}$$

This completes the proof.

Theorem 4.3. *The following result that is similar to the identity $ch(x-y)=ch(x)ch(y)-sh(x)sh(y)$ is valid for the hyperbolic balancing and Lucas-balancing functions.*

$$chC(x+y)=chC(x)cC(y)-8shB(x)shB(y).$$

Proof. The proof is analogous to Theorem 4.2.

Theorem 4.4. *The following correlations that are similar to the derivative classical hyperbolic functions*

$$[sh(x)]^n=\begin{cases} ch(x), & \text{for n=2k+1;}\\ sh(x), & \text{for n=2k.}\end{cases},\quad [ch(x)]^n=\begin{cases} sh(x), & \text{for n=2k+1;}\\ ch(x), & \text{for n=2k.}\end{cases}$$

are valid for the derivative hyperbolic balancing and Lucas-balancing functions. $[shB(x)]^n=\begin{cases} \frac{1}{\sqrt{8}}(\ln\lambda)^n chC(x), & \text{for n=2k+1;}\\ (\ln\lambda)^n shB(x), & \text{for n=2k.}\end{cases}$, $[chC(x)]^n=\begin{cases} \sqrt{8}(\ln\lambda)^n shB(x), & \text{for n=2k+1;}\\ (\ln\lambda)^n chC(x), & \text{for n=2k.}\end{cases}$

Proof. Based on the Definitions 2.1 and 2.2, we obtain

$$\begin{aligned}
[\mathrm{shB(x)}]' &= \left(\frac{\lambda^x-\lambda^{-x}}{2\sqrt{8}}\right)' = \frac{\lambda^x\ln\lambda+\lambda^{-x}\ln\lambda}{2\sqrt{8}} = \frac{\ln\lambda}{\sqrt{8}}\ chC(x)\\
[\mathrm{chC(x)}]' &= \left(\frac{\lambda^x+\lambda^{-x}}{2}\right)' = \frac{\lambda^x\ln\lambda-\lambda^{-x}\ln\lambda}{2} = \ln\lambda\sqrt{8}\ shB(x)\\
[\mathrm{shB(x)}]'' &= \left(\frac{\ln\lambda}{\sqrt{8}}\ chC(x)\right)' = (\ln\lambda)^2 shB(x)\\
[\mathrm{chC(x)}]'' &= \left(\ln\lambda\sqrt{8}\ shB(x)\right)' = (\ln\lambda)^2 chC(x)\\
&\cdots\cdots\cdot\\
[\mathrm{shB(x)}]^n &= \begin{cases} \frac{1}{\sqrt{8}}(\ln\lambda)^n chC(x), & \text{for n=2k+1;}\\ (\ln\lambda)^n shB(x), & \text{for n=2k.}\end{cases}\\
[\mathrm{chC(x)}]^n &= \begin{cases} \sqrt{8}(\ln\lambda)^n shB(x), & \text{for n=2k+1;}\\ (\ln\lambda)^n chC(x), & \text{for n=2k.}\end{cases}
\end{aligned}$$

This ends the proof.

In Table 3 and Table 4, we indicate some known properties of classical hyperbolic functions and the appropriate properties of the hyperbolic balancing and Lucas-balancing functions for comparison.

Table 4.1:

