#A3 INTEGERS 20 (2020)

THE STRUCTURE OF A SEQUENCE WITH PRESCRIBED ZERO-SUM SUBSEQUENCES

David J. Grynkiewicz
Department of Mathematics, University of Memphis, Memphis, Tennessee
diambri@hotmail.com

Chunlin Wang
Department of Mathematics, Sichuan Normal University, Chengdu, China
c-l.wang@outlook.com

Kevin Zhao[1]
Department of Mathematics, South China Normal University, Guangzhou, China
zhkw-hebei@163.com

Received: 10/7/17, Revised: 4/2/19, Accepted: 1/3/20, Published: 1/8/20

Abstract

Let G be a finite additive abelian group. For a positive integer k, let $\mathsf{s}_{\leq k}(G)$ denote the smallest integer ℓ such that every sequence of ℓ elements from G (repetition allowed) has a nonempty zero-sum subsequence with length not exceeding k. The authors investigate the inverse problem of $\mathsf{s}_{\leq \mathsf{D}(G)-k}(G)$ for the groups $G = C_n \oplus C_n$, where $\mathsf{D}(G)$ denotes the Davenport constant of G. When $n = p^m \geq 5$ for some prime p and positive integer m, $2 \leq k \leq \frac{2p^m+1}{3}$, and $p \nmid k$, we solve the inverse problem.

1. Introduction

Let C_n denote the cyclic group of n elements. Let G be an additive finite abelian group. It is well known that $|G| = 1$ or $G = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid n_2 \mid \cdots \mid n_r$. Then, $r(G) = r$ is the rank of G and the exponent $\exp(G)$ of G is n_r. Let

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

be a sequence of terms $g_i \in G$ (a finite, unordered string of terms from G, repetition allowed) written multiplicatively using the bold dot operation $\boldsymbol{\cdot}$. We let $\mathcal{F}(G)$ denote the set of all such sequences $S \in \mathcal{F}(G)$ with terms from G, use $g^{[k]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{k}$ to denote the sequence consisting of the term $g \in G$ repeated k times, and we call S *a*

[1]Corresponding author

zero-sum sequence if $g_1+\ldots+g_\ell = 0$. We say that S is *a minimal zero-sum sequence* if S is a nonempty zero-sum sequence and no proper, nonempty subsequence is zero-sum. The *Davenport constant* $\mathsf{D}(G)$ is the minimal integer $\ell \in \mathbb{N}$ such that every sequence S over G of length $|S| \geq \ell$ has a nonempty zero-sum subsequence. Set

$$\mathsf{D}^*(G) := 1 + \sum_{i=1}^{r}(n_i - 1).$$

It is known that $\mathsf{D}(G) \geq \mathsf{D}^*(G)$ and that equality holds if $r(G) \leq 2$ or if G is an abelian p-group [5]. In particular, it follows that

$$\mathsf{D}(C_n \oplus C_n) = 2n - 1.$$

Let $\mathsf{d}(G)$ denote the maximal length of zero-sum free sequences in a group G. It is easy to see that $\mathsf{d}(G) = \mathsf{D}(G) - 1$. Let $\eta(G)$ denote the smallest integer $\ell \in \mathbb{N}$ such that every sequence S over G of length $|S| \geq \ell$ has a nonempty zero-sum subsequence T of length $|T| \leq \exp(G)$. Denote by $\mathsf{s}_{\leq k}(G)$ the smallest integer $\ell \in \mathbb{N} \cup \{+\infty\}$ such that every sequence of ℓ elements from G has a nonempty zero-sum subsequence with length not exceeding k ($k \in \mathbb{N}$). In particular, when $k \geq \mathsf{D}(G)$,

$$\mathsf{s}_{\leq \mathsf{D}(G)}(G) = \mathsf{D}(G);$$

and when $k = \exp(G)$,

$$\mathsf{s}_{\leq \exp(G)}(G) = \eta(G).$$

In [8], the authors determined $\mathsf{s}_{\leq k}(G)$ for all finite abelian groups of rank two.

Theorem 1 ([8], Theorem 2). *Let $G = C_m \oplus C_n$, where m and n are integers with $1 \leq m \mid n$. Then*

$$\mathsf{s}_{\leq \mathsf{D}(G)-k}(G) = \mathsf{D}(G) + k = m + n - 1 + k \quad \text{for every } k \in [0, m-1].$$

Let $G = C_n \oplus C_n$. By Theorem 1, we know that

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

and

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

We investigate the inverse problem of the invariant $\mathsf{s}_{\leq 2n-1-k}(C_p \oplus C_p)$ for $k \in [0, n-1]$, that is, characterizing the structure of those sequences S with $|S| = \mathsf{s}_{\leq 2n-1-k}(C_n \oplus C_n) - 1 = 2n - 2 + k$ having no zero-sum subsequences of length from $[1, 2n-1-k]$. Our focus is on the case when $n = p^m$ is a prime power, and in particular, when $n = p$ is prime.

Definition 2. Let $G = C_n \bigoplus C_n$ with $n \geq 2$. We say that n has

- Property B, if every minimal zero-sum sequence $S \in \mathcal{F}(G)$ with length $|S| = 2n-1$ contains some element with multiplicity $n-1$;
- Property C, if every sequence $S \in \mathcal{F}(G)$ with length $|S| = 3n-3$ which contains no zero-sum subsequence of length at most n has the form $S = a^{[n-1]}b^{[n-1]}c^{[n-1]}$ for some distinct elements $a, b, c \in G$ of order n.

In fact, it is known that Property B holds for all $n \geq 2$. The paper [2] of Gao, Geroldinger and Grynkiewicz reduces its validity to the prime case, which was resolved by Reiher in [7]. From then on, the structure of minimal zero-sum sequences with length $\mathsf{D}(G)$ in the group $G = C_n \bigoplus C_n$ is known. It is worth noting that in [2] the authors fully described the structure of the minimal zero-sum sequence with length $\mathsf{D}(G)$ in the abelian group of rank two. Property C was investigated by Weidong Gao and Alfred Geroldinger [4] in detail. From [3] and [4], we know that the property C holds for any positive integer $n \geq 2$. We have $\mathsf{s}_{\leq k}(G) = \infty$ for $k < \exp(G)$, while $\mathsf{s}_{\leq \mathsf{D}(G)}(G) = \mathsf{D}(G)$ if $k \geq \mathsf{D}(G)$, and $\mathsf{s}_{\leq k}(G) = \eta(G)$ if $k = \exp(G)$. From the above, we see that the inverse problems were solved for the group $C_n \bigoplus C_n$ if $k \geq \mathsf{D}(G) - 1$ or $k = \exp(G)$. It is natural to consider the inverse problems for $k \in [\exp(G) + 1, \mathsf{D}(G) - 2]$. For these problems, we give a conjecture in the prime case.

Conjecture 3. Let $G = C_p \oplus C_p$ with a prime p and let $k \in [2, p-2]$. If a sequence S of terms from G with length $\mathsf{D}(G) + k - 1 = 2p - 2 + k$ has no zero-sum subsequences with length from $[1, \mathsf{D}(G) - k] = [1, 2p - 1 + k]$, then there is a basis (e_1, e_2) for G such that

$$S = e_1^{[p-1]} \cdot e_2^{[p-1]} \cdot (e_1 + e_2)^{[k]}.$$

Our main result is the following, establishing Conjecture 3 for $k \leq \frac{2p+1}{3}$.

Theorem 4. *Let $G = C_p \oplus C_p$ with $p \geq 5$ a prime and let $k \in [2, \frac{2p+1}{3}]$ be an integer. If S is a sequence of terms from G with length $|S| = \mathsf{D}(G) + k - 1 = 2p - 2 + k$ such that $0 \notin \sum_{\leq \mathsf{D}(G) - k}(S) = \sum_{\leq 2p-1-k}(S)$, then there is a basis (e_1, e_2) for G such that*

$$S = e_1^{[p-1]} \cdot e_2^{[p-1]} \cdot (e_1 + e_2)^{[k]}.$$

We derive Theorem 4 from the following result applicable in the prime power case.

Theorem 5. *Let $G = C_{p^n} \oplus C_{p^n}$ with $p^n \geq 5$ a prime power, and let $k \in [2, \frac{2p^n+1}{3}]$ be an integer with $p \nmid k$. If S is a sequence of terms from G with length $|S| = \mathsf{D}(G) + k - 1 = 2p^n - 2 + k$ such that $0 \notin \sum_{\leq \mathsf{D}(G)-k}(S) = \sum_{\leq 2p^n-1-k}(S)$, then there is a basis (e_1, e_2) for G such that*

$$S = e_1^{[p^n-1]} \cdot e_2^{[p^n-1]} \cdot (e_1 + e_2)^{[k]}.$$

2. Preliminaries

In this paper, our notation is consistent with [5], and we briefly present some key concepts. For any set A, denote by $|A|$ the size of A. Let $\mathbb{N}$ denote the set of positive integers and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. All intervals are discrete, so $[x, y] = \{z \in \mathbb{Z} : \ x \le z \le y\}$ for x, $y \in \mathbb{R}$.

Let $\mathcal{F}(G)$ be the free abelian monoid, multiplicatively written, with basis G. The elements of $\mathcal{F}(G)$ are called sequences over G. Each sequence from $\mathcal{F}(G)$ has the form

$$S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell = \prod\nolimits^{\bullet}_{g \in G} g^{[\mathsf{v}_g(S)]} \in \mathcal{F}(G)$$

with $\mathsf{v}_g(S) \in \mathbb{N}_0$ for all $g \in G$ and almost all $\mathsf{v}_g(S) = 0$. We call $\mathsf{v}_g(S)$ the multiplicity of g in S, and if $\mathsf{v}_g(S) > 0$, we say that S contains g. If $\mathsf{v}_g(S) = 0$ for every $g \in G$, then we call S the empty sequence, denoted by $S = 1 \in \mathcal{F}(G)$. We use $T \mid S$ to denote that T is a subsequence of S, meaning $\mathsf{v}_g(T) \le \mathsf{v}_g(S)$ for all $g \in G$, and let $S \boldsymbol{\cdot} T^{[-1]} = T^{[-1]} \boldsymbol{\cdot} S$ denote the sequence obtained from S by removing the terms from T, so $\mathsf{v}_g(S \boldsymbol{\cdot} T^{[-1]}) = \mathsf{v}_g(S) - \mathsf{v}_g(T)$. For $k \ge 1$, $g \in G$ and $T \in \mathcal{F}(G)$, we let $g^{[k]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{k}$ and $T^{[k]} = \underbrace{T \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T}_{k}$ be a sequence with the term g repeated k times and the sequence T repeated k times. Moreover, if $T^{[k]} \mid S$, then $S \boldsymbol{\cdot} T^{[-k]} = T^{[-k]} \boldsymbol{\cdot} S = S \boldsymbol{\cdot} (T^{[k]})^{[-1]}$ is the subsequence of S having the terms from $T^{[k]}$ removed. We have the following:

$$|S| = \ell = \sum_{g \in G} v_g(S) \in \mathbb{N}_0, \text{ the length of } S;$$

$$h(S) = \max\{v_g(S) : \ g \in G\} \in [0, |S|], \text{ the maximum multiplicity of } S;$$

$$Supp(S) = \{g \in G : \ v_g(S) > 0\} \subseteq G, \text{ the support of } S;$$

$$\sigma(S) = \sum_{i=1}^{\ell} g_i = \sum_{g \in G} v_g(S) g \in G, \text{ the sum of } S;$$

$$\Sigma(S) = \{\sum_{i \in I} g_i : \ I \subseteq [1, \ell] \ with \ 1 \le |I| \le \ell\}, \text{ the set of all subsums of } S;$$

$$\Sigma_k(S) = \{\sum_{i \in I} g_i : \ I \subseteq [1, \ell] \ with \ |I| = k\}, \text{ the set of } k\text{-term subsums of } S.$$

We write

$$\Sigma_{\le k}(S) = \bigcup_{j \in [1,k]} \Sigma_j(S) \quad \text{ and } \quad \Sigma_{\ge k}(S) = \bigcup_{j \ge k} \Sigma_j(S).$$

The 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 $S \neq 1_{\mathcal{F}(G)}$, $\sigma(S) = 0$, and every $S' \mid S$ with $1 \leq |S'| < |S|$ is zero-sum free.

Every map of abelian groups $\varphi : G \to H$ extends to a map from $\mathcal{F}(G)$ to $\mathcal{F}(H)$ by setting

$$\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_\ell).$$

If φ is a homomorphism, then $\varphi(S)$ is a zero-sum sequence if and only if $\sigma(S) \in \ker \varphi$.

We will have need of the following results.

Definition 6. Let G be an abelian group, let $S = g_1 \cdot \ldots \cdot g_\ell \in \mathcal{F}(G)$ be a sequence of length $|S| = \ell \in \mathbb{N}_0$, and let $g \in G$.

1. For every $k \in \mathbb{N}_0$, let

$$\mathsf{N}_g^k(S) := \#\Big\{ I \subseteq [1, \ell] : \sum_{i \in I} g_i = g \quad \text{and} \quad |I| = k \Big\}$$

denote the number of subsequences T of S having sum $\sigma(T) = g$ and length $|T| = k$ (counted with the multiplicity of their appearance in S). When $g = 0$, $\mathsf{N}_g^k(S)$ is denoted by $\mathsf{N}^k(S)$ for short.

2. We define

$$\mathsf{N}_g(S) := \sum_{k \geq 0} \mathsf{N}_g^k(S), \quad \mathsf{N}_g^+(S) := \sum_{k \geq 0} \mathsf{N}_g^{2k}(S) \text{ and } \mathsf{N}_g^-(S) := \sum_{k \geq 0} \mathsf{N}_g^{2k+1}(S).$$

Thus $\mathsf{N}_g(S)$ denotes the number of subsequences T of S having sum $\sigma(T) = g$, $\mathsf{N}_g^+(S)$ denotes the number of all such subsequences of even length, and $\mathsf{N}_g^-(S)$ denotes the number of all such subsequences of odd length (each counted with the multiplicity of its appearance in S).

