JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p. 93-98
https://publishoa.com
ISSN: 1309-3452

A New Application of Generalized k-Horadam Sequence in Coding Theory

G. Srividhya[1], E. Kavitha Rani[2]
[1.] Assistant Professor, Department of Mathematics, Government Arts College. Trichy, Tamil Nadu, South India.
[2.] Guest lecturer, Department of Mathematics, Government Arts College. Trichy -22, Tamil Nadu, South India.

Received 2022 March 15; **Revised** 2022 April 20; **Accepted** 2022 May 10.

Abstract

This paper describes a brand new coding and decoding technique using the generalized k-Horadam sequence. Our version is based on a blocked message matrix and encryption of every message matrix with a special key. Experiment with this result in the Jacobsthal sequence.

Keywords: Coding and decoding algorithm, Generalized k-Horadam Sequence, Jacobsthal Sequence.

AMS subject classification (2010): 68P30, 11B39, 11B37, 14G50, 11T71

Introduction

Encoding and deciphering algorithms are very crucial to help protection. Because of the reality facts protection is a extra great hassle in modern years.

This paper delineate about the application of generalized k-Horadam sequences in coding theory. Yasin Yazlik [8] discussed the generalized k-Horadam sequence. There are many authors, such as Hoggat, Koshy, Fikri Koken and Durmus Bozkart [1] Uterate about Fibonacci, Jacobsthal sequence.

NihalTas, Sumerya Ucar, Nihal Yilmaz Ozgur [3], [4] provides brief literature on the encoding and decoding methods of various sequences of such as Pell, Fibonacci and Lucas. The study by Stakhove [6] has been a great inspiration for introducing this paper.

In this study we instigate an algorithm for enciphering and deciphering the generalized k-Horadam sequence. We extend this result more concretely for Jacobsthal sequence.

Basic Definitions:

Generalized k-Horadam sequences are defined by Yasin Yazlik, Necati Taskara [8] as

$$H_{k,n+2} = f(k)H_{k,n+1} + g(k)H_{k,n} \qquad (1)$$

With $H_{k,0} = a, H_{k,1} = b$

The equation (1) representing the linear difference equation of second order whose characteristic equation can be written as $\lambda^2 = f(k)\lambda + g(k)$. The real roots of this equation are

$$r_1 = \frac{f(k)+\sqrt{f^2(k)+4g(k)}}{2},\ r_2 = \frac{f(k)-\sqrt{f^2(k)+4g(k)}}{2}, (r_1 > r_2)$$

$$r_1 + r_2 = f(k),\ r_1 - r_2 = \sqrt{f^2(k) + 4g(k)},\ r_1 r_2 = -g(k) \qquad (2)$$

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p. 93-98
https://publishoa.com
ISSN: 1309-3452

This definition can be reduced to certain special cases depending on the choice of parameters$(a, b, f(k), g(k))$.

Table – 1

S.no	Name of the sequences	$(a, b, k, f(k), g(k))$
1.	Generalized k-Fibonacci sequence	$(a, b, 1, k, 1)$
2.	k-Fibonacci sequence	$(0, 1, 1, k, 1)$
3.	k-Lucas sequence	$(2, k, 1, k, 1)$
4.	Horadam sequence	$(a, b, 1, p, q)$
5.	Fibonacci sequence	$(0, 1, 1, 1, 1)$
6.	Lucas sequence	$(2, 1, 1, 1, 1)$
7.	Pell sequence	$(0, 1, 1, 2, 1)$
8.	Jacobsthal sequence	$(0, 1, 1, 1, 2)$
9.	Jacobsthal Lucas sequence	$(2, 1, 1, 1, 2)$
10.	Mersenne sequence	$(0, 1, 1, 3, -2)$
11.	Fermat sequence	$(1, 3, 1, 3, 2)$

Matrix Representation:

By using the concepts of Yasin Yazlik, Necati Taskara [8] we can take the matrix as

$H_n = \left(H_{k,n-1}\ H_{k,n}\ H_{k,n}\ H_{k,n+1}\right)$ for $n \geq 1$,

We can write $|H_n| = \left(-g(k)\right)^{n-1}\left(a^2 g(k) + abf(k) - b^2\right)$ (3)

Main Results:

We put our message in an even size matrix by adding zero between the two words and the end of the message until we receive the message grid size to be even.

