Restricted sums of sets of cardinality $2p + 1$ in $\mathbb{Z}_p^2$

Jacob Terkel

September 24, 2024

Abstract

Let $A \subseteq \mathbb{Z}_p^2$ be a set of size $2p+1$ for prime $p \geq 5$. In this paper, we prove that $A \hat{+} A = \{a_1 + a_2 \mid a_1, a_2 \in A, a_1 \neq a_2\}$ has cardinality at least $4p$. This result is the first advancement in over two decades on a variant of the Erdős-Heilbronn problem studied by Eliahou and Kervaire.

Key Words— additive combinatorics, additive number theory, sumsets, restricted sumsets, Erdős-Heilbronn conjecture, Cauchy-Davenport theorem, small sumsets.

1 Introduction

In an abelian group G with $A, B \subseteq G$ we write

$$A + B = \{a + b \mid a \in A, b \in B\}$$

to be the sumset of A and B. Similarly, we define

$$A \hat{+} B = \{a + b \mid a \in A, b \in B, a \neq b\}$$

to be the *restricted* sumset of A and B. Often, we write $2A = A + A$ and $2\hat{}A = A \hat{+} A$. A topic of great importance in additive combinatorics is determining the minimum size of $2A$ or $2\hat{}A$ given that $A \subseteq G$ has size m. This question has been answered for all abelian groups in the unrestricted case for over twenty years now [5] but the restricted case remains unsolved in general. More specifically, we are interested in determining the value of the function

$$\rho(G, m) = \min\{|2\hat{}A| \mid A \subseteq G, |A| = m\}.$$

The cases for which the value of this function are known is very limited (see Chapter D.3.1 in [1] for more detail). The case that we are interested in today is a subset of the case where G is an elementary abelian p-group for an odd prime $p \geq 5$. This case was first studied extensively by Eliahou and Kervaire and they obtained the following results

Theorem 1.1 (Eliahou and Kervaire [3], [4]). *If $p \geq 5$ is prime and $p \nmid m-1$ for $m \leq (p+3)/2$*

$$\rho(\mathbb{Z}_p^r, m) = 2m-3.$$

If $p \mid m-1$ and $m \leq (p+3)/2$ we have that

$$2m-3 \leq \rho(\mathbb{Z}_p^r, m) \leq 2m-2.$$

If $m = p+1$ we have that

$$\rho(\mathbb{Z}_p^r, m) = 2m-2 = 2p.$$

This leaves $m = 2p+1$ as the smallest unsolved case.

In this paper, we determine that $\rho(\mathbb{Z}_p^2, 2p+1) = 4p$ for all prime $p \geq 5$. To do this, we will make use of two of the most ubiquitous theorems in additive combinatorics. Before this, we introduce the notation $\min_0$ which we define as

$$\min_0(X) = \max\{0, \min(X)\}.$$

ie. $\min_0(S)$ is equal to the minimum of S when $S \subseteq \mathbb{R}_{\geq 0}$ and 0 if S contains a negative number.

Theorem 1.2 (Cauchy-Davenport Theorem). *For $A, B \subseteq \mathbb{Z}_p$ for some prime p then we have that*

$$|A+B| \leq \min\{|A|+|B|-1, p\}.$$

Theorem 1.3 (Dias Da Silva and Hamidoune [2]). *If p is prime with $A, B \subseteq \mathbb{Z}_p$ we have that*

$$|A \hat{+} B| \geq \min_0\{|A|+|B|-3, p\}.$$

Furthermore, if $|A| \neq |B|$ then

$$|A \hat{+} B| \geq \min_0\{|A|+|B|-2, p\}.$$

Our main result is as follows:

Theorem 1.4. *If $p \geq 5$ is prime then*

$$\rho(\mathbb{Z}_p^2, 2p+1) = 4p.$$

We first establish this simple yet consequential result.

Lemma 1.5. *For $g \in \mathbb{Z}_p^2$ and $A \subseteq \mathbb{Z}_p^2$ we have that*

$$|2\hat{\ }A| = |2\hat{\ }(A+g)|$$

Proof. Note that $a_1 = a_2 \iff a_1 + g = a_2 + g$, and so we have that $2\hat{\ }(A+g) = 2g + 2\hat{\ }A$, from which our claim follows. □

Let H be some non-trivial proper subgroup of $\mathbb{Z}_p^2$ (ie. $H \cong \mathbb{Z}_p$). Similarly, index the cosets of H by $H_0, H_1, \dots, H_{p-1}$ where $H_0 = H$ and $H_i + H_j = H_{i+j}$, and index their intersections with A such that $A_i = A \cap H_i$ and similarly let $B_i = 2\hat{\ }A \cap H_i$. Sometimes we may refer to these indexed sets by indices outside of the range $[0, p-1]$, and these should be identified with their representative within the aforementioned interval modulo p (ie. $H_i = H_{kp+i}$ for all $k \in \mathbb{Z}$ and $i \in [0, p-1]$).

It is obvious that

$$|2\hat{\ }A| = \sum_{i=0}^{p-1} |B_i|$$

as $B_0, B_1, \dots, B_{p-1}$ is a partition of $2\hat{\ }A$. Additionally, we see that

$$B_i = \bigcup_{j=0}^{p-1} (A_j \hat{+} A_{i-j}),$$

and so

$$|B_i| \geq \max_{0 \leq j \leq p-1} |A_j \hat{+} A_{i-j}|.$$

Note that when $j \neq i - j$, A_j and A_{i-j} are disjoint and so $A_j \hat{+} A_{i-j} = A_j + A_{i-j}$. Thus, by Theorem 1.2, Theorem 1.3, and Lemma 1.5 we have that

$$|B_i| \geq \max_{0 \leq j \leq p-1} \{\min_0\{|A_j| + |A_{i-j}| - 1 - 2\epsilon_{i,j}, p\} \mid \emptyset \notin \{A_j, A_{i-j}\}\} \tag{1}$$

where $\epsilon_{i,j} = 1$ if $j = i - j$ and $\epsilon_{i,j} = 0$ otherwise. Now, let α be some index for which $|A_\alpha| \geq |A_i|$ for all i. By the pigeonhole principle, it is seen that $|A_\alpha| \geq 3$. By Lemma 1.5, we may assume, without sacrificing generality, that $\alpha = 0$ Additionally, let m be the number of non-zero i for which A_i is non-empty and let $S = \{1 \leq i \leq p \mid A_i \neq \emptyset\}$. Similarly, let $T = \{1 \leq i \leq p \mid B_i \neq \emptyset\}$, $S_0 = S \cup \{0\}$ and $T_0 = T \cup \{0\}$.

