Reprint from

ISSN 2220-5438

Moscow Journal of Combinatorics and Number Theory

URSS

МФТИ

Moscow Journal of Combinatorics and Number Theory

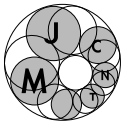
Volume 5 • Issue 3

2015

URSS

Volume 5 • Issue 3 2015

Moscow Journal
of Combinatorics
and Number Theory
2015, vol. 5, iss. 3,
pp. 3–58, [pp. 73–128]



On products of k atoms II

Alfred Geroldinger (Graz), David J. Grynkiewicz (Memphis), and
Pingzhi Yuan (Guangzhou)

Abstract: Let H be a Krull monoid with class group G such that every class contains a prime divisor (for example, rings of integers in algebraic number fields or holomorphy rings in algebraic function fields). For $k \in \mathbb{N}$, let $\mathcal{U}_k(H)$ denote the set of all $m \in \mathbb{N}$ with the following property: There exist atoms $u_1, \ldots, u_k, v_1, \ldots, v_m \in H$ such that $u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_m$. Furthermore, let $\lambda_k(H) = \min \mathcal{U}_k(H)$ and $\rho_k(H) = \sup \mathcal{U}_k(H)$. The sets $\mathcal{U}_k(H) \subset \mathbb{N}$ are intervals which are finite if and only if G is finite. Their minima $\lambda_k(H)$ can be expressed in terms of $\rho_k(H)$. The invariants $\rho_k(H)$ depend only on the class group G, and in the present paper they are studied with new methods from Additive Combinatorics.

Keywords: non-unique factorizations, sets of lengths, Krull monoids, zero-sum sequences

AMS Subject classification: 11B30, 11R27, 13A05, 13F05, 20M13

Received: 17.03.2015; **revised:** 08.07.2015

1. Introduction

Let H be a (commutative and cancelative) monoid. If an element $a \in H$ has a factorization $a = u_1 \cdot \ldots \cdot u_k$ into atoms $u_1, \ldots, u_k \in H$, then k is called the length of the factorization, and the set $\mathsf{L}(a)$ of all possible lengths is called the set of lengths

of a. For $k \in \mathbb{N}$, let $\mathcal{U}_k(H)$ denote the set of all $m \in \mathbb{N}$ with the following property: There exist atoms $u_1, \ldots, u_k, v_1, \ldots, v_m \in H$ such that $u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_m$. Thus $\mathcal{U}_k(H)$ is the union of all sets of lengths containing k. Sets of lengths (and all invariants derived from them, such as their unions) are the most investigated invariants in factorization theory. The sets $\mathcal{U}_k(H)$ were introduced by S.T. Chapman and W.W. Smith in Dedekind domains (see [14]) and since then have been studied in settings ranging from numerical monoids to Mori domains, including monoids of modules (see [3, 6, 10, 18, 24]). Their suprema $\rho_k(H) = \sup \mathcal{U}_k(H)$ and their minima $\lambda_k(H) = \min \mathcal{U}_k(H)$ have received special attention. Indeed, the invariants $\rho_k(H)$ were first studied in the 1980s for rings of integers in algebraic number fields (see [16, 36]). The supremum over all $\rho_k(H)/k$ is called the elasticity of H, whose investigation was a key topic in early factorization theory (see [1] for a survey, or to pick a few from many, see [12, Problem 38] and [2, 8, 11, 13, 32]).

In the present paper, we focus on Krull monoids having the property that every class in the class group contains a prime divisor. In Section 2 we present the necessary background and Proposition 4 gathers the present state of the art. Among others, if H is such a Krull monoid with class group G and $2 < |G| < \infty$, then $\mathcal{U}_k(H) \subset \mathbb{N}$ is a finite interval, hence $\mathcal{U}_k(H) = [\lambda_k(H), \rho_k(H)]$, and its minimum $\lambda_k(H)$ can be expressed in terms of $\rho_k(H)$. Moreover, $\rho_k(H)$ depends only on the class group G and hence it can be studied with methods from Additive Combinatorics. This is the starting point for the remainder of the paper.

Let $\mathsf{D}(G)$ denote the Davenport constant of G and set $\rho_k(G) = \rho_k(H)$. Then, for every $k \in \mathbb{N}$, we have $\rho_{2k}(G) = k\mathsf{D}(G)$ and there is the crucial inequality (see Lemma 1)

$$1 + k\mathsf{D}(G) \le \rho_{2k+1}(G) \le k\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor .$$

In Section 3 we analyze this inequality, formulate two conjectures (Conjecture 1), and outline the program of the paper in greater detail. Theorem 1 provides a list of groups for which $\rho_{2k+1}(G)$ equals the upper bound in the above inequality for all $k \in \mathbb{N}$. If G is cyclic, then $\rho_{2k+1}(G)$ equals the lower bound for all $k \in \mathbb{N}$ (this was proved in [20]). Theorem 2 characterizes all groups G of rank two for which $\rho_3(G)$ equals the upper bound. This result is based on the recent characterization of all minimal zero-sum sequences of maximal length in groups of rank two (see Main Proposition 7 on p. 27).

2. Unions of sets of lengths in Krull monoids: Background

Let $\mathbb{N}$ denote the set of positive integers and set $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, we denote by $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$ the discrete interval. By a monoid, we mean a commutative semigroup with identity which satisfies the cancellation law (that is, if a, b, c are elements of the monoid with $ab = ac$, then $b = c$ follows). The multiplicative semigroup of non-zero elements of an integral domain is a monoid.

Let G be an abelian group, and let $A,\ B \subset G$ be subsets. Then $\langle A \rangle \subset G$ is the subgroup generated by A, $-A = \{-a \mid a \in A\}$, and $A+B = \{a+b \mid a \in A, b \in B\}$ is the sumset of A and B. Furthermore, A is a generating set of G if $\langle A \rangle = G$, and A is a basis of G if all elements of A are nonzero and $G = \oplus_{a \in A} \langle a \rangle$.

Monoids and Sets of Lengths. A monoid F is free abelian, with basis $P \subset F$ and we write $F = \mathcal{F}(P)$, if every $a \in F$ has a unique representation of the form

$$a = \prod_{p \in P} p^{\mathsf{v}_p(a)} \quad \text{with} \quad \mathsf{v}_p(a) \in \mathbb{N}_0 \ \text{ and } \ \mathsf{v}_p(a) = 0 \ \text{ for almost all } \ p \in P\,.$$

Let H be a monoid. We denote by $H^\times$ the set of invertible elements of H and by $\mathsf{q}(H)$ a quotient group of H. For a subset $H_0 \subset H$, we denote by $[H_0] \subset H$ the submonoid generated by H_0. Let $a, b \in H$. We say that a divides b (and we write $a \mid b$) if there is an element $c \in H$ such that $b = ac$. We denote by $\mathcal{A}(H)$ the set of atoms (irreducible elements) of H. If $a = u_1 \cdot \ldots \cdot u_k$, where $k \in \mathbb{N}$ and $u_1, \ldots, u_k \in \mathcal{A}(H)$, then k is called the length of the factorization and $\mathsf{L}(a) = \{k \in \mathbb{N} \mid a \text{ has a factorization of length } k\} \subset \mathbb{N}$ is the set of lengths of a. For convenience, we set $\mathsf{L}(a) = \{0\}$ if $a \in H^\times$. Furthermore, we denote by

$$\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\} \quad \text{the system of sets of lengths of} \quad H\,.$$

Next we define the central concept of this paper. Let $k \in \mathbb{N}$ and suppose that $H \neq H^\times$. Then

$$\mathcal{U}_k(H) \ = \bigcup_{a \in H,\, k \in \mathsf{L}(a)} \mathsf{L}(a)$$

is the union of all sets of lengths containing k. Thus, $\mathcal{U}_k(H)$ is the set of all $m \in \mathbb{N}$ such that there are atoms $u_1, \ldots, u_k, v_1, \ldots, v_m$ with $u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_m$.

Finally, we define

$$\rho_k(H) = \sup \mathcal{U}_k(H) \quad \text{and} \quad \lambda_k(H) = \min \mathcal{U}_k(H) \,.$$

Krull monoids. A monoid homomorphism $\varphi\colon H \to F$ is said to be a divisor homomorphism if $\varphi(a) \mid \varphi(b)$ in F implies that $a \mid b$ in H for all $a, b \in H$. A monoid H is said to be a Krull monoid if one of the following equivalent properties is satisfied (see [23, Theorem 2.4.8] or [31]).

(a) H is completely integrally closed and satisfies the ascending chain condition on divisorial ideals.

(b) H has a divisor homomorphism into a free abelian monoid.

(c) H has a divisor theory: this is a divisor homomorphism $\varphi\colon H \to F = \mathcal{F}(P)$ into a free abelian monoid such that for each $p \in P$ there is a finite set $E \subset H$ with $p = \gcd\big(\varphi(E)\big)$.

Let H be a Krull monoid. Then every non-unit has a factorization into atoms, and all sets of lengths are finite. A divisor theory $\varphi\colon H \to F = \mathcal{F}(P)$ is essentially unique, and the class group $\mathcal{C}(H) = \mathrm{q}(F)/\mathrm{q}(\varphi(H))$ depends only on H. It will be written additively, and we say that every class contains a prime divisor if, for every $g \in \mathcal{C}(H)$, there is a $p \in P$ with $p \in g$.

An integral domain R is a Krull domain if and only if its multiplicative monoid $R \setminus \{0\}$ is a Krull monoid, and Property (a) shows that a noetherian domain is Krull if and only if it is integrally closed. Rings of integers, holomorphy rings in algebraic function fields, and regular congruence monoids in these domains are Krull monoids with finite class group such that every class contains a prime divisor (see [23, Section 2.11]). Monoid domains and power series domains that are Krull are discussed in [29, 33, 34]. For monoids of modules which are Krull we refer the reader to [3, 5, 17].

Main portions of the arithmetic of a Krull monoid—in particular, all questions dealing with sets of lengths—can be studied in the monoid of zero-sum sequences over its class group. We provide the relevant concepts and summarize the connection in the next subsection.

Transfer homomorphisms and Zero-sum sequences. Let G be an additively written abelian group, $G_0 \subset G$ a subset, and let $\mathcal{F}(G_0)$ be the free abelian monoid with basis G_0. According to the tradition of combinatorial number theory, the elements

of $\mathcal{F}(G_0)$ are called *sequences* over G_0. If $S = g_1 \cdot \ldots \cdot g_l$, where $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G_0$, then $\sigma(S) = g_1 + \ldots + g_l$ is called the sum of S, and the monoid

$$\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \sigma(S) = 0\} \subset \mathcal{F}(G_0)$$

is called the *monoid of zero-sum sequences* over G_0 (or the *block monoid* over G_0). Since the embedding $\mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$ is a divisor homomorphism, Property (b) shows that $\mathcal{B}(G_0)$ is a Krull monoid. The monoid $\mathcal{B}(G)$ is factorial if and only if $|G| \le 2$. If $|G| \ge 3$, then $\mathcal{B}(G)$ is a Krull monoid with class group isomorphic to G and every class contains precisely one prime divisor.

For every arithmetical invariant $*(H)$ defined for a monoid H, it is usual to write $*(G)$ instead of $*(\mathcal{B}(G))$ (although this is an abuse of language, but there will be no danger of confusion). In particular, we set $\mathcal{A}(G) = \mathcal{A}(\mathcal{B}(G))$, $\mathcal{L}(G) = \mathcal{L}(\mathcal{B}(G))$, $\mathcal{U}_k(G) = \mathcal{U}_k(\mathcal{B}(G))$, $\rho_k(G) = \rho_k(\mathcal{B}(G))$, and $\lambda_k(G) = \lambda_k(\mathcal{B}(G))$.

The next two propositions reveal the universal role of monoids of zero-sum sequences.

PROPOSITION 1. *Let H be a Krull monoid with class group G such that every class contains a prime divisor. Then there is a transfer homomorphism $\beta\colon H \to \mathcal{B}(G)$. In particular, for every $k \in \mathbb{N}$, we have*

$$\mathcal{U}_k(H) = \mathcal{U}_k(G)\,,\ \lambda_k(H) = \lambda_k(G)\,, \quad \text{and} \quad \rho_k(H) = \rho_k(G)\,.$$

PROOF. See [23, Theorem 3.4.10]. □

Whereas the proof of the above result is quite straightforward, there are recent deep results showing that there are non-Krull monoids (even non-commutative rings) which allow transfer homomorphisms to monoids of zero-sum sequences. The proof of part 1 can be found in [41, Theorem 1.1] (see [4] for related results of this flavor) and part 2 in [24, Theorem 5.8].

PROPOSITION 2.

1) *Let $\mathcal{O}$ be a holomorphy ring in a global field K, A a central simple algebra over K, and H a classical maximal $\mathcal{O}$-order of A such that every stably free left R-ideal is free. Then $\mathcal{U}_k(H) = \mathcal{U}_k(G)$ for every $k \in \mathbb{N}$, where G is a ray class group of $\mathcal{O}$ and hence finite abelian.*

2) *Let H be a seminormal order in a holomorphy ring of a global field with principal order $\widehat{H}$ such that the natural map $\mathfrak{X}(\widehat{H}) \to \mathfrak{X}(H)$ is bijective and there is an isomorphism $\overline{\vartheta}\colon \mathcal{C}_v(H) \to \mathcal{C}_v(\widehat{H})$ between the v-class groups. Then $\mathcal{U}_k(H) = \mathcal{U}_k(G)$ for every $k \in N$, where $G = \mathcal{C}_v(H)$ is finite abelian.*

We need some more notation for sequences over abelian groups (it is consistent with [23, 26, 30]). As before, we fix an additive abelian group G and a subset $G_0 \subset G$. Let

$$S = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G_0} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G_0)\,,$$

be a sequence over G_0 (whenever we write a sequence in this way, we tacitly assume that $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G_0$). We set $-S = (-g_1) \cdot \ldots \cdot (-g_l)$ and $\mathsf{v}_{G_1}(S) = \sum_{g \in G_1} \mathsf{v}_g(S)$ for a subset $G_1 \subset G_0$. We call $\mathsf{v}_g(S)$ the *multiplicity* of g in S,

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

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

$$\sigma(S) = \sum_{i=1}^{l} g_i \text{ the } \textit{sum} \text{ of } S\,, \quad \text{and}$$

$$\Sigma(S) = \Big\{ \sum_{i \in I} g_i \mid \varnothing \neq I \subset [1, l] \Big\} \text{ the } \textit{set of subsums} \text{ of } S\,.$$

For a sequence $T \in \mathcal{F}(G_0)$, we write $\gcd(S, T) \in \mathcal{F}(G_0)$ for the maximal length subsequence dividing S and T. We write $T \mid S$ to indicate that T is a subsequence of S, in which case $ST^{-1} = T^{-1}S$ denotes the subsequence obtained from S by removing the terms from T. The sequence S is said to be

- *zero-sum free* if $0 \notin \Sigma(S)$,
- a *zero-sum sequence* if $\sigma(S) = 0$,
- a *minimal zero-sum sequence* if it is a nontrivial zero-sum sequence and every proper subsequence is zero-sum free.

Clearly, the minimal zero-sum sequences are precisely the atoms of the monoid $\mathcal{B}(G_0)$, and they play a central role in our investigations. Now suppose that G is

finite. For $n \in \mathbb{N}$, let C_n denote a cyclic group with n elements. If $|G| > 1$, then we have

$$G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}, \quad \text{and we set} \quad \mathsf{d}^*(G) = \sum_{i=1}^{r} (n_i - 1) \quad \text{and} \quad \mathsf{D}^*(G) = \mathsf{d}^*(G) + 1,$$

where $r = \mathsf{r}(G) \in \mathbb{N}$ is the *rank* of G, $n_1, \ldots, n_r \in \mathbb{N}$ are integers with $1 < n_1 \mid \ldots \mid n_r$ and $n_r = \exp(G)$ is the exponent of G. If $|G| = 1$, then $\mathsf{r}(G) = 0$, $\exp(G) = 1$, and $\mathsf{d}^*(G) = 0$. The *Davenport constant* $\mathsf{D}(G)$ of G is the maximal length of a minimal zero-sum sequence over G, thus

$$\mathsf{D}(G) = \max\big\{ |U| \ \big| \ U \in \mathcal{A}(G) \big\} \in \mathbb{N}.$$

(note that $\mathcal{A}(G)$ is finite). In other words, $\mathsf{D}(G)$ is the smallest integer ℓ such that every sequence S over G of length $|S| \ge \ell$ has a nontrivial zero-sum subsequence. We denote by $\mathsf{d}(G)$ the maximal length of a zero-sum free sequence, and clearly we have $1 + \mathsf{d}(G) = \mathsf{D}(G)$. The next proposition gathers some facts on the Davenport constant which we will use without further mention. A proof can be found in [23, Chapter 5].

PROPOSITION 3. *Let G be a finite abelian group.*

1) $\mathsf{D}^*(G) \le \mathsf{D}(G) \le |G|$.

2) *If G is a p-group or $\mathsf{r}(G) \le 2$, then $\mathsf{D}^*(G) = \mathsf{D}(G)$.*

3) $\mathsf{D}(G) = 1$ *if and only if* $|G| = 1$, $\mathsf{D}(G) = 2$ *if and only if* $|G| = 2$, *and* $\mathsf{D}(G) = 3$ *if and only if G is cyclic of order* $|G| = 3$ *or isomorphic to* $C_2 \oplus C_2$.

Note that 1) is elementary and that 3) is a simple consequence of 1) and 2). There are more groups G with $\mathsf{D}^*(G) = \mathsf{D}(G)$ (beyond the ones listed in 2)), but we do not have equality in general (see [25, 40]).

The next proposition gathers the state of the art on unions of sets of lengths.

PROPOSITION 4. *Let H be a Krull monoid with class group G such that every class contains a prime divisor.*

1) *If* $|G| \le 2$, *then* $\mathcal{U}_k(H) = \{k\}$ *for all* $k \in \mathbb{N}$.

2) *If* $2 < |G| < \infty$, *then, for all* $k \in \mathbb{N}$, *we have* $\mathcal{U}_k(H) = [\lambda_k(G), \rho_k(G)]$ *and*

$$\lambda_{k\mathsf{D}(G)+j}(H) = \begin{cases} 2k & \text{for} \quad j = 0 \\ 2k+1 & \text{for} \quad j \in [1, \rho_{2k+1}(G) - k\mathsf{D}(G)] \\ 2k+2 & \text{for} \quad j \in [\rho_{2k+1}(G) - k\mathsf{D}(G) + 1, \mathsf{D}(G) - 1] \,, \end{cases}$$

provided that $k\mathsf{D}(G) + j \ge 1$.

3) *If* G *is infinite, then* $\mathcal{U}_k(H) = \mathbb{N}_{\ge 2}$ *for all* $k \ge 2$.

PROOF. 1) is classical, for 2) see [18, Theorem 4.1] and [22, Section 3.1], and 3) follows from [23, Theorem 7.4.1]. □

Let H be a Krull monoid with class group G such that every class contains a prime divisor, or any of the monoids in Proposition 2. Then Propositions 1, 2, and 4 show that, for a complete description of the sets $\mathcal{U}_k(H)$ of H, it remains to study the invariants $\rho_k(G)$ of an associated monoid of zero-sum sequences. We proceed with this goal in mind.

3. The extremal cases in the crucial inequality

We start with a simple and well-known lemma. For convenience, we provide its short proof.

LEMMA 1. *Let* G *be a finite abelian group with* $|G| \ge 3$, *and let* $k, l \in \mathbb{N}$.

1) $k + l \le \rho_k(G) + \rho_l(G) \le \rho_{k+l}(G)$.

2) $\rho_{2k}(G) = k\mathsf{D}(G)$ *and*

$$1 + k\mathsf{D}(G) \le \rho_{2k+1}(G) \le k\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor . \tag{3.1}$$

In particular, if $\mathsf{D}(G) = 3$, *then* $\rho_{2k+1}(G) = k\mathsf{D}(G) + 1$.

3) *If* $\rho_{2k+1}(G) \ge m$ *for some* $m \in \mathbb{N}$ *and* $l \ge k$, *then* $\rho_{2l+1}(G) \ge m + (l-k)\mathsf{D}(G)$.

PROOF.

1) By definition, we have $\rho_m(G) \ge m$ for each $m \in \mathbb{N}$ and hence $k+l \le \rho_k(G) + \rho_l(G)$. Since $\mathcal{U}_k(G) + \mathcal{U}_l(G) \subset \mathcal{U}_{k+l}(G)$, it follows that

$$\rho_k(G) + \rho_l(G) = \sup \mathcal{U}_k(G) + \sup \mathcal{U}_l(G) \le \sup \mathcal{U}_{k+l}(G) = \rho_{k+l}(G) .$$

2) A simple counting argument shows that $\rho_k(G) \le k\mathsf{D}(G)/2$; furthermore, if $U = g_1 \cdot \ldots \cdot g_{\mathsf{D}(G)} \in \mathcal{A}(G)$, then $(-U)^k U^k = \prod_{i=1}^{\mathsf{D}(G)} \big((-g_i)g_i\big)^k$, whence $k\mathsf{D}(G) \le \rho_{2k}(G)$ and thus $\rho_{2k}(G) = k\mathsf{D}(G)$ (details can be found in [22, Theorem 2.3.1]). Using this and 1), we infer that

$$1 + \mathsf{kD}(G) = \rho_1(G) + \rho_{2k}(G) \le \rho_{2k+1}(G) \le \frac{(2k+1)\mathsf{D}(G)}{2} .$$

Clearly, $\mathsf{D}(G) = 3$ implies that equality holds in both inequalities above.

3) By 1) and 2), it follows that

$$\rho_{2l+1}(G) \ge \rho_{2k+1}(G) + \rho_{2(l-k)}(G) \ge m + (l-k)\mathsf{D}(G) . \qquad \square$$

Our starting point is the crucial inequality (3.1). We conjecture that cyclic groups are the only groups where equality holds on the left hand side, whereas, for all noncyclic groups, there is a $k^* \in \mathbb{N}$ such that equality holds on the right hand side for all $k \ge k^*$. We are going to outline this in greater detail (see Conjecture 1 and Corollary 1).

