Pinned Distances in Modules over Finite Valuation Rings

Esen Aksoy Yazici

August 24, 2020

Abstract

Let $R$ be a finite valuation ring of order $q^r$ where $q$ is odd and $A$ be a subset of $R$. In the present paper, we prove that there exists a point $u$ in the Cartesian product set $A \times A \subset R^2$ such that the size of the pinned distance set at $u$ satisfies

$$|\Delta_u(A \times A)| \gg \min\left\{ q^r, \frac{|A|^2}{q^{2r-1}} \right\}.$$

This implies that if $|A| \geq q^{r-\frac{1}{2}}$, then the set $A \times A$ determines a positive proportion of all possible distances.

1 Introduction

Erdős-Falconer type problems in discrete geometry ask for a threshold on the size of a set so that the set determines the given geometric configurations. These problems have been studied by many authors both in continuous and discrete setting.

In [9], Erdős observed that $\sqrt{n} \times \sqrt{n}$ integer grid determines $C\left(\frac{n}{\sqrt{\log n}}\right)$ distances and he conjectured that the minimum number of distances determined by a $n$-point set in the plane is indeed $C\left(\frac{n}{\sqrt{\log n}}\right)$, where $C$ is an absolute constant. Despite many works and progress, the Erdős distance problem was open until recently. In 2010, Guth and Katz [10] employed a polynomial partitioning technique based on Elekes-Sharir framework to prove that $n$ points in the plane determine at least $C\frac{n}{\log n}$ distances. This result solved the Erdős distance problem up to a $\sqrt{\log}$ factor.

The distance problem in finite field plane was first studied by Bourgain, Katz and Tao in [5]. The result in [5] was later generalized by various authors to higher dimensional vector spaces. It was also extended to many other geometric configurations in finite field geometry, see for instance [2–4, 6, 7, 11, 13, 14, 16] and references therein. In particular, in [16], Petridis proved the following pinned distance result for Cartesian product subsets of vector spaces over prime fields.
Theorem 1.1. [16, Theorem 1.1] Let $p$ be an odd prime and $A \subset \mathbb{F}_p$. There exist $a, b \in A$ such that 
\[ |\Delta_{(a,b)}(A \times A)| = \Omega(\min\{p, |A|^{3/2}\}). \]

Similar geometric problems in modules over finite cyclic rings were studied by Covert, Iosevich and Pakianathan in [8]. Using a Fourier analytic approach, the authors of [8] proved the following.

Theorem 1.2. [8, Theorem 1.3] Let $E \subset \mathbb{Z}_q^d$, where $q = p^l$. Suppose 
\[ |E| \gg l(l + 1)q^{(2l-1)/d + \frac{1}{2l}}. \]

Then the distance set $\Delta(E)$ determined by the points of $E$ satisfies 
\[ \Delta(E) \supset \mathbb{Z}_q^d \cup \{0\}. \]

Later in [12], Hieu and Vinh proved the following distance result in the context of finite cyclic rings.

Theorem 1.3. [12, Theorem 2.7] Let $A \subset \mathbb{Z}_q$ be of cardinality $|A| \gg q^{1 - \frac{1}{2l}}$. Then, the size of the distance set determined by $A^n$ satisfies 
\[ |\Delta_{\mathbb{Z}_q}(A^n)| \gg \min\left\{ q, \frac{|A|^{2n-1}}{(rq^{2/l-1})^{n-1}} \right\}. \]

Now, let $R$ denote a finite valuation ring. In this paper, we study a variant of distance problem, namely pinned distance problem, for Cartesian product subsets $A \times A$ of $R^2$.

Note that, the method we use to prove the main result of this paper is analogous to the one given by Petridis in [16, Theorem 1.1]. More precisely, we first see pinned distances at a fixed point in $R^2$ as a point-plane incidence in $R^3$. Then we employ the point-plane incidence bound for multisets in $R^3$ which is recently given by Van The et al. in [17, Theorem 2.3]. This yields the lower bound for the size of the specified pinned distance set in $R^2$ in Theorem 1.4.

We should mention that the distance result we obtain in Theorem 1.4 recovers the pinned distance result in [16] in the finite field setting. Also, in the setting of modules over finite cyclic rings $\mathbb{Z}_q$, it is an improvement on the distance results given in [8, 12] for the Cartesian product sets $A \times A \subset \mathbb{Z}_q^2$.

