Directed cycles with zero weight in $\mathbb{Z}_p^k$

Shoham Letzter[*] Natasha Morrison[†]

June 15, 2023

Abstract

For a finite abelian group A, define $f(A)$ to be the minimum integer such that for every complete digraph Γ on f vertices and every map $w : E(\Gamma) \to A$, there exists a directed cycle C in Γ such that $\sum_{e \in E(C)} w(e) = 0$. The study of $f(A)$ was initiated by Alon and Krivelevich (2021). In this article, we prove that $f(\mathbb{Z}_p^k) = O(pk(\log k)^2)$, where p is prime, with an improved bound of $O(k \log k)$ when $p = 2$. These bounds are tight up to a factor which is polylogarithmic in k.

1 Introduction

Generally speaking, the area of 'zero-sum' Ramsey theory concerns the study of objects weighted by the elements of a group, and when a substructure of total weight zero can be found. This dates back to 1960 and the celebrated Erdős–Ginzburg–Ziv [9] theorem which asserts that, for every integer $m \geq 2$, every sequence of $2m - 1$ elements in $\mathbb{Z}_m$ contains a subsequence of m elements that sum to 0. Since then, a wide variety of interesting variations have been studied; see Caro [6] for a survey of this topic.

For a finite abelian group A, define $f(A)$ to be the minimum integer such that for every complete digraph Γ on f vertices and every map $w : E(\Gamma) \to A$, there exists a directed cycle C in Γ such that $\sum_{e \in E(C)} w(e) = 0$. We call w a *weighting* of $E(\Gamma)$ and C a *w-zero-sum cycle*. When it is

[*] Department of Mathematics, University College London, Gower Street, London WC1E 6BT, UK. Email: s.letzter@ucl.ac.uk. Research supported by the Royal Society.

[†] Department of Mathematics and Mathematical Statistics, University of Victoria, 3800 Finnerty Road, Victoria, BC V8P 5C2, Canada. Email: nmorrison@uvic.ca. Research supported by NSERC Discovery Grant RGPIN-2021-02511.

clear which map w is being referred to, we will simply call C a *zero-sum cycle*. The question of determining $f(A)$ arose in a paper by Alon and Krivelevich [3] from 2021, who showed that for any integer q, if $f = f(\mathbb{Z}_q)$, then every K_{2f}-minor contains a cycle whose length is divisible by q (see the end of Section 3 in [3]). In fact, they proved more generally that for every subcubic graph H and positive integer q, there is a (finite) number $g = g(H, q)$ such that every K_g-minor contains a subdivision of H where each edge is replaced by a path of length which is divisible by q. Their bound on $g(H, q)$ was improved by Das, Draganić, and Steiner [7] who showed that $g(H, q) = O(|H|q)$, which is tight up to a constant factor.

Alon and Krivelevich [3] proved that $f(\mathbb{Z}_p) \leq 2p-1$, for p prime, and $f(\mathbb{Z}_q) = O(q \log q)$, for any integer $q \geq 2$. This result was improved upon and generalised by Mészáros and Steiner [10], who showed that $f(A) \leq 8|A|$ for any finite abelian group A, and in particular, that $f(\mathbb{Z}_p) \leq \frac{3}{2}p$ for prime p. Recently, this was improved upon by Berendsohn, Boyadzhiyska, and Kozma [5], and independently by Akrami, Chaudhury, Garg, Mehlhorn, and Mehta [1], who gave a beautifully slick proof to show that $f(B) \leq 2|B|-1$, where B is any finite (not necessarily Abelian) group. In forthcoming work of Campbell, Hendrey, Gollin, and Steiner, this is improved to a tight bound $f(\mathbb{Z}_q) = q + 1$ for every positive integer q.

Our main result improves upon the results in [1, 5, 10] to give a sublinear bound in $|A|$ when $A = \mathbb{Z}_p^k$ and p is a prime.

Theorem 1.1. *Let p be a prime and let $k \geq 1$ be an integer. Then*

$$f(\mathbb{Z}_p^k) \leq 600p \cdot k(\log_2(10k))^2.$$

We obtain a stronger result when $p = 2$, which is tight up to an $O(\log k)$ factor.

Theorem 1.2. *Let $k \geq 2$ be an integer. Then*

$$f(\mathbb{Z}_2^k) \leq 600k \log_2(2k).$$

A simple construction shows that $f(\mathbb{Z}_p^k) \geq (p-1)k$. Indeed, let $e_1, \ldots, e_k$ be the elementary basis elements of $\mathbb{Z}_p^k$. Consider the complete digraph Γ on $(p-1)k$ vertices, let $\{V_1, \ldots, V_k\}$ be an equipartition of $V(\Gamma)$, and label a directed edge xy by e_i whenever $x \in V_i$. It is easy to see that, with this weighting, there are no zero-sum cycles in Γ, as every cycle contains at most $p-1$ edges labelled e_i, for every $i \in [k]$. Thus $f(\mathbb{Z}_p^k) \geq (p-1)k$, as claimed. The results in Theorem 1.1 and Theorem 1.2 are thus tight up to a factor which is polylogarithmic in k.

This problem was independently investigated by Sidorenko and Steiner (unpublished) who showed $f(\mathbb{Z}_p^k) = O(pk^2 \log k)$ with an improved bound of $O(k^2)$ when $p = 2$.

The proofs of Theorems 1.1 and 1.2 follow the same strategy. In Lemma 4.1 below, we show that $f(\mathbb{Z}_p^k)$ can be bounded by an expression involving the largest size of a 'reduced' multisubset of $\mathbb{Z}_p^k$. This parameter is bounded in general for $\mathbb{Z}_p^k$ in Theorem 2.1, and a better bound is easily obtained when $p = 2$, as we will see in Observation 2.2.

In Section 2 we introduce the notion of reduced sets, make some preliminary observations and prove Theorem 2.1. Then, in Section 3, we show how we can use particular subgraphs, called 'gadgets', collectively to find zero-sum cycles. These allow us to deduce information about the weights on our digraph and, in Section 4, to prove Lemma 4.1. This in turn completes the proofs of Theorem 1.1 and Theorem 1.2. We conclude in Section 5 with some discussion about bounding the largest size of a 'reduced' multisubset of $\mathbb{Z}_p^k$ and other directions for future research.

1.1 Notation and conventions

All logarithms will be taken in base 2.

For sets A and B, we write $A + B := \{a + b : a \in A, b \in B\}$.

We will often treat collections S of elements of $\mathbb{Z}_p^k$ as collections of vectors in $\mathbb{F}_p^k$. As such, we will refer to the span or dimension of such a collection S. We will use 0 to denote the identity element of any group A.

We will often be working with multisets. In order to minimise confusion for the reader, we now define some notation for multiset operations that will be used throughout.

Given an abelian group A and a multiset S, write $S \,\widetilde{\subseteq}\, A$ to denote that S is a multiset with the property that $s \in A$ for every $s \in S$. Write $T \subseteq S$ to denote that T is a (multi)subset of S. We will write $S - T$ to denote the multiset obtained from S by removing one copy of each element of the multiset T.