Observe that

$$|2\hat{\ }A| = \sum_{i=0}^{p-1} |B_i| \geq |2\hat{\ }A_0| + \sum_{s \in S} |A_0 + A_s|. \tag{2}$$

and since $|A_s| \leq |A_0|$ if $|A_0| \leq (p+1)/2$ then we have that

$$|2\hat{}A| = \geq |2\hat{}A_0| + \sum_{s \in S} (|A_0| + |A_s| - 1)$$

which can be taken advantage of in a multitude of ways. For this reason, we consider the cases of $|A_0| \leq (p+1)/2$ and $|A_0| \geq (p+3)/2$ separately Specifically, we define **Case 1:** $|A_0| \leq \frac{p+1}{2}$ and **Case 2:** $|A_0| \geq \frac{p+3}{2}$.

2 Case 1: $|A_0| \leq \frac{p+1}{2}$

As mentioned before, the reason we divided this problem into cases based on $|A_0|$ is that, no matter what, in Case 1 we have that $|A_i| + |A_j| - 1 \leq p$, and so

$$|A_i + A_j| \geq \min_0\{p, |A_i| + |A_j| - 1 - 2\epsilon_{i,j}\} = |A_i| + |A_j| - 1 - 2\epsilon_{i,j}$$

as per (1).

We will make use of the following definitions:

$$\mathcal{A} = \{A_i \mid |A_i| \neq \emptyset\},$$

$$\mathcal{A}' = \{A_i \mid |A_i| \neq \emptyset, i \neq 0\}$$

$$\mathcal{A}_w = \{A_i \mid |A_i| = w\},$$

$$\mathcal{B}_w = \{B_i \mid |B_i| = w\},$$

$$C_w = |\mathcal{A}_w|, \qquad D_w = |\mathcal{B}_w|, \qquad D'_w = \sum_{i \geq w} |\mathcal{B}_i|.$$

It is clear that

$$|A| = \sum_{w=1}^{p} wC_w \qquad \text{and} \qquad |2\hat{}A| = \sum_{w=1}^{p} wD_w.$$

Also observe that Now, note that $D'_w - D'_{w+1} = D_w$, and so we have that

$$|2\hat{}A| = \sum_{w=1}^{p} wD_w = \sum_{w=1}^{p} w(D'_w - D'_{w+1}) = \sum_{w=1}^{p} D'_w. \tag{3}$$

Let $m = |S| = |\mathcal{A}| - 1$ (ie. m is the number of non-zero i for which A_i is non-empty.)

By Theorem 1.3, there exists at least $\min_0\{2|\mathcal{A}| - 3, p\} = \min_0\{2m - 1, p\}$ distinct values of i for which there is some $X \in 2\hat{}\mathcal{A}$[1] satisfying $X \subseteq H_i$. In other words, $D_1' \geq \min_0\{2m-1, p\}$. This is the basis for our first instance of subcases, those being

(1A) $m \geq \frac{p+1}{2}$ (in which case B_i must be non-empty for all i) and

(1B) $m \leq \frac{p-1}{2}$ (in which case we must have that $|T \setminus S| \geq m-2$).

Before entering the subcases, we prove the following statement regarding Case 1 in general

Lemma 2.1. *In Case 1*

$$|2\hat{}A| \geq (m+1)(|A_0|-1) + 2p - 1 + \sum_{i \in T \setminus S} |B_i|.$$

Proof. Using (1), Theorem 1.2, and Theorem 1.3 and the fact that $|A_i| + |A_j| - 1 \leq 2|A_0| - 1 \leq p$ for all i, j[2] we get that

$$\sum_{i \in S_0} |B_i| \geq 2|A_0| - 3 + \sum_{i \in S} (|A_0| + |A_i| - 1) = (m+2)|A_0| - 3 - m + \sum_{i \in S} |A_i|$$

$$= (m+2)(|A_0|-1) - 1 + \sum_{i \in S} |A_i| = (m+2)(|A_0|-1) - 1 + (|A| - |A_0|)$$

$$= (m+1)(|A_0|-1) + 2p - 1.$$

Since

$$|2\hat{}A| = \sum_{B_i \in \mathcal{B}} |B_i|$$

we have that

$$|2\hat{}A| = \sum_{i \in T_0} |B_i| = \sum_{i \in S_0} |B_i| + \sum_{i \in T \setminus S} |B_i| \geq (m+1)(|A_0|-1) + 2p - 1 + \sum_{i \in T \setminus S} |B_i|,$$

and so our claim is proven. □

2.1 Case 1A: $m \geq \frac{p+1}{2}$

Lemma 2.2. *In Case 1A, if* $|2\hat{}A| < 4p$ *then* $|A_0| = 3$.

[1] Because the elements of $\mathcal{A}$ are pairwise disjoint and non-empty: every element of $2\hat{}\mathcal{A}$ is non-empty.

[2] From the fact that we are in Case 1.

