Canad. Math. Bull. Vol. 69 (1), 2026, pp. 116–130
http://dx.doi.org/10.4153/S0008439525100866
© The Author(s), 2025. Published by Cambridge University Press on behalf of Canadian Mathematical Society. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

On a theorem of Mattila in the finite p-adic setting

Boqing Xue, Thang Pham, Quang-Hung Le, Quang-Ham Le, and Duy-Phuong Nguyen

Abstract. Let A and B be subsets of $(\mathbb{Z}/p^r\mathbb{Z})^2$. In this note, we provide conditions on the densities of A and B such that $|gA - B| \gg p^{2r}$ for a positive proportion of $g \in SO_2(\mathbb{Z}/p^r\mathbb{Z})$. The conditions are sharp up to constant factors in the unbalanced case, and the proof makes use of tools from discrete Fourier analysis and results in restriction/extension theory.

1 Introduction

We begin with the following question.

Question 1.1 Let p be a prime, and A, B be subsets in $\mathbb{F}_p^d$. Under what conditions on A and B do we have $|gA - B| \gg p^d$ for a positive proportion of $g \in SO_d(\mathbb{F}_p)$?

The original version of this question was posed in the Euclidean setting and has a well-known history, which we will not detail here. It is necessary to mention that for $A, B \subset \mathbb{R}^d$ with $\dim_H(A) + \dim_H(B) > d$, Mattila [8] proved that if

$$\frac{(d-1)}{d}\dim_H(A) + \dim_H(B) > d \quad \text{or} \quad \dim_H(B) > \frac{d+1}{2},$$

then $\mathcal{L}^d(gA - B) > 0$ for almost all orthogonal matrices g in $\mathbb{R}^d$. Here, by $\dim_H$ and $\mathcal{L}(\cdot)$ we mean the Hausdorff dimension and the Lebesgue measure in $\mathbb{R}^d$, respectively. In two dimensions with $\dim_H(A) = \dim_H(B) = t$, he asked in the survey paper [9] whether or not the condition $t > 5/4$ would be enough to guarantee that $\mathcal{L}(gA - B) > 0$ by using the techniques due to Guth, Iosevich, Ou, and Wang in [2] on the Falconer distance problem.

In a recent paper, Pham and Yoo [12] answered this question affirmatively in the prime field setting by showing that if $|A| = |B| \gg p^{5/4}$ and $p \equiv 3 \pmod 4$, then there exists a set $E \subset SO_2(\mathbb{F}_p)$ with $|E| < p/2$ such that for each $g \in SO_2(\mathbb{F}_p)\backslash E$ there are at least $\gg p^2$ elements $z \in \mathbb{F}_p^2$ satisfying $|(gA + z) \cap B| \sim \frac{|A||B|}{p^2}$. When $p \equiv 1 \pmod 4$,

Received by the editors February 10, 2025; revised February 10, 2025; accepted June 29, 2025.
Published online on Cambridge Core July 14, 2025.
Author ordering is randomized.
AMS subject classification: **11T06**, **11L07**, **52C10**.
Keywords: Intersection patterns, p-adic, restriction/extension estimates, distance problems.

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

their method implies a weaker exponent, namely, 3/2 instead of 5/4. Notice that these exponents cannot be reduced to a number less than 1, to see this, one takes two sets A and B being on a circle centered at the origin of radius 1, then it is clear that $|gA - B| \sim |A||B|$.

In this note, we are interested in studying this topic in the plane over a finite p-adic ring. In particular, we consider the following question. Write $\delta_A = |A|/p^{2r}$ for any set $A \subset (\mathbb{Z}/p^r\mathbb{Z})^2$.

Question 1.2 Let A *and* B be sets in $(\mathbb{Z}/p^r\mathbb{Z})^2$. Under what conditions on δ_A and δ_B do we have that $|gA - B| \gg p^{2r}$ for a positive proportion of $g \in SO_2(\mathbb{Z}/p^r\mathbb{Z})$?

The following examples show that in order to have $|gA - B| \gg p^{2r}$, the sets A and B cannot both be small.

Example 1.3 Let $X = \{\mathbf{x} \in (\mathbb{Z}/p^r\mathbb{Z})^2 : \mathbf{x} \equiv \mathbf{0} \pmod{p}\}$. Let A (and B) be disjoint unions of m (and n, respectively,) cosets of X, where $1 \le m, n \le p^2$. So, $|A| = mp^{2r-2}$ and $|B| = np^{2r-2}$. One sees that $|gA| \le mp^{2r-2}$ and $|gA - B| \le mnp^{2r-2}$.

Our main theorem reads as follows.

Theorem 1.4 *Let p be a prime with $p \equiv 3 \pmod 4$, and r be a positive integer. Let A and $B \subset (\mathbb{Z}/p^r\mathbb{Z})^2$ be such that $\delta_A^{1/2} \cdot \delta_B \ge 2p^{-1}$. Then for a positive proportion of $g \in SO_2(\mathbb{Z}/p^r\mathbb{Z})$, we have*

$$|gA - B| \gg p^{2r}.$$

Based on Example 1.3, the condition $\delta_A^{1/2} \cdot \delta_B \ge 2p^{-1}$ is sharp up to constant factors. Indeed, if we take $m = 1$ and $n = \gamma(p)p^2$ with $\gamma(p)$ tending to 0 arbitrarily slowly as p tends to infinity, then $\delta_A^{1/2}\delta_B = \gamma(p)p^{-1}$ and $|gA - B| \le \gamma(p)p^{2r}$. Example 1.3 is most interesting when $r > 1$ since it shows the sharpness of the exponent 1/2 on the density condition of A.

To prove this result, we make use of tools from discrete Fourier analysis and results in restriction/extension theory. As in the finite field setting [12], the key estimate in our proof is the following sum:

$$\sum_{\mathbf{m}\neq\mathbf{0}} \sum_{\mathbf{m}'\in V_{\mathbf{m}}} \left|\widehat{A}(\mathbf{m})\right|^2 \left|\widehat{B}(\mathbf{m}')\right|^2,$$

where $V_{\mathbf{m}} := \{g\mathbf{m} : g \in SO_2(\mathbb{Z}/p^r\mathbb{Z})\}$. There are several approaches one can use to bound this sum:

1. Using the Plancherel formula is a standard argument and often yields a weak bound.
2. A more advanced approach employs restriction/extension estimates associated with circles. While such estimates are well understood in the finite field setting, see [1, 3], for example, they have only recently been developed in the p-adic setting [11]. This method will be used to prove Theorem 1.4.

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

3. When $r = 1$, a novel method, combining the L^2 norm of the distance function from [7] with a double-counting argument, is introduced in [12]. Extending this approach to the p-adic setting, however, presents challenges due to the limited understanding of incidence structures, particularly those involving points and planes in $(\mathbb{Z}/p^r\mathbb{Z})^3$. We hope to address this issue in the near future.

Although Theorem 1.4 is not as strong as Pham and Yoo's result in [12], it establishes that if $\delta_A^{1/2} \cdot \delta_B \geq 2p^{-1}$, then $|gA - B| \gg p^2$ for a positive proportion of $g \in SO_2(\mathbb{Z}/p\mathbb{Z})$. This aligns directly with Mattila's theorem in [8] with $d = 2$, as mentioned above.

Notice that when $p \equiv 1 \pmod 4$, the restriction/extension estimates are weaker, so the proof of Theorem 1.4 implies the condition of $\delta_A^{1/2} \cdot \delta_B \geq 2p^{-1/2}$. This is worse than the next theorem, which will be proved by using the Plancherel formula directly.

Theorem 1.5 *Let p be a prime with $p \equiv 1 \pmod 4$, and r be a positive integer. Let A and $B \subset (\mathbb{Z}/p^r\mathbb{Z})^2$ be such that $\delta_A \cdot \delta_B \geq 2p^{-1}$. Then for a positive proportion of $g \in SO_2(\mathbb{Z}/p^r\mathbb{Z})$, we have*

$$|gA - B| \gg p^{2r}.$$

In Example 1.3, by taking $A = B = X + Y$, where $Y \subset \{(x_1, x_2) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) : x_1^2 + x_2^2 \equiv 1 \pmod p\}$, then, for any $g \in SO_2(\mathbb{Z}/p^r\mathbb{Z})$, we have $|A| = |B| = |Y| \cdot p^{2r-2}$ and $|gA - B| \ll |Y|^2 \cdot p^{2r-2}$. Therefore, it is reasonable to make the following conjecture on the balanced case.

