Sets with few differences in abelian groups

Mitchell Lee*

Department of Mathematics
Harvard University
Cambridge, MA, U.S.A.

mitchell@math.harvard.edu

Submitted: Aug 21, 2015; Accepted: Jul 24, 2018; Published: Aug 10, 2018

Abstract

Let $(G, +)$ be an abelian group. In 2004, Eliahou and Kervaire found an explicit formula for the smallest possible cardinality of the sumset $A + A$, where $A \subseteq G$ has fixed cardinality r. We consider instead the smallest possible cardinality of the difference set $A - A$, which is always greater than or equal to the smallest possible cardinality of $A + A$ and can be strictly greater. We conjecture a formula for this quantity and prove the conjecture in the case that G is an elementary abelian p-group. This resolves a conjecture of Bajnok and Matzke on signed sumsets.

Mathematics Subject Classifications: 05D99,11B13

1 Introduction

Let G be a finite abelian group of order N written with additive notation. Given subsets $A, B \subseteq G$, the *sumset* of A and B is defined as

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

and the *difference set* of A and B is defined as

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

Let $-A$ denote the difference set $\{0\} - A = \{-a \mid a \in A\}$.

Given integers r and s with $1 \leqslant r, s \leqslant N$, define

$$\mu_G(r, s) = \min\{|A + B| \mid A, B \subseteq G, |A| = r, |B| = s\} \tag{1}$$
$$\rho_G^+(r) = \min\{|A + A| \mid A \subseteq G, |A| = r\} \tag{2}$$
$$\rho_G^-(r) = \min\{|A - A| \mid A \subseteq G, |A| = r\}. \tag{3}$$

*Supported by NSF Grant 1358659 and NSA Grant H98230-13-1-0273.

Observe that taking $B = A$ in (1) yields $\mu_G(r,r) \leqslant \rho_G^+(r)$ and taking $B = -A$ yields $\mu_G(r,r) \leqslant \rho_G^-(r)$.

The functions $\mu_G(r,s)$ and $\rho_G^+(r)$ have held considerable interest for over 200 years. In 1813, Cauchy [3] proved the following classical result, which was rediscovered by Davenport [4] in 1935.

Theorem 1 (Cauchy-Davenport Theorem [3, 4])**.** *Let $G = \mathbb{Z}/p\mathbb{Z}$ where p is prime. Then $\mu_G(r,s) = \min\{r+s-1, p\}$ for $1 \leqslant r, s \leqslant p$.*

In 2004, Eliahou and Kervaire [6] used a classical result of Kneser [8] to compute $\mu_G(r,s)$ and $\rho_G^+(r)$ for all finite abelian groups G.

Theorem 2 (Eliahou and Kervaire, [6, Theorem 2, Proposition 7])**.** *Let G be a finite abelian group of order N. Then*

$$\mu_G(r,s) = \min_{d \in D(N)} d\left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1\right)$$

for $1 \leqslant r, s \leqslant N$, where $D(N)$ denotes the set of positive divisors of N. Furthermore, we have $\rho_G^+(r) = \mu_G(r,r)$.

Remark 3. The quantities $\mu_G(r,s)$ and $\rho_G^+(r)$ depend only on N, r, and s (and not the group structure of G).

In contrast, there is no known explicit formula for the function $\rho_G^-(r)$, and it appears to exhibit more complicated behavior than $\rho_G^+(r)$. For example, if $G = (\mathbb{Z}/3\mathbb{Z})^2$, then $\rho_G^+(4) = \mu_G(4,4) = 7$ and $\rho_G^-(4) = 9$, so the inequality $\rho_G^+(r) = \mu_G(r,r) \leqslant \rho_G^-(r)$ need not hold with equality. Also, we will see that unlike $\rho_G^+(r)$, the quantity $\rho_G^-(r)$ may depend on the group structure of G and not only on N and r.

However, there are some cases in which $\rho_G^-(r)$ is known. The results of Bajnok and Matzke in [1, 2] yield a formula for $\rho_G^-(r)$ in the case that G is cyclic.

Theorem 4 (cf. [1, Theorem 4])**.** *Let $G = \mathbb{Z}/N\mathbb{Z}$. Then*

$$\rho_G^-(r) = \rho_G^+(r) = \min_{d \in D(N)} d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right)$$

for $1 \leqslant r \leqslant N$.

Their results also imply an upper bound for $\rho_G^-(r)$ for all groups G, which we conjecture holds with equality.

Theorem 5 (cf. [1, Theorem 5])**.** *Let G be a finite abelian group of order N. Let $e = \exp G$ be the exponent of G; that is, the least common multiple of the orders of the elements of G. For $1 \leqslant r \leqslant N$, define*

$$D(N,e,r) = \{d_1 d_2 \mid d_1 \in D(N/e), d_2 \in D(e), d_1 e \geqslant r\}.$$

Then

$$\rho_G^-(r) \leqslant \min_{d \in D(N,e,r)} d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right).$$

Conjecture 6 (cf. [1, Conjecture 10])**.** The inequality in Theorem 5 holds with equality. That is, under the hypotheses of Theorem 5, we have

$$\rho_G^-(r) = \min_{d \in D(N,e,r)} d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right).$$

The main goal of this paper is to prove a special case of Conjecture 6. Suppose that G is an elementary abelian p-group; that is, a group of the form $G = (\mathbb{Z}/p\mathbb{Z})^d$ where p is prime and $d \geqslant 0$. Then Theorem 7 below, which is our main result, computes $\rho_G^-(r)$. We will verify in Section 2 that Theorem 7 agrees with the prediction given by Conjecture 6.

