# Factorization in Finite Geometry

S.O. Oladejo[1], A.D.Adeshola[2] and A. W. Yekinni[3]

[1]*Department of Mathematics, Faculty of Science, Gombe State University, Gombe, Nigeria,*
[2]*Department of Statistics and Mathematical Sciences, College of Pure and Applied Science, Kwara State University, Malete P.M.B. 1530, Ilorin, Nigeria,*
[3]*Department of Computer Science, School of Technology, Lagos State Polytechnic, Lagos, Nigeria*

***Abstract:*** **This work centres on non-near-linear finite geometry. In it, lines in $Z(b) \times Z(b)$ for factorized as lines of $\prod_{j=1}^{k} Z(p_j) \times Z(pj)$, where $pj$'s are primes and $p1,p2,...,pk$ are relatively prime. Using the method of Good[18] which was built on Chinese remainders theorem, an isomorphism was established between$G(b)$ for $b$ a non-prime and $\prod_{j=1}^{k} G(p_j)$ where $p_j$ is a prime.**

***Keywords:*** **Non-near-linear Finite Geometry, Partial Ordering, Factorization.**

## I. INTRODUCTION

Finite geometry had received a lot of attentions from researchers of different discipline in recent past. The reason could be connected to its relevant in emerging technology like the quantum information and teleportation [1-10]. Over the years,most of the work done on finite geometry centres on near-linear geometry. In more recent times non-near-linear finite geometry started receiving audience from researcher [11-12] this could be linked to itsduality with the weak mutually unbiased bases in finite quantum systems with variables in $Z(b)$A method of decomposing a large dimensional finite geometry called non-near-linear finite geometry intoproducts of many prime dimensional finite geometry called the near-linear geometry is showcased in thisarticle. The same approach was adopted from the method of Good [18] in Fast Fourier transform. Thismethod came into existence due to difficult in solving problem which consists of a very large integer. In[18] large size integer was factorized as products of many small sizes integer. The same was adopted in[1] to factorize a large dimensional finite quantum systems with variables in $Z(b)$ as products of many smalldimensional finite quantum systems. We divide the whole work into the following parts; various notationsused throughout the work is defined in the preliminaries of this working section II. Section III covers finitegeometry $G(b)$. We discuss factorization of lines in finite geometry in section IV. Symplectic on $G(b)$ withnumerical examples was in section V. Finally section VI we conclude our work.

## II. PRELIMINARIES

This section focuses on concepts and terminology used in this work to aid an understanding of readers.

(a) $Z(b)$represents the ring of integer modulo $b$.

(b) $|Z^*(b)|$ represents the invertible integer modulo b. $|Z(b)|$ is $\varphi(b)$. Where

$$\varphi(b) = b\prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right);\ p_j = \text{prime} \tag{1}$$

(c) The Dedekind psi function $\psi(b)$ is defined in this work as

$$\psi(b) = b\prod\left(1+\frac{1}{p_j}\right), p_j = \text{prime} \tag{2}$$

(d) The set of divisor is denoted in this work by $\{D(b)\}$. Its cardinality is a divisor function $\sigma_0(b)$.

Here $d \mid b$ means $d$divides $b$: If $d \mid b$ it means there exists a number say $q$ an integer such that $\frac{b}{d} = q$

that is $b = dq$. We showed the existence of a bijection between the product of the distinct set

$\{b\}$of prime divisors $d$ and $b$. The elements of $Z(d)$ are embedded in $Z(b)$ for $d \mid b$ thus

$$Z(d) \ni \xi \to Z(b) \ni \tfrac{b\xi}{d}. \tag{3}$$

(e) GCD$(\delta,\gamma)$ represents the greatest common divisor of two elements $\delta$ and $\gamma$ is represented in this

work as.

(f) Integer $b$ is expressed as products of its distinct primes

$$b = p_1 \times p_2 \times ... \times p_k \tag{4}$$

$Z(b)$is a cyclic module.

