International Journal of Engineering, Science and Mathematics

Vol. 7 Special Issue 4(2), April 2018, ISSN: 2320-0294 Impact Factor: 6.765

Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com

Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Variations on the Narayana Universal Code

Monojit Das*

Abstract

The universal code maps positive integers which represents the source messages into codewords of different lengths. Elements of a codeword are a set of digits that are constructed according to specified rule. There are various universal codes such as Elias codes, the Fibonacci universal code, Levenshtein coding and non-universal codes including unary coding, Rice coding, Huffman coding and Golomb coding. In this paper we present universal coding scheme based on second order variant Narayana sequence. We have introduced Narayana code straight line in two-dimensional space. Each integral point (a, n) on Narayana code straight line presents second order variant Narayana universal code word. We describe the uses of this code in cryptography with an illustrative example.

Copyright © 2018 International Journals of Multidisciplinary Research Academy. All rights reserved.

Keywords:

Narayana sequence; universal code; Narayana code straight line; Cryptograph.

Author correspondence:

Monojit Das,

Guest Faculty, Shibpur Dinobundhoo Institution(College), Howrah, West Bengal.

Email: monojitbhu@gmail.com

1. Introduction

The universal code maps positive integers which represents the source messages into codewords of different lengths. Elements of a codeword are a set of digits that are constructed according to specified rule. There are various universal codes such as Elias codes, the Fibonacci universal code, Levenshtein coding and non-universal codes including unary coding, Rice coding, Huffman coding and Golomb coding [12, 10, 2, 9]. If one were to represent numbers as sum of two prime numbers using Goldbach conjecture, inverse sequence may also be sequence and also be used to construct a universal code [7].

The simplest of Elias codes is the gamma code in which the binary representation of the source code is preceded by $[log_2n]$ zeros indicate codeword for any natural number n. The time requirement for compression and decompression algorithms for cases where decompression time is a critical issue is advantageous in this coding [4, 5].

Fibonacci universal code is a universal code which encodes positive integers into binary codewords. These codewords end with 11 and have no consecutive 1 before the end. Fibonacci universal code has a useful property that sometimes makes it attractive in comparison to other universal codes. It is easier to recover data from a damaged stream.

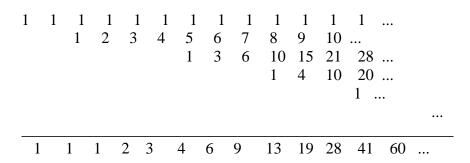
In 1356, Narayana (short for Narayana Pandit) wrote his famous book Gaita Kaumudi. His eponymous sequences [3, 6, 1] which are related to Fibonacci have potential applications in cryptography and data coding. In 2016, Kirti and Kak presents a method of universal coding based on the Narayana sequence [8]. In this paper we study on variant of Narayana coding scheme.

^{*} Guest Faculty, Shibpur Dinobundhoo Institution (College), Shibpur, Howrah

2. Narayana Sequence

The Narayana sequence is derived from the following problem that was proposed by Narayana: A cow gives birth to a calf every year. In turn, the calf gives birth to another calf when it is three years old. What is the number of progeny produced during twenty years by one cow? We assume that we begin with a new-born calf, who is shown in the first row of the matrix below. After three years, in each successive year, there is a new calf born to this one and additional calves are born to the 3-year or older calves, leading o second and additional rows in the matrix every 3 steps. This may be represented in the matrix below:

Table 1: Generation of the Narayana sequence



The Narayana sequence is defined as

$$N(k) = N(k-1) + N(k-3)$$
 where $N(0) = N(1) = N(2) = 1$. (1)

3. Variant of Narayana Coding Scheme

A more general Narayana sequence $N_a(k)$ is given by a, b, c, a + c, a + b + c, a + b + 2c, 2a + b + 2c, 3a + 2b + 4c and so on with a = 1, b = 2 and c = 3.

A variant of Narayana coding scheme can be obtained by defining second order variant Narayana sequence, $VN_a(k)$, such that b=3-a and c=1-a. This yields $VN_a(0)=a$ $(a \in Z)$, $VN_a(1)=3-a$, $VN_a(2)=1-a$ and for $k \ge 3$, $VN_a(k)=VN_a(k-1)+VN_a(k-3)$.