Theorem 7. *Let $G = (\mathbb{Z}/p\mathbb{Z})^d$ where p is prime and $d \geqslant 0$. Let t and r be integers with $0 \leqslant t \leqslant d$ and $p^t < r \leqslant p^{t+1}$. Then*

$$\rho_G^-(r) = p^t \min\left\{2\left\lceil \frac{r}{p^t} \right\rceil - 1, p\right\}.$$

Theorem 7 has applications to questions about h-fold signed sumsets, which were introduced by Bajnok and Matzke in 2014 [1]. As in [1], if $A = \{a_1, \ldots, a_m\} \subseteq G$ is a set of size m, we define the *h-fold signed sumset*

$$h_\pm A = \left\{ \sum_{i=1}^m \lambda_i a_i \;\middle|\; (\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m, \sum_{i=1}^m |\lambda_i| = h \right\}$$

and

$$\rho_\pm(G, r, h) = \min\{|h_\pm A| \mid A \subseteq G, |A| = r\}$$

for $h \geqslant 0$ and $1 \leqslant r \leqslant N$. In Section 6, we will prove the following result as a consequence of Theorem 7.

Theorem 8 ([2, Conjecture 18])**.** *Let $p > 2$ be a prime number, and let c and v be integers with $0 \leqslant c \leqslant p-1$ and $1 \leqslant v \leqslant p$. Let $m = cp + v$.*

(a) If $1 \leqslant c \leqslant (p-3)/2$, then

$$\rho_\pm((\mathbb{Z}/p\mathbb{Z})^2, m, 2) = (2c+1)p.$$

(b) If $c = (p-1)/2$ and $v \leqslant (p-1)/2$, then

$$\rho_\pm((\mathbb{Z}/p\mathbb{Z})^2, m, 2) = p^2 - 1.$$

2 An outline of the proof of Theorem 7

Sections 2 to 5 of this paper will contain the proof of Theorem 7, which can be divided into four steps:

1. We will show, with the notation of Theorem 7, that
$$\rho_G^-(r) \leqslant p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\}.$$
2. We will show that if p is a prime and $d_1 > d_2 \geqslant 0$ are integers, then $\rho^-_{(\mathbb{Z}/p\mathbb{Z})^{d_1}}(r) = \rho^-_{(\mathbb{Z}/p\mathbb{Z})^{d_2}}(r)$ for $1 \leqslant r \leqslant p^{d_2}$.
3. By applying the Cauchy-Davenport Theorem (Theorem 1) repeatedly, we will prove Theorem 7 in the case that $r \leqslant p^2$.
4. We will conclude the proof of the theorem by induction on r.

We start with the following result, which is step (1) above.

Lemma 9. *With the notation of Theorem 7, we have*
$$\rho_G^-(r) \leqslant p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\}.$$

Proof. Using the notation of Theorem 5, we have $N = |G| = p^d$ and $e = \exp G = p$, so
$$\begin{aligned} D(N, e, r) &= \{d_1 d_2 \mid d_1 \in D(p^{d-1}), d_2 \in D(p), d_1 p \geqslant r\} \\ &= \{p^t, p^{t+1}, \ldots, p^{d-1}, p^d\}. \end{aligned}$$
By Theorem 5, we have
$$\begin{aligned} \min_{d \in D(N,e,r)} d\left(2\left\lceil \frac{r}{d}\right\rceil - 1\right) &= \min\left\{p^t\left(2\left\lceil \frac{r}{p^t}\right\rceil - 1\right), p^{t+1}, \ldots, p^{d-1}, p^d\right\} \\ &= p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\}, \end{aligned}$$
as desired. □

Remark 10. Here is an explicit example of a subset $A \subseteq G$ achieving the bound of Lemma 9. Put a total order $<$ on $\mathbb{Z}/p\mathbb{Z}$ by identifying it with $\{0, 1, \ldots, p-1\}$ in the usual way. Then, recall that $(\mathbb{Z}/p\mathbb{Z})^d$ is totally ordered by the *lexicographic order*, which is defined as follows: we say that $x = (x_1, \ldots, x_d)$ precedes $y = (y_1, \ldots, y_d)$ in the lexicographic order if for some i we have $x_i < y_i$ and $x_j = y_j$ for $j < i$. Let A be the set of the smallest r elements of $(\mathbb{Z}/p\mathbb{Z})^d$ in the lexicographic order. Then one can easily verify that
$$|A - A| = p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\},$$
which provides an alternative constructive proof of Lemma 9. It is worth noting that by [5, Proposition 3.1], the same set A satisfies $|A + A| = \rho_G^+(r)$.