## III. LINES IN FINITE GEOMETRY $G(b)$

A finite geometry $G(b) = Z(b) \times Z(b)$ is defined as the combination

$$G(b) = (P(b), L(b)) \tag{5}$$

$P(b)$ represent points on a line and $L(b)$ represent lines in $G(b)$ where

$$P(b)=\{(k,g)\,|\,k,g\,\epsilon Z(b)\} \quad (6)$$

Definition III.1. A line $L(x,y)$ of $G(b)$ de_ned as

$$L(x;\ y)=\{(\alpha x,\alpha y)\,|\,x,y\,\epsilon \boldsymbol{Z}(\boldsymbol{b})\},\lambda\epsilon \boldsymbol{Z}(\boldsymbol{b}) \quad (7)$$

The representation

$\prod_{j=1}^{k} G(p_j)$ and $\prod_{j=1}^{k} Z(p_j)\times Z(p_j)$ have similar interpretation, so at times we interchange them. We discuss extensively finite geometry. As a result our point of focus is on both near-linear and non-near-linear geometry. Here, two lines intersect in at least one point. $Z(b)$is a ring of integer modulo . $b$.

If $d\,|\,b$, $Z(b)\times Z(b)$ and $G(d)$ is a subgeometry of $G(b)$. We represent this relation in this work by

$G(k)\prec G(b)$. Propositions of some related works in [10-11] were stated below without proof:

**Proposition III.2**.

(i) In $G(b)$ there exists $\psi(b)$ maximal lines with exactly $b$ points.

(ii) For $\alpha\in Z^{*}(b)$

$$L(\alpha x,\alpha y)=L(x,y), \quad (8)$$

also, if

$$\text{For } Z^{*}(b)'\ni\alpha\text{then } L(\alpha x,\alpha y)mod\prec L(x,y) \quad (9)$$

(iii) if $\text{GCD}(x,y)\in Z(b), L(x,y)$ is a maximal line in $G(b)$ and if $\text{GCD}(x,y)\in Z(b)-Z^{*}(b)$,

$L(x,y)$is a subline in $G(b)$.

(iv) Afinite geometry $G(b)$ in equation (7). The line

$$L(x,y)=L(tx,ty)=\{(t\alpha x,t\alpha y)\,|\,t\in Z(b)\}\text{in}G(tb) \quad (10)$$

A line $L(tx,ty)$ in $G(tb)$ is a subline of

$$L(x,y)=\{t'x,t'y)\,|\,t'=0,1,\dots\alpha b-1\} \quad (11)$$

(v) For $d\,|\,b$ two maximal lines have k points in common. The k points gives a subline $L(x,y)$ where

$$x,y\in\frac{b}{k}Z(q) \quad (12)$$

## IV. FACTORIZATION OF LINES IN FINITE GEOMETRY

In this section lines in $Z(b)\times Z(b)$ decomposed as products of lines in$\prod_{j=1}^{k} Z(p_j)\times Z(p_j)$this was achieved by creating a bijection between lines in $G(b)$ and its factor lines in $G(p)$. We adopted this concept from Good [18]. This same concept was used previously [1, 10-11] to factorize a big finite b dimensional finite quantum systems as products of its components in small dimensional finite systems.

Here we used the same to create two the ordinates of each of the points on the lines G(b) in non-near-linear geometries as products of many ordinates in the lines G(p) in -near-linear geometries. This wascarried out by creating two bijection for each of the two $xs'$and $ys'$ ordinates for each lines thus:

$$x\leftrightarrow(x_1,\dots,x_k),x_j=x\ mod\ p_j;x=\sum x_j s_j \quad (13)$$

$$x\leftrightarrow(\bar{x}_1,\dots,\bar{x}_k),\bar{x}_j=xt_j=x_j t_j\,(mod\ p_j);x=\sum\bar{x}_j r_j\ (mod\ b) \quad (14)$$

Where

$$r_j=\frac{b}{p_j},t_j r_j=1\,(mod\ p_j),s_j=\ t_j r_j\in Z(b) \quad (15)$$

$x$and $y$ ordinates in the non-near-linear geometry we factorised in line with equations (13) and (14).

Hence an existence of $one-to-one$ correspondence was confirmed between

$$L(x,y)\text{in}G(b) \quad (16)$$

and lines

$$L_{p_1}(x_1,y_1)\times\dots\times L_{p_k}(x_k,y_k)\in\prod_{j=1}^{k} Z(p_j)\times Z(p_j) \quad (17)$$

Where

$(x,y)\leftrightarrow(x_1,y_1)\times\dots\times(x_k,y_k)$and $p_j$ a prime

In the previous work of $[10-11]$ we confirm the following:

(i) $b\psi(b)$ maximal lines in total.

(ii) $\psi(b)$ distinct maximal lines.

Furthermore in this work,

(iii) We found an existence of $\psi\left(\frac{b}{p_j}\right)$ sublines each with $p$ points.

Analogously, we observe the following

(i) $L_{p_j}(a,\bar{b})$ are prime factor lines of $\prod_{j=1}^{k} Z(p_j)\times Z(p_j)$, where $p_j$ is a prime number.