Partition the message square matrix M of size 2m into block matrices named Di (1≤i≤m^2) of size

2 × 2 from left to right. We assemble a brand new coding method and provide an explanation for the symbol of our coding method. Let us assume that the matrices D_i, L_i, H_n are following

$D_i = \left(d_1^i\ d_2^i\ d_3^i\ d_4^i\right)$, $L_i = \left(L_1^i\ L_2^i\ L_3^i\ L_4^i\right)$, $H_n = \left(H_{k,n-1}\ H_{k,n}\ H_{k,n}\ H_{k,n+1}\right)$

Number of block matrix D_i can be represented by b.In accordance with. b we choose the number n as below

$n = \begin{cases} b & b \leq 3 \\ \left[\left|\frac{b}{2}\right|\right] & b > 3 \end{cases}$

By the help of chosen n, we define alphabets table according to mod 34 (This table can be expanded depending on the characters used in the message matrix)

A	B	C	D	E
n	$n+1$	$n+2$	$n+3$	$n+4$
F	G	H	I	J
$n+5$	$n+6$	$n+7$	$n+8$	$n+9$
K	L	M	N	O
$n+10$	$n+11$	$n+12$	$n+13$	$n+14$
P	Q	R	S	T
$n+15$	$n+16$	$n+17$	$n+18$	$n+19$
U	V	W	X	Y
$n+20$	$n+21$	$n+22$	$n+23$	$n+24$

Z	0	!	?	.
$n+25$	$n+26$	$n+27$	$n+28$	$n+29$
+	-	×	÷	
$n+30$	$n+31$	$n+32$	$n+33$	

We can introduce generalized k-Horadam sequence coding and decoding with the transformation.

$D_i \times H_n = L_i$

$Det(L_i) = Det(D_i \times H_n) \qquad = Det\ D_i \times Det\ H_n \left| L_1^i\ L_2^i\ L_3^i\ L_4^i \right|$
$= \left| d_1^i\ d_2^i\ d_3^i\ d_4^i \right| \left| H_{k,n-1}\ H_{k,n}\ H_{k,n}\ H_{k,n+1} \right| \qquad (4) L_1^i = d_1^i H_{k,n-1} + d_2^i H_{k,n} (1 \le i \le m^2) L_2^i$
$= d_1^i H_{k,n} + d_2^i H_{k,n+1} L_3^i = d_3^i H_{k,n-1} + d_4^i H_{k,n} L_4^i = d_3^i H_{k,n} + d_4^i H_{k,n+1}$

Let us name it as $Det\ D_i = r_i$ and from (3)

$$Det\ H_n = \left(-g(k)\right)^{n-1}(a^2 g(k) + abf(k) - b^2) \qquad (5)$$

Let $d_3^i = x_i$ Equation (4) also can be written as below for decoding by the substitution of (5)

$$\left| L_1^i\ L_2^i\ x_i H_{k,n-1} + d_4^i H_{k,n}\ x_i H_{k,n} + d_4^i H_{k,n+1} \right|$$
$$= r_i\left(-g(k)\right)^{n-1}\left(a^2 g(k) + abf(k) - b^2\right) r_i\left(-g(k)\right)^{n-1}\left(a^2 g(k) + abf(k) - b^2\right)$$
$$= L_1^i\left(x_i H_{k,n} + d_4^i H_{k,n+1}\right) - L_2^i\left(x_i H_{k,n-1} + d_4^i H_{k,n}\right) \qquad (6)$$

Blocking Algorithm

Coding Algorithm:

Step 1: Divide the message matrix M into block D_i $(1 \le i \le m^2)$

Step 2: Select n.

Step 3: Find $d_j^i (1 \le j \le 4)$

Step 4: Determine $det\ det\ (D_i) \rightarrow r_i$

Step 5: Constructing $E = \left[r_i\ \ d_p^i\right]_{p \in \{1,2,4\}}$

Step 6: The algorithm is now complete.

Decoding Algorithm:

Step 1: Compute H_n for chosen n

Step 2: Compute L_1^i, L_2^i to construct L_i

$L_1^i = d_1^i H_{k,n-1} + d_2^i H_{k,n},\ L_2^i = d_1^i H_{k,n} + d_2^i H_{k,n+1} (1 \le i \le m^2)$

Step 3: Solve

$$r_i\left(-g(k)\right)^{n-1}(a^2 g(k) + abf(k) - b^2) = L_1^i\left(x_i H_{k,n} + d_4^i H_{k,n+1}\right) - L_2^i\left(x_i H_{k,n-1} + d_4^i H_{k,n}\right)$$

Step 4:

Substitute for $x_i = d_3^i$

Step 5:

Construct D_i

Step 6:

Construct message matrix M

Step 7:

End of Algorithm.

We can explain the above algorithm more specifically by choosing any of the special cases defined in table 1.

Here we are considering Jacobsthal Sequence.

