A Multiplicative Property for Zero-Sums II

David J. Grynkiewicz   Chao Liu

Department of Mathematical Sciences
University of Memphis
Memphis, TN 38152, U.S.A.

diambri@hotmail.com   chaoliuac@gmail.com

Submitted: December 14, 2021; Accepted: May 22, 2022; Published: TBD

Abstract

For $n \geqslant 1$, let C_n denote a cyclic group of order n. Let $G \cong C_n \oplus C_{mn}$ with $n \geqslant 2$ and $m \geqslant 1$, and let $k \in [0, n-1]$. It is known that any sequence of $mn+n-1+k$ terms from G must contain a nontrivial zero-sum of length at most $mn+n-1-k$. The associated inverse question is to characterize those sequences with maximal length $mn+n-2+k$ that fail to contain a nontrivial zero-sum subsequence of length at most $mn+n-1-k$. For $k \leqslant 1$, this is the inverse question for the Davenport Constant. For $k = n-1$, this is the inverse question for the $\eta(G)$ invariant concerning short zero-sum subsequences. For $C_n \oplus C_n$ and $k \in [2, n-2]$, with $n \geqslant 5$ prime, it was conjectured in a paper of Grynkiewicz, Wang and Zhao that they must have the form $S = e_1^{[n-1]} \cdot e_2^{[n-1]} \cdot (e_1+e_2)^{[k]}$ for some basis (e_1, e_2), with the conjecture established in many cases and later extended to composite moduli n. In this paper, we focus on the case $m \geqslant 2$. Assuming the conjectured structure holds for $k \in [2, n-2]$ in $C_n \oplus C_n$, we characterize the structure of all sequences of maximal length $mn+n-2+k$ in $C_n \oplus C_{mn}$ that fail to contain a nontrivial zero-sum of length at most $mn+n-1-k$, showing they must either have the form $S = e_1^{[n-1]} \cdot e_2^{[sn-1]} \cdot (e_1+e_2)^{[(m-s)n+k]}$ for some $s \in [1, m]$ and basis (e_1, e_2) with $\mathsf{ord}(e_2) = mn$, or else have the form $S = g_1^{[n-1]} \cdot g_2^{[n-1]} \cdot (g_1+g_2)^{[(m-1)n+k]}$ for some generating set $\{g_1, g_2\}$ with $\mathsf{ord}(g_1+g_2) = mn$. In view of prior work, this reduces the structural characterization for a general rank two abelian group to the case $C_p \oplus C_p$ with p prime. Additionally, we give a new proof of the precise structure in the case $k = n-1$ for $m = 1$. Combined with known results, our results unconditionally establish the structure of extremal sequences in $G \cong C_n \oplus C_{mn}$ in many cases, including when n is only divisible by primes at most 7, when $n \geqslant 2$ is a prime power and $k \leqslant \frac{2n+1}{3}$, or when n is composite and $k = n-d-1$ or $n-2d+1$ for a proper, nontrivial divisor $d \mid n$.

Mathematics Subject Classifications: 11B75

1 Introduction and Preliminaries

Regarding combinatorial notation for sequences and subsums, we utilize the standardized system surrounding multiplicative strings as outlined in the references [15] [14] [19]. For the reader new to this notational system, we begin with a self-contained review.

Notation

All intervals will be discrete, so for $x, y \in \mathbb{Z}$, we have $[x, y] = \{z \in \mathbb{Z} : \; x \leqslant z \leqslant y\}$. For integers x and n with $n \geqslant 1$, let $(x)_n \in [0, n-1]$ denote the least non-negative representative for x modulo n. We use C_n to denote a cyclic group of order n. A finite abelian group G has the form $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$, where $n_r = \exp(G)$ is the **exponent** and $r \geqslant 0$ is the **rank** of G, which is the minimal cardinality of a generating set for G. For $r \leqslant 2$, an arbitrary rank at most two abelian group has the form $G \cong C_n \oplus C_{mn}$ with $n, m \geqslant 1$. When $n \geqslant 2$, so the rank $r = 2$, a (ordered) **basis** for G is a pair (e_1, e_2) of elements $e_1, e_2 \in G$ such that $G = \langle e_1 \rangle \oplus \langle e_2 \rangle \cong C_n \oplus C_{mn}$.

Let G be an abelian group. In the tradition of Combinatorial Number Theory, a sequence of terms from G is a finite, unordered string of elements from G. We let $\mathcal{F}(G)$ denote the free abelian monoid with basis G, which consists of all (finite and unordered) sequences S of terms from G written as multiplicative strings using the boldsymbol $\boldsymbol{\cdot}$. This means a sequence $S \in \mathcal{F}(G)$ has the form

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

with $g_1, \ldots, g_\ell \in G$ the terms in S. Then

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

denotes the multiplicity of the terms g in S, allowing us to represent a sequence S as

$$S = {\prod}^\bullet_{g \in G} g^{[\mathsf{v}_g(S)]},$$

where $g^{[n]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{n}$ denotes a sequence consisting of the term $g \in G$ repeated $n \geqslant 0$ times. The maximum multiplicity of a term of S is the height of the sequence, denoted

$$\mathsf{h}(S) = \max\{\mathsf{v}_g(S) : \; g \in G\}.$$

The support of the sequence S is the subset of all elements of G that are contained in S, that is, that occur with positive multiplicity in S, which is denoted

$$\mathrm{Supp}(S) = \{g \in G : \; \mathsf{v}_g(S) > 0\}.$$

The length of the sequence S is

$$|S| = \ell = \sum_{g \in G} \mathsf{v}_g(S).$$

A sequence $T \in \mathcal{F}(G)$ with $\mathsf{v}_g(T) \leqslant \mathsf{v}_g(S)$ for all $g \in G$ is called a subsequence of S, denoted $T \mid S$, and in such case, $S \boldsymbol{\cdot} T^{[-1]} = T^{[-1]} \boldsymbol{\cdot} S$ denotes the subsequence of S obtained by removing the terms of T from S, so $\mathsf{v}_g(S \boldsymbol{\cdot} T^{[-1]}) = \mathsf{v}_g(S) - \mathsf{v}_g(T)$ for all $g \in G$.

Since the terms of S lie in an abelian group, we have the following notation regarding subsums of terms from S. We let

$$\sigma(S) = g_1 + \ldots + g_\ell = \sum_{g \in G} \mathsf{v}_g(S) g$$

denote the sum of the terms of S and call S a **zero-sum** sequence when $\sigma(S) = 0$. A **minimal zero-sum** sequence is a zero-sum sequence that cannot have its terms partitioned into two proper, nontrivial zero-sum subsequences. For $n \geqslant 0$, let

$$\Sigma_n(S) = \{\sigma(T) :\ T \mid S,\ |T| = n\}, \quad \Sigma_{\leqslant n}(S) = \{\sigma(T) :\ T \mid S,\ 1 \leqslant |T| \leqslant n\}, \quad \text{and}$$
$$\Sigma(S) = \{\sigma(T) :\ T \mid S,\ |T| \geqslant 1\}$$

denote the variously restricted collections of subsums of S. The sequence S is **zero-sum free** if $0 \notin \Sigma(S)$. Finally, if $\varphi : G \to G'$ is a map, then

$$\varphi(S) = \varphi(g_1) \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} \varphi(g_\ell) \in \mathcal{F}(G')$$

denotes the sequence of terms from G' obtained by applying φ to each term from S.