Define the *multiset union* of sets $A_1, \dots, A_k$, denoted by $\widetilde{\bigcup}_{i\in[k]} A_i$ to be the multiset whose elements can be partitioned into $A_1, \dots, A_k$. If $a_1, \dots, a_k$ are elements of A, write $\widetilde{\bigcup}_{i\in[k]} a_i$ to denote the multiset containing $\{a_1, \dots, a_k\}$.

2 Reduced sets

Given a multiset S with elements in an abelian group A, the *sumset* of S, denoted $\Sigma(S)$, is defined to be the set of all subset sums of S, namely

$$\Sigma(S) := \left\{ \sum_{t\in T} t : T \subseteq S \right\},$$

where the sum of elements in the empty set is defined to be zero, and hence $|\Sigma(\emptyset)| = 1$. In particular, $0 \in \Sigma(S)$ for every multiset $S \mathrel{\widetilde{\subseteq}} A$. Say that S is *reduced* if $|\Sigma(S)| > |\Sigma(S - \{s\})|$, for all $s \in S$. Let $h_p(k)$ be the size of a largest reduced multiset in $\mathbb{Z}_p^k$.

The main result in this section is a general upper bound on $h_p(k)$.

Theorem 2.1. *$h_p(k) \leq (p-1)(\log k + 1) \cdot k$.*

This shows that the lower bound $h_p(k) \geq k(p-1)$, from Observation 2.2 (viii) below, is tight up to a $\log k + 1$ factor.

We begin by gathering together some straightforward observations about reduced multisets.

Observation 2.2. *Let A be a finite abelian group and let $S \mathrel{\widetilde{\subseteq}} A$.*

(i) *If S is reduced, then the identity element $0 \in A$ is not an element of S.*

(ii) *There exists $S' \subseteq S$ such that S' is reduced and $\Sigma(S) = \Sigma(S')$.*

(iii) *If S is reduced, then every $T \subseteq S$ is reduced.*

(iv) *Suppose that S is reduced and $A = \mathbb{Z}_p^k$. Let $f : \mathbb{Z}_p^k \to \mathbb{Z}_p^k$ be a non-degenerate linear map. Then $f(S) := \{f(s) : s \in S\}$ is reduced.*

(v) *$h_p(k) + h_p(\ell) \leq h_p(k + \ell)$.*

(vi) *$h_p(1) = p - 1$.*

(vii) *A multisubset of $\mathbb{Z}_2^k$ is reduced if and only if it is linearly independent. In particular, $h_2(k) = k$.*

(viii) *$h_p(k) \geq k(p - 1)$.*

Proof. For (i), observe that $\Sigma(S) = \Sigma(S - \{0\})$.

For (ii), if S is not reduced then sequentially remove elements t such that $\Sigma(S - \{t\}) = \Sigma(S)$ until a reduced multisubset S' remains.

For (iii), if $T \subseteq S$ and $\Sigma(T) = \Sigma(T - \{t\})$ for some $t \in T$, then $\Sigma(S - \{t\}) = \Sigma(S - T) + \Sigma(T - \{t\}) = \Sigma(S - T) + \Sigma(T) = \Sigma(S)$, contradicting the assumption that S is reduced. Thus $|\Sigma(T)| > |\Sigma(T - \{t\})|$ for every $t \in T$, showing that T is reduced.

Item (iv) follows from the observation that $\Sigma(f(T)) = f(\Sigma(T))$ for every multisubset T of $\mathbb{Z}_p^k$.

For (v), let $S \mathrel{\widetilde{\subseteq}} \mathbb{Z}_p^k$ and $T \mathrel{\widetilde{\subseteq}} \mathbb{Z}_p^\ell$ be reduced with respective sizes of $h_p(k)$ and $h_p(\ell)$. Define $R := \{(s, 0) : s \in S\} \cup \{(0, t) : t \in T\} \subseteq \mathbb{Z}_k^p \times \mathbb{Z}_p^\ell$. It is easy to see that R is a reduced multiset in $\mathbb{Z}_p^k \times \mathbb{Z}_p^\ell \cong \mathbb{Z}_p^{k+\ell}$ of size $h_p(k) + h_p(\ell)$, showing $h_p(k + \ell) \geq h_p(k) + h_p(\ell)$.

For (vi), suppose that $S \mathrel{\widetilde{\subseteq}} \mathbb{Z}_p$ is reduced. Enumerate the elements of S as $\{s_1, \dots, s_k\}$. By (iii), $\{s_1, \dots, s_i\}$ is reduced for all $i \in [k]$, and so

$$|\Sigma(S)| = \big|\Sigma(\{s_1, \dots, s_k\})\big| \geq \big|\Sigma(\{s_1, \dots, s_{k-1}\})\big| + 1 \geq \ldots \geq |\Sigma(\emptyset)| + k = k + 1.$$

Since, trivially, $|\Sigma(S)| \leq p$, we have $|S| = k \leq p - 1$.

Thinking of $\mathbb{Z}_2^k$ as a vector space over $\mathbb{F}_2$, the sumset of a set $S \subseteq \mathbb{Z}_2^k$ is the same as the span of S. Item (vii) follows.

Finally, for (viii), notice that the multiset consisting of $p - 1$ copies of each elementary basis element of $\mathbb{Z}_p^k$ is a reduced multiset of size $k(p - 1)$. □

2.1 Proof of Theorem 2.1

Before giving the proof, we will state two preliminary results. The first is the Matroid Packing theorem, due to Edmonds [8]. Before stating it, we will define matroids and some relevant notions.

A *matroid* is a pair $(V, \mathcal{I})$, where V is a set and $\mathcal{I}$ is a non-empty family of subsets of V, referred to as *independent sets*, which is closed under taking subsets, and satisfies the following *augmentation property*: if $I, I' \in \mathcal{I}$ satisfy $|I| > |I'|$, then there exists $x \in I \setminus I'$ such that $I' \cup \{x\} \in \mathcal{I}$. Define the *rank* of a subset $S \subseteq V$, denoted $\mathrm{rank}(S)$, as the size of a largest independent set contained in S. A *base* is an independent set of size $\mathrm{rank}(V)$.

Theorem 2.3 (Matroid Packing theorem, Edmonds [8])**.** *A matroid $M = (V, \mathcal{I})$ contains t pairwise disjoint bases if and only if every $T \subseteq V$ satisfies $|V| - |T| \geq t \cdot (\mathrm{rank}(V) - \mathrm{rank}(T))$.*

We draw the following almost immediate conclusion regarding disjoint bases in multisubsets of vector spaces. Given a (multi)subset S of a vector space, define $\mathrm{rank}(S) := \dim(\mathrm{span}(S))$.

