Lines of Finite Geometry Z_n^2

S.O. Oladejo[1*], A. W. Yekinni[2], and T. A. Mojeed[3]

[1]*Department of Mathematics, Faculty of Science, Gombe State University, Gombe, Nigeria,*

[2]*Department of Computer Science, School of Technology, Lagos State Polytechnic, Lagos, Nigeria*

[3]*Department of Computer Science, School of Computing, Federal University of Technology, Akure, Ondo State, Nigeria,*

**Corresponding author*

***Abstract:* - In this work, we examined thoroughly lines of finite geometryZ_n^2, where n is a non-prime. For m a divisor of n, an existence of non trivial subgeometries was discovered which form a partial ordered relation with subgeometries as partial order. For finite geometries G_n comparison were made between each lines of prime dimensional G_n, lines with L $(a\mu, a\lambda)$ is isomorphic to L (μ, λ) and lines that are isometric to each other have equal slope. For the non-prime dimension G_n, L $(a\mu, a\lambda) \cong$ L (μ, λ) if $a \in Z_n^*$ and L $(a\mu, a\lambda) \prec$ L (μ, λ) if $a \in Z_n - Z_n^*$for μ, and λ a coprime.**

***Keywords:* Near-linear geometry, Isometric lines, finite geometries**

I. INTRODUCTION

Attention of researchers was directed to certain areas of quantum mechanics especially, finite quantum systems with variables in $Z_{n.}$. Tobe specific, concepts like mutually unbiased bases in Finite Hilbert space got tremendous interests [1-6]. This development could be linked to its application in concepts quantum cryptography. The mutually unbiased is obtained by finding the dot product of two vectors each from different bases, the result gives $\frac{1}{\sqrt{n}}$ for n a prime. Ina prime dimensional finite system, the number of mutually unbiased bases is $n+1$. If $n = p^{\varepsilon}$where $\varepsilon > 1$and p is a prime integer, there exists $n+1$ mutually unbiased bases. However if n is an even integer, the number of mutually unbiased bases is not known till today [7].An existence of a link between finite geometry and finite dimensional Hilbert spaces was shown in [7].Not long ago, a non-near-linear finite geometry received attention [8-12], in it unlike the near-linear counterpart, two lines intersect in at least one point. In [13] some dualities which exists between lines non-near linear finite geometry and weak mutually unbiased bases infinite quantum systems was shown. In a near-linear geometryZ_n^2, for n a prime, there exists $\varphi(n)$ lines isometric to each other. This forms$n+1$ distinct partitions [16]. Also taking the gradients of any two arbitrary points in each $n+1$ partitions produce an equal slopes. Symplectic transformation plays a significant role in finite geometry in the sense acting a matrix which satisfies the Symplectic conditions on a line produce another line in the geometry. This yields all the lines for the near-linear geometry and hence forms complete set of near-linear finite geometry. In the non-near-linear finite geometry, lines in such finite geometry intersect in more than one points which forma partially ordered set with the m points. This forms a partial ordered relation where lines with $m$points as partial order. This section forms the basis of this work. In it, we intend to examine the set of lines generated from the finite geometry Z_n^2 where n is a non-prime.

The whole work is partitioned into six sections thus: preliminary of this work is discussed in section II. Here, we define the notation we used in the discourse. The concept of finite geometry along with there view of previous work is discussed in Section III. In section IV, we discuss isometric lines of Z_n^2. Symplectic transformation on Z_n^2 with numerical example is discussed in section V. The conclusion of our work isin section VI.

Definition: Let X *and* Y be two sets, a map $\pi: X \to Y$ is an isometry if and only if there exists a bijection between X *and* Y.In this article, X *and* Y are finite sets of integer modulo$n$. It is denoted by Z_n.

II. PRELIMINARIES

(i) $G_n = Z_n^2$

(ii) A ring of integer modulo n is denoted by Z_n where $Z_n = \{0,1,\dots,n-1\}$

(iii) In the ring of integer modulo n there are invertible and non-invertible elements, the number of invertible element is represented by $\varphi(n)$ where

$$\varphi(n) = n\prod\left(1-\frac{1}{n}\right);\ n = \text{prime} \tag{1}$$

(iv) in this work we used the Dedekind psi function, it is denoted by $\psi(n)$ where;

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

(v) The greatest common divisor of two elements α and β is denoted by GCD(α, β).

