# INVERSE ZERO-SUM PROBLEMS III

WEIDONG GAO, ALFRED GEROLDINGER, AND DAVID J. GRYNKIEWICZ

## 1. Introduction

We continue the investigations started in [4, ?]. Let $G = C_n \oplus C_n$ with $n \ge 2$. We say that $G$ has Property $\mathbf{B}$ if every minimal zero-sum sequence $S$ over $G$ of length $|S| = 2n-1$ contains an element with multiplicity $n-1$. The aim of the present paper is to prove the following two results.

**Theorem.** *Let $G = C_{mn} \oplus C_{mn}$ with $m, n \ge 3$ odd and $mn > 9$. If both $C_m \oplus C_m$ and $C_n \oplus C_n$ have Property $\mathbf{B}$, then $G$ has Property $\mathbf{B}$.*

**Corollary.** *Let $G = C_{n_1} \oplus C_{n_2}$ with $1 < n_1 \mid n_2$, and suppose that, for every prime divisor $p$ of $n_1$, the group $C_p \oplus C_p$ has Property $\mathbf{B}$. Then $C_{n_1} \oplus C_{n_1}$ has Property $\mathbf{B}$, and a sequence $S$ over $G$ of length $\mathsf{D}(G) = n_1 + n_2 - 1$ is a minimal zero-sum sequence if and only if it has one of the following two forms:*

-
$$S = e_j^{\operatorname{ord}(e_j)-1} \prod_{\nu=1}^{\operatorname{ord}(e_k)} (x_\nu e_j + e_k)\,, \qquad \text{where}$$
$(e_1, e_2)$ *is a basis of $G$ with* $\operatorname{ord}(e_i) = n_i$ *for $i \in \{1,2\}$, $\{j,k\} = \{1,2\}$, $x_1, \ldots, x_{\operatorname{ord}(e_k)} \in [0, \operatorname{ord}(e_j)-1]$, and $x_1 + \ldots + x_{\operatorname{ord}(e_k)} \equiv 1 \mod \operatorname{ord}(e_j)$.*

-
$$S = g_1^{sn_1-1} \prod_{\nu=1}^{n_2+(1-s)n_1} (-x_\nu g_1 + g_2)\,, \qquad \text{where}$$
*$\{g_1, g_2\}$ is a generating set of $G$ with* $\operatorname{ord}(g_2) = n_2$*, $x_1, \ldots, x_{n_2+(1-s)n_1} \in [0, n_1-1]$, $x_1 + \ldots + x_{n_2+(1-s)n_1} = n_1 - 1$, $s \in [1, n_2/n_1]$, and either $s = 1$ or $n_1 g_1 = n_2 g_2$.*

Thus Property $\mathbf{B}$ is multiplicative, and if $G = C_{n_1} \oplus C_{n_2}$ with $1 < n_1 \mid n_2$ is a group of rank two, and for every prime divisor $p$ of $n_1$ the group $C_p \oplus C_p$ has Property $\mathbf{B}$, then the minimal zero-sum sequences of maximal length over $G$ are explicitly characterized.

In Section 2, we fix our notation and gather the necessary tools (apart from former work on Property $\mathbf{B}$ and classical addition theorems, we use a confirmed conjecture of Y. ould Hamidoune, see Theorem 2.7). Section 3 contains some straightforward lemmas. The proof of the Theorem consists of two major parts: the first is given in Section 4 and the second, more involved one, is given in Section 5.

The Corollary is mainly based on the Theorem above, on former work of the authors [2], and on recent work by Wolfgang A. Schmid [?]. Its proof only needs a few lines and is given in Section 6.

---

2000 *Mathematics Subject Classification.* 11P70, 11B50, 11B75.

## 2. Preliminaries

Our notation and terminology are consistent with [4] and [5]. We briefly gather some key notions and fix the notation concerning sequences over finite abelian groups. Let $\mathbb{N}$ denote the set of positive integers and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$. Throughout, all abelian groups will be written additively. For $n \in \mathbb{N}$, let $C_n$ denote a cyclic group with $n$ elements. Let $G$ be an abelian group.

Let $A, B \subset G$ be nonempty subsets. Then $A + B = \{a + b \mid a \in A, b \in B\}$ denotes their *sumset* and $A - B = \{a - b \mid a \in A, b \in B\}$ their *difference set*. The *stabilizer* of $A$ is defined as $\mathrm{Stab}(A) = \{g \in G \mid g + A = A\}$, and $A$ is called *periodic* if $\mathrm{Stab}(A) \ne \{0\}$.

An $s$-tuple $(e_1, \ldots, e_s)$ of elements of $G$ is said to be *independent* if $e_i \ne 0$ for all $i \in [1, s]$ and, for every $s$-tuple $(m_1, \ldots, m_s) \in \mathbb{Z}^s$,

$$m_1e_1 + \ldots + m_se_s = 0 \qquad \text{implies} \qquad m_1e_1 = \ldots = m_se_s = 0\,.$$

An $s$-tuple $(e_1, \ldots, e_s)$ of elements of $G$ is called a *basis* if it is independent and $G = \langle e_1 \rangle \oplus \ldots \oplus \langle e_s \rangle$.

Let $G = C_n \oplus C_n$ with $n \ge 2$, and let $(e_1, e_2)$ be a basis of $G$. An endomorphism $\varphi \colon G \to G$ with

$$(\varphi(e_1), \varphi(e_2)) = (e_1, e_2) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \text{where} \qquad a, b, c, d \in \mathbb{Z}\,,$$

is an automorphism if and only if $(\varphi(e_1), \varphi(e_2))$ is a basis, which is equivalent to $\gcd(ad - bc, n) = 1$. If $f_1 \in G$ with $\mathrm{ord}(f_1) = n$, then clearly there is an $f_2 \in G$ such that $(f_1, f_2)$ is a basis of $G$.

Let $\mathcal{F}(G)$ be the free monoid with basis $G$. The elements of $\mathcal{F}(G)$ are called *sequences* over $G$. We write sequences $S \in \mathcal{F}(G)$ in the form

$$S = \prod_{g \in G} g^{\mathsf{v}_g(S)}\,, \quad \text{with} \quad \mathsf{v}_g(S) \in \mathbb{N}_0 \quad \text{for all} \quad g \in G\,.$$

We call $\mathsf{v}_g(S)$ the *multiplicity* of $g$ in $S$, and we say that $S$ *contains* $g$ if $\mathsf{v}_g(S) > 0$. A sequence $S_1$ is called a *subsequence* of $S$ if $S_1 \,|\, S$ in $\mathcal{F}(G)$ (equivalently, $\mathsf{v}_g(S_1) \le \mathsf{v}_g(S)$ for all $g \in G$). Given two sequences $S, T \in \mathcal{F}(G)$, we denote by $\gcd(S, T)$ the longest subsequence dividing both $S$ and $T$. If a sequence $S \in \mathcal{F}(G)$ is written in the form $S = g_1 \cdot \ldots \cdot g_l$, we tacitly assume that $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G$.

For a sequence

$$S \;=\; g_1 \cdot \ldots \cdot g_l \;=\; \prod_{g \in G} g^{\mathsf{v}_g(S)} \;\in \mathcal{F}(G)\,,$$

we call

$$|S| = l = \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0 \qquad \text{the } \textit{length} \text{ of } S\,,$$

$$\mathsf{h}(S) = \max\{\mathsf{v}_g(S) \mid g \in G\} \in [0, |S|] \qquad \text{the } \textit{maximum of the multiplicities} \text{ of } S\,,$$

$$\mathrm{supp}(S) = \{g \in G \mid \mathsf{v}_g(S) > 0\} \subset G \qquad \text{the } \textit{support} \text{ of } S\,,$$

$$\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g \in G} \mathsf{v}_g(S) g \in G \qquad \text{the } \textit{sum} \text{ of } S\,,$$

$$\Sigma_k(S) = \Big\{ \sum_{i \in I} g_i \;\Big|\; I \subset [1,l] \text{ with } |I| = k \Big\}$$

the *set of $k$-term subsums* of $S$, for all $k \in \mathbb{N}$,

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

and

$$\Sigma(S) = \Sigma_{\ge 1}(S) \text{ the } \textit{set of (all) subsums} \text{ of } S\,.$$

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 $1 \ne S$, $\sigma(S) = 0$, and every $S'|S$ with $1 \le |S'| < |S|$ is zero-sum free.

We denote by $\mathcal{A}(G) \subset \mathcal{F}(G)$ the set of all minimal zero-sum sequences over $G$. Every map of abelian groups $\varphi\colon G \to H$ extends to a homomorphism $\varphi\colon \mathcal{F}(G) \to \mathcal{F}(H)$ where $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_l)$. We say that $\varphi$ is *constant* on $S$ if $\varphi(g_1) = \ldots = \varphi(g_l)$. If $\varphi$ is a homomorphism, then $\varphi(S)$ is a zero-sum sequence if and only if $\sigma(S) \in \mathrm{Ker}(\varphi)$.

**Definition 2.1.** Let $G$ be a finite abelian group with exponent $n$.

1. Let $\mathsf{D}(G)$ denote the smallest integer $l \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a zero-sum subsequence. Equivalently, we have $\mathsf{D}(G) = \max\{|S| \mid S \in \mathcal{A}(G)\}$), and $\mathsf{D}(G)$ is called the *Davenport constant* of $G$.
2. Let $\eta(G)$ denote the smallest integer $l \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a zero-sum subsequence $T$ of length $|T| \in [1,n]$.
3. We say that $G$ has Property **C** if every sequence $S$ over $G$ of length $|S| = \eta(G) - 1$, with no zero-sum subsequence of length in $[1,n]$, has the form $S = T^{n-1}$ for some sequence $T$ over $G$.

**Lemma 2.2.** *Let $G = C_{n_1} \oplus C_{n_2}$ with $1 \le n_1 \mid n_2$.*

1. *We have $\mathsf{D}(G) = n_1 + n_2 - 1$ and $\eta(G) = 2n_1 + n_2 - 2$.*
2. *If $n_1 = n_2$ and $G$ has Property* **B**, *then $G$ has Property* **C**.

*Proof.* 1. See [5, Theorem 5.8.3].
2. See [2, Theorem 6.2] and [3, Theorem 6.7.2.(b)]. □

**Lemma 2.3.** *Let $G = C_n \oplus C_n$ with $n \ge 2$.*

1. *Then the following statements are equivalent:*
   (a) *If $S \in \mathcal{F}(G)$, $|S| = 3n - 3$ and $S$ has no zero-sum subsequence $T$ of length $|T| \ge n$, then there exists some $a \in G$ such that $0^{n-1}a^{n-2} \mid S$.*
   (b) *If $S \in \mathcal{F}(G)$ is zero-sum free and $|S| = 2n - 2$, then $a^{n-2} \mid S$ for some $a \in G$.*
   (c) *If $S \in \mathcal{A}(G)$ and $|S| = 2n - 1$, then $a^{n-1} \mid S$ for some $a \in G$.*

(d) *If* $S \in \mathcal{A}(G)$ *and* $|S| = 2n-1$, *then there exists a basis* $(e_1, e_2)$ *of* $G$ *and integers* $x_1, \ldots, x_n \in [0, n-1]$, *with* $x_1 + \ldots + x_n \equiv 1 \mod n$, *such that*

$$S = e_1^{n-1} \prod_{\nu=1}^{n} (x_\nu e_1 + e_2)\,.$$

2. *Let* $S \in \mathcal{A}(G)$ *be of length* $|S| = 2n-1$ *and* $e_1 \in G$ *with* $\mathsf{v}_{e_1}(S) = n-1$. *If* $(e_1, e_2')$ *is a basis of* $G$, *then there exist some* $b \in [0, n-1]$ *and* $a_1', \ldots, a_n' \in [0, n-1]$, *with* $\gcd(b, n) = 1$ *and* $\sum_{\nu=1}^{n} a_\nu' \equiv 1 \mod n$, *such that*

$$S = e_1^{n-1} \prod_{\nu=1}^{n} (a_\nu' e_1 + b e_2')\,.$$

3. *If* $S \in \mathcal{A}(G)$ *has length* $|S| = 2n-1$, *then* $\operatorname{ord}(g) = n$ *for all* $g \in \operatorname{supp}(S)$.

*Proof.* 1. See [5, Theorem 5.8.7].

2. This follows easily from 1; for details see [2, Proposition 4.1].

3. See [5, Theorem 5.8.4]. □

The characterization in Lemma 2.3.1 gives rise to the following definition.

**Definition 2.4.** Let $G = C_n \oplus C_n$ with $n \ge 2$.

1. Let $\Upsilon(G)$ be the set of all $S \in \mathcal{A}(G)$ for which there exists a basis $(e_1, e_2)$ of $G$ and integers $x_1, \ldots, x_n \in [0, n-1]$, with $x_1 + \ldots + x_n \equiv 1 \mod n$, such that $S = e_1^{n-1} \prod_{\nu=1}^{n} (x_\nu e_1 + e_2)$.
2. Let $\Upsilon_u(G)$ be the set of those $S \in \Upsilon(G)$ with a unique term of multiplicity $n-1$, and let $\Upsilon_{nu}(G) = \Upsilon(G) \setminus \Upsilon_u(G)$.

Thus, by Lemma 2.3.1, a group $G = C_n \oplus C_n$ with $n \ge 2$ has Property **B** if and only if $\mathcal{A}(G) = \Upsilon(G)$.

**Lemma 2.5.** *Let* $G = C_{mn} \oplus C_{mn}$ *with* $m, n \ge 2$, *let* $S \in \mathcal{A}(G)$ *be of length* $|S| = 2mn - 1$, *and let* $\varphi \colon G \to G$ *denote the multiplication by* $m$ *homomorphism.*

1. $\varphi(S)$ *is not a product of* $2m$ *zero-sum subsequences. Every zero-sum subsequence* $T$ *of* $\varphi(S)$ *of length* $|T| \in [1, n]$ *has length* $n$, *and* $0 \notin \operatorname{supp}(\varphi(S))$.
2. $S$ *may be written in the form* $S = W_0 \cdot \ldots \cdot W_{2m-2}$, *where* $W_0, \ldots, W_{2m-2} \in \mathcal{F}(G)$ *with* $|W_0| = 2n-1$, $|W_1| = \ldots = |W_{2m-2}| = n$ *and* $\sigma(W_0), \ldots, \sigma(W_{2m-2}) \in \operatorname{Ker}(\varphi)$.

*Proof.* See [2, Lemma 3.14]. □

The following is the Erdős-Ginzburg-Ziv Theorem and the corresponding characterization of extremal sequences.

**Theorem 2.6.** *Let* $G$ *be a cyclic group of order* $n \ge 2$ *and* $S \in \mathcal{F}(G)$.

1. *If* $|S| \ge 2n-1$, *then* $0 \in \Sigma_n(S)$.
2. *If* $|S| = 2n-2$ *and* $0 \notin \Sigma_n(S)$, *then* $S = g^{n-1} h^{n-1}$ *for some* $g, h \in G$ *with* $\operatorname{ord}(g-h) = n$.

*Proof.* 1. See [5, Corollary 5.7.5] or [8, Theorem 2.5].

2. See [1, Lemma 4] for one of the original proofs, and [**?**, Section 7.A]. □

The following result was a conjecture of Y. ould Hamidoune [7] confirmed in [6, Theorem 1].

**Theorem 2.7.** *Let $G$ be a finite abelian group, $S \in \mathcal{F}(G)$ of length $|S| \ge |G| + 1$, and $k \in \mathbb{N}$ with $k \le |\mathrm{supp}(S)|$. If $\mathsf{h}(S) \le |G| - k + 2$ and $0 \notin \Sigma_{|G|}(S)$, then $|\Sigma_{|G|}(S)| \ge |S| - |G| + k - 1$.*

## 3. Preparatory Results.

We first prove several lemmas determining in what ways a sequence $S \in \Upsilon(C_m \oplus C_m)$, where $m \ge 4$, can be slightly perturbed and still remain in $\Upsilon(C_m \oplus C_m)$. These will later be heavily used in Section 5, always in the setting where $K = \mathrm{Ker}(\varphi)$ and $\varphi \colon G \to G$ is the multiplication by $m$ map.

**Lemma 3.1.** *Let $K = C_m \oplus C_m$ with $m \ge 4$, let $g \in K$, and let $S = f_1^{m-1} \prod_{\nu=1}^m (x_\nu f_1 + f_2) \in \Upsilon_u(K)$ with $x_1, \ldots, x_m \in \mathbb{Z}$.*

1. *If $S' = f_1^{-2} S (f_1 + g)(f_1 - g) \in \Upsilon(K)$, then $g = 0$ and hence $S = S'$.*
2. *If $S' = f_1^{-1}(x_j f_1 + f_2)^{-1} S (f_1 + g)(x_j f_1 + f_2 - g) \in \Upsilon(K)$, then $g \in \{0,\, (x_j - 1)f_1 + f_2\}$ and hence $S = S'$.*
3. *If $S' = (x_j f_1 + f_2)^{-1}(x_k f_1 + f_2)^{-1} S (x_j f_1 + f_2 + g)(x_k f_1 + f_2 - g) \in \Upsilon(K)$ with $j, k \in [1, m]$ distinct, then $g \in \langle f_1 \rangle$.*

*Proof.* 1. Assume to the contrary that $g \ne 0$ and thus $S \ne S'$. Then $\mathsf{v}_{f_1}(S') < m - 1$ and, since $S \in \Upsilon_u(K)$, it follows that there is some $j \in [1, m]$ such that $(x_j f_1 + f_2)^{m-1} \mid S'$, $(x_j f_1 + f_2)^{m-3} \mid S$, and $x_j f_1 + f_2 = f_1 + g$. If we set $f_2' = x_j f_1 + f_2$, then $S = f_1^{m-1} \prod_{\nu=1}^m \big((x_\nu - x_j) f_1 + f_2'\big)$, and thus we may assume that $f_2 = f_2'$. Then $f_2 = f_1 + g$ and $f_1 - g = f_2 - 2g = 2f_1 - f_2$. Since $m \ge 4$, it follows that $f_1 \mid S'$. Since $S' \in \Upsilon(K)$, $f_2^{m-1} \mid S'$ and $f_1, 2f_1 - f_2 \in \mathrm{supp}(S') \setminus \{f_2\}$, it follows that $(2f_1 - f_2) - f_1 = f_1 - f_2 \in \langle f_2 \rangle$, a contradiction.

2. After renumbering, we may suppose that $j = n$. If $f_1^{m-1} | S'$ then $f_1 + g = f_1$ or $x_n f_1 + f_2 - g = f_1$, and $S' = S$. Otherwise, $f_1^{m-1} \nmid S'$ and we shall derive a contradiction. Observe that we cannot have $f_1 + g = x_n f_1 + f_2 - g = x_j f_1 + f_2$. Thus, since $S' \in \Upsilon(K)$ and $S \in \Upsilon_u(K)$, it follows that (after renumbering again if necessary) either

$$S' = f_1^{m-2}(x f_1 + f_2)^{m-1}(x_n f_1 + f_2 - g)(x_{n-1} f_1 + f_2) \quad \text{with} \quad f_1 + g = x f_1 + f_2\,,$$

or

$$S' = f_1^{m-2}(x f_1 + f_2)^{m-1}(f_1 + g)(x_{n-1} f_1 + f_2) \quad \text{with} \quad x_n f_1 + f_2 - g = x f_1 + f_2\,.$$

In the first case, we have $(x_n f_1 + f_2 - g) = (x_n - x + 1) f_1$ and hence $f_1^{m-2}((x_n - x + 1) f_1) | S'$. However, since $(x_n - x + 1) f_1 = (x_n f_1 + f_2 - g) \ne f_1$, it follows that $f_1^{m-2}((x_n - x + 1) f_1)$ is not zero-sum free, a contradiction. In the second case, one can derive a contradiction similarly.

3. Since $m \ge 3$, $f_1^{m-1} \mid S'$ and $S' \in \Upsilon(K)$, it follows that $(x_j f_1 + f_2 + g) - (x_l f_1 + f_2) \in \langle f_1 \rangle$, where $l \ne j$, $k$, and hence $g \in \langle f_1 \rangle$. □

**Lemma 3.2.** *Let* $K = C_m \oplus C_m$ *with* $m \ge 4$, $g \in K$ *and* $S = f_1^{m-1} f_2^{m-1}(f_1+f_2) \in \Upsilon_{nu}(K)$.

1. *If* $S' = f_1^{-2} S(f_1+g)(f_1-g) \in \Upsilon(K)$, *then* $g \in \langle f_2 \rangle$.
2. *If* $S' = f_2^{-2} S(f_2+g)(f_2-g) \in \Upsilon(K)$, *then* $g \in \langle f_1 \rangle$.
3. *If* $S' = f_1^{-1} f_2^{-1} S(f_1+g)(f_2-g) \in \Upsilon(K)$, *then* $S = S'$ *and* $g \in \{0, -f_1+f_2\}$.
4. *If* $S' = f_1^{-1}(f_1+f_2)^{-1} S(f_1+g)(f_1+f_2-g) \in \Upsilon(K)$, *then* $g \in \langle f_2 \rangle$.
5. *If* $S' = f_2^{-1}(f_1+f_2)^{-1} S(f_2+g)(f_1+f_2-g) \in \Upsilon(K)$, *then* $g \in \langle f_1 \rangle$.

*Proof.* 1. Since $f_2^{m-1} \mid S'$ and $S' \in \Upsilon(K)$, it follows that $f_1 + g - (f_1+f_2) \in \langle f_2 \rangle$, whence $g \in \langle f_2 \rangle$.

2. Analogous to 1.

3. If $f_1^{m-1} \mid S'$ or $f_2^{m-1} \mid S'$, the result follows. Otherwise, $m \ge 4$ and $\mathsf h(S') = m-1$ imply that $m = 4$ and $f_1 + g = f_2 - g = f_1 + f_2$, a contradiction.

4. Since $m \ge 3$, it follows that $f_1 \mid S'$. Now we have $f_2^{m-1} \mid S'$ and $S' \in \Upsilon(K)$ so that $(f_1+f_2-g)-f_1 \in \langle f_2 \rangle$, implying $g \in \langle f_2 \rangle$, as desired.

5. Analogous to 4. □

**Lemma 3.3.** *Let* $K = C_m \oplus C_m$ *with* $m \ge 4$, $g \in K$ *and* $S = f_1^{m-1} f_2^{m-1}(f_1+f_2) \in \Upsilon_{nu}(K)$.

1. *If* $S' = f_1^{-2} S(f_1+g)(f_1-g) \in \Upsilon_{nu}(K)$, *then* $g = 0$, *and hence* $S = S'$.
2. *If* $S' = f_2^{-2} S(f_2+g)(f_2-g) \in \Upsilon_{nu}(K)$, *then* $g = 0$, *and hence* $S = S'$.
3. *If* $S' = f_1^{-1} f_2^{-1} S(f_1+g)(f_2-g) \in \Upsilon_{nu}(K)$, *then* $g \in \{0, -f_1+f_2\}$, *and hence* $S = S'$.
4. *If* $S' = f_1^{-1}(f_1+f_2)^{-1} S(f_1+g)(f_1+f_2-g) \in \Upsilon_{nu}(K)$, *then* $g \in \{0, f_2\}$, *and hence* $S = S'$.
5. *If* $S' = f_2^{-1}(f_1+f_2)^{-1} S(f_2+g)(f_1+f_2-g) \in \Upsilon_{nu}(K)$, *then* $g \in \{0, f_1\}$, *and hence* $S = S'$.

*Proof.* 1. Assume to the contrary that $g \ne 0$ and $S \ne S'$. Since $S' \in \Upsilon_{nu}(K)$ and $m \ge 4$, we get $f_1 + g = f_1 - g = f_1 + f_2$ and hence $-2f_2 = 2g = 0$, a contradiction.

2. - 5. Similar. □

Next we prove two simple structural lemmas which will be our all-purpose tools for turning locally obtained information into global structural conditions on $S$. They are also the reason for the hypothesis of $m$ and $n$ odd in the Theorem.

**Lemma 3.4.** *Let* $G$ *be an abelian group,* $a \in G$ *with* $\mathrm{ord}(a) > 2$, *and* $S, T \in \mathcal F(G) \setminus \{1\}$ *with* $|\mathrm{supp}(S)| \ge |\mathrm{supp}(T)|$.

