PRODUCTS OF TWO ATOMS IN KRULL MONOIDS AND ARITHMETICAL CHARACTERIZATIONS OF CLASS GROUPS

PAUL BAGINSKI, ALFRED GEROLDINGER, DAVID J. GRYNKIEWICZ AND ANDREAS PHILIPP

Abstract. Let H be a Krull monoid with finite class group G such that every class contains a prime divisor and let $\mathsf D(G)$ be the Davenport constant of G. Then a product of two atoms of H can be written as a product of at most $\mathsf D(G)$ atoms. We study this extremal case and consider the set $\mathcal V_{\{2,\mathsf D(G)\}}(H)$ defined as the set of all $l \in \mathbb N$ with the following property: There are two atoms $u, v \in H$ such that uv can be written as a product of l atoms as well as a product of $\mathsf D(G)$ atoms. If G is cyclic, then $\mathcal V_{\{2,\mathsf D(G)\}}(H) = \{2, \mathsf D(G)\}$. If G has rank two, then we show that (apart from some exceptional cases) $\mathcal V_{\{2,\mathsf D(G)\}}(H) = [2, \mathsf D(G)] \setminus \{3\}$. This result is based on the recent characterization of all minimal zero-sum sequences of maximal length over groups of rank two. As a consequence, we are able to show that the arithmetical factorization properties encoded in the sets of lengths of a rank 2 prime power order group uniquely characterizes the group.

1. Introduction

Let H be a Krull monoid with finite class group G and suppose that every class contains a prime divisor (rings of integers in algebraic number fields are such Krull monoids, and other examples will be given in Section 2). Then every non-unit $a \in H$ can be written as a finite product of atoms (irreducible elements), say $a = u_1 \cdot \ldots \cdot u_k$, and the number k of atoms is called the length of the factorization. The set $\mathsf L(a) \subset \mathbb N$ of all possible k is called the set of lengths of a, and it is easy to argue that $\mathsf L(a)$ is finite. It is well-known that H is factorial if and only if $|G| = 1$, and that H is half-factorial (this means $|\mathsf L(a)| = 1$ for all non-units $a \in H$) if and only if $|G| \le 2$. Suppose that $|G| \ge 3$. Then there exists an $a \in H$ with $|\mathsf L(a)| > 1$, and therefore, for every $N \in \mathbb N$, there is an $a_N \in H$ with $|\mathsf L(a_N)| > N$ (indeed, a^N has this property).

Long sets of lengths have a well-defined structure: they are AAMPs (almost arithmetical multiprogressions) with a universal bound for all parameters ([17, Chapter 4]), and this description is the best possible ([31]). For every $k \in \mathbb N$, let $\mathcal V_k(H)$ denote the set of all $l \in \mathbb N$ such that a product of k atoms can be written as a product of l atoms (by definition, $\mathcal V_k(H)$ is the union of all sets of lengths $\mathsf L(a)$ with $k \in \mathsf L(a)$). It is not difficult to show that these unions $\mathcal V_k(H)$—first studied in [5]—are intervals ([14, Theorem 3.1.3]). Their maxima are $\rho_k(H)$, i.e., $\rho_k(H) = \max \mathcal V_k(H)$, which, like the elasticity $\rho(H) = \sup\{\rho_l(H)/l \mid l \in \mathbb N\}$, are widely studied invariants. An easy observation shows that $\rho_k(H) \le k\mathsf D(G)/2$, where $\mathsf D(G)$ is the Davenport constant of G, and that equality holds for even k ([17, Section 6.3]). The question for the precise value of $\rho_k(H)$ for odd k is settled for cyclic groups ([11]) but open in general ([16]).

Little is known about short sets of lengths. If $u, v \in H$ are two atoms, then $\max \mathsf L(uv) \le \mathsf D(G)$, and we will consider the extremal case where this maximum is attained. More precisely, we study the set $\mathcal V_{\{2,\mathsf D(G)\}}(H)$ which is defined as the set of all $l \in \mathbb N$ with the following property:

> There are two atoms $u, v \in H$ such that uv can be written as a product of l atoms as well as a product of $\mathsf D(G)$ atoms.

Thus $\mathcal V_{\{2,\mathsf D(G)\}}(H)$ is the union of all sets of lengths $\mathsf L(a)$ with $\{2, \mathsf D(G)\} \subset \mathsf L(a)$, and we have $\{2, \mathsf D(G)\} \subset V_{\{2,\mathsf D(G)\}}(H) \subset [2, \mathsf D(G)]$. Our starting point is the following result ([17, Theorem 6.6.3]):

Theorem A. Let H be a Krull monoid with finite class group G, $|G| \ge 3$, and suppose that every class contains a prime divisor. Then

$$\mathcal V_{\{2,\mathsf D(G)\}}(H) = \{2, \mathsf D(G)\} \qquad \text{if and only if} \qquad G \text{ is cyclic or an elementary 2-group}\,.$$

Our first main result (Theorem 3.5) shows that, in groups of rank two, $\mathcal V_{\{2,\mathsf D(G)\}}(H)$ equals $[2, \mathsf D(G)] \setminus \{3\}$ (apart from some exceptional cases). We extend this to groups of higher rank (Theorem 4.2), and these two results are the key for a characterization result on class groups (Theorem 5.6; the status on arithmetical characterizations of class groups will be discussed at the beginning of Section 5).

2010 *Mathematics Subject Classification.* 11B13, 11P70, 13A05, 20M13.
Key words and phrases. sets of lengths, Krull monoids, class groups, zero-sum sequences, inverse zero-sum problem.
This work was supported by the Austrian Science Fund FWF, Project Numbers P21576-N18.

It is well-known that all questions on sets of lengths in a Krull monoid translate into zero-sum problems in its class group. Thus, after applying well-studied transfer machinery (Lemma 2.1), all the algebraic problems outlined above turn out to be combinatorial ones. Indeed, the present progress is entirely based on the characterization of all minimal zero-sum sequences of maximal length over groups of rank two (see Theorem 3.1). The characterization result (Theorem 5.6) substantially uses recent work by Schmid ([31, 30, 33]).

2. Preliminaries

Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers and put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, we set $[a,b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$. For subsets $A, B \subset \mathbb{Z}$, we denote by $A + B = \{a+b \mid a \in A, b \in B\}$ their *sumset*, and by $\Delta(A)$ the *set of* (*successive*) *distances* of A (that is, $d \in \Delta(A)$ if and only if $d = b - a$ with $a, b \in A$ distinct and $[a,b] \cap A = \{a,b\}$).

Let G be an additively written finite abelian group and $G_0 \subset G$ a subset. Then $[G_0] \subset G$ denotes the sub-semigroup generated by G_0, and $\langle G_0 \rangle \subset G$ denotes the subgroup generated by G_0. A tuple $(e_i)_{i \in I}$ of elements of G is said to be *independent* if all elements are non-zero and

$$\sum_{i \in I} m_i e_i = 0 \quad \text{implies} \quad m_i e_i = 0 \quad \text{for all } i \in I, \qquad \text{where } m_i \in \mathbb{Z}\,.$$

The tuple $(e_i)_{i \in I}$ is called a *basis* if $(e_i)_{i\in I}$ is independent and $\langle \{e_i \mid i \in I\} \rangle = G$. For $p \in \mathbb{P}$, let $\mathsf r_p(G)$ denote the p-rank of G, $\mathsf r(G) = \max\{\mathsf r_p(G) \mid p \in \mathbb{P}\}$ denote the rank of G, and let $\mathsf r^*(G) = \sum_{p \in \mathbb{P}} \mathsf r_p(G)$ be the *total rank* of G. 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 $r = \mathsf r(G) \in \mathbb{N}$, $n_1, \ldots, n_r \in \mathbb{N}$ are integers with $1 < n_1 \mid \ldots \mid n_r$ and $n_r = \exp(G)$ is the exponent of G. If $g \in G$ with $\operatorname{ord}(g) = \exp(G)$, then there exist $e_1, \ldots, e_{r-1} \in G$ with $\operatorname{ord}(e_i) = n_i$ for all $i \in [1, r-1]$ such that $(e_1, \ldots, e_{r-1}, g)$ is a basis of G. If $|G| = 1$, then $\mathsf r(G) = 0$, $\exp(G) = 1$, $\mathsf d^*(G) = 0$, and $\mathsf D^*(G) = 1$.

Monoids and factorizations. By a *monoid*, we always mean a commutative semigroup with identity which satisfies the cancelation 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 H be a monoid. We denote by $H^\times$ the set of invertible elements of H, and we say that H is *reduced* if $H^\times = \{1\}$. Let $\mathsf q(H)$ be a quotient group and $\mathcal A(H)$ the set of atoms of H. Let $a \in H \setminus H^\times$. If $a = u_1 \cdot \ldots \cdot u_k$, with $u_1, \ldots, u_k \in \mathcal A(H)$, then k is called the length of the factorization, and the set $\mathsf L_H(a) = \mathsf L(a) \subset \mathbb{N}$ of all possible k is called the *set of lengths* of a (with respect to the monoid H). For convenience, we set $\mathsf L(a) = \{0\}$ for $a \in H^\times$. We denote by

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

$$\Delta(H) = \bigcup_{L \in \mathcal L(H)} \Delta(L) \ \subset \mathbb{N} \qquad \text{the } \textit{set of distances} \text{ of } H\,.$$

For a subset $M \subset \mathbb{N}$, we set

$$\mathcal V_M(H) \ = \ \begin{cases} \bigcup_{M \subset L, L \in \mathcal L(H)} L & H \ne H^\times \\ M & H = H^\times, \end{cases}$$

which—for $H \ne H^\times$—is the union of all sets of lengths containing M. In the case $|M| = 1$, these unions are well studied (see for example [5, 6, 2]).

A monoid F is called *free* (*abelian, with basis* $P \subset F$) if every $a \in F$ has a unique representation of the form

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

We set $F = \mathcal F(P)$ and call

$$|a|_F = |a| = \sum_{p \in P} \mathsf v_p(a) \quad \text{the } \textit{length} \text{ of } a\,.$$

Krull monoids. The theory of Krull monoids is presented in the monographs [23, 17]. We briefly summarize what is needed in what follows. The monoid H is called a *Krull monoid* if it satisfies one of the following equivalent conditions ([17, Theorem 2.4.8]):

- H is v-noetherian and completely integrally closed.
- H has a divisor theory. This means that there is a monoid homomorphism $\varphi\colon H \to D = \mathcal{F}(P)$ into a free monoid with the following properties:
  - For every $a, b \in H$, $\varphi(a) \mid \varphi(b)$ implies that $a \mid b$.
  - For every $p \in P$, there exists a finite subset $\emptyset \ne X \subset H$ such that $\gcd\big(\varphi(X)\big) = p$.

Let H be a Krull monoid. Then a divisor theory $\varphi\colon H \to D$ is essentially unique, and the group $\mathcal{C}(H) = \mathsf{q}(D)/\mathsf{q}(\varphi(H))$—called the *class group* of H—does indeed depend only on H. It will be written additively, and the set

$$G_P = \{[p] = p\mathsf{q}(\varphi(H)) \mid p \in P\} \subset \mathcal{C}(H)$$

is called the *set of classes containing prime divisors.* We have $[G_P] = \mathcal{C}(H)$.

An integral domain R is a Krull domain if and only if its multiplicative monoid $R\setminus\{0\}$ is a Krull monoid, and 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 ([17, Section 2.11]). Monoid domains and power series domains that are Krull and have prime divisors in all classes are discussed in [24, 25, 3].

Main portions of the arithmetic of a Krull monoid—in particular, all questions dealing with sets of lengths—can be studied in the associated block monoid over its class group. We first provide these concepts and summarize the connection in Lemma 2.1.

Zero-sum sequences. Let $G_0 \subset G$ be a subset. For our purposes, it is convenient to consider sequences over G_0 as elements in the free monoid $\mathcal{F}(G_0)$. Thus sequences will be written multiplicatively. For such a sequence

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

we set $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_l)$ for any homomorphism $\varphi\colon G \to G'$, and in particular, we have $-S = (-g_1) \cdot \ldots \cdot (-g_l)$. We call $\mathsf{v}_g(S)$ the *multiplicity* of g in S,

$$|S| = l = \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0 \text{ the } \textit{length} \text{ of } S\,, \quad \operatorname{supp}(S) = \{g \in G \mid \mathsf{v}_g(S) > 0\} \subset G \text{ the } \textit{support} \text{ of } S\,,$$

$$\sigma(S) = \sum_{i=1}^{l} g_i \text{ the } \textit{sum} \text{ of } S \quad \text{and} \quad \Sigma(S) = \Big\{ \sum_{i \in I} g_i \mid \emptyset \ne I \subset [1, l] \Big\} \text{ the } \textit{set of subsequence sums} \text{ of } S\,.$$

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.

The monoid $\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \sigma(S) = 0\}$ is called the *monoid of zero-sum sequences* over G_0, and we have $\mathcal{B}(G_0) = \mathcal{B}(G) \cap \mathcal{F}(G_0)$. It is a Krull monoid, and its atoms are precisely the minimal zero-sum sequences.

For every arithmetical invariant $*(H)$ defined for a monoid H, it is usual to write $*(G_0)$ instead of $*(\mathcal{B}(G_0))$ (although this is an abuse of language, there will be no danger of confusion). In particular, we set $\mathcal{A}(G_0) = \mathcal{A}(\mathcal{B}(G_0))$, $\mathcal{L}(G_0) = \mathcal{L}(\mathcal{B}(G_0))$, and $\mathcal{V}_M(G_0) = \mathcal{V}_M(\mathcal{B}(G_0))$ for a subset $M \subset \mathbb{N}$. The *Davenport constant*

$$\mathsf{D}(G_0) = \max\big\{|U| \;\big|\; U \in \mathcal{A}(G_0)\big\} \in \mathbb{N}_0$$

is a classical constant in Combinatorial Number Theory (see the surveys [10, 14], or [19, 34, 7] for recent progress). We denote by $\mathsf{d}(G)$ the maximal length of a zero-sum free sequence, and get

$$1 + \mathsf{d}^*(G) \le 1 + \mathsf{d}(G) = \mathsf{D}(G)\,. \tag{2.1}$$

We will use without further mention that equality holds if G is a p-group or $\mathsf{r}(G) \le 2$ (see [17, Chapter 5] and [14, Section 4.2]).

Lemma 2.1. *Let H be a Krull monoid, $\varphi\colon H \to F = \mathcal{F}(P)$ a divisor theory, G its class group, and $G_P \subset G$ the set of classes containing prime divisors. Let $\widetilde{\boldsymbol{\beta}}\colon F \to \mathcal{F}(G_P)$ denote the unique homomorphism defined by $\widetilde{\boldsymbol{\beta}}(p) = [p]$ for all $p \in P$. Then $\mathcal{B}(G_P)$ is called the block monoid associated to H, and the homomorphism $\boldsymbol{\beta} = \widetilde{\boldsymbol{\beta}} \circ \varphi\colon H \to \mathcal{B}(G_P)$ has the following property:*

$$\mathsf{L}_H(a) = \mathsf{L}_{\mathcal{B}(G_P)}(\boldsymbol{\beta}(a)) \quad \textit{for every} \quad a \in H\,.$$

This implies that $\mathcal{L}(H) = \mathcal{L}(G_P)$ and $\mathcal{V}_M(H) = \mathcal{V}_M(G_P)$ for every $M \subset \mathbb{N}$.

Proof. See [17, Theorem 3.4.10]. □

The following simple technical lemma will be used without further mention.