(vi) The notation $x \cong y$ means $x$maps y.

(vii) The symbol, $\prec$ denotes partial ordering.

(viii) $m \mid n$ means m divides n , this implies a G_m is a subgeometry of G_n.

(ix)$\frac{\Delta y}{\Delta x}$ means increment or change in y with respect to x.

III. FINITE GEOMETRY G_n

Definitions: (i) A finite geometry is ageometry with the combination of points and lines. It is denoted by

$$G_n = (P_{n,} L_n), \tag{3}$$

Where$P_{n,}$ and L_n denote the set of points and lines in G_n respectively

$$P_{n,} = \{(g,h) \mid g,h \in Z_n\}. \tag{4}$$

(ii) A line through the origin is defined as

$$\mathrm{L}\ (\alpha,\beta) = \{(\lambda\alpha,\lambda\beta) \mid \alpha,\beta \in Z_n\}, \lambda \in Z_n \tag{5}$$

The non-near-linear finite geometry is our focus in this article. In this type of geometry, any two arbitrary lines which belong to the same representation have $m$points in common for$m$ a divisor of n**.**

The reason is linked to the fact that Z_n is a ring of integer modulo n,and in this case, not every elements in the set has an inverse. From the previous work of [6] we confirm the following propositions:

Proposition III.1.

(i)$\mathrm{L}\ (\mu,\lambda) = \mathrm{L}\ (p\mu,p\lambda), \forall p \in Z_n^*$ (6)

and

$\mathrm{L}\ (p\mu,p\lambda) \prec \mathrm{L}\ (\mu,\lambda), \forall p \in Z_n - Z_n^*$ (7)

A line L $(p\mu,p\lambda)$ is a maximal line in G_n if GCD$(\mu,\lambda) \in Z_n^*$, and L (μ,λ) is a subline in G_n if GCD$(\mu,\lambda) \in Z_n - Z_n^*$

(ii) There are $\psi(n)$ maximal lines in finite geometry G_n with exactly n points each.

(iii) If two maximal lines have m points in common where $m \mid n$. The m points gives a subline$L(\alpha,\beta)$ where $\alpha,\beta \in \frac{n}{m} Z_n$.

(iv) There are $\psi(m)$ maximal lines in finite subgeometry $G_m$each line of it with exactly m points in each lines of finite geometry $G_n$with n points each.

(v) Suppose we define a line in finite geometry $G_n$as in equation (5), $L(\alpha,\beta)$ is also

$$L(t\alpha,t\beta) = \{(t\alpha, t\beta) \mid \in Z_n\}, in\ G_n, \tag{8}$$

at the same time the line $L(\mu\alpha,\mu\beta) in\ G_n$is a subline of

$$L(\alpha,\beta) = \{(\alpha t', \beta t') \mid t' \in Z_{\mu n}\} \tag{9}$$

IV. ISOMETRIC LINES OF G_n

Suppose $G_n = Z_n \times Z_n$ where Z_n is a ring of integer modulo n, if $q \in Z_n^*$,if q is an invertible element in Z_n then

$L(\alpha,\beta)$is isometric to $L(q\alpha,q\beta)$. However, $q \in Z_n - Z_n^*$then $L(q\alpha,q\beta) \prec L(\alpha,\beta)$that is $L(q\alpha,q\beta)$ is a subline of $L(\alpha,\beta)$.

Hence $L(\alpha,\beta)$ and $L(q\alpha,q\beta)$ are isometric to each other.

From our analogy we deduce the following propositions:

Proposition IV.1: If $L(\alpha,\beta)$ is a line of non- near-linear finite geometry $G_n$and $\gcd(\alpha,\beta) \in Z_n^*$, then$L(\alpha,\beta)$ is isometric to $L(p\alpha,p\beta) \forall p \in Z_n^*$ (10)

Proof: Let $\alpha,\beta \in Z_n$for$n$ is a non-prime integer. Since n is a non-prime integer, Z_n is a ring and not every members of the set has an inverse as a result $L(\alpha,\beta)$is isometric to $L(p\alpha,p\beta)$if and only if $\alpha$and $\beta$are coprime and $\gcd(\alpha,\beta)$ has an inverse in Z_n. Hence the proof.