1. *If* $\mathrm{supp}(S) - \mathrm{supp}(T) = \{0\}$, *then* $S = g^{|S|}$ *and* $T = g^{|T|}$, *for some* $g \in G$.
2. *If* $\mathrm{supp}(S) - \mathrm{supp}(T) \subset \{0, a\}$, *then* $S = g^s (g+a)^{|S|-s}$ *and* $T = g^{|T|}$, *for some* $g \in G$ *and* $s \in [0, |S|]$.
3. *If* $|S|, |T| \ge 2$ *and* $\bigcup_{i=1}^{2} (\Sigma_i(S) - \Sigma_i(T)) \subset \{0, a\}$, *then either* $S = g^{|S|-1}(g+a)$ *and* $T = g^{|T|}$, *or else* $S = g^{|S|}$ *and* $T = g^{|T|}$, *for some* $g \in G$.

*Proof.* Note that $\Sigma_1(S) = \mathrm{supp}(S)$ and that all hypotheses imply $\mathrm{supp}(S) - \mathrm{supp}(T) \subset \{0, a\}$. Since $\mathrm{ord}(a) > 2$, it follows that $\{0, a\}$ contains no periodic subset, and thus Kneser's Theorem (see e.g., [5, Theorem 5.2.6]) implies that

$$2 \ge |\mathrm{supp}(S) - \mathrm{supp}(T)| \ge |\mathrm{supp}(S)| + |\mathrm{supp}(T)| - 1\,.$$

Therefore we get $|\mathrm{supp}(S)| \le 2$ and $|\mathrm{supp}(T)| = 1$. Items 1 and 2 now easily follow. For the proof of part 3, we apply 2, and thus we may assume that $\mathrm{supp}(S) \subset \{g, (g+a)\}$ and $T = g^{|T|}$. Now if item 3 is false, then $(g+a)^2 \mid S$, whence

$$2a = ((g+a)+(g+a)) - (g+g) \in \bigcup_{i=1}^{2} (\Sigma_i(S) - \Sigma_i(T)) \subset \{0, a\},$$

contradicting that $\mathrm{ord}(a) > 2$. □

**Lemma 3.5.** *Let $G$ be an abelian group and let $S \in \mathcal{F}(G)$.*

1. *If $k \in [1, |S|-1]$ and $|\Sigma_k(S)| \le 2$, then $|\mathrm{supp}(S)| \le 2$.*
2. *If $k \in [2, |S|-2]$ and $|\Sigma_k(S)| \le 2$ and $\Sigma_k(S)$ is not a coset of a cardinality two subgroup, then either $S = g^{|S|}$ or $S = g^{|S|-1}h$, for some $g, h \in G$.*
3. *If $k \in [1, |S|-1]$ and $|\Sigma_k(S)| \le 1$, then $S = g^{|S|}$ for some $g \in G$.*

*Proof.* 1. Assume to the contrary that $|\mathrm{supp}(S)| \ge 3$, and pick three distinct elements $x, y, z \in \mathrm{supp}(S)$. If $k = |S|-1$, then $\Sigma_{|S|-1}(S) = \sigma(S) - \Sigma_1(S)$ and hence $|\Sigma_{|S|-1}(S)| = |\mathrm{supp}(S)| \ge 3$, a contradiction. Therefore $k \le |S|-2$. Let $T$ be a subsequence of $(xyz)^{-1}S$ of length $|T| = k-1 \le |S|-3$. Then $\{x, y, z\} + \sigma(T)$ is a cardinality three subset of $\Sigma_k(S)$, a contradiction.

2. By 1, we have $S = g^{s_1}h^{s_2}$, with $s_1, s_2 \in \mathbb{N}_0$, $s_1 \ge s_2$ and $g, h \in G$ distinct. Assume to the contrary that $s_2 \ge 2$. Since $\Sigma_{|S|-k}(S) = \sigma(S) - \Sigma_k(S)$, it suffices to consider the case $k \le \frac{1}{2}|S|$, and thus we have $s_1 \ge \frac{1}{2}|S| \ge k \ge 2$. Hence the elements $kg$, $(k-1)g + h$ and $(k-2)g + 2h$ are all contained in $\Sigma_k(S)$. Thus, since $|\Sigma_k(S)| \le 2$ and $g \ne h$, it follows $\mathrm{ord}(h-g) = 2$ and $\Sigma_k(S) = kg + \{0, h-g\}$, contradicting that $\Sigma_k(S)$ is not a coset of a cardinality two subgroup.

3. If the conclusion is false, there are distinct $x, y \in G$ with $xy|S$, and then $\{x, y\} + \sigma(S')$ is a cardinality two subset of $\Sigma_k(S)$ for any $S'|(xy)^{-1}S$ with $0 \le |S'| = k-1 \le |S|-2$. □

## 4. On the Structure of $\varphi(S)$

**Definition 4.1.** Let $G = C_{mn} \oplus C_{mn}$ with $m, n \ge 2$, let $S \in \mathcal{A}(G)$ with $|S| = 2mn-1$, and let $\varphi\colon G \to G$ be the multiplication by $m$ homomorphism. Let

$$\Omega'(S) = \Omega' = \{(W_0, \ldots, W_{2m-2}) \in \mathcal{F}(G)^{2m-1} \mid S = W_0 \cdot \ldots \cdot W_{2m-2},$$
$$\sigma(W_i) \in \mathrm{Ker}(\varphi) \text{ and } |W_i| > 0 \text{ for all } i \in [0, 2m-2]\}$$

and

$$\Omega(S) = \Omega = \{(W_0, \ldots, W_{2m-2}) \in \Omega' \mid |W_1| = \ldots = |W_{2m-2}| = n\}.$$

The elements $(W_0, \ldots, W_{2m-2}) \in \Omega'(S)$ will be called *product decompositions* of $S$. If $W \in \Omega'$, we implicitly assume that $W = (W_0, \ldots, W_{2m-2})$.

By Lemma 2.5, $\Omega \ne \emptyset$, and if $W \in \Omega$, then $\varphi(W_0), \ldots, \varphi(W_{2m-2})$ are minimal zero-sum sequences over $\varphi(G)$. Proposition 4.2 below shows that $\varphi(S)$ is highly structured. We will later in CLAIMS A, B and C of Section 5 (with much effort) show that this structure lifts to the original sequence $S$. As this lift will only be 'near perfect' (there will be one exceptional term $x|S$ for which the structure is not shown to lift), we will then, in CLAIM D of Section 5, need Theorem 2.7 to finish the proof of the Theorem.

**Proposition 4.2.** *Let $G = C_{mn} \oplus C_{mn}$ with $m, n \ge 2$, and suppose that $C_n \oplus C_n$ has Property* **B**. *Let $S \in \mathcal{A}(G)$ with $|S| = 2mn-1$, and let $\varphi\colon G \to G$ be the multiplication by $m$ homomorphism. Then there exist a product decomposition $(W_0, \ldots, W_{2m-2})$ of $S$ and a basis $(e_1, e_2)$ of $\varphi(G)$ such that*

$$\varphi(W_0) = e_1^{n-1} \prod_{\nu=1}^{n} (x_\nu e_1 + e_2) \quad \text{and} \quad \varphi(W_i) \in \Big\{ e_1^n, \ \prod_{\nu=1}^{n} (c_{i,\nu} e_1 + e_2) \Big\}, \tag{1}$$

*where $x_1, \ldots, x_n \in [0, n-1]$, $x_1 + \ldots + x_n \equiv 1 \mod n$, all $c_{i,\nu} \in [0, n-1]$, and $c_{i,1} + c_{i,2} + \ldots + c_{i,n} \equiv 0 \mod n$ for all $i$. In particular,*

$$\varphi(S) = e_1^{\ell n - 1} \prod_{\nu=1}^{2mn-\ell n} (x_\nu e_1 + e_2)\,,$$

*where $\ell \in [1, 2m-1]$ and $x_\nu \in [0, n-1]$ for all $\nu \in [1, 2mn - \ell n]$.*

*Proof.* If $n = 2$, then it is easy to see (in view of Lemma 2.5) that (1) holds. From now on we assume that $n \ge 3$. We distinguish two cases.

CASE 1: For every product decomposition $W \in \Omega$, there exist distinct elements $g_1, g_2 \in \varphi(G)$ such that $\mathsf{v}_{g_1}\big(\varphi(W_0)\big) = \mathsf{v}_{g_2}\big(\varphi(W_0)\big) = n-1$.

Let us fix a product decomposition $W \in \Omega$. By Lemma 2.3, there is a basis $(e_1, e_2')$ of $\varphi(G)$ such that

$$\varphi(W_0) = e_1^{n-1} \prod_{\nu=1}^{n} (x_\nu e_1 + e_2')$$

where $x_1, \ldots, x_n \in [0, n-1]$ and$x_1 + \ldots + x_n \equiv 1 \mod n$. Thus, by assumption of CASE 1, it follows that

$$\varphi(W_0) = e_1^{n-1} (x e_1 + e_2')^{n-1} \big( (1+x) e_1 + e_2' \big) \quad \text{with} \quad x \in [0, n-1]\,.$$

As a result,

$$(e_1, e_2) = (e_1, x e_1 + e_2') = (e_1, e_2') \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

is a basis of $\varphi(G)$ and

$$\varphi(W_0) = e_1^{n-1} e_2^{n-1} (e_1 + e_2)\,.$$

We continue with the following assertion.

**A.** For every $i \in [1, 2m-2]$, $\varphi(W_i)$ has one of the following forms:

$$e_1^n, e_2^n, (e_1+e_2)^n, (-e_1+e_2)^n, (e_1-e_2)^n, e_1(e_1+e_2)^{n-2}(e_1+2e_2), e_2(e_1+e_2)^{n-2}(2e_1+e_2)\,.$$

Suppose that **A** is proved. If the two forms $(e_1 - e_2)^n$ and $e_1(e_1+e_2)^{n-2}(e_1+2e_2)$ do not occur, then $\varphi(W_i)$ has the required form with basis $(e_1, e_2)$. If the two forms $(-e_1+e_2)^n$ and $e_2(e_1+e_2)^{n-2}(2e_1+e_2)$ do not occur, then $\varphi(W_i)$ has the required form with basis $(e_2, e_1)$. Thus by symmetry, it remains to verify that there are no distinct $i, j \in [1, 2m-2]$ such that

(i) $\varphi(W_i) = e_1(e_1+e_2)^{n-2}(e_1+2e_2)$ and $\varphi(W_j) = e_2(e_1+e_2)^{n-2}(2e_1+e_2)$,
(ii) $\varphi(W_i) = e_1(e_1+e_2)^{n-2}(e_1+2e_2)$ and $\varphi(W_j) = (-e_1+e_2)^n$, or
(iii) $\varphi(W_i) = (e_1-e_2)^n$ and $\varphi(W_j) = (-e_1+e_2)^n$.

Indeed, if (i) held, then $(2e_1 + e_2)(e_1 + 2e_2)(e_1 + e_2)^{n-3}$ would be a zero-sum subsequence of $\varphi(W_i W_j)$ of length $n-1$, contradicting Lemma 2.5. If (ii) held, then $(-e_1 + e_2)(e_1 + 2e_2)e_2^{n-3}$ would be a zero-sum subsequence of $\varphi(W_0 W_i W_j)$ of length $n-1$, contradicting Lemma 2.5. Finally, if (iii) held, then $(e_1 - e_2)(-e_1 + e_2)$ would be a zero-sum subsequence of $\varphi(W_i W_j)$ of length 2, also contradicting Lemma 2.5. Thus it remains to establish **A** to complete the case. To that end, let $i \in [1, 2m-2]$ be arbitrary. Then $\mathsf h\big(\varphi(W_0 W_i)\big) \ge n-1$, and we distinguish three subcases.

CASE 1.1: $\mathsf h\big(\varphi(W_0 W_i)\big) > n$.

Then $\mathsf v_g\big(\varphi(W_0 W_i)\big) > n$ for some $g \in \{e_1, e_2, e_1 + e_2\}$. If $g = e_1 + e_2$, then $\varphi(W_i) = (e_1 + e_2)^n$. Now suppose that $g \in \{e_1, e_2\}$, say $g = e_1$. Then

$$\varphi(W_0 W_i) = e_2^{n-1}(e_1 + e_2)e_1^n \prod_{\nu=1}^{n-1}(c_\nu e_1 + d_\nu e_2)\,,$$

where $c_\nu, d_\nu \in [0, n-1]$ for all $\nu \in [1, n-1]$, and $c_\nu = 1$ and $d_\nu = 0$ for some $\nu \in [1, n-1]$. By Lemma 2.5,

$$W_0' = e_2^{n-1}(e_1 + e_2)\prod_{\nu=1}^{n-1}(c_\nu e_1 + d_\nu e_2)$$

is a minimal zero-sum subsequence of $\varphi(S)$. Since $W'$ contains two distinct elements with multiplicity $n-1$ (by assumption of CASE 1), and since $e_1 | W_0'$, it follows that either

$$W_0' = e_1^{n-1}e_2^{n-1}(e_1 + e_2) \quad \text{or} \quad W_0' = e_1 e_2^{n-1}(e_1 + e_2)^{n-1}\,.$$

But in the second case, we would get $\sigma(W_0') = -2e_2 \ne 0$. Thus $W_0' = e_1^{n-1}e_2^{n-1}(e_1+e_2)$ and $\varphi(W_i) = e_1^n$.

CASE 1.2: $\mathsf h\big(\varphi(W_0 W_i)\big) = n$. We distinguish two further subcases.

CASE 1.2.1: $\varphi(W_i) = g^n$ for some $g \in \varphi(G) \setminus \{e_1, e_2, e_1 + e_2\}$.

We set $g = ce_1 + de_2$ with $c, d \in [0, n-1]$. By Lemmas 2.2 and 2.5, it follows that $\varphi(W_0)g^{n-1}$ has a zero subsequence $T$ of length $|T| = n$ and that $\varphi(W_i W_0)T^{-1}$ is a minimal zero-sum subsequence of $\varphi(S)$ of length $2n-1$, say

$$\varphi(W_i W_0)T^{-1} = e_2^q e_1^r (e_1 + e_2)^s (ce_1 + de_2)^t,$$

where $q \ge 1$, $r \ge 1$, $s \ge 0$ and $t \in [1, n-1]$.

Since $g \ne e_1 + e_2$, we infer that $s \le 1$. If $s = 1$, then, by assumption of CASE 1, we get

$$2n-1 = |W_i W_0 T^{-1}| = q + r + s + t \ge 1 + (q + r + t) \ge 1 + (n-1+n-1+1) > 2n-1\,,$$

a contradiction. Hence $s = 0$. Again, by assumption of CASE 1, we have the following possibilities:

- $q = r = n-1$ and $t = 1$.
- $q = t = n-1$ and $r = 1$.
- $q = 1$ and $r = t = n-1$.

If $q = r = n-1$ and $t = 1$, then $\sigma\big(\varphi(W_0 W_i)T^{-1}\big) = 0$ implies that $g = e_1 + e_2$, a contradiction. If $q = t = n-1$ and $r = 1$, then $\sigma\big((W_0 W_i)T^{-1}\big) = 0$ implies that $g = e_1 - e_2$ and $\varphi(W_i) = (e_1 - e_2)^n$. Finally, if $q = 1$ and $r = t = n-1$, then $\sigma\big(\varphi(W_0 W_i)T^{-1}\big) = 0$ implies that $g = -e_1 + e_2$ and $\varphi(W_i) = (-e_1 + e_2)^n$.

CASE 1.2.2: $\mathsf v_g\big(\varphi(W_0 W_i)\big) = n$ for some $g \in \{e_1, e_2, e_1 + e_2\}$.

Since $|W_i| = n$, $\sigma(\varphi(W_i)) = 0$ and $\mathsf{v}_{e_1+e_2}\big(\varphi(W_0)\big) = 1$, it follows that $g \ne e_1 + e_2$. Thus $g \in \{e_1, e_2\}$, say $g = e_1$. Then

$$\varphi(W_0 W_i) = e_2^{n-1}(e_1+e_2)e_1^n \prod_{\nu=1}^{n-1}(c_\nu e_1 + d_\nu e_2),$$

where $c_\nu, d_\nu \in [0, n-1]$ for all $\nu \in [1, n-1]$. By Lemma 2.5 and the assumption of CASE 1.2,

$$W_0' = e_2^{n-1}(e_1+e_2) \prod_{\nu=1}^{n-1}(c_\nu e_1 + d_\nu e_2)$$

is a minimal zero-sum subsequence of $\varphi(S)$ with $e_1 \nmid W_0'$. Since $W'$ contains two distinct elements with multiplicity $n-1$ (by the assumption of CASE 1), since $\sigma(\varphi(W_i)) = 0$, and since $e_1 \nmid W_0'$, it follows that

$$W_0' = e_2^{n-1}(e_1+e_2)^{n-1}(e_1+2e_2),$$

and thus

$$\varphi(W_i) = e_1(e_1+e_2)^{n-2}(e_1+2e_2)\,.$$

CASE 1.3: $\mathsf{h}\big(\varphi(W_0W_i)\big) = n-1$.

Since $\sigma(\varphi(W_i)) = 0$, it follows $\mathsf{v}_g(\varphi(W_0W_i)) \ne n-1$ for $g \notin \{e_1, e_2, e_1+e_2\}$. Suppose $\mathsf{v}_{e_1+e_2}(\varphi(W_0W_i)) = n-1$. Then

$$\varphi(W_i) = (e_1+e_2)^{n-2}(c_1e_1+d_1e_1)(c_2e_1+d_2e_2),$$

where $c_1, d_1, c_2, d_2 \in [0, n-1]$. By Lemmas 2.2 and 2.5 and the definition of Property **C**,

$$\varphi(W_0W_i)(e_1+e_2)^{-1}(c_2e_1+d_2e_2)^{-1}$$

has a zero-sum subsequence $T$ of length $|T| = n$ and $\varphi(W_0W_i)T^{-1}$ is a minimal zero-sum subsequence of $\varphi(S)$ of length $2n-1$. Thus it follows, in view of the assumptions of CASE 1 and CASE 1.3, and in view of

$$\varphi(W_0W_i) = e_1^{n-1}e_2^{n-1}(e_1+e_2)^{n-1}(c_1e_1+d_1e_2)(c_2e_1+d_2e_2),$$

that $\mathsf{h}(T) = n-1$, contradicting that $\sigma(T) = 0$. So we conclude that

$$\mathsf{v}_g\big(\varphi(W_0W_i)\big) < n-1 \quad \text{for all} \quad g \in \varphi(G) \setminus \{e_1, e_2\}\,. \tag{2}$$

We set $\varphi(W_i) = \prod_{\nu=1}^{n}(c_\nu e_1 + d_\nu e_2)$, where $c_\nu, d_\nu \in [0, n-1]$ for all $\nu \in [1, n]$, and pick some $\lambda \in [1, n]$. By Lemmas 2.2 and 2.5, it follows that $\varphi(W_0W_i)(c_\lambda e_1 + d_\lambda e_2)^{-1}$ has a zero-sum subsequence $T$ of length $|T| = n$ and that $\varphi(W_iW_0)T^{-1}$ is a minimal zero-sum subsequence of $\varphi(S)$ of length $2n-1$. By assumption of CASE 1 and (2), it follows that

$$\varphi(W_0W_i)T^{-1} = e_1^{n-1}e_2^{n-1}(e_1+e_2),$$

and thus $c_\lambda e_1 + d_\lambda e_2 = e_1 + e_2$. As $\lambda \in [1, n]$ was arbitrary, this implies that $\varphi(W_i) = (e_1+e_2)^n$, contradicting the hypothesis of CASE 1.3.

CASE 2: There exists a product decomposition $W \in \Omega$ such that $\mathsf{v}_g\big(\varphi(W_0)\big) = n-1$ for exactly one element $g \in \varphi(G)$.

By Lemma 2.3 and the assumption of CASE 2, there exists a basis $(e_1, e_2)$ of $\varphi(G)$ such that

$$\varphi(W_0) = e_1^{n-1} \prod_{\nu=1}^{n} (x_\nu e_1 + e_2),$$

where $x_1, \ldots, x_n \in [0, n-1]$ and $x_1 + \ldots + x_n \equiv 1 \mod n$ and at most $n-2$ of the elements $x_1, \ldots, x_n$ are equal. Let $i \in [1, 2m-2]$ be arbitrary, and let $\varphi(W_i) = \prod_{\nu=1}^{n}(c_\nu e_1 + d_\nu e_2)$, where $c_\nu, d_\nu \in [0, n-1]$ for all $\nu \in [1, n]$. We proceed to show that there exists $m_i \in \{0, n\}$ such that

$$\varphi(W_i) = e_1^{m_i} \prod_{\nu=1}^{n-m_i} (c_\nu e_1 + e_2),$$

which will complete the proof. We distinguish six subcases.

CASE 2.1: $\mathsf{h}\big(\varphi(W_i) \prod_{\nu=1}^{n}(x_\nu e_1 + e_2)\big) > n$.

Then there exists some $x \in [0, n-1]$ such that (after renumbering if necessary)

$$\varphi(W_i) \prod_{\nu=1}^{n} (x_\nu e_1 + e_2) = (x e_1 + e_2)^n \prod_{\nu=1}^{r} (c_\nu e_1 + d_\nu e_2) \prod_{\nu=1}^{s} (x_\nu e_1 + e_2),$$

where $r \in [1, n-1]$, $s \in [2, n-1]$ and $r + s = n$. Since

$$e_1^{n-1} \prod_{\nu=1}^{r} (c_\nu e_1 + d_\nu e_2) \prod_{\nu=1}^{s} (x_\nu e_1 + e_2)$$

is a minimal zero-sum subsequence of $\varphi(S)$, Lemma 2.3 implies that $d_1 = \ldots = d_r = 1$, whence $\varphi(W_i) = \prod_{\nu=1}^{n}(c_\nu e_1 + e_2)$.

CASE 2.2: $\mathsf{h}\big(\varphi(W_i) \prod_{\nu=1}^{n}(x_\nu e_1 + e_2)\big) = n$.

If $(c_1, d_1) = \ldots = (c_n, d_n)$ does not hold, then, similar to CASE 2.1, we obtain that $d_1 = \ldots = d_n = 1$. Therefore $c_1 = \ldots = c_n = c$ and $d_1 = \ldots = d_n = d$ for some $c, d \in [0, n-1]$.

Pick some $\lambda \in [1, n]$. By Lemmas 2.2 and 2.5, the definition of Property **C**, and the assumption of CASE 2,

$$\varphi(W_0 W_i)(x_\lambda e_1 + e_2)^{-1}(c e_1 + d e_2)^{-1} = (c e_1 + d e_2)^{n-1} e_1^{n-1} \prod_{\nu \in [1,n] \setminus \{\lambda\}} (x_\nu e_1 + e_2)$$

has a zero-sum subsequence $T$ of length $n$ and

$$\varphi(W_0 W_i) T^{-1}$$

is a minimal zero-sum subsequence of $\varphi(S)$ of length $2n-1$. Since $\varphi(G)$ has Property **B**, we have either

$$e_1^{n-1} \,|\, \varphi(W_0 W_i) T^{-1} \quad \text{or} \quad (c e_1 + d e_2)^{n-1} \,|\, \varphi(W_0 W_i) T^{-1} .$$

If $e_1^{n-1} \,|\, \varphi(W_0 W_i) T^{-1}$, then, since $(x_\lambda e_1 + e_2)(c e_1 + d e_2) \,|\, \varphi(W_0 W_i) T^{-1}$, it would follow that $d = 1$, whence $\varphi(W_i) = (c e_1 + e_2)^n$, as desired. Therefore $(c e_1 + d e_2)^{n-1} \,|\, \varphi(W_0 W_i) T^{-1}$.