Conjecture 1.6 *Let p be an odd prime, and r be a positive integer. Let A and $B \subset (\mathbb{Z}/p^r\mathbb{Z})^2$ be such that $\delta_A = \delta_B \gg p^{-1}$. Then for a positive proportion of $g \in SO_2(\mathbb{Z}/p^r\mathbb{Z})$, we have*

$$|gA - B| \gg p^{2r}.$$

This conjecture appears highly challenging and could be as difficult as the Erdős-Falconer distance problem. Regarding further open questions, a natural direction is to explore similar problems in other group settings or in higher dimensions. To generalize Theorem 1.4 to higher dimensions, the first step is to extend the results in Section 2, but we found these extensions too complicated in this setting. This suggests exploring alternative approaches to address the problem. We refer the reader to [4, 5, 6, 11] for recent progress on the distance problem and extensions in the finite p-adic setting.

Notations 1 In this article, by $X \gg Y$ we mean $X \geq CY$ for some absolute positive constant C, and $X \sim Y$ means $X \gg Y$ and $Y \gg X$.

2 Preliminaries

Throughout this article, the letter p always denotes an odd prime, and r a positive integer.

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

Let

$$G_r := SO_2(\mathbb{Z}/p^r\mathbb{Z}) = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \pmod{p^r} : \ a^2 + b^2 \equiv 1 \pmod{p^r} \right\}.$$

For $\mathbf{x} = (x_1, x_2) \in (\mathbb{Z}/p^r\mathbb{Z})^2$, the distance function is denoted by $\|\mathbf{x}\| := x_1^2 + x_2^2 \pmod{p^r}$. Then $\|g\mathbf{x}\| \equiv \|\mathbf{x}\| \pmod{p^r}$ for any $g \in G_r$ and $\mathbf{x} \in (\mathbb{Z}/p^r\mathbb{Z})^2$. Write the orbit of $\mathbf{x}$ by

$$\mathrm{orb}_r(\mathbf{x}) = \left\{ \theta\mathbf{x} : \ \theta \in G_r \right\},$$

and the stabilizer of $\mathbf{x}$ by

$$\mathrm{stab}_r(\mathbf{x}) = \{\theta \in G_r : \ \theta\mathbf{x} \equiv \mathbf{x} \pmod{p^r}\}.$$

For any $j \in \mathbb{Z}/p^r\mathbb{Z}$, let $C_{j,r}$ be the circle centered at the origin of radius j, i.e.,

$$C_{j,r} = \{\mathbf{x} \in (\mathbb{Z}/p^r\mathbb{Z})^2 : \ \|\mathbf{x}\| \equiv j \pmod{p^r}\}.$$

For $x \in \mathbb{Z}/p^r\mathbb{Z}$ and $u \in \{0, 1, \ldots, r-1\}$, the expression $v_p(x) = u$ means that $x \equiv 0 \pmod{p^u}$ and $x \not\equiv 0 \pmod{p^{u+1}}$. We also denote $v_p(0) = r$ for $0 \in \mathbb{Z}/p^r\mathbb{Z}$. When $\mathbf{x} = (x_1, x_2)$, we write $v_{\mathbf{x}} = \min\{v_p(x_1), v_p(x_2)\}$. Then, the vector $\mathbf{x}$ can be expressed as $\mathbf{x} = p^{v_{\mathbf{x}}}\tilde{\mathbf{x}}$, where $\tilde{\mathbf{x}}$ is a vector in $(\mathbb{Z}/p^{r-v_{\mathbf{x}}}\mathbb{Z})^n$ such that $v_{\tilde{\mathbf{x}}} = 0$.

We recall the following facts from [11].

Lemma 2.1 ([11], Lemma 4.5) *Let $p \equiv 3 \pmod 4$. For any $\mathbf{0} \neq \mathbf{x} \in (\mathbb{Z}/p^r\mathbb{Z})^2$, let $\mathbf{x} = p^{v_{\mathbf{x}}}\tilde{\mathbf{x}}$ for some $\tilde{\mathbf{x}} \in (\mathbb{Z}/p^{r-v_{\mathbf{x}}}\mathbb{Z})^2$ with $v_{\tilde{\mathbf{x}}} = 0$. Then $orb_r(\mathbf{x}) = p^{v_{\mathbf{x}}} C_{\|\tilde{\mathbf{x}}\|, r-v_{\mathbf{x}}}$, and*

$$|stab_r(\mathbf{x})| = p^{v_{\mathbf{x}}}, \qquad |orb_r(\mathbf{x})| = p^{r-v_{\mathbf{x}}}\left(1 + \frac{1}{p}\right).$$

Lemma 2.2 ([11], Lemma 4.9) *Let $p \equiv 1 \pmod 4$. For any $\mathbf{0} \neq \mathbf{x} \in (\mathbb{Z}/p^r\mathbb{Z})^2$, let $\mathbf{x} = p^{v_{\mathbf{x}}}\tilde{\mathbf{x}}$ for some $\tilde{\mathbf{x}} \in (\mathbb{Z}/p^{r-v_{\mathbf{x}}}\mathbb{Z})^2$ with $v_{\tilde{\mathbf{x}}} = 0$. Then $orb_r(\mathbf{x}) = p^{v_{\mathbf{x}}} orb_{r-v_{\mathbf{x}}}(\tilde{\mathbf{x}})$, and*

$$|stab_r(\mathbf{x})| = p^{v_{\mathbf{x}}}, \qquad |orb_r(\mathbf{x})| = p^{r-v_{\mathbf{x}}}\left(1 - \frac{1}{p}\right).$$

For a function $f : (\mathbb{Z}/p^r\mathbb{Z})^2 \to \mathbb{C}$, the Fourier transform $\widehat{f} : (\mathbb{Z}/p^r\mathbb{Z})^2 \to \mathbb{C}$ is defined by

$$\widehat{f}(\mathbf{m}) := p^{-2r} \sum_{\mathbf{x} \in (\mathbb{Z}/p^r\mathbb{Z})^2} \chi_r(-\mathbf{m} \cdot \mathbf{x}) f(\mathbf{x}),$$

where $\chi_r(x) = e^{\frac{2\pi i x}{p^r}} \ (x \bmod p^r)$.

We have the following basic properties of χ and $\widehat{f}$.

- The orthogonality property

$$\sum_{\boldsymbol{\alpha} \in (\mathbb{Z}/p^r\mathbb{Z})^2} \chi_r(\boldsymbol{\beta} \cdot \boldsymbol{\alpha}) = \begin{cases} p^{2r}, & \text{if} \quad \boldsymbol{\beta} \equiv \mathbf{0} \pmod{p^r}, \\ 0, & \text{if} \quad \boldsymbol{\beta} \not\equiv \mathbf{0} \pmod{p^r}. \end{cases}$$

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

- The Fourier inversion formula

$$f(\mathbf{x}) = \sum_{\mathbf{m}\in(\mathbb{Z}/p^r\mathbb{Z})^2} \widehat{f}(\mathbf{m})\chi_r(\mathbf{m}\cdot\mathbf{x}).$$

- The Plancherel formula

$$\sum_{\mathbf{m}\in(\mathbb{Z}/p^r\mathbb{Z})^2} \left|\widehat{f}(\mathbf{m})\right|^2 = p^{-2r} \sum_{\mathbf{x}\in(\mathbb{Z}/p^r\mathbb{Z})^2} |f(\mathbf{x})|^2.$$

For a set A, by abuse of notation, we also denote its characteristic function by $A(x)$, i.e. $A(x) = 1$ if $x \in A$ and $A(x) = 0$ if $x \notin A$.

Now we state a more general restriction problem,.