PROPOSITION 5. *Let G be a finite abelian group with $\mathsf{D}(G) \ge 4$.*

1) *If there exist $U \in \mathcal{A}(G)$ and $S_1, S_2 \in \mathcal{F}(G)$ such that*

$$U = S_1 S_2 , \ |U| = \mathsf{D}(G) \quad \text{and} \quad \Sigma(S_1) \cup \Sigma(-S_2) \ne G \setminus \{0\} ,$$

then $\rho_3(G) > \mathsf{D}(G) + 1$.

2) *If G is cyclic, then the property in 1) does not hold and $\rho_{2k+1}(G) = k\mathsf{D}(G) + 1$ for each $k \in \mathbb{N}$.*

3) *The following conditions are equivalent.*

   a) *There is a* $k^* \in \mathbb{N}$ *such that*

$$\rho_{2k^*+1}(G) = k^*\mathsf{D}(G) + \Big\lfloor \frac{\mathsf{D}(G)}{2} \Big\rfloor .$$

   b) *There is a* $k^* \in \mathbb{N}$ *such that*

$$\rho_{2k+1}(G) = k\mathsf{D}(G) + \Big\lfloor \frac{\mathsf{D}(G)}{2} \Big\rfloor \qquad \textit{for every } k \ge k^* .$$

PROOF.

1) Let S_1, S_2, and U have the above property. Then we choose an element

$$g \in G \setminus \big(\Sigma(S_1) \cup \Sigma(-S_2) \cup \{0\}\big) .$$

Since $g \notin \Sigma(S_1)$, the sequence $(-S_1)g$ is zero-sum free and $U_2 = (-S_1)g \cdot \big(\sigma(S_1) - g\big) \in \mathcal{A}(G)$. Similarly, it follows that $U_3 = (-S_2)(-g)\big(\sigma(S_2) + g\big) \in \mathcal{A}(G)$. Since $-\big(\sigma(S_1) - g\big) = \sigma(S_2) + g$ in view of $0 = \sigma(U) = \sigma(S_1) + \sigma(S_2)$, the product UU_2U_3 has a factorization into $|S_1| + |S_2| + 2 = \mathsf{D}(G) + 2$ atoms of length 2.

2) Suppose that G is cyclic of order $|G| = n$. Then [20, Theorem 5.3] implies that $\rho_{2k+1}(G) = k\mathsf{D}(G) + 1$ for each $k \in \mathbb{N}$ (see [22, Theorem 5.3.1] for a slightly modified proof). Clearly, every $U \in \mathcal{A}(G)$ of length $|U| = |G|$ has the form $U = g^n$ for some $g \in G$ with $\mathrm{ord}(g) = n$. Thus there are no S_1 and S_2 with the given properties.

3) (a) $\Rightarrow$ (b) If $l \in \mathbb{N}$, then Lemma 1 implies that

$$\begin{aligned}(k^*+l)\mathsf{D}(G) + \Big\lfloor \frac{\mathsf{D}(G)}{2} \Big\rfloor &\ge \rho_{2(k^*+l)+1}(G) \ge \rho_{2k^*+1}(G) + \rho_{2l}(G) = \\ &= \Big(k^*\mathsf{D}(G) + \Big\lfloor \frac{\mathsf{D}(G)}{2} \Big\rfloor\Big) + l\mathsf{D}(G) = (k^*+l)\mathsf{D}(G) + \Big\lfloor \frac{\mathsf{D}(G)}{2} \Big\rfloor .\end{aligned}$$

(b) $\Rightarrow$ (a) This is obvious. □

CONJECTURE 1. Let G be a noncyclic finite abelian group with $\mathsf{D}(G) \ge 4$. Then the following two conditions hold:

C1. There exist $U \in \mathcal{A}(G)$ and $S_1, S_2 \in \mathcal{F}(G)$ such that

$$U = S_1 S_2\,,\ |U| = \mathsf{D}(G)\,, \quad \text{and} \quad \Sigma(S_1) \cup \Sigma(-S_2) \neq G \setminus \{0\}\,.$$

C2. There exists some $k^* \in \mathbb{N}$ such that

$$\rho_{2k+1}(G) = k\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor \qquad \text{for each} \quad k \ge k^*\,.$$

In Proposition 6, we show that Conjecture **C1** holds for groups G with $\mathsf{D}(G) = \mathsf{D}^*(G)$. All results of the present paper support Conjecture **C2**. In particular, Theorem 1 provides groups satisfying **C2** with $k^* = 1$, and Theorem 2 shows that **C2** need not hold with $k^* = 1$.

We start with some consequences of the above conjecture. The Characterization Problem is a central topic in factorization theory for Krull monoids (we refer to [23, Sections 7.1–7.3] for general information, and to [7, 27, 37, 38] for recent progress). The Characterization Problem studies the question whether or not the system of sets of lengths of a Krull monoid, which has a prime divisor in every class, determines the class group. Thus, if G and G' are two finite abelian groups with $\mathsf{D}(G) \ge 4$ such that $\mathcal{L}(G) = \mathcal{L}(G')$, does it follow that G and G' are isomorphic? The answer is affirmative (among others) for groups of rank at most two, and there are no counter examples so far. Corollary 1 offers a simple proof in case of cyclic groups which relies only on the $\rho_k(\cdot)$-invariants.

COROLLARY 1. *Suppose that Conjecture* **C1** *holds.*

1) *Let H be a Krull monoid with finite class group G such that every class contains a prime divisor and suppose that $\mathsf{D}(G) \ge 4$. Then the following statements are equivalent:*

   (a) *G is cyclic.*

   (b) *$\rho_{2k+1}(H) = k\mathsf{D}(G) + 1$ for every $k \in \mathbb{N}$.*

   (c) *$\rho_3(H) = \mathsf{D}(G) + 1$.*

2) *Let G be cyclic with $\mathsf{D}(G) \ge 4$. If G' is a finite abelian group with $\mathcal{L}(G) = \mathcal{L}(G')$, then $G \cong G'$.*

PROOF.

- By Proposition 1, it suffices to consider $\rho_k(G)$ for all $k \in \mathbb{N}$. The implication (a) $\Rightarrow$ (b) follows from Proposition 5, statement 2), and (b) $\Rightarrow$ (c) is obvious.

  (c) $\Rightarrow$ (a) If G would be noncyclic, then **C1** and Proposition 5, statement 1) would imply that $\rho_3(G) > \mathsf{D}(G) + 1$.

- Suppose that $\mathcal{L}(G) = \mathcal{L}(G')$. Then

$$\mathsf{D}(G)=\rho_2(G)=\rho_2(G')=\mathsf{D}(G') \quad \text{and} \quad \mathsf{D}(G')+1=\mathsf{D}(G)+1=\rho_3(G)=\rho_3(G').$$

  Thus 1) implies that G' is cyclic, and since $|G| = \mathsf{D}(G) = \mathsf{D}(G') = |G'|$, G and G' are isomorphic. □

For Conjecture **C1** and for Corollary 1, the assumption $\mathsf{D}(G) \ge 4$ is crucial. By Proposition 3, the groups C_3 and $C_2 \oplus C_2$ are the only groups (up to isomorphism) whose Davenport constant is equal to three. The group $C_2 \oplus C_2$ does not satisfy **C1**, $\rho_3(C_2 \oplus C_2) = 4$ (in contrast to Corollary 1, statement 1)), and $\mathcal{L}(C_3) = \mathcal{L}(C_2 \oplus C_2)$ (see [23, Theorem 7.3.2]).

The only groups G with $\mathsf{D}(G) > \mathsf{D}^*(G)$, for which the precise value of $\mathsf{D}(G)$ is known, are groups of the form $C_2^4 \oplus C_{2n}$. We verify Conjecture **C1** for them too.

PROPOSITION 6. *Let G be a noncyclic finite abelian group with $\mathsf{D}(G) \ge 4$.*

1) *Let $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ where $1 < n_1 \mid \ldots \mid n_r$ and suppose that there is some $s \in [1, r-1]$ such that $n_s < n_{s+1} = \ldots = n_r$. Then $\rho_3(G) \ge \mathsf{D}^*(G) + n_s$.*

2) *If $\mathsf{D}(G) = \mathsf{D}^*(G)$, then Conjecture* **C1** *holds.*

3) *If $G = C_2^4 \oplus C_{2n}$ with $n \ge 70$, then Conjecture* **C1** *holds.*

PROOF. Let $\{e_1, \ldots, e_r\}$ be a basis of G with $\mathrm{ord}(e_i) = n_i$ for $i \in [1, r]$ and $n_1 \mid \ldots \mid n_r$. Set $e_0 = e_1 + \ldots + e_{r-1}$.

1) Let

$$\begin{aligned}
U_1 &= e_1^{n_1-1} \cdot \ldots \cdot e_r^{n_r-1}(e_0 + e_r),\\
U_2 &= (-e_1)^{n_1-1} \cdot \ldots \cdot (-e_{s-1})^{n_{s-1}-1}(-e_s + e_r)^{n_s-1}(-e_{s+1})^{n_{s+1}-1} \cdot \ldots\\
&\quad \ldots \cdot (-e_r)^{n_r-1}(-e_0 - n_s e_r),\\
U_3 &= (-e_s)^{n_s-1}(e_s - e_r)^{n_s-1}(-e_0 - e_r)(e_0 + n_s e_r).
\end{aligned}$$

Then the U_i are each atoms, and clearly $U_1U_2U_3$ is a product of

$$\frac{1}{2}|U_1U_2U_3| = \frac{1}{2}(2\mathsf{D}^*(G) + 2n_s) = \mathsf{D}^*(G) + n_s$$

atoms of length 2. The assertion follows.

2) We consider the sequence

$$U = e_1^{n_1-1} \cdot \ldots \cdot e_r^{n_r-1} e_0\,,$$

and distinguish two cases.

First, suppose that $n_r > 2$. We set $S_1 = e_r^{n_r-1}$ and $S_2 = S_1^{-1}U$. Then $-e_1 - \ldots - e_{r-1} + e_r \notin \Sigma(S_1)$ and $e_1 + \ldots + e_{r-1} - e_r \notin \Sigma(S_2)$ because $-e_r \neq e_r$.

Second, suppose that $n_r = 2$. Then G is an elementary 2-group and $r \geq 3$ (as $\mathsf{d}(G) \geq 3$). We set $S_1 = e_1e_2$ and $S_2 = e_3 \cdot \ldots \cdot e_r e_0$. Then $e_2 + e_3 \notin \Sigma(S_1) \cup \Sigma(-S_2)$.

3) Suppose that $\mathrm{ord}(e_1) = \ldots = \mathrm{ord}(e_4) = 2$ and $\mathrm{ord}(e_5) = 2n$ with $n \geq 70$. If n is even, then $\mathsf{D}(G) = \mathsf{D}^*(G)$ by [15, Theorem 5.8], and the assertion follows from 2. Suppose that n is odd. Then $\mathsf{D}(G) = \mathsf{D}^*(G) + 1$ by [15, Theorem 5.8]. By [28, Theorem 4], the sequence

$$\begin{aligned}
U = {} & (e_1 + e_5)(e_2 + e_5)(e_3 + e_5)(e_4 + e_5)(e_0 - e_1)(e_0 - e_2)(e_0 - e_3) \cdot\\
& (e_0 - e_4 + e_5)^{2n-3}(-e_5)
\end{aligned}$$

is a minimal zero-sum sequence of length $|U| = \mathsf{D}(G)$. We set

$$S_1 = (e_0 - e_4 + e_5)^{2n-3}(-e_5) \quad \text{and} \quad S_2 = S_1^{-1}U.$$

Then the element $e_1 + e_2 + e_3 - 2e_5 \notin \Sigma(S_1)$, and we assert that its inverse—namely $e_1 + e_2 + e_3 + 2e_5 = e_0 - e_4 + e_5$—does not lie in $\Sigma(S_2)$. If there would be a subsequence T of S_2 with $\sigma(T) = e_1 + e_2 + e_3 + 2e_5$, then we would have $|T| = 2$. But none of the subsequences of S_2 of length two has sum $e_1 + e_2 + e_3 + 2e_5$, a contradiction. □

4. Inductive Bounds

It is the aim of this section to prove the following result which confirms Conjecture **C2** (with $k^* = 1$) for the groups G having the form below and satisfying $\mathsf{D}(G) = \mathsf{D}^*(G)$.

THEOREM 1. *Let H be a Krull monoid with finite class group G such that every class contains a prime divisor. Suppose that $G = C_{n_1}^{s_1} \oplus \ldots \oplus C_{n_r}^{s_r}$ where $1 < n_1 \mid \ldots \mid n_r$ and $s_i \ge 2$ for all $i \in [1, r]$. Then*

$$\rho_{2k+1}(H) \ge \mathsf{D}^*(G) + \Big\lfloor \frac{\mathsf{D}^*(G)}{2} \Big\rfloor + (k-1)\mathsf{D}(G) \quad \text{for every } k \ge 1 \,.$$

In particular, if $\mathsf{D}(G) = \mathsf{D}^*(G)$, then $\rho_{2k+1}(H) = k\mathsf{D}(G) + \Big\lfloor \frac{\mathsf{D}(G)}{2} \Big\rfloor$ for every $k \ge 1$.

Theorem 1 has the following straightforward consequences. Let $n \ge 2$. It is known that $\mathsf{D}(C_n^r) = \mathsf{D}^*(C_n^r)$ for $r \in [1, 2]$ and if $\mathsf{D}(C_n^r) = \mathsf{D}^*(C_n^r)$ holds for some $r \ge 3$, then $\mathsf{D}(C_n^s) = \mathsf{D}^*(C_n^s)$ for all $s \in [1, r]$. The standing conjecture is that $\mathsf{D}(C_n^r) = \mathsf{D}^*(C_n^r)$ for all $r \in \mathbb{N}$.

COROLLARY 2. *Let $G = C_n^r$, where $n \ge 2$ and $r \ge 1$, and suppose that $\mathsf{D}(G) = \mathsf{D}^*(G)$. Then, for every $k \ge 1$, we have*

$$\rho_{2k+1}(G) = \begin{cases} k\mathsf{D}(G) + 1 & r = 1 \\ k\mathsf{D}(G) + \Big\lfloor \dfrac{\mathsf{D}(G)}{2} \Big\rfloor & r \ge 2 \,. \end{cases}$$

PROOF. For $r = 1$, this follows from Proposition 5 2). For $r \ge 2$, it follows from Theorem 1. □

COROLLARY 3. *Let $G = C_{q_1}^{s_1} \oplus \ldots \oplus C_{q_r}^{s_r}$ be a p-group where $q_1, \ldots, q_r$ are powers of a fixed prime and $s_1, \ldots, s_r \in \mathbb{N}_{\ge 2}$. Then*

$$\rho_{2k+1}(G) = k\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor \quad \text{for every } k \ge 1 .$$

PROOF. Since G is a p-group, we have $\mathsf{D}(G) = \mathsf{D}^*(G)$ by Proposition 3, and hence the assertion follows from Theorem 1. □

We start with the preparations for the proof of Theorem 1. Let G be a finite abelian group. The inequality $\rho_3(G) \ge \omega$ means there are $U_1, U_2, U_3, W_1, \ldots, W_\rho \in \mathcal{A}(G)$ with

$$U_1U_2U_3 = W_1 \cdot \ldots \cdot W_\rho \quad \text{and} \quad \rho \ge \omega. \tag{4.1}$$

For each W_i, where $i \in [1, \rho]$, we may write $W_i = T_{i,1}T_{i,2}T_{i,3}$ with the $T_{i,j} \mid U_j$ subsequences such that $\prod_{i=1}^{\rho} T_{i,j} = U_j$ for each $j \in [1, 3]$. There may be multiple ways to do so. If there is a way to do so with $|T_{i,j}| \le 1$ for all i and j, then we say that the factorization (4.1) is *weakly reduced*. Let W_i' be the sequence obtained from $W_i = T_{i,1}T_{i,2}T_{i,3}$ by replacing each nonempty $T_{i,j}$ with the sum of its terms. Likewise, let U_j' be the sequence obtained from $U_j = \prod_{i=1}^{\rho} T_{i,j}$ by replacing each nonempty $T_{i,j}$ with the sum of its terms. The sequence $X = \prod_{i=1}^{\rho} |W_i'| \in \mathcal{F}(\mathbb{Z})$ is called a *spread* for the factorization (4.1), and it depends on the $T_{i,j}$ (so a given factorization (4.1) may have multiple spreads). It is readily seen that if $U \in \mathcal{A}(G)$ is an atom and $T \mid U$ is nontrivial, then the sequence $UT^{-1}\sigma(T)$, obtained by replacing the terms from T with their sum, is also an atom. Hence the W_i' and U_i' are atoms with $U_1'U_2'U_3' = W_1' \cdot \ldots \cdot W_\rho'$ a weakly reduced factorization having $|W_i'| \le 3$ for all i. Thus, when $\rho_3(G) \ge \omega$, we may always assume our factorization (4.1) is weakly reduced. We say that $\rho_3(G) \ge \omega$ *with spread* $X \in \mathcal{F}(\{1, 2, 3\})$ if there exists a factorization (4.1) having spread X, in which case, per the argument above, we may also assume there is a weakly reduced factorization having spread X.

If $1 \in \mathrm{supp}(X)$, then some W_i, say W_1, has $W_1 = T_{1,j}$ for some j, implying that the zero-sum sequence $W_1 = T_{1,j}$ is a subsequence of U_j. As U_j is an atom, this is only possible if $W_1 = T_{1,j} = U_j$, which forces all other $T_{i,j}$ with $i \ne 1$ to be empty in view of $\prod_{i=1}^{\rho} T_{i,j} = U_j$. In particular, $|W_i'| \le 2$ for all i when $1 \in \mathrm{supp}(X)$, meaning we cannot have both $1,\ 3 \in \mathrm{supp}(X)$. From this, we see that we have three

mutually exclusive possibilities for a spread X:

$$1 \in \operatorname{supp}(X) \quad \text{or} \quad \operatorname{supp}(X) = \{2\} \quad \text{or} \quad 3 \in \operatorname{supp}(X).$$

Note there is a spread X with $1 \in \operatorname{supp}(X)$ precisely when $W_s = U_t$ for some $s \in [1, \rho]$ and $t \in [1, 3]$. If $0 \in \operatorname{supp}(U_1U_2U_3)$, then 1 will be a term in any spread X. If $\operatorname{supp}(X) = \{2\}$ and (4.1) is weakly reduced, so that $|W_i| = 2$ for all i, then U_1 must have a subsequence $xy \mid U_1$ with $-x \in \operatorname{supp}(U_2)$ and $-y \in \operatorname{supp}(U_3)$, with similar statements holding for U_2 and U_3. When $3 \in \operatorname{supp}(X)$, we refer to a W_i with $|W_i'| = 3$ as a *traversal* for the factorization (4.1).

LEMMA 2. *Let $G = G_1 \oplus G_2$ be a finite abelian group where $G_1, G_2 \subset G$ are nontrivial subgroups with $\mathsf{D}(G_1) \le \mathsf{D}(G_2)$. Then $\rho_3(G) \ge 2\mathsf{D}(G_1) + \mathsf{D}(G_2) - 2$ with spread $X \in \mathcal{F}(\{2, 3\})$ having $\mathsf{v}_3(X) = 1$.*

PROOF. Let

$$V = v_0 \cdot \ldots \cdot v_{\mathsf{d}(G_1)} \in \mathcal{A}(G_1) \quad \text{and} \quad W = w_0 \cdot \ldots \cdot w_{\mathsf{d}(G_2)} \in \mathcal{A}(G_2)$$

be atoms with maximal lengths $|V| = \mathsf{d}(G_1) + 1 = \mathsf{D}(G_1)$ and $|W| = \mathsf{d}(G_2) + 1 = \mathsf{D}(G_2)$. Since G_1 and G_2 are nontrivial, $0 \notin \operatorname{supp}(VW)$. Let $V' = v_1 \cdot \ldots \cdot v_{\mathsf{d}(G_1)}$ and $W' = w_1 \cdot \ldots \cdot w_{\mathsf{d}(G_1)}$ and define

$$U_1 = (v_0 + w_0)V'W' \prod_{i=\mathsf{d}(G_1)+1}^{\mathsf{d}(G_2)} w_i = (Vv_0^{-1})(Ww_0^{-1})(v_0 + w_0),$$

$$U_2 = (-w_0)(-V') \prod_{i=1}^{\mathsf{d}(G_1)} (v_i - w_i) \prod_{i=\mathsf{d}(G_1)+1}^{\mathsf{d}(G_2)} (-w_i), \quad \text{and}$$

$$U_3 = (-v_0)(-W') \prod_{i=1}^{\mathsf{d}(G_1)} (w_i - v_i).$$

It is easily seen that $U_1, U_2, U_3 \in \mathcal{A}(G)$ are atoms with $(U_1(v_0+w_0)^{-1})(U_2(-w_0)^{-1}) \cdot (U_3(-v_0)^{-1})$ having a factorization into atoms of length 2, evidencing that $\rho_3(G) \ge 1 + \frac{1}{2}(4\mathsf{d}(G_1) + 2\mathsf{d}(G_2)) = 2\mathsf{D}(G_1) + \mathsf{D}(G_2) - 2$ with $(v_0+w_0)(-w_0)(-v_0)$ the unique traversal. □

LEMMA 3. *Let $G = G_1 \oplus G_2$ be a finite abelian group where $G_1, G_2 \subset G$ are nontrivial subgroups such that $\rho_3(G_1) \geq \omega_1$ and $\rho_3(G_2) \geq \omega_2$ both hold with respective spreads $X,\ Y \in \mathcal{F}(\{2,3\})$.*

1. *If $\mathsf{v}_3(X)+\mathsf{v}_3(Y) \geq 1$, then $\rho_3(G) \geq \omega_1+\omega_2-1$ holds with spread $Z \in \mathcal{F}(\{2,3\})$ having $\mathsf{v}_3(Z) = \mathsf{v}_3(X) + \mathsf{v}_3(Y) - 1$.*
2. *If $\mathrm{supp}(X) = \mathrm{supp}(Y) = \{2\}$, then $\rho_3(G) \geq \omega_1 + \omega_2 - 2$ holds with spread $Z \in \mathcal{F}(\{2,3\})$ having $\mathsf{v}_3(Z) = 1$.*

PROOF. For $i \in \{1,2\}$, let $\pi_i\colon\ G = G_1 \oplus G_2 \to G_i$ denote the canonical projection.

