International Journal of Information Security, Privacy and Digital Forensics
Vol. 8, No. 2, December, 2024

Information Communication and Network Security System Modelling using Geometry Based Block Code in Information Theory (GBCIT) Technique

S.O. Oladejo
Department of Mathematical Sciences, Faculty of Science, Gombe State University, P.M.B 127, Gombe, Nigeria.
sooladejo@gsu.edu.ng

A. D. Adeniyi
Department of Mathematical and Computer Sciences, Faculty of Science, University of Medical Sciences, P.M.B. 536, Ondo City, Ondo-State, Nigeria.
aadeniyi@unimed.edu.ng

A.O. Adesola
Department of Mathematics and Statistics, Faculty of Pure and Applied Sciences, Kwara State University, Malete, P.M.B. 1530, Ilorin, Nigeria
ogunfeyimi.o@lasustech.edu.ng

Abstract. Information are transmitted over networks between two or more communicating and co-operating parties, through an established logical information channel which defines a route from source to destination, this method of information transmission in recent time, has becomes vulnerable to third party's threat to confidentiality, authenticity and security of such information. To alleviate these challenges, this work presents the design of a novel information communication and Network security model using Geometry Based Block Code in Information Theory (GBCIT) Technique. To this effect, a new concept is introduced to coding theory, codes $\mathbb{C}$ (where $\mathbb{C} \in \mathbb{Z}_{2k+1}^2, k \in \mathbb{Z}^+$) were expressed as set of blocks $\mathbb{B}(x_i, y_i), x_i, y_i \in \mathbb{Z}(2k+1)$ is a prime integer. Each block is isomorphic to any other points on the same code. As a result, a key was formulated which serve as check to know whether a block in a code is a representative of the set code or not. This serve as key dual function to decode a message which is transfer through a noisy channel and to check redundancy in data transmission. In this work, blocks $\mathbb{B}_i$ in code $\mathbb{C} \in \mathbb{Z}_{2k+1}^2$ were discussed. A comparison were made between each codes generated from $\mathbb{Z}_{2k+1}^2$, as a result, codes with $\mathbb{B}_{2k+1}(\alpha\beta, \alpha\gamma)$ is isomorphic to $\mathbb{B}_{2k+1}(\beta, \gamma)$ for β, γ a coprime.

Keywords: Block, Code, Near-linear geometries, Network Security, information transmission, Information theory.

1. Introduction

In recent time the common slogan of people of this generation is that the world is a global village. This means that transmission of message is easier nowadays compare to what was obtainable two-three decades ago, back then, sending messages from one location to another sometimes take days. Whereas in what takes ages to send to the one who needs a message could be transfer in microsecond nowadays. As the birth of internet facilities brought about a drastic change in the way we communicate, sending message sometimes has certain issues. For an example Eavesdroppers try their best possible ways to access what we send to authorized recipient with the intention of using such information for their personal gain. In other to address this loopholes, new technology improvement has to come to play so that anytime communication is initiated from one end the recipient should be able to have certain degree of assurance that the legitimate recipient is able to receive the message in full without compromising integrity or any alteration from unauthorized individuals, no matter the odds or disturbance in the communication channel.

The work of [1] and [2] in the early fifty's marked the beginning of Mathematical theoretical framework of the new area called coding theory. Also, the degree of importance attach to a message could probably determine its level of its secrecy. Human being by default would like to make a message of emotional attachment or love secret between the two parties sharing this feeling. Likewise sending a message that involves a financial transaction which requires certain token by the institution to confirm that the claimer is the rightful owner of the message. Manually, dealings of these categories are easy to handle since it involves face-to-face conversation. Also, it would be difficult for one party to

deny having such dealing once it is established and necessary paper works are carried out.

To solve problem of this nature, called cryptosystem concept addresses (to a significant level) problem of this type. Although being in existence as old as human race and practicalised for ages especially, during the world war II, this celebrated work was discussed in Kahn's The Codebreakers [3]. Since then it has become an area of attention for applied mathematicians and computing scientists. An existence of connection between finite geometry and coding was discussed in [4]. This argument was further strengthened in [5] and [6].

