ACTA ARITHMETICA
Online First version

The set of minimal distances in Krull monoids

by

Alfred Geroldinger and Qinghai Zhong (Graz)

1. Introduction. Let H be a Krull monoid with class group G (we have in mind holomorphy rings in global fields and give more examples later). Then every nonunit of H has a factorization as a finite product of atoms (or irreducible elements), and all these factorizations are unique (i.e., H is factorial) if and only if G is trivial. Otherwise, there are elements having factorizations which differ not only up to associates and up to the order of the factors. These phenomena are described by arithmetical invariants such as sets of lengths and sets of distances. We first recall some concepts and then we formulate a main result of the present paper.

For a finite nonempty set $L = \{m_1, \ldots, m_k\}$ of positive integers with $m_1 < \cdots < m_k$, we denote by $\Delta(L) = \{m_i - m_{i-1} \mid i \in [2,k]\}$ the set of distances of L. Thus $\Delta(L) = \emptyset$ if and only if $|L| \le 1$. If a nonunit $a \in H$ has a factorization $a = u_1 \cdot \ldots \cdot u_k$ into atoms $u_1, \ldots, u_k$, then k is called the *length* of the factorization, and the set $\mathsf{L}_H(a) = \mathsf{L}(a)$ of all possible k is called the *set of lengths* of a. If there is an element $a \in H$ with $|\mathsf{L}(a)| > 1$, then it immediately follows that $|\mathsf{L}(a^n)| > n$ for every $n \in \mathbb{N}$. Since H is Krull, every nonunit has a factorization into atoms and all sets of lengths are finite. The set of distances $\Delta(H)$ is the union of all sets $\Delta(\mathsf{L}(a))$ over all nonunits $a \in H$. Thus, by definition, $\Delta(H) = \emptyset$ if and only if $|\mathsf{L}(a)| = 1$ for all nonunits $a \in H$, and $\Delta(H) = \{d\}$ if and only if $\mathsf{L}(a)$ is an arithmetical progression with difference d for all nonunits $a \in H$. The *set of minimal distances* $\Delta^*(H)$ is defined as

$$\Delta^*(H) = \{\min \Delta(S) \mid S \subset H \text{ is a divisor-closed submonoid with } \Delta(S) \ne \emptyset\}.$$

By definition, we have $\Delta^*(H) \subset \Delta(H)$, and $\Delta^*(H) = \emptyset$ if and only if $\Delta(H) = \emptyset$. If the class group G is finite, then $\Delta(H)$ is finite and sets of

2010 *Mathematics Subject Classification*: 11B30, 11R27, 13A05, 20M13.
Key words and phrases: nonunique factorizations, sets of distances, Krull monoids, zero-sum sequences, cross numbers.
Received 25 August 2014; revised 25 February 2016.
Published online *.

 © Instytut Matematyczny PAN, 2016

lengths have a well-defined structure which is given in the next theorem [13, Chapter 4.7].

THEOREM A. *Let H be a Krull monoid with finite class group. Then there is a constant $M \in \mathbb{N}$ such that the set of lengths $\mathsf{L}(a)$ of any nonunit $a \in H$ is an* AAMP (*almost arithmetical multiprogression*) *with difference $d \in \Delta^*(H)$ and bound M.*

The structural description given above is best possible [32]. The set of minimal distances $\Delta^*(H)$ has been studied by Chapman, Geroldinger, Halter-Koch, Hamidoune, Plagne, Smith, Schmid and others, and there are a variety of results. We refer the reader to the monograph [13, Chapter 6.8] for an overview and mention some results which have appeared since then. Suppose that G is finite and that every class contains a prime divisor. Then the set of distances $\Delta(H)$ is an interval [18]. A simple example shows that the interval $[1, \mathsf{r}(G) - 1]$ is contained in $\Delta^*(H)$ (Lemma 2.3) and thus, by Theorem 1.1 below, $\Delta^*(H)$ is an interval too if $\mathsf{r}(G) \ge \exp(G) - 1$. Cyclic groups stand in sharp contrast to this. Indeed, if G is cyclic with $|G| > 3$, then $\max(\Delta^*(H) \setminus \{|G| - 2\}) = \lfloor |G|/2 \rfloor - 1$ (see [14]). A detailed study of the structure of $\Delta^*(H)$ for cyclic groups is given in a recent paper by Plagne and Schmid [23].

The goal of the present paper is to study the maximum of $\Delta^*(H)$, and here is the main direct result.

THEOREM 1.1. *Let H be a Krull monoid with class group G.*

(1) *If $|G| \le 2$, then $\Delta^*(H) = \emptyset$.*
(2) *If $2 < |G| < \infty$, then*

$$\max \Delta^*(H) \le \max\{\exp(G) - 2, \mathsf{r}(G) - 1\}$$

where $\mathsf{r}(G)$ denotes the rank of G.

(3) *Suppose that every class contains a prime divisor. If G is infinite, then $\Delta^*(H) = \mathbb{N}$, while if $2 < |G| < \infty$, then*

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

Theorem 1.1 will be complemented by an associated inverse result (Theorem 4.5) describing how $\max \Delta^*(H)$ is attained and disproving a former conjecture (Remark 4.6). Both the direct and the inverse result have number-theoretic relevance beyond the occurrence in Theorem A. Indeed, they are key tools in the characterization of those Krull monoids whose systems of sets of lengths are closed under set addition [17], in the study of arithmetical characterizations of class groups via sets of lengths [13, Chapter 7.3], [31, 16], as well as in the asymptotic study of counting functions associated to periods of sets of lengths [30], [13, Theorem 9.4.10].

In Section 2 we gather the required background from the theory of Krull monoids and from additive combinatorics. In particular, we indicate that the set of minimal distances of H equals the set of minimal distances of an associated monoid of zero-sum sequences (Lemma 2.1), and therefore it can be studied with methods from additive combinatorics. The proof of Theorem 1.1 will be given in Section 3 and the associated inverse result will be given in Section 4.

