STRUCTURE OF A SEQUENCE WITH PRESCRIBED ZERO-SUM SUBSEQUENCES: RANK TWO p-GROUPS

JOHN J. EBERT AND DAVID J. GRYNKIEWICZ

ABSTRACT. Let $G = (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$. Let $\mathrm{s}_{\le k}(G)$ be the smallest integer ℓ such that every sequence of ℓ terms from G, with repetition allowed, has a nonempty zero-sum subsequence with length at most k. It is known that $\mathrm{s}_{\le 2n-1-k}(G) = 2n-1+k$ for $k \in [0, n-1]$, with the structure of extremal sequences showing this bound tight determined when $k \in \{0, 1, n-1\}$, and for various special cases when $k \in [2, n-2]$. For the remaining values $k \in [2, n-2]$, the characterization of extremal sequences of length $2n-2+k$ avoiding a nonempty zero-sum of length at most $2n-1-k$ remained open in general, with it conjectured that they must all have the form $e_1^{[n-1]} \cdot e_2^{[n-1]} \cdot (e_1+e_2)^{[k]}$ for some basis (e_1, e_2) for G. Here $x^{[n]}$ denotes a sequence consisting of the term x repeated n times. In this paper, we establish this conjecture for all $k \in [2, n-2]$ when n is prime, which in view of other recent work, implies the conjectured structure for all rank two abelian groups.

1. Introduction

Let C_n denote a cyclic group of order n. Let G be a finite abelian group written additively. Then $G = C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus C_{n_r}$ with $1 < n_1 \mid n_2 \mid \ldots \mid n_r$, where $\mathrm{r}(G) = r$ is the rank of G, and $\exp(G) = n_r$ is the exponent of G. Following standardized notation [14] [15] [19] detailed in Section 2, let

$$S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$$

be a (finite and unordered) sequence of terms $g_i \in G$, written as a multiplicative string with repetition of terms allowed. Such a sequence is called *zero-sum* if the sum of its terms equals zero, $\sum_{i=1}^{\ell} g_i = 0$.

The Davenport Constant of G is the minimal integer $\mathrm{D}(G)$ such that any sequence of terms from G with length $|S| \ge \mathrm{D}(G)$ must have a nonempty zero-sum subsequence. It is one of the most well studied combinatorial invariants in Additive Number Theory, both of interest from a purely combinatorial perspective as well due to its relevance to the study of Factorization in structures from Commutative Algebra [14] [15]. Despite this, its exact value is known only for very limited groups, including p-groups and groups of rank at most 2. There, it is known that $\mathrm{D}(G) = 1 + \sum_{i=1}^{r}(n_i - 1)$ [25] [6] [26] [14]. In particular,

$$\mathrm{D}(C_n) = n, \quad \mathrm{D}(C_n \oplus C_n) = 2n-1, \qquad \text{and} \quad \mathrm{D}(C_p \oplus C_p \oplus C_p) = 3p-2,$$

for any $n \ge 1$ and any $p \ge 2$ prime, which we will use implicitly throughout the paper.

The standard proof of $\mathrm{D}(C_n \oplus C_n) = 2n-1$ [6] [26] [14] relies upon an inductive strategy, reducing the general case to when $n = p$ is prime, and making use of the axillary invariant $\eta(G)$, defined as the minimal integer such that any sequence of terms from G with length $|S| \geq \eta(G)$ must have a nonempty zero-sum subsequence of length at most $\exp(G)$. Later, Delorme, Ordaz and Quiroz introduced [5] the invariant $\mathrm{s}_{\leq k}(G)$ as a common generalization, defined as the minimal integer such that any sequence of terms from G with length $|S| \geq \mathrm{s}_{\leq k}(G)$ must have a nonempty zero-sum subsequence of length at most k. Indeed, when $k \geq \mathrm{D}(G)$, then $\mathrm{s}_{\leq k}(G) = \mathrm{D}(G)$, and when $k = \exp(G)$, then $\mathrm{s}_{\leq k}(G) = \eta(G)$. The relations between $\mathrm{s}_{\leq k}(G)$ and Coding Theory were explored by Cohen and Zemor in [4]. Other related works that deal with $\mathrm{s}_{\leq k}(G)$ can be found in [7] [31] [12]. The authors in [35] determined $\mathrm{s}_{\leq k}(G)$ for all finite abelian groups of rank two. Note, since $\mathrm{s}_{\leq k}(G) = \infty$ when $k < \exp(G)$, while $\mathrm{s}_{\leq k}(G) = \mathrm{s}_{\leq \mathrm{D}(G)}(G)$ for all $k \geq \mathrm{D}(G)$, that $\mathrm{s}_{\leq \mathrm{D}(G)-k}(G)$ is primarily of interest for $k \in [0, \mathrm{D}(G) - \exp(G)] = [0, m-1]$, meaning there is little need to consider values of k outside this range.

Theorem 1.1 ([35], Theorem 2)**.** *Let $G = C_m \oplus C_n$, where m and n are integers with $1 \leq m \mid n$, and let $k \in [0, m-1]$. Then*

$$\mathrm{s}_{\leq \mathrm{D}(G)-k}(G) = \mathrm{s}_{\leq n+m-1-k}(G) = \mathrm{D}(G) + k = m + n - 1 + k.$$

In particular, for $G = C_n \oplus C_n$, we know that

$$\mathrm{s}_{\leq \mathrm{D}(G)}(G) = \mathrm{D}(G) = 2n-1$$

and

$$\mathrm{s}_{\leq \exp(G)}(G) = \eta(G) = 3n-2.$$

It is then natural to ask which extremal sequences with terms from G show these bounds are tight, i.e., can those sequences S with length $|S| = \mathrm{D}(G)-1+k = 2n-2+k$ having no nonempty zero-sum subsequence of length at most $\mathrm{D}(G) - k = 2n-1-k$ be characterized? The cases $k \in \{0, 1, n-1\}$ were eventually resolved, with precise structure following due to the combined efforts from numerous papers [8] [9] [30] [20] [34] (See Conjecture 1.2 and Theorem 2.4). The resulting characterization has proved useful in various applications, e.g., [1] [2] [10] [13] [16] [17] [18] [24] [27] [28] [29] [32]. In [23], the problem of characterizing the extremal sequences for the invariant $\mathrm{s}_{\leq \mathrm{D}(G)-k}(C_n \oplus C_n)$ was proposed (for n prime), with the conjecture stated in [23] naturally extended to composite values of n in [21]. The conjectured structure, including the known cases for $k \in \{0, 1, n-1\}$, can be summarized as follows. Here $x^{[m]} = x \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} x$ denotes the sequence consisting of the element $x \in G$ repeated m times.

Conjecture 1.2 ([21], Conjecture 1.1)**.** *Let $n \geq 2$, let $G = C_n \oplus C_n$, let $k \in [0, n-1]$, and let S be a sequence of terms from G with length $|S| = \mathrm{D}(G) + k - 1 = 2n - 2 + k$ having no nonempty zero-sum subsequence of length at most $\mathrm{D}(G) - k = 2n - 1 - k$. Then there exists a basis (e_1, e_2) for G such that the following hold.*

1. *If $k = 0$, then $S \boldsymbol{\cdot} g$ satisfies the description given in Item 2, where $g = -\sigma(S)$.*

2. *If* $k = 1$*, then*
$$S = e_1^{[n-1]} \cdot \prod\nolimits_{i\in[1,n]}^{\bullet}(x_i e_1 + e_2),$$
for some $x_1, ..., x_n \in [0, n-1]$ *with* $x_1 + ... + x_n \equiv 1 \mod n$.
3. *If* $k \in [2, n-2]$*, then*
$$S = e_1^{[n-1]} \cdot e_2^{[n-1]} \cdot (e_1 + e_2)^{[k]}.$$
4. *If* $k = n-1$*, then*
$$e_1^{[n-1]} \cdot e_2^{[n-1]} \cdot (xe_1 + e_2)^{[k]}.$$
for some $x \in [1, n-1]$ *with* $\gcd(x, n) = 1$.

