Control and Cybernetics

vol. **48** (2019) No. 4

On $h(x)$ Lucas polynomials with application to coding*

by

Bandhu Prasad

Department of Mathematics
Kandi Raj College
Kandi - 742137, India
bandhu_iit@rediffmail.com

Abstract: In this paper, we study the $h(x)$ Lucas polynomials of order m and the U_n matrix, whose elements are Lucas polynomials, $h(x)(> 0)$ being a polynomial with real coefficients. We also establish the relations among the code matrix elements.

Keywords: Lucas numbers, Lucas polynomials, golden mean, code matrix

1. Introduction

The Lucas numbers, L_n, see Stakhov (1977) are defined by the recurrence relation

$$L_n = L_{n-1} + L_{n-2}, \qquad n \geq 2 \tag{1}$$

with initial conditions

$$L_0 = 2, L_1 = 1. \tag{2}$$

The Lucas numbers, L_n, and the golden mean,

$$\tau = \lim_{n \longrightarrow \infty} \frac{L_n}{L_{n-1}} = \frac{1+\sqrt{5}}{2} \tag{3}$$

have been appearing in physics, chemistry, life sciences, information and coding theory etc., see Stakhov (2006), Prasad (2016), Mac Williams and Sloane (1977), Basu and Prasad (2009), Esmaeli, Gulliwer and Kakhbod (2009), El Naschie (2009), Blahut (1983), Cover and Thomas (1991).

*Submitted: August 2019; Accepted: January 2020.

Tasci and Kilic (2004) defined order k generalization of the well known Lucas sequence for $n > 0$ and $1 \leq i \leq k$

$$L_n^i = L_{n-1}^i + L_{n-2}^i + \cdots + L_{n-k}^i$$

with initial conditions

$$L_n^i = \begin{cases} 2 & \text{if } i = 2 - n, \\ -1 & \text{if } i = 1 - n \text{ for } 1 - k \leq n \leq 0, \\ 0 & \text{otherwise,} \end{cases}$$

where L_n^i is the nth term of the ith sequence.

Nalli and Haukkanen (2009) introduced $h(x)$ Lucas polynomials, $L_{h,n}(x)$ (where $h(x)$ is a polynomial with real coefficients), with the recurrence relation

$$L_{h,n+1}(x) = h(x)L_{h,n}(x) + L_{h,n-1}(x), \quad n \geq 1 \tag{4}$$

and initial conditions

$$L_{h,0}(x) = 2, L_{h,1}(x) = h(x). \tag{5}$$

In this paper, we introduce $h(x)$ (> 0) Lucas polynomials of order m, $L_h^i(n, x)$, by the recurrence relation

$$L_h^i(n, x) = h(x)L_h^i(n - 1, x) + L_h^i(n - 2, x) + \cdots + L_h^i(n - m, x) \tag{6}$$

with initial conditions

$$L_h^i(n, x) = \begin{cases} 2 & \text{if } i = 2 - n, \\ -1 & \text{if } i = 1 - n \text{ for } 1 - k \leq n \leq 0, \\ 0 & \text{otherwise,} \end{cases}$$

where $h(x)$ (> 0) is a polynomial with real coefficients, and $L_h^i(n, x)$ is the nth term of the ith generalized Lucas polynomials.

The characteristic equation of $h(x)$ (> 0) Lucas polynomials of order m is

$$y^m - h(x)y^{m-1} - y^{m-2} \cdots - y - 1 = 0. \tag{7}$$

At the same time, the characteristic equation of Lucas polynomials of order m is

$$y^m - y^{m-1} - y^{m-2} \cdots - y - 1 = 0. \tag{8}$$

The equation (8) has m roots and only one real positive root when m is even or odd, but when m is even it has only one negative real root also. When $m \longrightarrow \infty$, then the positive real root is 2 and the negative real root is -1.

We write

$$\begin{pmatrix} L_h^i(n+1,x) \\ L_h^i(n,x) \\ . \\ . \\ . \\ L_h^i(n-m+2,x) \end{pmatrix} = Q_h \begin{pmatrix} L_h^i(n,x) \\ L_h^i(n-1,x) \\ . \\ . \\ . \\ L_h^i(n-m+1,x) \end{pmatrix},$$

where

$$Q_h = \begin{pmatrix} h(x) & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

In this paper, we define a new U_n matrix, whose elements are Lucas polynomials of order m and we also study the properties of this U_n matrix. In 2015, the present author published the paper Prasad (2015), which is based on Fibonacci numbers. This paper is based on Lucas polynomials of order m for the suitable initial conditions, so that U_n matrix is applicable for coding and decoding method.