Proof. As mentioned in the introduction, $|A_0| \geq 3$ by the pigeonhole principle, and so it suffices to prove that $|A_0| \leq 3$. Indeed, since $|B_i| \geq 1$ for all i (implying $|T| = p-1$) with the help of Lemma 2.1 we get that

$$|2\hat{}A| \geq (m+1)(|A_0|-1) + 2p - 1 + \sum_{i \in T \setminus S} |B_i| \geq (m+1)(|A_0|-1) + 2p - 1 + (p - |\mathcal{A}|)$$

$$= 3p + (m+1)(|A_0|-2) - 1.$$

If indeed it is true that $|2\hat{}A| < 4p$ then the above implies

$$4p - 1 \geq 3p + (m+1)(|A_0|-2) - 1$$

which then gives us that

$$|A_0| \leq 2 + \frac{p}{m+1} \leq 2 + \frac{2p}{p+3} = 4 - \frac{2}{p+3} < 4.$$

Thus, $|A_0| \leq 3$ as it is an integer. □

From this, it follows that every set in Case 1A satisfies

$$C_0 + C_1 + C_2 + C_3 = p, \tag{4}$$

$$3C_3 + 2C_2 + C_1 = 2p + 1, \tag{5}$$

and

$$C_1 + C_2 + C_3 = m + 1. \tag{6}$$

Lemma 2.3. *In Case 1A*

$$D_3' \geq \min\nolimits_0\{2C_3 + C_2 + C_1 - 1, p\}.$$

Proof. Via Theorem 1.2, we have that

$$\mathcal{A} + \mathcal{A}_3 = \{A_i \hat{+} A_j \mid A_i \in \mathcal{A}, A_j \in \mathcal{A}_3\}$$

contains members which are subsets of at least $\min_0\{|\mathcal{A}_3| + |\mathcal{A}| - 1, p\} = \min_0\{2C_3 + C_2 + C_1 - 1, p\}$ distinct cosets. Additionally, via (1) we have that $|X| \geq 3$. for all $X \in \mathcal{A} + \mathcal{A}_3$, and from this our claim follows[3]. □

[3] While it is true that the elements $A_i \hat{+} A_j$ of $\mathcal{A} + \mathcal{A}_3$ are restricted sums, for $(A_i, A_j) \in \mathcal{A} \times \mathcal{A}_3$ we have that $A_i \hat{+} A_j = A_i + A_j$ for $|A_i| \neq 3$ implying $|A_i \hat{+} A_j| \geq |A_i| + |A_j| - 1 \geq |A_j| = 3$, and if $|A_i| = 3$ then $|A_i \hat{+} A_j| \geq |A_i| + |A_j| - 3 = 3$.

Similar arguments on

$$\mathcal{A}_3 + \mathcal{A}_2 = \{A_i \hat{+} A_j \mid A_i \in \mathcal{A}_2, A_j \in \mathcal{A}_3\} = \{A_i + A_j \mid A_i \in \mathcal{A}_2, A_j \in \mathcal{A}_3\}$$

and

$$2\hat{\ }\mathcal{A}_3 = \{A_i \hat{+} A_j \mid A_i, A_j \in \mathcal{A}_3, i \neq j\} = \{A_i + A_j \mid A_i, A_j \in \mathcal{A}_3, i \neq j\}$$

result in

Lemma 2.4. *In Case 1A*

$$D'_4 \geq \min_0\{C_3 + C_2 - 1, p\}.$$

and

Lemma 2.5. *In Case 1A*

$$D'_5 \geq \min_0\{2C_3 - 3, p\}.$$

respectively.

Now, we utilize these Lemmas.

Lemma 2.6. *In Case 1A, if $|2\hat{\ }A| < 4p$ and $D_3 \neq p$ then $3 \geq 2C_3 + C_1 + C_0$*

Proof. Since $D'_3 \neq p$, it follows that $D'_4, D'_5 \neq p$ either. Together with facts that $D'_1 = p$, $D'_2 \geq D'_3$, Lemma 2.3, Lemma 2.4, Lemma 2.5, and (3) we get that

$$|2\hat{\ }A| \geq D'_5 + D'_4 + D'_3 + D'_2 + D'_1 \geq p + D'_5 + D'_4 + 2D'_3 \geq p + 7C_3 + 3C_2 + 2C_1 - 6.$$

With (5) and our assumption $|2\hat{\ }A| \leq 4p - 1$ we get that

$$4p - 1 \geq 5p - 4 + C_3 - C_2,$$

and via some rearrangement we get that

$$C_2 + 3 \geq p + C_3,$$

and via substitution of (4) this gives us

$$3 \geq 2C_3 + C_1 + C_0$$

□

Lemma 2.7. *In Case 1A, if $|2\hat{\ }A| < 4p$ and $D'_3 = p$ then $C_0 + C_3 \leq 2$*

Proof. Clearly, if $D_4' = p$ or $D_5' = p$ then $|2\hat{}A| \geq 4p$, and so we may assume D_4' and D_5' are both less than p, and so by Lemma 2.4, Lemma 2.5, and (3) we have that

$$|2\hat{}A| \geq D_5 + D_4 + 3p \geq 3C_3 + C_2 - 4 + 3p.$$

If we have that $4p - 1 \geq 3C_3 + C_2 - 4 + 3p$ which implies

$$p + 3 \geq 3C_3 + C_2.$$

By (5) we now have that

$$C_1 + C_2 \geq p - 2,$$

and thus $C_0 + C_3 \leq 2$ by (4). □

Lemma 2.8. *In Case 1A if $C_3 = 1$ then $C_0 = C_1 = 0$.*

Proof. If $C_3 = 1$ then by (4) and (5) we have that

$$2p - 2 = 2C_2 + C_1 \leq 2C_2 + 2C_1 + 2C_0 = 2p - 2$$

implying $C_1 + 2C_0 = 0$ and our claim follows. □

Lemma 2.9. *In Case 1A, if $C_3 = 2$, $C_0 = 0$ then $|2\hat{}A| \geq 4p$.*

Proof. In the case of $C_3 = 2$ and $C_0 = 0$, by (5) and (4) we have that $C_2 = p - 3$ and so $C_1 = 1$. Without loss of generality, let $|A_0| = 3$, and also $|A_x| = 3$, and $|A_y| = 1$ for $x \neq 0$. For all other i we have that $|A_i| = 2$. (1) now gives us that

$$|B_i| \geq \max_{0 \leq j \leq p-1} \{\min_0\{|A_j| + |A_{i-j}| - 1 - 2\epsilon_{i,j}, p\} \mid \emptyset \notin \{A_j, A_{i-j}\}\}$$

which implies

$$|B_i| \geq \max\{\min_0\{p, |A_x| + |A_{i-x}| - 1\}, \min_0\{p, |A_0| + |A_i| - 1\}\},$$

and because $|A_x| = |A_0| = 3$, and $p \geq 5$ we have that

$$|B_i| \geq 2 + \max\{|A_{i-x}|, |A_i|\}.$$

But now, since $x \neq 0$ it follows that $A_x \neq A_{i-x}$, and thus it follows that at least one of A_x and A_{i-x} are not y which then means that at least one of them has cardinality greater than or equal to 2 meaning for all i we have that $|B_i| \geq 4$ implying $D_4' = p$ and thus $|2\hat{}A| \geq 4p$.

