Lines of Finite Geometry $Z^2_n$

S.O. Oladejo1, A. W. Yekinni2, and T. A. Mojeed3

1Department of Mathematics, Faculty of Science, Gombe State University, Gombe, Nigeria,
2Department of Computer Science, School of Technology, Lagos State Polytechnic, Lagos, Nigeria
3Department 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 geometry $Z^2_n$, 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 $G_m$ lines with $L(\alpha, \lambda)$ is isomorphic to $L(\mu, \lambda)$ and lines that are isometric to each other have equal slope. For the non-prime dimension $G_n$, $L(\alpha, \lambda) \equiv L(\mu, \lambda)$ if $a \in Z^*_n$ and $L(\alpha, \lambda) + L(\mu, \lambda)$ if $a \in Z_n - Z^*_n$ for $\mu$, and $\lambda$ 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 $Z_n$. To be 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.

In a prime dimensional finite system, the number of mutually unbiased bases is $n + 1$. If $n = p^e$, where $e > 1$ 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 near-linear finite geometry received attention [8-12], in it the unlike the near-linear counterpart, two lines intersect in at least one point. In [13] some dualities which exist between lines non-linear finite geometry and weak mutually unbiased bases infinite quantum systems was shown. In a near-linear geometry $Z^2_n$, 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-linear finite geometry, lines in such finite geometry intersect in more than one points which form 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 $Z^2_n$, 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 isomorphic lines of $Z^2_n$. Symplectic transformation on $Z^2_n$ with numerical example is discussed in section V. The conclusion of our work is in section VI.

Definition: Let $X$ and $Y$ be two sets, a map $\pi: X \rightarrow Y$ 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. It is denoted by $Z_n$.

II. PRELIMINARIES

(i) $G_n = Z^2_n$

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

(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

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

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

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

(v) The greatest common divisor of two elements $\alpha$ and $\beta$ is denoted by $\text{GCD}(\alpha, \beta)$.

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

(vii) The symbol, $+$ denotes partial ordering.

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

www.rsisinternational.org  Page 139
III. FINITE GEOMETRY $G_n$

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

$$G_n = (P_n, L_n).$$

(3)

Where $P_n$ and $L_n$ denote the set of points and lines in $G_n$ respectively

$$P_n = \{(g, h) \mid g, h \in Z_n\}. \quad (4)$$

(ii) A line through the origin is defined as

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

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 form 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) $L(\mu, \lambda) = L(p\mu, p\lambda), \forall p \in Z_n^*$

(6)

and

$$L(p\mu, p\lambda) \neq L(\mu, \lambda), \forall p \in Z_n - Z_n^*.$$  \hspace{1cm} (7)

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

(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 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

$$L(t(\alpha, \beta)) = \{(ta, t\beta) \mid t \in Z_n\}, \text{in } G_m.$$ \hspace{1cm} (8)

at the same time the line $L(\mu \alpha, \mu \beta)$ in $G_m$ is a subline of $L(\alpha, \beta) = \{(at', \beta t') \mid t' \in Z_m\}$

(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

$L(q\alpha, q\beta) \neq L(\alpha, \beta)$ 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 $L(pa, pb)$ for $p \in Z_n^*$.

(10)

**Proof:** Let $\alpha, \beta \in Z_n$ form 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 $L(pa, pb)$ 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 $L(\delta \gamma, \delta \delta)$ is an isometric line to $L(\gamma, \delta)$ if $\gamma$ and $\delta$ are non-zero element of $Z_m$ and $\delta \in Z_m^*$.

