

Restricted Sumsets with Bounded-Degree Relations Near the Critical Line

Boyan Duan*

Minghui Ouyang†

Zheng Wang‡

Abstract

Given a prime number p , nonempty subsets $A, B \subseteq \mathbb{F}_p$, and a binary relation $R \subseteq A \times B$, define the restricted sumset $A +_R B := \{a + b : a \in A, b \in B, (a, b) \notin R\}$. When $A = B$ and R is the equality relation, this is the classical Erdős–Heilbronn problem, which was solved by Dias da Silva and Hamidoune, and by Alon, Nathanson and Ruzsa. For an arbitrary binary relation R with maximum degree at most a fixed integer Δ , earlier results give sharp lower bounds when $|A| + |B| \leq (1 - \varepsilon)p$ for fixed $\varepsilon > 0$ and sufficiently large p . In this paper, we study the regime $|A| + |B| \approx p$. Writing $S := \mathbb{F}_p \setminus (A +_R B)$, we prove that $|S| \ll_{\Delta} p^{1/3}$ whenever $|A| + |B| \geq p$. This improves Lev’s square-root bound when R is a matching and $|A| + |B| \geq p + 1$. For $|A| + |B| = p - h$ with $h \geq 0$, we prove $|S| \ll_{\Delta} h + 1 + p^{1/3}(h + 1)^{1/3}$.

We also construct examples with $|S| = \Omega(\log p)$, improving Huicochea’s lower bound of $\Omega(\log p / \log \log p)$. These examples give a negative answer to a question of Lev concerning restricted sumsets defined by injective maps.

1 Introduction

Given a prime number p and two nonempty subsets $A, B \subseteq \mathbb{F}_p$, their sumset is defined by $A + B := \{a + b : a \in A, b \in B\}$. The classical Cauchy–Davenport theorem [5, 6] states that

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

A natural generalization is to exclude some pairs from $A \times B$ and consider the sums formed by the remaining pairs. The classical Erdős–Heilbronn problem concerns the case $A = B$, with the diagonal pairs forbidden; see [2]. Dias da Silva and Hamidoune [7] proved the original conjecture. Alon, Nathanson and Ruzsa [2, 3] subsequently solved the general nonsymmetric case. Their method also applies to restrictions of the form $P(a, b) \neq 0$, where $P(x, y) \in \mathbb{F}_p[x, y]$ has low degree; see also Alon’s Combinatorial Nullstellensatz [1].

In this paper, we study restrictions given by a binary relation $R \subseteq A \times B$. Define $A +_R B := \{a + b : a \in A, b \in B, (a, b) \notin R\}$, where R consists of the forbidden pairs. We write $\Delta(R)$ for the maximum degree of the bipartite graph associated with R , taking the maximum over both vertex classes. A relation R is a matching if $\Delta(R) \leq 1$. We focus on relations satisfying $\Delta(R) \leq \Delta$, where $\Delta \geq 1$ is a fixed integer. This setting includes the classical Erdős–Heilbronn problem, restrictions given by matchings [15], and restrictions of the form $a - b \in T$ for sets $T \subseteq \mathbb{F}_p$ of bounded size [19].

There has been substantial progress when $|A| + |B|$ is bounded away from p . Lev [16, Theorem 5] proved that $|\{a + b : a \in A, b \in B, b \neq \tau(a)\}| \geq |A| + |B| - 3$ for arbitrary maps $\tau : A \rightarrow B$, provided that $|B| < p/2$ and $|A| < \sqrt{|B|} + 1$. Bollobás, Leader and Tiba [4, Theorem 9] proved that $|A +_R A| \geq 2|A| - 1 - 2\Delta$ when each $a \in A$ has at most Δ forbidden partners, provided that $|A| < (1 - \varepsilon)p/2$ and $|A|$ is sufficiently large in terms of ε and Δ . Ouyang [18, Theorem 1.7] extended their method to possibly distinct summands A and B , obtaining $|A +_R B| \geq |A| + |B| - 1 - 2\Delta$ when $|A| + |B| \leq (1 - \varepsilon)p$ and p is sufficiently large in terms of ε and Δ . His proof also uses the rectification theorem of Green and Ruzsa [9]. Huicochea [12, Theorem 1.6] proved that $|\{a + b : a \in A, b \in B, b \neq \tau(a)\}| \geq |A| + |B| - 3$ for arbitrary maps $\tau : A \rightarrow \mathbb{F}_p$, provided that $|A| \leq |B|$, $p \geq 10^{60000}$, and $2|A| + |B| \leq p - 1800p^{31/32}$.

*School of Computer Science, ETH Zürich, Zürich 8092, Switzerland. boduan@student.ethz.ch.

†School of Mathematical Sciences, Peking University, Beijing 100871, China. ouyangminghui1998@gmail.com.

‡School of Mathematical Sciences, Peking University, Beijing 100871, China. wangzheng0401@hotmail.com.

We now consider the range where $|A| + |B|$ is close to p . In this range, the main object of interest is the *avoiding set* $S := \mathbb{F}_p \setminus (A +_R B)$ [18]. Lev [15, Theorem 3] proved that S is a Sidon set if R is a matching and $|A| + |B| \geq p + 1$, giving $|S| = O(\sqrt{p})$. Our first result gives a cubic-root bound on $|S|$ for relations of bounded degree on both sides when $|A| + |B| \geq p$, and also covers the subcritical case.

Theorem 1.1. *Let p be a prime and let $\Delta \geq 1$ be an integer. Let A and B be two nonempty subsets of $\mathbb{F}_p$, and let $R \subseteq A \times B$ have maximum degree at most Δ on both sides.*

(i) (Critical and supercritical case) *If $|A| + |B| \geq p$, then*

$$|\mathbb{F}_p \setminus (A +_R B)| \ll_{\Delta} p^{1/3}.$$

(ii) (Subcritical case) *Suppose that $|A| + |B| = p - h$ with $h \geq 0$. Then*

$$|\mathbb{F}_p \setminus (A +_R B)| \ll_{\Delta} h + 1 + p^{1/3}(h + 1)^{1/3}.$$

We next construct examples with large avoiding sets. Lev constructed examples in which R is a matching, with two missing residues when $|A| + |B| \geq p + 2$ and three when $|A| + |B| = p + 1$ [15]. Ouyang extended the latter example to larger symmetric sets, still with R a matching [18, Theorem 1.11(ii)]. More recently, Huicochea constructed examples with $\Omega(\log p / \log \log p)$ missing residues at every fixed distance below p [12, Corollary 1.5]. Our construction improves the number of missing residues to order $\log p$ for every fixed value of $|A| + |B| - p$.

Theorem 1.2. *Let $p > 3$ be prime and let $K, \Delta, m \geq 1$ be integers. If*

$$\left\lfloor \frac{p}{3^m} \right\rfloor + 1 - \left(\Delta - \frac{2}{3} \right) 3^m \geq K,$$

then there exist nonempty $A, B \subseteq \mathbb{F}_p$ and $R \subseteq A \times B$ with $|A| + |B| = p + K$ and $\Delta(R) \leq \Delta$ such that

$$|\mathbb{F}_p \setminus (A +_R B)| = \Delta(m + 1).$$

By choosing m appropriately in Theorem 1.2 and passing to subsets when necessary, we obtain the following corollary.

Corollary 1.3. *Let p be prime, and let $\Delta \geq 1$ and $1 \leq K \leq p$ be integers. Then there exist nonempty $A, B \subseteq \mathbb{F}_p$ and $R \subseteq A \times B$ satisfying $|A| + |B| = p + K$, $\Delta(R) \leq \Delta$, and*

$$|\mathbb{F}_p \setminus (A +_R B)| \geq \frac{\Delta}{2 \log 3} \log \frac{p}{K} - O_{\Delta}(1).$$

Taking $K = 1$ and passing to suitable nonempty subsets of A and B , we also obtain $|A| + |B| = p$, $\Delta(R) \leq \Delta$, and

$$|\mathbb{F}_p \setminus (A +_R B)| \geq \frac{\Delta}{2 \log 3} \log p - O_{\Delta}(1).$$

Lev [15] asked whether, for every prime p , nonempty sets $A, B \subseteq \mathbb{F}_p$, and injection $\tau : A \rightarrow B$, the relation $R = \{(a, \tau(a)) : a \in A\}$ satisfies

$$|A +_R B| \geq \begin{cases} |A| + |B| - 3, & |A| + |B| \leq p, \\ p - 3, & |A| + |B| = p + 1, \\ p - 2, & |A| + |B| \geq p + 2. \end{cases} \quad (1)$$

Such a relation R is a matching covering every vertex of A . For $\Delta = 1$, after interchanging the summands if necessary, we can complete the matchings in Corollary 1.3 to injections by adding forbidden pairs. This can only shrink the restricted sumset, giving counterexamples to (1). Huicochea [12] also refutes this conjecture in the subcritical case using a construction that yields the

weaker lower bound $\Omega(\log p / \log \log p)$ for the size of the avoiding set (see the comparison at the end of Section 3).