Lemma 7 ([5], Proposition 5.5.8). *Let p be a prime, let G be an abelian p-group, and let $S = g_1 \cdot \ldots \cdot g_\ell \in \mathcal{F}(G)$. If $\ell \geq \mathsf{D}(G)$, then $\mathsf{N}_g^+(S) \equiv \mathsf{N}_g^-(S) \mod p$ for all $g \in G$. In particular, $\mathsf{N}_0^+(S) \equiv \mathsf{N}_0^-(S) \mod p$.*

Lemma 8 ([2, 7]). *Let $G = C_n \oplus C_n$ with $n \geq 2$ and let $S \in \mathcal{F}(G)$ be a minimal zero-sum sequence with length $\mathsf{D}(G) = 2n - 1$. Then S has the following form:*

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

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 9 ([1], Theorem 1.4). *Let G be an abelian group, let $n \geq 1$ be an integer, and let $S \in \mathcal{F}(G)$ be a sequence of terms from G of length $|S| \geq n+1$. Then either*

$$|\Sigma_n(S)| \geq \min\{n+1,\ |S| - n + |\operatorname{Supp}(S)| - 1\}$$

or $ng \in \Sigma_n(S)$ for every $g \in G$ whose multiplicity in S is at least $\mathsf{v}_g(S) \geq \mathsf{h}(S) - 1$.

Corollary 10. *Let G be an abelian group of order n. Let $S \in \mathcal{F}(G)$ be a sequence of terms from G with length $|S| \geq n+1$ and $0 \notin \Sigma_n(S)$. Then*

$$|\Sigma_n(S)| \geq |S| - n + |\operatorname{Supp}(S)| - 1.$$

Lemma 11 ([6], Erdős-Ginzburg-Ziv Theorem). *If G is an abelian group and $S \in \mathcal{F}(G)$ with $|S| \geq 2|G| - 1$, then $0 \in \Sigma_{|G|}(S)$.*

For subsets $A_1, \ldots, A_n \subseteq G$ with G an abelian group, we define the sumset $\sum_{i=1}^{n} A_i = \{\sum_{i=1}^{n} a_i :\ a_i \in A_i\}$. For $A \subseteq G$, we use $\mathsf{H}(A) = \{h \in G :\ h + A = A\} \leq G$ to denote the stabilizer of A. Note A is a union of $\mathsf{H}(A)$-cosets.

Lemma 12 ([6], Kneser's Theorem). *Let G be an abelian group, and let A, $B \subseteq G$ be nonempty subsets. Then $|A + B| \geq |A + H| + |B + H| - |H|$. In particular, if $A_1, \ldots, A_n \subseteq G$ are nonempty subsets, then*

$$|\sum_{i=1}^{n} A_i| \geq \left(\sum_{i=1}^{n} |\phi_H(A_i)| - n + 1\right) |H|,$$

where $\phi_H : G \to G/H$ is the natural homomorphism.

Lemma 13 ([6], Subsum Kneser's Theorem). *Let G be an abelian group, let $S \in \mathcal{F}(G)$, let $n \in [1, |S|]$ be an integer, and let $H = \mathsf{H}(\Sigma_n(S))$. Then*

$$\begin{aligned} |\Sigma_n(S)| &\geq \left(\sum_{g \in G/H} \min\{n,\ \mathsf{v}_g(\phi_H(S))\} - n + 1\right) |H| \\ &= ((N-1)n + e + 1)|H|, \end{aligned}$$

where $\phi_H : G \to G/H$ is the natural homomorphism, N is the number of elements of G/H having multiplicity at least n in $\phi_H(S)$, and e is the number of terms in $\phi_H(S)$ having multiplicity strictly less than n.

Given a fixed integer $n \geq 2$ and $x \in \mathbb{Z}$ or $x \in \mathbb{Z}/n\mathbb{Z}$, we let $\overline{x} \in [1, n]$ denote the least positive representative for x modulo n. Note n is not indicated in the notation, but will always be clear in contexts where the notation is used.

3. Proofs of Theorems 4 and 5

In this section, we prove Theorems 4 and 5. We proceed in a series of lemmas.

Lemma 14. *Let $G = C_{p^m} \oplus C_{p^m}$ with p prime and $m \geq 1$, let $k \in [1, \frac{\mathsf{D}(G)+2}{3}]$ be an integer, and let $S \in \mathcal{F}(G)$ be a sequence of terms from G with $|S| = \mathsf{D}(G) + k - 1$ and $0 \notin \Sigma_{\leq \mathsf{D}(G)-k}(S)$. Then*

$$\mathsf{N}^{\mathsf{D}(G)+1-t}(S) \equiv \binom{k}{t} \mod p \quad \text{for every } t \in [1, k].$$

In particular, if $k \not\equiv 0 \mod p$, then there exists a minimal zero-sum subsequence $T \mid S$ of length $\mathsf{D}(G)$.

Proof. For convenience, we set $d := \mathsf{D}(G) = 2p^m - 1$. Note that $k \leq \frac{\mathsf{D}(G)+2}{3} = \frac{d+2}{3}$ ensures that

$$|S| = d + k - 1 \leq 2d - 2k + 1.$$

Because the sequence S of length $|S| = d + k - 1$ has no zero-sum subsequences of length in $[1, d - k]$, we have $\mathsf{N}^i(S) = 0$ for $i \in [1, d - k]$. By definition of $d = \mathsf{D}(G)$ and the pigeonhole principle, any zero-sum sequence of length i with $i \in [d+1, |S|] \subseteq [d+1, 2d-2k+1]$ has a nonempty zero-sum subsequence of length at most $d - k$. Thus we conclude that $\mathsf{N}^i(S) = 0$ for $i \in [d + 1, |S|]$.

Let T be a subsequence of S with $|T| = |S| - t = d + k - 1 - t$, where t is an integer such that $0 \leq t \leq k - 1$. Obviously $0 \leq \mathsf{N}^i(T) \leq \mathsf{N}^i(S) = 0$ holds for $i \in [1, d - k] \cup [d + 1, |S|]$. Then, by Lemma 7, we have the following equation:

$$1 + (-1)^{d-k+1}\mathsf{N}^{d-k+1}(T) + \ldots + (-1)^d\mathsf{N}^d(T) \equiv 0 \mod p.$$

It follows that

$$\sum_{T|S,\ |T|=|S|-t} \left(1 + (-1)^{d-k+1}\mathsf{N}^{d-k+1}(T) + \ldots + (-1)^d\mathsf{N}^d(T)\right) \equiv 0 \mod p.$$

Analysing the number of times each subsequence is counted, one obtains

$$\begin{aligned}
&\binom{|S|}{|T|} + (-1)^{d-k+1}\binom{|S| - (d-k+1)}{|T| - (d-k+1)}\mathsf{N}^{d-k+1}(S) \\
&\quad + \ldots + (-1)^d\binom{|S| - d}{|T| - d}\mathsf{N}^d(S) \\
= &\binom{|S|}{t} + (-1)^{d-k+1}\binom{2k-2}{t}\mathsf{N}^{d-k+1}(S) \\
&\quad + \ldots + (-1)^d\binom{k-1}{t}\mathsf{N}^d(S) \equiv 0 \mod p. \qquad (3.3)
\end{aligned}$$

Set $X = (1, (-1)^{d-k+1}\mathsf{N}^{d-k+1}(S), \ldots, (-1)^d\mathsf{N}^d(S))^T = (1, x_1, \ldots, x_k)^T$ and

$$A := \begin{pmatrix} \binom{|S|}{0} & \binom{2k-2}{0} & \cdots & \binom{k-1}{0} \\ \binom{|S|}{1} & \binom{2k-2}{1} & \cdots & \binom{k-1}{1} \\ \cdots & \cdots & \cdots & \cdots \\ \binom{|S|}{k-1} & \binom{2k-2}{k-1} & \cdots & \binom{k-1}{k-1} \end{pmatrix}.$$

On the one hand, it can be deduced from (3.3) that

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

We take some row transformations of A as follows (with the rows operations performed top to bottom each time by using $\binom{n}{i} - \binom{n-1}{i-1} = \binom{n-1}{i}$). It is easy to see that

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

Multiplying the first row of $A_{0,0}$ by -1 and then adding it to the second row of $A_{0,0}$ yields $A_{0,1}$:

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

Repeat this process $k-1$ times, i.e., for $1 \le i \le k-1$ multiply the first row of $A_{0,i}$ by -1 and then add it to the second row of $A_{0,i}$. It follows that

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

Again repeating the above technique on row transformations $l-1$ $(1 \le l \le k-1)$ times one obtains

$$A_{l-1,k-1} = \begin{pmatrix} \binom{|S|-l}{0} & \binom{2k-2-l}{0} & \cdots & \binom{k-1-l}{0} \\ \binom{|S|-l}{1} & \binom{2k-2-l}{1} & \cdots & \binom{k-1-l}{1} \\ \cdots & \cdots & \cdots & \cdots \\ \binom{|S|-l}{k-1} & \binom{2k-2-l}{k-1} & \cdots & \binom{k-1-l}{k-1} \end{pmatrix}.$$

In particular,

$$A_{k-2,k-1} = \begin{pmatrix} \binom{\mathsf{D}(G)}{0} & \binom{k-1}{0} & \cdots & \binom{0}{0} \\ \binom{\mathsf{D}(G)}{1} & \binom{k-1}{1} & \cdots & \binom{0}{1} \\ \cdots & \cdots & \cdots & \cdots \\ \binom{\mathsf{D}(G)}{k-1} & \binom{k-1}{k-1} & \cdots & \binom{0}{k-1} \end{pmatrix}.$$

Consequently, since $AX \equiv 0 \mod p$ and $\binom{a}{b} = 0$ if $0 \le a < b$, we find that $AX \equiv A_{k-2,k-1}X \equiv 0 \mod p$, i.e.,

$$\binom{\mathsf{D}(G)}{k-s} + \binom{k-1}{k-s}x_1 + \ldots + \binom{k-s}{k-s}x_s \equiv 0 \mod p, \quad \text{for } s \in [1,k].$$

We proceed by induction on $s \in [1,k]$ to show

$$x_s \equiv (-1)^{k-s+1}\binom{k}{k-s+1} \mod p.$$

Note $\mathsf{D}(G) = 2p^m - 1$ and $k \le \frac{\mathsf{D}(G)+2}{3} = \frac{2p^m+1}{3} < p^m$. In consequence, $\binom{\mathsf{D}(G)}{h} \equiv (-1)^h \mod p$ for $h \in [0,k]$, and $\binom{\mathsf{D}(G)+1}{h} \equiv 0 \mod p$ for $h \in [1,k]$. When $s = 1$, we have $0 \equiv \binom{\mathsf{D}(G)}{k-1} + \binom{k-1}{k-1}x_1 \equiv (-1)^{k-1} + x_1 \mod p$. It follows that $x_1 \equiv (-1)^k\binom{k}{k} \mod p$, as desired. So we assume $s \ge 2$ and that the formula has been established for all smaller values $h \in [1, s-1]$. Since $\binom{\mathsf{D}(G)}{k-s+1} + \binom{k-1}{k-s+1}x_1 + \ldots + \binom{k-s+1}{k-s+1}x_{s-1} \equiv 0 \mod p$ and $\binom{\mathsf{D}(G)}{k-s} + \binom{k-1}{k-s}x_1 + \ldots + \binom{k-s}{k-s}x_s \equiv 0 \mod p$, it follows that

$$\begin{aligned} x_s &\equiv -\binom{\mathsf{D}(G)}{k-s+1} - \binom{\mathsf{D}(G)}{k-s} - \sum_{h=1}^{s-1}\left(\binom{k-h}{k-s+1} + \binom{k-h}{k-s}\right)x_h \\ &= -\binom{\mathsf{D}(G)+1}{k-s+1} - \sum_{h=1}^{s-1}\binom{k-h+1}{k-s+1}x_h \equiv -\sum_{h=1}^{s-1}\binom{k-h+1}{k-s+1}x_h \\ &\equiv -\sum_{h=1}^{s-1}(-1)^{k-h+1}\binom{k-h+1}{k-s+1}\binom{k}{k-h+1} \\ &= (-1)^{k-s}\binom{k}{k-s+1}\sum_{h=1}^{s-1}(-1)^{s-h}\binom{s-1}{s-h} \\ &= (-1)^{k-s+1}\binom{k}{k-s+1} \mod p, \end{aligned} \tag{1}$$

completing the induction. Therefore,

$$(-1)^{d-(k-s)}\mathsf{N}^{d-(k-s)}(S) = x_s \equiv (-1)^{(k-s)+1}\binom{k}{(k-s)+1} \mod p,$$

for $s \in [1,k]$, implying $\mathsf{N}^{d+1-t}(S) \equiv (-1)^{d+1}\binom{k}{t} \equiv \binom{k}{t} \mod p$, for $t = k-s+1 \in [1,k]$ (since $d = \mathsf{D}(G) = 2p^m - 1$ is odd). In particular, $\mathsf{N}^{\mathsf{D}(G)}(S) \equiv k \mod p$. Thus, if $k \not\equiv 0 \mod p$, then there must exist a zero-sum subsequence $T \mid S$ of length $\mathsf{D}(G) = 2p^m - 1$. If it were not minimal zero-sum, then it would contain a nonempty zero-sum subsequence of length at most $p^m - 1 < 2p^m - 1 - k = \mathsf{D}(G) - k$, contrary to hypothesis. Therefore $T \mid S$ is a minimal zero-sum subsequence of length $\mathsf{D}(G)$. □

Lemma 15. *Let $G = C_n \oplus C_n$ with $n \geq 4$, let (e_1, e_2) be a basis for G, let $k \in [2, n-2]$, and let*

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

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 $0 \notin \Sigma_{\leq \mathsf{D}(G)-k}(S)$, then there exists a basis (e_1, f_2) for G, where $f_2 = xe_1 + e_2$ for some $x \in [1, n]$, such that

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

Proof. Let

$$S_1 = \prod\nolimits^\bullet_{i \in [1, n+k-1]} x_i e_1 \in \mathcal{F}(C_n).$$

We have $|S_1| = n + k - 1 \geq n + 1$.

