ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha*, Vol. 52(2) (2022), 77-81**
(Dedicated to Professor D. S. Hooda on His 80th Birth Anniversary Celebrations)

A NOTE ON LINEAR CODES WITH GENERALIZED FIBONACCI MATRICES

Munesh Kumari[1], Kalika Parasd[1,*] and Jagmohan Tanti[2]
[1] Department of Mathematics, Central University of Jharkhand-835205, Ranchi, India
[2] Department of Mathematics, Babasaheb Bhimrao Ambedkar University, Lucknow-226025, Uttar Pradesh, India
Email: muneshnasir94@gmail.com, jagmohan.t@gmail.com
[*]Corresponding author: Email: klkaprsd@gmail.com
(Received: August 10*,* 2022*; Revised: September* 25*,* 2022*; Accepted: September* 30*,* 2022*)*

DOI: https://doi.org/10.58250/jnanabha.2022.52209

Abstract

In this paper, we investigate the linear codes from generalized Fibonacci matrices in the context of coding theory. We show that Fibonacci matrices form a generator matrix for the first order ReedMuller codes $R(1,1)$. Further, we see that Multinacci matrices form a basis for $[n,n,1]$ *MDS*-code.
2020 Mathematical Sciences Classification: 11B39, 11T71, 94B05.
Keywords and Phrases: Basis, Coding Theory, Fibonacci Matrix, Linear code, *LCD* code.

1. Introduction and Preliminaries

A linear code C over a finite field $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ and it is denoted as $[n,k]$-linear code. If minimum Hamming distance of linear code C is d then it is called a $[n,k,d]$-linear code.

Fibonacci matrix F_2 is a square matrix of size 2×2 of the form $F_2 = \begin{bmatrix} t_2 & t_1 \\ t_1 & t_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ and its kth power is defined as $F_2^k = \begin{bmatrix} t_{k+1} & t_k \\ t_k & t_{k-1} \end{bmatrix}$, where t_k is the k^{th} term of Fibonacci sequence. Fibonacci matrices are enriched with many interesting properties like direct formula for its k^{th} power, determinant, inverse, etc. irrespective of size k. Due to special properties, Fibonacci matrices are of great interest among researchers and used in coding theory, cryptography, secret sharing problem etc. Some recent works on coding theory and cryptographic schemes with special matrices can be seen in [1,2,7-12].

In this paper, we show application of multinacci matrices in coding theory. We consider Multinacci matrices as base generator matrix for different type of linear codes. Further, using multinacci matrices as generator only a number can be used for encryption and decryption instead of a matrix which increase the efficiency of encryption scheme.

Some useful definitions and terminology[4] used in our work are as follows.

Definition 1.1. *For $[n,k]$-linear code C, we have*

1. *A generator matrix G in the form $(I_k|X)$ is said to be in standard form.*
2. *A parity-check matrix H in the form $(Y|I_{n-k})$ is said to be in standard form.*

Definition 1.2. *(ReedMuller codes) The first order ReedMuller codes $R(1,m)$ are binary codes defined for all $m \in \mathbb{N}$ recursively as:*

1. $R(1,1) = F_2^2 = \{00, 01, 10, 11\}$,
2. *For $m \geq 1$, $R(1,m+1) = \{(v,v) : v \in R(1;m)\} \cup \{(v,v+1) : v \in R(1;m)\}$.*

By the virtue of [5], we have the following useful lemma.

Lemma 1.1. *Let $G_{k\times n}$ be a generator matrix of $[n,k]$-linear code C. Then the $[n,k]$-linear code C is an LCD code if and only if $Det(GG^T) \neq 0$.*

1.1. Generalized Fibonacci Matrices

Definition 1.3. *The generalized Fibonacci sequence of order $n \geq 2$ is defined by the recurrence relation,*

$$t_{k+n} = t_k + t_{k+1} + t_{k+2} + ... + t_{k+n-1}, \qquad k \geq 0 \tag{1.1}$$

with $t_0 = t_1 = ... = t_{n-2} = 0$ and $t_{n-1} = 1$.