Before stating the main theorem, let us recall some necessary definitions.
1.1 Notation.

We note that a detailed definition of finite valuation ring can be found in [15]. In order to make the statements precise and self contained, we will review the definition and provide some key examples in this note. A finite valuation ring is a finite principal ideal domain which is local. Given a finite valuation ring \( R \), we associate two parameters \( q \) and \( r \) to \( R \) as follows. Let the maximal ideal \( M \) of \( R \) be of the form \( M = (\pi) \), where \( \pi \) is the uniformizer of \( R \), i.e. a non unit defined up to a unit of \( R \). Let \( r \) be the nilpotency degree of \( \pi \), that is the smallest positive integer with the property that \( \pi^r = 0 \) and \( q \) be the size of the residue field \( F = R/(\pi) \). Therefore, \( R \) has the filtration

\[
R \supset (\pi) \supset (\pi^2) \cdots \supset (\pi^r) = 0,
\]

where \( |R| = q^r \). Some examples of finite valuation rings are as follows.

1. Finite fields \( \mathbb{F}_q \), where \( q = p^k \) is a prime power.
2. Finite cyclic rings \( \mathbb{Z}_{p^k} \), where \( p \) is a prime.
3. Function fields \( F[x]/(f^k) \), where \( F \) is a finite field and \( f \) is an irreducible polynomial in \( F[x] \).
4. \( \mathcal{O}/(p^k) \), where \( \mathcal{O} \) is the ring of integers in a number field and \( p \) is a prime in \( \mathcal{O} \).

Let us also write some of the examples above with parameters \( q \) and \( r \) as stated in the definition. Note that for the finite field \( R = \mathbb{F}_{p^k} \), \( p \) is a prime, we have \( q = p^k \) and \( r = 1 \). And for the finite cyclic ring \( \mathbb{Z}_{p^k} \) we have the filtration

\[
\mathbb{Z}_{p^k} \supset (p) \supset (p^2) \cdots \supset (p^k) = 0.
\]

Hence \( r = k \) and \( q = |\mathbb{Z}_{p^k}/(p)| = p \) in this case.

Next we recall the notion of distance in this context. For two points \( u = (u_1, \ldots, u_d) \) and \( v = (v_1, \ldots, v_d) \) in \( R^d \), the distance between them is given by

\[
||u - v|| = (u_1 - v_1)^2 + \cdots + (u_d - v_d)^2.
\]

For a subset \( E \subset R^d \), the distance set determined by \( E \) is

\[
\Delta(E) = \{ ||u - v|| : u, v \in E \},
\]

and the distance set pinned at a fixed point \( u \) of \( E \) is defined by

\[
\Delta_u(E) = \{ ||u - v|| : v \in E \}.
\]

Throughout \( R \) will denote a finite valuation of order \( q^r \), where \( q \) is an odd prime power. \( X \gg Y \) means that there exists an absolute constant \( c \) such that \( X \geq cY \), and “\( \ll \)” is defined similarly.
1.2 Statement of Main Result

Our main result is the following theorem.

**Theorem 1.4.** Let $R$ be a finite valuation ring of order $q^r$, $q$ is an odd prime power, and $A \subset R$. There exists a point $u \in A \times A \subset R^2$ such that

$$|\Delta_u(A \times A)| \gg \min\left\{q^r, \frac{|A|^3}{q^{2r-1}}\right\}.$$

In particular, if $|A| \geq q^r - \frac{q}{2}$, then $\Delta_u(A \times A) \gg q^r$ for some $u \in A \times A$ and hence $A \times A$ determines a positive proportion of all possible distances.

**Remark 1.5.** Let $R = \mathbb{F}_p$, where $p$ is an odd prime. Note that in this case we can take $q = p$ and $r = 1$ in Theorem 1.4 and conclude that if $A \subset \mathbb{F}_p$, then there exists $u \in A \times A \subset \mathbb{F}_p^2$ such that

$$|\Delta_u(A \times A)| \gg \min\left\{p, \frac{|A|^3}{p}\right\}.$$

In particular, if $|A| > p^2$, then $|\Delta_u(A \times A)| \gg p$ for some $u \in A \times A$. This result matches with the result of Petridis given in [16, Theorem 1.1] in the context of prime fields and generalize it to the broader context of finite valuation rings.

