

A NEW APPLICATION TO CODING THEORY VIA GUGLIELMO NUMBERS

S. Uygun¹, M. Topatas²

¹ Department of Mathematics, Science Faculty, Gaziantep
University, Campus, Gaziantep, Turkey
e-mail: suygun@gantep.edu.tr

² Department of Mathematics, Science Faculty, Gaziantep
University, Campus, Gaziantep, Turkey
e-mail: mhrbnt.07@gmail.com

Abstract

This paper describes a new coding and decoding technique based on the Guglielmo sequence. Our version is based on a blocked message matrix, with every message matrix encrypted using a special key. The amount of information transmitted over the internet has increased as internet use has become more prevalent. Consequently, the importance of the algorithms used in data encryption methods has increased. The proposed method is fast because it is based on fundamental matrix operations and is suitable for cryptographic applications due to its use of the ASCII character encoding system. For this reason, it differs from classical algebraic methods described in the literature. Using

Guglielmo numbers we define Guglielmo G-matrices. We can process any given message with a special encryption and we can decode the encrypted message with the method we use.

Math. Subject Classification: 68P30, 11B39, 11B50, 11B37, 11T71, 11B83

Key Words and Phrases: Encoding-Decoding algorithms, Guglielmo sequence

1 Introduction and Preliminaries

You can easily see that matrix sequences have many applications in scientific areas such as physics, engineering and architecture and art. Communication for humans has shown its importance throughout history. A researcher working on coding/decoding theory is Lester Hill, who created the Hill algorithm. It is included matrix multiplying and matrix inverses. This algorithm is the first step of the modern mathematical theory. However, this method was not safe nowadays. It is relatively broken by using a computer. Alan Turing, a computer scientist, after inventing an encryption machine, broke the encrypted messages made by the Germans Enigma machine during World War II. It helped change the course of World War II. Many researchers have delved into the study of coding/decoding algorithms using special integer sequences in existing literature.

Many researchers have introduced coding/decoding algorithms using Fibonacci, Lucas and other special numbers [1–15] and their references. Stakhov presented Cassini formula for Fibonacci matrices [1]. Basu and Prasad studied the generalized relations among the code elements for Fibonacci coding theory in [2]. Tahghighi et. al. investigated a generalization of golden cryptography based on k-Fibonacci numbers in [3]. Prajapat et al proposed a method with automatic variable key using Fibonacci Q-matrix in [4]. Esmaeili presented a coding method with error detection and correction based on Fibonacci-polynomials in [5]. Prasad introduced a new

method for coding/decoding algorithms using Lucas p-numbers [6]. Ucar et al. introduced Fibonacci Q-matrices and R-matrices [7, 8]. Basu and Das found new coding methods with Tribonacci matrices and Fibonacci n-step numbers in [9, 10]. Agarwal et al. developed an algorithm for data encryption & decryption using Fibonacci prime in [11]. Hashemi and Mehraban found some new codes by the k-Fibonacci sequence in [12]. Mehraban and Hashemi studied a coding theory on the generalized balancing sequence in [13]. Mehraban et al. used new sequences from the generalized Pell p-numbers and Mersenne numbers and their application in cryptography in [14]. Prasad and Mahato presented a coding method using generalized Fibonacci matrices with Affine-Hill cipher in [15].

The studies given above encouraged us to study an encryption method using new numbers especially not so well known number sequences. For this reason, we choose Guglielmo number sequences. In this study, we define Guglielmo matrix sequence and investigate a encryption and decryption algorithm using Guglielmo numbers. Our method is based on a blocked message matrix and encryption of every message matrix with a special key. Our study consists of two parts. In the first part, we present a coding algorithm using Guglielmo G-matrix. We explain this model with an example. We divide the message matrix into $2m \times 2m$ block matrices then mapping each character in the message to a different number, we obtain a coded matrix. In the second part, we present a decoding algorithm.