Lemma 2.2. *Let G be a finite abelian group and $U, V \in \mathcal{A}(G \setminus \{0\})$.*

1. $\max \mathsf{L}(UV) \le \min\{|U|, |V|\} \le \mathsf{D}(G)$*, and* $\max \mathsf{L}(UV) = \mathsf{D}(G)$ *if and only if* $V = -U$ *and* $|U| = \mathsf{D}(G)$.
2. *If* $V \mid (-U)U$*, then* $2 + |U| - |V| \in \mathsf{L}\big((-U)U\big)$*. In particular, if* $g \in G$ *with* $g^{\mathrm{ord}(g)-1} \mid U$*, then* $\mathrm{ord}(g) \in \mathsf{L}\big((-U)U\big)$.

Proof. See [17, Lemmas 6.4.4 and 6.4.5]. □

3. Products of two atoms in Krull monoids with class group of rank two

The following characterization of minimal zero-sum sequences of maximal length over groups of rank two—formulated in Theorem 3.1—will be crucial for the present paper. The characterization was achieved by contributions of many authors including Bhowmik, Gao, Halupczok, Reiher, Schlage-Puchta, Schmid, and the second and third authors of the present article ([9, 1, 12, 32, 27]). We have reworded the description of type II so that it is described in terms of a basis, rather than a generating set. This alternative description is routinely derived from the original formulation using the fact, previously mentioned, that in a rank 2 group, any element of maximal order $\exp(G)$ can always be paired with another existent element to form a basis. We have also made the description of type II slightly stronger, in order to minimize the overlap between sequences described by type I and those described by type II.

Theorem 3.1. *Let $G = C_m \oplus C_{mn}$ with $m, n \in \mathbb{N}$ and $m \ge 2$. 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:*

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

  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* $x_1 + \ldots + x_{\mathrm{ord}(e_2)} \equiv 1 \mod \mathrm{ord}(e_1)$.
  In this case, we say that S is of type I.
- $$S = (e_1 + ye_2)^{sm-1} e_2^{(n-s)m+\epsilon} \prod_{i=1}^{m-\epsilon} (-x_i e_1 + (-x_i y + 1) e_2),$$

  where
  (a) (e_1, e_2) *is a basis of G with* $\mathrm{ord}(e_1) = m$ *and* $\mathrm{ord}(e_2) = mn$,
  (b) $y \in [0, mn-1]$, $\epsilon \in [1, m-1]$*, 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) $mye_2 \ne 0$*, and*
  (e) *either* $s = 1$ *or* $mye_2 = me_2$.
  In this case, we say that S is of type II.

Proof. See the Corollary in [12, page 104]. Apart from [12], the Corollary is based on [32], and its assumption is satisfied by [27]. In the original formulation, it was also allowed that $s = n$ in type II and (d) was not included. We provide a short explanation here as to why, in both these cases, we instead fall under the hypotheses of type I.

If $s = n$, then $e_1' := e_1 + ye_2$ is an element of multiplicity $mn - 1 = \exp(G) - 1$, and thus we must have $\mathrm{ord}(e_1') = mn$ (else S will not be a minimal zero-sum sequence). In this case, as previously mentioned, there is some $e_2' \in G$, with $\mathrm{ord}(e_2') = m$, such that (e_1', e_2') gives a basis of G. We can then write $S = {e_1'}^{mn-1} T$ with $T = \prod_{i=1}^{m} (y_i e_1' + z_i e_2')$ and y_i, $z_i \in [0, mn-1]$. Let $H = \langle e_1' \rangle$. Since $\Sigma^*({e_1'}^{mn-1}) = H$, any proper zero-sum modulo H subsequence of T can be extended to a proper zero-sum subsequence of S, contradicting that $S \in \mathcal{A}(G)$. Thus $\phi_H(T)$ must be a minimal zero-sum sequence in $G/H \cong C_m$. Since $|\phi_H(T)| = m = |G/H| = \mathsf{D}(G/H)$, the characterization [17, Theorem 5.1.10.1] of such sequences implies that all terms of $\phi_H(T)$ are equal to a generating element, which allows us to assume $z_i = z_j = z$ for all i, $j \in [1, m]$ with $\mathrm{ord}(ze_2') = m$. But now, we see that S also has type I, as desired.

If $mye_2 = 0$, then $\operatorname{ord}(e_1 + ye_2) = m$, so that $(e_1 + ye_2, e_2)$ is a basis of G. Moreover, since (b) implies $s \in [1, n-1]$, we have $n \ge 2$, whence (a) gives $\operatorname{ord}(e_2) = mn > m$. Thus $me_2 \ne 0 = mye_2$, so that (e) implies $s = 1$. But now it is easily seen that S also has type I, as desired. □

Lemma 3.2. *Let $G = C_m \oplus C_{mn}$ with $m, n \in \mathbb{N}$ and $m \ge 2$.*

1. *We have $\{2, m, mn, \mathsf{D}(G)\} \subset \mathcal{V}_{\{2,\mathsf{D}(G)\}}(G)$.*
2. *If $m = 2$, then $\big\{L \in \mathcal{L}(G) \mid \{2, \mathsf{D}(G)\} \subset L\big\} = \big\{\{2, 2a, 2n, 2n+1\} \mid a \in [1, n]\big\}$.*

Proof. 1. This follows immediately from the special case in Lemma 2.2.2 and from the (easy direction of) Theorem 3.1.

2. For $n = 1$, the statement is obvious. Suppose that $n \ge 2$. If $L \in \mathcal{L}(G)$ with $\{2, \mathsf{D}(G)\} \subset L$, then $L = \mathsf{L}\big((-U)U\big)$ with $U \in \mathcal{A}(G)$ and $|U| = \mathsf{D}(G)$. Furthermore, there exists a basis (e_1, e_2) of G with $\operatorname{ord}(e_1) = 2$ and $\operatorname{ord}(e_2) = 2n$ such that U has one of the forms given in Case 1 or in Case 2 (this can be seen by a careful analysis of Theorem 3.1 for $m = 2$, or directly from [8, Corollary 3.4]).

Case 1. $U = e_1 e_2^v (e_1 + e_2)^{2n-v}$ with $v \in [3, 2n-3]$ odd.

We set $V_1 = e_1(-e_2)(e_1 + e_2)$, $V_2 = (e_1 + e_2)(e_1 - e_2)$ and $V_3 = e_2(-e_2)$. If $V \in \mathcal{A}(G)$ with $(e_1 + e_2) \mid V \mid (-U)U$, then $V \in \{V_1, V_2, U\}$. This implies that $(-U)U = V_1(-V_1)V_2^{2n-v-1}V_3^{v-1}$ is the only factorization of length $l \in [3, \mathsf{D}(G) - 1]$, and clearly we have $l = 2n$.

Case 2. $U = e_2^{2n-1}(e_1 + ae_2)\big(e_1 + (1-a)e_2\big)$ with $a \in [0, 2n-1]$.

Let $a \in [0, 2n-1]$ and suppose that

$$(-U)U = V_1 \cdot \ldots \cdot V_l \quad \text{where} \quad V_1, \ldots, V_l \in \mathcal{A}(G) \text{ with } |V_2| \ge \ldots \ge |V_l| \text{ and } (e_1 + ae_2) \mid V_1 .$$

If $V_1 = (e_1 + ae_2)(e_1 - ae_2)$, then—up to renumbering if necessary—$V_2 = \big(e_1 + (1-a)e_2\big)\big(e_1 + (a-1)e_2\big)$, $V_3 = \ldots = V_l = (-e_2)e_2$, and hence $l = 2n+1$.

If $(e_1 + ae_2)\big(e_1 + (1-a)e_2\big) \mid V_1$, then either $V_1 = U$, $V_2 = -U$ and $l = 2$, or $V_1 = (e_1 + ae_2)\big(e_1 + (1-a)e_2\big)(-e_2)$, $V_2 = -V_1$, $V_3 = \ldots = V_l = (-e_2)e_2$, and hence $l = 2n$.

Suppose that $(e_1 + ae_2)\big(e_1 + (a-1)e_2\big) \mid V_1$, and let $b_1, b_2 \in [0, 2n-1]$ be such that

$$2a - 1 + b_1 \equiv 0 \mod 2n \qquad \text{and} \qquad 2a - 1 - b_2 \equiv 0 \mod 2n .$$

Then either $V_1 = (e_1 + ae_2)(e_1 + (a-1)e_2)e_2^{b_1}$, $V_2 = -V_1$, $V_3 = \ldots = V_l = (-e_2)e_2$ and hence $l = 2n + 1 - b_1 \equiv 0 \mod 2$, or $V_1 = (e_1 + ae_2)(e_1 + (a-1)e_2)(-e_2)^{b_2}$, $V_2 = -V_1$, $V_3 = \ldots = V_l = (-e_2)e_2$ and hence $l = 2n + 1 - b_2 \equiv 0 \mod 2$. It is easy to see that all even lengths between 2 and $2n$ are actually obtained. □

Lemma 3.3. *Let $G = G_1 \oplus C_m \oplus C_{mn}$, with $G_1 \le G$ possibly trivial, be a group with $m, n \in \mathbb{N}$, $m \ge 2$, and $\mathsf{d}^*(G) = \mathsf{d}^*(G_1) + \mathsf{d}^*(C_m \oplus C_{mn})$. Then there exists some $L \in \mathcal{L}(G)$ with $\{2\} \cup [\mathsf{d}^*(G_1) + mn, \mathsf{D}^*(G)] \subset L$.*

Proof. Let $e_1, e_2 \in G$ with $\operatorname{ord}(e_1) = m$, $\operatorname{ord}(e_2) = mn$ and $G = G_1 \oplus \langle e_1 \rangle \oplus \langle e_2 \rangle$. Furthermore, let S be a zero-sum free sequence over G_1 of length $|S| = \mathsf{d}^*(G_1)$, and choose $k \in [0, m-1]$ such that $k \equiv 2 - \frac{1}{2}m(m-1) \mod m$. We define

$$U = S e_1^{m-1} e_2^{mn-m+1} \big(ke_1 + e_2 - \sigma(S)\big) \prod_{\nu=2}^{m-1} (\nu e_1 + e_2).$$

Then $|U| = \mathsf{D}^*(G)$, $\big(ke_1 + e_2 - \sigma(S)\big)^{-1} U$ is zero-sum free, and since

$$k + \sum_{\nu=2}^{m-1} \nu = (k-1) + \frac{m(m-1)}{2} \equiv 2 - \frac{m(m-1)}{2} - 1 + \frac{m(m-1)}{2} \equiv 1 \mod m,$$

it follows that $U \in \mathcal{A}(G)$. We set $V_1 = (-e_1)^{m-1}(-e_1 + e_2)(-e_2)$ and, for every $i \in [2, m-1]$, we set $V_i = e_1^{m-i}(ie_1 + e_2)(-e_2)$. Then, for every $i \in [1, m-1]$, $V_i \in \mathcal{A}(G)$ is a divisor of $(-U)U$ of length $|V_i| = m - i + 2$. Since $2 + |U| - |V_i| = \mathsf{d}^*(G_1) + mn + i - 1$, the assertion follows from Lemma 2.2. □

The following proposition is one of the more lengthy and difficult portions of the paper.

Proposition 3.4. *Let $G = C_m \oplus C_{mn}$ with $m, n \in \mathbb{N}$ and $m \ge 5$, and let $U \in \mathcal{A}(G)$ with $|U| = \mathsf{D}(G)$. Then $3 \notin \mathsf{L}\big((-U)U\big)$.*

Proof. Per Theorem 3.1, there are two main possibilities for the structure of U. We handle these cases separately.

Case 1. U has type I in Theorem 3.1.

Then there is a basis of G, say (e_1, e_2) with $\mathrm{ord}(e_1) = n_1$ and $\mathrm{ord}(e_2) = n_2$, such that $U = e_1^{n_1-1}\prod_{i=1}^{n_2}(x_ie_1 + e_2)$ with $\sum_{i=1}^{n_2} x_i \equiv 1 \mod n_1$. If $n_2 < m$, then, since $n_1n_2 = |G| = m^2n$, it would follow that $n_1 > mn$. But this would mean e_2 was an element with $\mathrm{ord}(e_2) > mn = \exp(G)$, which is not possible. Therefore we conclude that

$$n_2 \ge m \ge 5.$$

Likewise, $n_1 \ge m \ge 5$. We continue with the following assertion.

A. Let $V = e_1^{n_1-k}\prod_{i\in I}(x_ie_1+e_2)\prod_{i\in J}(-x_ie_1-e_2) \in \mathcal{A}(G)$ with $k \in [1, n_1]$, $V \mid U(-U)$, $V \ne U$ and $V \ne e_1\prod_{i=1}^{n_2}(-x_ie_i - e_2)$. Then $|I| = |J| \le \min\{k, n_2\}$.

Proof of **A**. Since $V \mid (-U)U$, clearly $|I|, |J| \le n_2$. If V is trivial, then clearly $|I| = |J| = 0 \le k$ holds. So we may assume V is nontrivial.

Since V is a zero-sum sequence, its sum must have zero as its e_2-coordinate. Thus either $|I| = |J|$ or $|I|,\ |J| \in \{0,\ n_2\}$. Suppose the latter occurs. If $|J| = 0$, then V is a nontrivial subsequence of the minimal zero-sum sequence U, whence $V = U$, contrary to hypothesis. Therefore $|J| = n_2$. If $|I| = n_2$, then V will contain $n_2 \ge 2$ nontrivial, zero-sum subsequences of the form $(x_ie_1 + e_2)(-x_ie_1 - e_2)$, contradicting that V is assumed to be an atom. Therefore $|I| = 0$. But now, since $\sum_{i=1}^{n_2} x_i \equiv 1 \mod n_1$ with $|I| = 0$ and $J = [1, n_2]$, we easily deduce that $V = e_1\prod_{i=1}^{n_2}(-x_ie_i - e_2)$, contrary to hypothesis. So we instead conclude that $|I| = |J|$ must hold.

Since V is a zero-sum sequence, we have $\sum_{i\in I} x_i + \sum_{i\in J}(-x_i) \equiv k \mod n_1$. Write $|I| = |J| = l$, $I = \{i_1, \ldots, i_l\}$, and $J = \{j_1, \ldots, j_l\}$. Now we find $\sum_{q=1}^{l}(x_{i_q} - x_{j_q}) \equiv k \mod n_1$.

If, for some $q \in [1, l]$, $x_{i_q} = x_{j_q}$, then $(x_{i_q}e_1 + e_2)(-x_{j_q}e_1 - e_2)$ is a non-trivial zero-sum subsequence of V. Thus, since V is an atom, this is only possible if $V = (x_{i_q}e_1 + e_2)(-x_{j_q}e_1 - e_2)$, in which case $|I| = |J| = 1 \le k$, as desired. Therefore we may assume $x_{i_q} \ne x_{j_q}$ for all $q \in [1, l]$.

Assume by contradiction that $l > k$. Consider the partial sums $\sum\limits_{q=1}^{r}(x_{i_q} - x_{j_q})$ for $r = 1, 2, \ldots, l$. If 2 of these sums were equal modulo n_1, then the terms contained in the longer sum but not the shorter sum would sum to zero modulo n_1, corresponding to a proper, nontrivial zero-sum subsequence of V, contradicting that V is an atom. As a result, we conclude that sums $\sum\limits_{q=1}^{r}(x_{i_q} - x_{j_q})$, for $r = 1, 2, \ldots, l$, are distinct modulo n_1. Consequently, since $l \ge k+1$, it follows that there is some nonempty subset $M \subset [1, l]$ such that $\sum\limits_{q\in M}(x_{i_q} - x_{j_q}) \equiv k' \mod n_1$ with $k' \in [k+1, n_1]$. Moreover, since $\sum\limits_{q\in[1,l]}(x_{i_q} - x_{j_q}) \equiv k \mod n_1$ as noted above, we see that $M \subset [1, l]$ must be a proper subset. But this leads to a proper, non-trivial zero-sum subsequence

$$e_1^{n_1-k'}\prod_{q\in M}(x_{i_q}e_1 + e_2)(-x_{j_q}e_1 - e_2) \mid V,$$

once more contradicting that V is an atom. □

Now assume by contradiction that $3 \in \mathsf{L}\big((-U)U\big)$. Then there are $T_1,\ T_2,\ T_3 \in \mathcal{A}(G)$ with $T_1T_2T_3 = (-U)U$. We write

$$T_j = e_1^{k_j}(-e_1)^{k'_j}\prod_{i\in I_j}(x_ie_1 + e_2)\prod_{i\in J_j}(-x_ie_1 - e_2)$$

for $j \in [1, 3]$. Then $I_1 \uplus I_2 \uplus I_3 = J_1 \uplus J_2 \uplus J_3 = [1, n_2]$.