In this paper, by using the method described in [8] on second order variant Narayana sequence, we study for what values of n the second order variant Narayana universal code is available for $a \le -1$. For n = 1, 2, ..., 50 the representation and not available (N/A) of second order variant Narayana codewords for $a \le -1$ are displayed in Tables 2 and 3.

n	NY_{-1}	NY_{-2}	NY_3	NY_4	NY_5	NY_6	NY_7	NY_8	NY_9	NY_10
1	00011	00011	00011	00011	00011	00011	00011	00011	00011	00011
2	0011	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	0011	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4 5	011 000011	100011	0011 N/A	100011	100011 N/A	100011 N/A	100011 N/A	100011 N/A	100011 N/A	100011 N/A
6	101011	000011	011	N/A	0011	N/A	N/A	N/A	N/A	N/A
7	0000011	101011	000011	011	N/A	0011	N/A	N/A	N/A	N/A
8	00000011	N/A	101011	000011	011	N/A	0011	N/A	N/A	N/A
9	00010011	0000011	N/A	101011	000011	011	N/A	0011	N/A	N/A
ō	00100011	00000011	N/A	N/A	101011	000011	011	N/A	0011	N/A
1	N/A	00010011	0000011	N/A	N/A	101011	000011	011	N/A	0011
2	01000011	N/A	00000011	N/A	N/A	N/A	101011	00011	011	N/A
3	000000011	00100011	00010011	0000011	N/A	N/A	N/A	101011	000011	011
4	000100011	10001011	N/A	00000011	N/A	N/A N/A	N/A	N/A	101011	000011
5	001000011	01000011	N/A	00010011	0000011	N/A	N/A	N/A	N/A	101011
6	N/A	000000011	00100011	N/A	00000011	0000011	N/A	N/A	N/A	N/A
7	010000011	000100011	N/A	N/A	00010011	00000011	N/A	N/A	N/A	N/A
8	000010011	N/A	01000011	10001011	N/A	00010011	N/A	N/A	N/A	N/A
9	N/A	001000011	000000011	00100011	N/A	N/A	0000011	N/A	N/A	N/A
20	0000000011	N/A	000100011	N/A	10001011	N/A	00000011	N/A	N/A	N/A
1	0001000011	010000011	N/A	01000011	N/A	N/A	00010011	0000011	N/A	N/A
22	0010000011	000010011	N/A	000000011	00100011	10001011	N/A	00000011	N/A 0000011	N/A
4	N/A 0100000011	N/A N/A	001000011 N/A	000100011 N/A	N/A 01000011	N/A N/A	N/A 10001011	00010011 N/A	00000011	N/A N/A
5	0000100011	0000000011	010000011	N/A	000000011	00100011		N/A	00010011	0000011
6	N/A	0001000011	000010011	N/A N/A	000100011	N/A	N/A N/A	10001011	N/A	00000011
7	0000010011	N/A	N/A	001000011	N/A	N/A	N/A	N/A	N/A	00010011
8	00000000011	0010000011	N/A	N/A	N/A	N/A 000000011	N/A	N/A	10001011	N/A
9	00010000011	N/A	N/A	010000011	N/A	000100011	N/A	N/A	N/A	N/A
10	00100000011	0100000011	0000000011	000010011	N/A	N/A	01000011	N/A	N/A	10001011
1	N/A	0000100011	0001000011	N/A	001000011	N/A	000000011	00100011	N/A	N/A
12	01000000011	N/A	N/A	N/A	N/A	N/A	000100011	N/A	N/A	N/A
33	00001000011	N/A 0000010011	N/A	N/A	010000011	N/A	N/A	01000011	N/A	N/A
14	N/A		0010000011	N/A	000010011	N/A	N/A	000000011	00100011	N/A
5	00000100011	0000000011	N/A	0000000011	N/A	001000011	N/A	000100011	N/A	N/A
16	00000010011	00010000011	0100000011	0001000011	N/A	N/A 010000011	N/A	N/A	01000011	N/A
7	00010010011	N/A	0000100011	N/A	N/A	010000011	N/A	N/A	000000011	00100011
18	00100010011	00100000011	N/A	N/A	N/A	000010011	N/A	N/A	000100011	N/A
9	N/A	N/A	N/A	N/A	N/A	N/A	001000011	N/A	N/A	01000011
10	01000010011	01000000011	N/A	0010000011	0000000011	N/A	N/A	N/A	N/A	000000011
1	000000000011	00001000011	0000010011	N/A	0001000011	N/A	010000011	N/A	N/A	000100011
3	000100000011 001000000011	N/A	00000000011	0100000011 0000100011	N/A	N/A	000010011	001000011	N/A	N/A
		N/A	N/A		N/A	N/A	N/A	N/A	N/A	N/A
14	N/A 010000000011	00000100011 00000010011	N/A N/A	N/A N/A	N/A N/A	N/A 0000000011	N/A N/A	N/A 010000011	N/A N/A	N/A N/A
6	000010000011	00010010011	00100000011	N/A N/A	00100000011	0001000011	N/A N/A	000010011	N/A N/A	N/A N/A
17	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
18	000001000011	00100010011	01000000011	0000010011	01000000011	N/A	N/A	N/A	N/A	N/A
19	000001000011	N/A	00001000011	0000000011	0000100011	N/A N/A	N/A	N/A	010000011	N/A
50	000100100011	01000010011	N/A	00010000011	N/A	N/A	0000000011	N/A	000010011	N/A