The generalized Fibonacci sequence is also known as $n-$nacci sequence. The sequence $\{t_k\}_{k\in\mathbb{N}}$ can be also extended to negative direction, which is given by rearranging the relation (1.1) as,

$$t_{-k} = t_{-k+n} - (t_{-k+1} + ... + t_{-k+n-1}), \qquad for \;\; k \geq 1. \tag{1.2}$$

In particular, for $n = 2$ it gives the Fibonacci sequence [A000045] and for $n = 3$, the tribonacci sequence [A000073][3].

The matrix sequence associated with the generalized Fibonacci sequence as proposed in [6] of order n is given by

$$F_n^k = \begin{bmatrix} t_{k+n-1} & t_{k+n-2} + t_{k+n-3} + ... + t_k & \cdots & t_{k+n-2} \\ t_{k+n-2} & t_{k+n-3} + t_{k+n-4} + ... + t_{k-1} & \cdots & t_{k+n-3} \\ \vdots & \vdots & \ddots & \vdots \\ t_{k+1} & t_k + t_{k-1} + ... + t_{k-n+2} & \cdots & t_k \\ t_k & t_{k-1} + t_{k-2} + ... + t_{k-n+1} & \cdots & t_{k-1} \end{bmatrix}_{n\times n}, \quad \text{for } \; k = 0, \pm 1, \pm 2, ... \tag{1.3}$$

where $F_n^0 = I_n$, I_n is the identity matrix of order n and t_k is the k^{th} term of generalized Fibonacci sequence of same order as of given matrix. Matrix F_n^k refers to the Multinacci matrix of order n.

The initial (generator) matrix for Fibonacci matrix is given by

$$F_n^1 = \begin{bmatrix} 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 0 & 0 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & ... & 1 & 0 \end{bmatrix}_{n\times n} = F_n. \tag{1.4}$$

By the virtue of [6], Multinacci matrices F_n^k have following properties, given in the next lemma.

Lemma 1.2. *For $n \geq 2$ and $k \in \mathbb{Z}$, we have*

1. $(F_n^1)^k = F_n^k$,
2. $(F_n^k)^{-1} = F_n^{-k}$,
3. $F_n^k F_n^l = F_n^{k+l}$ *for* $k, l \in \mathbb{Z}$,
4. $det(F_n^k) = (-1)^{(n-1)k}$.

Inverse of Multinacci matrix. *Inverse of Multinacci matrices are obtained by replacing k with $-k$ in the definition of matrix F_n^k in eqn.* (1.3).

2. Codes with Fibonacci Matrices

Theorem 2.1. *Let $S = \{F_2^k$ over $\mathbb{Z}_p$, p is a prime and $k \in \mathbb{Z}\}$, then S forms an abelian group with respect to usual matrix multiplication.*

Proof. Here we show that the collection S satisfies the condition of commutative group.

Closure: For all $k_1, k_2 \in \mathbb{Z}$,

$$F_2^{k_1} * F_2^{k_2} = F_2^{k_1+k_2} = \begin{bmatrix} t_{k_1+k_2+1} & t_{k_1+k_2} \\ t_{k_1+k_2} & t_{k_1+k_2-1} \end{bmatrix} \in S. \tag{2.1}$$

Associativity: Trivially satisfied.

Identity: $\exists\, F_2^0 \in S$ such that for all $F_2^k \in S$, $F_2^k * F_2^0 = F_2^k = F_2^0 * F_2^k$.

Inverse: For any $F_2^k \in S$ $\exists\, F_2^{-k} \in S$ such that $F_2^k * F_2^{-k} = F_2^0 = F_2^{-k} * F_2^k$.

Commutativity: For all $F_2^{k_1}, F_2^{k_2} \in S$, $F_2^{k_1} * F_2^{k_2} = F_2^{k_1+k_2} = F_2^{k_2} * F_2^{k_1}$.

So, $S = \{F_2^k = [t_{ij}] | t_{ij} \in \mathbb{F}_p$, p is a prime and $k \in \mathbb{Z}\}$ forms an abelian group w.r.t. multiplication operation*.