Case 1.1. Some T_i has length 2, say w.l.o.g. $|T_1| = 2$.

If T_2 or T_3 also has length 2, say w.l.o.g. T_2, then $|T_3| = |(-U)U| - |T_1| - |T_2| = 2m + 2mn - 6 > m + mn - 1 = \mathsf{D}(G)$ is a contradiction. So $|T_2|, |T_3| > 2$, and therefore $|\operatorname{supp}(T_i) \cap \{e_1, -e_1\}| \le 1$ for $i = 2, 3$. After renumbering if necessary, we find

$$T_2 = e_1^{n_1-k}\prod_{i\in I_2}(x_ie_1 + e_2)\prod_{i\in J_2}(-x_ie_1 - e_2) \ \text{ and}$$

$$T_3 = (-e_1)^{n_1-k}\prod_{i\in I_3}(x_ie_1 + e_2)\prod_{i\in J_3}(-x_ie_1 - e_2)$$

with $k \in \{1, 2\}$ and $k = 2$ only possible if $T_1 = (-e_1)(e_1)$. Since $n_1 \ge 4$ and $k \le 2$, we have $n_1 - k \ge 2$, whence $T_2 \ne e_1\prod_{i=1}^{n_2}(x_ie_1 + e_2)$ and $T_3 \ne (-e_1)\prod_{i=1}^{n_2}(-x_ie_1 - e_2)$. Consequently, Assertion **A** implies that $|I_2| = |J_2| \le k$ and $|I_3| = |J_3| \le k$. But now, if $T_1 = (-e_1)(e_1)$, then $n_2 = |I_2| + |I_3| \le 2k = 4$, a contradiction, while if instead $T_1 = (x_ie_1 + e_2)(-x_ie_1 - e_2)$ for some $i \in [1, n_2]$, then $n_2 - 1 = |I_2| + |I_3| \le 2k = 2$, also a contradiction.

Case 1.2. $|T_i| > 2$ for all $i \in [1,3]$.

Then $I_i \cap J_i = \emptyset$ and $|\operatorname{supp}(T_i) \cap \{e_1, -e_1\}| \le 1$ for all $i \in [1,3]$, and thus by the pigeon-hole principle, we find, after renumbering and possibly switching e_1 and $-e_1$ if necessary, that $e_1^{n_1-1} \mid T_1$. Thus, by **A**, it follows that $|I_1| = |J_1| = 1$, say $I_1 = \{a\}$ and $J_1 = \{b\}$, and therefore $|I_2| + |I_3| = n_2 - 1$ and $|J_2| + |J_3| = n_2 - 1$.

Now, since $|I_1|, |J_1| \ge 1$ and since $|\operatorname{supp}(T_i) \cap \{e_1, -e_1\}| \le 1$ for all $i \in [1,3]$, we see that we can again imply Assertion **A** to conclude $|I_2| = |J_2|$ and $|I_3| = |J_3|$.

Since $|T_2|, |T_3| > 2$, it follows that $I_2 \cap J_2 = \emptyset$ and $I_3 \cap J_3 = \emptyset$. Thus we find that

$$I_2 \subset J_3 \cup \{b\}, \quad I_3 \subset J_2 \cup \{b\}, \quad J_2 \subset I_3 \cup \{a\} \quad \text{ and } \quad J_3 \subset I_2 \cup \{a\}.$$

Consequently, if $I_2 \cap J_3 = \emptyset$, then $J_3 \subset I_2 \cup \{a\}$ would imply $|I_3| = |J_3| \le 1$, in which case $I_2 \subset J_3 \cup \{b\}$ would further imply $|I_2| \le |J_3| + 1 \le 2$, and then $n_2 - 1 = |I_2| + |I_3| \le 2 + 1$ follows, contradicting that $n_2 \ge 5$. Therefore there is some $\alpha \in I_2 \cap J_3$. Similarly, if $I_3 \cap J_2 = \emptyset$, then $J_2 \subset I_3 \cup \{a\}$ would imply $|I_2| = |J_2| \le 1$, whence $I_3 \subset J_2 \cup \{b\}$ would further imply $|I_3| \le 2$, and then $n_2 - 1 = |I_2| + |I_3| \le 1 + 2$ follows, contradicting that $n_2 \ge 5$. Therefore, we conclude that there is some $\beta \in I_3 \cap J_2$.

But now, since there exists $\alpha \in I_2 \cap J_3$ and $\beta \in I_3 \cap J_2$, we have

$$(x_\alpha e_1 + e_2)(-x_\beta e_1 - e_2) \mid T_2 \text{ and } (-x_\alpha e_1 - e_2)(x_\beta e_1 + e_2) \mid T_3.$$

Let $k \in [0, n_1 - 1]$ be the integer such that $(-e_1)^k \mid T_2$ and $(-e_1)^{n_1-1-k} \mid T_3$ and let $l \in [0, n_1 - 1]$ be the integer such that $x_\alpha - x_\beta \equiv l \mod n_1$.

Suppose $l \le k$. Then

$$(-e_1)^l (x_\alpha e_1 + e_2)(-x_\beta e_1 - e_2) \mid T_2$$

is either a proper zero-sum subsequence of T_2, contradicting that T_2 is an atom, or else $|I_2| = |J_2| = 1$. However, in the latter case, we derive from $I_3 \subset J_2 \cup \{b\}$ that $|I_3| \le |J_2| + 1 \le 2$, whence $n_2 = |I_1| + |I_2| + |I_3| \le 1 + 1 + 2$, contradicting that $n_2 \ge 5$. So we can instead assume $l \in [k+1, n_1 - 1]$.

In this case, $-l \equiv l' \mod n_1$ for some $l' \in [1, n_1 - 1 - k]$, and thus we again find a contradiction by applying the same argument as above using l' and T_3 in place of l and T_2. This completes Case 1.

Case 2. U has type II in Theorem 3.1.

In this case, we have a basis (e_1, e_2) of G, with $\operatorname{ord}(e_2) = mn$ and $\operatorname{ord}(e_1) = m$, such that

$$U = (e_1 + ye_2)^{sm-1} e_2^{(n-s)m+\epsilon} \prod_{i=1}^{m-\epsilon} (-x_i e_1 + (-x_i y + 1)e_2),$$

where $y \in [0, mn-1]$, $\epsilon \in [1, m-1]$, $s \in [1, n-1]$, $x_i \in [1, m-1]$, $\sum\limits_{i=1}^{m-\epsilon} x_i = m - 1$ and

$$mye_2 \neq 0; \tag{3.1}$$

furthermore,

$$\text{either} \quad s = 1 \quad \text{or} \quad mye_2 = me_2. \tag{3.2}$$

Let $W = \prod_{i=1}^{m-\epsilon}(-x_i e_1 + (-x_i y + 1)e_2)$. Since $s \in [1, n-1]$, we must have $n \ge 2$.

Assume by contradiction that we have a factorization $(-U)U = V_1 V_2 V_3$ with $V_1, V_2, V_3 \in \mathcal{A}(G)$. For each $j \in [1,3]$, factor $V_j = S_j T_j$ such that $\operatorname{supp}(S_j) \subset \pm\{e_1 + ye_2, e_2\}$ and

$$T_j = \prod_{i \in I_j} (-x_i e_1 + (-x_i y + 1)e_2) \prod_{i \in J_j} (x_i e_1 + (x_i y - 1)e_2),$$

where $I_j, J_j \subset [1, m - \epsilon]$. Let $\Delta_j = |I_j| - |J_j|$ and let $\sigma_j = -\sum\limits_{i \in I_j} x_i + \sum\limits_{i \in J_j} x_i \in \mathbb{Z}$, so that

$$\sigma(T_j) = \sigma_j e_1 + (\sigma_j y + \Delta_j) e_2.$$

From the description of U, we trivially have

$$\Delta_j \in [-(m-\epsilon), m-\epsilon] \subset [-(m-1), m-1] \quad \text{ and } \quad \sigma_j \in [-(m-1), m-1], \tag{3.3}$$

for each $j \in [1,3]$.

We begin by handling the case when $|V_i| = 2$ for some $i \in [1,3]$.

Case 2.1. Suppose $|V_i| = 2$ for some $i \in [1, 3]$, say $|V_1| = 2$.

Since $|(-U)U| - 4 = 2mn + 2m - 6 > mn + m - 1 = \mathsf{D}(G)$, there can be at most one atom V_i with $|V_i| = 2$. Therefore $|V_2|, |V_3| > 2$. For every element a of $\text{Supp}(U)$, we cannot have both a and $-a$ in V_2 (or in V_3). Hence, since V_1 already contains an element and its negative, V_2V_3 consists of pairs $a(-a)$, with each pair split evenly between V_2 and V_3. In other words, $V_3 = -V_2$ and thus

$$|V_2| = \mathsf{D}(G) - 1 = nm + m - 2. \tag{3.4}$$

Without loss of generality, we either have

$$(e_1 + ye_2)^{sm-2}(-e_2)^{(n-s)m+\epsilon-1}|V_2 \quad \text{or} \quad (e_1 + ye_2)^{sm-2}e_2^{(n-s)m+\epsilon-1}|V_2.$$

Case 2.1.1. Suppose $(e_1 + ye_2)^{sm-2}(-e_2)^{(n-s)m+\epsilon-1}|V_2$.

Suppose $1 < s < n$. Then $(e_1 + ye_2)^m(-e_2)^m|V_2$. Since $s > 1$, (3.2) implies $mye_2 = me_2$. But now $\sigma((e_1 + ye_2)^m(-e_2)^m) = me_1 + mye_2 - me_2 = 0$. As a result, since V_2 is an atom, we conclude that $(e_1 + ye_2)^m(-e_2)^m = V_2$, so that (3.4) implies $2m = |V_2| = nm + m - 2 \geq 2m + m - 2 > 2m$, a contradiction. So we instead conclude that $s = 1$ (in view of $s \in [1, n-1]$).

If there is an $i \in I_2$ such that $x_i \leq m - 2$, then $(e_1 + ye_2)^{x_i}(-e_2)(-x_ie_1 + (-x_iy + 1)e_2)$ is a zero-sum subsequence of the atom V_2, whence $V_2 = (e_1 + ye_2)^{x_i}(-e_2)(-x_ie_1 + (-x_iy + 1)e_2)$. But in such case, (3.4) yields $m - 2 + 2 \geq x_i + 2 = |V_2| = nm + m - 2 > m$, a contradiction. Therefore any $i \in I_2$ has $x_i = m - 1$.

Thus, if I_2 is nonempty, then this is only possible, in view of $\sum\limits_{i=1}^{m-\epsilon} x_i = m - 1$ with $x_i \in [1, m-1]$, if $\epsilon = m - 1$, $|W| = 1$ and $J_2 = \emptyset$. So, recalling that $|V_1| = 2$ and $s = 1$, we necessarily find, in this case, that V_2 has the form

$$V_2 = (e_1 + ye_2)^{m-2}(-e_2)^{(n-1)m+m-1}(e_1 + (-my + y + 1)e_2) \quad \text{or}$$
$$V_2 = (e_1 + ye_2)^{m-1}(-e_2)^{(n-1)m+m-2}(e_1 + (-my + y + 1)e_2).$$

However, in the former case, $\sigma(V_2)$ has e_1-coordinate equal to $(m-1)e_1 \neq 0$, while in the latter case, $\sigma(V_2)$ has e_2-coordinate equal to $3e_2 \neq 0$ (in view of $mn \geq 4$). Since V_2 is zero-sum, these are both contradictions, and we thereby conclude that $I_2 = \emptyset$.

If V_1 does not consist of a pair of terms from W, then V_2 must, in view of $I_2 = \emptyset$ and (3.4), contain every term from $\prod_{i=1}^{m-\epsilon}(x_ie_1 + (x_iy - 1)e_2)$, i.e., $J_2 = [1, m - \epsilon]$. But in this case, $\sigma(V_2)$ has e_1-coordinate equal to either $(m - 2 + \sum\limits_{i=1}^{m-\epsilon} x_i)e_1 = -3e_1$ or $(m - 1 + \sum\limits_{i=1}^{m-\epsilon} x_i)e_1 = -2e_1$, both nonzero in view of $m \geq 4$, thus contradicting that V_2 is zero-sum. Therefore, this only leaves the possibility of V_1 consisting of a pair of terms from W, in which case

$$V_2 = (e_1 + ye_2)^{m-1}(-e_2)^{(n-1)m+\epsilon} \prod_{i \in J_2}(x_ie_1 + (x_iy - 1)e_2)$$

with $|J_2| = m - \epsilon - 1$. Considering the e_1-coordinate of $\sigma(V_2)$, which must be zero, we conclude that $\sum\limits_{i \in J_2} x_i \equiv 1 \mod m$, which, in view of $\sum\limits_{i \in J_2} x_i \in [0, m-1]$, implies $\sum\limits_{i \in J_2} x_i = 1$. Consequently, in view of $|J_2| = m - \epsilon - 1$ and $x_i \in [1, m-1]$, it follows that $1 = |J_2| = m - \epsilon - 1$ with $x_i = 1$ for the unique $i \in J_2$. But now the e_2-coordinate of $\sigma(V_2)$ is easily calculated to be $((m-1)y + m - \epsilon + y - 1)e_2 = (my + 1)e_2$. Since this must be zero with $\text{ord}(e_2) = nm$, we must have $my + 1 \equiv 0 \mod m$, a subcase concluding contradiction.

Case 2.1.2. Suppose $(e_1 + ye_2)^{sm-2}e_2^{(n-s)m+\epsilon-1}|V_2$

In this case, $J_2 \neq \emptyset$, for otherwise $V_2|U$, a contradiction.

Suppose $x_i > 1$ for some $i \in J_2$. Then, in view of $\sum\limits_{i=1}^{m-\epsilon} x_i = m - 1$ with $x_i \in [1, m-1]$, we conclude that $\epsilon > 1$, whence

$$S = (e_1 + ye_2)^{sm-x_i}e_2^{(n-s)m+1}(x_ie_1 + (x_iy - 1)e_2)$$

is a subsequence of V_2. We claim that S now contains a nontrivial zero-sum subsequence. Indeed, if $s > 1$, then (3.2) implies that $mye_2 = me_2$, in which case a short calculation shows that S is itself a zero-sum sequence. On the other hand, if $s = 1$, then $mye_2 = -bme_2$ for some $b \in [1, n-1]$ (in view of (3.1)), and now $(e_1 + ye_2)^{m-x_i}e_2^{bm+1}(x_ie_1 + (x_iy - 1)e_2)$ is a nontrivial zero-sum subsequence of S, as claimed. Consequently, since S divides the atom V_2 and contains a nontrivial zero-sum subsequence, we conclude that $S = V_2$. Thus (3.4), $x_i \geq 2$ and $m \geq 3$ combine to imply $nm+m-2 = |V_2| = |S| = nm+2-x_i \leq nm$, a contradiction. So we instead conclude that $x_i = 1$ for every $i \in J_2$. In particular, since $J_2 \neq \emptyset$, we conclude that $(e_1 + (y-1)e_2)$ is a term of V_2.