1) First suppose $\mathsf{v}_3(X) = r \geq 1$ and $\mathsf{v}_3(Y) = s \geq 1$. Let $V_1,\ V_2,\ V_3 \in \mathcal{A}(G_1)$ and $W_1,\ W_2,\ W_3 \in \mathcal{A}(G_2)$ be atoms having weakly reduced factorizations

$$V_1V_2V_3 = X_1 \cdot \ldots \cdot X_{\rho_1} \qquad \text{and} \qquad W_1W_2W_3 = Y_1 \cdot \ldots \cdot Y_{\rho_2}$$

with the $X_i \in \mathcal{A}(G_1)$, the $Y_i \in \mathcal{A}(G_2)$, $\rho_i \geq \omega_i$ for $i \in [1,2]$, and X_i and Y_j traversals in their respective factorizations for $i \in [1,r]$ and $j \in [1,s]$. In particular, $|X_i| = |Y_j| = 2$ for $i \geq r+1$ and $j \geq s+1$, $X_1 = a_1a_2a_3$ with $a_i \in \mathrm{supp}(V_i)$ for $i \in [1,3]$, and $Y_1 = b_1b_2b_3$ with $b_i \in \mathrm{supp}(W_i)$ for $i \in [1,3]$. Let $V_i' = V_ia_i^{-1}$ and $W_i' = W_ib_i^{-1}$ for $i \in [1,3]$. Now we define

$$\begin{aligned} U_1 &= V_1'W_1'(a_1+b_1) = (V_1a_1^{-1})(W_1b_1^{-1})(a_1+b_1), \\ U_2 &= V_2'W_2'(a_2+b_2) = (V_2a_2^{-1})(W_2b_2^{-1})(a_2+b_2) \quad \text{and} \\ U_3 &= V_3'W_3'(a_3+b_3) = (V_3a_3^{-1})(W_3b_3^{-1})(a_3+b_3). \end{aligned}$$

It is easily observed that the U_i are atoms. Moreover, $V_1'V_2'V_3' = (V_1V_2V_3)X_1^{-1} = = X_2 \cdot \ldots \cdot X_{\rho_1}$ and $W_1'W_2'W_3' = (W_1W_2W_3)Y_1^{-1} = Y_2 \cdot \ldots \cdot Y_{\rho_2}$. Thus $U_1U_2U_3 = = X_2 \cdot \ldots X_{\rho_1}Y_2 \cdot \ldots \cdot Y_{\rho_2}W$ with $W = (a_1+b_1)(a_2+b_2)(a_3+b_3)$ a traversal in view of $a_1+a_2+a_3+b_1+b_2+b_3 = \sigma(X_1)+\sigma(Y_1) = 0$. Moreover, $X_2, \ldots, X_s, Y_2, \ldots, Y_r$ also remain traversals in this factorization, while no X_i nor Y_j with $i \geq r+1$ or $j \geq s+1$ can be a traversal in view of $|X_i| = |Y_j| = 2$. Thus $\rho_3(G) \geq \rho_1+\rho_2-1 \geq \omega_1+\omega_2-1$ holds with spread Z having $\mathsf{v}_3(Z) = \mathsf{v}_3(X)+\mathsf{v}_3(Y)-1 > 0$, ensuring $Z \in \mathcal{F}(\{2,3\})$ (noted before Lemma 2).

Next suppose that either $\mathsf{v}_3(X) > 0 = \mathsf{v}_3(Y)$ or $\mathsf{v}_3(Y) > 0 = \mathsf{v}_3(X)$, say w.l.o.g. the former, so

$$\mathsf{v}_3(X) = r > 0 \quad \text{and} \quad \operatorname{supp}(Y) = \{2\},$$

the latter in view of $Y \in \mathcal{F}(\{2,3\})$. Let V_1, V_2, $V_3 \in \mathcal{A}(G_1)$ and W_1, W_2, $W_3 \in \mathcal{A}(G_2)$ be atoms having weakly reduced factorizations

$$V_1V_2V_3 = X_1 \cdot \ldots \cdot X_{\rho_1} \quad \text{and} \quad W_1W_2W_3 = Y_1 \cdot \ldots \cdot Y_{\rho_2}$$

with the $X_i \in \mathcal{A}(G_1)$, the $Y_i \in \mathcal{A}(G_2)$, $\rho_i \ge \omega_i$ for $i \in [1,2]$, the X_i with $i \in [1,r]$ traversals in their factorization, and $|Y_i| = 2$ and $|X_j| = 2$ for all $i \in [1,\rho_2]$ and $j \ge r+1$. In particular, $X_1 = a_1a_2a_3$ with $a_i \in \operatorname{supp}(V_i)$ for $i \in [1,3]$. Since $1 \notin \operatorname{supp}(XY)$, we have $0 \notin \operatorname{supp}(V_1V_2V_3W_1W_2W_3)$ implying $|V_i|$, $|W_i| \ge 2$ for all $i \in [1,3]$. Also, as discussed before Lemma 2, there must be a length two subsequence $xy \mid W_1$ with $-x \mid W_2$ and $-y \mid W_3$. Now we define

$$\begin{aligned} U_1 &= (V_1a_1^{-1})(W_1x^{-1}y^{-1})(x-a_2)(y+a_1+a_2)\,, \\ U_2 &= (V_2a_2^{-1})(W_2(-x)^{-1})(a_2-x) \quad \text{and} \\ U_3 &= (V_3a_3^{-1})(W_3(-y)^{-1})(a_3-y)\,. \end{aligned}$$

Obviously, we have $U_2, U_3 \in \mathcal{A}(G)$ and $U_1 \in \mathcal{B}(G)$. Letting $S = U_1(y+a_1+a_2)^{-1}$ and considering $\pi_2(S)$ and $\pi_1(S)$ shows that S is zero-sum free, implying that $U_1 \in \mathcal{A}(G)$. Since $a_1+a_2+a_3 = \sigma(X_1) = 0$, we have $(y+a_1+a_2)+(a_3-y) = 0$. Thus, since $(V_1a_1^{-1})(V_2a_2^{-1})(V_3a_3^{-1}) = (V_1V_2V_3)X_1^{-1} = X_2 \cdot \ldots \cdot X_{\rho_1}$ and since $W_1W_2W_3$ has a factorization into ρ_2 atoms of length 2, it is now clear that $U_1U_2U_3$ has a factorization using $(\rho_1-1)+(\rho_2-2)+2 \ge \omega_1+\omega_2-1$ atoms, say

$$U_1U_2U_3 = X_2 \cdot \ldots \cdot X_{\rho_1}Z_1 \cdot \ldots \cdot Z_{\rho_2} \tag{4.2}$$

with $|Z_i| = 2$ for all i. Hence $\rho_3(G) \ge \rho_1 + \rho_2 - 1 \ge \omega_1 + \omega_2 - 1$. Moreover, each X_i with $i \in [2,r]$ remains a traversal for (4.2), while this cannot be the case for X_j with $j \ge r+1$ nor any Z_i as $|X_j| = |Z_i| = 2$ for $j \ge s+1$ and all i. Thus (4.2) has a spread Z with

$$\mathsf{v}_3(Z) = \mathsf{v}_3(X) - 1 = \mathsf{v}_3(X) + \mathsf{v}_3(Y) - 1.$$

If $\mathsf{v}_3(X) \ge 2$, this shows $3 \in \operatorname{supp}(Z)$, whence $Z \in \mathcal{F}(\{2,3\})$ as discussed before Lemma 2. On the other hand, if $\mathsf{v}_3(X) = 1$, then all atoms in the factorization (4.2) have length 2. Thus, since $|U_j| = |V_j| + |W_j| - 1 \ge 3$ for all $j \in [1,3]$, we see that none of these atoms of length two can equal some U_j, meaning $1 \notin \operatorname{supp}(Z)$ for any spread Z for (4.2), also explained above Lemma 2. In this case, $\operatorname{supp}(Z) = \{2\}$, completing the proof of Part 1.

2) Suppose $\operatorname{supp}(X) = \operatorname{supp}(Y) = \{2\}$. Let V_1, V_2, $V_3 \in \mathcal{A}(G_1)$ be atoms such that $V_1V_2V_3$ has a weakly reduced factorization into $\rho_1 \ge \omega_1$ atoms of length 2 and let W_1, W_2, $W_3 \in \mathcal{A}(G_2)$ be atoms such that $W_1W_2W_3$ has a weakly reduced factorization into $\rho_2 \ge \omega_2$ atoms of length 2. As explained before Lemma 2, we may assume there is a length 2 subsequence $xy \mid W_1$ with $-x \mid W_2$ and $-y \mid W_3$ and a length 2 subsequence $ab \mid V_2$ with $-a \mid V_1$ and $-b \mid V_3$. Now we define

$$\begin{aligned} U_1 &= (V_1(-a)^{-1})(W_1x^{-1}y^{-1})(x-a)(y)\,, \\ U_2 &= (V_2a^{-1}b^{-1})(W_2(-x)^{-1})(a-x)(b) \quad \text{and} \\ U_3 &= (V_3(-b)^{-1})(W_3(-y)^{-1})(-b-y)\,. \end{aligned}$$

Obviously, we have $U_3 \in \mathcal{A}(G)$ and U_1, $U_2 \in \mathcal{B}(G)$. Letting $S = U_1y^{-1}$ and considering $\pi_2(S)$ and $\pi_1(S)$ shows that S is zero-sum free, implying that $U_1 \in \mathcal{A}(G)$. Likewise, letting $T = U_2b^{-1}$ and considering $\pi_1(T)$ and $\pi_2(T)$ shows that T is zero-sum free, implying that $U_2 \in \mathcal{A}(G)$. Let $c_1 = y$, $c_2 = b$ and $c_3 = -b - y$. Since $V_1V_2V_3$ and $W_1W_2W_3$ both have factorizations into atoms of length 2, it is now clear that $(U_1c_1^{-1})(U_2c_2^{-1})(U_3c_3^{-1})$ has a factorization into $(\rho_1 - 2) + (\rho_2 - 2) + 1 = \rho_1 + \rho_2 - 3$ atoms of length 2, which together with the unique traversal $c_1c_2c_3$ gives a factorization of $U_1U_2U_3$ into $\rho_1 + \rho_2 - 2$ atoms, showing that $\rho_3(G) \ge \rho_1 + \rho_2 - 2 \ge \omega_1 + \omega_2 - 2$ holds with spread Z having $\mathsf{v}_3(Z) = 1$, ensuring $Z \in \mathcal{F}(\{2,3\})$ (noted before Lemma 2). □

LEMMA 4. *Let $G = C_n^3$ with $n \ge 2$. Then $\rho_3(G) \ge \mathsf{D}^*(G) + \lfloor \frac{\mathsf{D}^*(G)}{2} \rfloor$ with spread $X \in \mathcal{F}(\{2,3\})$. Moreover, $\mathsf{v}_3(X) = 1$ if $\mathsf{D}^*(G)$ is odd, and $\operatorname{supp}(X) = \{2\}$ if $\mathsf{D}^*(G)$ is even.*

PROOF. Let $\{e_1, e_2, e_3\}$ be a basis of G and for $i \in [1,3]$, let $\pi_i \colon G = \langle e_1\rangle \oplus \langle e_2\rangle \oplus \langle e_3\rangle \to \langle e_i\rangle$ denote the canonical projection. Note that $\mathsf{D}^*(G) = 3n - 2 \equiv n \bmod 2$. We handle two cases.

CASE 1: n is odd.

Then $\mathsf D^*(G) = 3n-2 \ge 7$ is odd. We define

$$U_1 = e_1^{n-1}e_2^{n-1}(e_1+e_2+e_3)^{n-1}c_1 \quad \text{with}$$

$$c_1 = 2e_1+2e_2+e_3\,,$$

$$U_2 = (-e_1)^{n-1}e_3^{n-1}(-e_1-e_2-e_3)^{(n-1)/2}(e_1-e_2)^{(n-1)/2}c_2 \quad \text{with}$$

$$c_2 = -e_1-e_2+\frac{n+1}{2}e_3 \quad \text{and}$$

$$U_3 = (-e_3)^{n-1}(-e_2)^{n-1}(-e_1-e_2-e_3)^{(n-1)/2}(-e_1+e_2)^{(n-1)/2}c_3 \quad \text{with}$$

$$c_3 = -e_1-e_2+\frac{n-3}{2}e_3\,.$$

Clearly, $U_i \in \mathcal B(G)$ for $i \in [1,3]$. Considering $\pi_3(U_1c_1^{-1})$, $\pi_2(U_2c_2^{-1})$ and $\pi_1(U_3c_3^{-1})$, we infer that the sequences $U_ic_i^{-1}$ are zero-sum free for every $i \in [1,3]$. Therefore, we have $U_1, U_2, U_3 \in \mathcal A(G)$, and it is now easily seen that $(U_1c_1^{-1})(U_2c_2^{-1})(U_3c_3^{-1})$ has a factorization into atoms of length 2, which together with the unique traversal $c_1c_2c_3$ shows that $\rho_3(G) \ge 1+(9n-9)/2 = \mathsf D^*(G)+\lfloor \frac{\mathsf D^*(G)}{2}\rfloor$ holds with spread X having $\mathsf v_3(X)=1$, so that $X \in \mathcal F(\{2,3\})$ as noted before Lemma 2.

CASE 2: n is even.

Then $\mathsf D^*(G) = 3n-2 \ge 4$ is even. We define

$$U_1 = e_1^{n-1}e_2^{n-1}(e_1+e_2+e_3)^{n-2}(2e_1+e_2+e_3)(e_1+2e_2+e_3)\,,$$

$$U_2 = (-e_1)^{n-1}e_3^{n-1}(-e_1-e_2-e_3)^{n/2-1}(e_1-e_2+e_3)^{n/2-1}(-2e_1-e_2-e_3)\cdot$$
$$(e_1-e_2+2e_3) \quad \text{and}$$

$$U_3 = (-e_3)^{n-1}(-e_2)^{n-1}(-e_1-e_2-e_3)^{n/2-1}(-e_1+e_2-e_3)^{n/2-1}(-e_1-2e_2-e_3)\cdot$$
$$(-e_1+e_2-2e_3)\,.$$

Clearly, $U_i \in \mathcal B(G)$ for $i \in [1,3]$. Considering $\pi_3(U_1)$, $\pi_2(U_2)$ and $\pi_1(U_3)$, we infer that $U_1, U_2, U_3 \in \mathcal A(G)$. By construction, $U_1U_2U_3$ has a factorization into atoms of length 2, say $U_1U_2U_3 = Z_1\cdot\ldots\cdot Z_{\frac12|U_1U_2U_3|}$, implying that $\rho_3(G) \ge \frac12|U_1U_2U_3| = 3(3n-2)/2 = \mathsf D^*(G)+\lfloor\frac{\mathsf D^*(G)}{2}\rfloor$. Moreover, since $|U_i| = 3n-2 > 2 = |Z_j|$ for all i and j, we see that $1 \notin \operatorname{supp}(X)$ in any spread X, whence $\operatorname{supp}(X) = \{2\}$, completing the proof. □

PROOF OF THEOREM 1 By Proposition 1, we have $\rho_k(H) = \rho_k(G)$ for all $k \geq 1$. By Lemma 1, statement 1) and Lemma 1, statement 2), it suffices to prove the assertion for $k = 1$. By hypothesis, G can be written in the form

$$G = C_{m_1}^{t_1} \oplus \ldots \oplus C_{m_\alpha}^{t_\alpha},$$

where $\{m_1, \ldots, m_\alpha\} = \{n_1, \ldots, n_r\}$ with $t_i \in \{2, 3\}$. We proceed by induction on α to show that $\rho_3(G) \geq \mathsf{D}^*(G) + \lfloor \frac{\mathsf{D}^*(G)}{2} \rfloor$ holds with spread $X \in \mathcal{F}(\{2, 3\})$ with $\mathsf{v}_3(X) = 1$ when $\mathsf{D}^*(G)$ is odd and with $\mathrm{supp}(X) = \{2\}$ when $\mathsf{D}^*(G)$ is even, which will complete the proof.

Since $n_1 \mid \ldots \mid n_r$ with $\{m_1, \ldots, m_\alpha\} = \{n_1, \ldots, n_r\}$, we have

$$\mathsf{D}^*(G) = \mathsf{d}^*(C_{m_1}^{t_1}) + \mathsf{d}^*(C_{m_2}^{t_2} \oplus \ldots \oplus C_{m_\alpha}^{t_\alpha}) + 1 = \mathsf{D}^*(K) + \mathsf{D}^*(L) - 1,$$

where $K = C_{m_1}^{t_1}$ and $L = C_{m_2}^{t_2} \oplus \ldots \oplus C_{m_\alpha}^{t_\alpha}$. If $t_1 = 2$, then $\mathsf{D}^*(K) = \mathsf{D}^*(C_{m_1}^2) = 2m_1 - 1$ is odd and Lemma 2 implies that $\rho_3(K) = \rho_3(C_{m_1}^2) \geq 3m_1 - 2 = (2m_1 - 1) + \lfloor \frac{2m_1 - 1}{2} \rfloor = \mathsf{D}^*(K) + \lfloor \frac{\mathsf{D}^*(K)}{2} \rfloor$ with spread X having $\mathsf{v}_3(X) = 1$, so that $X \in \mathcal{F}(\{2, 3\})$. If $t_1 = 3$, then Lemma 4 implies that $\rho_3(K) = \rho_3(C_{m_1}^3) \geq \mathsf{D}^*(K) + \lfloor \frac{\mathsf{D}^*(K)}{2} \rfloor$ with spread $X \in \mathcal{F}(\{2, 3\})$. Moreover, $\mathsf{v}_3(X) = 1$ if $\mathsf{D}^*(K)$ is odd, and $\mathrm{supp}(X) = \{2\}$ if $\mathsf{D}^*(K)$ is even. This completes the base case when $\alpha = 1$. Thus we may assume $\alpha \geq 2$, in which case the induction hypothesis ensures that

$$\rho_3(K) \geq \mathsf{D}^*(K) + \lfloor \frac{\mathsf{D}^*(K)}{2} \rfloor \quad \text{and} \quad \rho_3(L) \geq \mathsf{D}^*(L) + \lfloor \frac{\mathsf{D}^*(L)}{2} \rfloor$$

with respective spreads $X, Y \in \mathcal{F}(\{2, 3\})$.

If $\mathsf{D}^*(K)$ and $\mathsf{D}^*(L)$ are both even, then $\mathsf{D}^*(G) = \mathsf{D}^*(K) + \mathsf{D}^*(L) - 1$ is odd and $\mathrm{supp}(X) = \mathrm{supp}(Y) = \{2\}$, whence Lemma 3, statement 2) yields

$$\rho_3(G) \geq \mathsf{D}^*(K) + \frac{\mathsf{D}^*(K)}{2} + \mathsf{D}^*(L) + \frac{\mathsf{D}^*(L)}{2} - 2 = \mathsf{D}^*(G) + \frac{\mathsf{D}^*(G) - 1}{2}$$

with spread $Z \in \mathcal{F}(\{2, 3\})$ having $\mathsf{v}_3(Z) = 1$, as desired. If $\mathsf{D}^*(K)$ and $\mathsf{D}^*(L)$ are both odd, then $\mathsf{v}_3(X) = \mathsf{v}_3(Y) = 1$ and $\mathsf{D}^*(G) = \mathsf{D}^*(K) + \mathsf{D}^*(L) - 1$ is odd, whence Lemma 3, statement 1) yields

$$\rho_3(G) \geq \mathsf{D}^*(K) + \frac{\mathsf{D}^*(K) - 1}{2} + \mathsf{D}^*(L) + \frac{\mathsf{D}^*(L) - 1}{2} - 1 = \mathsf{D}^*(G) + \frac{\mathsf{D}^*(G) - 1}{2}$$

with spread $Z \in \mathcal{F}(\{2,3\})$ having $\mathsf{v}_3(Z) = \mathsf{v}_3(X) + \mathsf{v}_3(Y) - 1 = 1$, as desired. Finally, if $\mathsf{D}^*(K)$ and $\mathsf{D}^*(L)$ have different parities, then $\mathsf{v}_3(X) + \mathsf{v}_3(Y) = 1$, $\mathsf{D}^*(G) = \mathsf{D}^*(K) + \mathsf{D}^*(L) - 1$ is even, and Lemma 3, statement 1) yields

$$\rho_3(G) \ge \mathsf{D}^*(K) + \frac{\mathsf{D}^*(K)}{2} + \mathsf{D}^*(L) + \frac{\mathsf{D}^*(L)}{2} - \frac{1}{2} - 1 = \mathsf{D}^*(G) + \frac{\mathsf{D}^*(G)}{2}$$

with spread $Z \in \mathcal{F}(\{2,3\})$ having $\mathsf{v}_3(Z) = \mathsf{v}_3(X) + \mathsf{v}_3(Y) - 1 = 0$, forcing $\mathrm{supp}(Z) = \{2\}$. This completes the induction. When $\mathsf{D}^*(G) = \mathsf{D}(G)$, the needed upper bound comes from Lemma 1, statement 2) □

5. Groups of rank two

The aim of this section is to prove the following characterization. It provides the first non-cyclic groups G for which $\rho_{2k+1}(G)$ is strictly smaller than the upper bound $k\mathsf{D}(G) + \lfloor \frac{\mathsf{D}(G)}{2} \rfloor$ for some $k \in \mathbb{N}$.