This work aims to look into coding theory from the perspective of geometry. Its application to data transmission over a noisy channel without compromising integrity and confidentiality. We define a finite geometry as a geometry with finite set of lines and finite set of points where points in the geometry are obtained by taking the Cartesian products of Z_d×Z_d where Z_d denotes an integer modulo d. In this work, d is a prime number and it is expressed as d=2k+1, k is a positive integer. Points in the geometry is denoted by P_d, it is obtained by taking an ordered pair of integer modulo d. Mathematically, it is denoted by Z(2k+1). In the past, researchers in this area have carried out a lot of work focusing on instances whereby two lines in a finite geometry intersect mostly at a point [7]. More work in this area was carried out by [8,9,10, and 11].

We divide the whole work into the following parts; Section one of this work presented the introduction to the research work. In Section two, we present the methodology adopted in the work, we define the notation used in the discourse which covers finite geometry G_(2k+1), discussion on the geometric approach to block code in information theory with numerical example, the symplectic group on G_(2k+1) was also presented. Potential areas of applications of this concept was discussed in section three. Finally, section four concludes our work.

2. Methodology

Many Mathematical concepts were used in this work, in other to aid the understanding of readers on the content of this article we define each concept as follows:

(i) A field of integer modulo 2k+1 is denoted by Z(2k+1) where k is an integer and 2k+1 is a prime number.

(ii) The notation ψ(2k+1) is called an Euler totient function. It cardinalities is the number of invertible elements in integer modulo 2k+1 where

$$\psi(2k+1) = 2k+1\prod_{k=0}^{2k}(1-\frac{1}{2k+1})$$

(iii) Let ψ(2k+1) represent the Dedekind psi function, it is defined as:

$$\psi(2k+1) = 2k+1\prod\left(1+\frac{1}{2k+1}\right); 2k+1 = \text{prime}$$

(iv) $\mathbb{G}\mathbb{c}\mathbb{D}(\theta,\lambda)$ denote the greatest common divisor of two elements θ and λ in Z(2k+1).

(v) The notation by a≅b means a maps b..

2.1. Finite Geometry $\mathbb{G}(2k+1)$

A finite geometry is a geometry which consists of a finite set of points and a finite set of lines. Mathematically it consists of the pair

$$\mathbb{G}(2k+1) = \left(\mathbb{p}(2k+1), \mathbb{L}(2k+1)\right) \quad (3)$$

Where $\mathbb{p}(2k+1)\ and\ \mathbb{L}(2k+1)$ denote the set of points and lines in $\mathbb{G}(2k+1)$ respectively

$$\mathbb{p}(2k+1) = \{(m,n)\mid m,n \epsilon\ \mathbb{Z}(2k+1)\} \quad (4)$$

and a line through the origin is define as

$$\mathbb{L}(\gamma,\beta) = \{(p\gamma, p\beta) \mid \gamma,\beta \epsilon\ \mathbb{Z}(2k+1), p\ \epsilon\ \mathbb{Z}(2k+1) \quad (5)$$

denotes set of lines. Equation (5) was discussed extensively in [12] and [13]

In this work, we generated codes from $\mathbb{Z}^2(2k+1))$ by acting $\alpha \epsilon\ \mathbb{Z}(2k+1)$ on $\alpha \epsilon\ \mathbb{Z}(2k+1)$ where $x, y \epsilon\ \mathbb{Z}(2k+1)$.

Near-linear finite geometry is our point of focus in this work as a result, two lines for example meets in one point at most (that is the origin). It is connected to the fact that Z(2k+1) is a field of integer modulo (2k+1) and all the lines in this work are through the origin. From [12] and [13] we deduce the following:

Proposition III.1.

