Control and Cybernetics

vol. **44** (2015) No. 4

Multivariable extension of m sequences for Fibonacci numbers in cryptography*

by

Bandhu Prasad

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

Abstract: In this paper, we introduce multivariable extension of m sequences of the Fibonacci number polynomials of order m and a new S_n matrix of order m. Consequently, we discuss various properties of the S_n matrix. The polynomial, derived therefrom, h_j, contains m multiple variables which improves the cryptography protection and security, and complexity increases as m increases.

Keywords: Fibonacci p-numbers, Fibonacci numbers of order m, golden mean, code matrix

1. Introduction

The Fibonacci p-numbers are defined by the recurrence relation:

$$F_p(n) = F_p(n-1) + F_p(n-p-1) \quad \text{for} \quad n > p+1 \tag{1}$$

with the initial seeds

$$F_p(1) = F_p(2) = F_p(3) = \cdots = F_p(p+1) = 1 \tag{2}$$

where $p = 0, 1, 2, 3, \cdots$.

For $p = 1$, the Fibonacci p-numbers coincide with the classical Fibonacci numbers, $F_n = F_1(n)$ (see Stakhov, 1977). The Fibonacci numbers, F_n and golden mean,

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

have appeared in arts, sciences, high energy physics and information and coding theory (see Cover and Thomas, 1991; El Naschie, 2009; Esmaeili, Gulliver and Kakhbod, 2009; MacWilliams and Sloane, 1977, or Stakhov, 2006).

*Submitted: May 2015; Accepted: April 2016

In 1960, Miles (1960) introduced the generalized k-Fibonacci numbers by the following recurrence relation

$$F_n = F_{n-1} + F_{n-2} + \cdots + F_{n-k}, \quad n > k \geq 2$$

with the initial seeds

$$F_1 = F_2 = \cdots = F_{n-k} = 0, F_{k-1} = F_k = 1.$$

Then, Er (1984) introduced k sequences of the Fibonacci numbers of order k, by the following recurrence relation

$$u_n^i = c_1 u_{n-1}^i + c_2 u_{n-2}^i + \cdots + c_k u_{n-k}^i, \quad n \geq 2$$

with the initial value for u_n^i being given for $1-k \leq n \leq 0$ through the relation:

$$u_n^i = \begin{cases} 1 & \text{if } i = 1-n, \\ 0 & \text{otherwise,} \end{cases}$$

where $c_1, c_2, \cdots, c_k$ are constant coefficients, i is an index, not an exponent, and the index i is an integer having only k values: $i = 1, 2, 3, \cdots, k$ with $k \geq 2$, while u_n^i is the nth term of the ith generalized Fibonacci numbers.

Er (1984) showed that

$$\begin{pmatrix} u_{n+1}^i \\ u_n^i \\ \cdot \\ \cdot \\ \cdot \\ u_{n-k+2}^i \end{pmatrix} = A \begin{pmatrix} u_n^i \\ u_{n-1}^i \\ \cdot \\ \cdot \\ \cdot \\ u_{n-k+1}^i \end{pmatrix}$$

where

$$A = \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_{k-1} & c_k \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Again, Er (1984) derived the following relation

$$G_{n+1} = AG_n$$

where

$$G_n = \begin{pmatrix} u_n^1 & u_n^2 & \cdots & u_n^k \\ u_{n-1}^1 & u_{n-1}^2 & \cdots & u_{n-1}^k \\ \vdots & \vdots & \ddots & \vdots \\ u_{n-k+1}^1 & u_{n-k+1}^2 & \cdots & u_{n-k+1}^k \end{pmatrix}.$$

The Fibonacci polynomials are defined by the Fibonacci-like recurrence relations. In 1883, the famous Belgian mathematician Eugene Charles Catalan* defined the recurrence relation

$$F_n(x) = xF_{n-1}(x) + F_{n-2}(x), \quad n \geq 3$$

with the initial seeds

$$F_1(x) = 1, \quad F_2(x) = x.$$

Later on, the German mathematician Ernst Jacobsthal defined the Fibonacci polynomials by the following recurrence relation

$$J_n(x) = J_{n-1}(x) + xJ_{n-2}(x), \quad n \geq 3$$

with the initial seeds

$$J_1(x) = J_2(x) = 1.$$

We would also like to refer to Paul F. Byrd (see, e.g., Byrd, 1975), who defined the recurrence relation

$$\phi_n(x) = x\phi_{n-1}(x) + \phi_{n-2}(x), \quad n \geq 2$$

with the initial seeds

$$\phi_0(x) = 0, \phi_1(x) = 1.$$

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

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

and the initial seeds

$$F_{h,0}(x) = 0, F_{h,1}(x) = 1.$$

We obtain therefrom the Catalan's Fibonacci polynomials for $h(x) = x$ and Byrd's Fibonacci polynomials for $h(x) = 2x$.

