*Pacific Journal of Mathematics*

# DISTRIBUTION OF DISTANCES IN POSITIVE CHARACTERISTIC

THANG PHAM AND LÊ ANH VINH

Volume 309 No. 2 December 2020

PACIFIC JOURNAL OF MATHEMATICS
Vol. 309, No. 2, 2020
https://doi.org/10.2140/pjm.2020.309.437

# DISTRIBUTION OF DISTANCES IN POSITIVE CHARACTERISTIC

THANG PHAM AND LÊ ANH VINH

**Let $\mathbb{F}_q$ be an arbitrary finite field, and $\mathcal{E}$ be a point set in $\mathbb{F}_q^d$. Let $\Delta(\mathcal{E})$ be the set of distances determined by pairs of points in $\mathcal{E}$. Using Kloosterman sums, Iosevich and Rudnev (2007) proved that if $|\mathcal{E}| \geq 4q^{(d+1)/2}$ then $\Delta(\mathcal{E}) = \mathbb{F}_q$. In general, this result is sharp in odd-dimensional spaces over arbitrary finite fields. We use the point-plane incidence bound due to Rudnev to prove that if $\mathcal{E}$ has Cartesian product structure in vector spaces over prime fields, then we can break the exponent $(d+1)/2$ and still cover all distances. We also show that the number of pairs of points in $\mathcal{E}$ of any given distance is close to its expected value.**

## 1. Introduction

Let $\mathcal{E}$ be a finite subset of $\mathbb{R}^d$ $(d \geq 2)$, and $\Delta(\mathcal{E})$ be the distance set determined by $\mathcal{E}$. The Erdős distinct distances problem is to find the best lower bound of the size of the distance set $\Delta(\mathcal{E})$ in terms of the size of the point set $\mathcal{E}$.

In the plane case, Erdős [1946] conjectured that $|\Delta(\mathcal{E})| \gg |\mathcal{E}|/\sqrt{\log|\mathcal{E}|}$. This conjecture was proved up to logarithmic factor by Guth and Katz [2015] in 2010. More precisely, they showed that $|\Delta(\mathcal{E})| \gg |\mathcal{E}|/\log|\mathcal{E}|$. In higher dimension cases, Erdős [1946] also conjectured that $|\Delta(\mathcal{E})| \gg |\mathcal{E}|^{2/d}$. Interested readers are referred to [Solymosi and Vu 2008] for results on Erdős distinct distances problem in three and higher dimensions.

In this paper, we use the following notation: $X \ll Y$ means that there exists some absolute constant $C_1 > 0$ such that $X \leq C_1 Y$, $X \sim Y$ means $Y \ll X \ll Y$, $X \gtrsim Y$ means $X \gg (\log Y)^{-C_2} Y$ for some absolute constant $C_2 > 0$, and $X \gtrsim_d Y$ means $X \geq C_3 (\log Y)^{-C_4} Y$ for some positive constants $C_3, C_4$ depending on $d$.

As a continuous analogue of the Erdős distinct distances problem, Falconer [1985] asked how large the Hausdorff dimension of $\mathcal{E} \subset \mathbb{R}^d$ needs to be to ensure that the Lebesgue measure of $\Delta(\mathcal{E})$ is positive. He conjectured that for any subset $\mathcal{E} \subset \mathbb{R}^d$ of the Hausdorff dimension greater than $d/2$, $\mathcal{E}$ determines a distance set of a positive Lebesgue measure. This conjecture is still open in all dimensions.

*MSC2020:* 14N10, 51A45, 52C10.
*Keywords:* distances, finite fields, incidence, Rudnev's point-plane incidence bound.

We refer readers to [Du et al. 2018; Guth et al. 2020] for recent updates on this conjecture.

Let $\mathbb{F}_q$ be the finite field of order $q$, where $q$ is an odd prime power. Given two points $\boldsymbol{x} = (x_1, \dots, x_d)$ and $\boldsymbol{y} = (y_1, \dots, y_d)$ in $\mathbb{F}_q^d$, we denote the distance between $\boldsymbol{x}$ and $\boldsymbol{y}$ by

$$\|\boldsymbol{x} - \boldsymbol{y}\| := (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2.$$

Note that the distance function defined here is not a metric but it is invariant under translations and actions of the orthogonal group.

For a subset $\mathcal{E} \subset \mathbb{F}_q^d$, we denote the set of all distances determined by $\mathcal{E}$ by

$$\Delta(\mathcal{E}) := \{\|\boldsymbol{x} - \boldsymbol{y}\| : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\}.$$

The finite field analogue of the Erdős distinct distances problem was first studied by Bourgain, Katz, and Tao [Bourgain et al. 2004]. More precisely, they proved that in the prime field $\mathbb{F}_p$ with $p \equiv 3 \bmod 4$, $|\Delta(\mathcal{E})| \gg |\mathcal{E}|^{1/2+\epsilon}$ for some $\epsilon = \epsilon(\alpha) > 0$, for any subset $\mathcal{E} \subset \mathbb{F}_p^2$ of the cardinality $|\mathcal{E}| = p^\alpha$, $0 < \alpha < 2$,

Note that the condition $p \equiv 3 \bmod 4$ in Bourgain, Katz, and Tao's result is necessary, since if $p \equiv 1 \bmod 4$, then there exists $i \in \mathbb{F}_p$ such that $i^2 = -1$. By taking $\mathcal{E} = \{(x, ix) : x \in \mathbb{F}_p\}$, we have $|\mathcal{E}| = p$ and $\Delta(\mathcal{E}) = \{0\}$.

In the setting of arbitrary finite fields $\mathbb{F}_q$, Iosevich and Rudnev [2007] showed that Bourgain, Katz, and Tao's result does not hold. For example, assuming that $q = p^2$, one can take $\mathcal{E} = \mathbb{F}_p^2$, then $\Delta(\mathcal{E}) = \mathbb{F}_p$ or $|\Delta(\mathcal{E})| = |\mathcal{E}|^{1/2}$. Thus, Iosevich and Rudnev reformulated the problem in the spirit of the Falconer distance conjecture over the Euclidean spaces. More precisely, they asked, for a subset $\mathcal{E} \subset \mathbb{F}_q^d$, how large $|\mathcal{E}|$ needs to be to ensure that $\Delta(\mathcal{E})$ covers the whole field or at least a positive proportion of all elements of the field?

Using Fourier analytic methods, Iosevich and Rudnev [2007] proved that $\Delta(\mathcal{E}) = \mathbb{F}_q$ for any point set $\mathcal{E} \subset \mathbb{F}_q^d$ with the cardinality $|\mathcal{E}| \geq 4q^{(d+1)/2}$. Hart, Iosevich, Koh, and Rudnev [Hart et al. 2011] showed that, in general, the exponent $(d+1)/2$ cannot be improved when $d$ is odd, even if we only want to cover a positive proportion of all the distances. In even-dimensional cases, it has been conjectured that the exponent $(d+1)/2$ can be improved to $d/2$, which is in line with the Falconer distance conjecture in the Euclidean space.

