On sumsets of multisets in $\mathbb{Z}_p^m$

Kaisa Matomäki*

Department of Mathematics
University of Turku
20014 Turku, Finland

ksmato@utu.fi

Submitted: Apr 5, 2013; Accepted: Aug 20, 2013; Published: Aug 30, 2013
Mathematics Subject Classifications: 11B13

Abstract

For a sequence A of given length n contained in $\mathbb{Z}_p^2$ we study how many distinct subsums A must have when A is not "wasteful" by containing too many elements in same subgroup. Martin, Peilloux and Wong have made a conjecture for a sharp lower bound and established it when n is not too large whereas Peng has previously established the conjecture for large n. In this note we build on these earlier works and add an elementary argument leading to the conjecture for every n.

Martin, Peilloux and Wong also made a more general conjecture for sequences in $\mathbb{Z}_p^m$. Here we show that the special case $n = mp - 1$ of this conjecture implies the whole conjecture and that the conjecture is equivalent to a strong version of the additive basis conjecture of Jaeger, Linial, Payan and Tarsi.

1 Introduction

For a sequence A contained in an abelian group $\mathbf{G}$ we write $\sum A$ for the set of all subsums of A, that is, for $A = (a_1, \dots, a_n)$,

$$\sum A = \left\{ \sum_{i \in I} a_i \colon I \subseteq \{1, \dots, n\} \right\}.$$

Note that $\sum A$ always contains 0, the sum of an empty sequence. As the order of the elements of A is not relevant here, we will from now on think of A as a multiset. For a set or multiset B, we write $|B|$ for the cardinality of B, counted with multiplicity, and $\#B$ for the cardinality of B counted without multiplicity.

*Supported by the Academy of Finland grant no. 137883

Here we are interested in the relationship between $|A|$ and $\#\sum A$. As pointed out for instance in [3, Lemma 1.3], in case $\mathbf{G} = \mathbb{Z}_p$ one gets the following result easily by multiple applications of the Cauchy-Davenport inequality (see [6, Theorem 5.4]).

Lemma 1. *Let $p \in \mathbb{P}$ and let A be a multiset contained in $\mathbb{Z}_p^*$. Then*

$$\#\sum A \geqslant \min\{p, |A| + 1\}.$$

This lower bound is sharp as A may consist of $|A|$ copies of a single element.

Let us now consider the case $\mathbf{G} = \mathbb{Z}_p^2$. In this case one might not get a better lower bound than the above if much of A is contained in a single subgroup. In particular it is "wasteful" for A to contain more than $p-1$ elements from any subgroup since by Lemma 1 already $p-1$ elements guarantee that $\sum A$ contains the whole subgroup. In light of this we make the following definition (following [3]).

Definition 2. A multiset A contained in $\mathbb{Z}_p^2$ is called *valid* if $0 \notin A$ and every non-trivial subgroup of $\mathbb{Z}_p^2$ contains at most $p-1$ points of A (counting multiplicity).

For a valid multiset A in $\mathbb{Z}_p^2$ with at most $p-1$ elements, one has again the sharp lower bound $\#\sum A \geqslant |A| + 1$. On the other hand, for large multisets Peng [4] has shown the following.

Theorem 3. *Let $p \in \mathbb{P}$ and let A be a valid multiset contained in $\mathbb{Z}_p^2$ with $|A| \geqslant 2p-1$. Then $\sum A = \mathbb{Z}_p^2$.*

Hence we can concentrate on the case $p \leqslant |A| \leqslant 2p-2$. Martin, Peilloux and Wong [3] have made the following conjecture.

Conjecture 4. Let $p \in \mathbb{P}$, let k be a non-negative integer, and let A be a valid multiset contained in $\mathbb{Z}_p^2$ with $|A| = p + k$. If $k \leqslant p-3$, then $\#\sum A \geqslant (k+2)p$ and if $k = p-2$, then $\#\sum A \geqslant p^2 - 1$.