Let $\mathbf{m} \in (\mathbb{Z}/p^r\mathbb{Z})^2$. When r is given, we also use the simplified notation $V_{\mathbf{m}}$ for $\mathrm{orb}_r(\mathbf{m})$. Let $d\sigma_{V_{\mathbf{m}}}$ be the corresponding surface measure on $V_{\mathbf{m}}$ and for all $f : V_{\mathbf{m}} \to \mathbb{C}$, define

$$(fd\sigma_{V_{\mathbf{m}}})^\vee(\mathbf{y}) := \frac{1}{|V_{\mathbf{m}}|} \sum_{\mathbf{x}\in V_{\mathbf{m}}} f(\mathbf{x})\chi_r(\mathbf{y}\cdot\mathbf{x}).$$

As computed in [11], we have

$$\sum_{\mathbf{m} \pmod{p^r}} |(fd\sigma_{V_{\mathbf{m}}})^\vee(\mathbf{m})|^4 = \frac{p^{2r}}{|V_{\mathbf{m}}|^4} \sum_{\substack{\xi,\xi',\eta,\eta'\in V_{\mathbf{m}} \\ \xi-\eta\equiv\xi'-\eta' \pmod{p^r}}} f(\xi)f(\xi')\overline{f(\eta)f(\eta')}.$$

If f is the characteristic function of a set $A \subset V_{\mathbf{m}}$, then $|V_{\mathbf{m}}|^4 p^{-2r} \sum_{\mathbf{m} \pmod{p^r}} |(fd\sigma_{V_{\mathbf{m}}})^\vee(\mathbf{m})|^4$ counts the number of energy quadruples in A.

The following theorems give upper bounds of that sum for general functions f.

Theorem 2.3 ([11], Theorem 4.1) *Let $p \equiv 3 \pmod 4$ be a prime and $r \geq 1$ be an integer. Let $\mathbf{m} \in (\mathbb{Z}/p^r\mathbb{Z})^2$ be such that $\mathbf{m} \neq \mathbf{0}$. Then*

$$\left(\sum_{\mathbf{x}\in(\mathbb{Z}/p^r\mathbb{Z})^2} |(fd\sigma_{V_{\mathbf{m}}})^\vee(\mathbf{x})|^4\right)^{\frac{1}{2}} \ll p^{-\frac{r-3v_{\mathbf{m}}+1}{2}} \sum_{\mathbf{x}\in V_{\mathbf{m}}} |f(\mathbf{x})|^2.$$

Theorem 2.4 ([11], Theorem 4.2) *Let $p \equiv 1 \pmod 4$ be a prime and $r \geq 1$ be an integer. Let $\mathbf{m} \in (\mathbb{Z}/p^r\mathbb{Z})^2$ be such that $\mathbf{m} \neq \mathbf{0}$. Suppose that $\mathbf{m} = p^{v_m}\tilde{\mathbf{m}}$ with $\tilde{\mathbf{m}} \in (\mathbb{Z}/p^{r-v_m}\mathbb{Z})^2$.*

If $\|\tilde{\mathbf{m}}\| \not\equiv 0 \pmod p$, then

$$\left(\sum_{\mathbf{x}\in(\mathbb{Z}/p^r\mathbb{Z})^2} |(fd\sigma_{V_{\mathbf{m}}})^\vee(\mathbf{x})|^4\right)^{\frac{1}{2}} \ll p^{-\frac{r-3v_{\mathbf{m}}+1}{2}} \sum_{\mathbf{x}\in V_{\mathbf{m}}} |f(\mathbf{x})|^2.$$

If $\|\tilde{\mathbf{m}}\| \equiv 0 \pmod p$, we have

$$\left(\sum_{\mathbf{x}\in(\mathbb{Z}/p^r\mathbb{Z})^2} |(fd\sigma_{V_{\mathbf{m}}})^\vee(\mathbf{x})|^4\right)^{\frac{1}{2}} \ll p^{-\frac{r-3v_{\mathbf{m}}}{2}} \sum_{\mathbf{x}\in V_{\mathbf{m}}} |f(\mathbf{x})|^2.$$

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

Remark 2.5 In comparison between Theorem 2.3 and Theorem 2.4, the latter is weaker, which comes from elements $\mathbf{m}$ with $\|\tilde{\mathbf{m}}\| \equiv 0 \pmod{p}$.

The next two lemmas are duality versions of Theorem 2.3 and Theorem 2.4.

Lemma 2.6 *Let $p \equiv 3 \pmod 4$. Let $E \subset (\mathbb{Z}/p^r\mathbb{Z})^2$ and $\mathbf{m} \in (\mathbb{Z}/p^r\mathbb{Z})^2$ be such that $\mathbf{m} \neq \mathbf{0}$. Then*

$$\sum_{\mathbf{x}\in V_{\mathbf{m}}} \left|\widehat{E}(\mathbf{x})\right|^2 \ll p^{-\frac{5r+v_{\mathbf{m}}+1}{2}} |E|^{3/2}.$$

Proof By Hölder's inequality and Theorem 2.3, we have

$$\frac{p^{2r}}{|V_{\mathbf{m}}|} \sum_{\mathbf{x}\in V_{\mathbf{m}}} \left|\widehat{E}(\mathbf{x})\right|^2 = \frac{p^{2r}}{|V_{\mathbf{m}}|} \sum_{\mathbf{x}\in V_{\mathbf{m}}} \widehat{E}(\mathbf{x})\overline{\widehat{E}(\mathbf{x})} = \sum_{\mathbf{y}\in(\mathbb{Z}/p^r\mathbb{Z})^2} E(\mathbf{y}) \overline{\frac{1}{|V_{\mathbf{m}}|} \sum_{\mathbf{x}\in V_{\mathbf{m}}} \chi_r(\mathbf{y}\cdot\mathbf{x})\widehat{E}(\mathbf{x})}$$

$$= \sum_{\mathbf{y}\in(\mathbb{Z}/p^r\mathbb{Z})^2} E(\mathbf{y})(\widehat{E}d\sigma_{V_{\mathbf{m}}})^{\vee}(\mathbf{y}) \leq \left(\sum_{\mathbf{y}\in(\mathbb{Z}/p^r\mathbb{Z})^2} |E(\mathbf{y})|^{\frac{4}{3}}\right)^{\frac{3}{4}} \left(\sum_{\mathbf{y}\in(\mathbb{Z}/p^r\mathbb{Z})^2} \left|(\widehat{E}d\sigma_{V_{\mathbf{m}}})\right|^4\right)^{\frac{1}{4}}$$

$$\ll |E|^{\frac{3}{4}} \left(p^{-\frac{r-3v_{\mathbf{m}}+1}{2}} \sum_{\mathbf{x}\in V_{\mathbf{m}}} \left|\widehat{E}(\mathbf{x})\right|^2\right)^{\frac{1}{2}}.$$

Recall from Lemma 2.1 that $|V_{\mathbf{m}}| \sim p^{r-v_{\mathbf{m}}}$, the previous inequality implies

$$p^{r+v_{\mathbf{m}}} \sum_{\mathbf{x}\in V_{\mathbf{m}}} \left|\widehat{E}(\mathbf{x})\right|^2 \ll |E|^{\frac{3}{4}} \left(p^{\frac{-r+3v_{\mathbf{m}}-1}{2}} \sum_{\mathbf{x}\in V_{\mathbf{m}}} \left|\widehat{E}(\mathbf{x})\right|^2\right)^{\frac{1}{2}}.$$

It follows that:

$$\sum_{\mathbf{x}\in V_{\mathbf{m}}} \left|\widehat{E}(\mathbf{x})\right|^2 \ll p^{-\frac{5r+v_{\mathbf{m}}+1}{2}} |E|^{\frac{3}{2}}.$$

■

Lemma 2.7 *Let $p \equiv 1 \pmod 4$ be a prime and $r \geq 1$ be an integer. Let $E \subset (\mathbb{Z}/p^r\mathbb{Z})^2$ and $\mathbf{m} \in (\mathbb{Z}/p^r\mathbb{Z})^2$ be such that $\mathbf{m} \neq \mathbf{0}$. Suppose that $\mathbf{m} = p^{v_{\mathbf{m}}}\tilde{\mathbf{m}}$, where $v_{\tilde{\mathbf{m}}} = 0$.*