THEOREM 2. *Let H be a Krull monoid with finite class group G such that every class contains a prime divisor. Suppose that $G = C_m \oplus C_{mn}$ with $n \ge 1$ and $m \ge 2$. Then*

$$\rho_3(H) = \mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor \qquad \textit{if and only if} \qquad n = 1 \ \textit{ or } \ m = n = 2\,.$$

We start with two corollaries providing examples of groups G having rank two which show that Theorem 2 is sharp in two aspects. Indeed, Corollary 4 shows that these groups G satisfy

$$\rho_3(G) = \mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor - 1 \quad \text{but} \quad \rho_{2k+1}(G) = k\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor \quad \text{for all } k \ge 2\,.$$

After that, we deal with groups of the form $G = C_2 \oplus C_{2n}$ where $n \ge 3$. Since for cyclic groups G we have $\rho_{2k+1}(G) = k\mathsf{D}(G) + 1$ for all $k \ge 1$, groups of the form $C_2 \oplus C_{2n}$ are the canonical first choice for testing Conjecture **C2**. Indeed, we verify Conjecture **C2** for them and show that there exists an integer $k^* \in \mathbb{N}$ (by Theorem 2 we must have $k^* > 1$ for $n > 2$) such that

$$\rho_{2k+1}(G) = k\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor \quad \text{for all } k \ge k^*\,.$$

Moreover, Corollary 5 provides the first example of a group where, for some odd $k \in \mathbb{N}$, strict inequalities hold in the crucial inequality (3.1).

COROLLARY 4. *Let $G = C_m \oplus C_{2m}$ with $m \geq 2$.*

1) *If $m = 2$, then $\rho_{2k+1}(G) = k\mathsf{D}(G) + \lfloor \frac{\mathsf{D}(G)}{2} \rfloor$ for every $k \geq 1$.*
2) *If $m \geq 3$, then $\rho_5(G) \geq 2\mathsf{D}(G) + (m+1)$.*
3) *If $m \in \{3, 4\}$, then $\rho_3(G) = \mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor - 1$ and $\rho_{2k+1}(G) = k\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor$ for all $k \geq 2$.*

PROOF. Let $\{e_1, e_2\}$ be a basis of G with $\mathrm{ord}(e_1) = m$ and $\mathrm{ord}(e_2) = 2m$. Then $\mathsf{D}(G) = 3m - 1$.

1) We define

$$U_1 = e_1 e_2 (e_1 + e_2)^3, \quad U_2 = e_1 (-e_2)^3 (e_1 - e_2) \quad \text{and} \quad U_3 = e_2^2 (e_1 - e_2)^2 .$$

Obviously, $U_1 U_2 U_3$ may be written as a product of 7 which implies that $\rho_3(G) = \mathsf{D}(G) + \lfloor \frac{\mathsf{D}(G)}{2} \rfloor$. Now the assertion follows from Lemma 1, statement 3).

2) We define

$$\begin{aligned} U_1 &= e_1^{m-1} e_2^{2m-1} (e_1 + e_2), \\ U_2 &= (-e_1)^{m-1} e_2^{2m-1} (-e_1 + e_2) \\ U_3 &= (e_1 + e_2)^{m-1} (-e_2)^{2m-1} (e_1 + m e_2) \text{ and} \\ U_4 &= (-e_1 - e_2)^{2m-1} (-e_1 + m e_2)^2 (e_1 - e_2). \end{aligned}$$

Then $U_1, U_2, U_3, U_4 \in \mathcal{A}(G)$ (note we need $m \geq 3$ to ensure $U_4 \in \mathcal{A}(G)$), $|U_1| = |U_2| = |U_3| = \mathsf{D}(G)$ and $|U_4| = 2m + 2$). By construction, $U_1 U_2 U_3^2 U_4$ has a factorization into atoms of length 2, which implies that

$$\rho_5(G) \geq \frac{|U_1 U_2 U_3^2 U_4|}{2} = 2\mathsf{D}(G) + (m+1) .$$

3) Proposition 6, statement 1) and Theorem 2 imply that

$$\mathsf{D}(G) + m \leq \rho_3(G) \leq \mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor - 1 ,$$

which is an equality because $m \in \{3, 4\}$. By Lemma 1, statement 3), it suffices to show that

$$\rho_5(G) \ge 2\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor ,$$

which follows from 2. above because $m \in \{3, 4\}$ ensures $\left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor = m + 1$. □

COROLLARY 5. *Let $G = C_2 \oplus C_{2n}$ with $n \ge 3$. Then*

$$\mathsf{D}(G) + 1 < \rho_3(G) < \mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor \quad \textit{and}$$

$$\rho_{2k+1}(G) = k\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor \quad \textit{for every } k \ge 2n - 1 .$$

PROOF. We have $\mathsf{D}(G) = \mathsf{D}^*(G) = 2n + 1$. The left inequality follows from Proposition 6, statement 2) and from Proposition 5, statement 1), and the right inequality follows from Theorem 2.

To prove the second statement, let $\{e_1, e_2\}$ be a basis of G with $\mathrm{ord}(e_1) = 2$ and $\mathrm{ord}(e_2) = 2n$. For $i \in [1, n]$, we define

$$U_i = e_2^{2n-1}\big(e_1 - (i-1)e_2\big)\big(e_1 + ie_2\big) \in \mathcal{A}(G) .$$

Let

$$V_1 = (e_1 + e_2)^{2n-1} e_2 e_1 \in \mathcal{A}(G) .$$

Let $W = e_2(e_1+e_2)(e_1-2e_2)$. By construction, $S = \Big(U_2^2(-U_1)^2\Big) \cdot \ldots \cdot \Big(U_n^2(-U_1)^2\Big) \cdot \Big(U_1(-U_2)V_1\Big)$ is a product of $4(n-1)+3 = 4n-1$ atoms and SW^{-1} has a factorization into atoms of length 2. This implies that

$$\rho_{2(2n-1)+1}(G) \ge 1 + \frac{|S| - 3}{2} = 1 + \frac{(4n-1)(2n+1) - 3}{2} = (2n-1)\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor .$$

The result now follows from Lemma 1, statement 3). □

The proof of Theorem 2 is based on the recent characterization of minimal zero-sum sequences of maximal length in groups of rank two, which will be formulated in Main Proposition 7. The proof of the characterization is obtained by combining the main results from [19], [21], [35], [39] with a few small order groups handled by direct computation [9]. The version below is derived from this original in a few

short lines [7, Theorem 3.1] (apart from (e) and the fact that both parts of (d) hold when $n = 2$, which we will deduce from the rest of theorem in the explanations below). It eliminates some overlap between type I and II in the original statement.

MAIN PROPOSITION 7 *Let $G = C_m \oplus C_{mn}$ with $n \geq 1$ and $m \geq 2$. A sequence S over G of length $\mathsf{D}(G) = m + mn - 1$ is a minimal zero-sum sequence if and only if it has one of the following two forms*:

1)

$$S = e_1^{\mathrm{ord}(e_1)-1} \prod_{i=1}^{\mathrm{ord}(e_2)} (x_i e_1 + e_2),$$

where

(*a*) $\{e_1, e_2\}$ *is a basis of* G,

(*b*) $x_1, \ldots, x_{\mathrm{ord}(e_2)} \in [0, \mathrm{ord}(e_1) - 1]$ *and* $x_1 + \ldots + x_{\mathrm{ord}(e_2)} \equiv 1 \bmod \mathrm{ord}(e_1)$.

In this case, we say that S is of type I(a) or I(b) according to whether $\mathrm{ord}(e_2) = m$ *or* $\mathrm{ord}(e_2) = mn > m$.

2)

$$S = f_1^{sm-1} f_2^{(n-s)m+\epsilon} \prod_{i=1}^{m-\epsilon} (-x_i f_1 + f_2),$$

where

(*a*) $\{f_1, f_2\}$ *is a generating set for G with* $\mathrm{ord}(f_2) = mn$ *and* $\mathrm{ord}(f_1) > m$,

(*b*) $\epsilon \in [1, m-1]$ *and* $s \in [1, n-1]$,

(*c*) $x_1, \ldots, x_{m-\epsilon} \in [1, m-1]$ *with* $x_1 + \ldots + x_{m-\epsilon} = m - 1$,

(*d*) *either* $s = 1$ *or* $mf_1 = mf_2$, *with both holding when* $n = 2$, *and*

(*e*) *either* $\epsilon \geq 2$ *or* $mf_1 \neq mf_2$.

In this case, we say that S is of type II.

We gather some simple consequences of the above characterization which will be used without further mention. Let all notation be as in the Main Proposition 7.

It is easy to see that $|\operatorname{supp}(S)| \geq 3$.

When S has type II, it is always possible to find some $f_1' \in G$ such that $\{f_1', f_2\}$ is a basis for G with $\mathrm{ord}(f_1') = m$ and $f_1 = f_1' + \alpha f_2$ for some $\alpha \in [1, mn-1]$ (see

[7]). In particular, since $mf_1 \neq 0$ (in view of $\mathrm{ord}(f_1) > m$), we have $\mathrm{ord}(f_1) = tm$ for some $t \geq 2$ with $t \mid n$. Moreover, it is now readily checked that, regardless of whether S has type I or II, every term of S must have its order being a multiple of m.

When S has type II, it is clear that $-x_i f_1 + f_2 = -x_i f_1' + (1 - \alpha x_i) f_2 \neq f_2$ in view of $x_i \in [1, m-1]$, for any $i \in [1, m-\epsilon]$. Likewise, a term $-x_i f_1 + f_2 = -x_i f_1' + (1 - \alpha x_i) f_2$ could only equal $f_1 = f_1' + \alpha f_2$ if $x_i = m - 1$ and $1 - \alpha(m-1) = 1 - \alpha x_i \equiv \alpha \bmod mn$, implying $1 \equiv \alpha m \bmod mn$, which is not possible. Consequently, we see that a term $-x_i f_1 + f_2$ can never equal f_1 or f_2. Likewise, since $\mathrm{ord}(f_1) \geq 2m$, $-x_i f_1 + f_2 = -x_j f_1 + f_2$ is only possible if $x_i = x_j \in [1, m-1]$.

When S has type II, the condition $x_1 + \ldots + x_{m-\epsilon} = m - 1$ with $x_i \in [1, m-1]$ forces $\max x_i \leq (m-1) - (m-\epsilon-1) = \epsilon$. Thus we always have $x_i \leq \epsilon$. In particular, if $\epsilon = 1$, then $x_i = 1$ for all $i \in [1, m-1]$.

When S has type II, then $s \in [1, n-1]$ forces $n \geq 2$. Suppose $n = 2$. Then $s = 1$ and $\mathrm{ord}(f_1) = \mathrm{ord}(f_2) = 2m$. Let $f_1' \in G$ be such that $\{f_1', f_2\}$ is a basis for G with $\mathrm{ord}(f_1') = m$. Let $g = xf_1' + yf_2 \in G$ with $x, y \in \mathbb{Z}$. If y is odd, then $mg = xmf_1' + ymf_2 = ymf_2 \neq 0$, implying $\mathrm{ord}(g) > m$ and thus $\mathrm{ord}(g) = 2m$. On the other hand, if $\mathrm{ord}(g) = 2m$, then $0 \neq mg = ymf_2$, implying y is odd. Consequently, the elements $g \in G$ with $\mathrm{ord}(g) = 2m$ are precisely those $g = xf_1' + yf_2$ with $x, y \in \mathbb{Z}$ and y odd, meaning any $g \in G$ with $\mathrm{ord}(g) = 2m$ has $mg = mf_2$. In particular, $mf_1 = mf_2$. This explains why both conditions of (d) always hold when $n = 2$.

If $n > 1$, then there are at most $m - 1$ terms of order m in S. Indeed, if S has type I(a), then all terms of order m are contained in $\prod_{i=1}^{m}(x_i e_1 + e_2)$. However, since $m\sum_{i=1}^{m}(x_i e_1 + e_2) = me_1 \neq 0$, they cannot all have order m, meaning there are at most $m - 1$ such terms. If S has type I(b), then it is clear that all terms of the form $x_i e_1 + e_2$ have order $mn > m$, leaving at most $m - 1$ of order m, all equal to e_1. Finally, if S has type II, then we have $\mathrm{ord}(f_1) \geq 2m$ as remarked above. Thus only terms contained in $\prod_{i=1}^{m-\epsilon}(-x_i f_1 + f_2)$ can have order m, meaning there are at most $m - \epsilon \leq m - 1$ such terms

Moreover, if S has type II and contains precisely $m - 1$ terms of order m, then we must have $\epsilon = 1$ with each term from $\prod_{i=1}^{m-1}(-x_i f_1 + f_2)$ having order m. However, since we have $x_i \in [1, \epsilon]$ as remarked above, this is only possible if

$$S = f_1^{sm-1} f_2^{(n-s)m+1}(f_2 - f_1)^{m-1} \quad \text{with} \quad \mathrm{ord}(f_2 - f_1) = m\,.$$

In such case, $\{f_2, f_2 - f_1\}$ is also a generating set for G with $\mathrm{ord}(f_2) = mn$ and $\mathrm{ord}(f_2 - f_1) = m$, which forces $\{f_2, f_2 - f_1\}$ to be a basis for G. Thus S has type I(b) (taking $e_1 = f_2 - f_1$ and $e_2 = f_2$).

In particular, if S had type II with $mf_1 = mf_2$ and $\epsilon = 1$, then S would also have type I(b). Indeed $\epsilon = 1$ forces $x_i = 1$ for all $i \in [1, m-1]$ in view of $x_i \in [1, \epsilon]$, while each $-x_i f_1 + f_2 = -f_1 + f_2$ has order m in view of $mf_1 = mf_2$ (and the fact that every term of S has its order being a multiple of m). Thus we would have $m - 1$ elements of order m, so that the above argument shows that S has type I(b). This argument is what allows us to assume (e) in Main Proposition 7. In particular, if S has type II and $n = 2$, then $\epsilon \geq 2$ and $m \geq 3$ (as $\epsilon \in [2, m-1]$).

The following lemma regarding type II sequences will be needed in the proof.

LEMMA 5. *Let $G = C_m \oplus C_{mn}$ with $n \geq 1$ and $m \geq 2$. Suppose S is a minimal zero-sum sequence over G of length $\mathsf{D}(G) = m + mn - 1$ that is of type II, say*

$$S = f_1^{sm-1} f_2^{(n-s)m+\epsilon} \prod_{i=1}^{m-\epsilon} (-x_i f_1 + f_2)$$

with all notation as in Main Proposition 7. Suppose $T \mid S$ is a subsequence with $|T| \geq 2m-1$. Then T contains a subsequence $T_1 \mid T$ with $\sigma(T_1) = mf_2$. Furthermore, if T has no proper subsequence with this property, then $T = f_1^{m-1} f_2^{\epsilon} \prod_{i=1}^{m-\epsilon} (-x_i f_1 + f_2)$.

PROOF. Since $s \in [1, n-1]$, we conclude that $n \geq 2$. If $s = 1$, then $\mathsf{v}_{f_1}(T) \leq \leq \mathsf{v}_{f_1}(S) = m - 1$. On the other hand, if $s > 1$, then $mf_1 = mf_2$, in which case we must also have $\mathsf{v}_{f_1}(T) \leq m - 1$ else $f_1^m \mid T$ will be a proper subsequence whose sum is $mf_1 = mf_2$, as desired. Thus we may assume

$$\mathsf{v}_{f_1}(T) = m - 1 - t \quad \text{for some } t \in [0, m-1]. \tag{5.1}$$

Likewise, we must have $\mathsf{v}_{f_2}(T) \leq m - 1$ else $f_2^m \mid T$ will be a proper subsequence whose sum is mf_2, as desired. By re-indexing the $-x_i f_1 + f_2$ appropriately, we may w.l.o.g. assume

$$\prod_{i=1}^{\ell} (-x_i f_1 + f_2) = \gcd\left(\prod_{i=1}^{m-\epsilon} (-x_i f_1 + f_2), T \right), \quad \text{where } \ell \in [0, m-\epsilon]. \tag{5.2}$$

Hence, from the hypothesis $|T| \ge 2m-1$, we deduce that

$$\mathsf{v}_{f_2}(T) = |T| - \mathsf{v}_{f_1}(T) - \ell \ge m + t - \ell. \tag{5.3}$$

In particular, $\mathsf{v}_{f_2}(T) \le m-1$ forces $\ell \ge t+1 \ge 1$.

Recall that $x_1 + \ldots + x_{m-\epsilon} = m-1$ with $x_i \in [1, m-1]$ for all i. Thus

$$x_1 + \ldots + x_\ell = m - 1 - x \quad \text{with} \quad x := \sum_{i=\ell+1}^{m-\epsilon} x_i \ge m - \epsilon - \ell \ge 0.$$

Consequently, if $t \le x$, then the sequence $f_1^{m-1-t} \prod_{i=1}^{\ell}(-x_i f_1 + f_2)$ contains at least ℓ disjoint subsequences each having sum f_2 and containing precisely one term of the form $-x_i f_1 + f_2$, while if $t \ge x$, then the sequence $f_1^{m-1-t} \prod_{i=1}^{\ell}(-x_i f_1 + f_2)$ contains at least $\ell - \Big((m-1-x) - (m-1-t)\Big) = \ell - t + x$ disjoint subsequences each having sum f_2 and containing precisely one term of the form $-x_i f_1 + f_2$. In either case, we have

$$R_1 \cdot \ldots \cdot R_w \mid f_1^{m-1-t} \prod_{i=1}^{\ell}(-x_i f_1 + f_2) \quad \text{with} \quad \sigma(R_i) = f_2 \ \text{ for } i \in [1, w],$$

where $w = \min\{\ell, \ell - t + x\}$. Moreover, the subsequence $R_1 \cdot \ldots \cdot R_w$ of $f_1^{m-1-t} \cdot \prod_{i=1}^{\ell}(-x_i f_1 + f_2)$ will be proper unless $m-1-t = x_1 + \ldots + x_\ell = m-1-x$, i.e., unless $t = x$.

Now, if $t < x$, then $T_1 = R_1 \cdot \ldots \cdot R_\ell f_2^{m-\ell}$ is a proper subsequence of T (in view of (5.1), (5.2), (5.3) and $t \ne x$) with sum $\sigma(T_1) = mf_2$, as desired. On the other hand, if $t \ge x$, then $T_1 = R_1 \cdot \ldots \cdot R_{\ell-t} f_2^{m-\ell+t}$ is a subsequence of T (in view of (5.1), (5.2) and (5.3)) with sum $\sigma(T_1) = mf_2$. Moreover, it will be a proper subsequence of T unless $t = x = 0$ and equality holds in (5.3). From $x_1 + \ldots + x_\ell = m - 1 - x = m - 1$, we deduce that $\ell = m - \epsilon$ in this case (recall that $x_1 + \ldots + x_{m-\epsilon} = m-1$ with $x_i \in [1, m-1]$ for all i), and now

$$T = f_1^{m-1-t} f_2^{m+t-\ell} \prod_{i=1}^{\ell}(-x_i f_1 + f_2) = f_1^{m-1} f_2^{\epsilon} \prod_{i=1}^{m-\epsilon}(-x_i f_1 + f_2),$$

completing the proof. □

We are now ready to proceed with the proof of Theorem 2.

PROOF OF THEOREM 2. By Proposition 1, we have $\rho_3(H) = \rho_3(G)$. We study $\rho_3(G)$ and recall that $\mathsf{D}(G) = \mathsf{D}^*(G) = m + mn - 1$. If $n = 1$, then $G = C_m \oplus C_m$, and the theorem follows from Corollary 2. If $m = n = 2$, then $G = C_2 \oplus C_4$, and the theorem follows from Corollary 4 1). We now assume $n \ge 2$ with $m \ge 3$ when $n = 2$. In particular, $\mathsf{D}(G) \ge 7$. It remains to show $\rho_3(G) < \rho := \lfloor 3\frac{\mathsf{D}(G)}{2} \rfloor = \lfloor \frac{3m+3mn-3}{2} \rfloor$ in this case. Assume by contradiction that there are $U_1, U_2, U_3, V_1, \ldots, V_\rho \in \mathcal{A}(G)$ such that

$$U_1U_2U_3 = V_1 \cdot \ldots \cdot V_\rho \, .$$

Without loss of generality, we may assume $|U_1| \ge |U_2| \ge |U_3|$ and $|V_1| \ge \ldots \ge |V_\rho|$. We continue by showing we can assume the following assertion holds true. Note that $|U_3| = \mathsf{D}(G) - 1$ is only possible in Assertion A if $\mathsf{D}(G)$ is odd and $|V_1| = 2$.

ASSERTION A. $|U_1| = |U_2| = \mathsf{D}(G)$ *and* $\mathsf{D}(G) - 1 \le |U_3| \le \mathsf{D}(G)$ *with the* U_i *satisfying either*

$$U_1 = AB, \quad -U_2 = AC, \quad U_3 = (-B)C,$$
$$|A| = \left\lceil \frac{\mathsf{D}(G)}{2} \right\rceil \quad \textit{and} \quad |V_1| = 2 \quad \textit{or}$$
$$U_1 = ABw_1, \quad -U_2 = ACw_2, \quad U_3 = (-B)C(w_2 - w_1),$$
$$|A| = \frac{\mathsf{D}(G) - 1}{2} \quad \textit{and} \quad |V_1| = 3, \quad \textit{where}$$
$$A = \gcd(U_1, -U_2), \quad B = \gcd(U_1, -U_3), \quad C = \gcd(-U_2, U_3),$$
$$|B| = |C| = \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor \quad \textit{and} \quad w_1,\ w_2 \in G.$$

PROOF OF ASSERTION A. We trivially have $|U_1U_2U_3| = |U_1| + |U_2| + |U_3| \le 3\mathsf{D}(G)$. Also, $|V_i| \ge 2$ for each i (as 0 cannot divide any U_i, else $\rho \le \mathsf{D}(G) + 1$), implying

$$3\mathsf{D}(G) \ge |U_1U_2U_3| = |V_1 \cdot \ldots \cdot V_\rho| = \sum_{i=1}^{\rho} |V_i| \ge 2\rho = 2\lfloor 3\mathsf{D}(G)/2 \rfloor \ge 3\mathsf{D}(G) - 1,$$

with equality in the latter estimate only possible when $\mathsf{D}(G)$ is odd. It follows that, if $\mathsf{D}(G)$ is even, then $|U_1| = |U_2| = |U_3| = \mathsf{D}(G)$ with $|V_i| = 2$ for all i, while if

$\mathsf D(G)$ is odd, then either $|U_1| = |U_2| = |U_3| = \mathsf D(G)$ with $|V_1| = 3$ and $|V_i| = 2$ for all $i \ge 2$ or else $|U_1| = |U_2| = \mathsf D(G)$ and $|U_3| = \mathsf D(G) - 1$ with $|V_i| = 2$ for all i.