2. Main results

2.1. The U_n matrix and its properties

We define a new U_n matrix of order m, which is given by

$$U_n = \begin{pmatrix} L_h^1(n,x) & L_h^2(n,x) & \cdots & L_h^m(n,x) \\ L_h^1(n-1,x) & L_h^2(n-1,x) & \cdots & L_h^m(n-1,x) \\ \vdots & \vdots & \ddots & \vdots \\ L_h^1(n-m+1,x) & L_h^2(n-m+1,x) & \cdots & L_h^m(n-m+1,x) \end{pmatrix}. \quad (9)$$

We will prove that $U_n = Q_h^{n-1}U_1$,
where

$$U_1 = \begin{pmatrix} -h(x) & 2h(x)-1 & 1 & \cdots & 1 & 1 \\ -1 & 2 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 2 & \cdots & 0 & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 2 \end{pmatrix}.$$

Proof:

$$U_n = \begin{pmatrix} h(x) & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \times$$

$$\times \begin{pmatrix} L_h^1(n-1,x) & L_h^2(n-1,x) & \cdots & L_h^m(n-1,x) \\ L_h^1(n-2,x) & L_h^2(n-2,x) & \cdots & L_h^m(n-2,x) \\ \vdots & \vdots & \ddots & \vdots \\ L_h^1(n-m,x) & L_h^2(n-m,x) & \cdots & L_h^m(n-m,x) \end{pmatrix}$$

$$= Q_h U_{n-1}.$$

Therefore, we can write $U_n = Q_h(Q_h U_{n-2}) = \cdots = Q_h^{n-1} U_1$.

Now

$$U_1 = \begin{pmatrix} L_h^1(1,x) & L_h^2(1,x) & \cdots & L_h^m(1,x) \\ L_h^1(0,x) & L_h^2(0,x) & \cdots & L_h^m(0,x) \\ \vdots & \vdots & \ddots & \vdots \\ L_h^1(2-m,x) & L_h^2(2-m,x) & \cdots & L_h^m(2-m,x) \end{pmatrix}$$

$$= \begin{pmatrix} -h(x) & 2h(x)-1 & 1 & \cdots & 1 & 1 \\ -1 & 2 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 2 & \cdots & 0 & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 2 \end{pmatrix} = U_1.$$

Hence $U_n = Q_h^{n-1} U_1$.

Theorem 1 *For matrix U_n in (9) and for $n \geq 1$ and $m \geq 2$, $Det\ U_n = 1$ or -1.*

Proof:
$Det\ U_n = Det\ (Q_h^{n-1} U_1) = (Det\ Q_h)^{n-1} Det\ U_1$ as $Det\ Q_h = (-1)^{m+1}$ for $m \geq 2$ and $Det\ U_1 = (-1)$. Hence, $Det\ U_n = (-1)^{mn-m+n} = 1$ or -1. □

2.2. Note

The code matrix, E is defined by the following formula: $E = M \times U_n$. According to the matrix theory (see Hohn, 1973) we have

$$Det\ E = Det\ (M \times U_n) = Det\ M \times Det\ U_n. \tag{10}$$

2.3. Relations between the code matrix elements for U_n matrix of order 2, V_2

In this case, let the message, M be

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

Then the V_2 coding of the message M is

$$M \times V_2 = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$$

$$\begin{pmatrix} L_h^1(n,x) & L_h^2(n,x) \\ L_h^1(n-1,x) & L_h^2(n-1,x) \end{pmatrix} = \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix} = E.$$

Hence,

$$V_2 = \begin{pmatrix} L_h^1(n,x) & L_h^2(n,x) \\ L_h^1(n-1,x) & L_h^2(n-1,x) \end{pmatrix}. \tag{11}$$

$$Det\ V_2 = 1 \text{ or } -1.$$

The message, M, let be given, like above, as

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

Then, the V_2 coding of the message, M, is

$$M \times V_2 = \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix} = E$$

and decoding of the message M is

$$M = E \times V_2^{-1} = \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix} \begin{pmatrix} -L_h^2(n-1,x) & L_h^2(n,x) \\ L_h^1(n-1,x) & -L_h^1(n,x) \end{pmatrix}$$

$$= \begin{pmatrix} -e_1L_h^2(n-1,x)+e_2L_h^1(n-1,x) & e_1L_h^2(n,x)-e_2L_h^1(n,x) \\ -e_3L_h^2(n-1,x)+e_4L_h^1(n-1,x) & e_3L_h^2(n,x)-e_4L_h^1(n,x) \end{pmatrix}.$$

Since $m_1,\ m_2,\ m_3,\ m_4$ are positive integers, we have

$$m_1 = -e_1L_h^2(n-1,x)+e_2L_h^1(n-1,x) > 0, \tag{12}$$

$$m_2 = e_1L_h^2(n,x)-e_2L_h^1(n,x) > 0, \tag{13}$$

$$m_3 = -e_3L_h^2(n-1,x)+e_4L_h^1(n-1,x) > 0, \tag{14}$$

$$m_4 = e_3L_h^2(n,x)-e_4L_h^1(n,x) > 0. \tag{15}$$

By (12), we get

$$\frac{L_h^1(n-1,x)}{L_h^2(n-1,x)} > \frac{e_1}{e_2}, \tag{16}$$

By (14), we get

$$\frac{L_h^1(n-1,x)}{L_h^2(n-1,x)} > \frac{e_3}{e_4}, \tag{17}$$

By (13), we get

$$\frac{L_h^1(n,x)}{L_h^2(n,x)} < \frac{e_1}{e_2}, \tag{18}$$

By (15), we get

$$\frac{L_h^1(n,x)}{L_h^2(n,x)} < \frac{e_3}{e_4}. \tag{19}$$

By (16) and (18), we get

$$\frac{L_h^1(n,x)}{L_h^2(n,x)} < \frac{e_1}{e_2} < \frac{L_h^1(n-1,x)}{L_h^2(n-1,x)}. \tag{20}$$