2. Background on Krull monoids and on additive combinatorics. We denote by $\mathbb{N}$ the set of positive integers, and, for $a, b \in \mathbb{Z}$, we denote by $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$ the discrete, finite interval between a and b. We use the convention that $\max \emptyset = 0$. By a *monoid*, we mean a commutative semigroup with identity that satisfies the cancellation laws. If H is a monoid, then $H^\times$ denotes the unit group, $\mathsf{q}(H)$ the quotient group, and $\mathcal{A}(H)$ the set of atoms (or irreducible elements) of H. A submonoid $S \subset H$ is called *divisor-closed* if $a \in S$, $b \in H$, and b divides a imply that $b \in S$. A monoid H is said to be

- *atomic* if every nonunit can be written as a finite product of atoms;
- *factorial* if it is atomic and every atom is prime;
- *half-factorial* if it is atomic and $|\mathsf{L}(a)| = 1$ for each nonunit $a \in H$ (equivalently, $\Delta(H) = \emptyset$);
- *decomposable* if there exist submonoids H_1, H_2 with $H_i \not\subset H^\times$ for $i \in [1, 2]$ such that $H = H_1 \times H_2$ (and H is called *indecomposable* otherwise).

A monoid F is factorial with $F^\times = \{1\}$ if and only if it is free abelian. If this holds, then the set of primes $P \subset F$ is a basis of F, we write $F = \mathcal{F}(P)$, and every $a \in F$ has a representation of the form

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

A monoid homomorphism $\theta \colon H \to B$ is called a *transfer homomorphism* if it has the following properties:

(T1) $B = \theta(H) B^\times$ and $\theta^{-1}(B^\times) = H^\times$.
(T2) If $u \in H$, $b, c \in B$ and $\theta(u) = bc$, then there exist $v, w \in H$ such that $u = vw$, $\theta(v) \simeq b$ and $\theta(w) \simeq c$.

If H and B are atomic monoids and $\theta \colon H \to B$ is a transfer homomorphism, then (see [13, Chapter 3.2])

$$\mathsf{L}_H(a) = \mathsf{L}_B(\theta(a)) \quad \text{for all } a \in H, \quad \Delta(H) = \Delta(B), \quad \Delta^*(H) = \Delta^*(B).$$

Krull monoids. A monoid H is said to be a *Krull monoid* if it satisfies the following two conditions:

(a) There exists a monoid homomorphism $\varphi\colon H \to F = \mathcal{F}(P)$ into a free abelian monoid F such that $a \mid b$ in H if and only if $\varphi(a) \mid \varphi(b)$ in F.
(b) For every $p \in P$, there exists a finite subset $E \subset H$ such that $p = \gcd(\varphi(E))$.

Let H be a Krull monoid and $\varphi\colon H \to \mathcal{F}(P)$ a homomorphism satisfying properties (a) and (b). Then φ is called a *divisor theory* of H,

$$G = \mathsf{q}(F)/\mathsf{q}(\varphi(H))$$

is the *class group*, and

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

the *set of classes containing prime divisors*. The class group will be written additively, and the tuple (G, G_P) is uniquely determined by H. To provide some examples of Krull monoids, we recall that a domain is a Krull domain if and only if its multiplicative monoid of nonzero elements is a Krull monoid, and that a noetherian domain is Krull if and only if it is integrally closed. Rings of integers, holomorphy rings in algebraic function fields, and regular congruence monoids in these domains are Krull monoids with finite class group such that every class contains a prime divisor [12], [13, Chapter 2.11]. For monoids of modules and monoid domains which are Krull we refer to [22, 4, 3, 1].

Next we introduce Krull monoids having a combinatorial flavor which are used to model arbitrary Krull monoids. Let G be an additively written abelian group and $G_0 \subset G$ a subset. An element $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G_0)$ is called a *sequence* over G_0, $\sigma(S) = g_1 + \cdots + g_l$ is called its *sum*, $|S| = l$ its *length*, and $\mathsf{h}(S) = \max\{\mathsf{v}_g(S) \mid g \in \operatorname{supp}(S)\}$ the *maximal multiplicity* of S. The monoid

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

is a Krull monoid, called the *monoid of zero-sum sequences* over G_0. Its significance for the study of general Krull monoids is summarized in the following lemma (see [13, Theorem 3.4.10 and Proposition 4.3.13]).

LEMMA 2.1. *Let H be a Krull monoid, $\varphi\colon H \to D = \mathcal{F}(P)$ a divisor theory with class group G, and $G_P \subset G$ the set of classes containing prime divisors. Let $\widetilde{\boldsymbol{\beta}}\colon D \to \mathcal{F}(G_P)$ denote the unique homomorphism defined by $\widetilde{\boldsymbol{\beta}}(p) = [p]$ for all $p \in P$. Then the homomorphism $\boldsymbol{\beta} = \widetilde{\boldsymbol{\beta}} \circ \varphi\colon H \to \mathcal{B}(G_P)$ is a transfer homomorphism. In particular,*

$$\Delta^*(H) = \Delta^*\big(\mathcal{B}(G_P)\big) = \{\min \Delta(\mathcal{B}(G_0)) \mid G_0 \subset G_P \text{ is a subset such that } \mathcal{B}(G_0) \text{ is not half-factorial}\}.$$

Thus $\Delta^*(H)$ can be studied in an associated monoid of zero-sum sequences and can thus be tackled by methods of additive combinatorics. Such transfer results to monoids of zero-sum sequences are not restricted to Krull monoids, but they also exist for certain seminormal weakly Krull monoids and certain maximal orders in central simple algebras over global fields. We do not dwell on this here but refer to [33, Theorem 1.1], [15], and [2, Section 7].

Zero-sum theory is a subfield of additive combinatorics (see the monograph [20], the survey [10], and for a sample of recent papers on direct and inverse zero-sum problems with a strong number-theoretic flavor see [19, 8, 21, 34, 9]). We gather together the concepts needed in what follows.