By Lemma 2.5 we have that $D_5' \geq 1$. □

Combining Lemma 2.6, Lemma 2.7, Lemma 2.8, and Lemma 2.9 we can now do the following.

Corollary 2.10. *In Case 1A, if* $|2\hat{\ }A| < 4p$ *then* $C_3 = 1$*,* $C_2 = p - 1$*,* $C_1 = 0$*, and* $C_0 = 0$*.*

Proof. Keep in mind throughout this proof that $C_3 \geq 1$ by the pigeonhole principle.

If $D'_3 = p$ then by Lemma 2.7 we have that $C_3 + C_0 \leq 2$. Thus $C_3 \leq 2$. Since $C_3 \neq 0$ we have either $C_3 = 2$, in which case $C_0 = 0$ by the inequality or $C_3 = 1$ which by Lemma 2.8 implies that $C_0 = C_1 = 0$.

In the case of $C_3 = 2$ and $C_0 = 0$, Lemma 2.9 implies that $|2\hat{\ }A| \geq 4p$.

If $D'_3 \neq p$ then Lemma 2.6 $3 \geq 2C_3 + C_1 + C_0$ directly implies $C_3 = 1$, and so by Lemma 2.8 we have that $C_0 = C_1 = 0$.

Thus, regardless of D'_3 if $|2\hat{\ }A| < 4p$ then we must have that $C_3 = 1$, $C_1 = 0$, $C_0 = 0$, and thus via extension by (4): $C_2 = p - 1$.

□

With the potential number of $2p+1$-subsets narrowed down in Case 1A drastically, we ask the reader to note that if $|2\hat{\ }A| < 4p$ then (WLOG via Lemma 1.5) we have that $|A_0| = 3$ and $|A_i| = 2$ for all non-zero i.

Now we must utilize another famous addition theorem.

Theorem 2.11 (Vosper [7])**.** *If* $A, B \subseteq \mathbb{Z}_p$ *satisfy* $2 \leq |A|, |B|$ *then*

$$|A + B| \leq \min\{|A| + |B| - 1, p - 2\}$$

if and only if A *and* B *are arithmetic progressions with a common difference.*

From this, we can prove the following

Lemma 2.12. *In Case 1A for* $p \geq 7$*, if* $|2\hat{\ }A| < 4p$*, then there exists some* d *for which each* A_i *is an arithmetic progression of difference* d *and this* d *is the same for all* A_i*.*

Proof. First, note that if A_0 was not an arithmetic progression then by Theorem 2.11, for $p \geq 7$, we would have that

$$|B_i| \geq |A_0 + A_i| \geq |A_0| + |A_i| \geq 5$$

for all non-zero i, and because $|B_0| \geq |2\hat{}A_0| \geq 2|A_0| - 3 = 3$ we would have that $|2\hat{}A| \geq 5p - 2 > 4p$.

Thus, A_0 is an arithmetic progression with some difference d.

Since for non-zero i we have $|A_i| = 2$ it is trivial that A_i is an arithmetic progression (let us say with difference d_i). But I now claim that if $|2\hat{}A| \leq 4p - 1$ then for all i: $d_i = d$. We can prove this as follows: By Theorem 2.11 observe that for $i \neq 0$ we have $|B_i| \geq |A_0| + |A_i| - 1 = 5 - \epsilon_i$ where $\epsilon_i = \begin{cases} 1 & d_i = d \\ 0 & d_i \neq d \end{cases}$. Recall that $|B_0| \geq 3$, and by Assuming $|2\hat{}A| \leq 4p - 1$ and letting E be the number of non-zero i for which $\epsilon_i = 1$ we have that

$$4p - 1 \geq 5(p-1) - E + 3 = 5p - 2 - E \geq 4p - 1,$$

and so we equality holds throughout implying $E = p - 1$ and our claim is proven. □

By Lemma 1.5 it suffices to consider only when A_0 takes the form

$$A_0 = \{0, d, 2d\}$$

for some non-zero $d \in H$. Additionally, for non-zero i define a_i such that

$$A_i = \{a_i, a_i + d\}.$$

It should be noted that by (1) that

$$|B_i| \geq \begin{cases} 3 & i = 0; \\ 4 & i \neq 0. \end{cases}, \tag{7}$$

and so if we are to have $|2\hat{}A| \leq 4p - 1$ then equality must hold in (7) for all i.

We now prove some facts regarding our a_i.

Lemma 2.13. *In Case 1A for $p \geq 7$, if $|2\hat{}A| \leq 4p - 1$ then all of the following hold for non-zero i, j with $i \neq j$:*

1. $B_i = \{a_i, a_i + d, a_i + 2d, a_i + 3d\}$,
2. $a_j + a_{i-j} \in A_i = \{a_i, a_i + d\}$,
3. $a_{2i} = 2a_i + \delta d$ *for some* $\delta \in \{-2, -1, 0, 1\}$
4. $B_0 = \{d, 2d, 3d\}$

5. $a_i + a_{-i} = d.$

Proof. With Lemma 2.12 and the above discussion in mind we can prove the statements as follows:

The first claim follows from the fact that we must have that $|B_i| = 4$, $A_0 + A_i = \{a_i, a_i + d, a_i + 2d, a_i + 3d\}$ has size 4 and $A_0 + A_i \subseteq B_i$ meaning $A_0 + A_i = B_i$.

To prove the second claim we see that $A_j + A_{j-i} = \{a_j + a_{i-j}, a_j + a_{i-j} + d, a_j + a_{i-j} + 2d\} \subseteq B_i$ and since $p \geq 7$ this means we must either have that $a_j + a_{i-j} = a_i$ or $a_j + a_{i-j} = a_i + d$, ie. $a_j + a_{i-j} \in A_i$.