Background

Let G be a finite abelian group. The Davenport Constant for G is the minimal integer $\mathsf{D}(G)$ such that any sequence of terms from G with length at least $\mathsf{D}(G)$ must contain a nontrivial zero-sum subsequence. Equivalently, $\mathsf{D}(G)$ is the maximal length of a minimal zero-sum sequence (see [21] [14]). Besides being of interest as an independent topic in Combinatorial Number Theory, it also plays an important role when studying factorization in Krull Domains and, more generally, in (Transfer) Krull Monoids. See [14] [15]. For a general rank at most two abelian group $G \cong C_n \oplus C_{mn}$, where $m, n \geqslant 1$, we have [14, Theorem 5.8.3]

$$\mathsf{D}(C_n \oplus C_{mn}) = mn + n - 1.$$

This is a classical result of Olson [25] or van Emde Boas and Kruyswijk [6] whose proof requires the constant $\eta(G)$, defined as the minimal length such that any sequence of terms from G with length at least $\eta(G)$ contains a nontrivial zero-sum subsequence of length at most $\exp(G)$. For rank at most two groups, we have [25] [6] [14, Theorem 5.8.3]

$$\eta(C_n \oplus C_{mn}) = mn + 2n - 2.$$

Specializing a particular case of a more general invariant [3] [13], Delorme, Ordaz and Quiroz introduced [4] the constant $\mathsf{s}_{\leqslant \ell}(G)$ defined as the minimal length such that

$$|S| \geqslant \mathsf{s}_{\leqslant \ell}(G) \quad \text{implies} \quad 0 \in \Sigma_{\leqslant \ell}(S).$$

For connections with Coding Theory, see [3]. The constant $\mathsf{s}_{\leqslant \ell}(G)$ has also been studied in various other contexts [7] [29] [11].

Since $\mathsf{s}_{\leqslant \ell}(G) = \infty$ for $\ell < \exp(G)$ and coincides with the invariants $\eta(G)$ and $\mathsf{D}(G)$ for the values $\ell = \exp(G)$ and $\ell = \mathsf{D}(G)$, it may be viewed as a means of interpolating these constants as $\ell \in [\exp(G), \mathsf{D}(G)]$. For the case of rank two groups, Chunlin Wang and Kevin Zhao determined its exact value [32]:

$$\mathsf{s}_{\leqslant mn+n-1-k}(C_n \oplus C_{mn}) = mn + n - 1 + k, \qquad \text{for } k \in [0, n-1].$$

The associated inverse question is to characterize all extremal sequences of maximal length $mn + n - 2 + k$ with $0 \notin \Sigma_{\leqslant mn+n-1-k}(S)$. For $k = 0$, this means characterizing all zero-sum free sequences of maximal length $mn + n - 2 = \mathsf{D}(G) - 1$. For $k = 1$, this means characterizing all minimal zero-sum sequences of maximal length $mn+n-1 = \mathsf{D}(G)$. For $k = n-1$, this means characterizing all extremal sequences of length $mn+2n-3 = \eta(G)-1$ with $0 \notin \Sigma_{\leqslant mn}(S)$. The precise structure in all three of these cases is known.

For $k \leqslant 1$, this was an involved undertaking achieved by combining the individual results of Gao, Geroldinger, Grynkiewicz, Reiher and Schmid from [8] [10] [31] [20] [28] with the numerical verification of the case when $m = 1$ and $n = 9$ [2]. This characterization has since proved quite useful, being employed in the proofs of several other results, e.g., [1] [12] [16] [17] [26] [30] [27].

For $k = n-1$, this was accomplished by Schmid [30]. For simplicity, we assume $m = 1$ in the following discussion. The group $G \cong C_n \oplus C_n$ has **Property C** if every sequence S with $|S| = \eta(G)-1 = 3n-3$ and $0 \notin \Sigma_{\leqslant n}(S)$ must have the form $S = e_1^{[n-1]} \boldsymbol{\cdot} e_2^{[n-1]} \boldsymbol{\cdot} e_3^{[n-1]}$. It was shown in [9] that, assuming Conjecture 1 holds for $k = 1$ in G (meaning, assuming the structure of minimal zero-sums of length $2n-1$ were known), then Property C holds for G. Once this case in Conjecture 1 was resolved (as described above), this meant Property C was established without condition. However, it was a surprisingly nontrivial question to determine which $e_1, e_2, e_3 \in G$ would give rise to a sequence $S = e_1^{[n-1]} \boldsymbol{\cdot} e_2^{[n-1]} \boldsymbol{\cdot} e_3^{[n-1]}$ with $0 \notin \Sigma_{\leqslant n}(S)$. For $n = p$ prime, a derivation of the precise characterization from Property C can be found in [5], and the derivation of the precise characterization from Property C in the general case (when n may be composite) follows as a particular case of a more general result of Schmid [30]. The exact formulation is stated in Conjecture 1.4. In Section 2, we give a short alternative proof of this case, deriving the precise characterization given in Conjecture 1.4 from Property C using the arguments from [22].

The structure of sequences S of terms from $C_n \oplus C_n$ with $|S| = 2n - 2 + k$ but $0 \notin \Sigma_{\leqslant 2n-1-k}(S)$ was studied in [23] [21] for $k \in [2, n-2]$. In [23], the case when n is prime and $k \leqslant \frac{2n+1}{3}$ was resolved, showing all such sequences must have the form

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

for some basis (e_1, e_2) for $G \cong C_n \oplus C_n$. It was conjectured in [23] [32] that this should also hold for $k \in [2, n-2]$ (we remark that the conjecture appeared in an earlier submitted version of [23] authored only by Wang and Zhao), and the results of [21] extended this conjecture to general n as follows, where we incorporate the already established cases $k \leqslant 1$ and $k = n - 1$ into the statement.

Conjecture 1. Let $n \geqslant 2$, let $G \cong C_n \oplus C_n$, let $k \in [0, n-1]$, and let S be a sequence of terms from G with

$$|S| = 2n - 2 + k \qquad \text{and} \qquad 0 \notin \Sigma_{\leqslant 2n-1-k}(S).$$

Then there exists a basis (e_1, e_2) for G such that the following hold.

1. If $k = 0$, then $S \cdot g$ satisfies Item 2, where $g = -\sigma(S)$.
2. If $k = 1$, then $S = e_1^{[n-1]} \cdot \prod^\bullet_{i \in [1,mn]}(x_i e_1 + e_2)$, for some $x_1, \ldots, x_{mn} \in [0, n-1]$ with $x_1 + \ldots + x_{mn} \equiv 1 \mod n$.
3. If $k \in [2, n-2]$, then $S = e_1^{[n-1]} \cdot e_2^{[sn-1]} \cdot (e_1 + e_2)^{[(m-s)n+k]}$, for some $s \in [1, m]$.
4. If $k = n - 1$, then $S = e_1^{[n-1]} \cdot e_2^{[sn-1]} \cdot (xe_1 + e_2)^{[(m-s)n+n-1]}$, for some $s \in [1, m]$ and $x \in [1, n-1]$ with $\gcd(x, n) = 1$.

In [21], a multiplicative property for the conjecture was established, showing that, if the structure from Conjecture 1 holds for k_m in $C_m \oplus C_m$ and for k_n in $C_n \oplus C_n$, where $k_m \in [0, m-1]$ and $k_n \in [0, n-1]$, then Conjecture 1 also holds for $k = k_m n + k_n$ in $C_{mn} \oplus C_{mn}$. This reduced the characterization problem in $C_n \oplus C_n$ to the case when n is prime.