In the plane case, Bennett, Hart, Iosevich, Pakianathan, and Rudnev [Bennett et al. 2017] proved that if $\mathcal{E}$ is a subset of $\mathbb{F}_q^2$ of cardinality $|\mathcal{E}| \geq q^{4/3}$, then $\Delta(\mathcal{E})$ covers a positive proportion of all distances. Murphy and Petridis [2019] showed that there are infinite subsets of $\mathbb{F}_q^2$ of size $q^{4/3}$ whose distance sets do not cover the whole field $\mathbb{F}_q$. It is not known whether there exist a small $c > 0$ and a set $\mathcal{E} \subset \mathbb{F}_q^2$ with $|\mathcal{E}| \geq cq^{3/2}$ such that $\Delta(\mathcal{E}) \neq \mathbb{F}_q$. We refer the interested reader to [Hart et al. 2011, Theorem 2.7] for a construction in odd-dimensional spaces.

Chapman et al. [2012] broke the exponent $(d+1)/2$ to $d^2/(2d-1)$ under the additional assumption that the set $\mathcal{E}$ has Cartesian product structure. However, in this case, they can cover only a positive proportion of all distances. In the setting of prime fields, it has been proved in [Pham et al. 2019] that for $A \subset \mathbb{F}_p$, we have $|\Delta(A^d)| \geq \frac{1}{c} \cdot \min\{|A|^{2-1/2^{d-2}}, p\}$ with $c = 2^{(2^{d-1}-1)/2^{d-2}}$. Therefore, $|\Delta(A^d)| \geq p/c$ under the condition $|A| \geq p^{2^{d-2}/(2^{d-1}-1)}$. However, this result again only gives us a positive proportion of all distances, and does not tell us the number of pairs of any given distance.

We will show that if $\mathcal{E} \subset \mathbb{F}_p^d$ has Cartesian product structure, we can break the exponent $(d+1)/2$ due to Iosevich and Rudnev [2007] and still cover all possible distances. Our main tool is the point-plane incidence bound due to Rudnev [2018].

Our first result is for odd-dimensional cases.

**Theorem 1.1.** *Let $\mathbb{F}_p$ be a prime field, and $A$ be a set in $\mathbb{F}_p$. For an integer $d \geq 3$, suppose the set $A^{2d+1} \subset \mathbb{F}_p^{2d+1}$ satisfies*

$$|A^{2d+1}| \gtrsim_d p^{\frac{2d+2}{2} - \frac{3\cdot 2^{d-2}-d-1}{3\cdot 2^{d-1}-1}};$$

*then*:

- *The distance set covers all elements in $\mathbb{F}_p$, namely,*
$$\Delta(A^{2d+1}) = \underbrace{(A-A)^2 + \cdots + (A-A)^2}_{2d+1 \text{ terms}} = \mathbb{F}_p.$$
- *The number of pairs $(\boldsymbol{x}, \boldsymbol{y}) \in A^{2d+1} \times A^{2d+1}$ satisfying $\|\boldsymbol{x} - \boldsymbol{y}\| = \lambda$ is $\sim p^{-1}|A|^{4d+2}$ for any $\lambda \in \mathbb{F}_p$.*

**Corollary 1.2.** *For $A \subset \mathbb{F}_p$, suppose that $|A| \gtrsim p^{6/11}$; then we have*

$$\begin{aligned}\Delta(A^7) &= (A-A)^2+(A-A)^2+(A-A)^2+(A-A)^2+(A-A)^2+(A-A)^2+(A-A)^2\\ &= \mathbb{F}_p.\end{aligned}$$

Our second result is for even-dimensional cases.

**Theorem 1.3.** *Let $\mathbb{F}_p$ be a prime field, and $A$ be a set in $\mathbb{F}_p$. For an integer $d \geq 3$, suppose the set $A^{2d} \subset \mathbb{F}_p^{2d}$ satisfies*

$$|A^{2d}| \gtrsim_d p^{\frac{2d+1}{2} - \frac{2^d-2d-1}{2^{d+1}-2}};$$

*then*:

- *The distance set covers all elements in $\mathbb{F}_p$, namely,*
$$\Delta(A^{2d}) = \underbrace{(A-A)^2 + \cdots + (A-A)^2}_{2d \text{ terms}} = \mathbb{F}_p.$$
- *The number of pairs $(\boldsymbol{x}, \boldsymbol{y}) \in A^{2d} \times A^{2d}$ satisfying $\|\boldsymbol{x} - \boldsymbol{y}\| = \lambda$ is $\sim p^{-1}|A|^{4d}$ for any $\lambda \in \mathbb{F}_p$.*

**Corollary 1.4.** *For $A \subset \mathbb{F}_p$, suppose that $|A| \gtrsim p^{4/7}$; then we have*

$$\Delta(A^6) = (A-A)^2 + (A-A)^2 + (A-A)^2 + (A-A)^2 + (A-A)^2 + (A-A)^2 = \mathbb{F}_p.$$

**Remark.** In the setting of arbitrary finite fields $\mathbb{F}_q$, it is not possible to break the exponent $(d+1)/2$ and still cover all distances with the method in this paper and the distance energy in [Pham et al. 2017, Lemma 3.1]. More precisely, for $A \subset \mathbb{F}_q$, one can follow the proofs of Theorems 1.1 and 1.3 to get the conditions $|A^{2d+1}| \gg q^{(2d+2)/2+1/(4d)}$ and $|A^{2d}| \gg q^{(2d+1)/2+1/(4d-2)}$ for odd and even dimensions, respectively.

**Remark.** The Cauchy–Davenport theorem states that for subsets $X$ and $Y$ of $\mathbb{F}_p$, we have $|X+Y| \geq \min\{p, |X|+|Y|-1\}$. It is not hard to check that $\Delta(A^{2d}) = \Delta(A^d) + \Delta(A^d)$. The result of [Chapman et al. 2012] tells us that $|\Delta(A^d)| \geq p/2$ whenever $|A| \gg p^{d/(2d-1)}$. Therefore, one can apply the Cauchy–Davenport theorem to show that $|\Delta(A^{2d})| \geq p-1$ under the condition $|A| \geq p^d/(2d-1)$. However, our set $A^{2d}$ lies on the $2d$-dimensional space $\mathbb{F}_p^{2d}$; thus the exponent $d/(2d-1)$ is worse than the Iosevich–Rudnev's exponent $(2d+1)/(4d)$. The same happens for odd-dimensional spaces. Note that the bound $|\Delta(A^d)| \geq 1/c \cdot \min\{|A|^{2-1/2^{d-2}}, p\}$ with $c = 2^{(2^{d-1}-1)/2^{d-2}}$ in [Pham et al. 2019] is not suitable for this approach since the constant factor $1/c$ is too small.