Since $\varphi(W_i)$ is a minimal zero-sum sequence, it follows that

$$n = \operatorname{ord}(c e_1 + d e_2) = \frac{n}{\gcd(c, d, n)} ,$$

and hence there are $u, v \in \mathbb{Z}$ such that $uc + vd \equiv 1 \mod n$. Thus

$$(e_1', e_2') = (ce_1 + de_2, -ve_1 + ue_2) = (e_1, e_2) \cdot \begin{pmatrix} c & -v \\ d & u \end{pmatrix}$$

is a basis of $\varphi(G)$ and, for some sequence $Q$ over $\varphi(G)$,

$$\begin{aligned}\varphi(W_0 W_i) T^{-1} &= (ce_1 + de_2)^{n-1} e_1 (x_\lambda e_1 + e_2) Q \\ &= {e_1'}^{n-1} (ue_1' - de_2') \big( (x_\lambda u + v) e_1' + (c - x_\lambda d) e_2' \big) Q \,.\end{aligned}$$

Now Lemma 2.3 implies that $-d \equiv c - x_\lambda d \mod n$, whence $x_\lambda d \equiv c + d \mod n$. Therefore, since $\lambda$ was arbitrary, we get

$$d \equiv \sum_{\nu=1}^{n} x_\nu d \equiv n(c+d) \equiv 0 \mod n,$$

and thus $d = 0$. If $c \in [2, n]$, then $(ce_1) e_1^{n-c}$ is a zero-sum subsequence of $\varphi(S)$ of length $n - c + 1 < n$, a contradiction. Thus $c = 1$ and $\varphi(W_i) = e_1^n$.

CASE 2.3: $\mathsf{h}\big(\varphi(W_i) \prod_{\nu=1}^n (x_\nu e_1 + e_2)\big) = n - 1$ and $\mathsf{v}_{e_1}\big(\varphi(W_i)\big) \ge 2$.

After renumbering if necessary, we have

$$\varphi(W_0 W_i) = e_1^{n+1} (xe_1 + e_2)^{n-1} \prod_{\nu=1}^{r} (x_\nu e_1 + e_2) \prod_{\nu=1}^{s} (c_\nu e_1 + d_\nu e_2)$$

where $x \in [0, n-1], r \in [1, n-1], s \in [1, n-2]$ and $r + s = n - 1$. By Lemma 2.5,

$$W' = e_1 (xe_1 + e_2)^{n-1} \prod_{\nu=1}^{r} (x_\nu e_1 + e_2) \prod_{\nu=1}^{s} (c_\nu e_1 + d_\nu e_2)$$

is a minimal zero-sum subsequence of $\varphi(S)$ of length $2n - 1$. Since

$$(e_1, e_2') = (e_1, xe_1 + e_2) = (e_1, e_2) \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

is a basis of $\varphi(G)$ and

$$W' = e_1 {e_2'}^{n-1} \prod_{\nu=1}^{r} \big( (x_\nu - x) e_1 + e_2' \big) \prod_{\nu=1}^{s} \big( (c_\nu - x d_\nu) e_1 + d_\nu e_2' \big) \,,$$

Lemma 2.3 implies that $x_\nu - x \equiv 1 \mod n$ for all $\nu \in [1, r]$. Therefore we get $(n-r)x + r(x+1) \equiv \sum_{\nu=1}^n x_\nu \equiv 1 \mod n$. Hence $r = 1$ and

$$\varphi(W_0) = e_1^{n-1} (xe_1 + e_2)^{n-1} \big( (x+1) e_1 + e_2 \big) \,,$$

a contradiction to our assumption on $x_1, \ldots, x_n$ for CASE 2.

CASE 2.4: $\mathsf{h}\big(\varphi(W_i) \prod_{\nu=1}^n (x_\nu e_1 + e_2)\big) = n - 1$ and $\mathsf{v}_{e_1}(W_i) = 1$.

After renumbering if necessary, we get

$$\varphi(W_0 W_i) = e_1^{n} (xe_1 + e_2)^{n-1} \prod_{\nu=1}^{r} (x_\nu e_1 + e_2) \prod_{\nu=1}^{s} (c_\nu e_1 + d_\nu e_2)$$

with $x \in [0, n-1]$, $r \in [1, n-1]$, $s \in [1, n-1]$ and $r + s = n$. By Lemma 2.5,

$$W' = (xe_1 + e_2)^{n-1} \prod_{\nu=1}^{r} (x_\nu e_1 + e_2) \prod_{\nu=1}^{s} (c_\nu e_1 + d_\nu e_2)$$

is a minimal zero-sum subsequence of $\varphi(S)$ of length $2n-1$. Since

$$(e_1, e_2') = (e_1, xe_1 + e_2) = (e_1, e_2) \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

is a basis of $\varphi(G)$ and

$$W' = {e_2'}^{n-1} \prod_{\nu=1}^{r} \big( (x_\nu - x) e_1 + e_2' \big) \prod_{\nu=1}^{s} \big( (c_\nu - x d_\nu) e_1 + d_\nu e_2' \big) \,,$$

Lemma 2.3 implies that

$$x_1 - x \equiv \ldots \equiv x_r - x \equiv c_1 - x d_1 \equiv \ldots \equiv c_s - x d_s \mod n. \tag{3}$$

If $d_1 = \ldots = d_s = 1$, then $\varphi(W_i) = \prod_{\nu=1}^{n} (c_\nu e_1 + e_2)$, as desired. Therefore there is some $\nu \in [1, s]$ with $d_\nu \ne 1$, say $\nu = s$. Hence, since $\sigma(W_i) = 0$, it follows that there is also another $\nu' \in [1, s]$ with $d_{\nu'} \ne 1$ and $s = \nu \ne \nu'$. Thus, by Lemmas 2.2 and 2.5 and the definition of Property **C**,

$$\varphi(W_0 W_i) e_1^{-1} (c_s e_1 + d_s e_2)^{-1}$$

has a zero-sum subsequence $T$ of length $|T| = n$ and $\varphi(W_0 W_i) T^{-1}$ is a minimal zero-sum subsequence of $\varphi(S)$ of length $2n-1$. Since $\varphi(G)$ has Property **B**, it follows that either

$$e_1^{n-1} \,|\, \varphi(W_0 W_i) T^{-1} \quad \text{or} \quad (xe_1 + e_2)^{n-1} \,|\, \varphi(W_0 W_i) T^{-1} \,.$$

If $e_1^{n-1} \,|\, \varphi(W_0 W_i) T^{-1}$, then, since $(c_s e_1 + d_s e_2) \,|\, \varphi(W_0 W_i) T^{-1}$ and $(x_j e_1 + e_2) \,|\, \varphi(W_0 W_i) T^{-1}$ for some $j \in [1, n]$, Lemma 2.3 implies that $d_s = 1$, a contradiction. Therefore $(xe_1 + e_2)^{n-1} \,|\, \varphi(W_0 W_i) T^{-1}$. Thus, for some sequence $Q$ over $\varphi(G)$, we have

$$\varphi(W_0 W_i) T^{-1} = (xe_1 + e_2)^{n-1} e_1 (c_s e_1 + d_s e_2) Q \,.$$

Since

$$(e_1, e_2') = (e_1, xe_1 + e_2) = (e_1, e_2) \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

is a basis of $\varphi(G)$ and

$$\varphi(W_0 W_i) T^{-1} = e_1 {e_2'}^{n-1} \big( (c_s - x d_s) e_1 + d_s e_2' \big) Q \,,$$

Lemma 2.3 implies that $c_s - x d_s = 1$. Thus it follows from (3) that $x_1 \equiv \ldots \equiv x_r \equiv x + 1 \mod n$. Therefore we get $(n - r)x + r(x+1) \equiv \sum_{\nu=1}^{n} x_\nu \equiv 1 \mod n$. Hence $r = 1$ and

$$\varphi(W_0) = e_1^{n-1} (xe_1 + e_2)^{n-1} \big( (x+1) e_1 + e_2 \big) \,,$$

a contradiction to our assumption on $x_1, \ldots, x_n$ for CASE 2.

CASE 2.5: $\mathsf h\big(\varphi(W_i) \prod_{\nu=1}^{n} (x_\nu e_1 + e_2)\big) = n - 1$ and $\mathsf v_{e_1}\big(\varphi(W_i)\big) = 0$.

If $d_1 = \ldots = d_n = 1$, then the assertion follows. Therefore there is some $\nu \in [1, n]$ with $d_\nu \ne 1$, say $\nu = n$. Since $d_1 + \ldots + d_n \equiv 0 \mod n$, we may also assume that $d_{n-1} \ne 1$. We distinguish two subcases.

CASE 2.5.1: $\varphi(W_i)\prod_{\nu=1}^{n}(x_\nu e_1+e_2)$ contains two distinct elements with multiplicity $n-1$, say $xe_1+e_2$ and $ye_1+e_2$, where $x,\ y\in[0,n-1]$.

Then

$$\varphi(W_i)=(xe_1+e_2)^r(ye_1+e_2)^s(c_{n-1}e_1+d_{n-1}e_2)(c_ne_1+d_ne_2)$$

and

$$\prod_{\nu=1}^{n}(x_\nu e_1+e_2)=(xe_1+e_2)^{n-1-r}(ye_1+e_2)^{n-1-s},$$

where $r,\ s\in[1,n-3]$ and $r+s=n-2\geq 2$. By Lemmas 2.2 and 2.5, $\varphi(W_0W_i)(c_ne_1+d_ne_2)^{-1}$ has a zero-sum subsequence $T$ of length $|T|=n$ and $\varphi(W_0W_i)T^{-1}$ is a minimal zero-sum subsequence of $\varphi(S)$ of length $2n-1$. Since $\varphi(G)$ has Property **B**, it follows that

$$\mathsf{v}_g\big(\varphi(W_iW_0)T^{-1}\big)=n-1 \quad \text{for some} \quad g\in\{e_1,xe_1+e_2,ye_1+e_2\}\,.$$

Clearly, we have

$$e_1(xe_1+e_2)(ye_1+e_2)(c_ne_1+d_ne_2)\,|\,\varphi(W_0W_i)T^{-1}\,.$$

Since $d_n\neq 1$, Lemma 2.3 implies that $g\neq e_1$. Thus w.l.o.g. $g=xe_1+e_2$. Consequently, for some sequence $Q$ over $\varphi(G)$, we have

$$\varphi(W_0W_i)T^{-1}=(xe_1+e_2)^{n-1}e_1(ye_1+e_2)Q\,.$$

As before,

$$(e_1,e_2')=(e_1,xe_1+e_2)=(e_1,e_2)\cdot\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}$$

is a basis of $\varphi(G)$ and

$$\varphi(W_0W_i)T^{-1}={e_2'}^{n-1}e_1\big((y-x)e_1+e_2'\big)Q\,.$$

Now we obtain a contradiction as in CASE 2.3.

CASE 2.5.2: $\varphi(W_i)\prod_{\nu=1}^{n}(x_\nu e_1+e_2)$ contains exactly one element with multiplicity $n-1$, say $xe_1+e_2$ where $x\in[0,n-1]$.

After renumbering if necessary, we get

$$\varphi(W_0W_i)=e_1^{n-1}(xe_1+e_2)^{n-1}\prod_{\nu=1}^{r}(c_\nu e_1+d_\nu e_2)\prod_{\nu=1}^{s}(x_\nu e_1+e_2),$$

where $r\in[1,n-1], s\in[2,n-1]$ and $r+s=n+1$. If $d_1=\ldots=d_r=1$, then the assertion follows. So after renumbering again, we suppose that $d_r\neq 1$. Let $\lambda\in[1,s]$.

By Lemmas 2.2 and 2.5, the definition of Property **C**, and the assumption of CASE 2.5.2,

$$\varphi(W_0W_i)(c_re_1+d_re_2)^{-1}(x_\lambda e_1+e_2)^{-1}$$

has a zero-sum subsequence $T$ of length $|T|=n$ and $\varphi(W_0W_i)T^{-1}$ is a minimal zero-sum subsequence of $\varphi(S)$ of length $2n-1$. Since $\varphi(G)$ has Property **B**, it follows that

$$\mathsf{v}_g\big(\varphi(W_0W_i)T^{-1}\big)=n-1 \quad \text{for some} \quad g\in\{e_1,xe_1+e_2,\}\,.$$

Clearly, we have

$$e_1(xe_1+e_2)(c_re_1+d_re_2)(x_\lambda e_1+e_2)\,|\,\varphi(W_0W_i)T^{-1}\,.$$

Since $d_r \neq 1$, Lemma 2.3 implies that $g \neq e_1$, and hence $g = xe_1 + e_2$. Thus, for some sequence $Q$ over $\varphi(G)$, we have

$$\varphi(W_0 W_i) T^{-1} = (xe_1 + e_2)^{n-1} e_1 (x_\lambda e_1 + e_2) Q\,.$$

As before,

$$(e_1, e_2') = (e_1, xe_1 + e_2) = (e_1, e_2) \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

is a basis of $\varphi(G)$ and

$$\varphi(W_0 W_i) T^{-1} = {e_2'}^{n-1} e_1 \big( (x_\lambda - x) e_1 + e_2' \big) Q\,.$$

Hence Lemma 2.3 implies that $1 \equiv x_\lambda - x \mod n$. As $\lambda \in [1, s]$ was arbitrary, it follows that $x_1 \equiv \ldots \equiv x_s \equiv x + 1 \mod n$, and, as in CASE 2.3, we obtain a contradiction.

CASE 2.6: $\mathsf h\big(\varphi(W_i) \prod_{\nu=1}^{n} (x_\nu e_1 + e_2)\big) < n - 1$.

Let $\lambda \in [1, n]$ be arbitrary. By Lemmas 2.2 and 2.5,

$$\varphi(W_0 W_i)(c_\lambda e_1 + d_\lambda e_2)^{-1}$$

has a zero-sum subsequence $T$ of length $|T| = n$, and

$$\varphi(W_0 W_i) T^{-1}$$

is a minimal zero-sum subsequence of $\varphi(S)$ of length $2n - 1$. Since $\varphi(G)$ has Property **B**, it follows that $e_1^{n-1}$ divides $\varphi(W_0 W_i) T^{-1}$. Furthermore there is some $\nu \in [1, n]$ such that

$$(x_\nu e_1 + e_2)(c_\lambda e_1 + d_\lambda e_2) | \varphi(W_0 W_i) T^{-1}\,.$$

Thus Lemma 2.5 implies that either $d_\lambda = 1$ or $(c_\lambda, d_\lambda) = (1, 0)$. Thus, since $\lambda \in [1, n]$ was arbitrary and $\sigma(\varphi(W_i)) = 0$, we must either have $d_\lambda = 1$ for all $\lambda \in [1, n]$ or $(c_\lambda, d_\lambda) = (1, 0)$ for all $\lambda \in [1, n]$, and so either $\varphi(W_i) = e_1^n$ or $\varphi(W_i) = \prod_{\nu=1}^{n} (c_\nu e_1 + e_2)$, as desired □

## 5. Proof of the Theorem

Let $G = C_{mn} \oplus C_{mn}$, with $m$, $n \geq 3$ odd, $mn > 9$ and w.l.o.g. $m \geq 5$, such that Property **B** holds both for $C_m \oplus C_m$ and $C_n \oplus C_n$. Let $S \in \mathcal{A}(G)$ be a minimal zero-sum sequence of length $|S| = 2mn - 1$. The sequence $S$ will remain fixed throughout the rest of this section. Our goal is to show that $S$ contains an element with multiplicity $mn - 1$ (in other words, $\mathsf h(S) = mn - 1$). We proceed in the following way:

- First, using Proposition 4.2, we establish the setting and some detailed notation necessary to formulate the key ideas of the proof.
- Next, we proceed with four lemmas, Lemmas 5.1, 5.2, 5.3 and 5.4, that collect several arguments used repeatedly in the proof.
- Then we divide the main part of the proof into four claims, CLAIMS A, B, C and D, where in CLAIM D we finally show that $\mathsf h(S) = mn - 1$.

**The Setting and Key Definitions**

Since $S$ is fixed, we write $\Omega'$ and $\Omega$ instead of $\Omega'(S)$ and $\Omega(S)$ (see Definition 4.1). Recall that Lemma 2.3.3 implies that $\mathrm{ord}(x) = mn$ for all $x \in \mathrm{supp}(S)$. Let $\varphi \colon G \to G$ denote the multiplication by $m$ map. Then $\mathrm{Ker}(\varphi) = nG \cong C_m \oplus C_m$ and $\varphi(G) = mG \cong C_n \oplus C_n$.

Let $\Omega_0 \subset \Omega$ be all those $W \in \Omega$ for which there exists a basis $(me_1, me_2)$ of $\varphi(G)$, where $e_1, e_2 \in G$, such that $\varphi(W_0) = (me_1)^{n-1} \prod_{\nu=1}^{n} (x_\nu me_1 + me_2)$, where $x_1, \ldots, x_n \in \mathbb{Z}$ with $x_1 + \ldots + x_n \equiv 1 \mod n$, and such that for every $i \in [1, 2m-2]$, $\varphi(W_i)$ is either of the form $\varphi(W_i) = (me_1)^n$, or of the form $\varphi(W_i) = \prod_{\nu=1}^{n} (y_{i,\nu} me_1 + me_2)$, where $y_{i,1}, \ldots, y_{i,n} \in \mathbb{Z}$ with $y_{i,1} + \ldots + y_{i,n} \equiv 0 \mod n$. By Proposition 4.2, $\Omega_0$ is nonempty.

Let $W \in \Omega'$, and define $\widetilde{\sigma}(W) = \prod_{\nu=0}^{2m-2} \sigma(W_\nu) \in \mathcal{F}\big(\mathrm{Ker}(\varphi)\big)$. Since $S \in \mathcal{A}(G)$, it follows that $\widetilde{\sigma}(W) \in \mathcal{A}\big(\mathrm{Ker}(\varphi)\big)$. Thus, since Property **B** holds for $\mathrm{Ker}(\varphi)$, it follows that $\widetilde{\sigma}(W) \in \Upsilon\big(\mathrm{Ker}(\varphi)\big)$. Partition $\Omega_0 = \Omega_0^u \cup \Omega_0^{nu}$ by letting $\Omega_0^u$ be those $W \in \Omega_0$ with $\widetilde{\sigma}(W) \in \Upsilon_u\big(\mathrm{Ker}(\varphi)\big)$, and letting $\Omega_0^{nu}$ be those $W \in \Omega_0$ with $\widetilde{\sigma}(W) \in \Upsilon_{nu}\big(\mathrm{Ker}(\varphi)\big)$.

Let $W \in \Omega_0$, let $(me_1, me_2)$ be a basis of $\varphi(G)$ satisfying the definition of $\Omega_0$, with $e_1$, $e_2 \in G$, and let $(f_1, f_2)$ be a basis for $\mathrm{Ker}(\varphi)$ such that $\widetilde{\sigma}(W)$ can be written as in the definition of $\Upsilon\big(\mathrm{Ker}(\varphi)\big)$. Let $S_1$ be the subsequence of $S$ consisting of all terms $x$ with $\varphi(x) = me_1$, and define $S_2$ by $S = S_1S_2$. Let $I \subset \mathbb{Z}$ be an interval of length $n$. Then each term $x$ of $S_1$ has a unique representation of the form $x = e_1 + ng$, with $ng \in \mathrm{Ker}(\varphi)$ (where $g \in G$), and each term $x$ of $S_2$ has a unique representation of the form $x = ae_1 + e_2 + ng$, with $a \in I$ and $ng \in \mathrm{Ker}(\varphi)$ (where $g \in G$). Define $\psi(x) = ng \in \mathrm{Ker}(\varphi)$ and, for $x \in \mathrm{supp}(S_2)$, define $\iota(x) = a \in I \subset \mathbb{Z}$. We set $\psi(x) = \psi_1(x) + \psi_2(x)$, where $\psi_1(x) \in \langle f_1 \rangle$ and $\psi_2(x) \in \langle f_2 \rangle$. If $y \in \mathrm{Ker}(\varphi)$, with $y = y_1 f_1 + y_2 f_2$, then we also use $\psi_i(y)$ to denote $y_i f_i$. Note that, for $x \in \mathrm{supp}(S_1)$, the value of $\psi(x)$ depends upon the choice of $(e_1, e_2)$, and that, for $x \in \mathrm{supp}(S_2)$, the values of $\psi(x)$ and $\iota(x)$ depend upon the choice of $(e_1, e_2)$ and $I$. We will frequently need to vary the underlying choices for $(e_1, e_2)$ and $I$, and each time we do so the corresponding values of $\psi$ and $\iota$ will be affected. All maps will be extended to sequences as explained before Definition 2.1.

Let $\mathcal{A}_1(W)$ be those $W_i$ either with $i = 0$ or $\varphi(W_i) = (me_1)^n$, let $\mathcal{A}_2(W)$ be all remaining $W_i$ as well as $W_0$, and let $\mathcal{A}_i^*(W) = \mathcal{A}_i(W) \setminus \{W_0\}$ for $i \in \{1, 2\}$. If $W \in \Omega_0^u$, let $\mathcal{C}_0(W)$ be all those $W_i$ with $\mathsf{v}_{\sigma(W_i)}\big(\widetilde{\sigma}(W)\big) < m-1$, let $\mathcal{C}_1(W)$ be all remaining $W_i$, and let $\mathcal{C}_i^*(W) = \mathcal{C}_i(W) \setminus \{W_0\}$ for $i \in \{0, 1\}$. If $W \in \Omega_0^{nu}$, let $\mathcal{C}_0(W)$ be the unique $W_i$ with $\mathsf{v}_{\sigma(W_i)}\big(\widetilde{\sigma}(W)\big) < m-1$, and divide the remaining $2m-2$ blocks $W_i$ into either $\mathcal{C}_1(W)$ or $\mathcal{C}_2(W)$ depending on the value of $\sigma(W_i)$; analogously define $\mathcal{C}_i^*(W)$ for $i \in \{0, 1, 2\}$. When the context is clear, the $W$ will be omitted from the notation. We regard the elements $W_i$, $W_j \in \mathcal{A}_1$ as distinct when $i \neq j$, follow the same convention for all other similar collections of $W_i$, and will refer to them as blocks.

We further subdivide $W_0 = W_0^{(1)} W_0^{(2)}$ with $W_0^{(1)} = \gcd(W_0, S_1)$ and $W_0^{(2)} = \gcd(W_0, S_2)$, and for a pair of subsequences $X$ and $Y$ with $XY \mid S_2$, we define $\epsilon'(X, Y)$ to be the integer in $[1, n]$ congruent to $\sigma(\iota(X)) - \sigma(\iota(Y))$ modulo $n$, and define $\epsilon(X, Y)$ to be the integer such that

$$n - \epsilon'(X, Y) + \sigma(\iota(X)) - \sigma(\iota(Y)) = \epsilon(X, Y)n.$$

The main idea of the proof is to swap individual terms contained in the blocks of $W \in \Omega_0$ in such a way so as to maintain that the resulting product decomposition still lies in $\Omega'$. Using the lemmas from Section 3, we will then derive information about the possible values of $\psi$ and $\iota$ obtained on the terms that have been swapped. The next three paragraphs detail the three major types of swaps that we will use.