Let G be a finite abelian group and $G_0 \subset G$ a subset. Then $\langle G_0 \rangle \subset G$ denotes the subgroup generated by G_0. A family $(e_i)_{i\in I}$ of elements of G is said to be *independent* if $e_i \neq 0$ for all $i \in I$ and, for every family $(m_i)_{i\in I} \in \mathbb{Z}^{(I)}$,

$$\sum_{i\in I} m_i e_i = 0 \quad \text{implies} \quad m_i e_i = 0 \text{ for all } i \in I.$$

A family $(e_i)_{i\in I}$ is called a *basis* for G if $e_i \neq 0$ for all $i \in I$ and $G = \bigoplus_{i\in I} \langle e_i \rangle$. The set G_0 is said to be independent if the tuple $(g)_{g\in G_0}$ is independent. If for a prime $p \in \mathbb{P}$, $\mathsf{r}_p(G)$ is the p-rank of G, then

$$\mathsf{r}(G) = \max\{\mathsf{r}_p(G) \mid p \in \mathbb{P}\} \text{ is the } \textit{rank} \text{ of } G, \text{ and}$$
$$\mathsf{r}^*(G) = \sum_{p\in\mathbb{P}} \mathsf{r}_p(G) \text{ is the } \textit{total rank} \text{ of } G.$$

The monoid $\mathcal{B}(G_0)$ of zero-sum sequences over G_0 is a finitely generated Krull monoid. It is traditional to set

$$\mathcal{A}(G_0) := \mathcal{A}(\mathcal{B}(G_0)), \quad \Delta(G_0) := \Delta(\mathcal{B}(G_0)), \quad \Delta^*(G_0) := \Delta^*(\mathcal{B}(G_0)).$$

Clearly, the atoms of $\mathcal{B}(G_0)$ are precisely the minimal zero-sum sequences over G_0. The set $\mathcal{A}(G_0)$ is finite, and $\mathsf{D}(G_0) = \max\{|S| \mid S \in \mathcal{A}(G_0)\}$ is the *Davenport constant* of G_0. The set G_0 is called

- *half-factorial* if the monoid $\mathcal{B}(G_0)$ is half-factorial (equivalently, $\Delta(G_0) = \emptyset$);
- *non-half-factorial* if the monoid $\mathcal{B}(G_0)$ is not half-factorial (equivalently, $\Delta(G_0) \neq \emptyset$);
- *minimal non-half-factorial* if $\Delta(G_0) \neq \emptyset$ but every proper subset is half-factorial;
- *(in)decomposable* if the monoid $\mathcal{B}(G_0)$ is (in)decomposable.

If G_0 is not half-factorial, then $\min \Delta(G_0) = \gcd \Delta(G_0)$ [13, Proposition 1.4.4]. (Maximal) half-factorial and (minimal) non-half-factorial subsets have found a lot of attention in the literature (see [11, 28, 24, 25, 29, 5, 6]), and cross numbers are a crucial tool for their study. For a sequence $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G_0)$, we call

$$\mathsf{k}(S) = \sum_{i=1}^{l} \frac{1}{\operatorname{ord}(g_i)} \in \mathbb{Q}_{\ge 0} \quad \text{the } \textit{cross number} \text{ of } S, \text{ and}$$

$$\mathsf{K}(G_0) = \max\{\mathsf{k}(S) \mid S \in \mathcal{A}(G_0)\} \quad \text{the } \textit{cross number} \text{ of } G_0.$$

The following simple result [13, Proposition 6.7.3] will be used throughout the paper without further mention.

LEMMA 2.2. *Let G be a finite abelian group and $G_0 \subset G$ a subset. Then the following statements are equivalent:*

(a) *G_0 is half-factorial.*
(b) *$\mathsf{k}(U) = 1$ for every $U \in \mathcal{A}(G_0)$.*
(c) *$\mathsf{L}(B) = \{\mathsf{k}(B)\}$ for every $B \in \mathcal{B}(G_0)$.*

In the remainder of this section we gather some simple, partly well-known results on the set of minimal distances. A proof of the next lemma can be found in [13, Chapter 6.8], but for better readability we provide the short argument here.

LEMMA 2.3. *Let G be a finite abelian group with $|G| > 2$.*

(1) *If $g \in G$ with $\operatorname{ord}(g) > 2$, then $\operatorname{ord}(g) - 2 \in \Delta^*(G)$. In particular, $\exp(G) - 2 \in \Delta^*(G)$.*
(2) *If $\mathsf{r}(G) \ge 2$, then $[1, \mathsf{r}(G) - 1] \subset \Delta^*(G)$.*
(3) *Let $G_0 \subset G$ be a subset.*
   (a) *If there exists $U \in \mathcal{A}(G_0)$ with $\mathsf{k}(U) < 1$, then $\min \Delta(G_0) \le \exp(G) - 2$.*
   (b) *If $\mathsf{k}(U) \ge 1$ for all $U \in \mathcal{A}(G_0)$, then $\min \Delta(G_0) \le |G_0| - 2$.*

Proof. (1) Let $g \in G$ with $\operatorname{ord}(g) = n > 2$ and set $G_0 = \{g, -g\}$. Then $\mathcal{A}(G_0) = \{g^n, (-g)^n, (-g)g\}$, $\Delta(G_0) = \{n-2\}$, and hence $\min \Delta(G_0) = n - 2$.

(2) Let $s \in [2, \mathsf{r}(G)]$. Then there is a prime $p \in \mathbb{P}$ such that C_p^s is isomorphic to a subgroup of G, and it suffices to show that $s - 1 \in \Delta^*(C_p^s)$. Let $(e_1, \ldots, e_s)$ be a basis of C_p^s and set $e_0 = e_1 + \cdots + e_s$ and $G_0 = \{e_0, \ldots, e_s\}$. Then a simple calculation (details can be found in [13, Proposition 6.8.1]) shows that $\Delta(G_0) = \{s - 1\}$ and hence $\min \Delta(G_0) = s - 1$.

(3)(a) Let $U = g_1 \cdot \ldots \cdot g_l \in \mathcal{A}(G_0)$ with $\mathsf{k}(U) < 1$ and $n = \exp(G)$ (note that $\mathsf{k}(U) < 1$ implies $U \ne 0$, $l \ge 2$ and $\mathsf{k}(U) > 1/n$). Then $U_i = g_i^{\operatorname{ord}(g_i)} \in \mathcal{A}(G_0)$ for all $i \in [1, l]$, and

$$U^n = \prod_{i=1}^{l} U_i^{n/\operatorname{ord}(g_i)}$$

implies that $n\mathsf{k}(U) = \sum_{i=1}^{l} n/\mathrm{ord}(g_i) \in \mathsf{L}(U^n)$. Since $\mathsf{k}(U) < 1$, we have $n\mathsf{k}(U) \in [2, n-1]$ and $\min \Delta(G_0) \le n - n\mathsf{k}(U) \in [1, n-2]$.