If $\|\tilde{\mathbf{m}}\| \not\equiv 0 \pmod p$, then

$$\sum_{\mathbf{x}\in V_{\mathbf{m}}} \left|\widehat{E}(\mathbf{x})\right|^2 \ll p^{-\frac{5r+v_{\mathbf{m}}+1}{2}} |E|^{\frac{3}{2}};$$

If $\|\tilde{\mathbf{m}}\| \equiv 0 \pmod p$, then

$$\sum_{\mathbf{x}\in V_{\mathbf{m}}} \left|\widehat{E}(\mathbf{x})\right|^2 \ll p^{-\frac{5r+v_{\mathbf{m}}}{2}} |E|^{\frac{3}{2}}.$$

Proof The proof is same as that of Lemma 2.6, with applying Theorem 2.4. ■

Corollary 2.8 *Let p be a prime, and Let $p \equiv 3 \pmod 4$. Let A, B be sets in $(\mathbb{Z}/p^r\mathbb{Z})^2$. Then we have*

$$\sum_{\mathbf{m}\neq\mathbf{0}} \sum_{\mathbf{m}'\in V_{\mathbf{m}}} p^{v_{\mathbf{m}}} \left|\widehat{A}(\mathbf{m})\right|^2 \left|\widehat{B}(\mathbf{m}')\right|^2 \ll p^{-4r-1}|A||B|^{\frac{3}{2}}.$$

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

Proof Applying Lemma 2.6 and Plancherel formula, as above, one has

$$\sum_{\substack{\mathbf{m}\neq\mathbf{0},\\ \mathbf{m}'\in V_{\mathbf{m}}}} p^{\nu_{\mathbf{m}}}\left|\widehat{A}(\mathbf{m})\right|^2\left|\widehat{B}(\mathbf{m}')\right|^2 \leq \sum_{\mathbf{m}}|\widehat{A}(\mathbf{m})|^2\cdot\max_{\mathbf{z}\neq\mathbf{0}}\left(p^{\nu_{\mathbf{z}}}\sum_{\mathbf{m}'\in V_{\mathbf{z}}}|\widehat{B}(\mathbf{m}')|^2\right)$$
$$\ll p^{-2r}|A|\cdot\max_{\mathbf{z}\neq\mathbf{0}}\left(p^{\nu_{\mathbf{z}}}\cdot p^{-\frac{5r+\nu_{\mathbf{z}}+1}{2}}|B|^{\frac{3}{2}}\right)\ll p^{-4r-1}|A||B|^{\frac{3}{2}},$$

by noting that $\max \nu_{\mathbf{z}} = r-1$ for $\mathbf{z}\neq\mathbf{0}$. Thus, the theorem follows. ∎

Corollary 2.9 *Let $p\equiv 1 \pmod 4$ be a prime, let A, B be sets in $(\mathbb{Z}/p^r\mathbb{Z})^2$. Then we have*

$$\sum_{\mathbf{m}\neq\mathbf{0}}\sum_{\mathbf{m}'\in V_{\mathbf{m}}} p^{\nu_{\mathbf{m}}}\left|\widehat{A}(\mathbf{m})\right|\left|\widehat{B}(\mathbf{m}')\right| \ll p^{-4r-1/2}|A||B|^{3/2}.$$

Proof The proof is same as that of Corollary 2.8, with applying Lemma 2.7. ∎

3 Incidences between points and rigid-motions

Recall that $G_r = SO_2(\mathbb{Z}/p^r\mathbb{Z})$. We denote the set of rigid motion over $\mathbb{Z}/p^r\mathbb{Z}$ by

$$\mathcal{R}_r := \{(g,\mathbf{z}) : g\in G_r,\ \mathbf{z}\in(\mathbb{Z}/p^r\mathbb{Z})^2\}.$$

Indeed, it is a semi-direct product of groups (see [10] for example). As a set, one has $\mathcal{R}_r = G_r\times(\mathbb{Z}/p^r\mathbb{Z})^2$ and $|\mathcal{R}_r|\sim p^{3r}$.

We say a pair of points $(\mathbf{x},\mathbf{y})\in(\mathbb{Z}/p^r\mathbb{Z})^2\times(\mathbb{Z}/p^r\mathbb{Z})^2$ is incident to a rigid-motion $(g,\mathbf{z})$ if $g\mathbf{y}+\mathbf{z}=\mathbf{x}$. For $P=A\times B\subset(\mathbb{Z}/p^r\mathbb{Z})^2\times(\mathbb{Z}/p^r\mathbb{Z})^2$ and $R\subset\mathcal{R}_r$, we define

$$\mathcal{I}(P,R) := \left\{\big((g,\mathbf{z}),(\mathbf{x},\mathbf{y})\big)\in R\times P : g\mathbf{y}+\mathbf{z}=\mathbf{x}\right\}$$

as the number of incidences between P and R. This section is devoted to bounding $\mathcal{I}(P,R)$ from above and below.

We first state a universal bound that will be proved by using a standard discrete Fourier analysis argument, followed by an improvement obtained via Corollary 2.8.

Theorem 3.1 *Let p be an odd prime, let $P=A\times B\subset(\mathbb{Z}/p^r\mathbb{Z})^2\times(\mathbb{Z}/p^r\mathbb{Z})^2$ and $R\subset\mathcal{R}_r$. Then*

$$\left|\mathcal{I}(P,R)-\frac{|P||R|}{p^{2r}}\right|\ll p^{\frac{3r-1}{2}}|P|^{\frac{1}{2}}|R|^{\frac{1}{2}}.$$

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

Proof We have

$$\begin{aligned}\mathcal{I}(P,R) &= \sum_{\substack{(\mathbf{x},\mathbf{y})\in P,\\(g,\mathbf{z})\in R}} 1_{\mathbf{x}=g\mathbf{y}+\mathbf{z}} = \frac{1}{p^{2r}} \sum_{\mathbf{m}\in(\mathbb{Z}/p^r\mathbb{Z})^2} \sum_{\substack{(\mathbf{x},\mathbf{y})\in P,\\(g,\mathbf{z})\in R}} \chi_r\left(\mathbf{m}\cdot(\mathbf{x}-g\mathbf{y}-\mathbf{z})\right)\\ &= \frac{|P||R|}{p^{2r}} + \frac{1}{p^{2r}} \sum_{\mathbf{m}\in(\mathbb{Z}/p^r\mathbb{Z})^2\setminus\{\mathbf{0}\}} \sum_{\substack{(\mathbf{x},\mathbf{y})\in P,\\(g,\mathbf{z})\in R}} \chi_r(\mathbf{m}\cdot(\mathbf{x}-g\mathbf{y}-\mathbf{z}))\\ &= \frac{|P||R|}{p^{2r}} + p^{2r} \sum_{\mathbf{m}\neq\mathbf{0}} \sum_{(g,\mathbf{z})\in R} \widehat{P}(-\mathbf{m},g\mathbf{m})\chi_r(-\mathbf{m}\mathbf{z}) =: I + II,\end{aligned}$$

where,

$$\widehat{P}(\mathbf{u},\mathbf{v}) = p^{-4r} \sum_{(\mathbf{x},\mathbf{y})\in P} \chi_r(-\mathbf{x}\cdot\mathbf{u}-\mathbf{y}\cdot\mathbf{v}).$$