If true, this conjecture would be sharp as pointed out in [3]: First, for $k \leqslant p-3$, the multiset A may consist of $p-1$ copies of $(1,0)$ and $k+1$ copies of $(0,1)$, so that $\sum A = \mathbb{Z}_p \times \{0, \ldots, k+1\}$. Second, for $k = p-2$, A may consist of $p-2$ copies of $(1,0)$ and one copy of each $(i,1), 0 \leqslant i \leqslant p-1$, so that $\sum A = \mathbb{Z}_p^2 \setminus \{(p-1,0)\}$.

Martin, Peilloux and Wong [3] proved the conjecture when

$$k \leqslant \max\{1, \sqrt{p/(2\log p + 1)} - 1\}.$$

Here we will prove the conjecture for every k.

Theorem 5. *Conjecture 4 holds.*

Martin, Peilloux and Wong [3] also generalised Conjecture 4 to $\mathbb{Z}_p^m$ for $m \geqslant 2$. They again want to avoid "wasteful" sets and thus only consider "valid" sets. To easily define validity in this setting, for a subgroup $\mathbf{H}$ of $\mathbb{Z}_p^m$, we write $\dim \mathbf{H} = d$ where d is the integer for which $\mathbf{H}$ is isomorphic to $\mathbb{Z}_p^d$.

Definition 6. Let $m \geqslant 2$. A multiset A contained in $\mathbb{Z}_p^m$ is called *valid* if $0 \notin A$ and every non-trivial subgroup $\mathbf{H}$ of $\mathbb{Z}_p^m$ contains fewer than $p \cdot \dim \mathbf{H}$ points of A (counting multiplicity).

Taking $\mathbf{H} = \mathbb{Z}_p^m$ one sees that every valid multiset has size at most $mp - 1$. On the other hand, there are valid multisets of this size, see [3, Example 4.2]. Furthermore in case $m = 2$ the definition of validity agrees with Definition 2 in the interesting case $|A| \leqslant 2p - 1$. Martin, Peilloux and Wong [3] made the following conjecture.

Conjecture 7. Let p be an odd prime, let $m \geqslant 2$ be a positive integer, and let A be a valid multiset contained in $\mathbb{Z}_p^m$ with $|A| = qp + k$, where $q \geqslant 1$ and $0 \leqslant k \leqslant p - 1$.

(a) If $0 \leqslant k \leqslant p - 3$, then $\# \sum A \geqslant (k+2)p^q$;

(b) If $k = p - 2$, then $\# \sum A \geqslant p^{q+1} - 1$.

(c) If $k = p - 1$, then $\# \sum A \geqslant p^{q+1}$.

Again the definition of validity is such that, assuming Conjecture 7, it would be "wasteful" for a multiset to be non-valid. Also, if the conjecture is true, it gives the best possible lower bounds, see [3, Discussion after Conjecture 4.3].

Notice in particular the following special case of the conjecture.

Conjecture 8. Let p be an odd prime, let m be a positive integer, and let A be a valid multiset contained in $\mathbb{Z}_p^m$ with $|A| = mp - 1$. Then $\sum A = \mathbb{Z}_p^m$.

In Section 4 we will show that the methods used in the proof of Theorem 5 can be adapted to show the following theorem.

Theorem 9. *Conjecture 8 implies Conjecture 7.*

Hence a special case generalising Peng's result (Theorem 3) implies the whole conjecture. Peng has actually generalised his result to $\mathbb{Z}_p^m$ in [5] but he considers a much wider class of multisets than the valid sets here, so the result in [5] is not helpful here.

Let us close the introduction by discussing the additive basis conjecture of Jaeger, Linial, Payan and Tarsi [2]. We need the following definition from [1].

Definition 10. For a prime p and a positive integer m, let $f(p, m)$ denote the minimal integer t such that, for any t bases $B_1, \dots, B_t$ of $\mathbb{Z}_p^m$ one has

$$\sum \left(\bigcup_{i=1}^{t} B_i \right) = \mathbb{Z}_p^m,$$

where the union is let to be a multiset.

