

Algebraic Theoretic Properties of the Non-associative Class of (132)-Avoiding Patterns of AUNU Permutations: Applications in the Generation and Analysis of a General Cyclic Code

Chun P. B^{1,*}, Ibrahim A.A², Garba A.I²

¹Department of Mathematics, Plateau State University, Nigeria

²Department of Mathematics, Usmanu Danfodiyo University, Nigeria

Copyright©2016 by authors, all rights reserved. Authors agree that this article remains permanently open access under the terms of the Creative Commons Attribution License 4.0 International License

Abstract The author had in [1] and based on the report as in [2], established interplay between the adjacency matrices due to Eulerian graphs constructed by the application of AUNU numbers and the generation and analysis of a general linear code. That was achieved by constructing a $[5\ 3\ 2]$ -linear code C of size $M = 8$. This paper reviews such a construction of a linear code as in [1] extending the approach to a larger (linear cyclic) code which is a super code say C^1 of the $[5\ 3\ 2]$ -linear code C of size $M = 8$, i.e $C \subseteq C^1$. To achieve this, the generator matrix G as in [1] that generated C is further developed to give a matrix say G^1 which now spans a larger linear code C^1 of length $n = 5$, dimension $k = 4$ and size $M = 32$. This is attainable by exhausting the cyclic shifts in the rows of the matrix G to give G^1 . It is then shown through some existing remarks and proven theorems that the linear code generated by G^1 is cyclic and has generator polynomial $g(x) = 1 + x$.

Keywords AUNU Numbers, Non-associative Class of AUNU Patterns, Linear Codes, Cyclic Shifts, Cyclic Codes, Generator Polynomials, Irreducible Polynomials, Generator Matrix

1. Introduction

The generation of a class of linear codes by the adjacency matrix of an Eulerian graph which is due to the AUNU numbers has been reported in [1]. The special class of the (132) and (123)-avoiding class of permutation patterns was first reported by Ibrahim A.A and Audu M.S (2005) where

they identified some group and graph theoretic properties of these numbers. Since then, this special class of permutation patterns has enjoyed a wide range of studies centered on applications in various areas of Mathematics in the last decade, since they were reported. Such areas of application ranges from, Association/Succession schemes, thin cyclic design, Latin squares, lattices theory, graph theory, automata theory, Coding theory e.t.c

Graph theory and Coding theory had proven to be interesting areas of research in recent times due to its increasing patronage by Mathematicians, computer scientists and Engineers alike. While Graph theory is generally concerned with the formulation of interconnection networks, the first paper on graph theory was said to be concerned with the formulation of a network for the crossing of the Kongsberg bridges [Euler, 2005]. Eulerian circuits have also of recent been reported to have found application to the problem of DNA fragment assembly [3].

Coding theory on the other hand which is concerned with the study of methods for efficient and reliable, storage and transfer of information from one place to another is said to have emanated in the early 1940s with Claude Shannon's paper titled "A Mathematical theory of Communication". Over the years, the theory had found a wide range of applications in areas such as, in the minimization of noise in compact disc recordings, data transfer from one electronic device to another, transmission of data through a distance source such as weather and communication satellites e.t.c. Coding theory had also witnessed tremendous development over the years with the generation and analysis of some important and practical codes such as, Hamming codes, Hadamard codes, BCH codes, Reed Muller codes, Reed Solomon codes, Golay codes etc.

The class of cyclic codes is equally an important class of codes due to their easy encoding and decoding schemes. The

natural requirement that a cyclic shift (π) in the bits of a codeword of a cyclic code C is still a codeword of C makes their encoding and decoding easy. A code C is said to be cyclic, if a cyclic shift of each of its codeword results to another word also in C . In this paper, we review the approach in the use of the adjacency matrices of subsets C_1, C_2 and C_3 of $\pi_A(132) \times \Omega_5$ as in [3] used in the generation of a class of linear codes [1] and use it in the generation and analysis of a larger class of linear cyclic codes.

2. Methodology

We first make some remarks and prove some existing theorem that would be of help in the understanding of our methodology;

Remark: By the generator polynomial of a linear cyclic code C , we mean a unique non-zero polynomial of minimum degree in C .

Theorem 1: (D.G Hoffman, . . . [et al], 1992)

Let $u, w \in C$ and that $\pi(u+w) = \pi(u) + \pi(w)$ and $\pi(av) = a\pi(v)$, $a \in K = [0, 1]$ where π denotes a cyclic shift. Then C is cyclic.

Proof:

To show that the linear code C is cyclic, it is enough to show that $\pi(v) \in C$ for each word in the basis for C .

Now, let $v = (v_0, v_1, \dots, v_{n-1})$, $w = (w_0, w_1, \dots, w_{n-1})$, then

$$\begin{aligned} v+w &= (v_0+w_0, v_1+w_1, \dots, v_{n-1}+w_{n-1}) \text{ and} \\ \pi(v+w) &= (v_{n-1}+w_{n-1}, v_0+w_0, \dots, v_{n-2}+w_{n-2}) \\ \pi(v+w) &\quad \square \end{aligned}$$

Theorem 2: (San ling and Chaoping Xing, 2004)

Let C be a cyclic code of length n and let $g(x)$ be the generator polynomial.