By (17) and (19), we get

$$\frac{L_h^1(n,x)}{L_h^2(n,x)} < \frac{e_3}{e_4} < \frac{L_h^1(n-1,x)}{L_h^2(n-1,x)}. \tag{21}$$

Therefore, for the large value of n, we get

$$\frac{e_1}{e_2} \approx \frac{h(x)+\sqrt{h^2(x)+4}}{2},\ \frac{e_3}{e_4} \approx \frac{h(x)+\sqrt{h^2(x)+4}}{2} \tag{22}$$

and when $h(x)=1$, we have

$$\frac{e_1}{e_2} \approx \tau,\ \frac{e_3}{e_4} \approx \tau;\ \text{where } \tau = \frac{1+\sqrt{5}}{2}.$$

2.4. Relations among the code matrix elements for U_n matrix of order 3, V_3

In this case, let the message, M, be

$$M = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix}.$$

Then, the V_3 coding of the message M is

$$M \times V_3 = \begin{pmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix} = E$$

and

$$\begin{aligned} M &= E \times V_3^{-1} \\ &= \begin{pmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix} \begin{pmatrix} L_h^1(n,x) & L_h^2(n,x) & L_h^3(n,x) \\ L_h^1(n-1,x) & L_h^2(n-1,x) & L_h^3(n-1,x) \\ L_h^1(n-2,x) & L_h^2(n-2,x) & L_h^3(n-2,x) \end{pmatrix}^{-1} \\ &= \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix}. \end{aligned}$$

$$Det\ V_3 = -1.$$

$$\begin{aligned} Det\ V_3 = L_h^1(n,x)[L_h^2(n-1,x)L_h^3(n-2,x) - L_h^3(n-1,x)L_h^2(n-2,x)] \quad + \\ L_h^2(n,x)[L_h^3(n-1,x)L_h^1(n-2,x) - L_h^1(n-1,x)L_h^3(n-2,x)] \quad + \\ L_h^3(n,x)[L_h^1(n-1,x)L_h^2(n-2,x) - L_h^2(n-1,x)L_h^1(n-2,x)] = -1 \end{aligned} \tag{23}$$

and

$$M = \begin{pmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix} \begin{pmatrix} A & B & C \\ D & E & F \\ G & H & I \end{pmatrix}$$

where

$$A = L_h^2(n-1,x)L_h^3(n-3,x) - L_h^2(n-2,x)L_h^3(n-1,x),$$

$$B = L_h^3(n,x)L_h^2(n-2,x) - L_h^2(n,x)L_h^3(n-3,x),$$

$$C = L_h^2(n,x)L_h^3(n-1,x) - L_h^2(n-1,x)L_h^3(n,x),$$

$$D = L_h^3(n-1,x)L_h^1(n-2,x) - L_h^1(n-1,x)L_h^3(n-3,x),$$

$$E = L_{p,h}^1(n,x)L_{p,h}^3(n-3,x) - L_{p,h}^3(n,x)L_{p,h}^1(n-2,x),$$

$$F = L_{p,h}^1(n-1,x)L_{p,h}^3(n,x) - L_{p,h}^1(n,x)L_{p,h}^3(n-1,x),$$

$$G = L_h^1(n-1,x)L_h^2(n-2,x) - L_h^1(n-2,x)L_h^2(n-1,x),$$

$$H = L_h^2(n,x)L_h^1(n-2,x) - L_h^1(n,x)L_h^2(n-2,x),$$

$$I = L_h^1(n,x)L_h^2(n-1,x) - L_h^1(n-1,x)L_h^2(n,x).$$

Since $m_1,\ m_2,\ m_3,\ m_4,\ m_5,\ m_6,\ m_7,\ m_8,\ m_9$ are positive integers, we have

$$\begin{aligned} m_1 = e_1[L_h^2(n-1,x)L_h^3(n-3,x) - L_h^2(n-2,x)L_h^3(n-1,x)] \quad + \\ e_2[L_h^3(n-1,x)L_h^1(n-2,x) - L_h^1(n-1,x)L_h^3(n-3,x)] \quad + \\ e_3[L_h^1(n-1,x)L_h^2(n-2,x) - L_h^1(n-2,x)L_h^2(n-1,x)] > 0, \end{aligned} \tag{24}$$

$$\begin{aligned} m_2 = e_1[L_h^3(n,x)L_h^2(n-2,x) - L_h^2(n,x)L_h^3(n-3,x)] \quad + \\ e_2[L_h^1(n,x)L_h^3(n-3,x) - L_h^3(n,x)L_h^1(n-2,x)] \quad + \\ e_3[L_h^2(n,x)L_h^1(n-2,x) - L_h^1(n,x)L_h^2(n-2,x)] > 0, \end{aligned} \tag{25}$$