The characterization in the case $C_n \oplus C_{mn}$ with $m \geqslant 2$, even including a precise statement of the potential structure for sequences of length $mn + n - 2 + k$ avoiding a nontrivial zero-sum of length at most $mn + n - 1 - k$, was completely open apart from the boundary cases $k \leqslant 1$ and $k = n - 1$. Our main result is Theorem 2.1, which fully determines the structure of S for k in $C_n \oplus C_{mn}$ assuming Conjecture 1 holds for k in $C_n \oplus C_n$, as follows. Note, Theorem 2.2, handling the case $k = n - 1$, is due to Schmid [30] and is incorporated into the statement of Theorem 2 for completeness.

Theorem 2. *Let $m \geqslant 1$, let $n \geqslant 3$, let $G \cong C_n \oplus C_{mn}$, let $k \in [2, n-1]$ and let S be a sequence of terms from G with*

$$|S| = mn + n - 2 + k \qquad \textit{and} \qquad 0 \notin \Sigma_{\leqslant mn+n-1-k}(S).$$

If Conjecture 1 holds for k in $C_n \oplus C_n$, then there exists a basis (e_1, e_2) for G with $\mathrm{ord}(e_2) = mn$ or a generating set $\{g_1, g_2\}$ for G with $\mathrm{ord}(g_1 + g_2) = mn$ such that the following hold.

1. *If $k \in [2, n-2]$, then either*
   (a) $S = e_1^{[n-1]} \cdot e_2^{[sn-1]} \cdot (e_1 + e_2)^{[(m-s)n+k]}$, *for some $s \in [1, m]$, or*
   (b) $S = g_1^{[n-1]} \cdot g_2^{[n-1]} \cdot (g_1 + g_2)^{[(m-1)n+k]}$.
2. *If $k = n - 1$, then either*
   (a) $S = e_1^{[n-1]} \cdot e_2^{[sn-1]} \cdot (xe_1 + e_2)^{[(m-s)n+n-1]}$, *for some $s \in [1, m]$ and $x \in [1, n-1]$ with $\gcd(x, n) = 1$, or*

(b) $S = g_1^{[n-1]} \cdot g_2^{[n-1]} \cdot (g_1+g_2)^{[(m-1)n+n-1]}$.

Theorem 2 reduces the characterization in a general rank two abelian group to the case $C_n \oplus C_n$, which in turn is reduced to the case $C_p \oplus C_p$ with $p \geqslant 11$ prime by the results of [21]. The reduction to the case $C_n \oplus C_n$ is the main aim of the paper and emulates the strategy successfully used to characterize the extremal sequences for the Davenport Constant (the case $k \leqslant 1$), where the characterization problem was reduced to case $C_n \oplus C_n$ by Schmid [31] and resolved in this case by the results from [8] [10] [20] [28] (as well as the case $n = 9$ [2]). However, combining Theorem 2 with known cases in Conjecture 1 yields many group $C_n \oplus C_{mn}$ where the structure of extremal sequences is determined here without restriction. As several examples, we list the following corollaries.

Corollary 3. *If $m \geqslant 1$ and $n = 2^{s_1}3^{s_2}5^{s_3}7^{s_4} \geqslant 2$ with $s_1, s_2, s_3, s_4 \geqslant 0$, then the conclusion of Theorem 2 holds in $C_n \oplus C_{mn}$ for all $k \in [2, n-1]$.*

Corollary 4. *For any prime power $n \geqslant 2$ and $m \geqslant 1$, the conclusion of Theorem 2 holds in $C_n \oplus C_{mn}$ for all $2 \leqslant k \leqslant \frac{2n+1}{3}$.*

Corollary 5. *For $n \geqslant 4$ composite, $m \geqslant 1$ and $d \mid n$ a proper, nontrivial divisor, the conclusion of Theorem 2 holds in $C_n \oplus C_{mn}$ when $k = n-d-1 \geqslant 2$ or $k = n-2d+1 \geqslant 2$.*

2 The case $k = n - 1$

As noted in the introduction, Conjecture 1 holding for $k = 1$ in $G \cong C_n \oplus C_n$ implies that Property C holds for G, meaning any sequence S of $3n-3$ terms from $G \cong C_n \oplus C_n$ with $0 \notin \Sigma_{\leqslant n}(S)$ must have the form $S = e_1^{[n-1]} \cdot e_2^{[n-1]} \cdot e_3^{[n-1]}$ for some distinct $e_1, e_2, e_3 \in G$. The goal of this section is to give a new proof of the characterization of which elements $e_1, e_2, e_3 \in G$ result in a sequence $S = e_1^{[n-1]} \cdot e_2^{[n-1]} \cdot e_3^{[n-1]}$ with $0 \notin \Sigma_{\leqslant n}(S)$. Clearly, $0 \notin \Sigma_{\leqslant n}(S)$ ensures $\mathrm{ord}(e_1) = \mathrm{ord}(e_2) = \mathrm{ord}(e_3) = n$. Thus there is some $f_1 \in G$ such that (f_1, e_2) is a basis for G. Letting $e_1 = xf_1 + ye_2$, we see that (e_1, e_2) is a basis for G unless $\gcd(x, n) := n/h > 1$. However, if this were the case, then $T = e_1^{[h]} \cdot e_2^{[xh]}$ is a zero-sum subsequence of S for some $x \in [0, \frac{n}{h} - 1]$ having length $|T| = h + xh \leqslant n$, contradicting that $0 \notin \Sigma_{\leqslant n}(S)$. Therefore (e_1, e_2) is a basis for G, and likewise (e_1, e_3) and (e_2, e_3) must also be bases for G. However, obtaining further restriction on e_1, e_2 and e_3 is much less trivial. We begin with the following lemma showing how the characterization is related to a statement involving the index (see [22]) of the sequence $(-x_1) \cdot (-x_2) \cdot 1$, where $e_3 = x_1e_1 + x_2e_2$, and continue afterwards with a series of lemmas modifying slightly the main line of argument for the prime case from [22]

Lemma 6. *Let $G \cong C_n \oplus C_n$ with $n \geqslant 2$. Suppose (e_1, e_2) is a basis for G and $S = e_1^{[n-1]} \cdot e_2^{[n-1]} \cdot (x_1e_1 + x_2e_2)^{[n-1]}$, where $x_1, x_2 \in [0, n-1]$. Then $0 \notin \Sigma_{\leqslant n}(S)$ if and only if $(-x_1k)_n + (-x_2k)_n + (k)_n > n$ for every $k \in [1, n-1]$.*

Proof. Consider an arbitrary zero-sum subsequence T of S and then let $T = e_1^{[k_1]} \cdot e_2^{[k_2]} \cdot (x_1e_1 + x_2e_2)^{[k]}$, where $k_1, k_2, k \in [0, n-1]$. Note we cannot have $k = 0$ (assuming T

nontrivial) as (e_1, e_2) is a basis, so $k \in [1, n-1]$. Then we have $k_1 = (-x_1k)_n$ and $k_2 = (-x_2k)_n$. Conversely, given any $k \in [1, n-1]$, the subsequence T defined above with $k_1 = (-x_1k)_n$ and $k_2 = (-x_2k)_n$ will be a nontrivial zero-sum. Now

$$|T| = k_1 + k_2 + k = (-x_1k)_n + (-x_2k)_n + (k)_n.$$

If $(-x_1k)_n+(-x_2k)_n+(k)_n \leqslant n$ for some $k \in [1, n-1]$, then the corresponding subsequence T defined using k is a nontrivial zero-sum subsequence of length at most n, showing $0 \in \Sigma_{\leqslant n}(S)$. On the other hand, if $0 \in \Sigma_{\leqslant n}(S)$, then there is a nontrivial zero-sum of the form $T = e_1^{[k_1]} \cdot e_2^{[k_2]} \cdot (x_1e_1 + x_2e_2)^{[k]}$, for some $k \in [1, n-1]$, which satisfies $|T| = (-x_1k)_n + (-x_2k)_n + (k)_n \leqslant n$. $\square$

The following is special case of [22, Proposition 2.1.1].