**Remark 1.6.** We note that the result in [8, Theorem 1.3] in the special case $d = 2$ implies that if $E \subset \mathbb{Z}_q^2$, where $q = p^l$, and $|E| \gg l(l+1)q^{2-\frac{1}{2}}$, then

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

On the other hand, Theorem 1.4 implies that if $E = A \times A \subset \mathbb{Z}_q^2$, where $q = p^l$, and $|E| = |A \times A| \geq q^{2-\frac{1}{2}}$, then $|\Delta(E)| = |\Delta(A \times A)| \gg q$.

Therefore, in terms of getting a positive proportion of all possible distances, Theorem 1.4 improves the result in [8, Theorem 1.3] for Cartesian product sets of the form $A \times A \subset \mathbb{Z}_q^2$.

**Remark 1.7.** In [12, Theorem 2.7], for $n = 2$, the following result was obtained for subsets of finite cyclic rings. Let $A \subset \mathbb{Z}_q$ be of cardinality $|A| \gtrsim q^{1-1/2r}$, where $q = p^r$. Then the number of distances determined by $A \times A$ satisfies

$$|\Delta_{\mathbb{Z}_q}(A \times A)| \gtrsim \min\left\{q, \frac{|A|^3}{rq^{2-1/r}}\right\}.$$

Theorem 1.4 can be seen as a generalization of this result to finite valuation rings and a slight improvement in the context of finite cyclic rings.
2 Proof of Theorem 1.4

For the proof of Theorem 1.4, we will need the following lemma from [16]. We note here that though Petridis stated Lemma 2.1 for subsets of finite fields \( \mathbb{F}_q \), it can be readily checked that the same proof applies for subsets of any finite valuation ring.

**Lemma 2.1.** Let \( E \subset \mathbb{R}^2 \) and \( N \) be the number of solutions to
\[
2u \cdot (v - w) + \|w\| - \|v\| = 0, \tag{2.1}
\]
where \( u, v, w \in E \). Then there exists \( u \in E \) such that \( |\Delta_u(E)| \geq \frac{|E|^3}{N} \).

We will also use the following point-plane incidence bound in \( \mathbb{R}^3 \) from [17].

**Theorem 2.2.** [17, Theorem 2.3] Let \( Q, \Pi \) be weighted set of points and planes in \( \mathbb{R}^3 \) with the weighted integer function \( w \), both total weight \( W \). Suppose that maximum weights are bounded by \( w_0 \geq 1 \). Let the number of weighted incidences be
\[
I_w = \sum_{q \in Q, \pi \in \Pi} w(q)w(\pi)\delta_{q\pi},
\]
where
\[
\delta_{q\pi} = \begin{cases} 1 & \text{if } q \in \pi, \\ 0 & \text{if } q \notin \pi. \end{cases}
\]
Then the number \( I_w \) of weighted incidences is bounded as follows:
\[
I_w = \sum_{q \in Q, \pi \in \Pi} w(q)w(\pi) \ll \frac{1}{q^6}W^2 + q^{2r-1}W.
\]

**Proof of Theorem 1.4.** We first note that if we write \( u = (u_1, u_2) \), \( v = (v_1, v_2) \) and \( w = (w_1, w_2) \), where \( u_i, v_i, w_i \in A \), then the equation (2.1) can be written as
\[
2u_1(v_1 - w_1) + 2u_2(v_2 - w_2) + (w_2^2 - v_2^2) = v_1^2 - w_1^2
\]
which can be restated as
\[
(2u_1, v_2 - w_2, w_2^2 - v_2^2) \cdot (v_1 - w_1, 2u_2, 1) = v_1^2 - w_1^2. \tag{2.2}
\]
Next we define a set of points \( Q \) and a set of planes \( \Pi \) in \( \mathbb{R}^3 \) as follows:
\[
Q = \{(2u_1, v_2 - w_2, w_2^2 - v_2^2) : u_1, v_2, w_2 \in A\}
\]
and
\[
\Pi = \{x \in \mathbb{R}^3 : x \cdot (v_1 - w_1, 2u_2, 1) = v_1^2 - w_1^2 : v_1, w_1, u_2 \in A\}
\]
Then it follows that the number of incidences $|I(Q, \Pi)|$ between $Q$ and $\Pi$ is equal to the number of solutions of the equation (2.2) which is $N$ in Lemma 2.1.