When $|V_i| = 2$ for all i, then $S = U_1U_2U_3$ has a factorization into length 2 atoms. Thus $U_1 = AB$, $-U_2 = AC$ and $U_3 = (-B)C$ for some $A,\ B,\ C \in \mathcal F(G)$. Since $|A|+|B| = |U_1| = \mathsf D(G) = |U_2| = |A|+|C|$, it follows that $|B| = |C|$. But now $2|B| = |B| + |C| = |U_2| \in \{\mathsf D(G),\ \mathsf D(G) - 1\}$, implying $|B| = |C| = \left\lfloor \frac{\mathsf D(G)}{2} \right\rfloor$ and $|A| = |U_1| - |B| = \mathsf D(G) - \left\lfloor \frac{\mathsf D(G)}{2} \right\rfloor = \left\lceil \frac{\mathsf D(G)}{2} \right\rceil$. If there is some $g \in \mathrm{supp}(B) \cap \mathrm{supp}(C)$, then U_3 will contain both g and $-g$. However, since U_3 is an atom, this is only possible if $|U_3| = 2$, contradicting that $|U_3| \ge \mathsf D(G) - 1 \ge 6$. Therefore we instead conclude that $\mathrm{supp}(B) \cap \mathrm{supp}(C) = \varnothing$, implying $\gcd(U_1, -U_2) = A$. Similar arguments show that $B = \gcd(U_1, -U_3)$ and $C = \gcd(-U_2, U_3)$, completing the proof of Assertion A in this case. It remains to consider the case when $|V_1| = 3$ with $|V_i| = 2$ for $i \ge 2$, which is only possible when $|U_1| = |U_2| = |U_3| = \mathsf D(G)$ is odd.

If some U_i, say w.l.o.g. U_3, contains two terms from V_1, say $g_1g_2 \mid \gcd(V_1, U_3)$, then replacing U_3 by $U_3' = U_3(g_1g_2)^{-1}(g_1 + g_2)$ and replacing V_1 by $V_1' = V_1(g_1g_2)^{-1}(g_1 + g_2)$ yields atoms $U_1,\ U_2,\ U_3' \in \mathcal A(G)$ having a factorization $U_1U_2U_3' = V_1'V_2 \ldots V_\rho$ with $|U_1| = |U_2| = \mathsf D(G)$, $|U_3'| = \mathsf D(G) - 1$ and $|V_1'| = |V_2| = \ldots = |V_\rho| = 2$. These atoms also provide a counter-example to the theorem and satisfy the previously handled case of Assertion A. Thus we may assume (for the purpose of proving the theorem) that this does not occur: no length two subsequence of V_1 divides any U_i. In consequence, precisely one of each of the three terms of V_1 occurs in each U_i while $(U_1U_2U_3)V_1^{-1}$ has a factorization into length 2 atoms (in view of $|V_i| = 2$ for $i \ge 2$). It follows that $U_1 = ABw_1$, $-U_2 = ACw_2$ and $U_3 = (-B)C(w_2 - w_1)$ for some $A,\ B,\ C \in \mathcal F(G)$, where $V_1 = w_1(-w_2)(w_2 - w_1)$.

Since $|A| + |B| + 1 = |U_1| = \mathsf D(G) = |U_2| = |A| + |C| + 1$, it follows that $|B| = |C|$. But now $2|B| + 1 = |B| + |C| + 1 = |U_3| = \mathsf D(G)$ follows, implying $|B| = |C| = \frac{\mathsf D(G)-1}{2} = \left\lfloor \frac{\mathsf D(G)}{2} \right\rfloor$ and $|A| = |U_1| - |B| - 1 = \mathsf D(G) - \frac{\mathsf D(G)-1}{2} - 1 = \frac{\mathsf D(G)-1}{2}$.

Suppose there were some $g \in \mathrm{supp}(Bw_1) \cap \mathrm{supp}(Cw_2)$. Note $w_1 \ne w_2$, else V_1 would contain a length 2 zero-sum subsequence, contradicting that V_1 is an atom. Consequently, if $g = w_1$, then $w_1 = g \in \mathrm{supp}(C)$, in which case U_3 contains the two term subsequence $w_1(w_2 - w_1)$ of V_1, contrary to assumption. Likewise, if $g = w_2$, then $w_2 \in \mathrm{supp}(B)$, in which case U_3 contains the two term subsequence $(-w_2)(w_2 - w_1)$ of V_1, once more contrary to assumption. On the other hand, if $g \in \mathrm{supp}(B) \cap \mathrm{supp}(C)$, then U_3 will contain both g and $-g$, yielding the contradiction $2 = |U_3| \ge \mathsf D(G) - 1 = 6$ as argued when $|V_i| = 2$ for all i. So we

instead conclude that $\operatorname{supp}(Bw_1) \cap \operatorname{supp}(Cw_2) = \varnothing$, implying $\gcd(U_1, -U_2) = A$. Similar arguments show that $B = \gcd(U_1, -U_3)$ and $C = \gcd(-U_2, U_3)$, completing the proof of Assertion A. □

We continue the proof of Theorem 2. In view of Assertion A, we see that we can apply Main Proposition 7 to U_1 and $-U_2$ to characterize the possible structures for U_1 and $-U_2$. Since the roles of U_1 and U_2 are symmetric, this gives us six cases.

CASE 1: U_1 and $-U_2$ are both of type I(b), say

$$U_1 = e_1^{m-1} \prod_{i=1}^{mn} (x_i e_1 + e_2) \quad \text{and} \quad -U_2 = f_1^{m-1} \prod_{i=1}^{mn} (y_i f_1 + f_2),$$

where $\{e_1, e_2\}$ and $\{f_1, f_2\}$ are bases for G with $\operatorname{ord}(e_1) = \operatorname{ord}(f_1) = m$ and $\operatorname{ord}(e_2) = \operatorname{ord}(f_2) = mn > n$.

Let $H = \langle e_1, f_1 \rangle$. Since $\operatorname{ord}(e_1) = \operatorname{ord}(f_1) = m$, we conclude that H is isomorphic to a subgroup of C_m^2. In particular, $\mathsf{D}(H) \le \mathsf{D}(C_m^2) = 2m - 1$. Since $m, n \ge 2$ with $n \ge 3$ when $m = 2$, we have $|B| = |C| \ge \frac{\mathsf{D}(G)-1}{2} = \frac{mn+m-2}{2} > m$. Likewise $|A| \ge \frac{\mathsf{D}(G)-1}{2} > m$. Any element of the form $xe_1 + e_2$ or $yf_1 + f_2$, where $x, y \in \mathbb{Z}$, has order $mn > m = \operatorname{ord}(e_1) = \operatorname{ord}(f_1)$ and thus cannot be equal to e_1 nor f_1. Since $|A| \ge m + 1$, we conclude that A must contain a term from U_1 of the form $xe_1 + e_2$, which must, by the previously mentioned order restriction, be equal to a term from $-U_2$ of the form $yf_1 + f_2$. Hence $f_2 - e_2 \in H$. But now it is clear that difference between any two terms of the form $x'e_1 + e_2$ and $y'f_1 + f_2$, where $x', y' \in \mathbb{Z}$, must also be an element from H.

If $e_1 = f_1$, then $H \cong C_m$ and $\mathsf{D}(H) = \mathsf{D}(C_m) = m$. In this case, $B = b_1 \cdot \ldots \cdot b_\ell$ consists entirely of terms of the form $xe_1 + e_2$ while $C = c_1 \cdot \ldots \cdot c_\ell$ consists entirely of terms of the form $yf_1 + f_2$, where $\ell = |B| = |C| \ge m + 1$. Consequently, $(-b_1 + c_1) \cdot \ldots \cdot (-b_m + c_m) \in \mathcal{F}(H)$ is a sequence of $m = \mathsf{D}(H)$ terms from H, meaning $(-B)C$ contains a nontrivial zero-sum subsequence of length at most $2m < 2\ell = |B| + |C| \le |U_3|$. But this contradicts that U_3 is an atom with $(-B)C \mid U_3$. Therefore we may now assume $e_1 \ne f_1$.

In view of $e_1 \ne f_1$ and the previously mentioned order restriction, neither e_1 nor f_1 can be a term from A. Thus every term equal to e_1 in U_1 must be contained in B except possibly one such term equal to w_1. Likewise, every term equal to f_1 in $-U_2$ must be contained in C except possibly one such term equal to w_2. It follows

that $m-2 \le \mathsf{v}_{e_1}(B) \le m-1$ and $m-2 \le \mathsf{v}_{f_1}(C) \le m-1$. Consequently, in view of $|B| = |C| \ge m+1$, there must be subsequences $b_1 \cdot b_2 \mid B$ and $c_1 \cdot c_2 \mid C$ with each term b_i of the form $b_i = x_i' e_1 + e_2$ and each term c_i of the form $c_i = y_i' f_1 + f_2$. Moreover, if $\mathsf{v}_{e_1}(B) = \mathsf{v}_{f_1}(C) = m-2$, then there exists a third term b_3 from B also of the form $b_3 = x_3' e_1 + e_2$ and a third term c_3 from C also of the form $c_3 = y_3' f_1 + f_2$ so that $b_1 \cdot b_2 \cdot b_3 \mid B$ and $c_1 \cdot c_2 \cdot c_3 \mid C$. Observe that $\mathsf{v}_{f_1}(C) < m-1$, as well as $\mathsf{v}_{e_1}(B) < m-1$, is only possible if $U_3 = (-B)C(w_2 - w_1)$.

If $\mathsf{v}_{e_1}(B) = \mathsf{v}_{f_1}(C) = m-1$, then $(-e_1)^{m-1} f_1^{m-1}(-b_1 + c_1) \in \mathcal{F}(H)$ is a sequence of terms from H of length $2m-1 \ge \mathsf{D}(H)$, meaning $(-B)C$ contains a nontrivial zero-sum subsequence of length at most $2m < 2\ell = |B| + |C| \le |U_3|$. But this contradicts that U_3 is an atom with $(-B)C \mid U_3$.

If $\mathsf{v}_{e_1}(B) = \mathsf{v}_{f_1}(C) = m-2$, then $(-e_1)^{m-2} f_1^{m-2}(-b_1 + c_1)(-b_2 + c_2) \cdot (-b_3 + c_3) \in \mathcal{F}(H)$ is a sequence of length $2m-1 \ge \mathsf{D}(H)$, meaning $(-B)C$ contains a nontrivial zero-sum subsequence, contradicting that U_3 is an atom since $U_3 = (-B)C(w_2 - w_1)$.

If $\mathsf{v}_{e_1}(B) = m-1$ and $\mathsf{v}_{f_1}(C) = m-2$, then $(-e_1)^{m-1} f_1^{m-2}(-b_1 + c_1) \cdot (-b_2 + c_2) \in \mathcal{F}(H)$ is a sequence of length $2m-1 \ge \mathsf{D}(H)$, meaning $(-B)C$ contains a nontrivial zero-sum subsequence, contradicting that U_3 is an atom since $U_3 = (-B)C(w_2 - w_1)$.

If $\mathsf{v}_{e_1}(B) = m-2$ and $\mathsf{v}_{f_1}(C) = m-1$, then $(-e_1)^{m-2} f_1^{m-1}(-b_1 + c_1) \cdot (-b_2 + c_2) \in \mathcal{F}(H)$ is a sequence of length $2m-1 \ge \mathsf{D}(H)$, meaning $(-B)C$ contains a nontrivial zero-sum subsequence, contradicting that U_3 is an atom since $U_3 = (-B)C(w_2 - w_1)$, which completes CASE 1.

CASE 2: U_1 and $-U_2$ are both of type I(a), say

$$U_1 = e_1^{mn-1} \prod_{i=1}^{m} (x_i e_1 + e_2) \quad \text{and} \quad -U_2 = f_1^{mn-1} \prod_{i=1}^{m} (y_i f_1 + f_2)\,.$$

where $\{e_1, e_2\}$ and $\{f_1, f_2\}$ are bases for G with $\mathrm{ord}(e_1) = \mathrm{ord}(f_1) = mn > m$ and $\mathrm{ord}(e_2) = \mathrm{ord}(f_2) = m$.

Since $m, n \ge 2$ with $n \ge 3$ when $m = 2$, we have $mn - 1 > \frac{mn+m}{2} = \frac{\mathsf{D}(G)+1}{2} \ge$ $\ge |A|$. If $e_1 = f_1$, then $\gcd(U_1, -U_2) = A$ implies $|A| \ge \mathsf{v}_{e_1}(U_1) = mn - 1$, contrary to what we just noted. Therefore $e_1 \ne f_1$. On the other hand, since $\mathsf{v}_{e_1}(U_1) = \mathsf{v}_{f_1}(-U_2) = mn - 1 > \frac{\mathsf{D}(G)+1}{2} \ge \mathsf{D}(G) - |A| = |U_1| - |A| = |U_2| - |A|$,

we must have $e_1,\ f_1 \in \mathrm{supp}(A)$. It follows that

$$e_1 = yf_1 + f_2 \qquad \text{and} \qquad f_1 = xe_1 + e_2 \qquad \text{for some } x,\ y \in \mathbb{Z}.$$

Since U_1 contains at most m terms not equal to e_1, we deduce that $\mathsf{v}_{e_1}(A) \geq |A| - m \geq \frac{\mathsf{D}(G)-1}{2} - m = \frac{1}{2}mn - \frac{m}{2} - 1$. However, since $e_1 \neq f_1$ with the highest multiplicity of a term in $-U_2$ other than f_1 being $m-1$, we have

$$\mathsf{v}_{e_1}(A) \leq \mathsf{v}_{yf_1+f_2}(-U_2) \leq m - 1.$$

Hence $\frac{1}{2}mn - \frac{m}{2} - 1 \leq \mathsf{v}_{e_1}(A) \leq m - 1$, implying $n \leq 3$.

Suppose $n = 3$. Then $\mathsf{D}(G) = 4m - 1$ and equality must hold in all estimates used to derive $n \leq 3$ above. In particular, $|A| = \frac{\mathsf{D}(G)-1}{2}$, forcing the case corresponding to $|V_1| = 3$ in Assertion A, and all m terms of U_1 not equal to e_1 must be contained in A. Arguing as in the previous paragraph, we must also have

$$\frac{1}{2}mn - \frac{m}{2} - 1 \leq |A| - m \leq \mathsf{v}_{f_1}(A) \leq \mathsf{v}_{xe_1+e_2}(U_1) \leq m - 1,$$

implying $n \leq 3$. Once more, equality must hold in all these estimates, meaning all m terms of $-U_2$ not equal to f_1 must be contained in A. Consequently,

$$\begin{aligned} U_3 = (-B)C(w_2 - w_1) &= (-e_1)^{2m-1} f_1^{2m-1}(f_1 - e_1) = \\ &= (-e_1)^{2m-1}(xe_1 + e_2)^{2m-1}((x-1)e_1 + e_2). \end{aligned}$$

Since $\sigma(U_3) = 0$, we see that $x \equiv 1 \bmod 3$, and now it is easily noted that $(-e_1)^m(xe_1 + e_2)^m$ is a proper zero-sum subsequence of U_3, contradicting that U_3 is an atom. So we may instead assume $n = 2$.

Since $n = 2$, it follows that $\mathsf{D}(G) = 3m - 1$ and $m \geq 3$. Recall that $e_1 = yf_1 + f_2$ and $f_1 = xe_1 + e_2$. Thus, since $\mathrm{ord}(e_1) = \mathrm{ord}(f_1) = 2m$, we conclude that x and y are both odd, whence

$$me_1 = myf_1 = mf_1 = mxe_1 \qquad \text{with} \qquad \mathrm{ord}(me_1) = \mathrm{ord}(mf_1) = 2. \tag{5.4}$$

If $\mathsf{v}_{-e_1}(-B) \geq m$ and $\mathsf{v}_{f_1}(C) \geq m$, then $(-e_1)^m f_1^m$ is a zero-sum subsequence of U_3 (in view of (5.4)) of length $2m < 3m - 2 = \mathsf{D}(G) - 1 \leq |U_3|$, contradicting that U_3 is an atom. Therefore we may assume either $\mathsf{v}_{-e_1}(-B) < m$ or $\mathsf{v}_{f_1}(C) < m$, say w.l.o.g. $\mathsf{v}_{-e_1}(-B) < m$ (the role of e_1 in U_1 is identical to that of f_1 in $-U_2$).

As noted earlier, $\mathsf{v}_{e_1}(A) \le m-1$. Consequently, if $|V_1| = 2$, then $\mathsf{v}_{-e_1}(-B) = \mathsf{v}_{e_1}(U_1) - \mathsf{v}_{e_1}(A) \ge 2m-1-(m-1) = m$, contrary to our assumption above. Thus we must have $|V_1| = 3$, which is only possible (in view of Assertion A) if $|U_3| = \mathsf{D}(G) = 3m-1$ is odd. Thus $2 \mid m$ and $m \ge 4$.

Applying the above argument when $|V_1| = 3$, we again obtain the contradiction $\mathsf{v}_{-e_1}(U_3) \ge m$ unless $\mathsf{v}_{e_1}(A) = m-1$ and $w_1 = e_1$. It follows that there are at most $|A| - \mathsf{v}_{e_1}(A) = \frac{m}{2}$ terms of A not equal to e_1. Hence, since $f_1 \ne e_1$, we conclude that $\mathsf{v}_{f_1}(A) \le \frac{m}{2}$, implying

$$\mathsf{v}_{f_1}(C) \ge 2m-1-\frac{m}{2}-1 = \frac{3}{2}m-2, \tag{5.5}$$

with equality only possible if $w_2 = f_1$ and $w_2 - w_1 = f_1 - e_1 = (x-1)e_1 + e_2$. Since $\mathsf{v}_{e_1}(A) = m-1$ and $w_1 = e_1$, we have

$$-B = (-e_1)^{m-1} \prod_{i=1}^{m/2} (-x_i e_1 - e_2),$$

where we have appropriately re-indexed the terms $x_i e_1 + e_2$ in U_1 so that the first $\frac{m}{2}$ terms correspond to those from B. Thus

$$U_3 = (-e_1)^{m-1} \left(\prod_{i=1}^{m/2} (-x_i e_1 - e_2) \right) f_1^{\frac{3}{2}m-2} g_1 g_2 =$$

$$= (-e_1)^{m-1} \left(\prod_{i=1}^{m/2} (-x_i e_1 - e_2) \right) (xe_1 + e_2)^{\frac{3}{2}m-2} g_1 g_2$$

with w.l.o.g. $g_1 \in \{f_1, y_1 f_1 + f_2\}$ (by re-indexing the $y_i f_1 + f_2$ appropriately) and $g_2 = w_2 - w_1 = w_2 - e_1$.

If $g_1 = f_1$, let $g = g_1 = f_1 = xe_1 + e_2$. If $g_1 \ne f_1$, the equality must hold in (5.5). In this case, let $g = g_2 = f_1 - e_1 = (x-1)e_1 + e_2$. Regardless, we see that $g = g_j = ze_1 + e_2$ for some $z \in \{x, x-1\}$ and $j \in [1,2]$. To avoid a zero-sum subsequence of

$$(-e_1)^{m-1}(-x_1 e_1 - e_2)(ze_1 + e_2),$$

which would contradict that U_3 is an atom, we must have $x_1 \notin \{z, z-1, \ldots, z-(m-1)\}$ modulo $2m$. On the other hand, in view of (5.4), we have $\sigma((xe_1 + e_2)^m) = me_1$,

so that to avoid a zero-sum subsequence of

$$(-e_1)^{m-1}(xe_1+e_2)^m(-x_1e_1-e_2)(ze_1+e_2),$$

which would contradict that U_3 is an atom in view of $\frac{3}{2}m-2 \geq m$, we must have $x_1 \notin \{m+z, m+z-1, \ldots, m+z-(m-1)\}$ modulo $2m$. However, this leaves no possibilities left for the value of x_1 modulo $2m$, which is a contradiction that concludes CASE 2.

CASE 3: Either U_1 is of type I(b) and $-U_2$ is of type I(a) or else U_1 is of type I(a) and $-U_2$ is of type I(b), say w.l.o.g. the former with

$$U_1 = e_1^{m-1}\prod_{i=1}^{mn}(x_ie_1+e_2) \quad \text{and} \quad -U_2 = f_1^{mn-1}\prod_{i=1}^{m}(y_if_1+f_2),$$

where $\{e_1, e_2\}$ and $\{f_1, f_2\}$ are bases of G with $\mathrm{ord}(e_1) = \mathrm{ord}(f_2) = m$ and $\mathrm{ord}(e_2) = \mathrm{ord}(f_1) = mn > m$.