The purpose of this study is not only to increase the reliability of information security technology, but also to provide the ability to verify information at a high rate. Furthermore, Guglielmo matrix sequence improves an unheard of method for the cryptography. It is given a mix model named Guglielmo G-matrix encryption method.

2 Guglielmo Number and Matrix Sequence

In this part, we use the papers named "Generalized Guglielmo numbers: An investigation of properties of triangular, oblong, and pentagonal numbers via their third-order linear recurrence relations" and "A Study on Matrix Sequence with Generalized Guglielmo Numbers Components" in reference [16, 17].

Definition 1. Guglielmo number sequence $\{T_n\}$ is defined recurrently by

$$T_n = 3T_{n-1} - 3T_{n-2} + T_{n-3}, \quad n \geq 3$$

with the initial conditions $T_0 = 0, T_1 = 1, T_2 = 3$ where n is any positive integer.

Some of the first Guglielmo numbers are 0, 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, ... For all integers n ; Guglielmo numbers using initial conditions can be obtained using Binet formula as $T_n = \frac{n(n+1)}{2}$.

Definition 2. Guglielmo matrix sequence $\{G_n\}$ is defined recurrently by

$$G_n = 3G_{n-1} - 3G_{n-2} + G_{n-3}, \quad n \geq 3$$

with the initial conditions

$$G_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad G_1 = \begin{pmatrix} 3 & -3 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 6 & -8 & 3 \\ 3 & -3 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

where n is any positive integer.

Theorem 3. The Guglielmo matrix sequence $\{G_n\}$ is denoted using Guglielmo numbers as

$$G_n = \begin{pmatrix} T_{n+1} & -3T_n + T_{n-1} & T_n \\ T_n & -3T_{n-1} + T_{n-2} & T_{n-1} \\ T_{n-1} & -3T_{n-2} + T_{n-3} & T_{n-2} \end{pmatrix}.$$

Proof. By induction method, the proof is easily observed. $\square$

Theorem 4. *We are pleased to observe that for any positive integer n , we have*

$$G_n = G_1^n.$$

Proof. For proof, we use induction method. For $n = 0$, the assertion is true. Let assume that it is also true for $k \leq n$. Then for $k = n + 1$, we get

$$G_1^{n+1} = G_1^n G_1 = \begin{pmatrix} T_{n+1} & -3T_n + T_{n-1} & T_n \\ T_n & -3T_{n-1} + T_{n-2} & T_{n-1} \\ T_{n-1} & -3T_{n-2} + T_{n-3} & T_{n-2} \end{pmatrix} \begin{pmatrix} 3 & -3 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = G_{n+1}.$$

$\square$

$$\text{Especially } \det \begin{pmatrix} 3 & -3 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = 1. \text{ So, } \det(G_n) = 1.$$

Theorem 5. *For every integer n ; the Binet's formula of the Guglielmo matrix sequences is given by*

$$G_n = \begin{pmatrix} \frac{(n+2)(n+1)}{2} & -n^2 - 2n & \frac{n(n+1)}{2} \\ \frac{n(n+1)}{2} & 1 - n^2 & \frac{n(n-1)}{2} \\ \frac{n(n-1)}{2} & 2n - n^2 & \frac{(n-2)(n-1)}{2} \end{pmatrix}.$$

2.1 Coding/ Decoding Algorithm with Guglielmo Numbers

In this part, we instigate a method for enciphering and deciphering the Guglielmo sequence.

Before using the method (M.....is not zero. In this part, we give a new coding algorithm using third order Guglielmo matrix sequence. We put our message in a matrix of third order. Dividing the $3m \times 3m$ message matrix M into 3×3 block matrices from left to right, M_i for $i = 1, \dots, m^2$, we get a new coding method.