For the third claim, we similarly observe that $2\hat{}A_i = \{2a_i + d\} \subseteq B_{2i} = \{a_{2i}, a_{2i} + d, a_{2i} + 2d, a_{2i} + 3d\}$ and we see our claim follows.

For the fourth claim follows from the facts that $|B_0| = 3$ and $2\hat{}A = \{d, 2d, 3d\} \subseteq B_0$ like our proof of Claim 1.

For the fifth claim we see that $A_i + A_{-i} = \{a_i + a_{-i}, a_i + a_{-i} + d, a_i + a_{-i} + 2d\} \subseteq B_0 = \{d, 2d, 3d\}$ implying that $a_i + a_{-i} = d$. □

Let us define $\mu_i = \frac{a_i - (a_{i-1} + a_1)}{d}$. By Lemma 2.13, we have that $\mu_i \in \{0, 1\}$ for all $i \in [3, p-1]$ and $\mu_2 \in \{-2, -1, 0, 1\}$.

Thus, we have the recurrence relation $a_{i+1} = a_1 + a_i + \mu_i$ based on a predefined a_i which gives us

$$d - a_1 = a_{-1} = a_{p-1} = a_1 + \sum_{i=2}^{p-1}(a_1 + d\mu_i) = (p-1)a_1 + d\sum_{i=2}^{p-1}\mu_i,$$

and so it is implied that

$$\sum_{i=2}^{p-1}\mu_i = 1 \mod p,$$

and because the sum cannot exceed p or go below -1, the implication is that $\sum_{i=2}^{p-1}\mu_i = 1$ exactly.

Because $\mu_i \geq 0$ for $i \neq 2$ and $\mu_2 \in \{-2, -1, 0, 1\}$ we have that the number of i (other than 2) for which $\mu_i = 1$ is $1 - \mu_2 \in \{0, 1, 2, 3\}$.

Thus, it follows that, for every a_i we have that for some $\mu_2 \leq u \leq 1 - \mu_2$ we have that $a_i - ud \in K = \langle a_1 \rangle$ Thus, by the 1st and 4th statements in Lemma 2.13 we have that for any $a \in A$ we there exists an integer u within satisfying $\mu_2 \leq u \leq 4 - \mu_2$ such that $a - ud \in K$. However, this then implies that there are at most 5 cosets K_i of K

where $K_i \cap A$ is non-empty, and so we have that there is some other subgroup of $\mathbb{Z}_p^2$ that intersects A at most $5 \leq \frac{p-1}{2}$ different cosets and so we have as follows:

Lemma 2.14. *In Case 1A, for $p \geq 11$, if $|2\hat{}A| < 4p$ then there is an instance in Case 1B or Case 2 with $|2\hat{}A| < 4p$. This then implies that if one manages to prove that $|2\hat{}A| \geq 4p$ in Case 1B and Case 2 then $|2\hat{}A| \geq 4p$ in Case 1A.*

With this, we move towards proving that $|2\hat{}A|$ in Case 1B and Case 2.

2.2 Case 1B: $m \leq \frac{p-1}{2}$

Lemma 2.15. *In Case 1B, if $|2\hat{}A| \leq 4p-1$ then $|A_0|(m+1) - |A| \leq 2$.*

Proof. In this case, since $|\mathcal{B}| \geq \min_0\{p, 2|\mathcal{A}|-3\} = \min_0\{p, 2m-1\}$, we guarantee the existence of at least $m-2$ distinct i such that $i \in T \setminus S$. Let $d = |A_0|(m+1) - |A|$. Now, by Lemma 2.1 we have that

$$4p-1 \geq |2\hat{}A| \geq (m+1)(|A_0|-1)+2p-1+\sum_{i \in T\setminus S} |B_i| \geq (m+1)(|A_0|-1)+2p-1+(m-2)$$

implying

$$2p+3 \geq |A| + d = 2p+1+d,$$

and our claim follows. □

Lemma 2.16. *In Case 1B, $|2\hat{}A| \geq 4p$.*

Proof. Lemma 2.15 implies that there exists some selection of $\omega, \psi \in S$ such that for all $i \in S' = S_0 \setminus \{\omega, \psi\}$ we have that $|A_i| = |A_0|$, and also $2|A_0| - 2 \leq |A_\psi| + |A_\omega| \leq 2|A_0|$.

From this and (1), we may deduce that

$$|B_i| \geq \begin{cases} 2|A_\omega| - 3 & i = 2\omega; \\ 2|A_\psi| - 3 & i = 2\psi; \\ 2|A_0| - 3 & \text{otherwise.} \end{cases} \tag{8}$$

Additionally, via 1.2 there must exist at least $\min_0\{2|\mathcal{A}|-1, p\} = 2m+1$ distinct $x \in [0, p-1]$ such that $x = i + j$ for some (not necessarily distinct) $i, j \in S_0$ Let the set of such x's be $\mathcal{X}$. We account for $m+1$ of these via $0+i = i$ for $i \in S_0$, and so using Lemma 2.1, (8), the facts that $(m+1)|A_0| = 2p+1+d$, $|A_\omega|+|A_\psi| \geq 2|A_0| - d$, $|A_0| \leq (p+1)/2$, and $m \leq (p-1)/2$ we have that

$$|2\hat{}A| \geq (m+1)(|A_0|-1) + 2p - 1 + \sum_{i \in \mathcal{X} \setminus S_0} |B_i|$$

$$\geq (m+1)(|A_0|-1) + 2p - 1 + (m-2)(2|A_0|-3) + (2|A_\omega|-3) + (2|A_\psi|-3)$$

$$= 4p + d - (m+1) + (m-2)(2|A_0|-3) + (2|A_\omega|-3) + (2|A_\psi|-3)$$

$$= 4p + d - m - 1 + (2m|A_0| - 4|A_0| - 3m + 6) + (4|A_0| - 2d - 6)$$

$$= 4p + 2m|A_0| - 4m - d - 1$$

$$= 4p + 2(m+1)|A_0| - 4m - d - 1 - 2|A_0|$$

$$= 8p + d + 1 - 2|A_0| - 4m \geq 8p + 1 - (p+1) - 2(p-1) = 5p + 2 > 4p.$$

Our claim now follows from the above and Lemma 2.15. □

3 Case 2: $|A_0| \geq \frac{p+3}{2}$

In this section, we yet again introduce more terminology. Let ℓ be the number of non-zero i for which $|A_0| + |A_i| - 1 \geq p$, and let s be the number of non-zero i where A_i is non-empty and $|A_0| + |A_i| - 1 < p$. It follows that $m = \ell + s$. This distinction is made as ℓ is the number of $i \in S$ for which $|A_0 + A_i|$ is guaranteed to have size p per Theorem 1.2. We now will move towards proving a Lemma akin to Lemma 2.1, but instead for Case 2.