If $U$, $V \in \mathcal{A}_1$ are distinct (thus $U = W_i$ and $V = W_j$ for some $i$ and $j$ distinct), then we may exchange any subsequence $X|U$ for a subsequence $Y|V$ with $|Y| = |X|$ (if $U = W_0$, then $X$ must additionally lie within $W_0^{(1)}$, and likewise for $V$) and the resulting product decomposition $W'$ will still lie in $\Omega_0$, equal to $W$ except that the blocks $U$ and $V$ of $W$ have been replaced by the blocks $U' := X^{-1}UY$ and $V' := Y^{-1}VX$. Moreover,

$$\sigma(V') = \sigma(V) + \sigma(\psi(X)) - \sigma(\psi(Y)). \tag{4}$$

We refer to this as a *type I swap.*

If $V \in \mathcal{A}_2^*$, and $Y|V$ and $X|W_0^{(2)}$ are subsequences with $|X| = |Y|$, then by exchanging the sequence $Y|V$ for the sequence $RX|W_0$, where $R|W_0^{(1)}$ is any subsequence with $|R| = n - \epsilon'(X, Y)$, we obtain a product decomposition $W'$ that still lies in $\Omega'$, equal to $W$ except that the blocks $V$ and $W_0$ of $W$ have been replaced by the blocks $V' := Y^{-1}VXR$ and $W_0' := R^{-1}X^{-1}W_0Y$. Moreover,

$$\sigma(V') = \sigma(V) + \epsilon(X, Y)ne_1 + \sigma(\psi(X)) - \sigma(\psi(Y)) + \sigma(\psi(R)). \tag{5}$$

We refer to this as a *type II swap.*

If $U$, $V \in \mathcal{A}_2$ are distinct, then we may exchange any subsequence $X|U$ for a subsequence $Y|V$ with $|Y| = |X|$ and $\sigma(\iota(X)) = \sigma(\iota(Y))$ (and if $U = W_0$, then $X$ must additionally lie within $W_0^{(2)}$, and likewise for $V$) and the resulting product decomposition $W'$ will still lie in $\Omega_0$, equal to $W$ except that the blocks $U$ and $V$ of $W$ have been replaced by the blocks $U' := X^{-1}UY$ and $V' := Y^{-1}VX$. Moreover,

$$\sigma(V') = \sigma(V) + \sigma(\psi(X)) - \sigma(\psi(Y)). \tag{6}$$

We refer to this as a *type III swap.*

We will often also have need to change from $W \in \Omega_0$ to another $W' \in \Omega_0$. One common way that this will be done will be to find $U \in \mathcal{A}_2^*$ and $X|UW_0^{(2)}$ ($X$ will often be a single element dividing $U$). Then $|X^{-1}UW_0^{(2)}| = 2n - |X|$. If there is an $n$-term subsequence $U'|X^{-1}UW_0^{(2)}$ with $\sigma(U') \in \mathrm{Ker}(\varphi)$ (as is guaranteed by Theorem 2.6.1 in case $|X| = 1$), then, defining $W_0'$ by $W_0'U' = W_0U$, we obtain a new product decomposition $W' \in \Omega_0$ by replacing the blocks $W_0$ and $U$ by $W_0'$ and $U'$. Moreover, $X \mid W_0'^{(2)}$. We refer to such a procedure as *pulling $X$ up into the new product decomposition $W'$.*

All of the above procedures result in a new product decomposition $W' \in \Omega'$, and we will always assume $W' = (W_0', \ldots, W_{2m-2}')$, with $W_k' = W_k$ for all blocks $W_k$ not involved in the procedure, and with $W_i'$ and $W_j'$ defined as above for the two blocks $W_i$ and $W_j$ involved in the procedure.

## Four Lemmas

We will often only consider $W \in \Omega_0^{nu}$ when $\Omega_0 = \emptyset$ (with one exception in CASE 3 of CLAIM C). The reason for this is to ensure that, if a swapping procedure applied to $W$ results in a new product decomposition $W' \in \Omega_0$, then $W' \in \Omega_0^{nu}$ is guaranteed, and hence the more powerful Lemma 3.3 is available (instead of the weaker Lemma 3.2).

The following lemma will be used in CASE 3 of CLAIM C to avoid having to consider a $W'' \in \Omega_0^{nu}$ when $\Omega_0^u \neq \emptyset$.

**Lemma 5.1.** *Let $W \in \Omega_0^u$, $U \in \mathcal{C}_1$ and $V_1, V_2 \in \mathcal{C}_0$ be distinct. Suppose there exist $X|U$ and $Y_1|V_1$ such that swapping $X$ for $Y_1$ yields a new product decomposition $W' \in \Omega'$ with the new block $U' = X^{-1}UY_1$ in $W'$ having $\sigma(U') \neq \sigma(U)$. If $Y_2|Y_1^{-1}V_1$ and $Z|V_2$ are nontrivial subsequences such that swapping $Y_2$ for $Z$ in $W$ yields a new product decomposition $W'' \in \Omega_0$, then $W'' \in \Omega_0^u$.*

*Proof.* Assume by contradiction that $W'' \in \Omega_0^{nu}$, so that w.l.o.g. $\widetilde{\sigma}(W'') = f_1^{m-1}f_2^{m-1}(f_1+f_2)$ with $\sigma(U) = f_1$ (since $\sigma(U)$ is a maximal multiplicity term in $\widetilde{\sigma}(W)$ and all blocks involved in the swap resulting in $W''$ are not of maximal multiplicity, it follows that $\sigma(U'') = \sigma(U)$ must be a maximal multiplicity term in $\widetilde{\sigma}(W'')$ as well). Since $m \geq 4$ (so that $f_2f_1^{m-1}|\widetilde{\sigma}(W)$), let $\sigma(V_1) = Cf_1 + f_2$ with $C \in [0, m-1]$. By hypothesis, we may swap $Y_1|V_1'' = Y_2^{-1}V_1Z$ for $X|U'' = U$ to obtain a new product decomposition $W''' \in \Omega'$, with new respective terms $V_1'''$ and $U'''$. Since (by hypothesis) swapping $X$ for $Y_1$ in $W$ yields a new product decomposition $W' \in \Omega'$ such that the new block $U' = X^{-1}UY_1$ in $W'$ has $\sigma(U') \neq \sigma(U)$, it follows from Lemma 3.1.2 that $\sigma(U''') = \sigma(U') = Cf_1 + f_2$ and $\sigma(V_1''') = \sigma(V_1'') + (1-C)f_1 - f_2$.

Suppose $\sigma(V_1'') = f_2$. Then, from the above paragraph, we conclude that

$$\widetilde{\sigma}(W''') = f_2^{m-2}(f_1+f_2)((1-C)f_1)f_1^{m-2}(Cf_1+f_2)\,.$$

Thus, since $\widetilde{\sigma}(W''') \in \Upsilon(\mathrm{Ker}(\varphi))$ and $m \geq 4$, it follows that $C = 0$, whence $\sigma(V_1'') = f_2 = Cf_1 + f_2 = \sigma(V_1)$. However, this implies that $\widetilde{\sigma}(W) = \widetilde{\sigma}(W'') \in \Upsilon_0^{nu}$, contrary to $W \in \Omega_0^u$. So we may assume instead that $\sigma(V_1'') = f_1 + f_2$ (note $\sigma(V_1'') \neq f_1$, since $\sigma(U) = f_1$, $U \in \mathcal{C}_1(W)$ and no terms from $\mathcal{C}_1(W)$ were involved in the swap resulting in $W''$).

In this case, we instead conclude that

$$\widetilde{\sigma}(W''') = f_2^{m-1}((2-C)f_1)f_1^{m-2}(Cf_1+f_2).$$

Thus, since $\widetilde{\sigma}(W''') \in \Upsilon(\mathrm{Ker}(\varphi))$ and $m \geq 3$, we conclude that $C = 1 = 2 - C$, and once more $\sigma(V_1'') = \sigma(V_1)$, yielding the same contradiction as in the previous paragraph, completing the lemma. □

The next two lemmas will often be used in conjunction, and will form one of our main swapping strategy arguments used for CLAIMS A and B. Note that Lemma 5.2(i) gives a strong structural description as well as a term of multiplicity at least $(|\mathcal{D}_1|+1)n-1$ in $S$, while Lemma 5.2(ii) allows us to invoke Lemma 5.3.

**Lemma 5.2.** *Let $W \in \Omega_0$ and, if $\Omega_0^u \neq \emptyset$, assume that $W \in \Omega_0^u$. Let $\mathcal{D}_1, \mathcal{D}_2 \subset \mathcal{A}_2^*$ be such that, for each (relevant) $i \in [0,2]$, there do not exist $U \in \mathcal{D}_1$ and $V \in \mathcal{D}_2$ with $U, V \in \mathcal{C}_i$. If either*

(a) *$|\mathcal{D}_1| \geq 1$ and every type III swap between $x|W_0^{(2)}$ and $y|W_j$, with $W_j \in \mathcal{D}_1$ and $\iota(x) = \iota(y)$, results in a new product decomposition $W'$ with $\sigma(W_0') = \sigma(W_0)$, or*

(b) *$|\mathcal{D}_1| \geq 2$ and $|\mathcal{D}_2| \geq 1$,*

*then one of the following two statements hold:*

(i) *There exist $x_0|W_0^{(2)}$, $g \in I$ and $\alpha \in \mathrm{Ker}(\varphi)$ such that $\iota(x_0) \equiv g+1 \mod n$, $\iota(x) = g$ and $\psi(x) = \alpha$, for all $x|x_0^{-1}W_0^{(2)}\prod_{V\in\mathcal{D}_1}V$.*

(ii) *There exist $W_j \in \mathcal{D}_1$, $X|W_0^{(2)}$ and $Y|W_j$ such that $|X| = |Y|$ and $\epsilon'(X,Y) \notin \{1,n\}$.*

*Proof.* We assume that (ii) fails and show that (i) holds. If $W_0 \in \mathcal{C}_0$, then choose $f_2$ such that $\sigma(W_0) = f_1 + f_2$; if $W \in \Omega_0^{nu}$, then choose $f_2$ such that $\widetilde{\sigma}(W) = f_1^{m-1}f_2^{m-1}(f_1+f_2)$ (note, in case $W_0 \in C_0$ and

$W \in \Omega_0^{nu}$, that this choice of $f_2$ agrees with the previous choice), and assume $\mathcal{C}_1$ consists of those $W_i$ with $\sigma(W_i) = f_1$; and if $W_0 \notin \mathcal{C}_0$, then w.l.o.g. assume $W_0 \in \mathcal{C}_1$.

Applying Lemma 3.4.3 to $\iota(W_0^{(2)})$ and each $\iota(V)$ with $V \in \mathcal{D}_1$, with both sequences considered modulo $n$ (since (ii) fails, the hypothesis of Lemma 3.4.3 holds with $\{0, a\}$ equal to $\{n, 1\}$ modulo $n$), we conclude, in view of $\sigma(\iota(W_0^{(2)})) \equiv 1 \mod n$ (and hence $|\mathrm{supp}(\iota(W_0^{(2)}))| > 1$), that there exist $x_0|W_0^{(2)}$ and $g \in I$ such that $\iota(x_0) \equiv g + 1 \mod n$ and $\iota(x) = g$ for all $x|x_0^{-1}W_0^{(2)} \prod_{V\in\mathcal{D}_1} V$. If (a) holds, then performing type III swaps between $W_0$ and the $V \in \mathcal{D}_1$ completes the proof. Therefore assume (a) fails and (b) holds instead.

CASE 1: $W_0 \in \mathcal{C}_0$.

Thus, since $|\mathcal{D}_1|, |\mathcal{D}_2| \geq 1$, let $U \in \mathcal{A}_2^* \cap (\mathcal{D}_1 \cup \mathcal{D}_2)$ with $\sigma(U) = f_1$ and let $V \in \mathcal{A}_2^* \cap (\mathcal{D}_1 \cup \mathcal{D}_2)$ with $\sigma(V) = Cf_1 + f_2$ for some $C \in \mathbb{Z}$. Performing a type II swap between some fixed $u|U$ and each $x|x_0^{-1}W_0^{(2)}$ (using the same fixed subsequence $R|W_0^{(1)}$ in every swap, which is possible since $\iota(x) = g$ for all $x|x_0^{-1}W_0^{(2)}$), we conclude from either Lemma 3.1.2 (since $\sigma(W_0) = f_1 + f_2$) or Lemma 3.2.4 that $\psi_1$ is constant on $x_0^{-1}W_0^{(2)}$. Likewise performing a type II swap between some fixed $v|V$ and each $x|x_0^{-1}W_0^{(2)}$, we conclude from either Lemma 3.1.3 or Lemma 3.2.5 that $\psi_2$ is constant on $x_0^{-1}W_0^{(2)}$. Consequently, $\psi(x) = \alpha$ (say) for all $x|x_0^{-1}W_0^{(2)}$.

Suppose $W \in \Omega_0^{nu}$. Then $\mathcal{D}_1 \subset \mathcal{A}_2^* \cap \mathcal{C}_i$, for some $i \in \{1, 2\}$ (in view of the hypotheses of CASE 1 and the lemma), and performing type III swaps between the $Z \in \mathcal{D}_1$, we conclude, in view of $|\mathcal{D}_1| \geq 2$ and Lemma 3.3.1 or 3.3.2, that $\psi(x) = \alpha'$ (say) for all $x| \prod_{V\in\mathcal{D}_1} V$. Further applying type III swaps between $W_0$ and any $Z \in \mathcal{D}_1$, we conclude from Lemma 3.4.3 and either Lemma 3.3.4 or 3.3.5 that $\alpha = \alpha'$, completing the proof. So we may assume $W \in \Omega_0^u$.

If $\mathcal{D}_1 \subset \mathcal{C}_1$, then repeating the argument of the previous paragraph using Lemma 3.1 in place of Lemma 3.3 completes the proof. Therefore we may assume $\mathcal{D}_1 \subset \mathcal{C}_0$. Let $Z \in \mathcal{D}_1$ and $z|Z$. We proceed to show $\psi(z) = \alpha$, which, since $z|Z \in \mathcal{D}_1$ is arbitrary, will complete the proof.

If performing a type III swap between $z|Z$ and some $x|x_0^{-1}W_0^{(2)}$ results in a new product decomposition $W' \in \Omega_0^u$, then $W_0' \in \mathcal{C}_0$ (as both $W_0$, $Z \in \mathcal{C}_0$) and, repeating the arguments of the first paragraph of CASE 1 this time for $W'$, we conclude that $\psi(z) = \alpha$. If $W' \in \Omega_0^{nu}$, then we can choose a new $f_2$ such that $\widetilde{\sigma}(W') = f_1^{m-1} f_2^{m-1} (f_1 + f_2)$. If also $W_0' \in \mathcal{C}_0$, then $\sigma(W_0') = f_1 + f_2$, and repeating the arguments of the first paragraph for $W'$ shows $\psi(z) = \alpha$. Therefore suppose $W' \in \Omega_0^{nu}$ and $\sigma(W_0') = f_2$. In view of Lemma 3.1.3, we have $\alpha - \psi(z) \in \langle f_1 \rangle$. However, if $\alpha \neq \psi(z)$, then performing a type II swap between some $y|U' = U$ and both $z|W_0'$ and $z'|W_0'$, where $\iota(z') = g$ and $\psi(z') = \alpha$, we conclude from Lemma 3.2.3 that

$$\epsilon n e_1 + \sigma(\psi(R)) - \psi(y) + \{\psi(z), \alpha\} = \{0, f_2 - f_1\},$$

where $\epsilon = \epsilon(z, y) = \epsilon(z', y)$ (in view of $\iota(z) = \iota(z') = g$) and $R$ is the same fixed subsequence of $W_0'^{(1)}$ used in both swaps (also possible since $\iota(z) = \iota(z') = g$). Hence $\psi(z) - \alpha = \pm(f_2 - f_1)$, contradicting that $\alpha - \psi(z) \in \langle f_1 \rangle$, and completing CASE 1.

CASE 2: $W_0 \notin C_0$ and $W \in \Omega_0^{nu}$.

Then $W_0 \in \mathcal{C}_1$ (by our normalizing assumptions). If there is $Z \in \mathcal{D}_1 \cap \mathcal{C}_0$ and $\mathcal{D}_1 \cap \mathcal{C}_2 = \emptyset$, then, in view of Lemma 3.3.4, we may assume that performing any type III swap between $z|Z$ and $x|x_0^{-1}W_0^{(2)}$ results in a product decomposition $W'$ with $\sigma(W_0') = \sigma(W_0)$, else CASE 1 applied to $W'$ completes the proof. Note that Lemma 3.3.1 guarantees the same for any $Z \in \mathcal{D}_1 \cap \mathcal{C}_1$. Thus if $\mathcal{D}_1 \cap \mathcal{C}_2 \neq \emptyset$, then (a) holds, contrary to assumption, and so we may assume instead that $\mathcal{D}_1 \cap C_2 \neq \emptyset$.

Suppose there is $Z \in \mathcal{D}_2$ with $\sigma(Z) = f_1 + f_2$. Then performing type II swaps between some $z|Z$ and each $x|x_0^{-1}W_0^{(2)}$ (using the same $R|W_0^{(1)}$ for every swap, which is possible since $\iota(x) = g$ for all $x|x_0^{-1}W_0^{(2)}$), we conclude from Lemma 3.2.4 that $\psi_1$ is constant on $x_0^{-1}W_0^{(2)}$. If we perform type III swaps between $U$ and $W_0$ with $U \in \mathcal{D}_1 \cap \mathcal{C}_2$, then we conclude from Lemmas 3.2.3 and 3.4.3 that there is $u_0|x_0^{-1}W_0^{(2)}U$ such that $\psi(x) = \alpha$ (say) for all $x|u_0^{-1}x_0^{-1}W_0^{(2)}U$ and $\psi(u_0) = \alpha$ or $\alpha \pm (f_2 - f_1)$. Thus, as $\psi_1$ is constant on $x_0^{-1}W_0^{(2)}$, we conclude that $\psi(x) = \alpha$ for all $x|x_0^{-1}W_0^{(2)}$. If $u_0|U$ with $\psi(u_0) = \alpha + f_2 - f_1$, then swapping $u_0|U$ for $x|x_0^{-1}W_0^{(2)}$ results in a new product decomposition $W'$ such that $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$, $\sigma(W_0') = f_2$, and $\psi_2$ is not constant on $x_0^{-1}W_0'^{(2)}$. However repeating the argument from the beginning of the paragraph for $W'$, using Lemma 3.2.5 in place of Lemma 3.2.4, we see that $\psi_2$ must be constant on $x_0^{-1}W_0'^{(2)}$, a contradiction. Thus we see that any type III swap between $u|U \in \mathcal{D}_1 \cap \mathcal{C}_2$ and $x|x_0^{-1}W_0^{(2)}$ results in a product decomposition $W'$ with $\sigma(W_0') = \sigma(W_0)$. As a result, since $Z \in \mathcal{D}_2$ with $\sigma(Z) = f_1 + f_2$, it follows from Lemma 3.3.1 that (a) holds, contrary to assumption. So we may assume $\mathcal{D}_2 \cap \mathcal{C}_0$ is empty. Thus, in view of $\mathcal{D}_1 \cap \mathcal{C}_2 \neq \emptyset$ and the hypotheses, it follows that there is $U \in \mathcal{D}_2 \cap \mathcal{C}_1$.

Performing type II swaps between some $y|U$ and each $x|x_0^{-1}W_0^{(2)}$ (using the same $R|W_0^{(1)}$ for every swap), we conclude from Lemma 3.2.1 that $\psi_1$ is constant on $x_0^{-1}W_0^{(2)}$. Consequently, performing type III swaps between $W_0$ and each $V_i \in \mathcal{D}_1 \cap \mathcal{C}_2$, we conclude from Lemmas 3.2.3 and 3.4.3 that there exists $v_i|V_i$ such that $\psi(x) = \alpha$ (say) for all $x|v_i^{-1}x_0^{-1}W_0^{(2)}V_i$; moreover, $\psi(v_i) = \alpha$ or $\alpha + f_2 - f_1$. If there is $Z \in \mathcal{D}_1 \cap \mathcal{C}_0$, then, performing type III swaps between the $x|x_0^{-1}W_0^{(2)}$ and $z|Z$, and between the $x|V_i \in \mathcal{D}_1 \cap \mathcal{C}_2$ and $z|Z$, we conclude from Lemmas 3.3.4 and 3.3.5 that $\psi(x) = \alpha$ for all $x|Z$.

If $Z \in \mathcal{D}_1 \cap \mathcal{C}_0$ does not exist, then $|\mathcal{D}_1| \geq 2$ and $|\mathcal{D}_2 \cap \mathcal{C}_1| \geq 1$ ensure $|\mathcal{D}_1 \cap \mathcal{C}_2| \geq 2$, and, performing type III swaps between the $V \in \mathcal{D}_1 \cap \mathcal{C}_2$, we conclude from Lemma 3.3.2 that $\psi(x) = \alpha$ for all $x|V$ with $V \in \mathcal{D}_1 \cap \mathcal{C}_2$, completing the proof. On the other hand, if there is $Z \in \mathcal{D}_1 \cap \mathcal{C}_0$, then applying type III swaps between $Z$ and each $V_i \in \mathcal{D}_1 \cap \mathcal{C}_2$, we conclude from Lemma 3.2.5 that $\psi_2$ is constant on $V_i$ and $Z$; consequently, since $\psi(v_i) = \alpha$ or $\alpha + f_2 - f_1$, and since $\psi(v) = \alpha$ for all $v|v_i^{-1}V_i$, we conclude that $\psi(v_i) = \alpha$ as well, completing the proof.

CASE 3: $W_0 \notin C_0$ and $W \in \Omega_0^u$.

Then $W_0 \in \mathcal{C}_1$ and $\mathcal{D}_1 \subset \mathcal{C}_0$ (else (a) holds in view of Lemma 3.1.1). Since $|\mathcal{D}_2| \geq 1$, there is $U \in \mathcal{A}_2^* \cap \mathcal{C}_1$. Performing type II swaps between each $x|x_0^{-1}W_0$ and some fixed $u|U$ (using the same fixed sequence $R|W_0^{(1)}$ in each swap), it follows from Lemma 3.1.1 that $\psi(x) = \alpha$ (say) for all $x|x_0^{-1}W_0^{(2)}$. Let $V_i \in \mathcal{D}_1$. Performing type III swaps between $W_0$ and $V_i$, we conclude from Lemmas 3.1.2 and 3.4.3 that $\psi(z) = \alpha$ for all $z|v_i^{-1}V_i$, for some $v_i|V_i$; moreover, either $\psi(v_i) = \alpha$ or $\psi(v_i) = \alpha - \sigma(W_0) + \sigma(V_i)$. However, in the latter case, since $V_i \in \mathcal{C}_0$ and $W_0 \in \mathcal{C}_1$ (so that $\sigma(W_0) = f_1$ and $\sigma(V_i) = Cf_1 + f_2$, for some $C \in \mathbb{Z}$), we see that $\psi_2(v_i) \neq \psi_2(\alpha)$. Since $|\mathcal{D}_1| \geq 2$, performing type III swaps between the $V_i \in \mathcal{D}_1$, we conclude from Lemma 3.1.3 that $\psi_2$ is constant on each $V_i$, whence $\psi_2(v_i) \neq \psi_2(\alpha)$ is impossible. Thus $\psi(z) = \alpha$ for all $z|V_i$ with $V_i \in \mathcal{D}_1$, completing the proof. □

Lemma 5.3 allows us to conclude detailed information concerning the values of $\psi$ on $W_0^{(1)}$. Depending on $\sigma(W_j)$ and $\sigma(W_0)$, the appropriate part of Lemma 3.1, 3.2 or 3.3 will ensure that one of the hypotheses in 1, 2, or 3 holds.

**Lemma 5.3.** *Let $W \in \Omega_0$ and $W_j \in \mathcal{A}_2^*$ be such that there are $Y|W_j$ and $X|W_0^{(2)}$ with $|X| = |Y|$ and $\epsilon'(X,Y) \notin \{1,n\}$, and set*

$$\mathcal{D} = \{W' \in \Omega' \mid W' \text{ is the result of performing a type II swap between } X|W_0 \text{ and } Y|W_j\}.$$

1. *If $\sigma(W_j') - \sigma(W_j) = 0$, for all $W' \in \mathcal{D}$, then $|\mathrm{supp}(\psi(W_0^{(1)}))| = 1$.*
2. *If $\sigma(W_j') - \sigma(W_j) \in \langle f_i \rangle$, where $i \in \{1,2\}$, for all $W' \in \mathcal{D}$, then $|\mathrm{supp}(\psi_{3-i}(W_0^{(1)}))| = 1$.*
3. *If $\sigma(W_j') - \sigma(W_j) \in \{0, F\}$, for all $W' \in \mathcal{D}$, where $F \in \mathrm{Ker}(\varphi)$, then $\mathrm{supp}(\psi(W_0^{(1)})) = \{\gamma, \beta\}$ for some $\gamma,\, \beta \in \mathrm{Ker}(\varphi)$ with $\gamma - \beta \in \{0, \pm F\}$.*

*Proof.* 1. By hypothesis, there is only one possibility for $\sigma(\psi(R))$, where $R|W_0^{(1)}$ is any subsequence with $|R| = n - \epsilon'(X,Y)$. Furthermore, we have $1 \le |R| \le n-2 < |\psi(W_0^{(1)})|$, and thus 1 follows from Lemma 3.5.3 applied to $\psi(W_0^{(1)})$.

2. The argument is analogous to that of item 1, using the group $\mathrm{Ker}(\varphi)/\langle f_i \rangle \cong \langle f_{3-i} \rangle$ in place of $\mathrm{Ker}(\varphi)$.