Since $m, n \geq 2$ with $n \geq 3$ when $m = 2$, we have $\mathsf{v}_{f_1}(-U_2) = mn-1 > > (\mathsf{D}(G)+1)/2 \geq \mathsf{D}(G) - |A| = |U_2| - |A|$, implying $f_1 \in \mathrm{supp}(A)$. Consequently, since f_1 cannot equal e_1 due to $\mathrm{ord}(f_1) = mn > m = \mathrm{ord}(e_1)$, it follows that

$$f_1 = xe_1 + e_2 \quad \text{for some } x \in \mathbb{Z}.$$

Let

$$y = \mathsf{v}_{e_1}(B) \in [0, m-1]. \tag{5.6}$$

Then $\mathsf{v}_{e_1}(A) = m-1-y-\epsilon$, where $\epsilon = 1$ if $|V_1| = 3$ and $w_1 = e_1$, and $\epsilon = 0$ otherwise. Since $f_1 \neq e_1$, it follows that $\mathsf{v}_{f_1}(A) \leq |A| - \mathsf{v}_{e_1}(A) = |A| - m + 1 + y + \epsilon$, implying

$$\mathsf{v}_{f_1}(C) \geq mn - 1 - \delta - |A| + m - 1 - y - \epsilon \geq \frac{1}{2}mn + \frac{1}{2}m - 3 - y, \tag{5.7}$$

where $\delta = 1$ if $|V_1| = 3$ and $w_2 = f_1$, and $\delta = 0$ otherwise. Moreover, the estimate on the far right of (5.7) improves by 1 unless $w_1 = e_1$ and $w_2 = f_2$, in which case $w_2 - w_1 = (x-1)e_1 + e_2$ is a term of U_3. As a result, we see that $U_3(-B)^{-1}$ contains at least $\frac{1}{2}mn + \frac{1}{2}m - 2 - y$ terms from $e_2 + \langle e_1\rangle$, say $c_1 \cdot \ldots \cdot c_s \mid U_3(-B)^{-1}$ with

$$s \geq \frac{1}{2}mn + \frac{1}{2}m - 2 - y \quad \text{and} \quad c_i \in e_2 + \langle e_1\rangle \text{ for all } i. \tag{5.8}$$

On the other hand, per definition of y, we see that $-B$ contains $|B| - y \ge \frac{1}{2}mn + \frac{1}{2}m - 1 - y$ terms from $-e_2 + \langle e_1\rangle$, say $b_1 \cdot \ldots \cdot b_t \mid -B$ with

$$t \ge \frac{1}{2}mn + \frac{1}{2}m - 1 - y \quad \text{and} \quad b_i \in -e_2 + \langle e_1\rangle \ \text{ for all } i. \tag{5.9}$$

Now $e_1 \in \langle e_1\rangle$ and $b_i + c_i \in \langle e_1\rangle$ for all $i \in [1, \min\{s,t\}]$, while $\mathsf D(\langle e_1\rangle) = \mathsf D(C_m) = m$. Moreover, $(\frac{1}{2}mn + \frac{1}{2}m - 2 - y) + y > m - 1$ in view of $m, n \ge 2$ with $n \ge 3$ when $m = 2$. Consequently, we conclude from (5.6), (5.8) and (5.9) that U_3 contains a nontrivial zero-sum subsequence of length at most $2\lceil \frac{1}{2}mn + \frac{1}{2}m - 2 - y\rceil + y \le mn + m - 3 < \mathsf D(G) - 1 \le |U_3|$, contradicting that U_3 is an atom.

CASE 4: U_1 and $-U_2$ are both of type II, say

$$U_1 = f_1^{s_1m-1} f_2^{(n-s_1)m+\epsilon_1} \prod_{i=1}^{m-\epsilon_1} (-y_i f_1 + f_2) \quad \text{and}$$

$$-U_2 = g_1^{s_2m-1} g_2^{(n-s_2)m+\epsilon_2} \prod_{i=1}^{m-\epsilon_2} (-z_i g_1 + g_2),$$

where $\{f_1,\ f_2\}$ and $\{g_1,\ g_2\}$ are generating sets for G such that $\mathrm{ord}(f_2) = \mathrm{ord}(g_2) = mn > m$ and $\mathrm{ord}(f_1), \mathrm{ord}(g_1) \ge 2m$, where $s_1, s_2 \in [1, n-1]$, $\epsilon_1,\ \epsilon_2 \in [1, m-1]$ and $y_i,\ z_i \in [1, m-1]$ for all i, and where $y_1 + \ldots + y_{m-\epsilon_1} = z_1 + \ldots + z_{m-\epsilon_2} = m-1$. Moreover, either $s_1 = 1$ or $mf_1 = mf_2$ and either $s_2 = 1$ or $mg_1 = mg_2$.

Per the remarks after Main Proposition 7, let $\{f_1',\ f_2\}$ and $\{g_1',\ g_2\}$ be bases for G with $\mathrm{ord}(f_1') = \mathrm{ord}(g_1') = m$ such that

$$f_1 = f_1' + \alpha f_2 \quad \text{and} \quad g_1 = g_1' + \beta g_2$$

for some $\alpha,\ \beta \in \mathbb{Z}$. We distinguish two subcases.

CASE 4.1: $n \ge 3$.

Since $n \ge 3$, we have $|A| \ge |B| = |C| \ge (mn + m - 2)/2 \ge 2m - 1$. Thus $\mathsf v_{\{f_1,\, f_2\}}(A) \ge |A| - (m - \epsilon_1) \ge |A| - m + 1 \ge m > m - \epsilon_2$, implying

$$\{f_1, f_2\} \cap \{g_1, g_2\} \ne \varnothing. \tag{5.10}$$

Also, applying Lemma 5 to $B \mid U_1$ and $C \mid -U_2$, we conclude that there exist subsequences $T_1 \mid B$ and $T_2 \mid C$ with $\sigma(T_1) = mf_2$, $\sigma(T_2) = mg_2$ and $|T_1|, |T_2| \le 2m-1$.

Suppose $mf_2 = mg_2$, so that $\sigma(T_1) = \sigma(T_2)$. Then $(-T_1)T_2$ is a zero-sum subsequence of $(-B)C \mid U_3$, which contradicts that U_3 is an atom unless $(-T_1)T_2 = (-B)C = U_3$ with $|B| = |C| = |T_1| = |T_2| = 2m-1$, implying $n = 3$. However, in view of the equality conditions in Lemma 5, this is only possible if

$$U_3 = (-B)C = (-f_1)^{m-1}(-f_2)^{\epsilon_1} \prod_{i=1}^{m-\epsilon_1}(y_i f_1 - f_2) \cdot g_1^{m-1} g_2^{\epsilon_2} \prod_{i=1}^{m-\epsilon_2}(-z_i g_1 + g_2).$$

In particular, the terms $-f_1$, $-f_2$, g_1 and g_2 all occur in U_3 in view of $m \ge 2$ and $\epsilon_1, \epsilon_2 \ge 1$. But then (5.10) ensures that U_3 contains a zero-sum subsequence of length 2, contradicting that U_3 is an atom with $|U_3| = 4m-2 > 2$. So we instead conclude that

$$mf_2 \ne mg_2. \tag{5.11}$$

If $s_1 > 1$ and $s_2 > 1$, then $mf_1 = mf_2$ and $mg_1 = mg_2$, which combined with (5.10) yields $mf_1 = mf_2 = mg_1 = mg_2$, contrary to (5.11). Therefore we may w.l.o.g. assume

$$s_2 = 1 \quad \text{and} \quad \mathsf{v}_{g_1}(-U_2) = m-1.$$

Since $|A| \ge 2m-1 > \mathsf{v}_{g_1}(-U_2) + m - \epsilon_2$, we conclude that $g_2 \in \operatorname{supp}(A)$. Observe that

$$g_2 \ne f_2,$$

for $g_2 = f_2$ would contradict (5.11). In consequence, we find that

$$g_2 = f_1 \quad \text{or} \quad g_2 = -yf_1 + f_2 \ \text{ for some } y \in [1, m-1].$$

This gives two further subcases.

CASE 4.1.1: $g_2 = -yf_1 + f_2$ for some $y \in [1, m-1]$.

Now $g_2 \ne f_2$ as already remarked. Also, $g_2 = -yf_1 + f_2 \ne f_1$ as remarked after Main Proposition 7. Thus (5.10) ensures that we must have

$$g_1 = f_1 \quad \text{or} \quad g_1 = f_2.$$

If $g_1 = f_1$, then f_1 can have multiplicity at most $\mathsf{v}_{g_1}(-U_2) = m-1$ in A, meaning f_2 must also be contained in A in view of $|A| \ge 2m-1$. By an analogous argument, if $g_1 = f_2$, then f_1 must be contained in A. In other words, in both cases, we have

$$f_1,\ f_2 \in \operatorname{supp}(A).$$

Suppose that $g_1 = f_1$. Then, as $f_2 \in \operatorname{supp}(A)$ but $f_2 \neq f_1 = g_1$ and $f_2 \neq g_2$, it follows that $f_2 = -zg_1 + g_2$ for some $z \in [1, m-1]$. Thus

$$f_2 = -zg_1 + g_2 = -zf_1 + g_2 = -zf_1 - yf_1 + f_2,$$

implying that $(z+y)f_1 = 0$ with $z+y \in [2, 2m-2]$. However, since $\operatorname{ord}(f_1) \ge 2m$, this is not possible. So we instead conclude that

$$g_1 = f_2.$$

Now $f_1 \in \operatorname{supp}(A)$ but $g_1 = f_2 \neq f_1$ and $g_2 = -yf_1 + f_2 \neq f_1$ as remarked after Main Proposition 7. In consequence, $f_1 = -zg_1 + g_2$ for some $z \in [1, m-1]$. Thus

$$f_1' + \alpha f_2 = f_1 = -zg_1 + g_2 = -zf_2 + g_2 = -zf_2 - yf_1 + f_2 = -yf_1' + (1 - z - \alpha y)f_2,$$

which, in view of $y \in [1, m-1]$, is only possible if $y = m-1$ and

$$\alpha \equiv 1 - z - \alpha y \equiv 1 - z - \alpha(m-1) \bmod mn.$$

The above congruence implies that $z \equiv 1 - \alpha m \bmod mn$, which, in view of $z \in [1, m-1]$, is only possible if $z = 1$ and $\alpha m \equiv 0 \bmod mn$. Thus $mf_1 = m(f_1' + \alpha f_2) = mf_1' + \alpha m f_2 = 0$, contradicting that $\operatorname{ord}(f_1) \ge 2m$ for type II.

CASE 4.1.2: $g_2 = f_1$.

If $s_1 > 1$, then $mg_2 = mf_1 = mf_2$, contrary to (5.11). Therefore

$$s_1 = 1 \qquad \text{and} \qquad \mathsf{v}_{f_1}(U_1) = m-1.$$

Since $|A| \geq 2m-1 > \mathsf{v}_{f_1}(-U_2)+m-\epsilon_1$, we conclude that $f_2 \in \operatorname{supp}(A)$. As already remarked, we have $f_2 \neq g_2$. Consequently,

$$f_2 = g_1 \quad \text{or} \quad f_2 = -zg_1 + g_2 \text{ for some } z \in [1, m-1].$$

Observe, however, that the roles of U_1 and $-U_2$ are now symmetric (we have the same information about $-U_2$ that we did about U_1 before CASE 4.1.1). Thus, if $f_2 = -zg_1 + g_2$ for some $z \in [1, m-1]$, then, swapping the roles of U_1 and $-U_2$, we fall under the hypotheses of CASE 4.1.1, and the proof is complete by those prior arguments. So, combined with the subcase hypothesis, we may instead assume

$$f_2 = g_1 \quad \text{and} \quad f_1 = g_2. \tag{5.12}$$

Now $\mathsf{v}_{f_1}(A) \leq m-1$ and $\mathsf{v}_{f_2}(A) = \mathsf{v}_{g_1}(A) \leq m-1$ in view of $s_1 = s_2 = 1$. Consequently, since $|A| \geq 2m-1$, we conclude from (5.12) that $-yf_1 + f_2 = -zg_1 + g_2 = -zf_2 + f_1$ for some $y,\ z \in [1, m-1]$. Thus

$$0 = (1+y)f_1 - (1+z)f_2 = (1+y)f_1' + (\alpha(1+y) - 1 - z)f_2,$$

which, in view of $y \in [1, m-1]$, is only possible if $y = m-1$ and

$$0 \equiv \alpha(1+y) - 1 - z \equiv \alpha m - 1 - z \bmod mn.$$

The above congruence implies that $z \equiv \alpha m - 1 \bmod mn$, which, in view of $z \in [1, m-1]$, is only possible if $z = m-1$ and $\alpha m \equiv m \bmod mn$. Thus $mg_2 = mf_1 = m(f_1' + \alpha f_2) = mf_2$, contradicting (5.11) and completing CASE 4.1.

CASE 4.2: $n = 2$.

Since $s_1,\ s_2 \in [1, n-1] = [1, 1]$, we conclude that $s_1 = s_2 = 1$. We also have $m \geq 3$ and $\epsilon_1,\ \epsilon_2 \geq 2$ in view of $n = 2$ (the latter per (d) and (e) in Main Proposition 7). Now

$$U_1 = f_1^{m-1} f_2^{m+\epsilon_1} \prod_{i=1}^{m-\epsilon_1} (-y_i f_1 + f_2) \quad \text{and} \quad -U_2 = g_1^{m-1} g_2^{m+\epsilon_2} \prod_{i=1}^{m-\epsilon_2} (-z_i g_1 + g_2)$$

with $\operatorname{ord}(f_1) = \operatorname{ord}(f_2) = \operatorname{ord}(g_1) = \operatorname{ord}(g_2) = 2m$ and (as remarked after Main Proposition 7)

$$mf_1 = mf_2 = mg_1 = mg_2. \tag{5.13}$$

Observe that

$$\frac{3}{2}m - 1 \le |A| \le \frac{3}{2}m \quad \text{and} \quad \frac{3}{2}m - 1 \le |B| = |C| \le \frac{3}{2}m - \frac{1}{2}.$$

If neither f_2 nor g_2 is a term from A, then $(-f_2)^m g_2^m$ will be a subsequence of U_3 which is zero-sum (in view of (5.13)) and has length $2m < 3m - 2 \le |U_3|$, contradicting that U_3 is an atom. Therefore

$$f_2 \in \operatorname{supp}(A) \quad \text{or} \quad g_2 \in \operatorname{supp}(A). \tag{5.14}$$

We handle several subcases.

CASE 4.2.1: $f_2 = g_2$.

We may w.l.o.g. assume $\epsilon_1 \le \epsilon_2$. Then $\mathsf{v}_{f_2}(A) = m + \epsilon_1$ and $\mathsf{v}_{f_2}(B) = 0$. As remarked after Main Proposition 7, we have $y_i \le \epsilon_1$ and $z_j \le \epsilon_2$ for all i and j. Also, since there are precisely $2m > 3m - 1 - (\frac{3}{2}m - 1) \ge \mathsf{D}(G) - |B|$ terms of U_1 of the form $-xf_1 + f_2$ with $x \in [0, m-1]$, and since $\mathsf{v}_{f_2}(B) = 0$, it follows that

$$yf_1 - f_2 \in \operatorname{supp}(-B) \quad \text{for some } y \in [1, \epsilon_1] \subseteq [1, m-1].$$

Now, since $\mathsf{v}_{f_2}(B) = 0$, we have $\mathsf{v}_{f_1}(B) \ge |B| - (m - \epsilon_1) \ge \frac{m}{2} - 1 + \epsilon_1 \ge \epsilon_1$. Thus $(-f_1)^y(yf_1 - f_2)$ is a subsequence of $-B$. If $f_2 = g_2 \in \operatorname{supp}(C)$, then $(-f_1)^y(yf_1 - f_2)f_2$ would be a zero-sum subsequence of U_3 of length $y+2 \le m+1 < 3m-2 \le |U_3|$, contradicting that U_3 is an atom. Therefore we may instead assume $\mathsf{v}_{g_2}(C) = 0$. But now, repeating the prior arguments for $-U_2$ instead of U_1, we find that

$$-zg_1 + g_2 = -zg_1 + f_2 \in \operatorname{supp}(C) \quad \text{for some } z \in [1, \epsilon_2] \subseteq [1, m-1]$$

and that $\mathsf{v}_{g_1}(C) \ge |C| - (m - \epsilon_2) \ge \frac{m}{2} - 1 + \epsilon_2 \ge \epsilon_2$. Thus $g_1^z(-zg_1 + f_2)(-f_1)^y(yf_1 - f_2)$ is a zero-sum subsequence of U_3 of length $z+y+2 \le \epsilon_1 + \epsilon_2 + 2 \le 2m < 3m-2 \le |U_3|$ (in view of $m \ge 3$), contradicting that U_3 is an atom and completing the subcase.

CASE 4.2.2: $f_2 = g_1$ or $g_2 = f_1$.

By symmetry, we may w.l.o.g. assume

$$f_2 = g_1.$$

Then $\mathsf{v}_{f_2}(A) = \mathsf{v}_{g_1}(A) = m-1$, meaning $\mathsf{v}_{g_1}(C) = \mathsf{v}_{f_2}(C) = 0$ and $\epsilon_1 + 1 \ge \mathsf{v}_{-f_2}(-B) \ge \epsilon_1$.

Suppose $g_2 = f_1$. Then $\mathsf{v}_{f_1}(A) = \mathsf{v}_{g_2}(A) = m-1$, yielding $\mathsf{v}_{g_2}(C) = \mathsf{v}_{f_1}(C) \ge \epsilon_2$ and $\frac{3}{2}m \ge |A| \ge \mathsf{v}_{f_2}(A) + \mathsf{v}_{f_1}(A) = 2m-2$, which is only possible if $3 \le m \le 4$ with $|A| = 2m-2$ and $|V_1| = 2$. In this case,

$$(-f_2)^{\epsilon_1} f_1^{\epsilon_2} \prod_{i=1}^{m-\epsilon_1} (y_i f_1 - f_2) \prod_{i=1}^{m-\epsilon_2} (-z_i f_2 + f_1) \mid U_3.$$

Thus, if $\epsilon_1 = \epsilon_2 = m-1$, then $\prod_{i=1}^{m-\epsilon_1}(y_i f_1 - f_2) \prod_{i=1}^{m-\epsilon_2}(-z_i f_2 + f_1)$ is a proper subsequence of U_3 with sum $(m-1)f_1 - f_2 - (m-1)f_2 + f_1 = mf_1 - mf_2 = 0$ (in view of (5.13)), contradicting that U_3 is an atom. Therefore we may w.l.o.g. assume that $\epsilon_1 \le m-2$. Hence, since $\epsilon_i \in [2, m-1]$ for $n = 2$, it follows that $m = 4$ with $2 \le \epsilon_1 \le m-2$, so that $\epsilon_1 = 2$. Consequently, since $y_1 + y_2 = m-1 = 3$ with $y_i \in [1, \epsilon_1] = [1, 2]$, we see that w.l.o.g. $y_1 = 1$ and $y_2 = 2$. Likewise, if $\epsilon_2 = 2$, then w.l.o.g. $z_1 = 1$ and $z_2 = 2$, while if $\epsilon_2 = 3 = m-1$, then $z_1 = m-1 = 3$. In the former case, $(-2f_2 + f_1)(f_1 - f_2)(2f_1 - f_2)$ is a proper zero-sum subsequence of U_3 (in view of (5.13) and $m = 4$), while in the latter case, $(-3f_2 + f_1)(2f_1 - f_2)f_1$ is a proper zero-sum subsequence of U_3 (again, in view of (5.13) and $m = 4$), both contradicting that U_3 is an atom. So we instead conclude that

$$g_2 \ne f_1.$$

Suppose next that $f_1,\ g_2 \in \mathrm{supp}(A)$. In view of $g_2 \ne f_1$ and $g_1 = f_2$, this is only possible if

$$f_1 = -zg_1 + g_2 = -zf_2 + g_2 \qquad \text{and} \qquad g_2 = -yf_1 + f_2$$
$$\text{for some } y \in [1, m-1] \text{ and } z \in [1, m-1].$$

Thus

$$f_1' + \alpha f_2 = f_1 = -zf_2 + g_2 = -zf_2 - yf_1 + f_2 = -yf_1' + (1 - z - \alpha y)f_2.$$

However, since $y \in [1, m-1]$, this is only possible if $y = m-1$ and $1 - z - \alpha y = 1 - z - \alpha(m-1) \equiv \alpha \bmod 2m$. Hence $z \equiv 1 - \alpha m \bmod 2m$, which, in view of $z \in [1, m-1]$, is only possible if $z = 1$ with $\alpha m \equiv 0 \bmod 2m$, implying $mf_1 = mf_1' + \alpha m f_2 = 0$. Since this contradicts that $\mathrm{ord}(f_1) = 2m > m$, we may now assume

$$f_1 \notin \mathrm{supp}(A) \quad \text{or} \quad g_2 \notin \mathrm{supp}(A).$$

Suppose $f_1 \notin \operatorname{supp}(A)$. Then $A \mid f_2^{m-1} \prod_{i=1}^{m-\epsilon_1}(-y_i f_1 + f_2)$. If $|\operatorname{supp}(A)| \ge 3$, then, since $g_1 = f_2$, we must have $-yf_1+f_2 = -zg_1+g_2$ and $-y'f_1+f_2 = -z'g_1+g_2$ for some distinct $y,\ y' \in [1, m-1]$ and distinct $z,\ z' \in [0, m-1]$, implying

$$(y-y')f_1' + \alpha(y-y')f_2 = (y-y')f_1 = (z-z')g_1 = (z-z')f_2.$$

Thus $y \equiv y' \bmod m$, which, in view of $y,\ y' \in [1, m-1]$, forces $y = y'$, contrary to assumption. Therefore we must instead have

$$|\operatorname{supp}(A)| = 2.$$

Let $-yf_1 + f_2$ be the element of $\operatorname{supp}(A) \setminus \{f_2\}$, where $y \in [1, m-1]$. Then $-yf_1 + f_2$ has multiplicity at least $\mathsf{v}_{-yf_1+f_2}(A) = |A| - \mathsf{v}_{f_2}(A) = |A| - (m-1) \ge \frac{m}{2}$. Consequently, $\frac{m}{2}y \le \mathsf{v}_{-yf_1+f_2}(A)y \le y_1 + \ldots + y_{m-\epsilon_1} = m-1$, which together with $y \in [1, m-1]$ ensures that $y = 1$, so that $-f_1 + f_2 \in \operatorname{supp}(A)$. Since $-f_1 + f_2 \in \operatorname{supp}(A)$ with $g_1 = f_2$, it follows that

$$-f_1 + f_2 = -zg_1 + g_2 = -zf_2 + g_2 \in \operatorname{supp}(A) \quad \text{for some } z \in [0, \epsilon_2].$$

If $z = 0$, then $mg_2 = -mf_1 + mf_2 = 0$ (in view of (5.13)), contradicting that $\operatorname{ord}(g_2) = 2m$. Therefore we must have $z \in [1, m-1]$. Then $-zg_1 + g_2 = -f_1 + f_2$ has multiplicity at least $\mathsf{v}_{-zg_1+g_2}(A) = \mathsf{v}_{-f_1+f_2}(A) = \mathsf{v}_{-yf_1+f_2}(A) \ge \frac{m}{2}$. Consequently, $\frac{m}{2}z \le \mathsf{v}_{-zg_1+g_2}(A)z \le z_1 + \ldots + z_{m-\epsilon_2} = m-1$, which together with $z \in [1, m-1]$ ensures that $z = 1$. Thus

$$-f_1 + f_2 = -zg_1 + g_2 = -zf_2 + g_2 = -f_2 + g_2.$$

Hence $g_2 = -f_1 + 2f_2$ and $\operatorname{supp}(A) = \{f_2,\ -f_1 + f_2\} = \{g_1,\ -g_1 + g_2\}$.