(i) The code C(γ,β) is the same as code C(αγ,αβ),

Where

$$\mathbb{C}(\gamma,\beta) = \{(\alpha\gamma_1\ \alpha\beta_1), (\alpha\gamma_2\ \alpha\beta_2), \ldots, (\alpha\gamma_k\ \alpha\beta_k)\} \quad (6)$$

$$\mathbb{C}(s\gamma, s\beta) = \{(s\alpha\gamma_1, s\alpha\beta_1), (s\alpha\gamma_2, s\alpha\beta_2), \ldots (s\alpha_k, s\alpha_k, s\ \epsilon\ \ell(2k+1),$$

$$\alpha\ \epsilon\ \mathbb{Z}^*(2k+1), \gamma,\beta \epsilon\ \mathbb{Z}(2k+1) \quad (7)$$

$$\mathbb{C}(s\gamma, s\beta) \prec \mathbb{C}(\gamma,\beta) \quad (8)$$

(ii) There are ψ(2k+1) maximal code in finite geometry C(2k+1) with exactly 2k+1 points each.

2.2 Geometry Approach to Block Code in Information Theory

A code C over Z(p) is defined as a subset of the set Z^2 (p) with component from Z(p). It is denoted by C= Z^2 (p). Here, Z(p) is a field of integer modulo p. In this work we label it as word in this work.

Mathematically, it is defined as

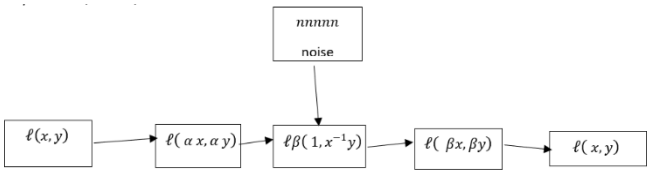
$$\mathbb{C}(a,b) = \{(\alpha a, \alpha b) \mid a,b \in \mathbb{Z}(p)\}, \alpha \in \mathbb{Z}(p), i = 1,2,\dots,p \quad (9)$$

A code is defined as collection of message that are transmitted over a communication channel. In this work each point of a line in Z^2 (2k+1) is interpreted to be a block which houses message. Transmission of messages from sender to a receiver is subjected to noise or disturbance. As a result, a message may be corrupted before transmission through a channel to the recipient. In this work we define a model for generating the block and formulate a code as protection for the transmitted data which recipient use to cross check and confirm that what is transmitted is what is received. This model ensure redundancy to check-mate an instance if a message has been tempered with by an unauthorized person, spy or adversaries. Hence confirm confidentiality and integrity of such a message.

We define encoding as a changing process whereby a message from a sender or sources passes through a channel using some uncomprehendable dialect to the receiver or destination. Technically, changing a plaintext to cipher text next transmission over a noisy channel thereafter, change the cipher text back to the original message that is plaintext. Let C(2k+1)={0,1,2,…,2k} represents the message to be transmitted through a channel. Coding is defined in our context as the relationship between the set Z(2k+1) and Z(2k+1). Mathematically, a coding is defined as a Cartesian products A×B where A=B=Z(2k+1). This concept was used in [14] where projective lines were defined over a finite quotient ring of integers. That is in this work, a code K=Z(2k+1)× Z(2k+1). Each subset represents a block. Suppose we define α as set where $\alpha \in \ell(2k+1)$ acting α on K yields a coded word. Using the language of algebra, K becomes a cyclic module. Pairing any element of K yields a code.

The communication system whose diagram is shown in figure 1 is algebraic in nature in the sense that the source selects a code out of all the codes generated arbitrarily and transmits the sequence of algebraic symbols from a given options (code) to the channel based on certain rule. The channel transmits this symbolic information to the receiver having decoded the message under certain rule. Furthermore, the set of all possible pair of A×B yields complete set of block code in Z(2k+1).

FIG. 1: The diagram showing the structure of



communication systems, for β,α $\in \beta, \alpha \in \mathbb{Z}^*(2k+1)$

From proposition III.1 we confirm the following:

$$G(\mu,\lambda)=G(q\mu,q\lambda) \quad (10)$$
$$\forall q \in l_(2k+1)\hat{}^*$$
$$G(\mu,\lambda)\cong G(p\mu,p\lambda), \quad (11)$$

Hence G(μ,λ) and G(qμ,qλ) are isometric to each other.

Proposition IV.1. If l(μ,λ) is a line of near-linear finite geometry G_(2k+1)where 2k+1 is a prime integer.