3. By the arguments for item 1, replacing Lemma 3.5.3 by Lemma 3.5.1, we conclude that $\psi(W_0^{(1)}) = \gamma^l \beta^{n-1-l}$ (say), where $l \ge n-1-l \ge 1$ and $\gamma \ne \beta$ (else the lemma is complete); moreover,

$$\epsilon(X,Y)ne_1 + \sigma(\psi(X)) - \sigma(\psi(Y)) + \min\{t,\, l\} \cdot \gamma + (t - \min\{t,\, l\}) \cdot \beta + \{0, \beta - \gamma\} = \{0,\, F\},$$

where $t = n - \epsilon'(X,Y)$. Thus $\beta - \gamma = \pm F$, as desired. □

The following lemma encapsulates an alignment argument for the $\iota$ values that forces them to live in near disjoint intervals. It will be a key part of the more difficult portions of CLAIM C.

**Lemma 5.4.** *Let $W \in \Omega_0$, let $\mathcal{D} \subset \mathcal{A}_2^*$ be nonempty, and let $Z|W_0^{(2)}$ be nontrivial. For $x|S$, let $\psi_0(x) = \psi(x)$, and for $x \in \mathrm{Ker}(\varphi)$, let $\psi_0$ be the identity map. Let $i \in \{0,1,2\}$. If $\psi_i(ne_1) \ne 0$ and*

$$\psi_i(x) - \psi_i(y) + \psi_i(\epsilon(x,y)ne_1) = 0 \tag{7}$$

*for every $x|Z$ and $y|U \in \mathcal{D}$, then there exist intervals $J_1$, $J_2$ and $J_3$ of $\mathbb{Z}$ with either*

$$\mathrm{supp}(\iota(\prod_{U\in\mathcal{D}} U)) \subset J_3,\ \mathrm{supp}(\iota(Z)) \subset J_1 \cup J_2, \quad \textit{and} \quad \max J_1 \le \min J_3 \le \max J_3 < \min J_2, \quad \textit{or} \tag{8}$$

$$\mathrm{supp}(\iota(Z)) \subset J_3,\ \mathrm{supp}(\iota(\prod_{U\in\mathcal{D}} U)) \subset J_1 \cup J_2, \quad \textit{and} \quad \max J_1 < \min J_3 \le \max J_3 \le \min J_2. \tag{9}$$

*Moreover, $I$ can be chosen such that:*

1. *$\min I$ is congruent to an element in $\iota(Z)$ modulo $n$,*
2. *$\iota(x) \le \iota(y)$ and $\epsilon(x,y) = 0$ for all $x|Z$ and $y|U \in \mathcal{D}$, and*
3. *$\psi_i(x) = \psi_i(y)$ for all $xy|Z\prod_{U\in\mathcal{D}} U$.*

*Proof.* Observe, for $xy|S_2$, that

$$\epsilon(x,y) = \begin{cases} 0, & \iota(x) \le \iota(y); \\ 1, & \iota(x) > \iota(y). \end{cases} \tag{10}$$

Consequently, we conclude from (7) that

$$\psi_i(x) = \psi_i(y), \tag{11}$$

for all $x|Z$ and $y|U \in \mathcal{D}$ with $\iota(x) \le \iota(y)$, and that

$$\psi_i(x) = \psi_i(y) - \psi_i(ne_1), \tag{12}$$

for all $x|Z$ and $y|U \in \mathcal{D}$ with $\iota(x) > \iota(y)$.

If there do not exist $x|Z$ and $yy'|\prod_{U\in\mathcal{D}} U$ with $\iota(x) \le \iota(y)$ and $\iota(x) > \iota(y')$, then, for every $x|Z$, we have either $\iota(x) \le \iota(y)$ for all $y|\prod_{U\in\mathcal{D}} U$, or $\iota(x) > \iota(y)$ for all $y|\prod_{U\in\mathcal{D}} U$. Thus we see that (8) holds (with $J_3 = [\min(\text{supp}(\iota(\prod_{U\in\mathcal{D}} U))), \max(\text{supp}(\iota(\prod_{U\in\mathcal{D}} U)))]$, $J_1$ being any nonempty interval containing those $\iota(x)$ with $\iota(x) \le \iota(y)$ for all $y|\prod_{U\in\mathcal{D}} U$ and $\max J_1 \le \min J_3$, and $J_2$ being any nonempty interval containing those $\iota(x)$ with $\iota(x) > \iota(y)$ for all $y|\prod_{U\in\mathcal{D}} U$ and $\min J_2 > \max J_3$).

Now instead let $x|Z$ and $yy'|\prod_{U\in\mathcal{D}} U$ with $\iota(x) \le \iota(y)$ and $\iota(x) > \iota(y')$, and factor $\prod_{U\in\mathcal{D}} U = J_1'J_2'$, where $J_1'$ are those terms $a|\prod_{U\in\mathcal{D}} U$ with $\iota(a) < \iota(x)$, and $J_2'$ are those terms $b|\prod_{U\in\mathcal{D}} U$ with $\iota(b) \ge \iota(x)$. By assumption, both $J_i'$ are nontrivial. Moreover, from (11) and (12) and $\psi_i(ne_1) \ne 0$, we see that

$$\psi_i(b) = \psi_i(x) \tag{13}$$

and

$$\psi_i(a) = \psi_i(x) + \psi_i(ne_1) \ne \psi_i(x), \tag{14}$$

for all $a|J_1'$ and $b|J_2'$. Thus $\psi_i$ is constant on $J_1'$ and also on $J_2'$ but the two values assumed are distinct. If there were $x'|Z$ such that $\iota(x') \le \max(\text{supp}(\iota(J_1')))$, then by (11) and (13) we would conclude that $\psi_i(x') = \psi_i(b) = \psi_i(x)$, where $b$ is any term of $J_2'$, while by applying (11) and (14) between $x'$ and $\max(\text{supp}(\iota(J_1'))) := a_0$, we would conclude that $\psi_i(x') = \psi_i(a_0) = \psi_i(x) + \psi_i(ne_1) \ne \psi_i(x)$, a contradiction to what we have just seen. We likewise obtain a contradiction if there were $x'|Z$ such that $\iota(x') > \min(\text{supp}(\iota(J_2')))$. Therefore we see that (9) holds with $J_1 = [\min(\text{supp}(\iota(J_1'))), \max(\text{supp}(\iota(J_1')))]$, $J_2 = [\min(\text{supp}(\iota(J_2'))), \max(\text{supp}(\iota(J_2')))]$, and $J_3 = [\min(\text{supp}(\iota(Z))), \max(\text{supp}(\iota(Z)))]$.

Choosing $I$ such that $\min I$ is congruent to $\min(\text{supp}(\iota(Z)))$ modulo $n$, if either (9) holds or else (8) holds with $\text{supp}(\iota(Z)) \cap J_2 = \emptyset$, and congruent to $\min(\text{supp}(\iota(Z)) \cap J_2)$ otherwise, the remaining properties follow in view of (7) and (10). □

Now we choose a product decomposition $W \in \Omega_0$, and if $\Omega_0^u \ne \emptyset$, we assume that $W \in \Omega_0^u$.

**CLAIM A:** $\mathsf{h}(S_1) \ge |S_1| - 1$.

*Proof.* We need to show that there exists $x_0|S_1$ such that $\psi(x) = \psi(y)$ for all $xy|x_0^{-1}S_1$. We divide the proof into four main cases. In many of the cases, we obtain partial works towards showing $\mathsf{h}(S_1) = |S_1|$, which will later be utilized in CLAIM B.

CASE 1: $\Omega_0^u \ne \emptyset$, $|\mathcal{A}_1| \ge 2$ and $|\mathcal{C}_1 \cap \mathcal{A}_1| \ge 1$.

In this case, we will moreover show that $\mathsf{h}(S_1) = |S_1|$ unless $|\mathcal{A}_1 \cap \mathcal{C}_0| = 1$ or $|\mathcal{A}_1 \cap \mathcal{C}_1| = 1$, and that $|\text{supp}(\psi(U))| > 1$ for $U \in \mathcal{A}_1 \cap \mathcal{C}_i$, where $i \in \{1, 2\}$, is only possible when $|\mathcal{A}_1 \cap \mathcal{C}_i| = 1$.

If $U, V \in \mathcal{A}_1$ are distinct, then we can perform a type I swap between $U$ and $V$, and by (4) and Lemma 3.1, we conclude that

$$\begin{aligned} &\sigma(\psi(X)) - \sigma(\psi(Y)) = 0, && \text{if } U, V \in \mathcal{C}_1 \\ &\sigma(\psi(X)) - \sigma(\psi(Y)) \in \{0, (1-C)f_1 - f_2\}, && \text{if } U \in \mathcal{C}_1,\ V \in \mathcal{C}_0 \text{ and } \sigma(V) = Cf_1 + f_2 \\ &\sigma(\psi(X)) - \sigma(\psi(Y)) \in \langle f_1 \rangle, && \text{if } U, V \in \mathcal{C}_0, \end{aligned} \tag{15}$$

for $X|U$ and $Y|V$ with $|X| = |Y|$.

If $|\mathcal{A}_1 \cap \mathcal{C}_0| \geq 2$, then using (15) (running over all $X$ and $Y$ with $|X| = |Y| = 1$), we conclude that $\psi(x) - \psi(y) \in \langle f_1 \rangle$ for all $x$ and $y$ dividing a block from $\mathcal{A}_1 \cap \mathcal{C}_0$.

If $|\mathcal{A}_1 \cap \mathcal{C}_1| \geq 2$, then using (15) (running over all $X$ and $Y$ with $|X| = |Y| = 1$) and Lemma 3.4.1, we conclude that $\psi(x) = \psi(y)$ for all $x$ and $y$ dividing a block from $\mathcal{A}_1 \cap \mathcal{C}_1$.

If $U \in \mathcal{A}_1 \cap \mathcal{C}_1$ and $V \in \mathcal{A}_1 \cap \mathcal{C}_0$ with $U$ and $V$ distinct, then, using (15) (running over all $X$ and $Y$ with $|X| = |Y| \leq 2 \leq n-1$) and Lemma 3.4.3, we conclude that $\psi(x) = \alpha$ (say) for all $x|x_0^{-1}UV$, for some $x_0|UV$; moreover, $\psi(x_0) = \alpha$ or $\alpha \pm ((1-C)f_1 - f_2)$.

Suppose $x_0|U$ and $\psi(x_0) \neq \alpha$. Then in view of the fourth paragraph of CASE 1, we see that $|\mathcal{A}_1 \cap \mathcal{C}_1| = 1$. Thus performing type I swaps between $U$ and all possible $V \in \mathcal{A}_1 \cap \mathcal{C}_0$ completes CLAIM A, for $n \geq 5$ or $U \neq W_0$, and, when $n = 3$ and $U = W_0$, we instead conclude that either $\psi(V) = \alpha^n$ or $\psi(V) = \beta^n$, where $\psi(W_0^{(1)}) = \alpha\beta$, for all $V \in \mathcal{A}_1 \cap \mathcal{C}_0$. However, if there are $V,\, V' \in \mathcal{A}_1 \cap \mathcal{C}_0$ with $\psi(V) = \alpha^n$ and $\psi(V') = \beta^n$ and $\alpha \neq \beta$, then (15) implies that $\beta - \alpha = (1-C)f_1 - f_2$ and $\alpha - \beta = (1-C')f_1 - f_2$, where $\sigma(V) = Cf_1 + f_2$ and $\sigma(V') = C'f_1 + f_2$, from which we conclude that $(2 - C' - C)f_1 - 2f_2 = 0$, contradicting that $m \geq 3$. So we may instead assume $x_0|V$.

In this case, in combination with the results of the previous paragraphs, we find that there is at most one $v_i|V_i$, for each $V_i \in \mathcal{A}_1 \cap C_0$, such that $\psi(x) = \alpha$ for all $x|S_1$ not equal to any $v_i$. In this scenario, CLAIM A is done unless we have two distinct $V_1,\, V_2 \in \mathcal{A}_1 \cap \mathcal{C}_0$ such that $\psi(v_1) \neq \alpha$ and $\psi(x) = \alpha$ for all $x|v_1^{-1}v_2^{-1}UV_1V_2$. However, applying a type I swap between $y|U$ and $v_1|V_1$, we conclude from (15) that $\alpha - \psi(v_1) = (1-C)f_1 - f_2 \notin \langle f_1 \rangle$, for some $C \in \mathbb{Z}$, which, in view of $\alpha\psi(v_1)|\psi(V_1)$, contradicts the conclusion of the third paragraph of CASE 1. This completes CASE 1.

CASE 2: $|\mathcal{A}_1| = 1$.

In this case, we will show that $\mathsf{h}(S_1) = |S_1|$.

Suppose $W_0 \in \mathcal{C}_0$. Then we may choose $f_2$ such that $\sigma(W_0) = f_1 + f_2$, and if $\Omega_0^u = \emptyset$, such that $\widetilde{\sigma}(W) = f_1^{m-1}f_2^{m-1}(f_1 + f_2)$ also. Let $\mathcal{D}_1$ be those blocks $W_i$ with $\sigma(W_i) = f_1$ and let $\mathcal{D}_2$ be all other blocks from $\mathcal{A}_2^*$. Applying Lemma 5.2, we see that Lemma 5.2(ii) must hold, else $ge_1 + e_2 + \alpha$ will have multiplicity at least $mn - 1$ in $S$, as desired. Performing a type II swap between the $X|W_0$ and $Y|W_j$ given by Lemma 5.2(ii), we conclude, from Lemmas 5.3.2 and either 3.1.2 (since $\sigma(W_0) = f_1 + f_2$) or 3.2.4, that $\psi_1$ is constant on $W_0^{(1)}$. However, reversing the roles of $\mathcal{D}_1$ and $\mathcal{D}_2$ and repeating the above argument using Lemmas 3.1.3 and 3.2.5 in place of Lemmas 3.1.2 and 3.2.4, we conclude that $\psi_2$ is also constant on $W_0^{(1)}$, whence $\psi$ is constant on $W_0^{(1)}$, completing the proof of CLAIM A. So we may assume $W_0 \notin \mathcal{C}_0$.

Suppose $\Omega_0^u = \emptyset$. Then we may w.l.o.g. assume $\widetilde{\sigma}(W) = f_1^{m-1}f_2^{m-1}(f_1 + f_2)$, that $\mathcal{C}_1$ consists of those blocks $W_i$ with $\sigma(W_i) = f_1$, and that $\sigma(W_0) = f_1$. Let $\mathcal{D}_1 = \mathcal{C}_2$ and $\mathcal{D}_2 = \mathcal{C}_1^* \cup \mathcal{C}_0$. Applying Lemma 5.2, we see that Lemma 5.2(ii) must hold, else there will be a term with multiplicity at least $mn - 1$ in $S$, as desired. Thus Lemmas 5.3.3 and 3.2.3 imply that $\mathrm{supp}(\psi(W_0^{(1)})) = \{\gamma,\, \beta\}$ (say) with $\beta - \gamma = \pm(f_2 - f_1)$ (else CLAIM A follows).

Reversing the roles of $\mathcal{D}_1$ and $\mathcal{D}_2$ and again applying Lemma 5.2, we once more see that Lemma 5.2(ii) must hold, else there is a term with multiplicity $mn - 1$ in $S$, as desired. Thus Lemma 5.3.2 and either Lemma 3.2.1 or 3.2.4 imply that $\psi_1$ is constant on $W_0^{(1)}$, contradicting that $\beta - \gamma = \pm(f_2 - f_1)$. So we may assume $\Omega_0^u \neq \emptyset$.

Let w.l.o.g. $W_1, \ldots, W_{m-2}$ be the blocks of $\mathcal{C}_1^* \cap \mathcal{A}_2$, and let $\mathcal{D}_1 = \mathcal{C}_1^*$ and $\mathcal{D}_2 = \mathcal{C}_0$. Apply Lemma 5.2. If Lemma 5.2(ii) holds, then Lemmas 5.3.1 and 3.1.1 imply that $\psi$ is constant on $W_0^{(1)}$, whence CLAIM A follows. Therefore we may instead assume $\iota(x) = g$ and $\psi(x) = \alpha$ (say) for all terms $x | x_0^{-1} W_0^{(2)} W_1 \ldots W_{m-2}$, for some $x_0 | W_0^{(2)}$ with $\iota(x_0) \equiv g + 1 \mod n$.

Consider $W_j$ with $j \geq m-1$. If $\iota(W_j) \neq g^n$, then there exist $x | W_0^{(2)}$ and $y | W_j$ with $\epsilon'(x, y) \notin \{1, n\}$, whence Lemmas 5.3.3 and 3.1.2 imply that $\mathrm{supp}(\psi(W_0^{(1)})) = \{\gamma, \beta\}$ (say) with $\beta - \gamma = \pm F_j$ (else CLAIM A follows), where $F_j = (1 - C_j) f_1 - f_2$ and $\sigma(W_j) = C_j f_1 + f_2$.

If $W_k$ is another block with $k \geq m-1$ and $\iota(W_k) \neq g^n$, then the above paragraph implies that $\beta - \gamma = \pm F_k$, where $F_k = (1 - C_k) f_1 - f_2$ and $\sigma(W_k) = C_k f_1 + f_2$. Thus, since $m \geq 3$ and $\beta - \gamma = \pm F_j$, we conclude that $F_j = F_k$ and $C_j \equiv C_k \mod m$. As a result, we see that any two blocks $W_j$ and $W_k$, with $j, k \geq m-1$ and $\iota(W_k), \iota(W_j) \neq g^n$, must have $\sigma(W_j) = \sigma(W_k)$. Hence, since $W \in \Omega_0^u$, we conclude that there are at least two distinct blocks $W_s$ and $W_r$ with $s, r \geq m-1$ and $\iota(W_s) = \iota(W_r) = g^n$. Performing type III swaps between $W_0$ and both $W_s$ and $W_r$, we conclude from Lemmas 3.1.2 and 3.4.3 that $\psi(x) = \alpha$ for all but at most two terms of $W_s W_r$, whence $g e_1 + e_2 + \alpha$ has multiplicity at least $(m-1)n - 1 + 2n - 2 \geq mn$ in $S$, contradicting that $S \in \mathcal{A}(G)$ and completing CASE 2.

CASE 3: $\Omega_0^u \neq \emptyset$, $|\mathcal{A}_1| \geq 2$ and $|\mathcal{C}_1 \cap \mathcal{A}_1| = 0$.

In this case, we will moreover show that $\mathsf{h}(S_1) = |S_1|$.

We may w.l.o.g. assume $W_1, \ldots, W_{m-1}$ are the blocks in $\mathcal{C}_1 \cap \mathcal{A}_2$. Let $\mathcal{D}_1 = \mathcal{C}_1$ and $\mathcal{D}_2 = \mathcal{C}_0^* \cap \mathcal{A}_2$. If $|\mathcal{D}_2| \geq 1$, then we can apply Lemma 5.2. Otherwise, in view of Lemma 3.1.2, we may assume hypothesis (a) holds in Lemma 5.2, else applying CASE 1 to the resulting product decomposition $W'$ would imply, in view of $|\mathcal{D}_2| = 0$, that $\psi(x) = \alpha$ (say) for all $x | W_i' = W_i$ with $i \in [m, 2m-2]$, in which case $\sigma(W_i') = n e_1 + n\alpha$ has multiplicity $m-1$ in $\widetilde{\sigma}(W')$, contradicting that $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$ (in view of Lemma 3.1.2) with $W \in \Omega_0^u$. Thus, in either case Lemma 5.2 is available. If Lemma 5.2(i) holds, then $g e_1 + e_2 + \alpha$ is a term with multiplicity at least $mn - 1$ in $S$, as desired. Therefore there is $X | W_0^{(2)}$ and $Y | W_j$, for some $j \in [1, m-1]$, such that $|X| = |Y|$ and $\epsilon'(X, Y) \notin \{1, n\}$. Hence Lemmas 5.3.3 and 3.1.2 imply that $\mathrm{supp}(\psi(W_0^{(1)})) = \{\gamma, \beta\}$ (say) with $\gamma - \beta \in \{0, \pm F\}$, where $F = (C-1) f_1 + f_2$ and $\sigma(W_0) = C f_1 + f_2$. Since $|\mathcal{A}_1| \geq 2$, let $V \in \mathcal{C}_0^* \cap \mathcal{A}_1$. Performing type I swaps between $W_0$ and $V$, we conclude from Lemma 3.1.3 that $\psi_2$ is constant on $V W_0^{(1)}$, whence $\gamma - \beta \in \{0, \pm F\}$ implies $\gamma = \beta$.

Performing type I swaps among the $V \in \mathcal{C}_0 \cap \mathcal{A}_1$, we conclude from Lemma 3.1.3 that $\psi_2(x) = \psi_2(\gamma)$ for all $x | V \in \mathcal{C}_0 \cap \mathcal{A}_1$. Let $W'$ be the product decomposition resulting from performing a type II swap between $X | W_0$ and $Y | W_j$ (with $X$ and $Y$ as given by Lemma 5.2(ii) in the previous paragraph). Since $\epsilon'(X, Y) \notin \{1, n\}$, we conclude that there is a block $W_k' \in \mathcal{C}_1$, with $k \in \{0, j\}$, having $(e_1 + \gamma) | W_k'$. Since $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$ (in view of Lemma 3.1.2), performing type I swaps between $W_k'$ and each distinct block $V' = V \in \mathcal{C}_0^* \cap \mathcal{A}_1$, we conclude from Lemma 3.1.2 that either $\psi(x) = \gamma$ or $\psi(x) = \gamma + \sigma(V') - \sigma(W_k')$, for each $x | V'$. However, since $W_k' \in \mathcal{C}_1$ and $V' \in \mathcal{C}_0$, it follows that the latter contradicts that $\psi_2$ is constant on $V | W_0^{(1)}$ with value $\psi_2(\gamma)$. Therefore we conclude that $\psi(x) = \gamma$ for all $x | V'$, with $V' = V^* \in \mathcal{C}_0 \cap \mathcal{A}_1$, whence $\psi(x) = \gamma$ for all $x | S_1$, as desired, completing CASE 3.

CASE 4: $\Omega_0^u = \emptyset$ and $|\mathcal{A}_1| \geq 2$.

We may w.l.o.g. assume $\widetilde{\sigma}(W) = f_1^{m-1} f_2^{m-1} (f_1 + f_2)$, by an appropriate choice of $f_2$, whence CLAIM A follows easily by performing type I swaps between the blocks of $\mathcal{A}_1$ and using Lemmas 3.3 and 3.4. This completes CASE 4. □

In view of CLAIM A, we may assume $S_1 = e_1^{|S_1|-1}(e_1 + a)$, for some $a \in \text{Ker}(\varphi)$. Let $y_0 = e_1 + a$.

**CLAIM B:** $\mathsf{h}(S_1) = |S_1|$.

*Proof.* We assume by contradiction $a \neq 0$. In view of the partial conclusions of CLAIM A, we may assume $|\mathcal{A}_1| \geq 2$ (in view of CASE 2 of CLAIM A), and, if $\Omega_0^u \neq \emptyset$, that $|\mathcal{A}_1 \cap \mathcal{C}_1| \geq 1$ (in view of CASE 3 of CLAIM A). We proceed in four cases.

CASE 1: $\Omega_0^u \neq \emptyset$ and $y_0 | U$ for some $U \in \mathcal{A}_1 \cap \mathcal{C}_1$.

In view of CASE 1 of CLAIM A, we have $|\mathcal{A}_1 \cap \mathcal{C}_1| = 1$. Hence, if $U \neq W_0$, then $W_0 \in \mathcal{C}_0$, and performing a type I swap between $y_0|U$ and some $y|W_0$ results (in view of Lemma 3.1.2) in a new product decomposition $W'$ with $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$, $U' \in \mathcal{C}_0$, $W_0' \in \mathcal{C}_1$, $y_0|W_0'$ and $W'$ also satisfying the hypothesis of CASE 1. On the other hand, if $U = W_0$, then $|\mathcal{A}_1| \geq 2$ and $|\mathcal{A}_1 \cap \mathcal{C}_1| = 1$ imply that there is $V \in \mathcal{A}_1^* \cap \mathcal{C}_0$, and performing a type I swap between $y_0|W_0$ and some $y|V$ results (in view of Lemma 3.1.2) in a new product decomposition $W'$ with $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$, $W_0' \in \mathcal{C}_0$, $V' \in \mathcal{C}_1$, $y_0|V'$ and $W'$ also satisfying the hypothesis of CASE 1. Thus w.l.o.g. we may assume $U \neq W_0$. Since $U \in \mathcal{C}_1$ and $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$ with $W_0' \in \mathcal{C}_1$ (with $W'$ as in the second sentence of CASE 1), then, letting $\sigma(W_0) = Cf_1 + f_2$, we see that $a = (1-C)f_1 - f_2$.