As a result, if $I_2 \neq \emptyset$, then $(e_1 + ye_2)^{x_i-1}(-x_ie_1 + (-x_iy + 1)e_2)(e_1 + (y-1)e_2)$ is a zero-sum subsequence of V_2 for any $i \in I_2$, and therefore must be equal to the atom V_2, whence (3.4) yields $mn + m - 2 = |V_2| = x_i + 1 \le m$, contradicting $m \ge 4$. Therefore, we see that $I_2 = \emptyset$. Consequently

$$V_2 = (e_1 + ye_2)^{a_1} e_2^{a_2} (e_1 + (y-1)e_2)^{a_3}$$

where $sm-2 \le a_1 \le sm-1$, $(n-s)m+\epsilon-1 \le a_2 \le (n-s)m+\epsilon$, $\max\{1, m-\epsilon-1\} \le a_3 \le m-\epsilon$, and exactly one of the a_i does not achieve its upper bound. Since the e_1-coordinate of $\sigma(V_2)$ must be zero, it follows that $a_1 + a_3 \equiv 0 \mod m$, which means that either $a_1 = sm-2$ and $a_3 = 2$, or else $a_1 = sm-1$ and $a_3 = 1$.

Suppose $a_1 = sm-2$ and $a_3 = 2$. Then equality must hold in the upper bound for a_3, whence $2 = a_3 = m - \epsilon$ and $J_2 = [1, m-\epsilon]$. In view of $J_2 = [1, m-\epsilon]$ with $x_i = 1$ for all $i \in J_2$, we obtain $m - 1 = \sum_{i=1}^{m-\epsilon} x_i = \sum_{i \in J_2} x_i = |J_2| = m - \epsilon = 2$, where the final equality follows in view of $2 = a_3 = m - \epsilon$, contradicting that $m \ge 4$. So it remains to consider when $a_1 = sm-1$ and $a_3 = 1$.

In this case, we either have $1 = a_3 = m-\epsilon$ and $a_2 = (n-s)m + \epsilon - 1$, or else $1 = a_3 = m - \epsilon - 1$ and $a_2 = (n-s)m + \epsilon$. In both cases, the e_2-coordinate of $\sigma(V_2)$ is $(sym - sm + m - 3)e_2$. Thus, since $\mathrm{ord}(e_2) = mn$, we obtain the case concluding contradiction $sym - sm + m - 3 \equiv 0 \mod m$ in view of $m \ge 4$.

Case 2.2. $|V_i| \ge 3$ for all $i \in [1,3]$.

In this case, we conclude that the atoms V_j cannot contain both terms equal to e_2 and $-e_2$. As a result, the pigeonhole principle guarantees that some V_j, say V_1, either contains all terms equal to e_2 or all terms equal to $-e_2$. Hence, by symmetry, we can w.l.o.g. assume

$$e_2^{(n-s)m+\epsilon} \mid V_1.$$

Suppose $\pm(e_1 + ye_2) \notin \mathrm{supp}(V_1)$. Then, by considering the e_1-coordinate of $\sigma(V_1)$, we conclude that $\sigma_1 = 0$. In particular, we cannot have $|I_1| = m - \epsilon$ or $|J_1| = m - \epsilon$, since that would force $\pm\sigma_1 = \pm\sum_{i=1}^{m-\epsilon} x_i = \pm(m-1) \neq 0$. Consequently, we have

$$\sigma(T_1) = \Delta_1 e_2 \in [-(m-\epsilon-1), m-\epsilon-1] \cdot e_2. \tag{3.5}$$

However, since $-\sigma(T_1) = \sigma(V_1T_1^{-1}) = |V_1T_1^{-1}|e_2 = ((n-s)m+\epsilon)e_2$, it follows that the e_2-coordinate of $\sigma(T_1)$ is congruent to $sm - \epsilon$ modulo mn. However, since $sm - \epsilon \ge m - \epsilon$ and $-nm + sm - \epsilon \le -(m-\epsilon)$, we see that the e_2-coordinate of $\sigma(T_1)$ being congruent to $sm-\epsilon$ modulo mn is contrary to (3.5). So we instead conclude that $(e_1 + ye_2) \in \mathrm{supp}(V_1)$ or $(-e_1 - ye_2) \in \mathrm{supp}(V_1)$, which gives us two subcases

Case 2.2.1. $\mathsf{v}_{-e_1-ye_2}(V_1) > 0$.

Let $\mathsf{v}_{-e_1-ye_2}(V_1) = s'm + l > 0$, where $s' \in [0, s-1]$ and $l \in [0, m-1]$. Considering the sum of the e_1-coordinates of the terms of V_1, we conclude that $\sigma_1 \equiv l \mod m$. Thus, in view of (3.3), we have $\sigma_1 \in \{l, l-m\}$. But now, considering the sum of the e_2-coordinates of the terms of V_1 modulo m, we conclude that $\Delta_1 \equiv -\epsilon \mod m$, which in view of (3.3) forces $\Delta_1 \in \{m-\epsilon, -\epsilon\}$.

Suppose $\Delta_1 = -\epsilon < 0$. Then there will be at least ϵ terms from $-W$ contained in V_1. If one of these terms is equal to $e_1 + (y-1)e_2$, then

$$(-e_1 - ye_2)\big(e_1 + (y-1)e_2\big)e_2$$

will be a proper zero-sum subsequence of V_1, contradicting that V_1 is an atom. Therefore we instead have $x_i \ge 2$ for each of the ϵ terms of V_1 from $-W$. Since the remaining $m - 2\epsilon$ terms of $-W$ have $x_i \ge 1$, we obtain the estimate $m - 1 = \sum_{i=1}^{m-\epsilon} x_i \ge 2\epsilon + m - 2\epsilon = m$, which is a contradiction. So we cannot have $\Delta_1 = -\epsilon$, and instead conclude that $\Delta_1 = m - \epsilon$.

However, $\Delta_1 = m - \epsilon$ is only possible if V_1 contains all $m-\epsilon$ terms of W and no term from $-W$, in which case $\sigma_1 = -(m-1) \in \{l, l-m\}$. Hence $\sigma_1 = l - m$ with $l = 1$. But now

$$0 = \sigma(V_1) = (-s'my - ly + \sigma_1 y + \Delta_1 + (n-s)m + \epsilon)e_2 = -((s'+1)my + (s-1)m)e_2. \tag{3.6}$$

If $s = 1$, then $s' \in [0, s-1]$ forces $s' = 0$, whence (3.6) implies $mye_2 = 0$, contrary to (3.1). Therefore we can assume $s \ge 2$, in which case (3.2) implies $mye_2 = me_2$. But then

$$W(-e_1 - ye_2)e_2^{\epsilon}$$

is a proper zero-sum subsequence of V_1, contradicting that V_1 is an atom. This completes Case 2.2.1.

Case 2.2.2. $\mathsf{v}_{e_1+ye_2}(V_1) > 0$.

Let $\mathsf{v}_{e_1+ye_2}(V_1) = s'm + l > 0$, where $s' \in [0, s-1]$ and $l \in [0, m-1]$. Considering the sum of the e_1-coordinates of the terms of V_1, we conclude that $\sigma_1 \equiv -l \mod m$. Thus, in view of (3.3), we have $\sigma_1 \in \{-l, m-l\}$. But now, considering the sum of the e_2-coordinates of the terms of V_1 modulo m, we conclude that $\Delta_1 \equiv -\epsilon \mod m$, which in view of (3.3) forces $\Delta_1 \in \{m-\epsilon, -\epsilon\}$. Since $\Delta_1 = m - \epsilon$ is only possible if V_1 contains all $m-\epsilon$ terms of W and none from $-W$, we see that $\Delta_1 = m-\epsilon$ would imply $V_1 \mid U$, which is not possible as U has no proper nontrivial zero-sum subsequences. Therefore

$$\Delta_1 = -\epsilon.$$

Thus

$$0 = \sigma(V_1) = (s'my + ly + \sigma_1 y - sm)e_2. \tag{3.7}$$

Suppose $\sigma_1 = -l$. If also $s = 1$, then $s' = 0$, whence (3.7) implies $me_2 = 0$, contradicting that $\operatorname{ord}(e_2) = mn \geq 2m$. On the other hand, if $s > 1$, then $mye_2 = me_2$, whence (3.7) instead implies $(s'-s)me_2 = 0$. Thus $s' \equiv s \mod n$. However, since $s' \in [0, s-1] \subset [0, n-2]$, this is not possible. So we conclude that $\sigma_1 = -l$ is not possible, and we must instead have

$$\sigma_1 = m - l.$$

If $s > 1$, then (3.2) implies that

$$mye_2 = me_2 \tag{3.8}$$

holds. On the other hand, if $s = 1$, then $s' = 0$, whence (3.7) yields $(my - m)e_2 = 0$, and now (3.8) holds again. Thus we now know (3.8) holds in all cases.

From (3.7) and (3.8), we derive that $(s' - s + 1)me_2 = 0$, whence $s' \equiv s - 1 \mod n$. Thus, since $s' \in [0, s-1] \subset [0, n-2]$, we conclude that

$$s' = s - 1.$$

Also, since $m - l = \sigma_1 \leq m - 1$ holds by (3.3), we conclude that $l \neq 0$, and thus $l \in [1, m-1]$.

As in Case 2.2.1, if all terms of V_1 from $-W$ have $x_i \geq 2$, then we obtain the contradiction $m - 1 = \sum_{i=1}^{m-\epsilon} x_i \geq 2\epsilon + m - 2\epsilon = m$. Therefore there must be some term of V_1 equal to $e_1 + (y-1)e_2$, i.e.,

$$\mathsf{v}_{e_1+(y-1)e_2}(V_1) > 0. \tag{3.9}$$

Suppose $l = m - 1$. Then

$$(e_1 + ye_2)^{sm-1}\big(e_1 + (y-1)e_2\big)e_2^{(n-s)m+1}$$

will be a zero-sum subsequence of V_1 in view of (3.8). Moreover, it will be proper, contradicting that V_1 is an atom, unless $\epsilon = 1$ and V_1 contains only one term from $W(-W)$, which must be equal to $e_1 + (y-1)e_2$. However, $\epsilon = 1$ together with $\sum_{i=1}^{m-\epsilon} x_i = m - 1$ and $x_i \geq 1$ then forces $x_i = 1$ for all $i \in [1, m-1]$. But now the only terms of U not contained in V_1 are all equal to $-e_1 + (-y+1)e_2$. Since each atom V_j must contain a term from U and a term from $-U$, we see that $-e_1 + (-y+1)e_2 \in \operatorname{supp}(V_2) \cap \operatorname{supp}(V_3)$. However, V_2 and V_3 must also contain the remaining $m - 2 \geq 2$ terms of $-W$ all equal to $e_1 + (y-1)e_2$, which forces $V_2 = V_3 = \big(-e_1 + (-y+1)e_2\big)\big(e_1 + (y-1)e_2\big)$, contradicting that $V_1V_2V_3 = (-U)U$. So we instead conclude that

$$l \in [1, m-2].$$

Since $l < m - 1$ and $|V_i| \geq 3$ for all $i \in [1, 3]$, we see that one of either V_2 or V_3, say V_3, must contain all remaining $m - 1 - l > 0$ terms equal to $e_1 + ye_2$, while the other atom V_2 must contain all $sm - 1$ terms equal to $-e_1 - ye_2$. In summary,

$$\mathsf{v}_{e_1+ye_2}(V_3) = m - 1 - l \quad \text{and} \quad \mathsf{v}_{-e_1-ye_2}(V_2) = sm - 1. \tag{3.10}$$

Let us next examine the atom V_2 more closely. Letting $\beta \in [0, (n-s)m + \epsilon]$ be the multiplicity of $-e_2$ in V_3, we derive that $(n-s)m + \epsilon - \beta$ is the multiplicity of $-e_2$ in V_2. If $\beta = 0$, then

$$(-e_1 - ye_2)^{sm-1}(-e_2)^{(n-s)m+\epsilon} \mid V_2\,,$$

in which case, by symmetry, we are in the same situation as when $l = m - 1$ for the atom V_1 (simply swap e_2 for $-e_2$ in the arguments) and obtain the corresponding contradiction. Therefore

$$\beta \geq 1.$$

In view of (3.10), we see by summing the e_1-coordinates of the terms of V_2 that $\sigma_2 \equiv -1 \mod m$. Thus, in view of (3.3), we have $\sigma_2 \in \{-1, m-1\}$, However, if $\sigma_2 = m - 1$, then V_2 must contain all terms from $-W$, which is not possible since we showed earlier that V_1 contains a term from $-W$ equal to $e_1+(y-1)e_2$ (see (3.9)). Therefore we conclude that

$$\sigma_2=-1.$$

But then

$$0=\sigma(V_2)=(-(sm-1)y-y+\Delta_2+sm-\epsilon+\beta)e_2.$$

In view of the above equation and (3.8), we derive

$$\Delta_2\equiv\epsilon-\beta \mod mn.$$

As a result, observing that $nm+\epsilon-\beta\geq nm+\epsilon-((n-s)m+\epsilon)\geq m$ and that $-mn+\epsilon-\beta\leq -mn+m-1\leq -m-1$, we conclude from (3.3) that

$$\Delta_2=\epsilon-\beta\in[-(m-\epsilon),m-\epsilon].$$

However, we can slightly improve this estimate by recalling that $\Delta_1=-\epsilon$ forced there to be at least ϵ terms of V_1 from $-W$, leaving only at most $m-2\epsilon$ terms from $-W$ available for V_2. Thus

$$\Delta_2=\epsilon-\beta\in[-(m-2\epsilon),m-\epsilon]. \tag{3.11}$$

From (3.11), we infer that

$$\beta\leq m-\epsilon. \tag{3.12}$$

Let us next examine the atom V_3 more closely. Noting that $\sigma_1+\sigma_2+\sigma_3=0$, we deduce that

$$\sigma_3=-(\sigma_1+\sigma_2)=l+1-m.$$

Noting that $\Delta_1+\Delta_2+\Delta_3=0$, we deduce that

$$\Delta_3=-\Delta_1-\Delta_2=\epsilon-\epsilon+\beta=\beta.$$

Since $\Delta_3=\beta\geq 1$, we see that there must be at least β terms of V_3 from W.

In view of (3.9) and $|V_i|\geq 3$ for all $i\in[1,3]$, we find that the term $-e_1+(-y+1)e_2$ must be contained in either V_2 or V_3. This gives 2 final subcases.

Case 2.2.2.1. Suppose $-e_1+(-y+1)e_2\notin \operatorname{supp}(V_3)$.

Then $-e_1+(-y+1)e_2\in\operatorname{supp}(V_2)$ and all of the at least β terms of V_3 from W have $x_i\geq 2$. Thus we obtain the estimate

$$2\beta+(m-\epsilon-\beta)\leq\sum_{i=1}^{m-\epsilon}x_i=m-1,$$

yielding $\beta\leq\epsilon-1$. Since $-e_1+(-y+1)e_2\in\operatorname{supp}(V_2)$ and $\beta\leq\epsilon-1$, we see in view of (3.8) that

$$(-e_2)^{(n-s)m+1}(-e_1-ye_2)^{sm-1}(-e_1+(-y+1)e_2)$$

is a zero-sum subsequence of V_2. Thus we contradict that V_2 is an atom unless $\beta=\epsilon-1$ and $(-e_1+(-y+1)e_2)$ is the unique term of V_2 from $W(-W)$. However, equality in the estimate $\beta\leq\epsilon-1$ is only possible if V_3 contains exactly β terms from W, which in view of $\Delta_3=\beta$ is only possible if V_3 contains no terms of $-W$. Furthermore, each of the β terms of V_3 from W must have $x_i=2$—else we again contradict that equality holds in the estimate $\beta\leq\epsilon-1$. In particular, since $\beta\geq 1$, we see that

$$(-2e_1+(-2y+1)e_2)\in\operatorname{supp}(V_3). \tag{3.13}$$

Since we have just derived that neither V_2 nor V_3 contains terms from $-W$, it follows that V_1 contains all the terms from $-W$, and thus none from W in view of $|V_1|\geq 3$. Consequently, it follows that $m-l=\sigma_1=m-1$, implying $l=1$. However, in view of $\beta\geq 1$, (3.13), and $l=1$ with $m\geq 5$, it follows that

$$(e_1+ye_2)^2(-e_2)(-2e_1+(-2y+1)e_2)$$

is a proper zero-sum subsequence of V_3, contradicting that V_3 is an atom.