Suppose $|\operatorname{Supp}(S_1)| \geq 3$. Since $0 \notin \Sigma_n(S_1)$ (lest $0 \in \Sigma_{\leq n}(S)$, contrary to hypothesis), then by Corollary 10, we have

$$|\Sigma_n(S_1)| \geq k + 1.$$

Therefore, there exists a subset $T \subseteq [1, n+k-1]$ whose terms index a subsequence $S(T) = \prod^\bullet_{i \in T} x_i$ with length $|T| = n$ such that $\overline{\sigma(S(T))} \geq k + 1$. Let

$$S_2 = e_1^{n - \overline{\sigma(S(T))}} \cdot \prod\nolimits^\bullet_{i \in T} (x_i e_1 + e_2).$$

We have that S_2 is a zero-sum subsequence of S with $|S_2| = |T| + n - \overline{\sigma(S(T))} \leq 2n - k - 1 = \mathsf{D}(G) - k$. This derives a contradiction. If $|\operatorname{Supp}(S_1)| = 1$, we can also find a zero-sum subsequence with length n in S. This derives a contradiction. So, we have $|\operatorname{Supp}(S_1)| = 2$.

Without loss of generality, let $\operatorname{Supp}(S_1) = \{0, ae_1\}$ where $a \in [1, n-1]$. We have

$$S = e_1^{[n-1]} \cdot e_2^{[s]} \cdot (ae_1 + e_2)^{[n+k-1-s]} \quad \text{with } s \in [k, n-1]. \tag{2}$$

Note $k \leq s \leq n - 1$ lest S contain a zero-sum subsequence of length $n \leq \mathsf{D}(G) - k$, contrary to hypothesis. By Corollary 10, we have

$$|\Sigma_n(S_1)| \geq k.$$

As before, if there exists a subset $T \subseteq [1, n+k-1]$ whose elements index a length n subsequence $S(T) = \prod^\bullet_{i \in T} x_i$ with $\overline{\sigma(S(T))} \geq k + 1$, then we derive a contradiction to $0 \in \Sigma_{\leq \mathsf{D}(G)-k}(S)$. Therefore,

$$\Sigma_n(S_1) = [1, k]_{e_1} := \{e_1, 2e_2, \ldots, ke_1\},$$

which is an arithmetic progression with difference e_1. However, from the structure of S given in (2), $\Sigma_n(S_1)$ must also be an arithmetic progression with difference

ae_1. It is well-known (and easily shown) that the difference d of an arithmetic progression is uniquely defined up to sign, so long as there are strictly less than $\mathrm{ord}(d)-1$ terms and at least 2 terms (see also [6, Exercise 4.2]). Since $2 \le k = |\Sigma_n(S_1)| \le n-2 = \mathrm{ord}(e_1)-2$, these hypotheses hold, forcing $a=1$ or $n-1$.

If $a = 1$, then $n - s = (n-s)a \equiv 1 \mod n$ (in view of the structure of S given in (2) combined with $\Sigma_n(S_1) = [1,k]_{e_1}$), implying $s = n-1$, and then S has the desired form taking $f_2 = e_2$. If $a = n-1$, then arguing similarly gives $s \equiv (n-s)a \equiv k \mod n$, implying $s = k$, in which case S has the desired form taking $f_2 = -e_1 + e_2$. □

Lemma 16. *Let $n \ge 2$ and let $S \in \mathcal{F}([2,n])$ be a nonempty sequence of integers. Then there exists a nonempty subsequence $T \mid S$ with*

$$\overline{\sigma(T)} \ge \min\left\{\left\lceil\frac{n-1}{2}\right\rceil,\ \sigma(S)-|S|\right\} + |T|,$$

where $\overline{\sigma(T)} \in [1,n]$ is the least positive representative for $\sigma(T)$ modulo n. In particular,

$$\overline{\sigma(T)} \ge \min\left\{\left\lceil\frac{n-1}{2}\right\rceil,\ |S|\right\} + |T|.$$

Proof. Since all terms in S are at least 2 by hypothesis, we have $\sigma(S) \ge 2|S|$, so it suffices to prove the main bound in lemma. Let $S = x_1 \cdot \ldots \cdot x_\ell$, where $\ell = |S|$ is the length of S. Moreover, choose the indexing so that $x_1 \ge x_2 \ge \ldots \ge x_\ell$. Let $M = \min\left\{\left\lceil\frac{n-1}{2}\right\rceil,\ \sigma(S)-|S|\right\}$. Then

$$2M \le n \qquad \text{and} \qquad \sigma(S) \ge M + |S| = M + \ell. \tag{3}$$

If $x_1 \ge M+1$, then the sequence T consisting of the single term x_1 satisfies the lemma. Therefore we may assume $x_1 \le M$. In view of (3), we have $x_1 + \ldots + x_\ell \ge M + \ell$. Consequently, there is a maximal $s \in [1, \ell-1]$ such that

$$x_1 + \ldots + x_s \le M + s - 1.$$

Since $s \le \ell - 1$, the term x_{s+1} exits. Since $S \in \mathcal{F}([2,n])$, we have $x_i \ge 2$ for all i, implying $2s \le x_1 + \ldots + x_s \le M + s - 1$, whence

$$1 \le s \le M-1 \qquad \text{and} \qquad M \ge 2.$$

By the maximality of s, it follows that $x_1 + \ldots + x_{s+1} \ge M + s + 1$. As a result, if $x_1 + \ldots + x_{s+1} \le n$, then $\overline{x_1 + \ldots + x_{s+1}} = x_1 + \ldots + x_{s+1} \ge M + s + 1$, in which case $T = x_1 \cdot \ldots \cdot x_{s+1}$ satisfies the lemma. Therefore we can instead assume $x_1 + \ldots + x_{s+1} \ge n+1$, which combined with $x_1 + \ldots + x_s \le M + s - 1$ implies

$x_{s+1} \geq n-M-s+2$. By our choice of indexing, we have $x_i \geq x_{s+1} \geq n-M-s+2$ for all $i \leq s+1$, whence

$$s(n-M-s+2) \leq x_1 + \ldots + x_s \leq M+s-1.$$

Rearranging the above inequality, it follows that

$$s^2 - (n+1-M)s + (M-1) \geq 0 \tag{4}$$

with $s \in [1, M-1]$. If $s = 1$, then (4) yields $2M - 1 - n \geq 0$, contradicting (3). Therefore, (4) fails for $s = 1$, in which case it must hold for the maximum allowed valued for s (since we know it holds for some value of s), namely $s = M-1$. Substituting this value into (4) and using that $M \geq 2$, we obtain $(M-1)-(n+1-M)+1 \geq 0$, in turn implying $2M-1-n \geq 0$, which again gives the contradiction $2M \geq n+1$ to (3). □

Lemma 17. *Let $n \geq 3$ and let $S \in \mathcal{F}([3,n])$ be a nonempty sequence of integers for which the multiplicity of the term $\lceil \frac{n+1}{2} \rceil$ is at most one. Then there exists a nonempty subsequence $T \mid S$ with*

$$\overline{\sigma(T)} \geq \min\left\{ \left\lfloor \frac{2n-2}{3} \right\rfloor,\ 2|S| \right\} + |T|,$$

where $\overline{\sigma(T)} \in [1,n]$ is the least positive representative for $\sigma(T)$ modulo n.

Proof. Let $S = x_1 \cdot \ldots \cdot x_\ell$, where $|S| = \ell$ is the length of S. Moreover, choose the indexing so that $x_1 \geq x_2 \geq \ldots \geq x_\ell$. Let $M = \min\left\{ \left\lfloor \frac{2n-2}{3} \right\rfloor,\ 2|S| \right\}$. Then

$$M \leq \frac{2n-2}{3} \qquad \text{and} \qquad 2\ell = 2|S| \geq M. \tag{5}$$

By hypothesis, $3 \leq x_i \leq n$, and $x_i = \lceil \frac{n+1}{2} \rceil$ for at most one $i \in [1,\ell]$. If $x_1 \geq M+1$, then the sequence T consisting of the single term x_1 satisfies the lemma. Therefore we may assume

$$3 \leq x_1 \leq M.$$

In particular, (5) gives $\ell \geq \lceil \frac{1}{2}M \rceil \geq 2$.

Case 1: $x_1 + x_2 \leq n$.

We have $x_1 \leq M$, while (5) ensures $x_1 + \ldots + x_\ell \geq 3\ell \geq M + \ell$. Consequently, there is a maximal $s \in [1, \ell-1]$ such that

$$x_1 + \ldots + x_s \leq M + s - 1.$$

Since $s \leq \ell - 1$, the term x_{s+1} exists. If $s = 1$, then the maximality of s ensures $M+2 \leq x_1 + x_2 \leq n$, with the latter inequality by case hypothesis. Thus $\overline{x_1 + x_2} =$

$x_1+x_2 \geq M+2$, and the lemma holds taking $T = x_1 \cdot x_2$. Therefore we can assume $s \geq 2$. We have $3s \leq x_1 + \ldots + x_s \leq M + s - 1$, which implies

$$2 \leq s \leq \frac{M-1}{2} \quad \text{and} \quad M \geq 2s+1 \geq 5.$$

By the maximality of s, it follows that $x_1 + \ldots + x_{s+1} \geq M + s + 1$. As a result, if $x_1 + \ldots + x_{s+1} \leq n$, then $\overline{x_1 + \ldots + x_{s+1}} = x_1 + \ldots + x_{s+1} \geq M + s + 1$, in which case $T = x_1 \cdot \ldots \cdot x_{s+1}$ satisfies the lemma. Therefore we can instead assume $x_1 + \ldots + x_{s+1} \geq n+1$, which combined with $x_1 + \ldots + x_s \leq M + s - 1$ implies $x_{s+1} \geq n - M - s + 2$. By our choice of indexing, we have $x_i \geq x_{s+1} \geq n - M - s + 2$ for all $i \leq s+1$, whence $s(n - M - s + 2) \leq x_1 + \ldots + x_s \leq M + s - 1$. Multiplying by 4 and rearranging yields

$$4M + 4s - 4 - 2s(2n - 2M - 2s + 4) \geq 0 \tag{6}$$

with $s \in [2, \frac{M-1}{2}]$. If $s = 2$, then (6) yields $M \geq \frac{2n-1}{3}$, contrary to (5). If $s = \frac{M-1}{2}$, so that $2s = M - 1$, then (6) becomes $6(M-1) - (M-1)(2n - 3M + 5) \geq 0$, implying (in view of $M > 1$) that $M \geq \frac{2n-1}{3}$, contrary to (5). However, since the expression in (6) is quadratic in s with positive lead coefficient, we now conclude that (6) fails for all possible values of s, completing Case 1.

Case 2: $x_1 + x_2 \geq n + 1$.

In view of the case hypothesis and $x_1 \geq x_2$, we conclude that $x_1 \geq \frac{n+1}{2}$. Thus there is a maximal $t \in [1, \ell]$ such that

$$\frac{2n-2}{3} \geq M \geq x_1 \geq \ldots \geq x_t \geq \frac{n+1}{2}. \tag{7}$$

Then

$$n \geq 7 \quad \text{and} \quad x_i \leq \frac{n}{2} \quad \text{for all } i \geq t+1.$$

Since there is at most one term x_i equal to $\lceil \frac{n+1}{2} \rceil$, we must have

$$x_i \geq \lceil \frac{n+3}{2} \rceil \quad \text{for } i \leq t-1. \tag{8}$$

If $n \leq 12$, then $\lfloor \frac{2n-2}{3} \rfloor = \lceil \frac{n+1}{2} \rceil$ (or $\lfloor \frac{2n-2}{3} \rfloor < \lceil \frac{n+1}{2} \rceil$ in case $n = 8$, in which case (7) cannot hold). In such case, (7) ensures $x_i = \lceil \frac{n+1}{2} \rceil$ for all $i \geq t$, forcing $t = 1$ by (8). In summary,

$$n \leq 12 \quad \text{implies} \quad t = 1. \tag{9}$$

If t is odd, modify the sequence S by replacing each pair of terms $x_{2i-1} \cdot x_{2i}$ with the single term $x_{2i-1} + x_{2i} - n$, for $i \in [1, \frac{t-1}{2}]$. If t is even, modify the sequence S by replacing each pair of terms $x_{2i-1} \cdot x_{2i}$ with the single term $x_{2i-1} + x_{2i} - n$, for $i \in [1, \frac{t-2}{2}]$, and then remove the term x_t. In either case, let

$$S' = y_1 \cdot \ldots \cdot y_{\ell'}, \quad \text{where } \ell' = \ell - \lfloor \tfrac{t}{2} \rfloor \geq \tfrac{1}{2}\ell,$$

denote the resulting sequence, and choose the indexing on the y_i such that $y_1 \geq y_2 \geq \ldots \geq y_{\ell'}$. Let $I_{\mathsf{new}} \subseteq [1, \ell']$ consist of the 'new' terms in S', each having the form $x_{2i-1} + x_{2i} - n$ for some $i \in [1, \lfloor \frac{t-1}{2} \rfloor]$.

If y_j is a new term, so $j \in I_{\mathsf{new}}$, then $y_j = x_{2i-1} + x_{2i} - n$ for some $i \in [1, \lfloor \frac{t-1}{2} \rfloor]$, ensuring

$$3 = \frac{n+3}{2} + \frac{n+3}{2} - n \leq y_j \leq 2M - n \leq \frac{n-4}{3} \quad \text{for } j \in I_{\mathsf{new}}, \tag{10}$$

with the final inequality above from (5). Thus $y_1 \geq \frac{n+1}{2}$ is the unique term in S' strictly larger than $\frac{n}{2}$, and

$$y_i \geq 3 \quad \text{for all } i \in [1, \ell'].$$

Note $y_1 = x_t$ or x_{t-1} by construction.