Throughout the paper, $\log$ denotes the natural logarithm. For $X \subseteq \mathbb{F}_p$, write $X^c := \mathbb{F}_p \setminus X$. For nonnegative quantities f, g , we write $f \ll_{\Delta} g$ if $f \leq C_{\Delta} g$ for a constant $C_{\Delta} > 0$ depending only on Δ . We write $f \asymp_{\Delta} g$ if both $f \ll_{\Delta} g$ and $g \ll_{\Delta} f$. When the subscript is omitted, the implied constants are absolute.

Paper organization. In Section 2, we prove Theorem 1.1. In Section 3, we prove Theorem 1.2 using a periodic construction and deduce Corollary 1.3. We include further remarks and open problems in Section 4. In Appendices A and B, we give an alternative upper-bound argument and an asymmetric grid construction for the critical case.

2 Upper bounds near the critical line

We begin with the graph-theoretic proof of Lev's square-root bound for the avoiding set $S := \mathbb{F}_p \setminus (A +_R B)$ [15, Theorem 3]. This argument is the starting point for our proof.

Consider the bipartite graph Γ_S whose vertex classes are two disjoint copies of $\mathbb{F}_p$, denoted by $\mathbb{F}_p^{(L)}$ and $\mathbb{F}_p^{(R)}$. Vertices $x^{(L)}$ and $y^{(R)}$ are adjacent if and only if $x + y \in S$. Let $G_S := \Gamma_S[A^{(L)} \cup B^{(R)}]$ denote the subgraph induced by $A^{(L)} \cup B^{(R)}$.

The graph Γ_S is $|S|$ -regular, and translating its left vertices by t and its right vertices by $-t$ preserves adjacency. The edges of G_S correspond to representations of elements of S as sums of elements of A and B . We identify an edge $a^{(L)}b^{(R)}$ of G_S with the pair (a, b) . Since S is the avoiding set, every such pair is forbidden, and hence $E(G_S) \subseteq R$.

The key fact is that Γ_S is $K_{2,2}$ -free when R is a matching and $|A| + |B|$ is slightly above the critical line, that is, when $|A| + |B| \geq p + 1$. Indeed, since $E(G_S) \subseteq R$, the graph G_S contains no copy of $K_{1,2}$ centered in either vertex class. If Γ_S contained a copy of $K_{2,2}$, then translating its left vertices by t and its right vertices by $-t$ would produce another copy of $K_{2,2}$ for every $t \in \mathbb{F}_p$. As t ranges over $\mathbb{F}_p$, the four moving vertices have a total of $2(|A| + |B|) > 2p$ incidences with $A^{(L)} \cup B^{(R)}$. Some translate therefore has at least three vertices in this union. This gives a vertex of degree at least two in G_S , a contradiction. Counting copies of $K_{1,2}$ centered in the right vertex class of Γ_S gives $p \binom{|S|}{2} \leq \binom{p}{2}$, and hence $|S| < \sqrt{p} + 1/2$.

When $|A| + |B| \leq p$ or $\Delta \geq 2$, the argument above no longer excludes $K_{2,2}$. We therefore count copies of $K_{1,2}$ in G_S by a different argument.

2.1 Translation boundaries and counts of $K_{1,2}$

To compare a set with its translates, we use the following quantity.

Definition 2.1. For $X \subseteq \mathbb{F}_p$ and $d \in \mathbb{F}_p$, define the *translation boundary* of X at d by

$$\partial X(d) := |X \triangle (X + d)|.$$

Since $|X| = |X + d|$, we have $\partial X(d) = 2|(X + d) \setminus X|$. The quantity $|(X + d) \setminus X|$ was studied by Erdős and Heilbronn [8] and Olson [17]. Its basic properties are discussed by Konyagin and Lev [13]; see also Lev [16] and Huicochea [11].

The following lemma records the basic properties of the translation boundary.

Lemma 2.2. Let $X \subseteq \mathbb{F}_p$. For all $x, y \in \mathbb{F}_p$, $\partial X(x + y) \leq \partial X(x) + \partial X(y)$. Moreover,

$$\frac{1}{p} \sum_{x \in \mathbb{F}_p} \partial X(x) = 2|X| \left(1 - \frac{|X|}{p}\right). \quad (2)$$

In particular, if $|X| \leq p/2$, this average is at least $|X|$.

Proof. For the first assertion,

$$X \triangle (X + x + y) \subseteq (X \triangle (X + x)) \cup ((X + x) \triangle (X + x + y)).$$

The two sets on the right have sizes $\partial X(x)$ and $\partial X(y)$, respectively, which proves the first assertion.

For the second assertion, translation invariance gives $\partial X(x) = 2(|X| - |X \cap (X + x)|)$. Moreover, $\sum_{x \in \mathbb{F}_p} |X \cap (X + x)| = |X|^2$, since the sum counts ordered pairs of elements of X according to their difference. Summing the preceding identity for $\partial X(x)$ over $x \in \mathbb{F}_p$ and dividing by p proves (2). The final assertion follows immediately from (2). $\square$

For $X, Y \subseteq \mathbb{F}_p$ and $u \in \mathbb{F}_p$, define

$$r_{X,Y}(u) := |\{(x, y) \in X \times Y : x + y = u\}|.$$

We write $e_u := r_{A,B}(u)$. If $u \in S$, every representation counted by e_u is an edge of R . Therefore, with $n = \min\{|A|, |B|\}$,

$$\sum_{u \in S} e_u \leq \Delta n. \quad (3)$$

For $d \in \mathbb{F}_p$, we shall also write

$$\rho(d) := |S \cap (S - d)| = |\{(u, v) \in S \times S : u - v = d\}|.$$

Thus $\rho(d)$ is the number of representations of d as a difference of two elements of S , with order taken into account.

The following lemma bounds $\partial A(u - v)$ in terms of the numbers of representations of u and v as $a + b$, where $a \in A$ and $b \in B$.

Lemma 2.3. *Suppose that $|A| + |B| = p - h$ with $h \in \mathbb{Z}$. For all $u, v \in \mathbb{F}_p$, we have*

$$\partial A(u - v) \leq 2(e_u + e_v + h).$$

Proof. Put $d := u - v$. Since $|A| = |A + d|$, we have $\partial A(d) = 2|\{a \in A : a + d \notin A\}|$. We count these elements a according to whether $v - a$ belongs to B .

If $v - a \in B$, then $(a, v - a)$ is a representation of v in $A \times B$. There are at most $r_{A,B}(v) = e_v$ such elements a .

If $v - a \notin B$, then $a + d = u - (v - a) \notin A$, so $(a + d, v - a)$ is a representation of u in $A^c \times B^c$. Distinct elements a give distinct representations. By inclusion-exclusion, we have

$$r_{A^c, B^c}(u) = p - |A| - |B| + r_{A,B}(u) = e_u + h.$$

Hence there are at most $e_u + h$ elements a in this case. The two cases together give at most $e_u + e_v + h$ elements, proving the lemma. $\square$

Summing Lemma 2.3 over $u, v \in S$ with $u \neq v$ and applying (3) gives an estimate for $\sum_{d \in \mathbb{F}_p \setminus \{0\}} \rho(d) \partial A(d)$. In Appendix A, we combine this with a moment estimate for $\rho(d)$ to obtain the

upper bound $|S| = O_\Delta(p^{\Delta/(2\Delta+1)})$, which is weaker for $\Delta > 1$. However, for differences in $S - S$ with many representations, we obtain a stronger bound by counting copies of $K_{1,2}$ in G_S . Put $h := p - |A| - |B|$. Since $E(G_S) \subseteq R$, every vertex of G_S has degree at most Δ . For $d \in \mathbb{F}_p \setminus \{0\}$, define

$$\sigma_B(d) := |\{(b, a_0, a_1) : b \in B, a_0, a_1 \in A, a_0 + b, a_1 + b \in S, a_1 - a_0 = d\}|.$$

Thus $\sigma_B(d)$ counts copies of $K_{1,2}$ centered in B , with ordered leaves (a_0, a_1) satisfying $a_1 - a_0 = d$. Define $\sigma_A(d)$ by the same formula with A and B interchanged. To prove the first inequality in the following lemma, we distinguish three cases according to whether a translate of $\{0, d\}$ meets A in zero, one, or two points. Compare the translation counts in Ouyang [18, Section 4].

Lemma 2.4. *Suppose that G_S has maximum degree at most Δ . For every $d \in \mathbb{F}_p \setminus \{0\}$, we have*

$$\sigma_B(d) \geq -h\rho(d) + \left(\frac{\rho(d)}{2} - \Delta\right) \partial A(d). \quad (4)$$

Moreover,

$$\sum_{d \in \mathbb{F}_p \setminus \{0\}} \sigma_B(d) \leq (\Delta - 1)|E(G_S)| \leq \Delta(\Delta - 1) \min\{|A|, |B|\}. \quad (5)$$

The same bounds hold with A and B interchanged.