Case 2.2.2.2. Suppose $-e_1+(-y+1)e_2 \in \operatorname{supp}(V_3)$.

Since $m-l-1 \ge 1$, $\beta \ge 1$ and $-e_1+(-y+1)e_2 \in \operatorname{supp}(V_3)$, we find that

$$(e_1+ye_2)\big(-e_1+(-y+1)e_2\big)(-e_2)$$

is a zero-sum subsequence of V_3. Since V_3 is an atom, this cannot be a proper subsequence, which implies

$$l = m-2, \quad \beta = 1, \quad \text{ and that } -e_1+(-y+1)e_2 \text{ is the only term of } V_3 \text{ from } W(-W).$$

Since $\Delta_1 = -\epsilon < 0$, we know that there are ϵ terms of V_1 from $-W$. However, if these were all the terms of $-W$, then V_1 could contain no terms from W (in view of $|V_1| \ge 3$) and we would have $m-l = \sigma_1 = m-1$; hence $l=1$, contradicting that $l = m-2$ with $m \ge 4$. As a result, we see that the ϵ terms of V_1 from $-W$ cannot be all the terms of $-W$, from which we derive that $\epsilon < |W| = m-\epsilon$, and thus that

$$\epsilon < \frac{m}{2}.$$

We established in (3.9) that $x_i = 1$ for some $i \in [1, m-\epsilon]$. However, if there is only one $i \in [1, m-\epsilon]$ such that $x_i = 1$, then we would obtain the estimate $m-1 = \sum_{i=1}^{m-\epsilon} x_i \ge 2(m-\epsilon-1)+1$, contradicting that $\epsilon < \frac{m}{2}$. As a result, we see that $(-e_1+(-y+1)e_2)^2 \mid U(-U)$. In view of (3.9) and $|V_1| \ge 3$, we see that V_1 cannot contain a term equal to $-e_1+(-y+1)e_2$. On the other hand, since $-e_1+(-y+1)e_2$ is the only term of V_3 from $W(-W)$, we see that V_3 cannot contain both terms of $U(-U)$ equal to $-e_1+(-y+1)e_2$. In consequence, we conclude that $-e_1+(-y+1)e_2 \in \operatorname{supp}(V_2)$.

But now, if $\epsilon \ge 2$, then

$$(-e_2)^{(n-s)m+1}(-e_1-ye_2)^{sm-1}(-e_1+(-y+1)e_2)$$

is a zero-sum subsequence of V_2 in view of (3.8). Furthermore, it will be a proper zero-sum subsequence, contradicting that V_2 is an atom, unless $\epsilon = 2$ and $(-e_1+(-y+1)e_2)$ is the only term of V_2 from $W(-W)$. However, in such case, we would have $|T_2|+|T_3| = 2$, which is only possible, in view of $|V_1| \ge 3$, if the 2 terms of T_2 and T_3, both with $x_i = 1$, cover all $m-\epsilon$ terms of W. But this implies $2 = \sum_{i=1}^{m-\epsilon} x_i = m-1$, contradicting that $m \ge 4$. Thus it remains only to consider the case when $\epsilon = 1$, which, in view of $\sum_{i=1}^{m-\epsilon} x_i = m-1$ with $x_i \in [1, m-1]$, is only possible if $x_i = 1$ for all $i \in [1, m-\epsilon] = [1, m-1]$.

Since $\epsilon = 1$ and $\beta = 1$, we have $\Delta_2 = \epsilon - \beta = 0$. In consequence, we see that V_2 must contain an equal number of terms from W and from $-W$. However, since $x_i = 1$ for all $i \in [1, m-\epsilon]$ and since $|V_2| \ge 3$, this forces V_2 to contain no terms from $W(-W)$ at all, whence $\sigma_2 = 0$, contradicting that we already showed $\sigma_2 = -1$, thus completing the proof. □

Theorem 3.5. *Let H be a Krull monoid with class group $G \cong C_m \oplus C_{mn}$, where $m, n \in \mathbb{N}$ and $m \ge 2$, and suppose that every class contains a prime divisor. Then*

$$\mathcal{V}_{\{2,\mathsf{D}(G)\}}(H) = \begin{cases} \{2a \mid a \in [1,n]\} \cup \{\mathsf{D}(G)\} & m = 2, \\ [2, \mathsf{D}(G)] & m \in [3,4], \\ [2, \mathsf{D}(G)] \setminus \{3\} & m \ge 5. \end{cases}$$

Proof. By Lemma 2.1, it suffices to prove the assertion for the monoid $\mathcal{B}(G)$ where $G = C_m \oplus C_{mn}$. We have $\mathsf{D}(G) = \mathsf{D}^*(G) = m+mn-1$ and set $M = \{2, \mathsf{D}(G)\}$. Recall that

$$\{2, m\} \cup [mn, \mathsf{D}(G)] \subset \mathcal{V}_M(G) \subset [2, \mathsf{D}(G)]$$

by Lemmas 3.2.1 and 3.3 (with $G_1 = \{0\}$). Moreover, by Proposition 3.4, we have $3 \notin \mathcal{V}_M(G)$ if $m \ge 5$. We choose a basis (e_1, e_2) of G with $\operatorname{ord}(e_1) = m$ and $\operatorname{ord}(e_2) = mn$ and provide a series of examples which cover all cases.

Case 1. $m = 2$. This follows from Lemma 3.2.2.

Case 2. $m = 3$. For $j \in [1, 3n-1]$, we set

$$\begin{aligned} U &= e_2^{3n-1} e_1 (e_1 + je_2)\big(e_1 + (1-j)e_2\big), \\ V_1 &= e_2^{3n-j}(e_1+je_2)(-e_1), \\ V_2 &= \big(e_1+(1-j)e_2\big)(-e_1+(j-1)e_2), \\ V_3 &= e_2(-e_2). \end{aligned}$$

We have $U, V_1, V_2, V_3 \in \mathcal{A}(G)$, $|U| = \mathsf{D}(G)$, $V_1(-V_1)V_2V_3^{j-1} = (-U)U$, and thus $2+j \in \mathsf{L}\big((-U)U\big)$ for $j \in [1, 3n-1]$. This shows $[3, 3n+1] \subset \mathcal{V}_M(G)$.

Case 3. $m=4$. For $j \in [2, 4n-2]$, we set

$$\begin{aligned} U &= e_2^{4n-1} e_1 (e_1+e_2)\big(e_1+je_2\big)\big(e_1-je_2\big), \\ V_1 &= e_2^{j+1}\big(e_1-je_2\big)(-e_1-e_2), \\ V_2 &= (-e_2)^j\big(e_1+je_2\big)(-e_1), \\ V_3 &= (-e_2)e_1(e_1+e_2)\big(-e_1-je_2\big)\big(-e_1+je_2\big), \\ V_4 &= e_2(-e_2). \end{aligned}$$

We have $U, V_1, \ldots, V_4 \in \mathcal{A}(G)$, $|U| = \mathsf{D}(G)$, $V_1V_2V_3V_4^{4n-2-j} = (-U)U$, and thus $4n+1-j \in \mathsf{L}\big((-U)U\big)$ for $j \in [2, 4n-2]$. This shows $[3, 4n-1] \subset \mathcal{V}_M(G)$.

Case 4. $m \ge 5$ odd. We begin by showing that $4 \in \mathcal{V}_M(G)$. Set

$$\begin{aligned} U &= e_2^{mn-1}(ne_2+e_1)^{\frac{m-1}{2}-1}(-2ne_2+e_1)(-ne_2+e_1)^{\frac{m-1}{2}-1}((2n+1)e_2+e_1)e_1, \\ V_1 &= e_2^{mn-n}(ne_2+e_1)(-e_1), \\ V_2 &= (-e_2)^{mn-n}(-2ne_2+e_1)(ne_2-e_1), \\ V_3 &= (ne_2+e_1)^{\frac{m-1}{2}-2}(ne_2-e_1)^{\frac{m-1}{2}-2}((2n+1)e_2+e_1)(2ne_2-e_1)e_2^{n-1}, \\ V_4 &= (-ne_2+e_1)^{\frac{m-1}{2}-1}(-ne_2-e_1)^{\frac{m-1}{2}-1}(-(2n+1)e_2-e_1)e_1(-e_2)^{n-1}. \end{aligned}$$

We have U, $V_1, \ldots, V_4 \in \mathcal{A}(G)$, $|U| = \mathsf{D}(G)$, $V_1V_2V_3V_4 = (-U)U$, and thus $4 \in \mathsf{L}\big((-U)U\big) \subset \mathcal{V}_M(G)$. It remains to show $[5, mn-1] \subset \mathcal{V}_M(G)$.

For $i \in [0, mn-1]$, we set

$$\begin{aligned} U &= e_2^{mn-1}(e_2+e_1)^{\frac{m-5}{2}}\big((m+i+1)e_2+e_1\big)\big((3-m)e_2+e_1\big)(-e_2+e_1)^{\frac{m-5}{2}} \\ &\quad \big((-1-i)e_2+e_1\big)(-2e_2+e_1)e_1, \\ V_1 &= (e_2+e_1)^{\frac{m-5}{2}}\big((3-m)e_2+e_1\big)(e_2-e_1)^{\frac{m-5}{2}}(2e_2-e_1), \\ V_2 &= e_2^{mn-1-i}e_1\big((1+i)e_2-e_1\big), \\ V_3 &= \big((m+i+1)e_2+e_1\big)\big(-(m+i+1)e_2-e_1\big), \\ V_4 &= e_2(-e_2). \end{aligned}$$

We have $U, V_1, \ldots, V_4 \in \mathcal{A}(G)$, $|U| = \mathsf{D}(G)$, $V_1(-V_1)V_2(-V_2)V_3V_4^i = (-U)U$, and thus $5+i \in \mathsf{L}\big((-U)U\big)$ for $i \in [0, mn-1]$, and therefore $[5, mn+4] \subset \mathcal{V}_M(G)$.

Case 5. $m \ge 6$ even. We begin by showing that $4 \in \mathcal{V}_M(G)$. Set

$$\begin{aligned} U &= e_2^{mn-1}(ne_2+e_1)^{\frac{m}{2}-2}(-ne_2+e_1)^{\frac{m}{2}}((2n+1)e_2+e_1)e_1, \\ V_1 &= (ne_2+e_1)^{\frac{m}{2}-2}(ne_2-e_1)^{\frac{m}{2}-1}((2n+1)e_2+e_1)e_2^{n-1}, \\ V_2 &= (-ne_2+e_1)(-e_1)(-e_2)^{mn-n}. \end{aligned}$$

We have U, V_1, $V_2 \in \mathcal{A}(G)$, $|U| = \mathsf{D}(G)$, $V_1(-V_1)V_2(-V_2) = (-U)U$, and thus $4 \in \mathsf{L}\big((-U)U\big) \subset \mathcal{V}_M(G)$.

Next we show that $5 \in \mathcal{V}_M(G)$. Set

$$\begin{aligned} U &= e_2^{mn-1}(ne_2+e_1)^{\frac{m-2}{2}-1}(-ne_2+e_1)^{\frac{m-2}{2}}(-2ne_2+e_1)((3n+1)e_2+e_1)e_1, \\ V_1 &= e_2^{mn-n}(ne_2+e_1)(-e_1), \\ V_2 &= (-e_2)^{mn-n}(-2ne_2+e_1)(ne_2-e_1), \\ V_3 &= (ne_2+e_1)^{\frac{m-2}{2}-2}(ne_2-e_1)^{\frac{m-2}{2}-2}((3n+1)e_2+e_1)(2ne_2-e_1)e_2^{n-1}, \\ V_4 &= (-ne_2+e_1)^{\frac{m-2}{2}-1}(-ne_2-e_1)^{\frac{m-2}{2}-1}(-(3n+1)e_2-e_1)e_1(-e_2)^{n-1}, \\ V_5 &= (-ne_2+e_1)(ne_2-e_1). \end{aligned}$$

We have U, $V_1, \ldots, V_5 \in \mathcal{A}(G)$, $|U| = \mathsf{D}(G)$, $V_1V_2V_3V_4V_5 = (-U)U$, and thus $5 \in \mathsf{L}\big((-U)U\big) \subset \mathcal{V}_M(G)$. It remains to show $[6, mn-1] \subset \mathcal{V}_M(G)$.

For $i \in [0, mn-1]$, we set

$$\begin{aligned} U &= e_2^{mn-1}(e_2+e_1)^{\frac{m-6}{2}}\big((m+i+2)e_2+e_1\big)\big((3-m)e_2+e_1\big)(-e_2+e_1)^{\frac{m-6}{2}} \\ &\quad \big((-1-i)e_2+e_1\big)(-3e_2+e_1)e_1^2, \\ V_1 &= (e_2+e_1)^{\frac{m-6}{2}}\big((3-m)e_2+e_1\big)(e_2-e_1)^{\frac{m-6}{2}}(3e_2-e_1), \\ V_2 &= e_2^{mn-1-i}e_1\big((1+i)e_2-e_1\big), \\ V_3 &= \big((m+i+2)e_2+e_1\big)\big(-(m+i+2)e_2-e_1\big), \\ V_4 &= e_2(-e_2), \\ V_5 &= e_1(-e_1). \end{aligned}$$

We have $U, V_1, \ldots, V_5 \in \mathcal{A}(G)$, $|U| = \mathsf{D}(G)$, $V_1(-V_1)V_2(-V_2)V_3V_4^iV_5 = (-U)U$, and thus $6+i \in \mathsf{L}\big((-U)U\big)$ for $i \in [0, mn-1]$, and therefore $[6, mn+5] \subset \mathcal{V}_M(G)$. □

4. Products of two atoms in Krull monoids with class group of rank greater than two

We start with a simple technical lemma.

Lemma 4.1. *Let $G = G_1 \oplus G_2$ with $G_1, G_2 \subset G$ non-trivial subgroups satisfying $\mathsf{d}^*(G_1)+\mathsf{d}^*(G_2) = \mathsf{d}^*(G)$ and suppose that $U_1 \in \mathcal{A}(G_1)$ with $|U_1| = \mathsf{D}^*(G_1)$ and $l \in \mathsf{L}\big((-U_1)U_1\big) \cap [2, \mathsf{d}^*(G_1)]$. Then there exists a $U \in \mathcal{A}(G)$ with $|U| = \mathsf{D}^*(G)$ such that $l \in \mathsf{L}\big((-U)U\big)$. In particular,*

$$\mathcal{V}_{\{2,\mathsf{D}^*(G_1)\}}(G_1) \setminus \{\mathsf{D}^*(G_1)\} \subset \mathcal{V}_{\{2,\mathsf{D}^*(G)\}}(G).$$

Proof. By hypothesis, there are $V_1, \ldots, V_l \in \mathcal{A}(G_1)$ such that

$$(-U_1)U_1 = V_1 \cdot \ldots \cdot V_l\,.$$

Moreover, by re-indexing as need be, we can assume $|V_1| = \ldots = |V_k| = 2$ and $|V_i| \ge 3$ for all $i \in [k+1, l]$, where $k \in [0, l]$. Since $l \le \mathsf{d}^*(G_1) < \mathsf{D}^*(G_1) = |U_1|$, it follows that $k < l$. Clearly, there is an $S \in \mathcal{F}(G)$ such that $V_{k+1} \cdot \ldots \cdot V_l = (-S)S$. Furthermore, there are $g \in G$ and $S_{l-1}, S_l \in \mathcal{F}(G)$ such that w.l.o.g. $V_l = gS_l$ and $V_{l-1} = (-g)S_{l-1}$.