Note that the total weight of $Q$ and $\Pi$ are both $W = |A|^3$. Hence, Theorem 2.2 implies that

$$N = |I(Q, \Pi)|$$

$$\leq \frac{1}{q^r} W^2 + q^{2r-1} W$$

$$= \frac{1}{q^r} |A|^6 + q^{2r-1} |A|^3.$$

Therefore, by Lemma 2.1, there exists $u \in A \times A$ such that

$$|\Delta_u(A \times A)| \geq \frac{|A|^6}{N} \gg \min\left\{q^r, \frac{|A|^3}{q^{2r-1}}\right\}$$

which completes the proof of Theorem 1.4.

Acknowledgments. The author would like to thank Brendan Murphy for valuable comments.

References

[1] E. Aksoy Yazici, *Sum-product type estimates for subsets of finite valuation rings*, Acta Arith. 185 (2018), no. 1, 918.

[2] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, and M. Rudnev, *Group actions and geometric combinatorics in $\mathbb{F}_q^d$*, Forum Math. 29 (2017), no. 1, 91-110.

[3] M. Bennett, A. Iosevich and J. Pakianathan, *Three-point configurations determined by subsets of $\mathbb{F}_q^2$ via the Elekes-Sharir paradigm*, Combinatorica 34 (2014), no. 6, 689-706.

[4] P. Birklbauer, A. Iosevich, *A two-parameter finite field Erdős-Falconer distance problem*, Bull. Hellenic Math. Soc. 61 (2017), 2130.

[5] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. 14 (2004), no. 1, 27-57.

[6] J. Chapman, M. B. Erdogan, D. Hart, A. Iosevich and D. Koh, *Pinned distance sets, $k$-simplices , Wolf’s exponent in finite fields and sum-product estimates*, Mathematische Zeitschrift, Math. Z. 271(2012) no. 1-2, 63-93.
[7] D. Covert, D. Hart, A. Iosevich, S. Senger, I. Uriarte-Tuero, \textit{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. 1

[8] D. Covert, A. Iosevich, J. Pakianathan, \textit{Geometric configurations in the ring of integers modulo $p^l$}, Indiana Univ. Math. J. 61 (2012), no. 5, 1949-1969. 2, 4

[9] P. Erdős, \textit{On sets of distances of $n$ points}, Amer. Math. Montly 53(1946) 248-250. 1

[10] L. Guth, N. Katz, \textit{On the Erdős distinct distances problem in the plane}, Ann. of Math. (2) 181 (2015), no. 1, 155-190. 1

[11] D. Hart, A. Iosevich, D. Koh and M. Rudnev, \textit{Averages over hyperplanes, sum-product theory in finite fields, and the Erdős-Falconer distance conjecture}, Transaction of the AMS, 363 (2011) 3255-3275. 1

[12] D. D. Hieu, ; L. A. Vinh, \textit{On distance sets and product sets in vector spaces over finite rings}, Michigan Math. J. 62 (2013), no. 4, 779792. 2, 4

[13] A. Iosevich and M. Rudnev, \textit{Erdős distance problem in vector spaces over finite fields}, Trans. Amer. Math. Soc. 359 (2007) no. 12, 6127-6142. 1

[14] A. Iosevich, M. Rudnev, and Y. Zhai, \textit{Areas of triangles and Beck's theorem in planes over finite fields}, Combinatorica 35 (2015), no. 3, 295-308. 1

[15] B. Nica \textit{Unimodular graphs and Eisenstein sums}, J. Algebraic Combin. 45 (2017), no. 2, 423-454. 3

[16] G. Petridis, \textit{Pinned algebraic distances determined by Cartesian products in $\mathbb{F}_p^2$}, Proc. Amer. Math. Soc. 145 (2017), no. 11, 4639-4645. 1, 2, 4, 5

[17] N. Van The, P. D. Tran, L. Q. Ham, L. A. Vinh \textit{On three-variable expanders over finite valuation rings}, https://arxiv.org/pdf/2007.05251.pdf, 2020 2, 5