G(μ,λ) is isometric to $\mathcal{G}(p\mu, p\lambda)., \forall q \in \ell^*_{2k+1}$ (12)

Proof. Let $a, b \in \ell(2k+1)$ where (2k+1) is a prime integer, since $\ell(2k+1)$ is a field, it means every non-zero integer has an inverse and each of the non-zero element is an additive generator.

Hence complete the proof.

From equation (9) above, Lines in geometry $\mathbb{G}(5)\Xi\mathbb{Z}^2(5)$ is obtained as follows:

$\mathcal{G}(0,1) \cong \mathcal{G}(0,1) \cong \mathcal{G}(0,2) \cong \mathcal{G}(0,3) \cong \mathcal{G}(0,4)$ (13)
$\mathcal{G}(1,0) \cong \mathcal{G}(1,0) \cong \mathcal{G}(2,0) \cong \mathcal{G}(3,0) \cong \mathcal{G}(4,0)$ (14)
$\mathcal{G}(1,1) \cong \mathcal{G}(1,1) \cong \mathcal{G}(2,2) \cong \mathcal{G}(3,3) \cong \mathcal{G}(4,4)$ (15)
$\mathcal{G}(1,2) \cong \mathcal{G}(1,2) \cong \mathcal{G}(2,4) \cong \mathcal{G}(3,1) \cong \mathcal{G}(4,3)$ (16)

$\mathcal{G}(1,3) \cong \mathcal{G}(1,3) \cong \mathcal{G}(2,1) \cong \mathcal{G}(3,4) \cong \mathcal{G}(4,2)$ (17)
$\mathcal{G}(1,4) \cong \mathcal{G}(1,4) \cong \mathcal{G}(2,3) \cong \mathcal{G}(3,2) \cong \mathcal{G}(4,1)$ (18)

Where

G(1,2)≅{Ɓ (0,0), Ɓ (1,2), Ɓ (2,4), Ɓ (3,1), Ɓ (4,3)}

2.3 **Symplectic Group On $\mathcal{G}(2k+1)$**

The Symplectic group is a linear transformation which change a set to another set in the group and preserves the properties that constitute the group. This concept was discussed and used in [15] to generate a complete set of mutually unbiased bases in prime dimensional Hilbert space. It is used in quantum cryptography. More contributions were made by [16] and [17]. It is a $2n \times 2n$ which is denoted by $Sp(2n)$ matrix whose determinant is 1 for $n = 1$. In this work, it is a unitary transformation which satisfies the condition $|\mu| = 1(mod(2k+1))$. Mathematically,suppose $\mu = (\xi,\zeta \mid \gamma,\beta)$ be defined as unitary matrices where $\mu = (\xi,\zeta \mid \gamma,\beta) = \begin{pmatrix} \xi & \zeta \\ \gamma & \theta \end{pmatrix}$, $|\mu| = |\xi\theta - \zeta\gamma| = 1(mod\ 2k+1)$, where $\xi,\zeta\ \boldsymbol{\lambda},\theta \in \ell(2k+1)$, μ form a group called symplectic group $Sp(2,\ell(2k+1))$ group. Acting μ on all blocks of code $\mathcal{G}(x,y)$ in $\ell(2k+1)$ it generates all of the code $\ell(\xi x + \zeta y)$. That is $\mu(\xi,\zeta \mid \gamma,\beta)\ell(x,y)^T$. Example suppose $k = 2$ then $2k+1 = 5$ and we substitute 2,1,1 and 1 for ξ,ζ,γ,β respectively into μ and act it on $\ell(x,y)$ where $x = 0, y \in \ell_5$ it yields $\mathcal{G}(1,1)$ in eq.(10). Suppose d is a prime, acting $\mu = (0,1 \mid -1,\chi)$ on the code $\mathcal{G}(0,1)$, we obtain all the codes (maximal lines) through the origin. For

$$\chi = 0, \dots, d-1 \to \Xi(\chi) = \mu = (0,1|\ -1,\chi)\ \mathcal{G}(0,1) = \ell(1,\chi) \quad (20)$$

In this work, we fix a rule that $\chi = -1, .\mu(0,1|\ -1,\chi)$ is replaced by $\mu(1,0 \mid 0,1)$.