Corollary 2.4. *Let U be a finite dimensional vector space and let $S \mathrel{\widetilde{\subseteq}} U$ have full rank. Then S contains t pairwise disjoint bases of U if and only if every multisubset $T \subseteq S$ satisfies $|S| - |T| \geq t \cdot (\mathrm{rank}(S) - \mathrm{rank}(T))$.*

Proof. We define a matroid $M = (V, \mathcal{I})$, as follows. For each element $s \in S$ of multiplicity m_s, add the elements $(s, 1), \dots, (s, m_s)$ to V and say that each of these elements *corresponds* to s. So V is a set (rather than a multiset) which emulates S. Define $\mathcal{I}$ to be the subsets of V with the property that the collection of vectors they correspond to in S is linearly independent. It is easy to check that M is indeed a matroid and that a base in M corresponds to a basis of U. It follows from Theorem 2.3 that M contains t pairwise disjoint bases of U if and only if $|V| - |T| \geq t \cdot (\mathrm{rank}(V) - \mathrm{rank}(T))$ for every $T \subseteq V$. This proves the statement, as $|V| = |S|$ and $\mathrm{rank}(V) = \mathrm{rank}(S)$. □

We will also need the following result of Alon, Linial, and Meshulam [4].

Theorem 2.5 (Proposition 3.1 in [4])**.** *Let $S_1, \dots, S_\ell$ be ℓ bases of the vector space $\mathbb{Z}_p^k$, where $\ell \geq (p-1)\log k + p - 2$, and let $S = \widetilde{\bigcup}_{i\in\ell} S_i$. Then $\Sigma(S) = \mathbb{Z}_p^k$.*

We now have all the pieces we need to prove Theorem 2.1, restated here.

Theorem 2.1. *$h_p(k) \leq (p-1)(\log k + 1) \cdot k$.*

Proof of Theorem 2.1. We will prove the statement by induction on k. Notice that it follows directly from Observation 2.2 (vi) if $k = 1$, so take $k \geq 2$ and assume that the statement holds for all $k' \in [k-1]$. Write $\ell_k = (p-1)(\log k + 1)$. Suppose that $T \widetilde{\subseteq} \mathbb{Z}_p^k$ is reduced and $|T| > \ell_k \cdot k$. Let $S \subseteq T$ such that $|S| = \ell_k \cdot k$. By Observation 2.2 (iii), S is reduced. We will show that $\Sigma(S) = \mathbb{Z}_p^k$, contradicting the assumption that T is reduced.

By induction, every $S' \widetilde{\subsetneq} S$ with $r := \operatorname{rank}(S') < k$ satisfies $|S'| \leq \ell_r \cdot r \leq \ell_k \cdot \operatorname{rank}(S')$, because S' is a reduced multisubset of an r-dimensional subspace of $\mathbb{Z}_p^k$ (using Observation 2.2 (iii) and (iv)). In particular, we have $\operatorname{rank}(S) = k$, and if $S' \widetilde{\subsetneq} S$ satisfies $\operatorname{rank}(S') < k$, then

$$\frac{|S| - |S'|}{\operatorname{rank}(S) - \operatorname{rank}(S')} \geq \frac{\ell_k \cdot k - \ell_k \cdot \operatorname{rank}(S')}{k - \operatorname{rank}(S')} \geq \ell_k.$$

It thus follows from Corollary 2.4 that S is the multiset union of ℓ_k pairwise disjoint bases. By Theorem 2.5, this implies that $\Sigma(S) = \mathbb{Z}_p^k$, as suffices to complete the result. □

3 Gadgets

Let Γ be a complete digraph, A be an abelian group, and let $w : E(\Gamma) \to A$. We will write uv to denote the directed edge from u to v.

Definition 3.1 (Gadgets)**.** Let u and v be distinct vertices in Γ. A *gadget* rooted at (u, v) is defined to be a pair g of paths P and Q directed from u to v. Let $u(g), v(g), P(g)$ and $Q(g)$ refer to u, v, P and Q, respectively.

Define the *vertex set* of g by $V(g) := V(P) \cup V(Q)$, and its *value* by $g^* := w(Q) - w(P)$, where the *weight* of a subdigraph $H \subseteq \Gamma$ is $w(H) := \sum_{e\in E(H)} w(H)$.

The next lemma provides a simple condition for a collection of gadgets to yield a zero-sum cycle in Γ. The point is that if the collection of values is 'rich' enough, then by passing through the gadgets, choosing either P or Q at each one, we are able to use the collection to generate a zero-sum cycle.

Lemma 3.2. *Let Γ be a complete digraph whose edges have weights in the abelian group A. Let $\mathcal{G}$ be a family of pairwise vertex-disjoint gadgets in Γ. Let $S := \widetilde{\bigcup}_{g\in\mathcal{G}} g^*$. If $\Sigma(S) = A$, then Γ contains a zero-sum cycle.*

Proof. Let $\mathcal{G} = \{g_1, \ldots, g_t\}$, where $g_i = g_i(u_i, v_i)$. For ease of notation, define $u_{t+1} := u_1$. Let $I \subseteq [t]$ be a set of indices such that the following holds, where $(u_i, v_i, P_i, Q_i) := (u(g_i), v(g_i), P(g_i), Q(g_i))$.

$$\sum_{i\in I} g_i^* = -\sum_{i=1}^{t} w(P_i) - \sum_{i=1}^{t} w(v_i u_{i+1}),$$

Such a set exists as $\Sigma(S) = A$. Using $\sum_{i\in I} g_i^* = \sum_{i\in I}\big(w(Q_i) - w(P_i)\big)$ and rearranging yields

$$0 = \sum_{i\in I} w(Q_i) + \sum_{i\notin I} w(P_i) + \sum_{i=1}^{t} w(v_i u_{i+1}). \tag{1}$$

Now let C be the directed cycle $R_1 v_1 u_2 R_2 v_2 u_2 \ldots R_t v_t u_1$, where

$$R_i := \begin{cases} Q_i & i \in I \\ P_i & i \notin I. \end{cases}$$

Note that $\sum_{e\in C} w(e)$ is precisely the right hand side of the expression (1), and so C is a zero-sum cycle. □

The following lemma allows us to modify a weighting to ensure all out-edges from a particular vertex receive weight 0, whilst preserving properties of the weighting. This idea was also used by Mészáros and Steiner [10].