$$\begin{aligned} m_3 = e_1[L_h^2(n,x)L_h^3(n-1,x) - L_h^2(n-1,x)L_h^3(n,x)] \quad + \\ e_2[L_h^1(n-1,x)L_h^3(n,x) - L_h^1(n,x)L_h^3(n-1,x)] \quad + \\ e_3[L_h^1(n,x)L_h^2(n-1,x) - L_h^1(n-1,x)L_h^2(n,x)] > 0, \end{aligned} \tag{26}$$

$$\begin{aligned} m_4 = e_4[L_h^2(n-1,x)L_h^3(n-3,x) - L_h^2(n-2,x)L_h^3(n-1,x)] \quad + \\ e_5[L_h^3(n-1,x)L_h^1(n-2,x) - L_h^1(n-1,x)L_h^3(n-3,x)] \quad + \\ e_6[L_h^1(n-1,x)L_h^2(n-2,x) - L_h^1(n-2,x)L_h^2(n-1,x)] > 0, \end{aligned} \tag{27}$$

$$\begin{aligned} m_5 = e_4[L_h^3(n,x)L_h^2(n-2,x) - L_h^2(n,x)L_h^3(n-3,x)] \quad + \\ e_5[L_h^1(n,x)L_h^3(n-3,x) - L_h^3(n,x)L_h^1(n-2,x)] \quad + \\ e_6[L_h^2(n,x)L_h^1(n-2,x) - L_h^1(n,x)L_h^2(n-2,x)] > 0, \end{aligned} \tag{28}$$

$$\begin{aligned} m_6 = e_4[L_h^2(n,x)L_h^3(n-1,x) - L_h^2(n-1,x)L_h^3(n,x)] \quad + \\ e_5[L_h^1(n-1,x)L_h^3(n,x) - L_h^1(n,x)L_h^3(n-1,x)] \quad + \\ e_6[L_h^1(n,x)L_h^2(n-1,x) - L_h^1(n-1,x)L_h^2(n,x)] > 0, \end{aligned} \tag{29}$$

$$\begin{aligned} m_7 = e_7[L_h^2(n-1,x)L_h^3(n-3,x) - L_h^2(n-2,x)L_h^3(n-1,x)] \quad + \\ e_8[L_h^3(n-1,x)L_h^1(n-2,x) - L_h^1(n-1,x)L_h^3(n-3,x)] \quad + \\ e_9[L_h^1(n-1,x)L_h^2(n-2,x) - L_h^1(n-2,x)L_h^2(n-1,x)] > 0, \end{aligned} \tag{30}$$

$$\begin{aligned} m_8 = e_7[L_h^3(n,x)L_h^2(n-2,x) - L_h^2(n,x)L_h^3(n-3,x)] \quad + \\ e_8[L_h^1(n,x)L_h^3(n-3,x) - L_h^3(n,x)L_h^1(n-2,x)] \quad + \\ e_9[L_h^2(n,x)L_h^1(n-2,x) - L_h^1(n,x)L_h^2(n-2,x)] > 0, \end{aligned} \tag{31}$$

$$\begin{aligned} m_9 = e_7[L_h^2(n,x)L_h^3(n-1,x) - L_h^2(n-1,x)L_h^3(n,x)] \quad + \\ e_8[L_h^1(n-1,x)L_h^3(n,x) - L_h^1(n,x)L_h^3(n-1,x)] \quad + \\ e_9[L_h^1(n,x)L_h^2(n-1,x) - L_h^1(n-1,x)L_h^2(n,x)] > 0. \end{aligned} \tag{32}$$

By (24), we get

$$\begin{aligned} & e_1L_h^2(n-1,x)L_h^3(n-3,x) + e_2L_h^1(n-1,x)L_h^3(n,x) + \\ & +e_3L_h^1(n-1,x)L_h^2(n-2,x) > e_1L_h^2(n-2,x)L_h^3(n-1,x) + \\ & +e_2L_h^1(n-1,x)L_h^3(n-3,x) + e_3L_h^1(n-2,x)L_h^2(n-1,x). \end{aligned} \tag{33}$$

By (25), we get

$$\begin{aligned} e_1L_h^3(n,x)L_h^2(n-2,x) + e_2L_h^1(n,x)L_h^3(n-3,x) + e_3L_h^2(n,x)L_h^1(n-2,x) \quad > \\ e_1L_h^2(n,x)L_h^3(n-3,x) + e_2L_h^3(n,x)L_h^1(n-2,x) + e_3L_h^1(n,x)L_h^2(n-2,x). \end{aligned} \tag{34}$$

By (26), we get

$$\begin{aligned} e_1L_h^2(n,x)L_h^3(n-1,x) + e_2L_h^1(n-1,x)L_h^3(n,x) + e_3L_h^2(n,x)L_h^1(n-2,x) \quad > \\ e_1L_h^2(n-1,x)L_h^3(n,x) + e_2L_h^1(n,x)L_h^3(n-1,x) + e_3L_h^1(n-1,x)L_h^2(n,x). \end{aligned} \tag{35}$$