Identities for classical hyperbolic functions	**Identities for hyperbolic balancing**
$[\cosh x]^2 - [\sinh x]^2 = 1$	$[chC(x)]^2 - 8[shB(x)]^2 = 1$
$ch(x \pm y) = ch(x)ch(y) \pm sh(x)sh(y)$	$\frac{1}{\sqrt{8}} chB(x \pm y) = chB(x)chB(y) \pm shB(x)shB(y)$
$sh(x \pm y) = sh(x)ch(y) \pm ch(x)sh(y)$	$\frac{1}{\sqrt{8}} shB(x \pm y) = shB(x)chB(y) \pm chB(x)shB(y)$
$ch(2x) = [ch(x)]^2 + [sh(x)]^2$	$\frac{1}{\sqrt{8}} chB(2x) = [chB(x)]^2 + [shB(x)]^2$
$sh(2x) = 2sh(x)ch(x)$	$\frac{1}{\sqrt{8}} shB(2x) = 2shB(x)chB(x)$
$[ch(x)]^{(n)} = \begin{cases} sh(x), & \text{for n=2k+1;} \\ ch(x), & \text{for n=2k.} \end{cases}$	$[chB(x)]^{(n)} = \begin{cases} (\ln\lambda)^n shB(x), & \text{for n=2k+1;} \\ (\ln\lambda)^n chB(x), & \text{for n=2k.} \end{cases}$
$[sh(x)]^{(n)} = \begin{cases} ch(x), & \text{for n=2k+1;} \\ sh(x), & \text{for n=2k.} \end{cases}$	$[shB(x)]^{(n)} = \begin{cases} (\ln\lambda)^n chB(x), & \text{for n=2k+1;} \\ (\ln\lambda)^n shB(x), & \text{for n=2k.} \end{cases}$
$\int\int\int_n ch(x)dx = \begin{cases} sh(x), & \text{for n=2k+1;} \\ ch(x), & \text{for n=2k.} \end{cases}$	$\int\int\int_n chB(x)dx = \begin{cases} (\ln\lambda)^{-n} shB(x), & \text{for n=2k+1;} \\ (\ln\lambda)^{-n} chB(x), & \text{for n=2k.} \end{cases}$
$\int\int\int_n sh(x)dx = \begin{cases} ch(x), & \text{for n=2k+1;} \\ sh(x), & \text{for n=2k.} \end{cases}$	$\int\int\int_n shB(x)dx = \begin{cases} (\ln\lambda)^{-n} chB(x), & \text{for n=2k+1;} \\ (\ln\lambda)^{-n} shB(x), & \text{for n=2k.} \end{cases}$

Table 4.2:

Identities for classical hyperbolic functions	**Identities for Lucas-balancing functions**
$[\cosh x]^2 - [\sinh x]^2 = 1$	$[shC(x)]^2 - 8[chB(x)]^2 = -1$
$ch(x \pm y) = ch(x)ch(y) \pm sh(x)sh(y)$	$chC(x \pm y) = chC(x)cC(y) \pm shC(x)shC(y)$
$sh(x \pm y) = sh(x)ch(y) \pm ch(x)sh(y)$	$sC(x \pm y) = shC(x)chC(y) \pm chC(x)shC(y)$
$ch(2x) = [ch(x)]^2 + [sh(x)]^2$	$chC(2x) = [chC(x)]^2 + [shC(x)]^2$
$sh(2x) = 2sh(x)ch(x)$	$shC(2x) = 2shC(x)chC(x)$
$[ch(x)]^{(n)} = \begin{cases} sh(x), & \text{for n=2k+1;} \\ ch(x), & \text{for n=2k.} \end{cases}$	$[chC(x)]^{(n)} = \begin{cases} (\ln\lambda)^n shC(x), & \text{for n=2k+1;} \\ (\ln\lambda)^n chC(x), & \text{for n=2k.} \end{cases}$
$[sh(x)]^{(n)} = \begin{cases} ch(x), & \text{for n=2k+1;} \\ sh(x), & \text{for n=2k.} \end{cases}$	$[shC(x)]^{(n)} = \begin{cases} (\ln\lambda)^n chC(x), & \text{for n=2k+1;} \\ (\ln\lambda)^n shC(x), & \text{for n=2k.} \end{cases}$
$\int\int\int_n ch(x)dx = \begin{cases} sh(x), & \text{for n=2k+1;} \\ ch(x), & \text{for n=2k.} \end{cases}$	$\int\int\int_n chC(x)dx = \begin{cases} (\ln\lambda)^{-n} shC(x), & \text{for n=2k+1;} \\ (\ln\lambda)^{-n} chC(x), & \text{for n=2k.} \end{cases}$
$\int\int\int_n sh(x)dx = \begin{cases} ch(x), & \text{for n=2k+1;} \\ sh(x), & \text{for n=2k.} \end{cases}$	$\int\int\int_n sC(x)dx = \begin{cases} (\ln\lambda)^{-n} cC(x), & \text{for n=2k+1;} \\ (\ln\lambda)^{-n} sC(x), & \text{for n=2k.} \end{cases}$