Proof. Put $n := \min\{|A|, |B|\}$. We first prove (4). Put $X := S \cap (S - d)$ and $Y := \{0, d\}$. Then $|X| = \rho(d)$ and $X + Y \subseteq S$. For $z \in \mathbb{F}_p$, define $\alpha(z) := |(X + z) \cap B|$ and $\beta(z) := |(Y - z) \cap A|$. Thus $\beta(z)$ counts how many of the two points $-z$ and $d - z$ lie in A . If $\beta(z) = 2$, each of the $\alpha(z)$ possible centers b gives a triple $(b, -z, d - z)$ counted by $\sigma_B(d)$. If $\beta(z) = 1$, each possible center is adjacent in G_S to the unique A -vertex in $Y - z$, and hence $\alpha(z) \leq \Delta$. If $\beta(z) = 0$, no degree estimate is available and we use the trivial bound $\alpha(z) \leq \rho(d)$. Consequently,

$$\sum_{\substack{z \in \mathbb{F}_p \\ \beta(z)=2}} \alpha(z) = \sigma_B(d) \quad \text{and} \quad \sum_{z \in \mathbb{F}_p} \alpha(z) = \rho(d)|B|.$$

Writing $x = d - z$, we have $-z = x - d$. Thus the bijection $z \mapsto x$, together with $|A| = |A + d|$, gives

$$\begin{aligned} |\{z \in \mathbb{F}_p : \beta(z) = 2\}| &= |A \cap (A + d)| = |A| - \frac{1}{2}\partial A(d), \\ |\{z \in \mathbb{F}_p : \beta(z) = 1\}| &= |A \Delta (A + d)| = \partial A(d), \\ |\{z \in \mathbb{F}_p : \beta(z) = 0\}| &= p - |A \cup (A + d)| = |A^c| - \frac{1}{2}\partial A(d). \end{aligned}$$

Splitting the sum over $z \in \mathbb{F}_p$ into these three classes and using the upper bounds on $\alpha(z)$ established above, we obtain

$$\begin{aligned} \sigma_B(d) &= \sum_{\substack{z \in \mathbb{F}_p \\ \beta(z)=2}} \alpha(z) \\ &= \sum_{z \in \mathbb{F}_p} \alpha(z) - \sum_{\substack{z \in \mathbb{F}_p \\ \beta(z)=1}} \alpha(z) - \sum_{\substack{z \in \mathbb{F}_p \\ \beta(z)=0}} \alpha(z) \\ &\geq \rho(d)|B| - \Delta|\{z \in \mathbb{F}_p : \beta(z) = 1\}| - \rho(d)|\{z \in \mathbb{F}_p : \beta(z) = 0\}| \\ &= \rho(d)|B| - \Delta\partial A(d) - \rho(d)\left(|A^c| - \frac{1}{2}\partial A(d)\right) \\ &= \rho(d)(|B| - |A^c|) + \left(\frac{\rho(d)}{2} - \Delta\right) \partial A(d) \\ &= -h\rho(d) + \left(\frac{\rho(d)}{2} - \Delta\right) \partial A(d), \end{aligned}$$

where we used $|B| - |A^c| = -h$ in the last step. This proves (4).

Let $\deg_{G_S}(b)$ be the degree of $b \in B$ in G_S . Every ordered pair of distinct edges incident to b determines one nonzero difference, so

$$\sum_{d \in \mathbb{F}_p \setminus \{0\}} \sigma_B(d) = \sum_{b \in B} \deg_{G_S}(b)(\deg_{G_S}(b) - 1) \leq (\Delta - 1)|E(G_S)|.$$

Since $|E(G_S)| \leq \Delta n$, this is at most $\Delta(\Delta - 1)n$.

Both bounds for σ_A follow by interchanging A and B . □

At the critical line $|A| + |B| = p$, Lemma 2.4 shows that every nonzero d with $\rho(d) \geq 4\Delta$ satisfies $\rho(d)\partial A(d) \leq 4\sigma_B(d)$. Summing over these differences and applying (5), we obtain

$$\sum_{\substack{d \in \mathbb{F}_p \setminus \{0\} \\ \rho(d) \geq 4\Delta}} \rho(d)\partial A(d) \leq 4\Delta(\Delta - 1) \min\{|A|, |B|\}.$$

We finish with two elementary observations. The first is a weighted form of Markov's inequality. The second uses the Cauchy–Davenport theorem and subadditivity to bound $\partial A(x)$ for every $x \in \mathbb{F}_p$; related arguments combining sumset growth with subadditivity appear in [8, 10, 13, 16].

Lemma 2.5 (Markov's inequality). *Let I be finite and let $w_i, x_i \geq 0$. Suppose $M := \sum_{i \in I} w_i > 0$. If*

$\sum_{i \in I} w_i x_i \leq K$, then there is $D \subseteq I$ such that

$$\sum_{i \in D} w_i \geq \frac{M}{2} \quad \text{and} \quad x_i \leq \frac{2K}{M} \quad \text{for all } i \in D.$$

Proof. Take $D := \{i : x_i \leq 2K/M\}$. The complement of D has total weight at most $M/2$. $\square$

Lemma 2.6. *Let $\emptyset \neq D \subseteq \mathbb{F}_p \setminus \{0\}$. If $\partial A(d) \leq L$ for every $d \in D$, then for every $x \in \mathbb{F}_p$, we have*

$$\partial A(x) \leq \left\lceil \frac{p-1}{|D|} \right\rceil L \ll \frac{pL}{|D|}.$$

Proof. Put $D_0 := D \cup \{0\}$ and $m := \lceil (p-1)/|D| \rceil$. Since $\partial A(0) = 0$, we have $\partial A(d) \leq L$ for every $d \in D_0$. Repeated application of the Cauchy–Davenport theorem [5, 6] gives

$$\left| \underbrace{D_0 + \cdots + D_0}_{m \text{ times}} \right| \geq \min\{p, m|D| + 1\} = p.$$

Write $x = d_1 + \cdots + d_m$ with $d_i \in D_0$. By Lemma 2.2, $\partial A(x) \leq \sum_{i=1}^m \partial A(d_i) \leq mL$. Since $m \leq (p-1)/|D| + 1 \leq 2p/|D|$, the stated bound follows. $\square$

2.2 The main estimate

The following proposition gives an upper bound on $|S|$ in terms of $h = p - |A| - |B|$ and the size of the smaller summand.

Proposition 2.7. *Let p be prime and let $\Delta \geq 1$ be an integer. Let $A, B \subseteq \mathbb{F}_p$ be nonempty with $|A| + |B| \leq p$, and let $R \subseteq A \times B$ satisfy $\Delta(R) \leq \Delta$. Put $h := p - |A| - |B|$ and $S := \mathbb{F}_p \setminus (A +_R B)$. Then we have*

$$|S| \ll_{\Delta} p^{1/3} + \frac{ph}{\min\{|A|, |B|\}}.$$

Proof. Put $n := \min\{|A|, |B|\}$ and $s := |S|$. After interchanging A and B if necessary, assume that $|A| \leq |B|$. Since $h \geq 0$, we have $n \leq (|A| + |B|)/2 = (p - h)/2 \leq p/2$. By Lemma 2.2,

$$\frac{1}{p} \sum_{x \in \mathbb{F}_p} \partial A(x) = 2n \left(1 - \frac{n}{p}\right) \geq 2n \left(1 - \frac{1}{2}\right) = n.$$

If $\partial A(d) \leq L$ on a nonempty set $D \subseteq \mathbb{F}_p \setminus \{0\}$, then Lemma 2.6 and the preceding average bound give

$$n \leq \frac{1}{p} \sum_{x \in \mathbb{F}_p} \partial A(x) \leq \max_{x \in \mathbb{F}_p} \partial A(x) \ll \frac{pL}{|D|}.$$

Summing Lemma 2.3 over ordered non-diagonal pairs in $S \times S$ and using (3) and $h \geq 0$, we obtain

$$\begin{aligned}
\sum_{d \in \mathbb{F}_p \setminus \{0\}} \rho(d) \partial A(d) &= \sum_{\substack{u, v \in S \\ u \neq v}} \partial A(u - v) \\
&\leq 2 \sum_{\substack{u, v \in S \\ u \neq v}} (e_u + e_v + h) \\
&= 4(s-1) \sum_{u \in S} e_u + 2hs(s-1) \\
&\leq 4\Delta ns + 2hs^2.
\end{aligned} \tag{6}$$

Lemma 2.4 shows that whenever $\rho(d) \geq 4\Delta$,

$$\frac{1}{4} \rho(d) \partial A(d) \leq \sigma_B(d) + h\rho(d).$$

Summing over these differences and using $h \geq 0$ and (5), we obtain

$$\begin{aligned}
\sum_{\substack{d \in \mathbb{F}_p \setminus \{0\} \\ \rho(d) \geq 4\Delta}} \rho(d) \partial A(d) &\leq 4 \sum_{d \in \mathbb{F}_p \setminus \{0\}} \sigma_B(d) + 4h \sum_{d \in \mathbb{F}_p \setminus \{0\}} \rho(d) \\
&\leq 4\Delta(\Delta-1)n + 4hs(s-1) \\
&\ll_{\Delta} n + hs^2.
\end{aligned} \tag{7}$$

Here $\sum_{d \in \mathbb{F}_p \setminus \{0\}} \rho(d) = s(s-1)$, since the sum counts ordered pairs of distinct elements of S according to their difference.

