Erdős Type Configuration Problems in Modules over Finite Rings

by

Esen Aksoy Yazici

Submitted in Partial Fulfillment

of the

Requirements for the Degree

Doctor of Philosophy

Supervised by

Professor Alex Iosevich
Professor Jonathan Pakianathan

Department of Mathematics
Arts, Sciences and Engineering
School of Arts and Sciences

University of Rochester
Rochester, New York

2014

Biographical Sketch

Esen Aksoy Yazici was born on March 14, 1981, in Elazig, Turkey. She started her studies of mathematics in 1999 at Ankara University and received a B.S. In September 2004, she joined the Mathematics Program at Sabanci University and graduated with a master's degree in 2007. She started her Ph.D. studies at Sabanci University and took some doctorate level courses in 2007-2010. She was then accepted to the University of Rochester in August 2011. She resumed her Ph.D. studies in the areas of geometric combinatorics and number theory under the guidance of her advisor, Alex Iosevich, and co-advisor, Jonathan Pakianathan, at the University of Rochester.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my advisor, Alex Iosevich, for his excellent guidance during my graduate studies. His expertise and broad vision in mathematics has constantly inspired me and eventually led me to my current research. I thank him for sharing his knowledge and supporting me throughout this stage.

I am also exceptionally grateful to my co-advisor, Jonathan Pakianathan, for his helpful suggestions and comments during this work. His excellent supervision contributed greatly to this dissertation and my mathematical insight.

I am sincerely thankful to the faculty, staff and graduate students in the Department of Mathematics at the University of Rochester for their friendship and assistance.

I, also, would like to thank Alev Topuzoğlu for her invaluable mentorship and encouragement. I appreciate my collaboration with Ayça Çesmelioğlu, Wilfried Meidl, and Alev Topuzoğlu from Sabanci University.

Finally, I especially thank my husband for his understanding and helping me get through some difficult times. I am grateful to my family for their love and endless support.

Abstract

Throughout this thesis we study two types of discrete problems over finite fields and rings.

In the first part, we study Erdős type geometric problems for vector spaces over finite fields and modules over residue rings.

The second part starts with some basic facts about permutation polynomials (PPs) over finite fields. We then introduce the Carlitz rank of a permutation polynomial and study related results.

Contributors and Funding Sources

This work was supervised by a dissertation committee consisting of Alex Iosevich (advisor), Jonathan Pakianathan (co-advisor) of the Department of Mathematics, and Alice Quillen of the Department of Physics and Astronomy.

This work is partially funded by TÜBİTAK 2211 - National Ph.D. Fellowship Programme.

Table of Contents

1 Introduction

In this work we consider geometric and arithmetical configurations in discrete settings arising in additive combinatorics, discrete geometry, and number theory. In particular, we study various Erdős type geometric problems over finite fields and residue rings $\mathbb{Z}_q$, where $q = p^l$ is an odd prime power. We also work on some enumerative problems on permutation polynomials over finite fields.

The main focus of Erdős type problems is to determine the size of a discrete set so that the configuration of a given type is obtained. In this setting, it is well known that there is a rich analogy between discrete and continuous problems. More specifically, the techniques used for the geometry in the Euclidean plane are applicable to those in vector spaces over finite fields and conversely, the results coming from finite field geometry shed some light on the Erdős type problems in Euclidean settings.

Recently, Erdős type geometric problems are of great interest and several problems have been studied by various authors in the context of finite fields, see for example [4], [3], [7], [8],[13], [14], [16] and the references therein. The results in them are mostly achieved via Fourier analytic methods for large enough sets and some other combinatorial and probabilistic approaches for relatively small ones.

Our main focus here is to extend the results for Erdős type geometric prob-

lems to the setting of finite cyclic rings $\mathbb{Z}_{p^l} = \mathbb{Z}/p^l\mathbb{Z}$ where p is a fixed odd prime. Among the Erdős type geometric problems, we study Erdős-Falconer distance problem, congruence classes of k-simplices up to orthogonal transformations, distribution of r-hinges, dot product problem, and distribution of areas of triangles determined by a given discrete set. It is worth to note here that the new problems in the study of these questions in these rings are due to the non unit elements that must be taken into arithmetical consideration separately.

In Chapter 2 of this thesis, we present Fourier analytic tools defined on the finite cyclic groups $\mathbb{Z}_q$ that are used throughout this work. For a further exploration we refer the reader to [18].

In Chapter 3 and 4, we first present various Erdős-Falconer type configuration questions in the context of finite fields $\mathbb{F}_q$ together with a statement of the best known results. We then introduce our results for finite cyclic groups $\mathbb{Z}_q$, where $q = p^l$.

Chapter 3 starts with a complete description of the distance problem. Letting $G = \mathbb{F}_q$ or $\mathbb{Z}_q$, the distance map λ on G^d is given by the map,

$$\begin{aligned} \lambda : G^d \times G^d &\longrightarrow G \\ (x, y) &\longmapsto \|x - y\| = (x_1 - y_1)^2 + \ldots + (x_d - y_d)^2. \end{aligned}$$

This map does not induce a metric on G^d. However, it is invariant under orthogonal transformations of G^d.

For subsets $E \subset G^d$, we shall consider the restriction map

$$\lambda|_{E\times E} : E \times E \to G$$

and ask for a threshold on the size of E to guarantee that the image of the map $\lambda|_{E\times E}$, $\Delta(E) = \{||x - y|| : (x, y) \in E \times E\}$, is about the size $|G| = q$. In other words, almost all distances are achieved.

An extension of this notion is the congruence classes of triangles, more generally, distribution of k-simplices with the vertices from the points of E. In Section 3.2, we introduce these problems on the base field $G = \mathbb{F}_q$, with a brief summary on the progress in this context. In Section 3.3, we focus on analogous problems for $G = \mathbb{Z}_q$. An asymptotically sharp bound for the distance set $\Delta(E)$ for $E \subset \mathbb{Z}_q^d$ is given in [9] and we first note that result. Then in Theorem 3.3.2 we prove a sufficient lower bound on $|E|$ to get a positive proportion of all triangle classes up to orthogonal transformations. In the rest of this section we study the Hinges problem. For a subset $E \subset \mathbb{Z}_q^d$, and a distance set $\alpha = \{\alpha_i\}_{i=1}^{r-1} \in (\mathbb{Z}_q^*)^{r-1}$, we define the r-hinges determined by the points of E as

$$H_{r,\alpha} = \{(x, x^1, \ldots, x^{r-1}) \in E \times \ldots \times E : \|x - x^i\| = \alpha_i\},$$

where $r > 2$ is an integer. In Theorem 3.3.3 we determine a sufficient condition on the size of E so that the distribution of r-hinges among the points of E is uniform. This result is similar to the result obtained in [8, Theorem 3.1] in the context of finite fields.

Chapter 4 focuses on the problems of dot product and volume set determined by subsets E of G^d where $G = \mathbb{F}_q$ or $\mathbb{Z}_q$. Given a subset E of G^d, the dot product is defined as

$$\prod(E) = \{x.y : \ x, y \in E\},$$

where dot product of two vectors is defined by the usual formula

$$x.y = x_1y_1 + \ldots + x_dy_d,$$

for $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$.

We define the d- dimensional non-zero volumes of $(d+1)$-simplices whose vertices are in E by

$$V_d(E) = \{det(x^1 - x^{d+1}, \ldots, x^d - x^{d+1}) : \ x^j \in E\} \setminus \{0\}.$$

Section 4.2 is dedicated to recapping known results for dot products and volume sets in $\mathbb{F}_q^d$. We then move to the residue ring $G = \mathbb{Z}_q$ in Section 4.3. First, in Theorem 4.3.2 for the sets of the form $E = \underbrace{A \times ... \times A}_{\text{d-fold}}$ with $A \subset \mathbb{Z}_q$, we find a condition on the size of E, so that dot product set of E, $\prod(E)$, contains a positive proportion of the elements of $\mathbb{Z}_q$. This result can be seen as a variant of the dot product result for an arbitrary subset E of $\mathbb{Z}_q^d$ given in [9]. Later in this section, we prove a triangle area result in Theorem 4.3.3 for subsets of $\mathbb{Z}_q^2$.

In Chapter 5, permutation polynomials (PPs) over finite fields $\mathbb{F}_q$ are studied. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a PP of $\mathbb{F}_q$ if the induced map

$$\begin{aligned} \mathbb{F}_q &\longrightarrow \mathbb{F}_q \\ \alpha &\longmapsto f(\alpha) \end{aligned}$$

is bijective. These polynomials play an important role in the study of secure transmission of data and combinatorial designs. In this chapter we first study the cycle structure of a PPs. Then in Section 5.1 we turn our attention to the problem of enumerating permutation polynomials of a given Carlitz rank. From a well known result of L. Carlitz (see [6]), it immediately follows that any permutation polynomial $f(x)$ of $\mathbb{F}_q$ can be represented by a polynomial

$$\mathcal{P}_n(x) = (\dots((a_0x + a_1)^{q-2} + a_2)^{q-2} \dots + a_n)^{q-2} + a_{n+1},\ n \geq 0, \tag{1.1}$$

where $a_1, a_{n+1} \in \mathbb{F}_q$, $a_i \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ for $i = 0, 2, \dots, n$.

This representation is not necessarily unique and we define the Carlitz rank of a permutation polynomial $f(x)$ to be to smallest n, i.e, smallest number of inversions, such that $\mathcal{P}_n(x)$ represents $f(x)$. In Theorem 5.1.1, we give a formula for the number of permutations of $\mathbb{F}_q$ with Carlitz rank n, $B(n)$, where $2 \leq n < \frac{q-1}{2}$. The results in Chapter 5 are published in [2].

2 Background on Fourier Analysis

For background on Fourier analysis on finite groups we refer the reader [18]. Here we present the necessary background for the modules $\mathbb{Z}_q^d$ over $\mathbb{Z}_q$.

Let $f, g : \mathbb{Z}_q^d \to \mathbb{C}$. The Fourier transform of f is defined as

$$\widehat{f}(m) = q^{-d} \sum_{x \in \mathbb{Z}_q^d} \chi(-x.m) f(x),$$

where $\chi(z) = exp(2\pi iz/q)$. We note the following properties:

$$q^{-d} \sum_{x \in \mathbb{Z}_q^d} \chi(x.m) = \begin{cases} 1, & \text{if } m = 0 \\ 0, & otherwise \end{cases} \qquad \text{(Orthogonality)}$$

$$f(x) = \sum_{m \in \mathbb{Z}_q^d} \chi(x.m) \widehat{f}(m) \qquad \text{(Inversion)}$$

$$\sum_{m \in \mathbb{Z}_q^d} \widehat{f}(m) \overline{\widehat{g}(m)} = q^{-d} \sum_{x \in \mathbb{Z}_q^d} f(x) \overline{g(x)} \qquad \text{(Parseval)}$$

In particular, taking $g = f$ in Parseval's identity, we have

$$\sum_{m \in \mathbb{Z}_q^d} |\widehat{f}(m)|^2 = q^{-d} \sum_{x \in \mathbb{Z}_q^d} |f(x)|^2. \qquad \text{(Plancherel)}$$

Finally the average value of of $f(x)$ is given by

$$Avg(f) = \widehat{f}(0, \ldots, 0) = q^{-d} \sum_{x \in \mathbb{Z}_q^d} f(x).$$

3 Distinct Distances-Congruence classes of k-simplices determined by subsets of $\mathbb{F}_q^d$ and $\mathbb{Z}_q^d$

The classical Erdős distance problem in discrete geometry asks for the number of distinct distances determined by n points in Euclidean space. In [11] Erdős conjectured that the minimum number of distinct distances determined by n points in the Euclidean plane is $C\frac{n}{\sqrt{logn}}$. Recently, Guth and Katz [12] settled the conjecture, up to a square log factor showing that n points determine at least $C\frac{n}{logn}$ distances. We should note that in higher dimensions the conjecture is still open, and the best results are due to Solymosi and Vu which can be found in [20]. Before stating the best known result in the context of finite fields and integer rings let us first introduce the necessary background.

3.1 Preliminaries

Throughout, $T_k^d(E)$ will denote the the set of congruence classes of k-simplices determined by $E \subset \mathbb{F}_q^d$ or $\mathbb{Z}_q^d$. We simply write $\Delta(E)$ for $T_1^d(E)$, the set of distinct distances determined by the points of E.

3.2 $\mathbb{F}_q^d$ Setting:

The geometry of subsets of vector spaces over finite fields is analogous to that of discrete points in the Euclidean setting. Iosevich and Rudnev (see [15]) proved that for $E \subset \mathbb{F}_q^d$, if $|E| > 2q^{\frac{d+1}{2}}$ then the points of E determine all possible distances. They also showed that one cannot in general get Cq distinct distances, i.e a positive proportion of all distances, if $|E| \leq q^{\frac{d}{2}}$.

In [14], the authors showed the following:

(i) Let $d > 2$. If $|E| > Cq^{\frac{d}{2}}$ with a sufficiently large constant C, then there exist $c > 0$ such that $|\Delta(E)| \geq cq$.

(ii) If d is odd, there exist $c > 0$ and $E \subset \mathbb{F}_q^d$ such that $|E| \geq cq^{\frac{d+1}{2}}$ and $\Delta(E) \neq \mathbb{F}_q$. Which implies that the exponent $\frac{d+1}{2}$ in [15] is sharp to get all q distances in odd dimensions. The question of whether the exponent $\frac{d}{2}$ in (i) can be reduced to get a positive proportion of all distances is still open in odd dimensions.

(iii) If $d > 2$ is even, $|E| > Cq^{\frac{d}{2}}$ with a sufficiently large constant C gives $\Delta(E) = \mathbb{F}_q$. Also there exists $c > 0$ and $|E| > cq^{\frac{d}{2}}$ with $\Delta(E) \neq \mathbb{F}_q$. That is the exponent $\frac{d}{2}$ is sharp to get all q distances in even dimensions greater than 2. The question of whether the exponent $\frac{d}{2}$ can be smaller to get a positive proportion of all distances is open.

For $d = 2$, in [7, Theorem 2.2], it was shown that if $E \subset \mathbb{F}_q^2$ with $|E| > q^{\frac{4}{3}}$, where $q = 3 \bmod 4$, then $|\Delta(E)| > cq$. In [3] this result has been generalized to an arbitrary odd q. The question of whether the exponent $\frac{4}{3}$ here can be reduced is still open.

A natural generalization of distance problem is the problem of distribution of k-simplices and in [3], it is proved that for $E \subset \mathbb{F}_q^2$, q odd, if $|E| \geq Cq^{\frac{8}{5}}$, then $T_2^2(E) \geq cq^3$, which improves the previous known result of $|E| \gg q^{\frac{7}{4}}$ in [4].

In more general setting, the following non-trivial exponent for congruence classes of k-simplices $T_k^d(E)$ is examined in [3].