3 Independence of dimension

The following result is step 2 in the proof of Theorem 7.

Lemma 11. *Let p be a prime and let $d_1 > d_2 \geqslant 0$ be integers. Let $G = (\mathbb{Z}/p\mathbb{Z})^{d_1}$ and $H = (\mathbb{Z}/p\mathbb{Z})^{d_2}$. Then $\rho_G^-(r) = \rho_H^-(r)$ for $1 \leqslant r \leqslant p^{d_2}$.*

Proof. It suffices to consider the case that $d_1 = d_2+1$. Since H embeds in G as a subgroup, we have $\rho_G^-(r) \leqslant \rho_H^-(r)$, so it remains to show that $\rho_H^-(r) \leqslant \rho_G^-(r)$.

Take a subset $A \subseteq G$ with $|A| = r$ and $|A - A| = \rho_G^-(r)$. Considering G as a vector space of dimension $d_1 = d_2 + 1$ over the finite field $\mathbb{F}_p$, there are

$$\frac{p^{d_1} - 1}{p - 1} = 1 + p + \cdots + p^{d_2} \geqslant p^{d_2}$$

lines containing 0 (that is, vector subspaces of dimension 1) in G. On the other hand, there are only

$$|A - A| - 1 \leqslant \rho_G^-(r) - 1 \leqslant \rho_H^-(r) - 1 < p^{d_2}$$

nonzero elements of $A - A$. Since no two distinct lines in G containing 0 share a nonzero element, we conclude that there is a line ℓ in G such that $\ell \cap (A - A) = \{0\}$.

Considering H as a vector space of dimension $d_2 = d_1 - 1$ over $\mathbb{F}_p$, fix an $\mathbb{F}_p$-linear transformation $\pi : G \to H$ whose kernel is the line ℓ. We claim that the restriction $\pi|_A$ is an injection. To show this, take $x, y \in A$ with $\pi(x) = \pi(y)$; we will show that $x = y$. Since π is linear, we have $\pi(x - y) = 0$, so $x - y \in \ker \pi = \ell$. Therefore, we have $x - y \in \ell \cap (A - A) = \{0\}$. That is, we have $x = y$, as desired.

Since $\pi|_A$ is an injection, we have $|\pi(A)| = |A| = r$, where $\pi(A)$ is the image of A under the map π. Therefore

$$\rho_H^-(r) \leqslant |\pi(A) - \pi(A)| = |\pi(A - A)| \leqslant |A - A| = \rho_G^-(r)$$

as desired. □

4 The case $r \leqslant p^2$

In this section, we show that the statement of Theorem 7 holds when $r \leqslant p^2$, which is step (3) in the proof of Theorem 7.

Lemma 12. *Let p be a prime and let d be a nonnegative integer. Let G be the group $(\mathbb{Z}/p\mathbb{Z})^d$. Then*

$$\rho_G^-(r) = p^t \min\left\{2\left\lceil \frac{r}{p^t} \right\rceil - 1, p\right\}$$

for $1 \leqslant r \leqslant \min\{p^d, p^2\}$, where t is the unique integer satisfying $p^t < r \leqslant p^{t+1}$.

The following lemma will be instrumental in the proof of Lemma 12.

Lemma 13. *Let p be a prime, and let m and n be integers with $3 \leqslant n+2 \leqslant m \leqslant (p-1)/2$. Let $\lambda = (\lambda_1, \ldots, \lambda_m)$ be a sequence of integers with $p \geqslant \lambda_1 \geqslant \cdots \geqslant \lambda_m > 0$ and $\sum_{k=1}^{m} \lambda_k \geqslant np+1$. Let $\mu = (\mu_1, \ldots, \mu_{2m-1})$ be a sequence of integers such that $\mu_{i+j-1} \geqslant \min\{\lambda_i + \lambda_j - 1, p\}$ for $1 \leqslant i, j \leqslant m$. Then*

$$\sum_{k=1}^{2m-1} \mu_k \geqslant (2n+1)p.$$

Proof. We defer the proof to Appendix A. □

Proof of Lemma 12. By Lemma 9, we have

$$\rho_G^-(r) \leqslant p^t \min\left\{2\left\lceil \frac{r}{p^t} \right\rceil - 1, p\right\},$$

so it remains to show that

$$\rho_G^-(r) \geqslant p^t \min\left\{2\left\lceil \frac{r}{p^t} \right\rceil - 1, p\right\}. \tag{4}$$

If $r \leqslant p$, then this follows directly from Lemma 11 and the Cauchy-Davenport Theorem. Thus, we may assume $r > p$.