If $s = O_{\Delta}(1)$, then $s \ll_{\Delta} 1 \leq p^{1/3} + \frac{ph}{n}$. Otherwise, we may assume that s is sufficiently large in terms of Δ . In particular, $s(s-1) \asymp s^2$. Split the nonzero differences into the *light* and *heavy* classes

$$\mathcal{D}_{\text{light}} := \{d \in \mathbb{F}_p \setminus \{0\} : \rho(d) < 4\Delta\} \quad \text{and} \quad \mathcal{D}_{\text{heavy}} := \{d \in \mathbb{F}_p \setminus \{0\} : \rho(d) \geq 4\Delta\}.$$

For a fixed number of ordered pairs, small multiplicity gives more distinct differences, and hence a stronger lower bound for $|D|$ after applying Lemma 2.5. On the other hand, (7) gives a stronger estimate for the sum over $\mathcal{D}_{\text{heavy}}$. We therefore compare the sums of $\rho(d)$ over the two sets. We consider ordered pairs $(u, v) \in S^2$ with $u \neq v$. Since these sets partition $\mathbb{F}_p \setminus \{0\}$ and $\sum_{d \in \mathbb{F}_p \setminus \{0\}} \rho(d) = s(s-1)$, at least one of the following two cases occurs.

Case 1: At least half of the pairs have light differences.

Suppose that

$$\sum_{d \in \mathcal{D}_{\text{light}}} \rho(d) \geq \frac{1}{2} s(s-1).$$

Apply Lemma 2.5 with $I = \mathcal{D}_{\text{light}}$, $w_d = \rho(d)$, and $x_d = \partial A(d)$. Here $M = \sum_{d \in \mathcal{D}_{\text{light}}} \rho(d) \gg s^2$. By

(6), we may take $K = 4\Delta ns + 2hs^2$. Thus $2K/M \ll_{\Delta} n/s + h$, and the lemma gives a set $D \subseteq \mathcal{D}_{\text{light}}$ such that

$$\sum_{d \in D} \rho(d) \gg_{\Delta} s^2 \quad \text{and} \quad \partial A(d) \ll_{\Delta} \frac{n}{s} + h \quad \text{for all } d \in D.$$

Since $s^2 \ll_{\Delta} \sum_{d \in D} \rho(d) \leq 4\Delta |D|$, we have $|D| \gg_{\Delta} s^2 > 0$. Apply Lemma 2.6 with $L = C_{\Delta}(n/s + h)$ for a sufficiently large constant C_{Δ} . Since $n \leq p/2$, (2) gives

$$n \leq \frac{1}{p} \sum_{x \in \mathbb{F}_p} \partial A(x) \leq \max_{x \in \mathbb{F}_p} \partial A(x) \ll_{\Delta} \frac{p}{|D|} \left(\frac{n}{s} + h \right) \ll_{\Delta} \frac{pn}{s^3} + \frac{ph}{s^2}.$$

At least one of the last two terms is $\gg_\Delta n$. Thus either $s^3 \ll_\Delta p$ or $s^2 \ll_\Delta ph/n$, and hence $s \ll_\Delta p^{1/3} + (ph/n)^{1/2}$.

Case 2: At least half of the pairs have heavy differences.

Suppose that

$$\sum_{d \in \mathcal{D}_{\text{heavy}}} \rho(d) \geq \frac{1}{2}s(s-1).$$

Apply Lemma 2.5 with $I = \mathcal{D}_{\text{heavy}}$, $w_d = \rho(d)$, and $x_d = \partial A(d)$. Now $M = \sum_{d \in \mathcal{D}_{\text{heavy}}} \rho(d) \gg s^2$.

By (7), we may take K with $K \ll_\Delta n + hs^2$. Hence $2K/M \ll_\Delta n/s^2 + h$, and the lemma gives $D \subseteq \mathcal{D}_{\text{heavy}}$ such that

$$\sum_{d \in D} \rho(d) \gg_\Delta s^2 \quad \text{and} \quad \partial A(d) \ll_\Delta \frac{n}{s^2} + h \quad \text{for all } d \in D.$$

Since $s^2 \ll_\Delta \sum_{d \in D} \rho(d) \leq s|D|$, we have $|D| \gg_\Delta s > 0$. Arguing as in Case 1, we apply Lemma 2.6 and (2) to obtain

$$n \ll_\Delta \frac{p}{|D|} \left(\frac{n}{s^2} + h \right) \ll_\Delta \frac{pn}{s^3} + \frac{ph}{s},$$

which yields $s \ll_\Delta p^{1/3} + ph/n$.

When $h = 0$, both cases give $s \ll_\Delta p^{1/3}$. When $h \geq 1$, we have $ph/n \geq 1$ and hence $(ph/n)^{1/2} \leq ph/n$. Thus both cases yield $s \ll_\Delta p^{1/3} + ph/n$, proving the proposition. $\square$

2.3 The critical and supercritical cases

Proof of Theorem 1.1(i). First assume that $|A| + |B| = p$. Taking $h = 0$ in Proposition 2.7 gives $|S| \ll_\Delta p^{1/3}$.

To pass to the supercritical range, choose nonempty subsets $A_0 \subseteq A$ and $B_0 \subseteq B$ with $|A_0| + |B_0| = p$, and put $R_0 := R \cap (A_0 \times B_0)$. Then $A_0 +_{R_0} B_0 \subseteq A +_R B$, so the avoiding set for (A, B, R) is contained in the avoiding set for (A_0, B_0, R_0) . Applying the critical case to (A_0, B_0, R_0) completes the proof. $\square$

Remark 2.8. For $|A| + |B| \geq p$, an alternative argument excludes certain complete bipartite subgraphs of Γ_S and yields a moment estimate for $\rho(d)$ that replaces the $K_{1,2}$ count above. Combining it with the translation boundary estimates and Lemma 2.6 gives $|S| \ll_\Delta p^{\Delta/(2\Delta+1)}$. This agrees with the cubic-root bound when $\Delta = 1$, but is weaker for $\Delta > 1$. We give the proof in Appendix A. When $|A| + |B| = p - h$ with $h \geq 0$, the same approach gives $|S| \ll_\Delta h + 1 + p^{\Delta/(2\Delta+1)}(h+1)^{1/(2\Delta+1)}$; we omit the details of this extension.

2.4 The subcritical case

Assume that $|A| + |B| = p - h$ with $h \geq 0$, and put $n := \min\{|A|, |B|\}$. The term ph/n in Proposition 2.7 can be large when n is small. We use the following form of Pollard's theorem [20] to obtain a bound that is effective when n is small. Recall that $e_u = r_{A,B}(u) = |\{(a, b) \in A \times B : a + b = u\}|$.

Theorem 2.9 (Pollard). *Let A and B be two nonempty subsets of $\mathbb{F}_p$. For every integer $1 \leq k \leq \min\{|A|, |B|\}$, we have*

$$\sum_{u \in \mathbb{F}_p} \min\{r_{A,B}(u), k\} \geq k \cdot \min\{p, |A| + |B| - k\}.$$

Combining Theorem 2.9 with the degree bound gives the following estimate.

Lemma 2.10. *For every integer $1 \leq k \leq n$, we have $|S| \leq h + k + \frac{\Delta n}{k}$. In particular, we have $|S| \leq h + C_\Delta n^{1/2}$.*

Proof. For every integer k with $1 \leq k \leq n$, Theorem 2.9 gives

$$\sum_{u \in \mathbb{F}_p} \min(e_u, k) \geq k(|A| + |B| - k) = k(p - h - k).$$

Equivalently,

$$\sum_{u \in \mathbb{F}_p} (k - \min(e_u, k)) \leq k(h + k).$$

Restricting the left-hand side to S , and using $\sum_{u \in S} \min(e_u, k) \leq \sum_{u \in S} e_u \leq \Delta n$, yields $k|S| - \Delta n \leq k(h + k)$, which proves the first assertion. Taking $k = \lceil n^{1/2} \rceil$, which lies in $[1, n]$, gives

$$|S| \leq h + (\Delta + 1)n^{1/2} + 1 \leq h + (\Delta + 2)n^{1/2}.$$

This proves the second assertion. $\square$

We now complete the proof of Theorem 1.1(ii).