(3)(b) The proof is similar to that of (3)(a)—see [13, Lemma 6.8.6] for details. ■

Lemma 2.3(3) motivates the following definitions (see [30, 31]). A subset $G_0 \subset G$ is called an LCN-*set* (*large cross number set*) if $\mathsf{k}(U) \ge 1$ for each $U \in \mathcal{A}(G_0)$ and

$$\mathsf{m}(G) = \max\{\min \Delta(G_0) \mid G_0 \subset G \text{ is a non-half-factorial LCN-set}\}.$$

Clearly, if G has a non-half-factorial LCN-set, then $|G| \ge 4$. The following result (due to Schmid [31]) is crucial for our approach.

PROPOSITION 2.4. *Let G be a finite abelian group with $|G| > 2$. Then*

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

If G is a p-group, then $\mathsf{m}(G) = \mathsf{r}(G) - 1$, and thus

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

Proof. See [31, Theorem 3.1, Lemma 3.3(4), and Proposition 3.6]. ■

LEMMA 2.5. *Let G be a finite abelian group and $G_0 \subset G$ a subset.*

(1) *The following statements are equivalent*:
   - (a) *G_0 is decomposable.*
   - (b) *There are nonempty subsets $G_1, G_2 \subset G_0$ such that $G_0 = G_1 \uplus G_2$ and $\mathcal{B}(G_0) = \mathcal{B}(G_1) \times \mathcal{B}(G_2)$.*
   - (c) *There are nonempty $G_1, G_2 \subset G_0$ such that $G_0 = G_1 \uplus G_2$ and $\mathcal{A}(G_0) = \mathcal{A}(G_1) \uplus \mathcal{A}(G_2)$.*
   - (d) *There are nonempty $G_1, G_2 \subset G_0$ such that $\langle G_0 \rangle = \langle G_1 \rangle \oplus \langle G_2 \rangle$.*

(2) *If G_0 is minimal non-half-factorial, then G_0 is indecomposable.*

Proof. (1) See [26, Lemma 3.7] and [1, Lemma 3.2].

(2) This follows immediately from (1)(b). ■

We will use the following simple fact throughout. For every subset G_0 in G and every $g \in G_0$, we have

$$\begin{aligned} (2.1) \quad & \gcd(\{\mathsf{v}_g(B) \mid B \in \mathcal{B}(G_0)\}) = \gcd(\{\mathsf{v}_g(A) \mid A \in \mathcal{A}(G_0)\}) \\ & = \min(\{\mathsf{v}_g(A) \mid \mathsf{v}_g(A) > 0,\ A \in \mathcal{A}(G_0)\}) \\ & = \min(\{\mathsf{v}_g(B) \mid \mathsf{v}_g(B) > 0,\ B \in \mathcal{B}(G_0)\}) \\ & = \min(\{k \in \mathbb{N} \mid kg \in \langle G_0 \setminus \{g\} \rangle\}) = \gcd(\{k \in \mathbb{N} \mid kg \in \langle G_0 \setminus \{g\} \rangle\}). \end{aligned}$$

In particular, $\min(\{k \in \mathbb{N} \mid kg \in \langle G_0 \setminus \{g\} \rangle\})$ divides $\mathrm{ord}(g)$.

LEMMA 2.6. *Let G be a finite abelian group and $G_0 \subset G$ a subset.*

(1) *Suppose that for any distinct $h, h' \in G_0$ we have $h \notin \langle G_0 \setminus \{h, h'\}\rangle$. Then for any atom A with $\mathrm{supp}(A) \subsetneq G_0$ and any $h \in \mathrm{supp}(A)$, we have $\gcd(\mathsf{v}_h(A), \mathrm{ord}(h)) > 1$.*
(2) *If G_0 is minimal non-half-factorial, then there exists a minimal non-half-factorial subset $G_0^* \subset G$ with $|G_0| = |G_0^*|$ and a transfer homomorphism $\theta \colon \mathcal{B}(G_0) \to \mathcal{B}(G_0^*)$ such that:*
   (a) *For each $g \in G_0^*$, we have $g \in \langle G_0^* \setminus \{g\}\rangle$.*
   (b) *For each $B \in \mathcal{B}(G_0)$, we have $\mathsf{k}(B) = \mathsf{k}(\theta(B))$.*
   (c) *If G_0^* has the property that for each $h \in G_0^*$, $h \notin \langle E\rangle$ for any $E \subsetneq G_0^* \setminus \{h\}$, then G_0 also has this property.*
   (d) *If G_0^* has the property that there exists $h \in G_0^*$ such that $G_0^* \setminus \{h\}$ is independent, then G_0 also has this property.*

Proof. (1) Assume to the contrary that there are A and h as above such that $\gcd(\mathsf{v}_h(A), \mathrm{ord}(h)) = 1$. Choose $h' \in G_0 \setminus \mathrm{supp}(A)$; then $h \in \langle \mathrm{supp}(A) \setminus \{h\}\rangle \subset \langle G_0 \setminus \{h, h'\}\rangle$, a contradiction.

(2) By [13, Theorem 6.7.11], there are a subset $G_0^* \subset G$ satisfying property (a) and a transfer homomorphism $\theta \colon \mathcal{B}(G_0) \to \mathcal{B}(G_0^*)$. Moreover, θ is a composition of transfer homomorphisms θ' of the following form:

- Let $g \in G_0$, $m = \min\{k \in \mathbb{N} \mid kg \in \langle G_0 \setminus \{g\}\rangle\}$, $G_0' = G_0 \setminus (\{g\} \cup \{mg\})$, and define
$$\theta' \colon \mathcal{B}(G_0) \to \mathcal{B}(G_0'), \quad \theta'(B) = g^{-\mathsf{v}_g(B)} (mg)^{\mathsf{v}_g(B)/m} B,$$
It is shown in [13] that $m \mid \mathsf{v}_g(B)$ and $m \mid \mathrm{ord}(g)$.

Therefore it is sufficient to show that $|G_0| = |G_0'|$ and that θ' satisfies properties (b)–(d).

(i) By definition, we have $\mathsf{k}(B) = \mathsf{k}(\theta'(B))$ for all $B \in \mathcal{B}(G_0)$.

(ii) Since G_0 is a minimal non-half-factorial set, the same is true for G_0' by [13, Lemma 6.8.9]. If $mg \in G_0 \setminus \{g\}$, then $G_0' \subsetneq G_0$ would be non-half-factorial, contrary to the minimality of G_0. Hence $mg \notin G_0 \setminus \{g\}$, which implies that $|G_0'| = |G_0|$.