We choose a basis $(e_1, \ldots, e_r)$ of G_2 such that $\mathsf{d}^*(G_2) = \sum_{i=1}^r (n_i - 1)$, where $n_i = \operatorname{ord}(e_i)$ for $i \in [1, r]$, and set $e_0 = e_1 + \ldots + e_r$. We define

$$T = e_1^{n_1-1} \cdot \ldots \cdot e_r^{n_r-1}, \ V_l' = T(e_0+g)S_l, \ V_{l-1}' = (-T)(-e_0-g)S_{l-1}, \quad \text{and} \quad U = T(e_0+g)g^{-1}U_1\,.$$

Then $V_{l-1}', V_l', U \in \mathcal{A}(G)$, and it follows that

$$(-U)U = V_1 \cdot \ldots \cdot V_{l-2}V_{l-1}'V_l'$$

and

$$|U| = (|U_1|-1) + |T| + 1 = \mathsf{d}^*(G_1) + \mathsf{d}^*(G_2) + 1 = \mathsf{d}^*(G) + 1 = \mathsf{D}^*(G)\,.$$

The in particular statement is an immediate consequence. □

Theorem 4.2. *Let H be a Krull monoid with class group $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$, where $r \ge 3$, $n_{r-1} \ge 3$ and $1 < n_1 \mid \ldots \mid n_r$, and suppose that every class contains a prime divisor. Then $\mathcal{V}_{\{2,\mathsf{D}^*(G)\}}(H) = [2, \mathsf{D}^*(G)]$.*

Proof. By Lemma 2.1, it suffices to prove the assertion for the monoid $\mathcal{B}(G)$ where $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$. We start with the following assertion.

A1. Let $r = 3$. Then there exists a $U \in \mathcal{A}(G)$ such that $\{2, 3, \mathsf{D}^*(G)\} \subset \mathsf{L}\big((-U)U\big)$.

Suppose that **A1** holds. We set $M = \{2, \mathsf{D}^*(G)\}$ and proceed by induction on r. If $r = 3$, then Theorem 3.5, **A1**, and Lemma 4.1 show that $[2, \mathsf{d}^*(C_{n_2} \oplus C_{n_3})] \subset \mathcal{V}_M(G)$, and Lemma 3.3 implies that $[\mathsf{d}^*(C_{n_1}) + n_3, \mathsf{D}^*(G)] \subset \mathcal{V}_M(G)$. Suppose that $r \ge 4$ and observe that, for $G' = C_{n_2} \oplus \ldots \oplus C_{n_r}$, the induction hypothesis implies that $[2, \mathsf{D}^*(G')] \subset \mathcal{V}_{\{2,\mathsf{D}^*(G')\}}(G')$. Then by Lemma 4.1 we have $[2, \mathsf{d}^*(G')] \subset \mathcal{V}_M(G)$, and Lemma 3.3 implies that $[\mathsf{d}^*(C_{n_1} \oplus \ldots \oplus C_{n_{r-2}}) + n_r, \mathsf{D}^*(G)] \subset \mathcal{V}_M(G)$.

Thus it remains to prove **A1**. To do so, we need two auxiliary assertions.

A2. Let $m, n \in \mathbb{N}$ with $m \ge 5$ odd and $m \mid n$. Then there is a sequence $S \in \mathcal{F}(C_n)$ of length $|S| = m-1$ with a decomposition $S = S_1S_2s$ with $S_1, S_2 \in \mathcal{F}(C_n)$, $|S_1| = \frac{m-1}{2}$, $|S_2| = \frac{m-3}{2}$, and $s \in C_n$ such that the following conditions are fulfilled:

- $2\sigma(S_1) = s$ and $\sigma(S) = 0$.

- Any zero-sum subsequence of S does not have the same number of terms from S_1 as from $S_2 s$ unless it is the entire sequence or trivial.

A3. Let $m, n \in \mathbb{N}$ with $m \ge 8$ even, $m \,|\, n$, and let $e \in C_n$ have order n. Then there is a sequence $S \in \mathcal{F}(C_n)$ of length $|S| = m-2$ with a decomposition $S = s_1 s_2 S_1 S_2$ with $S_1, S_2 \in \mathcal{F}(C_n)$, $|S_1| = \frac{m}{2} - 1$, $|S_2| = \frac{m}{2} - 3$, and $s_1, s_2 \in C_n$ such that the following conditions are fulfilled:
- $\sigma(s_1 s_2 S_1 S_2) = -e$.
- $2(s_1 + s_2) - \sigma(S_1) + \sigma(S_2) = -e$.
- Any subsequence from $s_1 s_2 S_1 S_2$ with sum 0 or $-e$ does not have the same number of terms from $s_1 s_2 S_2$ as from S_1 unless it is the entire sequence or trivial.

Proof of **A2**. We choose an element $e \in C_n$ with $\operatorname{ord}(e) = n$ and distinguish two cases.

Case 1. n is odd.

We set
$$S_1 = \left(\frac{n+1}{2}e\right) 0^{\frac{m-3}{2}}, \quad S_2 = e^{\frac{m-5}{2}} \left(\frac{n-m+2}{2}e\right), \quad \text{and} \quad s = e.$$
Now we find $|S_1| = \frac{m-1}{2}$, $|S_2| = \frac{m-3}{2}$, and $|S| = m-1$. Next we show the two additional conditions.

We find
$$2\sigma(S_1) = 2 \cdot \frac{n+1}{2}e = (n+1)e = e = s \quad \text{and} \quad \sigma(S) = (\frac{n+1}{2} + \frac{n-3}{2} + 1)e = 0,$$
and thus the first condition is satisfied. Next we calculate the sumsets of $S_2 s$ and S_1. We have
$$\Sigma(S_2 s) = \left\{e, \ldots, \frac{m-3}{2}e\right\} \cup \left\{\frac{n-m+2}{2}e, \ldots, \frac{n-1}{2}e\right\} \quad \text{and} \quad \Sigma(S_1) = \left\{0, \frac{n+1}{2}e\right\}.$$
If $T \,|\, S$ is a non-trivial zero-sum subsequence with a decomposition $T = T_1 T_2$, where $1 \ne T_1 \,|\, S_1$, $1 \ne T_2 \,|\, S_2 s$, and $|T_1| = |T_2|$, then we find $S_2 s (\frac{n+1}{2}e) \,|\, T$, and thus $T_2 = S_2 s$, $T_1 = S_1$, and $T = S$.

Case 2. n is even.

Note that m odd and n even implies that $2m \le n$. We set
$$S_1 = \left(\frac{n+2}{2}e\right) 0^{\frac{m-3}{2}}, \quad S_2 = (2e)^{\frac{m-5}{2}} \left(\left(\frac{n}{2} - m + 2\right)e\right), \quad \text{and} \quad s = 2e.$$
Now we again find $|S_1| = \frac{m-1}{2}$, $|S_2| = \frac{m-3}{2}$, and $|S| = m-1$. Next we show the two additional conditions.

We find
$$2\sigma(S_1) = 2 \cdot \frac{n+2}{2}e = 2e = s \quad \text{and} \quad \sigma(S) = (\frac{n}{2} + 1 + \frac{n}{2} - 3 + 2)e = 0,$$
and thus the first condition is satisfied. Next we calculate the sumsets of $S_2 s$ and S_1. We have
$$\Sigma(S_1) = \left\{0, \frac{n+2}{2}e\right\} \quad \text{and}$$
$$\Sigma(S_2 s) = \{2e, 4e, \ldots, (m-3)e\} \cup \left\{\left(\frac{n}{2} - m + 2\right)e, \left(\frac{n}{2} - m + 4\right)e, \ldots, (\frac{n}{2} - 1)e\right\}.$$
If $T \,|\, S$ is a non-trivial zero-sum subsequence with a decomposition $T = T_1 T_2$, where $1 \ne T_1 \,|\, S_1$, $1 \ne T_2 \,|\, S_2 s$, and $|T_1| = |T_2|$, then we find $S_2 s (\frac{n+1}{2}e) \,|\, T$, and thus $T_2 = S_2 s$, $T_1 = S_1$, and $T = S$. □

Proof of **A3**. Let $e \in C_n$ with $\operatorname{ord}(e) = n$. We set
$$S_1 = (2e)^{\frac{m}{2}-2}\big((4-m)e\big), \quad S_2 = 0^{\frac{m}{2}-4}(-e), \quad \text{and} \quad s_1 = s_2 = 0.$$
Now we find $|S_1| = \frac{m}{2} - 1$, $|S_2| = \frac{m}{2} - 3$, and $|S| = m-2$. Furthermore, we have
$$\sigma(s_1 s_2 S_1 S_2) = -e \quad \text{and} \quad 2(s_1 + s_2) - \sigma(S_1) + \sigma(S_2) = -e\,,$$
and thus the first two conditions are fulfilled. Next we calculate the sumsets of $s_1 s_2 S_2$ and S_1. We have
$$\Sigma(S_1) = \{2e, 4e, \ldots, (m-4)e\} \cup \{-(m-4)e, -(m-6)e, \ldots, -2e, 0\} \quad \text{and} \quad \Sigma(s_1 s_2 S_2) = \{0, -e\}\,.$$
Since S_1 has no proper non-trivial zero-sum subsequence, we find that the third condition is satisfied. □

Proof of **A1**. If $n_1 \in [3,4]$ and $G_1 = C_{n_1} \oplus C_{n_2}$, then $3 \in \mathcal{V}_{\{2, \mathsf{D}^*(G_1)\}}(G_1)$ by Theorem 3.5. Since $3 \le \mathsf{d}^*(G_1)$, Lemma 4.1 implies the assertion. Thus we may assume that $n_1 \ge 5$.

Let (e_1, e_2, e_3) be a basis of G with $\operatorname{ord}(e_i) = n_i$, and let $p_i \colon G \to \langle e_i \rangle$ denote the canonical projection for every $i \in [1,3]$. For an element $g = a_1 e_1 + a_2 e_2 + a_3 e_3 \in G$, with $a_i \in [0, n_i - 1]$ for all $i \in [1,3]$, we set
$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = a_1 e_1 + a_2 e_2 + a_3 e_3\,.$$

Moreover, for an element $a_1e_1 \in \langle e_1\rangle$ with $a_1 \in [0, n_1-1]$, a sequence $S_2 \in \mathcal{F}(\langle e_2\rangle)$ and a sequence $S_3 \in \mathcal{F}(\langle e_3\rangle)$ with $|S_2| = |S_3|$, we denote by

$$S = \begin{pmatrix} a_1 \\ S_2 \\ S_3 \end{pmatrix} \in \mathcal{F}(G) \quad \text{a sequence satisfying} \quad \begin{cases} p_1(S) = (a_1e_1)^{|S_2|} \\ p_2(S) = S_2 \\ p_3(S) = S_3. \end{cases}$$

Now we distinguish three cases based on n_1.

Case 1. $n_1 = 6$.

In this particular case, we set

$$\begin{aligned} U &= e_2^{n_2-1}e_3^{n_3-1}(e_1-e_3)(e_1+2e_2-e_3)(e_1+3e_2+3e_3)(e_1-2e_2-2e_3)(e_1-e_2)(e_1-e_2+2e_2)\,, \\ V_1 &= (-e_2)^{n_2-4}e_3^{n_3-4}(e_1-e_2)(e_1-e_2+2e_3)(-e_1+e_3)(-e_1-2e_2+e_3)\,, \\ V_2 &= (-e_2)^3(-e_3)^{n_3-1}(e_1+3e_2+3e_3)(e_1-2e_2-2e_3)(-e_1+e_2)(-e_1+e_2-2e_3)\,, \\ V_3 &= e_3^3e_2^{n_2-1}(e_1-e_3)(e_1+2e_2-e_3)(-e_1-3e_2-3e_3)(-e_1+2e_2+2e_3)\,, \end{aligned}$$

and we find U, V_1, V_2, $V_3 \in \mathcal{A}(G)$, $|U| = \mathsf{D}^*(G)$, and $V_1V_2V_3 = (-U)U$, and thus $\{2, 3, \mathsf{D}^*(G)\} \subset \mathsf{L}\big((-U)U\big)$.

Case 2. $n_1 \ge 8$ even.

Let $S = (s_1e_2)(s_2e_2)S_1S_2 \in \mathcal{F}(\langle e_2\rangle)$ with $s_1, s_2 \in [0, n_2-1]$ and $T = (t_1e_3)(t_2e_3)T_1T_2 \in \mathcal{F}(\langle e_3\rangle)$ with $t_1, t_2 \in [0, n_3-1]$ be two sequences of length $|S| = |T| = n_1-2$ fulfilling the conditions from **A3**. Now we set

$$\begin{aligned} U &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}^{n_2-1} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}^{n_3-1} \begin{pmatrix} 1 \\ s_1 \\ 1+t_2 \end{pmatrix} \begin{pmatrix} 1 \\ s_2 \\ 1+t_1 \end{pmatrix} \begin{pmatrix} 1 \\ s_1+1 \\ t_1 \end{pmatrix} \begin{pmatrix} 1 \\ s_2+1 \\ t_2 \end{pmatrix} \begin{pmatrix} 1 \\ -S_1 \\ -T_1 \end{pmatrix} \begin{pmatrix} 1 \\ S_2 \\ T_2 \end{pmatrix}, \\ V_1 &= \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}^{n_2-2} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}^{n_3-2} \begin{pmatrix} 1 \\ s_1 \\ 1+t_2 \end{pmatrix} \begin{pmatrix} 1 \\ s_2 \\ 1+t_1 \end{pmatrix} \begin{pmatrix} -1 \\ -s_1-1 \\ -t_1 \end{pmatrix} \begin{pmatrix} -1 \\ -s_2-1 \\ -t_2 \end{pmatrix}, \\ V_2 &= \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}^{n_3-1} \begin{pmatrix} -1 \\ -s_1 \\ -1-t_2 \end{pmatrix} \begin{pmatrix} -1 \\ -s_2 \\ -1-t_1 \end{pmatrix} \begin{pmatrix} 1 \\ -S_1 \\ -T_1 \end{pmatrix} \begin{pmatrix} -1 \\ -S_2 \\ -T_2 \end{pmatrix}, \\ V_3 &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}^{n_2-1} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ s_1+1 \\ t_1 \end{pmatrix} \begin{pmatrix} 1 \\ s_2+1 \\ t_2 \end{pmatrix} \begin{pmatrix} 1 \\ S_2 \\ T_2 \end{pmatrix} \begin{pmatrix} -1 \\ S_1 \\ T_1 \end{pmatrix}, \end{aligned}$$

and we find $|U| = \mathsf{D}^*(G)$ and $V_1V_2V_3 = (-U)U$. Since S and T have the special properties from **A3**, we have U, V_1, V_2, $V_3 \in \mathcal{A}(G)$, and thus $\{2, 3, \mathsf{D}^*(G)\} \subset \mathsf{L}\big((-U)U\big)$.

Case 3. $n_1 \ge 5$ odd.