Dividing both sides of (33) by $e_1L_h^2(n-2,x)L_h^3(n-1,x)(>0)$, of (34) by $e_1L_h^2(n,x)L_h^3(n-3,x)(>0)$ and of (35) by $e_1L_h^2(n-1,x)L_h^3(n,x)(>0)$, we get

$$\begin{aligned} & \frac{e_3}{e_1}[L_h^1(n-1,x)L_h^2(n-2,x) - L_h^1(n-2,x)L_h^2(n-1,x)] > \\ & \frac{e_2}{e_1}[L_h^1(n-1,x)L_h^3(n-3,x) - L_h^3(n-1,x)L_h^1(n-2,x)] + \\ & [L_h^3(n-1,x)L_h^2(n-2,x) - L_h^2(n-1,x)L_h^3(n-3,x)], \end{aligned} \tag{36}$$

$$\begin{aligned} & \frac{e_3}{e_1}[L_h^1(n-2,x)L_h^2(n,x) - L_h^1(n,x)L_h^2(n-2,x)] < \\ & \frac{e_2}{e_1}[L_h^3(n,x)L_h^1(n-2,x) - L_h^1(n,x)L_h^3(n-3,x)] + \\ & [L_h^2(n,x)L_h^3(n-3,x) - L_h^3(n,x)L_h^2(n-2,x)], \end{aligned} \tag{37}$$

$$\begin{aligned}&\frac{e_3}{e_1}[L_h^1(n,x)L_h^2(n-1,x)-L_h^1(n-1,x)L_h^2(n,x)]>\\&\frac{e_2}{e_1}[L_h^1(n,x)L_h^3(n-1,x)-L_h^1(n-1,x)L_h^3(n,x)]+\\&[L_h^2(n-1,x)L_h^3(n,x)-L_h^2(n,x)L_h^3(n-1,x)].\end{aligned}\tag{38}$$

Let

$$a=[L_h^1(n-1,x)L_h^2(n-2,x)-L_h^1(n-2,x)L_h^2(n-1,x)],$$

$$b=[L_h^1(n-2,x)L_h^2(n,x)-L_h^1(n,x)L_h^2(n-2,x)]$$

and

$$c=[L_h^1(n,x)L_h^2(n-1,x)-L_h^1(n-1,x)L_h^2(n,x)].$$

Now $3^3=27$ cases arise for $a,b,c\gtreqless 0$.

In this paper, we consider three cases and the rest of the cases can be analysed in similar ways.

Case 1 When $a,b,c>0$.

For this case, by (36), we have

$$\begin{aligned}\frac{e_3}{e_1}>u \text{ where } u=\frac{e_2}{e_1}&[\frac{L_h^1(n-1,x)L_h^3(n-3,x)-L_h^3(n-1,x)L_h^1(n-2,x)}{L_h^1(n-1,x)L_h^2(n-2,x)-L_h^1(n-2,x)L_h^2(n-1,x)}]\\&+\frac{L_h^3(n-1,x)L_h^2(n-2,x)-L_h^2(n-1,x)L_h^3(n-3,x)}{L_h^1(n-1,x)L_h^2(n-2,x)-L_h^1(n-2,x)L_h^2(n-1,x)}.\end{aligned}\tag{39}$$

By (37), we get

$$\begin{aligned}\frac{e_3}{e_1}<v \text{ where } v=\frac{e_2}{e_1}&[\frac{L_h^3(n,x)L_h^1(n-2,x)-L_h^1(n,x)L_h^3(n-3,x)}{L_h^1(n-2,x)L_h^2(n,x)-L_h^1(n,x)L_h^2(n-2,x)}]\quad+\\&\frac{L_h^2(n,x)L_h^3(n-3,x)-L_h^3(n,x)L_h^2(n-2,x)}{L_h^1(n-2,x)L_h^2(n,x)-L_h^1(n,x)L_h^2(n-2,x)}.\end{aligned}\tag{40}$$

By (39) and (40), we get

$$\frac{e_1}{e_2}>\frac{L_h^1(n-2,x)}{L_h^2(n-2,x)}\quad ,using(23).\tag{41}$$

By (38), we get

$$\frac{e_3}{e_1} > w \text{ where } w = \frac{e_2}{e_1}\left[\frac{L_h^1(n,x)L_h^3(n-1,x) - L_h^1(n-1,x)L_h^3(n,x)}{L_h^1(n,x)L_h^2(n-1,x) - L_h^1(n-1,x)L_h^2(n,x)}\right] \quad + \\ \frac{L_h^2(n-1,x)L_h^3(n,x) - L_h^2(n,x)L_h^3(n-1,x)}{L_h^1(n,x)L_h^2(n-1,x) - L_h^1(n-1,x)L_h^2(n,x)}. \quad (42)$$