(ii) Lines in $Z(b)\times Z(b)=\prod_{j=1}^{k} Z(p_j)\times Z(p_j)$is related to expressing a non-prime integer as productsof its prime.

(iii) The sublin$eG(q)$ is related to the divisor $q$ of an integer.

As an illustration, we express all maximal lines in $G(b) = Z(b) \times Z(b)$ for $b = 14$ in terms of its primesdiscussed in equations (13) and (14) above by decomposing line $L_{14}(2,5)$.

Using equation (13) the ordinate 2 in $L_{14}(2,5)$ is decomposed as;

$$2 \leftrightarrow (0;\ 2) \tag{18}$$

also using equation (14) the ordinate 5 in $L14(2,5)$ is decomposed as;

$$5 \leftrightarrow (1,6) \tag{19}$$

Therefore $L_{14}(2,5)$ is decomposed as;

$$L_2(0,1) \times L_7(2,6) \tag{20}$$

*A. Symplectic Transformation on $G(p)$*

The matrix $\mathcal{M}(p,q \mid y,x)$ defined as

$$\mathcal{M}(p,q|y,x) = \begin{pmatrix} p & q \\ y & x \end{pmatrix} \text{where} p,q,y,x \in Z(b)$$

$$\text{and } |\mathcal{M}| = 1\ (mod\ p) \tag{21}$$

form a Symplectic group.

$$\mathcal{M}(p,q|y,x)(\beta_i,\gamma_i)^T = L(p\beta_i + q\gamma_i, y\beta_i + x\gamma_i);\ i = 1;\ 2,\dots,p \tag{22}$$

As an illustration, acting a matrix $\mathcal{M}(0,1|-1,x)$, on a line $L(1,x)$ this produces $\psi(b)$ set of lines

through the origin.

*B. .Symplectic Transformation on$G(d)$ As $\prod_{j=1}^{k} G(p_j)$*

We showcase how prime dimensional finite geometry are embedded in non-prime dimensional finitegeometry via divisor function. Using the symplectic matrix defined in equation (21), we factorized lines

infinite geometry $G(b)$ as product of its prime finite geometry with respect to equations(13) and (14).

Thus, $Sp(2;Z(b))$ is factorized as $Sp(2,Z(p1)) \times \dots \times Sp(2,Z(p_k))$;

where$\mathcal{M}(p,q|y,x)$ is defined in equation (23) above

In general, using equations (13) and (14); $Sp(2,Z(b))$ is factorized as $Sp(2,Z(p1)) \times \dots \times Sp(2,Z(p_k))$.

That is

$$\mathcal{M}(p,q|y,x) = \otimes\mathcal{M}(p_j, r_j q_j | \bar{y}_j, x_j) \tag{23}$$

where$p_j, q_j, x_j$ are related $x$ in equation (13) and $\bar{y}_j$ is related to $y$ in equation(14).

## V. ISOMETRIC LINES OF$Z(b) \times Z(b)$

Suppose we recall a line through the origin (that is point (0,0)) defined earlier in equation (7). For $f \in Z^*(b)$, then$L(x,y) \cong L(fx;\ fy)$.

We obtain $b\psi(b)$ lines in altogether in the finite geometry $\boldsymbol{Z(b) \times Z(b)}$out of $b\psi(b)$ lines, only $\psi(b)$ are distinct. Others are isomorphic to one or another in the partition.

Consider the set of points in the line

$$L(x,y) = \{(gx_1, gy_1) \times \dots \times (gx_k, gy_k)\}\ g \in Z^*(b) \tag{24}$$

and

$$L(hx,hy) = \{(hgx_1, hgy_1) \times \dots \times (hgx_k, hgy_k)\}\ h \in Z^*(b) \tag{25}$$

We confirmed that there exist a $one - to - one$ correspondence between the points of $L(x,y)$ and

$L(hx;hy)$.

Hence $L(x,y)$ is isomorphic to $L(h\sigma;h\rho)$,If GCD$(\sigma,\rho) = 1$.

From equation (8), we confirmed that if

$$L(x,y) = L(mx,my), m \in Z^*(b)\ ), \tag{26}$$

$$L(x,y) \cong L(mx,my), \tag{27}$$

Hence $L(x,y)$ and $L(mx,my)$ are isometric to each other.