Theorem 3.2.1. *Let Q be a non-degenerate quadratic form on $\mathbb{F}_q^d$, where q is odd and $d \geq 2$. Let $E \subset \mathbb{F}_q^d$. There exist constants C, c, depending only on $1 \leq k \leq d$, such that: if $|E| \geq Cq^{d-\frac{d-1}{k+1}}$, then*

$$|T_{k,Q}^d(E)| \geq cq^{\binom{k+1}{2}}.$$

3.3 $\mathbb{Z}_q^d$ Setting:

In this section we concentrate on the distance relevant problems in context of finite cyclic rings Z_{p^l}, where p is an odd prime. Compared to configurations in vector spaces over finite fields, to overcome the difficulties arising from the zero divisors in these cyclic rings, an extra arithmetical machinery is developed.

The distance problem for subsets of residue rings, namely for $\mathbb{Z}_q^d$ where q is an odd prime power, is studied by Covert, Iosevich and Pakianathan in [9]. Here is the related theorem.

Theorem 3.3.1. *Let $E \subset \mathbb{Z}_q^d$, where $q = p^l$ and p is odd. Suppose $|E| \gg l(l+1)q^{\frac{(2l-1)d}{2l}+\frac{1}{2l}}$. Then,*

$$\Delta(E) \supset \mathbb{Z}_q^*$$

where $\mathbb{Z}_q^*$ denotes the the set of unit elements in $\mathbb{Z}_q$.

Given $E \subset \mathbb{Z}_q^2$, using a group theoretical approach analogous to [3], for $T_2^2(E)$, the congruence classes of triangles determined by the points of E, we will prove the following result.

Theorem 3.3.2. *Suppose $E \subset \mathbb{Z}_q^2$ with $q = p^l$ and $p \equiv 3 \bmod 4$. If $|E| \geq \sqrt[3]{3}p^{2l-\frac{1}{3}}$, then $|T_2^2(E)| \gtrsim q^3$.*

For the proof we will need the following lemmas.

Let us first denote by $SO_2(\mathbb{Z}_q) = \{A \in M_2(\mathbb{Z}_q) : AA^T = I,\ det(A) = 1\}$ the special orthogonal group.

Lemma 3.3.1. *Let $\xi = (\xi_1, \xi_2) \in \mathbb{Z}_q^2$, where $q = p^l$ and p is an odd prime. If $\|\xi\| = \xi_1^2 + \xi_2^2 \neq 0$, then $|Stab(\xi)| \leq p^{l-1}$, where Stab is the stabilizer under the action of the special orthogonal group.*

Proof. Let $\xi = (x, y) \in \mathbb{Z}_q^2$. Since $\|\xi\| \neq 0$, we can write $\|\xi\| = x^2 + y^2 = p^i u,\ 0 \leq i \leq l-1,\ u \in \mathbb{Z}_q^*$. Now if $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in SO_2(\mathbb{Z}_q)$ fixes ξ, then from the identity

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$$

we get

$$\begin{aligned} (a-1)x + by &= 0 \\ -bx + (a-1)y &= 0, \end{aligned}$$

and hence

$$\begin{aligned} (a-1)(x^2+y^2) &\equiv 0 \mod p^l, \\ b(x^2+y^2) &\equiv 0 \mod p^l. \end{aligned} \tag{3.1}$$

Putting $x^2 + y^2 = p^i u$ in (3.1), we have

$$a = p^{l-i}k + 1,\ 0 \leq k < p^i, \text{ and } b = p^{l-i}m,\ 0 \leq m < p^i, \tag{3.2}$$

where

$$a^2 + b^2 \equiv 1 \bmod p^l. \tag{3.3}$$

Now to conclude the argument, we claim that for $a_0 \neq a$ if b_0 and b are satisfying $a_0^2 + b_0^2 \equiv 1 \mod p^l$ and $a^2 + b^2 \equiv 1 \mod p^l$ and condition (3.2),

respectively, then $b_0 \neq b$. This will prove the lemma, for then the number of pairs (a, b) satisfying the conditions (3.2) and (3.3) is at most the number of possibilities of b which is p^i. This is at most p^{l-1} as the valuation of a nonzero element is at most $l-1$.

It remains to prove the claim and we will prove its contrapositive here. Suppose that $b_0 = b$ and $a_0^2 + b_0^2 \equiv 1 \bmod p^l$, $a^2 + b^2 \equiv 1 \bmod p^l$, so that $a_0^2 \equiv a^2 \bmod p^l$. Writing $a_0 = p^{l-i}k_0 + 1$ and $a = p^{l-i}k + 1$, It follows that

$$\begin{aligned} (p^{l-i}k_0 + 1)^2 &\equiv (p^{l-i}k + 1)^2 \bmod p^l, \\ p^{2l-2i}k_0^2 + 2p^{l-i}k_0 &\equiv p^{2l-2i}k^2 + 2p^{l-i}k \bmod p^l, \end{aligned}$$

therefore,

$$\begin{aligned} p^{2l-2i}(k_0^2 - k^2) + 2p^{l-i}(k_0 - k) &\equiv 0 \bmod p^l, \\ p^{l-i}(k_0 - k)(p^{l-i}(k_0 + k) + 2) &\equiv 0 \bmod p^l. \end{aligned}$$

Thus $p^l \mid p^{l-i}(k_0 - k)(p^{l-i}(k_0 + k) + 2)$, and since $p \nmid p^{l-i}(k_0 + k) + 2$ as p is odd, we must have $p^i \mid k_0 - k < p^i$. Hence we have $k_0 - k = 0$, i.e., $k_0 = k$ and therefore $a_0 = a$. □

Lemma 3.3.2. *Let $\xi \in \mathbb{Z}_q^2 \setminus (0,0)$, where $q = p^l$ and $p \equiv 3$ mod 4. If $\|\xi\| = 0$, then $|Stab(\xi)| \leq p^{l-1}$.*

For the proof of Lemma 3.3.2 we will use Hensel's Lemma.

Lemma 3.3.3 (Hensel's Lemma)**.** *Let $f(x) \in \mathbb{Z}[x]$, $f(r) \equiv 0 \bmod p$ and $f'(r) \not\equiv 0 \bmod p$ so that r is a simple root of f modulo p. Then for any $k \geq 2$, there exists a unique $\hat{r}$ in $\mathbb{Z}_{p^k}$ such that $f(\hat{r}) \equiv 0 \bmod p^k$ with $\hat{r} \equiv r \bmod p$.*

Proof of Lemma 3.3.2. We first note that as $p \equiv 3 \bmod 4$, for $\xi \in \mathbb{Z}_q^2 \setminus (0,0)$, $\|\xi\| = 0$ implies that $\xi = (p^m u, p^m v)$ for some $m \geq \frac{l}{2}$ and $u, v \in \mathbb{Z}_q^*$. Now if $A \in SO_2(\mathbb{Z}_q)$ fixes $\xi = (p^m u, p^m v)$, it can be readily shown that it also fixes $\eta = (-p^m v, p^m u)$. Hence A also fixes $Span\{\xi, \eta\} = p^m(\mathbb{Z}_{p^l} \times \mathbb{Z}_{p^l}) \cong \mathbb{Z}_{p^{l-m}} \times \mathbb{Z}_{p^{l-m}}$.

Since $\xi \neq (0,0)$, we have $m \leq l-1$. We shall note that $\mathbb{Z}_{p^{l-m}} \times \mathbb{Z}_{p^{l-m}}$ is smallest, and hence the number of matrices A that fixes $\mathbb{Z}_{p^{l-m}} \times \mathbb{Z}_{p^{l-m}}$ is largest, when $m = l-1$. Therefore it is sufficient to consider the case $m = l-1$. In this case A fixes $p^{l-1}(\mathbb{Z}_{p^l} \times \mathbb{Z}_{p^l}) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

We now write

$$A = I_2 + B,$$

where I_2 denotes the 2×2 identity matrix and $B \in M_2(\mathbb{Z}_q)$. Then for any $y \in \mathbb{Z}_q^2$ we have

$$Ap^{l-1}y = p^{l-1}y + Bp^{l-1}y,$$

so that $Bp^{l-1}y = 0$ as A fixes $p^{l-1}y$. This implies that $B = pB'$ for some $B' \in M_2(\mathbb{Z}_q)$, and

$$A = I_2 + pB' \in \Gamma_1 \cap SO_2(\mathbb{Z}_q).$$

where Γ_1 denotes the matrices in $M_2(\mathbb{Z}_q)$ congruent to $I_2 \bmod p$.

It follows that

$$A \in \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{Z}_q,\ a^2 + b^2 \equiv 1 \bmod q,\ a \equiv 1 \bmod p,\ b \equiv 0 \bmod p \right\}. \tag{3.4}$$

Now we count the number of matrices in (3.4). We first fix b. Since $b \equiv 0 \bmod p$, we have p^{l-1} choices for b. Then we consider the polynomial $f(x) = x^2 - (1-b^2) \in \mathbb{Z}[x]$. Note that $f(x) = x^2 - 1$ in $\mathbb{Z}_p$ as $b \equiv 0 \bmod p$. Hence 1 is a root of $f(x)$ and $f'(1) = 2 \neq 0$ in $\mathbb{Z}_p$ as p is odd. Hence by Hensel's Lemma there exists a unique a in $\mathbb{Z}_q$ such that $f(a) = a^2 - (1-b^2) = 0$ in $\mathbb{Z}_q$ with $a \equiv 1 \bmod p$. Therefore the number matrices of the form in (3.4) is p^{l-1}. This completes the proof.

□

We make use of the following lemma from [3].

Lemma 3.3.4. *For any finite space F, any function $f : F \to \mathbb{R}_{\geq 0}$, and any $n \geq 2$ we have*

$$\sum_{z \in F} f^n(z) \leq |F| \left(\frac{\|f\|_1}{|F|} \right)^n + \frac{n(n-1)}{2} \|f\|_\infty^{n-2} \sum_{z \in F} \left(f(z) - \frac{\|f\|_1}{|F|} \right)^2,$$

where $\|f\|_1 = \sum_{z \in F} |f(z)|$, and $\|f\|_\infty = max_{z \in F} f(z)$.

Lastly, we state the following lemma from [9] and use Remark 3.3.1 for the proof of Theorem 3.3.2.

Lemma 3.3.5. *Let $d \geq 2$ and $j \in \mathbb{Z}_q^*$, where q is odd. Set $||x|| = x_1^2 + ... + x_d^2$. Denote by $S_j = \{x \in \mathbb{Z}_q^d : ||x|| = j\}$ the sphere of radius j. Then,*

$$|S_j| = q^{d-1}(1 + o(1)).$$

Remark 3.3.1. *Note that*

$$SO_2(\mathbb{Z}_q) = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a^2 + b^2 = 1 \right\} \tag{3.5}$$

and hence if we denote by S_1 the sphere of radius 1 in $\mathbb{Z}_q^2$, then $|SO_2(\mathbb{Z}_q)| = |S_1| \sim q$, by Lemma 3.3.5.

Proof of Theorem 3.3.2. We first recall that $SO_2(\mathbb{Z}_q) = \{A \in M_2(\mathbb{Z}_q) : AA^T = I,\ det(A) = 1\}$ and define an equivalence relation on $(\mathbb{Z}_q^2)^3$ as

$$(a, b, c) \sim (a', b', c')$$

if $\exists \theta \in SO_2(\mathbb{Z}_q)$ with $a' = \theta a,\ b' = \theta b,\ c' = \theta c$.

For $E \subset \mathbb{Z}_q^2$ and $a, b, c \in \mathbb{Z}_q^2$, let

$$\mu(a, b, c) = |\{(x, y, z) \in E^3 : \exists \theta \in SO_2(\mathbb{Z}_q) \text{ such that } x - y = \theta a, y - z = \theta b, x - z = \theta c.\}|.$$

Note that $\mu(\theta a, \theta b, \theta c) = \mu(a, b, c)$ for all $\theta \in SO_2(\mathbb{Z}_q)$, so μ can be viewed as a function $\mu : (\mathbb{Z}_q^2)^3 / \sim \to \mathbb{Z}_{\geq 0}$.

Then by the Cauchy-Schwarz inequality,

$$|E|^6 = \left(\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim} \mu(a,b,c) \right)^2 \leq |T_2^2(E)| \left(\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim} \mu^2(a,b,c) \right),$$

where

$$|T_2^2(E)| = |\{(a,b,c) \in (\mathbb{Z}_q^2)^3/\sim: \mu(a,b,c) \neq 0\}|,$$

which is equal to

$$|\{(a,b,c) \in (\mathbb{Z}_q^2)^3/\sim: \exists (x,y,z) \in E^3 \text{and } \theta \in SO_2(\mathbb{Z}_q) \text{ such that } x-y=\theta a, y-z=\theta b, x-z=\theta c\}|.$$

We have,

$$\begin{aligned}
\mu^2(a,b,c) &= |\{(x,y,z,x',y',z') \in E^6 : \exists \theta_1,\theta_2 \in SO_2(\mathbb{Z}_q) \text{ such that} \\
&\quad x-y=\theta_1 a,\ x'-y'=\theta_2 a \\
&\quad y-z=\theta_1 b,\ y'-z'=\theta_2 b \\
&\quad x-z=\theta_1 c,\ x'-z'=\theta_2 c\}| \\
&= |\{(x,y,z,x',y',z') \in E^6 : \exists \theta_1,\theta_2 \in SO_2(\mathbb{Z}_q) \text{ such that} \\
&\quad \theta_1^{-1}(x-y)=\theta_2^{-1}(x'-y')=a \\
&\quad \theta_1^{-1}(y-z)=\theta_2^{-1}(y'-z')=b \\
&\quad \theta_1^{-1}(x-z)=\theta_2^{-1}(x'-z')=c\}|
\end{aligned}$$

so that

$$\begin{aligned}\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim}\mu^2(a,b,c) &= |\{(x,y,z,x',y',z')\in E^6 : \exists\theta_1,\theta_2\in SO_2(\mathbb{Z}_q) \text{ such that}\\ &\quad \theta_1^{-1}(x-y)=\theta_2^{-1}(x'-y')\\ &\quad \theta_1^{-1}(y-z)=\theta_2^{-1}(y'-z')\\ &\quad \theta_1^{-1}(x-z)=\theta_2^{-1}(x'-z')\}|\\ &= |\{(x,y,z,x',y',z')\in E^6 : \exists\theta\in SO_2(\mathbb{Z}_q) \text{ such that}\\ &\quad \theta(x-y)=x'-y',\ \theta(y-z)=y'-z',\ \theta(x-z)=x'-z'\}|\\ &= |\{(x,y,z,x',y',z')\in E^6 : \exists\theta\in SO_2(\mathbb{Z}_q) \text{ such that}\\ &\quad x'-\theta x=y'-\theta y=z'-\theta z\}|.\end{aligned}$$

For a fixed $\theta\in SO_2(\mathbb{Z}_q)$, let

$$\nu_\theta(t)=|\{(u,v)\in E\times E:\ u-\theta(v)=t\}|. \tag{3.6}$$

Then we have

$$\nu_\theta^3(t)=|\{(x,y,z,x',y',z')\in E^6 : x'-\theta x=y'-\theta y=z'-\theta z=t\}|,$$

and therefore

$$\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim}\mu^2(a,b,c)\le\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ t\in\mathbb{Z}_q^2}}\nu_\theta^3(t). \tag{3.7}$$

By Lemma 3.3.4,

$$\sum_{t\in\mathbb{Z}_q^2}\nu_\theta^3(t)\le q^2\left(\frac{\|\nu_\theta\|_1}{q^2}\right)^3+3\|\nu_\theta\|_\infty\sum_{t\in\mathbb{Z}_q^2}\left(\nu_\theta(t)-\frac{\|\nu_\theta\|_1}{q^2}\right)^2$$

where $\|\nu_\theta\|_1=\sum_{t\in\mathbb{Z}_q^2}\nu_\theta(t)=|E|^2$ and $\|\nu_\theta\|_\infty=sup_t|\nu_\theta(t)|\le|E|$ as when we first fix v in (3.6), u is uniquely determined.