Theorem 4.5. *The following identity which is similar to D'Moivre's theorem is valid for the hyperbolic balancing and Lucas-balancing functions:*

$$\left[chC(x) \pm \sqrt{8}shB(x)\right]^n = chC(nx) \pm \sqrt{8}shB(nx)$$

and,

$$\left[shC(x) \pm \sqrt{8}chB(x)\right]^n = shC(nx) \pm \sqrt{8}chB(nx)$$

Proof. By using Binet's formulas described in (2.3) again, we obtain

$$\begin{aligned}\left[chC(x)+\sqrt{8}shB(x)\right]^n &= \left(\tfrac{\lambda^x+\lambda^{-x}}{2}+\sqrt{8}\tfrac{\lambda^x-\lambda^{-x}}{2\sqrt{8}}\right)^n\\ &= \lambda^{nx}\\ &= \tfrac{\lambda^{nx}+\lambda^{-nx}}{2}+\sqrt{8}\tfrac{\lambda^{nx}+\lambda^{-nx}}{2\sqrt{8}}\\ &= chC(nx)+\sqrt{8}shB(nx),\end{aligned}$$

which ends the proof.

5. Balancing matrices

Ray [14] has introduced balancing Q-matrix of order 2 whose entries are the first three balancing numbers 0, 1 and 6 as follows:

$$Q_B = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix}. \tag{5.1}$$

He has also proved that for all $n \in \mathbf{Z}$, the n^{th} power of this matrix is

$$Q_B^n = \begin{pmatrix} B_{n+1} & -B_n \\ B_n & -B_{n-1} \end{pmatrix}. \tag{5.2}$$

It has also been shown in [14] that the matrix (5.2) coincides with the Cassini formula

$$\det Q_B^n = B_n^2 - B_{n+1}B_{n-1} = 1 \tag{5.3}$$

for balancing numbers.

We observe from Theorem 3.3 that, the formula $shB(x)^2 - shB(x+1)shB(x-1) = 1$ is a generalization of the Cassini formula for balancing numbers $B_n^2 - B_{n+1}B_{n-1} = 1$ for continues domain. In the present paper, we develop a theory of balancing matrices which are the generalization of the matrix in (5.2) in continuous domain. Based on these matrices, a new kind of cryptography method is also considered.

5.1. Some properties of balancing matrices

The following are some valid properties of balancing matrices which can be easily deduced by using usual properties of matrices. The recurrence relation of balancing matrices is similar to that of balancing numbers, that is for $n \in \mathbf{Z}$,

$$Q_B^n = 6Q_B^{n-1} - Q_B^{n-2}, \tag{5.4}$$

and for all positive integers m, n,

$$Q_B^n Q_B^m = Q_B^m Q_B^n = Q_B^{n+m}. \tag{5.5}$$

Based on the recurrence relation mentioned in (5.4), a representation of the matrices Q_B^n are given in Table 5. Also Table 5 gives the matrices Q_B^n and their inverses Q_B^{-n} in explicit form.

We observe that the inverse matrix Q_B^{-n} can easily obtain from Q_B^n by rearranging the matrix in (5.2) to diagonal elements B_{n+1} and B_{n-1} and to take its diagonal elements B_n with an opposite sign. It means that the inverse matrix Q_B^{-n} has the following form:

$$Q_B^{-n} = \begin{pmatrix} -B_{n-1} & B_n \\ -B_n & B_{n+1} \end{pmatrix}. \tag{5.6}$$