By Lemma 11, we may assume that $d = 2$, so $G = (\mathbb{Z}/p\mathbb{Z})^2$. If $p = 2$, then the theorem follows easily from enumerating all possible values of r and all sets $A \subseteq G$, so assume that $p > 2$. Let

$$r' = \begin{cases} p\left(\lceil r/p \rceil - 1\right) + 1 & \text{if } r \leqslant p(p-1)/2 \\ p(p-1)/2 + 1 & \text{if } r > p(p-1)/2 \end{cases}.$$

Since $r \geqslant r'$, replacing r by r' cannot increase the left-hand side of (4), and it is easy to check that this replacement leaves the right-hand side unchanged. Therefore, we may assume that $r = np+1$ where $1 \leqslant n \leqslant (p-1)/2$. Take a subset $A \subset G$ with $|A| = r$; we will show that

$$|A - A| \geqslant (2n+1)p = p^t \min\left\{2\left\lceil \frac{r}{p^t} \right\rceil - 1, p\right\}.$$

Identify G with the two-dimensional vector space $\mathbb{F}_p^2$ over the field $\mathbb{F}_p$. We will now count the two-element subsets of A in two ways. By definition, the number of two-element subsets of A is the binomial coefficient $\binom{np+1}{2}$. On the other hand, every two-element subset of A is contained in a unique line (that is, affine subspace of G of dimension 1), so we can count these subsets according to the lines containing them. This yields

$$\sum_{\ell \subset G} \binom{|A \cap \ell|}{2} = \binom{np+1}{2} \tag{5}$$

where the sum is over all lines $\ell \subset G$. Every line in G is parallel to exactly one line $\ell' \subset G$ containing 0, so (5) can be rewritten as

$$\sum_{\substack{\ell' \subset G \\ \ell' \ni 0}} \sum_{\substack{\ell \subset G \\ \ell \| \ell'}} \binom{|A \cap \ell|}{2} = \binom{np+1}{2}$$

where the outer sum is over all lines $\ell' \subset G$ containing 0, and the inner sum is over all lines $\ell \subset G$ parallel to ℓ'. Since there are exactly $p+1$ lines in G containing 0, there is a particular line $\ell_0 \subset G$ containing 0 such that

$$\sum_{\substack{\ell \subset G \\ \ell \| \ell_0}} \binom{|A \cap \ell|}{2} \geqslant \frac{1}{p+1} \binom{np+1}{2}.$$

We may assume, by applying an $\mathbb{F}_p$-linear change of coordinates, that ℓ_0 is the line $\{(0,y) \mid y \in \mathbb{F}_p\} \subset \mathbb{F}_p^2 = G$. For any $x \in \mathbb{F}_p$, define the line

$$\ell_x = \{(x,y) \mid y \in \mathbb{F}_p\}.$$

Then, the lines in G parallel to ℓ_0 are exactly the lines ℓ_x for $x \in \mathbb{F}_p$. Let

$$m = \max_{x \in \mathbb{F}_p} |A \cap \ell_x|.$$

Since

$$\sum_{x \in \mathbb{F}_p} |A \cap \ell_x| = |A| = np+1,$$

we have $m \geqslant \lceil (np+1)/p \rceil = n+1$. We consider three cases, depending on whether $m \geqslant (p+1)/2$, or $m = n+1$, or $n+2 \leqslant m \leqslant (p-1)/2$.

Case 1 ($\boldsymbol{m \geqslant (p+1)/2}$):
Take $x \in \mathbb{F}_p$ such that $|A \cap \ell_x| = m$. Since ℓ_x is a translate of ℓ_0, which is isomorphic as a group to $\mathbb{Z}/p\mathbb{Z}$, the Cauchy-Davenport Theorem applies to the difference $(A \cap \ell_x) - (A \cap \ell_x) \subseteq \ell_0$, yielding

$$|(A-A) \cap \ell_0| \geqslant |(A \cap \ell_x) - (A \cap \ell_x)| \geqslant \min\{2m-1, p\} = p.$$

(Essentially, we are applying the Cauchy-Davenport Theorem only to the second coordinates of the elements of $A \cap \ell_x$, which lie in $\mathbb{Z}/p\mathbb{Z}$.) That is, the line ℓ_0 is a subset of $A - A$.

Now, take *any* line $\ell' \subset G$ containing 0. There is a line ℓ parallel to ℓ' such that $|A \cap \ell| \geqslant \lceil (np+1)/p \rceil = n+1$. Since ℓ is a translate of ℓ', which is isomorphic as a group to $\mathbb{Z}/p\mathbb{Z}$, the Cauchy-Davenport Theorem again applies to the difference $(A \cap \ell) - (A \cap \ell) \subseteq \ell'$, yielding

$$|(A-A) \cap \ell'| \geqslant |(A \cap \ell) - (A \cap \ell)| \geqslant \min\{2(n+1)-1, p\} = 2n+1.$$

Since $G \setminus \{0\}$ is equal to the disjoint union

$$\bigsqcup_{\substack{\ell' \subset G \\ \ell' \ni 0}} (\ell' \setminus \{0\})$$

over all lines $\ell' \subset G$ containing 0, we conclude

$$\begin{aligned}|A-A| &= 1 + \sum_{\substack{\ell' \subset G \\ \ell' \ni 0}} (|(A-A) \cap \ell'| - 1) \\ &\geqslant 1 + (p-1) + p \cdot ((2n+1) - 1) \\ &= (2n+1)p\end{aligned}$$

which is the desired inequality.