**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 $\delta \gamma = \delta \delta$ 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

$$L(0; 1) \equiv L(0; 2)$$

(11)

$$L(1; 0) \equiv L(2; 0)$$

(12)

$$L(1; 1) \equiv L(2; 2)$$

(13)

$$L(1; 2) \equiv L(2; 1)$$

(14)

For $m_2 = 5$, we get.

$$L(0; 1) \equiv L(0; 2) \equiv L(0; 3) \equiv L(0; 4)$$

(15)

$$L(1; 0) \equiv L(2; 0) \equiv L(3; 0) \equiv L(4; 0)$$

(16)

$$L(1; 1) \equiv L(2; 2) \equiv L(3; 3) \equiv L(4; 4)$$

(17)

$$L(1; 2) \equiv L(2; 4) \equiv L(3; 1) \equiv L(4; 3)$$

(18)

$$L(1; 3) \equiv L(2; 1) \equiv L(3; 4) \equiv L(4; 2)$$

(19)

$$L(1; 4) \equiv L(2; 3) \equiv L(3; 2) \equiv L(4; 1)$$

(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 \( L(\alpha, \beta) \cong L(\alpha \beta, \beta \alpha) \) 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

\[
\frac{\Delta \beta}{\Delta \alpha} = \frac{2 - 1}{1 - 2} = 2 \equiv 2 \quad \text{(mod 5)}
\]

\[
\frac{1 - 3}{2 - 3} \equiv 4 (\text{mod 5}) \equiv 4 - 1
\]

\[
\frac{1 - 4}{2} \equiv \frac{2}{2} \cdot \frac{2}{4} \equiv \frac{4}{4} \equiv 4 - 2
\]

\[
\equiv 4 - 1 \equiv 3 - 2 \equiv 3 - 1 \equiv 2 - 1 \equiv (\text{mod 5})
\]

For \( n = 15 \) we obtain the following

\[
L(0,1) \equiv L(0,2) \equiv L(0,4) \equiv L(0,7) \equiv L(0,8) \equiv L(0,11) \equiv L(0,13) \equiv L(0,14)
\]

\[
L(0,0) \equiv L(0,0) \equiv L(0,0) \equiv L(0,0) \equiv L(0,0) \equiv L(0,0) \equiv L(0,0) \equiv L(0,0)
\]

\[
L(1,1) \equiv L(2,2) \equiv L(4,4) \equiv L(7,7) \equiv L(8,8) \equiv L(11,11) \equiv L(13,13) \equiv L(14,14)
\]

\[
L(1,2) \equiv L(4,8) \equiv L(7,14) \equiv L(8,14) \equiv L(11,17) \equiv L(13,11) \equiv L(14,13)
\]

\[
L(3,1) \equiv L(2,6) \equiv L(4,12) \equiv L(7,6) \equiv L(8,9) \equiv L(11,3) \equiv L(13,9) \equiv L(14,12)
\]

\[
L(1,4) \equiv L(2,8) \equiv L(4,1) \equiv L(7,13) \equiv L(8,2) \equiv L(11,14) \equiv L(13,7) \equiv L(14,11)
\]

\[
L(5,1) \equiv L(2,10) \equiv L(4,5) \equiv L(7,5) \equiv L(8,10) \equiv L(11,10) \equiv L(13,5) \equiv L(14,10)
\]

\[
L(1,6) \equiv L(2,12) \equiv L(4,9) \equiv L(7,12) \equiv L(8,3) \equiv L(11,6) \equiv L(13,3) \equiv L(14,9)
\]

\[
L(1,7) \equiv L(2,14) \equiv L(4,13) \equiv L(7,4) \equiv L(8,11) \equiv L(11,2) \equiv L(13,1) \equiv L(14,8)
\]

\[
L(1,8) \equiv L(2,1) \equiv L(4,2) \equiv L(7,11) \equiv L(8,4) \equiv L(11,13) \equiv L(13,14) \equiv L(14,7)
\]

\[
L(1,9) \equiv L(2,3) \equiv L(4,6) \equiv L(7,3) \equiv L(8,12) \equiv L(11,9) \equiv L(13,12) \equiv L(14,6)
\]

\[
L(1,10) \equiv L(2,5) \equiv L(4,10) \equiv L(7,10) \equiv L(8,5) \equiv L(11,5) \equiv L(13,10) \equiv L(14,5)
\]

\[
L(1,11) \equiv L(2,7) \equiv L(4,14) \equiv L(7,2) \equiv L(8,13) \equiv L(11,1) \equiv L(13,8) \equiv L(14,4)
\]