Lemma 3.3. *Let Γ be a complete digraph, let A be an abelian group, and let $w : E(\Gamma) \to A$. Suppose that there are no zero-sum cycles with respect to w, and let $v_0 \in V(\Gamma)$. Then there exists $w' : E(\Gamma) \to A$ such that: $w'(v_0 u) = 0$ for every $u \in V(\Gamma)$; there are no zero-sum cycles with respect to w'; and every gadget g in Γ has the same value with respect to both w and w'.*

Proof. Let $u \in V(\Gamma)$ and let $\alpha \in A$. Define $f_{u,\alpha}(w) : E(\Gamma) \to A$ as follows

$$f_{u,\alpha}(w)(e) := \begin{cases} w(e) & \text{if } e \in \Gamma \setminus \{u\} \\ w(e) + \alpha & \text{if } e = uv \text{ for some } v \in V(\Gamma) \\ w(e) - \alpha & \text{if } e = vu \text{ for some } v \in V(\Gamma). \end{cases}$$

It is easy to check that $w(C) = f_{u,\alpha}(w)(C)$ for every directed cycle C. Similarly, if P and Q are two directed paths with the same start and end points, then $w(P) - w(Q) = f_{u,\alpha}(w)(P) -$

$f_{u,\alpha}(w)(Q)$. It follows that there are no w-zero-sum cycles if and only if there are no $f_{u,\alpha}(w)$-zero-sum cycles, and that the value of any gadget g is the same with respect to w and $f_{u,\alpha}(w)$. Let $u_1, \ldots, u_{n-1}$ be an arbitrary ordering of $V(\Gamma) \setminus \{v_0\}$, and let $\alpha_i := w(v_0 u_i)$. Let

$$w' := f_{u_{n-1},\alpha_{n-1}} \circ \ldots \circ f_{u_1,\alpha_1}(w).$$

Notice that $w'(v_0 u_i) = w(v_0 u_i) - \alpha_i = 0$, for every $i \in [n-1]$; equivalently, $w'(v_0 u) = 0$ for every $u \in V(\Gamma) \setminus \{v_0\}$. By the above discussion, there are no w'-zero-sum cycles, and every gadget in Γ has the same value with respect to w' and w. □

We now introduce some notation and terminology that we will use to refer to particular families of gadgets.

Definition 3.4. Let Γ be a complete digraph, let p be prime, let k be a positive integer and let $w : E(\Gamma) \to \mathbb{Z}_p^k$. A collection of families of gadgets $\mathcal{G}_1, \ldots, \mathcal{G}_t$ in Γ is said to be *useful* if it satisfies the following properties:

(P1) The collections $\mathcal{G}_1, \ldots, \mathcal{G}_t$ are pairwise disjoint, and $V(g_1) \cap V(g_2) = \emptyset$ for all distinct $g_1, g_2 \in \bigcup_{i=1}^t \mathcal{G}_i$;

(P2) $|V(g)| = 3$ for all $g \in \bigcup_{i=1}^t \mathcal{G}_i$;

(P3) defining the multiset $U_i := \widetilde{\bigcup}_{g \in \mathcal{G}_i} g^*$, the sequence $|\Sigma(U_1)|, \ldots, |\Sigma(U_t)|$ is as late as possible in the lexicographic ordering[1] on $\mathbb{R}^t$ among sequences satisfying (P1) and (P2).

We say that a useful family is also *reduced* if the following holds.

(P4) U_i is a reduced multiset, for every $i \in [t]$.

By Observation 2.2 (ii), for every useful family of gadgets $\mathcal{G}_1, \ldots, \mathcal{G}_t$ in Γ there is a useful and reduced family $\mathcal{G}'_1, \ldots, \mathcal{G}'_t$ with $\Sigma(U'_i) = \Sigma(U_i)$ (where $U'_i := \widetilde{\bigcup}_{g \in \mathcal{G}'_i} g^*$).

For each $i \in [t]$ define

$$V_i := \bigcup_{g \in \mathcal{G}_i} V(g), \qquad B_i := \{x \in \mathbb{Z}_p^k : x + \Sigma(U_i) = \Sigma(U_i)\}. \tag{2}$$

Observe that the sets V_i are pairwise disjoint, that B_i is a subgroup of $\mathbb{Z}_p^k$, and $B_i \subseteq \Sigma(U_i)$ (using $0 \in \Sigma(U_i)$). Let $d_i := \dim(B_i)$, where B_i is treated as a vector subspace of the vector space $\mathbb{Z}_p^k$.

[1] Recall that $a_1, a_2, \ldots, a_t < b_1, b_2, \ldots, b_t$ in the *lexicographic ordering* on $\mathbb{R}^t$ if there is some $i \in [t]$ such that $a_j = b_j$ for all $j < i$ and $a_i > b_i$.

The next lemma shows that once we have 'pulled out' a useful collection of gadgets, we have control over the weights of many of the edges in the digraph.

Lemma 3.5. *Let Γ be a complete digraph, let p be prime and let $w : E(\Gamma) \to \mathbb{Z}_p^k$ be a labelling with no zero-sum cycles. Let $\mathcal{G}_1, \dots, \mathcal{G}_t$ be a useful collection of families of gadgets in Γ, and define V_i, B_i, d_i as above. Suppose that $v_0 \in V(\Gamma) \setminus \bigcup_{j=1}^{i} V_j$ satisfies $w(v_0u) = 0$ for every vertex $u \neq v_0$. Then:*

(i) *For each $i \in [t]$, every edge $e \in \Gamma \setminus (\{v_0\} \cup \bigcup_{j=1}^{i} V_j)$ satisfies $w(e) \in B_i$.*

(ii) *We have $k > d_1 > \ldots > d_t$.*

Proof. Suppose that $e = uv$ violates (i). Then the gadget g with $V(g) = \{u, v, v_0\}$, $P(g) = v_0v$ and $Q(g) = v_0uv$ has value

$$w(Q(g)) - w(P(g)) = w(v_0uv) - w(v_0v) = w(uv),$$

which is not in B_i. By definition of B_i, this shows $|\Sigma(U_i \cup \{g^*\})| > |\Sigma(U_i)|$. Thus, taking $\mathcal{G}_i' := \mathcal{G}_i \cup \{g\}$, we reach a contradiction to property (P3).

Define for convenience $B_0 = \mathbb{Z}_p^k$ and $d_0 = k$, and let $i \in [t-1]$. For (ii), by (i) we have $U_i \subseteq B_{i-1}$ (this holds trivially for $i = 1$). It follows that $B_i \subseteq \Sigma(U_i) \subseteq B_{i-1}$ (where the first inclusion holds by definition of B_i and the second holds because B_{i-1} is a group), and thus $d_i \leq d_{i-1}$. Suppose, towards a contradiction, that $d_i = d_{i-1}$. Then $B_{i-1} = B_i$ and, by $B_i \subseteq \Sigma(U_i) \subseteq B_{i-1}$, we get $B_i = \Sigma(U_i)$. But now applying Lemma 3.2 with the subgraph $\Gamma[V_i]$, whose edges are weighted by elements of $\Sigma(U_i)$, yields a zero-sum cycle. This contradicts our assumption that Γ contains no zero-sum cycles. Hence $d_{i-1} > d_i$, proving (ii). □

4 Zero-sum cycles and reduced sets

Given a prime p and integer k, recall that let $f(\mathbb{Z}_p^k)$ is the minimum f such that every complete digraph on f vertices, whose edges have weights in $\mathbb{Z}_p^k$, has a zero-sum cycle. For ease of notation, write $f_p(k) := f(\mathbb{Z}_p^k)$. Recall that $h_p(k)$ is the maximum size of a reduced multiset in $\mathbb{Z}_p^k$.