Case 2 ($m = n+1$):
Let $S = \{x \in \mathbb{F}_p \mid |A \cap \ell_x| = n+1\}$ and let $s = |S|$. For each $x \in \mathbb{F}_p \setminus S$ we have $|A \cap \ell_x| \leqslant n$, so

$$\begin{aligned}\frac{1}{p+1}\binom{np+1}{2} &\leqslant \sum_{x \in \mathbb{F}_p} \binom{|A \cap \ell_x|}{2} \\ &= s\binom{n+1}{2} + \sum_{x \in \mathbb{F}_p \setminus S} \binom{|A \cap \ell_x|}{2} \\ &\leqslant s\binom{n+1}{2} + \sum_{x \in \mathbb{F}_p \setminus S} \frac{n-1}{2}|A \cap \ell_x| \\ &= s\binom{n+1}{2} + \frac{n-1}{2}((np+1) - (n+1)s),\end{aligned}$$

Simplifying this inequality and using the bound $n \leqslant (p-1)/2$, we obtain

$$\begin{aligned}s &\geqslant \frac{p+1-n}{p+1} \cdot \frac{np+1}{n+1} \\ &\geqslant \frac{p+1-(p-1)/2}{p+1} \cdot \frac{p(p-1)/2+1}{(p-1)/2+1} \\ &= \frac{p-1}{2} + \frac{p^2+7}{2(p+1)^2} \\ &> \frac{p-1}{2}.\end{aligned}$$

Thus $s \geqslant (p+1)/2$, so by the Cauchy-Davenport Theorem, we have $|S-S| \geqslant \min\{2s-1, p\} = p$, so $S - S = \mathbb{F}_p$.

Now, take any $x \in \mathbb{F}_p$. Since $x \in S - S$, there is $y \in \mathbb{F}_p$ such that $y, x+y \in S$. By the Cauchy-Davenport Theorem again, we have

$$|(A-A) \cap \ell_x| \geqslant |A \cap \ell_{x+y} - A \cap \ell_y| \geqslant \min\{2(n+1)-1, p\} = 2n+1.$$

Summing over all $x \in \mathbb{F}_p$ yields

$$|A-A| = \sum_{x \in \mathbb{F}_p} |(A-A) \cap \ell_x| \geqslant (2n+1)p$$

as desired.

Case 3 ($n+2 \leqslant m \leqslant (p-1)/2$):
For $1 \leqslant k \leqslant p$, define

$$\begin{aligned}\Lambda_k &= \{x \in \mathbb{F}_p \mid |A \cap \ell_x| \geqslant k\} \\ M_k &= \{x \in \mathbb{F}_p \mid |(A-A) \cap \ell_x| \geqslant k\} \\ \lambda_k &= |\Lambda_k| \\ \mu_k &= |M_k|.\end{aligned}$$

By definition, we have $p \geqslant \lambda_1 \geqslant \cdots \geqslant \lambda_m > 0$ and $p \geqslant \mu_1 \geqslant \cdots \geqslant \mu_p \geqslant 0$. We have

$$\sum_{k=1}^{m} \lambda_k = \sum_{x \in \mathbb{F}_p} |A \cap \ell_x| = |A| = ap + 1$$

because each line ℓ_x contributes exactly $|A \cap \ell_x|$ to the sum. Similarly

$$\sum_{k=1}^{p} \mu_k = \sum_{x \in \mathbb{F}_p} |(A-A) \cap \ell_x| = |A-A|.$$

We claim that $M_{i+j-1} \supseteq \Lambda_i - \Lambda_j$ for $1 \leqslant i, j \leqslant m$. To show this, take $x_1 \in \Lambda_i$ and $x_2 \in \Lambda_j$; we will show that $x_1 - x_2 \in M_{i+j-1}$. By the Cauchy-Davenport Theorem, we have

$$\begin{aligned}|(A-A) \cap \ell_{x_1-x_2}| &\geqslant |A \cap \ell_{x_1} - A \cap \ell_{x_2}| \\ &\geqslant \min\{|A \cap \ell_{x_1}| + |A \cap \ell_{x_2}| - 1, p\} \\ &\geqslant \min\{i+j-1, p\} \\ &= i+j-1\end{aligned}$$

where the last equality follows from the bound $i, j \leqslant m \leqslant (p-1)/2$. That is, we have $x_1 - x_2 \in M_{i+j-1}$, as desired.

By the Cauchy-Davenport Theorem again, we conclude

$$\mu_{i+j-1} = |M_{i+j-1}| \geqslant |\Lambda_i - \Lambda_j| \geqslant \min\{\lambda_i + \lambda_j - 1, p\} \tag{6}$$

for $1 \leqslant i, j \leqslant m$.

Therefore, the conditions of Lemma 13 are satisfied, so

$$|A-A| = \sum_{k=1}^{p} \mu_k \geqslant (2n+1)p$$

as desired. □

5 Completing the proof of Theorem 7

Before proceeding to the proof of Theorem 7, we prove a general lemma about sets in vector spaces over finite fields.