Let $\mathbb{F}_q$ be an arbitrary finite field, and $\mathcal{E} \subset \mathbb{F}_q^d$. The product set of $\mathcal{E}$, denoted by $\Pi(\mathcal{E})$, is defined as follows:

$$\Pi(\mathcal{E}) := \{\boldsymbol{x} \cdot \boldsymbol{y} : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\}.$$

Using Fourier analysis, Hart and Iosevich [2008] proved that if $|\mathcal{E}| \gg q^{(d+1)/2}$, then $\Pi(\mathcal{E}) \supseteq \mathbb{F}_q \setminus \{0\}$. Moreover, under the same condition on the size of $\mathcal{E}$, we have that the number of pairs $(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{E} \times \mathcal{E}$ satisfying $\boldsymbol{x} \cdot \boldsymbol{y} = \lambda$ is $\sim q^{-1}|\mathcal{E}|^2$ for any $\lambda \neq 0$. If $\mathcal{E}$ has Cartesian product structure, i.e., $\mathcal{E} = A^d$ for some $A \subset \mathbb{F}_q$, then the condition $|\mathcal{E}| \gg q^{(d+1)/2}$ is equivalent with $|A| \gg q^{1/2+1/(2d)}$.

In the setting of prime fields $\mathbb{F}_p$, if $d = 8$, Glibichuk and Konyagin [2007] proved that for $A, B \subset \mathbb{F}_p$, if $|A|\lceil |B|/2 \rceil \geq p$, then we have $8A \cdot B = \mathbb{F}_p$. This result has been extended to arbitrary finite fields in [Glibichuk and Rudnev 2009].

In this paper, using the techniques in the proof of Theorem 1.3, we are able to obtain the following theorem.

**Theorem 1.5.** *For $A \subset \mathbb{F}_p$, suppose that $|A| \gtrsim p^{4/7}$; then*:

- $6A \cdot A = A \cdot A + A \cdot A + A \cdot A + A \cdot A + A \cdot A + A \cdot A = \mathbb{F}_p$.
- *For any $\lambda \in \mathbb{F}_p$, the number of pairs $(\boldsymbol{x}, \boldsymbol{y}) \in A^6 \times A^6$ such that $\boldsymbol{x} \cdot \boldsymbol{y} = \lambda$ is $\sim p^{-1}|A|^{12}$.*

Note that our exponent $4/7$ improves the exponent $7/12$ of Hart and Iosevich [2008] in the case $d = 6$. The following is the conjecture due to Iosevich.

**Conjecture 1.6.** *Let $A$ be a set in $\mathbb{F}_p$ and suppose that $|A| \gg p^{\frac{1}{2}+\epsilon}$ for any $\epsilon > 0$. Then,*

$$A \cdot A + A \cdot A = \mathbb{F}_p, \quad (A-A)^2 + (A-A)^2 = \mathbb{F}_p.$$

In the spirit of sum-product problems, it has been proved in [Pham et al. 2019] that for $A \subset \mathbb{F}_p$, if $|A| \ll p^{1/2+1/(5\cdot 2^{d-1}-2)}$, $d \geq 2$, then we have

$$\max\{|\Delta(A^d)|, |\Pi(A^d)|\} \gg |A|^{2-\frac{1}{5\cdot 2^d-3}}.$$

Using our energies (Lemmas 2.2 and 2.4 below), and the prime field analogue of Balog–Wooley decomposition energy due to Rudnev, Shkredov, and Stevens [Rudnev et al. 2020], we are able to give the energy variant of this result.

**Theorem 1.7.** *Let $d \geq 2$ be an integer and $A$ a set in $\mathbb{F}_p$ with $|A| \ll p^{1/2+1/(5\cdot 2^{d-1}-2)}$. There exist two disjoint subsets $B$ and $C$ of $A$ such that $A = B \sqcup C$ and*

$$\max\{E_d((B-B)^2), E_d(C \cdot C)\} \ll d^4(\log|A|)^4|A|^{4d-2+\frac{1}{5\cdot 2^{d-3}}},$$

*where $E_d((B-B)^2)$ is the number of $4d$-tuples $\{(a_i, b_i, c_i, e_i)\}_{i=1}^d$ with $a_i, c_i, b_i, e_i$ in $B$ such that $(a_1-b_1)^2+\cdots+(a_d-b_d)^2 = (c_1-e_1)^2+\cdots+(c_d-e_d)^2$, and $E_d(C\cdot C)$ be the number of $4d$-tuples $\{(a_i, b_i, c_i, e_i)\}_{i=1}^d$ with $a_i, c_i, b_i, e_i \in C$ such that $a_1b_1+\cdots+a_db_d = c_1e_1+\cdots+c_de_d$.*

## 2. Preliminaries

Let $E$ and $F$ be multisets in $\mathbb{F}_p^2$. We denote by $\bar{E}$ and $\bar{F}$ the sets of distinct elements in $E$ and $F$, respectively. For any multiset $X$, we use the notation $|X|$ to denote the size of $X$. For $\lambda \in \mathbb{F}_p$, let $N(E, F, \lambda)$ be the number of pairs $((e_1, e_2), (f_1, f_2)) \in E \times F$ such that $e_1f_1 + e_2 + f_2 = \lambda$. In the following lemma, we provide an upper bound and a lower bound of $N(E, F, \lambda)$ for any $\lambda \in \mathbb{F}_p$. Note that, this lemma is essentially the weighted version of the point-line incidences of [Vinh 2011] in the plane $\mathbb{F}_q^2$ (see also [Hanson et al. 2016, Lemma 14]).

**Lemma 2.1.** *Let $E$, $F$ be multisets in $\mathbb{F}_p^2$. For any $\lambda \in \mathbb{F}_p$, we have*

$$\left|N(E, F, \lambda) - \frac{|E||F|}{p}\right| \leq p^{\frac{1}{2}}\left(\sum_{(e_1,e_2)\in\bar{E}} m_E((e_1, e_2))^2 \sum_{(f_1,f_2)\in\bar{F}} m_F((f_1, f_2))^2\right)^{1/2},$$

*where $m_X((a, b))$ is the multiplicity of $(a, b)$ in $X$ with $X \in \{E, F\}$.*

*Proof.* Let $\chi$ be a nontrivial additive character on $\mathbb{F}_p$. We have

$$N(E, F, \lambda) = \sum_{(e_1,e_2)\in\bar{E},(f_1,f_2)\in\bar{F}} \frac{1}{p} m_E((e_1, e_2))m_F((f_1, f_2)) \sum_{s\in\mathbb{F}_p} \chi(s\cdot(e_1f_1+e_2+f_2-\lambda)).$$

This gives us

$$N(E, F, \lambda) = \frac{|E||F|}{p} + L,$$

where

$$L = \sum_{(e_1,e_2)\in\bar{E},(f_1,f_2)\in\bar{F}} m_E((e_1, e_2))m_F((f_1, f_2))\frac{1}{p}\sum_{s\neq 0}\chi(s\cdot(e_1f_1 + e_2 + f_2 - \lambda)).$$