If $n-k = \deg(g(x))$, then;

- i. C has dimension k .
- ii. The codewords words corresponding to $g(x), xg(x), \dots, x^{k-1}g(x)$ are a basis for C .

Proof: The prove of (i) is obvious from definition.

To prove (ii), if $g(x)$ has degree $n-k$, then $g(x), xg(x), \dots, x^{k-1}g(x)$ must be linearly independent. Since $g(x)$ divides every codeword, there is a unique polynomial $a(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$ such that;

$$c(x) = a(x)g(x) = a_0g(x) + a_1xg(x) + \dots + a_{k-1}x^{k-1}g(x).$$

Therefore $c(x)$ is in $\langle \{g(x), xg(x), \dots, x^{k-1}g(x)\} \rangle$ and thus $\{g(x), xg(x), \dots, x^{k-1}g(x)\}$ is a basis for C . \square

We consider the adjacency matrices constructed as in [3] using subsets C_1, C_2 and C_3 of $\pi_A(132) \times \Omega_5$ as follows;

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Adjacency Matrix for subset C_1 of $\pi_{(132) \times \Omega_5}$

$$B = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Adjacency Matrix for subset C_2 of $\pi_{(132) \times \Omega_5}$

$$C = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Adjacency matrix for subset C_3 of $\pi_{(132) \times \Omega_5}$

Formation of the Generator Matrix G

Remark: Observe that the rows of matrix B which are all equal are a cyclic shift of the rows of matrix A and those of C are, a cyclic shift of the rows of B respectively.

Now, let G be the required generator matrix, then;

- i. Take an arbitrary row of A to be the first row of G .
 - ii. Take an arbitrary row of B to be the second row of G .
 - iii. Take an arbitrary row of C to be the third row of G .
- Then G becomes the matrix given by

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Formation of the Matrix G^1 That Spans C^1

Next, we consider the generator matrix G as above and transform it into a matrix G^1 . This transformation is achieved by exhausting the cyclic shifts in the rows of G since the rows of G are cyclic shifts of their predecessors;

After two more cyclic shifts of the last row of G , we obtain G^1 .

$$i.e G^1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

3. Findings

The rows of the matrix G^1 above, spans a cyclic code C^1 of length $n = 5$, size $M = 32$, has generator polynomial $g(x) = 1 + x$ and dimension $k = 4$. Furthermore, the matrix G^1 is also row equivalent with the generator matrix of C^1 .

4. Conclusions

This paper had succeeded in extending the applications of the graph theoretic properties of this special class of the (132)-avoiding Patterns in the generation and analysis of the linear class of codes, to that of the construction of a larger class of the cyclic class of codes.

Acknowledgements

We acknowledge the support enjoyed in this research Endeavour by the Institution Based Research (IBR) TETFund Grand 2015, of the Sokoto State University, Sokoto, Nigeria.

REFERENCES

- [1] Chun P. B, Ibrahim A. A, Garba A. I, Ajai P. T (Accepted; yet to be published) Algebraic theoretic properties of the (132)-avoiding class of AUNU permutation patterns: Application in the generation and analysis linear codes. *International Organization for Scientific Research (IOSR), Journal of Mathematics*.
- [2] Willem H. Haemers (2011) Matrices for graphs, Designs and Codes, (NATO Science for Peace and security, series 29 Information Security), *Coding theory and Related Combinatorics, IOS press, 2011*.
- [3] Ibrahim M, Ibrahim A. A, Yakubu M.A. (2012) Algebraic theoretic properties of the (132)-Avoiding class of AUNU patterns application in Eulerian graphs, *Journal of Science and Technology Research, 2012*.
- [4] Chun P. B, Ibrahim A. A, Nimyel T. N, Choji N. M (Accepted; yet to be published) Algebraic theoretic properties of the (132)-avoiding class of AUNU permutation patterns: Application in cyclic codes generation and analysis. *American Journal of engineering research*.
- [5] T. Mac Williams and N. Sloane (1997). The theory of Error – correcting Codes, *North Holland Mathematical library, 1997*.
- [6] D.G Hoffman, [et al] (1992) Coding Theory: The Essentials. *Mercel Dekker, Inc, 1992*.
- [7] Ibrahim A. A and Abubakar S. I (yet to be Published) Non-associative property of (123)-avoiding class of AUNU permutation patterns.
- [8] Robert H. Morelos-Zaragoza (2002). The Art of error-correcting coding. *John Wiley & Sons Ltd, England*.
- [9] Chun P.B (yet to be published), On Algebraic Structures and their Applications in Codes Generation and Analysis. *Department of Mathematics, Usmanu Danfodiyo University Sokoto, Nigeria*.