**Proposition V.1.** If $L(x,y)$ is a line of near-linear finite geometry $G(b)$ where $b$ is a prime integer.

then$L(\sigma,\rho)$ is isometric to $L(h\sigma,h\rho)\ \forall\ h \in Z(b), \forall\ h \in Z(b)$ (28)

**Proof**. Suppose $b$ is a prime integer and $\rho,\sigma \in Z(b)$ then $Z(b)$ is a field of integer modulo $b$, in this case,every non-zero members of this set is invertible, and their additive generator is $h$.

Hence complete the proof.

Furthermore, we confirmed that finding the slope any two lines which are isomorphic to each other yieldsan identical result. However for $b$ a non-prime integer,

$$L(mx,my) \subset L(x,y), m \in Z(b) - Z^*(b)\ ), \tag{29}$$

then$L(x,y) \prec L(mx,my)$ (30)

As a result in this case $L(X,y)$ and $L(mx,my)$ are conditionally isometric to each other in the sense thattaking any two arbitrary points in any lines of $G(b)$ where $b$ is non-prime does not guarantee the sameresult. Examples are shown below for lines in near-linear geometry $G(b)$, for $b = 7$.

*A. Equigradient Lines*

Suppose a line is expressed as defined in equation (7), then

$$L(x,y) = L(hx,hy), h \in Z^*(b)\ ), \tag{31}$$

Hence $L(x,y) \cong L(hx,hy)$.Finding the slope by taking any two arbitrary points of a line yields an identical result with anotherline of the same partitions. Here in this work it is named an equigradient lines. The reason being thatalthough lines may have different naming externally, however by examine their internal structure, these lines are equivalent due toa $one-to-one$ correspondence between points of the two lines being examined. Furthermore it wasfound that equigradient lines come to existence if and only $b$ is a prime.

**Examples**

(1) Lines in geometry $G(7) = Z(7) \times Z(7)$is obtained as follows:

$$L(0,1) \cong L(0,2) \cong L(0,3) \cong L(0,4) \cong L(0,5) \cong L(0,6) \tag{32}$$

$$L(1,0) \cong L(2,0) \cong L(3,0) \cong L(4,0) \cong L(5,0) \cong L(6,0) \tag{33}$$

$$L(1,1) \cong L(2,2) \cong L(3,3) \cong L(4,4) \cong L(5,5) \cong L(6,6) \tag{34}$$

$$L(1,2) \cong L(2,4) \cong L(3,6) \cong L(4,1) \cong L(5,3) \cong L(6,5) \tag{35}$$

$$L(1,3) \cong L(2,6) \cong L(3,2) \cong L(4,5) \cong L(5,1) \cong L(6,4) \tag{36}$$

$$L(1,4) \cong L(2,1) \cong L(3,5) \cong L(4,2) \cong L(5,6) \cong L(6,3) \tag{37}$$

$$L(1,5) \cong L(2,3) \cong L(3,1) \cong L(4,6) \cong L(5,4) \cong L(6,2) \tag{38}$$

$$L(1,6) \cong L(2,5) \cong L(3,4) \cong L(4,3) \cong L(5,2) \cong L(6,1) \tag{39}$$

where

$$L(2,5) = \{(0,0),(2,5),(4,3),(6,1),(1,6),(3,4),(5,2)\} \tag{40}$$

(2) $L_b \leftrightarrow L_{p_1}(x_1,y_1) \times L_{p_2}(x_2,y_2) b = 14, p1 = 2, p2 = 7, r1 = 7, r2 = 2, t1 = 1, t2 = 4.$

If we substitute the variables in equation (41) into equation (17) we obtain the$\psi(14)$=24 maximal lines as shown in tables (1) and (ii) below:

Table (i)

| $L_{14}$ | $L_2$ | $L_7$ |
|---|---|---|
| $L14(0;\ 1)$ | $L2(0;\ 1)$ | $L7(0;\ 1)$ |
| $L14(1;\ 0)$ | $L2(1;\ 0)$ | $L7(1;\ 0)$ |
| $L14(1;\ 1)$ | $L2(1;\ 1)$ | $L7(1;\ 4)$ |
| $L14(1;\ 2)$ | $L2(1;\ 0)$ | $L7(1;\ 1)$ |
| $L14(1;\ 3)$ | $L2(1;\ 1)$ | $L7(1;\ 5)$ |
| $L14(1;\ 4)$ | $L2(1;\ 0)$ | $L7(1;\ 2)$ |
| $L14(1;\ 5)$ | $L2(1;\ 1)$ | $L7(1;\ 6)$ |
| $L14(1;\ 6)$ | $L2(1;\ 0)$ | $L7(1;\ 3)$ |
| $L14(1;\ 7)$ | $L2(1;\ 1)$ | $L7(1;\ 0)$ |
| $L14(1;8)$ | $L2(1;\ 0)$ | $L7(1;\ 4)$ |
| $L14(1;9)$ | $L2(1;\ 1)$ | $L7(1;1)$ |
| $L14(1;10)$ | $L2(1;\ 0)$ | $L7(1;\ 5)$ |