By (40) and (42), we get

$$\frac{e_1}{e_2} < \frac{L_h^1(n,x)}{L_h^2(n,x)} \quad , \text{ using } (23). \quad (43)$$

By (41) and (43), we get

$$\frac{L_h^1(n-2,x)}{L_h^2(n-2,x)} < \frac{e_1}{e_2} < \frac{L_h^1(n,x)}{L_h^2(n,x)}. \quad (44)$$

Similarly, we get

$$\frac{L_h^2(n-2,x)}{L_h^3(n-2,x)} < \frac{e_2}{e_3} < \frac{L_h^2(n,x)}{L_h^3(n,x)} \quad and \quad \frac{L_h^1(n-2,x)}{L_h^3(n-2,x)} < \frac{e_1}{e_3} < \frac{L_h^1(n,x)}{L_h^3(n,x)}. \quad (45)$$

Case 2 When $a = 0,\ b, c > 0$.

By (36), we get

$$\frac{e_1}{e_2} > \frac{L_h^1(n-2,x)}{L_h^2(n-2,x)} \quad , using\ a = 0. \quad (46)$$

By (37) and (38), we get

$$\frac{e_1}{e_2} < \frac{L_h^1(n,x)}{L_h^2(n,x)} \quad , using(23)\ and\ a = 0. \quad (47)$$

By (46) and (47), we get

$$\frac{L_h^1(n-2,x)}{L_h^2(n-2,x)} < \frac{e_1}{e_2} < \frac{L_h^1(n,x)}{L_h^2(n,x)}. \quad (48)$$

Similarly, we get

$$\frac{L_h^2(n-2,x)}{L_h^3(n-2,x)} < \frac{e_2}{e_3} < \frac{L_h^2(n,x)}{L_h^3(n,x)} \quad and \quad \frac{L_h^1(n-2,x)}{L_h^3(n-2,x)} < \frac{e_1}{e_3} < \frac{L_h^1(n,x)}{L_h^3(n,x)}. \quad (49)$$

Case 3 When $a, b, c < 0$.

In this case, by (36), we have

$$\frac{e_3}{e_1} < u \text{ where } u = \frac{e_2}{e_1}\Big[\frac{L_h^1(n-1,x)L_h^3(n-3,x) - L_h^3(n-1,x)L_h^1(n-2,x)}{L_h^1(n-1,x)L_h^2(n-2,x) - L_h^1(n-2,x)L_h^2(n-1,x)}\Big] + \frac{L_h^3(n-1,x)L_h^2(n-2,x) - L_h^2(n-1,x)L_h^3(n-3,x)}{L_h^1(n-1,x)L_h^2(n-2,x) - L_h^1(n-2,x)L_h^2(n-1,x)}. \tag{50}$$

By (37), we get

$$\frac{e_3}{e_1} > v \text{ where } v = \frac{e_2}{e_1}\Big[\frac{L_h^3(n,x)L_h^1(n-2,x) - L_h^1(n,x)L_h^3(n-3,x)}{L_h^1(n-2,x)L_h^2(n,x) - L_h^1(n,x)L_h^2(n-2,x)}\Big] + \frac{L_h^2(n,x)L_h^3(n-3,x) - L_h^3(n,x)L_h^2(n-2,x)}{L_h^1(n-2,x)L_h^2(n,x) - L_h^1(n,x)L_h^2(n-2,x)}. \tag{51}$$

By (50) and (51), we get

$$\frac{e_1}{e_2} < \frac{L_h^1(n-2,x)}{L_h^2(n-2,x)} \quad \text{, using (23).} \tag{52}$$

By (38), we get

$$\frac{e_3}{e_1} < w \text{ where } w = \frac{e_2}{e_1}\Big[\frac{L_h^1(n,x)L_h^3(n-1,x) - L_h^1(n-1,x)L_h^3(n,x)}{L_h^1(n,x)L_h^2(n-1,x) - L_h^1(n-1,x)L_h^2(n,x)}\Big] + \frac{L_h^2(n-1,x)L_h^3(n,x) - L_h^2(n,x)L_h^3(n-1,x)}{L_h^1(n,x)L_h^2(n-1,x) - L_h^1(n-1,x)L_h^2(n,x)}. \tag{53}$$

By (51) and (53), we get

$$\frac{e_1}{e_2} > \frac{L_h^1(n,x)}{L_h^2(n,x)} \quad \text{, using (23).} \tag{54}$$

By (52) and (54), we get

$$\frac{L_h^1(n,x)}{L_h^2(n,x)} < \frac{e_1}{e_2} < \frac{L_h^1(n-2,x)}{L_h^2(n-2,x)}. \tag{55}$$

Similarly, we get

$$\frac{L_h^2(n,x)}{L_h^3(n,x)} < \frac{e_2}{e_3} < \frac{L_h^2(n-2,x)}{L_h^3(n-2,x)} \text{ and } \frac{L_h^1(n,x)}{L_h^3(n,x)} < \frac{e_1}{e_3} < \frac{L_h^1(n-2,x)}{L_h^3(n-2,x)}. \tag{56}$$