For instance by splitting the set A of size $2p-2$ below Conjecture 4 into $p-1$ bases of $\mathbb{Z}_p^2$, one sees that for $p \geqslant 3$ and $m \geqslant 2$, $f(p,m) \geqslant p$. Jaeger, Linial, Payan and Tarsi [2] conjectured that $f(p,m)$ can be bounded from above by a function of p alone and suggested that perhaps even $f(p,m) = p$. They showed that the conjecture has implications to group connectivity of graphs. Alon, Linial and Meshulam [1] showed that $f(p,m) \leqslant (p-1)\log m + p - 2$, a bound which depends mildly on m.

We make the following related conjecture.

Conjecture 11. If $B_1, B_2, \ldots, B_{p-1}$ are bases of $\mathbb{Z}_p^m$ and $A \subset \mathbb{Z}_p^m$ is a (linearly) independent set of size $m-1$, then

$$\sum \left(A \cup \bigcup_{i=1}^{p-1} B_i \right) = \mathbb{Z}_p^m,$$

where these unions are as multisets.

Clearly this conjecture in particular implies $f(p,m) \leqslant p$, so that the following theorem which we will prove in Section 4 shows that the conjecture of Martin, Peilloux and Wong actually implies the strongest possible form of the additive basis conjecture.

Theorem 12. *Conjecture 11 is equivalent to Conjecture 8.*

2 Auxiliary results

As in [3], we will take advantage of direct sum representations of $\mathbb{Z}_p^m$. Recall that a group $\mathbf{G}$ is an *internal direct sum* of subgroups $\mathbf{H}$ and $\mathbf{K}$ iff $\mathbf{H} \cap \mathbf{K} = \{e\}$ and $\mathbf{H} + \mathbf{K} = \mathbf{G}$. As usual, we write in this case $\mathbf{G} = \mathbf{H} \oplus \mathbf{K}$. In particular there exists a *projection homomorphism* $\pi_{\mathbf{H}} \colon \mathbf{G} \to \mathbf{H}$ that is the identity in $\mathbf{H}$ and vanishes in $\mathbf{K}$.

The following lemma shows that one can deduce information about $\# \sum A$ by studying a subgroup and a projection.

Lemma 13. *Let $\mathbf{G} = \mathbf{H} \oplus \mathbf{K}$, and let C be a multiset contained in $\mathbf{G}$. Let $D = C \cap \mathbf{H}$, let $F = C \setminus D$, and let $E = \pi_{\mathbf{K}}(F)$. Then*

$$\# \sum C \geqslant \# \sum D \cdot \# \sum E.$$

Proof. This is [3, Lemma 2.8], but we give a short proof for completeness. Let $y \in \sum E$. Then by definition of E, $x + y \in \sum F$ for some $x \in \mathbf{H}$. Furthermore

$$x + y + \sum D \subseteq (x + y + \mathbf{H}) \cap \left(\sum F + \sum D \right) = (y + \mathbf{H}) \cap \sum C.$$

Hence, for each $y \in \sum E \subseteq \mathbf{K}$, the coset $y + \mathbf{H}$ contains at least $\# \sum D$ points of $\sum C$, and the claim follows since these cosets are disjoint. $\square$

Let us now cite Theorem 3 as Peng states and proves it (see [4, Theorem 2]) as it actually tells us something about non-valid sets as well.

Lemma 14. *Let $p \in \mathbb{P}$ and let A be a multiset of size $2p-1$ contained in $\mathbb{Z}_p^2$. Assume that $0 \notin A$ and each non-trivial subgroup of $\mathbb{Z}_p^2$ contains at most p elements of A. Then $\sum A = \mathbb{Z}_p^2$.*

Actually Lemma 14 is no stronger than Theorem 3 but follows from it, see Lemma 18. Lemma 14 lets us prove the case $k = p-2$ of Conjecture 4 easily.