By correlation of (2.5) with the matrix described in (5.2) and (5.6) can be written in terms of hyperbolic balancing functions as

$$Q_B^n = \begin{pmatrix} shB(n+1) & -shB(n) \\ shB(n) & -shB(n-1) \end{pmatrix}, \tag{5.7}$$

and

$$Q_B^{-n} = \begin{pmatrix} -shB(n-1) & shB(n) \\ -shB(n) & shB(n+1) \end{pmatrix} \tag{5.8}$$

where n is a discrete variable, $n = 0, \pm 1, \pm 2, \pm 3, \ldots$. If we replace the discrete variable n by continuous variable x in the matrices given in (5.7) and (5.8), we get the following unusual matrices which are the functions of the continuous variable x.

$$Q_B^n = \begin{pmatrix} shB\,(n+1) & -shB\,(n) \\ shB\,(n) & -shB\,(n-1) \end{pmatrix} \tag{5.9}$$

and

$$Q_B^{-x} = \begin{pmatrix} -shB(x-1) & shB(x) \\ -shB(x) & shB(x+1) \end{pmatrix}. \tag{5.10}$$

In order to prove, the matrix of (5.10) is the inverse of the matrix given in (5.9), we need to do the following.

$$\mathrm{Q}_B^x Q_B^{-x} = \begin{pmatrix} shB\,(x+1) & -shB\,(x) \\ shB\,(x) & -shB\,(x-1) \end{pmatrix} \begin{pmatrix} -shB\,(x-1) & shB\,(x) \\ -shB\,(x) & shB\,(x+1) \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \tag{5.11}$$

where

$$\begin{aligned} a_{11} &= shB(x)^2 - shB(x+1)shB(x-1) \\ a_{12} &= shB(x+1)shB(x) - shB(x)shB(x+1) \\ a_{21} &= shB(x)shB(x-1) - shB(x-1)shB(x) \\ a_{22} &= shB(x)^2 - shB(x+1)shB(x-1) \end{aligned}$$

We notice from (5.13) and (5.14) that,

$$a_{12} = a_{21} = 0. \tag{5.12}$$

Also by virtue of Theorem 3.3, we obtain

$$a_{11} = a_{22} = 1. \tag{5.13}$$

Thus, by (5.16) and (5.17), (5.7) can be reduced to

$$Q_B^x Q_B^{-x} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

which is valid for any value of the variable x. It follows that (5.10) is the inverse of (5.9).

5.2. Determinant of balancing matrices in continuous domain

By virtue of Theorem 3.3, the determinant of the matrix (5.9) is given by

$$\det(Q_B^x) = shB(x)^2 - shB(x+1)shB(x-1) = 1.$$

It is observed that, the identity $\det(Q_B^x) = 1$ is nothing but a generalization of Cassini formula for balancing matrix given in the (5.3) for continuous domain.

6. Cryptography using Balancing Matrices

6.1. A New Cryptography Method

So far we have introduced the direct and the inverse matrices of (5.9) and (5.10). These matrices enable us to develop a new kind of cryptography method that is being used to protect the initial message from the hackers. Let the initial message is a digital signal. Recall that a digital signal is any sequence of real numbers

$$a_0, a_1, a_3, a_4, a_5, a_6 \dots, \tag{6.1}$$

where the separate real numbers are known as readings. We consider a new kind cryptography based on the balancing matrices described in (5.9) and (5.10) as follows: Let us choose the first four readings a_1, a_2, a_3, a_4 of (6.1) to form a 2×2 matrix

$$M = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}. \tag{6.2}$$

Note that the initial matrix M can be considered as plaintext [19] . Since, there are $4! = 24$ permutations to form the matrix of (6.2) from the readings a_1, a_2, a_3, a_4, the initial step of cryptography protection of these readings is a choice of the permutations P_i, where P_i denote the i^{th} permutation of the four readings a_1, a_2, a_3, a_4. Let us choose the direct matrix of (5.2) as enciphering matrix and its inverse from (5.6) as deciphering matrix. Based on matrix multiplication, we now consider the following encryption and decryption method:

Encryption:	Decryption:
$M \times Q_B^x = E(x)$	$E(x) \times Q_B^{-x} = M$

Here the matrix M is the plaintext from (6.2) that is formed according to the permutations P_i. $E(x)$ is the ciphertext and the matrices Q_B^x and Q_B^{-x} are respectively the enciphering and the deciphering matrices. The variable x can be used as cryptography key or simply key which indicates that depending on the value of key x, there is an infinite numbers of plaintext M into ciphertext $E(x)$.