Lemma 14. *Let p be a prime and let m be an integer. Let G be a vector space over the field $\mathbb{F}_p$ of dimension $d \geqslant 3$, and let S be a subset of G such that*

$$|S \cap H| \geqslant mp^{d-2}$$

for each vector hyperplane H (that is, vector subspace of dimension $d-1$) in G. Then $|S| \geqslant mp^{d-1}$.

Proof of Lemma 14. Assume for the sake of contradiction that $|S| < mp^{d-1}$. We first claim that there is a $(d-2)$-dimensional vector subspace $V_0 \subset G$ with $|S \cap V_0| \leqslant mp^{d-3}$. To show this, take a $(d-2)$-dimensional vector subspace $V \subset G$ uniformly at random. It is clear that V has $p^{d-2}-1$ nonzero elements, that G has $p^d - 1$ nonzero elements, and that each nonzero element of G is in V with equal probability. Therefore, the probability that $x \in V$ for a fixed $x \in G \setminus \{0\}$ is

$$\frac{p^{d-2}-1}{p^d-1}.$$

Clearly, the probability that $0 \in V$ is 1. Therefore, by the linearity of expectation, the expected value of $|S \cap V|$ is given by

$$\begin{aligned}
\mathbb{E}[|S \cap V|] &= 1 + (|S|-1)\frac{p^{d-2}-1}{p^d-1} \\
&< 1 + (mp^{d-1}-1)\frac{p^{d-2}-1}{p^d-1} \\
&= mp^{d-3} + \frac{(p^2-1)(p-m)p^{d-3}}{p^d-1} \\
&< mp^{d-3} + 1.
\end{aligned}$$

Since mp^{d-3} is an integer, we conclude that there is a particular $(d-2)$-dimensional vector subspace $V_0 \subset G$ with $|S \cap V_0| \leqslant mp^{d-3}$.

Finally, consider the integer N defined by the sum

$$N = \sum_H |S \cap H|$$

where H ranges over all vector hyperplanes with $V_0 \subset H \subset G$. Such hyperplanes H are in bijection with lines through the origin in the two-dimensional quotient space G/V_0, so there are $p+1$ of them. Therefore, by the assumption of the theorem, we have

$$N \geqslant \sum_H mp^{d-2} = (p+1)mp^{d-2}.$$

On the other hand, the sum defining N counts every element of $S \setminus V_0$ once and every element of $S \cap V_0$ exactly $p+1$ times, so

$$N = |S| + p|S \cap V_0|.$$

Therefore, we have

$$|S| = N - p|S \cap V_0| \geqslant (p+1)mp^{d-2} - p \cdot mp^{d-3} = mp^{d-1},$$

which contradicts our assumption that $|S| < mp^{d-1}$. □

We are now ready to restate and prove Theorem 7.

Theorem 7. *Let $G = (\mathbb{Z}/p\mathbb{Z})^d$ where p is prime and $d \geqslant 0$. Let t and r be integers with $0 \leqslant t \leqslant d$ and $p^t < r \leqslant p^{t+1}$. Then*

$$\rho_G^-(r) = p^t \min\left\{2\left\lceil \frac{r}{p^t} \right\rceil - 1, p\right\}.$$

Proof. We proceed by induction on r. If $t < 2$, then the result follows from Lemma 12, so we may assume $t \geqslant 2$. By Lemma 11, we may also assume that $d = t+1$. Let $m = \min\{2\lceil r/p^t \rceil - 1, p\}$. We wish to show that $\rho_G^-(r) = mp^t$. By Lemma 9, we have $\rho_G^-(r) \leqslant mp^t$, so it remains to show that $\rho_G^-(r) \geqslant mp^t$. Let A be a subset of G with $|A| = r$; we will show that $|A - A| \geqslant mp^t$.

Consider G as a vector space of dimension $d = t+1 \geqslant 3$ over $\mathbb{F}_p$. By Lemma 14 applied to $S = A - A$, it suffices to show that $|(A-A) \cap H| \geqslant mp^{t-1}$ for each vector hyperplane $H \subset G$. For this, note that there are exactly p distinct translates $H + x$, where $x \in G$, and that the entire space G is the disjoint union of these p translates. Therefore, there exists $x_0 \in G$ such that $|A \cap (H + x_0)| \geqslant \lceil r/p \rceil$. By the inductive hypothesis,

$$|(A-A) \cap H| \geqslant |(A \cap (H+x_0)) - (A \cap (H+x_0))| \geqslant \rho_H^-(\lceil r/p \rceil) = mp^{t-1}$$

as desired. □

6 Applications to signed sumsets

In this section, we prove Theorem 8. In particular, we will show that it is a consequence of the following more general result.

Lemma 15. *Let G be a finite abelian group of order N. Then*

$$\rho_{\pm}(G, m, 2) \geqslant \min\{\rho_G^-(m), \rho_G^-(2m) - 1\}$$

for $1 \leqslant m \leqslant N/2$.

Proof. Let $A \subseteq G$ be a subset with $|A| = m$. We will show that

$$2_{\pm}A \geqslant \min\{\rho_G^-(m), \rho_G^-(2m) - 1\}.$$

We consider two cases, depending on whether or not $A \cap (-A) = \emptyset$.