As already noted, Conjecture 1.2 is known for $k \in \{0, 1, n-1\}$, leaving the range $k \in [2, n-2]$ open. In this range, Conjecture 1.2 is known in various specialized cases, including when $k \leq \frac{2n+1}{3}$ with n a prime power [23] [21], as well as for several very specialized cases derived in [21]. In [21], it was shown how the Conjecture 1.2 holding when $n = p$ is prime would imply the general case. Specifically, the following was shown.

Theorem 1.3 ([21], Theorem 1.2)**.** *Let* $n, m \geq 2$ *and let* $k \in [0, mn-1]$ *with* $k = k_m n + k_n$*, where* $k_m \in [0, m-1]$ *and* $k_n \in [0, n-1]$*. Suppose Conjecture 1.2 holds for* k_n *in* $C_n \oplus C_n$ *and also for* k_m *in* $C_m \oplus C_m$*. Then Conjecture 1.2 holds for* k *in* $C_{mn} \oplus C_{mn}$*.*

In another recent paper [22], a more complicated description of all extremal sequences for a general rank two abelian group $G = C_m \oplus C_n$ was given and also shown to follow from Conjecture 1.2. Thus the complete characterization of all extremal sequences for the invariant $\mathrm{s}_{\leq \mathrm{D}(G)-k}(C_m \oplus C_n)$ is reduced to the case $\mathrm{s}_{\leq \mathrm{D}(G)-k}(C_p \oplus C_p)$ with p prime, where it remained open for $k \geq \frac{2p+2}{3}$. The goal of this paper is to resolve this case, establishing Item 3 in Conjecture 1.2 for all $k \in [2, n-2]$ when $n = p$ is prime, which as discussed, thereby implies Conjecture 1.2 holds without restriction, and gives the full characterization of all extremal sequences for a general rank two group. Specifically, we will show the following. As our proof does not rely on the main result from [23] and works equally well for all values of $k \in [2, p-2]$, this also gives a new proof of the cases $k \leq \frac{2p+1}{3}$ versus that from [23], though we will use arguments and lemmas from [23].

Theorem 1.4. *Let* $G = C_p \oplus C_p$ *with* p *a prime, let* $k \in [2, p-2]$ *be an integer, and let* S *be a sequence of terms from* G *with* $|S| = \mathrm{D}(G) + k - 1 = 2p - 2 + k$ *having no nonempty zero-sum subsequence of length at most* $\mathrm{D}(G) - k = 2p - 1 - k$*. Then there is a basis* (e_1, e_2) *for* G *such that*
$$S = e_1^{[p-1]} \cdot e_2^{[p-1]} \cdot (e_1 + e_2)^{[k]}.$$

The proof of Theorem 1.4 makes use of the characterization of extremal sequences for the Davenport Constant $\mathrm{D}(C_p \oplus C_p)$, some combinatorial arguments, and the arguments from *two*

separate proofs of Theorem 1.1 (when $m = n = p$ is prime): the original given in [35], as well as a new one derived here and accomplished by lifting to the group $C_p \oplus C_p \oplus C_p$. The latter is a variant on a strategy used for studying the Erdő-Ginzburg-Ziv Constant $\mathrm{s}(G)$ (see e.g. [14, Proposition 5.8.1]), defined as the minimal integer such that any sequence of terms from G with length $|S| \geq \mathrm{s}(G)$ must have a nonempty zero-sum subsequence of length exactly $\exp(G)$. We do not explicitly detail the argument separately, simply remarking that the proof of Lemma 3.5 easily modifies (when applied to an arbitrary sequence of length $|S| = 2p - 1 - k$ rather than a specialized one of length $|S| = 2p - 2 + k$) to show $\mathrm{s}_{\leq 2p-1-k}(C_p \oplus C_p) = 2p - 1 + k$.

2. Preliminaries

We will briefly present key concepts and notation used throughout this paper. Let $\mathbb{N}$ denote the set of positive integers and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $x, y \in \mathbb{R}$, we use $[x, y] = \{z \in \mathbb{Z} : x \leq z \leq y\}$ for the discrete interval between x and y. We use C_n to denote a cyclic group of order $n \geq 1$.

Following standardized notation for combinatorial sequences ([15] [14] [19]), for an abelian group G, we let $\mathcal{F}(G)$ be the free abelian monoid with basis G, whose elements consist of finite strings of terms from G, with the order of terms in the string disregarded. The elements $S \in \mathcal{F}(G)$ are called (finite and unordered) sequences S of terms from G, which have the form

$$S = g_1 \boldsymbol{\cdot} g_2 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell = \prod\nolimits^{\bullet}_{i \in [1,\ell]} g_i \in \mathcal{F}(S),$$

with the $g_i \in G$ the terms of the sequence S. For $k \geq 0$ and $g \in G$, we let $g^{[k]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{k}$ be the sequence with the term g repeating k times, with $g^{[0]}$ the empty sequence consisting of no terms. Letting

$$\mathsf{v}_g(S) = \{i \in [1, \ell] : \ g_i = g\} \geq 0$$

denote the multiplicity of the term g in S, we can then write S as

$$S = \prod\nolimits^{\bullet}_{g \in G} g^{[\mathsf{v}_g(S)]} \in \mathcal{F}(S).$$

If $\mathsf{v}_g(S) \geq 1$, then we say that S contains g. We call T a subsequence of S if $\mathsf{v}_g(T) \leq \mathsf{v}_g(S)$ for all $g \in G$. In such case, let $T^{[-1]} \boldsymbol{\cdot} S = S \boldsymbol{\cdot} T^{[-1]}$ denote the subsequence of S obtained by removing the terms of T, that is,

$$T^{[-1]} \boldsymbol{\cdot} S = \prod\nolimits^{\bullet}_{g \in G} g^{[\mathsf{v}_g(S) - \mathsf{v}_g(T)]} \in \mathcal{F}(S).$$

If $T \in \mathcal{F}(G)$ and $k \geq 1$, we let $T^{[k]} = \underbrace{T \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T}_{k}$ be the sequence consisting of T repeating k times. If $T^{[k]}$ is a subsequence of S, then $T^{[-k]} \boldsymbol{\cdot} S = S \boldsymbol{\cdot} T^{[-k]} = (T^{[k]})^{[-1]} \boldsymbol{\cdot} S$. We use the following notation:

- $|S| = \ell = \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0$ is the length of S,
- $\mathrm{h}(S) = \max\{\mathsf{v}_g(S) : \ g \in G\}$ is the maximum multiplicity of S,

- $\sigma(S) = \sum_{i=1}^{\ell} g_i = \sum_{g \in G} \mathsf{v}_g(S) g \in G$ is the sum of terms in S,
- $\Sigma(S) = \left\{ \sum_{i \in I} g_i : I \subseteq [1, \ell] \text{ with } 1 \le |I| \le \ell \right\}$ is the set of all subsums of S,
- $\Sigma_k(S) = \left\{ \sum_{i \in I} g_i : I \subseteq [1, \ell] \text{ with } |I| = k \right\}$ is the set of all length k subsums of S,
- $\Sigma_{\le k}(S) = \bigcup_{i \in [1,k]} \Sigma_i(S)$.

A sequence S is called

- *zero-sum free* if $0 \notin \Sigma(S)$,
- *a zero-sum sequence* if $\sigma(S) = 0$,
- *a minimal zero-sum sequence* if S is a nonempty zero-sum sequence that does not contain any proper, nonempty zero-sum subsequence.

If G and H are abelian groups. Then any map $\phi : G \to H$ can be extended to a map from $\mathcal{F}(G)$ to $\mathcal{F}(H)$ by setting

$$\phi(S) = \prod\nolimits^{\bullet}_{i \in [1,\ell]} \phi(g_i).$$

We will need the following results and definitions.

Definition 2.1. *Let G be an abelian group, let $S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \in \mathcal{F}(G)$ be a sequence of terms from G, where $\ell = |S|$, and let $k \ge 0$. Then*

$$N^k(S) := |\{I \subseteq [1, |S|] : \sum_{i \in I} g_i = 0 \text{ and } |I| = k\}|$$

denotes the number of zero-sum subsequence of S having length k.