The main result of this section is the following lemma, which together with Theorem 2.1 yields Theorem 1.1.

Lemma 4.1. *Let p be a prime and let $k \geq 1$ be integer. Then*

$$f_p(k) \leq 60 \log(2k) \cdot h_p(10k). \tag{3}$$

Before proving Lemma 4.1, we show how it implies Theorem 1.1 and Theorem 1.2.

Proof of Theorem 1.1. By Lemma 4.1 and Theorem 2.1, we have

$$\begin{aligned} f_p(k) &\leq 60\log(2k)\cdot h_p(10k) \\ &\leq 60\log(2k)\cdot(p-1)(\log(10k)+1)\cdot(10k) \\ &\leq 600p\cdot k(\log(10k))^2, \end{aligned}$$

as required. □

Proof of Theorem 1.2. By Observation 2.2(vii) and Theorem 2.1, we have

$$f_2(k) \leq 60\log(2k)\cdot h_2(10k) \leq 60\log(2k)\cdot 10k = 600\cdot k\log(2k).$$

as required. □

Proof of Lemma 4.1. We prove the lemma by induction on k. Notice that, by [3, 10], $f_p(1) \leq 2p$, and by Observation 2.2(vii) we have $60\cdot h_p(10) \geq 60\cdot h_p(1) = 60(p-1)$, so the statement holds for $k=1$.

Let Γ be a complete digraph on n vertices that does not contain a zero-sum cycle. Our goal is to show that $n \leq 60\log(2k)\cdot h_p(10k)$. Suppose to the contrary that $n \geq 60\log(2k)\cdot h_p(10k)$.

Let $t := \lceil 10\log k\rceil$, let $\mathcal{G}_1,\ldots,\mathcal{G}_t$ be a useful and reduced collection of families of gadgets in Γ, and define V_i, U_i, B_i, d_i as in (P3) and (2). As U_i is reduced, $|U_i| \leq h_p(k)$ and thus $|V_i| \leq 3h_p(k)$ (by (P2)), showing $|\bigcup_{i\in[t]} V_i| \leq 3t\cdot h_p(k) \leq 3\cdot(10\log k+1)\cdot h_p(k) \leq n-1$, with room to spare, showing that such $\mathcal{G}_1,\ldots,\mathcal{G}_t$ can indeed be defined.

Let v_0 be a vertex not in $\bigcup_{i\in[t]} V_i$. Apply Lemma 3.3 to obtain $w' : E(\Gamma) \to \mathbb{Z}_p^k$ such that: $w'(v_0u) = 0$ for every vertex $u \neq v_0$; there are no w'-zero-sum cycles; and every gadget in Γ has the same weight with respect to w and w'. In particular, a sequence of gadgets is useful with respect to w if and only if it is useful with respect to w', and similarly for useful and reduced sequences. Altogether, this means that we may and will replace w by w', allowing us to assume $w(v_0u) = 0$ for $u \in V(\Gamma)\setminus\{v_0\}$.

Hence we can apply Lemma 3.5 to obtain:

(i) For each $i \in [t]$, every edge e in $\Gamma\setminus(\bigcup_{j=1}^{i} V_j \cup \{v_0\})$ satisfies $w(e) \in B_i$.

(ii) We have $k > d_1 > \ldots > d_t$. In particular, $0 < d_i < k$ for $i \in [t-1]$.

Claim 4.2. *There exists $m \in [3,t]$ such that $k - d_m \leq 10(k - d_{m-2})$.*

Proof. Suppose $k - d_m > 10(k - d_{m-2})$ for all $m \in [3, t]$. Then, as $1 \le k - d_1 \le k - d_2 \le k$,

$$k \ge k - d_t > 10^{t/2-1}(k - d_2) \ge 10^{t/2-1} \ge k^5/10 > k,$$

a contradiction. □

Fix m as in Claim 4.2. Our next goal is to show that there is a small set Z of vertices from Γ such that the weights of all edges not touching Z lie in a proper subgroup of $\mathbb{Z}_p^k$. We can then apply our inductive hypothesis to bound $|V(\Gamma \setminus Z)|$.

For each $i \in [t]$, let $\tau_i : \mathbb{Z}_p^k \to \mathbb{Z}_p^k/B_i$ be the natural map sending a to $a + B_i$ for $a \in \mathbb{Z}_p^k$. For a multisubset X of $\mathbb{Z}_p^k$, let $\tau_i(X) := \widetilde{\bigcup}_{x \in X} \tau_i(x)$.

For each $j \in [m-2]$, define $\mathcal{X}_j$ to be a minimal subset of $\mathcal{G}_j$ such that $X_j := \widetilde{\bigcup}_{g \in \mathcal{X}_j} g^*$ satisfies $\Sigma(\tau_m(X_j)) = \Sigma(\tau_m(U_j))$. Similarly, define $\mathcal{Y}_j$ to be a minimal set of gadgets in $\mathcal{G}_j$ such that $Y_j := \widetilde{\bigcup}_{g \in \mathcal{Y}_j} g^*$ satisfies $\Sigma(\tau_{m-1}(Y_j)) = \Sigma(\tau_{m-1}(U_j))$. Observe that X_j is reduced in $\mathbb{Z}_p^k/B_m$ and Y_j is reduced in $\mathbb{Z}_p^k/B_{m-1}$. In particular,

$$|\mathcal{X}_j| \le h_p(k - d_m), \qquad |\mathcal{Y}_j| \le h_p(k - d_{m-1}). \tag{4}$$

Notice that, by definition of $\mathcal{X}_j$ and $\mathcal{Y}_j$,

$$\Sigma(U_j) \subseteq \Sigma(X_j \,\widetilde{\cup}\, U_m), \qquad \Sigma(U_j) \subseteq \Sigma(Y_j \,\widetilde{\cup}\, U_{m-1}). \tag{5}$$

Indeed, if $u \in \Sigma(U_j)$ then there exist $x \in \Sigma(X_j)$ and $v \in B_m$ such that $u = x + v$, showing $\Sigma(U_j) \subseteq \Sigma(X_j) + B_m \subseteq \Sigma(X_j) + \Sigma(U_m) = \Sigma(X_j \,\widetilde{\cup}\, U_m)$. A similar argument holds for Y_j. Define

$$Z := \{v_0\} \cup \bigcup_{i \in [m-2]} \big(V(\mathcal{X}_i) \cup V(\mathcal{Y}_i)\big), \tag{6}$$

where $V(\mathcal{X}_i)$ denotes the union of vertex sets of gadgets in $\mathcal{X}_i$, and similarly for $V(\mathcal{Y}_i)$.

Claim 4.3. $|Z| \le 6m \cdot h_p(k - d_m)$.