It follows that

$$\begin{aligned}\sum_{t\in\mathbb{Z}_q^2}\nu_\theta^3(t) &\le q^{-4}|E|^6+3|E|\sum_{t\in\mathbb{Z}_q^2}\left(\nu_\theta(t)-\frac{\|\nu_\theta\|_1}{q^2}\right)^2\\ &\le q^{-4}|E|^6+3q^2|E|\sum_{\xi\in\mathbb{Z}_q^2\setminus(0,0)}|\widehat{\nu}_\theta(\xi)|^2\ (\textit{by Plancherel Theorem})\end{aligned}$$

and thus

$$\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ t\in\mathbb{Z}_q^2}} \nu_\theta^3(t) \le |SO_2(\mathbb{Z}_q)|q^{-4}|E|^6 + 3q^2|E| \sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ \xi\in\mathbb{Z}_q^2\setminus(0,0)}} |\widehat{\nu}_\theta(\xi)|^2$$

By Remark 3.3.1, $|SO_2(\mathbb{Z}_q)| \sim q$ and hence

$$\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ t\in\mathbb{Z}_q^2}} \nu_\theta^3(t) \lesssim q^{-3}|E|^6 + 3q^2|E| \sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ \xi\in\mathbb{Z}_q^2\setminus(0,0)}} |\widehat{\nu}_\theta(\xi)|^2 \tag{3.8}$$

Noting that

$$\begin{aligned}
\nu_\theta(t) &= \sum_{v\in\mathbb{Z}_q^2} E(v)E(t+\theta v)\\
&= \sum_{v,\alpha\in\mathbb{Z}_q^2} E(v)\chi(\alpha.(t+\theta v))\widehat{E}(\alpha)\\
&= \sum_{v,\alpha\in\mathbb{Z}_q^2} \widehat{E}(\alpha)\chi(t.\alpha)E(v)\chi(\alpha.\theta v)\\
&= \sum_{\alpha\in\mathbb{Z}_q^2} \widehat{E}(\alpha)\chi(t.\alpha)\sum_{v\in\mathbb{Z}_q^2}\chi(\alpha.\theta v)E(v)\\
&= \sum_{\alpha\in\mathbb{Z}_q^2} \widehat{E}(\alpha)\chi(t.\alpha)\sum_{v\in\mathbb{Z}_q^2}\chi(\theta^T(\alpha).v)E(v)\\
&= q^2\sum_{\alpha\in\mathbb{Z}_q^2} \widehat{E}(\alpha)\chi(t.\alpha)\widehat{E}(-\theta^T(\alpha)),
\end{aligned}$$

and

$$\begin{aligned}
\widehat{\nu}_\theta(\xi) &= q^{-2}\sum_{t\in\mathbb{Z}_q^2}\chi(-t.\xi)\nu_\theta(t)\\
&= q^{-2}\sum_{t\in\mathbb{Z}_q^2}\chi(-t.\xi)q^2\sum_{\alpha\in\mathbb{Z}_q^2}\widehat{E}(\alpha)\chi(t.\alpha)\widehat{E}(-\theta^T(\alpha))\\
&= \sum_{\alpha\in\mathbb{Z}_q^2}\widehat{E}(\alpha)\widehat{E}(-\theta^T(\alpha))\sum_{t\in\mathbb{Z}_q^2}\chi(t.(\alpha-\xi))\\
&= q^2\widehat{E}(\xi)\widehat{E}(-\theta^T(\xi)),
\end{aligned}$$

we have

$$\begin{aligned}\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ \xi\in\mathbb{Z}_q^2\setminus(0,0)}}|\widehat{\nu}_\theta(\xi)|^2 &= q^4\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ \xi\in\mathbb{Z}_q^2\setminus(0,0)}}|\widehat{E}(\xi)|^2|\widehat{E}(-\theta^T(\xi))|^2\\ &= q^4\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ \xi\in\mathbb{Z}_q^2\setminus(0,0)}}|\widehat{E}(\xi)|^2|\widehat{E}(\theta^T(\xi))|^2\\ &\leq q^4\left(\max_{\xi\in\mathbb{Z}_q^2\setminus(0,0)}|Stab(\xi)|\right)\sum_{\xi\neq(0,0)}|\widehat{E}(\xi)|^2\sum_{\substack{\eta\neq(0,0)\\ \|\eta\|=\|\xi\|}}|\widehat{E}(\eta)|^2\end{aligned}$$

Plugging this value in (3.8) and using (3.7) we get

$$\begin{aligned}\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim}\mu^2(a,b,c) &\leq \sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ t\in\mathbb{Z}_q^2}}\nu_\theta^3(t)\\ &\lesssim q^{-3}|E|^6+3q^6|E|\left(\max_{\xi\in\mathbb{Z}_q^2\setminus(0,0)}|Stab(\xi)|\right)\sum_{\xi\neq(0,0)}|\widehat{E}(\xi)|^2\sum_{\substack{\eta\neq(0,0)\\ \|\eta\|=\|\xi\|}}|\widehat{E}(\eta)|^2\\ &= q^{-3}|E|^6+3q^6|E|\mathrm{I} \qquad (3.9)\end{aligned}$$

where

$$\mathrm{I}=\left(\max_{\xi\in\mathbb{Z}_q^2\setminus(0,0)}|Stab(\xi)|\right)\sum_{\xi\neq(0,0)}|\widehat{E}(\xi)|^2\sum_{\substack{\eta\neq(0,0)\\ \|\eta\|=\|\xi\|}}|\widehat{E}(\eta)|^2$$

We first note that $|Stab(\xi)|\leq p^{l-1}$ for $\xi\neq(0,0)$ by Lemma 3.3.1 and 3.3.2. Extending the summation in η over all η and using Plancherel twice in I, we get

$$\mathrm{I}\leq p^{l-1}q^{-4}|E|^2.$$

Plugging this value in (3.9) gives

$$\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim}\mu^2(a,b,c)\lesssim q^{-3}|E|^6+3q^2|E|^3p^{l-1}, \qquad (3.10)$$

so that

$$\begin{aligned}|T_2^2(E)| &\geq \frac{|E|^6}{q^{-3}|E|^6+3q^2|E|^3p^{l-1}}\\ &\geq \frac{|E|^6}{2q^{-3}|E|^6}=\frac{q^3}{2}\end{aligned}$$

whenever $|E| \geq \sqrt[3]{3}p^{2l-\frac{1}{3}}$, which completes the proof. $\square$

Another distance related problem is the hinges problem in the discrete setting. Employing the methods of [8], we have the following related result in the context of $\mathbb{Z}_{p^l}$.

Theorem 3.3.3. *Let $r > 2$ be an integer. For $E \subset \mathbb{Z}_q^d$, where $q = p^l$, p is an odd prime, and a distance set $\alpha = \{\alpha_i\}_{i=1}^{r-1} \in (\mathbb{Z}_q^*)^{r-1}$, let*

$$H_{r,\alpha} = \{(x, x_1, \ldots, x_{r-1}) \in E \times \ldots \times E : \|x - x_i\| = \alpha_i\}$$

denote the r-hinges with distances α determined by the points of E. Then ,

$$|H_{r,\alpha}| = \frac{|E|^r}{q^{r-1}}(1 + o(1))$$

whenever $|E| \gg l(l+1)q^{d\left(1-\frac{1}{2l(r-2)}\right)+\frac{1}{2l(r-2)}}$.

For the proof we shall make use of Lemma 3.3.5 and the following lemma from [9].

Lemma 3.3.6. *For $j \in \mathbb{Z}_q^*$ and $q = p^l$, we have*

$$sup_{m \neq 0} \left|\widehat{S}_j(m)\right| \leq l(l+1)q^{-\frac{d+2l-1}{2l}}.$$

Proof of Theorem 3.3.3. The proof will proceed by induction on r. We first consider the basis step $r = 3$:

$$\begin{aligned} |H_{3,\alpha}| &= \{(x, x_1, x_2) \in E \times E \times E : \|x - x_1\| = \alpha_1, \|x - x_2\| = \alpha_2\} \\ &= \sum_{x, x_1, x_2} S_{\alpha_1}(x - x_1) S_{\alpha_2}(x - x_2) E(x) E(x_1) E(x_2) \\ &= \sum_{x \in E} \left(\sum_y S_{\alpha_1}(x - y) E(y) \right) \left(\sum_{y'} S_{\alpha_2}(x - y') E(y') \right). \end{aligned} \tag{3.11}$$

Note that

$$\begin{aligned}
\sum_y S_{\alpha_i}(x-y)E(y) &= \sum_m \sum_y \chi(m.(x-y))\widehat{S}_{\alpha_i}(m)E(y) \\
&= \sum_m \chi(m.x)\widehat{S}_{\alpha_i}(m)\sum_y \chi(-m.y)E(y) \\
&= q^d \sum_m \chi(m.x)\widehat{S}_{\alpha_i}(m)\widehat{E}(m) \\
&= q^d \widehat{S}_{\alpha_i}(0)\widehat{E}(0) + q^d \sum_{m\neq 0} \chi(m.x)\widehat{S}_{\alpha_i}(m)\widehat{E}(m) \\
&= q^{-d}|E||S_{\alpha_i}| + q^d \sum_{m\neq 0} \chi(m.x)\widehat{S}_{\alpha_i}(m)\widehat{E}(m)
\end{aligned}$$

By Lemma 3.3.5, $|S_{\alpha_i}| = q^{d-1}(1+o(1))$ for any $\alpha_i \in \mathbb{Z}_q^*$. Hence

$$\sum_y S_{\alpha_i}(x-y)E(y) = q^{-1}|E|(1+o(1)) + q^d \sum_{m\neq 0} \chi(m.x)\widehat{S}_{\alpha_i}(m)\widehat{E}(m),$$

and (3.11) is equal to

$$\sum_{x\in E}(q^{-1}|E|(1+o(1))+q^d \sum_{m\neq 0} \chi(m.x)\widehat{S}_{\alpha_1}(m)\widehat{E}(m))(q^{-1}|E|(1+o(1))+q^d \sum_{n\neq 0} \chi(n.x)\widehat{S}_{\alpha_2}(n)\widehat{E}(n))$$

$$\begin{aligned}
&= \sum_{x\in E} q^{-2}|E|^2(1+o(1)) \\
&+ \sum_{x\in E} q^{d-1}|E|(1+o(1))\left(\sum_{m\neq 0} \chi(m.x)\widehat{S}_{\alpha_1}(m)\widehat{E}(m) + \sum_{n\neq 0} \chi(n.x)\widehat{S}_{\alpha_2}(n)\widehat{E}(n)\right) \\
&+ q^{2d}\sum_{x\in E}\sum_{\substack{m\neq 0\\ n\neq 0}} \chi(m.x)\chi(n.x)\widehat{S}_{\alpha_1}(m)\widehat{E}(m)\widehat{S}_{\alpha_2}(n)\widehat{E}(n) \\
&= \frac{|E|^3}{q^2}(1+o(1)) + \mathrm{I} + \mathrm{II},
\end{aligned}$$

where

$$\mathrm{I} = \sum_{x\in E} q^{d-1}|E|(1+o(1))\left(\sum_{m\neq 0} \chi(m.x)\widehat{S}_{\alpha_1}(m)\widehat{E}(m) + \sum_{n\neq 0} \chi(n.x)\widehat{S}_{\alpha_2}(n)\widehat{E}(n)\right),$$

and

$$\mathrm{II} = q^{2d} \sum_{x \in E} \sum_{\substack{m \neq 0 \\ n \neq 0}} \chi(m.x)\chi(n.x)\widehat{S}_{\alpha_1}(m)\widehat{E}(m)\widehat{S}_{\alpha_2}(n)\widehat{E}(n).$$

Observe that

$$\begin{aligned}
\mathrm{I} &\leq 2\sum_{x \in E} q^{d-1}|E|(1+o(1)) \sum_{m \neq 0} \chi(m.x)\widehat{S}_{\alpha_i}(m)\widehat{E}(m) \\
&= 2|E|q^{d-1}(1+o(1)) \sum_{m \neq 0} \sum_{x} \chi(m.x)\widehat{S}_{\alpha_i}(m)\widehat{E}(m)E(x) \\
&= 2|E|q^{2d-1}(1+o(1)) \sum_{m \neq 0} \widehat{E}(-m)\widehat{E}(m)\widehat{S}_{\alpha_i}(m) \\
&= 2|E|q^{2d-1}(1+o(1)) \sum_{m \neq 0} |\widehat{E}(m)|^2 \widehat{S}_{\alpha_i}(m)
\end{aligned}$$

so that by Lemma 3.3.6 and Plancherel equality

$$\begin{aligned}
|\mathrm{I}| &\leq 2|E|q^{2d-1}(1+o(1))l(l+1)q^{-\frac{d+2l-1}{2l}}q^{-d}|E| \\
&= 2|E|^2 q^{d-1}(1+o(1))l(l+1)q^{-\frac{d+2l-1}{2l}}.
\end{aligned}$$

Also,

$$\begin{aligned}
|\mathrm{II}| &\leq q^{2d} \sum_{x \in E} |\sum_{m \neq 0} \chi(m.x)\widehat{S}_{\alpha_1}(m)\widehat{E}(m)||\sum_{n \neq 0} \chi(n.x)\widehat{S}_{\alpha_2}(n)\widehat{E}(n)| \\
&\leq q^{2d} \sum_{x \in E} |\sum_{m \neq 0} \chi(m.x)\widehat{S}_{\alpha_i}(m)\widehat{E}(m)|^2 \\
&\leq q^{2d} \sum_{x \in \mathbb{Z}_q^d} \sum_{\substack{m \neq 0 \\ n \neq 0}} \chi(m.x)\widehat{S}_{\alpha_i}(m)\widehat{E}(m)\chi(-n.x)\overline{\widehat{S}_{\alpha_i}(n)}\ \overline{\widehat{E}(n)} \\
&= q^{2d} \sum_{\substack{m \neq 0 \\ n \neq 0}} \widehat{S}_{\alpha_i}(m)\widehat{E}(m)\overline{\widehat{S}_{\alpha_i}(n)}\ \overline{\widehat{E}(n)} \sum_{x \in \mathbb{Z}_q^d} \chi((m-n).x) \\
&= q^{3d} \sum_{m \neq 0} |\widehat{S}_{\alpha_i}(m)|^2 |\widehat{E}(m)|^2 \\
&\leq q^{3d} l^2 (l+1)^2 q^{-\frac{d+2l-1}{l}} \sum_{m \neq 0} |\widehat{E}(m)|^2 \ (\textit{by Lemma 3.3.6}) \\
&\leq q^{2d} l^2 (l+1)^2 q^{-\frac{d+2l-1}{l}} |E|.
\end{aligned}$$