Prasad (2015) introduced $h(x)$ (> 0) extension of m sequences of the Fibonacci numbers polynomials of order m, $F_h^i(n, x)$, by the recurrence relation

$$F_h^i(n, x) = h(x)F_h^i(n-1, x) + F_h^i(n-2, x) + \cdots + F_h^i(n-m, x) \tag{4}$$

with the initial values for $F_h^i(n, x)$ being given for $1 - k \leq n \leq 0$ through the relation:

$$F_h^i(n, x) = \begin{cases} 1 & \text{if } n + i = 1, \\ 0 & \text{otherwise,} \end{cases}$$

*In the literature, the constructs recalled or implied here, are considered as Fibonacci, Bernoulli, Euler and Lucas numbers or sequences, see e.g., Koshy (2001) (ed.)

where $h(x)$ (> 0) is a polynomial with real coefficients, i is an index, not an exponent, and the index i is an integer having only m values: $i = 1, 2, 3, \cdots, m$ with $m \geq 2$, and $F_h^i(n, x)$ is the nth term of the ith generalized Fibonacci numbers polynomials.

In this paper, we introduce h_j (> 0) extension of m sequences of the Fibonacci numbers polynomials of order m, $F^i_{h_1,h_2,\cdots,h_m}(n, x_1, x_2, \cdots, x_m)$, by the recurrence relation

$$\begin{aligned} F^i_{h_1,h_2,\cdots,h_m}(n, x_1, \cdots, x_m) &= \\ h_1 F^i_{h_1,h_2,\cdots,h_m}(n-1, x_1, \cdots, x_m) &+ \\ h_2 F^i_{h_1,h_2,\cdots,h_m}(n-2, x_1, \cdots, x_m) & \\ + \cdots + h_m F^i_{h_1,h_2,\cdots,h_m}(n-m, x_1, \cdots, x_m) & \end{aligned} \tag{5}$$

with the initial values for $F^i_{h_1,h_2,\cdots,h_m,}(n, x_1, x_2, \cdots, x_m)$ being given for $1 - k \leq n \leq 0$ through the relation:

$$F^i_{h_1,h_2,\cdots,h_m}(n, x_1, x_2, \cdots, x_m) = \begin{cases} 1 & \text{if } n + i = 1, \\ 0 & \text{otherwise,} \end{cases}$$

where $j = 1, 2, \cdots, m$, the index i is an integer having only m values: $i = 1, 2, 3, \cdots, m$ with $m \geq 2$, and h_j (> 0) are polynomials, while $x_1, x_2, \cdots, x_m$ are non negative integers, so that h_j are positive integers and

$$F^i_{h_1,h_2,\cdots,h_m}(n, x_1, x_2, \cdots, x_m)$$

is the nth term of the ith generalized Fibonacci numbers polynomials.

The characteristic equation of m sequences of the Fibonacci numbers polynomials of order m is

$$y^m - y^{m-1} - y^{m-2} - \cdots - y - 1 = 0. \tag{6}$$

The equation (6) 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

$$\begin{pmatrix} F^i_{h_1,h_2,\cdots,h_m}(n+1, x_1, x_2, \cdots, x_m) \\ F^i_{h_1,h_2,\cdots,h_m}(n, x_1, x_2, \cdots, x_m) \\ \cdot \\ \cdot \\ \cdot \\ F^i_{h_1,h_2,\cdots,h_m}(n-m+2, x_1, x_2, \cdots, x_m) \end{pmatrix} =$$

$$Q_{h_1,h_2,\cdots,h_m}\begin{pmatrix} F^i_{h_1,h_2,\cdots,h_m}(n,x_1,x_2,\cdots,x_m) \\ F^i_{h_1,h_2,\cdots,h_m}(n-1,x_1,x_2,\cdots,x_m) \\ . \\ . \\ . \\ F^i_{h_1,h_2,\cdots,h_m}(n-m+1,x_1,x_2,\cdots,x_m) \end{pmatrix}$$

where

$$Q_{h_1,h_2,\cdots,h_m} = \begin{pmatrix} h_1 & h_2 & h_3 & \cdots & h_{m-1} & h_m \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

2. The S_n matrix and its properties

In this section, we define a new S_n matrix of order m. The matrix S_n is given by

$$S_n = \begin{pmatrix} F(1,n) & F(2,n) & \cdots & F(m,n) \\ F(1,n-1) & F(2,n-1) & \cdots & F(m,n-1) \\ \cdots & \cdots & \cdots & \cdots \\ F(1,n-m+1) & F(2,n-m+1) & \cdots & F(m,n-m+1) \end{pmatrix}, \quad (7)$$

where $\quad F(v,w) = F^v_{h_1,h_2,\cdots,h_m}(w,x_1,x_2,\cdots,x_m)$.