Let $\mathcal{D}_1 = \mathcal{A}_2^*(W') \cap \mathcal{C}_1(W')$ and $\mathcal{D}_2 = \mathcal{A}_2^*(W') \cap \mathcal{C}_0(W')$. Since $|\mathcal{A}_1 \cap \mathcal{C}_1| = 1$ and $W_0' \in \mathcal{C}_1$, we have $|\mathcal{D}_1| = m-2$, and by CLAIM A we have $|\mathcal{D}_2| \geq 1$ (else $e_1$ is a term with multiplicity at least $(m+1)n - 2 \geq mn$, contradicting that $S \in \mathcal{A}(G)$). If Lemma 5.2(ii) holds for $W'$, then Lemmas 5.3.1 and 3.1.1 imply that $a = 0$, a contradiction. Therefore Lemma 5.2(i) holds for $W'$. Let $g$ and $\alpha$ be as given by Lemma 5.2(i).

Since $|\mathcal{D}_2| \geq 1$, let $V \in \mathcal{A}_2^*(W) \cap \mathcal{C}_0(W)$. If $\iota(V) = g^n$, then, performing type III swaps between $V$ and some $Z \in \mathcal{A}_2^* \cap \mathcal{C}_1$, and between $V$ and $W_0$, we conclude from Lemmas 3.1.2, 3.1.3 and 3.4.3 that $\psi(x) = \alpha$ for all $x|V$, whence $ge_1 + e_2 + \alpha$ has multiplicity at least $mn - 1$ in $S$, as desired. Therefore, in view of $\iota(W_0^{(2)}) \equiv g^{n-1}(g+1) \mod n$, we see that there exists $x|W_0^{(2)} = W_0'^{(2)}$ and $y|V = V'$ such that $\epsilon'(x,y) \notin \{1, n\}$. Hence, from Lemmas 5.3.3 (applied to $W'$) and 3.1.2, it follows that $a = \pm((1-C')f_1 - f_2)$, where $\sigma(V) = C'f_1 + f_2$. Thus, since $a = (1-C)f_1 - f_2$ and $m \geq 3$, we conclude that $C'f_1 = Cf_1$ and $\sigma(V) = \sigma(W_0)$. As $V \in \mathcal{A}_2^*(W) \cap \mathcal{C}_0(W)$ was arbitrary, we see that $\sigma(V) = Cf_1 + f_2$ for all $V \in \mathcal{A}_2(W) \cap \mathcal{C}_0(W)$. On the other hand, if $Z \in \mathcal{A}_1(W) \cap \mathcal{C}_0(W)$, then, performing type I swaps between $U$ and $Z$, we conclude from Lemma 3.1.2 that $a = (1 - C'')f_1 - f_2$, where $\sigma(Z) = C''f_1 + f_2$. Thus $a = (1-C)f_1 - f_2$ implies that $C''f_1 = Cf_1$, and now $\sigma(Z) = Cf_1 + f_2$ for all $Z \in \mathcal{A}_1(W) \cap \mathcal{C}_0(W)$. Consequently, $\sigma(Z) = Cf_1 + f_2$ for all $Z \in \mathcal{C}_0(W)$, contradicting that $\mathsf{h}(\widetilde{\sigma}(W)) < m$. This completes CASE 1.

CASE 2: $\Omega_0^u \neq \emptyset$ and $y_0|U$ for some $U \in \mathcal{A}_1 \cap \mathcal{C}_0$

Recall that $|\mathcal{A}_1 \cap \mathcal{C}_1| \geq 1$ and $|\mathcal{A}_1| \geq 2$. CASE 1 of CLAIM A and the hypothesis of CASE 2 further imply that $|\mathcal{A}_1 \cap \mathcal{C}_0| = 1$. Thus, if $U \neq W_0$, then $W_0 \in \mathcal{C}_1$, and performing a type I swap between $y_0|U$ and some $y|W_0$ results (in view of Lemma 3.1.2) in a product decomposition $W'$ with $y_0|W_0'$, $W_0' \in \mathcal{C}_0$, $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$ and $W'$ satisfying the hypotheses of CASE 2. Thus w.l.o.g. we may assume $U = W_0$.

Since $|\mathcal{A}_1 \cap \mathcal{C}_1| \geq 1$, let $V \in \mathcal{A}_1^* \cap \mathcal{C}_1$. Performing a type I swap between $y_0|W_0$ and some $y|V$, letting $W'$ be the resulting product decomposition, we conclude from Lemma 3.1.2 that $a = (C-1)f_1 + f_2$, where $\sigma(W_0) = Cf_1 + f_2$. Since $|\mathcal{A}_1 \cap \mathcal{C}_0| = 1$ and $W_0 \in \mathcal{C}_0$, let w.l.o.g. $W_1, \ldots, W_{m-1}$ be the blocks of $\mathcal{A}_2^* \cap \mathcal{C}_0$. If $x|W_0^{(2)}$ and $y|W_j$, with $j \in [1, m-1]$ and $\iota(x) = \iota(y)$, then, performing a type III swap between $x|W_0$ and $y|W_j$ and between $x|W_0'$ and $y|W_j'$, we conclude in view of Lemmas 3.1.3 and 3.1.2 that $\psi(x) = \psi(y)$; thus, letting $\mathcal{D}_1 = \mathcal{A}_2^* \cap \mathcal{C}_0$ and $\mathcal{D}_2 = \mathcal{A}_2^* \cap \mathcal{C}_1$, we see that hypothesis (a) holds in Lemma 5.2. If Lemma 5.2(i) holds, then $ge_1 + e_2 + \alpha$ is a term of $S$ with multiplicity at least $mn - 1$, as desired. Therefore Lemma 5.2(ii) holds, whence Lemmas 5.3.2 and 3.1.3 imply that $a \in \langle f_1 \rangle$, contradicting that $a = (C-1)f_1 + f_2$. This completes CASE 2.

Note that if $\Omega_0^u = \emptyset$, then (in view of $|\mathcal{A}_1| \geq 2$) we may w.l.o.g. assume $y_0|U$ with $U \neq W_0$, by an appropriate type I swap. Moreover, when $\Omega_0^u = \emptyset$, we will w.l.o.g. assume $\widetilde{\sigma}(W) = f_1^{m-1} f_2^{m-1}(f_1 + f_2)$ with $\mathcal{C}_1$ consisting of those blocks $W_i$ with $\sigma(W_i) = f_1$.

CASE 3: $\Omega_0^u = \emptyset$ and $y_0|U$ for some $U \in \mathcal{A}_1^* \cap \mathcal{C}_0$.

We may w.l.o.g. assume $W_0 \in \mathcal{C}_1$. Performing a type I swap between $y_0|U$ and some $y|W_0$, letting $W'$ be the resulting product decomposition, we conclude from Lemma 3.3.4 that $a = f_2$. Let $\mathcal{D}_1 = \mathcal{A}_2^*(W') \cap \mathcal{C}_2(W')$ and let $\mathcal{D}_2 = A_2^*(W') \cap \mathcal{C}_1(W')$. Observe that $|\mathcal{D}_1| = m - 1$, else performing a type I swap between $y_0|U$ and some $V \in \mathcal{A}_1 \cap \mathcal{C}_2$ would imply in view of Lemma 3.3.5 that $a = f_1$, contradicting that $a = f_2$. If a type III swap between $W_0'$ and some $W_j' \in \mathcal{D}_1$ results in a new product decomposition $W''$ with $\sigma(W_0'') \neq \sigma(W_0')$, then Lemma 3.3.5 implies $\sigma(W_0'') = f_2$, whence, performing a type I swap between $y_0|W_0''^{(1)} = W_0'^{(1)}$ and $U'' = U'$, we conclude from Lemma 3.2.3 that $-a = f_1 - f_2$, contradicting that $a = f_2$. Thus hypothesis (a) of Lemma 5.2 holds for $W'$. If Lemma 5.2(i) holds, then $ge_1 + e_2 + \alpha$ has multiplicity at least $mn - 1$ in $S$, as desired. Therefore, Lemma 5.2(ii) holds, whence Lemmas 5.3.2 and 3.2.5 imply that $a \in \langle f_1 \rangle$, contradicting that $a = f_2$ and completing CASE 3.

CASE 4: $\Omega_0^u = \emptyset$ and $y_0|U \in \mathcal{A}_1^*$ with $U \notin \mathcal{C}_0$.

We may w.l.o.g. assume $U \in \mathcal{C}_1$. If $W_0 \in \mathcal{C}_1$, then performing type I swaps between $W_0$ and $U$ would imply, in view of Lemma 3.3.1, that $a = 0$, a contradiction. Moreover, this also shows that $\mathcal{A}_1 \cap \mathcal{C}_1 = \{U\}$.

Suppose $W_0 \in \mathcal{C}_2$. Performing a type I swap between $y_0|U$ and some $y|W_0$, letting $W'$ be the resulting product decomposition, we conclude from Lemma 3.2.3 that $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$, $W_0' \in \mathcal{C}_1$, $a = f_1 - f_2$ and $ne_1 = \sigma(U') = f_2$. Let $\mathcal{D}_1 = \mathcal{A}_2^*(W') \cap \mathcal{C}_1(W')$ and let $\mathcal{D}_2 = \mathcal{A}_2^*(W') \cap C_0(W')$. Since $\mathcal{A}_1 \cap \mathcal{C}_1 = \{U\}$, we have $|\mathcal{D}_1| = m - 2$. Since $ne_1 = f_2 \neq f_1 + f_2$, we have $Z \in \mathcal{C}_0$ with $Z \in \mathcal{A}_2^*$, and thus $|\mathcal{D}_2| \geq 1$. Apply Lemma 5.2 to $W'$. If Lemma 5.2(ii) holds, then Lemmas 5.3.1 and 3.2.1 imply $\psi_1(a) = 0$, contradicting that $a = f_1 - f_2$. Therefore Lemma 5.2(i) holds, whence $gne_1 + ne_2 + n\alpha = \sigma(V) = f_1$, where $V \in \mathcal{D}_1$. If there is a type III swap between $Z' = Z$ and $W_0'$ resulting in a product decomposition $W''$ with $\sigma(W_0'') \neq \sigma(W_0')$, then Lemma 3.3.4 implies that $\sigma(W_0'') = f_1 + f_2$, whence, performing a type I swap between $y_0|W_0''$ and $y|U'' = U'$, we conclude from Lemma 3.3.5 that $-a = -f_1$, contradicting that $a = f_1 - f_2$. Therefore hypothesis (a) holds in Lemma 5.2 for $W'$ with the roles of $\mathcal{D}_1$ and $\mathcal{D}_2$ reversed. Apply Lemma 5.2 in this case. If Lemma 5.2(ii) holds, then Lemmas 5.3.2 and 3.2.4 imply that $a \in \langle f_2 \rangle$, contradicting that $a = f_1 - f_2$. Therefore Lemma 5.2(i) holds, whence $gne_1 + ne_2 + n\alpha = \sigma(Z) = f_1 + f_2$, contradicting that $gne_1 + ne_2 + n\alpha = f_1$. So we may assume instead that $W_0 \in \mathcal{C}_0$.

Performing a type I swap between $y_0|U$ and some $y|W_0$, letting $W'$ be the resulting product decomposition, we conclude from Lemma 3.3.4 that $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$, $W_0' \in \mathcal{C}_1$, $a = -f_2$, and $ne_1 = \sigma(U') = f_1 + f_2$. Let $\mathcal{D}_1 = \mathcal{A}_2^*(W') \cap \mathcal{C}_2(W')$. If there is $V \in \mathcal{A}_1 \cap \mathcal{C}_2$, then, performing a type I swap between $y_0|U$ and some $y|V$, we conclude from Lemma 3.2.3 that $a = f_1 - f_2$, contradicting that $a = -f_2$. Therefore $|\mathcal{D}_1| = m - 1$. Let $\mathcal{D}_2 = \mathcal{A}_2^*(W') \cap \mathcal{C}_1(W')$. Since $\mathcal{A}_1 \cap \mathcal{C}_1 = \{U\}$, we have $|\mathcal{D}_2| \geq m - 2$. Thus we may apply Lemma 5.2 to $W'$. If Lemma 5.2(i) holds, then $ge_1 + e_2 + \alpha$ is a term of $S$ with multiplicity at least $mn - 1$, as desired. Therefore Lemma 5.2(ii) holds, whence Lemmas 5.3.3 and 3.2.3 imply that $a = \pm(f_1 - f_2)$, contradicting that $a = -f_2$. This completes CASE 4. □

There exists $e_2' \in e_2 + nG$ such that $(e_1, e_2')$ is a basis for $G$. Thus, after changing notation if necessary, we may suppose that $(e_1, e_2)$ is a basis of $G$. If $g \in G$ and $x, y \in \mathbb{Z}$ with $g = xe_1 + ye_2$, then we set $\pi_1(g) = xe_1$ and $\pi_2(g) = ye_2$.

**CLAIM C:** There exists $x_0|S_2$ such that $x - y \in \langle e_1 \rangle$ for all $xy|x_0^{-1}S_2$.

*Proof.* We need to show that there exists $x_0|S_2$ such that $\pi_2(\psi(x)) = \pi_2(\psi(y))$ for all $xy|x_0^{-1}S_2$. We divide the proof into four cases.

CASE 1: $\Omega_0^u \neq \emptyset$ and there is $U \in \mathcal{A}_1^* \cap \mathcal{C}_1$.

In this case, we have

$$ne_1 = \sigma(U) = f_1. \tag{16}$$

Let $V \in \mathcal{A}_2^*$. Perform type (II) swaps between $W_0$ and $V$. If $V,\, W_0 \in \mathcal{C}_1$, then we conclude from Lemmas 3.1.1 and 3.4.1 that $\pi_2(\psi(x)) = \alpha_2$ (say) for all $x|VW_0^{(2)}$. If $V,\, W_0 \in \mathcal{C}_0$, then we conclude, from Lemmas 3.1.3 and 3.4.1 and (16), that $\psi_2$ is constant on $VW_0^{(2)}$, whence (16) further implies that $\pi_2(\psi(x)) = \alpha_2$ for all $x|VW_0^{(2)}$. If $|\{V,\, W_0\} \cap \mathcal{C}_1| = 1$, then we conclude from Lemmas 3.1.2 and 3.4.3 that $\pi_2(\psi(x)) = \alpha_2$ for all $z|x_0^{-1}VW_0^{(2)}$, for some $x_0|VW_0^{(2)}$. If $\pi_2(\psi(x_0)) \neq \alpha_2$ and $x_0|V$, then pull $x_0$ up into a new product decomposition $W'$ and assume we began with $W'$ instead of $W$ (note that (16) holds independent of $W'$ and that $\widetilde{\sigma}(W) = \widetilde{\sigma}(W')$ follows by Lemma 3.1.2, so all previous arguments can be applied to $W'$ regardless of whether $\mathcal{A}_1^*(W') \cap \mathcal{C}_1(W')$ is nonempty or not). Doing this for all $V \in \mathcal{A}_2^*$, we conclude that there is an $x_0|S_2$ such that $\pi_2(\psi(x)) = \alpha_2$ for all $x|x_0^{-1}S_2$, completing CASE 1.

CASE 2: $\Omega_0^u \neq \emptyset$ and $\mathcal{A}_1 \cap \mathcal{C}_1 = \{W_0\}$.

Performing type II swaps between $W_0$ and each $U \in \mathcal{A}_2^* \cap \mathcal{C}_1$, we conclude from Lemmas 3.4.1 and 3.1.1 that $\pi_2(\psi(x)) = \alpha_2$ (say) for all $x|W_0^{(2)}U$, with $U \in \mathcal{A}_2^* \cap \mathcal{C}_1$. Let w.l.o.g. $W_1, \ldots, W_l$ be the blocks in $\mathcal{A}_2 \cap \mathcal{C}_0$, and let $W_{m+1}, \ldots, W_{2m-2}$ be the blocks in $\mathcal{A}_2^* \cap \mathcal{C}_1$. Note $l \geq 1$ else CLAIM C follows by the previous conclusion. Performing type II swaps between $W_0$ and $W_j$, with $j \in [1, l]$, we conclude from Lemmas 3.4.3 and 3.1.2 that $\pi_2(\psi(x)) = \alpha_2$ for all $x|z_j^{-1}W_j$, for some $z_j|W_j$. We may w.l.o.g. assume $\pi_2(\psi(z_j)) \neq \alpha_2$ for $j \in [1, l']$ and $\pi_2(\psi(z_j)) = \alpha_2$ for $j \in [l'+1, l]$. We have $l' \geq 2$ else CLAIM C follows.

Perform a type II swap between $z_1|W_1$ and any term $y|W_0^{(2)}$, and let $W'$ denote the resulting product decomposition. Since $\pi_2(\psi(z_1)) \neq \alpha_2$, we are assured that $\pi_2(\sigma(W_0)) \neq \pi_2(\sigma(W_0'))$, and hence $\sigma(W_0) \neq \sigma(W_0')$. Thus Lemma 3.1.2 implies that $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$, $W_0' \in \mathcal{C}_0$ and $W_1' \in \mathcal{C}_1$.

Now pull the term $z_2|W_2$ up into a new product decomposition $W''$. Note by Lemma 3.1.2 that $\widetilde{\sigma}(W'') = \widetilde{\sigma}(W)$. If $W_0'' \in \mathcal{C}_1$, then the arguments of the first paragraph show that $\pi_2(\psi(z_2)) = \alpha_2$, contradicting that $l' \geq 2$. Therefore $W_2'' \in \mathcal{C}_1$ instead. However, noting that $yW_0^{(1)}|W_0''$, for some $y|W_0^{(2)}$ (since $\sigma(\iota(W_0^{(2)})) \equiv 1 \mod n$ and $\sigma(\iota(W_2')) \equiv 0 \mod n$), we can still perform the swap between $y|W_0''$ and $z_1|W_1'' = W_1$ described in the previous paragraph, which results in a new product decomposition $W'''$ in which the $m$ blocks

$$W_1''' = W_1',\, W_2''' = W_2'',\, W_{m+1}''' = W_{m+1}, \ldots, W_{2m-2}''' = W_{2m-2}$$

all have equal sum $f_1$, contradicting that $S' \in \mathcal{A}(G)$, and completing CASE 2.

CASE 3: Either $(\Omega_0^u \neq \emptyset$ and $\mathcal{A}_1 \cap \mathcal{C}_1 = \emptyset)$ or $(\Omega_0^u = \emptyset$ and $W_0 \notin \mathcal{C}_0)$.

If $\Omega_0^u = \emptyset$, we may w.l.o.g. assume $\widetilde{\sigma}(W) = f_1^{m-1} f_2^{m-1}(f_1 + f_2)$ with $\mathcal{C}_1$ those blocks with sum $f_1$ and $\mathcal{C}_2$ those blocks with sum $f_2$, and that $W_0 \in \mathcal{C}_2$. Let w.l.o.g. $W_1, \ldots, W_s$ be the $s \leq m-1$ blocks of $\mathcal{C}_1 \cap \mathcal{A}_2^*$. Let $\sigma(W_0) = Cf_1 + f_2$ and $F = (C-1)f_1 + f_2$. If $\Omega_0^u \neq \emptyset$, then we have $s = m-1$ by hypothesis. If $s = 0$, then $|\mathcal{A}_1^* \cap \mathcal{C}_1| = m-1$, implying $e_1$ is a term with multiplicity at least $mn-1$ in $S$ (in view of CLAIM B), as desired. Therefore we may assume $s > 0$.

We claim, for any $W$ satisfying the hypothesis of CASE 3 and notated as above (and in fact, if $W \in \Omega_0^{nu}$, we will not need that $\Omega_0^u = \emptyset$), that

$$\pi_2(\psi(x_0^{-1} W_0^{(2)} \prod_{\nu=1}^{s} W_\nu)) = q_2^{(s+1)n-1} \tag{17}$$

for some $x_0 | W_0^{(2)} \prod_{\nu=1}^{s} W_\nu$ and $q_2 \in \mathrm{Ker}(\varphi)$. To show this, perform type II swaps between $W_0$ and $W_i$, $i \in [1, s]$. If $\pi_2(F) = 0$, then Lemmas 3.4.1 and either 3.1.2 or 3.2.3 imply that (17) holds with $\pi_2(x_0) = q_2$ as well. If $\pi_2(F) \neq 0$ and (17) fails, then Lemmas 3.4.3 and either 3.1.2 or 3.2.3 imply that $\pi_2(\psi(z)) = q_2$ (say) for all $z | x_i^{-1} x_0^{-1} W_0^{(2)} W_i$, for some $x_i | W_i$, $i \in [1, s]$; moreover, $s \geq 2$ and w.l.o.g. $\pi_2(\psi(x_1))$ and $\pi_2(\psi(x_2))$ are not equal to $q_2$. Pull $x_1 | W_1$ up into a new product decomposition $W'$. If $\sigma(W_0') = \sigma(W_0)$, then the arguments of the previous sentence imply either $\pi_2(\psi(x_1)) = q_2$ or $\pi_2(\psi(x_2)) = q_2$, a contradiction. If $\sigma(W_0') \neq \sigma(W_0)$ and $W \in \Omega_0^u$, then Lemma 3.1.2 implies that $W' \in \Omega_0^u$ with $W_0' \in \mathcal{C}_1$, whence CLAIM C follows in view of CASE 2 applied to $W'$. Therefore we may assume $\sigma(W_0') \neq \sigma(W_0)$, $W \in \Omega_0^{nu}$ and $W_0' \in \mathcal{C}_1$ (in view of Lemma 3.2.3). Let $y$ be a term that divides both $W_0^{(2)}$ and $W_0'^{(2)}$ (possible since $\sigma(\iota(W_0)) \equiv 1 \mod n$). Choose $I$ such that $\min I \equiv \iota(y) \mod n$, and consequently $\epsilon(y, z) = 0$ for any $z$ (in view of (10)). Note that while the new choice of $I$ may change the overall value of $\psi(x)$, where $x | S_2$, in a nontrivial manner, nonetheless, the value of $\pi_2(\psi(x))$ remains unchanged. Perform type II swaps between $y | W_0$ and any $z | W_2$. In view of our choice of $I$, Lemma 3.2.3 and $\pi_2(\psi(x_2)) \neq q_2$, we conclude that $-\psi(x_2) + \psi(y) = F = -f_1 + f_2$ (since $-\pi_2(\psi(x_2)) + \pi_2(\psi(y)) \neq 0$, implying $-\psi(x_2) + \psi(y) \neq 0$), and that $-\psi(z) + \psi(y) = 0$ if $z \neq x_2$ (since $-\pi_2(\psi(z)) + \pi_2(\psi(y)) = 0$); in particular, $\psi_1(x_2) \neq \psi_1(z)$ for $z | x_2^{-1} W_2$. However, performing type II swaps between $y | W_0'$ and any $z | W_2' = W_2$, we conclude from Lemma 3.2.1 and the choice of $I$ that $\psi_1$ is constant on $W_2' = W_2$, contradicting the previous sentence. Thus (17) is established in all cases.

Next we proceed to show that $s = m-1$. To this end, suppose $s < m-1$. As noted before, we may then assume $\Omega_0^u = \emptyset$. Let $U \in \mathcal{A}_1^* \cap \mathcal{C}_1$ (which is nonempty by the assumption $s < m-1$). Then $f_1 = \sigma(U) = ne_1$. Let $x_0$ and $q_2$ be as defined by (17). Thus, performing type II swaps between a fixed $x_1 | x_0^{-1} W_0^{(2)}$ and any $y | V \in \mathcal{A}_2^* \cap (\mathcal{C}_2 \cup \mathcal{C}_0)$, we conclude from $f_1 = \sigma(U) = ne_1$ and Lemmas 3.2.2 and 3.2.5 that $\psi_2(V) = \psi_2(x_1)^n$ for all such blocks $V \in \mathcal{A}_1^* \cap (\mathcal{C}_2 \cup \mathcal{C}_0)$. Hence, in view of $ne_1 = f_1$, we conclude that $\pi_2(\psi(V)) = \pi_2(\psi(x_1))^n = q_2^n$ for all such $V$, which combined with (17) implies CLAIM C. So we may assume $s = m-1$.