Theorem 2.2. *The set $S = \{F_n^k$ over $\mathbb{Z}_p$, p is a prime and $k \in \mathbb{Z}\}$ forms an abelian group with respect to usual matrix multiplication.*

Proof. Clearly, set S satisfies all the hypothesis of commutative group, so we omit the proof.

Theorem 2.3. *Order of initial Fibonacci matrix F_n over $\mathbb{Z}_2$ is $n+1$.*

Proof. From (1.1), initial values of generalized Fibonacci sequence are $t_0 = t_1 = ... = t_{n-2} = 0$ and $t_{n-1} = 1$. Over $\mathbb{Z}_2$, the proceeding terms are $t_n = 1$, $t_{n+1} = ... = t_{n+(n-1)} = 0$, $t_{2n} = t_{2n+1} = 1$ and so on. Using (1.3) over $\mathbb{Z}_2$, we have

$$F_n^{n+1} = \begin{bmatrix} t_{2n} & t_{2n-1} + t_{2n-2} + ... + t_{n+1} & \cdots & t_{2n-1} \\ t_{2n-1} & t_{2n-2} + t_{2n-3} + ... + t_n & \cdots & t_{2n-2} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n+2} & t_{n+1} + t_n + ... + t_3 & \cdots & t_{n+1} \\ t_{n+1} & t_n + t_{n-1} + ... + t_2 & \cdots & t_n \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 1 & 0 \\ 0 & 0 & 0 & ... & 0 & 1 \end{bmatrix}$$

i.e. $F_n^{n+1} = I_n$. Hence, over $\mathbb{Z}_2$ we have $|F_n| = n + 1$.

Theorem 2.4. *Rows of the Fibonacci matrix F_2 forms a basis for $R(1,1)$.*

Proof. From Definition 1.2, we have $R(1,1) = \{00, 01, 10, 11\}$ which is a binary $[2,2,1]$-linear code. Now, the Fibonacci matrix is rearranged as,

$$\begin{aligned} F_2 &= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad (R_2 \leftrightarrow R_1) \\ &\sim \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad (R_2 \leftrightarrow R_2 - R_1) \end{aligned}$$

Thus, $\{11, 10\}$ forms a basis for $R(1,1)$ as $R(1,1) = \{00, 01, 10, 11\} = < \{11, 10\} >$. Here, we consider rows of Fibonacci matrices as code (C).

Theorem 2.5. *Rows of the Fibonacci matrix F_2^k forms a basis for $R(1,1)$ over the field $\mathbb{F}_2$.*

Proof. Let S be the collection of F_2^k matrices over field $\mathbb{F}_2$, i.e

$$S = \{F_2^k \pmod 2\} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}.$$

Since for all k, $det(F_2^k) \neq 0$ over $\mathbb{F}_2$, so rows of F_2^k are linearly independent over $\mathbb{F}_2$. Thus, rows of any matrix from the set S forms a basis for $R(1,1)$. As,

$$R(1,1) = \{00, 01, 10, 11\} =< \{10, 01\} >=< \{11, 10\} >=< \{01, 11\} > .$$

Observe that the Hamming distance $d(C) = 1$ for each linear code C made from rows of elements of S.

Theorem 2.6. *Rows of multinacci matrix F_n forms a basis for $[n, n, 2]$-linear code.*

Proof. Consider a code $C =< \{111...1, 10...0, 010...0, ..., 0...10\} >$ whose matrix representation is F_n i.e. initial multinacci matrix. On performing row reduced echelon form (*RREF*) on matrix F_n, we obtain

$$F_n \sim \begin{bmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 0 & 1 \end{bmatrix}_{n \times n} = I_n.$$

Here rows of F_n are linearly independent after *RREF*, so they form a basis for a $[n, n]-$linear code, so C is $[n, n]$-code. Now, we have
$d\{11...1, 10...0\} = d\{11...1, 01...0\} = \cdots = d\{11...1, 00...10\} = n - 1$,
$d\{10...0, 01...0\} = d\{10...0, , 001...0\} = \cdots = d\{10...0, 00...10\} = 2$,
$\vdots$
$d\{00...01, 10...0\} = d\{00...01, 01...0\} = \cdots = d\{00...01, , 00...100\} = 2$
and, $d(C) = min\{n - 1, 2, 2..., 2\} = 2$.
So this is a $[n, n, 2]-$linear code. Thus, rows of F_n form a basis for $[n, n, 2]-$linear code. We should note that F_n refers to the generator matrix of the above $[n, n, 2]-$linear code.