Lemma 15. *Let $p \in \mathbb{P}$ and let A be a valid multiset contained in $\mathbb{Z}_p^2$ with $|A| = 2p-2$. Then $\# \sum A \geqslant p^2 - 1$.*

Proof. Assume, contrary to the claim, that there are two distinct points $z, w \in \mathbb{Z}_p^2 \setminus \sum A$. Let B be the multiset A joined by $z-w$. This multiset satisfies the hypothesis of Lemma 14 but $z \notin \sum A + \{0, z-w\} = \sum B$, a contradiction. □

The following simple lemma will be the main tool in our inductive argument.

Lemma 16. *Let $\mathbf{G}$ be an abelian group and let $A \subseteq \mathbf{G}$. Then for every $m \geqslant 2$,*

$$\#(A + \{0, z, 2z, \dots, mz\}) - \#(A + \{0, z\}) \leqslant (m-1)(\#(A + \{0, z\}) - \#A).$$

Proof. Here

$$\begin{aligned}
\#(A + \{0, z, 2z, \dots, mz\}) &= \# \left(\bigcup_{i=0}^{m} (A + iz) \right) \\
&= \# \left(A \cup \bigcup_{i=1}^{m} ((A + iz) \setminus (A + (i-1)z)) \right) \\
&\leqslant \#A + \sum_{i=1}^{m} \#((A + iz) \setminus (A + (i-1)z)) \\
&= \#A + m \cdot \#((A + z) \setminus A),
\end{aligned}$$

and the claim follows after a rearrangement. □

For the proof of Theorem 12 we need the following direct consequence of the matroid union theorem (see for instance [7, Theorem 2 in Section 8.4]).

Lemma 17. *Let V be a vector space and let A be a multiset contained in V. If $|U \cap A| \leqslant k \cdot \dim U$ for every subspace $U \leqslant V$, then A may be partitioned into k sets $A_1, \dots, A_k$ where every A_i is linearly independent.*

3 Proof of Theorem 5

Let A be a valid multiset of size $p+k$ contained in $\mathbb{Z}_p^2$. As the case $k = p-2$ was handled in Lemma 15, we can assume that $0 \leqslant k \leqslant p-3$. For $z \in A$, write $A_z = A \cap \langle z \rangle$ and

$A_z^{\mathsf{c}} = A \setminus A_z$. We will induct on k but let us first handle the case $|A_z| \geqslant k+1$ for some $z \in A$ as in [3]. In this case $|A_z^{\mathsf{c}}| = |A| - |A_z| \leqslant p-1$, and by Lemmas 13 and 1

$$\#\sum A \geqslant (|A_z|+1)(|A_z^{\mathsf{c}}|+1) = (|A_z|+1)(|A|-|A_z|+1) = |A_z|(|A|-|A_z|) + |A| + 1$$

which attains its minimum when $|A_z|$ is minimal or maximal. For both $|A_z| = k+1$ and $|A_z| = p-1$, the right hand side is $(k+2)p$ and the claim follows.

Hence we can assume from now on that, for every $z \in A$, $|A_z| \leqslant k$. Notice that as in [3] this in particular resolves the case $k=0$.

At this point our proof diverges from that in [3], where the authors modified the set A to contain more elements in some subgroup by replacing $2l$ points $x_i, z-x_i \in A$, $i = 1, \ldots, l$ by l copies of z. Here we instead set up an induction on k (recall that $|A| = p+k$). As we already handled the case $k=0$, we can proceed directly to the induction step.

Assume, contrary to the claim, that $\#\sum A \leqslant (k+2)p-1$. Notice that, for every $z \in A$,

$$\sum A = \sum(A \setminus \{z\}) + \{0, z\},$$

and here by the induction hypothesis $\#\sum(A \setminus \{z\}) \geqslant (k+1)p$. Hence

$$\#\left(\sum(A \setminus \{z\}) + \{0,z\}\right) - \#\sum(A \setminus \{z\}) \leqslant (k+2)p - 1 - (k+1)p = p-1. \tag{1}$$