If we view $L$ as a sum in $(e_1, e_2) \in \bar{E}$, then we can apply the Cauchy–Schwarz inequality to derive the following:

$$\begin{aligned}
L^2 \leq & \sum_{(e_1,e_2)\in\bar{E}} m_E((e_1, e_2))^2 \\
& \sum_{(e_1,e_2)\in\mathbb{F}_p^2} \frac{1}{p^2} \sum_{s,s'\neq 0} \sum_{(f_1,f_2),(f_1',f_2')\in\bar{F}} m_F((f_1, f_2))m_F((f_1', f_2')) \\
& \qquad \times\chi(s\cdot(e_1f_1 + e_2 + f_2 - \lambda))\chi(s'\cdot(-e_1f_1' - e_2 - f_2' + \lambda)) \\
= & \sum_{(e_1,e_2)\in\bar{E}} m_E((e_1, e_2))^2\frac{1}{p^2} \\
& \sum_{\substack{(e_1,e_2)\in\mathbb{F}_p^2,\ (f_1,f_2)\in\bar{F} \\ (f_1',f_2')\in\bar{F},\ s,s'\neq 0}} m_F((f_1, f_2))m_F((f_1', f_2'))\chi(e_1(sf_1 - s'f_1'))\chi(e_2(s - s')) \\
& \qquad \times\chi(s(f_2 - \lambda) - s'(f_2' - \lambda)) \\
= & \sum_{(e_1,e_2)\in\bar{E}} m_E((e_1, e_2))^2 \\
& \sum_{\substack{s\neq 0,\ (f_1,f_2)\in\bar{F} \\ (f_1',f_2')\in\bar{F},\ f_1=f_1'}} m_F((f_1, f_2))m_F((f_1', f_2'))\chi(s\cdot(f_2 - f_2')) = I + II,
\end{aligned}$$

where $I$ is the sum over all pairs $((f_1, f_2), (f_1, f_2'))$ with $f_2 = f_2'$, and $II$ is the sum over all pairs $((f_1, f_2), (f_1', f_2'))$ with $f_2 \neq f_2'$.

It is not hard to check that if $f_2 \neq f_2'$, then

$$\sum_{s\neq 0}\chi(s\cdot(f_2 - f_2')) = -1,$$

so $II < 0$. Note that $|II| \leq I$ since $L^2 \geq 0$.

On the other hand, if $f_2 = f_2'$, then

$$\sum_{s\neq 0}\chi(s\cdot(f_2 - f_2')) = p - 1.$$

In other words,

$$I \le p \sum_{(e_1,e_2)\in \bar{E}} m_E((e_1,e_2))^2 \sum_{(f_1,f_2)\in \bar{F}} m_F((f_1,f_2))^2,$$

which implies that

$$|L| \le \sqrt{I+II} \le p^{\frac{1}{2}} \left( \sum_{(e_1,e_2)\in \bar{E}} m_E((e_1,e_2))^2 \sum_{(f_1,f_2)\in \bar{F}} m_F((f_1,f_2))^2 \right)^{1/2}.$$

This completes the proof of the lemma. □

For $A \subset \mathbb{F}_p$, let $E_d((A-A)^2)$ be the number of $4d$-tuples $\{(a_i,b_i,c_i,e_i)\}_{i=1}^d$ with $a_i, c_i, b_i, e_i \in A$ such that

$$(a_1-b_1)^2+\cdots+(a_d-b_d)^2=(c_1-e_1)^2+\cdots+(c_d-e_d)^2.$$

Similarly, let $E_d(A\cdot A)$ be the number of $4d$-tuples $\{(a_i,b_i,c_i,e_i)\}_{i=1}^d$ with $a_i, c_i, b_i, e_i \in A$ such that

$$a_1b_1+\cdots+a_db_d=c_1e_1+\cdots+c_de_d.$$

In our next lemmas, we give recursive formulas for $E_d((A-A)^2)$ and $E_d(A\cdot A)$.

**Lemma 2.2.** *For $A \subset \mathbb{F}_p$, we have*

$$E_d((A-A)^2) \le Cd^2(\log|A|)^2\left(\frac{|A|^{4d}}{p}+|A|^{2d+1}\sqrt{E_{d-1}((A-A)^2)}\right),$$

*for some positive constant $C$.*

The proof of this lemma will be given in the next section. The following result is a direct consequence, which tells us an upper bound of $E_d((A-A)^2)$.

**Corollary 2.3.** *Let $A$ be a set in $\mathbb{F}_p$. For $d \ge 2$, suppose that $|A| \gg (d\log|A|)p^{1/2}$; then we have*

$$E_d((A-A)^2) \ll d^2(\log|A|)^2\frac{|A|^{4d}}{p}+d^4(\log|A|)^4|A|^{4d-2+\frac{1}{2^{d-1}}}.$$

*Proof.* We prove by induction on $d$ that

$$E_d((A-A)^2) \le 2C^2d^2(\log|A|)^2\frac{|A|^{4d}}{p}+2C^2d^4(\log|A|)^4|A|^{4d-2+\frac{1}{2^{d-1}}},$$

whenever $|A| \ge \sqrt{2}C(d\log|A|)p^{1/2}$, where the constant $C$ comes from Lemma 2.2.

The base case $d=2$ follows directly from Lemma 2.2 by using the trivial upper bound $|A|^3$ of $E_1((A-A)^2)$.

Suppose the statement holds for any $d-1 \geq 2$; we now prove that it also holds for $d$. Indeed, by induction hypothesis, we have

$$
\begin{aligned}
(1)\quad E_{d-1}((A-A)^2) &\leq 2C^2(d-1)^2(\log|A|)^2\frac{|A|^{4(d-1)}}{p} + 2C^2(d-1)^4(\log|A|)^4|A|^{4d-6+\frac{1}{2^{d-2}}} \\
&\leq 2C^2d^2(\log|A|)^2\frac{|A|^{4(d-1)}}{p} + 2C^2d^4(\log|A|)^4|A|^{4d-6+\frac{1}{2^{d-2}}}.
\end{aligned}
$$

On the other hand, it follows from Lemma 2.2 that

$$
(2)\quad E_d((A-A)^2) \leq Cd^2(\log|A|)^2\left(\frac{|A|^{4d}}{p} + |A|^{2d+1}\sqrt{E_{d-1}((A-A)^2)}\right).
$$

Putting (1) and (2) together, we obtain

$$
\begin{aligned}
E_d((A-A)^2) \leq Cd^2(\log|A|)^2\frac{|A|^{4d}}{p} &+ \sqrt{2}C^2d^2(\log|A|)^2|A|^{2d+1} \\
&\times\left(d\log|A|\frac{|A|^{2(d-1)}}{p^{1/2}} + d^2(\log|A|)^2|A|^{2d-3+\frac{1}{2^{d-1}}}\right).
\end{aligned}
$$

Since $\sqrt{2}C(d\log|A|)p^{1/2} \leq |A|$, we have

$$
\sqrt{2}C^2d\log|A|\frac{|A|^{2(d-1)}}{p^{1/2}} \leq C\frac{|A|^{2d-1}}{p}.
$$

This implies that

$$
E_d((A-A)^2) \leq 2Cd^2(\log|A|)^2\frac{|A|^{4d}}{p} + 2C^2d^4(\log|A|)^4|A|^{4d-2+\frac{1}{2^{d-1}}}. \qquad \square
$$

Similarly, for the case of product sets, we have:

**Lemma 2.4.** *For $A \subset \mathbb{F}_p$,*

$$
E_d(A\cdot A) \leq Cd^2(\log|A|)^2\left(\frac{|A|^{4d}}{p} + |A|^{2d+1}\sqrt{E_{d-1}(A\cdot A)}\right),
$$

*for some positive constant $C$.*

*Proof.* The proof of this lemma is almost identical to that of Lemma 2.2, so we omit it. $\square$

**Corollary 2.5.** *Let $A$ be a set in $\mathbb{F}_p$. For $d \geq 2$, suppose that $|A| \gg (d\log|A|)p^{1/2}$; then we have*

$$
E_d(A\cdot A) \ll d^2(\log|A|)^2\frac{|A|^{4d}}{p} + d^4(\log|A|)^4|A|^{4d-2+\frac{1}{2^{d-1}}}.
$$

*Proof.* The proof of Corollary 2.5 is identical to that of Corollary 2.3 with Lemma 2.4 in the place of Lemma 2.2; thus we omit it. $\square$

**2.1.** ***Proof of Lemma 2.2.*** In the proof of Lemma 2.2, we will use a point-plane incidence bound due to Rudnev [2018] and an argument in [Shkredov 2018, Theorem 32].