Lemma 3.1. *In Case 2, $|2\hat{}A_0| = p$.*

Proof. From Theorem 1.3, we have that

$$p \geq |2\hat{}A_0| \geq \min_0\{2|A_0| - 3, p\} \geq \min_0\left\{2\frac{p+3}{2} - 3, p\right\} = \min_0\{p, p\} = p.$$

□

Lemma 3.2. *In Case 2,*

$$|2\hat{}A| \geq (l+1)p + s|A_0| + \sum_{i \in T \setminus S} |B_i|.$$

Proof. Keeping (1) and specifically Theorem 1.2 in mind we have that

$$|2\hat{}A| = \sum_{i \in T_0} |B_i| = \sum_{i \in S_0} |B_i| + \sum_{i \in T \setminus S} |B_i| \geq |2\hat{}A_0| + \sum_{i \in S} |B_i| + \sum_{i \in T \setminus S} |B_i|,$$

and now with Lemma 3.1 we get that

$$|2\hat{}A| \geq p + \sum_{i\in S} |B_i| + \sum_{i\in T\setminus S} |B_i| \geq p + \sum_{i\in S} |A_0 + A_i| + \sum_{i\in T\setminus S} |B_i|$$

$$\geq (l+1)p + s|A_0| + \sum_{i\in T\setminus S} |B_i|.$$

□

We now will demonstrate that, for each value of ℓ we have that $|4\hat{}A| \geq 4p$

Lemma 3.3. *In Case 2, If $\ell \geq 3$ then $|2\hat{}A| \geq 4p$.*

Proof. From Lemma 3.2, if $\ell \geq 3$ then

$$|2\hat{}A| \geq 4p + s|A_0| + \sum_{i\in T\setminus S} |B_i| \geq 4p.$$

□

For $\ell \leq 2$, we must often provide special consideration to smaller values of s.

Lemma 3.4. *In Case 2, If $\ell = 2$ and $s \geq 2$ then $|2\hat{}A| \geq 4p$.*

Proof. From Lemma 3.2, if $\ell = 2$ then

$$|2\hat{}A| \geq 3p + s|A_0| + \sum_{i\in T\setminus S} |B_i| \geq 3p + s\frac{p+3}{2},$$

and so if $s \geq 2$ then $|2\hat{}A| \geq 4p$. □

Lemma 3.5. *In Case 2, If $\ell = 2$ and $s = 1$ then $|4\hat{}A| \geq 4p$.*

Proof. In this case we may define β, γ, and δ to be the three distinct elements of $[1, p-1]$ such that A_β, A_γ, and A_δ are not empty satisfying

$$|A_0| \geq |A_\beta| \geq |A_\gamma| \geq p + 1 - |A_0| > |A_\delta|$$

and

$$|A_0| + |A_\beta| + |A_\gamma| + |A_\delta| = 2p + 1.$$

These conditions intersect to give us that

$$2p+1 < p+1+|A_\beta|+|A_\gamma|$$

or

$$p < |A_\beta|+|A_\gamma|,$$

and thus $|A_\beta| \geq \frac{p+1}{2}$.

Now see that

$$S=\{0,\beta,\gamma,\delta\}$$

and

$$\beta+S=\{\beta,2\beta,\beta+\gamma,\beta+\delta\}$$

must not be the same set as this would imply that the sets have that same sum, and thus

$$4\beta=0$$

which cannot be as $\beta \neq 0$. Thus, for some $\iota \in S$ we have that $\beta+\iota \in T \setminus S$. If $\iota=\beta$ then it is seen that

$$|B_{\beta+\iota}|=|B_{2\beta}| \geq |2\hat{}A_\beta| \geq 2|A_\beta|-3 \geq |A_\beta|+\frac{p-5}{2} \geq |A_\beta|$$

as $p \geq 5$. It is also observed that if $\iota \neq \beta$ then

$$|B_{\beta+\iota}| \geq |A_\beta|+|A_\iota|-1 \geq |A_\beta|.$$

Regardless, $|B_{\beta+\iota}| \geq |B_\beta| \geq \frac{p+1}{2}$.

Thus, by Lemma 3.2 we have

$$|2\hat{}A| \geq 3p+|A_0|+|B_{\beta+\iota}| \geq 4p+2 \geq 4p.$$

□

Lemma 3.6. *In Case 2, If $\ell=2$ and $s=0$ then $|2\hat{}A| \geq 4p$.*

Proof. We let $S=\{\beta,\gamma\}$ such that

$$p \geq |A_0| \geq |A_\beta| \geq |A_\gamma| \geq 1.$$

By Theorem 1.2, there are at least 5 distinct elements in the set

$$2\{0,\beta,\gamma\}=\{0,\beta,\gamma,\beta+\gamma,2\beta,2\gamma\}.$$

Since $0, \beta, \gamma$ are distinct by Lemma 3.2 we then have that

$$|2\hat{}A| \geq 3p + |B_{2\beta}| + |B_{2\gamma}| + |B_{\beta+\gamma}| - \max\{|B_{2\beta}|, |B_{2\gamma}|, |B_{\gamma+\beta}|\}.$$

Note now that because $|A_0|+|A_\beta|+|A_\gamma| = 2p+1$ and $|A_0| \leq p$ we have that $|A_\beta|+|A_\gamma| \geq p+1$, and so we have that

$$|B_{\beta+\gamma}| \geq |A_\beta + A_\gamma| \geq |A_\beta| + |A_\gamma| - 1 \geq p.$$

This then gives us that

$$|2\hat{}A| \geq 3p + |B_{2\beta}| + |B_{2\gamma}| \geq 3p + |2\hat{}A_\beta| + |2\hat{}A_\gamma|$$

$$\geq 3p + \min\nolimits_0\{p, 2|A_\beta| - 3\} + \min\nolimits_0\{p, 2|A_\gamma| - 3\}.$$

Thus, if $|2\hat{}A| \leq 4p - 1$ then we must have that

$$|2\hat{}A| \geq 3p + 2|A_\beta| + 2|A_\gamma| - 6 \geq 5p - 4 > 4p.$$

□

For the case of $\ell = 1$ we let β be the unique element of S such that $|A_0|+|A_\beta|-1 \geq p$.