Table (ii)

| $L_{14}$ | $L_2$ | $L_7$ |
|---|---|---|
| $L14(1,11)$ | $L2(1;\ 1)$ | $L7(1;\ 2)$ |
| $L14(1,12)$ | $L2(1;\ 0)$ | $L7(1;\ 6)$ |
| $L14(1,13)$ | $L2(1;\ 1)$ | $L7(13)$ |
| $L14(2,1)$ | $L2(0,1)$ | $L7(2,4)$ |
| $L14(2,3)$ | $L2(0,1)$ | $L7(2;\ 5)$ |
| $L14(2;\ 5)$ | $L2(0;\ 1)$ | $L7(2;\ 6)$ |
| $L14(2;\ 7)$ | $L2(0;\ 1)$ | $L7(2;\ 0)$ |
| $L14(2;\ 9)$ | $L2(0;\ 1)$ | $L7(2;\ 1)$ |
| $L14(2;\ 11)$ | $L2(0;\ 1)$ | $L7(2;\ 2)$ |
| $L14(2;\ 13)$ | $L2(0;\ 1)$ | $L7(2;\ 3)$ |
| $L14(7;\ 1)$ | $L2(1;\ 1)$ | $L7(0;\ 4)$ |
| $L14(7;\ 2)$ | $L2(1;\ 0)$ | $L7(0;\ 1)$ |

## VI. CONCLUSION

Non-near-linear finite geometry was studied. Lines of the geometry were factorized as lines in near-linear geometry. Symplectic operator was used to generate all points of line $L(x_i,y_i)$ and at the end, abijection was created between lines in $G(b)$ and products of line in near-linear geometry $\prod_{j=1}^{k} G(p_j)$.

## REFERENCES


[1]. A. Vourdas, Rep. Prog. Phys. 67, 1 (2004)
[2]. A. Vourdas, J. Phys. A: Math. Gen. 36, 5646 (2003)
[3]. N. Cotfasand , J.P. Gazeau, J.Phys. A43, 193001(2010)
[4]. T. Durt, B.G. Englert, I. Bengtsson, and K. Zyczkowski, Int. J. Quantum Comp. 8, 535 (2010)
[5]. Tolar, and G. Chadzitaskos, J. Phys. A42, 245306 (2009)
[6]. K. Gibbons, M.J. Hoffman, and W. Wootters, Phys. Rev. A70, 062101 (2004)
[7]. A. Klappenecker, and M. Rotteler, Lect. Notes Comp. Science 2948, 137 (2004)
[8]. M. Saniga, and M. Planat, J. Phys. A39, 435 (2006)
[9]. P. Sulc. and J. Tolar, J. Phys A. Math. Theor. 15099 (2007)
[10]. O. Albouy, J. Phys. A: Math. Theor. 42, 072001 (2009)
[11]. M. Shalaby, A. Vourdas, Ann. Phys. 337, 208 (2013)
[12]. S.O. Oladejo,C.Lei, and A. Vourdas, J. Phys. A: Math. Theor. 47 485204 (2014)

[13]. L.M. Batten, `Combinatorics of finite geometries', Cambridge Univ. Press, Cambridge, 1997
[14]. J.W.P. Hirchfeld, `Projective geometries over finite fields' (Oxford Univ. Press, Oxford, 1979)
[15]. M. Planat, M. Saniga, M. R. Kibler, SIGMA, 2, 66 (2006)
[16]. H. Havlicek, M. Saniga, J. Phys. A41, 015302 (2008)
[17]. M. Korbelar, J. Tolar, J. Phys. A43, 375302 (2010)
[18]. I.J. Good, IEEE Trans. Computers, C-20, 310 (1971)
[19]. A. Vourdas, C. Banderier, J. Phys. A43, 042002 (2010)
[20]. A. Rogers, 'Very brief summary lecture notes for introductory quantum theory' (Department of Mathematics
[21]. King's College Strand London, 2010).
[22]. T. Shubin (2006), Lecture Notes on Finite Geometries Dept. of Math, San Jose State University, California, USA.