Since $\ell \geq 2$, $\ell' = 1$ would imply $t = \ell = 2$ with $M \geq x_1 \geq x_2 \geq \frac{n+1}{2}$ and $x_1 \geq \frac{n+3}{2}$. In such case, the sequence T consisting of the single term $x_1 = \frac{n+3}{2}$ has $\overline{\sigma(T)} \geq \frac{n+3}{2} \geq 5 = 2|S| + |T|$ in view of $n \geq 7$, as desired. Therefore we may assume $\ell' \geq 2$, so that y_2 exists. Define

$$\epsilon = \begin{cases} 0 & \text{if } y_1 + y_2 \leq n \\ 1 & \text{if } y_1 + y_2 \geq n+1. \end{cases}$$

If $\epsilon = 1$, then $y_2 \geq n + 1 - y_1 \geq n + 1 - M \geq \frac{n+5}{3} > \frac{n-4}{3}$, with the third inequality in view of (5). Thus (10) ensures that $y_2 \leq \frac{n}{2}$ is not a new term when $\epsilon = 1$, so

$$t \leq \ell - \epsilon \qquad \text{and} \qquad \ell' = \ell - \left\lfloor \frac{t}{2} \right\rfloor \geq \frac{\ell + \epsilon}{2}. \tag{11}$$

Since $y_2 \leq \frac{n}{2}$, we see the hypothesis $y_1 + y_2 \geq n + 1$ needed for $\epsilon = 1$ forces $y_1 \geq \frac{n}{2} + 1$. Thus

$$y_1 \geq \frac{n + 1 + \epsilon}{2}. \tag{12}$$

If $t = 1$ and $\epsilon = 0$, then $\ell = \ell'$ with $y_i = x_i$ for all i, whence $n \geq y_1 + y_2 = x_1 + x_2$, contrary to case hypothesis. Thus (9) ensures

$$n \geq 13 - 6\epsilon. \tag{13}$$

It suffices to find a nonempty subsequence $T' \mid S'$ with

$$\overline{\sigma(T')} \geq M + |T'| + |T'_{\mathsf{new}}|, \tag{14}$$

where $T'_{\mathsf{new}} \mid T$ denotes the subsequence of new terms, for then the corresponding sequence $T \mid S$ obtained by replacing each new term $y_j = x_{2i-1} + x_{2i} - n$ in T' with the pair of terms $x_{2i-1} \cdot x_{2i}$ from S that originated y_j will satisfy the lemma since $\sigma(T') \equiv \sigma(T) \mod n$ and $|T| = |T'| + |T'_{\mathsf{new}}|$.

Suppose $y_1 + (y_{2+\epsilon} + \ldots + y_{\ell'}) \le M + 2(\ell' - \epsilon) - 2$. Then

$$0 \ge y_1 + y_{2+\epsilon} + \ldots + y_{\ell'} - M - 2\ell' + 2\epsilon + 2 \ge \frac{n-1-\epsilon}{2} + \ell' - M$$
$$\ge \frac{n-1}{2} + \frac{\ell}{2} - M \ge \frac{n-1}{2} - \frac{3}{4}M \ge 0$$

with the second inequality in view of (12) and $y_i \ge 3$ for all $i \in [2+\epsilon, \ell']$, the third in view of (11), the fourth in view of $\ell \ge \frac{1}{2}M$ (by (5)), and the fifth in view of $M \le \frac{2n-2}{3}$ (also by (5)). As a result, we must have equality in all these estimates. In particular, equality in (12) forces $y_1 = \frac{n+1+\epsilon}{2}$, while equality in (11) forces $t = \ell - \epsilon$ to be even. However, when t is even, we have $y_1 = x_{t-1} \ge \frac{n+3}{2}$ by definition of the y_i, contradicting that $y_1 = \frac{n+1+\epsilon}{2} \le \frac{n+2}{2}$. So we instead conclude that $y_1 + y_{2+\epsilon} + \ldots + y_{\ell'} \ge M + 2(\ell' - \epsilon) - 1$. Combined with $y_1 \le M$, it follows that there is a maximal $s \in [1, \ell' - \epsilon - 1]$ such that

$$y_1 + (y_{2+\epsilon} + \ldots + y_{s+\epsilon}) \le M + 2s - 2.$$

Since $s \le \ell' - \epsilon - 1$, the term $y_{s+\epsilon+1}$ exists.

Suppose $s = 1$. Then the maximality of s ensures that $y_1 + y_{2+\epsilon} \ge M + 3$. If $y_1 + y_{2+\epsilon} \le n$, then $\overline{y_1 + y_{2+\epsilon}} = y_1 + y_{2+\epsilon} \ge M + 3$, and since $y_1 = x_t$ or x_{t-1} is not a new term, it follows that (14) holds taking $T' = y_1 \cdot y_{2+\epsilon}$, completing the proof. On the other hand, if $y_1 + y_{2+\epsilon} \ge n + 1$, then the definition of ϵ forces $\epsilon = 1$ with $y_1 + y_2 \ge n + 1$ and $y_1 + y_3 \ge n + 1$. It follows that $\frac{n}{2} \ge y_2 \ge n + 1 - y_1 \ge n + 1 - M \ge \frac{n+5}{3}$ and $\frac{n}{2} \ge y_3 \ge n + 1 - y_1 \ge n + 1 - M \ge \frac{n+5}{3}$ (in view of (5)). Consequently, (10) implies that neither y_2 nor y_3 is a new term, while $\overline{y_2 + y_3} = y_2 + y_3 \ge \frac{2n+10}{3} \ge M + 3$ (in view of (5)), in which case (14) holds taking $T = y_2 \cdot y_3$, completing the proof. So we may instead assume $s \ge 2$.

Since $y_1 \ge \frac{n+1+\epsilon}{2}$ (by (12)) and $y_i \ge 3$ for all i, we have $\frac{n+1+\epsilon}{2} + 3(s-1) \le y_1 + y_{2+\epsilon} + \ldots + y_{s+\epsilon} \le M + 2s - 2$, implying

$$2 \le s \le M - \frac{n-1+\epsilon}{2}. \tag{15}$$

In view of the maximality of s, we have $y_1 + y_{2+\epsilon} + \ldots + y_{s+\epsilon+1} \ge M + 2s + 1$. If $y_1 + y_{2+\epsilon} + \ldots + y_{s+\epsilon+1} \le n$, then $T' = y_1 \cdot y_{2+\epsilon} \cdot \ldots \cdot y_{s+\epsilon+1}$ satisfies (14) (as y_1 is not a new term), and the proof is complete. Therefore we may assume $y_1 + y_{2+\epsilon} + \ldots + y_{s+\epsilon+1} \ge n + 1$, which combined with $y_1 + y_{2+\epsilon} + \ldots + y_s \le M + 2s - 2$ yields $y_{s+\epsilon+1} \ge n - M - 2s + 3$. Since $y_1 \ge \frac{n+1+\epsilon}{2}$ (by (12)) and $y_{2+\epsilon} \ge \ldots \ge y_{s+\epsilon} \ge y_{s+\epsilon+1}$, it follows that $\frac{n+1+\epsilon}{2} + (s-1)(n - M - 2s + 3) \le y_1 + y_{2+\epsilon} + \ldots + y_{s+\epsilon} \le M + 2s - 2$. Multiplying this inequality by 2 and rearranging terms yields

$$2M + 4s - 5 - \epsilon - n - (2s-2)(n - M - 2s + 3) \ge 0 \tag{16}$$

with $s \in [2, M - \frac{n-1+\epsilon}{2}]$. If $s = 2$, then (16) yields $M \ge \frac{3n-5+\epsilon}{4} > \frac{2n-2}{3}$, with the latter inequality in view of (13), contrary to (5). If $s = M - \frac{n-1+\epsilon}{2}$, so that

$$4 \le 2s \le 2M - n + 1 - \epsilon, \tag{17}$$

then (16) yields $3(2M-n-1-\epsilon)-(2M-n-1-\epsilon)(2n-3M+2+\epsilon)\geq 0$, in turn implying $3-(2n-3M+2+\epsilon)\geq 0$ (as $2M-n-1-\epsilon>0$ follows from (17)). Hence $M\geq \frac{2n-1+\epsilon}{3}\geq \frac{2n-1}{3}$, contrary to (5). As a result, since the expression in (16) is quadratic in s with positive lead coefficient, we conclude that (16) cannot hold for any possible value of s, completing Case 2 and the proof. □

Lemma 18. *Let $G=C_n$ be a cyclic group with $n\geq 2$, let $b\in G$, let $S\in\mathcal{F}(G)$ be a sequence with $0\notin\Sigma_n(S)$, and let $m\in[1,|S|]$ be an integer. Then there is some $x\in b+\Sigma_m(S)$ with*

$$\overline{x}\geq \min\{n,\, m+1,\, |S|-m+1,\, |S|-\mathsf{h}(S)+1,\, |S|-\frac{n}{2}+1\},$$

where $\overline{x}\in[1,n]$ denotes the least positive representative for x modulo n.

Proof. Since $1\leq m\leq |S|$, we can apply the Subsum Kneser's Theorem to $\Sigma_m(S)$. Then, letting $H=\mathsf{H}(\Sigma_m(S))$, we conclude that

$$|\Sigma_m(S)|\geq ((N-1)m+e+1)|H|, \tag{18}$$

where $N\geq 0$ is the number of *elements* of $\mathrm{Supp}(\phi_H(S))$ having multiplicity at least m, and $e\geq 0$ is the number of *terms* of $\phi_H(S)$ whose multiplicity is less than m. Here $\phi_H: G\to G/H$ denotes the natural homomorphism.

Since $H=\{|G/H|,2|G/H|,\ldots,(|H|-1)|G/H|,|G|\}\mod |G|=\{i\cdot|G/H|(\mod |G|):\ 1\leq i\leq |H|\}$ and $H+\Sigma_m(S)=\Sigma_m(S)$, the pigeonhole principle ensures that we can always find some $x\in b+\Sigma_m(S)$ with

$$\overline{x}\geq |G|-|G/H|+|\Sigma_m(\phi_H(S))|\geq |G|-|G/H|+(N-1)m+e+1, \tag{19}$$

with the latter inequality in view of (18). Thus we may assume $N\leq 1$ lest $\overline{x}\geq m+1$ follows, as desired. If $N=0$, then $e=|S|$, and we obtain $\overline{x}\geq |S|-m+1$, as desired. Therefore we conclude that $N=1$, meaning there is exactly one term in $\phi_H(S)$ with multiplicity at least m. If $H=G$, then $b+\Sigma_m(S)=G$, and we can find $x\in b+\Sigma_m(S)$ with $\overline{x}=n$, as desired. If H is trivial, then $N=1$ implies $e=|S|-\mathsf{h}(S)$, and $\overline{x}\geq |S|-\mathsf{h}(S)+1$ follows, as desired. We are left to consider when $H<G$ is a proper, nontrivial subgroup.

By translating all terms of S appropriately, as well as b, we can w.l.o.g. assume 0 is the unique term with multiplicity at least m in $\phi_H(S)$. Let $S_H\mid S$ denote the subsequence of S consisting of terms from H, so $e=|S\boldsymbol{\cdot} S_H^{[-1]}|$. If $|S_H|\geq |G|+|H|-1$, then repeated application of the Erdős-Ginzburg-Ziv Theorem yields a zero-sum subsequence of length $n=|G|$ (with all terms from H), contrary to hypothesis. Therefore we instead conclude $|S_H|\leq |G|+|H|-2$, whence (19) now gives

$$\begin{aligned}\overline{x}&\geq |G|-|G/H|+(|S|-|G|-|H|+2)+1\\&=|S|-|G/H|-|H|+3\geq |S|-\frac{|G|}{2}+1=|S|-\frac{n}{2}+1,\end{aligned}$$

with the final inequality above in view of H being proper and nontrivial, which completes the proof. □

Corollary 19. *Let $G = C_n$ be a cyclic group with $n \geq 2$, let $b \in G$, let $S \in \mathcal{F}(G)$ be a sequence such that $0 \notin \Sigma_n(S)$, and let $m \leq |S|$ be an integer with $1 \leq m < n$. Then there is some $x \in b + \Sigma_m(S)$ with*

$$\overline{x} \geq \min\{|S| - n + 2,\, m + 1\},$$

where $\overline{x} \in [1, n]$ denotes the least positive representative for x modulo n.