Proposition IV.2: If $L(\alpha,\beta)$ is a line in a subgeometry $G_m$of non- near-linear finite geometry G_n, m is a prime integer then $L(\vartheta\gamma,\vartheta\delta)$ is an isometric line to $L(\gamma,\delta)$ if γ and , δ are non-zero element of Z_m and $\vartheta \in Z_m^*$.

Proof: The proof is self evident since Z_m is a field, it implies that every non-zero members of Z_m has an inverse and if replace we$p = \vartheta$ in equation (10) is the additive generator.

Hence complete the proof.

An illustration of isometric lines is shown as $n = m_1 \times m_2$, for $n = 15$.

Examples: Suppose $n = 15 \equiv 3 \times 5$: using equation (3).

For $m_1 = 3$, we get

L (0;1) ≅ L(0; 2) (11)

L (1; 0) ≅ L (2; 0) (12)

L (1; 1) ≅ L (2; 2) (13)

L (1; 2) ≅ L (2; 1) (14)

For $m_2 = 5$, we get.

L (0;1) ≅ L(0; 2) ≅ L (0; 3) ≅ L(0; 4) (15)

L (1; 0) ≅ L (2; 0) ≅ L (3;0) ≅ L (4; 0) (16)

L (1; 1) ≅ L (2; 2) ≅ L (3;3) ≅ L (4; 4) (17)

L (1; 2) ≅ L (2; 4) ≅ L (3;1) ≅ L(4; 3) (18)

L (1; 3) ≅ L (2; 1) ≅ L (3; 4) ≅ L (4; 2) (19)

L (1; 4) ≅ L (2; 3) ≅ L (3; 2) ≅ L (4; 1) (20)

For n a prime integer,finding the slope of lines in a prime dimensional finite geometry by taking any two arbitrary points of any line $L(\alpha,\beta) \cong L(q\alpha, q\beta)$yield identical results in general. However, for n a non-prime there is no absolute assurance producing identical results when carrying out the same tasks as we illustrated for $n = 3\ and\ 5$ above. These results further strengthen our claim. To consider points of $L(1,2)$ of finite geometry G_5, we obtained the following results. Here $\alpha = 1, \beta = 2$ That is

$$\frac{\Delta\beta}{\Delta\alpha} = \frac{2-1}{1-2} = 2 \equiv \frac{2-1}{1-3} = \frac{1}{-2} \equiv \frac{1}{3} = 4\big(i.e\ 3^{-1}(mod\ 5)\big)$$
$$= 2 \equiv \frac{2-3}{1-4} = \frac{4}{2}(mod\ 5) \equiv \frac{4-1}{2-3}$$
$$= 3\big(i.e\ 4^{-1}(mod\ 5)\big) \equiv \frac{4-3}{2-4}$$
$$= 3^{-1}(mod\ 5) \equiv \frac{1-3}{3-4} \equiv \frac{3-1}{4-3} \equiv \frac{3-4}{4-2}$$
$$\equiv \frac{3-2}{4-1} \equiv \frac{1-4}{3-2} \equiv \frac{1-2}{3-1} \equiv \frac{4-2}{2-1}$$
$$= 2(mod\ 5)$$

For $n = 15$ we obtain the following

L (0,1)≅ L(0,2)≅ L(0,4)≅ L(0,7)≅ L(0,8)≅ L(0,11) ≅ L(0,13) ≅ L(0,14)

L (1,0)≅ L(2,0)≅ L(4,0)≅ L(7,0)≅ L(8,0)≅ L(11,0) ≅ L(13,0) ≅ L(14,0)

L (1,1)≅ L(2,2)≅ L(4,4)≅ L(7,7)≅ L(8,8)≅ L(11,11) ≅ L(13,13) ≅ L(14,14)

L(1,2)≅ L(2,4)≅ L(4,8)≅ L(7,14)≅ L(8,1)≅ L(11,7) ≅ L(13,11) ≅ L(14,13)

L(1,3)≅ L(2,6)≅ L(4,12)≅ L(7,6)≅ L(8,9)≅ L(11,3) ≅ L(13,9) ≅ L(14,12)

L(1,4)≅ L(2,8)≅ L(4,1)≅ L(7,13)≅ L(8,2)≅ L(11,14) ≅ L(13,7) ≅ L(14,11)

L(1,5)≅ L(2,10)≅ L(4,5)≅ L(7,5)≅ L(8,10)≅ L(11,10) ≅ L(13,5) ≅ L(14,10)