Lemma 2.2 ([14], Proposition 5.5.8)**.** *Let p be a prime, let G be a finite abelian p-group, and let $S \in \mathcal{F}(G)$ be a sequence of terms from G. If $|S| \ge \mathrm{D}(G)$, then $\sum_{i=0}^{|S|} (-1)^i N^i(S) \equiv 0 \mod p$.*

Lemma 2.3 ([11], Lemma 2.7)**.** *Let G be an abelian group and let $S \in \mathcal{F}(G)$ be a zero-sum free sequence. Then*

$$|\Sigma(S)| \ge |S| + |\mathrm{supp}(S)| - 1.$$

Theorem 2.4 ([9, 30])**.** *Let $G = C_n \oplus C_n$ with $n \ge 2$ and let $S \in \mathcal{F}(G)$ be a minimal zero-sum sequence with length $\mathrm{D}(G) = 2n - 1$. Then S has the following form:*

$$S = e_1^{[n-1]} \boldsymbol{\cdot} \prod\nolimits^{\bullet}_{i \in [1,n]} (x_i e_1 + e_2)$$

with $x_i \in [0, n-1]$ and $\sum_{i=1}^{n} x_i \equiv 1 \mod n$, for some basis (e_1, e_2) for G.

Lemma 2.5 ([23], Lemma 15)**.** *Let $G = C_n \oplus C_n$, let $k \in [2, n-2]$, and let*

$$S = e_1^{[n-1]} \boldsymbol{\cdot} \prod\nolimits^{\bullet}_{i \in [1,n+k-1]} (x_i e_1 + e_2) \in \mathcal{F}(G),$$

where $x_i \in [1, n]$ for $i \in [1, n+k-1]$ and $\sum_{i=1}^{n} x_i \equiv 1 \mod n$. If $0 \notin \Sigma_{\le 2n-1-k}(S)$, then there exists a basis (e_1, f_2) for G, where $f_2 = x e_1 + e_2$ for some $x \in [1, n]$, such that

$$S = e_1^{[n-1]} \boldsymbol{\cdot} f_2^{[n-1]} \boldsymbol{\cdot} (e_1 + f_2)^{[k]}.$$

3. Proof of main result

To start determining the structure of $S \in \mathcal{F}(C_p^2)$ where $|S| = 2p-2+k$ and $0 \notin \Sigma_{\le \mathrm{D}(C_p^2)-k}(S)$, we will first show that S has a zero-sum subsequence of length $\mathrm{D}(C_p^2)$. To accomplish this, we will need the following two lemmas, which extend arguments used in [23, Lemma 14], themselves based on the original proof of Theorem 1.1 given in [35].

Lemma 3.1. *Let p be a prime and $k \in [1, p-1]$. Consider the family of k linear congruencies in the variables $x_1, \ldots, x_k$:*

$$\binom{2p-2+k}{t} + \binom{2k-2}{t}x_1 + \binom{2k-3}{t}x_2 + \ldots + \binom{k-1}{t}x_k \equiv 0 \mod p, \tag{1}$$

where $t \in [0, k-1]$. Then the unique solution to the above system is $x_s \equiv (-1)^{k-s+1}\binom{k}{k-s+1} \mod p$ for $s \in [1, k]$.

Proof. Let $X = (1, x_1, ..., x_k)^T$ and

$$A := \begin{pmatrix} \binom{2p-2+k}{0} & \binom{2k-2}{0} & \binom{2k-3}{0} & \cdots & \binom{k-1}{0} \\ \binom{2p-2+k}{1} & \binom{2k-2}{1} & \binom{2k-3}{1} & \cdots & \binom{k-1}{1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{2p-2+k}{k-1} & \binom{2k-2}{k-1} & \binom{2k-3}{k-1} & \cdots & \binom{k-1}{k-1} \end{pmatrix}.$$

From (1), we have

$$AX \equiv 0 \mod p.$$

Since $\binom{n}{0} = 1$, for any n, we have

$$A = A_{1,0} = \begin{pmatrix} \binom{2p-3+k}{0} & \binom{2k-3}{0} & \binom{2k-4}{0} & \cdots & \binom{k-2}{0} \\ \binom{2p-2+k}{1} & \binom{2k-2}{1} & \binom{2k-3}{1} & \cdots & \binom{k-1}{1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{2p-2+k}{k-1} & \binom{2k-2}{k-1} & \binom{2k-3}{k-1} & \cdots & \binom{k-1}{k-1} \end{pmatrix}.$$

By multiplying the first row of $A_{1,0}$ by -1, adding it to the second row of $A_{1,0}$ and using the property $\binom{n}{i} - \binom{n-1}{i-1} = \binom{n-1}{i}$, we obtain

$$A_{1,1} = \begin{pmatrix} \binom{2p-3+k}{0} & \binom{2k-3}{0} & \binom{2k-4}{0} & \cdots & \binom{k-2}{0} \\ \binom{2p-3+k}{1} & \binom{2k-3}{1} & \binom{2k-4}{1} & \cdots & \binom{k-2}{1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{2p-2+k}{k-1} & \binom{2k-2}{k-1} & \binom{2k-3}{k-1} & \cdots & \binom{k-1}{k-1} \end{pmatrix}.$$

We can repeat this process $k-1$ times. That is, for $0 \le i \le k-2$, multiply row $i+1$ of $A_{1,i}$ by -1 and add the result to row $i+2$ to construct $A_{1,i+1}$. Then

$$A_{1,k-1} = \begin{pmatrix} \binom{2p-3+k}{0} & \binom{2k-3}{0} & \binom{2k-4}{0} & \cdots & \binom{k-2}{0} \\ \binom{2p-3+k}{1} & \binom{2k-3}{1} & \binom{2k-4}{1} & \cdots & \binom{k-2}{1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{2p-3+k}{k-1} & \binom{2k-3}{k-1} & \binom{2k-4}{k-1} & \cdots & \binom{k-2}{k-1} \end{pmatrix}.$$

Repeating the above technique of row operations $\ell \le k-1$ times, we obtain

$$A_{\ell,k-1} = \begin{pmatrix} \binom{2p-2+k-\ell}{0} & \binom{2k-2-\ell}{0} & \binom{2k-3-\ell}{0} & \cdots & \binom{k-1-\ell}{0} \\ \binom{2p-2+k-\ell}{1} & \binom{2k-2-\ell}{1} & \binom{2k-3-\ell}{1} & \cdots & \binom{k-1-\ell}{1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{2p-2+k-\ell}{k-1} & \binom{2k-2-\ell}{k-1} & \binom{2k-3-\ell}{k-1} & \cdots & \binom{k-1-\ell}{k-1} \end{pmatrix}.$$

Ultimately, for $\ell = k-1$, we obtain

$$A_{k-1,k-1} = \begin{pmatrix} \binom{2p-1}{0} & \binom{k-1}{0} & \binom{k-2}{0} & \cdots & \binom{0}{0} \\ \binom{2p-1}{1} & \binom{k-1}{1} & \binom{k-2}{1} & \cdots & \binom{0}{1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{2p-1}{k-1} & \binom{k-1}{k-1} & \binom{k-2}{k-1} & \cdots & \binom{0}{k-1} \end{pmatrix},$$

which is simply equal to A when $k=1$. Since $AX \equiv 0 \mod p$ and $\binom{n}{h} = 0$ when $0 \le n < h$, it follows that $AX \equiv A_{k-1,k-1}X \equiv 0 \mod p$. That is, for $s \in [1,k]$,

$$\binom{2p-1}{k-s} + \binom{k-1}{k-s}x_1 + \binom{k-2}{k-s}x_2 + \ldots + \binom{k-s}{k-s}x_s \equiv 0 \mod p.$$