(iii) We set $G_0 = \{g = g_1, \ldots, g_k\}$ (note that $k \ge 2$), $G_0' = \{mg, g_2, \ldots, g_k\}$, and suppose that $h \notin \langle E\rangle$ for each $h \in G_0'$ and for any $E \subsetneq G_0' \setminus \{h\}$. Assume to the contrary that there exist $h \in G_0$ and $E \subsetneq G_0 \setminus \{h\}$ such that $h \in \langle E\rangle$. If $h = g$, then $mg \in \langle E\rangle$, a contradiction.

Suppose that $h \ne g$, say $h = g_k \in \langle E\rangle$ with $E \subsetneq \{g, g_2, \ldots, g_{k-1}\}$. If $g \notin E$, then $E \subsetneq G_0' \setminus \{mg\}$, a contradiction. Thus $g \in E$, and we set $E' = E \setminus \{g\} \cup \{mg\}$. Since $h \in \langle E\rangle$, we have $h = \sum_{x \in E \setminus \{g\}} t_x x + tg$ where $t_x, t \in \mathbb{Z}$. Thus $tg = h - \sum_{x \in E \setminus \{g\}} t_x x \in \langle E \cup \{h\} \setminus \{g\}\rangle \subset \langle G_0 \setminus \{g\}\rangle$.

By (2.1), we deduce that $m \mid t$ and hence $h = \sum_{x \in E \setminus \{g\}} t_x x + \frac{t}{m} mg \in \langle E' \rangle$, a contradiction.

(iv) We set $G_0 = \{g = g_1, \ldots, g_k\}$, $G_0' = \{mg, g_2, \ldots, g_k\}$, and suppose that there exists $h \in G_0'$ such that $G_0' \setminus \{h\}$ is independent. If $h = mg$, then $G_0 \setminus \{g\} = G_0' \setminus \{h\}$ is independent. Suppose that $h \neq mg$, say $h = g_k$. Then $\{mg, g_2, \ldots, g_{k-1}\}$ is independent and assume to the contrary that $G_0 \setminus \{h\} = \{g, g_2, \ldots, g_{k-1}\}$ is not independent. Then there exist $t_1, \ldots, t_{k-1} \in \mathbb{Z}$ such that $t_1 g + t_2 g_2 + \cdots + t_{k-1} g_{k-1} = 0$ but $t_i g_i \neq 0$ for at least one $i \in [1, k-1]$. This implies that $t_1 g \in \langle g_2, \ldots, g_{k-1} \rangle \subset \langle G_0 \setminus \{g\} \rangle$. By (1), we infer that $m \mid t_1$ and hence $\frac{t_1}{m} mg + t_2 g_2 + \cdots + t_{k-1} g_{k-1} = 0$, contrary to $\{mg, g_2, \ldots, g_{k-1}\}$ being independent. ∎

3. Direct results on $\Delta^*(H)$

LEMMA 3.1. *Let G be a finite abelian group and $G_0 \subset G$ a subset with $|G_0| \geq \mathsf{r}(G) + 2$ such that:*

(a) *For each $h \in G_0$, $G_0 \setminus \{h\}$ is half-factorial and $h \notin \langle G_0 \setminus \{h, h'\} \rangle$ for any $h' \in G_0 \setminus \{h\}$.*
(b) *There exists $g \in G_0$ such that $g \in \langle G_0 \setminus \{g\} \rangle$ and $\operatorname{ord}(g)$ is not a prime power.*

Then $|G_0| \leq \exp(G) - 2$.

Proof. We set $\exp(G) = n = p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$, where $t \geq 2$, $k_1, \ldots, k_t \in \mathbb{N}$ and $p_1, \ldots, p_t$ are distinct primes. By Lemma 2.6(1), we know that for any atom A with $\operatorname{supp}(A) \subsetneq G_0$ and any $h \in \operatorname{supp}(A)$, we have $\gcd(\mathsf{v}_h(A), \operatorname{ord}(h)) > 1$. In particular,

$$\mathsf{v}_h(A) \geq 2 \quad \text{for each } h \in \operatorname{supp}(A). \tag{3.1}$$

We assert the following:

A. *For each $\nu \in [1, t]$ with $p_\nu \mid \operatorname{ord}(g)$, there is an atom $U_\nu \in \mathcal{A}(G_0)$ such that $\mathsf{v}_g(U_\nu) \mid n/p_\nu^{k_\nu}$, $\mathsf{k}(U_\nu) = 1$, $\operatorname{supp}(U_\nu) \subsetneq G_0$, and*

$$|\operatorname{supp}(U_\nu) \setminus \{g\}| \leq (n - \mathsf{v}_g(U_\nu))/2.$$

Proof of **A**. Let $\nu \in [1, t]$ with $p_\nu \mid \operatorname{ord}(g)$. Since $g \in \langle G_0 \setminus \{g\} \rangle$ and $t \geq 2$, it follows that $0 \neq (n/p_\nu^{k_\nu}) g \in G_\nu = \langle (n/p_\nu^{k_\nu}) h \mid h \in G_0 \setminus \{g\} \rangle$. Obviously, G_ν is a p_ν-group. Let $E_\nu \subset G_0 \setminus \{g\}$ be minimal such that $(n/p_\nu^{k_\nu}) g \in \langle (n/p_\nu^{k_\nu}) E_\nu \rangle$. The minimality implies that $|E_\nu| = |(n/p_\nu^{k_\nu}) E_\nu|$ and $(n/p_\nu^{k_\nu}) E_\nu$ is a minimal generating set of $G_\nu' := \langle (n/p_\nu^{k_\nu}) E_\nu \rangle$. Thus [13, Lemma A.6.2] implies that $|(n/p_\nu^{k_\nu}) E_\nu| \leq \mathsf{r}^*(G_\nu')$. Putting all together we obtain

$$|E_\nu| = \left| \frac{n}{p_\nu^{k_\nu}} E_\nu \right| \leq \mathsf{r}^*(G_\nu') = \mathsf{r}(G_\nu') \leq \mathsf{r}(G).$$