Lemma 7. *Let $n \geqslant 2$ and let $x_1, x_2, x_3 \in \mathbb{Z}$ with $x_1 + x_2 + x_3 \equiv 0 \mod n$. There there exists $k \in [1, n-1]$ with $\gcd(k, n) = 1$ and $(kx_1)_n + (kx_2)_n + (kx_3)_n \leqslant n$.*

Lemma 8. *Let $n \geqslant 2$. For $x \in [1, n-1]$ with $\gcd(x, n) = 1$, let*

$$X(x) = \left\{ \left\lceil \frac{n}{x} \right\rceil, \left\lceil \frac{2n}{x} \right\rceil, \ldots, \left\lceil \frac{(x-1)n}{x} \right\rceil \right\} \subseteq [2, n-1].$$

1. *$|X(x)| = x - 1$.*
2. *Let $d = \lfloor \frac{n}{x} \rfloor$. The difference between any two consecutive elements in $X(x)$ is either d or $d+1$ with $\min X(x) = d+1$ and $\max X(x) = n-d$ (for $x \geqslant 2$).*
3. *$[2, n-1] = X(x) \cup X(n-x)$ is a disjoint union.*
4. *Let $\Delta(u, x) = (ux)_n - ((u-1)x)_n$. For every $u \in [1, n-1]$, $\Delta(u, x) \in \{x, x-n\}$ with $u \in X(x)$ iff $\Delta(u, x) = x - n$.*

Proof. Item 1–3 are given in [22, Lemma 2.4]. For Item 4, we have $-n < \Delta(u, x) < n$, and since $\Delta(u, x) \equiv x \mod n$, it follows that $\Delta(u, x) \in \{x, x-n\}$. Let $u \in \mathbb{Z}$ and $t = \lfloor \frac{ux}{n} \rfloor$, so

$$tn \leqslant ux < (t+1)n \qquad \text{and} \qquad ux = (ux)_n + tn = ((u-1)x)_n + \Delta(u, x) + tn.$$

Hence $\Delta(u) = x - n$ when $(u-1)x = ((u-1)x)_n + (t-1)n < tn$, and $\Delta(u) = x$ when $(u-1)x = ((u-1)x)_n + tn \geqslant tn$. Thus $\Delta(u) = x - n$ if and only if $(u-1)x < tn$. Since $tn \leqslant ux$ always holds, this is equivalent to $\frac{tn}{x} \leqslant u < \frac{tn}{x} + 1$, and as u is an integer, this is equivalent to $u = \lceil \frac{tn}{x} \rceil$. Therefore $\Delta(u, x) = x - n$ if and only if $u = \lceil \frac{tn}{x} \rceil$, where $t = \lfloor \frac{ux}{n} \rfloor$. Now restrict to $u \in [1, n-1]$. Since $u < n$, we have $t = \lfloor \frac{ux}{n} \rfloor \leqslant x - 1$. Since $u, x \geqslant 1$, we have $t = \lfloor \frac{ux}{n} \rfloor \geqslant 0$. However, $u = \lceil \frac{tn}{x} \rceil$ with $u \geqslant 1$ forces $t \neq 0$, while $u = \lceil \frac{tn}{x} \rceil = \frac{tn+r}{x}$ with $t \in [1, x-1]$ (and $r \in [0, x-1]$) ensures $t = \frac{ux-r}{n} = \lfloor \frac{ux}{n} \rfloor$ (as $0 \leqslant r < x \leqslant n$). As a result, for $u \in [1, n-1]$, we find that $\Delta(u, x) = x - n$ if and only if $u = \lceil \frac{tn}{x} \rceil$ for some $t \in [1, x-1]$, as desired. $\square$

Lemma 9. *Let $n \geqslant 2$ and let $x_1, x_2, x_3 \in \mathbb{Z}$ with $\gcd(x_i, n) = 1$ for all $i \in [1,3]$. If $(kx_1)_n + (kx_2)_n + (kx_3)_n > n$ for every $k \in [1, n-1]$, then $x_i + x_j \equiv 0 \mod n$ for some distinct $i, j \in [1,3]$.*

Proof. If $\gcd(x_1+x_2+x_3, n) \neq 1$, then there exists some $r \in [1, n-1]$ such that $rx_1+rx_2+rx_3 \equiv 0 \mod n$. Applying Lemma 7 to $rx_1, rx_2, rx_3 \in \mathbb{Z}$, we find some $s \in [1, n-1]$ with $\gcd(s,n) = 1$ and $(srx_1)_n+(srx_2)_n+(srx_3)_n \leqslant n$. But then, setting $k = (sr)_n \in [0, n-1]$, we have $(kx_1)_n+(kx_2)_n+(kx_3)_n \leqslant n$ with $k = (sr)_n \neq 0$ since $r \in [1, n-1]$ and $\gcd(s, n) = 1$, which is contrary to hypothesis. Therefore, we conclude that $\gcd(x_1 + x_2 + x_3, n) = 1$. As a result, replacing $x_1, x_2, x_3 \in \mathbb{Z}$ with $sx_1, sx_2, sx_3 \in \mathbb{Z}$, where $s \in \mathbb{Z}$ is an integer congruent to the inverse of $x_1 + x_2 + x_3$ modulo n, we can w.l.o.g. assume

$$x_1 + x_2 + x_3 \equiv 1 \mod n.$$

Replacing each x_i by $(x_i)_n$, we can w.l.o.g. assume $x_1, x_2, x_3 \in [1, n-1]$. If $n = 2$, then $x_1 = x_2 = x_3 = 1$, and the lemma holds. Therefore we may assume $n \geqslant 3$.

Claim 1. For every $u \in [1, n-1]$,

$$(ux_1)_n + (ux_2)_n + (ux_3)_n = n + u.$$

Proof. Indeed, $(ux_1)_n+(ux_2)_n+(ux_3)_n \equiv u(x_1+x_2+x_3) \equiv u$, so $(ux_1)_n+(ux_2)_n+(ux_3)_n = kn+u$ for some $k \in \{0, 1, 2\}$. By hypothesis $kn+u \geqslant n+1$, so $(ux_1)_n+(ux_2)_n+(ux_3)_n \in \{n+u, 2n+u\}$ for every $u \in [1, n-1]$. Since $u \in [1, n-1]$ and $\gcd(x_i, n) = 1$ for every $i \in [1,3]$, we have $(ux_i)_n \neq 0$ and $((n-u)x_i)_n = n - (ux_i)_n$ for all $i \in [1,3]$. Consequently, if $(ux_1)_n + (ux_2)_n + (ux_3)_n = 2n + u$ for some $u \in [1, n-1]$, then we find $((n-u)x_1)_n + ((n-u)x_2)_n + ((n-u)x_3)_n = \big(n-(ux_1)_n\big) + \big(n-(ux_1)_n\big) + \big(n-(ux_1)_n\big) = 3n - (2n+u) = n - u \leqslant n$, which is contrary to hypothesis. $\square$(**Claim 1**)

Let $X_i = X(x_i)$ and $\Delta(u, x_i)$ for $i \in [1,3]$ be as defined in Lemma 8. The special case $u = 1$ in Claim 1 ensures

$$x_1 + x_2 + x_3 = n + 1.$$

Hence, if $x_k = 1$ for some $k \in [1,3]$, then the desired conclusion follows with $\{i, j\} = [1,3] \setminus k$, so we may assume

$$x_1,\ x_2,\ x_3 \geqslant 2, \tag{1}$$

ensuring X_1, X_2 and X_3 are each nonempty (by Lemma 8.1).