Therefore,

$$\begin{aligned}|H_{3,\alpha}| &= \frac{|E|^3}{q^2}(1+o(1)) + \mathrm{I} + \mathrm{II} \\ &= \frac{|E|^3}{q^2}(1+o(1)) + O(2|E|^2 q^{d-1}(1+o(1))l(l+1)q^{-\frac{d+2l-1}{2l}} + q^{2d}l^2(l+1)^2 q^{-\frac{d+2l-1}{l}}|E|).\end{aligned}$$

It follows that if $|E| \gg l(l+1)q^{d(1-\frac{1}{2l})+\frac{1}{2l}}$, then

$$|H_{3,\alpha}| = \frac{|E|^3}{q^2}(1+o(1)).$$

Now for the inductive step we assume that $|H_{r,\alpha}| = \frac{|E|^r}{q^{r-1}}(1+o(1))$ when $|E| \gg l(l+1)q^{d\left(1-\frac{1}{2l(r-1)}\right)+\frac{1}{2l(r-1)}}$. Setting $S := S_{\alpha_r}$, we can write

$$\begin{aligned}|H_{r+1,\alpha}| &= \sum_{x,x_1,\ldots x_r} H_{r,\alpha}(x,x_1,\ldots,x_{r-1})E(x_r)S(x-x_r) \\ &= \sum_{x,x_1,\ldots x_r} H_{r,\alpha}(x,x_1,\ldots,x_{r-1})E(x_r)\sum_m \chi(m.(x-x_r))\widehat{S}(m) \\ &= \sum_{x,x_1,\ldots x_{r-1}} H_{r,\alpha}(x,x_1,\ldots,x_{r-1})\sum_m \widehat{S}(m)\chi(m.x)\sum_{x_r}\chi(-m.x_r)E(x_r) \\ &= q^d \sum_{x,x_1,\ldots x_{r-1}} H_{r,\alpha}(x,x_1,\ldots,x_{r-1})\sum_m \widehat{S}(m)\chi(m.x)\widehat{E}(m) \\ &= q^d \sum_m \widehat{S}(m)\widehat{E}(m)\sum_{x,x_1,\ldots x_{r-1}} H_{r,\alpha}(x,x_1,\ldots,x_{r-1})\chi(m.x) \\ &= q^{d(r+1)}\sum_m \widehat{S}(m)\widehat{E}(m)\widehat{H}_{r,\alpha}(-m,0,\ldots,0) \\ &= q^{-d}|S||E||H_{r,\alpha}| + q^{d(r+1)}\sum_{m\neq 0}\widehat{S}(m)\widehat{E}(m)\widehat{H}_{r,\alpha}(-m,0,\ldots,0) \\ &= \frac{|E|^{r+1}}{q^r}(1+o(1)) + R \textit{ (by induction hypotesis)}\end{aligned}$$

where

$$R = q^{d(r+1)}\sum_{m\neq 0}\widehat{S}(m)\widehat{E}(m)\widehat{H}_{r,\alpha}(-m,0,\ldots,0).$$

Now using the Cauchy-Schwarz inequality,

$$\begin{aligned}
R^2 &= |R|^2 \\
&= q^{2d(r+1)} |\sum_{m\neq 0} \widehat{S}(m)\widehat{E}(m)\widehat{H}_{r,\alpha}(-m,0,\ldots,0)|^2 \\
&\leq q^{2d(r+1)} \left(\sum_{m\neq 0} |\widehat{S}(m)||\widehat{E}(m)||\widehat{H}_{r,\alpha}(-m,0,\ldots,0)|\right)^2 \\
&\leq q^{2d(r+1)} \sum_{m\neq 0} |\widehat{S}(m)|^2 |\widehat{E}(m)|^2 \sum_{m\neq 0} |\widehat{H}_{r,\alpha}(-m,0,\ldots,0)|^2 \\
&\leq q^{2d(r+1)} l^2(l+1)^2 q^{-\frac{d+2l-1}{l}} q^{-d}|E| \sum_{m\neq 0} |\widehat{H}_{r,\alpha}(-m,0,\ldots,0)|^2 \\
&\leq q^{2dr+d-\frac{d+2l-1}{l}} l^2(l+1)^2|E| \sum_{m} |\widehat{H}_{r,\alpha}(m,0,\ldots,0)|^2. \qquad (3.12)
\end{aligned}$$

Note that the third inequality above follows from Lemma 3.3.6 and Plancherel theorem.

Let $A := \sum_m |\widehat{H}_{r,\alpha}(m,0,\ldots,0)|^2$. We first see that

$$\begin{aligned}
\widehat{H}_{r,\alpha}(m,0,\ldots,0) &= q^{-dr} \sum_{x,x_1,\ldots x_{r-1}} \chi(-x.m) H_{r,\alpha}(x,x_1,\ldots,x_{r-1}) \\
&= q^{-dr} \sum_{x,x_1,\ldots x_{r-1}} \chi(-x.m) E(x)\ldots E(x_{r-1}) S_{\alpha_1}(x-x_1)\ldots S_{\alpha_{r-1}}(x-x_{r-1}) \\
&= q^{-dr+d}\widehat{f}(m),
\end{aligned}$$

where

$$\begin{aligned}
f(x) &= E(x) \sum_{x_1,\ldots,x_{r-1}} E(x_1)\ldots E(x_{r-1}) S_{\alpha_1}(x-x_1)\ldots S_{\alpha_{r-1}}(x-x_{r-1}) \\
&= E(x) \sum_{x_1} E(x_1) S_{\alpha_1}(x-x_1) \sum_{x_2} E(x_2) S_{\alpha_2}(x-x_2) \ldots \sum_{x_{r-1}} E(x_{r-1}) S_{\alpha_{r-1}}(x-x_{r-1}) \\
&= E(x) \sum_{x_1} E(x_1) S_{\alpha_1}(x-x_1) |E\cap(x-S_{\alpha_2})| \ldots |E\cap(x-S_{\alpha_{r-1}})| \\
&\leq q^{(r-2)(d-1)}(1+o(1)) E(x) \sum_{x_1} E(x_1) S_{\alpha_1}(x-x_1)
\end{aligned}$$

where in the last step we used the fact that $|E\cap(x-S)| \leq |S| = q^{d-1}(1+o(1))$.

It follows that

$$\begin{aligned}
A &= \sum_m |\widehat{H}_{r,\alpha}(m,0,\ldots,0)|^2 \\
&= q^{-2dr+2d}\sum_m |\widehat{f}(m)|^2 \\
&= q^{-2dr+d}\sum_x |f(x)|^2 \\
&\leq q^{-2dr+d}q^{2(r-2)(d-1)}(1+o(1))\sum_x E(x)\sum_{x_1,x_2} E(x_1)E(x_2)S_{\alpha_1}(x-x_1)S_{\alpha_1}(x-x_2) \\
&\leq q^{-2dr+d}q^{2(r-2)(d-1)}(1+o(1))|H_{3,\alpha}| \\
&\leq q^{-2dr+d}(q^{d-1})^{2(r-2)}|E|^3q^{-2}(1+o(1))
\end{aligned}$$

Now plugging this value of A in (3.12) we get

$$R^2 \leq q^{2d-2}(q^{d-1})^{2(r-2)}q^{-\frac{d+2l-1}{l}}|E|^4l^2(l+1)^2(1+o(1)),$$

so that

$$\begin{aligned}
|R| &\leq q^{d-1}(q^{d-1})^{r-2}q^{-\frac{d+2l-1}{2l}}|E|^2l(l+1)(1+o(1)) \\
&= q^{(d-1)(r-1)}q^{-\frac{d+2l-1}{2l}}|E|^2l(l+1)(1+o(1)).
\end{aligned}$$

We conclude that,

$$|H_{r+1,\alpha}| = \frac{|E|^{r+1}}{q^r}(1+o(1)) + O\left(q^{(d-1)(r-1)}q^{-\frac{d+2l-1}{2l}}|E|^2l(l+1)(1+o(1))\right),$$

and hence

$$|H_{r+1,\alpha}| = \frac{|E|^{r+1}}{q^r}(1+o(1))$$

whenever $|E| \gg l(l+1)q^{d\left(1-\frac{1}{2l(r-1)}\right)+\frac{1}{2l(r-1)}}$. □

4 Product-Volume set of subsets of $\mathbb{F}_q^d$ and $\mathbb{Z}_q^d$

An important problem in additive combinatorics is the sum-product problem for finite subsets of abelian groups, e.g. given $A \subset \mathbb{F}_q$ or $\mathbb{Z}_q$, how large does A need to be to ensure that $dA^2 = \underbrace{A.A + \ldots + A.A}_{\text{d-fold}}$ contains all q elements or a positive proportion of them. It is an easy observation that sum-product problem is closely related to the dot product problem in the context of finite fields and rings.

Also, it turns out that dot product problem has immediate implications for the volume of simplices in d-dimensional spaces, which we will discuss in detail in the subsequent sections.

4.1 Preliminaries

Given a subset E of $\mathbb{F}_q^d$ or $\mathbb{Z}_q^d$, the dot product is defined as

$$\prod(E) = \{x.y : \ x, y \in E\},$$

where dot product of two vectors is defined by the usual formula

$$x.y = x_1y_1 + \ldots + x_dy_d,$$

for $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$.

Let

$$A(E) = \{x.y^{\perp} : \ x, y \in E\} = \prod(E, E^{\perp})$$

denote the set of triangle areas determined by two arbitrary points of E with the third vertex pinned at the origin. More generally, throughout

$$V_d(E) = \{det(x^1 - x^{d+1}, \ldots, x^d - x^{d+1}) : \ x^j \in E\} \setminus \{0\}.$$

will denote the set of d-dimensional nonzero volumes, defined by $(d+1)$-simplices whose vertices are in E.

4.2 $\mathbb{F}_q^d$ Setting:

4.2.1 Dot Product

It is shown in [13] that for $d \geq 2$, $E \subset \mathbb{F}_q^d$ if $|E| > q^{\frac{d+1}{2}}$, then $\prod(E) \supset \mathbb{F}_q^*$. Later in [14], it is shown that the exponent $\frac{d+1}{2}$ above is sharp. More precisely, in quadratic extension of prime fields they construct a subset E of $\mathbb{F}_q^d$ of size $q^{\frac{d+1}{2}-\epsilon}$ for which $|\prod(E)| = o(q)$.

4.2.2 Volume Set

For $d = 2$ the dot product result in [13] in particular implies that if $E \subset \mathbb{F}_q^2$ has size greater than $q^{\frac{3}{2}}$, then the points of E with the third vertex at the origin determines all possible nonzero distinct triangle areas. In [16], using a point-line incidence approach to the area problem, Iosevich et al. prove that if $E \subset \mathbb{F}_q^2$ with $|E| > q$, then $|V_2(E)| \geq \frac{q-1}{2}$ and the triangles giving at least $\frac{q-1}{2}$ distinct areas can be chosen such that they share the same base.

4.3 $\mathbb{Z}_q^d$ Setting:

4.3.1 Dot Product

In [9], the authors prove the following.

Theorem 4.3.1. *Let $E \subset \mathbb{Z}_q^d$, where $q = p^l$. Suppose $|E| \gg lq^{\frac{(2l-1)d}{2l}+\frac{1}{2l}}$. Then,*

$$\prod(E) \supset \mathbb{Z}_q^*.$$

In particular for product sets $E = \underbrace{A \times ... \times A}_{\text{d-fold}} \subset \mathbb{Z}_q^d$, we prove the following:

Theorem 4.3.2. *Let $E = \underbrace{A \times \ldots \times A}_{d\text{-}fold}$ be a subset $\mathbb{Z}_q^d$, where $A \subset \mathbb{Z}_q$, $q = p^l$. Suppose $|E| \geq q^{d(\frac{2l-1}{2l})+\frac{1}{2l}}$. Then $\prod(E) \gtrsim q$.*

Proof. Let

$$\nu(t) = |\{(x, y) \in E \times E : x.y = t\}|.$$

Then by Cauchy-Schwarz inequality,

$$|E|^4 = \left(\sum_{t\in\mathbb{Z}_q} \nu(t)\right)^2 \leq |\prod(E)| \sum_{t\in\mathbb{Z}_q} \nu(t)^2. \tag{4.1}$$

We can write

$$\begin{aligned} \nu(t) &= \sum_{x.y=t} E(x)E(y) \\ &= \sum_{x\in E} \sum_{x.y=t} E(y). \end{aligned}$$

From the Cauchy-Schwarz inequality, it follows that

$$\nu^2(t) \leq |E| \sum_{x\in E} \sum_{x.y=x.y'=t} E(y)E(y')$$

so that

$$\begin{aligned}\sum_t \nu^2(t) &\leq |E| \sum_{x.y=x.y'} E(x)E(y)E(y') \\ &= |E|q^{-1} \sum_s \sum_{x,y,y'} \chi(s(x.y - x.y'))E(x)E(y)E(y') \\ &= \frac{|E|^4}{q} + \sum_{i=0}^{l-1} e_i, \end{aligned} \tag{4.2}$$

where

$$\begin{aligned} e_i &= |E|q^{-1} \sum_{\substack{s \\ \upsilon(s)=i}} \sum_{x,y,y'} \chi(sx(y-y'))E(x)E(y)E(y') \\ &= |E|q^{2d-1} \sum_{\substack{s \\ \upsilon(s)=i}} \sum_x E(x)|\widehat{E}(sx)|^2 \\ &= |E|q^{2d-1} \sum_{s' \in \mathbb{Z}^*_{p^{l-i}}} \sum_x E(x)|\widehat{E}(p^i s'x)|^2 \\ &= |E|q^{2d-1} \sum_{s' \in \mathbb{Z}^*_{p^{l-i}}} \sum_x E(s'x)|\widehat{E}(p^i x)|^2. \end{aligned}$$

Now denoting $l^i_x = \{s'x : s' \in \mathbb{Z}^*_{p^{l-i}}\}$, we can write

$$e_i = |E|q^{2d-1} \sum_x |E \cap l^i_x||\widehat{E}(p^i x)|^2.$$

We note here that $|E \cap l^i_x| \leq |A| = p^\alpha$. To see this, let $x = (x_1, \ldots, x_d)$ and

$$\overline{l^i_x} := \{sx : s \in \mathbb{Z}_{p^{l-i}}\} \supset \{s'x : s' \in \mathbb{Z}^*_{p^{l-i}}\} = l^i_x$$

From the definition, it is clear that $|E \cap l^i_x| \leq |E \cap \overline{l^i_x}|$ and we will show that $|E \cap \overline{l^i_x}| \leq |A|$ where $E = \underbrace{A \times \ldots \times A}_{\text{d-fold}}$.

Note that we can assume that at least one of the coordinates of $x = (x_1, \ldots, x_d)$ is unit. Since otherwise if $val_p(x_j) = n > 0$ is among the smallest, we can write $x = p^n \tilde{x}$ where $\tilde{x} = (\tilde{x_1}, \ldots, \tilde{x_j}, \ldots, \tilde{x_d})$ with $\tilde{x_j}$ is unit and $\overline{l^i_{\tilde{x}}} = \overline{l^i_x}$ gives $|E \cap \overline{l^i_{\tilde{x}}}| = |E \cap \overline{l^i_x}|$.