Let $d_\nu \in \mathbb{N}$ be minimal such that $d_\nu g \in \langle E_\nu \rangle$. By (2.1), $d_\nu \mid n/p_\nu^{k_\nu}$ and there exists an atom U_ν such that $\mathsf{v}_g(U_\nu) = d_\nu$ and $|\mathrm{supp}(U_\nu)| \le |E_\nu| + 1 \le \mathsf{r}(G) + 1 \le |G_0| - 1$, whence $\mathrm{supp}(U_\nu) \subsetneq G_0$. Thus property (a) implies that $\mathsf{k}(U_\nu) = 1$. Let

$$U_\nu = g^{\mathsf{v}_g(U_\nu)} \prod_{h \in \mathrm{supp}(U_\nu) \setminus \{g\}} h^{\mathsf{v}_h(U_\nu)}.$$

Since $\mathsf{v}_h(U_\nu) \ge 2$ for each $h \in \mathrm{supp}(U_\nu) \setminus \{g\}$ by (3.1), it follows that

$$1 = \mathsf{k}(U_\nu) \ge \frac{\mathsf{v}_g(U_\nu)}{n} + |\mathrm{supp}(U_\nu) \setminus \{g\}| \frac{2}{n},$$

whence $|\mathrm{supp}(U_\nu) \setminus \{g\}| \le (n - \mathsf{v}_g(U_\nu))/2$. ■Proof of **A**

Let $s \in \mathbb{N}$ be minimal such that there exists a nonempty subset $E \subsetneq G_0 \setminus \{g\}$ with $sg \in \langle E \rangle$; suppose E is a minimal such set. By (2.1), there is an atom V with $\mathsf{v}_g(V) = s$ and $\mathrm{supp}(V) = \{g\} \cup E \subsetneq G_0$. Then

$$1 = \mathsf{k}(V) = \frac{s}{\mathrm{ord}(g)} + \sum_{h \in E} \frac{\mathsf{v}_h(V)}{\mathrm{ord}(h)}.$$

By (3.1), we have $\mathsf{v}_h(V) \ge 2$ for each $h \in E$, and hence the equation above implies that $|E| \le (n-s)/2$.

Case 1: *s is a power of a prime, say a power of p_1.* Let $E_1 = \mathrm{supp}(U_1) \setminus \{g\}$. Since $\mathsf{v}_g(U_1) \mid n/p_1^{k_1}$, we have $g \in \langle sg, \mathsf{v}_g(U_1) g \rangle \subset \langle E \cup E_1 \rangle$. Property (a) implies that $E \cup E_1 = G_0 \setminus \{g\}$, and thus

$$|G_0| \le 1 + |E| + |E_1| \le 1 + \frac{n-s}{2} + \frac{n - \mathsf{v}_g(U_1)}{2} = 1 + n - \frac{\mathsf{v}_g(U_1) + s}{2}.$$

Since $\gcd(\mathsf{v}_g(U_1), s) = 1$, it follows that $\mathsf{v}_g(U_1) + s \ge 5$, hence $|G_0| \le n - 3/2$, and thus $|G_0| \le n-2$.

Case 2: *s is not a prime power, say $p_1 p_2 \mid s$.* Then $s \ge 6$. Let $d = \gcd(s, \mathsf{v}_g(U_1))$ and $E_1 = \mathrm{supp}(U_1) \setminus \{g\}$. Then $d < s$ and $dg \in \langle sg, \mathsf{v}_g(U_1) g \rangle \subset \langle E \cup E_1 \rangle \subset \langle G_0 \setminus \{g\} \rangle$. The minimality of s implies that $E \cup E_1 = G_0 \setminus \{g\}$, and thus

$$\begin{aligned} |G_0| &\le 1 + |E| + |E_1| \le 1 + \frac{n-s}{2} + \frac{n - \mathsf{v}_g(U_1)}{2} \\ &= 1 + n - \frac{\mathsf{v}_g(U_1) + s}{2} \le n - 3. \ ■ \end{aligned}$$

Lemma 3.2. *Let G be a finite abelian group with* $\exp(G) = n$. *Let $G_0 \subset G$ be a minimal non-half-factorial* LCN*-set, and suppose that there is a subset $G_2 \subset G_0$ such that $\langle G_2 \rangle = \langle G_0 \rangle$ and $|G_2| \le |G_0| - 2$. Then* $\min \Delta(G_0) \le \max\{1, n-4\}$.

Proof. Assume to the contrary that $\min \Delta(G_0) \ge \max\{2, n-3\}$. By [27, Corollary 3.1], the existence of G_2 implies that $\mathsf{k}(U) \in \mathbb{N}$ for each $U \in \mathcal{A}(G_0)$

and

$$\min \Delta(G_0) \mid \gcd(\{\mathsf{k}(A) - 1 \mid A \in \mathcal{A}(G_0)\}).$$

We set

$$W_1 = \{A \in \mathcal{A}(G_0) \mid \mathsf{k}(A) = 1\}, \qquad W_2 = \{A \in \mathcal{A}(G_0) \mid \mathsf{k}(A) > 1\}.$$

Then, for any $U_1, U_2 \in W_2$,

$$\begin{aligned} &\mathsf{k}(U_1) \ge \max\{3, n-2\} \quad \text{and} \\ &\text{either } \mathsf{k}(U_1) = \mathsf{k}(U_2) \text{ or } |\mathsf{k}(U_1) - \mathsf{k}(U_2)| \ge \max\{2, n-3\}. \end{aligned} \tag{3.2}$$

We choose $U \in W_2$. Then $\operatorname{supp}(U) = G_0$, and we pick $g \in G_0 \setminus G_2$. Then $g \in \langle G_2 \rangle$ and, by (2.1), there is an atom A with $\mathsf{v}_g(A) = 1$ and $\operatorname{supp}(A) \subset G_2 \cup \{g\} \subsetneq G_0$. This implies that $A \in W_1$, and

$$UA^{\operatorname{ord}(g) - \mathsf{v}_g(U)} = g^{\operatorname{ord}(g)} S$$

for some zero-sum sequence S over G. Since $\operatorname{supp}(S) = G_0 \setminus \{g\}$ and G_0 is minimal non-half-factorial, S has a factorization into a product of atoms from W_1. Therefore, for each $U \in W_2$, there are $A_1, \ldots, A_m \in W_1$, where $m \le \operatorname{ord}(g) - \mathsf{v}_g(U) \le n - 1$, such that $UA_1 \cdot \ldots \cdot A_m$ can be factorized into a product of atoms from W_1.