By considering (a, n) as a point in the (x, y) plane, from the above tables we conclude that:

- 1. For $a \le -1$, there is the straight line y = 1 such that the points (a, 1) lie on this line which give the second order variant Narayana codeword 00011.
- 2. For $a \le -1$, there is the straight line y = 4 such that the points (a, 4) lie on this line which give the second order variant Narayana codeword 100011.
- 3. For $a \le -1$, there are the straight lines y + x = i, i = 1, 3, 4, 5 such that the points (a, 1 a), (a, 3 a), (a, 4 a), (a, 5 a) lie on this lines for i = 1, 3, 4, 5 respectively which give the respective second order variant Narayana codewords 0011, 011, 000011 and 1010111.
- 4. For $a \le -1$, there are the straight lines y + 2x = i, i = 5, 6, 7, 10 such that the points (a, 5 2a), (a, 6 2a), (a, 7 2a), (a, 10 2a) lie on this lines for i = 5, 6, 7, 10 respectively which give the respective second order variant Narayana codewords 0000011, 00000011, 00010011 and 10001011.
- 5. For $a \le -1$, there are the straight lines y + 3x = i, i = 7, 9, 10, 11 such that the points (a, 7 3a), (a, 9 3a), (a, 10 3a), (a, 11 3a) lie on this lines for i = 7, 9, 10, 11 respectively which give the respective second order variant Narayana codewords 00100011, 01000011, 000000011 and 000100011.
- 6. For $a \le -1$, there are the straight lines y + 4x = i, i = 11, 13, 14 such that the points (a, 11 4a), (a, 13 4a), (a, 14 4a) lie on this lines for i = 11, 13, 14 respectively which give the respective second order variant Narayana codewords 001000011, 010000011, 000010011.

- 7. For $a \le -1$, there is the straight line y + 5x = i, i = 15, 16 such that the points (a, 15 5a), (a, 16 5a) lie on this lines for i = 15, 16 respectively which give the respective second order variant Narayana codewords 0001000011 and 000010011.
- 8. For $a \le -1$, there is the straight line y + 6x = i, i = 16, 18, 19 such that the points (a, 16 6a), (a, 18 6a), (a, 19 6a) lie on this lines for i = 16, 18, 19 respectively which give the respective second order variant Narayana codewords 0010000011, 0100000011 and 0000100011.