\[
L(1,12) \equiv L(2,9) \equiv L(4,3) \equiv L(7,9) \equiv L(8,6) \equiv L(11,12) \equiv L(13,6) \equiv L(14,3)
\]

\[
L(1,13) \equiv L(2,11) \equiv L(4,7) \equiv L(7,1) \equiv L(8,14) \equiv L(11,8) \equiv L(13,4) \equiv L(14,2)
\]

\[
L(1,14) \equiv L(2,13) \equiv L(4,11) \equiv L(7,8) \equiv L(8,7) \equiv L(11,4) \equiv L(13,2) \equiv L(14,1)
\]

\[
L(3,1) \equiv L(6,2) \equiv L(12,4) \equiv L(9,8) \equiv L(6,7) \equiv L(3,11) \equiv L(9,13) \equiv L(12,14)
\]

\[
L(3,2) \equiv L(6,4) \equiv L(12,8) \equiv L(9,11) \equiv L(6,14) \equiv L(3,7) \equiv L(9,11) \equiv L(12,13)
\]

\[
L(3,4) \equiv L(6,8) \equiv L(12,1) \equiv L(9,2) \equiv L(6,13) \equiv L(3,14) \equiv L(9,7) \equiv L(12,11)
\]

\[
L(3,5) \equiv L(6,10) \equiv L(12,5) \equiv L(9,10) \equiv L(6,5) \equiv L(3,10) \equiv L(9,5) \equiv L(12,10)
\]

\[
L(3,8) \equiv L(6,1) \equiv L(12,2) \equiv L(9,4) \equiv L(6,11) \equiv L(3,13) \equiv L(9,14) \equiv L(12,7)
\]

\[
L(5,1) \equiv L(10,2) \equiv L(5,4) \equiv L(5,7) \equiv L(10,8) \equiv L(10,11) \equiv L(5,13) \equiv L(10,14)
\]

\[
L(5,2) \equiv L(10,4) \equiv L(5,8) \equiv L(5,14) \equiv L(10,1) \equiv L(10,7) \equiv L(5,11) \equiv L(10,13)
\]

\[
L(5,3) \equiv L(10,6) \equiv L(5,12) \equiv L(5,6) \equiv L(10,9) \equiv L(10,3) \equiv L(5,9) \equiv L(10,12)
\]

Where

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

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

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

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

represents a unitary transformation where

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

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

Acting \( S \) on all points of line \( L (x, y) \) in \( Z_n^2 \) generates all the points of the line \( L (\sigma x + \tau y, \lambda x + \mu y) \).

This is expressed in this work as \( S (\sigma, \tau \mid \lambda, \mu) L (x, y) \).
Example: Suppose \( n = 5 \) and we substitute 2,1,1, and 1 for \( \sigma, \tau, \lambda, \mu \) respectively into \( S \) and act \( S \) on
\[
L(x, y) \text{ where } x = 0; \quad y \in Z_5 \text{ it yields } L(1,1) \text{ in equation (12).}
\]
Suppose \( n \) is a prime, acting \( S(0, 1) \rightarrow -1:A \)
on the line \( L(0, 1) \), we obtain all the lines through the origin. For
\[
A = 0,1,\ldots,n-1 \rightarrow \mathbf{N}(A)=S(0, 1 \mid -1:A) L(0,1) = L(1, A),
\]
(iii)
In this work, we fix a rule that if \( A =-1 \), \( S(0, 1 \mid -1:A) \) is replaced by \( S(l, 0 \mid 0, l) \).

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

VI. CONCLUSION
In this article, we focused on finite geometry. Lines of \( Z_n^2 \) 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 of \( Z_n^2 \) partitioned into \( \prod_{i=1}^{n}(n_i + 1) \) 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.

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 of \( Z_n^2 \) partitioned into \( n + 1 \) distinct lines and with each partition having \( \varphi(n) \) lines isometric to each other.

REFERENCES
[13]. T. Shubin (2006), Lecture Notes on Finite Geometries Dept. of Math, San Jose State University, California, USA.