We will now proceed by induction on $s \in [1,k]$. By Lucas's Theorem, $\binom{2p-1}{h} \equiv \binom{p-1}{h} \equiv (-1)^h \mod p$ for $0 \le h \le p-1$. When $s=1$, we have $(-1)^{k-1} + x_1 \equiv \binom{2p-1}{k-1} + \binom{k-1}{k-1}x_1 \equiv 0 \mod p$, which implies that $x_1 \equiv (-1)^k \equiv (-1)^k\binom{k}{k} \mod p$. We will now assume $s \ge 2$ and that $x_h \equiv (-1)^{k-h+1}\binom{k}{k-h+1} \mod p$ for all $h \in [1, s-1]$. Since $\binom{2p-1}{k-s}+\binom{k-1}{k-s}x_1+\binom{k-2}{k-s}x_2+\ldots+\binom{k-s}{k-s}x_s \equiv 0 \mod p$ and $\binom{2p-1}{k-s+1} + \binom{k-1}{k-s+1}x_1 + \binom{k-2}{k-s+1}x_2 + \ldots + \binom{k-s+1}{k-s+1}x_{s-1} \equiv 0 \mod p$, it follows that

$$\begin{aligned} x_s &\equiv -\binom{2p-1}{k-s+1} - \binom{2p-1}{k-s} - \sum_{h=1}^{s-1}\left(\binom{k-h}{k-s+1} + \binom{k-h}{k-s}\right)x_h \\ &= -\binom{2p}{k-s+1} - \sum_{h=1}^{s-1}\binom{k-h+1}{k-s+1}x_h \qquad (2) \\ &\equiv -\sum_{h=1}^{s-1}(-1)^{k-h+1}\binom{k-h+1}{k-s+1}\binom{k}{k-h+1} \qquad (3) \\ &= (-1)^{k+1}\binom{k}{k-s+1}\sum_{h=1}^{s-1}(-1)^{h-1}\binom{s-1}{s-h} \qquad (4) \\ &= (-1)^{k-s+1}\binom{k}{k-s+1} \mod p, \qquad (5) \end{aligned}$$

where (2) follows in view of the binomial identity $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$, where (3) follows in view of $1 \le s \le k \le p-1$ and the induction hyopthesis, where (4) follows in view of the binomial identity $\binom{b}{a}\binom{c}{b} = \binom{c}{a}\binom{c-a}{b-a}$ for $0 \le a \le b$, and where (5) follows by evaluating the polynomial identity $(x-1)^{s-1} = \sum_{h=1}^{s-1} x^{s-h}\binom{s-1}{s-h}(-1)^{h-1} + (-1)^{s-1}$ at $x=1$, which yields the desired value for x_s. □

Lemma 3.2. *Let $G = C_p \oplus C_p$ with p prime, let $k \in [1, p-1]$ be an integer, and let $S \in \mathcal{F}(G)$ be a sequence of terms from G with $|S| = \mathrm{D}(G) + k - 1 = 2p - 2 + k$ and $0 \notin \Sigma_{\le \mathrm{D}(G)-k}(S) = \Sigma_{\le 2p-1-k}(S)$. Then the following hold.*

(a) *For all $i \in [1, \mathrm{D}(G)-k] \cup [\mathrm{D}(G)+1, 2\mathrm{D}(G)-2k+1] = [1, 2p-1-k] \cup [2p, 4p-2k-1]$, we have $N^i(S) = 0$.*

(b) *$N^{\mathrm{D}(G)}(S) \equiv k \mod p$. In particular, S contains at least k zero-sum subsequences of length $\mathrm{D}(G) = 2p-1$, and any such zero-sum is minimal.*

(c) *If $k \ge 2$, then $\sigma(S) \neq 0$.*

Proof. Recall that

$$\mathrm{D}(G) = 2p - 1.$$

(a): By hypothesis, $N^i(S) = 0$ for all $i \in [1, \mathrm{D}(G)-k]$. If $i \in [\mathrm{D}(G)+1, 2\mathrm{D}(G)-2k+1]$ and $N^i(S) \neq 0$, then S has a zero-sum subsequence of length i, say T. Since $i > \mathrm{D}(G)$, then T has a nonempty zero-sum subsequence of length at most $\mathrm{D}(G)$, say R. Then R and $R^{[-1]} \cdot T$ are both nonempty, proper zero-sum subsequences of S, and one of them has length at most $\mathrm{D}(G) - k$, which is contrary to hypothesis.

(b): Let T be a subsequence of S of length $|T| = |S| - t \ge 2p - 1$, where $t \in [0, k-1]$.

Suppose $k \le \dfrac{2p+1}{3}$. Then $|S| = 2p - 2 + k \le 4p - 2k - 1 = \mathrm{D}(G) - 2k + 1$. By Lemma 2.2 and (a), we have

$$1 + \sum_{i=2p-k}^{2p-1} (-1)^i N^i(T) \equiv 0 \mod p.$$

From this, we have

$$\sum_{T|S, |T|=|S|-t} \left(1 + \sum_{i=2p-k}^{2p-1} (-1)^i N^i(T) \right) \equiv 0 \mod p, \quad \text{for every } t \in [0, k-1].$$

By counting the number of times each zero-sum subsequence of S occurs in the above sum, we obtain

$$\binom{|S|}{|T|} + \sum_{i=2p-k}^{2p-1} (-1)^i \binom{|S|-i}{|T|-i} N^i(S) = \binom{|S|}{t} + \sum_{i=2p-k}^{2p-1} (-1)^i \binom{|S|-i}{t} N^i(S) \equiv 0 \mod p, \tag{6}$$

for every $t \in [0, k-1]$. Let us next derive a similar congruence when $k \ge \frac{2p+2}{3}$.

Suppose $k \ge \dfrac{2p+2}{3}$. Then $|S| = 2p - 2 + k > 4p - 2k - 1$, so by Lemma 2.2 and (a),

$$1 + \sum_{i=2p-k}^{2p-1} (-1)^i N^i(T) + \sum_{i=4p-2k}^{2p-2+k} (-1)^i N^i(T) \equiv 0 \mod p.$$

Through the same process we used when $k \leq \dfrac{2p+1}{3}$, we obtain

$$\binom{|S|}{t} + \sum_{i=2p-k}^{2p-1} (-1)^i \binom{|S|-i}{t} N^i(S) + \sum_{i=4p-2k}^{2p-2+k} (-1)^i \binom{|S|-i}{t} N^i(S) \equiv 0 \mod p.$$

We have $t \leq k-1 \leq p-1$, so by Lucas's Theorem, we find that $\binom{|S|-i}{t} \equiv \binom{p+|S|-i}{t} \mod p$ for $i \in [4p-2k, 2p-2+k]$. As a result, we obtain

$$\binom{|S|}{t} + \sum_{i=2p-k}^{2p-1} (-1)^i \binom{|S|-i}{t} N^i(S) + \sum_{i=4p-2k}^{2p+k-2} (-1)^i \binom{p+|S|-i}{t} N^i(S) \equiv 0 \mod p.$$

By re-indexing the third summation, we obtain

$$\binom{|S|}{t} + \sum_{i=2p-k}^{2p-1} (-1)^i \binom{|S|-i}{t} N^i(S) + \sum_{i=3p-2k}^{p+k-2} (-1)^{i+p} \binom{|S|-i}{t} N^{i+p}(S) \equiv 0 \mod p.$$

Since $k < p$, then $2p-k < 3p-2k$ and $p+k-2 < 2p-1$, so we obtain

$$\begin{aligned} &\binom{|S|}{t} + \sum_{i=2p-k}^{3p-2k-1} (-1)^i \binom{|S|-i}{t} N^i(S) \\ &\quad + \sum_{i=3p-2k}^{p+k-2} \binom{|S|-i}{t} \left((-1)^i N^i(S) + (-1)^{i+p} N^{i+p}(S)\right) \\ &\quad + \sum_{i=p+k-1}^{2p-1} (-1)^i \binom{|S|-i}{t} N^i(S) \equiv 0 \mod p, \end{aligned} \tag{7}$$

for every $t \in [0, k-1]$.

In view of (6) and (7), we can apply Lemma 3.1 to yield $(-1)^{2p-1} N^{2p-1}(S) \equiv -\binom{k}{1} \mod p$. Since $2p-1$ is odd, then $N^{2p-1}(S) \equiv k \mod p$. Since $k \not\equiv 0 \mod p$ and $N^{2p-1}(S) \geq 0$, then $N^{2p-1}(S) \geq k$. Lastly, if a zero-sum subsequence of S of length $2p-1$ was not minimal, then S would contain a subsequence of length at most $p \leq 2p-1-k$, which is contrary to hypothesis.