Let $S = S_1S_2(se_2) \in \mathcal{F}(\langle e_2\rangle)$ with $s \in [0, n_2-1]$ and $T = T_1T_2(te_3) \in \mathcal{F}(\langle e_3\rangle)$ with $t \in [0, n_3-1]$ be two sequences of length $|S| = |T| = n_1-1$ fulfilling the conditions from **A2**. Now we set

$$\begin{aligned} U &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}^{n_2-1} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}^{n_3-1} \begin{pmatrix} 1 \\ S_1 \\ T_1 \end{pmatrix} \begin{pmatrix} 1 \\ -S_2 \\ -T_2 \end{pmatrix} \begin{pmatrix} 1 \\ 1-s \\ -t \end{pmatrix} \begin{pmatrix} 1 \\ -s \\ 1-t \end{pmatrix}, \\ V_1 &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}^{n_2-1} \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}^{n_3-1} \begin{pmatrix} 1 \\ 1-s \\ -t \end{pmatrix} \begin{pmatrix} -1 \\ s \\ t-1 \end{pmatrix}, \\ V_2 &= \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}^{n_2-1} \begin{pmatrix} 1 \\ S_1 \\ T_1 \end{pmatrix} \begin{pmatrix} -1 \\ S_2 \\ T_2 \end{pmatrix} \begin{pmatrix} -1 \\ s-1 \\ t \end{pmatrix}, \\ V_3 &= \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}^{n_3-1} \begin{pmatrix} 1 \\ -S_2 \\ -T_2 \end{pmatrix} \begin{pmatrix} 1 \\ -s \\ 1-t \end{pmatrix} \begin{pmatrix} -1 \\ -S_1 \\ -T_1 \end{pmatrix}, \end{aligned}$$

and we find $|U| = \mathsf{D}^*(G)$ and $V_1V_2V_3 = (-U)U$. Since S and T have the special properties from **A2**, we have U, V_1, V_2, $V_3 \in \mathcal{A}(G)$, and thus $\{2, 3, \mathsf{D}^*(G)\} \subset \mathsf{L}\big((-U)U\big)$. □

5. Arithmetical characterizations of class groups

Two reduced Krull monoids H and H' are isomorphic if and only if there is a group isomorphism $\Phi\colon \mathcal{C}(H) \to \mathcal{C}(H')$ such that, for every class $g \in \mathcal{C}(H)$, the number of primes in g equals the number of primes in the class $\Phi(g) \in \mathcal{C}(H')$ ([17, Theorem 2.5.4]). This justifies the classical philosophy in algebraic number theory that the class group of a ring of integers completely determines its arithmetic. Initiated by Narkiewicz in the 1970s, the reverse question—to what extent do arithmetical phenomena characterize the class group—has been tackled and has received a wide variety of different arithmetical characterizations (for an overview, see [17, Sections 7.1 and 7.2]). Sets of lengths are the most investigated invariant in factorization theory, and the problem of whether the system of all sets of lengths $\mathcal{L}(H) = \mathcal{L}(G)$ is characteristic for the class group G has received special attention. An affirmative answer—that is, if $\mathcal{L}(G) = \mathcal{L}(G')$, then G and G' are isomorphic—was given so far for cyclic groups, groups of the form $C_n \oplus C_n$ and others (see [28, 14, 30, 29, 33]). In this section, we use our results on $\mathcal{V}_{\{2,\mathsf{D}^*(G)\}}(G)$ to obtain some characterization results for groups of rank two (see Theorem 5.6).

To introduce the necessary concepts, let G be a finite abelian group and $S = g_1 \cdot \ldots \cdot g_l$ a sequence over G. Then

$$\mathsf{k}(S) = \sum_{i=1}^{l} \frac{1}{\operatorname{ord}(g_i)} \in \mathbb{Q} \qquad \text{resp.} \qquad \mathsf{K}(G) = \max\{\mathsf{k}(S) \mid S \in \mathcal{A}(G)\}$$

denote the *cross number* of S (resp. the *cross number* of G; for recent progress on $\mathsf{K}(G)$, see [15, 20, 21]).

Let $d, l \in \mathbb{N}$ and $M \in \mathbb{N}_0$. A subset $L \subset \mathbb{Z}$ is called an *almost arithmetical progression* (AAP for short) with *difference* d, *length* l, and *bound* M if

$$L = y + (L' \cup L^* \cup L'') \subset y + d\mathbb{Z},$$

where $y \in \mathbb{Z}$, $L^* = \{\nu d \mid \nu \in [0, l]\}$ is an arithmetical progression with difference d and length l, $L' \subset [-M, -1]$, and $L'' \subset \max L^* + [1, M]$.

We set

$$\Delta^*(G) = \{\min \Delta(G_0) \mid G_0 \subset G \text{ with } \Delta(G_0) \neq \emptyset\}$$

and let $\Delta_1(G) \subset \Delta(G)$ denote the set of all $d \in \mathbb{N}$ with the following property:

For every $k \in \mathbb{N}$, there exists some $L \in \mathcal{L}(G)$ which is an AAP with difference d and length $l \geq k$.

The sets $\Delta^*(G)$ and $\Delta_1(G)$ have been studied by Chapman, Geroldinger, Hamidoune, Plagne, Smith and others (see, for example, [18, 4, 26] and [17, Section 6.8] for some basic information).

A subset $G_0 \subset G$ is called an LCN-set if $\mathsf{k}(A) \geq 1$ for all $A \in \mathcal{A}(G_0)$. Moreover, we define

$$\mathsf{m}(G) = \max\{\min \Delta(G_0) \mid G_0 \subset G \text{ is an LCN-set with } \Delta(G_0) \neq \emptyset\},$$

using the convention that $\max \emptyset = 0$.

Lemma 5.1. *Let G be a finite abelian group with $|G| \geq 3$.*

1. $\mathsf{m}(G) \leq \max\{\mathsf{r}^*(G) - 1, \mathsf{K}(G) - 1\}$.
2. $\max \Delta^*(G) = \max\{\exp(G) - 2, \mathsf{m}(G)\}$.

Proof. For item 1, see [29, Proposition 3.6], while item 2 is a consequence of [17, Theorem 6.8.10]. □

Lemma 5.2. *Let G and G' be finite abelian groups with $|G'| \geq 3$ such that $\mathcal{L}(G) = \mathcal{L}(G')$. Then we have $\mathsf{D}(G) = \mathsf{D}(G')$, $\Delta_1(G) = \Delta_1(G')$ and $\max \Delta^*(G) = \max \Delta^*(G')$. Moreover, we have*

$$\Big\{d \in \Delta^*(G) \mid d > \frac{\max \Delta^*(G)}{2}\Big\} = \Big\{d \in \Delta^*(G') \mid d > \frac{\max \Delta^*(G')}{2}\Big\}$$

Proof. The first three statements are proved in [17, Proposition 7.3.1]. Since

$$\Delta^*(G) \subset \Delta_1(G) \subset \{d_1 \in \Delta(G) \mid d_1 \text{ divides some } d \in \Delta^*(G)\}$$

by [17, Corollary 4.3.16], the moreover statement follows from the first assertions. □

Lemma 5.3. *Let $G = C_2^s \oplus \widetilde{G}$, where $s \in \mathbb{N}_0$ and $\widetilde{G} \subset G$ is a subgroup which has no direct summand isomorphic to C_2. Then $\mathsf{d}^*(G) \geq s + 2\mathsf{r}^*(\widetilde{G})$, and equality holds if and only if G is an elementary 2-group or an elementary 3-group.*

Proof. By [22, Lemma 4.1], we have

$$\mathsf{d}^*(G) \ge \mathsf{d}^*(C_2^s) + \mathsf{d}^*(\widetilde{G}) = s + \mathsf{d}^*(\widetilde{G}) .$$

We choose a basis $(e_1, \ldots, e_t)$ of $\widetilde{G}$ with $t = \mathsf{r}^*(\widetilde{G})$ and $\operatorname{ord}(e_i) = q_i$ prime powers for all $i \in [1,t]$. Moreover, we suppose that $q_1 \le \ldots \le q_t$, and by assumption we get $2 < q_1$. Thus [17, Proposition 5.1.7] implies that

$$\mathsf{d}^*(\widetilde{G}) \ge \operatorname{ord}(e_1) + \ldots + \operatorname{ord}(e_t) - \mathsf{r}(\widetilde{G}) \ge \sum_{i=1}^{t} (q_i - 1) \ge 2t = 2\mathsf{r}^*(\widetilde{G}) .$$

Putting this all together, we obtain

$$\mathsf{d}^*(G) \ge s + 2\mathsf{r}^*(\widetilde{G}) .$$

If G is an elementary 2-group, then $\widetilde{G} = 0$ and $\mathsf{d}^*(G) = s$. If G is an elementary 3-group, then $s = 0$, $G = \widetilde{G}$ and $\mathsf{d}^*(G) = 2\mathsf{r}^*(G)$.

Now suppose that G is neither an elementary 2-group nor an elementary 3-group. Then $t \ge 1$. If $q_t \ge 4$, then the previous argument implies that

$$\mathsf{d}^*(\widetilde{G}) \ge \sum_{i=1}^{t-1} (q_i - 1) + (q_t - 1) \ge 2(t-1) + 3 = 1 + 2\mathsf{r}^*(\widetilde{G}) ,$$

and hence $\mathsf{d}^*(G) \ge s + 1 + 2\mathsf{r}^*(\widetilde{G})$.

Suppose that $q_t = 3$. Since G is not an elementary 3-group, it follows that $s \ge 1$. Therefore $r = \min\{s, t\} \ge 1$ and

$$G = C_2^s \oplus C_3^t \cong C_6^r \oplus C_2^{s-r} \oplus C_3^{t-r} .$$

We again use [22, Lemma 4.1] and infer that

$$\begin{aligned} \mathsf{d}^*(G) &\ge \mathsf{d}^*(C_6^r) + \mathsf{d}^*(C_2^{s-r}) + \mathsf{d}^*(C_3^{t-r}) \\ &= 5r + (s-r) + 2(t-r) = s + 2t + 2r \ge s + 2\mathsf{r}^*(\widetilde{G}) + 2 . \end{aligned}$$

□

It is easy to verify that $\mathcal{L}(C_1) = \mathcal{L}(C_2)$ and that $\mathcal{L}(C_3) = \mathcal{L}(C_2 \oplus C_2)$ ([17, Section 7.3]).

Proposition 5.4. *Let G and G' be finite abelian groups such that $\mathcal{L}(G) = \mathcal{L}(G')$ and suppose that $\{G, G'\} \ne \{C_1, C_2\}$ and $\{G, G'\} \ne \{C_3, C_2^2\}$. If $\min\{\mathsf{r}(G), \mathsf{r}(G')\} \le 2$, then $\exp(G) = \exp(G')$.*

Proof. If G or G' is either cyclic or an elementary 2-group, then $G \cong G'$ by [17, Theorem 7.3.3], and hence $\exp(G) = \exp(G')$. Suppose that neither G nor G' is cyclic or an elementary 2-group. We w.l.o.g. set $G' = C_m \oplus C_{mn}$ with $m \ge 2$ and $n \in \mathbb{N}$. If $m = 2$, then the assertion follows from [13, Satz 4]. If $n = 1$, then the assertion follows from [29, Theorem 4.1]. So we may suppose that $n > 1$ and $m > 2$.

Lemma 5.2 and [17, Corollary 6.8.11] imply that

$$\max \Delta^*(G) = \max \Delta^*(C_m \oplus C_{mn}) = mn - 2 \quad \text{and} \quad \mathsf{D}(G) = \mathsf{D}(C_m \oplus C_{mn}) = m + mn - 1 ,$$

and thus, by Lemma 5.1.2, we get

$$mn - 2 = \max\{\exp(G) - 2, \mathsf{m}(G)\} .$$

Assume to the contrary that $\exp(G) - 2 < \mathsf{m}(G) = mn - 2$. Then it follows from Lemma 5.1.1 that

$$\exp(G) - 1 \le mn - 2 = \mathsf{m}(G) \le \max\{\mathsf{r}^*(G) - 1, \mathsf{K}(G) - 1\} ,$$

and we distinguish two cases.

First, suppose that the maximum on the right hand side equals $\mathsf{K}(G) - 1$. Since $\mathsf{D}(G) \ge 2\mathsf{K}(G)$ (which follows trivially from the definitions involved), we get

$$m + mn - 1 = \mathsf{D}(G) \ge 2\mathsf{K}(G) \ge 2(mn - 1) ,$$

a contradiction.

Second, suppose that the maximum on the right hand side equals $\mathsf{r}^*(G) - 1$. Then

$$\exp(G) - 1 \le \mathsf{m}(G) = mn - 2 \le \mathsf{r}^*(G) - 1 . \tag{5.1}$$

We set $G = C_2^s \oplus \widetilde{G}$, where $s \in \mathbb{N}_0$ and $\widetilde{G} \subset G$ is a subgroup which has no direct summand isomorphic to C_2. Then $\mathsf{r}^*(G) = s + \mathsf{r}^*(\widetilde{G})$, and Lemma 5.3 implies that

$$mn + m - 1 = \mathsf{D}(G) \ge \mathsf{d}^*(G) + 1 \ge s + 1 + 2\mathsf{r}^*(\widetilde{G}) .$$

Therefore, using (5.1), we get

$$mn + m - 1 \ge s + 1 + 2\mathsf{r}^*(G) - 2s \ge -s + 1 + 2(mn - 1),$$

and hence $s \ge mn - m > 0$. Thus G is not an elementary 3-group. Repeating the above calculation with the sharper statement of Lemma 5.3, we get

$$mn + m - 1 \ge \mathsf d^*(G) + 1 \ge s + 2 + 2\mathsf r^*(\widetilde G) \ge s + 2 + 2\mathsf r^*(G) - 2s \ge -s + 2mn, \quad \text{and thus} \quad s \ge mn - m + 1\,.$$

Hence, using [17, Corollary 6.8.3], we obtain

$$\Delta^*(G) \supset \Delta^*(C_2^s) = [1, s-1] \supset [1, mn-m]\,. \tag{5.2}$$

Clearly, we have $\Delta^*(C_m \oplus C_{mn}) \subset \Delta^*(C_{mn} \oplus C_{mn})$. Corollaries 3.7 and 3.8 in [29] imply that

$$\max\big(\Delta^*(C_{mn} \oplus C_{mn}) \setminus \{mn-2, mn-3\}\big) = \Big\lfloor \frac{mn}{2} \Big\rfloor - 1 \tag{5.3}$$

and that (note $n > 1$ and $\mathsf m(C_m \oplus C_{mn}) \le \mathsf m(C_{mn} \oplus C_{mn}) \le \lfloor mn/2 \rfloor - 1$)

$$mn - 3 \notin \Delta^*(C_m \oplus C_{mn})\,. \tag{5.4}$$

By Lemma 5.2, we have

$$D := \Big\{ d \in \Delta^*(G) \;\big|\; d > \frac{\max \Delta^*(G)}{2} \Big\} = \Big\{ d \in \Delta^*(C_m \oplus C_{mn}) \;\big|\; d > \frac{\max \Delta^*(C_m \oplus C_{mn})}{2} \Big\}.$$

Thus, in view of $mn - m > \frac{mn-2}{2} = \frac{\max \Delta^*(G)}{2}$ and (5.2), we see that $mn - m \in D$. However, in view of $\lfloor mn/2 \rfloor - 1 \le \frac{\max \Delta^*(C_m \oplus C_{mn})}{2}$, (5.3) and (5.4), we see that the only possible element of $\Delta^*(C_m \oplus C_{mn})$ that is larger than $\lfloor mn/2 \rfloor - 1$—and thus the only possible element of $\Delta^*(C_m \oplus C_{mn})$ larger than $\frac{\max \Delta^*(C_m \oplus C_{mn})}{2}$—is $mn - 2$. As a result, $D \subset \{mn-2\}$, which combined with $mn - m \in D$ shows that $mn - m = mn - 2$, contradicting $m > 2$. ☐

There is a recent result due to Schmid ([33, Proposition 5.2]) which derives the conclusion of Proposition 5.4, namely that $\exp(G) = \exp(G')$, under a much weaker assumption. We decided to provide the proof of the special situation, because this is precisely what we need, and because the proof is simpler than that of the more general case.