Proof. We have

$$\begin{aligned}
|Z| &\le 3 \sum_{j \in [m-2]} \big(|\mathcal{X}_j| + |\mathcal{Y}_j|\big) + 1 \\
&\le 3 \sum_{j \in [m-2]} \big(h_p(k - d_m) + h_p(k - d_{m-1})\big) + 1 \\
&\le 6m \cdot h_p(k - d_m),
\end{aligned}$$

where for the first inequality we used that gadgets consist of three vertices, for the second we used (4), and for the third we used (ii) and the monotonicity of $h_p(\cdot)$. □

Claim 4.4. *Every edge $e \in E(\Gamma \setminus Z)$ satisfies $w(e) \in B_{m-2}$.*

Proof. Suppose there exists an edge xy with no endpoint in Z such that $w(xy) \notin B_{m-2}$. Define, for convenience, $V_\infty := V(\Gamma) \setminus \bigcup_{i \in [m]} V_i$. Let g be the v_0y-gadget with $V(g) = \{v_0, x, y\}$, $P(g) = v_0y$, and $Q(g) = v_0xy$. Its value is

$$g^* = w(Q(g)) - w(P(g)) = w(v_0xy) - w(v_0y) = w(v_0x) + w(xy) - w(v_0y) = w(xy),$$

using $w(v_0u) = 0$ for $u \neq v_0$. As B_{m-2} is a subgroup and $w(xy) \notin B_{m-2}$, it follows that $g^* \notin B_{m-2}$.

We will show that it is possible to find a collection of families of vertex-disjoint gadgets $\mathcal{G}'_1, \dots, \mathcal{G}'_{m-3}, \mathcal{G}''_{m-2}$ in Γ with corresponding sets $U'_1, \dots, U'_{m-3}, U''_{m-2}$ (where $U'_i := \widetilde{\bigcup}_{g \in \mathcal{G}'_i} g^*$ and similarly for U''_{m-2}) satisfying properties (P1) and (P2) with the additional conditions

(C1) $|\Sigma(U'_j)| = |\Sigma(U_j)|$ for all $j \in [m-3]$, and

(C2) $|\Sigma(U''_{m-2})| > |\Sigma(U_{m-2})|$.

This will imply that $\mathcal{G}_1, \dots, \mathcal{G}_t$ does not satisfy property (P3), as we are able to obtain a sequence that is later in the lexicographic ordering, a contradiction.

Suppose $x \in V_a$ and $y \in V_b$, where $a, b \in [m] \cup \{\infty\}$ and $a \leq b$. We need an ad-hoc piece of notation; let m', m'' satisfy $\{m', m''\} = \{m-1, m\}$ and, if $b \in \{m-1, m\}$ but $a \notin \{m-1, m\}$, then $m' \neq b$. We define $\mathcal{G}'_1, \dots, \mathcal{G}'_{m-2}$ as follows.

$$\mathcal{G}'_j := \begin{cases} \mathcal{G}_j & \text{if } j \in [m-2] \setminus \{a, b\}, \\ \mathcal{X}_j \cup \mathcal{Y}_j \cup \mathcal{G}_{m'} & \text{if } j \in [m-2] \text{ and } j = a \\ \mathcal{X}_j \cup \mathcal{Y}_j \cup \mathcal{G}_{m''} & \text{if } j \in [m-2] \text{ and } j = b > a. \end{cases}$$

Notice that the gadgets in each $\mathcal{G}_j$, with $j \in [m-2]$, are pairwise vertex-disjoint. Indeed, this holds because $V(\mathcal{X}_j), V(\mathcal{Y}_j) \subseteq V_j$ and the sets V_j are pairwise vertex-disjoint. Similarly, any two gadgets from distinct sets $\mathcal{G}'_j$ are vertex-disjoint. Additionally, the gadgets in $\bigcup_{j \in [m-2]} \mathcal{G}'_j$ are vertex-disjoint from $(V_a \cup V_b \cup V_\infty) \setminus Z$ (if $b \in \{m-1, m\}$ and $a \notin \{m-1, m\}$ this follows from the choice of m'), and hence they are vertex-disjoint from $V(g) = \{x, y, v_0\}$. Altogether, writing $\mathcal{G}''_{m-2} := \mathcal{G}'_{m-2} \cup \{g\}$, this shows that $\mathcal{G}'_1, \dots, \mathcal{G}'_{m-3}, \mathcal{G}''_{m-2}$ satisfies (P1). Property (P2) holds by construction.

Next, we claim that $\Sigma(U_j') = \Sigma(U_j)$ for $j \in [m-2]$. This is clear when $j \neq a, b$. Suppose now that $\mathcal{G}_j' = \mathcal{X}_j \cup \mathcal{Y}_j \cup \mathcal{G}_{m-1}$. Because $\mathcal{X}_j, \mathcal{Y}_j \subseteq U_j$ and by Lemma 3.5 (i), which shows $U_{m-1} \subseteq \Sigma(U_j)$, we have $\sum(U_j') \subseteq \Sigma(U_j)$. Now, if $u \in \Sigma(U_j)$, then by choice of $\mathcal{Y}_j$ there exists $w \in \Sigma(\mathcal{Y}_j)$ such that $u + B_{m-1} = w + B_{m-1}$. Equivalently, $u - w \in B_{m-1}$ and thus $u - w \in \Sigma(U_{m-1})$. This implies that $u \in \Sigma(\mathcal{Y}_j \mathbin{\tilde{\cup}} U_{m-1}) \subseteq \Sigma(U_j')$, as claimed. An analogous argument shows the same when $\mathcal{G}_j' = \mathcal{X}_j \cup \mathcal{Y}_j \cup \mathcal{G}_m$. This proves (C1).

Notice that, by (5), we have $\Sigma(U_{m-2}) \subseteq \Sigma(U_{m-2}')$. This, the definition of B_{m-2}, and that $g^* \notin B_{m-2}$ show that

$$\Sigma(U_{m-2}'') = \Sigma(U_{m-2}' \mathbin{\tilde{\cup}} \{g^*\}) \supseteq \Sigma(U_{m-2} \mathbin{\tilde{\cup}} \{g^*\}) \supsetneq \Sigma(U_{m-2}).$$

Thus (C2) holds. □

Claims 4.3 and 4.4 show that, by removing at most $6m \cdot h_p(k - d_m)$ vertices from Γ, we can obtain a graph whose edge weights are contained in a subgroup isomorphic to $\mathbb{Z}_p^{d_{m-2}}$. But as we presumed Γ has no zero-sum cycle, then $|V(\Gamma \setminus Z)| \leq f_p(d_{m-2})$. Hence

$$\begin{aligned}
n = |V(\Gamma)| &= |V(Z)| + |V(\Gamma \setminus Z)| \\
&\leq 6m \cdot h_p(k - d_m) + f_p(d_{m-2}) \\
&\leq 60 \log k \cdot h_p\big(10(k - d_{m-2})\big) + 60 \log(2d_{m-2}) \cdot h_p(10 d_{m-2}) \\
&\leq 60 \log(2k) \cdot h_p\big(10(k - d_{m-2})\big) + 60 \log(2k) \cdot h_p(10 d_{m-2}) \\
&\leq 60 \log(2k) \cdot h_p(10k).
\end{aligned}$$

where in the third line we used the bounds $m \leq 10 \log k$ and $k - d_m \leq 10(k - d_{m-2})$ and the monotonicity of $h_p(\cdot)$, as well as the induction hypothesis on $f_p(\cdot)$ (using $d_{m-2} \leq k - 1$; see (ii)), and in the last line we applied Observation 2.2(v). □

5 A few concluding remarks

Our main result shows $f(\mathbb{Z}_p^k) = O(pk(\log k)^2)$ when p is prime, with a better bound of $O(k \log k)$ when $p = 2$. This is tight up to a factor which is polylogarithmic in k, due to the easy lower bound $f(\mathbb{Z}_p^k) \geq (p-1)k$. It would be nice to close the gap between these upper and lower bound.