Let us first recall that if $\mathcal{R}$ is a set of points in $\mathbb{F}_p^3$ and $\mathcal{S}$ is a set of planes in $\mathbb{F}_p^3$, then the number of incidences between $\mathcal{R}$ and $\mathcal{S}$, denoted by $\mathcal{I}(\mathcal{R},\mathcal{S})$, is the cardinality of the set $\{(r,s)\in\mathcal{R}\times\mathcal{S} : r\in s\}$. The following is a version of Rudnev's point-plane incidence bound, which can be found in [de Zeeuw 2016].

**Theorem 2.6** [Rudnev 2018; de Zeeuw 2016]. *Let $\mathcal{R}$ be a set of points in $\mathbb{F}_p^3$ and $\mathcal{S}$ be a set of planes in $\mathbb{F}_p^3$, with $|\mathcal{R}|\le|\mathcal{S}|$. Suppose that there is no line that contains $k$ points of $\mathcal{R}$ and is contained in $k$ planes of $\mathcal{S}$. Then*

$$\mathcal{I}(\mathcal{R},\mathcal{S}) \ll \frac{|\mathcal{R}||\mathcal{S}|}{p} + |\mathcal{R}|^{1/2}|\mathcal{S}| + k|\mathcal{S}|.$$

*Proof of Lemma 2.2.* We first have

$$E_d((A-A)^2) = \sum_{t_1,t_2} r_{(d-1)(A-A)^2}(t_1) r_{(d-1)(A-A)^2}(t_2) f(t_1,t_2),$$

where $r_{(d-1)(A-A)^2}(t)$ is the number of $2(d-1)$ tuples $(a_1,\dots,a_{d-1},b_1,\dots,b_{d-1})$ in $A^{2d-2}$ such that $(a_1-b_1)^2+\cdots+(a_{d-1}-b_{d-1})^2=t$, and $f(t_1,t_2)$ is the sum $\sum_s r_{(A-A)^2+t_1}(s) r_{(A-A)^2+t_2}(s)$. We now split the sum $E_d((A-A)^2)$ into intervals:

$$E_d((A-A)^2) \ll \sum_{i=1}^{L_1}\sum_{j=1}^{L_2}\sum_{t_1,t_2} f(t_1,t_2) r^{(i)}_{(d-1)(A-A)^2}(t_1) r^{(j)}_{(d-1)(A-A)^2}(t_2),$$

where $L_1\le\log(|A|^{2d-2})$, $L_2\le\log(|A|^{2d-2})$, and $r^{(i)}_{(d-1)(A-A)^2}(t_1)$ is the restriction of the function $r_{(d-1)(A-A)^2}(x)$ on the set $P_i := \{t : 2^i \le r_{(d-1)(A-A)^2}(t) < 2^{i+1}\}$.

Using the pigeon-hole principle two times, there exist sets $P_{i_0}$ and $P_{j_0}$ for some $i_0$ and $j_0$ such that

$$\begin{aligned} E_d((A-A)^2) &\le (2d-2)^2(\log|A|)^2 \sum_{t_1,t_2} f(t_1,t_2) r^{(i_0)}_{(d-1)(A-A)^2}(t_1) r^{(j_0)}_{(d-1)(A-A)^2}(t_2) \\ &\ll d^2(\log|A|)^2 2^{i_0} 2^{j_0} \sum_{t_1,t_2} f(t_1,t_2) P_{i_0}(t_1) P_{j_0}(t_2). \end{aligned}$$

One can check that the sum $\sum_{t_1,t_2} f(t_1,t_2) P_{i_0}(t_1) P_{j_0}(t_2)$ is equal to the number of incidences between the point set $\mathcal{R}$ of points $(-2a, e, t_1+a^2-e^2)\in\mathbb{F}_p^3$ with $a\in A$, $e\in A$, $t_1\in P_{i_0}$, and the plane set $\mathcal{S}$ of planes in $\mathbb{F}_p^3$ defined by

$$bX + 2cY + Z = t_2 - b^2 + c^2,$$

where $b\in A$, $c\in A$ and $t_2\in P_{j_0}$. Without loss of generality, we can assume that $|P_{i_0}|\le|P_{j_0}|$.

To apply Theorem 2.6, we need to bound the maximal number of collinear points in $\mathcal{R}$. The projection of $\mathcal{R}$ into the plane of the first two coordinates is the set $-2A \times A$; thus if a line is not vertical, then it contains at most $|A|$ points from $\mathcal{R}$. If a line is vertical, then it contains at most $|P_{i_0}|$ points from $\mathcal{R}$, but that line is not contained in any plane in $\mathcal{S}$. In other words, we can apply Theorem 2.6 with $k = |A|$, and obtain

$$\sum_{t_1,t_2} f(t_1,t_2)P_{i_0}(t_1)P_{j_0}(t_2) \ll \frac{|A|^4|P_{i_0}||P_{j_0}|}{p} + |A|^3|P_{i_0}|^{1/2}|P_{j_0}| + |A|^3|P_{j_0}|$$
$$\ll \frac{|A|^4|P_{i_0}||P_{j_0}|}{p} + |A|^3|P_{i_0}|^{1/2}|P_{j_0}|.$$

We now fall into the following cases:

**Case 1:** If the first term dominates, we have

$$\sum_{t_1,t_2} f(t_1,t_2)P_{i_0}(t_1)P_{j_0}(t_2) \ll \frac{|A|^4|P_{i_0}||P_{j_0}|}{p}.$$

**Case 2:** If the second term dominates, we have

$$\sum_{t_1,t_2} f(t_1,t_2)P_{i_0}(t_1)P_{j_0}(t_2) \ll |A|^3|P_{i_0}|^{1/2}|P_{j_0}|.$$

Therefore,

$$E_d((A-A)^2) \ll d^2(\log|A|)^2 2^{i_0}2^{j_0}\left(\frac{|A|^4|P_{i_0}||P_{j_0}|}{p} + |A|^3|P_{i_0}|^{1/2}|P_{j_0}|\right)$$
$$\ll d^2(\log|A|)^2\left(\frac{|A|^{4d}}{p} + |A|^{2d+1}\sqrt{E_{d-1}((A-A)^2)}\right),$$

where we have used the facts that

- $2^{i_0}|P_{i_0}|^{1/2} \ll \sqrt{E_{d-1}((A-A)^2)}$.
- $2^{j_0}|P_{j_0}| \ll |A|^{2d-2}$.
- $2^{i_0}|P_{i_0}| \ll |A|^{2d-2}$.