Lemma 3.7. *In Case 2, If $\ell = 1$ and $|2\hat{}A| \leq 4p - 1$ then either*

1. *$s = 1$ or*
2. *$s = 2$ and $|A_\beta| = |A_\alpha|$.*

Proof. Note that $s \neq 0$ as we must have that $2 \leq m = \ell + s = s + 1$.

We now observe that

$$|2\hat{}A| \geq \sum_{i \in S_0} |B_i| \geq 2p + \sum_{i \in S\setminus\{\beta\}} |B_i| \geq 2p + \sum_{i \in S\setminus\{\beta\}} |A_0 + A_i| \geq 2p + \sum_{i \in S\setminus\{\beta\}} (|A_0| + |A_i| - 1).$$

$$= 2p + s(|A_0| - 1) + (|A| - |A_0| - |A_\beta|) = 4p + (s-1)(|A_0| - 1) - |A_\beta|.$$

If $s \geq 3$ we have that

$$|2\hat{}A| \geq 4p + 2(|A_0| - 1) - |A_\beta| \geq 4p + |A_0| - 2 \geq 4p.$$

If $s = 2$, let us define $\delta = |A_0| - |A_\beta|$ and see that

$$|2\hat{}A| \geq 4p + (|A_0| - 1) - |A_\beta| \geq 4p - 1 + \delta,$$

and so if $\delta \neq 0$ (or equivalently $|A_0| = |A_\beta|$) then $|2\hat{}A| \geq 4p$.

Our claim now follows. □

Lemma 3.8. *In Case 2, if $\ell = 1$ and $s = 2$ then $|2\hat{}A| \geq 4p$.*

Proof. In this case, consider the typical coset partition $A = A_0 \cup A_\beta \cup A_\gamma \cup A_\delta$ with

$$|A_0| \geq |A_\beta| \geq p + 1 - |A_0| > |A_\gamma|, |A_\delta|.^{4}$$

By Lemma 3.7 we also have that $|A_0| = |A_\beta|$ and so

$$|B_{2\beta}| \geq |2\hat{}A_\beta| \geq \min_0\{2|A_\beta| - 3, p\} \geq \min_0\left\{2\frac{p+3}{2}, p\right\} \geq \min_0\{p, p\} = p.$$

If $2\beta \notin \{\gamma, \delta\}$ then we have that $\{0, \beta, \gamma, \delta, 2\beta\}$ are distinct and so we have that

$$|2\hat{}A| \geq |B_0| + |B_\beta| + |B_{2\beta}| + |B_\gamma| + |B_\delta| \geq 3p + 2|A_0| \geq 4p + 3 \geq 4p.$$

Assume WLOG then that $\delta = 2\beta$. This then implies $\{0, \beta, 2\beta, \gamma\}$ are pairwise distinct. If $\delta + \beta$ is also pairwise distinct from these four then we similarly obtain

$$|2\hat{}A| \geq |B_0| + |B_\beta| + |B_{2\beta}| + |B_\gamma| + |B_{\beta+\delta}| \geq 3p + 2|A_0| \geq 4p + 3 \geq 4p.$$

Thus, if $|2\hat{}A| \leq 4p - 1$ then $\delta + \beta \in \{0, \beta, 2\beta, \gamma\}$, but clearly we cannot have $\delta + \beta = \beta$ or $\delta + \beta = 2\beta$ We additionally see that $\delta + \beta \neq 0$, as this would mean that $3\beta = 0$ which cannot be as $p \geq 5$ and $\beta \neq 0$.

Thus, if $|2\hat{}A| \leq 4p - 1$ then $\delta + \beta = \gamma$ which implies that $3\beta = \gamma$ and so

$$S_0 = \{0, \beta, 2\beta, 3\beta\}$$

in which case (implied by the fact that $p \geq 5$) gives us

$$|2\hat{}A| \geq |B_0| + |B_\beta| + |B_{2\beta}| + |B_{3\beta}| + |B_{4\beta}| = 3p + |B_\delta| + |B_{\beta+\delta}|$$

$$\geq 3p + 2|A_0| \geq 4p + 2 > 4p.$$

[4] Unlike the case of $\ell = 2$ and $s = 1$ we may have that $|A_\gamma| < |A_\delta|$.

□

Lemma 3.9. *In Case 2, if $\ell = 1$ then $s \neq 1$.*

Proof. We have the coset partition $A = A_0 \cup A_\beta \cup A_\gamma$ with

$$|A_0| \geq |A_\beta| \geq p + 1 - |A_0| > |A_\gamma|$$

and

$$|A_0| + |A_\beta| + |A_\gamma| = 2p + 1.$$

Together, these imply that $|A_\beta| > p$, which cannot be. □

We now move to the final case: $\ell = 0$.

Lemma 3.10. *In Case 2, if $\ell = 0$ then $|2\hat{}A| \geq 4p$.*

Proof. If $\ell = 0$ then it follows that for all non-zero i we have $|A_i| + |A_0| - 1 \leq p - 1$, and since $|A_0| \geq \frac{p+3}{2}$ we have that

$$|A_i| \leq \frac{p-3}{2}.$$

Additionally, observe that for any $j \in S$ we have that

$$2p + 1 = |A| = \sum_{i \in S_0} |A_i| = (|A_0| + |A_j|) + \sum_{i \in S \setminus \{j\}} |A_i| \leq p + (s-1)\frac{p-3}{2},$$

and so we have that

$$s \geq 1 + \frac{2p+2}{p-3} = 3 + \frac{8}{p-3} > 3,$$

and so we must have $s \geq 4$.