Claim 2. $[2, n-1] = X_1 \cup X_2 \cup X_3$ is a disjoint union.

Proof. By Claim 1, for every $u \in [2, n-1]$, we have

$$\sum_{i=1}^{3} \Delta(u, x_i) = \sum_{i=1}^{3} (ux_i)_n - \sum_{i=1}^{3} ((u-1)x_i)_n = (n+u) - (n+u-1) = 1.$$

On the other hand, if u belongs to $s \in [0,3]$ of the sets X_1, X_2 and X_3, then Lemma 8.4 implies $1 = \sum_{i=1}^{3} \Delta(u, x_i) = x_1+x_2+x_3-sn = 1+(1-s)n$, forcing $s = 1$, which completes the claim as $X_i = X(x_i) \subseteq [2, n-1]$ holds trivially for any $x_i \in [1, n-1]$. $\square$(**Claim 2**)

Note that $2 \in X_i = X(x_i)$ precisely when $\lceil \frac{n}{x_i} \rceil = 2$, i.e., when $\frac{n}{2} \leqslant x_i \leqslant n-1$. Consequently, in view of Claim 2 and $n \geqslant 3$, we can w.l.o.g. assume

$$x_2, x_3 < \frac{n}{2} \leqslant x_1.$$

Let $x_1' = n - x_1 \in [1, \frac{n}{2}]$ and set $X_1' = X(x_1')$. By Lemma 8.3 and Claim 2, we have

$$X_1' = [2, n-1] \setminus X_1 = X_2 \cup X_3, \tag{2}$$

with the union disjoint. Hence, since X_2 and X_3 are nonempty, as noted above, it follows that X_1' is also nonempty, ensuring $x_1' \geqslant 2$ (by Lemma 8.1).

As in Lemma 8, let $d_2 = \lfloor \frac{n}{x_2} \rfloor$, $d_3 = \lfloor \frac{n}{x_3} \rfloor$ and $d_1' = \lfloor \frac{n}{x_1'} \rfloor$. Note $d_2, d_3, d_1' \geqslant 2$ since $x_2, x_3, x_1' \leqslant \frac{n}{2}$. By Lemma 8.2, the minimal element in X_i for $i = 2, 3$ (resp. the minimal element in X_1') is $d_i + 1$ (resp. $d_1' + 1$). Since $X_1' = X_2 \cup X_3$, the minimal element $d_1' + 1$ in X_1' must either equal the minimal element in X_2 or the minimal element in X_3, say w.l.o.g. the former, in which case $d_1' + 1 = d_2 + 1 \in X_2$. Denote this joint value by $d := d_1' = d_2$.

Claim 3. $X_1' = X_2$.

Proof. By (2), we have $X_2 \subseteq X_1'$, and the first element of X_1' is in X_2 by assumption, equal to the first element of X_2. Let $d + 1 = z_1 < z_2 < \cdots < z_{x_1'-1}$ denote the elements of X_1'. Assume $z_k \in X_2$ for $k < x_1' - 1$. By Lemma 8.2 applied to X_1', since $d \geqslant 2$, z_{k+1} is one of the values $z_k + d$ or $z_k + d + 1$, and exactly one of these elements is in X_1'. But $d_2 = d$, so Lemma 8.2 applied to X_2 yields that the next element of X_2 after $z_k \in X_2$ is also either $z_k + d$ or $z_k + d + 1$. Since only one of these two possibilities lies in X_1', namely the value between them equal to z_{k+1}, we are forced to conclude from $X_2 \subseteq X_1'$ that the next element in X_2 after $z_k \in X_2$ is $z_{k+1} \in X_2$. This shows, via induction on k, that X_2 equals the first $|X_2|$ elements of X_1'. However, Lemma 8.2 implies that $\max X_2 = n - d_2 = n - d = n - d_1' = \max X_1'$, which combined with the previous conclusion forces $X_1' = X_2$. □(**Claim 3**)

Since $X_1' = X_2 \cup X_3$ is a disjoint union, we conclude from Claim 3 that $X_3 = \emptyset$, whence $x_3 - 1 = |X_3| = 0$ by Lemma 8.1, contradicting (1). □

Proposition 10. *For any $n \geqslant 2$, Conjecture 1.4 holds for $k = n - 1$ in $C_n \oplus C_n$.*

Proof. Let $G \cong C_n \oplus C_n$ and let $S \in \mathcal{F}(G)$ be a sequence with $|S| = 3n-3$ and $0 \notin \Sigma_{\leqslant n}(S)$. Then $S = e_1^{[n-1]} \cdot e_2^{[n-1]} \cdot e_3^{[n-1]}$ for some $e_1, e_2, e_3 \in G$ which pairwise form bases for G, as noted at the start of Section 2. Write $e_3 = x_1 e_1 + x_2 e_2$ with x_1, $x_2 \in [1, n-1]$. By Lemma 6, the hypothesis that $0 \notin \Sigma_{\leqslant n}(S)$ is equivalent to $(-x_1 \cdot k)_n + (-x_2 \cdot k)_n + (k \cdot 1)_n > n$ holding for all $k \in [1, n-1]$. Since (e_1, e_3) and (e_2, e_3) are both bases, we must have $\gcd(x_1, n) = \gcd(x_2, n) = 1$. Applying Lemma 9 using the elements $-x_1$, $-x_2$ and 1, we deduce that either $x_1 + x_2 \equiv 0 \mod n$, or $x_1 = 1$, or $x_2 = 1$. If $x_1 = 1$, then the conclusion of Conjecture 1.4 holds using the basis (e_2, e_1). If $x_2 = 1$, then the conclusion of Conjecture 1.4 holds using the basis (e_1, e_2). If $x_1 + x_2 \equiv 0 \mod n$, then $e_3 = x_1 e_1 - x_1 e_2$.

In this final case, letting $y \in [1, n-1]$ be the multiplicative inverse of x_1 modulo n, we find that $ye_3 = e_1 - e_2$ and $e_1 = ye_3 + e_2$, in which case Conjecture 1.4 holds using the basis (e_3, e_2), which completes the proof. □

3 Reduction to the Diagonal Case

The goal of this section is to prove Theorem 2.1 as well as the three corollaries giving examples where our results hold without restriction. For the proof, we will need the following characterization of maximal length minimal zero-sums in a cyclic group [14][Corollary 5.4.6] [15][Corollary 4.4].

Theorem 11. *Let $n \geqslant 2$, let $G \cong C_n$. If $S \in \mathcal{F}(G)$ is a minimal zero-sum sequence of length $|S| = \mathsf{D}(G) = n$, then $S = g^{[n]}$ for some $g \in G$ with $\mathrm{ord}(g) = n$. If $S \in \mathcal{F}(G)$ is a zero-sum free sequence of length $|S| = \mathsf{D}(G) - 1 = n - 1$, then $S = g^{[n-1]}$ for some $g \in G$ with $\mathrm{ord}(g) = n$*

We continue with the proof of Theorem 2.1.