We next bound the second term. By the Cauchy-Schwarz inequality, we have

$$\begin{aligned}II &= p^{2r} \sum_{(g,\mathbf{z})\in R} \sum_{\mathbf{m}\neq\mathbf{0}} \widehat{P}(-\mathbf{m},g\mathbf{m})\chi_r(-\mathbf{m}\mathbf{z})\\ &\le p^{2r}|R|^{1/2}\left(\sum_{(g,\mathbf{z})\in\mathcal{R}_r} \sum_{\mathbf{m}_1,\mathbf{m}_2\neq\mathbf{0}} \widehat{P}(-\mathbf{m}_1,g\mathbf{m}_1)\overline{\widehat{P}(-\mathbf{m}_2,g\mathbf{m}_2)}\chi_r(\mathbf{z}\cdot(-\mathbf{m}_1+\mathbf{m}_2))\right)^{1/2}\\ &= p^{2r}|R|^{1/2}\left(\sum_{g\in G_r} \sum_{\mathbf{m}_1,\mathbf{m}_2\neq\mathbf{0}} \widehat{P}(-\mathbf{m}_1,g\mathbf{m}_1)\overline{\widehat{P}(-\mathbf{m}_2,g\mathbf{m}_2)} \sum_{\mathbf{z}\in(\mathbb{Z}/p^r\mathbb{Z})^2} \chi_r(\mathbf{z}\cdot(-\mathbf{m}_1+\mathbf{m}_2))\right)^{1/2}\\ &= p^{2r}|R|^{1/2}\left(p^{2r}\sum_{g\in G_r}\sum_{\mathbf{m}\neq\mathbf{0}}|\widehat{P}(\mathbf{m},-g\mathbf{m})|^2\right)^{1/2}.\end{aligned}$$

Since $P = A\times B$, we have

$$\widehat{P}(\mathbf{m},-g\mathbf{m}) = \widehat{A}(\mathbf{m})\widehat{B}(-g\mathbf{m}).$$

Thus, following Lemma 2.2 and Plancherel fomula, we have

$$\begin{aligned}&\sum_{g\in G_r}\sum_{\mathbf{m}\neq\mathbf{0}}|\widehat{P}(\mathbf{m},-g\mathbf{m})|^2 = \sum_{\mathbf{m}\neq\mathbf{0}}|\widehat{A}(\mathbf{m})|^2\sum_{g\in G_r}|\widehat{B}(-g\mathbf{m})|^2\\ &\ll \sum_{\mathbf{m}\neq\mathbf{0}}|\widehat{A}(\mathbf{m})|^2\sum_{\mathbf{m}'\in V_{\mathbf{m}}}p^{\nu_{\mathbf{m}}}|\widehat{B}(\mathbf{m}')|^2 \le \sum_{\mathbf{m}\neq\mathbf{0}}p^{\nu_{\mathbf{m}}}|\widehat{A}(\mathbf{m})|^2\sum_{\mathbf{m}'}|\widehat{B}(\mathbf{m}')|^2\\ &\le p^{r-1}\sum_{\mathbf{m}}|\widehat{A}(\mathbf{m})|^2\sum_{\mathbf{m}'}|\widehat{B}(\mathbf{m}')|^2 = p^{r-1}\cdot\frac{|A|}{p^{2r}}\cdot\frac{|B|}{p^{2r}} = \frac{|A||B|}{p^{3r+1}}.\end{aligned}$$

Here, we have used the fact that the stabilizer of a nonzero element $\mathbf{m}$ in $SO_2(\mathbb{Z}/p^r\mathbb{Z})$ is $\sim p^{\nu_{\mathbf{m}}} \le p^{r-1}$.

Finally, we obtain that

$$II \ll p^{3r}|R|^{\frac{1}{2}}\left(\frac{|A||B|}{p^{3r+1}}\right)^{\frac{1}{2}} = p^{\frac{3r-1}{2}}|R|^{\frac{1}{2}}|P|^{\frac{1}{2}}.$$

This completes the proof. ∎

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

Next, we estimate the number of incidences in another way.

Theorem 3.2 *Let p be an odd prime. Let $P = A \times B \subset (\mathbb{Z}/p^r\mathbb{Z})^2 \times (\mathbb{Z}/p^r\mathbb{Z})^2$ and $R \subset \mathcal{R}_r$.*

If $p \equiv 3 \pmod 4$, then

$$\left| \mathcal{I}(P,R) - \frac{|P||R|}{p^{2r}} \right| \ll p^{r-\frac{1}{2}} |P|^{\frac{1}{2}} |R|^{\frac{1}{2}} |B|^{\frac{1}{4}}.$$

If $p \equiv 1 \pmod 4$, then

$$\left| \mathcal{I}(P,R) - \frac{|P||R|}{p^{2r}} \right| \ll p^{r-\frac{1}{4}} |P|^{\frac{1}{2}} |R|^{\frac{1}{2}} |B|^{\frac{1}{4}}.$$

Proof As previous, we have

$$\mathcal{I}(P,R) = \frac{|P||R|}{p^{2r}} + p^{2r} \sum_{\mathbf{m}\neq\mathbf{0}} \sum_{(g,\mathbf{z})\in R} \widehat{P}(-\mathbf{m}, g\mathbf{m}) \chi_r(-\mathbf{m}\cdot\mathbf{z}) =: I + II,$$

and

$$\begin{aligned} II &\leq p^{3r} |R|^{\frac{1}{2}} \left(\sum_{g\in G_r} \sum_{\mathbf{m}\neq\mathbf{0}} |\widehat{P}(\mathbf{m}, -g\mathbf{m})|^2 \right)^{\frac{1}{2}} \\ &\ll p^{3r} |R|^{\frac{1}{2}} \left(\sum_{\substack{\mathbf{m}\neq\mathbf{0},\\ \mathbf{m}'\in V_{\mathbf{m}}}} p^{\nu_{\mathbf{m}}} |\widehat{A}(\mathbf{m})|^2 |\widehat{B}(\mathbf{m}')|^2 \right)^{\frac{1}{2}}. \end{aligned}$$

To prove the first assertion, we use Corollary 2.8 and obtain

$$II \ll p^{3r} |R|^{\frac{1}{2}} \left(p^{-4r-1} |A||B|^{\frac{3}{2}} \right)^{\frac{1}{2}} = p^{2r-\frac{1}{2}} |R|^{\frac{1}{2}} |P|^{\frac{1}{2}} |B|^{\frac{1}{4}}.$$

To prove the second assertion, we use Corollary 2.9 and obtain

$$II \ll p^{3r} |R|^{\frac{1}{2}} \left(p^{-4r-\frac{1}{2}} |A||B|^{\frac{3}{2}} \right)^{\frac{1}{2}} = p^{r-\frac{1}{4}} |R|^{\frac{1}{2}} |P|^{\frac{1}{2}} |B|^{\frac{1}{4}}.$$

This completes the proof. ∎

Remark 3.3 Compared to Theorem 3.1, Theorem 3.2 gives improvements in the ranges $|B| < p^{2r}$ and $|B| < p^{2r-1}$, corresponding to $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 4$, respectively.

4 Proof of main theorems

Proof of Theorem 1.4 Since $\delta_A^{1/2} \cdot \delta_B \geq 2p^{-1}$, we have $\delta_A \geq 4p^{-2}$. Thus, $|A| \geq 4p^{2r-2}$. The number of elements $\mathbf{x}$ in $(\mathbb{Z}/p^r\mathbb{Z})^2$ with $\nu_{\mathbf{x}} \neq 0$ does not exceed p^{2r-2}. So, without loss of generality, we may assume that $|A| \geq 3p^{2r-2}$ and $\nu_{\mathbf{x}} = 0$ for any $\mathbf{x} \in A$.

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

Let

$$\widetilde{G} = \left\{ g \in G_r : \left| \left\{ \mathbf{z} \in (\mathbb{Z}/p^r\mathbb{Z})^2 : B \cap (gA + \mathbf{z}) = \varnothing \right\} \right| \geq \frac{p^{2r}}{2} \right\}.$$

It is sufficient to show that $|\widetilde{G}| \ll |G_r|$.