Proof of Theorem 1.1(ii). Put $n := \min\{|A|, |B|\}$. Combining Proposition 2.7 with Lemma 2.10, we obtain

$$|S| \leq h + C_\Delta \min \left\{ n^{1/2}, p^{1/3} + \frac{ph}{n} \right\}.$$

But

$$\min \left\{ n^{1/2}, p^{1/3} + \frac{ph}{n} \right\} \leq p^{1/3} + \min \left\{ n^{1/2}, \frac{ph}{n} \right\} \leq p^{1/3} + (ph)^{1/3},$$

where the last inequality follows by considering $n \leq (ph)^{2/3}$ and $n \geq (ph)^{2/3}$ separately. We obtain $|S| \ll_\Delta h + 1 + p^{1/3}(h + 1)^{1/3}$, proving part (ii). $\square$

3 Periodic ternary construction and logarithmic lower bounds

In this section, we prove Theorem 1.2 and deduce Corollary 1.3. Adapting the periodic construction of Ouyang [18, Section 4], we first work in $\mathbb{Z}_{3^m}$, then repeat the construction periodically in $\mathbb{Z}$. We then delete a short terminal interval before passing to $\mathbb{F}_p$.

3.1 The ternary construction

Fix $m \geq 1$, put $N_m := 3^m$ and $C_m := \{0, 1, 3, \dots, 3^{m-1}\}$, and for $\Delta \geq 1$ set $D_{m,\Delta} := \bigcup_{j=0}^{\Delta-1} (jN_m + C_m)$.

Then $|D_{m,\Delta}| = \Delta(m + 1)$. Let $L_{m,\Delta} := \max D_{m,\Delta} = \left(\Delta - \frac{2}{3}\right)N_m$.

We write each residue $x \in \mathbb{Z}_{N_m}$ in base 3 as

$$x = x_0 + x_1 3 + \dots + x_{m-1} 3^{m-1},$$

where $x_i \in \{0, 1, 2\}$. For $x \in \mathbb{Z}_{N_m} \setminus \{0\}$, let $v(x)$ be the least index for which $x_{v(x)} \neq 0$. Define X_0 and Y_0 by

$$\begin{aligned} X_0 &:= \{0\} \cup \{x \in \mathbb{Z}_{N_m} \setminus \{0\} : x_{v(x)} = 1\}, \\ Y_0 &:= \{0\} \cup \{x \in \mathbb{Z}_{N_m} \setminus \{0\} : x_{v(x)} = 2\}. \end{aligned}$$

Then

$$X_0 \cup Y_0 = \mathbb{Z}_{N_m}, \quad X_0 \cap Y_0 = \{0\}, \quad \text{and} \quad |X_0| + |Y_0| = N_m + 1. \quad (8)$$

The two sets satisfy the following matching property.

Lemma 3.1. *In the bipartite graph with left side X_0 , right side Y_0 , and edge condition $y - x \in C_m \pmod{N_m}$, every vertex has degree exactly one.*

Proof. For $x \in X_0 \setminus \{0\}$, put $v = v(x)$. Among $c \in C_m$, we have $x + c \in Y_0$ exactly when $c = 3^v$. For $x = 0$, only $c = 0$ works. The resulting map $\phi(0) = 0$ and $\phi(x) = x + 3^{v(x)}$ is a bijection from X_0 to Y_0 , with inverse $y \mapsto y - 3^{v(y)}$ for $y \neq 0$. Hence the edges form a perfect matching. $\square$

We now pass from $\mathbb{Z}_{N_m}$ to $\mathbb{F}_p$ by periodic repetition and truncation.

Proof of Theorem 1.2. We use the standard representatives $0, 1, \dots, p-1$ for the elements of $\mathbb{F}_p$ and define $\hat{X}$ and $\hat{Y}$ by

$$\begin{aligned}\hat{X} &:= \{x \in [0, p-1] : x \bmod N_m \in X_0\}, \\ \hat{Y} &:= \{y \in [0, p-1] : y \bmod N_m \in Y_0\}.\end{aligned}$$

Consider the bipartite graph on $\hat{X} \sqcup \hat{Y}$ with edge condition $y - x = jN_m + c$ in $\mathbb{Z}$, for some integer j with $0 \leq j < \Delta$ and some $c \in C_m$. This graph has maximum degree at most Δ . Indeed, modulo N_m there is at most one choice of c by Lemma 3.1, and each value of j gives at most one endpoint.

A congruence $y - x \equiv d \pmod{p}$ with $d \in D_{m,\Delta}$ can also hold when the integer difference is $y - x = d - p$. This forces $x \geq p - d \geq p - L_{m,\Delta}$. We therefore put $X' := \hat{X} \cap [0, p - L_{m,\Delta} - 1]$. The bipartite graph on $X' \sqcup \hat{Y}$ defined by $y - x \equiv d \pmod{p}$ for some $d \in D_{m,\Delta}$ is therefore a subgraph of the graph above and has maximum degree at most Δ .

Write $p = QN_m + r$, where $Q = \lfloor p/N_m \rfloor$ and $1 \leq r < N_m$. Each integer in $[0, p-1]$ is counted once in $\hat{X} \sqcup \hat{Y}$, except for a multiple of N_m , which is counted twice by (8). There are $Q + 1$ such multiples. Consequently, $|\hat{X}| + |\hat{Y}| = p + Q + 1$. After deleting the elements of $\hat{X}$ in $[p - L_{m,\Delta}, p-1]$, we obtain

$$|X'| + |\hat{Y}| \geq p + \left\lfloor \frac{p}{N_m} \right\rfloor + 1 - L_{m,\Delta}.$$

The condition of Theorem 1.2 therefore allows us to choose subsets $X \subseteq X'$ and $Y \subseteq \hat{Y}$ such that $|X| + |Y| = p + K$.

We now identify X, Y , and $D_{m,\Delta}$ with the corresponding sets of residue classes modulo p . Set $A := -X$ and $B := Y$, and forbid precisely the pairs $(-x, y)$ for which $y - x \in D_{m,\Delta}$. The preceding degree calculation gives $\Delta(R) \leq \Delta$. Every representation of an element of $D_{m,\Delta}$ is forbidden. Conversely, Cauchy–Davenport gives $A + B = \mathbb{F}_p$, while every edge of R has sum in $D_{m,\Delta}$. Hence every residue outside $D_{m,\Delta}$ still has an allowed representation. Thus $\mathbb{F}_p \setminus (A +_R B) = D_{m,\Delta}$, and $|D_{m,\Delta}| = \Delta(m+1)$ gives the required size. $\square$

3.2 Logarithmic lower bounds on $|S|$

Proof of Corollary 1.3. The first assertion is trivial when $p/K < 9\Delta$, since $\log(p/K) = O_\Delta(1)$ and we may enlarge the constant in the $O_\Delta(1)$ term.

Otherwise, put

$$m := \left\lfloor \frac{1}{2} \log_3 \frac{p}{\Delta K} \right\rfloor \geq 1, \quad N_m = 3^m.$$

Then $p \geq 9\Delta K > 3$ and $p \geq \Delta K N_m^2$, so

$$\left\lfloor \frac{p}{N_m} \right\rfloor + 1 - \left(\Delta - \frac{2}{3} \right) N_m \geq \Delta(K-1)N_m + \frac{2}{3}N_m + 1 \geq K.$$

Hence Theorem 1.2 gives the required sets and relation with

$$|S| = \Delta(m+1) \geq \frac{\Delta}{2 \log 3} \log \frac{p}{\Delta K} = \frac{\Delta}{2 \log 3} \log \frac{p}{K} - O_\Delta(1).$$

For the second assertion, apply the first assertion with $K = 1$ and remove one vertex from a side containing at least two vertices, restricting R accordingly. Both sides remain nonempty and

their sizes sum to p . Neither the maximum degree nor the restricted sumset increases, so the same lower bound holds. $\square$

For comparison, Huicochea's construction [12, Theorem 1.4] and the construction in Appendix B both begin with sets of points in a high-dimensional integer grid, which are then embedded into $\mathbb{F}_p$ through a suitable encoding $\Phi : \mathbb{Z}^d \rightarrow \mathbb{F}_p$. To illustrate the idea, consider the construction in Appendix B where $|A| + |B| = p$ and R is a matching. We first fix integers $d \geq 2$ and $N \geq 1$ and define the discrete simplex $\Lambda = \{\mathbf{x} \in \mathbb{Z}_{\geq 0}^d : x_1 + \dots + x_d \leq N\}$. We then remove a set D of integer points so that certain pairs between Λ and the remaining points form a matching. When the pairs in this matching are excluded from addition, none of the d standard basis vectors $\mathbf{e}_1, \dots, \mathbf{e}_d \in \mathbb{Z}^d$ can be obtained. We then set $A = \Phi(\Lambda)$ and choose a suitable subset $B \subseteq \mathbb{F}_p \setminus \Phi(D)$. To choose B with $|A| + |B| = p$, it suffices to have $|D| \leq |\Lambda|$. Taking $N = d^3$ gives $|D| < |\Lambda|$. With this choice, the encoding with base $2N + 1$ is injective on $[-N, N]^d$ provided that $(2d^3 + 1)^d < p$. This allows $d \asymp \log p / \log \log p$. The detailed parameter calculations are given in Appendix B.