Proof of Theorem 2.1. Let $G \cong C_n \oplus C_{mn}$ and let $\varphi : G \to G$ be a homomorphism with

$$\ker \varphi \cong C_m \qquad \text{and} \qquad \varphi(G) \cong C_n \oplus C_n.$$

Since $k \in [2, n-2]$, we have $n \geqslant 4$. Let $S \in \mathcal{F}(G)$ be a sequence with

$$|S| = mn + n - 2 + k \qquad \text{and} \qquad 0 \notin \Sigma_{\leqslant mn+n-1-k}(S). \tag{3}$$

Define a *block decomposition* of S to be a factorization

$$S = W \boldsymbol{\cdot} W_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} W_{m-1}$$

with $1 \leqslant |W_i| \leqslant n$ and $\varphi(W_i)$ zero-sum for each $i \in [1, m-1]$. Since $\mathsf{s}_{\leqslant n}(\varphi(G)) = \mathsf{s}_{\leqslant n}(C_n \oplus C_n) = 3n - 2$ and $|S| = (m-2)n + 3n - 2 + k \geqslant (m-2)n + 3n - 2$, it follows by repeated application of $\mathsf{s}_{\leqslant n}(\varphi(G))$ that S has a block decomposition.

Claim A. If $S = W \boldsymbol{\cdot} W_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} W_{m-1}$ is a block decomposition of S, then $|W_i| = n$ for all $i \in [1, m-1]$, $|W| = 2n - 2 + k$, $0 \notin \Sigma_{\leqslant 2n-1-k}(\varphi(W))$, and $0 \notin \Sigma_{\leqslant n-1}(\varphi(S))$. In particular, Conjecture 1 holds for $\varphi(W)$.

Proof. Suppose $0 \in \Sigma_{\leqslant 2n-1-k}(\varphi(W))$. Then there is a nontrivial subsequence $W_0 \mid W$ with $|W_0| \leqslant 2n-1-k$ and $\varphi(W_0)$ zero-sum. Now $\sigma(W_0) \boldsymbol{\cdot} \sigma(W_1) \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} \sigma(W_{2m-2+k_m})$ is a sequence of m terms from $\ker \varphi \cong C_m$. Since $\mathsf{D}(C_m) = m$, it follows that it has a nontrivial zero-sum subsequence, say $\prod^\bullet_{i \in I} \sigma(W_i)$ for some nonempty $I \subseteq [0, m-1]$. But then $\prod^\bullet_{i \in I} W_i$ is a nontrivial zero-sum subsequence of S with $|\prod^\bullet_{i \in I} W_i| \leqslant (m-1)n + (2n - 1 - k) = mn + n - 1 - k$, contrary to (3). So we instead conclude that $0 \notin \Sigma_{\leqslant 2n-1-k}(\varphi(W))$.

As a result, since $\mathsf{s}_{\leqslant 2n-1-k}(\varphi(G)) = \mathsf{s}_{\leqslant 2n-1-k}(C_n \oplus C_n) = 2n-1+k$, and since $|W_i| \leqslant n$ for all $i \in [1, m-1]$, it follows that

$$2n-2+k = mn+n-2+k-(m-1)n \leqslant |S| - \sum_{i=1}^{m-1} |W_i| = |W| \leqslant 2n-2+k,$$

forcing equality to hold in all estimates, i.e., $|W_i| = n$ for $i \in [1, m-1]$ and $|W| = 2n-2+k$. If $0 \in \Sigma_{\leqslant n-1}(\varphi(S))$, then we can find a nontrivial subsequence $W_1' \mid S$ with $|W_1'| \leqslant n-1$ and $\varphi(W_1')$ zero-sum. Applying the argument used to show the existence of a block decomposition, we obtain a block decomposition $S = W' \cdot W_1' \cdot \ldots \cdot W_{m-1}'$ with $|W_1'| \leqslant n-1$, contradicting what was just shown. Therefore $0 \notin \Sigma_{\leqslant n-1}(\varphi(S))$. Finally, since $|W| = 2n-2+k$ and $0 \notin \Sigma_{\leqslant 2n-1-k}(\varphi(W))$ with Conjecture 1 holding for k in $C_n \oplus C_n$ by hypothesis, it follows that Conjecture 1 holds for $\varphi(W)$. $\square$(**Claim A**)

Suppose

$$S = \widetilde{W} \cdot W_0 \cdot W_1 \cdot \ldots \cdot W_{m-1}$$

with each $\varphi(W_i)$ a nontrivial zero-sum for $i \in [0, m-1]$ and $|\widetilde{W}| \geqslant 2k-n-1$. We call this a *weak block decomposition* of S with associated sequence

$$S_\sigma = \sigma(W_0) \cdot \sigma(W_1) \cdot \ldots \cdot \sigma(W_{m-1}) \in \mathcal{F}(\ker \varphi).$$

Since $\ker \varphi \cong C_m$ and $|S_\sigma| = m = \mathsf{D}(C_m)$, it follows that S_σ contains a nontrivial zero-sum. In view of Claim A, we have $|W_i| \geqslant n$ for all $i \in [0, m-1]$. As a result, if S_σ contained a proper, nontrivial zero-sum subsequence, then S would have a nontrivial zero-sum of length at most $|S| - |\widetilde{W}| - n \leqslant (mn+n-2+k) - (2k-n-1) - n = mn+n-1-k$, contrary to (3). We conclude that the associated sequence S_σ must be a minimal zero-sum of length $\mathsf{D}(C_m) = m$, in which case Theorem 11 implies that there is some $g_0 \in \ker \varphi$ with $\mathrm{ord}(g_0) = m$ such that

$$\sigma(W_0) = \sigma(W_1) = \ldots = \sigma(W_{m-1}) = g_0. \tag{4}$$

Now let $S = W \cdot W_1 \cdot \ldots \cdot W_{m-1}$ be a fixed but otherwise arbitrary block decomposition. In view of Claim A, we have $|W| = 2n-2+k$ with $0 \notin \Sigma_{\leqslant 2n-1-k}(\varphi(W))$ and Conjecture 1 holding for $\varphi(W)$ using $k \in [2, n-2]$. As a result, there is a basis $(\overline{e}_1, \overline{e}_2)$ for $\varphi(G) \cong C_n \oplus C_n$ such that

$$\varphi(W) = \overline{e}_1^{[n-1]} \cdot \overline{e}_2^{[n-1]} \cdot (\overline{e}_1 + \overline{e}_2)^{[k]},$$

and there is a subsequence $W_0 \mid W$ with

$$\varphi(W_0) = \overline{e}_1^{[n-k]} \cdot \overline{e}_2^{[n-k]} \cdot (\overline{e}_1 + \overline{e}_2)^{[k]}.$$

Setting $\widetilde{W} = W \cdot W_0^{[-1]}$, so

$$\varphi(\widetilde{W}) = \overline{e}_1^{[k-1]} \cdot \overline{e}_2^{[k-1]},$$

we find $|\widetilde{W}| = 2k-2 > 2k-n-1$ (as $n \geqslant 2$), meaning $S = \widetilde{W} \cdot W_0 \cdot W_1 \cdot \ldots \cdot W_{m-1}$ is a weak block decomposition with associated sequence $S_\sigma = \sigma(W_0) \cdot \sigma(W_1) \cdot \ldots \cdot \sigma(W_{m-1})$ satisfying (4) for some $g_0 \in \ker \varphi$ with $\mathrm{ord}(g_0) = m$.

Claim B. For any $j \in [1, m-1]$, if $W'_j \mid W \cdot W_j$ is a subsequence with $|W'_j| = n$ and $\varphi(W'_j)$ zero-sum, then $\varphi(W \cdot W_j \cdot (W'_j)^{[-1]}) = \varphi(W) = \overline{e}_1^{[n-1]} \cdot \overline{e}_2^{[n-1]} \cdot (\overline{e}_1 + \overline{e}_2)^{[k]}$.