This completes the proof of the lemma. □

## 3. Proof of Theorem 1.1

*Proof of Theorem 1.1.* Let $\lambda$ be an arbitrary element in $\mathbb{F}_p$. Let $E$ be the multiset of points $(2x, x^2+(y_1-z_1)^2+\cdots+(y_d-z_d)^2) \in \mathbb{F}_p^2$ with $x, y_i, z_i \in A$, and $F$ be the multiset of points $(-t, t^2+(u_1-v_1)^2+\cdots+(u_d-v_d)^2) \in \mathbb{F}_p^2$ with $t, u_i, v_i \in A$. We have $|E| = |F| = |A|^{2d+1}$.

It follows from Lemma 2.1 that

$$(3)\quad \left|N(E,F,\lambda)-\frac{|E||F|}{p}\right| \le p^{\frac{1}{2}}\left(\sum_{(e_1,e_2)\in\bar{E}} m_E((e_1,e_2))^2 \sum_{(f_1,f_2)\in\bar{F}} m_F((f_1,f_2))^2\right)^{1/2}.$$

We observe that $N(E,F,\lambda)$ equals the number of pairs $(\boldsymbol{x},\boldsymbol{y})\in A^{2d+1}\times A^{2d+1}$ such that $\|\boldsymbol{x}-\boldsymbol{y}\|=\lambda$.

From the setting of $E$ and $F$, it is not hard to see that

$$(4)\quad \begin{aligned}\sum_{(e_1,e_2)\in\bar{E}} m_E((e_1,e_2))^2 &= |A|E_d((A-A)^2),\\ \sum_{(f_1,f_2)\in\bar{F}} m_F((f_1,f_2))^2 &= |A|E_d((A-A)^2).\end{aligned}$$

Putting (3) and (4) together, we have

$$(5)\quad \left|N(E,F,\lambda)-\frac{|A|^{4d+2}}{p}\right| \le p^{\frac{1}{2}}|A|E_d((A-A)^2).$$

On the other hand, Corollary 2.3 gives us

$$(6)\quad E_d((A-A)^2) \ll d^2(\log|A|)^2\frac{|A|^{4d}}{p}+d^4(\log|A|)^4|A|^{4d-2+\frac{1}{2^{d-1}}}.$$

Substituting (6) into (5), we obtain $N(E,F,\lambda)\sim|A|^{4d+2}p^{-1}$ whenever

$$|A^{2d+1}| \gtrsim_d p^{\frac{2d+2}{2}-\frac{3\cdot2^{d-2}-d-1}{3\cdot2^{d-1}-1}}.$$

Since $\lambda$ is arbitrary in $\mathbb{F}_p$, the theorem follows. □

## 4. Proofs of Theorems 1.3 and 1.5

The proof of Theorem 1.3 is similar to that of Theorem 1.1, but we need a higher-dimensional version of Lemma 2.1.

Let $E$ and $F$ be multisets in $\mathbb{F}_p^3$. For $\lambda\in\mathbb{F}_p$, let $N(E,F,\lambda)$ be the number of pairs $((e_1,e_2,e_3),(f_1,f_2,f_3))\in E\times F$ such that $e_1f_1+e_2f_2+e_3+f_3=\lambda$. One can follow step by step the proof of Lemma 2.1 to obtain the following.

**Lemma 4.1.** *Let $E$, $F$ be multisets in $\mathbb{F}_p^3$. For any $\lambda\in\mathbb{F}_p$, we have*

$$\left|N(E,F,\lambda)-\frac{|E||F|}{p}\right| \le p\left(\sum_{(e_1,e_2,e_3)\in\bar{E}} m_E((e_1,e_2,e_3))^2 \sum_{(f_1,f_2,f_3)\in\bar{F}} m_F((f_1,f_2,f_3))^2\right)^{1/2}.$$

We are now ready to prove Theorem 1.3.

*Proof of Theorem 1.3.* Let $\lambda$ be an arbitrary element in $\mathbb{F}_p$. Let $E$ be the multiset of points $(2x_1, 2x_2, x_1^2+x_2^2+(y_1-z_1)^2+\cdots+(y_{d-1}-z_{d-1})^2) \in \mathbb{F}_p^3$ with $x_i, y_i, z_i \in A$, and $F$ the multiset of points $(-t_1, -t_2, t_1^2+t_2^2+(u_1-v_1)^2+\cdots+(u_{d-1}-v_{d-1})^2) \in \mathbb{F}_p^3$ with $t_i, u_i, v_i \in A$. We have $|E| = |A|^{2d}$ and $|F| = |A|^{2d}$.

It follows from Lemma 4.1 that

$$\left|N(E,F,\lambda) - \frac{|E||F|}{p}\right| \leq p\left(\sum_{(e_1,e_2,e_3)\in\bar{E}} m_E((e_1,e_{2,3}))^2 \sum_{(f_1,f_2,f_3)\in\bar{F}} m_F((f_1,f_2,f_3))^2\right)^{1/2}. \tag{7}$$

We observe that $N(E,F,\lambda)$ is equal to the number of pairs $(\boldsymbol{x},\boldsymbol{y}) \in A^{2d}\times A^{2d}$ such that $\|\boldsymbol{x}-\boldsymbol{y}\| = \lambda$.

From the setting of $E$ and $F$, it is not hard to see that

$$\begin{aligned}\sum_{(e_1,e_2,e_3)\in\bar{E}} m_E((e_1,e_2,e_3))^2 &= |A|^2 E_{d-1}((A-A)^2),\\ \sum_{(f_1,f_2,f_3)\in\bar{F}} m_F((f_1,f_2,f_3))^2 &= |A|^2 E_{d-1}((A-A)^2).\end{aligned} \tag{8}$$

Putting (7) and (8) together, we have

$$\left|N(E,F,\lambda) - \frac{|A|^{4d}}{p}\right| \leq p|A|^2 E_{d-1}((A-A)^2). \tag{9}$$

On the other hand, Corollary 2.3 gives us

$$E_{d-1}((A-A)^2) \ll d^2(\log|A|)^2\frac{|A|^{4d-4}}{p} + d^4(\log|A|)^4|A|^{4d-6+\frac{1}{2^{d-2}}}. \tag{10}$$

Substituting (10) into (9), we obtain $N(E,F,\lambda) \sim |A|^{4d}p^{-1}$ whenever

$$|A^{2d}| \gtrsim_d p^{\frac{2d+1}{2}-\frac{2^d-2d-1}{2^{d+1}-2}}.$$

Since $\lambda$ is arbitrary in $\mathbb{F}_p$, the theorem follows. □

*Proof of Theorem 1.5.* The proof of Theorem 1.5 is similar to that of Theorem 1.3 with Corollary 2.5 in the place of Corollary 2.3. □

## 5. Proof of Theorem 1.7

Let us first recall the prime field analogue of Balog–Wooley decomposition energy due to Rudnev, Shkredov and Stevens [Rudnev et al. 2020].