Let $\widetilde{R}$ be the set of pairs $(g, \mathbf{z}) \in \mathcal{R}_r$ such that $g \in \widetilde{G}$ and $B \cap (gA + \mathbf{z}) = \varnothing$. It is clear that $\mathcal{I}(B \times A, \widetilde{R}) = 0$. Alternatively, from Theorem 3.2 (1), we have

$$\left| \mathcal{I}(B \times A, \widetilde{R}) - \frac{|A||B||\widetilde{R}|}{p^{2r}} \right| \ll p^{r-\frac{1}{2}} |A|^{\frac{3}{4}} |B|^{\frac{1}{2}} |\widetilde{R}|^{\frac{1}{2}}. \tag{1}$$

Thus, we deduce that

$$|\widetilde{R}| \ll p^{6r-1} |A|^{-\frac{1}{2}} |B|^{-1}.$$

On the other hand, one sees by the construction of $\widetilde{G}$ that $|\widetilde{R}| \geq |\widetilde{G}| \cdot p^{2r}/2$, we have

$$|\widetilde{G}| \ll p^{4r-1} |A|^{-\frac{1}{2}} |B|^{-1}. \tag{2}$$

It leads to $|\widetilde{G}| \ll p^r$, in view of the condition $|A|^{1/2}|B| \geq 2p^{3r-1}$. ∎

In above arguments, if we use Theorem 3.2 (2), then the condition $|A|^{1/2}|B| \geq 2p^{3r-\frac{1}{2}}$ is required. By a direct computation, we can see that this condition is worse than those of Theorem 1.5.

Proof of Theorem 1.5 The proof is same as that of Theorem 2.6. In this case, one deduces from $\delta_A \cdot \delta_B \geq 2p^{-1}$ that $\delta_A \geq 2p^{-1}$. Then the cardinality of A is at least $2p^{2r-1}$, which is much larger than the number of elements $\mathbf{x}$ with $\nu_{\mathbf{x}} \neq 0$. From Theorem 3.1, the bound on the right-hand side of (1) is replaced by $p^{\frac{3r-1}{2}} |A|^{\frac{1}{2}} |B|^{\frac{1}{2}} |\widetilde{R}|^{\frac{1}{2}}$. And (2) becomes

$$|\widetilde{G}| \ll p^{-2r} |\widetilde{R}| \ll p^{5r-1} |A|^{-1} |B|^{-1},$$

which gives $|\widetilde{G}| \ll p^r$ provided that $|A||B| \geq 2p^{4r-1}$. ∎

A Appendix: Proof of Theorem 2.4

As shown in [11], the proof of Theorem 2.4 is almost identical with that of Theorem 2.3 for the case $p \equiv 3 \pmod 4$. For clarity, we provide a detailed proof here.

In this section, the letter p is always a prime with $p \equiv 1 \pmod 4$, and r is a positive integer. Recall that $G_r = SO_2(\mathbb{Z}/p^r\mathbb{Z})$.

Lemma 5.1 ([11], Lemma 2.1) *For any prime p, let*

$$\mathbf{G}(\mathbf{x}) = \left(\widetilde{G}(x_1, \ldots, x_n), \ldots, G_m(x_1, \ldots, x_n) \right)$$

be a map from $\mathbb{Z}^n$ to $\mathbb{Z}^m$, with G_i polynomials with integer coefficients. Let l be a positive integer and $\mathbf{y} \in \mathbb{Z}^n$. Suppose that $\mathbf{G}(\mathbf{y}) \equiv \mathbf{0} \pmod{p^l}$. Let $R = \operatorname{rank} J_{\mathbf{G}}(\mathbf{y})$, where $J_{\mathbf{G}}(\mathbf{y})$

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

is the Jocobi matrix modulo p, i.e.,

$$J_{\mathbf{G}}(\mathbf{y}) = \begin{bmatrix} \frac{\partial \widetilde{G}}{\partial x_1}(\mathbf{y}) & \frac{\partial \widetilde{G}}{\partial x_2}(\mathbf{y}) & \cdots & \frac{\partial \widetilde{G}}{\partial x_n}(\mathbf{y}) \\ \frac{\partial G_2}{\partial x_1}(\mathbf{y}) & \frac{\partial G_2}{\partial x_2}(\mathbf{y}) & \cdots & \frac{\partial G_2}{\partial x_n}(\mathbf{y}) \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial G_m}{\partial x_1}(\mathbf{y}) & \frac{\partial G_m}{\partial x_2}(\mathbf{y}) & \cdots & \frac{\partial G_m}{\partial x_n}(\mathbf{y}) \end{bmatrix} \quad (mod\ p).$$

Then

$$\#\left\{\mathbf{z}\,(mod\ p^k) : \mathbf{G}(\mathbf{y} + p^l\mathbf{z}) \equiv \mathbf{0}\,(mod\ p^{l+k})\right\} \le p^{k(n-R)} \tag{3}$$

for any integer $k \ge 1$. When $R = m$, the "$\le$" can be replaced by "$=$".

Lemma 5.2 *We have $|G_r| = p^r(1 - 1/p)$.*

Proof For $r = 1$, we have $|G_1| = p - 1$. Now consider the circumstances that $r \ge 2$. For any $\theta = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in G_r$, there is some $\theta_0 = \begin{bmatrix} a_0 & -b_0 \\ b_0 & a_0 \end{bmatrix} \in G_1$ such that $\theta \equiv \theta_0 \pmod p$. Applying Lemma 5.1 to (a_0, b_0) and the polynomial $F(x, y) = x^2 + y^2 - 1$, one obtains that $(\nabla F)(a_0, b_0) = (2a_0, 2b_0) \not\equiv (0, 0) \pmod p$, since $a_0^2 + b_0^2 \equiv 1 \pmod p$. Thus,

$$\#\left\{(z_1, z_2) \pmod{p^{r-1}} : (a_0 + pz_1)^2 + (b_0 + pz_2)^2 \equiv 1 \pmod{p^r}\right\} = p^{r-1}.$$

It follows that

$$|G_r| = p^{r-1}|G_1| = p^r(1 - 1/p). \qquad \blacksquare$$

Proof of Lemma 2.2 Here $0 \le v_{\mathbf{x}} \le r - 1$. The equation $\theta\mathbf{x} \equiv \mathbf{x} \pmod{p^r}$ is equivalent to

$$\begin{bmatrix} a-1 & -b \\ b & a-1 \end{bmatrix} \begin{bmatrix} p^{v_{\mathbf{x}}}\tilde{x}_1 \\ p^{v_{\mathbf{x}}}\tilde{x}_2 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{p^r}, \tag{4}$$

or equivalently,

$$\begin{bmatrix} \tilde{x}_1 & -\tilde{x}_2 \\ \tilde{x}_2 & \tilde{x}_1 \end{bmatrix} \begin{bmatrix} a-1 \\ b \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{p^{r-v_{\mathbf{x}}}}. \tag{5}$$

If $\tilde{x}_1{}^2 + \tilde{x}_2{}^2 \not\equiv 0 \pmod p$, then the coefficient matrix is invertible modulo p^r, and

$$\begin{bmatrix} a \\ b \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \pmod{p^{r-v_{\mathbf{x}}}}.$$

By Lemma 5.1, the number of $(a, b) \in (\mathbb{Z}/p^r\mathbb{Z})^2$ satisfying $a^2 + b^2 \equiv 1 \pmod{p^r}$ and the above equivalence is exactly $p^{v_{\mathbf{x}}}$.

If $\tilde{x}_1{}^2 + \tilde{x}_2{}^2 \equiv 0 \pmod p$, then one deduce from $(\tilde{x}_1, \tilde{x}_2) \not\equiv (0, 0) \pmod p$ that $\tilde{x}_1, \tilde{x}_2 \not\equiv 0 \pmod p$. Therefore, let $u = a - 1, v = b$, we have a system of linear equation

$$\begin{cases} \tilde{x}_1 u - \tilde{x}_2 v \equiv 0 \\ \tilde{x}_2 u + \tilde{x}_1 v \equiv 0 \\ (u+1)^2 + v^2 \equiv 1 \end{cases} \pmod{p^{r-v_{\mathbf{x}}}}.$$

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

It follows that

$$\begin{cases} u \equiv \tilde{x_1}^{-1}\tilde{x_2}v \\ 2\tilde{x_1}\tilde{x_2}v \equiv 0 \end{cases} \pmod{p^{r-\nu_{\mathbf{x}}}}.$$

Hence, $(u,v) \equiv (0,0) \pmod{p^{r-\nu_{\mathbf{x}}}}$, or equivalently, $(a,b) \equiv (1,0) \pmod{p^{r-\nu_{\mathbf{x}}}}$. By Lemma 5.1 again, the number of such (a,b) modulo p^r is exactly $p^{\nu_{\mathbf{x}}}$. So

$$\left|\mathrm{stab}_{\mathbf{x}}\right| = p^{\nu_{\mathbf{x}}}.$$

It then follows that $|\mathrm{orb}(\mathbf{x})| = |G_r|/|\mathrm{stab}_{\mathbf{x}}| = p^{r-\nu_{\mathbf{x}}}(1-1/p)$.