(c): Assume by contradiction that part (c) is false, that is, $\sigma(S) = 0$. Since $k \not\equiv 0 \mod p$, then $N^{2p-1}(S) \geq 1$ by (b), so S has a zero-sum subsequence of length $2p-1$, which we call T. Since S is a zero-sum sequence, then $T^{[-1]} \cdot S$ will be a zero-sum subsequence of S of length $|S| - |T| = k-1 \in [1, p-2] \subseteq [1, 2p-1-k]$ (for $k \geq 2$), which is contrary to hypothesis. □

Lemma 3.3. *Let $G = C_p \oplus C_p$ with p prime, let $k \in [1, p-2]$ be an integer, and let $S \in \mathcal{F}(G)$ be a sequence of terms from G with $|S| = \mathrm{D}(G) + k - 1 = 2p - 2 + k$ and $0 \notin \Sigma_{\leq \mathrm{D}(G)-k}(S) = \Sigma_{\leq 2p-1-k}(S)$. If (e_1, e_2) is a basis for G such that $S = e_1^{[p-1]} \cdot e_2^{[p-1]} \cdot T$, then $S = e_1^{[p-1]} \cdot e_2^{[p-1]} \cdot (e_1 + e_2)^{[k]}$.*

Proof. If $k = 1$, then $|S| = 2p - 1 = \mathrm{D}(G)$ with $0 \notin \Sigma_{\le 2p-2}(S)$ ensures that S is a minimal zero-sum sequence of length $2p-1$, forcing $T = e_1 + e_2$, as desired. Therefore we can assume $k \ge 2$.

Let $\overline{n} \in [1, p]$ be the least positive integer congruent to n modulo p. Let $\phi : G \to \mathbb{Z}/p\mathbb{Z}$ be defined by $xe_1 + ye_2 \mapsto \overline{x + y - 1} \mod p$. Let $T' = \prod^{\bullet}_{i\in[1,|T'|]}(x_ie_1 + y_ie_2)$, where $x_i, y_i \in [1, p]$, be an arbitrary nonempty subsequence of T. Then

$$\sigma(\phi(T')) \equiv \sum_{i\in[1,|T'|]} \overline{x_i + y_i - 1} \equiv \overline{\sum_{i\in[1,|T'|]} x_i} + \overline{\sum_{i\in[1,|T'|]} y_i} - |T'| \mod p.$$

Since $S' := e_1^{[p-\overline{\sum_{i\in[1,|T'|]} x_i}]} \cdot e_2^{[p-\overline{\sum_{i\in[1,|T'|]} y_i}]} \cdot T'$ is a nonempty zero-sum subsequence of S, then by Lemma 3.2 parts (a) and (c), we have

$$|S'| = 2p - \overline{\sum_{i\in[1,|T'|]} x_i} - \overline{\sum_{i\in[1,|T'|]} y_i} + |T'| \in [2p-k, 2p-1] \cup [4p-2k, 2p-3+k].$$

From this, we find that

$$\sigma(\phi(T')) \equiv \overline{\sum_{i\in[1,|T'|]} x_i} + \overline{\sum_{i\in[1,|T'|]} y_i} - |T'| \in [1,k] \cup [3-k, 2k-2p] \equiv [1,k] \cup [p+3-k, 2k-p] \mod p.$$

Since $[p + 3 - k, 2k - p] \subseteq [4, k - 1]$, then $\sigma(\phi(T')) \in [1, k] \mod p$, and as T' was an arbitrary nonempty subsequence of T, this shows that

$$\Sigma(\phi(T)) \subseteq [1, k] \mod p.$$

Since $k \le p-2$, then $-1, 0 \notin \Sigma(\phi(T))$. Thus we can apply Lemma 2.3 to obtain $|\mathrm{supp}(\phi(T))| = 1$, say $\phi(T) = g^{[k]}$ with $g \ne 0$. As a result $\Sigma(\phi(T)) = \{g, 2g, \ldots, kg\} \subseteq [1, k] \mod p$ is an arithmetic progression with difference g and length $k \in [2, p-2]$, and thus also equal to the arithmetic progression $[1, k]$ with difference 1 which contains it. Since an arithmetic progression with difference g and length from $[2, \mathrm{ord}(g) - 2]$ has its difference unique up to sign (as is easily verified), it follows that $g = \pm 1$, and as $-1 \notin \Sigma(\phi(T))$, we are left to conclude that $g = 1$, meaning $\phi(T) = 1^{[k]}$.

So for any term of T, say $\alpha e_1 + \beta e_2$ where $\alpha, \beta \in [1, p]$, we have $\alpha + \beta - 1 \equiv 1 \mod p$. Due to the bounds on α and β, it follows that $\alpha + \beta = 2$ or $\alpha + \beta = p + 2$. If $\alpha + \beta = p + 2$, then $e_1^{[p-\alpha]} \cdot e_2^{[p-\beta]} \cdot (\alpha e_1 + \beta e_2)$ is a zero-sum subsequence of S of length $2p - \alpha - \beta + 1 = p - 1 \le 2p - 1 - k$, contrary to hypothesis. Therefore $\alpha + \beta = 2$, which forces $\alpha = \beta = 1$ and $T = (e_1 + e_2)^{[k]}$. □

Lemma 3.4. *Let $G = C_p \oplus C_p \oplus C_p$ with p prime and let $S \in \mathcal{F}(G)$ be a minimal zero-sum sequence of length $\mathrm{D}(G) = 3p - 2$. If there is an $e_1 \in G$ such that $\mathsf{v}_{e_1}(S) \ge p - 1$, then there exists $e_2, e_3 \in G$ such that (e_1, e_2, e_3) is a basis of G and S has the following form:*

$$S = e_1^{[p-1]} \cdot \prod^{\bullet}_{i\in[1,p-1]}(\alpha_i e_1 + e_2) \cdot \prod^{\bullet}_{i\in[1,p]}(\beta_i e_1 + \gamma_i e_2 + e_3),$$

with $\alpha_i, \beta_i, \gamma_i \in [0, p-1]$ and $\sum_{i=1}^{p-1} \alpha_i + \sum_{i=1}^{p} \beta_i \equiv \sum_{i=1}^{p} \gamma_i \equiv 1 \mod p$.

Proof. Since S is a minimal zero-sum of length $3p-2 > p$, we must have $\mathsf{v}_{e_1}(S) \le p-1$, whence $\mathsf{v}_{e_1}(S) = p-1$. Since $e_1 \neq 0$, there exists an $H \le G$ such that $G = \langle e_1 \rangle \oplus H$, so S will have the form

$$S = e_1^{[p-1]} \cdot \prod\nolimits^{\bullet}_{i\in[1,2p-1]} (x_i e_1 + h_i) \tag{8}$$

where $h_i \in H$, $x_i \in [0, p-1]$ and, clearly, $\sum_{i=1}^{2p-1} x_i \equiv 1 \mod p$. Consider the sequence $S' = \prod^{\bullet}_{i\in[1,2p-1]} h_i$. Since S is zero-sum, it follows that S' is zero-sum. Moreover, if S' has a proper, nonempty zero-sum T', then the corresponding subsequence of $\prod^{\bullet}_{i\in[1,2p-1]}(x_i e_1 + h_i)$ will be a proper, nonempty subsequence whose sum lies in $\langle e_1 \rangle$, which can be made into a proper, nonempty zero-sum subsequence of S by concatenating an appropriate number of terms from $e_1^{[p-1]}$. Since this would contradict that S is a minimal zero-sum, we conclude that S' is a minimal zero-sum of length $2p-1$ with terms from $H \cong C_p \oplus C_p$. Then by Theorem 2.4, it follows that S' has the form

$$S' = e_2^{[p-1]} \cdot \prod\nolimits^{\bullet}_{i\in[1,p]} (\gamma_i e_2 + e_3)$$

with $\gamma_i \in [0, p-1]$ and $\sum_{i=1}^{p} \gamma_i \equiv 1 \mod p$, for some basis (e_2, e_3) of H. By re-indexing S', we have that $h_i = e_2$ for $i \in [1, p-1]$ and $h_i = \gamma_{i-p+1} e_2 + e_3$ for $i \in [p, 2p-1]$. By setting $\alpha_i = x_i$ for $i \in [1, p-1]$ and $\beta_i = x_{i+p-1}$ for $i \in [1, p]$, we can rewrite (8), and S will have the form

$$S = e_1^{[p-1]} \cdot \prod\nolimits^{\bullet}_{i\in[1,p-1]} (\alpha_i e_1 + e_2) \cdot \prod\nolimits^{\bullet}_{i\in[1,p]} (\beta_i e_1 + \gamma_i e_2 + e_3). \tag{9}$$