Let B be the multiset which consists of A and $p-k-2$ additional copies of z, so that $|B| = 2p-2$. Since $|A \cap \langle z \rangle| \leqslant k$, B is valid, so that by Lemma 15, $\#\sum B \geqslant p^2 - 1$. On the other hand, applying Lemma 16 and recalling (1), one gets

$$\begin{aligned}
\#\sum B &= \#\left(\sum(A \setminus \{z\}) + \{0, z, 2z, \ldots, (p-k-1)z\}\right) \\
&\leqslant \left(\#\sum(A \setminus \{z\}) + \{0,z\}\right) \\
&\qquad + (p-k-2)\left(\#\left(\sum(A \setminus \{z\}) + \{0,z\}\right) - \#\sum(A \setminus \{z\})\right) \\
&\leqslant \#\sum A + (p-k-2)(p-1) \leqslant (k+2)p - 1 + (p-k-2)(p-1) \\
&= p^2 - p + k + 1 \leqslant p^2 - 2
\end{aligned}$$

since $k \leqslant p-3$. Hence we have arrived to a contradiction so one must indeed have $\#\sum A \geqslant (k+2)p$. □

4 Proofs of Theorems 9 and 12

To prove Theorem 9, we need a few lemmas. The first lemma shows that a stronger statement follows from Conjecture 8, in particular Lemma 14 follows from Theorem 3.

Lemma 18. *Conjecture 8 implies the following: Let p be an odd prime and let m be a positive integer. Let A be a multiset contained in $\mathbb{Z}_p^m$ for which*

$$|A \cap \mathbf{H}| \leqslant p \dim \mathbf{H} \tag{2}$$

for every subgroup $\mathbf{H} \leqslant \mathbb{Z}_p^m$. If $|A| \geqslant mp-1$, then $\sum A = \mathbb{Z}_p^m$.

Proof. Let us induct on m. Case $m = 1$ follows from Lemma 1, so we can move to the induction step. We can clearly assume that $|A| = mp - 1$. Let $\mathbf{H}$ be a maximal subgroup of $\mathbb{Z}_p^m$ for which equality holds in (2) (possibly $\mathbf{H} = \{0\}$), and write $\mathbb{Z}_p^m = \mathbf{H} \oplus \mathbf{K}$. If $\pi_{\mathbf{K}}(A \setminus \mathbf{H})$ were not a valid multiset, there would exist a non-trivial subgroup $K_1 \leqslant K$ such that $|(A \setminus \mathbf{H}) \cap (\mathbf{H} \oplus \mathbf{K_1})| \geqslant p \cdot \dim \mathbf{K_1}$ and consequently

$$\begin{aligned} A \cap (\mathbf{H} \oplus \mathbf{K_1}) &= |A \cap \mathbf{H}| + |(A \setminus \mathbf{H}) \cap (\mathbf{H} \oplus \mathbf{K_1})| \\ &\geqslant p \cdot (\dim \mathbf{H} + \dim \mathbf{K_1}) = p \cdot (\dim \mathbf{H} \oplus \mathbf{K_1}) \end{aligned}$$

which contradicts the maximality of $\mathbf{H}$.

Hence $\pi_{\mathbf{K}}(A \setminus \mathbf{H})$ is a valid multiset contained in $\mathbf{K}$ with size

$$|A| - |A \cap \mathbf{H}| = mp - 1 - p \cdot \dim \mathbf{H} = p \cdot \dim \mathbf{K} - 1,$$

so that $\sum \pi_{\mathbf{K}}(A \setminus \mathbf{H}) = \mathbf{K}$ by the assumed Conjecture 8. Furthermore $A \cap \mathbf{H}$ has size $p \cdot \dim \mathbf{H}$ and dimension smaller than m, and thus by induction hypothesis $\sum (A \cap \mathbf{H}) = \mathbf{H}$, and the claim follows from Lemma 13. $\square$

Theorem 12 follows now immediately:

Proof of Theorem 12. Conjecture 8 implies Conjecture 11 by Lemma 18 and Conjecture 11 implies Conjecture 8 by Lemma 17. $\square$

The following lemma follows from the previous lemma as Lemma 15 follows from Lemma 14.