n	NY_11	NY_{-12}	NY_13	NY_14	NY_15	NY_16	NY_17	NY_18	NY_19	NY_20
1	00011	00011	00011	00011	00011	00011	00011	00011	00011	00011
2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A N/A	N/A	N/A	N/A	N/A N/A	N/A N/A	N/A	N/A	N/A
12	N/A 0011	N/A	N/A N/A	N/A N/A	N/A N/A	N/A	N/A	N/A N/A	N/A N/A	N/A N/A
13	N/A	0011	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	011	N/A	0011	N/A	N/A	N/A	N/A	N/A	N/A	N/A
15	000011	011	N/A	0011	N/A	N/A	N/A	N/A	N/A	N/A
16	N/A	000011	011	N/A	0011	N/A	N/A	N/A	N/A	N/A
17	N/A	N/A	000011	011	N/A	0011	N/A	N/A	N/A	N/A
18	N/A	N/A	N/A	000011	011	N/A	0011	N/A	N/A	N/A
19	N/A	N/A	N/A	N/A	000011	011	N/A	0011	N/A	N/A
20	N/A	N/A	N/A	N/A	N/A	000011	011	N/A	0011	N/A
21	N/A	N/A	N/A	N/A	N/A	N/A	000011	011	N/A	0011
22	N/A	N/A	N/A	N/A	N/A	N/A	N/A	000011	011	N/A
23	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	000011	011
24	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	000011
25	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
26	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
27	0000011	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
28	00000011	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
29	00010011	0000011	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
30	N/A	0001011	0000011	N/A	N/A	N/A	N/A	N/A	N/A	N/A
31	N/A	010011	0000011	N/A	N/A	N/A N/A	N/A N/A	N/A	N/A	N/A
33	N/A N/A	N/A N/A	0001011 00010011	N/A 0000011	N/A N/A	N/A N/A	N/A N/A	N/A N/A	N/A N/A	N/A N/A
34	N/A	N/A	N/A	0001011	N/A	N/A	N/A	N/A	N/A	N/A
35	N/A	N/A	N/A	00010011	0000011	N/A	N/A	N/A	N/A	N/A
36	N/A	N/A	N/A	N/A	0001011	N/A	N/A	N/A	N/A	N/A
37	N/A	N/A	N/A	N/A	00010011	0000011	N/A	N/A	N/A	N/A
38	N/A	N/A	N/A	N/A	N/A	00000011	N/A	N/A	N/A	N/A
39	N/A	N/A	N/A	N/A	N/A	00010011	0000011	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A	N/A	00000011	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A	N/A	00010011	0000011	N/A	N/A
12	000000011	N/A	N/A	N/A	N/A	N/A	N/A	00000011	N/A	N/A
13	000100011	00100011	N/A	N/A	N/A	N/A	N/A	00010011	0000011	N/A
14	N/A	0100011	N/A	N/A	N/A	N/A	N/A	N/A	00000011	N/A
15	N/A	01000011	N/A	N/A	N/A	N/A	N/A	N/A	00010011	0000011
16	N/A	000000011	00100011	N/A	N/A	N/A	N/A	N/A	N/A	00000011
17	N/A	000100011	N/A	N/A	N/A	N/A	N/A	N/A	N/A	00010011
18	N/A	N/A	01000011	N/A	N/A	N/A	N/A	N/A	N/A	N/A
49	N/A	N/A	000000011	00100011	N/A	N/A	N/A	N/A	N/A	N/A
50	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Definition 3.1. If all the integral points (a,n) for $a \le -1$, $n \ge 1$ on a straight line have second order variant Narayana universal codeword then we call it Narayana code straight straight line. Otherwise it is called Non-Narayana code straight line.

- **Note 3.1.** The point (a, n), satisfying more than one Narayana code straight line, does not have unique second order variant Narayana universal codeword.
- **Note 3.2.** The point (a, n), lying on the intersecting point of the Narayana code straight line and the Non-Narayana code straight line, gives the second order variant Narayana universal codeword corresponding to the Narayana code straight line.
- **Note 3.3.** Each Narayana code straight line has unique second order variant Narayana universal codeword.

Figure 1 shows some Narayana code straight lines.