In case $W \in \Omega_0^{nu}$, we have assumed $\Omega_0^u = \emptyset$. However, we will temporarily drop this assumption, allowing consideration of $W \in \Omega_0^{nu}$ even when $\Omega_0^u \neq \emptyset$, provided it still satisfies the hypothesis of CASE 3 and follows the notation given in the first paragraph with $s = m-1$. This will extend until the end of assertion **A1** below, which shows that the exceptional term $x_0$ in (17) is not necessary.

**A1.** For every $W \in \Omega_0$ satisfying the hypotheses of CASE 3 (allowing $W \in \Omega_0^{nu}$ even if $\Omega_0^u \neq \emptyset$), we have $\pi_2(\psi(x_0)) = q_2$, where $q_2$ and $x_0$ are as given by (17).

*Proof of* **A1**. Assume instead there exists $W \in \Omega_0$ satisfying the hypotheses of CASE 3 with $\pi_2(\psi(x_0)) \neq q_2$.

Suppose $x_0|W_j$ with $j > 0$. Pull up an arbitrary $y|W_k \in \mathcal{A}_2$, with $k \geq m$, into a resulting product decomposition $W''$ (such a block exists, else (17) completes CLAIM C). If $W''$ satisfies the hypotheses of CASE 3, then applying (17) to $W''$ we conclude that $\pi_2(\psi(y)) = q_2$, whence CLAIM C follows in view of (17) and the arbitrariness of $y$. Therefore we may instead assume $W''$ does not satisfy the hypotheses of CASE 3, whence, in view of CASES 1 and 2, we may assume $W'' \in \Omega_0^{nu}$ with $W''_0 \in \mathcal{C}_0(W'')$.

Let $z$ be a term dividing both $W_0^{(2)}$ and $W_0''^{(2)}$ (which exists in view of $\sigma(\iota(W_0^{(2)})) \equiv 1 \mod n$). Note that we cannot have $0 = \psi(z) - \psi(x_0) + \epsilon(z, x_0)ne_1$, as then $0 = \pi_2(\psi(x_0)) - \pi_2(\psi(z)) = \pi_2(\psi(x_0)) - q_2$, a contradiction to $\pi_2(\psi(x_0)) \neq q_2$. Thus, in view of (17) and Lemma 3.2.3 or 3.1.2, it follows that performing a type II swap between $x_0|W_j$ and $z|W_0^{(2)}$ results in a new product decomposition $W'$ in which $\sigma(W'_j) = Cf_1 + f_2$ and $\sigma(W'_0) = f_1$. Thus, if $W \in \Omega_0^u$, then we can apply Lemma 5.1 to conclude $W'' \in \Omega_0^u$, contrary to the conclusion of the previous paragraph. Therefore we may assume $W \in \Omega_0^{nu}$. Hence, from $W'' \in \Omega_0^{nu}$ and Lemma 3.3, it follows that $\widetilde{\sigma}(W'') = \widetilde{\sigma}(W)$, whence $\sigma(W''_0) = f_1 + f_2$ (in view of $W''_0 \in \mathcal{C}_0(W'')$). However, since $z|W_0''^{(2)}$, we may still apply the previously described swap between $x_0|W''_j = W_j$ and $z|W''_0$ now in $W''$, which results in a product decomposition $W''' \in \Omega'$ with $\mathsf{v}_{f_2}(\widetilde{\sigma}(W''')) = m$ (as $\sigma(W'''_j) = \sigma(W'_j) = Cf_1 + f_2 = f_2$ and $\sigma(W''_j) = \sigma(W_j) = f_1$), contradicting that $S \in \mathcal{A}(G)$. So we may assume $x_0|W_0$.

Perform a type II swap between an arbitrary $x|W_0^{(2)}$ and $y|W_j$ with $j \in [1, m-1]$. In view of Lemma 3.1.2 or 3.2.3, it follows that

$$\epsilon(x, y)ne_1 + \psi(x) - \psi(y) \in \{0,\ F\}. \tag{18}$$

If $x = x_0$, then it follows, in view of $\pi_2(\psi(x_0)) - \pi_2(\psi(y)) = \pi_2(\psi(x_0)) - q_2 \neq 0$ and (18), that $\epsilon(x_0, y)ne_1 + \psi(x_0) - \psi(y) = F$, and thus

$$0 \neq \pi_2(\psi(x_0)) - q_2 = \pi_2(\psi(x_0)) - \pi_2(\psi(y)) = \pi_2(F). \tag{19}$$

Consequently, if $x \neq x_0$, then, from $\pi_2(\psi(x)) - \pi_2(\psi(y)) = q_2 - q_2 = 0$ (in view of (17)) and (18) and (19), it follows that

$$\epsilon(x, y)ne_1 + \psi(x) - \psi(y) = 0.$$

As $y|W_j$ with $j \in [1, m-1]$ and $x|x_0^{-1}W_0^{(2)}$ were arbitrary above, we see that we can apply Lemma 5.4 with $i = 0$, $Z = x_0^{-1}W_0^{(2)}$ and $\mathcal{D} = \{W_1, \ldots, W_{m-1}\}$.

Thus we can choose $I$ appropriately so that, for some $q \in \mathrm{Ker}(\varphi)$, we have that

$$\psi(x) = q \tag{20}$$

for all $x|x_0^{-1}W_0^{(2)}\prod_{\nu=1}^{m-1} W_\nu$, and that

$$\iota(x) \leq \iota(y) \tag{21}$$

for all $x|x_0^{-1}W_0^{(2)}$ and $y|W_i$, $i \in [1, m-1]$. By performing a type II swap between $x_0|W_0$ and each $y|W_i$, with $i \in [1, m-1]$, we conclude, from $\pi_2(\psi(x_0)) \neq q_2 = \pi_2(q)$ and either Lemma 3.1.2 or 3.2.3, that

$$\psi(x_0) - q + \epsilon(x_0, y)ne_1 = (C-1)f_1 + f_2. \tag{22}$$

Thus $\epsilon(x_0, y)$ must be the same for every $y|W_j$ with $j \in [1, m-1]$. As a result, it follows in view of (10) that either $\iota(x_0) \le \min(\mathrm{supp}(\iota(\prod_{\nu=1}^{m-1} W_\nu)))$ or $\iota(x_0) > \max(\mathrm{supp}(\iota(\prod_{\nu=1}^{m-1} W_\nu)))$. In the latter case, we may choose $I$ such $\min I \equiv \iota(x_0) \mod n$, and thus, in both cases, we have (in view of (21))

$$\iota(x) \le \iota(y) \tag{23}$$

for all $x|W_0^{(2)}$ and $y|W_i$, $i \in [1, m-1]$, while still preserving that (20) holds for some $q \in \mathrm{Ker}(\varphi)$ (since (23) was all that was required in the proof of Lemma 5.4 to ensure (20) held). Consequently, (22) and (10) imply that

$$\psi(x_0) = q + F = q + (C-1)f_1 + f_2. \tag{24}$$

Let $y|W_k \in \mathcal{A}_2$ with $k \ge m$ and $\pi_2(\psi(y)) \ne q_2$; such a term and block exists else CLAIM C follows in view of (17). If $y|W_k$ could be pulled up into a new product decomposition $W'$ with $x_0|W_0'$, then $W'$ must still satisfy the hypothesis of CASE 3 (by the same arguments used when $x_0|W_j$ with $j > 0$), whence applying (17) to $W'$ implies $\pi_2(\psi(x_0)) = q_2$ or $\pi_2(\psi(y)) = q_2$, contrary to our assumption. Therefore we may assume this is not the case, whence Theorem 2.6.2 implies that

$$\iota(W_0^{(2)}) = g_1^l g_2^{n-1-l}\iota(x_0) \text{ and } \iota(W_k) = g_1^{n-1-l} g_2^l \iota(y), \tag{25}$$

for some $g_1$, $g_2 \in \mathbb{Z}$ with $\gcd(g_1 - g_2, n) = 1$. If there existed $x_0'|W_0^{(2)}$ such that $\epsilon(x_0', z) = \epsilon(x_0, z)$ for some $z|W_k$, then we could apply a type II swap between $z|W_k$ and each of $x_0|W_0$ and $x_0'|W_0$, which in view of Lemma 3.1.3 or Lemma 3.2 would imply that $\psi_2(x_0) = \psi_2(x_0') = \psi_2(q)$, contradicting (24). Therefore we may assume otherwise, whence (10) implies either

$$\iota(x_0) \le \min(\mathrm{supp}(\iota(W_k)) \le \max(\mathrm{supp}(\iota(W_k)) < \min(\mathrm{supp}(\iota(x_0^{-1}W_0^{(2)})) \tag{26}$$

or

$$\iota(x_0) > \max(\mathrm{supp}(\iota(W_k)) \ge \min(\mathrm{supp}(\iota(W_k)) \ge \max(\mathrm{supp}(\iota(x_0^{-1}W_0^{(2)})). \tag{27}$$

In either case, we see that $|\mathrm{supp}(\iota(W_k)) \cap \mathrm{supp}(\iota(W_0^{(2)}))| \le 1$. As a result, (25) implies that w.l.o.g. $l = n-1$, $\iota(W_0^{(2)}) = g_1^{n-1}\iota(x_0)$ and $\iota(W_k) = g_2^{n-1}\iota(y)$. Thus $\sigma(\iota(W_k)) \equiv 0 \mod n$ and $\sigma(\iota(W_0^{(2)})) \equiv 1 \mod n$ imply that $\iota(W_k) = g_2^n$ and $\iota(x_0) \equiv g_1 + 1 \mod n$.

If (26) holds, then from $\iota(x_0) \equiv g_1 + 1 \mod n$ and (26) it follows that $\max I \equiv g_1 \mod n$. However, in view of (23), this is only possible if $\iota(x) \equiv g_1 \mod n$ for all $x|x_0^{-1}W_0^{(2)} \prod_{\nu=1}^{m-1} W_\nu$, in which case, since $\psi(x) = q$ also holds for all such terms (in view of (20)), it follows that $S$ contains a term with multiplicity $mn-1$, as desired. Therefore we can instead assume (27) holds. In this case, it follows, in view of (27), $\iota(x_0^{-1}W_0^{(2)}) = g_1^{n-1}$ and $\iota(x_0) \equiv g_1 + 1 \mod n$, that

$$\{g_2\} = \mathrm{supp}(\iota(W_k)) = \mathrm{supp}(\iota(x_0^{-1}W_0^{(2)})) = \{g_1\},$$

contradicting that $\gcd(g_1 - g_2, n) = 1$. □

We now return to arguments where we assume $\Omega_0^u = \emptyset$ when $W \in \Omega_0^{nu}$. In view of **A1**, we may assume $\pi_2(\psi(x)) = q_2$ for all $x|W_0^{(2)} \prod_{\nu=1}^{m-1} W_\nu$. Let $y|W_k$, with $W_k \in \mathcal{A}_2$ and $k \ge m$, be arbitrary. If we can pull up $y$ into a new product decomposition $W'$ such that either $W' \in \Omega_0^u$, or else $W' \in \Omega_0^{nu}$ and $W_0' \notin \mathcal{C}_0(W')$, then it follows, in view of CASES 1 and 2, **A1** and (17), that we may assume $\pi_2(\psi(y)) = q_2$ also (note this is where we need that $W\in\Omega_0^{nu}$ is allowed in **A1** even when $\Omega_0^u\neq\emptyset$). However, this can only fail if (by an appropriate choice for $f_2$ in the case when $W\in\Omega_0^u$) w.l.o.g.

$$\widetilde{\sigma}(W)=f_1^{m-1}f_2^{m-2}(Cf_1+f_2)((1-C)f_1+f_2), \tag{28}$$

with $\sigma(W_k)=(1-C)f_1+f_2$ and (recall) $\sigma(W_0)=Cf_1+f_2$. Consequently, we see that there is at most one block $W_k$ for which this can fail (as $W_0\notin\mathcal{C}_0$ when $\Omega_0^u=\emptyset$). As CLAIM C follows otherwise, we may assume $W_k\in\mathcal{A}_2$ exists and that $\widetilde{\sigma}(W)$ is of such form, and w.l.o.g. assume $k=2m-2$. Then

$$Cf_1+f_2=\sigma(W_0)=Y_1ne_1+ne_2+nq_2, \tag{29}$$

$$f_1=\sigma(W_1)=Y_2ne_1+ne_2+nq_2, \tag{30}$$

for some $Y_i\in\mathbb{Z}$. From (29) and (30), we conclude that

$$(C-1)f_1+f_2\in\langle ne_1\rangle. \tag{31}$$

If there exists $U\in\mathcal{A}_1^*$, then $ne_1=\sigma(U)=f_2$ (in view of (28), $s=m-1$ and $W_k=W_{2m-2}\in\mathcal{A}_2$); thus from (31) it follows that $(C-1)f_1\in\langle f_2\rangle$, which is only possible if $C\equiv 1 \mod m$, contradicting that $W\notin\mathcal{C}_0$ when $W\in\Omega_0^{nu}$ (in view of (28)). So we may instead assume $|\mathcal{A}_1|=1$. This same argument also shows that $\psi_1(ne_1)\neq 0$. Let $\mathcal{D}=\{W_m,\ldots,W_{2m-2}\}$.

If $\psi_2(ne_1)=0$, then $ne_1\in\langle f_1\rangle$, which combined with (31) yields a contradiction to $(f_1,f_2)$ being a basis. Therefore $\psi_2(ne_1)\neq 0$. Thus, in view of Lemma 3.1.3 or Lemmas 3.2.5 and 3.2.2, it follows that we may apply Lemma 5.4 with $Z=W_0^{(2)}$, $i=2$ and $\mathcal{D}$ as given above. Choose $I$ as directed by Lemma 5.4 (as mentioned before, changing $I$ does not affect the value of $\pi_2(\psi(x))$, and thus (17) remains unaffected). Then

$$\psi_2(x)=\alpha_2, \tag{32}$$

for all $x|W_0^{(2)}\prod_{\nu=m}^{2m-2}W_\nu$ and some $\alpha_2\in\langle f_2\rangle$, and

$$\iota(x)\leq\iota(y), \tag{33}$$

for all $x|W_0^{(2)}$ and $y|\prod_{\nu=m}^{2m-2}W_\nu$.

Let $y_0|W_{2m-2}$ with $\pi_2(\psi(y_0))\neq q_2$ (such $y_0$ exists, as discussed above, else CLAIM C follows). Let $W'$ be an arbitrary product decomposition resulting from pulling up $y_0$ into a new product decomposition. Since $\pi_2(\psi(y_0))\neq q_2$, we have (as discussed earlier) $\widetilde{\sigma}(W')=f_1^{m-1}f_2^{m-1}(f_1+f_2)$ with $\sigma(W_0')=f_1+f_2$. Let $X=\gcd(W_0^{(2)},W_0'^{(2)})$ and let $X'$, $Y'$ and $Y$ be defined by $W_0^{(2)}=XX'$, $W_0'^{(2)}=XY'$ and $W_{2m-2}=YY'$. Thus $W'_{2m-2}=X'Y$. Note that all four of these newly defined subsequences are nontrivial in view of $\sigma(\iota(W_0^{(2)}))\equiv 1 \mod n$ and $\sigma(\iota(W_{2m-2}))\equiv 0 \mod n$.

Let $\mathcal{D}'=\{W_0',W_1',\ldots,W_{m-1}'\}$. In view of Lemma 3.2.4 and $\psi_1(ne_1)\neq 0$, it follows that we can apply Lemma 5.4 with $i=1$, $Z=W_0'^{(2)}$, and $\mathcal{D}$ taken to be $\mathcal{D}'$ (however, do NOT change $I$). If (9) holds, then (in view of (10)) we can find $z|W_j'$, for some $j\in[1,m-1]$, such that $\epsilon(y_0,z)=\epsilon(x,z)$, where $x|X$. Applying a type II swap between $z|W_j'$ and each of $x|W_0'$ and $y_0|W_0'$, we conclude from Lemma 3.2.4 that $\psi_1(x)=\psi_1(y_0)$. However, since $x|X$ and $X|W_0^{(2)}$, it follows from (32) that $\psi_2(x)=\psi_2(y_0)$ also, whence $\psi(x)=\psi(y_0)$, implying $q_2=\pi_2(\psi(x))=\pi_2(\psi(y_0))$, contrary to assumption. Therefore we may instead assume (8) holds. Moreover, if both $y_0$ and some $x|X$ are contained in the same interval $J_i$ (from (8)), then we can repeat the above argument to obtain the same contradiction. Therefore it follows, in view of (33), that $y_0 \in J_2$ and $X \subset J_1$.

Let $z | W_0'^{(2)}$ and $z' | W_j'$ with $j \ge m$ be arbitrary. Performing a type II swap between $z | W_0'^{(2)}$ and $z' | W_j'$, we conclude from Lemma 3.2.5 that

$$\psi_2(z) - \psi_2(z') + \psi_2(\epsilon(z, z') n e_1) = 0.$$

Thus (32) implies that $\psi_2(\epsilon(z, z') n e_1) = 0$, which, in view of $\psi_2(ne_1) \neq 0$ and (10), implies that $\epsilon(z, z') = 0$ and

$$\iota(z) \le \iota(z'), \tag{34}$$

for any $z | W_0'^{(2)}$ and $z' | W_j'$ with $j \ge m$.

Applying (34) using $z | Y'$ and $z' | X'$ and $j = 2m-2$, we conclude in view of (33) that

$$\iota(z) = \max(\mathrm{supp}(\iota(W_0'^{(2)}))) = \min(\mathrm{supp}(\iota(\prod_{\nu=m}^{2m-2} W_\nu'))) = \iota(z'), \tag{35}$$

for any $z' | X'$ and $z | Y'$.

From (35) applied with $z = y_0$, we see that there is $y_0' | W_0^{(2)}$ with $\iota(y_0') = \iota(y_0)$. Thus $y$ can be pulled up into a new decomposition $W''$ by exchanging $y_0 | W_{2m-2}$ and $y_0' | W_0$, and all of the above arguments (valid for an arbitrary $W'$ obtained by pulling up $y_0 | W_{2m-2}$) are applicable for $W''$. In particular, ${y_0'}^{-1} W_0^{(2)} = X \subset J_1$ and $y_0 \in J_2$ imply, in view of $Y = y_0^{-1} W_{2m-2}$, (8) and (35), that

$$\max(\mathrm{supp}(\iota({y_0'}^{-1} W_0^{(2)}))) < \min(\mathrm{supp}(\iota(W_{2m-2}))). \tag{36}$$

If we could pull up $y_0' y_0 | W_0 W_{2m-2}$ into a new product decomposition $W'''$, then (36) would imply that $X'$ contains a $z'$ with $\iota(z') < \iota(y_0)$, which would contradict (34) applied with $z = y_0$ and $z' = z'$. Therefore we can assume otherwise, whence Theorem 2.6.2 and (36) imply that $|\mathrm{supp}(\iota({y_0'}^{-1} W_0^{(2)}))| = |\mathrm{supp}(\iota(y_0^{-1} W_{2m-2}))| = 1$. Thus $\sigma(\iota(W_0^{(2)})) \equiv 1 \mod n$ and $\sigma(\iota(W_{2m-2})) \equiv 0 \mod n$ force that $\iota(W_{2m-2}) = g^n$ and $\iota(W_0^{(2)}) = (g-1)^{n-1} g$, where $\iota(y_0) = \iota(y_0') = g$. Consequently, (8), $X \subset J_1$ and $y_0 \in J_2$ (in the case when $W' = W''$) force that $\iota(z) = g$ for all $z | {y_0'}^{-1} W_0^{(2)} \prod_{\nu=1}^{m-1} W_i$.

Applying type III swaps among the $W_i$, $i \in [1, m-1]$, we conclude from Lemma 3.3.1 or 3.1.1 that $\psi(x) = q$ (say) for all $x | W_i$, $i \in [1, m-1]$. Applying type III swaps between $W_0$ and $W_1$, we conclude from Lemma 3.2.3 or 3.1.2 and Lemma 3.4.3 that $\psi(x) = q$ for all $x | {y_0''}^{-1} {y_0'}^{-1} W_0^{(2)}$, for some $y_0'' | {y_0'}^{-1} W_0^{(2)}$, and that $\psi(y_0'') = q$ or $q + (C-1) f_1 + f_2$. Applying a type III swap between $y_0'' | W_0''$ and some $z | W_1''$ in $W''$, we conclude from Lemma 3.2.4 that $\psi_1(y_0'') = \psi_1(z) = \psi_1(q)$, whence we see that $\psi(y_0'') = q + (C-1) f_1 + f_2$ is impossible (since $C \equiv 1 \mod m$ would contradict that $W_0 \notin \mathcal{C}_0$ when $W \in \Omega_0^{nu}$; see (28)). Thus $\psi(y_0'') = q$ as well, and $g e_1 + e_2 + q$ has multiplicity at least $mn - 1$ in $S$, as desired, completing CASE 3.

CASE 4: $\Omega_0^u = \emptyset$ and $W_0 \in \mathcal{C}_0$.

We start with the following assertion.

**A2.** If $\Omega_0^u = \emptyset$, $W \in \Omega_0^{nu}$ with $\widetilde{\sigma}(W) = f_1^{m-1} f_2^{m-1} (f_1 + f_2)$, $W_0 \in \mathcal{C}_0$, and $|\mathcal{A}_2 \cap \mathcal{C}_i| \ge 1$ for all $i \in \{1, 2\}$, then $I$ can be chosen such that one of the following properties holds:

(i) $|\mathrm{supp}(\psi(W_0^{(2)}))| = 1$, or

(ii) (a) $\psi_i(ne_1) \neq 0$ for all $i \in \{1, 2\}$,

(b) there exist $g_1$, $g_2 \in \mathbb{Z}$ such that $\gcd(g_1 - g_2, n) = 1$ and $\iota(U) = g_1^n$ and $\iota(V) = g_2^n$, for every $U \in \mathcal{A}_2^* \cap \mathcal{C}_1$ and $V \in \mathcal{A}_2^* \cap \mathcal{C}_2$,

(c) $g_1 > g_2$ and $\iota(x) \leq g_1$ for all $x|W_0^{(2)}$, and

(d) if also $|\mathcal{A}_2 \cap \mathcal{C}_i| \geq 2$ for all $i \in \{1, 2\}$, then there exist $c$, $d \in \mathrm{Ker}(\varphi)$ such that $\psi(U) = c^n$ and $\psi(V) = d^n$ for every $U \in \mathcal{A}_2^* \cap \mathcal{C}_1$ and $V \in \mathcal{A}_2^* \cap \mathcal{C}_2$.

*Proof of* **A2**. We may w.l.o.g. assume $\mathcal{C}_1$ are those blocks with sum $f_1$. Performing type II swaps between each $x|W_0^{(2)}$ and each $y|U \in \mathcal{A}_2^* \cap \mathcal{C}_1$, and between each $x|W_0^{(2)}$ and each $z|V \in \mathcal{A}_2^* \cap \mathcal{C}_2$, we conclude from Lemma 3.2 that

$$\psi_1(x) = \psi_1(y) - \psi_1(\epsilon(x,y)ne_1), \tag{37}$$

$$\psi_2(x) = \psi_2(z) - \psi_2(\epsilon(x,z)ne_1), \tag{38}$$

where (10) holds.