Lemma 19. *Conjecture 8 implies the following: Let p be an odd prime, let m be a positive integer, and let A be a valid multiset contained in $\mathbb{Z}_p^m$ with $|A| = mp - 2$. Then $\# \sum A \geqslant p^m - 1$.*

The third and fourth lemmas will let us show that we can assume that our multiset A is not too concentrated in any subgroup (recall that also in the proof of Theorem 5 we first showed that we can assume that $|A \cap \langle z \rangle| \leqslant k$ for every $z \in A$).

Lemma 20. *Let $m \geqslant 2$ and $\mathbb{Z}_p^m = \mathbf{H} \oplus \mathbf{K}$, where $0 < \dim \mathbf{H} < m$. If A is a valid multiset contained in $\mathbb{Z}_p^m$ with*

$$|A \setminus \mathbf{H}| \leqslant p \cdot \dim \mathbf{K} - 1, \tag{3}$$

then there exists a non-trivial subgroup $\mathbf{K}' \lneq \mathbb{Z}_p^m$ such that, writing $\mathbb{Z}_p^m = \mathbf{H}' \oplus \mathbf{K}'$, $\pi_{\mathbf{K}'}(A \setminus \mathbf{H}')$ is a valid multiset contained in $\mathbf{K}'$.

Proof. If $\pi_{\mathbf{K}}(A \setminus \mathbf{H})$ is valid, the claim follows immediately. Otherwise there is a non-trivial subgroup $\mathbf{K}_1 \leqslant \mathbf{K}$ such that

$$|(A \setminus \mathbf{H}) \cap (\mathbf{H} \oplus \mathbf{K}_1)| \geqslant p \cdot \dim \mathbf{K}_1. \tag{4}$$

Let $\mathbf{K}_1$ be maximal such subgroup and $\mathbf{K} = \mathbf{K}_1 \oplus \mathbf{K}_2$. The bounds (4) and (3) together imply that $\mathbf{K}_1 \lneq \mathbf{K}$ so that $\mathbf{K}_2 \neq \{0\}$.

If $\pi_{\mathbf{K}_2}(A \setminus (\mathbf{H} \oplus \mathbf{K}_1))$ is valid, the claim follows with $\mathbf{K}' = \mathbf{K}_2$ and $\mathbf{H}' = \mathbf{H} \oplus \mathbf{K}_1$. Otherwise there exists a non-trivial subgroup $\mathbf{K}_3 \leqslant \mathbf{K}_2$ such that

$$|(A \setminus (\mathbf{H} \oplus \mathbf{K}_1)) \cap (\mathbf{H} \oplus \mathbf{K}_1 \oplus \mathbf{K}_3)| \geqslant p \cdot \dim \mathbf{K}_3.$$

Combining with (4) gives

$$|(A \setminus \mathbf{H}) \cap (\mathbf{H} \oplus \mathbf{K}_1 \oplus \mathbf{K}_3)| \geqslant p \cdot (\dim \mathbf{K}_1 + \dim \mathbf{K}_3) = p \cdot \dim(\mathbf{K}_1 \oplus \mathbf{K}_3)$$

which contradicts the maximality of $\mathbf{K}_1$. $\square$

Lemma 21. *Let p be an odd prime and define $f\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{N}$ by putting for each $q \geqslant 0$ and $0 \leqslant k \leqslant p-1$,*

$$f(qp+k) = \begin{cases} k+1 & \text{if } q = 0 \text{ and } 0 \leqslant k \leqslant p-1; \\ (k+2)p^q & \text{if } q \geqslant 1 \text{ and } 0 \leqslant k \leqslant p-3; \\ p^{q+1} - 1 & \text{if } q \geqslant 0 \text{ and } k = p-2; \\ p^{q+1} & \text{if } q \geqslant 0 \text{ and } k = p-1;. \end{cases}$$

Then for every $n_1, n_2 \in \mathbb{Z}_{\geqslant 0}$ one has $f(n_1) \cdot f(n_2) \geqslant f(n_1 + n_2)$.