If we substitute the value of $\chi = -1, \dots, 2k$, we obtain all the lines in $\mathcal{G}(2k+1)$ we obtain all the points. Hence $\mu(0,1|\ -1,\chi)\ \ell(0,1) \cong \ell(1,\chi)$.

The Geometry Based Block Code Information Theory (GBCIT) Algorithm is presented in algorithm listening 1.

Algorithm listening 1: The Geometry Based Block Code Information Theory (GBCIT) Algorithm.

1. Function
2. Let $\mathbb{C}(2k+1) = \{0,1,2, \dots, 2k\}$ represents the message to be transmitted through a channel.
3. Let coding be defined as the relationship between the set $\mathbb{Z}(2k+1)$ and $\mathbb{Z}(2k+1)$ i.e. the Cartesian products $\mathcal{A} \times \mathcal{B}$ where $\mathcal{A} = \mathcal{B} = \mathbb{Z}(2k+1)$.
4. Let each subset code $\mathrm{K} = \mathbb{Z}(2k+1) \times \mathbb{Z}(2k+1)$. represents a block and α is defined as set where $\alpha \in \ell(2k+1)$ acting α on K yields a coded word. K becomes a cyclic module. Pairing any element of K yields a code.
5. The set of all possible pair of $\mathcal{A} \times \mathcal{B}$ yields complete set of block code in $\mathbb{Z}(2k+1)$.
6. Let $\mathrm{a}, \mathrm{b} \in \ell(2\mathrm{k}+1)$ where $(2\mathrm{k}+1)$ is a prime integer, since $\ell(2\mathrm{k}+1)$ is a field, it means every non-zero integer has an inverse and each of the non-zero element is an additive generator.
7. A code is a finite geometry G_d over Z_d representing a set of messages stored in a medium such as magnetic disk over a period of time.
8. Given a plain text message $M(x,y)$ from source , the message is sent and received as $M(\kappa x, \kappa y)$ by the destination.
9. The destination checks for a bijection between the received message and the original message from the source. That is, if $M(x,y) \cong M(\kappa x, \kappa y)$.
10. K represents redundancy in the message.
11. Check for reasonable level of noise, if $\ell(x,y) \cong \kappa\ell(x,y)$, i.e. if the noise is reasonable, then
12. The message is secure otherwise
13. The message receive is corrupt.
14. End Function

3. Application of the proposed Geometry Based Block Code Information Theory (GBCIT) Technique

The concept presented in this work can be applied in different area of information and network security specifically, it can be used in generating social security number of a population, encoding and decoding messages on the transmission networks it can also be used for generating International Standard Book Number (ISBN) and many more.

As an illustration, suppose there are two individuals Alice and Bob who want to exchange a message. Alice has a message to deliver to bob, the message is digitized. She sends it to Bob via an untrusted channel. Such message is coded before sending and Bob receive a coded message. A code in the context of this work is a finite geometry G_d over Z_d is a set of messages stored in a medium such as magnetic disk over a period of time. An individual, Alice is the entity communicating to herself by storing information in the disk in the same location over a period of time.

In this work, $M(x,y)$ is the message Alice sent. Bob, who is far away receive $M(\kappa x, \kappa y)$. To confirm whether the message has been tampered with, he checks for a bijection between the content of what he received and what he was communicated initially by Alice. That is $M(x,y) \cong M(\kappa x, \kappa y)$.

Between the storage time and retrieval time, there are possibilities that certain unwanted incident must have happened to the content of the disk. This incident could be natural one such as flood, climate change, or man-made such as denial of service (DOS), virus, worms, Trojan, etc among others which has the potential of tampering with the content of the disk.

In other to protect the content disk or message sent by Alice to Bob over a noisy / untrusted channel, error detection or content validation code safeguards the integrity of a message.

Our aim in this work is that if the noise is reasonable, then $\ell(x,y) \cong \kappa\ell(x,y)$ otherwise the message receive is corrupt. As the reason for encoding is to safeguard the integrity of data, this is carried out by adding redundancy to a message. Here in this work, κ represents redundancy in the message. In the context of this work, an area of application of isometric lines is in Coding of message specifically in redundancy code.