**Theorem 5.1** [Rudnev et al. 2020]. *Let $A$ be a set in $\mathbb{F}_p$ with $|A| \le p^{5/8}$. There exist two disjoint subsets $B$ and $C$ of $A$ such that $A = B \sqcup C$ and*

$$\max\{E^+(B), E^\times(C)\} \lesssim |A|^{14/5},$$

*where*

$$E^+(B) = |\{(a,b,c,d) \in B^4 : a+b=c+d\}|, \quad E^\times(C) = |\{(a,b,c,d) \in C^4 : ab=cd\}|.$$

We refer the interested reader to [Balog and Wooley 2017] for the original result over $\mathbb{R}$. The most up to date bound for this result over $\mathbb{R}$ is due to Shakan [2019].

The following is another corollary of Lemma 2.2.

**Corollary 5.2.** *Let $A$ be a set in $\mathbb{F}_p$, and $B$ be a subset of $A$. For an integer $d \ge 2$, suppose that $|A| \ll p^{1/2+1/(5\cdot 2^{d-1}-2)}$ and $E^+(B) \lesssim |A|^{14/5}$; then we have*

$$E_d((B-B)^2) \ll d^4(\log|A|)^4 |A|^{4d-2+\frac{1}{5\cdot 2^{d-3}}}.$$

*Proof.* We prove by induction on $d$ that

$$E_d((B-B)^2) \le 4C^2 d^4 (\log|A|)^4 |A|^{4d-2+\frac{1}{5\cdot 2^{d-3}}},$$

whenever $|A| \le (Cp)^{1/2+1/(5\cdot 2^{d-1}-2)}$, where the constant $C$ comes from Lemma 2.2.

The base case $d = 2$ follows from Lemma 2.2 and the facts that $E_1((B-B)^2) \ll E^+(B)$ and $|B| \le |A|$.

Suppose the corollary holds for $d-1 \ge 2$. We now show that it also holds for general $d$. Indeed, it follows from Lemma 2.2 that

$$E_d((B-B)^2) \le Cd^2(\log|A|)^2 \left( \frac{|B|^{4d}}{p} + |B|^{2d+1} \sqrt{E_{d-1}((B-B)^2)} \right).$$

On the other hand, by the inductions hypothesis, we have

$$\begin{aligned} E_{d-1}((B-B)^2) &\le 4C^2(d-1)^4(\log|A|)^4 |A|^{4d-6+\frac{1}{5\cdot 2^{d-4}}} \\ &\le 4C^2 d^4 (\log|A|)^4 |A|^{4d-6+\frac{1}{5\cdot 2^{d-4}}}. \end{aligned}$$

Thus, using the fact that $|B| \le |A|$, we obtain

$$\begin{aligned} E_d((B-B)^2) &\le d^2(\log|A|)^2 \left( C\frac{|A|^{4d}}{p} + 2C^2 d^2 (\log|A|)^2 |A|^{4d-2+\frac{1}{5\cdot 2^{d-3}}} \right) \\ &\le 4C^2 d^4 (\log|A|)^4 |A|^{4d-2+\frac{1}{5\cdot 2^{d-3}}}, \end{aligned}$$

whenever $|A| \le (Cp)^{1/2+1/(5\cdot 2^{d-1}-2)}$. □

Using the same argument, we also have another corollary of Lemma 2.4.

**Corollary 5.3.** *Let $A$ be a set in $\mathbb{F}_p$, and $C$ be a subset of $A$. For an integer $d \geq 2$, suppose that $|A| \ll p^{1/2+1/(5\cdot 2^{d-1}-2)}$ and $E^{\times}(C) \lesssim |A|^{14/5}$; then we have*

$$E_d(C \cdot C) \ll d^4(\log|A|)^4|A|^{4d-2+\frac{1}{5\cdot 2^{d-3}}}.$$

We are now ready to prove Theorem 1.7.

*Proof of Theorem 1.7.* It follows from Theorem 5.1 that there exist two disjoint subsets $B$ and $C$ of $A$ such that $A = B \sqcup C$ and $\max\{E^{+}(B), E^{\times}(C)\} \lesssim |A|^{14/5}$. One now can apply Corollaries 5.2 and 5.3 to derive

$$\max\{E_d((B-B)^2), E_d(C \cdot C)\} \ll d^4(\log|A|)^4|A|^{4d-2+\frac{1}{5\cdot 2^{d-3}}}. \qquad \square$$

**Acknowledgments:**

The authors are grateful to the referee for useful comments and corrections. Pham was supported by Swiss National Science Foundation grant P400P2-183916. Vinh was supported by the National Foundation for Science and Technology Development Project. 101.99-2019.318.

## References

[Balog and Wooley 2017] A. Balog and T. D. Wooley, "A low-energy decomposition theorem", *Q. J. Math.* **68**:1 (2017), 207–226. MR

[Bennett et al. 2017] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, and M. Rudnev, "Group actions and geometric combinatorics in $\mathbb{F}_q^d$", *Forum Math.* **29**:1 (2017), 91–110. MR

[Bourgain et al. 2004] J. Bourgain, N. Katz, and T. Tao, "A sum-product estimate in finite fields, and applications", *Geom. Funct. Anal.* **14**:1 (2004), 27–57. MR

[Chapman et al. 2012] J. Chapman, M. B. Erdoğan, D. Hart, A. Iosevich, and D. Koh, "Pinned distance sets, $k$-simplices, Wolff's exponent in finite fields and sum-product estimates", *Math. Z.* **271**:1-2 (2012), 63–93. MR

[Du et al. 2018] X. Du, L. Guth, Y. Ou, H. Wang, B. Wilson, and R. Zhang, "Weighted restriction estimates and application to Falconer distance set problem", 2018. arXiv

[Erdös 1946] P. Erdös, "On sets of distances of $n$ points", *Amer. Math. Monthly* **53** (1946), 248–250. MR

[Falconer 1985] K. J. Falconer, "On the Hausdorff dimensions of distance sets", *Mathematika* **32**:2 (1985), 206–212. MR

[Glibichuk and Konyagin 2007] A. A. Glibichuk and S. V. Konyagin, "Additive properties of product sets in fields of prime order", pp. 279–286 in *Additive combinatorics*, edited by M. B. N. Andrew Granville and J. Solymos, CRM Proc. Lecture Notes **43**, Amer. Math. Soc., Providence, RI, 2007. MR

[Glibichuk and Rudnev 2009] A. Glibichuk and M. Rudnev, "On additive properties of product sets in an arbitrary finite field", *J. Anal. Math.* **108** (2009), 159–170. MR

[Guth and Katz 2015] L. Guth and N. H. Katz, "On the Erdős distinct distances problem in the plane", *Ann. of Math.* (2) **181**:1 (2015), 155–190. MR

[Guth et al. 2020] L. Guth, A. Iosevich, Y. Ou, and H. Wang, "On Falconer's distance set problem in the plane", *Invent. Math.* **219**:3 (2020), 779–830. MR