Consider $f(k) = 1, g(k) = 2, a = 0, b = 1 \; and \; k = 1$

By the help of (1) we can rewrite equation of Jacobsthal sequence as $J_{1,n+2} = J_{1,n+1} + 2J_{1,n}$

From (3) $J_2 = [J_{1,1}\, J_{1,2}\, J_{1,2}\, J_{1,3}]$ (7)

Since $J_{1,0} = 0, J_{1,1} = 1, J_{1,2} = 1, J_{1,3} = 3$, Hence $J_2 = [1\ 1\ 1\ 3]$

Using Equation (4)

$$L_1^i = d_1^i(1) + d_2^i(1) \qquad L_2^i = d_1^i(1) + d_2^i(3) \quad where \quad (1 \le i \le 4) \tag{8}$$

Equation (6) can be simplified here as

$$r_i(-2)^{n-1}(-1) = L_1^i\left(x_i(1) + d_4^i(3)\right) - L_2^i\left(x_i(1) + d_4^i(1)\right) = L_1^i(x_i + 3d_4^i) - L_2^i(x_i + d_4^i) r_i(-1)^n 2^{n-1}$$
$$= L_1^i(x_i + 3d_4^i) - L_2^i(x_i + d_4^i) \tag{9}$$

Application:

Here we can discuss an example using above algorithm. Let us consider the message matrix for the message text "MATH SYMBOL + - * ."

Coding Algorithm:

Step 1:

Partition the message matrix M of size 4×4 matrices with the name label D_i $(1 \le i \le 4)$ from left to right, each of size 2×2

$M = [M\,A\,T\,H\ \ 0\,S\,Y\,M\ \ B\ +\ O\ -\ L\ *\ O\ .\ ]_{4\times4}$

$D_1 = [d_1^1\, d_2^1\, d_3^1\, d_4^1] = [M\ A\ 0\ S]$, $D_2 = [d_1^2\, d_2^2\, d_3^2\, d_4^2] = [T\ H\ Y\ M]$ $D_3 = [d_1^3\, d_2^3\, d_3^3\, d_4^3] = [B\ O\ +\ -]$, $D_4 = [d_1^4\, d_2^4\, d_3^4\, d_4^4] = [L\ 0\ *\ .]$

Step 2:

Since b represent number of Block Matrix $'D_i'$ hence $b = 4 \ge 3$

We find $n = \left[\left|\frac{b}{2}\right|\right] = 2$,

We can use the following character table for the message matrix M.

M	A	T	H	0	S	Y	M
14	2	21	9	28	20	26	14
B	0	L	0	+	-	*	.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p. 93-98
https://publishoa.com
ISSN: 1309-3452

3	16	13	28	32	33	34	31

Step 3:

We build components of the Block D_i $(1 \le i \le 4)$

$d_1^1 = 14$	$d_2^1 = 2$	$d_3^1 = 28$	$d_4^1 = 20$
$d_1^2 = 21$	$d_2^2 = 9$	$d_3^2 = 26$	$d_4^2 = 14$
$d_1^3 = 03$	$d_2^3 = 16$	$d_3^3 = 32$	$d_4^3 = 33$
$d_1^4 = 13$	$d_2^4 = 28$	$d_3^4 = 34$	$d_4^4 = 31$

Step 4:

Calculate determinant of r_i of the block matrix D_i

$D_1 = [M\ A\ 0\ S\ ] = [d_1^1\ d_2^1\ d_3^1\ d_4^1\ ] = [14\ 2\ 28\ 20\ ], r_1 = det\ det\ (D_1) = 280 - 56\ = 224$

$D_2 = [T\ H\ Y\ M\ ] = [d_1^2\ d_2^2\ d_3^2\ d_4^2\ ] = [21\ 9\ 26\ 14\ ], r_2 = det\ det\ (D_2) = 294 - 234\ = 60$

$$D_3 = [B\ 0\ -1\ -] = [d_1^3\ d_2^3\ d_3^3\ d_4^3\ ] = [3\ 16\ 32\ 33\ ], r_3 = det\ det\ (D_3) = 99 - 512\ = -413$$

$D_4 = [L\ 0\ *.] = [d_1^4\ d_2^4\ d_3^4\ d_4^4\ ] = [13\ 28\ 34\ 31\ ], r_1 = det\ det\ (D_4) = 403 - 952\ = -549$

Step 5:

Construct $E = \left[r_i, d_p^i\right], p \in \{1,2,4\} E = [224\ 14\ 2\ 20\ \ 60\ 21\ 9\ 14\ \ -413\ -549\ \ 3\ 13\ \ 16\ 28\ \ 33\ 31\ \ ]$

Step 6:

End Algorithm

Decoding Algorithm:

Step 1:

From equation (7) $H_2 = \left[J_{1,1}\ J_{1,2}\ J_{1,2}\ J_{1,3}\ \right] = [1\ 1\ 1\ 3\ ]$

Step 2:

Compute L_1^i, L_2^i to construct L_i

From equation (5) $L_1^i = d_1^i + d_2^i (1 \le i \le 4) L_1^1 = d_1^1 + d_2^1 = 16, L_1^2 = d_1^2 + d_2^1 = 30 L_1^3 = d_1^3 + d_2^3 = 19, L_1^4 = d_1^4 + d_2^4 = 41$

$$L_2^i = d_1^i + 3d_2^i$$

$L_2^1 = d_1^1 + 3d_2^1 = 20, L_2^2 = d_1^2 + 3d_2^2 = 48 L_2^3 = d_1^3 + 3d_2^3 = 51, L_2^4 = d_1^4 + 3d_2^4 = 97$

Step 3:

$when$ $1 \le i \le 4,, n = 2$, Equation (9) becomes

$$r_1(-1)^2 2^1 = L_1^1(x_1 + 3d_4^1) - L_2^1(x_1 + d_4^1) 448 = 16(x_1 + 60) - 20(x_1 + 20) x_1 = 28$$

$$r_2(-1)^2 2^1 = L_1^2(x_2 + 3d_4^2) - L_2^2(x_2 + d_4^2) 20 = 30x_2 + 1260 - 48x_2 - 672 x_2 = 26$$

$$r_3(-1)^2 2^1 = L_1^3(x_3 + 3d_4^3) - L_2^3(x_3 + d_4^3) - 826 = 19x_3 + 1881 - 51x_3 - 1683 x_3 = 32$$

$$r_4(-1)^2 2^1 = L_1^4(x_4 + 3d_4^4) - L_2^4(x_4 + d_4^4) - 1098 = 41x_4 + 3813 - 97x_4 - 3007 x_4 = 34$$

Step 4:

Substitute for $x_i = d_3^i$ $\quad\quad i = 1\ to\ 4$

Hence $d_3^1 = 28, d_3^2 = 26, d_3^3 = 32, d_3^4 = 34,$

Step 5:

Construct D_i $\quad\quad i = 1\ to\ 4$

(With the help of E step 5 in coding algorithm)

$D_1 = (14\ 2\ 28\ 20\ ), D_2 = (21\ 9\ 26\ 14\ ), D_3 = (3\ 16\ 32\ 33\ ), D_4 = (13\ 28\ 34\ 31\ )$

Step 6:

Message matrix $M = [14\ 2\ 21\ 9\ \ 28\ 20\ 26\ 14\ \ 3\ 32\ \ 16\ 33\ \ 13\ 34\ \ 28\ 31\ \ ] = [M\ A\ T\ H\ \ 0\ S\ Y\ M\ \ B\ +\ \ O\ -\ \ L\ *\ \ 0.\ ]$

Text Message "MATH SYMBOL +-*."

Step 7:

The algorithm is now complete.

Conclusion:

In this paper we introduced a new blocking algorithm to encrypt and decrypt a message. We explain these results more specifically for Jacobsthal. One can extend this result for other sequences like Oresmme, Fermat sequences. These new calculations won't just build the security of data yet in addition has high right capacity.

References:

[1]. Fikri Koken and Durmus Bozkurt " On the Jacobsthal numbers by matrix method " *Int.J.Contemp.Math Sciences.* Vol. 3, 2008, no. 13, 605 - 614.

[2]. Manjusri Basu, Bandhu Prasad " The generalized relations among the code elements for Fibonacci coding theory ", *Chaos, Solitons Fractals,* Vol. 41 (2009), no. 5, 2517 - 2525.

[3]. NihalTas, Sumerya Ucar and Yilmaz Ozgur " Pell coding and decoding methods with some Applications ". Arxiv: 1706.04377V1 [math.NT] 14 Jan 2017.*Contribution to discrete mathematics*, Vol. 15 Number 1, Page 15 - 66, Issn - 1715 - 0868

[4].Nihal Tas, Sumeyra Ucar, Nihal Yilmaz Ozgur and Oznur Oztunc Kaymak " *A new coding / decoding algorithm using Fibonacci numbers ".* Arxiv: 1712.02262v1[CS.IT]/ Dec 2017.

[5]. Srividhya. G, Kavitha Rani. E " Generalized k-Horadam hybrid numbers" Accepted in *The Mathematics Student - A periodical published by the Indian Mathematical Society.* 2023 January edition,

[6].Stakhove A.P, "Fibonacci matrices, a generalization of the Cassini formula and a new coding theory", *Chaos, Solitons Fractals* 30 (2006) no. 1, 56-66.

[7]. Sumeyra Ucar, Nihal Tas and Nihal Yilmaz Ozgur "A new application to coding theory via Fibonacci and Lucas Number" *Mathematical Sciences and Applications E. Notes* 7(1) 62-70 (2019)©MSAEN.

[8]. Yasin Yazlik, Necati Taskara "A note on generalized k-Horadam sequence" *Computers and Mathematics with applications.* 63, 2012 (36 - 41)