If we demonstrate the symbols of the coding method, that matrices M_i , E_i and G_n are of the following forms:

$$M_i = \begin{pmatrix} m_1^i & m_2^i & m_3^i \\ m_4^i & m_5^i & m_6^i \\ m_7^i & m_8^i & m_9^i \end{pmatrix}, \quad E_i = \begin{pmatrix} e_1^i & e_2^i & e_3^i \\ e_4^i & e_5^i & e_6^i \\ e_7^i & e_8^i & e_9^i \end{pmatrix}, \quad G_n = \begin{pmatrix} g_1 & g_2 & g_3 \\ g_4 & g_5 & g_6 \\ g_7 & g_8 & g_9 \end{pmatrix}.$$

Now, we explain the following new coding and decoding algorithms.

Coding Algorithm by third order Guglielmo matrix

1. Divide the message matrix M into blocks M_i ($1 \leq i \leq m$). The number of the block matrices M_i is denoted by m . According to m , let's assume that n is chosen as follows:

$$n = \begin{cases} m - 1, & m \leq 4 \\ 2m - 5, & m > 4 \end{cases} \quad (1)$$

2. Using the chosen n , we write the following letter table according to mod 40 (this table can be extended according to the used characters in the message matrix). We begin " n " for the first character.

A	B	C	D	E	F	G	H	I	J
n	n+1	n+2	n+3	n+4	n+5	n+6	n+7	n+8	n+9
K	L	M	N	O	P	R	Q	S	T
n+10	n+11	n+12	n+13	n+14	n+15	n+16	n+17	n+18	n+19
U	V	W	X	Y	Z	:	.	,	-
n+20	n+21	n+22	n+23	n+24	n+25	n+26	n+27	n+28	n+29
0	1	2	3	4	5	6	7	8	9
n+30	n+31	n+32	n+33	n+34	n+35	n+36	n+37	n+38	n+39

3. Determine $m_j^i, (1 \leq j \leq 9)$

4. Compute $\det(M_i) = \Psi_i$.

5. Construct the coding matrix as $F = [\Psi_i, m_j^i]_{j \in \{1,2,3,4,5,6,8,9\}}$.

Decoding Algorithm

1. Compute G_n .

2. Evaluate

$$\begin{aligned} g_1 m_1^i + g_2 m_4^i + g_3 m_7^i &\rightarrow e_1^i \\ g_1 m_2^i + g_2 m_5^i + g_3 m_8^i &\rightarrow e_2^i \\ g_1 m_3^i + g_2 m_6^i + g_3 m_9^i &\rightarrow e_3^i \\ g_4 m_1^i + g_5 m_4^i + g_6 m_7^i &\rightarrow e_4^i \\ g_4 m_2^i + g_5 m_5^i + g_6 m_8^i &\rightarrow e_5^i \\ g_4 m_3^i + g_5 m_6^i + g_6 m_9^i &\rightarrow e_6^i \\ g_7 m_1^i + g_8 m_4^i + g_9 m_7^i &\rightarrow e_7^i \\ g_7 m_2^i + g_8 m_5^i + g_9 m_8^i &\rightarrow e_8^i \\ g_7 m_3^i + g_8 m_6^i + g_9 m_9^i &\rightarrow e_9^i \end{aligned}$$

3. Evaluate

$$\begin{aligned} d_i = (g_1 m_1^i + g_2 m_4^i + g_3 x_i) &\begin{vmatrix} e_5^i & e_6^i \\ e_8^i & e_9^i \end{vmatrix} - (g_4 m_1^i + g_5 m_4^i + g_6 x_i) &\begin{vmatrix} e_2^i & e_3^i \\ e_8^i & e_9^i \end{vmatrix} + \\ (g_7 m_1^i + g_8 m_4^i + g_9 x_i) &\begin{vmatrix} e_2^i & e_3^i \\ e_5^i & e_6^i \end{vmatrix} \end{aligned}$$

4. Substitute for $x_i = m_7^i$

5. Construct M_i and therefore M .

In the following example we give an application of the above algorithm.

Example 6. *Let's consider the message matrix for the following message text*

"MY FAVORITE LESSON IS MATHEMATICS."