Since (e_1, e_2, e_3) is a basis of G due to (e_2, e_3) being a basis of H, $\sum_{i=1}^{n} \gamma_i \equiv 1 \mod p$, and $\sum_{i=1}^{p-1} \alpha_i + \sum_{i=1}^{p} \beta_i = \sum_{i=1}^{2p-1} x_i \equiv 1 \mod p$, then (9) has the desired properties. □

Lemma 3.5. *Let $G = C_p \oplus C_p$ with p prime, let $k \in [2, p-2]$ be an integer, and let $S \in \mathcal{F}(G)$ be a sequence of terms from G with $|S| = \mathrm{D}(G) + k - 1 = 2p - 2 + k$ and $0 \notin \Sigma_{\le \mathrm{D}(G)-k}(S) = \Sigma_{\le 2p-1-k}(S)$. If S has the form*

$$S = e_1^{[p-1]} \cdot \prod\nolimits^{\bullet}_{i\in[1,\ell]} (a_i e_1 + e_2) \cdot \prod\nolimits^{\bullet}_{i\in[1,v]} (b_i e_1 + x_i e_2),$$

where (e_1, e_2) is a basis of G, $\ell \ge p$, $a_i, b_i \in [1, p]$, $x_i \in [2, p-1]$, and $\sum_{i=1}^{p} a_i \equiv 1 \mod p$, then $\mathrm{h}\left(\prod^{\bullet}_{i\in[1,\ell]}(a_i e_1 + e_2)\right) = p-1$.

Proof. If $v = 0$, then we can apply Lemma 2.5 to complete the proof, so we will assume $v \ge 1$. Let $G' = C_p \oplus C_p \oplus C_p$ and let (e_1, e_2, e_3) be a basis of G'. Let $\phi : G \to G'$ be the map defined by $xe_1 + ye_2 \mapsto xe_1 + ye_2 + e_3$ and let

$$S' = \phi(S) \cdot (-e_3)^{[p-k-1]} \cdot (-\sigma(S) - (2k-1)e_3) = S'_1 \cdot S'_2 \cdot S'_3 \cdot S'_4 \cdot S'_5, \tag{10}$$

where

$$S_1' = \phi(e_1^{[p-1]}) = (e_1+e_3)^{[p-1]}, \tag{11}$$

$$S_2' = \phi\left(\prod\nolimits_{i\in[1,\ell]}^{\bullet}(a_ie_1+e_2)\right) = \prod\nolimits_{i\in[1,\ell]}^{\bullet}(a_ie_1+e_2+e_3), \tag{12}$$

$$S_3' = \phi\left(\prod\nolimits_{i\in[1,v]}^{\bullet}(b_ie_1+x_ie_2)\right) = \prod\nolimits_{i\in[1,v]}^{\bullet}(b_ie_1+x_ie_2+e_3), \tag{13}$$

$$S_4' = (-e_3)^{[p-k-1]}, \quad \text{and} \tag{14}$$

$$S_5' = -\sigma(S)-(2k-1)e_3 = -\left(\sum_{i=1}^{\ell}a_i+\sum_{i=1}^{v}b_i-1\right)e_1-\left(\ell+\sum_{i=1}^{v}x_i\right)e_2-(2k-1)e_3. \tag{15}$$

Claim A: S' is a minimal zero-sum sequence of length $3p-2$.

Proof of Claim A. Since $\ell+v+p-1=|S|=2p-2+k$, then $|S'|=3p-2$. Also,

$$\sigma(S') = (\sigma(S)+(2p-2+k)e_3)-(p-k-1)e_3-\sigma(S)-(2k-1)e_3 = pe_3 = 0,$$

so S' is zero-sum. Furthermore, by Lemma 3.2(c), $-\sigma(S)-(2k-1)e_3\neq 0$. Assume by contradiction that S' has a proper, nonempty zero-sum subsequence T'. We will examine two cases.

Case 1: Suppose $-\sigma(S)-(2k-1)e_3\notin\operatorname{supp}(T')$.

Then $T'=\phi(T)\cdot(-e_3)^{[i]}$ where $i\in[0,p-k-1]$ and T is a subsequence of S. Observe that

$$0=\sigma(T')=\sigma(T)+(|T|-i)e_3,$$

so $|T|\equiv i \mod p$, and T is a nonempty zero-sum subsequence of S. From Lemma 3.2 part (a),

$$i\equiv|T|\in[2p-k,2p-1]\cup[4p-2k,2p-2+k]\equiv[p-k,p-1] \mod p,$$

with the latter congruence holding since $p-k\leq 2p-2k$ and $k-2\leq p-3$, which is contrary to the definition of i.

Case 2: Suppose $-\sigma(S)-(2k-1)e_3\in\operatorname{supp}(T')$.

Then $T'=\phi(T)\cdot(-e_3)^{[i]}\cdot(-\sigma(S)-(2k-1)e_3)$ where $i\in[0,p-k-1]$ and T is a subsequence of S. Observe that

$$0=\sigma(T')=\sigma(T)-\sigma(S)+(|T|-i-2k+1)e_3,$$

so $\sigma(T)=\sigma(S)$ and $|T|\equiv i+2k-1 \mod p$. Consider $T^{[-1]}\cdot S$, which will be zero-sum. Also,

$$|T^{[-1]}\cdot S| = 2p-2+k-|T|\equiv 2p-k-1-i \mod p.$$

If $T=S$, then $2p-2+k=|S|=|T|\equiv i+2k-1$ forces $i=p-k-1$, in which case $T'=S'$, contradicting that T' is a proper zero-sum subsequence of S'. Therefore $T^{[-1]}\cdot S$ is a nonempty zero-sum subsequence of S, so Lemma 3.2 parts (a) and (c) implies

$$2p-k-1-i\in[2p-k,2p-1]\cup[4p-2k,2p-2+k]\equiv[p-k,p-1] \mod p.$$

From this, we have that $i \in [p-k, p-1] \mod p$, which is also contrary to the definition of i. $\square$

By Claim A, S' satisfies the hypothesis of Lemma 3.4. Thus, by setting

$$f_1 = e_1 + e_3,$$

there are f_2 and f_3 with (f_1, f_2, f_3) a basis for G' such that

$$S' = f_1^{[p-1]} \cdot \prod\nolimits^{\bullet}_{i\in[1,p-1]}(\alpha_i f_1 + f_2) \cdot \prod\nolimits^{\bullet}_{i\in[1,p]}(\beta_i f_1 + \gamma_i f_2 + f_3), \tag{16}$$

where $\alpha_i, \beta_i, \gamma_i \in [0, p-1]$. Since (e_1, e_2, e_3) is a basis for G' with $f_1 = e_1 + e_3$, it follows that (f_1, e_2, e_3) is also a basis for G'. Moreover, we can replace f_2 by $af_1 + f_2$, for any $a \in [0, p-1]$, and (16) remains true using this alternative value of f_2, adjusting the coefficients α_i and β_i appropriately. Thus, by choosing $a \in [0, p-1]$ appropriately, we can w.l.o.g. assume

$$f_2 \in \langle e_2\rangle \oplus \langle e_3\rangle. \tag{17}$$

Our goal now will be to determine f_2. By using the substitution $f_1 = e_1 + e_3$ in (11)–(15), we obtain

$$S'_1 = f_1^{[p-1]}, \tag{18}$$

$$S'_2 = \prod\nolimits^{\bullet}_{i\in[1,\ell]}(a_i f_1 + e_2 + (1-a_i)e_3), \tag{19}$$

$$S'_3 = \prod\nolimits^{\bullet}_{i\in[1,v]}(b_i f_1 + x_i e_2 + (1-b_i)e_3), \tag{20}$$

$$S'_4 = (-e_3)^{[p-k-1]}, \qquad \text{and} \tag{21}$$

$$S'_5 = -\left(\sum_{i=1}^{\ell} a_i + \sum_{i=1}^{v} b_i - 1\right) f_1 - \left(\ell + \sum_{i=1}^{v} x_i\right) e_2 + \left(\sum_{i=1}^{\ell} a_i + \sum_{i=1}^{v} b_i - 2k\right) e_3. \tag{22}$$