In these constructions, the coordinate directions give rise to the elements of the avoiding set, whose size grows linearly with the dimension. The two summands have substantially different sizes. Taking the largest admissible dimension in the stated parameter conditions gives $|A| = p^{3/4+o(1)}$ in Huicochea's construction when $|A| + |B| = p - h$ with fixed $h \geq 0$ [12, proof of Theorem 1.4]. At the critical line, the construction in Appendix B gives $|A| = p^{2/3+o(1)}$. In both cases, $|B| = p - |A| + O(1) \approx p$. By comparison, the construction in this section is simpler: it combines a ternary building block with periodic repetition. For fixed K and Δ , both summands can be chosen to have size $(1/2 + o(1))p$, and the dependence of the size of the avoiding set on p can be seen more directly.

4 Concluding remarks

For a fixed positive integer Δ , let

$$\mathcal{M}_\Delta(p) := \max \left\{ |\mathbb{F}_p \setminus (A +_R B)| : \begin{array}{l} A, B \subseteq \mathbb{F}_p \text{ nonempty, } R \subseteq A \times B, \\ |A| + |B| \geq p, \Delta(R) \leq \Delta \end{array} \right\}.$$

The results of this paper give

$$\log p \ll_\Delta \mathcal{M}_\Delta(p) \ll_\Delta p^{1/3}.$$

Question 4.1. What is the correct order of $\mathcal{M}_\Delta(p)$?

We next consider the subcritical case $|A| + |B| = p - h$, allowing h to vary with p . For every fixed $\varepsilon > 0$ and fixed Δ , Ouyang [18, Theorem 1.7] proved that, for all sufficiently large primes p ,

$$|A +_R B| \geq |A| + |B| - 1 - 2\Delta \quad \text{if} \quad |A| + |B| \leq (1 - \varepsilon)p.$$

Thus a bounded-degree restriction causes only bounded additional loss when $p - |A| - |B| \geq \varepsilon p$, whereas our examples give an additional loss of $\Omega(\log p)$ for fixed h .

To study this transition, for $0 \leq h \leq p - 2$ define the maximum loss relative to the Cauchy–Davenport bound by

$$\mathcal{L}_\Delta(p, h) := \max \left\{ (|A| + |B| - 1) - |A +_R B| : \begin{array}{l} A, B \subseteq \mathbb{F}_p \text{ nonempty, } R \subseteq A \times B, \\ |A| + |B| = p - h, \Delta(R) \leq \Delta \end{array} \right\}.$$

Equivalently, since $|A| + |B| = p - h$, this is the maximum of $|S| - h - 1$ over the same class of triples (A, B, R) . Ouyang's theorem gives $\mathcal{L}_\Delta(p, h) \leq 2\Delta$ whenever $h \geq \varepsilon p$ and p is sufficiently large in terms of ε and Δ . On the other hand, deleting h vertices from the critical construction in Corollary 1.3, while keeping both sides nonempty, gives

$$\mathcal{L}_\Delta(p, h) \geq \frac{\Delta}{2 \log 3} \log p - O_{\Delta, h}(1)$$

for every fixed h and Δ . Theorem 1.1(ii) gives the upper bound

$$\mathcal{L}_\Delta(p, h) \ll_\Delta h + 1 + p^{1/3}(h + 1)^{1/3}.$$

Question 4.2. How does $\mathcal{L}_\Delta(p, h)$ behave as h grows from a fixed value to a positive proportion of p ? In particular, how large must h be for this loss to be bounded independently of p ?

References

- [1] N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.* **8** (1999), no. 1–2, 7–29, <https://doi.org/10.1017/S0963548398003411>.
- [2] N. Alon, M. B. Nathanson and I. Z. Ruzsa, Adding distinct congruence classes modulo a prime, *Amer. Math. Monthly* **102** (1995), no. 3, 250–255, <https://doi.org/10.1080/00029890.1995.11990565>.
- [3] N. Alon, M. B. Nathanson and I. Z. Ruzsa, The polynomial method and restricted sums of congruence classes, *J. Number Theory* **56** (1996), no. 2, 404–417, <https://doi.org/10.1006/jnth.1996.0029>.
- [4] B. Bollobás, I. Leader and M. Tiba, Large sumsets from small subsets, *Israel J. Math.* **268** (2025), no. 1, 253–314, <https://doi.org/10.1007/s11856-025-2736-z>.
- [5] A.-L. Cauchy, Recherches sur les nombres, *J. École Polytech.* **9** (1813), cahier 16, 99–123.
- [6] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* (1) **10** (1935), no. 1, 30–32, <https://doi.org/10.1112/jlms/s1-10.37.30>.
- [7] J. A. Dias da Silva and Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994), no. 2, 140–146, <https://doi.org/10.1112/blms/26.2.140>.
- [8] P. Erdős and H. Heilbronn, On the addition of residue classes mod p , *Acta Arith.* **9** (1964), no. 2, 149–159, <https://doi.org/10.4064/aa-9-2-149-159>.
- [9] B. Green and I. Z. Ruzsa, Sets with small sumset and rectification, *Bull. London Math. Soc.* **38** (2006), no. 1, 43–52, <https://doi.org/10.1112/S0024609305018102>.
- [10] Y. O. Hamidoune, A. S. Lladó and O. Serra, On complete subsets of the cyclic group, *J. Combin. Theory Ser. A* **115** (2008), no. 7, 1279–1285, <https://doi.org/10.1016/j.jcta.2007.12.007>.
- [11] M. Huicochea, On the number of popular differences in $\mathbb{Z}/p\mathbb{Z}$, *J. Number Theory* **214** (2020), 202–239, <https://doi.org/10.1016/j.jnt.2020.04.011>.
- [12] M. Huicochea, Combinatorial generalizations of Erdős–Heilbronn conjecture I, unpublished manuscript (2026), 31 pp.
- [13] S. V. Konyagin and V. F. Lev, On the number of popular differences, *Israel J. Math.* **176** (2010), no. 1, 269–283, <https://doi.org/10.1007/s11856-010-0029-6>.
- [14] T. Kővári, V. T. Sós and P. Turán, On a problem of K. Zarankiewicz, *Colloq. Math.* **3** (1954), no. 1, 50–57, <https://doi.org/10.4064/cm-3-1-50-57>.
- [15] V. F. Lev, Restricted set addition in groups, II. A generalization of the Erdős–Heilbronn conjecture, *Electron. J. Combin.* **7** (2000), no. 1, Paper No. R4, 10 pp., <https://doi.org/10.37236/1482>.
- [16] V. F. Lev, Translation invariance in groups of prime order, *J. Number Theory* **131** (2011), no. 10, 1827–1832, <https://doi.org/10.1016/j.jnt.2011.03.002>.
- [17] J. E. Olson, An addition theorem modulo p , *J. Combin. Theory* **5** (1968), no. 1, 45–52, [https://doi.org/10.1016/S0021-9800\(68\)80027-4](https://doi.org/10.1016/S0021-9800(68)80027-4).
- [18] M. Ouyang, On restricted sumsets with bounded degree relations, *Mathematika* **71** (2025), no. 4, Paper No. e70045, <https://doi.org/10.1112/mtk.70045>.
- [19] H. Pan and Z.-W. Sun, A lower bound for $|\{a + b : a \in A, b \in B, \text{ and } P(a, b) \neq 0\}|$, *J. Combin. Theory Ser. A* **100** (2002), no. 2, 387–393, <https://doi.org/10.1006/jcta.2002.3294>.
- [20] J. M. Pollard, A generalisation of the theorem of Cauchy and Davenport, *J. London Math. Soc.* (2) **8** (1974), no. 3, 460–462, <https://doi.org/10.1112/jlms/s2-8.3.460>.

A An alternative approach to bounding $|S|$

In this appendix, we give an alternative bound when $|A| + |B| \geq p$. We combine the estimates for ∂A and the covering argument (Lemma 2.6) from Section 2 with a moment estimate for $\rho(d)$. This moment estimate follows by showing that Γ_S contains no $K_{r,q}$ for suitable r and q . This extends Lev's translation argument [15, Theorem 3], but gives a weaker exponent than Theorem 1.1(i) when $\Delta > 1$. The method also extends to the subcritical case, with the resulting bound stated in Remark 2.8.