Proof. Note $0 \notin \Sigma_n(S)$ ensures $\mathsf{h}(S) \leq n-1$. Thus $|S|-n+2 \leq |S|-\mathsf{h}(S)+1$. Since $m < n$, we have $|S|-n+2 \leq |S|-m+1$ and $m+1 \leq n$. Also, $|S|-n+2 \leq |S|-\frac{n}{2}+1$ since $n \geq 2$. Thus the desired bound follows by applying Lemma 18. □

Lemma 20. *Let $G = C_n \oplus C_n$ with $n \geq 5$, let $k \in [2, \frac{2n+1}{3}]$ be an integer, and suppose $S \in \mathcal{F}(G)$ is a sequence with $0 \notin \Sigma_{\mathsf{D}(G)-k}(S)$ and $|S| = \mathsf{D}(G) + k - 1$. If S contains a minimal zero-sum subsequence of length $\mathsf{D}(G)$, then there is a basis (e_1, e_2) for G such that*

$$S = e_1^{[n-1]} \boldsymbol{\cdot} e_2^{[n-1]} \boldsymbol{\cdot} (e_1 + e_2)^{[k]}.$$

Proof. By hypothesis,

$$2 \leq k \leq \frac{2n+1}{3} < n - 1,$$

with the latter inequality in view of $n \geq 5$. Since $\mathsf{D}(G) = 2n - 1$, we also have $|S| = 2n - 2 + k$ with

$$0 \notin \Sigma_{2n-1-k}(S) \tag{20}$$

by hypothesis, and since S contains a minimal zero-sum subsequence of length $\mathsf{D}(G) = 2n-1$, it follows from Property B and the characterization of such sequences (Lemma 8) that there is a basis (e_1, e_2) for G such that

$$S = e_1^{[n-1]} \boldsymbol{\cdot} U \boldsymbol{\cdot} V,$$

where

$$U = \prod\nolimits^{\bullet}_{i\in[1,|U|]} (a_i e_1 + e_2) \qquad \text{and} \qquad V = \prod\nolimits^{\bullet}_{i\in[1,|V|]} (b_i e_1 + x_i e_2),$$

with the $a_i, b_i \in [1, n]$ and the $x_i \in [2, n-1]$,

$$|U| \geq n, \quad a_1 + \ldots + a_n \equiv 1 \mod n, \qquad \text{and} \qquad |U| + |V| = n - 1 + k. \tag{21}$$

Note $x_i = 0$ for some i would ensure a zero-sum subsequence of length at most n with terms from $\langle e_1 \rangle$, contrary to (20). If $|V| = 0$, then Lemma 15 can be applied to complete the proof. Therefore we may assume $|V| \geq 1$. On the other hand, $|V| = n-1+k-|U| \leq k-1$ follows from (21). In summary:

$$1 \leq |V| \leq k-1. \tag{22}$$

Let $\pi_1 : G \to \langle e_1 \rangle$ and $\pi_2 : G \to \langle e_2 \rangle$ be the projection homomorphisms, so $z = xe_1 + ye_2$ has $\pi_1(z) = xe_1$ and $\pi_2(z) = ye_2$. Then $\pi_1(U) = a_1e_1 \cdot \ldots \cdot a_{|U|}e_1$. For an element xe_i with $x \in \mathbb{Z}$, we let $\overline{xe_i} \in [1, n]$ be the least positive integer congruent to x modulo n. By replacing e_2 by $ae_1 + e_2$ for an appropriate $a \in [1, n]$, we can w.l.o.g. assume

$$h := \mathsf{h}(\pi_1(U)) = \mathsf{v}_0(\pi_1(U)) \leq n-1, \tag{23}$$

where the upper bound follows lest S contain a zero-sum subsequence of length at most n, contrary to (20). Let

$$s = |U| - h = |U| - \mathsf{v}_0(\pi_1(U)) \geq 1$$

denote the number of nonzero terms in $\pi_1(U)$, where the inequality follows in view of $|U| \geq n$ and $h \leq n-1$. We may assume by contradiction that S is a counter example to the lemma, satisfying the above setup with respect to some basis (e_1, e_2), with $h \leq n-1$ maximal. For $I \subseteq [1, |V|]$, we let

$$V(I) = \prod\nolimits^{\bullet}_{i \in I} (b_ie_1 + x_ie_2),$$

and we likewise extend this notation to $\pi_2(V)(I) = \prod^{\bullet}_{i \in I} x_ie_2$, etc. If $0 \in \Sigma_n(\pi_1(U))$, then $0 \in \Sigma_n(S)$ follows (in view of the definition of U), contradicting (20). Therefore, we can assume

$$0 \notin \Sigma_n(\pi_1(U)). \tag{24}$$

Step A: $|V| \geq n-k+1$.

Assume by contradiction $1 \leq |V| \leq n-k$. Averaging this bound with (22), we obtain

$$|V| \leq \frac{n-1}{2}. \tag{25}$$

Since $\overline{\pi_2(V)} = x_1 \cdot \ldots \cdot x_{|V|} \in \mathcal{F}([2, n-1])$, Lemma 16 applied to $\overline{\pi_2(V)}$ implies that there is a nonempty subset $I \subseteq [1, |V|]$ such that

$$\sigma := \overline{\sigma\big(\pi_2(V)(I)\big)} \geq |I| + \min\{\lceil \frac{n-1}{2} \rceil, |V|\} = |I| + |V|, \tag{26}$$

with the equality in view of (25). Let $m = n - \sigma < n$ and let $b = \sigma\big(\pi_1(V)(I)\big)$. In view of (24), we can apply Corollary 19 to $\pi_1(U)$ (if $m = 0$, so $\sigma = n$, we do not apply Corollary 19 and simply take U' to be the trivial sequence) to find a subsequence $U' \mid U$ with $|U'| = n - \sigma$ and

$$r = \overline{b + \sigma\big(\pi_1(U')\big)} \geq \min\{|U| - n + 2, n - \sigma + 1\} \\ = \min\{k + 1 - |V|, n - \sigma + 1\}. \qquad (27)$$

It follows that $T = e_1^{[n-r]} \boldsymbol{\cdot} U' \boldsymbol{\cdot} V(I)$ is a non-empty zero-sum subsequence of S with

$$|T| = n - r + |U'| + |I| = 2n + |I| - \sigma - r.$$

We handle two short subcases based on which quantity attains the minimum in (27).

If $n - \sigma + 1 \leq k + 1 - |V|$, then (27) implies $|T| \leq 2n + |I| - \sigma - (n - \sigma + 1) = n + |I| - 1 \leq 2n - k - 1$, with the latter inequality in view of $|I| \leq |V| \leq n - k$, contradicting (20). If $k + 1 - |V| \leq n - \sigma + 1$, then (26) and (27) imply $|T| \leq 2n - |V| - (k + 1 - |V|) = 2n - 1 - k$, contradicting (20). As this covers all cases, Step A is complete.

In view of Step A and (22), we have $n - k + 1 \leq |V| \leq k - 1$, implying

$$k \geq \frac{n+2}{2}. \qquad (28)$$

Step B: $s \leq 2k - 1 - n$.

Assume by contradiction that $s \geq 2k - n$, so

$$h = \mathsf{h}(\pi_1(U)) \leq |U| - 2k + n. \qquad (29)$$

In view of Step A, let $V' \mid V$ be a subsequence with length $n - k$, say the first $n - k$ terms in V. Since $\overline{\pi_2(V')} = x_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} x_{n-k} \in \mathcal{F}([2, n-1])$, we can apply Lemma 16 to $\overline{\pi_2(V')}$ to find a nonempty subset $I \subseteq [1, n-k]$ such that

$$\sigma := \overline{\sigma\big(\pi_2(V')(I)\big)} \geq |I| + \min\{\lceil \frac{n-1}{2} \rceil, n - k\} = |I| + n - k, \qquad (30)$$

with the final equality above in view of (28). Then

$$m := n - \sigma \leq k - |I| \leq k - 1.$$

Let $b = \sigma\big(\pi_1(V')(I)\big)$. If $m = 0$, then $T = e_1^{[n-\bar{b}]} \boldsymbol{\cdot} V'(I)$ is a non-empty zero-sum subsequence of V with length $|T| \leq n - 1 + |I| \leq n - 1 + |V'| = 2n - 1 - k$, contradicting (20). Therefore we may assume $m \geq 1$. In view of (24), we can now apply Lemma 18 to $\pi_1(U)$ to find a subsequence $U' \mid U$ with $|U'| = n - \sigma$ and

$$r = \overline{b + \sigma\big(\pi_1(U')\big)} \geq \min\{n,\, m + 1, |U| - m + 1, |U| - h + 1, |U| - \frac{n}{2} + 1\}. \qquad (31)$$

It follows that $T = e_1^{[n-r]} \cdot U' \cdot V(I)$ is a non-empty zero-sum subsequence of S with

$$|T| = n - r + |U'| + |I| = 2n + |I| - \sigma - r \leq n + k - r,$$

with the latter inequality above in view of (30). We handle five short subcases based on which quantity attain the minimum in (31).

If $r \geq n$, then $|T| \leq n+k-n = k \leq n-2$, contrary to (20). If $r \geq m+1 = n-\sigma+1$, then $|T| \leq 2n + |I| - \sigma - (n - \sigma + 1) = n + |I| - 1 \leq 2n - k - 1$ (in view of $|I| \leq |V'| \leq n - k$), contrary to (20). If $r \geq |U| - m + 1 = |U| - n + \sigma + 1$, then

$$\begin{aligned}|T| &\leq 2n + |I| - \sigma - (|U| - n + \sigma + 1) = 3n + |I| - 1 - |U| - 2\sigma \\ &\leq n + 2k - |I| - 1 - |U| \leq 2k - 2,\end{aligned}$$

with the second inequality from (30), and the third in view of $|I| \geq 1$ and $|U| \geq n$. Combined with (20), it follows that $2n-k \leq 2k-2$, implying $k \geq \frac{2n+2}{3}$, contrary to hypothesis. If $r \geq |U|-h+1$, then $|T| \leq n+k-|U|+h-1 \leq 2n-1-k$ (in view of (29)), contrary to (20). Finally, if $r \geq |U| - \frac{n}{2} + 1$, then $|T| \leq n + k - |U| + \frac{n}{2} - 1 \leq k - 1 + \frac{n}{2}$, with the latter inequality in view of $|U| \geq n$. Combined with (20), it follows that $2n - k \leq k - 1 + \frac{n}{2}$, implying $k \geq \frac{3n+2}{4} \geq \frac{2n+2}{3}$, contrary to hypothesis. As this exhausts all possibilities, Step B is complete.

In view of Step B, $|U| \geq n$ and $k \leq \frac{2n+1}{3}$, it follows that

$$h = \mathsf{v}_0(\pi_1(U)) \geq |U| - 2k + 1 + n \geq 2n - 2k + 1 \geq \frac{2n+1}{3}. \tag{32}$$

Partition $V = V_2 \cdot V_{1/2} \cdot V_0$, where $V_2 \mid V$ consists of all terms x with $\pi_2(x) = 2e_1$, $V_{1/2} \mid V$ consists of either all terms x with $\pi_2(x) = \lceil \frac{n+1}{2} \rceil e_1$ (if there are no such terms or an odd number) or else all but one of the terms x with $\pi_2(x) = \lceil \frac{n+1}{2} \rceil e_1$ (if there are a nonzero even number of such terms), and V_0 contains all other terms. Note $|V_{1/2}|$ is either 0 or odd by construction. To reduce floor and ceiling use, let

$$\lceil \frac{n+1}{2} \rceil = \frac{n+\epsilon}{2}, \quad \text{ so } \epsilon \in [1,2] \text{ with } \epsilon \equiv n \mod 2.$$

Partition $[1, |V|] = J_2 \cup J_{1/2} \cup J_0$ with $V(J_2) = V_2$, $V(J_{1/2}) = V_{1/2}$ and $V(J_0) = V_0$. Let

$$\begin{aligned}&U \cdot e_2^{[-h]} = {\prod}^\bullet_{i\in[1,s]} (\alpha_i e_1 + e_2), \quad V_2 = {\prod}^\bullet_{i\in[1,|V_2|]} (\beta_i e_1 + 2e_2), \quad \text{and} \\ &V_{1/2} = {\prod}^\bullet_{i\in[1,|V_{1/2}|]} (\gamma_i e_1 + \frac{n+\epsilon}{2} e_2), \quad \text{where } \alpha_i \in [1, n-1] \text{ and } \beta_i, \gamma_i \in [1, n].\end{aligned}$$

Step C: $\beta_i \leq k - 2$ and $\gamma_j \leq k + 1 - \frac{n+\epsilon}{2} \leq \frac{n+8-3\epsilon}{6} \leq \frac{n+5}{6}$, for all $i \in [1, |V_2|]$ and $j \in [1, |V_{1/2}|]$.

Suppose $\beta_i = n$ for some i, i.e., $2e_2 \in \text{Supp}(V)$. Let $S' = S \boldsymbol{\cdot} (2e_2)^{[-1]} \boldsymbol{\cdot} e_2 \boldsymbol{\cdot} e_2$. Then $|S'| = |S| + 1 = \mathsf{D}(G) + k$, whence $0 \in \Sigma_{\leq \mathsf{D}(G)-k}(S')$ by Theorem 1. Thus there is a nonempty zero-sum subsequence $T' \mid S'$ with $|T'| \leq \mathsf{D}(G) - k$. If $\mathsf{v}_{e_2}(T') \geq 2$, then $T = T' \boldsymbol{\cdot} e_2^{[-2]} \boldsymbol{\cdot} 2e_2$ is a nonempty zero-sum subsequence of T with $|T| = |T'| - 1 \leq \mathsf{D}(G) - k - 1 = 2n - 2 - k$, contrary to (20). On the other hand, if $\mathsf{v}_{e_2}(T') \leq 1$, then $T' \mid S$ (since $\mathsf{v}_{e_2}(S) = h \geq 1$) is a non-empty zero-sum subsequence with $|T| = |T'| \leq 2n - 1 - k$, contrary to (20). So we instead conclude that $\beta_i \leq n - 1$ for all i. Next consider $T = e_1^{[n-\beta_i-1]} \boldsymbol{\cdot} (\beta_i e_1 + 2e_2) \boldsymbol{\cdot} \prod^\bullet_{j\in[1,n]}(a_j e_1 + e_2) \boldsymbol{\cdot} e_2^{[-2]}$. Note T is a nonempty subsequence in view of $\beta_i \leq n - 1$ and Step B, which ensures that $\mathsf{v}_{e_2}\left(\prod^\bullet_{j\in[1,n]}(a_j e_1 + e_2)\right) \geq n - (2k - 1 - n) = 2n - 2k + 1 \geq 2$. Moreover, T is zero-sum since $a_1 + \ldots + a_n \equiv 1 \mod n$ (from (21)). Thus (20) implies $2n - k \leq |T| = n - \beta_i + n - 2$, whence $\beta_i \leq k - 2$, as desired.

Suppose $\gamma_i \geq k+2-\frac{n+\epsilon}{2}$ for some $i \in [1, |V_{1/2}|]$. Then, since $h \geq \frac{2n+1}{3} \geq n - \frac{n+\epsilon}{2}$, it follows that $T = e_1^{[n-\gamma_i]} \boldsymbol{\cdot} (\gamma_i e_1 + \frac{n+\epsilon}{2} e_2) \boldsymbol{\cdot} e_2^{[\frac{n-\epsilon}{2}]}$ is a nonempty zero-sum subsequence of S with $|T| = n - \gamma_i + 1 + \frac{n-\epsilon}{2} \leq 2n - 1 - k$, contrary to (20). So we instead conclude that $\gamma_i \leq k + 1 - \frac{n+\epsilon}{2} \leq \frac{n+8-3\epsilon}{2}$ for all i, with the latter inequality in view of $k \leq \frac{2n+1}{3}$, completing Step C.