[Hanson et al. 2016] B. Hanson, B. Lund, and O. Roche-Newton, "On distinct perpendicular bisectors and pinned distances in finite fields", *Finite Fields Appl.* **37** (2016), 240–264. MR

[Hart and Iosevich 2008] D. Hart and A. Iosevich, "Sums and products in finite fields: an integral geometric viewpoint", pp. 129–135 in *Radon transforms, geometry, and wavelets*, edited by G. Ólafsson et al., Contemp. Math. **464**, Amer. Math. Soc., Providence, RI, 2008. MR

[Hart et al. 2011] D. Hart, A. Iosevich, D. Koh, and M. Rudnev, "Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős–Falconer distance conjecture", *Trans. Amer. Math. Soc.* **363**:6 (2011), 3255–3275. MR

[Iosevich and Rudnev 2007] A. Iosevich and M. Rudnev, "Erdős distance problem in vector spaces over finite fields", *Trans. Amer. Math. Soc.* **359**:12 (2007), 6127–6142. MR

[Murphy and Petridis 2019] B. Murphy and G. Petridis, "An example related to the Erdős–Falconer question over arbitrary finite fields", *Bull. Hellenic Math. Soc.* **63** (2019), 38–39. MR

[Pham et al. 2017] D. H. Pham, T. Pham, and L. A. Vinh, "An improvement on the number of simplices in $\mathbb{F}_q^d$", *Discrete Appl. Math.* **221** (2017), 95–105. MR

[Pham et al. 2019] T. Pham, L. A. Vinh, and F. de Zeeuw, "Three-variable expanding polynomials and higher-dimensional distinct distances", *Combinatorica* **39**:2 (2019), 411–426. MR

[Rudnev 2018] M. Rudnev, "On the number of incidences between points and planes in three dimensions", *Combinatorica* **38**:1 (2018), 219–254. MR

[Rudnev et al. 2020] M. Rudnev, I. Shkredov, and S. Stevens, "On the energy variant of the sum-product conjecture", *Rev. Mat. Iberoam.* **36**:1 (2020), 207–232. MR

[Shakan 2019] G. Shakan, "On higher energy decompositions and the sum-product phenomenon", *Math. Proc. Cambridge Philos. Soc.* **167**:3 (2019), 599–617. MR

[Shkredov 2018] I. D. Shkredov, "On asymptotic formulae in some sum-product questions", *Trans. Moscow Math. Soc.* **79** (2018), 231–281. MR

[Solymosi and Vu 2008] J. Solymosi and V. H. Vu, "Near optimal bounds for the Erdős distinct distances problem in high dimensions", *Combinatorica* **28**:1 (2008), 113–125. MR

[Vinh 2011] L. A. Vinh, "The Szemerédi–Trotter type theorem and the sum-product estimate in finite fields", *European J. Combin.* **32**:8 (2011), 1177–1181. MR

[de Zeeuw 2016] F. de Zeeuw, "A short proof of Rudnev's point-plane incidence bound", 2016. arXiv

Received June 18, 2020. Revised July 22, 2020.

THANG PHAM
DEPARTMENT OF MATHEMATICS
ETH, ZURICH
ZURICH
SWITZERLAND
phamanhthang.vnu@gmail.com

LÊ ANH VINH
VIETNAM INSTITUTE OF EDUCATIONAL SCIENCES
HA NOI
VIETNAM
vinhle@vnies.edu.vn

# PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

**EDITORS**

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Matthias Aschenbrenner
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
matthias@math.ucla.edu

Paul Balmer
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
balmer@math.ucla.edu

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Daryl Cooper
Department of Mathematics
University of California
Santa Barbara, CA 93106-3080
cooper@math.ucsb.edu

Wee Teck Gan
Mathematics Department
National University of Singapore
Singapore 119076
matgwt@nus.edu.sg

Kefeng Liu
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
liu@math.ucla.edu

Jiang-Hua Lu
Department of Mathematics
The University of Hong Kong
Pokfulam Rd., Hong Kong
jhlu@maths.hku.hk

Sorin Popa
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
popa@math.ucla.edu

Jie Qing
Department of Mathematics
University of California
Santa Cruz, CA 95064
qing@cats.ucsc.edu

Paul Yang
Department of Mathematics
Princeton University
Princeton NJ 08544-1000
yang@math.princeton.edu

**PRODUCTION**

Silvio Levy, Scientific Editor, production@msp.org

**SUPPORTING INSTITUTIONS**

ACADEMIA SINICA, TAIPEI
CALIFORNIA INST. OF TECHNOLOGY
INST. DE MATEMÁTICA PURA E APLICADA
KEIO UNIVERSITY
MATH. SCIENCES RESEARCH INSTITUTE
NEW MEXICO STATE UNIV.
OREGON STATE UNIV.
STANFORD UNIVERSITY
UNIV. OF BRITISH COLUMBIA
UNIV. OF CALIFORNIA, BERKELEY
UNIV. OF CALIFORNIA, DAVIS
UNIV. OF CALIFORNIA, LOS ANGELES
UNIV. OF CALIFORNIA, RIVERSIDE
UNIV. OF CALIFORNIA, SAN DIEGO
UNIV. OF CALIF., SANTA BARBARA
UNIV. OF CALIF., SANTA CRUZ
UNIV. OF MONTANA
UNIV. OF OREGON
UNIV. OF SOUTHERN CALIFORNIA
UNIV. OF UTAH
UNIV. OF WASHINGTON
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2020 is US $520/year for the electronic version, and $705/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2020 Mathematical Sciences Publishers

# PACIFIC JOURNAL OF MATHEMATICS

Volume 309 No. 2 December 2020



Thin subgroups isomorphic to Gromov–Piatetski-Shapiro lattices 257
SAMUEL A. BALLAS

Value distribution properties for the Gauss maps of the immersed harmonic surfaces 267
XINGDI CHEN, ZHIXUE LIU and MIN RU

Scattered representations of $SL(n, \mathbb{C})$ 289
CHAO-PING DONG and KAYUE DANIEL WONG

Number of singular fibres of surface fibrations over $\mathbb{P}^1$ 313
CHENG GONG and YI GU

Asymptotic behavior of solutions for some elliptic equations in exterior domains 333
ZONGMING GUO and ZHONGYUAN LIU

Ulrich elements in normal simplicial affine semigroups 353
JÜRGEN HERZOG, RAHELEH JAFARI and DUMITRU I. STAMATE

Notes on equivariant homology with constant coefficients 381
SOPHIE KRIZ

Local normal forms for multiplicity free $U(n)$ actions on coadjoint orbits 401
JEREMY LANE

Functional determinant on pseudo-Einstein 3-manifolds 421
ALI MAALAOUI

Distribution of distances in positive characteristic 437
THANG PHAM and LÊ ANH VINH

Elliptic gradient estimates for a parabolic equation with $V$-Laplacian and applications 453
JIAN-HONG WANG and YU ZHENG

Optimal $L^2$ extension of sections from subvarieties in weakly pseudoconvex manifolds 475
XIANGYU ZHOU and LANGFENG ZHU