So we assume that x_j is unit. If $\{s_1x, \ldots, s_tx\} = E \cap \overline{l_x^i}$, then the jth coordinates s_kx_j of the vectors s_kx, $1 \leq k \leq t$, are all different in A. Hence $t \leq |A|$. Thus,

$$|E \cap l_x^i| \leq |E \cap \overline{l_x^i}| = t \leq |A|.$$

Clearly, we also have $|E \cap l_x^i| \leq p^{l-i}$. Therefore $|E \cap l_x^i| \leq min\{p^{l-i}, |A|\}$, and

$$e_i \leq |E|q^{2d-1} \sum_x min\{p^{l-i}, p^\alpha\} |\widehat{E}(p^i x)|^2. \tag{4.3}$$

Now we estimate

$$\begin{aligned} \sum_x |\widehat{E}(p^i x)|^2 &= q^{-2d} \sum_x \sum_{u,v} \chi((u-v)p^i x) E(u)E(v) \\ &= q^{-d} \sum_{(u-v)p^i = 0} E(u)E(v) \end{aligned}$$

For $u = (u_1, \ldots, u_d), v = (v_1, \ldots, v_d) \in \underbrace{A \times \ldots \times A}_{\text{d-fold}}$ if

$$p^i(u-v) = p^i(u_1 - v_1, \ldots, u_d - v_d) = (0, \ldots, 0),$$

then $p^i(u_j - v_j) = 0$ for all $1 \leq j \leq d$. That implies $u_j - v_j \in \{p^{l-i}, 2p^{l-i}, \ldots, p^i p^{l-i}\}$ and we have p^i choices for $u_j - v_j$. If we first fix v_j in $|A|$ different ways, then u_j is uniquely determined. So we have $|A|p^i$ choices for each (u_j, v_j), giving $|A|^d p^{id}$ choices for (u, v).

It follows that

$$\begin{aligned} \sum_x |\widehat{E}(p^i x)|^2 &\leq q^{-d} p^{id} |A|^d \\ &= |E| q^{-d} p^{id} \end{aligned}$$

plugging this value in (4.3) and summing over all $e_i's$ for $i = 0, ..., l-1$, we get

$$\begin{aligned}
\sum_{i=0}^{l-1} e_i &\leq |E|^2 q^{d-1} \sum_{i=0}^{l-1} min\{p^{l-i}, p^{\alpha}\} p^{id} \\
&= |E|^2 q^{d-1} \left(\sum_{i=0}^{l-\alpha} p^{\alpha} p^{id} + \sum_{i=l-\alpha+1}^{l-1} p^{l-i} p^{id} \right) \\
&\lesssim |E|^2 q^{d-1} (p^{\alpha} p^{(l-\alpha)d} + p p^{(l-1)d}) \\
&= |E|^2 q^{d-1} (p^{\alpha+ld-\alpha d} + p^{1+ld-d}) \\
&= |E|^2 q^{d-1} p^{ld} (p^{\alpha(1-d)} + p^{1-d}) \\
&\lesssim |E|^2 q^{d-1} p^{ld} p^{1-d} \\
&= |E|^2 q^{d-1} q^{d} q^{\frac{1-d}{l}} \\
&= |E|^2 q^{2d-1} q^{\frac{1-d}{l}}.
\end{aligned}$$

Plugging this value in (4.2), the inequality (4.1) yields $|\prod(E)| \gtrsim \frac{|E|^4}{|E|^2 q^{2d-1} q^{\frac{1-d}{l}}} \gtrsim q$, whenever $|E|^2 \gtrsim q^{2d+\frac{1-d}{l}}$ i.e. $|E| \gtrsim q^{d(\frac{2l-1}{2l})+\frac{1}{2l}}$. □

4.3.2 Volume Set

We first note the dot product result, Theorem 4.3.1, for $d = 2$ implies that if $|E| \subset \mathbb{Z}_q^2$ with $|E| \gg l q^{2-\frac{1}{2l}}$ then $A(E) \supset \mathbb{Z}_q^*$. Applying an $\mathbb{F}_q^2$ analogous point-line incidence approach, for the subsets of $\mathbb{Z}_q^2$ we have the following result.

Theorem 4.3.3. *Let $E \subset \mathbb{Z}_q^2$ where $q = p^l$. Suppose that $|E| > p^{2l-\frac{1}{2}}$. Then $|V_2(E)| \geq \frac{q}{4}\frac{1+p}{p} - 1$.*

Now before giving the proof, let us introduce the necessary background.

Let $q = p^l$ and $(a, b) \in \mathbb{Z}_q^2$. Let $\langle (a, b) \rangle = \{t(a, b) \colon t \in \mathbb{Z}_q\}$be the submodule of $\mathbb{Z}_q^2$ generated by (a, b), which gives the line through origin and the point (a, b) in $\mathbb{Z}_q^2$. Now, consider the set

$$\Lambda_n = \{(a, b) \in \mathbb{Z}_q^2 : p^n | a, b \text{ but } (a, b) \neq (0, 0) \bmod p^{n+1}\},$$

and denote $|\Lambda_n| = \lambda_n$ for $n = 0, 1, \cdots, l-1$.

Lemma 4.3.1. $\lambda_n = p^{2(l-n)} - p^{2(l-n-1)}$.

Proof. Since $p^n | a, b$ in $\mathbb{Z}_q$ we have p^{l-n} choices for a and b each and hence $p^{2(l-n)}$ choices for (a, b). Now we need to subtract $p^{2(l-n-1)}$ cases where p^{n+1} divides both a and b to get the desired result. □

Lemma 4.3.2. *Let $\mathcal{L}_n = \{\langle (a, b) \rangle : (a, b) \in \Lambda_n\}$ denote the set of lines generated by the points of Λ_n. Then $|\mathcal{L}_n| = p^{l-n} + p^{l-n-1}$.*

Proof. For $(a, b) \in \Lambda_n$, note that $\langle (a, b) \rangle$ is cyclic and $|\langle (a, b) \rangle| = p^{l-n}$. Hence there exist $\phi(p^{l-n}) = p^{l-n} - p^{l-n-1}$ generators of the group which lies in Λ_n. So that for each n, we have

$$\frac{p^{2(l-n)} - p^{2(l-n-1)}}{p^{l-n} - p^{l-n-1}} = p^{l-n} + p^{l-n-1}$$

many lines in $\mathcal{L}_n$ each containing p^{l-n} points. □

We now conclude that the average number of points in a line in $\mathbb{Z}_q^2$ is

$$\begin{aligned} &= \frac{\sum_{n=0}^{l-1} (p^{l-n} + p^{l-n-1}) p^{l-n}}{\sum_{n=0}^{l-1} p^{l-n} + p^{l-n-1}} \\ &= \frac{p^{2l} + p^{2l-1} + p^{2l-2} + \cdots + p^2 + p}{p^l + 2p^{l-1} + 2p^{l-2} + \cdots + 2p + 1} \\ &\sim p^l \end{aligned}$$

In what follows we will only consider $\mathcal{L}_0$, i.e. the set of all lines of full length q in $\mathbb{Z}_q^2$.

Lemma 4.3.3. *For any $(a, b) \in \mathbb{Z}_q^2$ if $(a, b) \in \Lambda_n$, then (a, b) appears in p^n distinct lines in $\mathcal{L}_0$.*

Proof. Say $(a,b) \in \Lambda_n$ and $p^{n+1} \nmid a$. Then (a,b) belongs to the lines generated by $\left(\frac{a}{p^n}, ip^{l-n} + \frac{b}{p^n}\right)$ for $i = 0, ..., p^n - 1$. Note that $i_0 p^{l-n} + \frac{b}{p^n} = i_1 p^{l-n} + \frac{b}{p^n} \bmod p^l$ would imply

$$\begin{aligned} i_0 p^{l-n} &= i_1 p^{l-n} \bmod p^l \\ i_0 &= i_1 \bmod p^n \end{aligned}$$

which is not the case. Hence the given points are all distinct. Since $\frac{a}{p^n}$ is a unit in $\mathbb{Z}_q$, it follows that the lines determined by the given generators are all distinct. □

Lemma 4.3.4. *Let* $R_i = \{(x,y) \in \mathbb{Z}_q^2 \times \mathbb{Z}_q^2 : x - y \in \Lambda_i\}$ *and* $r_i = |R_i|$, *for* $i = 1, ..., l-1$. *Then* $r := r_1 p + r_2 p^2 + ... + r_{l-1} p^{l-1} \leq 2p^{4l-1}$.

Proof. Let $x = (x_1, x_2), y = (y_1, y_2)$ in Z_q^2. Now if $x - y = (x_1 - y_1, x_2 - y_2) \in \Lambda_i$ then $p^i | x_1 - y_1$ and $x_2 - y_2$ but $p^{i+1} \nmid x_1 - y_1$ or $x_2 - y_2$. $p^i | x_1 - y_1$ gives p^{l-i} choices for $x_1 - y_1$ in $\mathbb{Z}_q$, we have q choices for y_1 and y_1 determines x_1 uniquely. Hence we have qp^{l-i} choices for x_1 and y_1. Same argument applies for x_2 and y_2. Altogether the condition $p^i | x_1 - y_1$ and $x_2 - y_2$ gives $qp^{l-i} qp^{l-i}$ choices for $x = (x_1, x_2)$, $y = (y_1, y_2)$.

To exclude the cases where p^{i+1} divides both $x_1 - y_1$ and $x_2 - y_2$ we need to subtract $qp^{l-(i+1)} qp^{l-(i+1)}$ cases of x and y. Hence,

$$r_i = qp^{l-i} qp^{l-i} - qp^{l-i-1} qp^{l-i-1}.$$

Now summing $r_i p^i$'s over all $i = 1, ..., l-1$ we get

$$\begin{aligned} r &= (qp^{l-1} qp^{l-1} - qp^{l-2} qp^{l-2})p \\ &+ (qp^{l-2} qp^{l-2} - qp^{l-3} qp^{l-3})p^2 \\ &\vdots \\ &+ (qpqp - q^2)p^{l-1} \\ &= q^2(p^{2l-1} + p^{2l-2} - p^l - p^{l-1}) \\ &\leq 2q^2 p^{2l-1} = 2p^{4l-1} \end{aligned}$$

□

Proof of Theorem 4.3.3. Let L be a line in $\mathcal{L}_0$ and consider the sum set

$$E + L = \{e + l : e \in E,\, l \in L\}$$

Since $|L||E| > q^2$

$$e_1 + l_1 = e_2 + l_2 \text{ for some } l_1 \neq l_2$$

so that

$$l_2 - l_1 = e_1 - e_2. \tag{4.4}$$

Here we aim to average the solutions of the equation (4.4) over $p^l + p^{l-1}$ lines in $\mathcal{L}_0$. To start with, we count the number of solutions of (4.4) over all lines in $\mathcal{L}_0$ in two cases:

In the case $e_1 = e_2$, there are $|E|$ and q^2 choices for $e_1 = e_2$ and $l_1 = l_2$, respectively.

In the case $e_1 \neq e_2$, we can choose e_1 and e_2 in $|E|(|E| - 1)$ different ways, and once we fix them, we look at the difference $e_1 - e_2$. At that point let $S_i = \{(e_1, e_2) \in E \times E : e_1 - e_2 \in \Lambda_i\}$ and $s_i = |S_i|$ for $i = 0, ...l - 1$. We know from Lemma 4.3.3 that if $(e_1, e_2) \in S_i$, then $e_1 - e_2$ lies on p^i lines in $\mathcal{L}_0$ and when we fix the line, $l_2 - l_1$ can be written q different ways on that line. In other words, for all s_i pairs $(e_1, e_2) \in S_i$, l_1, l_2 is chosen $p^i q$ different ways over the lines in $\mathcal{L}_0$.

So altogether we have

$$\begin{aligned}
& |\{(e_1, e_2, l_1, l_2) \in E \times E \times L \times L : \text{ (4.4) holds for some } L \in \mathcal{L}_0\}| \\
= \;& |E|q^2 + s_0 q + s_1 pq + s_2 p^2 q + ... + s_{l-1} p^{l-1} q \\
\leq \;& |E|^2 q + (s_0 + s_1 p + s_2 p^2 + ... + s_{l-1} p^{l-1}) q \\
= \;& |E|^2 q + (|E|^2 + s) q
\end{aligned}$$

where $s = s_1 p + s_2 p^2 + ... + s_{l-1} p^{l-1}$. Note that $s \leq r \leq 2p^{4l-1} \leq 2|E|^2$ by Lemma 4.3.4 and the assumption on the size of E.

Hence we get,

$$|\{(e_1, e_2, l_1, l_2) \in E \times E \times L \times L : \text{ (4.4) holds for some } L \in \mathcal{L}_0\}| \leq 4|E|^2 q$$

It follows that there exists a $L \in \mathcal{L}_0$ such that

$$\begin{aligned} |\{(e_1, e_2, l_1, l_2) \in E \times E \times L \times L : \text{ (4.4) holds}\}| &\leq 4|E|^2 \frac{p^l}{p^l + p^{l-1}} \\ &= 4|E|^2 \frac{p}{1+p}. \end{aligned}$$

If we let $\nu(n)$ denote the number of representation of n as $e + l$ for some $e \in E$, $l \in L$, then by Cauchy-Schwarz, for this particular L,

$$\begin{aligned} |E|^2 |L|^2 &= \left(\sum_{n \in E+L} \nu(n) \right)^2 \\ &\leq |E+L| \sum_{n \in E+L} \nu^2(n) \\ &= |E+L| |\{(e_1, e_2, l_1, l_2) \in E \times E \times L \times L : \text{ (4.4) holds}\}|. \end{aligned}$$

Hence,

$$\begin{aligned} |E+L| &\geq \frac{|E|^2 |L|^2}{|\{(e_1, e_2, l_1, l_2) \in E \times E \times L \times L : \text{ (4.4) holds}\}|} \\ &\geq \frac{|E|^2 p^{2l}}{4|E|^2 \frac{p}{1+p}} = \frac{q^2}{4} \frac{1+p}{p}. \end{aligned}$$

We conclude that there exist points of E in at least $\frac{q}{4}\frac{1+p}{p}$ parallel lines. Here we shall note that there are totally q parallel lines to L, including itself, and one of them must contain two points of E with a unit distance in between. For otherwise, on each of these parallel lines there would be at most p^{l-1} points of E yielding $|E| \leq qp^{l-1} = p^{2l-1}$ which is not the case. It follows that points of E determines at least $\frac{q}{4}\frac{1+p}{p} - 1$ distinct triangle areas with the same unit base on one of the parallel lines and with the third vertex being on $\frac{q}{4}\frac{1+p}{p} - 1$ different parallel lines.

□

5 Permutation Polynomials over $\mathbb{F}_q$

Permutation polynomials (PPs) over finite fields play an important role in combinatorics, cryptograph and coding theory. More specifically, they are used for construction of several combinatorial designs, generating pseudorandom sequences by recursive procedures, and enhancing secure transmission of data. Although permutation polynomials have been studied for long, there are still many open problems regarding the subject. For a detailed literature on this subject we refer to [17] and [19]. In this chapter, we intend to introduce some basic facts about PPs first, and then present the Carlitz rank construction described in [2].