We now prove that the described cryptography method ensures one-valued transformation of the plaintext M into the ciphertext E and the ciphertext E into the plaintext M. By considering the matrix from (5.9) as enciphering matrix, we observe that for the given value of the cryptography key $x = x_1$, the encryption can be represented as follows:

$$M \times Q_B^x = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} shB(x_1+1) & -shB(x_1) \\ shB(x_1) & -shB(x_1-1) \end{pmatrix} \left(= \begin{matrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{matrix} = E(x), \right) \tag{6.3}$$

where

$$e_{11} = a_1 shB(x_1+1) + a_2 shB(x_1), \tag{6.4}$$

$$e_{12} = -a_1 shB(x_1) - a_2 shB(x_1-1), \tag{6.5}$$

$$e_{21} = a_3 shB(x_1+1) + a_4 shB(x_1), \tag{6.6}$$

$$e_{22} = -a_3 shB(x_1) - a_4 shB(x_1-1) \tag{6.7}$$

For this case the decryption can be represented as follows:

$$E(x_1) \times Q_B^{-x} = \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix} \begin{pmatrix} -shB(x_1-1) & shB(x_1) \\ -shB(x_1) & shB(x_1+1) \end{pmatrix} \left(= \begin{matrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{matrix} = D, \right) \tag{6.8}$$

where

$$d_{11} = -e_{11} shB(x_1-1) - e_{12} shB(x_1), \tag{6.9}$$

$$d_{12} = e_{11} shB(x_1) + e_{12} shB(x_1+1), \tag{6.10}$$

$$d_{21} = -e_{21} shB(x_1-1) - e_{22} shB(x_1), \tag{6.11}$$

$$d_{22} = e_{21} shB(x_1) + e_{22} shB(x_1+1) \tag{6.12}$$

By using (6.4) in (6.8) and using Theorem 3.3 , we get

$$d_{11} = -\left(a_1 shB(x_1+1) + a_2 shB(x_1)\right) sB(x_1-1) + \left(a_1 shB(x_1) + a_2 shB(x_1-1)\right) shB(x_1),$$

$$= \text{-}a_1 shB(x_1+1) shB(x_1-1) - a_2 shB(x_1) shB(x_1-1) + a_1 [shB(x)]^2 + a_2 shB(x_1-1) shB(x_1),$$
$$= a_1 \left[[shB(x)]^2 - shB(x_1+1) shB(x_1-1) \right] = a_1$$

Similarly after corresponding transformation, one can get

$$d_{12} = a_2, \quad d_{21} = a_3 \text{ and } d_{22} = a_4.$$

Thus, the matrix D can be written as follows:

$$D = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} \left(= \begin{matrix} a_1 & a_2 \\ a_3 & a_4 \end{matrix} = M. \right)$$

Hence, the described cryptographic method ensures one-valid transformation of the initial plaintext M at the entrance of the coder into the same plaintext M at the exit of the decoder.

We observe that,

$$\det E(x) = \det M \det Q_B^x,$$

and since $\det Q_B^x = 1$, we have

$$\det E(x) = \det M.$$

This follows that the determinant of the matrix $E(x)$ can be determined identically by the determinant of the initial matrix M.

6.2. Encryption and Decryption Time

We notice from (6.3-6.7) that, the encrypted matrix can be generated by 8-multiplications and 4-additions. Therefore the total encryption time T_E is given by

$$T_E = 8\triangle_\times + 4\triangle_+, \tag{6.13}$$

where $\triangle_\times$ and $\triangle_+$ are respectively denote the time of one multiplication and one addition.