Moreover, for any $\theta \in G_r$, there is some $\theta_0 \in G_{r-\nu_{\mathbf{x}}}$ such that $\theta \equiv \theta_0 \pmod{p^{r-\nu_{\mathbf{x}}}}$. It can be verified that $\theta\tilde{\mathbf{x}} \equiv \theta_0\tilde{\mathbf{x}} \pmod{p^{r-\nu_{\mathbf{x}}}}$. So

$$\mathrm{orb}_r(\mathbf{x}) = \left\{\theta(p^{\nu_{\mathbf{x}}}\tilde{\mathbf{x}}) : \theta \in G_r\right\} = \left\{p^{\nu_{\mathbf{x}}}\theta_0\tilde{\mathbf{x}} : \theta_0 \in G_{r-\nu_{\mathbf{x}}}\right\}.$$

Note that $|G_{r-\nu_{\mathbf{x}}}| = p^{r-\nu_{\mathbf{x}}}(1-1/p)$ by Lemma 5.2, the elements on the right-hand side of the above formula give different members of the orbit. The proof is completed. ∎

Lemma 5.3 *Let $p \equiv 1 \pmod 4$. Suppose that $\mathbf{m} = p^{\nu_{\mathbf{m}}}\tilde{\mathbf{m}} \in (\mathbb{Z}/p^r\mathbb{Z})^2$ with $\tilde{\mathbf{m}} \in \left((\mathbb{Z}/p^{r-\nu_{\mathbf{m}}}\mathbb{Z})^*\right)^2$. Then for any $\mathbf{z} \in (\mathbb{Z}/p^r\mathbb{Z})^2$, we have*

(6)

$$\#\{(\mathbf{x},\mathbf{y}) \in (orb_r(\mathbf{m}))^2 : \mathbf{x}-\mathbf{y} \equiv \mathbf{z} (mod\ p^r)\} \ll \begin{cases} p^{r-\nu_{\mathbf{m}}-1}, & if\ \|\tilde{\mathbf{m}}\| \not\equiv 0\ (mod\ p), \\ p^{r-\nu_{\mathbf{m}}}, & if\ \|\tilde{\mathbf{m}}\| \equiv 0\ (mod\ p). \end{cases}$$

Proof When $\mathbf{m} = \mathbf{0}$, the conclusion holds automatically. In the following, we assume that $\mathbf{m} \neq \mathbf{0}$. By Lemma 2.2, one has $\mathrm{orb}_r(\mathbf{m}) = p^{\nu_{\mathbf{m}}}\mathrm{orb}_{r-\nu_{\mathbf{m}}}(\tilde{m})$. Let us write $\mathbf{x} = p^{\nu_{\mathbf{m}}}\tilde{\mathbf{x}}$ and $\mathbf{y} = p^{\nu_{\mathbf{m}}}\tilde{\mathbf{y}}$, with $\tilde{\mathbf{x}}, \tilde{\mathbf{y}} \in \mathrm{orb}_{r-\nu_{\mathbf{m}}}(\tilde{\mathbf{m}})$. When $\nu_{\mathbf{z}} < \nu_{\mathbf{m}}$, the equation $\mathbf{x}-\mathbf{y} \equiv \mathbf{z} \pmod{p^r}$ has no solution. When $\nu_{\mathbf{z}} \geq \nu_{\mathbf{m}}$, we denote $\mathbf{z} = p^{\nu_{\mathbf{m}}}\tilde{\mathbf{z}}$ and obtain that $\tilde{\mathbf{x}} - \tilde{\mathbf{y}} \equiv \tilde{\mathbf{z}} \pmod{p^{r-\nu_{\mathbf{m}}}}$. Noting that $\nu_{\tilde{\mathbf{m}}} = 0$, it is sufficient to show that

$$\#\{(\tilde{\mathbf{x}},\tilde{\mathbf{y}}) \in (\mathrm{orb}_r(\tilde{\mathbf{m}}))^2 : \tilde{\mathbf{x}}-\tilde{\mathbf{y}} \equiv \tilde{\mathbf{z}} (\mathrm{mod}\ p^{r-\nu_{\mathbf{m}}})\} \ll \begin{cases} p^{(r-\nu_{\mathbf{m}})-\nu_{\tilde{\mathbf{m}}}-1}, & \text{if } \|\tilde{\mathbf{m}}\| \not\equiv 0\ (\mathrm{mod}\ p), \\ p^{(r-\nu_{\mathbf{m}})-\nu_{\nu_{\tilde{m}}}}, & \text{if } \|\tilde{\mathbf{m}}\| \equiv 0\ (\mathrm{mod}\ p). \end{cases}$$

Therefore, we may assume at the beginning of the proof that $\nu_{\mathbf{m}} = 0$.

Since $\mathbf{y}$ is determined by $\mathbf{x}$ modulo p^r, the cardinality on the left-hand-side of (6) does not exceed $|\mathrm{orb}_r(\tilde{\mathbf{m}})|$, which is $\sim p^r$ by Lemma 2.2. The second upper bound follows.

Next, we consider the case $\|\mathbf{m}\| \not\equiv 0 \pmod p$. We have assumed that $\nu_{\mathbf{m}} = 0$, so $|\mathrm{stab}_r(\mathbf{m})| = 1$ by Lemma 2.2. For $\mathbf{x},\mathbf{y} \in \mathrm{orb}_r(\mathbf{m})$, there exist unique $a,b,a',b' \in \mathbb{Z}/p^r\mathbb{Z}$ such that $a^2+b^2 \equiv a'^2+b'^2 \equiv 1 \pmod{p^r}$ and

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\mathbf{m} \equiv \mathbf{x}, \quad \begin{bmatrix} a' & -b' \\ b' & a' \end{bmatrix}\mathbf{m} \equiv \mathbf{y}, \quad (\mathrm{mod}\ p^r).$$

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

The set on the left-hand side of (6) involves a system of congruences

$$\begin{cases} (a-a')m_1-(b-b')m_2 \equiv z_1, \\ (b-b')m_1+(a-a')m_2 \equiv z_2, \\ a^2+b^2 \equiv 1, \\ a'^2+b'^2 \equiv 1. \end{cases} \tag{7}$$

We first consider (7) modulo p.

Since $m_1^2+m_2^2 \not\equiv 0 \pmod{p}$, either m_2 or $m_1 \not\equiv 0 \pmod{p}$. Without loss of generality, we assume that $m_1 \not\equiv 0 \pmod{p}$, so one sees that

$$\begin{cases} a-a' \equiv m_1^{-1}(z_1+(b-b')m_2), \\ (b-b')m_1+m_1^{-1}(z_1+(b-b')m_2)m_2 \equiv z_2, \end{cases} \pmod{p},$$

or equivalently,

$$\begin{cases} a-a' \equiv m_1^{-1}(z_1+(b-b')m_2), \\ (b-b')(m_1^2+m_2^2) \equiv z_2m_1-z_1m_2. \end{cases} \pmod{p}.$$

Now (a,b) is determined by (a',b') and system (7) has at most 2 solutions modulo p.

In the following, we will apply Hensel's lemma. The Jacobi matrix of $G(a,b,a',b') = ((a-a')m_1-(b-b')m_2-z_1, (b-b')m_1+(a-a')m_2-z_2, a^2+b^2-1, a'^2+b'^2-1)$ in (a,b,a',b') is given by

$$\begin{bmatrix} m_1 & -m_2 & -m_1 & m_2 \\ m_2 & m_1 & -m_2 & -m_1 \\ 2a & 2b & 0 & 0 \\ 0 & 0 & 2a' & 2b' \end{bmatrix}.$$

By elementary operations, we obtain

$$\begin{bmatrix} 0 & 0 & -m_1 & m_2 \\ 0 & 0 & -m_2 & -m_1 \\ 2a & 2b & 0 & 0 \\ 2a' & 2b' & 2a' & 2b' \end{bmatrix}.$$

In view of the fact that $m_1^2+m_2^2 \not\equiv 0 \pmod{p}$, the rank of the above Jacobi matrix, modulo p, is at least 3. By Lemma 5.1, the number of solutions of (a,b,a',b') to (7) modulo p^r is at most p^{r-1}. The first upper bound then follows. ∎

Next, we complete the proof of Theorem 2.4.