Definition 5.0.1. *Let $\mathbb{F}_q$ be a finite field of q elements, where $q = p^n$, p is a prime and n is a positive integer. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a PP of $\mathbb{F}_q$ if the induced map $\alpha \to f(\alpha)$ from $\mathbb{F}_q$ to itself is bijective.*

Given a permutation σ of the elements of $\mathbb{F}_q$, there exists a unique polynomial $f_\sigma \in \mathbb{F}_q[x]$ with $deg(f_\sigma) < q$ and $f_\sigma(c) = \sigma(c)$ for all $c \in \mathbb{F}_q$. The polynomial f_σ can be given by the formula

$$f_\sigma(x) = \sum_{c \in \mathbb{F}_q} \sigma(c)(1 - (x - c)^{q-1}). \tag{5.1}$$

or by the Lagrange interpolation formula, see for instance [17]. From (5.1), we note that $deg(f_\sigma) \leq q - 2$, since all elements of $\mathbb{F}_q$ sum up to zero.

Consider an (arbitrary) polynomial $f \in \mathbb{F}_q[x]$. One can associate f to the reduction polynomial $g \in \mathbb{F}_q[x]$ by taking f mod $(x^q - x)$, since g and f induce the same map over $\mathbb{F}_q$, as stated in the following lemma.

Lemma 5.0.5. *For $f, g \in \mathbb{F}_q[x]$, $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if $f(x) \equiv g(x)$ mod $(x^q - x)$.*

Proof. Using division algorithm we have, $f(x) - g(x) = h(x)(x^q - x) + r(x)$ for some $h, r \in \mathbb{F}_q[x]$ with $deg(r) < q$. Substituting c for x, we get $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if $r(c) = 0$ for all $c \in \mathbb{F}_q$, which is equivalent to $r = 0$. □

Definition 5.0.2. Let n be a positive integer. The set of all one-to-one mappings, i.e. permutations, from the set $\{1, 2, ..., n\}$ onto $\{1, 2, ..., n\}$ forms a group under the composition. This group is called the *symmetric group* of *degree* n, and denoted by S_n.

Let $S = \{f(x) |\ f(x)$ is a PP of $\mathbb{F}_q\}$. Define an operation "." on the set S in such a way that $g(x).f(x) = h(x)$ whenever $f(g(x)) \equiv h(x)$ mod $(x^q - x)$. Under this operation $(S, .)$ is a group and it is isomorphic to the symmetric group S_q.

Theorem 5.0.4. *For $q > 2$, S_q is generated by x^{q-2} and all (non-constant) linear polynomials over $\mathbb{F}_q$.*

Proof. Note that the polynomial $f_a(x) = -a^2(((x - a)^{q-2} + a^{-1})^{q-2} - a)^{q-2}$ represents the transposition $(0a)$, $a \in \mathbb{F}_q^*$. Since every permutation of $\mathbb{F}_q$ is a product of transpositions and every transposition (bc) can be written as a product $(0b)(0c)(0b)$, we conclude the proof. □

Hence, as pointed out in [10], any permutation (or permutation polynomial) of a finite field $\mathbb{F}_q$ can be represented by a polynomial of the form

$$\mathcal{P}_n(x) = (\ldots((a_0x + a_1)^{q-2} + a_2)^{q-2} \ldots + a_n)^{q-2} + a_{n+1},\ n \geq 0, \tag{5.2}$$

where $a_1, a_{n+1} \in \mathbb{F}_q, a_i \in \mathbb{F}_q^*$ for $i = 0, 2, \ldots, n$.

Here, we make the following convention for $\mathcal{P}_n(x)$. We put $\mathcal{P}_n = P_n$ or $\bar{P}_n$ in the cases $a_{n+1} = 0$ or $a_{n+1} \neq 0$, respectively. Obviously, in both cases n is the number of times x^{q-2} occurs in the representation (5.2).

For the polynomial $\mathcal{P}_n(x)$, we consider the rational function

$$r_n(x) = (\ldots((a_0x + a_1)^{-1} + a_2)^{-1} \ldots + a_n)^{-1} + a_{n+1},$$

and we have the following lemma accordingly.

Lemma 5.0.6. *$r_n(x)$ with its continued fraction expansion*

$$a_{n+1} + 1/(a_n + 1/(\ldots + a_2 + 1/(a_0x + a_1)\ldots)),$$

can be represented by the n'th convergent

$$\mathcal{R}_n(x) = \frac{\alpha_{n+1}x + \beta_{n+1}}{\alpha_n x + \beta_n}, \tag{5.3}$$

where the α_k and the β_k are given recursively by

$$\alpha_k = a_k\alpha_{k-1} + \alpha_{k-2} \quad \textit{and} \quad \beta_k = a_k\beta_{k-1} + \beta_{k-2}, \tag{5.4}$$

for $k \geq 2$, with initial values $\alpha_0 = 0, \alpha_1 = a_0, \beta_0 = 1, \beta_1 = a_1$. Note that α_k and β_k cannot both be zero.

Proof. The proof proceeds by induction. First note that

$$\mathcal{R}_1(x) = a_2 + \frac{1}{a_0x + a_1} = \frac{\alpha_2 x + \beta_2}{\alpha_1 x + \beta_1},$$

where $\alpha_2 = a_2a_0, \beta_2 = a_2a_1 + 1, \alpha_1 = a_0, \beta_1 = a_1$. Now assuming the assertion for $\mathcal{R}_{k-2}$, we have

$$\begin{aligned} \mathcal{R}_{k-1} &= a_k + \frac{1}{R_{k-2}} = a_k + \frac{1}{\frac{\alpha_{k-1}x+\beta_{k-1}}{\alpha_{k-2}x+\beta_{k-2}}} \\ &= a_k + \frac{\alpha_{k-2}x + \beta_{k-2}}{\alpha_{k-1}x + \beta_{k-1}} = \frac{\alpha_k x + \beta_k}{\alpha_{k-1}x + \beta_{k-1}}, \end{aligned}$$

where $\alpha_k = a_k\alpha_{k-1} + \alpha_{k-2}$ and $\beta_k = a_k\beta_{k-1} + \beta_{k-2}$. □

Note that when $a_{n+1} = 0$, $\mathcal{R}_n$ reduces to $(\alpha_{n-1}x+\beta_{n-1})/(\alpha_n x+\beta_n)$, as $\alpha_{n+1} = \alpha_{n-1}$ and $\beta_{n+1} = \beta_{n-1}$ in this case.

We define the set of *poles*, $\mathbf{O}_n$, as

$$\mathbf{O}_n = \{x_i : x_i = \frac{-\beta_i}{\alpha_i}, i = 1, \ldots, n\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}. \tag{5.5}$$

and the string of *poles* as $\mathcal{O}_n$:

$$\mathcal{O}_n = (x_i)_{i=1}^n = (x_1, x_2, \ldots, x_n).$$

Observe that a rational function $R(x) = \frac{ax+b}{cx+d}$, $c \neq 0$, is onto from $\mathbb{F}_q \setminus \{-d/c\}$ to $\mathbb{F}_q \setminus \{a/c\}$ so for every rational function $\mathcal{R}_n(x)$ in the form (5.3) we can define a corresponding permutation $\mathcal{F}_n(x)$ via $\mathcal{F}_n(x) = \mathcal{R}_n(x)$ for $x \neq x_n = \frac{-\beta_n}{\alpha_n}$ and $\mathcal{F}_n(x_n) = \frac{\alpha_{n+1}}{\alpha_n}$ when $x_n \in \mathbb{F}_q$.

As for $\mathcal{P}_n$, we distinguish two cases for $\mathcal{R}_n$ and $\mathcal{F}_n$ and write $\mathcal{R}_n(x) = R_n(x)$, $\mathcal{F}_n(x) = F_n(x)$ for $a_{n+1} = 0$, and $\mathcal{R}_n(x) = \bar{R}_n(x)$, $\mathcal{F}_n(x) = \bar{F}_n(x)$ for $a_{n+1} \neq 0$

An easy observation yields that

$$\mathcal{P}_n(x) = \mathcal{F}_n(x) \textit{ for all } x \in \mathbb{F}_q \setminus \mathbf{O}_n.$$

We will explore how $\mathcal{P}_n$ and $\mathcal{F}_n$ differs from each other for the elements in $\mathbf{O}_n$ subsequently. We will first state the following observation.

Lemma 5.0.7. *Let $\mathcal{P}_m(x) = \mathcal{P}_n(x)$ on $\mathbb{F}_q$, with associated rational functions $\mathcal{R}_m(x)$ and $\mathcal{R}_n(x)$, respectively. If $m + n < q - 2$, then $\mathcal{R}_m(x) = \mathcal{R}_n(x)$.*

Proof. Let $\mathcal{F}_m(x)$ and $\mathcal{F}_n(x)$ be the permutations corresponding to $\mathcal{P}_m(x)$ and $\mathcal{P}_n(x)$ respectively. Then $\mathcal{F}_m(x)$ differs from $\mathcal{P}_m(x)$ for at most m elements, and $\mathcal{F}_n(x)$ differs from $\mathcal{P}_n(x)$ for at most n elements of $\mathbb{F}_q$. Since $\mathcal{P}_m(x) = \mathcal{P}_n(x)$ on $\mathbb{F}_q$, $\mathcal{F}_m(x) = \mathcal{F}_n(x)$ for at least $q - m - n$ elements of $\mathbb{F}_q$. We know that if $\mathcal{F}_m(x) \neq \mathcal{F}_n(x)$, then $\mathcal{F}_m(x) = \mathcal{F}_n(x)$ has at most two solutions on $\mathbb{F}_q$. Thus, $q - m - n > 2$ implies $\mathcal{F}_m = \mathcal{F}_n$. □

In sequel, for a cycle $\tau \in S_q$, the length of τ will be denoted by $l(\tau)$, and $\text{supp}(\tau) := \{a : \tau(a) \neq a\}$ will denote the elements of $\mathbb{F}_q$ that are not fixed by τ.

Suppose that the permutation $P_n(x)$ can be decomposed into $F_n(x)$ and m disjoint cycles $\tau_1^{(n)} \dots \tau_m^{(n)}$, that is,

$$P_n(x) = \tau_1^{(n)} \dots \tau_m^{(n)} F_n(x), \tag{5.6}$$

where $l(\tau_i^{(n)}) \geq 2$, and $\tau_i^{(n)} = (F_n(x_1^i) \dots F_n(x_{l_i}^i))$, for $1 \leq i \leq m$.

We define the set $\overline{\mathbf{O}}_n$ as

$$\overline{\mathbf{O}}_n = \{y \in \mathbf{O}_{n-1} : F_n(y) \in \text{supp}(\tau_i^{(n)}) \text{ for some } 1 \leq i \leq m\} \cup \{x_n\}$$

if $x_n \in \mathbb{F}_q$. $\overline{\mathbf{O}}_n$ does not contain x_n if $x_n = \infty$.

Theorem 5.0.5. *Let $P_{n-1}(x)$ be given by*

$$P_{n-1}(x) \;=\; \tau_1^{(n-1)} \dots \tau_m^{(n-1)} F_{n-1}(x), \tag{5.7}$$

where

1. *$\tau_1^{(n-1)}, \dots, \tau_m^{(n-1)}$ are disjoint cycles.*
2. *If $P_{n-1}(x_{n-1}) = F_{n-1}(x_{n-1})$ we assume that $\tau_1^{(n-1)} = (F_{n-1}(x_{n-1}))$ and $l(\tau_i^{(n-1)}) = l_i \geq 2$, for $2 \leq i \leq m$.*
3. *If $P_{n-1}(x_{n-1}) \neq F_{n-1}(x_{n-1})$ by permuting the cycles if necessary, we assume that $F_{n-1}(x_{n-1}) \in \text{supp}(\tau_1^{(n-1)})$ with $x_1^1 = x_{n-1}$, and $l(\tau_i^{(n-1)}) = l_i \geq 2$, for $1 \leq i \leq m$.*

Assuming $x_{n-1}, x_n \in \mathbb{F}_q$, we have

$$P_n(x) = (F_n(x_n)F_n(x_{n-1}))\tau_1^{(n)} \dots \tau_m^{(n)} F_n(x).$$

Proof. We consider three cases:

Case 1: Suppose that $F_{n-1}(x_n)$ is not in $\mathrm{supp}(\tau_i^{(n-1)})$ for any $i = 1, \ldots m$ in the decomposition (5.7), i.e. $x_n \notin \overline{\mathbf{O}}_{n-1}$. we need to show the following three properties:

(i) If $x \notin \overline{\mathbf{O}}_{n-1}$ and $x \neq x_n$, then $P_n(x) = F_n(x)$.

(ii) If $y \in \overline{\mathbf{O}}_{n-1}$ satisfies $y \neq x_{l_1}^1$, and $P_{n-1}(y) = F_{n-1}(y')$, then $P_n(y) = F_n(y')$.

(iii) $P_n(x_{l_1}^1) = F_n(x_n)$, and $P_n(x_n) = F_n(x_{n-1})$.

(i) If $x \notin \overline{\mathbf{O}}_{n-1}$, then $P_{n-1}(x) = F_{n-1}(x)$. Since $x \neq x_{n-1},\ x_n$, we have

$$\begin{aligned} P_n(x) &= (P_{n-1}(x) + a_n)^{q-2} = \left(\frac{\alpha_{n-2}x + \beta_{n-2}}{\alpha_{n-1}x + \beta_{n-1}} + a_n\right)^{q-2} \\ &= \left(\frac{(a_n\alpha_{n-1} + \alpha_{n-2})x + a_n\beta_{n-1} + \beta_{n-2}}{\alpha_{n-1}x + \beta_{n-1}}\right)^{q-2} \\ &= \left(\frac{\alpha_n x + \beta_n}{\alpha_{n-1}x + \beta_{n-1}}\right)^{q-2} = \frac{\alpha_{n-1}x + \beta_{n-1}}{\alpha_n x + \beta_n} = F_n(x). \end{aligned}$$

This proves (i).