We set

$$W_0 = \big\{A \in \mathcal{A}(G_0) \;\big|\; \mathsf{k}(A) = \min\{\mathsf{k}(B) \mid B \in W_2\}\big\} \subset W_2,$$

and we consider all tuples $(U, A_1, \ldots, A_m)$, where $U \in W_0$ and $A_1, \ldots, A_m \in W_1$, such that $UA_1 \cdot \ldots \cdot A_m$ can be factorized into a product of atoms from W_1. We fix one such tuple $(U, A_1, \ldots, A_m)$ with m minimal possible. Note that $m \le n - 1$. Let

$$UA_1 \cdot \ldots \cdot A_m = V_1 \cdot \ldots \cdot V_t \quad \text{with } t \in \mathbb{N} \text{ and } V_1, \ldots, V_t \in W_1. \tag{3.3}$$

We observe that $\mathsf{k}(U) = t - m$ and assert the following:

A1. *For each $\nu \in [1, t]$, we have $V_\nu \nmid UA_1 \cdot \ldots \cdot A_{m-1}$.*

Proof of **A1**. Assume to the contrary that there is a $\nu \in [1, t]$, say $\nu = 1$, with $V_1 \mid UA_1 \cdot \ldots \cdot A_{m-1}$. Then there are $l \in \mathbb{N}$ and $T_1, \ldots, T_l \in \mathcal{A}(G_0)$ such that

$$UA_1 \cdot \ldots \cdot A_{m-1} = V_1 T_1 \cdot \ldots \cdot T_l.$$

By the minimality of m, there exists $\nu \in [1, l]$ such that $T_\nu \in W_2$, say $\nu = 1$. Since

$$\sum_{\nu=2}^{l} \mathsf{k}(T_\nu) = \mathsf{k}(U) + (m-1) - 1 - \mathsf{k}(T_1) \le m - 2 \le n - 3,$$

and $\mathsf{k}(T') \ge n - 2$ for all $T' \in W_2$, it follows that $T_2, \ldots, T_l \in W_1$, whence $l = 1 + \sum_{\nu=2}^{l} \mathsf{k}(T_\nu) \le m - 1$. We obtain

$$V_1 T_1 \cdot \ldots \cdot T_l A_m = UA_1 \cdot \ldots \cdot A_m = V_1 \cdot \ldots \cdot V_t,$$

and thus

$$T_1 \cdot \ldots \cdot T_l A_m = V_2 \cdot \ldots \cdot V_t .$$

The minimality of m implies that $\mathsf k(T_1) > \mathsf k(U)$. It follows that

$$\mathsf k(T_1) - \mathsf k(U) = m-1-l \le m-2 \le n-3 \le \max\{n-3, 2\} \le \mathsf k(T_1) - \mathsf k(U).$$

Therefore $l = 1$, $m = n-1$, $n \ge 5$, and $\mathsf k(T_1) = \mathsf k(U) + n - 3$. Thus

$$T_1 A_{n-1} = V_2 \cdot \ldots \cdot V_t , \quad \text{and hence} \quad t-1 \le |A_{n-1}| .$$

This equation shows that $\mathsf k(T_1) = t-2 \le |A_{n-1}| - 1 \le n-1$, and hence $n-2 \le \mathsf k(U) = \mathsf k(T_1) - n + 3 \le 2$, contradicting $n \ge 5$. $\blacksquare$Proof of **A1**

Since $\exp(G) = n$ and $\mathsf k(A_m) = 1$, it follows that $|A_m| \le n$. By **A1**, for each $\nu \in [1,t]$ there exists $h_\nu \in \operatorname{supp}(A_m)$ such that

$$\mathsf v_{h_\nu}(V_\nu) > \mathsf v_{h_\nu}(UA_1 \cdot \ldots \cdot A_{m-1}).$$

For each $h \in \operatorname{supp}(A_m)$ we define

$$F_h = \{\nu \in [1,t] \mid \mathsf v_h(V_\nu) > \mathsf v_h(UA_1 \cdot \ldots \cdot A_{m-1})\} \subset [1,t].$$

Thus

$$\bigcup_{h \in \operatorname{supp}(A_m)} F_h = [1,t],$$

and for each $h \in \operatorname{supp}(A_m)$, we have

$$\begin{aligned} \mathsf v_h(A_m) + \mathsf v_h(UA_1 \cdot \ldots \cdot A_{m-1}) &= \sum_{i=1}^{t} \mathsf v_h(V_i) \ge \sum_{i \in F_h} \mathsf v_h(V_i) \\ &\ge |F_h| (\mathsf v_h(UA_1 \cdot \ldots \cdot A_{m-1}) + 1). \end{aligned}$$

Since $|A_m| > |\operatorname{supp}(A_m)|$ (otherwise $A_m \mid U$, a contradiction), we obtain

$$\begin{aligned} t = \Big| \bigcup_{h \in \operatorname{supp}(A_m)} F_h \Big| &\le \sum_{h \in \operatorname{supp}(A_m)} |F_h| \\ &\le \sum_{h \in \operatorname{supp}(A_m)} \frac{\mathsf v_h(A_m) + \mathsf v_h(UA_1 \cdot \ldots \cdot A_{m-1})}{\mathsf v_h(UA_1 \cdot \ldots \cdot A_{m-1}) + 1} \\ &\le \sum_{h \in \operatorname{supp}(A_m)} \frac{\mathsf v_h(A_m) + 1}{2} = \frac{|A_m|}{2} + \frac{|\operatorname{supp}(A_m)|}{2} < |A_m| \le n. \end{aligned}$$

By (3.3) and (3.2), we have $\max\{3, n-2\} \le \mathsf k(U) = t - m \le n-1-m$ and hence $m = 1$, $n \ge 5$, $t = n-1$, and $\mathsf k(U) = n-2$. Therefore

$$UA_1 = V_1 \cdot \ldots \cdot V_{n-1}, \quad |A_1| = n, \quad n-2 \le |\operatorname{supp}(A_1)| \le n-1, \tag{3.4}$$

and

$$\sum_{h \in \operatorname{supp}(A_1)} |F_h| = n-1, \quad \text{with } F_h,\ h \in \operatorname{supp}(A_1), \text{ pairwise disjoint.} \tag{3.5}$$

Furthermore, $|F_h| \le \frac{\mathsf{v}_h(A_1)+\mathsf{v}_h(U)}{\mathsf{v}_h(U)+1}$ for all $h \in \mathrm{supp}(A_1)$. Then for $h \in \mathrm{supp}(A_1)$,

$$|F_h| \le 1 \quad \text{when } \mathsf{v}_h(A_1) \le 2, \quad |F_h| \le 2 \quad \text{when } \mathsf{v}_h(A_1) \le 4. \tag{3.6}$$

Now we consider all atoms $A_1 \in W_1$ such that UA_1 can be factorized into a product of $n-1$ atoms from W_1, and among them we consider the atoms A_1' for which $|\mathrm{supp}(A_1')|$ is minimal; from these we choose an atom A_1'' for which $\mathsf{h}(A_1'')$ is minimal. Changing notation if necessary we suppose that A_1 has this property. By (3.4), we distinguish three cases depending on $|\mathrm{supp}(A_1)|$ and $\mathsf{h}(A_1)$.