L(1,6)≅ L(2,12)≅ L(4,9)≅ L(7,12)≅ L(8,3)≅ L(11,6) ≅ L(13,3) ≅ L(14,9)

L(1,7)≅ L(2,14)≅ L(4,13)≅ L(7,4)≅ L(8,11)≅ L(11,2) ≅ L(13,1) ≅ L(14,8)

L(1,8)≅ L(2,1)≅ L(4,2)≅ L(7,11)≅ L(8,4)≅ L(11,13) ≅ L(13,14) ≅ L(14,7)

L(1,9)≅ L(2,3)≅ L(4,6)≅ L(7,3)≅ L(8,12)≅ L(11,9) ≅ L(13,12) ≅ L(14,6)

L(1,10)≅ L(2,5)≅ L(4,10)≅ L(7,10)≅ L(8,5)≅ L(11,5) ≅ L(13,10) ≅ L(14,5)

L(1,11)≅ L(2,7)≅ L(4,14)≅ L(7,2)≅ L(8,13)≅ L(11,1) ≅ L(13,8) ≅ L(14,4)

L(1,12)≅ L(2,9)≅ L(4,3)≅ L(7,9)≅ L(8,6)≅ L(11,12) ≅ L(13,6) ≅ L(14,3)

L(1,13)≅ L(2,11)≅ L(4,7)≅ L(7,1)≅ L(8,14)≅ L(11,8) ≅ L(13,4) ≅ L(14,2)

L(1,14)≅ L(2,13)≅ L(4,11)≅ L(7,8)≅ L(8,7)≅ L(11,4) ≅ L(13,2) ≅ L(14,1)

L(3,1)≅ L(6,2)≅ L(12,4)≅ L(9,8)≅ L(6,7)≅ L(3,11) ≅ L(9,13) ≅ L(12,14)

L(3,2)≅ L(6,4)≅ L(12,8)≅ L(9,1)≅ L(6,14)≅ L(3,7) ≅ L(9,11) ≅ L(12,13)

L(3,4)≅ L(6,8)≅ L(12,1)≅ L(9,2)≅ L(6,13)≅ L(3,14) ≅ L(9,7) ≅ L(12,11)

L(3,5)≅ L(6,10)≅ L(12,5)≅ L(9,10)≅ L(6,5)≅ L(3,10) ≅ L(9,5) ≅ L(12,10)

L(3,8)≅ L(6,1)≅ L(12,2)≅ L(9,4)≅ L(6,11)≅ L(3,13) ≅ L(9,14) ≅ L(12,7)

L(5,1)≅ L(10,2)≅ L(5,4)≅ L(5,7)≅ L(10,8)≅ L(10,11) ≅ L(5,13) ≅ L(10,14)

L(5,2)≅ L(10,4)≅ L(5,8)≅ L(5,14)≅ L(10,1)≅ L(10,7) ≅ L(5,11) ≅ L(10,13)

L(5,3)≅ L(10,6)≅ L(5,12)≅ L(5,6)≅ L(10,9)≅ L(10,3) ≅ L(5,9) ≅ L(10,12)

Where

L(1,4)={(0,0)(1,4)(2,8)(3,12)(4,1)(5,4)(6,9)(7,13)(8,2)(9,6)(10,10)(11,13)(12,3)(13,7)(14,11)}(21)

L(1,5)={(0,0)(1,5)(2,10)(3,0)(4,5)(5,10)(6,0)(7,5)(8,10)(9,0)(10,5)(11,10)(12,0)(13,5)(14,10)}(22)

Finding the slope of L(1,4) of equation (21) by taking any two arbitrary points yields an identical results throughout where as carrying the same task in equation (22) does not guarantee uniform results.

V. SYMPLECTIC TRANSFORMATION ON G_n

Let

$$\mathbb{S}\ (\sigma,\tau \mid \lambda,\mu) \tag{23}$$

represents a unitary transformation where

$$\mathbb{S}\ (\sigma,\tau \mid \lambda,\mu) \equiv \begin{pmatrix} \sigma & \tau \\ \lambda & \mu \end{pmatrix}$$

$|\mathbb{S}| = |\sigma\mu - \tau\lambda| = 1\ (mod\ n)$, where$\mu, \sigma, \tau,\ \ \lambda \in Z_n$, $\mathbb{S}$ forms a group called Symplectic group Sp(2,Z_n) group.