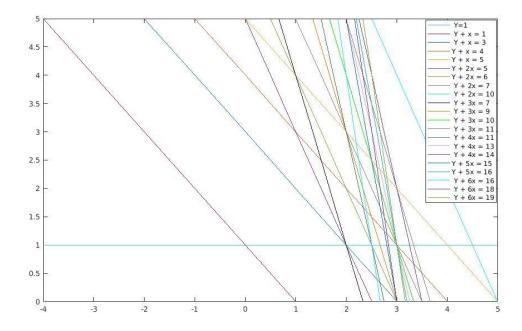


Figure 1: Narayana code straightlines

4. Second Order Variant Narayana Universal Code in Cryptography

We work over binary alphabets {0, 1}, since the second order variant Narayana universal code is binary.

Definition 4.1. A synchronous stream cipher is a tuple (P, C, K, L, E, D), together with a function g, such that the following conditions are satisfied:

- 1. P is a finite set of possible plaintexts
- 2. C is a finite set of possible cipher texts
- 3. K, is the keyspace, in a finite set of possible keys
- 4. L is a finite set called the keystream alphabet
- 5. g is the keystream generator. g takes a key K as a input, and generates an infinite string $z_1 z_2 z_3$... called the keystream, where $z_i \in L$ for all $i \ge 1$
- 6. For each $z \in L$, there is an encryption rule $e_z \in E$ and a corresponding decryption rule $d_z \in D$. $e_z: P \to C$ and $d_z: C \to P$ are functions such that $d_z(e_z(x)) = x$ for every plaintext element $x \in P[11]$.

In this paper, we consider $P = C = L = Z_2 = \{0, 1\}$. We set key as a binary t-tuple $(k_{1},k_{2,\ldots\!,}k_{t})$ and define the keystream as follows

$$z_i = \begin{cases} k_i, & 1 \le i \le t \\ z_{i-t}, & i \ge t+1 \end{cases}$$
This generates the keystream $k_1 k_2 \dots k_t k_1 k_2 \dots k_t k_1 k_2 \dots$ (2)

We define the encryption rule as:

$$e_z(x) = (z + x) \mod 2$$
, for all $x \in P$ (3)

and the decryption rule as:

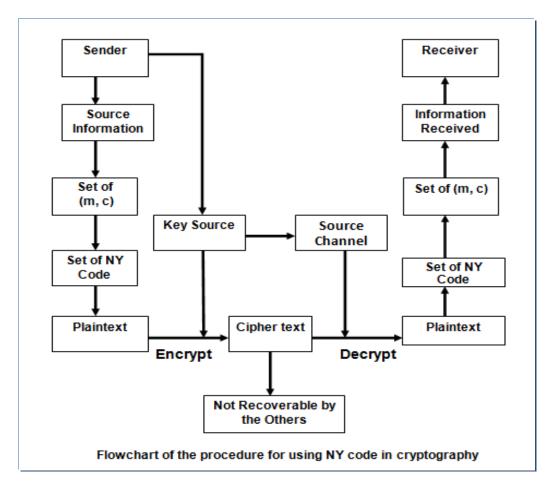
$$d_z(y) = (y+z) \bmod 2, \text{ for all } y \in C \tag{4}$$

First we associate Narayana code straight line (say y + mx = c) to every alphabet, space, number, special character etc. which we need for sending the text message. These associations are one-to-one and are known to both the sender as well as the receiver. We write y + mx = c as (m, c). The following algorithm states the procedure of using second order variant Narayana universal code in cryptography.

Algorithm 4.1.

- Step 1. Arrange message to (m, c) chronologically.
- Step 2. Write the corresponding second order variant Narayana universal codeword of (m, c) accordingly.
- Step 3. Write the plaintext and obtain its length 1.
- Step 4. Set the key and send it to the receiver via secure channel.
- Step 5. Obtain the keystream z of length 1 by using equation (2).
- Step 6. To obtain ciphertext, encrypt plaintext by using equation (3).
- Step 7. To obtain plaintext, the receiver decrypt ciphertext by using equation (4).
- Step 8. Break the plaintext into a number of parts so that each part ends with 11 so that each part represents second order variant Narayana universal codeword.
- Step 9. Convert second order variant Narayana universal codeword to (m, c).
- Step 10. Write (m, c) to message chronologically.