Theorem 2.7. *A $[n, n, 2]$-linear code formed with the rows of multinacci matrix F_n is a LCD code.*

Proof. From Theorem 2.6, we have F_n as a generator matrix for $[n, n, 2]$-linear code and $Det(F_n) = (-1)^{(n-1)} \neq 0$.
So, $Det(F_n * F_n^T) = (Det(F_n))^2 = 1 \neq 0$.
Hence by Lemma 1.1, the $[n, n, 2]$-linear code with generator matrix F_n is a *LCD* code.

Theorem 2.8. *Let $S = \{F_n^k$ over $\mathbb{F}_2$ where $k \in \mathbb{Z}, n \in \mathbb{N}\}$. Then rows of any element of S form a basis for $[n, n]$-linear code i.e. rows of the kth power of multinacci matrix form a basis for $[n, n]$-linear code over $\mathbb{F}_2$. Moreover, this $[n, n]$-linear code is a LCD code.*

Proof. From Lemma 1.2, we have $Det(F_n^k) = (-1)^{k(n-1)} \neq 0$, so all rows of F_n^k are linearly independent. Hence, F_n^k forms a generator matrix for $[n, n]$-linear code.

Further, we have $Det(F_n^k * (F_n^k)^T) = (Det(F_n^k))^2 = ((-1)^{k(n-1)})^2 = 1 \neq 0$.
So by Lemma 1.1, the above $[n, n]$-linear code is a *LCD* code.

Now, let us define a rectangular matrix A of order $n \times n-1$ by deleting the last column of F_n (see, (1.4)) and it is given by

$$A = \begin{bmatrix} 1 & 1 & 1 & ... & 1 \\ 1 & 0 & 0 & ... & 0 \\ 0 & 1 & 0 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & ... & 1 \end{bmatrix}_{n \times n-1} . \tag{2.2}$$

The columns of the matrix A forms a parity check code leads to the following result.

Theorem 2.9. *The transpose of A i.e. A^T forms a generator matrix for a $[n, n-1, 2]$ parity check code.*

Proof. We have

$$A^T = \begin{bmatrix} 1 & 1 & 0 & ... & 0 \\ 1 & 0 & 1 & ... & 0 \\ 1 & 0 & 0 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & ... & 1 \end{bmatrix}_{n-1 \times n} .$$

Now permute the columns of A^T as $(1, n, n-1, ..., 3, 2)$ leads to the following matrix G,

$$G = \begin{bmatrix} 1 & 0 & ... & 0 & 1 \\ 0 & 1 & ... & 0 & 1 \\ 0 & 0 & ... & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 1 & 1 \end{bmatrix}_{n-1 \times n} = (I_{n-1}|X), \quad \text{where } X = (1, 1, ..., 1)^T.$$

Thus from Definition 1.1, G be the standard form of generator matrix for $[n, n-1]-$linear code.
By a similar argument to Theorem 2.6, we should note that $d(C) = 2$ where C is a code generated by the rows of A^T. Hence, A^T forms a generator matrix for a $[n, n-1, 2]$ parity check code. Similar to above theorem, we have the following result on *LCD* code with matrix generated by deleting the last row of F_n.

Theorem 2.10. *Let B refers to the matrix generated by deleting the last row of F_n, then B be a generator matrix for $[n, n-1, 2]$ LCD code.*

Proof. We have

$$B = \begin{bmatrix} 1 & 1 & ... & 1 & 1 & 1 \\ 1 & 0 & ... & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 1 & 0 & 0 \end{bmatrix}_{n-1 \times n} .$$

After some elementary operations on rows of B, we get

$$G' = \begin{bmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & ... & 1 & 1 \end{bmatrix}_{n-1 \times n} = (I_{n-1}|X),$$

where $X = (0, 0, ..., 1)^T$. Thus, by Definition 1.1 G' is in standard form.
By a similar argument to Theorem 2.6 yields that $d(C) = 2$ where C is code generated by the rows of B. So, B forms a generator matrix for a $[n, n-1, 2]$ *LCD* code.