Step D: $\mathsf{v}_{\frac{n}{2}e_1+e_2}(S) \leq 1$

Assume to the contrary that $\mathsf{v}_{\frac{n}{2}e_1+e_2}(S) \geq 2$, which necessarily means n is even. Let $S' = S \boldsymbol{\cdot} (\frac{n}{2}e_1 + e_2)^{[-2]} \boldsymbol{\cdot} e_2 \boldsymbol{\cdot} e_2$. Then $|S'| = |S|$ and $\mathsf{h}(\pi_1(U')) = \mathsf{h}(\pi_1(U)) + 2$, where $U' \mid S'$ consists of all terms x with $\pi_2(x) = e_2$. Suppose there were a nonempty zero-sum subsequence $T' \mid S'$ with $|T'| \leq \mathsf{D}(G) - k$. If $\mathsf{v}_{e_2}(T') \geq 2$, then $T = T' \boldsymbol{\cdot} e_2^{[-2]} \boldsymbol{\cdot} (\frac{n}{2}e_1 + e_2)^{[2]}$ is a nonempty zero-sum subsequence of T with $|T| = |T'| \leq \mathsf{D}(G) - k = 2n-1-k$, contrary to (20). On the other hand, if $\mathsf{v}_{e_2}(T') \leq 1$, then $T' \mid S$ (since $\mathsf{v}_{e_2}(S) = h \geq 1$) is a nonempty zero-sum subsequence with $|T| = |T'| \leq 2n - 1 - k$, contrary to (20). So we instead conclude $0 \notin \Sigma_{\mathsf{D}(G)-k}(S')$. If the lemma holds for S' with basis (e_1', e_2'), then $\mathsf{v}_{e_1}(S') = n - 1$ forces $e_1' = e_1$ or $e_2' = e_1$, say w.l.o.g $e_1' = e_1$, and then also $\pi_2(x)$ is constant for all $x \neq e_1$ that occur in S'. However, the latter condition fails for S' as $|V| \geq 1$. Therefore S' is also a counterexample to the lemma, and one with $\mathsf{h}(\pi_1(U')) > \mathsf{h}(\pi_1(U)) = h$, contradicting the maximality of h. So we instead conclude that $\mathsf{v}_{\frac{n}{2}e_1+e_2}(S) \leq 1$, completing Step D.

Step E: $|V_0| \leq \frac{1}{3}n - 1$.

Assume to the contrary that $|V_0| \geq \frac{n-2}{3}$. Let $V_0' \mid V_0$ be a subsequence with $|V_0'| = \lceil \frac{n-2}{3} \rceil \leq \frac{1}{3}n$, say $V_0' = V_0(J_0')$ with $J_0' \subseteq J_0$. If $2|V_0'| \leq \lfloor \frac{2n-2}{3} \rfloor - 1 \leq \frac{2n-5}{3}$, then equality cannot hold in this inequality (as then $\frac{2n-5}{3}$ must be an even integer, which is never the case), whence $2|V_0'| \leq \frac{2n-6}{3}$, implying $|V_0'| \leq \frac{n-3}{3}$, contrary to assumption. Therefore $2|V_0'| \geq \lfloor \frac{2n-2}{3} \rfloor$. By construction, $\overline{\pi_2(V_0)} \in \mathcal{F}([3, n-1])$ with at most one term of $\overline{\pi_2(V_0)}$ equal to $\lceil \frac{n+1}{2} \rceil$. Thus we can apply Lemma 17 to

$\overline{\pi_2(V_0')}$ and thereby find a nonempty subset $I \subseteq J_0'$ with

$$\sigma := \overline{\sigma\big(\pi_2(V_0)(I)\big)} \geq |I| + \min\{\lfloor \frac{2n-2}{3} \rfloor, 2|V_0'|\} = |I| + \lfloor \frac{2n-2}{3} \rfloor. \tag{33}$$

If $\sigma = n$, then $T = e_1^{[n-b]} \cdot V_0(I)$ is a nonempty zero-sum subsequence, where $b = \overline{\sigma(\pi_1(V_0)(I))}$, with $|T| \leq n-1+|I| \leq n-1+|V_0'| \leq \frac{4}{3}n - 1 < 2n-k$, with the final inequality in view of $k \leq \frac{2n+1}{3}$, contradicting (20). Therefore $\sigma < n$. By (33), (32) and $|I| \geq 1$, we have $n - \sigma \leq n - |I| - \lfloor \frac{2n-2}{3} \rfloor \leq \frac{n+1}{3} \leq h$. Thus $T_i = e_1^{[n-b_i]} \cdot V_0'(I) \cdot e_2^{[n-\sigma-1]} \cdot (a_i e_1 + e_2)$ is a non-empty zero-sum subsequence of S for any $i \in [1,n]$, where $b_i = \overline{\sigma(\pi_1(V_0)(I)) + a_i e_1}$. Since $a_1 + \ldots + a_n \equiv 1 \mod n$ by (21), not all a_i can equal zero, meaning there are two distinct choices for the value of a_i, and thus two distinct possibilities for b_i. It follows that $b_i \geq 2$ for some $i \in [1,n]$, and now $T_i \mid S$ is a nonempty zero-sum subsequence with $|T| \leq n - b_i + n - \sigma + |I| \leq 2n-2+|I|-\sigma \leq 2n-2-\lfloor \frac{2n-2}{3} \rfloor \leq n + \frac{n-2}{3} < 2n-k$, with the third inequality by (33) and the final inequality in view of $k \leq \frac{2n+1}{3}$, contradicting (20), which completes Step E.

In view of Step E, we have

$$2|V_0| \leq \lfloor \frac{2n-2}{3} \rfloor. \tag{34}$$

Step F: $|V_{1/2}| = 0$.

Assume to the contrary that $|V_{1/2}| > 0$, and thus $|V_{1/2}|$ is odd. Observe that

$$U \cdot e_2^{[-h]} \cdot V_2 \cdot V_{1/2} = \prod\nolimits^\bullet_{i\in[1,s]} (\alpha_i e_1 + e_2) \cdot \prod\nolimits^\bullet_{i\in[1,|V_2|]} (\beta_i e_1 + 2e_2) \cdot$$
$$(\gamma_1 e_1 + \frac{n+\epsilon}{2} e_2) \cdot \prod\nolimits^\bullet_{i\in[1,\frac{1}{2}(|V_{1/2}|-1)]} \Big((\gamma_{2i} e_1 + \frac{n+\epsilon}{2} e_2) \cdot (\gamma_{2i+1} e_1 + \frac{n+\epsilon}{2} e_2) \Big).$$

Let

$$\ell = s + |V_2| + \frac{1}{2}(|V_{1/2}| - 1)$$

and define sequences T_i for $i \in [1,\ell]$ as follows:

$$\begin{aligned} T_i &= \alpha_i e_1 + e_2 && \text{for } i \in [1,s], \\ T_i &= \beta_j e_1 + 2e_2 && \text{for } i = s+j \in [s+1, s+|V_2|], \\ T_i &= (\gamma_{2j} e_1 + \frac{n+\epsilon}{2} e_2) \cdot (\gamma_{2j+1} e_1 + \frac{n+\epsilon}{2} e_2) && \text{for } i = s+|V_2|+j \\ & && \quad \text{with } j \geq 1. \end{aligned}$$

Note

$$|T_i| = \begin{cases} 1 & i \leq s+|V_2| \\ 2 & i \geq s+|V_2|+1 \end{cases} \quad \text{and} \quad \overline{\sigma(\pi_2(T_i))} = \begin{cases} 1 & i \leq s \\ 2 & s+1 \leq i \leq s+|V_2| \\ \epsilon & i \geq s+|V_2|+1. \end{cases}$$

Moreover, $1 \le \overline{\sigma(\pi_1(T_i))} \le n-1$ for $i \le s+|V_2|$ (by definition of the α_i and Step C), and (also by Step C)

$$2 \le \overline{\sigma(\pi_1(T_i))} \le 2k+2-n-\epsilon \le \frac{n+8-3\epsilon}{3} \le n-1 \quad \text{for } i \ge s+|V_2|+1. \quad (35)$$

Since $s \ge 1$, we have $\ell \ge 1$. Since $h \le n-1$ and $|U|+|V| = n-1+k$, Step E implies $s+|V_2|+|V_{1/2}| = |U|+|V|-h-|V_0| \ge (n-1+k)-(n-1)-(\frac{n}{3}-1) = k-\frac{n}{3}+1$. In summary:

$$s+|V_2|+|V_{1/2}| \ge k-\frac{n}{3}+1. \quad (36)$$

By (32), we have $h \ge \frac{n-\epsilon}{2} \ge 1$. If $\sum_{i=1}^{\ell}\overline{\sigma(\pi_2(T_i))} \ge \frac{n-\epsilon}{2}$, then let $\ell' \le \ell$ be the maximal index with $\sum_{i=1}^{\ell'}\overline{\sigma(\pi_2(T_i))} \le \frac{n-\epsilon}{2}$, in which case $\sum_{i=1}^{\ell'}\overline{\sigma(\pi_2(T_i))} = \frac{n-\epsilon}{2}$ or $\frac{n-\epsilon}{2}-1$. Otherwise, let $\ell' = \ell$. Since $s \ge 1$ and $\frac{n-\epsilon}{2} \ge 1$, we have $\ell' \ge 1$. Consider an arbitrary sequence T formed as follows. Begin with $\gamma_1 e_1 + \frac{n+\epsilon}{2}e_2$ and sequentially concatenate additional terms as follows. For each $i \in [1, \min\{s, \ell'\}]$, choose to either concatenate a term equal to e_2 or the sequence $T_i = \alpha_i e_1 + e_2$. Next, we proceed to concatenate the sequences $T_i = \beta_j e_1 + 2e_2$ for $i = s+j \in [s+1, \min\{\ell', s+|V_2|\}]$. For each $i = s+|V_2|+j \in [s+|V_2|+1, \ell']$, choose to either concatenate a term equal to e_2 or else concatenate the sequence $T_i = (\gamma_{2j}e_1 + \frac{n+\epsilon}{2}e_2)(\gamma_{2j+1}e_1 + \frac{n+\epsilon}{2}e_2)$ instead. If $\sum_{i=1}^{\ell'}\overline{\sigma(\pi_2(T_i))} < \frac{n-\epsilon}{2}$, concatenate an additional $\frac{n-\epsilon}{2} - \sum_{i=1}^{\ell'}\overline{\sigma(\pi_2(T_i))}$ terms each equal to e_2. Then the sum of the sequence as so constructed lies in $\langle e_1\rangle$, say equal to be_1. Complete the construction of T by now concatenating the sequence $e_1^{[n-\overline{b}]}$ to yield a nonempty zero-sum subsequence $T \mid S$ (T is a subsequence of S in view of $h \ge \frac{n-\epsilon}{2}$).

Let $x = \gamma_1 e_1 + \sum \beta_j e_1$, where the sum runs over all $j \in [1, |V_2|]$ with $s+j \le \ell'$. The possibilities for be_1 are precisely those elements from the sumset

$$B := x + \sum_{i=1}^{\min\{\ell', s\}} \{0,\ \alpha_i e_1\} + \sum_{i=s+|V_2|+j\in[s+|V_2|+1,\ell']} \{0,\ (\gamma_{2j}+\gamma_{2j+1})e_1\}$$

Note that B is a sumset of (say) $m \ge 1$ cardinality two subsets: we have $m \ge 1$ since ℓ', $s \ge 1$, and the sets have cardinality two since $\overline{\sigma(\pi_1(T_i))} \le n-1$ for all i as remarked at the start of Step F. Apply Kneser's Theorem to B and let $H = \mathsf{H}(B)$. If H is trivial, then Kneser's theorem implies there is some $be_1 \in B$ with $\overline{b} \ge m+1$. If $|H| \ge 2$, then there will be some $be_1 \in B$ with $\overline{b} \ge \frac{n}{2}+1 > \frac{n-\epsilon}{2}+1 \ge \ell'+1 \ge m+1$. In either case, we find some $be_1 \in B$ with

$$\overline{b} \ge m+1. \quad (37)$$

We proceed in several short subcases.

Suppose $\ell' = \ell$ and $\ell' \leq s$. Then, since $\ell \geq s$, we conclude that $\ell = \ell' = s$, in which case $|V_2| = 0$, $|V_{1/2}| = 1$ and $m = s$. It follows that $|T| = n - \overline{b} + \frac{n-\epsilon}{2} + 1 \leq \frac{3n-\epsilon}{2} - s \leq \frac{3n-\epsilon}{2} - k + \frac{n}{3} < 2n - k$, with the first inequality by (37) and the second by (36), which contradicts (20).

Suppose $\ell' < \ell$ and $\ell' \leq s$. Then $\ell' = m = \frac{n-\epsilon}{2}$, and $|T| = n - \overline{b} + \frac{n-\epsilon}{2} + 1 \leq n$ follows by (37), contradicting (20).

Suppose $\ell' = \ell$ and $s + 1 \leq \ell' \leq s + |V_2|$. Then $|V_{1/2}| = 1$, $\ell' = \ell = s + |V_2|$ and $m = s$. It follows that $|T| = n - \overline{b} + \frac{n-\epsilon}{2} + 1 - |V_2| \leq \frac{3n-\epsilon}{2} - s - |V_2| \leq \frac{3n-\epsilon}{2} - k + \frac{n}{3} < 2n - k$, with the first inequality by (37), and the second by (36), contradicting (20).

Suppose $\ell' < \ell$ and $s + 1 \leq \ell' \leq s + |V_2|$. Then $\ell' = \lfloor \frac{1}{2}(\frac{n-\epsilon}{2} - s) \rfloor + s$ and $m = s$. It follows that $|T| = n - \overline{b} + s + 1 + \lceil \frac{1}{2}(\frac{n-\epsilon}{2} - s) \rceil \leq n + \lceil \frac{1}{2}(\frac{n-\epsilon}{2} - s) \rceil \leq \frac{5}{4}n < 2n - k$, with the first inequality by (37), the second as $\epsilon \geq 1$ and $s \geq 1$, and third in view of $k \leq \frac{2n+1}{3}$ and $n \geq 5$, contradicting (20).