Proof. We can w.l.o.g. assume $j = 1$. Setting $W' = W \cdot W_1 \cdot (W'_1)^{[-1]}$, we find that $S = W' \cdot W'_1 \cdot W_2 \cdot \ldots \cdot W_{m-1}$ is a block decomposition, so Conjecture 1 must hold for $\varphi(W')$ by Claim A with respect to some basis $(\overline{f}_1, \overline{f}_2)$, meaning $\varphi(W \cdot W_1 \cdot (W'_1)^{[-1]}) = \varphi(W') = \overline{f}_1^{[n-1]} \cdot \overline{f}_2^{[n-1]} \cdot (\overline{f}_1 + \overline{f}_2)^{[k]}$. We need to show $\{\overline{f}_1, \overline{f}_2\} = \{\overline{e}_1, \overline{e}_2\}$. Assuming by contradiction that this fails, we can w.l.o.g. assume $\overline{f}_1 \notin \{\overline{e}_1, \overline{e}_2\}$, ensuring f_1 has multiplicity at least $n-1$ in $\varphi(W \cdot W_1)$. Note, since the n-term zero-sum $\varphi(W_1)$ cannot contain a term with multiplicity exactly $n-1$, any term $g \notin \{\overline{e}_1, \overline{e}_2\}$ with multiplicity at least $n-1$ in $\varphi(W \cdot W_1)$ must either have $\varphi(W_1) = g^{[n]}$ or else $g = \overline{e}_1 + \overline{e}_2$ with $\mathsf{v}_{\overline{e}_1+\overline{e}_2}(\varphi(W_1)) \geqslant n-1-k \geqslant 1$. In both cases, there cannot be a second term $g' \notin \{\overline{e}_1, \overline{e}_2\}$ with multiplicity at least $n-1$, the former since $\mathsf{v}_{\overline{e}_1+\overline{e}_2}(W_0 \cdot W_1) = k \leqslant n-2$, and the latter since $\varphi(W_1)$ cannot contain a term with multiplicity exactly $n-1$. As a result, we conclude that $\overline{e}_1$, $\overline{e}_2$ and $\overline{f}_1$ are the only terms with multiplicity at least $n-1$ in $\varphi(W \cdot W_1)$, and thus w.l.o.g. $\overline{f}_2 = \overline{e}_2$.

Suppose $\overline{f}_1 = \overline{e}_1 + \overline{e}_2$. Then $\varphi(W') = (\overline{e}_1 + \overline{e}_2)^{[n-1]} \cdot \overline{e}_2^{[n-1]} \cdot (\overline{e}_1 + 2\overline{e}_2)^{[k]}$, and since $n \geqslant 4$ ensures $\overline{e}_1 + 2\overline{e}_2 \neq \overline{e}_1$ with $\varphi(W'_1)$ an n-term zero-sum, it follows that $\varphi(W'_1) = \overline{e}_1^{[n]}$. In such case, $\varphi(W_1) = (\overline{e}_1 + \overline{e}_2)^{[n-1-k]} \cdot \overline{e}_1 \cdot (\overline{e}_1 + 2\overline{e}_2)^{[k]}$, which is only zero-sum for $k = 1$, contradicting that $k \in [2, n-2]$. So we conclude that $\overline{f}_1 \neq \overline{e}_1 + \overline{e}_2$, in which case we must instead have $\varphi(W_1) = \overline{f}_1^{[n]}$.

In this case, $\varphi(W') = \overline{f}_1^{[n-1]} \cdot \overline{e}_2^{[n-1]} \cdot (\overline{f}_1 + \overline{e}_2)^{[k]}$ with $\overline{f}_1 + \overline{e}_2 \in \{\overline{e}_1, \overline{e}_1 + \overline{e}_2\}$. Thus either $\overline{f}_1 = \overline{e}_1 - \overline{e}_2$ or $\overline{e}_1$. Since $\overline{f}_1 \neq \overline{e}_1$, this means $\overline{f}_1 = \overline{e}_1 - \overline{e}_2 \neq \overline{e}_1 + \overline{e}_2$ (as $n \geqslant 3$), $\varphi(W') = \overline{f}_1^{[n-1]} \cdot \overline{e}_2^{[n-1]} \cdot \overline{e}_1^{[k]} = (\overline{e}_1 - \overline{e}_2)^{[n-1]} \cdot \overline{e}_2^{[n-1]} \cdot \overline{e}_1^{[k]}$ and $\varphi(W'_1) = \overline{e}_1^{[n-1-k]} \cdot (\overline{e}_1 + \overline{e}_2)^{[k]} \cdot \overline{f}_1$. Hence, since $\varphi(W'_1)$ is an n-term zero-sum, it follows that $\overline{e}_1 - \overline{e}_2 = \overline{f}_1 = \overline{e}_1 - k\overline{e}_2$, contradicting that $k \in [2, n-2]$. $\square$(**Claim B**)

Claim C. $\varphi(W_j) \in \{\overline{e}_1^{[n]}, \overline{e}_2^{[n]}, (\overline{e}_1 + \overline{e}_2)^{[n]}\}$ for every $j \in [1, m-1]$.

Proof. Since each $\varphi(W_j)$, for $j \in [1, m-1]$, is a zero-sum of length n by Claim A, it suffices to show $\mathrm{Supp}(\varphi(W_1 \cdot \ldots \cdot W_{m-1})) \subseteq \{\overline{e}_1, \overline{e}_2, \overline{e}_1 + \overline{e}_2\}$. Let $g \in \mathrm{Supp}(W_j)$ and $j \in [1, m-1]$ be arbitrary. Since $0 \notin \Sigma_{\leqslant n-1}(\varphi(S))$ by Claim A and $|W \cdot W_j \cdot g^{[-1]}| = 3n-3+k \geqslant 3n-2 = \mathsf{s}_{\leqslant n}(C_n \oplus C_n)$, there is subsequence $W'_j \mid W \cdot W_j \cdot g^{[-1]}$ with $|W'_j| = n$, $\varphi(W'_1)$ zero-sum and $g \in \mathrm{Supp}(W \cdot W_j \cdot (W'_j)^{[-1]})$. Thus Claim B ensures that $\varphi(g) \in \{\overline{e}_1, \overline{e}_2, \overline{e}_1 + \overline{e}_2\}$, and as $g \in \mathrm{Supp}(W_j)$ and $j \in [1, m-1]$ were arbitrary, the claim follows. $\square$(**Claim C**)

Claim D. There are g_1, $g_2 \in G$ with $\varphi(g_1) = \overline{e}_1$, $\varphi(g_2) = \overline{e}_2$ and also $\mathrm{Supp}(S) = \{g_1, g_2, g_1 + g_2\}$.