Question 5.1. *Is it true that $f(\mathbb{Z}_p^k) = O(pk)$?*

It would also be interesting to determine whether similar bounds hold when p is not prime.

Lemma 4.1 provides a bound on $f_p(k)$ in terms of $h_p(k)$. In light of this, one way to improve Theorem 1.1 could be to improve our understanding of $h_p(k)$. Given that we know (see Observation 2.2 (vi)) that $h_p(1) = p - 1$, a next step in this direction could be to determine $h_p(2)$. Theorem 2.1 give $h_p(2) \leq 4(p - 1)$. To this end, we can prove the following.

Lemma 5.2. *Let $p \geq 7$ be prime. Then $h_p(2) < \frac{5}{2}(p - 1)$.*

For completeness, we provide a proof in Appendix A. However, we do not think that this bound is best possible.

Conjecture 5.3. *Let p be prime. Then there exists a constant C such that $h_p(2) \leq 2p + C$.*

Acknowledgements

We are very grateful to Lisa Sauermann for coming up with Theorem 2.1 and for sharing her solution with us; this allowed us to both shorten our paper and improve our results. We would also like to thank Noga Alon for interesting discussions regarding reduced sets and for bringing [4] to our attention. These discussions took place during the workshop 'Recent advances in probabilistic and extremal combinatorics' which was held in Ascona, Switzerland on 7–12 August 2022. The first author would like to thank Asaf Shapira and Benny Sudakov, the workshop's organisers, for inviting her and giving her the opportunity to give a talk.

References

[1] H. Akrami, B. R. Chaudhury, J. Garg, K. Mehlhorn, and R. Mehta, *EFX allocations: Simplifications and improvements*, arXiv:2205.07638 (2022). 2

[2] N. Alon, *Combinatorial Nullstellensatz*, vol. 8, 1999, Recent trends in combinatorics (Mátraháza, 1995), pp. 7–29. MR 1684621 15

[3] N. Alon and M. Krivelevich, *Divisible subdivisions*, J. Graph Theory **98** (2021), no. 4, 623–629. 2, 10

[4] N. Alon, N. Linial, and R. Meshulam, *Additive bases of vector spaces over prime fields*, J. Combin. Theory Ser. A **57** (1991), no. 2, 203–210. 6, 14, 15

[5] B. A. Berendsohn, S. Boyadzhiyska, and L. Kozma, *Fixed-point cycles and EFX allocations*, arXiv:2201.08753 (2022). 2

[6] R. Caro, *Zero-sum problems – a survey*, Discr. Math. **152** (1996), 93–113. 1

[7] S. Das, N. Draganić, and R. Steiner, *Tight bounds for divisible subdivisions*, arXiv:2111.05723 (2021). 2

[8] J. Edmonds, *Lehman's Switching Game and a Theorem of Tutte and Nash-Williams*, J. Res. Natl. Bur. Stand. Sect. B **69B** (1965), 73–77. 5

[9] P. Erdős, A. Ginzburg, and A. Ziv, *Theorem in the additive number theory*, Bull. Res. Council Israel Sect. F **10F** (1961), no. 1, 41–43. 1

[10] T. Mészáros and R. Steiner, *Zero sum cycles in complete digraphs*, arXiv:2103.04359 (2021). 2, 7, 10

A Proof of Lemma 5.2

The next lemma is a rephrasing of Corollary 3.4 in [4]. We give a similar proof here.

Lemma A.1 (Corollary 3.4 in [4], rephrased)**.** *Let $v_i = (v_i(1), \dots, v_i(k))$ be a sequence of $k(p-1)$ vectors in $\mathbb{Z}_p^k$. Suppose that*

$$\sum_{(I_1,\dots,I_k)\in\mathcal{I}} \prod_{i\in[k]} \prod_{j\in I_i} v_j(i) \neq 0,$$

where $\mathcal{I}$ is the collection of equipartitions of $[k(p-1)]$. Then $\Sigma(\{v_1, \dots, v_{k(p-1)}\}) = \mathbb{Z}_p^k$.

Our proof uses Alon's Combinatorial Nullstellensatz.

Theorem A.2 (Alon's Combinatorial Nullstellensatz [2])**.** *Let $f \in \mathbb{F}[x_1, \dots, x_n]$ be a polynomial with coefficients in a field $\mathbb{F}$ such that the degree of f is $\sum_{i=1}^n t_i$ and the coefficient of $\prod_{i=1}^n x_i^{t_i}$ is non-zero. Let $S_1, \dots, S_n$ be subsets of $\mathbb{F}$ such that $|S_i| > t_i$ for all i. Then there exists $(s_1, \dots, s_n) \in S_1 \times \dots \times S_n$ such that $f(s_1, \dots, s_n) \neq 0$.*

Proof of Lemma A.1. Fix $w = (w(1), \dots, w(k)) \in \mathbb{Z}_p^k$. Set $m := k(p-1)$ and define

$$P(x_1, \dots, x_m) := \prod_{i=1}^{k} \left(\left(\sum_{j\in[m]} x_j v_j(i) - w(i) \right)^{p-1} - 1 \right). \tag{7}$$

Let S be the multiset $\widetilde{\bigcup}_{i\in[m]} v_i$. Observe that $P(y) \neq 0$ for some $y \in \{0,1\}^m$ if and only if $w \in \Sigma(S)$ (via Fermat's little theorem).

Thus, applying Theorem A.2, with $S_i = \{0,1\}$ and $t_i = 1$ for every $i \in [m]$, we see that if the coefficient of $\prod_{i\in[m]} x_i$ in P is non-zero then $w \in \Sigma(S)$. This coefficient is the coefficient of $\prod_{i\in[m]} x_i$ in $\prod_{i=1}^k \left(\sum_{j\in[m]} x_j v_j(i)\right)^{p-1}$. In order to obtain a term of $\prod_{i\in[m]} x_i$ from the latter product, from each factor we must select a distinct variable x_j in such a way that every $j \in [m]$ appears exactly once. Recalling that $\mathcal{I}$ is the collection of equipartitions $(I_1, \dots, I_k)$ of $[m]$

and thinking of I_i as indexing the variables obtained from the ith factor of the product, this coefficient is

$$\big((p-1)!\big)^k \sum_{(I_1,\ldots,I_k)\in\mathcal{I}} \prod_{i\in[k]} \prod_{j\in I_i} v_j(i)$$

As p is prime, $(p-1)! \neq 0$, and (7) holds if and only if the coefficient of $\prod_{i\in[m]} x_i$ in P is non-zero, which implies that $w \in \Sigma(S)$. Since w was an arbitrary element in $\mathbb{Z}_p^k$, this shows that (7) implies $\Sigma(S) = \mathbb{Z}_p^k$. □

We now prove Lemma 5.2, restated here.