3. Conclusion

In our study, we obtained different kinds of linear codes from generalized Fibonacci matrices. We proved that rows of multinacci matrices form a basis for the first order ReedMuller codes $R(1, 1)$ and different linear codes. Also we showed their relations with *LCD* code.

Future work. This study can be extended to generalized Lucas matrices, where for $k \geq 0$ the generalized Lucas sequence $\{l_n\}_{n\geq 0}$ of order n are defined by the relation[7]

$$l_{k+n} = l_k + l_{k+1} + l_{k+2} + ... + l_{k+n-1}, \quad n \geq 2, \tag{3.1}$$

with initial values $l_0 = k$ and $l_r = 2^r - 1$ for $1 \leq r < n$.
On replacing t_i's by $l_i's$ in the matrix given in (1.3) gives the generalized Lucas matrix $L_n^{(k)}$ [8], where the initial (generator) matrix for Lucas matrix is given as

$$L_n^{(0)} = \begin{bmatrix} 2^{n-1}-1 & 2^{n-1} & 2^{n-1}-k & ... & 7.2^{n-4} & 3.2^{n-3} & 2^{n-2}-1 \\ 2^{n-2}-1 & 2^{n-2} & 2^{n-2}+1 & ... & 7.2^{n-5} & 3.2^{n-4} & 2^{n-3}-1 \\ 2^{n-3}-1 & 2^{n-3} & 2^{n-3}+1 & ... & 7.2^{n-6} & 3.2^{n-5} & 2^{n-4}-1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & & \\ 1 & 2 & 3 & ... & n-2 & n-1 & n \\ n & 1-n & 2-n & ... & -3 & -2 & -1 \end{bmatrix}_{n\times n}.$$

Acknowledgment
The authors extend their gratitude to the Editor and anonymous referees for their fruitful suggestions and corrections. The first and second author acknowledge the University Grant Commission(UGC), India for the financial support in the form of research fellowship.

References

[1] M. Basu and B. Prasad, Coding theory on the m-extension of the Fibonacci p-numbers, *Chaos, Solitons & Fractals*, **42**(4) (2009), 2522–2530.
[2] M. Basu and B. Prasad, The generalized relations among the code elements for Fibonacci coding theory, *Chaos, Solitons & Fractals*, **41**(5) (2009), 2517–2525.
[3] T. Koshy, *Fibonacci and Lucas numbers with applications*, John Wiley & Sons, 2019.
[4] S. Ling and C. Xing, *Coding theory: a first course*, Cambridge University Press, 2004.
[5] J. L. Massey, Linear codes with complementary duals, *Discrete Mathematics*, **106** (1992), 337–342.
[6] K. Prasad and H. Mahato, Cryptography using generalized Fibonacci matrices with Affine-Hill cipher, *Journal of Discrete Mathematical Sciences and Cryptography*, (2021), 1–12, doi: 10.1080/09720529.2020.1838744.
[7] K. Prasad, H. Mahato and M. Kumari, *A novel public key cryptography based on generalized lucas matrices*, (2022), *ArXiv preprint arXiv:2202.08156*.
[8] K. Prasad and H. Mahato, On some new identities of Lucas numbers and generalization of Fibonacci trace sequences, *Palestine Journal of Mathematics* , 2022, (Article in press).
[9] A. Stakhov, Fibonacci matrices, a generalization of the Cassini formula and a new coding theory, *Chaos, Solitons & Fractals*, **30**(1) (2006), 56–66.
[10] A. Stakhov, The golden matrices and a new kind of cryptography, *Chaos, Solitons & Fractals*, **32**(3) (2007), 1138–1146.
[11] U. Sümeyra, T. Nihal and 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.
[12] N. Taş, S. Uçar, N. Y. Özgür and Ö Kaymak, A new coding/decoding algorithm using Fibonacci numbers, *Discrete Mathematics, Algorithms and Applications*, **10**(02) (2018), 1850028.