Lemma 5.5. *Let $n \in \mathbb N_{\ge 2}$.*

1. *If $G = C_2^3 \oplus C_{4n}$, then $\{2, 4n, 4n+3\} \in \mathcal L(G)$.*
2. *If $G = C_4 \oplus C_{4n}$, then $\{2, 4n, 4n+3\} \notin \mathcal L(G)$.*

Proof. 1. Let $G = C_2^3 \oplus C_{4n}$ and let (e_1, e_2, e_3, e_4) be a basis of G with $\mathrm{ord}(e_1) = \mathrm{ord}(e_2) = \mathrm{ord}(e_3) = 2$ and $\mathrm{ord}(e_4) = 4n$. We set $e_0 = e_1 + \ldots + e_4$ and $U = e_1 e_2 e_3 e_4^{4n-1} e_0$. Then $U \in \mathcal A(G)$ with $|U| = 4n+3$, and we assert that $\mathsf L\big((-U)U\big) = \{2, 4n, 4n+3\}$. Clearly, we have $\{2, 4n+3\} \subset \mathsf L\big((-U)U\big)$. If $V \in \mathcal A(G)$ with $V \,|\, (-U)U$, $e_0 \in \mathrm{supp}(V)$ and $V \notin \{(-e_0)e_0, U\}$, then $V = e_0 e_1 e_2 e_3 (-e_4)$ and $(-U)U = (-V)V\big((-e_4)e_4\big)^{4n-2}$, which implies that $\mathsf L\big((-U)U\big) = \{2, 4n, 4n+3\}$.

2. Let $G = C_4 \oplus C_{4n}$ and assume to the contrary that $\{2, 4n, 4n+3\} \in \mathcal L(G)$. Since $4n + 3 = \mathsf D(G)$, there exists some $U \in \mathcal A(G)$ with $|U| = \mathsf D(G) = 4n+3$ and $\mathsf L\big((-U)U\big) = \{2, 4n, 4n+3\}$. We aim to construct a $V \in \mathcal A(G)$ of length $|V| \notin \{2, 5, 4n+3\}$ with $V \,|\, (-U)U$. Then Lemma 2.2 will imply that $2 + |U| - |V| \in \mathsf L\big((-U)U\big)$, contradicting that $\mathsf L\big((-U)U\big) = \{2, 4n, 4n+3\}$.

We will use Theorem 3.1 to describe the structure of U. If there exists a $g \in G$ with $\mathrm{ord}(g) \notin \{2, 4n\}$ and $g^{\mathrm{ord}(g)-1} \,|\, U$, then we are done by Lemma 2.2.

Therefore, if U has Type I in Theorem 3.1, then U must have the form

$$U = e_1^{4n-1} \prod_{i=1}^{4} (x_i e_1 + e_2),$$

where (e_1, e_2) is a basis of G with $\mathrm{ord}(e_2) = 4$ and $\mathrm{ord}(e_1) = 4n$, and where $x_i \in [0, 4n-1]$ with $x_1 + \ldots + x_4 \equiv 1 \mod 4n$. If $x_i \equiv x_j$ for all $i, j \in [1, 4]$, then $x_1 + \ldots + x_4 \equiv 4x_1 \not\equiv 1 \mod 4n$, a contradiction. Therefore we can w.l.o.g. assume $x_1 \not\equiv x_2 \mod 4n$. Thus $x_1 - x_2 \equiv l \mod 4n$ with $l \in [1, 4n-1]$. But then $V = (-e_1)^l (x_1 e_1 + e_2)(-x_2 e_1 - e_2) \in \mathcal A(G)$ and $V' - e_1^{4n-l}(x_1 e_1 + e_2)(-x_2 e_1 - e_2) \in \mathcal A(G)$ are both atoms dividing $U(-U)$ with length at least 3 and at most $4n - 1 + 2$. Thus we have found the desired length atom unless $l + 2 = |V| = 5 = |V'| = 4n - l + 2$, which implies $l = 2n$ and $2n + 2 = 5$, which is easily seen to be a contradiction by reducing modulo 2. So we conclude that U must instead have type II in Theorem 3.1

Thus Theorem 3.1 shows that U has the form

$$U = (e_1 + y e_2)^{4s-1} e_2^{4(n-s)+\epsilon} \prod_{i=1}^{4-\epsilon} (-x_i e_1 + (-x_i y + 1) e_2),$$

where (e_1, e_2) is a basis of G with $\mathrm{ord}(e_1) = 4$ and $\mathrm{ord}(e_2) = 4n$, where $y \in [0, 4n-1]$, $\epsilon \in [1, 3]$, $s \in [1, n-1]$, and where $x_i \in [1, 3]$ with $x_1 + \ldots + x_{4-\epsilon} = 3$. Moreover, either $s = 1$ or $4ye_2 = 4e_2$.

If $x_i = 1$ for some $i \in [1, 4-\epsilon]$, then $V = (e_1 + ye_2)(-e_2)(-e_1 + (-y+1)e_2) \in \mathcal{A}(G)$ has length $|V| = 3$ and divides $(-U)U$, as desired. Thus we may assume $x_i \geq 2$ for all $i \in [1, 4-\epsilon]$, which in view of $x_1 + \ldots + x_{4-\epsilon} = 3$ implies $\epsilon = 3$ and $x_1 = 3$. As result, we have

$$U = (e_1 + ye_2)^{4s-1} e_2^{4(n-s)+3}(-3e_1 + (-3y+1)e_2),$$

Let $4y - 1 \equiv l \mod 4n$ with $l \in [0, 4n-1]$. Note, since $4y - 1 \equiv -1 \mod 4$, that we actually have $l \in [1, 4n-1]$. Thus, if $s = 1$, then

$$e_2^{4n-l}(e_1 + ye_2)(3e_1 + (3y-1)e_2) \in \mathcal{A}(G) \quad \text{and} \quad (-e_2)^l(e_1 + ye_2)(3e_1 + (3y-1)e_2) \in \mathcal{A}(G)$$

are both atoms dividing $U(-U)$ with length at least 3 and at most $4n-1+2$, and we obtain a contradiction as we did when U had type I unless one of them has the desired length. Therefore we can assume $s \in [2, n-1]$, in which case we have

$$4ye_2 = 4e_2 \tag{5.5}$$

per part (e) in Theorem 3.1.

Suppose that $4(n-s) + 3 \geq 4s - 3$. Then (5.5) ensures that

$$V' = (e_1 + ye_2)^{4s-1}(-e_2)^{4s-3}(-3e_1 + (-3y+1)e_2) \in \mathcal{B}(G)$$

is a subsequence of $(-U)U$ of length $|V'| = 8s - 3 \notin \{2, 3, 4, 5, 4n+3\}$ (in view of $s \geq 2$). If V' is an atom, then we have found the desired length zero-sum subsequence. Otherwise, there must be an atom V dividing V' with support $\mathrm{supp}(V) = \{e_1 + ye_2, -e_2\}$. Let $k = \mathsf{v}_{e_1+ye_2}(V)$ and let $l = \mathsf{v}_{-e_2}(V)$. By considering the e_1-coordinate of $\sigma(V)$, we see that $k \equiv 0 \mod 4$. By then, considering the e_2-coordinate of $\sigma(V)$ modulo 4, we conclude that $l \equiv 0 \mod 4$. Hence, since $k, l \neq 0$, it follows that $|V| = k + l \geq 8$ with $|V| \equiv 0 \not\equiv 4n + 3 \mod 4$, and we have found the desired length zero-sum subsequence. So we may instead assume that $4(n-s) + 3 \leq 4s - 4$.

But now (5.5) ensures that

$$V' = (e_1 + ye_2)^{4n-(4s-1)}(-e_2)^{4n-(4s-3)}(3e_1 + (3y-1)e_2) \in \mathcal{B}(G)$$

is a subsequence of $(-U)U$ of length $|V'| = 8(n-s) + 5 \notin \{2, 5, 4n+3\}$ (in view of $s \in [2, n-1]$). If V' is an atom, then we have found the desired length zero-sum subsequence. Otherwise, there must be an atom V dividing V' with support $\mathrm{supp}(V) = \{e_1 + ye_2, -e_2\}$, and arguing as in the case $4(n-s) + 3 \geq 4s - 3$ shows that V has the desired length, completing the proof. □

Theorem 5.6. *Let G be a finite abelian group with $|G| \geq 4$, $m, n \in \mathbb{N}$ with $m^2 n \geq 4$, and suppose that $\mathcal{L}(G) = \mathcal{L}(C_m \oplus C_{mn})$.*

1. *If $\mathsf{d}(G) = \mathsf{d}^*(G)$, then $G \cong C_m \oplus C_{mn}$.*
2. *If mn is a power of a prime, then $G \cong C_m \oplus C_{mn}$.*

Proof. Proposition 5.4 implies that $\exp(G) = mn$. Thus, if mn is a power of a prime, then G is a p-group and hence $\mathsf{d}(G) = \mathsf{d}^*(G)$. Therefore it suffices to prove the first statement. Suppose that $\mathsf{d}(G) = \mathsf{d}^*(G)$.

If $m = 1$, then there are several proofs for the assertion (see [17, Theorem 7.3.3] or [14, Corollary 5.3.3]). If $m = 2$, then the assertion follows from [13, Satz 4]. So we may suppose that $m \geq 3$.

Since $\exp(G) = mn$, we set $G = G' \oplus C_{mn}$ for a subgroup $G' \subset G$ with $\exp(G') \,|\, mn$. We observe that $\mathsf{r}(G) = \mathsf{r}(G') + 1$ and, using Lemma 5.2, that

$$m + mn - 1 = \mathsf{D}(C_m \oplus C_{mn}) = \mathsf{D}(G) = \mathsf{d}^*(G) + 1 = \mathsf{d}^*(G') + mn.$$

If G' is cyclic, then $\mathsf{d}^*(G') = m - 1$ implies that $G' \cong C_m$, and thus $G \cong C_m \oplus C_{mn}$.

Now we suppose that G' is non-cyclic and note that $\mathsf{r}(G) = \mathsf{r}(G') + 1 \geq 3$. If $m = 3$, then

$$2 + 3n = \mathsf{D}(C_3 \oplus C_{3n}) = \mathsf{D}(G) = \mathsf{d}^*(G') + 3n\,,$$

which implies that $G' \cong C_2 \oplus C_2$ and that n is even. However, Theorem 5.3 in [33] implies that $\mathcal{L}(C_2 \oplus C_2 \oplus C_{3n}) \neq \mathcal{L}(C_3 \oplus C_{3n})$, a contradiction. Suppose that $m = 4$. Then

$$3 + 4n = \mathsf{D}(C_4 \oplus C_{4n}) = \mathsf{D}(G) = \mathsf{d}^*(G') + 4n\,,$$

which implies that G' is isomorphic to C_2^3. Now Lemma 5.5 yields a contradiction.

Suppose that $m \geq 5$. By Theorem 3.5, we have

$$3 \notin \mathcal{V}_{\{2, \mathsf{D}^*(C_m \oplus C_{mn})\}}(C_m \oplus C_{mn}) = \mathcal{V}_{\{2, \mathsf{D}(C_m \oplus C_{mn})\}}(C_m \oplus C_{mn}) = V_{\{2, \mathsf{D}(G)\}}(C_m \oplus C_{mn}),$$

and by Theorem 4.2 we have $3 \in \mathcal{V}_{\{2, \mathsf{D}^*(G)\}}(G) = \mathcal{V}_{\{2, \mathsf{D}(G)\}}(G)$, a contradiction. □

References

[1] G. Bhowmik, I. Halupczok, and J.-C. Schlage-Puchta, *The structure of maximal zero-sum free sequences*, Acta Arith. **143** (2010), 21 – 50.

[2] V. Blanco, P. A. García-Sánchez, and A. Geroldinger, *Semigroup-theoretical characterizations of arithmetical invariants with applications to numerical monoids and Krull monoids*, Ill. J. Math.

[3] Gyu-Whan Chang, *Every divisor class of Krull monoid domains contains a prime ideal*, J. Algebra **336** (2011), 370 – 377.

[4] S.T. Chapman, W.A. Schmid, and W.W. Smith, *On minimal distances in Krull monoids with infinite class group*, Bull. Lond. Math. Soc. **40** (2008), 613 – 618.

[5] S.T. Chapman and W.W. Smith, *Generalized sets of lengths*, J. Algebra **200** (1998), 449 – 471.

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

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

[8] W. Gao and A. Geroldinger, *On the order of elements in long minimal zero-sum sequences*, Period. Math. Hung. **44** (2002), 63 – 73.

[9] ______, *On zero-sum sequences in* $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, Integers **3** (2003), Paper A08, 45p.

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

[11] ______, *On products of* k *atoms*, Monatsh. Math. **156** (2009), 141 – 157.

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

[13] A. Geroldinger, *Systeme von Längenmengen*, Abh. Math. Semin. Univ. Hamb. **60** (1990), 115 – 130.

[14] ______, *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, pp. 1 – 86.

[15] A. Geroldinger and D.J. Grynkiewicz, *On the structure of minimal zero-sum sequences with maximal cross number*, J. Combinatorics and Number Theory **1 (2)** (2009), 9 – 26.

[16] A. Geroldinger, D.J. Grynkiewicz, and P. Yuan, *On products of* k *atoms II*, manuscript.

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

[18] A. Geroldinger and Y. ould Hamidoune, *Zero-sumfree sequences in cyclic groups and some arithmetical application*, J. Théor. Nombres Bordx. **14** (2002), 221 – 239.

[19] A. Geroldinger, M. Liebmann, and A. Philipp, *On the Davenport constant and on the structure of extremal sequences*, Period. Math. Hung.

[20] B. Girard, *A new upper bound for the cross number of finite abelian groups*, Isr. J. Math. **172** (2009), 253 – 278.

[21] ______, *Inverse zero-sum problems in finite abelian p-groups*, Colloq. Math. **120** (2010), 7 – 21.

[22] D.J. Grynkiewicz, L.E. Marchan, and O. Ordaz, *Representation of finite abelian group elements by subsequence sums*, J. Théor. Nombres Bordx. **21** (2009), 559 – 587.

[23] F. Halter-Koch, *Ideal Systems. An Introduction to Multiplicative Ideal Theory*, Marcel Dekker, 1998.

[24] H. Kim, *The distribution of prime divisors in Krull monoid domains*, J. Pure Appl. Algebra **155** (2001), 203 – 210.

[25] H. Kim and Y. S. Park, *Krull domains of generalized power series*, J. Algebra **237** (2001), 292 – 301.

[26] A. Plagne and W.A. Schmid, *On congruence half-factorial Dedekind domains with cyclic class group*, manuscript.

[27] C. Reiher, *A proof of the theorem according to which every prime number possesses property B*, J. Lond. Math. Soc., to appear.

[28] W.A. Schmid, *Differences in sets of lengths of Krull monoids with finite class group*, J. Théor. Nombres Bordx. **17** (2005), 323 – 345.

[29] ______, *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.

[30] ______, *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.

[31] ______, *A realization theorem for sets of lengths*, J. Number Theory **129** (2009), 990 – 999.

[32] ______, *Inverse zero-sum problems II*, Acta Arith. **143** (2010), 333 – 343.

[33] ______, *The inverse problem associated to the Davenport constant for* $C_2 \oplus C_2 \oplus C_{2n}$, *and applications to the arithmetical characterization of class groups*, Electron. J. Comb. **18(1)** (2011), Research Paper 33.

[34] D. Smertnig, *On the Davenport constant and group algebras*, Colloq. Math. **121** (2010), 179 – 193.

Department of Mathematics and Statistics, Smith College, Northampton, MA 01063, USA
E-mail address: baginski@gmail.com

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