Suppose $\ell' = \ell$, $\ell' \geq s + |V_2| + 1$ and n is even. Then $|V_{1/2}| \geq 3$, $\epsilon = 2$, $\ell' = s + |V_2| + \frac{1}{2}(|V_{1/2}| - 1)$ and $m = s + \frac{1}{2}(|V_{1/2}| - 1)$. It follows that $|T| = n - \overline{b} + 1 + \frac{n-\epsilon}{2} - |V_2| \leq n - s - \frac{1}{2}(|V_{1/2}| - 1) + \frac{n-\epsilon}{2} - |V_2| = \frac{3}{2}n - \ell - 1$, with the inequality by (37). In view of (36), $s \geq 1$ and the definition of ℓ, we find that $\ell \geq \frac{1}{2}(k - \frac{n}{3} - s) + s \geq \frac{k}{2} - \frac{n}{6} + \frac{1}{2}$. Combined with the previous estimate, we obtain $|T| \leq \frac{5}{3}n - \frac{k}{2} - \frac{3}{2} < 2n - k$, with the latter inequality in view of $k \leq \frac{2n+1}{3}$, contradicting (20).

Suppose $\ell' < \ell$, $\ell' \geq s + |V_2| + 1$ and n is even. Then $|V_{1/2}| \geq 3$, $\epsilon = 2$, and $m = s + \lfloor \frac{1}{2}(\frac{n-\epsilon}{2} - 2|V_2| - s) \rfloor = \lfloor \frac{n-2+2s}{4} \rfloor - |V_2| \geq \frac{n}{4} - \frac{1}{2} - |V_2|$. It follows that $|T| = n - \overline{b} + 1 + \frac{n-\epsilon}{2} - |V_2| \leq \frac{5}{4}n - \frac{1}{2} < 2n - k$, with the first inequality by (37), and the second in view of $k \leq \frac{2n+1}{3}$, contradicting (20).

In view of the above cases, it remains to consider when $\ell' \geq s + |V_2| + 1$ with n odd, so $\epsilon = 1$, $|V_{1/2}| \geq 3$ and $m > s$. We aim to improve the estimate (37) as follows:

$$\overline{b} \geq 2m - s + 1 \tag{38}$$

for some $be_1 \in B$. Let $B_0 = x + \sum_{i=1}^{s} \{0, \alpha_i e_1\}$, and for $t \in [0, m - s]$, let B_t be the sum of the first $s + t$ summands in the definition of B, so

$$B_t = B_{t-1} + \{0, (\gamma_{2t} + \gamma_{2t+1})e_1\} \quad \text{ for } t \geq 1.$$

We proceed inductively to show $|\max \overline{B_t}| \geq s + 1 + 2t$ for $t = 0, 1, \ldots, m - s$. Then the case $t = m - s$ will yield the desired bound (38). For $t = 0$, the argument used to establish (37) applied to B_0 rather than B yields $\max \overline{B_0} \geq |B_0| \geq s + 1$, which completes the base of the induction. Now assume $t \geq 1$. The elements $b \in B_{t-1}$ are the possibilities for those constructed sequences T that use 0 rather than $(\gamma_{2j} + \gamma_{2j+1})e_1$ for all $j \geq t$. For such T, we have $|T| \leq n - \overline{b} + \frac{n+1}{2} + t - 1$.

Since (20) ensures $|T| \geq 2n-k$, it follows that $\overline{b} \leq k - \frac{n+1}{2} + t$. This shows that

$$\max \overline{B_{t-1}} \leq k - \frac{n+1}{2} + t.$$

By (35), we have

$$2 \leq \gamma_{2t} + \gamma_{2t+1} \leq 2k+1-n.$$

Consequently, if $(2k+1-n) + (k - \frac{n+1}{2} + t) \leq n$, then adding $(\gamma_{2t} + \gamma_{2t+1})$ to the largest element $\overline{b'} \in \overline{B_{t-1}}$ yields an element $\overline{b} \in \overline{B_t}$ with $2 + \overline{b'} \leq \overline{b} \leq n$, and thus with $\overline{b} \geq s+1+2(t-1)+2 = s+1+2t$ by induction hypothesis, as desired. Assuming instead that $(2k+1-n)+(k-\frac{n+1}{2}+t) \geq n+1$, it follows that $\frac{1}{2}(|V_{1/2}|-1) \geq t \geq \frac{5}{2}n + \frac{1}{2} - 3k$. However, we have $|V_{1/2}| \leq |V| \leq k-1$ by (22), yielding $\frac{k-2}{2} \geq \frac{5}{2}n + \frac{1}{2} - 3k$, and thus $k \geq \frac{5n+3}{7}$. This contradicts that $k \leq \frac{2n+1}{3}$, completing the induction and thereby establishing the desired improvement (38). We are now ready to finish the last two subcases.

Suppose $\ell' = \ell$, $\ell' \geq s + |V_2| + 1$ and n is odd. Then $|V_{1/2}| \geq 3$, $\epsilon = 1$, $\ell' = s + |V_2| + \frac{1}{2}(|V_{1/2}|-1)$ and $m = s + \frac{1}{2}(|V_{1/2}|-1)$. It follows that $|T| = n - \overline{b} + 1 + \frac{n-1}{2} - |V_2| + \frac{1}{2}(|V_{1/2}|-1) \leq \frac{3}{2}n - |V_2| - \frac{1}{2}|V_{1/2}| - s = \frac{3}{2}n - \ell - \frac{1}{2}$, with the inequality in view of (38). In view of (36) and $s \geq 1$, we have $\ell \geq \frac{1}{2}(k - \frac{n}{3} - s) + s \geq \frac{k}{2} - \frac{n}{6} + \frac{1}{2}$. Combined with the previous estimate, we find that $|T| \leq \frac{5}{3}n - \frac{k}{2} - 1 < 2n - k$, with the latter inequality in view of $k \leq \frac{2n+1}{3}$, contradicting (20).

Suppose $\ell' < \ell$, $\ell' \geq s + |V_2| + 1$ and n is odd. Then $|V_{1/2}| \geq 3$, $\epsilon = 1$, and $m = \frac{n-1}{2} - 2|V_2|$. Moreover, by definition of $\ell' < \ell$, we have

$$\frac{n-1}{2} \geq \sum_{i=1}^{\ell'} \overline{\sigma(\pi_2(T_i))} \geq s + 2|V_2| + 1, \tag{39}$$

with the latter inequality following in view of $\ell' \geq s + |V_2| + 1$, and the former in view of $\epsilon = 1$. It follows that $|T| = n - \overline{b} + 1 + s + |V_2| + 2(\frac{n-1}{2} - s - 2|V_2|) = 2n - \overline{b} - s - 3|V_2| \leq n + |V_2|$, with the inequality in view of (38). As a result, (20) implies that $|V_2| \geq n-k$. However, (39) and $s \geq 1$ imply $|V_2| \leq \frac{n-5}{4}$, which combined with $n-k \leq |V_2|$ yields $k \geq \frac{3n+5}{4}$, contradicting the hypothesis $k \leq \frac{2n+1}{3}$, and completing the final subcase in Step F.

Since $\overline{\pi_2(V_0)} \in \mathcal{F}([3, n-1])$ with at most one term of $\overline{\pi_2(V_0)}$ equal to $\lceil \frac{n+1}{2} \rceil$ (by construction), we can apply Lemma 17 to $\overline{\pi_2(V_0)}$ and thereby find a nonempty subset $I \subseteq J_0$ with

$$\sigma := \overline{\sigma\big(\pi_2(V_0)(I)\big)} \geq |I| + \min\{\lfloor \frac{2n-2}{3} \rfloor, 2|V_0|\} = |I| + 2|V_0|, \tag{40}$$

with the latter equality in view of (34). Note, if $|V_0| = 0$, then we simply take I to be the empty set and set $\sigma = 0$ (without using Lemma 17). In view of (32) and $k \leq \frac{2n+1}{3}$, it follows that

$$h \geq 2n - 2k + 1 \geq k.$$

Let

$$s' = \min\{s,\, s-(n-\sigma-h)\}.$$

We claim that

$$|V_0| + |V_2| + s' \geq k-1, \tag{41}$$

with equality only possible if $s' < s$ and $|V_0| = 0$. Indeed, if $s' = s$, then Step F implies $|V_0|+|V_2|+s' = |V_0|+|V_2|+s = |U|+|V|-h = n-1+k-h \geq k$, with the final inequality in view of $h \leq n-1$ (by (23)). On the other hand, if $s' < s$, then $|V_0|+|V_2|+s' = |V_0|+|V_2|+s-(n-\sigma-h) = |U|+|V|-h-(n-\sigma-h) = k-1+\sigma \geq k-1+2|V_0|$, with the final inequality from (40). Thus (41) is established with the stated equality conditions.

By construction,

$$e_2^{[\min\{h,n-\sigma\}]} \cdot \prod\nolimits^{\bullet}_{i\in[s'+1,s]}(\alpha_i e_1 + e_2) = z_1 \cdot \ldots \cdot z_{n-\sigma} \tag{42}$$

is a subsequence of S with length $n-\sigma$, where $z_i = e_2$ for $i \leq \min\{h, n-\sigma\}$, and $z_{\min\{h,n-\sigma\}+i} = \alpha_{s'+i}e_1 + e_2$ for $i \in [1, s-s']$.

Step G: $s' \leq n-\sigma-2$ and $s' \leq \frac{1}{2}(h-1) < h-1$.

Note $s' \leq s \leq 2k-1-n \leq n-k \leq \frac{1}{2}(h-1) < h-1$, with the second inequality by Step B, the third in view of $k \leq \frac{2n+1}{3}$, the fourth from (32), and the fifth as $h \geq \frac{2n+1}{3} > 1$ (in view of (32)).

Letting $a = \overline{\sigma(\pi_1(V_0)(I)) + \alpha_{s'+1}e_1 + \ldots + \alpha_s e_1}$, it follows that $e_1^{[n-a]} \cdot V_0(I) \cdot z_1 \cdot \ldots \cdot z_{n-\sigma}$ is a nonempty zero-sum sequence of length $2n-a+|I|-\sigma \leq 2n-1+|V_0|-\sigma \leq 2n-2+\lfloor\frac{n}{3}\rfloor-\sigma$, with the latter inequality in view of Step E. Consequently, (20) ensures that $2n-k \leq 2n-2+\lfloor\frac{n}{3}\rfloor-\sigma$, in turn implying $\sigma \leq \lfloor\frac{n}{3}\rfloor+k-2 \leq \lfloor\frac{n}{3}\rfloor+\lfloor\frac{2n+1}{3}\rfloor-2 \leq n-2$. Let $m = n-\sigma \geq 2$ and $b = \sigma(\pi_1(V_0)(I))$. In view of (24) and $|U| \geq n$, we can apply Lemma 18 to $\pi_1(U)$ to find a subsequence $U' \mid U$ with $|U'| = n-\sigma$ and

$$r = \overline{b + \sigma\big(\pi_1(U')\big)} \geq \min\{n,\, m+1, |U|-m+1, |U|-h+1, |U|-\frac{n}{2}+1\}. \tag{43}$$

It follows that $T = e_1^{[n-r]} \cdot U' \cdot V_0(I)$ is a non-empty zero-sum subsequence of S with

$$2n-k \leq |T| = n-r+|U'|+|I| = 2n+|I|-\sigma-r, \tag{44}$$

with the first inequality above in view of (20).

In view of Step B, $k \leq \frac{2n+1}{3}$ and $|U| \geq n$, we have $s'+1 \leq s+1 \leq 2k-n \leq \frac{n}{2}+1 \leq n$ and $s'+1 \leq \frac{n}{2}+1 \leq |U|-\frac{n}{2}+1$. We also have $s'+1 \leq s+1 = |U|-h+1$. If $h \leq m = n-\sigma$, then $s'+1 = |U|-m+1$, while $h \geq m = n-\sigma$ implies $s'+1 = s+1 \leq h+s-m+1 = |U|-m+1$. Thus (43) implies

$$r \geq \min\{m+1, s'+1\} \geq \min\{m, s'+1\}.$$

If $s' \geq m-1$, then $r \geq m = n-\sigma$. In this case, (44) and Step E yield $2n-k \leq n+|I| \leq n+|V_0| \leq \frac{4n}{3}-1$, contradicting $k \leq \frac{2n+1}{3}$. Therefore $s' \leq m-2 = n-\sigma-2$, completing Step G.

Step H: $s' + 2|V_2| \geq n-\sigma+1$.