Analogous to (6.13), if we consider (6.8-6.12), total decryption time will be given by

$$T_D = 8\triangle_\times + 4\triangle_+. \tag{6.14}$$

We observe that, (6.13) involves 8-multiplications and 4-additions. The time complexity for solving this would be $O(n^3)$, where the matrix is a square matrix of order n. Indeed, the time complexity of computing (6.13) can be improved to $O(n^{2.81})$ by the well known Strassen's method.

While performing the encryption and decryption, we generally prefer the large values (In general, the entries of the higher degree balancing matrix are large) in order to make them more secure. Our main concern here to improve the time complexity of integer multiplication when the entries of the balancing matrix become large. The naive approach for multiplying two n-digit numbers with base r will take $O(n^2)$ time. On the other hand, we can use the divide and conquer approach for integer multiplication so that the complexity can be reduced, known as Karatsuba's algorithm.

Let ϕ denote the balancing n-digit number with base r from the balancing matrix and δ be an element in order r of the massage matrix. The initial step of multiplying ϕ and δ involves dividing both of them into equal parts each having $\frac{n}{2}$-digits as follows:

$$\phi = \boxed{\phi_L}\ \boxed{\phi_R} = r^{\frac{n}{2}}\phi_L + \phi_R,$$
$$\delta = \boxed{\delta_L}\ \boxed{\delta_R} = r^{\frac{n}{2}}\delta_L + \delta_R.$$

On multiplication of ϕ and δ produces the result,

$$\phi * \delta = r^n \phi_L \delta_L + r^{\frac{n}{2}} \left(\phi_L \delta_R + \phi_R \delta_L\right) + \phi_R \delta_R. \tag{6.15}$$

Even though (6.15) involves 4 subproblems of size $\frac{n}{2}$-digits using Karatsuba's insight, we only need 3 subproblems as follows:

$$\begin{aligned} u &= \phi_L \delta_L, \\ v &= \phi_R \delta_R, \\ w &= \left(\phi_L + \phi_R\right)\left(\delta_R + \delta_L\right), \end{aligned}$$

Hence (6.15) reduces to

$$\phi * \delta = u \cdot r^n + w \cdot r^{\frac{n}{2}} + v.$$

If $T(n)$ is the time required to multiply two $n-$digit numbers, then this shows the time complexity as

$$T(n) = 3T(\frac{n}{2}) + O(n),$$

which follows that, $T(n)$ is $O(n^{\log_2 3})$ i.e. $O(n^{1.584})$.

Conclusion

The present article focuses on the interconnection between balancing and Lucas-balancing numbers, hyperbolic balancing and hyperbolic Lucas-balancing functions, and hyperbolic functions with the help of reliable mathematical proof. Like hyperbolic Fibonacci and hyperbolic Lucas functions [16], [18], hyperbolic balancing and hyperbolic Lucas-balancing functions needn't require separate consideration of even and odd values for n and also these functions are an extension of Binet's formula for balancing and Lucas-balancing numbers in continuous domain. As an application to this concept, a new kind of cryptography using Balancing matrix is discussed. The main idea of any cryptosystem is the selection of key along with faster encryption and decryption technique. Here, using divide and conquer method it has been shown that the encryption and decryption time can be reduced. As a result of this, a simple, fast, robust and, reliable cryptosystem is expected.

References

[1] A. Behera and G. K. Panda, "On the square roots of triangular numbers", *The Fibonacci quarterly*, vol. 37, no. 2, pp. 98-105, 1999. [On line]. Available: https://bit.ly/37BXUOl

[2] A. Bérczes, K. Liptai, I. Pink, "On generalized balancing numbers", *The Fibonacci quarterly*, vol. 48, no. 2, pp. 121-128, May 2010. [On line]. Available: https://bit.ly/2U6YzU1

[3] R. Keskin and O. Karaath, "Some new properties of balancing numbers and square triangular numbers", *Journal of integer sequences*, vol. 15, no. 2, 2012. [On line]. Available: https://bit.ly/38Oids7