Let $\pi : G' \to \langle e_2\rangle \oplus \langle e_3\rangle$ be the projection map defined by $xf_1 + ye_2 + ze_3 \mapsto ye_2 + ze_3$. Let

$$\Omega := \pi(S'_2 \cdot S'_3 \cdot S'_4 \cdot S'_5) = \pi((f_1^{[p-1]})^{[-1]} \cdot S').$$

By (16) and (17), we have $\mathsf{v}_{f_2}(\Omega) \ge p-1$. Since $x_i \in [2, p-1]$, the supports of $\pi(S'_2)$, $\pi(S'_3)$ and $\pi(S'_4)$ are pairwise disjoint with $|\pi(S'_3)| = v = p+k-1-\ell < p-2$ and $|\pi(S'_4)| = p-k-1 < p-2$, so the only way that $\mathsf{v}_{f_2}(\Omega) \ge p-1$ is possible if either $\mathsf{v}_{f_2}(\pi(S'_2)) \ge p-1$, or else $\mathsf{v}_{f_2}(\pi(S'_2)) = p-2$ and $\pi(S'_5) = f_2$.

If $\mathsf{v}_{f_2}(\pi'(S_2)) \ge p-1$, then

$$p-1 \le \mathsf{v}_{f_2}(\pi(S'_2)) \le \mathrm{h}(\pi(S'_2)) = \mathrm{h}\left(\prod\nolimits^{\bullet}_{i\in[1,\ell]}(a_i e_1 + e_2)\right) \le p-1,$$

where the equality in the middle is due to $a_i e_1 + e_2$ in S corresponding to $e_2 + (1-a_i)e_3$ in $\pi(S'_2)$, and the desired conclusion holds. Therefore we now assume

$$\mathsf{v}_{f_2}(\pi(S'_2)) = p-2 \qquad \text{and} \qquad \pi(S'_5) = f_2. \tag{23}$$

Since $k \in [2, p-2]$ ensures that $p \geq 5$, we conclude from (23) that f_2 is a term of $\pi(S_2')$, whence $f_2 = e_2 + (1-a_j)e_3$ for some $j \in [1, \ell]$. Now the term $a_i e_1 + e_2$ in S corresponds to the term $e_2 + (1-a_i)e_3$ in $\pi(S_2')$. We can replace the basis (e_1, e_2) with the basis (e_1, e_2'), where $e_2' = a_j e_1 + e_2$, and the hypotheses of the lemma remain valid replacing a_i by $a_i' = a_i - a_j$ for $i \in [1, \ell]$, and likewise adjusting the values of the b_i. This leaves the value $f_1 = e_1 + e_3$ unchanged, with $f_2 = e_2' - a_j e_1 + (1-a_j)e_3 = e_2' + e_3 - a_j f_1$. Thus, by also replacing f_2 by $f_2' = f_2 + a_j f_1 = e_2' + e_3$, and defining π using the basis (f_1, e_2', e_3) rather than (f_1, e_2, e_3), we can w.l.o.g. assume that

$$f_2 = e_2 + e_3$$

with $a_i = 0$ for exactly $p-2$ values of $i \in [1, \ell]$, say w.l.o.g. $a_i = 0$ for $i \in [1, p-2]$. Then we can rewrite (18)–(22) as follows:

$$S_1' = f_1^{[p-1]}, \tag{24}$$

$$S_2' = f_2^{[p-2]} \cdot \prod\nolimits_{i \in [p-1, \ell]}^{\bullet} (a_i f_1 + f_2 - a_i e_3), \tag{25}$$

$$S_3' = \prod\nolimits_{i \in [1, v]}^{\bullet} (b_i f_1 + x_i f_2 + (1 - b_i - x_i)e_3), \tag{26}$$

$$S_4' = (-e_3)^{[p-k-1]}, \quad \text{and} \tag{27}$$

$$\begin{aligned} S_5' = &- \left(\sum_{i=p-1}^{\ell} a_i + \sum_{i=1}^{v} b_i - 1 \right) f_1 - \left(\ell + \sum_{i=1}^{v} x_i \right) f_2 \\ &+ \left(\ell + \sum_{i=1}^{v} x_i + \sum_{i=p-1}^{\ell} a_i + \sum_{i=1}^{v} b_i - 2k \right) e_3 = - \left(\sum_{i=p-1}^{\ell} a_i + \sum_{i=1}^{v} b_i - 1 \right) f_1 + f_2, \end{aligned} \tag{28}$$

where $a_i \in [1, p-1]$ for all $i \in [p-1, \ell]$, with the final equality in (28) since $\pi(S_5') = f_2$.

Since $f_1 = e_1 + e_3$ and $f_2 = e_2 + e_3$ with (e_1, e_2, e_3) a basis for G', it follows that (f_1, f_2, e_3) is a basis for G'. Thus $f_3 = a f_1 + b f_2 + c e_3$ for some $a, b \in [0, p-1]$ and $c \in [1, p-1]$, with $c \neq 0$ since (f_1, f_2, f_3) is also a basis for G'. Letting $c^{-1} \in [1, p-1]$ be the multiplicative inverse of c modulo p, we have

$$e_3 = (-c^{-1}a) f_1 + (-c^{-1}b) f_2 + (c^{-1}) f_3.$$

In view of (16) and (23), all terms of $S_3' \cdot S_4'$ must have their f_3-coefficient, when written using the basis (f_1, f_2, f_3), equal to 1. Likewise, all $\ell - (p-2) \geq 2$ terms x of S_2' with $\pi(x) \neq f_2$ must also have their f_3-coefficient, when written using the basis (f_1, f_2, f_3), equal to 1. As a result, substituting the value $e_3 = (-c^{-1}a) f_1 + (-c^{-1}b) f_2 + (c^{-1}) f_3$ into (25) yields $-a_i c^{-1} \equiv 1 \mod p$ for all $i \in [p-1, \ell]$, while substituting into (27) yields (in view of $k \leq p-2$) that $-c^{-1} \equiv 1 \mod p$. It follows that

$$c = -1 \quad \text{and} \quad a_i = 1 \quad \text{for all } i \in [p-1, \ell].$$

Recalling that $a_i = 0$ for $i \in [1, p-2]$, we conclude that S has the form

$$S = e_1^{[p-1]} \cdot e_2^{[p-2]} \cdot (e_1 + e_2)^{[\ell-p+2]} \cdot \prod\nolimits_{i\in[1,v]}^{\bullet} (b_i e_1 + x_i e_2), \tag{29}$$

where $\ell \geq p$ and $x_i \in [2, p-1]$ for all $i \in [1, v]$.

By Lemma 3.2 part (b) and $k \not\equiv 0 \mod p$, S has a minimal zero-sum subsequence of length $2p-1$, say T. Note that $|S \cdot \left(e_1^{[p-1]} \cdot e_2^{[p-2]}\right)^{[-1]}| = k+1 \leq p-1$. Thus, in view of (29), $\ell \geq p$ and $v \geq 1$, we see that e_1 is the only term of S with multiplicity $p-1$, while there are at most $v = |S| - (p-1) - \ell \leq |S| - 2p + 1 = k - 1 \leq p-2$ terms of S neither equal to e_1 nor from the coset $\langle e_1\rangle + e_2$. As a result, Theorem 2.4 implies that this zero-sum subsequence T must have the form

$$T = e_1^{[p-1]} \cdot e_2^{[\alpha]} \cdot (e_1 + e_2)^{[\beta]},$$

where $\alpha \in [0, p-2]$ and $\alpha + \beta = p$. But then $0 = \sigma(T) = (\beta - 1)e_1$, which implies that $\beta = 1$ and $\alpha = p-1$, contradicting that $\mathsf{v}_{e_2}(S) = p-2$ (in view of (29)), which completes the proof. □

We can now prove our main result.