4. Conclusion

In this work, we discussed a new prospective to coding theory, here we look at this concept from finite geometry perspective, in it, each block is obtain acting invertible element in finite integer modulo d for d a prime. Following this concept, a complete set of code is generated which can be encoded into a message to be transmitted by the source and decoded by the receivers of the message at the receiving end.

research on this issue has the potential to change the existing situation where a great number of rules are mined while few of them are interesting to business. The SEM-AKD model provides a transferable framework that can support various critical functions, including the development of targeted crime prevention strategies, optimization of resource allocation decisions, and formulation of evidence-based policy recommendations.

Based on the results obtained from our experimentation using datasets from crime domain and banking domain, we can surmise that this comprehensive approach bridges the gap between theoretical data mining and practical decision-making needs in law enforcement and public safety domains. SEM_AKD showed a 6.4% (banking Domain) and 7.4%(crime domain) accuracy improvement and actionable pattern prioritization. Though it depends on expert input, this framework supports crime prevention, resource allocation, and policymaking. Further work could automate weightings and extend to unstructured data, further enhancing real-world utility.

References

[1] D.Kahn (1967), The codebreakers: the story of secret writing. MacMillan Publishing Company, New York, NY, USA.

[2] R.W Hamming (1950), Error detecting and error correcting codes, Bell System Technical Journal 29, Pp. 147-160.

[3] C.E Shannon (1948), A mathematical theory of communication. Bell System Technical Journal 27, Pp. 379-423 and 623-656.

[4] David C. Clark (2011), Applications of finite geometries to designs and codes. Michigan Technological University, PhD Thesis.

[5] I.E Shparlinski (1999), Finite Fields: theory and computation, Kluwer Academic Publishers, Dordrecht. The meeting point of number theory, computer science, coding theory and cryptography.

[6] A.K. Sharma (1993), 'Operations Research: Theory and Practice' Prentice Hall Publishers, India.

[7] L.M Batten (1979), 'Combinatorics of finite geometrics', Cambridge Univ. Press, Cambridge.

[8] M. Planat, and M. Saniga (2007), Projective line over the finite quotient ring and quantum entanglement: Theoretical background. Journal of Theoretical and Mathematical Physics, Vol. 151, No. 1. https://doi.org/10.4213/tmf6010

[9] T. Shubin (2006), Lecture Notes on Finite Geometries, Department of Mathematics San Jose State University, Califonia, USA.

[10] O. Albouy (2009), The Isotropic Lines of Z_d^2, Journal of Physics A: Mathematical and Theoretical Vol. 42, No. 072001.

[11] S.O. Oladejo, C.Lei, and A. Vourdas (2014), Partial Ordering of Weak Mutually Unbiased Bases Journal of Physics A: Mathematical and Theoretical Vol.47, No. 485204.

[12] M. Shalaby, and A. Vourdas (2012), Weak Mutually Unbiased Bases, Journal of Physics A: Mathematical and Theoretical Vol.45, No.052001.

[13] M. Shalaby, A. Vourdas (2013), Mutually unbiased projectors and duality between lines and bases in finite quantum systems, Annals of Physics, Vol. 337, Pp. 208-220.

[14] M. Saniga, and M. Planat (2005), Viewing sets of mutually unbiased bases as arcs in finite projective planes (2005), Chaos, Solitons & Fractals, Vol.26, No.5, Pp. 1267-1270, https://doi.org/10.1016/j.chaos.2005.03.008.

[15] Durt, T., Englert, B.-G., Bengtsson, I. and Zyczkowski, K. (2010) On Mutually Unbiased Bases. International Journal of Quantum Information, 8, 535.https://doi.org/10.1142/S0219749910006502.

[16] K. Gibbons, M.J. Hoffman, and W. Wootters (2004), Discrete phase space based on finite fields. Physics Review A, Vol. 70, No. 062101. DOI: https://doi.org/10.1103/PhysRevA.70.062101Phys. Rev. A70, 062101.

[17] Maurice R Kibler, Michel Planat (2006), A SU (2) recipe for mutually unbiased bases, International Journal of Modern Physics B, Vol 20, Pp. 1802-1807. World Scientific Publishing Company.