Therefore, for the large value of n, we get

$$\frac{e_1}{e_2} \approx \mu,\ \frac{e_2}{e_3} \approx \mu \text{ and } \frac{e_1}{e_3} \approx \mu^2,$$

where

$$\mu = \frac{h(x)}{3} - \frac{2^{\frac{1}{3}}(-3 - h^2(x))}{3[27 + 9h(x) + 2h^3(x) + 3\sqrt{3}(\sqrt{23 + 18h(x) - h^2(x) + 4h^3(x)})]^{\frac{1}{3}}}$$

$$+ \frac{(27 + 9h(x) + 2h^3(x) + 3\sqrt{3}\sqrt{23 + 18h(x) - h^2(x) + 4h^3(x)})^{\frac{1}{3}}}{3(2)^{\frac{1}{3}}}.$$

Similarly, we get

$$\frac{e_4}{e_5} \approx \mu, \ \frac{e_5}{e_6} \approx \mu, \ \frac{e_4}{e_6} \approx \mu^2, \text{ and}$$

$$\frac{e_7}{e_8} \approx \mu, \ \frac{e_8}{e_9} \approx \mu, \ \frac{e_7}{e_9} \approx \mu^2.$$

2.5. Generalized relations among the code matrix elements for U_n matrix of order m

In general, we can establish the relations among the code matrix elements as

$$\frac{L_h^1(n-(m-1),x)}{L_h^2(n-(m-1),x)} > \frac{e_1}{e_2} > \frac{L_h^1(n,x)}{L_h^2(n,x)},$$

$$\frac{L_h^2(n-(m-1),x)}{L_h^3(n-(m-1),x)} > \frac{e_2}{e_3} > \frac{L_h^2(n,x)}{L_h^3(n,x)},$$

$\cdots\cdots\cdots$

$\cdots\cdots\cdots$

$\cdots\cdots\cdots$

$$\frac{L_h^{m-1}(n-(m-1),x)}{L_h^m(n-(m-1),x)} > \frac{e_{m-1}}{e_m} > \frac{L_h^{m-1}(n,x)}{L_h^m(n,x)},$$

$$\frac{L_h^1(n-(m-1),x)}{L_h^3(n-(m-1),x)} > \frac{e_1}{e_3} > \frac{L_h^1(n,x)}{L_h^3(n,x)},$$

$$\frac{L_h^2(n-(m-1),x)}{L_h^4(n-(m-1),x)} > \frac{e_2}{e_4} > \frac{L_h^2(n,x)}{L_h^4(n,x)},$$

$$\cdots\cdots\cdots$$

$$\cdots\cdots\cdots$$

$$\cdots\cdots\cdots$$

$$\frac{L_h^{m-2}(n-(m-1),x)}{L_h^m(n-(m-1),x)} > \frac{e_{m-2}}{e_m} > \frac{L_h^{m-2}(n,x)}{L_h^m(n,x)},$$

and

$$\frac{L_h^1(n-(m-1),x)}{L_h^4(n-(m-1),x)} > \frac{e_1}{e_4} > \frac{L_h^1(n,x)}{L_h^4(n,x)},$$

$$\frac{L_h^2(n-(m-1),x)}{L_h^5(n-(m-1),x)} > \frac{e_2}{e_5} > \frac{L_h^2(n,x)}{L_h^5(n,x)},$$

$$\cdots\cdots\cdots$$

$$\cdots\cdots\cdots$$

$$\cdots\cdots\cdots$$

$$\frac{L_h^{m-3}(n-(m-1),x)}{L_h^m(n-(m-1),x)} > \frac{e_{m-3}}{e_m} > \frac{L_h^{m-3}(n,x)}{L_h^m(n,x)},$$

$$\frac{L_h^1(n-(m-1),x)}{L_h^m(n-(m-1),x)} > \frac{e_1}{e_m} > \frac{L_h^1(n,x)}{L_h^m(n,x)}.$$

Therefore, for the large value of n, we get

$\frac{e_1}{e_2} \approx \nu,\ \frac{e_2}{e_3} \approx \nu,\ \cdots, \frac{e_{m-1}}{e_m} \approx \nu,$

$\frac{e_1}{e_3} \approx \nu^2,\ \frac{e_2}{e_4} \approx \nu^2,\ \cdots, \frac{e_{m-2}}{e_m} \approx \nu^2,$

$\cdots$

$\cdots$

$\frac{e_1}{e_m} \approx \nu^{m-1},$

where e_1, e_2, $e_3, \cdots, e_{m-1}$, e_m are the first row elements of the code matrix and

$$\nu = \lim_{n\longrightarrow\infty} \frac{L_h^i(n,x)}{L_h^{i+1}(n,x)} \quad \text{where } i = 1, 2, \cdots, m-1.$$

We also find similar type of relations for second row elements, third row elements, $\cdots$, mth row elements.