Proof. Write $n_i = q_i p + k_i$. First note that

$$f(q_1p+p-2)f(p-2) = (p^{q_1+1}-1)(p-1) \geqslant (p-2)(p^{q_1+1}-1) = f(q_1p+p-2+p-2),$$

so we can assume that if $k_1 = k_2 = p-2$ then $q_2 \neq 0$. One has

$$\frac{f(qp+k)}{f(qp+k-1)} = \begin{cases} \frac{k+1}{k} = 1 + \frac{1}{k} & \text{if } q = 0 \text{ and } 0 < k \leqslant p-1; \\ \frac{k+2}{k+1} = 1 + \frac{1}{k+1} & \text{if } q \geqslant 1 \text{ and } 0 \leqslant k \leqslant p-3; \\ \frac{p^{q+1}-1}{p^q(p-1)} = 1 + \frac{p^q-1}{p^q(p-1)} & \text{if } q \geqslant 1 \text{ and } k = p-2; \\ \frac{p^{q+1}}{p^{q+1}-1} = 1 + \frac{1}{p^{q+1}-1} & \text{if } q \geqslant 0 \text{ and } k = p-1. \end{cases}$$

From this we see that for every $q_1, q_2 \geqslant 0$ and $0 \leqslant k_1 \leqslant k_2 \leqslant p-2$ (with $q_1p+k_1 > 0$ and not $(k_1, k_2, q_2) = (p-2, p-2, 0)$) one has

$$\frac{f(q_1p+k_1)}{f(q_1p+k_1-1)} \geqslant \frac{f(q_2p+k_2+1)}{f(q_2p+k_2)}$$
$$\iff f(q_1p+k_1)f(q_2p+k_2) \geqslant f(q_1p+k_1-1)f(q_2p+k_2+1). \tag{5}$$

Applying (5) repeatedly to $f(n_1)f(n_2)$, we can assume that either $k_1 = p-1$ or $k_2 = p-1$, and consequently, by symmetry, that $k_1 = p-1$. The proof can then be completed by an easy case-by-case check according to the value of k_2. $\square$

Proof of Theorem 9. Let f be as in Lemma 21. Conjecture 7 is equivalent to the claim that for every $m \geqslant 1$ and any valid multiset A contained in $\mathbb{Z}_p^m$ one has $\#\sum A \geqslant f(|A|)$ (since the latter claim holds if $m = 1$ or if $|A| < p$ by Lemmas 1 and 13).

Let us induct on m. Lemma 1 takes care of the case $m = 1$, so we can move to the induction step. Let $|A| = qp + k$. We will induct also on k but let us first consider the case that for some non-trivial subgroup $\mathbf{H} \lneq \mathbb{Z}_p^m$ one has $|A \setminus \mathbf{H}| \leqslant p \cdot (m - \dim \mathbf{H}) - 1$. In this case Lemma 20 implies that there exists a non-trivial subgroup $\mathbf{K}' \lneq \mathbb{Z}_p^m$ such that, writing $\mathbb{Z}_p^m = \mathbf{H}' \oplus \mathbf{K}'$, $\pi_{\mathbf{K}'}(A \setminus \mathbf{H}')$ is a valid multiset contained in $\mathbf{K}'$. Since $\dim \mathbf{H}', \dim \mathbf{K}' < m$, by the induction hypothesis

$$\#\sum \pi_{\mathbf{K}'}(A \setminus \mathbf{H}') \geqslant f(|A \setminus \mathbf{H}'|) \quad \text{and} \quad \#\sum (A \cap \mathbf{H}') \geqslant f(|A \cap \mathbf{H}'|).$$

Hence by Lemmas 13 and 21

$$\#\sum A \geqslant f(|A \setminus \mathbf{H}'|) \cdot f(|A \cap \mathbf{H}'|) \geqslant f(|A|)$$

and the claim follows.