(ii) Let $P_{n-1}(y) = F_{n-1}(y')$. Then

$$\begin{aligned} P_n(y) &= (P_{n-1}(y) + a_n)^{q-2} = (F_{n-1}(y') + a_n)^{q-2} \\ &= \left(\frac{\alpha_{n-2}y' + \beta_{n-2}}{\alpha_{n-1}y' + \beta_{n-1}} + a_n\right)^{q-2} = \left(\frac{\alpha_n y' + \beta_n}{\alpha_{n-1}y' + \beta_{n-1}}\right)^{q-2} \\ &= \frac{\alpha_{n-1}y' + \beta_{n-1}}{\alpha_n y' + \beta_n} = F_n(y'). \end{aligned}$$

(iii)

$$\begin{aligned} P_n(x_{l_1}^1) &= (P_{n-1}(x_{l_1}^1) + a_n)^{q-2} = (F_{n-1}(x_{n-1}) + a_n)^{q-2} \\ &= \left(\frac{\alpha_{n-2}}{\alpha_{n-1}} + a_n\right)^{q-2} = \left(\frac{a_n\alpha_{n-1} + \alpha_{n-2}}{\alpha_{n-1}}\right)^{q-2} \\ &= \frac{\alpha_{n-1}}{\alpha_n} = F_n(x_n) \ \text{ and} \end{aligned}$$

$$\begin{aligned} P_n(x_n) &= (P_{n-1}(x_n)+a_n)^{q-2} = (F_{n-1}(x_n)+a_n)^{q-2} \\ &= \left(\frac{\alpha_{n-2}x_n+\beta_{n-2}}{\alpha_{n-1}x_n+\beta_{n-1}}+a_n\right)^{q-2} \\ &= \left(\frac{(a_n\alpha_{n-1}+\alpha_{n-2})x_n+a_n\beta_{n-1}+\beta_{n-2}}{\alpha_{n-1}x_n+\beta_{n-1}}\right)^{q-2} \\ &= \left(\frac{\alpha_n x_n+\beta_n}{\alpha_{n-1}x_n+\beta_{n-1}}\right)^{q-2} = 0 = F_n(x_{n-1}), \end{aligned}$$

where in the last step we used

$$F_n(x_{n-1}) = \frac{\alpha_{n-1}x_{n-1}+\beta_{n-1}}{\alpha_n x_{n-1}+\beta_n} = 0.$$

Case 2: Suppose that $F_{n-1}(x_n) \in \mathrm{supp}(\tau_1^{(n-1)})$, say $x_n = x_r^1$, i.e.

$$\tau_1^{(n-1)} = (F_{n-1}(x_{n-1}) \ \ldots \ F_{n-1}(x_{r-1}^1)\ F_{n-1}(x_n^1) \ \ldots \ F_{n-1}(x_{l_1}^1)).$$

In this case we need to show the following:

(i) If $x \notin \overline{\mathbf{O}}_{n-1}$ then $P_n(x) = F_n(x)$.

(ii) If $y \in \overline{\mathbf{O}}_{n-1}$ satisfies $y \neq x_{l_1}^1, x_{r-1}^1$, and $P_{n-1}(y) = F_{n-1}(y')$, then $P_n(y) = F_n(y')$.

(iii) $P_n(x_{l_1}^1) = F_n(x_n)$, and $P_n(x_{r-1}^1) = F_n(x_{n-1})$.
Note that (i), (ii) and the first statement of (iii) can be shown as in Case (1), so we will only show $P_n(x_{r-1}^1) = F_n(x_{n-1})$:

$$\begin{aligned} P_n(x_{r-1}^1) &= (P_{n-1}(x_{r-1}^1)+a_n)^{q-2} = (F_{n-1}(x_n)+a_n)^{q-2} \\ &= \left(\frac{\alpha_{n-2}x_n+\beta_{n-2}}{\alpha_{n-1}x_n+\beta_{n-1}}+a_n\right)^{q-2} = \left(\frac{\alpha_n x_n+\beta_n}{\alpha_{n-1}x_n+\beta_{n-1}}\right)^{q-2} \\ &= 0 = F_n(x_{n-1}). \end{aligned}$$

Case 3: Lastly, suppose that $F_{n-1}(x_n)$ is in the support of a cycle in (5.7), other than the first one, say in $\mathrm{supp}(\tau_2^{n-1})$ and $x_n = x_s^2$. We need to show:

(i) If $x \notin \overline{\mathbf{O}}_{n-1}$, then $P_n(x) = F_n(x)$.

(ii) If $y \in \overline{\mathbf{O}}_{n-1}$ satisfies $y \neq x^1_{l_1}, x^2_{s-1}$, and $P_{n-1}(y) = F_{n-1}(y')$, then $P_n(y) = F_n(y')$.

(iii) $P_n(x^1_{l_1}) = F_n(x_n)$, and $P_n(x^2_{s-1}) = F_n(x_{n-1})$.

The proofs are same as that of (i), (ii) in Case 1, and (iii) in Case 2.

□

Corollary 5.0.1. *Let $x_{n-1}, x_n \in \mathbb{F}_q$. Let*

$$\mathcal{P}_{n-1}(x) \;=\; \tau_1^{(n-1)} \dots \tau_m^{(n-1)} \mathcal{F}_{n-1}(x) \tag{5.8}$$

where

1. *$\tau_1^{(n-1)}, \dots, \tau_m^{(n-1)}$ are disjoint cycles.*
2. *If $\mathcal{P}_{n-1}(x_{n-1}) \neq \mathcal{F}_{n-1}(x_{n-1})$ we assume without loss of generality that $\mathcal{F}_{n-1}(x_{n-1}) \in \mathrm{supp}(\tau_1^{(n-1)})$ with $x^1_1 = x_{n-1}$, and $l(\tau_i^{(n-1)}) = l_i \geq 2$, for $1 \leq i \leq m$.*
3. *If $\mathcal{P}_{n-1}(x_{n-1}) = \mathcal{F}_{n-1}(x_{n-1})$ we assume without loss of generality that $\tau_1^{(n-1)} = (\mathcal{F}_{n-1}(x_{n-1}))$ and $l(\tau_i^{(n-1)}) = l_i \geq 2$, for $2 \leq i \leq m$.*

Then $\mathcal{P}_n(x)$ can be decomposed as follows:

(i) If $x_n \notin \overline{\mathbf{O}}_{n-1}$ then

$$\mathcal{P}_n(x) = (\mathcal{F}_n(x_n)\mathcal{F}_n(x_{n-1}) \dots \mathcal{F}_n(x^1_{l_1}))\tau_2^{(n)} \dots \tau_m^{(n)} \mathcal{F}_n(x), \tag{5.9}$$

(ii) if $\mathcal{F}_{n-1}(x_n) \in \mathrm{supp}(\tau_1^{(n-1)})$, say $x_n = x^1_r$, then

$$\mathcal{P}_n(x) = (\mathcal{F}_n(x_n)\mathcal{F}_n(x^1_{r+1}) \dots \mathcal{F}_n(x^1_{l_1}))\ (\mathcal{F}_n(x_{n-1})\mathcal{F}_n(x^1_2) \dots \mathcal{F}_n(x^1_{r-1}))\tau_2^{(n)} \dots \tau_m^{(n)} \mathcal{F}_n(x), \tag{5.10}$$

(iii) if $\mathcal{F}_{n-1}(x_n) \in \mathrm{supp}(\tau_i^{(n-1)})$, $j \neq 1$, say in $\mathrm{supp}(\tau_2^{(n-1)})$ and $x_n = x^2_s$, then

$$\begin{aligned} \mathcal{P}_n(x) \;=\; & (\mathcal{F}_n(x^2_s)\mathcal{F}_n(x^2_{s+1}) \dots \mathcal{F}_n(x^2_{l_2})\mathcal{F}_n(x^2_1) \dots \mathcal{F}_n(x^2_{s-1})\mathcal{F}_n(x^1_1) \dots \mathcal{F}_n(x^1_{l_1})) \\ & \tau_3^{(n)} \dots \tau_m^{(n)} \mathcal{F}_n(x). \end{aligned}$$

Theorem 5.0.6. *Suppose P_{n-1} can be decomposed as*

$$P_{n-1}(x) \;=\; \tau_1^{(n-1)} \dots \tau_m^{(n-1)} F_{n-1}(x).$$

Let $x_n = \infty$. Then

$$\begin{aligned} P_n(x) &= \tau_1^{(n)} \dots \tau_m^{(n)} F_n(x) \\ P_{n+1}(x) &= \tau_1^{(n+1)} \dots \tau_m^{(n+1)} F_{n+1}(x), \text{ and} \\ P_{n+2}(x) &= (F_{n+2}(x_{n+2}) F_{n+2}(x_{n+1})) \tau_1^{(n+2)} \dots \tau_m^{(n+2)} F_{n+2}(x), \end{aligned}$$

where $\tau_i^{(k)}$ denotes the cycle $(F_k(x_1^i) \dots F_k(x_{l_i}^i))$ as before.

Proof. To prove the first two equalities it is sufficient to show the following properties:

(i) If $x \notin \overline{\mathbf{O}}_{n-1}$, then $P_n(x) = F_n(x)$ and$P_{n+1}(x) = F_{n+1}(x)$.

(ii) If $y \in \overline{\mathbf{O}}_{n-1}$ satisfies $P_{n-1}(y) = F_{n-1}(y')$, then $P_n(y) = F_n(y')$ and $P_{n+1}(y) = F_{n+1}(y')$.

(i) Suppose that $x \notin \overline{\mathbf{O}}_{n-1}$. Then $P_{n-1}(x) = F_{n-1}(x)$, and

$$\begin{aligned} P_n(x) &= (P_{n-1}(x) + a_n)^{q-2} = \left(\frac{\alpha_{n-2} x + \beta_{n-2}}{\alpha_{n-1} x + \beta_{n-1}} + a_n \right)^{q-2} \\ &= \left(\frac{(a_n \alpha_{n-1} + \alpha_{n-2}) x + a_n \beta_{n-1} + \beta_{n-2}}{\alpha_{n-1} x + \beta_{n-1}} \right)^{q-2} \\ &= \left(\frac{\alpha_n x + \beta_n}{\alpha_{n-1} x + \beta_{n-1}} \right)^{q-2} = \frac{\alpha_{n-1} x + \beta_{n-1}}{\alpha_n x + \beta_n} = F_n(x). \end{aligned}$$

For $x \notin \overline{\mathbf{O}}_{n-1}$ and $x \neq x_{n+1}$ the equality $P_{n+1}(x) = F_{n+1}(x)$ also follows as above. Finally

$$\begin{aligned} P_{n+1}(x_{n+1}) &= (P_n(x_{n+1}) + a_n)^{q-2} = \left(\frac{\alpha_{n-1} x_{n+1} + \beta_{n-1}}{\alpha_n x_{n+1} + \beta_n} + a_n \right)^{q-2} \\ &= \left(\frac{(a_n \alpha_n + \alpha_{n-1}) x_{n+1} + a_n \beta_n + \beta_{n-1}}{\alpha_n x_{n+1} + \beta_n} \right)^{q-2} \\ &= \left(\frac{\alpha_{n+1} x_{n+1} + \beta_{n+1}}{\alpha_n x_{n+1} + \beta_n} \right)^{q-2} = 0 = F_{n+1}(x_{n+1}), \end{aligned}$$

where in the last step we used $F_{n+1}(x_{n+1}) = \frac{\alpha_n}{\alpha_{n+1}} = 0$.

(ii) If $y \in \overline{\mathbf{O}}_{n-1}$ and $P_{n-1}(y) = F_{n-1}(y')$, then

$$\begin{aligned} P_n(y) &= (P_{n-1}(y) + a_n)^{q-2} = (F_{n-1}(y') + a_n)^{q-2} \\ &= \left(\frac{\alpha_{n-2}y' + \beta_{n-2}}{\alpha_{n-1}y' + \beta_{n-1}} + a_n\right)^{q-2} = \left(\frac{\alpha_n y' + \beta_n}{\alpha_{n-1}y' + \beta_{n-1}}\right)^{q-2} \\ &= \frac{\alpha_{n-1}y' + \beta_{n-1}}{\alpha_n y' + \beta_n} = F_n(y'). \end{aligned}$$

The identity $P_{n+1}(y) = F_{n+1}(y')$ for $y' \neq x_{n+1}$ follows analogously. Finally for $y' = x_{n+1}$ we get

$$P_{n+1}(y) = 0 = F_{n+1}(y')$$

since in this case

$$F_{n+1}(y') = F_{n+1}(x_{n+1}) = \frac{\alpha_n}{\alpha_{n+1}} = 0.$$

The statement for P_{n+2} follows then from Theorem 5.0.5. □

Corollary 5.0.2. *Let $\mathcal{O}_n = x_1, x_2, \ldots, x_n$ be the string of poles of $\mathcal{P}_n$.*
If $x_t \neq \infty$, $1 \leq t \leq n$, then

$$\mathcal{P}_n(x) = (\mathcal{F}_n(x_n)\mathcal{F}_n(x_{n-1}))(\mathcal{F}_n(x_{n-1})\mathcal{F}_n(x_{n-2}))\ldots(\mathcal{F}_n(x_2)\mathcal{F}_n(x_1))\mathcal{F}_n(x).$$

If $x_{t_j} = \infty$ for some integers $3 \leq t_j \leq n$ and $s \leq n$ is the largest integer such that $x_{s-1}, x_s \neq \infty$, then

$$\begin{aligned} \mathcal{P}_n(x) &= (\mathcal{F}_n(x_s)\mathcal{F}_n(x_{s-1}))\ldots(\mathcal{F}_n(x_{t_j+2})\mathcal{F}_n(x_{t_j+1}))(\mathcal{F}_n(x_{t_j-1})\mathcal{F}_n(x_{t_j-2})) \\ &\quad \ldots(\mathcal{F}_n(x_2)\mathcal{F}_n(x_1))\mathcal{F}_n(x). \end{aligned}$$

Remark 5.0.1. *Given a permutation*

$$\mathcal{P}_n(x) = (\ldots((a_0x + a_1)^{q-2} + a_2)^{q-2}\ldots + a_n)^{q-2} + a_{n+1},\ n \geq 0,$$

where $a_1, a_{n+1} \in \mathbb{F}_q, a_i \in \mathbb{F}_q^*$ for $i = 0, 2, \ldots, n$, we can compute the α_k and the β_k, $i = 2, \ldots n+1$, recursively from

$$\alpha_k = a_k\alpha_{k-1} + \alpha_{k-2},\ \beta_k = a_k\beta_{k-1} + \beta_{k-2},$$

with the initial values $\alpha_0 = 0,\ \alpha_1 = a_0,\ \beta_0 = 1,\ \beta_1 = a_1$. *Subsequently, we get the string of poles* $\mathcal{O}_n = (x_i)_{i=1}^n$, $\mathcal{R}_n(x) = \frac{\alpha_{n+1}x+\beta_{n+1}}{\alpha_n x+\beta n}$, *and the corresponding permutation* $\mathcal{F}_n(x)$. *Corollaries 5.0.1 and 5.0.2 then gives the decomposition of* $\mathcal{P}_n(x)$ *as a product of cycles and* $\mathcal{F}_n(x)$.