2.6. Error detection and correction

In 2016, Prasad (2016) showed how to detect and correct the errors in the code message by using the Lucas coding and decoding theory. For $m = 2$, this method also allows to correct 14 cases among $({}^4C_1 +^4 C_2 +^4 C_3 +^4 C_4) = 2^4 - 1 = 15$ cases similar to [these from] Prasad (2016). It means that correct ability of this method is $\frac{14}{15} = 0.9333 = 93.33\%$.

Now we consider error detection and correction for case $m = 3$

$$M = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix}, V_3 = \begin{pmatrix} L_h^1(n,x) & L_h^2(n,x) & L_h^3(n,x) \\ L_h^1(n-1,x) & L_h^2(n-1,x) & L_h^3(n-1,x) \\ L_h^1(n-2,x) & L_h^2(n-2,x) & L_h^3(n-2,x) \end{pmatrix},$$

$$E = M \times V_3 =$$
$$\begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix} \begin{pmatrix} L_h^1(n,x) & L_h^2(n,x) & L_h^3(n,x) \\ L_h^1(n-1,x) & L_h^2(n-1,x) & L_h^3(n-1,x) \\ L_h^1(n-2,x) & L_h^2(n-2,x) & L_h^3(n-2,x) \end{pmatrix}$$
$$= \begin{pmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix}.$$

The code matrix, E, may contain single, double, $\cdots$, nine fold errors. Thus, there are

$${}^9C_1 +^9 C_2 +^9 C_3 +^9 C_4 +^9 C_5 +^9 C_6 +^9 C_7 +^9 C_8 +^9 C_9 = 2^{3^2} - 1 = 511$$

codes of errors in the code matrix, E. We use hypotheses from Prasad (2016) for single error, double error, $\cdots$, nine fold errors. The nine fold error of the code matrix is not correctable so the ability to correct eight cases of this method is $\frac{510}{511} = 0.9980 = 99.80$

In general, the correct ability of this method is

$$\frac{2^{m^2} - 2}{2^{m^2} - 1}.$$

Therefore, for large value of m the correct ability of the method is

$$\frac{2^{m^2} - 2}{2^{m^2} - 1} \approx 1 = 100\%.$$

3. Roles of polynomials in cryptography protection

Polynomials have a prominent position in mathematics. Day by day, its importance has become hihghly prominent in cryptography. The role of polynomials is very important in encryption and decryption for security purposes. The security and complexity are increasing very fast when the degree of polynomials is increasing.

4. Conclusion

The Lucas coding and decoding method is the main application of the $h(x)$ Lucas polynomials of order m and U_n matrix, whose elements are Lucas polynomials of order m. The correcting and detecting abilities of this method are very high in comparison to the classical algebraic coding and decoding method. When the degree of polynomial $h(x)$ increases, then the security and complexity of this method also increases very fast. In the future, we hope that this method will lead to hybrid cryptosystems, which are very fast and good in encryption and decryption.

5. Acknowledgments

The author would like to thank the reviewers and the editor for their valuable comments and suggestion for the improvement of this paper.

References

Basu, M. and Prasad, B. (2009) The generalized relations among the code elements for Fibonacci coding theory. *Chaos, Solitons and Fractals*, 41, 2517-2525.

Blahut, R. (1983) *The Theory and Practice of Error Control Codes.* Addison-Wesley, Reading, MA.

Cover, T.M. and Thomas, J.A.(1991) *Elements of Information Theory.* A Wiley-Interscience Publication. New York

El Naschie, M.S. (2009) The theory of Cantorian space time and high energy particle physics. *Chaos, Solitons and Fractals*, 41, 2635-2646.

Esmaeeili, M., Gulliver, T.A. and Kakhbod, A. (2009) The Golden mean, Fibonacci matrices and partial weakly super-increasing sources. *Chaos, Solitons and Fractals*, 42, 435-440.

Hohn, F.E. (1973) *Elementary Matrix Algebra.* Macmillan Company, New York.

MacWilliams, F.J. and Sloane, N.J.A. (1977) *Theory of Error-Correcting Codes.* North-Holland. Amsterdam

Nalli, A. and Haukkanen, P. (2009) On generalized Fibonacci and Lacus polynomials. *Chaos, Solitons and Fractals*, 42, 3179-3186.

Prasad, B. (2015) Coding theory on $h(x)$ extension of m sequences for Fibonacci numbers. *Discrete Mathematics, Algorithms and Applications*, **7**, 2, 1550008 (18 pages).

Prasad, B. (2016) Coding theory on Lucas p-numbers. *Discrete Mathematics, Algorithms and Applications*, **8**, 4, 1650074 (17 pages).

Prasad, B. (2019) Corrigendum: Coding theory on the m-extension of the Fibonacci p -numbers. *Chaos, Solitons and Fractals*, Article in press.

Stakhov, A.P. (1977) *Introduction into algorithm measurement theory.* Soviet Radio, Moscow (In Russian).

Stakhov, A.P. (2006) Fibonacci matrices, a generalization of the cassini formula and a new coding theory. *Chaos, Solitons and Fractals*, 30, 56-66.

Tasci, D. and Kilic, E. (2004) On the order k generalized Lucas numbers. *Appl Math Comput*, 155, 637-641.