We get the following message matrix M :

$$M = \begin{bmatrix} M & Y & - & F & A & V \\ O & R & I & T & E & - \\ L & E & S & S & O & N \\ - & I & S & - & M & A \\ T & H & E & M & A & T \\ I & C & S & . & - & - \end{bmatrix}$$

1. We divide the message matrix M of size 3×3 into the matrices, named M_i ($1 \leq i \leq 4$), from left to right:

$$\begin{aligned} M_1 &= \begin{bmatrix} M & Y & - \\ O & R & I \\ L & E & S \end{bmatrix}, & M_2 &= \begin{bmatrix} F & A & V \\ T & E & - \\ S & O & N \end{bmatrix}, \\ M_3 &= \begin{bmatrix} - & I & S \\ T & H & E \\ I & C & S \end{bmatrix}, & M_4 &= \begin{bmatrix} - & M & A \\ M & A & T \\ . & - & - \end{bmatrix} \end{aligned}$$

2. By 1, we get $n = 3$. We use the "character table" for the message matrix M : The elements of the blocks M_i ($1 \leq i \leq 4$) as follows: We calculate the determinants d_i of the blocks M_i :

$$\begin{aligned} M_1 &= \begin{bmatrix} 15 & 27 & 32 \\ 17 & 19 & 11 \\ 14 & 7 & 21 \end{bmatrix} & \text{then } d_1 &= \det(M_1) = -5355 \\ M_2 &= \begin{bmatrix} 8 & 16 & 24 \\ 22 & 7 & 32 \\ 21 & 17 & 16 \end{bmatrix} & \text{then } d_2 &= \det(M_2) = 7112 \\ M_3 &= \begin{bmatrix} 32 & 11 & 21 \\ 22 & 10 & 7 \\ 11 & 5 & 21 \end{bmatrix} & \text{then } d_3 &= \det(M_3) = 1365 \\ M_4 &= \begin{bmatrix} 32 & 16 & 3 \\ 16 & 3 & 12 \\ 30 & 32 & 32 \end{bmatrix} & \text{then } d_4 &= \det(M_4) = -10382 \end{aligned}$$

3. We construct the M matrix:

$$M = \begin{bmatrix} -5355 & 15 & 27 & 32 & 17 & 19 & 11 & 7 & 21 \\ 7112 & 8 & 16 & 24 & 22 & 7 & 32 & 17 & 16 \\ 1365 & 32 & 11 & 21 & 22 & 10 & 7 & 5 & 21 \\ -10382 & 32 & 16 & 3 & 16 & 3 & 12 & 32 & 32 \end{bmatrix}$$

Decoding Algorithm

1. We choose $n = 3$ and determine G_3 as

$$\begin{aligned} g_1 &= 10 & g_2 &= -15 & g_3 &= 6 \\ g_4 &= 6 & g_5 &= -8 & g_6 &= 3 \\ g_7 &= 3 & g_8 &= -3 & g_9 &= 1 \end{aligned}$$

2. Evaluate the followings respecticely to construct the matrix

E_i :

$$\begin{aligned} &[e_1^1 = -21 \quad e_2^1 = 27 \quad e_3^1 = 281 \quad e_4^1 = -4 \quad e_5^1 = 31 \quad e_6^1 = 167 \quad e_7^1 = 8 \quad e_8^1 = 31 \quad e_9^1 = 84] \\ &[e_1^2 = -124 \quad e_2^2 = 157 \quad e_3^2 = -144 \quad e_4^2 = -65] \\ &[e_5^2 = 91 \quad e_6^2 = -64 \quad e_7^2 = -21 \quad e_8^2 = 44 \quad e_9^2 = -8] \\ &[e_1^3 = 56 \quad e_2^3 = -10 \quad e_3^3 = 231 \quad e_4^3 = 49 \quad e_5^3 = 1 \quad e_6^3 = 133 \quad e_7^3 = 41 \quad e_8^3 = 8 \quad e_9^3 = 63] \\ &[e_1^4 = 260 \quad e_2^4 = 168 \quad e_3^4 = 5 \quad e_4^4 = 154 \quad e_5^4 = 168 \quad e_6^4 = 18 \quad e_7^4 = 78 \quad e_8^4 = 71 \quad e_9^4 = 5] \end{aligned}$$