Since $f_1 \notin \operatorname{supp}(A)$, we have

$$\mathsf{v}_{-f_1}(-B) \ge \mathsf{v}_{f_1}(U_1) - 1 = m-2, \tag{5.15}$$

with equality only possible if $|V_1| = 3$ with $w_1 = f_1$. Since $f_2 = g_1$ with $\mathsf{v}_{f_2}(A) = \mathsf{v}_{g_1}(A) = m-1$, we have

$$\mathsf{v}_{-f_2}(-B) \ge \mathsf{v}_{f_2}(U_1) - 1 - \mathsf{v}_{f_2}(A) = \epsilon_1 \ge 2$$

(recall that $\epsilon_2 \ge 2$ for $n = 2$). Since $g_2 = -f_1 + 2f_2 \notin \{-f_1 + f_2, f_2 = g_1\} = \operatorname{supp}(A)$,

we have

$$\mathsf{v}_{-f_1+2f_2}(C) = \mathsf{v}_{g_2}(C) \geq \mathsf{v}_{g_2}(-U_2) - 1 = m + \epsilon_2 - 1 \geq m + 1.$$

Since $-yf_1 + f_2 = -f_1 + f_2 \in \mathrm{supp}(A)$, we know $y_k = 1$ for some $k \in [1, m - \epsilon_1]$. If $y_i = 1$ for all $i \in [1, m - \epsilon_1]$, then $y_1 + \ldots + y_{m-\epsilon_1} = m - 1$ forces $\epsilon_1 = 1$, contradicting that $\epsilon_1 \geq 2$ for $n = 2$. Therefore we may instead assume there is some $y_j \geq 2$ with $j \in [1, m - \epsilon_1]$. Then, since $y_1 + \ldots + y_{m-\epsilon_1} = m - 1$ with at least one $y_k = y = 1$, we conclude that $2 \leq y_j \leq m - 2$, implying

$$m \geq 4.$$

Since $\mathrm{supp}(A) = \{f_2, -f_1 + f_2\}$, we must either have $y_j f_1 - f_2 \in \mathrm{supp}(-B)$ or $w_1 = -y_j f_1 + f_2$. In the former case,

$$(y_j f_1 - f_2)(-f_1 + 2f_2)(-f_1)^{y_j - 1}(-f_2)$$

is a zero-sum subsequence of U_3 of length $y_j + 2 \leq m < 3m - 2 \leq |U_3|$, contradicting that U_3 is an atom. In the latter case, $|V_3| = 3$ and we have strict inequality in (5.15), in which case

$$(-f_1)^{m-1}(-f_2)^2(-f_1 + 2f_2)^{m+1}$$

is a zero-sum subsequence of U_3 having length $2m + 2 < 3m - 1 = |U_3|$ (in view of $m \geq 4$), contradicting that U_3 is an atom. So we may now assume

$$f_1 \in \mathrm{supp}(A) \quad \text{and} \quad g_2 \notin \mathrm{supp}(A).$$

Since $g_2 \notin \mathrm{supp}(A)$, we have

$$A \mid g_1^{m-1} \prod_{i=1}^{m-\epsilon_2} (-z_i g_1 + g_2) = f_2^{m-1} \prod_{i=1}^{m-\epsilon_2} (-z_i f_2 + g_2).$$

Thus, since $f_1 \in \mathrm{supp}(A)$, we have

$$f_1 = -xg_1 + g_2 = -xf_2 + g_2 \quad \text{for some } x \in [1, m - 1].$$

If $\mathrm{supp}(A) \neq \{f_2,\ f_1\}$, then $-yf_1 + f_2 = -zg_1 + g_2$ for some $y,\ z \in [1, m-1]$. In this case,

$$-yf_1'+(1-\alpha y)f_2 = -yf_1+f_2 = -zg_1+g_2 = -zf_2+(xf_2+f_1) = f_1'+(x-z+\alpha)f_2.$$

Thus, since $y \in [1, m-1]$, it follows that $y = m-1$ with $x - z \equiv 1 - \alpha m \bmod 2m$. Since $x - z \in [-(m-2), m-2]$ (in view of $x,\ y \in [1, m-1]$), we conclude that $x - z = 1$ with $\alpha m \equiv 0 \bmod 2m$. But this means $mf_1 = mf_1' + \alpha m f_2 = 0$, contradicting that $\mathrm{ord}(f_1) = 2m$. Therefore, we instead conclude that

$$\mathrm{supp}(A) = \{f_1,\ f_2\},$$

whence $\mathsf{v}_{-xg_1+g_2}(A) = \mathsf{v}_{f_1}(A) = |A| - \mathsf{v}_{f_2}(A) = |A| - m + 1 \geq \frac{m}{2}$. Thus $f_1 = -xg_1 + g_2 = -g_1 + g_2$ in view of $\frac{m}{2}x \leq \mathsf{v}_{-xg_1+g_2}(A)x \leq z_1 + \ldots + z_{m-\epsilon_2} = m-1$ with $x \in [1, m-1]$. But this implies $mf_1 = -mg_1 + mg_2 = 0$ (in view of (5.13)), contradicting that $\mathrm{ord}(f_1) = 2m$, which completes CASE 4.2.2.

CASE 4.2.3: $f_1 = g_1$

In this case, $\mathsf{v}_{f_1}(A) = \mathsf{v}_{g_1}(A) = m-1$ and $\mathsf{v}_{f_1}(B) = \mathsf{v}_{g_1}(C) = 0$. In view of (5.14), we may w.l.o.g. assume $f_2 \in \mathrm{supp}(A)$. We have $f_2 \neq f_1 = g_1$ while we can assume $f_2 \neq g_2$ else CASE 4.2.1 completes the proof. Therefore

$$f_2 = -xg_1 + g_2 = -xf_1 + g_2 \quad \text{for some } x \in [1, m-1]. \tag{5.16}$$

Likewise, if $g_2 \in \mathrm{supp}(A)$, then $g_2 = -yf_1 + f_2$ for some $y \in [1, m-1]$, implying

$$f_2 = -xf_1 + g_2 = -xf_1 - yf_1 + f_2,$$

in which case $(x+y)f_1 = 0$ with $x + y \in [2, 2m-2]$, contradicting that $\mathrm{ord}(f_1) = 2m$. Therefore we conclude that $g_2 \notin \mathrm{supp}(A)$. As a result, all elements in $\mathrm{supp}(A) \setminus \{g_1\}$ have the form $-z_ig_1 + g_2 = -z_if_1 + g_2$ with $z_i \in [1, m-1]$.

Let $-zg_1 + g_2 \in \mathrm{supp}(A) \setminus \{g_1\}$ be arbitrary. Let us show that $z \geq x$. If $z = x$, this is trivial, so suppose $z \neq x$. Then $-yf_1 + f_2 = -zg_1 + g_2 = -zf_1 + g_2$ for some $y \in [1, m-1]$. In this case, (5.16) implies

$$-yf_1 + f_2 = -zf_1 + g_2 = -zf_1 + (xf_1 + f_2),$$

yielding $(x-z+y)f_1 = 0$. Consequently, since $\operatorname{ord}(f_1) = 2m$ with $x-z+y \in [-(m-1)+2, 2(m-1)-1] = [-m+3, 2m-3]$, we see that $z = x+y \geq x+1$, as claimed.

All terms of A not equal to $g_1 = f_1$ have the form $-z_i g_1 + g_2$. There are at least $|A| - \mathsf{v}_{g_1}(A) = |A| - m + 1 \geq \frac{m}{2}$ such terms all with $z_i \geq x$ as shown above. Consequently, $\frac{m}{2}x \leq z_1 + \ldots + z_{m-\epsilon_2} = m-1$, which implies $x = 1$. Hence

$$f_2 = -xf_1 + g_2 = -f_1 + g_2,$$

which yields $mf_2 = -mf_1 + mg_2 = 0$ (in view of (5.13)), contradicting that $\operatorname{ord}(f_2) = 2m$ and completing the subcase.

CASE 4.2.4: $\{f_1,\ f_2\} \cap \{g_1,\ g_2\} = \varnothing$.

Let

$$a_i = \mathsf{v}_{-if_1+f_2}(A) \quad \text{and} \quad b_i = \mathsf{v}_{-ig_1+g_2}(A) \quad \text{for } i \in [1, m-1].$$

Let

$$c = \left| \gcd\left(\prod_{i=1}^{m-\epsilon_2} (-z_i g_1 + g_2),\ \prod_{i=1}^{m-\epsilon_1} (-y_i f_1 + f_2) \right) \right|.$$

Thus c counts the number of terms of A simultaneously equal to some $-y_i f_1 + f_2$ as well as some $-z_j g_1 + g_2$. In view of the hypothesis $\{f_1,\ f_2\} \cap \{g_1,\ g_2\} = \varnothing$, we see that every term of A is either equal to some $-y_i f_1 + f_2$ or to some $-z_j g_1 + g_2$. As a result, the inclusion-exclusion principle gives

$$\sum_{i=1}^{m-1} a_i + \sum_{i=1}^{m-1} b_i - c = |A| \geq \frac{3}{2}m - 1. \tag{5.17}$$

Note $-f_1 + f_2$ and $-g_1 + g_2$ have order m (in view of (5.13)), meaning $\{-f_1+f_2,\ -g_1+g_2\} \cap \{f_1,\ f_2,\ g_1,\ g_2\} = \varnothing$. Consequently, if $-f_1 + f_2$ occurs in A, then it must be equal to some $-zg_1 + g_2$ with $z \in [1, m-1]$. It follows that $c \geq a_1$. Likewise, if $-g_1 + g_2$ occurs in A, then it must be equal to some $-yf_1 + f_2$, so that $c \geq b_1$. Averaging these estimates, we obtain

$$c \geq \frac{a_1 + b_1}{2}.$$

Applying this estimate in (5.17) along with the pigeon-hole principle, we conclude that either

$$\frac{1}{2}a_1 + \sum_{i=2}^{m-1} a_i \ge \frac{3}{4}m - \frac{1}{2} \quad \text{or} \quad \frac{1}{2}b_1 + \sum_{i=2}^{m-1} b_i \ge \frac{3}{4}m - \frac{1}{2},$$

and we w.l.o.g. assume the former:

$$\frac{1}{2}a_1 + \sum_{i=2}^{m-1} a_i \ge \frac{3}{4}m - \frac{1}{2}. \tag{5.18}$$

By definition of the a_i, we have

$$a_1 + \sum_{i=2}^{m-1} 2a_i \le a_1 + 2a_2 + 3a_3 + \ldots + (m-1)a_1 \le y_1 + \ldots + y_{m-\epsilon_1} = m - 1. \tag{5.19}$$

Combining (5.18) and (5.19) yields

$$\frac{3}{2}m - 1 \le 2\left(\frac{a_1}{2} + \sum_{i=2}^{m-1} a_i\right) \le m - 1,$$

which is a contradiction, concluding CASE 4.

If $|U_3| = \mathsf{D}(G)$, then it possible to also apply Main Proposition 7 to U_3 and (by symmetry) re-index the U_i with $i \in [1, 3]$ in any fashion. Consequently, if one of U_1, U_2 or U_3 has the same type from among I(a), I(b) and II, then we may w.l.o.g. re-index the U_i so that U_1 and $-U_2$ have the same type and apply CASE 1, 2 or 4 to yield the desired conclusion (note U_i and $-U_i$ have the same type). On the other hand, if U_1, U_2 and U_3 have distinct types I(a), I(b) and II, then we my re-index the U_i so that U_1 has type I(b) and $-U_2$ has type I(a), in which case CASE 3 completes the proof. In summary, the proof is now complete when $|U_3| = \mathsf{D}(G)$, so we instead assume

$$|U_3| = \mathsf{D}(G) - 1.$$

By Assertion A, this is only possible if

$$|V_1| = 2, \quad |A| = \frac{\mathsf{D}(G)+1}{2} \quad \text{and}$$
$$|B| = |C| = \frac{\mathsf{D}(G)-1}{2} \quad \text{with} \quad \mathsf{D}(G) = mn + m - 1 \text{ odd},$$

which we now assume for the final two cases of the proof, where by symmetry we now assume $-U_2$ has type II.

CASE 5: U_1 is of type I(b) and $-U_2$ is of type II, say

$$U_1 = e_1^{m-1} \prod_{i=1}^{mn} (x_i e_1 + e_2) \quad \text{and} \quad -U_2 = f_1^{sm-1} f_2^{(n-s)m+\epsilon} \prod_{i=1}^{m-\epsilon} (-y_i f_1 + f_2),$$

where $\{e_1, e_2\}$ is a basis for G with $\mathrm{ord}(e_2) = mn > m$ and $\mathrm{ord}(e_1) = m$, where $\{f_1, f_2\}$ is a generating set for G with $\mathrm{ord}(f_2) = mn$ and $\mathrm{ord}(f_1) \geq 2m$, and where $y_1 + \ldots + y_{m-\epsilon} = m - 1$ with $y_i \in [1, m-1]$, $\epsilon \in [1, m-1]$ and $s \in [1, n-1]$. Moreover, either $s = 1$ or $mf_1 = mf_2$, with both holding when $n = 2$.

Since $|A| \geq \frac{3}{2}m > m - 1$, we must have $f_\nu \in \mathrm{supp}(A)$ for some $\nu \in [1, 2]$. Since $\mathrm{ord}(f_\nu) \geq 2m > m = \mathrm{ord}(e_1)$, we cannot have $f_\nu = e_1$. Thus $f_\nu \in \langle e_1 \rangle + e_2$. It is easily noted that any $g \in \langle e_1 \rangle + e_2$ has $\mathrm{ord}(g) = \mathrm{ord}(e_2) = mn$. Moreover, U_1 will also have type I(b) using the basis $\{e_1, g\}$ replacing each x_i with $x_i - \alpha$, where $g = \alpha e_1 + e_2$. Consequently, since $f_\nu \in \langle e_1 \rangle + e_2$ for some $\nu \in [1, 2]$, we see that we may w.l.o.g. assume

$$f_1 = e_2 \quad \text{or} \quad f_2 = e_2. \tag{5.20}$$

CASE 5.1: $n \geq 3$

Let us first show that

$$mf_2 = me_2. \tag{5.21}$$

If $s > 1$, then this follows from Main Proposition 7 and (5.20). If $s = 1$, then $|A| = \frac{mn+m}{2} \geq 2m > 2m - 2$ (in view of $n \geq 3$), whence $f_2 \in \mathrm{supp}(A)$. Hence, by the argument above CASE 5.1, we may w.l.o.g. assume $f_2 = e_2$, implying $mf_2 = me_2$ in this case as well. Thus (5.21) is established.

Let $H = \langle me_2 \rangle$. Then $G/H \cong C_m^2$. Since $n \geq 3$, we have $|C| = |B| = \frac{mn+m-2}{2} \geq 2m - 1 = \mathsf{D}(G/H)$. Let $B' \mid B$ be a subsequence with $|B'| = 2m - 1$

and let $B' = e_1^t \cdot b_1 \cdot \ldots \cdot b_{2m-1-t}$, where $\mathsf{v}_{e_1}(B') = t \in [0, m-1]$. Then we may w.l.o.g. assume $b_i = x_i e_1 + e_2$ for $i \in [1, 2m-1-t]$. Since $2m-1-t \le 2m-1$ and since $t \le m-1$, it is readily seen that the only way B' can contain a nontrivial subsequence $T \mid B'$ with $\sigma(T) \in H = \langle me_2 \rangle$ is if T contains precisely m terms from $b_1 \cdot \ldots \cdot b_{2m-1-t}$, in which case $\sigma(T) = me_2$. Consequently, since $|B'| = 2m-1 = \mathsf{D}(G/H)$, we conclude that there exits a subsequence $T \mid B'$ with

$$\sigma(T) = me_2 = mf_2 \qquad \text{and} \qquad |T| \le m + t \le 2m-1.$$

Moreover, T will be a proper subsequence of B unless $n = 3$ (so that $2m-1 = |B| = |B'| = |T|$) and (w.l.o.g. re-indexing the $x_i e_1 + e_2$)

$$B = e_1^{m-1} \prod_{i=1}^{m} (x_i e_1 + e_2) \quad \text{with} \quad \sum_{i=1}^{m} x_i \equiv 1 \bmod m.$$

Since $|C| \ge 2m-1$, Lemma 5 ensures that there is a subsequence $R \mid C$ with $\sigma(R) = mf_2$ and $|R| \le 2m-1$. Moreover, R will be a proper subsequence unless $n = 3$ and

$$C = f_1^{m-1} f_2^{\epsilon} \prod_{i=1}^{m-\epsilon} (-y_i f_1 + f_2).$$

Now $(-T)R$ is a nontrivial zero-sum subsequence of $(-B)C = U_3$. Since U_3 is an atom, this is only possible if $T = B$ and $R = C$. Thus $n = 3$ and

$$U_3 = (-e_1)^{m-1} \prod_{i=1}^{m} (-x_i e_1 - e_2) f_1^{m-1} f_2^{\epsilon} \prod_{i=1}^{m-\epsilon} (-y_i f_1 + f_2),$$

where $\sum_{i=1}^{m} x_i \equiv 1 \bmod m$ and $\sum_{i=1}^{m-\epsilon} y_i = m-1$. Since $\mathsf{v}_{f_2}(-U_2) = (n-s)m + \epsilon \ge m + \epsilon > \epsilon$, we conclude that $f_2 \in \mathrm{supp}(A)$, whence (as argued before CASE 5.1) we may w.l.o.g. assume $e_2 = f_2$. As a result, we see that $(-x_1 e_1 - e_2)(-y_1 f_1 + e_2) f_1^{y_1} (-e_1)^z$, where $z \in [0, m-1]$ is the integer such that $z + x_1 \equiv 0 \bmod m$, will be a zero-sum subsequence of U_3 of length $2 + y_1 + z \le 2m < 4m - 2 = |U_3|$, contradicting that U_3 is an atom.

CASE 5.2: $n = 2$.

This is similar to CASE 4.2, we now have $\mathrm{ord}(e_2) = \mathrm{ord}(f_2) = \mathrm{ord}(f_1) = 2m$, $s = 1$, $\epsilon \ge 2$, $m \ge 4$ even (since $\mathsf{D}(G) = 3m - 1$ is odd), and

$$mf_1 = mf_2 = me_2, \tag{5.22}$$

with

$$U_1 = e_1^{m-1} \prod_{i=1}^{2m} (x_i e_1 + e_2) \quad \text{and} \quad -U_2 = f_1^{m-1} f_2^{m+\epsilon_2} \prod_{i=1}^{m-\epsilon} (-y_i f_1 + f_2).$$

We handle several subcases.

CASE 5.2.1: $e_1 = -f_1 + f_2$.

Let t be the number of terms from C of the form $-yf_1 + f_2$ with $y \in [1, m-1]$. Then, since $e_1 = -f_1 + f_2$, we see that $\mathsf{v}_{e_1}(A) \le m - \epsilon - t$, so that

$$\mathsf{v}_{-e_1}(-B) \ge \epsilon - 1 + t. \tag{5.23}$$

By (5.20), we have $f_1 = e_2$ or $f_2 = e_2$. In either case, the hypothesis $e_1 = -f_1 + f_2$ ensures that $f_1,\ f_2 \in \langle e_1 \rangle + e_2$. Thus there are $|C| - t = \frac{3}{2}m - 1 - t$ terms of C from $\langle e_1 \rangle + e_2$, say $c_1 \cdot \ldots \cdot c_{\ell_1} \mid C$ with $c_i \in \langle e_1 \rangle + e_2$ and $\ell_1 = \frac{3}{2}m - 1 - t$, and there are (by (5.23))

$$\ell_2 := |B| - \mathsf{v}_{-e_1}(-B) \le \frac{3}{2}m - 1 - (\epsilon - 1 + t) = \frac{3}{2}m - \epsilon - t \le \frac{3}{2}m - 2 - t$$

terms of $-B$ from $\langle e_1 \rangle - e_2$, say $b_1 \cdot \ldots \cdot b_{\ell_2} \mid -B$ with $b_i \in \langle e_1 \rangle - e_2$ and $\ell_2 < \ell_1$. Consequently, $(-e_1)^{\mathsf{v}_{-e_1}(-B)}(b_1 + c_1) \cdot \ldots \cdot (b_{\ell_2} + c_{\ell_2}) \in \mathcal{F}(\langle e_1 \rangle)$ is a sequence of terms from $\langle e_1 \rangle \cong C_m$ of length $|B| = \frac{3}{2}m - 1 \ge m = \mathsf{D}(\langle e_1 \rangle)$. Thus the proper (in view of $\ell_1 > \ell_2$) subsequence $(-e_1)^{\mathsf{v}_{-e_1}(-B)} b_1 \cdot \ldots \cdot b_{\ell_2} \cdot c_1 \cdot \ldots \cdot c_{\ell_2}$ of $(-B)C = U_3$ contains a nontrivial zero-sum subsequence, contradicting that U_3 is an atom.

CASE 5.2.2: $f_2 \in \mathrm{supp}(A)$.

In this case, we may assume

$$f_2 = e_2$$

per the argument before CASE 5.1.