We prove that $S_n = Q^n_{h_1,h_2,\cdots,h_m}$.
Proof: We refer to the previously introduced notation $F(v,w)$.

$$S_n = \begin{pmatrix} h_1 & h_2 & h_3 & \cdots & h_{m-1} & h_m \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$
$$\begin{pmatrix} F(1,n-1) & F(2,n-1) & \cdots & F(m,n-1) \\ F(1,n-2) & F(2,n-2) & \cdots & F(m,n-2) \\ \cdots & \cdots & \cdots & \cdots \\ F(1,n-m) & F(2,n-m) & \cdots & F(m,n-m) \end{pmatrix}$$

$$= Q_{h_1,h_2,\cdots,h_m} S_{n-1}.$$

Therefore, we can write

$$S_n = Q_{h_1,h_2,\cdots,h_m}(Q_{h_1,h_2,\cdots,h_m} S_{n-2}) = \cdots = Q^{n-1}_{h_1,h_2,\cdots,h_m} S_1.$$

Now,

$$S_1 = \begin{pmatrix} h_1 & h_2 & h_3 & \cdots & h_{m-1} & h_m \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} F(1,0) & F(2,0) & \cdots & F(m,0) \\ F(1,-1) & F(2,-1) & \cdots & F(m,-1) \\ \cdots & \cdots & \cdots & \cdots \\ F(1,1-m) & F(2,1-m) & \cdots & F(m,1-m) \end{pmatrix}$$

$$= \begin{pmatrix} h_1 & h_2 & h_3 & \cdots & h_{m-1} & h_m \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = Q_{h_1,h_2,\cdots,h_m}$$

Hence, $S_n = Q^n_{h_1,h_2,\cdots,h_m}$.

THEOREM 1 *For matrix S_n of order m in (7) for $n \geq 1$ and $m \geq 2$*

$$Det\ S_n = \begin{cases} (h_m)^n & \text{if } m \text{ is odd,} \\ (-1)^n (h_m)^n & \text{if } m \text{ is even.} \end{cases}$$

PROOF:
$Det\ S_n = Det\ (Q^n_{h_1,h_2,\cdots,h_m}) = (Det\ Q_{h_1,h_2,\cdots,h_m})^n$ as $Det\ Q_{h_1,h_2,\cdots,h_m} = (-1)^{m+1} h_m$ for $m \geq 2$.
Hence, we get

$$Det\ S_n = \begin{cases} (h_m)^n & \text{if } m \text{ is odd,} \\ (-1)^n (h_m)^n & \text{if } m \text{ is even.} \end{cases}$$

3. Fibonacci encryption and decryption method

We represent the initial message in the form of the non singular square matrix M of order m where $m \geq 2$. We take the S_n matrix of order m as the encryption matrix and its inverse matrix S_n^{-1} as the decryption matrix. We refer to the transformation $M \times S_n = E$ as encryption and to the transformation $E \times S_n^{-1} = M$ as decryption. We define E as code matrix.

4. Roles of multiple variables

The role of multiple variables is very important in encryption and decryption according to this method. By imposing m multiple variables $x_1, x_2, \cdots, x_m$, we can consider the combinations $x_1x_2, x_1x_3, x_1x_4, x_1x_5, \cdots,$ $x_1x_m, x_2x_3, x_2x_4, \cdots,$ $x_2x_m, x_1x_2x_3, x_1x_2x_4, x_1x_2x_5, \cdots,$ $x_1x_2x_m,$ $x_1x_2x_3x_4, x_1x_2x_3x_5, \cdots, x_1x_2x_3x_m$ etc. i.e. all the possible combinations of the variables. They are used in encryption and decryption for security purposes. When the number of variables increases the security and complexity of this methods also increases.

5. Conclusion

In this paper, encryption and decryption is proposed, based on multiple variables $x_1, x_2, x_3, \cdots, x_m$ and complexity of this method increases due to the use of multiple variables. In the future, we hope that this method can lead to hybrid cryptosystems, which will be very fast and effective in encryption and decryption.

Acknowledgement

The author would like to thank the anonymous referees for their comments, which have helped in improving the presentation and clarity of the paper.

References†

Byrd, P.E. (1975) New relations between Fibonacci and Bernoulli numbers. *The Fibonacci Quarterly* **13**, 1, 59–69.

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.

Er M.C. (1984) Sums of Fibonacci numbers by matrix methods. *The Fibonacci Quarterly* **22**, 204–207.

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

Koshy, Th. (2001) *Fibonacci and Lucas Numbers with Applications.* J. Wiley & Sons, New York.

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

Miles EP. (1960) Generalized Fibonacci numbers and associated matrices. *Am. Math. Month.* 67, 745-752.

†In view of the diverse, and often quate extreme, opinions, regarding some of the journals, referred to here, the Editors would like to emphasize that this paper has been subject to a scrupulous review precedure, involving three independent referees from three different academic centres and from different countries, and has been modified several times over (ed.)

NALLI A., HAUKKANEN P. (2009) On generalized Fibonacci and Lucas 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), 1550008–1550025.

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.