3. We calculate the elements

$$\begin{aligned} -5355 &= (150 - 15 * 17 + 6x_1) \begin{vmatrix} 31 & 167 \\ 31 & 84 \end{vmatrix} - (90 - 8 * 17 + 3x_1) \begin{vmatrix} 27 & 281 \\ 31 & 84 \end{vmatrix} \\ &\quad + (45 - 3 * 17 + x_1) \begin{vmatrix} 27 & 281 \\ 31 & 167 \end{vmatrix} \\ -5355 &= (-105 + 6x_1)(-2573) - (-46 + 3x_1)(-6443) + (-6 + x_1)(-4202) \\ 5355 + 105 * 2573 - 46 * 6443 + 6 * 4202 &= 4354 = 2573 * 6 - 6443 * 3 + 4202 = 311 \\ x_1 &= 14 \end{aligned}$$

and

$$\begin{aligned}
 7112 &= (-250 + 6x_2) \begin{vmatrix} 91 & -64 \\ 44 & -8 \end{vmatrix} - (-128 + 3x_2) \begin{vmatrix} 157 & -144 \\ 44 & -8 \end{vmatrix} + (x_2 - 42) \begin{vmatrix} 157 & -144 \\ 91 & -64 \end{vmatrix} \\
 7112 &= (-250 + 6x_2) * 2088 - (-128 + 3x_2) * 5080 + (-42 + x_2) * 3056 \\
 344x_2 &= 112 + 7112 \\
 x_2 &= 21
 \end{aligned}$$

and

$$\begin{aligned}
 1365 &= (10x_3 + 93) \begin{vmatrix} -631 & 246 \\ -431 & 169 \end{vmatrix} - (15x_3 + 103) \begin{vmatrix} 449 & 246 \\ 301 & 169 \end{vmatrix} + (6x_3 + 36) \begin{vmatrix} 449 & -631 \\ 301 & -431 \end{vmatrix} \\
 1365 &= (10x_3 + 93)(-613) + (15x_3 + 103)(1835) + (6x_3 + 36)(-3588) \\
 1365 &= -133x_3 + 2828 \\
 x_3 &= 11
 \end{aligned}$$

and

$$\begin{aligned}
 -10382 &= (10x_4 + 288) \begin{vmatrix} -617 & 243 \\ -300 & 117 \end{vmatrix} + (15x_4 + 352) \begin{vmatrix} 425 & 243 \\ 214 & 117 \end{vmatrix} + (128 + 6x_4) \begin{vmatrix} 425 & -617 \\ 214 & -300 \end{vmatrix} \\
 -10382 &= (10x_4 + 288)(711) + (15x_4 + 352)(-2277) + (128 + 6x_4)(4538) \\
 -10382 &= 183x_4 - 15872 \\
 x_4 &= 30
 \end{aligned}$$

4. We determine x_i

$$x_1 = m_7^1 = 14 \quad x_2 = m_7^2 = 21 \quad x_3 = m_7^3 = 11 \quad x_4 = m_7^4 = 30$$

5. We construct the block matrices M_i by

$$M_1 = \begin{bmatrix} 15 & 27 & 32 \\ 17 & 19 & 11 \\ 14 & 7 & 21 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 8 & 16 & 24 \\ 22 & 7 & 32 \\ 21 & 17 & 16 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 32 & 11 & 21 \\ 22 & 10 & 7 \\ 11 & 5 & 21 \end{bmatrix}, \quad M_4 = \begin{bmatrix} 32 & 16 & 3 \\ 16 & 3 & 12 \\ 30 & 32 & 32 \end{bmatrix}$$

Hence, we obtain the message matrix M :

Conclusions

In this article, we developed a new algorithm in coding theory with the help of G -matrix. In this algorithm, we divide the desired message into blocks and transform the message matrix into an encoded message matrix. In the decryption process, we converted the encrypted message matrix to the desired message matrix using the G -matrix.