Proposition A.1. *Let p be prime and let $\Delta \geq 1$ be an integer. Let $A, B \subseteq \mathbb{F}_p$ be nonempty sets with $|A| + |B| \geq p$, and let $R \subseteq A \times B$ have maximum degree at most Δ on both sides. Then*

$$|\mathbb{F}_p \setminus (A +_R B)| \ll_{\Delta} p^{\Delta/(2\Delta+1)}.$$

In what follows, let p, Δ, A, B, R satisfy the hypotheses of Proposition A.1, and put $S := \mathbb{F}_p \setminus (A +_R B)$ and $s := |S|$. We first show that the full bipartite graph Γ_S introduced in Section 2 contains no $K_{r,q}$ for suitable r, q .

Lemma A.2. *Let r, q be positive integers satisfying $\Delta/r + \Delta/q < 1$. Then Γ_S contains no $K_{r,q}$.¹ In particular, this holds for $q = \Delta + 1$ and $r = \Delta(\Delta + 1) + 1$.²*

Proof. Suppose instead that there are $X, Y \subseteq \mathbb{F}_p$ with $|X| = r$, $|Y| = q$, and $X + Y \subseteq S$. For $z \in \mathbb{F}_p$, define $\alpha(z) := |(X + z) \cap A|$ and $\beta(z) := |(Y - z) \cap B|$. Averaging over all translations gives

$$\frac{1}{p} \sum_{z \in \mathbb{F}_p} \left(\frac{\alpha(z)}{r} + \frac{\beta(z)}{q} \right) = \frac{|A| + |B|}{p} \geq 1.$$

If $\alpha(z) > 0$ and $\beta(z) > 0$, then every cross-pair between $(X + z) \cap A$ and $(Y - z) \cap B$ has its sum in $X + Y \subseteq S$. All these pairs therefore belong to R , and the degree bound gives $\alpha(z), \beta(z) \leq \Delta$. By the hypothesis, the summand in the preceding average is then strictly less than 1. If one of $\alpha(z), \beta(z)$ vanishes, that summand is at most 1 as well. If $|A| + |B| > p$, the average is greater than 1, a contradiction. Thus $|A| + |B| = p$, and equality must hold for every z . The strict inequality above therefore implies that $\alpha(z)\beta(z) = 0$ for all $z \in \mathbb{F}_p$. If $\beta(z) = 0$, equality forces $\alpha(z) = r$. If $\alpha(z) = 0$, it forces $\beta(z) = q$. Consequently, for every z , either $X + z \subseteq A$ or $(X + z) \cap A = \emptyset$.

Since $|X| = r > \Delta \geq 1$, choose distinct $x_1, x_2 \in X$ and put $\delta := x_2 - x_1 \neq 0$. Taking $z = w - x_1$ in the preceding dichotomy gives $\mathbb{1}_A(w) = \mathbb{1}_A(w + \delta)$ for every $w \in \mathbb{F}_p$. Since every nonzero element generates the additive group of $\mathbb{F}_p$, the set A is either empty or all of $\mathbb{F}_p$, contradicting the nonemptiness of A and B and the equality $|A| + |B| = p$.

Finally, for $q = \Delta + 1$ and $r = \Delta(\Delta + 1) + 1$,

$$\frac{\Delta}{q} + \frac{\Delta}{r} = \frac{\Delta}{\Delta + 1} + \frac{\Delta}{\Delta(\Delta + 1) + 1} < 1,$$

which proves the stated special case. $\square$

We next bound the $(\Delta + 1)$ -th moment of the difference multiplicities of S . The proof uses the counting idea behind the Kővári–Sós–Turán argument [14]. Here we count the translates of a fixed $(\Delta + 1)$ -element subset of S .

Lemma A.3. *Let $q := \Delta + 1$ and $\rho(d) := |S \cap (S - d)|$. Then we have*

$$\sum_{d \in \mathbb{F}_p} \rho(d)^q \ll_{\Delta} s^q.$$

¹Equivalently, S is a $C_{\min\{r,q\}}[\max\{r,q\}]$ -set in $\mathbb{F}_p$.

²The condition $\Delta/r + \Delta/q < 1$ requires $q \geq \Delta + 1$. For $q = \Delta + 1$, the smallest admissible value of r is $\Delta(\Delta + 1) + 1$.

Proof. Put $r := \Delta(\Delta + 1) + 1$ and fix a $(\Delta + 1)$ -element subset $Y \subseteq S$. There are at most $r - 1$ shifts d for which $Y + d \subseteq S$; otherwise, r such shifts would form a set X satisfying $X + Y \subseteq S$, contrary to Lemma A.2. Double-counting pairs (d, Y) with $d \in \mathbb{F}_p$, $Y \subseteq S$, $|Y| = q$, and $Y + d \subseteq S$ gives

$$\sum_{d \in \mathbb{F}_p} \binom{\rho(d)}{q} \leq (r - 1) \binom{s}{q}.$$

Since q and r depend only on Δ , and $t^q \ll_q \binom{t}{q} + t$ for every integer $t \geq 0$, we obtain

$$\sum_{d \in \mathbb{F}_p} \rho(d)^q \ll_{\Delta} s^q + \sum_{d \in \mathbb{F}_p} \rho(d) = s^q + s^2 \ll_{\Delta} s^q. \quad \square$$

Proof of Proposition A.1. As in the proof of Theorem 1.1(i), we may assume that $|A| + |B| = p$. Interchanging A and B if necessary, put $n := |A| \leq |B|$, and let $q := \Delta + 1$. We may assume that s is larger than a constant depending on Δ . For $u \in S$, let $e_u := r_{A,B}(u)$. The degree bound (3) and Lemma 2.3 with $h = 0$ give

$$\sum_{\substack{u, v \in S \\ u \neq v}} (e_u + e_v) \leq 2\Delta ns \quad \text{and} \quad \partial A(u - v) \leq 2(e_u + e_v).$$

Hence Lemma 2.5 gives a set $P \subseteq \{(u, v) \in S \times S : u \neq v\}$ such that

$$|P| \gg_{\Delta} s^2 \quad \text{and} \quad \partial A(u - v) \ll_{\Delta} \frac{n}{s} \quad \text{for all } (u, v) \in P. \quad (9)$$

Put $D := \{u - v : (u, v) \in P\}$. By Lemma A.3 and Hölder's inequality, we have

$$|P| \leq \sum_{d \in D} \rho(d) \leq |D|^{1-1/q} \left(\sum_{d \in D} \rho(d)^q \right)^{1/q} \ll_{\Delta} |D|^{1-1/q} s.$$

Together with (9), this yields $|D| \gg_{\Delta} s^{q/(q-1)}$.

Since $\emptyset \neq D \subseteq \mathbb{F}_p \setminus \{0\}$, we may apply Lemma 2.6. Every $d \in D$ satisfies the translation boundary estimate in (9), so for every $x \in \mathbb{F}_p$,

$$\partial A(x) \ll_{\Delta} \frac{p}{|D|} \frac{n}{s} \ll_{\Delta} \frac{pn}{s^{1+q/(q-1)}}.$$

Using $n \leq p/2$ in (2), we obtain

$$n \leq \frac{1}{p} \sum_{x \in \mathbb{F}_p} \partial A(x) \ll_{\Delta} \frac{pn}{s^{1+q/(q-1)}}.$$

Since $1 + q/(q - 1) = (2q - 1)/(q - 1)$, we obtain

$$s^{(2q-1)/(q-1)} \ll_{\Delta} p, \quad \text{or equivalently} \quad s \ll_{\Delta} p^{(q-1)/(2q-1)}.$$

Substituting $q = \Delta + 1$ proves $s \ll_{\Delta} p^{\Delta/(2\Delta+1)}$. $\square$

B An asymmetric construction from a high-dimensional discrete simplex

In this appendix, we give an asymmetric construction with a matching restriction at the critical line $|A| + |B| = p$. Using a high-dimensional discrete simplex, we obtain an avoiding set of size $\Omega(\log p / \log \log p)$, with $|A| = p^{2/3+o(1)}$ and $|B| = (1-o(1))p$. The method also extends to $|A| + |B| = p + K$ and $\Delta(R) \leq \Delta$, yielding avoiding sets of size $\Omega(\Delta \log(p/K) / \log \log(p/K))$ for every fixed integer $\Delta \geq 1$ and every positive integer-valued function $K = K(p) = o(p)$; see Proposition B.3.

Fix an integer $d \geq 2$ and put $N := d^3$ and $M := 2N + 1$. Define

$$\Lambda := \{\mathbf{x} = (x_1, \dots, x_d) \in \mathbb{Z}_{\geq 0}^d : x_1 + \dots + x_d \leq N\},$$

and put $q := |\Lambda| = \binom{N+d}{d}$.