On the other hand, given $\mathcal{R}_n(x)$ *(or the corresponding* $\mathcal{F}_n(x)$*) with a string of poles* $\mathcal{O}_n \subset \mathbb{P}^1(\mathbb{F}_q)$ *we can construct the permutation* $\mathcal{P}_n$ *as follows:*

Let $\mathcal{R}_n(x) = \frac{ax+b}{cx+d} = \frac{\epsilon ax+\epsilon b}{\epsilon cx+\epsilon d}$, $\epsilon \neq 0$, *so that*

$$\alpha_{n+1} = \epsilon a, \beta_{n+1} = \epsilon b, \alpha_n = \epsilon c, \beta_n = \epsilon d.$$

Then if $x_{k-2} \neq \infty$, *from* $x_{k-2} = \frac{-\beta_{k-2}}{\alpha_{k-2}} = \frac{-(\beta_k - a_k\beta_{k-1})}{\alpha_k - a_k\alpha_{k-1}}$ *we get*

$$\begin{aligned} x_{k-2}\alpha_k - a_k x_{k-2}\alpha_{k-1} &= -\beta_k + a_k\beta_{k-1} \\ \beta_k + x_{k-2}\alpha_k &= a_k(\beta_{k-1} + x_{k-2}\alpha_{k-1}) \\ a_k &= \frac{\beta_k + x_{k-2}\alpha_k}{\beta_{k-1} + x_{k-2}\alpha_{k-1}}, \end{aligned}$$

and if $x_{k-2} = \infty$, *i.e.* $\alpha_{k-2} = 0$, *then* $\alpha_k = a_k\alpha_{k-1}$ *hence* $a_k = \frac{\alpha_k}{\alpha_{k-1}}$ *for* $3 \leq k \leq n+1$. *Therefore we can get* a_k *as a multiple of* ϵ , $3 \leq k \leq n+1$, *from its recursive formulation here. Since* $\alpha_2 = a_2\alpha_1 + \alpha_0$, $a_2 = \frac{\alpha_2}{\alpha_1}$. *Now* a_2 *can be used to determine* ϵ *for* $\beta_2 = a_2\beta_1 + \beta_0 = a_2\beta_1 + 1$. *Knowing* $a_1 = \beta_1$ *and* $a_0 = \alpha_1$, *the complete formulation of* $\mathcal{P}_n$ *is constructed.*

5.1 Carlitz rank of a permutation polynomial

Note that given a permutation $p(x)$ of $\mathbb{F}_q$, $p(x)$ can be represented by a polynomial of the form $\mathcal{P}_n(x)$ as in (5.2) but this representation may not be unique. Accordingly, we can define the Carlitz rank of a permutation polynomial as follows.

Definition 5.1.1. *Let* $p(x)$ *be a permutation of* $\mathbb{F}_q$.*The smallest* n *satisfying* $p(x) = \mathcal{P}_n(x)$ *for all* $x \in \mathbb{F}_q$, *where* $\mathcal{P}_n(x)$ *is of the form (5.2), is called the Carlitz rank of* $p(x)$ *and denoted by* $\mathrm{Crk}(p)$.

We should note here that if Crk(p)=n, then $p(x)$ is composed of at least n "*inversions*" x^{q-2} with n (or $n+1$) linear polynomials.

Theorem 5.1.1. *Let $\mathcal{P}_s(x)$ be given by*

$$\mathcal{P}_s(x) = \tau_1 \dots \tau_m \mathcal{F}_s(x)$$

where τ_i are disjoint cycles of length $l_i \geq 2$, for $i = 1, \dots m$. Then we have one of the following three cases:

(i) If $\mathcal{F}_s$ is not linear, and $\mathcal{F}_s(x_s) \in \text{supp}(\tau_i)$ for some $1 \leq i \leq m$, then there exists a permutation $\mathcal{P}_n$ with $n = m + \sum_{i=1}^{m} l_i - 1$ and $\mathcal{P}_s(x) = \mathcal{P}_n(x)$ on $\mathbb{F}_q$.

(ii) If $\mathcal{F}_s$ is not linear, and $\mathcal{F}_s(x_s) \notin \text{supp}(\tau_i)$ for any $i = 1, \dots, m$, then there exists a permutation $\mathcal{P}_n$ with $n = m + \sum_{i=1}^{m} l_i + 1$ and $\mathcal{P}_s(x) = \mathcal{P}_n(x)$ on $\mathbb{F}_q$.

(iii) If $\mathcal{F}_s$ is linear, then there exists a permutation $\mathcal{P}_n$ with $n = m + \sum_{i=1}^{m} l_i$ and $\mathcal{P}_s(x) = \mathcal{P}_n(x)$ on $\mathbb{F}_q$.

In all three cases, if $n < \frac{q-1}{2}$, then Crk$(\mathcal{P}_s) = n$.

Proof.

(i) Let $\mathcal{F}_s$ not be linear, i.e. $x_s \neq \infty$ and $\mathcal{F}_s(x_s) \in \text{supp}(\tau_i)$ for some $1 \leq i \leq m$. Without loss of generality assume that $x_s = x_1^1$. We can choose $\mathcal{F}_n(x) = \mathcal{F}_s(x)$ with the string of poles

$$\mathcal{O}_n = x_{l_1}^1, \dots, x_1^1, \dots, x_{l_m}^m, \dots, x_1^m, x_1^{m-1}, x_1^{m-2}, \dots, x_1^1.$$

Then Corollary 5.0.1 and Remark 5.0.1 gives us the desired $\mathcal{P}_n$.

(ii) Let $\mathcal{F}_s$ not be linear, i.e. $x_s \neq \infty$, and $\mathcal{F}_s(x_s) \notin \text{supp}(\tau_i)$ for any $i = 1, \dots, m$. We choose $\mathcal{F}_n(x) = \mathcal{F}_s(x)$ with the string of poles

$$\mathcal{O}_n = x_s, x_{l_1}^1, \dots, x_1^1, \dots, x_{l_m}^m, \dots, x_1^m, x_1^{m-1}, x_1^{m-2}, \dots, x_1^1, x_s$$

to get the desired result.

(iii) Lastly, if $\mathcal{F}_s$ is linear, i.e. $x_s = \infty$, we choose $\mathcal{F}_n(x) = \mathcal{F}_s(x)$ with the string of poles

$$\mathcal{O}_n = x_{l_1}^1, \ldots, x_1^1, \ldots, x_{l_m}^m, \ldots, x_1^m, x_1^{m-1}, x_1^{m-2}, \ldots, x_1^1, \infty$$

to get the desired result.

Note that in all three cases above we took $\mathcal{F}_s(x) = \mathcal{F}_n(x)$. Now suppose for some $n' < n$, $\mathcal{F}_{n'}(x)$ not equal to $\mathcal{F}_n(x)$ on $\mathbb{F}_q$, but $\mathcal{P}_{n'}(x) = \mathcal{P}_n(x)$. Then by Lemma 5.0.7, we must have $2n > n + n' > q - 2$, i.e. $n > \frac{q-2}{2}$. Therefore, we conclude that $\mathrm{Crk}(\mathcal{P}_s) = n$, if $n < \frac{q-1}{2}$ in the above cases. □

Example 5.1.1. *Let* $F = \mathbb{F}_{11}$ *and*

$$p(x) = \mathcal{P}_7(x) = ((((((2x+1)^9 + 5)^9 + 3)^9 + 7)^9 + 4)^9 + 4)^9 + 2)^9$$

be in $\mathbb{F}_{11}[x]$. *Then*
String of poles: $5, 6, 8, 5, \infty, 1, 6$ *and*

$$p(x) = \mathcal{P}_7(x) = (F_7(6)F_7(8)F_7(1))F_7(x),$$

where

$$F_7(x) = \begin{cases} \frac{3x+8}{6x+8} & \text{if } x \neq 6 \\ 6 & \text{if } x = 6. \end{cases}$$

We can reduce $\mathcal{P}_7(x)$ *to* $\mathcal{P}_3(x)$, *where*

$$\mathcal{P}_3(x) = (((10x+1)^9 + 8)^9 + 1)^9 + 10.$$

Hence, $\mathrm{Crk}(p)$ *is* 3.

In the following theorem, we will use the Stirling numbers $S(t, k, m)$ of the first kind which is the number of ways of distributing k objects into m cycles each containing at least t elements. For $t = 2$, the recurrence relation

$$S(2, k+1, m+1) = kS(2, k, m+1) + kS(2, k-1, m)$$

is known.

Theorem 5.1.2. *The number $\mathcal{B}(n)$ of permutations of $\mathbb{F}_q$ with Carlitz rank n is given by*

$$\begin{aligned}\mathcal{B}(n) &= (q^2-q)\sum_{m=1}^{\lfloor\frac{n+1}{3}\rfloor}\binom{q}{n+1-m}\mathcal{S}(2,n+1-m,m)(n+1-m)\\ &+(q^2-q)\sum_{m=1}^{\lfloor\frac{n-1}{3}\rfloor}\binom{q}{n-1-m}\mathcal{S}(2,n-1-m,m)(q-(n-1-m))\\ &+(q^2-q)\sum_{m=1}^{\lfloor\frac{n}{3}\rfloor}\binom{q}{n-m}\mathcal{S}(2,n-m,m) \qquad (5.11)\end{aligned}$$

for all $2 \le n < (q-1)/2$.

Proof. Let $p(x) = \mathcal{P}_n(x)$, where

$$\mathcal{P}_n(x) = \tau_1 \dots \tau_m \mathcal{F}_n(x),$$

where $\mathcal{F}_n(x) = \frac{ax+b}{cx+d}$, $2 \le n < (q-1)/2$.

We will distinguish the proof in three cases in parallel to Theorem 5.1.1.

We first assume that $\mathcal{F}_n(x)$ is not linear. Then for simplicity we can write $\mathcal{F}_n(x) = \frac{ax+b}{x+d}$. Let $\mathcal{F}_n(-d) = a \in \tau_i$ for some $i = 1, \dots, m$. By part (i) of Theorem 5.1.1, $n = m + \sum_{i=1}^{m} l_i - 1$, that is, the total number of elements in τ_i's is $n+1-m$. Hence for the product $\tau_1 \dots \tau_m$ we have $\binom{q}{n+1-m}S(2, n+1-m, m)$ choices. Now we count the possible choices for $\mathcal{F}_n(x) = \frac{ax+b}{x+d}$. Note that for a we have $n+1-m$ choices, d is arbitrary so q choices for it, and lastly since $ad-b \neq 0$ we have $q-1$ choices for b. Altogether there are $(n+1-m)q(q-1)$ choices for $\mathcal{F}_n(x)$. Lastly, since $l_i \ge 2$ for all $i = 1, \dots, m$, $n+1-m \ge 2m$, i.e. $1 \le m \le \lfloor\frac{n+1}{3}\rfloor$. Combining what we get so far yields the first summand in 5.11.

Now assume that $\mathcal{F}(x)$ is not linear, so it is of the form $\frac{ax+b}{x+d}$ as in the previous case but $\mathcal{F}_n(-d) = a \notin \tau_i$ for any $i = 1, \dots, m$. Then part(ii) of Theorem 5.1.1 gives $n = m + \sum_{i=1}^{m} l_i + 1$, that is, the total number of elements in τ_i's is $n-1-m$. Hence for the product $\tau_1 \dots \tau_m$ we have $\binom{q}{n-1-m}S(2, n-1-m, m)$ choices. Now

we count the possible choices for $\mathcal{F}_x = \frac{ax+b}{x+d}$. For a, we have $q-(n+1-m)$ choices in this case, d is arbitrary, $ad-b \neq 0$ gives $q-1$ choices for b. Altogether there are $q(q-1)(q-(n+1-m))$ choices for $\mathcal{F}_n(x)$. Lastly, since $l_i \geq 2$ for all $i = 1, \ldots, m$, $n-1-m \geq 2m$, i.e. $1 \leq m \leq \left\lfloor \frac{n-1}{3} \right\rfloor$ and we form the second summand in 5.11.

Lastly, let $\mathcal{F}(x)$ be linear, say $\mathcal{F}(x) = ax+b$, $a \neq 0$. By part (iii) of Theorem 5.1.1, $n = m + \sum_{i=1}^{m} l_i$, that is, the total number of elements in τ_i's is $n-m$. Hence for the product $\tau_1 \ldots \tau_m$ we have $\binom{q}{n-m} S(2, n-m, m)$ choices. For $\mathcal{F}_n(x)$ we have $q(q-1)$ choices in this case and $n-m \geq 2m$ gives $1 \leq m \leq \left\lfloor \frac{n}{3} \right\rfloor$, which completes the proof. $\square$

Bibliography

[1] E. Aksoy, *On permutation polynomials over finite fields*, 2006, M.S. thesis.

[2] E. Aksoy, A. Çesmelioğlu, W. Meidl, A. Topuzoğlu, *On the Carlitz rank of permutation polynomials*, 2009, Finite Fields and Their Applications v15-4 (428-440).

[3] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, and M. Rudnev, *Group actions and geometric combinatorics in* $\mathbb{F}_q^d$, http://arxiv.org/pdf/1311.4788.pdf

[4] M. Bennett, A, Iosevich and J. Pakianathan, *Three-point configurations determined by subsets of* $\mathbb{F}_q^2$ *via the Elekes-Sharir paradigm,* Combinatorics (to appear)(2013)

[5] P. Brass, W. Moser, J. Pach, *Research problems in discrete geometry*, Springer, 2005.

[6] L. Carlitz, *Permutations in a finite field*, Proc. Amer. Math. Soc. 4 (1953) 538.

[7] J. Chapman, M. B. Erdogan, D. Hart, A. Iosevich and D. Koh, *Pinned distance sets, k- simplices , Wollf's exponent in finite fields and sum-product estimates,* Mathematische Zeitschrift, Math. Z. 271(2012) no. 1-2, 63-93.

[8] D. Covert, D. Hart, A. Iosevich, S. Senger, I. Uriarte-Tuero, *A Furstenberg-Katznelson-Weiss type theorem on $(d+1)$-point configurations in sets of positive density in finite field geometries*. Discrete Math. 311 (2011), no. 6, 423-430.

[9] D. Covert, A. Iosevich, J. Pakianathan, *Geometric configurations in the ring of integers modulo p^l,* http://arxiv.org/pdf/1105.5373.pdf

[10] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, *On the cycle structure of permutation polynomials*, Finite Fields and Their Applications, 2008, v14-3, 593-614

[11] P. Erdős, *On sets of distances of n points*, Amer. Math. Montly **53**(1946) 248-250.

[12] L. Guth and N. Katz, *On the Erdős distinct distance problem in the plane,* http://arxiv.org/pdf/1011.4105.pdf

[13] D. Hart, A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint,* Radon transforms, geometry, and wavelets, 129-135, Contemp. Math., 464, Amer. Math. Soc., Providence, RI, 2008.

[14] D. Hart, A. Iosevich, D. Koh and M. Rudnev, *Averages over hyperplanes, sum-product theory in finite fields, and the Erdős-Falconer distance conjecture,* Transaction of the AMS, **363** (2011) 3255-3275.

[15] A. Iosevich and M. Rudnev, *Erdős distance problem in vector spaces over finite fields*, Trans. Amer. Math. Soc. **359** (2007) no. 12, 6127-6142

[16] A. Iosevich, M. Rudnev, and Y. Zhai, *Areas of triangles and Beck's theorem in planes over finite fields,* http://arxiv.org/pdf/1205.0107.pdf

[17] R. Lidl, and H. Niederreiter. *Finite Fields*, Cambridge Univ. Press, Cambridge, 1997.

[18] W. Rudin, *Fourier analysis on groups*. Interscience Tracts in Pure and Applied Mathematics, No. 12 Interscience Publishers (a division of John Wiley and Sons), New York-London 1962 ix+285 pp.

[19] I.E. Shparlinski, *Finite Fields: Theory and Computation*, Kluver Academic Publishers, 1999.

[20] J. Solymosi and V. Vu, *Distinct distances in high dimensional homogeneous sets, Towards a theory of geometric graphs*, 259-268, Contemp. Math. **342** Amer. Math. Soc. Providence, 2004.