Acknowledgments The Authors are very thankful to the referees for their valuable comments.

References

- [1] A. P. Stakhov, Fibonacci matrices, a generalization of the Cassini formula and a new coding theory, *Chaos Solitons Fractals*, **30(1)** (2006), 56-66.
- [2] M. Basu, B. Prasad, The generalized relations among the code elements for Fibonacci coding theory, *Chaos Solitons Fractals*, **41(5)** (2009), 2517-2525.
- [3] M. Tahghighi, A. Jafaar, R. Mahmood, Generalization of Golden Cryptography based on k-Fibonacci Numbers, In: *International Conference on Intelligent Network and Computing (ICINC)* (2010)
- [4] S. Prajapat, A. Jain, R. S. Thakur, A novel approach for information security with automatic variable key using Fibonacci Q-matrix, *International Journal of Computer and Communication Technology IJCCT*, **3** (2012), 54-57.
- [5] M. Esmaeili, M. Esmaeili, Fibonacci-polynomial based coding method with error detection and correction, *Computers & Mathematics with Applications*, **60(10)** (2010), 2738-2752.
- [6] B. Prasad, Coding theory on Lucas p-numbers. *Discrete Mathematics, Algorithms and Applications*, **8(4)** (2016), 1650074.

- [7] N. Tas, S. Ucar, N. Y. Ozgur, O. O. Kaymak, A new coding/decoding algorithm using Finonacci numbers, *Discrete Mathematics, Discrete Mathematics, Algorithms and Applications*, **2** (2018), 1850028.
- [8] S. Uçar, N. Taş, N.Y. Özgür, A New Application to Coding Theory via Fibonacci and Lucas Numbers, *Mathematical Sciences and Applications e-Notes*, **7(1)** (2019), 62-70.
- [9] M. Basu, M. Das, Tribonacci matrices and a new coding theory. *Discrete Mathematics, Algorithms and Applications*, **6(1)** (2014)1450008. DOI: 10.1142/S1793830914500086
- [10] M. Basu, M. Das, Coding theory on Fibonacci n-step numbers. *Discrete Mathematics, Algorithms and Applications*, **6(2)** (2014) 1450017. DOI: 10.1142/S1793830914500177.
- [11] A. Agarwal, S. Agarwal, B. K. Singh, Algorithm for data encryption& decryption using Fibonacci prime, *Journal of Mathematical Control Science & Applications*, **6(1)** (2020), 63-71.
- [12] M. Hashemi, E. Mehraban, Some new codes on the k-Fibonacci sequence, *Mathematical Problems in Engineering*, **2021(1)** (2021), 7660902.
- [13] E. Mehraban, M. Hashemi, Coding theory on the generalized balancing sequence, *Notes on Number Theory and Discrete Mathematics*, **29(3)** (2023), 503-524.
- [14] E. Mehraban, T. A. Gulliver, S. M. Boulaaras, K. Hosseini, E. Hincal, New sequences from the generalized Pell p-numbers and Mersenne numbers and their application in cryptography, *AIMS Mathematics*, **9(5)** (2024), 13537-13552.
- [15] K. Prasad, H. Mahato, Cryptography using generalized Fibonacci matrices with Affine-Hill cipher, *Journal of Discrete Mathematical Sciences and Cryptography*, **25(8)** (2022), 2341-2352.

- [16] Y. Soykan, Generalized Guglielmo numbers: An investigation of properties of triangular, oblong, and pentagonal numbers via their third-order linear recurrence relations, *Earthline Journal of Mathematical Sciences*, **9(1)** (2022), 1-39.
- [17] B. Yilmaz, Y. Soykan, N. Gonul Bilgin, A Study on Matrix Sequence with Generalized Guglielmo Numbers Components, *Asian Research Journal of Mathematics*, **20(11)** (2024), 1-25.