Lemma 5.2. *Let $p \geq 7$ be prime. Then $h_p(2) < \frac{5}{2}(p-1)$.*

Proof of Lemma 5.2. Suppose that $T \mathrel{\widetilde{\subseteq}} \mathbb{Z}_p^2$ is reduced and $|T| \geq \frac{5}{2}(p-1)$. Let $S \subseteq T$ satisfy $|S| = \frac{5}{2}(p-1)$. By Observation 2.2 (iii), S is reduced. By Observation 2.2 (i), $(0,0) \notin S$. We will show that $\Sigma(S) = \mathbb{Z}_p^2$, which is a contradiction as this implies T is not reduced.

For $v \in \mathbb{Z}_p^2 \setminus \{(0,0)\}$, define $\langle v\rangle := \{\alpha v : \alpha \in \mathbb{Z}_p\}$. Choose v to minimise the size of the multiset intersection $\langle v\rangle \mathbin{\widetilde{\cap}} S$, defined to be the multisubset of S whose elements lie in $\langle v\rangle$. Notice that there are $p+1$ different 'directions', namely $(1,i)$ for $i \in [0,p-1]$ and $(0,1)$, and each $v \in \mathbb{Z}_p^k$ lies in $\langle d\rangle$ for exactly one direction d. Hence, as $|S| = \frac{5}{2}(p-1) < 3(p+1)$, we have $|\langle v\rangle \mathbin{\widetilde{\cap}} S| \leq 2$. Let $f : \mathbb{Z}_p^2 \to \mathbb{Z}_p^2$ be a non-degenerate linear transformation mapping v to $(0,1)$. Then, by Observation 2.2 (iv), $f(S)$ is a reduced multisubset of $\mathbb{Z}_p^2$ of size $\frac{5}{2}(p-1)$ with the property that $f(S)$ contains at most two vectors in direction $(0,1)$. That is, the multiset intersection $f(S) \mathbin{\widetilde{\cap}} \langle(0,1)\rangle$ has size at most 2.

Let S_0 be obtained from S by removing all elements in $\langle(0,1)\rangle$, and observe that $|S_0| \geq \frac{5}{2}(p-1) - 2 > p-1$. Let $v_1, \ldots, v_{p-1}$ be chosen as follows, defining $S_i := S_0 - \{v_1, \ldots, v_i\}$ once $v_1, \ldots, v_i$ are defined. Having chosen $v_1, \ldots, v_{i-1}$, choose $v_i \in S_{i-1}$ to maximise $|\langle v_i\rangle \mathbin{\widetilde{\cap}} S_{i-1}|$.

Write $S' := S - \{v_1, \ldots, v_{p-1}\}$ and define

$$m := \max_{v\in\mathbb{Z}_p^2\setminus\{(0,0)\}} |S' \mathbin{\widetilde{\cap}} \langle v\rangle|. \tag{8}$$

Claim A.3. $m \leq (p-1)/2$.

Proof. Let T be the set of elements $t \in \mathbb{Z}_p$ such that $\langle(1,t)\rangle \cap \{v_1, \ldots, v_{p-1}\} \neq \emptyset$. Then, by definition of $v_1, \ldots, v_{p-1}$, we have $|S' \mathbin{\widetilde{\cap}} \langle(1,t)\rangle| \in \{m-1, m\}$ for every $t \in T$.

If $|T| \leq 2$ then

$$2(p-1) \geq |S \mathbin{\widetilde{\cap}} \bigcup_{t\in T} \langle(1,t)\rangle| \geq p-1+m+m-1,$$

using that $|S \widetilde{\cap} \langle v\rangle| \leq p-1$ for $v \in \mathbb{Z}_p^2 \setminus \{(0,0)\}$ (which follows from Observation 2.2 (vi)). This implies that $m \leq p/2$, and thus $m \leq (p-1)/2$ because p is odd.

If $|T| \geq 3$ then

$$\frac{5}{2}(p-1) \geq \left|S \cap \widetilde{\bigcup}_{t\in T}\langle(1,t)\rangle\right| \geq p-1+m+(|T|-1)(m-1) \geq p+3m-3.$$

Thus $m \leq p/2+1/6$, implying that $m \leq (p-1)/2$, as p is odd. This completes the proof of Claim A.3. □

Claim A.4. *For every $t \in [0, p-1]$ there exists a multisubset $\widetilde{\bigcup}_{i\in[p-1+t]} v_i \subseteq S'$ such that*

$$\sum_{(I_1,I_2)\in\mathcal{I}_t} \prod_{i\in[2]} \prod_{j\in I_i} v_j(i) \neq 0, \tag{9}$$

where $\mathcal{I}_t$ is the collection of partitions (I_1, I_2) of $[p-1+t]$ such that $|I_1| = p-1$.

Proof. We prove the claim by induction on t. When $t = 0$, the expression in (9) is $\prod_{j\in I_1} v_j(1)$, which is non-zero as $v_1, \ldots, v_{p-1} \notin \langle(0,1)\rangle$.

Now suppose that $t \in [p-1]$ and $v_1, \ldots, v_{p-1+t-1}$ satisfy the requirements of the claim for $t-1$. Expanding the left-hand side of (9), with $v_{p-1+t} = (x, y)$, gives

$$xs_1 + ys_2,$$

where s_1 is a sum of terms depending on $v_1, \ldots, v_{p-1+t-1}$ and

$$s_2 = \sum_{(I_1,I_2)\in\mathcal{I}_{t-1}} \prod_{i\in[2]} \prod_{j\in I_i} v_j(i) \neq 0.$$

The multisubset of $S - \{v_1, \ldots, v_{p-1+t-1}\}$ of vectors (x, y) satisfying $xs_1 + ys_2 = 0$ is contained in a subspace of dimension 1. Because $m \leq (p-1)/2$ (by Claim A.3) and $|S - \{v_1, \ldots, v_{p-1+t-1}\}| \geq (p+1)/2$, we find that there is a suitable $v_{p-1+t} \in S - \{v_1, \ldots, v_{p-1+t-1}\}$. □

Lemma A.1 and Claim A.4 (with $t = p-1$) imply that there is a multisubset $S' \subseteq S$ of size $2(p-1)$ such that $\Sigma(S') = \mathbb{Z}_p^2$. As $S' \neq S$, this contradicts the assumption that S is reduced. □