Since $\mathrm{ord}(e_1) = mn$, one of $\psi_1(ne_1)$ or $\psi_2(ne_1)$ is nonzero, say the former (the other case will be identical). Then, in view of (37), we may apply Lemma 5.4 with $i = 1$, $Z = W_0^{(2)}$ and $\mathcal{D} = \mathcal{A}_2^* \cap \mathcal{C}_1$. Consequently, we can choose $I$ such that

$$\iota(x) \leq \iota(y), \tag{39}$$

for all $x|W_0^{(2)}$ and $y|U \in \mathcal{A}_2^* \cap \mathcal{C}_1$, and $\psi_1$ is constant on $W_0^{(2)}$. If $\psi_2(ne_1)$ is zero, then (38) implies that $\psi_2$ is also constant on $W_0^{(2)}$, whence (i) holds. Therefore we may assume otherwise, and (a) is established. Likewise, if there is some $z|V \in \mathcal{A}_2^* \cap \mathcal{C}_2$ with $\iota(z) \geq \max(\mathrm{supp}(\iota(W_0^{(2)}))$ or $\iota(z) < \min(\mathrm{supp}(\iota(W_0^{(2)})))$, then (i) again holds (in view of (10) and (38)). So we may assume otherwise:

$$\min(\mathrm{supp}(\iota(W_0^{(2)}))) \leq \iota(z) < \max(\mathrm{supp}(\iota(W_0^{(2)}))), \tag{40}$$

for all $z|V \in \mathcal{A}_2^* \cap \mathcal{C}_2$. Consequently, it follows in view of (39) that both $\mathrm{supp}(\iota(\prod_{U \in \mathcal{A}_2^* \cap \mathcal{C}_1} U))$ and $\mathrm{supp}(\iota(\prod_{V \in \mathcal{A}_2^* \cap \mathcal{C}_2} V))$ are disjoint.

Suppose $|\mathrm{supp}(\iota(U))| > 1$ or $|\mathrm{supp}(\iota(V))| > 1$, for some $U \in \mathcal{A}_2^* \cap \mathcal{C}_1$ or $V \in \mathcal{A}_2^* \cap \mathcal{C}_2$. Then we may find $u_0|U$ and $v_0|V$ such that $|\mathrm{supp}(\iota(u_0^{-1}U))| > 1$ or $|\mathrm{supp}(\iota(v_0^{-1}V))| > 1$, whence it follows, in view of Theorem 2.6.2 (applied to $\iota(u_0^{-1}v_0^{-1}UV)$ modulo $n$) and the fact that $\mathrm{supp}(\iota(\prod_{U \in \mathcal{A}_2^* \cap \mathcal{C}_1} U))$ and $\mathrm{supp}(\iota(\prod_{V \in \mathcal{A}_2^* \cap \mathcal{C}_2} V))$ are disjoint, that we can refactor $UV = U'V'$ such that $U'$ and $V'$ both contain terms from both $U$ and $V$. Replacing the blocks $U$ and $V$ by the blocks $U'$ and $V'$ yields a new product decomposition $W' \in \Omega_0$; in view of Lemma 3.2.3, we still have $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$, whence $W'$ satisfies the hypotheses of **A2**. However, since both $U'$ and $V'$ contain terms from both $U$ and $V$, it follows that both $U'$ and $V'$ contain a term $z'|U$ with $\iota(z') \geq \max(\mathrm{supp}(\iota(W_0^{(2)})))$ (in view of (39)), as well as a term $z|V$ with $\min(\mathrm{supp}(\iota(W_0^{(2)}))) \leq \iota(z') < \max(\mathrm{supp}(\iota(W_0^{(2)})))$ (in view of (40)), which makes it impossible for (8) or (9) to hold for $W'$, contradicting that the above arguments show Lemma 5.4 must hold for $W'$. So we may assume $|\mathrm{supp}(\iota(U))| = 1$ and $|\mathrm{supp}(\iota(V))| = 1$ for all $U \in \mathcal{A}_2^* \cap \mathcal{C}_1$ and $V \in \mathcal{A}_2^* \cap \mathcal{C}_2$. Moreover, this argument also shows that if $\iota(U) = g_1^n$ and $\iota(V) = g_2^n$, then $\gcd(g_1 - g_2, n) = 1$.

Suppose $|\mathrm{supp}(\iota(\prod_{U \in \mathcal{A}_2^* \cap \mathcal{C}_1} U))| > 1$ or $|\mathrm{supp}(\iota(\prod_{V \in \mathcal{A}_2^* \cap \mathcal{C}_2} V))| > 1$, say the former (the other case will be identical). Then there are $U_1$, $U_2 \in \mathcal{A}_2^* \cap \mathcal{C}_1$ and $V \in \mathcal{A}_2^* \cap \mathcal{C}_2$ with $\iota(U_1) = g_1$, $\iota(U_2) = g_1'$ and $\iota(V) = g_2$, where $g_1 \neq g_1'$. We have $\gcd(g_1 - g_1', n) = 1$, else repeating the arguments of the previous paragraph, using $U_1$ and $U_2$ in place of $U$ and $V$, we obtain a $W' \in \Omega_0$ satisfying the hypotheses of **A2** but such that the conclusion of the previous paragraph fails, whence $1 = |\mathrm{supp}(\psi(W_0'^{(2)}))| = |\mathrm{supp}(\psi({W_0}^{(2)}))|$ must hold by prior arguments, yielding (i). Hence, since $\gcd(g_1 - g_2, n) = 1$ and $\gcd(g_1' - g_2, n) = 1$, it follows that all $n$-term zero-sum modulo $n$ subsequences of $g_1^{n-1} {g_1'}^{n-1} g_2^{n-1}$ have support of cardinality three. Thus, by two applications of Theorem 2.6.1, we see that we can refactor $U_1U_2V = XYZ$ such that $X$, $Y$ and $Z$ all contain terms from each of $U_1$, $U_2$ and $V$ (note, since $|\mathrm{supp}(\iota(X))| = 3$, that $\iota(YZ) \subset g_1^{n-1} {g_1'}^{n-1} g_2^{n-1}$). Replacing $U_1$, $U_2$ and $V$ by $X$, $Y$ and $Z$ yields a new product decomposition $W' \in \Omega_0$; in view of $\Omega_0^u = \emptyset$ and $m \geq 5$, we still have $\widetilde{\sigma}(W') = \widetilde{\sigma}(W)$, whence $W'$ satisfies the hypotheses of **A2**. However, since $X$, $Y$ and $Z$ each contain terms from $U_1$, $U_2$ and $V$, we see that the condition $|\mathrm{supp}(\iota(U))| = 1$ for $U \in \mathcal{A}_2^* \cap \mathcal{C}_1$ fails for $W'$, whence previous arguments show $|\mathrm{supp}(\psi(W_0^{(2)}))| = |\mathrm{supp}(\psi({W_0'}^{(2)}))| = 1$, yielding (i). So we may assume $|\mathrm{supp}(\iota(\prod_{U \in \mathcal{A}_2^* \cap \mathcal{C}_1} U))| = 1$ and $|\mathrm{supp}(\iota(\prod_{V \in \mathcal{A}_2^* \cap \mathcal{C}_2} V))| = 1$, and w.l.o.g. assume $\mathrm{supp}(\iota(\prod_{U \in \mathcal{A}_2^* \cap \mathcal{C}_1} U)) = g_1$ and $\mathrm{supp}(\iota(\prod_{V \in \mathcal{A}_2^* \cap \mathcal{C}_2} V)) = g_2$. This establishes (b). Moreover, by the arguments from the second paragraph, we see that we can choose $I$ such that (c) holds.

We now assume $|\mathcal{A}_2 \cap \mathcal{C}_i| \geq 2$, for all $i \in \{1, 2\}$. Performing type III swaps between distinct $U_1$, $U_2 \in \mathcal{A}_2^* \cap \mathcal{C}_1$ and between distinct $V_1$, $V_2 \in \mathcal{A}_2^* \cap \mathcal{C}_2$, we conclude from Lemma 3.3 that $\psi(U) = c$ (say) for all $U \in \mathcal{A}_2^* \cap \mathcal{C}_1$ and that $\psi(U) = d$ (say) for all $V \in \mathcal{A}_2^* \cap \mathcal{C}_2$, establishing (d), and completing the proof of **A2**.□

Since $\Omega_0^u = \emptyset$, it follows, in view of Lemma 3.3, that if we pull up any term $y|U$, where $U \in \mathcal{A}_2^*$, then we may assume the resulting product decomposition still satisfies the hypothesis of CASE 4, else CASE 3 completes the proof. Thus, if for every product decomposition satisfying the hypothesis of CASE 4 we can find $I$ such that $|\mathrm{supp}(\psi(W_0^{(2)}))| = 1$, then, since modifying $I$ does not alter the values $\pi_2(\psi(x))$, we would be able to conclude $|\mathrm{supp}(\pi_2(\psi(S_2)))| = 1$—by successively pulling up terms $y|S_2$, yielding a sequence of product decompositions satisfying the hypotheses of CASE 4, until every such $y$ occurred in the $W_0^{(2)}$ part of one of these product decompositions, and then noting that there must always be a common term in $W_0^{(2)}$ between any two consecutive product decompositions in the sequence (in view of $\sigma(\iota(W_0^{(2)})) \equiv 1 \mod n$)—completing CLAIM C. Therefore we may assume this is not the case for $W$. Let w.l.o.g. $\widetilde{\sigma}(W) = f_1^{m-1} f_2^{m-1}(f_1 + f_2)$ and $\mathcal{C}_1$ consist of those blocks with sum $f_1$.

Note that we must have $\mathcal{A}_2^* \cap \mathcal{C}_1$ and $\mathcal{A}_2^* \cap \mathcal{C}_2$ both nonempty, else in view of CLAIM B it would follow that $e_1$ is a term of $S$ with multiplicity $mn - 1$, completing the proof. Thus **A2.(ii)(a)** implies that $\psi_i(ne_1) \neq 0$ for $i \in \{1, 2\}$. As a result, we cannot have a block $U \in \mathcal{A}_1^*$ (else $ne_1 = \sigma(U) = f_1$ or $f_2$). Hence $|\mathcal{A}_1| = 1$, implying $|\mathcal{A}_2^* \cap \mathcal{C}_1| \geq 2$ and $|\mathcal{A}_2^* \cap \mathcal{C}_2| \geq 2$. Thus, by choosing $I$ appropriately, **A2.(ii)(a–d)** holds for $W$.

Suppose $\mathrm{supp}(\iota(W_0^{(2)})) \neq \{g_1, g_2\}$. Then there must be some $x_0|W_0^{(2)}$ with $\iota(x_0) \notin \{g_1, g_2\}$ (in view of $\sigma(\iota(W_0^{(2)})) \equiv 1 \mod n$). Since $\gcd(g_1 - g_2, n) = 1$, there is no $n$-term zero-sum mod $n$ subsequence of $g_1^{n-1} g_2^{n-1}$. Thus applying Theorem 2.6.1 to $g_1^{n-1} g_2^{n-1} \iota(x_0)$ implies that we may find a subsequence $U_1|W_0^{(2)}UV$, where $U \in \mathcal{A}_2^* \cap \mathcal{C}_1$ and $V \in \mathcal{A}_2^* \cap \mathcal{C}_2$, such that $x_0|U_1$ and $\mathrm{supp}(\iota(z^{-1}U_1)) = \{g_1, g_2\}$. Consequently, $\mathsf{v}_{g_i}(U_1) \leq n - 2$, and thus $\mathsf{v}_{g_i}(\iota(U_1^{-1} W_0^{(2)} UV)) \geq 2$, for $i = \{1, 2\}$. Thus, if there were no $n$-term zero-sum mod $n$ subsequence of $\iota(U_1^{-1} u_1^{-1} v_1^{-1} W_0^{(2)} UV)$, where $u_1|U_1^{-1}U$ and $v_1|U_1^{-1}V$, then Theorem 2.6.2 would imply that $\iota(U_1^{-1} W_0^{(2)} UV) = g_1^n g_2^n$, whence

$$1 \equiv \sigma(\iota(W_0^{(2)}UV)) \equiv \sigma(\iota(U_1)) + ng_1 + ng_2 \equiv 0 \mod n,$$

which is a contradiction. Therefore we may assume there exists such a subsequence $\iota(U_2)$, where $U_2|U_1^{-1} u_1^{-1} v_1^{-1} W_0^{(2)} UV$. Let $W_0'$ be defined by $W_0UV = U_1U_2W_0'$. Then replacing the blocks $W_0$, $U$

and $V$ with the blocks $W_0'$, $U_1$, and $U_2$ yields a new product decomposition $W' \in \Omega_0$. Since $\Omega_0^u = \emptyset$ and $m \geq 4$, we must have $\widetilde{\sigma}(W) = \widetilde{\sigma}(W')$, and we may further assume $W_0' \in \mathcal{C}_0$ else CASE 3 completes the proof. Thus $W'$ satisfies the hypotheses of CASE 4, but since $|\mathrm{supp}(\iota(U_1))| > 1$, we see that $W'$ does not satisfy **A2.(ii)**. Thus **A2.(i)** implies that we must have $|\mathrm{supp}(\pi_2(\psi({W_0'}^{(2)}))| = 1$ (note we do not have $|\mathrm{supp}(\psi({W_0'}^{(2)})| = 1$ as we would need to change $I$ for this to hold); since $u_1v_1|W_0'$, this implies that $\pi_2(c) = \pi_2(\psi(u_1)) = \pi_2(\psi(v_1)) = \pi_2(d)$.

Let $x|x_0^{-1}W_0^{(2)}$ be arbitrary. By Theorem 2.6.1, it follows that there is an $n$-term zero-sum mod $n$ subsequence of $\iota(x^{-1}U_1^{-1}W_0^{(2)}UV)$, say $\iota(U_3)$ with $U_3|x^{-1}U_1^{-1}W_0^{(2)}UV$. Let $W_0''$ be defined by $W_0UV = U_1U_3W_0''$. Then replacing the blocks $W_0$, $U$ and $V$ with the blocks $W_0''$, $U_1$, and $U_3$ yields a new product decomposition $W'' \in \Omega_0$, and as before we may assume $W''$ satisfies the hypotheses of CASE 4 with $\widetilde{\sigma}(W'') = \widetilde{\sigma}(W)$. Thus, since $|\mathrm{supp}(\iota(U_1))| > 1$, we see that $W''$ does not satisfy **A2.(ii)**, and so we must have

$$|\mathrm{supp}(\pi_2(\psi({W_0''}^{(2)}))| = 1. \tag{41}$$

Since $x_0|U_1$, it follows in view of the pigeonhole principle that we must have a term $x'|{W_0''}^{(2)}$ with $x'|UV$, and thus with $\pi_2(\psi(x')) = \pi_2(c)$ (in view of the previous paragraph). Since $x|W_0''$, this implies $\pi_2(\psi(x)) = \pi_2(c)$ (in view of (41)). As $x|x_0^{-1}W_0^{(2)}$ was arbitrary, we conclude that every $x|x_0^{-1}S_2$ has $\pi_2(\psi(x)) = \pi_2(c) = \pi_2(d)$, completing the proof (in view of **A2.(ii)** holding for $W$). So we may instead assume $\mathrm{supp}(\iota(W_0^{(2)})) = \{g_1, g_2\}$.

Since $|\mathcal{A}_1| = 1$, let w.l.o.g. $W_1, \ldots, W_{m-1}$ be the blocks of $\mathcal{A}_2^* \cap \mathcal{C}_1$, and let $W_m, \ldots, W_{2m-2}$ be the blocks of $\mathcal{A}_2^* \cap \mathcal{C}_2$. Let $W_0^{(2)} = b_1 \cdot \ldots \cdot b_t b_1' \cdot \ldots \cdot b_{n-t}'$ with $\iota(b_i) = g_1$ and $\iota(b_j') = g_2$. Applying type III swaps between $b_i|W_0$ and $y|W_1$, it follows from Lemma 3.3.4 that we may assume $\psi(b_i) = \psi(y) = c$ for all $i$ (else CASE 3 completes the proof). Likewise applying type III swaps between $b_i'|W_0$ and $z|W_m$, it follows that $\psi(b_i') = \psi(z) = d$ for all $i$. Consequently, we may assume $t \in [2, n-2]$, else $S$ contains a term with multiplicity at least $mn-1$, as desired (either $g_1e_1 + e_2 + c$ or $g_2e_1 + e_2 + d$).

Applying type II swaps between $b_1|W_0$ and $z|W_m$ and between $b_1'|W_0$ and $y|W_1$, it follows, in view of Lemma 3.2, (10) and $g_1 > g_2$, that

$$d - c \in \langle f_2 \rangle, \tag{42}$$

$$c - d + ne_1 \in \langle f_1 \rangle. \tag{43}$$

Since $t \in [2, n-2]$, we have $b_1b_2|W_0^{(2)}$ and $b_1'b_2'|W_0^{(2)}$. Let $Y$ be a subsequence of $W_1$ and $Z$ be a subsequence of $W_m$ with $|Y| = |Z| = 2$. Applying type II swaps between $b_1'b_2'|W_0$ and $Y|W_1$ and between $b_1b_2|W_0$ and $Z|W_m$, we conclude from Lemma 3.2 that

$$2(d-c) + \epsilon(b_1'b_2', Y)ne_1 \in \langle f_2 \rangle, \tag{44}$$

$$2(c-d) + \epsilon(b_1b_2, Z)ne_1 \in \langle f_1 \rangle. \tag{45}$$

Observe (in view of $g_1 > g_2$) that

$$\epsilon(b_1'b_2', Y)ne_1 = \begin{cases} 0, & \text{if } g_1 - g_2 \leq \frac{n-1}{2}; \\ -ne_1, & \text{if } g_1 - g_2 \geq \frac{n+1}{2}. \end{cases}$$

Likewise

$$\epsilon(b_1b_2, Z)ne_1 = \begin{cases} ne_1, & \text{if } g_1 - g_2 \le \frac{n-1}{2}; \\ 2ne_1, & \text{if } g_1 - g_2 \ge \frac{n+1}{2}. \end{cases}$$

Thus, if $g_1 - g_2 \le \frac{n-1}{2}$, then (45) and (43) imply that $c - d \in \langle f_1 \rangle$, which combined with (42) implies that $c = d$, in which case CLAIM C follows. On the other hand, if $g_1 - g_2 \ge \frac{n+1}{2}$, then (44) and (42) imply that $ne_1 \in \langle f_2 \rangle$, which contradicts that **A2.(ii)(a)** holds for $W$, completing CASE 4. □

**CLAIM D:** $\mathsf{h}(S) = mn - 1$.

*Proof.* Let $S_2' = x_0^{-1}S_2$, with $x_0$ as in CLAIM C, and let $S' = S_1S_2'$. By Proposition 4.2 and CLAIM B, we have $S_1 = e_1{}^{|S_1|}$, $|S_1| = \ell n - 1$ and $|S_2'| = 2mn - \ell n - 1$, for some $\ell \ge 1$. If $\ell \ge m$, then $e_1$ is a term with multiplicity at least $mn - 1$, as desired. Therefore $\ell < m$. Moreover, since $S \in \mathcal{A}(G)$, it follows that $0 \notin \Sigma(S')$. In view of CLAIM C, we may assume every $x|S_2'$ is of the form $y_ie_1 + (1 + nq)e_2$, with $q \in [0, m-1]$. Let $T = \pi_1(S_2') \in \mathcal{F}(\langle e_1 \rangle)$, and let $H' = \langle e_1, (1 + qn)e_2 \rangle \cong C_{mn} \oplus C_{rn}$, where $rn = \text{ord}((1+qn)e_2)$. If $r < m$, then noting that $S' \in \mathcal{F}(H')$ with $|S'| = 2mn-2 \ge mn+rn-1 = \mathsf{D}(H')$, we see that $0 \in \Sigma(S')$, contradicting that $S \in \mathcal{A}(G)$. Thus we may choose $e_2$ to be $(1 + qn)e_2$ while still preserving that $(e_1, e_2)$ is a basis, and so w.l.o.g. we assume $q = 0$.

Since $\ell < m$, it follows that $|S_2'| = 2mn - \ell n - 1 \ge mn + n - 1 \ge mn + 2$ and

$$\Sigma(S_1) = \{e_1, 2e_1, \ldots, (\ell n - 1)e_1\}. \tag{46}$$

Consequently, $0 \notin \Sigma(S')$ implies

$$\Sigma_{mn}(S_2') = \Sigma_{mn}(T) \subset A := \{e_1, 2e_1, \ldots, (mn - \ell n)e_1\}, \tag{47}$$

and thus

$$|\Sigma_{mn}(T)| \le mn - \ell n = |T| - mn + 1. \tag{48}$$

Note $\mathsf{h}(T) = \mathsf{h}(S_2') \le mn - 2$, else the proof is complete. Thus we can apply Theorem 2.7, taking $k = 3$, whence it follows, in view of (48) and $0 \notin \Sigma_{mn}(T)$, that $|\text{supp}(T)| \le 2$.

We may assume $|\text{supp}(T)| = 2$, else $S$ will contain a term with multiplicity $|T| = 2mn - \ell n - 1 \ge mn + n - 1$, contradicting that $S \in \mathcal{A}(G)$. Thus $T = (g_0e_1)^{n_1}((g_0 + d)e_1)^{n_2}$ for some $g_0, d \in \mathbb{Z}$ with $de_1 \ne 0$. Since $(e_1, g_0e_1 + e_2)$ is also a basis for $G$, then, by redefining $e_2$ to be $g_0e_1 + e_2$, we may w.l.o.g. assume $g_0 = 0$. Thus

$$\Sigma_{mn}(T) = B := (mn - n_1)de_1 + \{0, de_1, \ldots, (mn - \ell n - 1)de_1\}, \tag{49}$$

which is an arithmetic progression of difference $de_1$ and length $mn - ln$ (in view of $0 \notin \Sigma_{nm}(T)$). In view of (47), we have $B = A$ with

$$2 \le n \le |A| = mn - \ell n \le mn - n \le mn - 2.$$

Thus $de_1 = \pm e_1$ (as the difference of an arithmetic progression under the above assumptions is unique up to sign). Consequently, (47) and (49) imply that $n_1 = nm - 1$ if $de_1 = e_1$ (since $|S'| \le 2nm - 2$), and that $n_1 = mn - \ell n$ if $de_1 = -e_1$ (since $|S'| < 2mn - \ell n$). However, in the former case, $e_2$ has the desired multiplicity in $S$, while in the latter case, $n_2 = 2mn - \ell n - 1 - n_1 = mn - 1$, and thus $de_1 + e_2 = -e_1 + e_2$ has the desired multiplicity, completing the proof. □

## 6. Proof of the corollary

Let $G = C_{n_1} \oplus C_{n_2}$, with $1 < n_1 \,|\, n_2$, and suppose that, for every prime divisor $p$ of $n_1$, the group $C_p \oplus C_p$ has Property **B**. The assertion that $C_{n_1} \oplus C_{n_1}$ has Property **B** follows from the Theorem and from the following two statements:

(a) For every $n \in [2, 10]$, the group $C_n \oplus C_n$ has Property **B**: for $n \le 6$ this may be found in [2, Proposition 4.2]; the cases $n \in \{8, 9, 10\}$ (and more) are settled in [**?**].

(b) If $n \ge 6$ and $C_n \oplus C_n$ has Property **B**, then $C_{2n} \oplus C_{2n}$ has Property **B** (see [2, Theorem 8.1]).

Since $C_{n_1} \oplus C_{n_1}$ has Property **B**, the characterization of the minimal zero-sum sequences over $G$ of length $\mathsf{D}(G)$ now follows from [**?**, Theorem 3.3].$\square$

**Acknowledgments.** This work was supported partially by NSFC with grant no. 10671101 and by the 973 Project with grant no 9732006CB805904. It was further supported by the Austrian Science Fund FWF (Project Number M1014-N13).

## References

[1] A. Bialostocki and P. Dierker, *On the Erdős-Ginzburg-Ziv theorem and the Ramsey numbers for stars and matchings*, Discrete Math. **110** (1992), 1 – 8.

[2] W. Gao and A. Geroldinger, *On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$*, Integers **3** (2003), Paper A08, 45p.

[3] ———, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337 – 369.

[4] W. Gao, A. Geroldinger, and W.A. Schmid, *Inverse zero-sum problems*, Acta Arith. **128** (2007), 245 – 279.

[5] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, 700p, Chapman & Hall/CRC, 2006.

[6] D.J. Grynkiewicz, *On a conjecture of Hamidoune for subsequence sums*, Integers **5(2)** (2005), Paper A07, 11p.

[7] Y. ould Hamidoune, *Subsequence sums*, Comb. Probab. Comput. **12** (2003), 413 – 425.

[8] M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
*E-mail address*: `wdgao_1963@yahoo.com.cn`

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria
*E-mail address*: `alfred.geroldinger@uni-graz.at, diambri@hotmail.com`