Let $\mathbf{e}_1, \dots, \mathbf{e}_d$ be the standard basis vectors of $\mathbb{Z}^d$, where $\mathbf{e}_i = (0, \dots, 0, \overset{\substack{\uparrow \\ \text{\textit{i-th position}}}}{1}, 0, \dots, 0)$. Put $E := \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$. Consider the bipartite graph with left vertex class Λ and right vertex class $\mathbb{Z}^d$, joining $\mathbf{x}$ to $\mathbf{y}$ when $\mathbf{x} + \mathbf{y} \in E$. We seek to remove fewer than q right vertices so that the remaining graph is a matching. For each $\mathbf{x} \in \Lambda$ with a zero coordinate, we delete all its right neighbors except $\mathbf{e}_i - \mathbf{x}$, where $i = \min\{j : x_j = 0\}$. For $1 \leq i \leq d$, put $H_i := \{\mathbf{x} \in \Lambda : x_i = 0, x_j > 0 \text{ for } j < i\}$. These sets partition the points of Λ with a zero coordinate according to the first such coordinate. Define

$$D := \bigcup_{i=1}^d (\mathbf{e}_i - (\Lambda \setminus H_i)) = (E - \Lambda) \setminus \bigcup_{i=1}^d (\mathbf{e}_i - H_i).$$

We will later embed this configuration into $\mathbb{F}_p$ and choose B disjoint from the embedded copy of D .

Lemma B.1. *The bipartite graph with vertex classes Λ and $\mathbb{Z}^d \setminus D$, joining $\mathbf{x}$ to $\mathbf{y}$ when $\mathbf{x} + \mathbf{y} \in E$, has maximum degree at most one. Moreover, we have $|D| < q$.*

Proof. Suppose that $\mathbf{e}_i - \mathbf{x} = \mathbf{e}_j - \mathbf{y}$ with $\mathbf{x} \in H_i$ and $\mathbf{y} \in \Lambda$. If $i \neq j$, then the i -th coordinate of $\mathbf{y} = \mathbf{x} + \mathbf{e}_j - \mathbf{e}_i$ is -1 , a contradiction. Thus $i = j$ and $\mathbf{x} = \mathbf{y}$. This uniqueness shows that no point of $\bigcup_{i=1}^d (\mathbf{e}_i - H_i)$ belongs to D . Hence $D = \left(\bigcup_{i=1}^d (\mathbf{e}_i - \Lambda) \right) \setminus \left(\bigcup_{i=1}^d (\mathbf{e}_i - H_i) \right)$. Every edge remaining after the deletion of D has the form $(\mathbf{x}, \mathbf{e}_i - \mathbf{x})$ with $\mathbf{x} \in H_i$. The sets H_i are pairwise disjoint, and the uniqueness just proved ensures that each right vertex has degree at most one. Thus the remaining graph is a matching.

To prove $|D| < q$, note that every point of D with no positive coordinate has the form $-\mathbf{z}$, where $\mathbf{z} \in \mathbb{Z}_{\geq 0}^d$ and $\sum_j z_j \leq N - 1$. Any other point of D has the form $\mathbf{e}_i - \mathbf{x}$ with $x_i = 0$ and $x_j = 0$ for some $j < i$. Consequently,

$$|D| \leq \binom{N+d-1}{d} + \binom{d}{2} \binom{N+d-2}{d-2} = q - \left(1 - \frac{d(d-1)^2}{2(N+d-1)} \right) \binom{N+d-1}{d-1} < q,$$

where the last inequality³ follows from $N = d^3$. □

Proposition B.2. *If p is prime and $M^d < p$, there are nonempty sets $A, B \subseteq \mathbb{F}_p$ and a matching $R \subseteq A \times B$ such that*

$$|A| = q, \quad |B| = p - q, \quad \text{and} \quad |\mathbb{F}_p \setminus (A +_R B)| = d.$$

³The top layer $\{\mathbf{x} \in \Lambda : \sum_j x_j = N\}$ has more points than the part of D with a positive coordinate.

Proof. Define $\Phi : \mathbb{Z}^d \rightarrow \mathbb{F}_p$ by

$$\Phi(\mathbf{x}) := \sum_{i=1}^d M^{i-1} x_i \pmod{p}.$$

The map Φ is clearly additive, and the box $[-N, N]^d$ contains $\Lambda \cup (E - \Lambda)$. Since $M = 2N + 1$, uniqueness of base- M expansions shows that the integer encodings of points in this box are distinct and lie in an interval of length $M^d - 1 < p$. Hence Φ is injective on this box.

Set $A := \Phi(\Lambda)$. Then $|A| = |\Lambda| = q$. By Lemma B.1, $|D| < q \leq (N + 1)^d < M^d < p$, so we can choose $B \subseteq \mathbb{F}_p \setminus \Phi(D)$ with $|B| = p - q$. Both sets are nonempty and $|A| + |B| = p$.

Define

$$R := \{(a, b) \in A \times B : a + b \in \Phi(E)\}.$$

Let $(a, b) \in R$ and write $a = \Phi(\mathbf{x})$ with $\mathbf{x} \in \Lambda$. For some $1 \leq i \leq d$, we have $\Phi(\mathbf{x}) + b = \Phi(\mathbf{e}_i)$, so by additivity of Φ , $b = \Phi(\mathbf{e}_i - \mathbf{x}) \in \Phi([-N, N]^d)$. Since $b \in B$ and B is disjoint from $\Phi(D)$, we have $\mathbf{e}_i - \mathbf{x} \notin D$. Thus

$$R \subseteq \{(\Phi(\mathbf{x}), \Phi(\mathbf{y})) : \mathbf{x} \in \Lambda, \mathbf{y} \notin D, \mathbf{x} + \mathbf{y} \in E\}.$$

The set on the right is a matching by Lemma B.1 and the injectivity of Φ on $\Lambda \cup (E - \Lambda)$. Hence R is a matching.

To prove $|\mathbb{F}_p \setminus (A +_R B)| = d$, we show that $A +_R B = \mathbb{F}_p \setminus \Phi(E)$. By definition, $A +_R B = (A + B) \setminus \Phi(E)$. For any $t \in \mathbb{F}_p \setminus (A + B)$, we have $t - A \subseteq \mathbb{F}_p \setminus B$. Since $|\mathbb{F}_p \setminus B| = p - |B| = |A|$, it follows that $t - A = \mathbb{F}_p \setminus B \supseteq \Phi(D)$. As $-(N - 1)\mathbf{e}_1, \mathbf{e}_2 \in D$, there are $\mathbf{u}, \mathbf{w} \in \Lambda$ such that $\Phi(\mathbf{u}) = t + (N - 1)$ and $\Phi(\mathbf{w}) = t - \Phi(\mathbf{e}_2)$. By additivity of Φ and its injectivity on $[-N, N]^d$, we obtain $\mathbf{u} - \mathbf{w} = (N - 1)\mathbf{e}_1 + \mathbf{e}_2$. Therefore $N \geq \sum_{i=1}^d u_i = N + \sum_{i=1}^d w_i$, which implies $\mathbf{w} = \mathbf{0}$. Hence $t = \Phi(\mathbf{e}_2) \in \Phi(E)$, and therefore $A +_R B = \mathbb{F}_p \setminus \Phi(E)$. Since Φ is injective on E , we obtain $|\mathbb{F}_p \setminus (A +_R B)| = |\Phi(E)| = |E| = d$. $\square$

For each sufficiently large prime p , choose the largest integer $d \geq 2$ satisfying $(2d^3 + 1)^d < p$. By the choice of d , we have $\log p = 3d \log d + O(d)$, and hence $d = (\frac{1}{3} + o(1)) \log p / \log \log p$. The construction therefore gives

$$|\mathbb{F}_p \setminus (A +_R B)| = \left(\frac{1}{3} + o(1)\right) \frac{\log p}{\log \log p},$$

with $|A| = q = \exp(2d \log d + O(d)) = p^{2/3+o(1)}$ and $|B| = p - |A| = (1 - o(1))p$.

By taking suitable copies of the simplex in an additional coordinate, the construction above extends to $|A| + |B| = p + K$ with $\Delta(R) \leq \Delta$. We omit the proof of this extension and state the strongest bound it gives.

Proposition B.3. *Fix an integer $\Delta \geq 1$, and let $K = K(p)$ be a positive integer-valued function with $K = o(p)$. For all sufficiently large primes p , there are nonempty $A, B \subseteq \mathbb{F}_p$ and a relation $R \subseteq A \times B$ with $|A| + |B| = p + K$ and $\Delta(R) \leq \Delta$ such that*

$$|\mathbb{F}_p \setminus (A +_R B)| \geq (1 - o_\Delta(1)) \Delta \min \left\{ \frac{\log p}{3 \log \log p}, \frac{\log(p/K)}{\log \log(p/K)} \right\}$$

as $p \rightarrow \infty$. Moreover, if $K \leq p^{2/3+o(1)}$, this construction gives $|A| = p^{2/3+o(1)}$ and $|B| = (1 - o(1))p$.