Proof of Theorem 1.4. Since $k \not\equiv 0 \mod p$, Lemma 3.2(b) implies that S contains a minimal zero-sum subsequence of length $\mathrm{D}(G) = 2p-1$, say T. By Theorem 2.4, there is a basis (e_1, e_2) for G such that $T = e_1^{[p-1]} \cdot \prod_{i\in[1,p]}^{\bullet} (a_i e_1 + e_2)$, for some $a_i \in [1, p]$ with $\sum_{i=1}^{p} a_i \equiv 1 \mod p$, ensuring that S satisfies the hypotheses of Lemma 3.5. Note, there can be at most $p - 1 = \mathrm{D}(C_p) - 1$ terms from $\langle e_1\rangle$ in S, else S contain a nonempty zero-sum subsequence with length at most $p \leq 2p - 1 - k$, contrary to hypothesis. Lemma 3.5 now implies that there is some term $e_2' := ae_1 + e_2$, where $a \in [1, p]$, having multiplicity $p-1$ in S. Since (e_1, e_2) is a basis for G, so too is (e_1, e_2'), with $S = e_1^{[p-1]} \cdot {e_2'}^{[p-1]} \cdot T'$ for some subsequence T' of S, allowing us to apply Lemma 3.3 to yield the desired structure for S. □

References

[1] P. Baginski, A. Geroldinger, D. J. Grynkiewicz, David, and A. Philipp, Products of two atoms in Krull monoids and arithmetical characterizations of class groups, *European J. Combin.* 34 (2013), no. 8, 1244–1268.

[2] G. Bhowmik, I. Halupczok, J.-C. Schlage-Puchta, Inductive methods and zero-sum free sequences, *Integers* 9 (2009), A40, 515–536.

[3] G. Bhowmik, I. Halupczok, J.-C. Schlage-Puchta, The structure of maximal zero-sum free sequences, *Acta Arith.* 143 (2010), no. 1, 21–50.

[4] G. Cohen and G. Zemor, Subset sums and coding theory, *Astérisque* 258 (1999) 327–339.

[5] C. Delorme, O. Ordaz and D. Quiroz, Some Remarks on Davenport Constant, *Discrete Math.* 237 (2001), 119–128.

[6] P. van Emde Boas and D. Kruyswijk, A combinatorial problem on finite Abelian groups, *Math. Centrum Amsterdam Afd. Zuivere Wisk.* 1967 (1967), ZW-009, 27 pp.

[7] M. Freeze and W. Schmid, Remarks on a generalization of the Davenport constant, *Discrete Math.* 310 (2010), 3373–3389.

[8] W. Gao and A. Geroldinger, On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, *Integers* 3 (2003), #A8.

[9] W. Gao, A. Geroldinger, D. J. Grynkiewicz, Inverse Zero-Sum Problems III, *Acta Arith.* **141.2** (2010), 245-279.

[10] Weidong Gao, A. Geroldinger, Qinghong Wang, A quantitative aspect of non-unique factorizations: the Narkiewicz constants, *Int. J. Number Theory* 7 (2011), no. 6, 1463–1502.

[11] W. Gao, D. J. Grynkiewicz, and X. Xia, On n-sums in an abelian group, *Combin, Probab. and Comput.* **25.3** (2016), 419-435.

[12] W. Gao, Y. Li, C. Liu and Y. Qu, Product-one subsequences over subgroups of a finite group, *Acta Arithmetica* 189 (2019), 209–221.

[13] A. Geroldinger, D. J. Grynkiewicz, and Pingzhi Yuan, On products of k atoms II, *Mosc. J. Comb. Number Theory* 5 (2015), no. 3, 3–59.

[14] A. Geroldinger and F. Halter-Koch, *Non-unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman and Hall/CRC, 2006.

[15] A. Geroldinger and I. Ruzsa, *Combinatorial number theory and additive group theory*, Courses and seminars from the DocCourse in Combinatorics and Geometry held in Barcelona, 2008. Advanced Courses in Mathematics. CRM Barcelona. Birkhäuser Verlag, Basel, 2009. xii+330 pp.

[16] A. Geroldinger and W. A. Schmid, A characterization of class groups via sets of lengths, *J. Korean Math. Soc.* 56 (2019), no. 4, 869–915.

[17] B. Girard, Inverse zero-sum problems and algebraic invariants, *Acta Arith.* 135 (2008), no. 3, 231–246.

[18] B. Girard, On the existence of zero-sum subsequences of distinct lengths, *Rocky Mountain J. Math.* 42 (2012), no. 2, 583–596.

[19] D. J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics 30 (2013), Springer.

[20] D. J. Grynkiewicz, Inverse Zero-Sum Problems III: Addendum, preprint, https://arxiv.org/abs/2107.10619.

[21] D. J. Grynkiewicz and Chao Liu, A multiplicative property for zero-sums I, *Discrete Math.* 345 (2022), no. 10, Paper No. 112974.

[22] D. J. Grynkiewicz and Chao Liu, A multiplicative property for zero-sums II, *The Electronic J. of Combin.* 29 (2022), no. 3, Paper No. P3.12, 16 pp.

[23] D. J. Grynkiewicz, Chunlin Wang and Kevin Zhao, The Structure of a Sequence with Prescribed Zero-Sum Subsequences, *Integers* **20** (2020), Paper No. A3, 31 pp.

[24] Huanhuan Guan, Pingzhi Yuan, and Xiangneng Zeng, Normal sequences over finite abelian groups, *J. Combin. Theory Ser. A* 118 (2011), no. 4, 1519–1524.

[25] J. E. Olson, A combinatorial problem on finite Abelian groups I. *J. Number Theory* 1 (1969), 8–10.

[26] J. E. Olson, A combinatorial problem on finite Abelian groups II. *J. Number Theory* 1 (1969), 195–199.

[27] O. Ordaz, A. Philipp, I. Santos, and W. A. Schmid, On the Olson and the strong Davenport constants, *J. Théor. Nombres Bordeaux* 23 (2011), no. 3, 715–750.

[28] Jiangtao Peng, Yongke Qu, and Yuanlin Li, Inverse problems associated with subsequence sums in $C_p \oplus C_p$, *Front. Math. China* 15 (2020), no. 5, 985–1000.

[29] Jiangtao Peng, Yuanlin Li, Chao Liu, and Meiling Huang, On subsequence sums of a zero-sum free sequence over finite abelian groups, *J. Number Theory* 217 (2020), 193–217.

[30] C. Reiher, *A proof of the theorem according to which every prime number possesses Property B*, Ph.D Dissertation, University of Rostock, 2010.

[31] B. Roy and R. Thangadurai, On zero-sum subsequences in a finite abelian p-group of length not exceeding a given number, *J. Number Theory* 191 (2018), 246–257.

[32] W. A. Schmid, The inverse problem associated to the Davenport constant for $C_2 \oplus C_2 \oplus C_{2n}$, and applications to the arithmetical characterization of class groups, *Electron. J. Combin.* 18 (2011), no. 1, Paper 33, 42 pp.

[33] W. A. Schmid, Restricted inverse zero-sum problems in groups of rank 2, *Quarterly journal of mathematics* 63 (2012), no. 2, 477–487.

[34] W. A. Schmid, Inverse zero-sum problems II, *Acta Arith.* 143 (2010), no. 4, 333–343.

[35] C. Wang and K. Zhao, On zero-sum subsequences of length not exceeding a given number, *J. Number Theory* 176 (2017), 365-374.

Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, USA
Email address: john.ebert01@gmail.com

Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, USA
Email address: diambri@hotmail.com