Acting $\mathbb{S}$ on all points of line L (x, y) in Z_n^2generates all the points of the line L (σx+ τ y,λx+ μ y).

This is expressed in this work as $\mathbb{S}\ (\sigma,\tau \mid \lambda,\mu\ )$L (x; y).

Example: Suppose n = 5 and we substitute 2,1,1, and 1 for $\sigma, \tau, \lambda, \mu$ respectively into $\mathbb{S}$ and act $\mathbb{S}$ on

L (x, y) where x = 0; y$\in Z_5$ it yields L (1,1) in equation (12). Suppose n is a prime, acting $\mathbb{S}$ (0, 1$\big|$ $-1;\Lambda$)

on the line L (0, 1), we obtain all the lines through the origin. For

Λ = 0,1,…,n-1→ $\aleph(\Lambda)$=$\mathbb{S}$ (0, 1$\big|$ $-1,\Lambda$)L (0,1) = L (1, Λ), (24)

In this work, we fix a rule that ifΛ =-1, $\mathbb{S}$ (0, 1$\big|$ $-1;\Lambda$) is replaced by $\mathbb{S}$ (*1*, 0$\big|$ 0,*1*).

If we substitute the value of Λ = -1,…n, for $n = 3$, we obtain all the lines in G_n we obtain all the points in theline as shown in equations(11) - (14) for a = 0; b $\in Z_n$.

VI. CONCLUSION

In this article, we focused on finite geometry. Lines ofZ_n^2 werethoroughly examined. The result of our findings are as follow:

(i) For n a non-prime, Z_n is a ring of integer modulo n and all lines ofZ_n^2 partitioned into $\prod_{i=1}^{k}(n_i + 1)$ distinct lines and with each partition having $\varphi(n)$ lines isometric to each other.

(ii) Having critically examined each partition, we confirm a one-to-one correspondence within each representation of the lines and other lines in the partition. In addition, For n a prime, an action of the Symplectic matrix on each lines of $Z_n^2$the remaining lines of the prime dimensional finite geometry. Hence they form complete isometric lines in the geometry.

(iii) Even though lines of finite geometry may not have identical label but looking at their internal structure they can have identical points. For n a prime, Z_n is a field of integer modulo n and all lines ofZ_n^2 partitioned into $n + 1$ distinct lines and with each partition having $\varphi(n)$ lines isometric to each other.

REFERENCES

[1]. T. Durt, B.G. Englert, I. Bengtsson, and K. Zyczkowski(2010), Int. J. Quantum Comp. 8, 535.
[2]. K. Gibbons, M.J. Hoffman, and W. Wootters(2004), Phys. Rev. A70, 062101.
[3]. M. Saniga, and M. Planat(2006), J. Phys. A39, 435.
[4]. O. Albouy(2009), J. Phys. A: Math. Theor. 42, 072001.
[5]. M. Kibler(2013), Entropy 15, 1726.
[6]. M. Shalaby, A. Vourdas(2012), J. Phys. A45, 052001.
[7]. M. Shalaby, A. Vourdas(2013), Ann. Phys. 337, 208.
[8]. S.O. Oladejo,C.Lei, and A. Vourdas(2014), J. Phys. A: Math. Theor. 47 485204.
[9]. L.M. Batten(1997), `Combinatorics of finite geometries', Cambridge Univ. Press, Cambridge.
[10]. M. Planat, M. Saniga, M. R. Kibler(2006), SIGMA, 2, 66.
[11]. H. Havlicek, M. Saniga(2007), J. Phys. A40, F943.
[12]. H. Havlicek, M. Saniga(2008), J. Phys. A41, 015302.
[13]. T. Shubin (2006), Lecture Notes on Finite Geometries Dept. of Math, San Jose State University, California, USA.
[14]. S.Ponnusamy (2014), Foundations of Functional Analysis, Narosa Publishing House, New Delhi 110002, India.
[15]. R.D. Bhatt (2009), Intermediate mathematical Analysis, ,Narosa Publishing House, New Delhi 110002, India.
[16]. S.O. Oladejo, A.D. Adeniyi, and A.D. Adeshola(2019) Isometric lines of $\mathfrak{Z}_d \times \mathfrak{Z}_d$, Journ. Nig. Assoc. of Maths. Phys. Vol. 49., No. 1.