Thus we can assume that

$$|A \setminus \mathbf{H}| \geqslant p \cdot (m - \dim \mathbf{H}) \tag{6}$$

for every non-trivial subgroup $\mathbf{H} \lneq \mathbb{Z}_p^m$. In particular taking $\mathbf{H} = \langle z \rangle$ for some $z \in \mathbb{Z}_p^m$, we see that we can assume that $q = m - 1$, so that $|A| = (m-1)p + k$. By this and (6) we can thus assume that for every subgroup $\mathbf{H} \leqslant \mathbb{Z}_p^m$ one has

$$|A \cap \mathbf{H}| = |A| - |A \setminus \mathbf{H}| \leqslant (m-1)p + k - p \cdot (m - \dim \mathbf{H}) = p \cdot (\dim \mathbf{H} - 1) + k. \tag{7}$$

Taking here $\mathbf{H} = \langle z \rangle$ for some $z \in A$, we see that we can assume that $k > 0$. On the other hand, Lemma 19 lets us assume that $k \leqslant p - 3$.

From now on the proof proceeds almost exactly as the proof of Theorem 5, so let us induct also on k and assume, contrary to the claim, that $\#\sum A \leqslant (k+2)p^{m-1} - 1$. Recall that, for every $z \in A$,

$$\sum A = \sum (A \setminus \{z\}) + \{0, z\},$$

and here by the induction hypothesis $\#\sum (A \setminus \{z\}) \geqslant (k+1)p^{m-1}$. Hence

$$\#\left(\sum (A \setminus \{z\}) + \{0, z\}\right) - \#\sum (A \setminus \{z\}) \leqslant (k+2)p^{m-1} - 1 - (k+1)p^{m-1} = p^{m-1} - 1. \tag{8}$$

Let B be the multiset which consists of A and $p - k - 2$ additional copies of z, so that $|B| = mp - 2$. Since (7) holds for every non-trivial subgroup $\mathbf{H}$, B is valid, so that, by Lemma 19, $\#\sum B \geqslant p^m - 1$. On the other hand, applying Lemma 16 recalling (8), one gets

$$\begin{aligned}
\#\sum B &= \#\left(\sum (A \setminus \{z\}) + \{0, z, 2z, \dots, (p-k-1)z\}\right) \\
&\leqslant \#\sum A + (p-k-2)\left(\#\sum A - \#\sum (A \setminus \{z\})\right) \\
&\leqslant (k+2)p^{m-1} - 1 + (p-k-2)(p^{m-1} - 1) = p^m - p + k + 1 \leqslant p^m - 2
\end{aligned}$$

since $k \leqslant p - 3$. $\square$

The proof actually tells us that if, for some $M \geqslant 2$, Conjecture 8 holds for every $m \leqslant M$, then so does Conjecture 7. In particular, as was shown already in Section 3, Theorem 3 implies Theorem 5.

Acknowledgements

The author would like to thank the referee for useful comments, in particular for suggesting the addition of Theorem 12 (and related Conjecture 11 and Lemma 17).

References

[1] N. Alon, N. Linial, and R. Meshulam. Additive bases of vector spaces over prime fields. *J. Combin. Theory Ser. A*, 57(2):203–210, 1991.

[2] F. Jaeger, N. Linial, C. Payan, and M. Tarsi. Group connectivity of graphs—a non-homogeneous analogue of nowhere-zero flow properties. *J. Combin. Theory Ser. B*, 56(2):165–182, 1992.

[3] G. Martin, A. Peilloux, and E. B. Wong. Lower bounds for sumsets of multisets in $\mathbb{Z}_p^2$. *Integers*, to appear, pre-print available at arXiv:1107.4392v3.

[4] C. Peng. Addition theorems in elementary abelian groups. I. *J. Number Theory*, 27:46–57, 1987.

[5] C. Peng. Addition theorems in elementary abelian groups. II. *J. Number Theory*, 27:58–62, 1987.

[6] T. Tao and V. H. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, paperback edition, 2010.

[7] D. J. A. Welsh. *Matroid Theory*. L.M.S. Monographs. Academic Press Inc. Ltd., London, 1976.