We now use (2), Lemma 3.1, and (1) to get

$$|2\hat{}A| = \sum_{i \in T_0} |B_i| \geq |2\hat{}A_0| + \sum_{i \in S} |A_0 + A_i| \geq p + \sum_{i \in S}(|A_0| + |A_i| - 1) = p + s(|A_0| - 1) + (|A| - |A_0|)$$

$$= 3p + (s-1)(|A_0| - 1).$$

We now recall that $s \geq 4$ and $|A_0| \geq \frac{p+3}{2}$ and so we have that

$$|2\hat{}A| \geq \frac{9p+9}{2} > 9p/2 > 4p.$$

□

Lemma 3.11. *In Case 2, we have that $|2\hat{}A| \geq 4p$.*

Proof. If $\ell \geq 3$ then our claim follows from Lemma 3.3. If $\ell = 2$ then our claim follows from Lemma 3.4, Lemma 3.5, and Lemma 3.6. If $\ell = 1$ then our claim follows from Lemma 3.7, Lemma 3.8, and Lemma 3.9. Lastly, if $\ell = 0$ then our claim follows from Lemma 3.10. □

4 Conclusion

With this, we have that regardless of m or $|A_0|$: $|2\hat{}A| \geq 4p$ for all $A \subseteq \mathbb{Z}_p^2$ for $p \geq 11$ and $|A| = 2p+1$ and so Theorem 1.4 is proven for all p except $p = 5, 7$. Using [6] with a powerful enough computer verifies the theorem for these two values of p, completing the proof of Theorem 1.4.

While this result is a major step forward, the author advises caution for a reader who wishes to generalize this result using the methods in this paper. There are two potential directions for generalization. The first is relaxing the condition of $G \cong \mathbb{Z}_p^2$ to $G \cong \mathbb{Z}_p^r$ for some r. While Case 1B (and to a lesser extent Case 2) seem capable make this generalization with only a few minor issues, Case 1A's reduction to the other two cases relies explicitly on both $H \cong \mathbb{Z}_p$ and $G/H \cong \mathbb{Z}_p$ which is only possible in the case of $G \cong \mathbb{Z}_p^2$. In order to prove that $\rho(\mathbb{Z}_p^r, 2p+1) = 4p$ is true for a sufficiently large p, a new method must be developed for Case 1A.

Regardless, the author believes that Theorem 1.4 generalizes in its entirety. Specifically:

Conjecture 4.1. *If $p \geq 5$ is prime then*

$$\rho(\mathbb{Z}_p^r, 2p+1) = 4p.$$

The second way that the results of this paper can be generalized is by determining $\rho(\mathbb{Z}_p^2, kp+1)$ for $k \geq 3$. Like before, Case 1B seems to generalize rather nicely, and Case 1A also does not appear to have any outstanding issues regarding its generalization (except perhaps, a stricter lower bound on when Lemma 2.14 reduces the problem to Cases 1B and 2). The problem occurs when examining Case 2. Here, to prove that Case 2 cannot provide a counterexample to $\rho(\mathbb{Z}_p^2, 2p+1) = 4p$ we considered each value of ℓ, one at a time. However, if one were to go out and prove, say $\rho(\mathbb{Z}_p^2, 3p+1) = 6p$ they would need to consider $\ell \leq 4$ if they wanted to directly adapt the methods used in this paper. And if one wishes to consider the general case of proving that $\rho(\mathbb{Z}_p^2, kp+1) = 2kp$ then they will need to consider every case when $\ell \leq 2kp - 2$ which will require a less "brute force" approach than what is used in Section 3.

Another natural question following the results of this paper is to solve the corresponding "inverse problem" of Theorem 1.4, ie. the problem of classifying all $2p+1$-sets $A \subseteq \mathbb{Z}_p^2$ such that $|2\hat{}A| = \rho(\mathbb{Z}_p^2, 2p+1) = 4p$. The equivalent problem for sets of size $p+1$ was solved in [4] as follows.

Theorem 4.2 (Eliahou and Kervaire [4])**.** *For prime $p \geq 5$ and $A \subseteq \mathbb{Z}_p^r$ if $|A| = p+1$ and $|2\hat{}A| = 2p$ then there exists an order p subgroup $Z < \mathbb{Z}_p^r$ such that A is the union of a coset of Z and a single element outside of said coset.*

We believe that our case is rather similar and offer the following conjecture:

Conjecture 4.3. *For prime $p \geq 7$ then for $A \subseteq \mathbb{Z}_p^2$ if $|A| = 2p+1$ and $|2\hat{}A| = 4p$ then there exists an order p subgroup $Z < \mathbb{Z}_p^2$ with canonical homomorphism $\phi : \mathbb{Z}_p^2 \to Z$ such that $\phi(A)$ is an arithmetic progression of length three and that there is a unique element $a \in A$ such that $A \setminus \{a\}$ is the union of two cosets of Z.*

References

[1] Bela Bajnok. *Additive Combinatorics: A Menu of Research Problems*. Discrete Mathematics and Its Applications. CRC Press, Boca Raton, FL, 2018.

[2] J. A. Dias Da Silva and Y. O. Hamidoune. Cyclic spaces for grassmann derivatives and additive theory. *Bulletin of the London Mathematical Society*, 26(2):140–146, 1994.

[3] Shalom Eliahou and Michel Kervaire. Sumsets in vector spaces over finite fields. *Journal of Number Theory*, 71(1):12–39, 1998.

[4] Shalom Eliahou and Michel Kervaire. Restricted sums of sets of cardinality $1+p$ in a vector space over $\mathbb{F}_p$. *Discrete Mathematics*, 235(1):199–213, 2001. Chech and Slovak 3.

[5] Shalom Eliahou, Michel Kervaire, and Alain Plagne. Optimally small sumsets in finite abelian groups. *Journal of Number Theory*, 101(2):338–348, 2003.

[6] John Llano. Sumset generator. http://cs.gettysburg.edu/~llanjo01/addcomb/sumsets.html, 2024.

[7] A. G. Vosper. The critical pairs of subsets of a group of prime order. *Journal of the London Mathematical Society*, s1-31(2):200–205, 1956.