Proof of Theorem 2.4 We have

$$\begin{aligned} \sum_{\mathbf{m}\in(\mathbb{Z}/p^r\mathbb{Z})^2} |(fd\sigma_{V_\mathbf{m}})^\vee(\mathbf{m})|^4 &= \sum_{\mathbf{m}} \left| \frac{1}{|V_\mathbf{m}|} \sum_{\mathbf{x}\in V_\mathbf{m}} \chi_r(\mathbf{m}\cdot\mathbf{x}) f(\mathbf{x}) \right|^4 \\ &= \frac{p^{2r}}{|V_\mathbf{m}|^4} \sum_{\xi,\xi',\eta,\eta'\in V_\mathbf{m}:\xi-\eta=\xi'-\eta'} f(\xi)f(\xi')\overline{f(\eta)f(\eta')}. \end{aligned}$$

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

Moreover,

$$\sum_{\xi,\xi',\eta,\eta'\in V:\xi-\eta=\xi'-\eta'} f(\xi)f(\xi')\overline{f(\eta)f(\eta')} = \sum_{\zeta}\left|\sum_{\xi-\eta=\zeta} f(\xi)\overline{f(\eta)}V_{\mathbf{m}}(\xi)V_{\mathbf{m}}(\eta)\right|^2.$$

For $\zeta \equiv \mathbf{0} \pmod{p^r}$, we have

$$\sum_{\zeta\equiv\mathbf{0} \pmod{p^r}}\left|\sum_{\xi-\eta=\zeta} f(\xi)\overline{f(\eta)}V_{\mathbf{m}}(\xi)V_{\mathbf{m}}(\eta)\right|^2 \ll \left(\sum_{\xi\in V_{\mathbf{m}}}|f(\xi)|^2\right)^2.$$

For $\zeta \not\equiv \mathbf{0} \pmod{p^r}$, the Cauchy-Schwarz inequality implies

$$\begin{aligned}&\sum_{\zeta\not\equiv\mathbf{0} \pmod{p^r}}\left|\sum_{\xi-\eta=\zeta} f(\xi)\overline{f(\eta)}V_{\mathbf{m}}(\xi)V_{\mathbf{m}}(\eta)\right|^2\\ &\leq \sum_{\zeta\not\equiv\mathbf{0} \pmod{p^r}}\left(\sum_{\xi-\eta=\zeta} V_{\mathbf{m}}(\xi)V_{\mathbf{m}}(\eta)\right)\sum_{\xi-\eta=\zeta}|f(\xi)|^2|f(\eta)|^2V_{\mathbf{m}}(\xi)V_{\mathbf{m}}(\eta).\end{aligned}$$

Now, to bound the sum $\sum_{\xi-\eta=\zeta} V_{\mathbf{m}}(\xi)V_{\mathbf{m}}(\eta)$, we use Lemma 5.3 and get

$$\begin{aligned}&\sum_{\zeta\not\equiv\mathbf{0} \pmod{p^r}}\left|\sum_{\xi-\eta=\zeta} f(\xi)\overline{f(\eta)}V_{\mathbf{m}}(\xi)V_{\mathbf{m}}(\eta)\right|^2\\ &\ll \begin{cases} p^{r-\nu_{\mathbf{m}}-1}\left(\sum_{\xi\in V_{\mathbf{m}}}|f(\xi)|^2\right)^2 & \text{if } \|\tilde{\mathbf{m}}\|\not\equiv 0 \pmod{p},\\ p^{r-\nu_{\mathbf{m}}}\left(\sum_{\xi\in V_{\mathbf{m}}}|f(\xi)|^2\right)^2 & \text{if } \|\tilde{\mathbf{m}}\|\equiv 0 \pmod{p}.\end{cases}\end{aligned}$$

So, one has

$$\left(\sum_{x\in(\mathbb{Z}/p^r\mathbb{Z})^2}|(fd\sigma_{V_{\mathbf{m}}})^\vee(x)|^4\right)^{1/2} \ll \frac{p^r}{|V_{\mathbf{m}}|^2}\begin{cases} p^{\frac{r-\nu_{\mathbf{m}}-1}{2}}\sum_{\xi\in V_{\mathbf{m}}}|f(\xi)|^2 & \text{if } \|\tilde{\mathbf{m}}\|\not\equiv 0 \pmod{p},\\ p^{\frac{r-\nu_{\mathbf{m}}}{2}}\sum_{\xi\in V_{\mathbf{m}}}|f(\xi)|^2 & \text{if } \|\tilde{\mathbf{m}}\|\equiv 0 \pmod{p}.\end{cases}$$

Next, Lemma 2.2 gives that $|V_{\mathbf{m}}| \sim p^{r-\nu_{\mathbf{m}}}$. Hence, the theorem follows. ∎

Acknowledgements Thang Pham would like to thank the Vietnam Institute for Advanced Study in Mathematics (VIASM) for the hospitality and for the excellent working condition. Thang Pham, Nguyen Duy Phuong, and Le Quang Ham were supported by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 101.99–2021.09.

References

[1] J. Chapman, M. B. Erdogan, 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**(2012), nos. 1–2, 63–93.
[2] L. Guth, A. Iosevich, Y. Ou, and H. Wang, *On Falconer's distance set problem in the plane*. Invent. Math. **219**(2019), no. 3, 779–830.
[3] D. Koh and H. Sun, *Distance sets of two subsets of vector spaces over finite fields*. Proc. Amer. Math. Soc. **143**(2015), no. 4, 1679–1692.

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press

[4] B. Lichtin, *Distance and sum–product problems over finite p-adic rings*. Proc. London Math. Soc. **118**(2019), no. 6, 1450–1470.
[5] B. Lichtin, *Averages of point configuration problems over finite p-adic rings*. Proc. Amer. Math. Soc. **149**(2021), no. 7, 2825–2839.
[6] B. Lichtin, *k-chain configurations of points over p-adic rings*. Proc. Amer. Math. Soc. **151**(2023), no. 10, 4113–4125.
[7] B. Murphy, G. Petridis, T. Pham, M. Rudnev, and S. Stevens, *On the pinned distances problem over finite fields*. J. London Math. Soc. **105**(2022), no. 1, 469–499.
[8] P. Mattila, *Hausdorff dimension and projections related to intersections*. Publ. Mat. **66**(2022), no. 1, 305–323.
[9] P. Mattila, *A survey on the Hausdorff dimension of intersections*. Math. Comput. Appl. **28**(2023), no. 2, 49.
[10] T. Pham and B. Xue, *New-type quasirandom groups and applications*. J. Fourier Anal. Appl. **64**(2024), 18.
[11] T. Pham and B. Xue, *On the distance problem over finite p-adic rings*. Preprint, 2024. arXiv:2405.07325.
[12] T. Pham and S. Yoo, *Intersection patterns and incidence theorems*. Preprint, 2023. arXiv:2304.08004.

Institute of Mathematical Sciences, ShanghaiTech University, Shanghai 201210, China
e-mail: xuebq@shanghaitech.edu.cn

University of Science, Vietnam National University, Hanoi 100000, Vietnam
e-mail: thangpham.math@vnu.edu.vn

Faculty of Mathematics and Informatics, Hanoi University of Science and Technology, Hanoi 100000, Vietnam
e-mail: hung.lequang@hust.edu.vn

Vietnam Institute of Educational Sciences, Hanoi 100000, Vietnam
e-mail: hamlq2022@gmail.com

People's Security Academy, Hanoi 100000, Vietnam
e-mail: duyphuong78@gmail.com

https://doi.org/10.4153/S0008439525100866 Published online by Cambridge University Press