Case 1 ($A \cap (-A) \neq \emptyset$)**:**
Choose $x \in A \cap (-A)$. By definition, the signed sumset $2_{\pm}A$ contains $0 = x + (-x)$ and it contains the difference of any two distinct elements of A. Therefore, we have $A - A \subseteq 2_{\pm}A$. It follows that

$$|2_{\pm}A| \geqslant |A - A| \geqslant \rho_G^-(m) \geqslant \min\{\rho_G^-(m), \rho_G^-(2m) - 1\},$$

as desired.

Case 2 ($A \cap (-A) = \emptyset$)**:**
Let $B = A \cup (-A)$. Then $|B| = 2|A|$. By definition, the signed sumset $2_{\pm}A$ contains $(B - B) \setminus \{0\}$, so

$$\begin{aligned} |2_{\pm}A| &\geqslant |B - B| - 1 \\ &\geqslant \rho_G^-(2m) - 1 \\ &\geqslant \min\{\rho_G^-(m), \rho_G^-(2m) - 1\}, \end{aligned}$$

as desired. □

Now, we shall restate and prove Theorem 8.

Theorem 8 ([2, Conjecture 18])**.** *Let $p > 2$ be a prime number, and let c and v be integers with $0 \leqslant c \leqslant p - 1$ and $1 \leqslant v \leqslant p$. Let $m = cp + v$.*

(a) If $1 \leqslant c \leqslant (p - 3)/2$, then

$$\rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) = (2c + 1)p.$$

(b) If $c = (p - 1)/2$ and $v \leqslant (p - 1)/2$, then

$$\rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) = p^2 - 1.$$

Proof. (a) By Lemma 15 and Theorem 7, we have

$$\begin{aligned} \rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) &\geqslant \min\{\rho_G^-(m), \rho_G^-(2m) - 1\} \\ &= \min\left\{(2c + 1)p, \left(4c + 2\left\lceil \frac{2v}{p} \right\rceil + 1\right)p - 1\right\} \\ &= (2c + 1)p. \end{aligned}$$

The reverse inequality $\rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) \leqslant (2c + 1)p$ follows from [1, Theorem 5].

(b) By Lemma 15 and Theorem 7, we have

$$\begin{aligned} \rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) &\geqslant \min\{\rho_G^-(m), \rho_G^-(2m) - 1\} \\ &= \min\{p^2, p^2 - 1\} \\ &= p^2 - 1. \end{aligned}$$

The reverse inequality $\rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) \leqslant p^2 - 1$ follows from [1, Proposition 8]. □

A Proof of Lemma 13

In this appendix, we prove Lemma 13. The main tool used in the proof is [7, Lemma 2.1], which we restate here for convenience.

Lemma 16 ([7, Lemma 2.1])**.** *If $a_1, \dots, a_m, b_1, \dots, b_n \in \mathbb{R}$, then*

$$\frac{1}{m+n-1}\sum_{i=2}^{m+n} \max_j\{a_j + b_{i-j} \mid 1 \leqslant j \leqslant m, 1 \leqslant i-j \leqslant n\} \geqslant \frac{1}{m}\sum_{i=1}^{m} a_i + \frac{1}{n}\sum_{i=1}^{n} b_i.$$

Proof of Lemma 13. For each i with $2 \leqslant i \leqslant 2m$, let

$$c_i = \max\{\lambda_j + \lambda_{i-j} \mid 1 \leqslant j \leqslant m, 1 \leqslant i-j \leqslant m\}.$$

Let h be the largest integer such that $c_{h+1} > p+1$, or 0 if no such integer exists. Then $\mu_i \geqslant p \geqslant c_{i+1} - p$ for $i \leqslant h$ and $\mu_i \geqslant c_{i+1} - 1$ for $i > h$.

Proceed by induction on m. We consider two cases, depending on whether $h \leqslant 1$ or $h \geqslant 2$.

Case 1 ($h \leqslant 1$):
First, assume $n = 1$ and $m = 3$ and $h = 1$. Then

$$\begin{aligned}\sum_{k=1}^{2m-1} \mu_k &= \mu_1 + \mu_2 + \mu_3 + \mu_4 + \mu_5 \\ &\geqslant p + (\lambda_1 + \lambda_2 - 1) + (\lambda_1 + \lambda_3 - 1) + (\lambda_2 + \lambda_3 - 1) + 1 \\ &\geqslant p + 2(\lambda_1 + \lambda_2 + \lambda_3) - 2 \\ &\geqslant p + 2(p+1) - 2 \\ &= 3p\end{aligned}$$

as desired.

Next, assume $n = 1$ and $m \geqslant 4$ and $h = 1$. Then $2\lambda_1 = c_2 > p+1$, so $\lambda_1 > (p+1)/2$. Therefore $\mu_k \geqslant \lambda_1 + \lambda_k - 1 > (p+1)/2$ for $1 < k < m$ and $\mu_k \geqslant \lambda_m + \lambda_{k-m+1} - 1 \geqslant \lambda_{k-m+1}$ for $k \geqslant m$, so

$$\begin{aligned}\sum_{k=1}^{2m-1} \mu_k &> p + \sum_{k=2}^{m-1} \frac{p+1}{2} + \sum_{k=m}^{2m-1} \lambda_{k-m+1} \\ &= p + (m-2)\frac{p+1}{2} + (np+1) \\ &> 3p\end{aligned}$$

as desired.