Assume to the contrary that $s' + 2|V_2| \leq n-\sigma$. Consider an arbitrary sequence T formed as follows. Begin with

$$V_0(I) \cdot V_2 \cdot z_{2|V_2|+s'+1} \cdot \ldots \cdot z_{n-\sigma}.$$

For each $i \in [1, s']$, choose to either concatenate the term $z_i = e_2$ (in view of Step G) or the term $\alpha_i e_1 + e_2$. In view of $s' + 2|V_2| \leq n-\sigma$, the sum of the sequence as so constructed lies in $\langle e_1 \rangle$, say equal to be_1. Complete the construction of T by now concatenating the sequence $e_1^{[n-\overline{b}]}$ to yield a nonempty zero-sum subsequence $T \mid S$. Note T being empty would imply $|I| = 0$ and $n-\sigma = 0$, while $|I| = 0$ is only possible by construction when $|V_0| = 0 = \sigma$, contradicting that $n-\sigma = 0$. Also,

$$|T| = 2n - \overline{b} + |I| - \sigma - |V_2| \leq 2n - \overline{b} - |V_2| - 2|V_0|, \tag{45}$$

with the inequality from (40). Let $x = \sigma\big(\pi_1\big(V_0(I) \cdot V_2 \cdot z_{2|V_0|+s'+1} \cdot \ldots \cdot z_{n-\sigma}\big)\big)$. Let

$$B_0 = \{0, \alpha_1 e_1\} + \ldots + \{0, \alpha_{s'} e_1\},$$

which is a sum of $s' \geq 0$ cardinality two sets in view of the definition of the α_i. The possibilities for be_1 are precisely the elements from the sumset $x + B_0$. Let $H = \mathsf{H}(B_0)$ and apply Kneser's Theorem to B_0. If H is trivial, then Kneser's Theorem implies $|B_0| \geq s'+1$, in which case there is some $be_1 \in x + B_0$ with $\overline{b} \geq s'+1$. On the other hand, if $|H| \geq 2$, then there is some $be_1 \in x + B_0$ with $\overline{b} \geq \frac{n}{2} + 1 > 2k - n \geq s + 1 \geq s' + 1$, with the second inequality since $k \leq \frac{2n+1}{3}$ and the third from Step B. In either case, we can find some such zero-sum subsequence T with $\overline{b} \geq s'+1$, with equality only possible if $\overline{x + B_0} = [1, s'+1]$. Thus (45) and (41) imply $|T| \leq 2n - 1 - s' - |V_2| - 2|V_0| \leq 2n - k - |V_0| \leq 2n - k$. Combined with (20), we conclude that $|T| = 2n-k$, and so equality must hold in all estimates used to derive $|T| \leq 2n-k$. In particular, equality holds in (45) and (41), ensuring $s' < s$, and thus $h < n - \sigma$, and we must also have

$$|V_0| = 0 \quad \text{and} \quad \overline{x + B_0} = [1, s'+1].$$

Since $s' \leq h - 2 < n - \sigma - 2$ (by Step G), it follows that $z_{s'+1} = z_{s'+2} = e_2$. Since $V = V_0 \cdot V_2$ (By Step F) with $|V| \geq 1$ and $|V_0| = 0$, it follows that $|V_2| \geq 1$.

Now consider the sequence $T' = e_1^{[-(n-\overline{b})]} \cdot T \cdot (\beta_1 e_1 + 2e_2)^{[-1]} \cdot e_2^{[2]}$. Since $|V_2| \geq 1$ and $z_{s'+1} = z_{s'+2} = e_2$, it follows that $T' \mid S \cdot e_1^{[-(n-1)]}$. Let $b' e_1 = \sigma(\pi_1(T')) = (b - \beta_1)e_1$. In view of $\overline{x + B_0} = [1, s'+1]$, we see that

$$\overline{-\beta_1 + [1, s'+1]}$$

is the set of possible values for $\overline{b'}$. Now $e_1^{[n-\overline{b'}]} \cdot T'$ is a nonempty zero-sum subsequence of S with length

$$|T'| = |T| + 1 - \overline{b'} + \overline{b} = 2n - \overline{b'} - |V_2| + 1 = 2n - k + s' + 2' - \overline{b'},$$

with the second equality following as equality holds in (45) and $|V_0| = 0$, and the third equality holding as equality holds in (41) and $|V_0| = 0$. As a result, (20) implies $\overline{b'} \in [1, s' + 2]$. Consequently, since $\overline{-\beta_1 + [1, s' + 1]}$ is the set of possible values for $\overline{b'}$, we conclude that $\beta_1 \in \{n-1, n\}$ (note $s' \leq s \leq 2k - 1 - n < n - 1$ by Step B). However, this contradicts Step C, completing Step H.

Step I: $\lfloor \frac{n-\sigma-s'}{2} \rfloor \geq 2k - 1 - n - \sigma + |I|$

If Step I fails, we obtain $\frac{n-\sigma-s'-1}{2} \leq 2k - 2 - n - \sigma + |I|$, which implies $2k \geq \frac{3n+3}{2} + \frac{1}{2}\sigma - \frac{1}{2}s' - |I| \geq \frac{3n+3}{2} - \frac{1}{2}s' + |V_0| - \frac{1}{2}|I| \geq \frac{3n+3}{2} - \frac{1}{2}s' \geq 2n + 2 - k$, with the second inequality from (40), the third since $0 \leq |I| \leq |V_0|$, and the fourth from Step B and $s' \leq s$. However, this contradicts the hypothesis $k \leq \frac{2n+1}{3}$, completing Step I.

Let

$$t_0 = \lfloor \frac{\min\{h, n-\sigma\} - s'}{2} \rfloor \geq 1, \quad t = \lfloor \frac{n-\sigma-s'}{2} \rfloor \geq 1, \quad \text{and}$$
$$t_1 = \min\{t_0,\, t - 2k + 2 + n + \sigma - |I|\} \geq 1,$$

with the inequalities in view of Steps G and I. Note $t_0 \leq t$. Consider an arbitrary sequence T formed as follows. Begin with $V_0(I)$ and sequentially concatenate additional terms as follows. For each $i \in [1, s']$, choose to either concatenate the term $z_i = e_2$ (by Step G) or the term $\alpha_i e_1 + e_2$. Next, for each $i = s' + j \in [s' + 1, s' + t_1]$, choose to either concatenate the sequence $z_{s'+2j-1} \cdot z_{s'+2j} = e_2^{[2]}$ (in view of $t_1 \leq t_0$ and the definition of t_0) or the term $\beta_j e_1 + 2e_2$ (this term exists in view of Step H). For each $i = s' + j \in [s' + t_1 + 1, s' + t]$, concatenate the term $\beta_j e_1 + 2e_2$ (there are enough such terms $\beta_j e_1 + 2e_2$ in view of Step H). Finally, if $n - \sigma - s'$ is odd, so that $t < \frac{n-\sigma-s'}{2}$, concatenate the term $z_{n-\sigma}$. The sum of the sequence as so constructed lies in $\langle e_1 \rangle$, say equal to be_1. Complete the construction of T by now concatenating the sequence $e_1^{[n-\overline{b}]}$ to yield a nonempty zero-sum subsequence $T \mid S$. Note T being empty would imply $|I| = 0$ and $n - \sigma = 0$, while $|I| = 0$ is only possible by construction when $|V_0| = 0 = \sigma$, contradicting that $n - \sigma = 0$. By construction,

$$|T| = 2n - \overline{b} - \sigma + |I| - r_2(T), \qquad \text{where } r_2(T) \in [t - t_1, t] \tag{46}$$

denotes the number of terms in T of the form $\beta_j e_1 + 2e_2$. Note, by definition of t_1, we have

$$r_2(T) \geq t - t_1 \geq 2k - 2 - n - \sigma + |I|. \tag{47}$$

Let $x=\sigma(\pi_1(V_0)(I))+\sum_{j=t_1+1}^{t}\beta_j e_1$ (if $n-\sigma-s'$ is even) or $x=\sigma(\pi_1(V_0)(I))+\sum_{j=t_1+1}^{t}\beta_j e_1+\pi_1(z_{n-\sigma})$ (if $n-\sigma-s'$ is odd). For $j\in[0,t_1]$, let

$$B_j=\sum_{i=1}^{s'}\{0,\ \alpha_i e_1\}+\sum_{i=1}^{j}\{0,\ \beta_i e_1\},$$

where we set $B_0:=\{0\}$ in case $s'=0$. Step C and the definition of the α_i ensures that each B_j is a sumset of cardinality two sets (except B_0 when $s'=0$). The possibilities for be_1 are precisely those elements from the sumset $x+B_{t_1}$. In view of (46) and (20), we have $2n-k\le|T|\le 2n-\overline{b}-\sigma+|I|-r_2(T)$, implying

$$\overline{b}\le k-\sigma+|I|-r_2(T)\le n-k+2, \tag{48}$$

with the latter inequality above in view of (47). Let $H=\mathsf{H}(B_0)$. Apply Kneser's Theorem to B_0. If $|H|\ge 3$, then, given any $y\in\langle e_1\rangle$, there will be some $ae_1\in y+B_0$ with $\overline{a}\ge\frac{2n}{3}+1>k$. In particular, there is some $be_1\in x+B_{t_0}$ with $\overline{b}>k$, contradicting (48) in view of (28). Therefore $|H|\le 2$. If H is trivial, then Kneser's Theorem implies $|B_0|\ge s'+1$. If $|H|=2$, then $s'\ge 1$, while Step D ensures that at most one of the sets in the defining sumset for B_0 has cardinality one modulo H (From $H=\mathsf{H}(B_0)$ it follows that $B_0=\cup_{i=1}^{t}(a_i+H)$ with $t=\frac{|B_0|}{|H|}$ is a disjoint union of H-cosets. Put $B_0(modulo\ H)=\{a_1,\dots,a_t\}$), in which case Kneser's Theorem implies $|B_0|\ge|H|s'=2s'\ge s'+1$. In either case,

$$|B_0|\ge s'+1.$$

We proceed to show by induction on $j=0,1,\dots,t_1$ that

$$\max\left(\overline{x+y+B_0+\sum\nolimits_{i=1}^{j}\beta_i}\right)\ge s'+1+j,\qquad\text{for any } y\in\sum_{i=j+1}^{t_1}\{0,\beta_i e_1\}. \tag{49}$$

The case $j=0$ follows from $|B_0|\ge s'+1$, so assume $j\ge 1$. By (48), we have $\beta_y:=\max\left(\overline{x+y+B_0+\sum_{i=1}^{j-1}\beta_i}\right)\le n-k+2$ for any $y\in\sum_{i=j}^{t_1}\{0,\beta_i e_1\}$, and thus also for any $y\in\sum_{i=j+1}^{t_1}\{0,\beta_i e_1\}\subseteq\sum_{i=j}^{t_1}\{0,\beta_i e_1\}$. By Step C, we have $\beta_j\le k-2$. Thus $\beta_y+\beta_j\le n$, ensuring $\beta_y+\beta_j=\overline{\beta_y+\beta_j}=\max\left(\overline{x+y+B_0+\sum_{i=1}^{j}\beta_i}\right)$, for any $y\in\sum_{i=j+1}^{t_1}\{0,\beta_i e_1\}$. Since $\beta_y+\beta_j>\beta_y$, the desired bound (49) follows in view of the induction hypothesis applied to $\beta_y=\max\left(\overline{x+y+B_0+\sum_{i=1}^{j-1}\beta_i}\right)$, and (49) is established.

In view of (49) applied with $j = t_1$, it follows that we can find some choice of T such that

$$r_2(T) = t \quad \text{and} \quad \overline{b} \geq s' + 1 + t_1. \tag{50}$$

We handle three final subcases based on which quantities obtain the minimums in the definitions of t_1 and t_0.

Suppose $t_1 = t - 2k + 2 + n + \sigma - |I|$. Then

$$\begin{aligned}|T| &= 2n - \overline{b} - \sigma + |I| - r_2(T) \leq 2n - 1 - s' - \sigma + |I| - t - t_1\\ &= n + 2k - s' - 3 + 2|I| - 2\sigma - 2t\\ &\leq 2k - 2 + 2|I| - \sigma \leq 2k - 2 - |V_0| \leq 2k - 2 \leq 2n - k - 1,\end{aligned}$$

with the first equality by (46), the first inequality in view of (50), the second inequality by definition of t, the third from (40) and $|I| \leq |V_0|$, the fourth as $|V_0| \geq 0$, and the fifth in view of $k \leq \frac{2n+1}{3}$. However, this contradicts (20).

Suppose $t_1 = t_0 = t$. Then

$$\begin{aligned}|T| &= 2n - \overline{b} - \sigma + |I| - r_2(T) \leq 2n - 1 - s' - \sigma + |I| - t - t_1\\ &= 2n - 1 - s' - \sigma + |I| - 2t\\ &\leq n + |I| \leq n + |V_0| \leq \frac{4}{3}n - 1 < 2n - k,\end{aligned}$$

with the first equality by (46), the first inequality in view of (50), the second equality in view of the assumption $t_1 = t_0 = t$, the second inequality by definition of t, the third since $|I| \leq |V_0|$, the fourth from Step E, and the fifth in view of $k \leq \frac{2n+1}{3}$. However, this contradicts (20).

Finally, suppose $t_1 = t_0 = \lfloor \frac{h-s'}{2} \rfloor < t$. Then

$$\begin{aligned}|T| &= 2n - \overline{b} - \sigma + |I| - r_2(T) \leq 2n - 1 - s' - \sigma + |I| - t - t_1\\ &= 2n - 1 - s' - \sigma + |I| - t - \lfloor \frac{h - s'}{2} \rfloor\\ &\leq \frac{3n - \sigma - h}{2} + |I| \leq \frac{3n - h - |V_0|}{2} \leq \frac{n-1}{2} + k < 2n - k,\end{aligned}$$

with the first equality in view of (46), the first inequality in view of (50), the second inequality by definition of t, the third from (40) and $|I| \leq |V_0|$, the fourth from $|V_0| \geq 0$, (32) and $|U| \geq n$, and the fifth in view of $k \leq \frac{2n+1}{3}$. However, this contradicts (20), completing the proof. □

We can now prove our main results quite readily.

Proof. (Theorem 5) Since $k \leq \frac{2p^n+1}{3} = \frac{\mathsf{D}(G)+2}{3}$ and $k \not\equiv 0 \mod p$, Lemma 14 implies there exists a minimal zero-sum subsequence $U \mid S$ with $|U| = \mathsf{D}(G)$. Since $2 \leq k \leq \frac{2p^n+1}{3}$, applying Lemma 20 completes the proof. □

Proof. (Theorem 4) Since $2 \leq k \leq \frac{2p+1}{3} < p$, it follows that $p \nmid k$, and so the result is simply a special case of Theorem 5. $\square$

Acknowledgments. This work is supported by NSFC (11671218) and NSFC (11901415).

References

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

[2] W. Gao, A. Geroldinger, and D. Grynkiewicz, Inverse zero-sum problems III, *Acta Arith.* **141.2** (2010), 245-279.

[3] W. Gao, A. Geroldinger, and W. Schmid, Inverse zero-sum problems, *Acta Arith.* **128.3** (2007), 245-279.

[4] 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.

[5] 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.

[6] D. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics, 30, Springer, Cham, 2013.

[7] C. Reiher, A proof of the theorem according to which every prime number possesses Property B, *J. Lond. Math. Soc.* (2013), in press.

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