First suppose that $e_1 \notin \mathrm{supp}(A)$. Then $\mathsf{v}_{-e_1}(-B) = m-1$. Since $|B| = \frac{3}{2}m - 1 > > m-1$, there must be some $-xe_1 - e_2 \in \mathrm{supp}(-B)$. If $\mathsf{v}_{e_2}(C) = \mathsf{v}_{f_2}(C) > 0$, then $(-xe_1 - e_2)e_2(-e_1)^z$, where $z \in [0, m-1]$ is the integer with $z + x \equiv 0 \bmod m$, will be a zero-sum subsequence of U_3 of length $z + 2 \le m + 1 < 3m - 2 = |U_3|$, contradicting that U_3 is an atom. Therefore we instead assume $\mathsf{v}_{f_2}(C) = 0$. Thus $m - 1 \ge \mathsf{v}_{f_1}(C) \ge |C| - (m - \epsilon) = \frac{m}{2} - 1 + \epsilon \ge \frac{m}{2}$, implying $\epsilon \le \frac{m}{2}$, and there are at least $|C| - m + 1 \ge \frac{m}{2} > 0$ terms in C of the form $-y_i f_1 + e_2$ with $y_i \in [1, \epsilon] \subseteq [1, \frac{m}{2}]$. Let $-yf_1 + e_2 \in \mathrm{supp}(C)$ with $y \in [1, \frac{m}{2}]$ be one such term. Then $f_1^y(-yf_1 + e_2)(-xe_1 - e_2)(-e_1)^z$, where $z \in [0, m-1]$ is the integer such that $x + z \equiv 0 \bmod 0$, is a zero-sum subsequence of U_3 of length $y+z+2 \le \frac{3}{2}m+1 < 3m-2 = |U_3|$, contradicting that U_3 is an atom. So we instead conclude that $e_1 \in \mathrm{supp}(A)$. As a result, since $\mathrm{ord}(e_1) = m < 2m = \mathrm{ord}(f_1) = = \mathrm{ord}(f_2) = \mathrm{ord}(e_2)$, we must have

$$e_1 = -yf_1 + f_2 = -yf_1 + e_2 \quad \text{for some } y \in [1, \epsilon]. \tag{5.24}$$

Furthermore, since $me_1 = 0$, we conclude from $\mathrm{ord}(e_2) = 2m$ that y is odd, and in view of CASE 5.2.1, we can assume $y \ge 3$.

Suppose $f_1 \in \mathrm{supp}(A)$. Then $f_1 = xe_1 + e_2$ for some $x \in \mathbb{Z}$. Combining this with (5.24) yields $-e_1 + e_2 = yf_1 = xye_1 + ye_2$, which implies $y \equiv 1 \bmod 2m$. Hence, since $y \in [1, m-1]$, we conclude that $y = 1$, which is contrary to our above assumption. So we may instead assume $f_1 \notin \mathrm{supp}(A)$, implying

$$\mathsf{v}_{f_1}(C) = m - 1.$$

Each term of A equal to $e_1 = -yf_1 + f_2 = -yf_1 + e_2$ is also equal to some $-y_i f_1 + f_2$. Thus $3\mathsf{v}_{e_1}(A) \le \mathsf{v}_{e_1}(A)y \le y_1 + \ldots + y_{m-\epsilon} = m - 1$, implying $\mathsf{v}_{e_1}(A) \le \frac{m-1}{3}$ and

$$\mathsf{v}_{-e_1}(-B) \ge \frac{2m-2}{3} \ge \frac{m}{2}.$$

Since $\mathsf{v}_{f_1}(C) = m - 1$, we find that there are precisely $|C| - m + 1 = \frac{m}{2}$ terms of C either equal to $e_2 = f_2$ or $-y_i f_1 + e_2$ for some i. Hence, since $y_1 + \ldots + y_{m-\epsilon} = m - 1 = \mathsf{v}_{f_1}(C)$ with the $y_i \in [1, m-1]$, we see that we can find disjoint subsequences $T_1 \cdot \ldots \cdot T_{m/2} \mid C$ with each $T_i \in \mathcal{F}(G)$ a subsequence having $\sigma(T_i) = e_2$. There are at least $|B| - m + 1 = \frac{m}{2}$ terms of $-B$ of the form $-xe_1 - e_2$, say $b_1 \cdot \ldots \cdot b_{m/2} \mid -B$ with $b_i \in \langle e_1 \rangle - e_2$ for

all i. Now $(\sigma(T_1)+b_1)\cdot\ldots\cdot(\sigma(T_{m/2})+b_{m/2})(-e_1)^{m/2}\in\mathcal{F}(\langle e_1\rangle)$ is a subsequence of terms from $\langle e_1\rangle$ of length $m=\mathsf{D}(\langle e_1\rangle)$. Consequently, the subsequence $T_1\cdot\ldots\cdot T_{m/2}\cdot b_1\cdot\ldots\cdot b_{m/2}\cdot(-e_1)^{m/2}$ of $(-B)C=U_3$ contains a nontrivial zero-sum subsequence of length at most $|T_1|+\ldots+|T_{m/2}|+m\le|C|+m=\frac{5}{2}m-1<3m-2=|U_3|$, contradicting that U_3 is an atom and completing CASE 5.2.1.

CASE 5.2.3: $f_2\notin\operatorname{supp}(A)$.

Since $f_2\notin\operatorname{supp}(A)$, all terms of A not equal to f_1 are equal to some $-y_if_1+f_2$, and there are at least $|A|-m+1=\frac{m}{2}+1$ such terms of A. If $y_i\ge 2$ for all these terms, then we obtain the contradiction $m+2=(\frac{m}{2}+1)2\le y_1+\ldots+y_{m-\epsilon}=m-1$. Thus $-f_1+f_2\in\operatorname{supp}(A)$. If $-f_1+f_2=xe_1+e_2$ for some $x\in\mathbb{Z}$, then (5.22) implies $0=-mf_1+mf_2=xme_1+me_2=me_2$, contradicting that $\operatorname{ord}(e_2)=2m$. Therefore we instead conclude that $-f_1+f_2=e_1$, so that CASE 5.2.1 completes the proof of CASE 5.

CASE 6: U_1 is of type I(a) and $-U_2$ is of type II, say

$$U_1=e_1^{mn-1}\prod_{i=1}^{m}(x_ie_1+e_2)\qquad\text{and}\qquad -U_2=f_1^{sm-1}f_2^{(n-s)m+\epsilon}\prod_{i=1}^{m-\epsilon}(-y_if_1+f_2),$$

where $\{e_1,\ e_2\}$ is a basis for G with $\operatorname{ord}(e_2)=m$ and $\operatorname{ord}(e_1)=mn>m$, where $\{f_1,\ f_2\}$ is a generating set for G with $\operatorname{ord}(f_2)=mn$ and $\operatorname{ord}(f_1)\ge 2m$, and where $y_1+\ldots+y_{m-\epsilon}=m-1$ with $y_i\in[1,m-1]$, $\epsilon\in[1,m-1]$ and $s\in[1,n-1]$. Moreover, either $s=1$ or $mf_1=mf_2$, with both holding when $n=2$.

CASE 6.1: $n\ge 3$.

Since $|A|=\frac{mn+m}{2}>m$, we must have $e_1\in\operatorname{supp}(A)$. If $e_1=-y_if_1+f_2$ for some $y_i\in[1,m-1]$, then we obtain the contradiction $|A|\le\mathsf{v}_{e_1}(A)+$ $+m\le(m-\epsilon)+m\le 2m-1<\frac{mn+m}{2}=|A|$ (in view of $n\ge 3$). Therefore either

$$e_1=f_1\quad\text{or}\quad e_1=f_2. \tag{5.25}$$

Suppose $s=1$. If $e_1=f_2$, then $\frac{mn+m}{2}=|A|\ge\mathsf{v}_{e_1}(A)=(n-1)m+\epsilon\ge$ $\ge mn-m+1$, contradicting that $n\ge 3$. If $e_1=f_1$, then $|A|\le\mathsf{v}_{e_1}(A)+m\le$ $\le\mathsf{v}_{f_1}(-U_2)+m=2m-1<\frac{mn+m}{2}=|A|$, again in view of $n\ge 3$, which is a contradiction. So (in view of (5.25)) we may instead assume $s>1$, whence

$$mf_2=mf_1=me_1, \tag{5.26}$$

where the first equality follows from Main Proposition 7 and the second from (5.25).

The argument is now similar to CASE 5.1. Let $H = \langle me_1 \rangle$. Then $G/H \cong C_m^2$. Since $n \geq 3$, we have $|C| = |B| = \frac{mn+m-2}{2} \geq 2m - 1 = \mathsf{D}(G/H)$. Let $B' \mid B$ be a subsequence with $|B'| = 2m - 1$. If $\mathsf{v}_{e_1}(B') \geq m$, then B' will contain a subsequence $T = e_1^m$ with $\sigma(T) = me_1$. If $\mathsf{v}_{e_1}(B') < m$, then this is only possible if

$$B' = e_1^{m-1} \prod_{i=1}^{m} (x_i e_1 + e_2) \quad \text{with} \quad \sum_{i=1}^{m} x_i \equiv 1 \bmod mn,$$

in which case it is easily seen that $T = B'$ is a subsequence of B' with $\sigma(T) = me_1$. Since $|C| \geq 2m - 1$, Lemma 5 ensures that there is a subsequence $R \mid C$ with $\sigma(R) = mf_2$ and $|R| \leq 2m - 1$. Moreover, R will be a proper subsequence unless $n = 3$ and

$$C = f_1^{m-1} f_2^{\epsilon} \prod_{i=1}^{m-\epsilon} (-y_i f_1 + f_2).$$

Now $(-T)R$ is a nontrivial zero-sum subsequence of $(-B)C = U_3$ (in view of (5.26)). Since U_3 is an atom, this is only possible if $T = B' = B$ and $R = C$. Thus $n = 3$ and

$$U_3 = (-e_1)^{m-1} \prod_{i=1}^{m} (-x_i e_1 - e_2) f_1^{m-1} f_2^{\epsilon} \prod_{i=1}^{m-\epsilon} (-y_i f_1 + f_2).$$

As a result, since $\mathsf{v}_{f_2}(-U_2) = (n - s)m + \epsilon \geq m + \epsilon > m > \epsilon$, we conclude that $f_2 \in \mathrm{supp}(A)$. Moreover, $\mathsf{v}_{f_2}(A) \geq m + \epsilon - \mathsf{v}_{f_2}(C) = m$. Hence, as the only term in U_1 with multiplicity at least m is e_1 (recall $|\mathrm{supp}(U_1)| \geq 3$ as remarked after Main Proposition 7, we conclude that $e_1 = f_2$, in which case $(-e_1)(f_2) = (-e_1)(e_1)$ is a proper zero-sum subsequence of U_3, contradicting that U_3 is an atom.

CASE 6.2: $n = 2$.

Similar to CASE 5.2, we now have $\mathrm{ord}(e_1) = \mathrm{ord}(f_2) = \mathrm{ord}(f_1) = 2m$, $s = 1$, $\epsilon \geq 2$, $m \geq 4$ even (since $\mathsf{D}(G) = 3m - 1$ is odd), and

$$mf_1 = mf_2 = me_1, \tag{5.27}$$

with

$$U_1 = e_1^{2m-1} \prod_{i=1}^{m} (x_i e_1 + e_2) \quad \text{and} \quad -U_2 = f_1^{m-1} f_2^{m+\epsilon} \prod_{i=1}^{m-\epsilon} (-y_i f_1 + f_2).$$

Since $|A| = \frac{3}{2}m > m$, we must have $e_1 \in \operatorname{supp}(A)$. We have three possibilities for e_1.

Suppose $e_1 = f_1$. Then $\mathsf{v}_{e_1}(A) = \mathsf{v}_{f_1}(A) = m - 1$, implying

$$\mathsf{v}_{-e_1}(-B) = m$$

and $\mathsf{v}_{f_1}(C) = 0$. Let $T = c_1 \cdot \ldots \cdot c_m \mid C$ be any length m subsequence of C. As $\mathsf{v}_{f_1}(C) = 0$, each $c_i = -z_i f_1 + f_2 = -z_i e_1 + f_2$ for some $z_i \in [0, m-1]$ with

$$0 \le z := z_1 + \ldots + z_m \le y_1 + \ldots + y_{m-\epsilon} = m - 1.$$

Then $\sigma(T) = -zf_1 + mf_2 = (m - z)e_1$ (in view of (5.27) and $e_1 = f_1$), in which case $(-e_1)^{m-z}T$ is a zero-sum subsequence of $(-B)C = U_3$ of length $m - z + |T| \le 2m < 3m - 2 = |U_3|$, contradicting that U_3 is an atom.

Suppose $e_1 = f_2$. Then $\mathsf{v}_{e_1}(A) = \mathsf{v}_{f_2}(A) = m + \epsilon \le |A| = \frac{3}{2}m$, implying $\epsilon \le \frac{m}{2}$,

$$\mathsf{v}_{-e_1}(-B) = m - 1 - \epsilon \ge \frac{m}{2} - 1 > 0$$

and $\mathsf{v}_{f_2}(C) = 0$. Since $\mathsf{v}_{f_2}(A) = m + \epsilon$, it follows that there are at most $|A| - \mathsf{v}_{f_2}(C) = \frac{m}{2} - \epsilon$ terms of A of the form $-y_i f_1 + f_2 = -y_i f_1 + e_1$, meaning there are at least $m - \epsilon - (\frac{m}{2} - \epsilon) = \frac{m}{2}$ terms of C of this form, say $b_1 \cdot \ldots \cdot b_\ell \mid C$ with w.l.o.g. $b_i = -y_i f_1 + f_2 = -y_i f_1 + e_1$ for $i \in [1, \ell]$ and $\ell \ge \frac{m}{2}$. If $b_i \ge 2$ for all $i \in [1, \ell]$, then we obtain the contradiction $m \le 2\ell \le b_1 + \ldots + b_\ell \le y_1 + \ldots + y_{m-\epsilon} = m - 1$. Therefore we may assume $y_i = 1$ for some $i \in [1, \ell]$, meaning

$$-f_1 + e_1 \in \operatorname{supp}(C).$$

Since $\mathsf{v}_{f_2}(A) = m + \epsilon$, there are also at most $|A| - m - \epsilon = \frac{m}{2} - \epsilon$ terms of A equal to f_1, whence $\mathsf{v}_{f_1}(C) \ge m - 1 - (\frac{m}{2} - \epsilon) = \frac{m}{2} - 1 + \epsilon > 0$. Hence $f_1(-e_1)(-f_1 + e_1)$ is a zero-sum subsequence of $(-B)C = U_3$ of length $3 < 3m - 2 = |U_3|$, contradicting that U_3 is an atom.

It remains to consider the case when $e_1 = -yf_1 + f_2$ for some $y \in [1, m-1]$. Moreover, in view of (5.27) and $\mathrm{ord}(e_1) = 2m$, we must have y even, whence $y \ge 2$. Thus $2\mathsf{v}_{e_1}(A) \le y_1 + \ldots + y_{m-\epsilon} = m-1$, implying $\mathsf{v}_{e_1}(A) \le \frac{m-1}{2}$. But now $\frac{3}{2}m = |A| \le \mathsf{v}_{e_1}(A) + m \le \frac{m-1}{2} + m$, which is a proof concluding contradiction. □

Acknowledgements

Part of this manuscript was written while the first author visited South China Normal University in Guangzhou. He wishes to thank the School of Mathematics for their support and hospitality.

This work was supported by the Austrian Science Fund FWF, Project No. P26036-N26 and by the National Science Foundation of China, Grant No. 11271142.

Bibliography

1. ***D. F. Anderson***, *Elasticity of factorizations in integral domains : a survey*, Factorization in Integral Domains, Lect. Notes Pure Appl. Math., vol. 189, Marcel Dekker, 1997, pp. 1–29.
2. ***D. F. Anderson, P.-J. Cahen, S. T. Chapman, W. W. Smith***, *Some factorizations properties of the ring of integer-valued polynomials*, Zero-Dimensional Commutative Rings, Lect. Notes Pure Appl. Math., vol. 171, Marcel Dekker, 1995, pp. 95–113.
3. ***N. R. Baeth, A. Geroldinger***, *Monoids of modules and arithmetic of direct-sum decompositions*, Pacific J. Math. **271** (2014), 257–319.
4. ***N. R. Baeth, D. Smertnig***, *Factorization theory from commutative to noncommutative settings*, J. Algebra **441** (2015), 475–551.
5. ***N. R. Baeth, R. Wiegand***, *Factorization theory and decomposition of modules*, Am. Math. Mon. **120** (2013), 3–34.
6. ***P. Baginski, S. T. Chapman, N. Hine, J. Paixao***, *On the asymptotic behavior of unions of sets of lengths in atomic monoids*, Involve, a journal of mathematics. **1** (2008), 101–110.
7. ***P. Baginski, A. Geroldinger, D. J. Grynkiewicz, A. Philipp***, *Products of two atoms in Krull monoids and arithmetical characterizations of class groups*, Eur. J. Comb. **34** (2013), 1244–1268.
8. ***M. Banister, J. Chaika, S. T. Chapman, W. Meyerson***, *A theorem on accepted elasticity in certain local arithmetical congruence monoids*, Abh. Math. Semin. Univ. Hamb. **79** (2009), 79–86.
9. ***G. Bhowmik, I. Halupczok, J.-C. Schlage-Puchta***, *The structure of maximal zero-sum free sequences*, Acta Arith. **143** (2010), 21–50.

10. ***V. Blanco, P. A. García-Sánchez, A. Geroldinger***, *Semigroup-theoretical characterizations of arithmetical invariants with applications to numerical monoids and Krull monoids*, Illinois J. Math. **55** (2011), 1385–1414.

11. ***P.-J. Cahen, J.-L. Chabert***, *Elasticity for integer-valued polynomials*, J. Pure Appl. Algebra **103** (1995), 303–311.

12. ***S. T. Chapman, S. Glaz***, *One hundred problems in commutative ring theory*, Non-Noetherian Commutative Ring Theory, Mathematics and Its Applications, vol. 520, Kluwer Academic Publishers, 2000, pp. 459–476.

13. ***S. T. Chapman, B. McClain***, *Irreducible polynomials and full elasticity in rings of integer-valued polynomials*, J. Algebra. **293** (2005), 595–610.

14. ***S. T. Chapman, W. W. Smith***, *Factorization in Dedekind domains with finite class group*, Isr. J. Math. **71** (1990), 65–95.

15. ***F. Chen, S. Savchev***, *Long minimal zero-sum sequences in the groups* $C_2^{r-1} \oplus C_{2k}$, Integers. **14** (2014), Paper A23.

16. ***A. Czogala***, *Arithmetic characterization of algebraic number fields with small class number*, Math. Z. **176** (1981), 247–253.

17. ***A. Facchini***, *Krull monoids and their application in module theory*, Algebras, Rings and their Representations (A. Facchini, K. Fuller, C. M. Ringel, C. Santa-Clara, eds.), World Scientific, 2006, 53–71.

18. ***M. Freeze, A. Geroldinger***, *Unions of sets of lengths*, Funct. Approximatio, Comment. Math. **39** (2008), 149–162.

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

20. ***W. Gao, A. Geroldinger***, *On products of k atoms*, Monatsh. Math. **156** (2009), 141–157.

21. ***W. Gao, A. Geroldinger, D. J. Grynkiewicz***, *Inverse zero-sum problems III*, Acta Arith. **141** (2010), 103–152.

22. ***A. Geroldinger***, *Additive group theory and non-unique factorizations*, Combinatorial Number Theory and Additive Group Theory (A. Geroldinger and I. Ruzsa, eds.), Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, 2009, 1–86.

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

24. ***A. Geroldinger, F. Kainrath, A. Reinhart***, *Arithmetic of seminormal weakly Krull monoids and domains*, J. Algebra **444** (2015), 201–245.

25. ***A. Geroldinger, M. Liebmann, A. Philipp***, *On the Davenport constant and on the structure of extremal sequences*, Period. Math. Hung. **64** (2012), 213–225.

26. ***A. Geroldinger, I. Ruzsa***, *Combinatorial Number Theory and Additive Group Theory*, Advanced Courses in Mathematics — CRM Barcelona, Birkhäuser, 2009.
27. ***A. Geroldinger, Wolfgang A. Schmid***, *A characterization of class groups via sets of lengths*, submitted.
28. ***A. Geroldinger, R. Schneider***, *On Davenport's constant*, J. Comb. Theory, Ser. A. **61** (1992), 147–152.
29. ***R. Gilmer***, *Commutative Semigroup Rings*, The University of Chicago Press, 1984.
30. ***D. J. Grynkiewicz***, *Structural Additive Theory*, Developments in Mathematics, Springer, 2013.
31. ***F. Halter-Koch***, *Ideal Systems. An Introduction to Multiplicative Ideal Theory*, Marcel Dekker, 1998.
32. ***F. Kainrath***, *Elasticity of finitely generated domains*, Houston J. Math. **31** (2005), 43–64.
33. ***H. Kim***, *The distribution of prime divisors in Krull monoid domains*, J. Pure Appl. Algebra. **155** (2001), 203–210.
34. ***H. Kim, Y. S. Park***, *Krull domains of generalized power series*, J. Algebra **237** (2001), 292–301.
35. ***C. Reiher***, *A proof of the theorem according to which every prime number possesses property B*, Ph.D. Thesis, Rostock, 2010.
36. ***L. Salce, P. Zanardo***, *Arithmetical characterization of rings of algebraic integers with cyclic ideal class group*, Boll. Unione. Mat. Ital., VI. Ser., D, Algebra Geom. **1** (1982), 117–122.
37. ***W. A. Schmid***, *Arithmetical characterization of class groups of the form* $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ *via the system of sets of lengths*, Abh. Math. Semin. Univ. Hamb. **79** (2009), 25–35.
38. ***W. A. Schmid***, *Characterization of class groups of Krull monoids via their systems of sets of lengths* : *a status report*, Number Theory and Applications : Proceedings of the International Conferences on Number Theory and Cryptography (S. D. Adhikari and B. Ramakrishnan, eds.), Hindustan Book Agency, 2009, pp. 189–212.
39. ***W. A. Schmid***, *Inverse zero-sum problems II*, Acta Arith. **143** (2010), 333–343.
40. ***D. Smertnig***, *On the Davenport constant and group algebras*, Colloq. Math. **121** (2010), 179–193.
41. ***D. Smertnig***, *Sets of lengths in maximal orders in central simple algebras*, J. Algebra **390** (2013), 1–43.

Alfred Geroldinger

Institute for Mathematics
and Scientific Computing,
University of Graz, NAWI Graz,
36 Heinrichstraße,
Graz 8010, Austria,
alfred.geroldinger@uni-graz.at

David J. Grynkiewicz

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

Pingzhi Yuan

School of Mathematics,
South China Normal University,
Guangzhou, 510631, P.R. China,
yuanpz@scnu.edu.cn