Thus we may assume that either $h = 0$, or $h = 1$ and $n \geqslant 2$. Then $h \leqslant n - 1$, so

$$\begin{aligned}\sum_{k=1}^{2m-1} \mu_k &\geqslant \sum_{k=2}^{2m} c_i - (2m - 1 - h) - ph \\ &\geqslant (2m-1)\frac{2}{m}(np+1) - (2m-1-h) - ph \\ &\geqslant (2m-1)\frac{2}{m}(np+1) - (2m-1) - (p-1)(n-1) \\ &= (3n+1)p + n + 4 - \frac{2}{m}(np+1) - 2m\end{aligned}$$

where the second inequality follows from Lemma 16. It remains to show that

$$(3n+1)p + n + 4 - \frac{2}{m}(np+1) - 2m \geqslant (2n+1)p. \tag{7}$$

for $3 \leqslant n + 2 \leqslant m \leqslant (p-1)/2$. Each side of (7) is a linear function of the variable p, so it is enough to verify (7) after substituting $p = 2m$ and in the limit as $p \to \infty$.

After substituting $p = 2m$ (or equivalently $m = p/2$), the left-hand side of (7) becomes

$$\begin{aligned}(3n+1)p + n + 4 - \frac{4}{p}(np+1) - p &= (2n+1)p + (n-1)(p-3) + \left(1 - \frac{4}{p}\right) \\ &\geqslant (2n+1)p\end{aligned}$$

as desired.

Observe that

$$3n + 1 - \frac{2n}{m} > 2n + 1,$$

so the coefficient of p on the left-hand side of (7) is greater than the coefficient of p on the right-hand side. Thus (7) also holds in the limit as $p \to \infty$, so it holds whenever $3 \leqslant n + 2 \leqslant m \leqslant (p-1)/2$.

Case 2 ($h \geqslant 2$):
Define the sequence $\lambda' = (\lambda'_1, \ldots, \lambda'_{m-1})$ by $\lambda'_k = \lambda_{k+1}$ for $1 \leqslant k \leqslant m-1$. Then, define $\mu' = (\mu'_1, \ldots, \mu'_{2m-3})$ by

$$\mu'_k = \max_{k=i+j-1} \min\{\lambda'_i + \lambda'_j - 1, p\}$$

for $1 \leqslant k \leqslant 2m-3$, where the maximum is over all $1 \leqslant i, j \leqslant m-1$ with $k = i + j - 1$. We have

$$\sum_{k=1}^{m-1} \lambda'_k = \left(\sum_{k=1}^{m} \lambda_k\right) - \lambda_1 \geqslant (n-1)p + 1,$$

so by the inductive hypothesis we have

$$\sum_{k=1}^{2m-3} \mu'_k \geqslant (2n-1)p.$$

On the other hand, we have

$$\mu_{k+2} = \max_{k+2=i+j-1}(\lambda_i + \lambda_j - 1) \geqslant \max_{k=i+j-1}(\lambda'_i + \lambda'_j - 1) = \mu'_k$$

for $1 \leqslant k \leqslant 2m-3$, where the inequality follows from replacing (i, j) with $(i-1, j-1)$. Therefore

$$\sum_{k=1}^{2m-1} \mu_k = 2p + \sum_{k=1}^{2m-3} \mu'_k \geqslant (2n+1)p$$

as desired. □

Acknowledgments

This research was conducted under the supervision of Joseph Gallian at the University of Minnesota Duluth REU. The author thanks Joseph Gallian, who ran the REU, brought this question to his attention, and provided helpful comments on the manuscript. He thanks his advisors Levent Alpoge and Benjamin Gunby for valuable discussions and advice.

References

[1] Béla Bajnok and Ryan Matzke. The minimum size of signed sumsets. *Electronic Journal of Combinatorics*, 22(2):#P2.50, 2015.

[2] Béla Bajnok and Ryan Matzke. On the minimum size of signed sumsets in elementary abelian groups. *Journal of Number Theory*, 159:384 – 401, 2016.

[3] Augustin-Louis Cauchy. Recherches sur les nombres. In *Oeuvres complètes*, volume 1, pages 39–63. Cambridge University Press, 2009. Cambridge Books Online.

[4] Harold Davenport. On the addition of residue classes. *Journal of the London Mathematical Society*, 1(1):30–32, 1935.

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

[6] Shalom Eliahou and Michel Kervaire. Minimal sumsets in infinite abelian groups. *Journal of Algebra*, 287(2):449 – 457, 2005.

[7] David Grynkiewicz and Oriol Serra. Properties of two-dimensional sets with small sumset. *Journal of Combinatorial Theory, Series A*, 117(2):164 – 188, 2010.

[8] Martin Kneser. Abschätzung der asymptotischen dichte von summenmengen. *Mathematische Zeitschrift*, 58(1):459–484, 1953.