Following figure presents the flowchart of this procedure.



Example: Let the message "2018" to be encrypted. We take an association between Narayana code straight lines and message characters which are displayed in Table 4. Table 4: An association between Narayana code straight line and message character

Message character	(m,c)	Codeword
0	(1,1)	0011
1	(1,3)	011
2	(1,4)	000011
3	(2,5)	0000011
4	(2,6)	0000011
5	(2,7)	00010011
6	(2,10)	10001011
7	(3,7)	00100011
8	(3,9)	01000011
9	(3,10)	00000011

Step 1: Arrange message to (m,c) chronologically

2 0 1 8 (1,4) (1,1) (1,3) (3,9)

Step 2: Write the corresponding codeword of (m,c) accordingly

(1,4) (1,1) (1,3) (3,9) 000011 0011 011 01000011

Step 3: The plaintext is

000011001101101000011

The length of plaintext is 21

Step 4: Set (1, 0, 0, 1) as the key so that t = 4 and send it to the receiver via a secure channel.

Step 5: The keystream of length 21 is

100110011001100110011

Step 6: After encryption the ciphertext is:

100101010100001110000

Step 7: After decryption the plaintext is:

000011001101101000011

Step 8: The receiver breaks the plaintext into a number of parts so that each part ends with 11 to obtain second order variant Narayana universal codewords.

000011 0011 011 01000011

Step 9: Convert each second order variant Narayana universal codewords to (m, c):

 $(1,4) \qquad (1,1) \qquad (1,3) \qquad (3,9)$

Step 10: Write (m, c) chronologically:

2018

5. Conclusion

It is clear that each Narayana code straight line has unique second order variant Narayana universal codeword and so we can use this straight lines in cryptography. Second order variant Narayana coding scheme improves the cryptography protection highly due to the formation of straight lines. Future researchers can develop more Narayana code straight lines and its properties.

References

- [1] Allouche, J. P. and Johnson, T. "Narayana's cows and delayed morphisms, Cahiers du GREYC Troisiemes Journes dInformatique Musicale," *JIM 96*, vol. 4, pp 2-7, 1996.
- [2] Buschmann, T. and Bystrykh, L. V. "Levenshtein error-correcting barcodes for multiplexed DNA sequencing," *BMC Bioinformatics*, vol. 14, no. 1, pp. 272, 2013.

- [3] Didkivska, T.V. and Stopochkina, M.V. "Properties of Fibonacci-Narayana numbers," *In the World of Mathematics*, vol. 9, no. 1, pp. 29-36, 2003.
- [4 Elias, P. "Universal codeword sets and representations of the integers," *IEEE Trans.Inform. Theory IT*, vol. 21, no. 2, pp. 194-203, 1975.
- [5] Filmus, Y. "Universal codes of the natural numbers," *Logical Methods in Computer Science*, vol. 9, pp. 1-11, 2013.
- [6] Flaut, C. and Shpakivskyi, V. "On generalized Fibonacci quaternions and Fibonacci Narayana quaternions," Adv. Appl. Clifford Algebras, vol. 23, pp. 673-688, 2013. arxiv:physics/0303001.
- [7] Kak, S. and Chatterjee, A. "On decimal sequences," *IEEE Trans. on Information Theory IT*, vol. 27, pp. 647 652, 1981.
- [8] Kirthi, K. and Kak, S. "The Narayana Universal Code," arxiv:1601.07110, 2016.
- [9] Malvar, H.S. "Adaptive Run-Length/Golomb-Rice encoding of quantized generalized Gaussian sources with unknown statistics," http://research-srv.microsoft.com/pubs/102069/Malvar DCC06.pdf
- [10] Platos, J., Baca, R., Snasel, V. and Kratky, M. "E El-Qawasmeh, Fast Fibonacci encoding algorithm," arXiv: cs/0712.0811v2 (2007) index.html, 2002.
- [11] Stinson, Douglas R. "Cryptography Theory and Practice" Third Edition. Chapman & Hall/CRC, 2006.
- [12] Thomas, J. H. "Variation on the Fibonacci universal code," arXiv:cs/0701085v2.