Proof. Let $x \in \mathrm{Supp}(\widetilde{W})$ and $y \in \mathrm{Supp}(W_j)$, for some $j \in [0, m-1]$, be arbitrary terms with $\varphi(x) = \varphi(y) = \overline{e}_1$, which exist as $k \geqslant 2$ and $\mathsf{v}_{\overline{e}_1}(\varphi(W_0)) = n - k \geqslant 1$. If we set $\widetilde{W}' = \widetilde{W} \cdot x^{[-1]} \cdot y$ and $W'_j = W_j \cdot y^{[-1]} \cdot x$, we find that $S = \widetilde{W}' \cdot W_1 \cdot \ldots \cdot W_{j-1} \cdot W'_j \cdot W_{j+1} \cdot \ldots \cdot W_{m-1}$ is a weak product decomposition with associated sequence $S_\sigma \cdot \sigma(W_j)^{[-1]} \cdot \sigma(W'_j) = g_0^{[m-1]} \cdot \sigma(W'_j)$. As a result, Theorem 11 implies that $g_0 - y + x = \sigma(W_j) - y + x = \sigma(W'_j) = g_0$, whence $x = y$. This shows that all terms $x \in \mathrm{Supp}(S)$ with $\varphi(x) = \overline{e}_1$ are equal to the same element (say) $g_1 \in G$. The same argument shows that all terms $x \in \mathrm{Supp}(S)$ with $\varphi(x) = \overline{e}_2$ are equal to the same element (say) $g_2 \in G$. Let $z \in \mathrm{Supp}(W_0 \cdot \ldots \cdot W_{m-1})$ be an arbitrary term with $\varphi(z) = \overline{e}_1 + \overline{e}_2$, which exists as $\mathsf{v}_{\overline{e}_1+\overline{e}_2}(\varphi(W_0)) = k \geqslant 2$. Let $g \in \mathrm{Supp}(W_j)$ with $j \in [0, m-1]$. Since $k \geqslant 2$, we have $g_1 \cdot g_2 \mid \widetilde{W}$. If we set $\widetilde{W}' = \widetilde{W} \cdot g_1^{[-1]} \cdot g_2^{[-1]} \cdot z$ and $W'_j = W_j \cdot z^{[-1]} \cdot g_1 \cdot g_2$, we find that $S = \widetilde{W}' \cdot W_1 \cdot \ldots \cdot W_{j-1} \cdot W'_j \cdot W_{j+1} \cdot \ldots \cdot W_{m-1}$ is a weak product decomposition with associated sequence $S_\sigma \cdot \sigma(W_j)^{[-1]} \cdot \sigma(W'_j) = g_0^{[m-1]} \cdot \sigma(W'_j)$. As a result, Theorem 11 implies that $g_0 - z + g_1 + g_2 = \sigma(W_j) - z + g_1 + g_2 = \sigma(W'_j) = g_0$, whence $z = g_1 + g_2$. This shows that all terms $x \in \mathrm{Supp}(W_0 \cdot \ldots \cdot W_{m-1})$ with $\varphi(z) = \overline{e}_2$ are equal to the same element $g_1 + g_2 \in G$. Since, by definition of $\widetilde{W}$, there are no terms $z \in \mathrm{Supp}(\widetilde{W})$ with $\varphi(z) = \overline{e}_1 + \overline{e}_2$, the claim follows. $\square$(**Claim D**)

In view of Claim D and (4), we find that

$$g_0 = \sigma(W_0) = (n-k)g_1 + (n-k)g_2 + k(g_1 + g_2) = ng_1 + ng_2. \tag{5}$$

Since $\varphi(g_1+g_2) = \overline{e}_1+\overline{e}_2$ has order n, it follows that n divides $\mathrm{ord}(g_1+g_2)$, which, combined with $n(g_1+g_2) = g_0$ having $\mathrm{ord}(g_0) = m$, forces $\mathrm{ord}(g_1+g_2) = mn$. If $\langle g_1, g_2 \rangle = G'$ were a proper subgroup of $G \cong C_n \oplus C_{mn}$, then $\mathrm{ord}(g_1+g_2) = mn$ ensures that $\langle g_1, g_2 \rangle \cong C_{n'} \oplus C_{mn}$ for some proper divisor $n' \mid n$. In such case, S would be a sequence of terms from $G' \cong C_{n'} \oplus C_{mn}$ with length $|S| = (m+1)n - 2 + k \geqslant mn + 2n' - 2 + k \geqslant \eta(G')$, ensuring that S has a zero-sum of length at most mn, contrary to (3). Therefore $\langle g_1, g_2 \rangle = G$, meaning $\{g_1, g_2\}$ is a generating set for G.

If there are $i, j \in [1, m-1]$ with $\varphi(W_i) = \overline{e}_1^{[n]}$ and $\varphi(W_j) = \overline{e}_2^{[n]}$, then Claim D ensures that $W_i = g_1^{[n]}$ and $W_j = g_2^{[n]}$. Combined with (4) and (5), this implies $ng_1 + ng_2 = g_0 = \sigma(W_i) = ng_1$ and $ng_1 + ng_2 = g_0 = \sigma(W_j) = ng_2$, whence $ng_1 = ng_2 = 0$ and $g_0 = ng_1 + ng_2 = 0$, contradicting that $\mathrm{ord}(g_0) = m \geqslant 2$. Therefore we can w.l.o.g. assume

$$W_1, W_2, \ldots, W_{m-1} \in \{g_2^{[n]}, (g_1 + g_2)^{[n]}\}.$$

If $W_1 = \ldots = W_{m-1} = (g_1 + g_2)^{[n]}$, then Theorem 2.1(b) holds, as desired. So we can w.l.o.g assume $W_1 = g_2^{[n]}$, in which case (4) and (5) yield $ng_1 + ng_2 = g_0 = \sigma(W_1) = ng_2$, implying

$$ng_1 = 0.$$

Let $s - 1 \in [1, m-1]$ be the number of $i \in [1, m-1]$ with $W_i = g_2^{[n]}$. Then

$$S = g_1^{[n-1]} \cdot g_2^{[sn-1]} \cdot (g_1 + g_2)^{[(m-s)n+k]}.$$

Since $ng_1 = 0$, we have $\mathrm{ord}(g_1) \leqslant n$. Thus

$$n^2 m = |G| = |\langle g_1, g_2\rangle| = \frac{|\langle g_1\rangle| \cdot |\langle g_2\rangle|}{|\langle g_1\rangle \cap \langle g_2\rangle|} \leqslant n(mn),$$

forcing equality to hold in all above estimates. As a result, $\mathrm{ord}(g_1) = n$, $\mathrm{ord}(g_2) = mn$ and $\langle g_1\rangle \cap \langle g_2\rangle = \{0\}$, meaning (g_1, g_2) is a basis for G, and now Theorem 2.1(a) holds, completing the proof. □

To conclude the paper, we note that Corollaries 3, 4 and 5 follow immediately by combining Theorem 2 with the respective result from [21, Corollaries 1.3, 1.4 and 1.5]. These corollaries represent the cases in [21] where Conjecture 1 was established unconditionally for C_n^2.

References

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

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

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

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

[5] P. van Emde Boas, A combinatorial problem on finite abelian groups II, *Math. Centrum Amsterdam Afd. Zuivere Wisk.*, 1969(ZW-007):60pp., 1969.

[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 and A. Geroldinger, On Long Minimal Zero Sequences in Finite Abelian Groups, *Period. Math. Hung.* 38 (1999), 179–211.

[10] W. Gao, A. Geroldinger, D. J. Grynkiewicz, Inverse Zero-Sum Problems III, *Acta Arith.* 141 (2010), no. 3, 103–152.

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

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

[13] A. Geroldinger, D. J. Grynkiewicz and W. A Schmid, Zero-sum problems with congruence conditions, *Acta Math. Hungar.* 131 (2011), no. 4, 323–345.

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

[18] D. J. Grynkiewicz, Representing Sequence Subsums as Sumsets of Near Equal Sized Sets, in *Combinatorial Number Theory IV*, ed. M. Nathanson, Springer (2021), Ch. 11.

[19] D. 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 Multplicative Property for Zero-Sums I, *Discrete Math.* 345 (2022), no. 10, 112974.

[22] D. J. Grynkiewicz and U. Vishne, The Index of Small Length Sequences, *International J. Algebra and Computation* 30 (2020), no. 5, 977–1014.

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

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

[26] 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.

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

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

[29] 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.

[30] W. A. Schmid, Restricted inverse zero-sum problems in groups of rank 2, *Q. J. Math.* 63 (2012), no. 2, 477–487.

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

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