[4] K. Liptai, "Fibonacci balancing numbers", *The Fibonacci quarterly*, vol. 42, no. 4. pp. 330-340, Nov. 2004, [On line]. Available: https://bit.ly/2Gww4aj

[5] K. Liptai, "Lucas balancing numbers", *Acta mathematica universitatis ostraviensis*, vol. 14, no. 1, pp. 43-47, 2006. [On line]. Available: https://bit.ly/2vsof3e

[6] K. Liptai, F. Luca, A. Pintér, and L. Szalay, "Generalized balancing numbers", *Indagationes mathematicae*, vol. 20, no. 1, pp. 87-100, Mar. 2009, doi: 10.1016/S0019-3577(09)80005-0.

[7] P. Olajos, "Properties of balancing, cobalancing and generalized balancing numbers", *Annales mathematicae et informaticae,* vol. 37, pp. 125-138, 2010. [On line]. Available: https://bit.ly/31495gp

[8] G. K. Panda and P. K. Ray, "Some links of balancing and cobalancing numbers with Pell and associated Pell numbers", *Bulletin of the institute of mathematics, Academia sinica (New Series),* vol. 6, no. 1, pp. 41-72, 2011. [On line]. Available: https://bit.ly/2U5nc3t

[9] B. K. Patel, P.K. Ray, and M Sahukar, "Positive integers solutions of certain Diophantine equations", *Proceeding: mathematical sciences*, vol. 128, no. 1, Art. ID. 5, Feb. 2018, doi: 10.1007/s12044-018-0377-4.

[10] B. K. Patel, N. Irmak, and P. K. Ray, "Incomplete balancing and Lucas-balancing numbers", *Mathematical reports,* vol. 20, no. 1, pp. 59- 72, 2018. [On line]. Available: https://bit.ly/2S0WNBb

[11] P. K. Ray, "Balancing polynomials and their derivatives", *Ukrainian mathematical journal*, vol. 69, no. 4, pp. 646-663, Sep. 2017, doi: 10.1007/s11253-017-1386-7.

[12] P. K. Ray, "On the properties of k-balancing and k-Lucas balancing numbers", *Acta et commentationes universitatis tartuensis de mathematica,* vol. 21, no. 2, pp. 259-274, Dec. 2017, doi: 10.12697/ACUTM.2017.21.18.

[13] B. K. Patel and P. K. Ray, "The period, rank and order of the sequence of balancing numbers modulo m", *Mathematical reports*, vol. 18, no. 3, pp. 395-401, 2016. [On line]. Available: https://bit.ly/2vAbaoR

[14] P. K. Ray and B. K Patel, "Uniform distribution of balancing numbers modulo m", *Uniform distribution theory,* vol. 11, no. 1, pp. 15-21, 2016, doi: 10.1515/udt-2016–0002.

[15] P. K. Ray, "Certain diophantine equations involving balancing and Lucas-balancing numbers", *Acta et commentationes universitatis tartuensis de mathematica*, vol. 20, no. 2, pp. 165-173, Dec. 2016, doi: 10.12697/ACUTM.2016.20.14.

[16] A. P. Stakhov and B. Rozin, "On a new class of hyperbolic function", C*haos, solitons & fractals*, vol. 23, no. 2, pp. 379-389, Jan. 2005, doi: 10.1016/j.chaos.2004.04.022.

[17] A. P. Stakhov, "Gazale formulas, a new class of hyperbolic Fibonacci and Lucas functions and the improved method of the 'golden' cryptography", *Akademiâ trinitarizma*, no. 77-6567, Art, ID. 14098, Dec. 2006, [On line]. Available: https://bit.ly/31co2gA

[18] A. P. Stakhov, "The 'golden' matrices and a new kind of cryptography", *Chaos, solutions & fractals,* vol. 32, no. 3 pp. 1138-1146, May 2007, doi: 10.1016/j.chaos.2006.03.069.

[19] D. R. Stinson, *Cryptography theory and practice*, 3rd ed. Boca Raton, FL: Chapman & Hall/ CRC, 2006.