CASE 1: $|\mathrm{supp}(A_1)| = n-1$. Let $\mathrm{supp}(A_1) = \{g_1, \ldots, g_{n-1}\}$ and $A_1 = g_1^2 g_2 \cdot \ldots \cdot g_{n-1}$. Since $\mathsf{h}(A_1) = 2$, (3.6) and (3.5) imply that $|F_h| = 1$ for each $h \in \mathrm{supp}(A_1)$. Note that $U g_1^2 g_2 \cdot \ldots \cdot g_{n-1} = V_1 \cdot \ldots \cdot V_{n-1}$. After renumbering if necessary we may suppose that $F_{g_i} = \{i\}$ for each $i \in [1, n-1]$. Therefore $\mathsf{v}_{g_i}(V_i) > \mathsf{v}_{g_i}(U) \ge 1$ for each $i \in [1, n-1]$. Hence $\mathsf{v}_{g_1}(V_1) \ge 2$ and we set $V_1 = g_1^2 Y_1$ for some Y_1 dividing U. Thus $UY_1^{-1} g_2 \cdot \ldots \cdot g_{n-1} = V_2 \cdot \ldots \cdot V_{n-1}$, which implies that $V_i = g_i Y_i$ for $i \in [2, n-1]$, where $Y_2 \cdot \ldots \cdot Y_{n-1} = UY_1^{-1}$. Summing up we have

$$U = Y_1 \cdot \ldots \cdot Y_{n-1} \text{ with } V_i = g_i Y_i \text{ for } i \in [2, n-1] \text{ and } V_1 = g_1^2 Y_1. \tag{3.7}$$

Since $\mathsf{k}(A_1^{\lfloor (n+1)/2 \rfloor} g_1^{-n}) = \lfloor (n+1)/2 \rfloor \mathsf{k}(A_1) - 1 = \lfloor (n+1)/2 \rfloor - 1 < \max\{3, n-2\}$, it follows that every atom X dividing $A_1^{\lfloor (n+1)/2 \rfloor} g_1^{-n}$ has cross number $\mathsf{k}(X) = 1$ by (3.2). Since $\mathsf{v}_{g_1}(A_1^{\lfloor (n+1)/2 \rfloor} g_1^{-n}) \le 1$, there is an atom C dividing $A_1^{\lfloor (n+1)/2 \rfloor} g_1^{-n}$ with $\mathrm{supp}(C) \subset \{g_2, \ldots, g_{n-1}\}$ and $|\mathrm{supp}(C)| \ge 2$, say $g_2, g_3 \in \mathrm{supp}(C)$. Therefore, $V_2 V_3 = g_2 g_3 Y_2 Y_3 \,|\, UC$, say $UC = V_2 V_3 V'$ for some $V' \in \mathcal{B}(G)$. Since

$$\mathsf{k}(UC) = \mathsf{k}(U) + \mathsf{k}(C) = n-1 = \mathsf{k}(V_2) + \mathsf{k}(V_3) + \mathsf{k}(V'),$$

we obtain $\mathsf{k}(V') = n-3$. Now (3.2) implies that V' is a product of atoms from W_1, and hence UC can be factorized into a product of $n-1$ atoms. Since $|\mathrm{supp}(C)| < n-1 = |\mathrm{supp}(A_1)|$, this contradicts the choice of A_1.

CASE 2: $|\mathrm{supp}(A_1)| = n-2$ *and* $\mathsf{h}(A_1) = 2$. Let $\mathrm{supp}(A_1) = \{g_1, \ldots, g_{n-2}\}$ and $A_1 = g_1^2 g_2^2 g_3 \cdot \ldots \cdot g_{n-2}$. Since $\mathsf{h}(A_1) = 2$, (3.6) implies that $|F_h| \le 1$ for each $h \in \mathrm{supp}(A_1)$. Thus $\sum_{h \in \mathrm{supp}(A_1)} |F_h| \le n-2$, contrary to (3.5).

CASE 3: $|\mathrm{supp}(A_1)| = n-2$ *and* $\mathsf{h}(A_1) = 3$. Let $\mathrm{supp}(A_1) = \{g_1, \ldots, g_{n-2}\}$ and $A_1 = g_1^3 g_2 \cdot \ldots \cdot g_{n-2}$. Since $\mathsf{h}(A_1) = 3$, (3.6) and (3.5) imply that $|F_{g_1}| = 2$ and $|F_{g_i}| = 1$ for each $i \in [2, n-2]$. Note that $U g_1^3 g_2 \cdot \ldots \cdot g_{n-2} = V_1 \cdot \ldots \cdot V_{n-1}$. After renumbering if necessary we may suppose that $F_{g_1} = \{1, n-1\}$ and $F_{g_i} = \{i\}$ for each $i \in [2, n-2]$. Therefore $\mathsf{v}_{g_i}(V_i) > \mathsf{v}_{g_i}(U) \ge 1$ for each $i \in [1, n-2]$ and $\mathsf{v}_{g_1}(V_{n-1}) > \mathsf{v}_{g_1}(U) \ge 1$. Hence we may set $V_{n-1} = g_1^2 Y_{n-1}$ for some Y_{n-1} dividing U. Thus $UY_{n-1}^{-1} g_1 g_2 \cdot \ldots \cdot g_{n-2} = V_1 \cdot \ldots \cdot V_{n-2}$, which implies that $V_i = g_i Y_i$ for each $i \in [1, n-2]$ where $Y_1 \cdot \ldots \cdot Y_{n-2} = U Y_{n-1}^{-1}$. Summing up we have

(3.8) $\quad U = Y_1 \cdot \ldots \cdot Y_{n-1}$ with $V_i = g_i Y_i$ for $i \in [1, n-2]$ and $V_{n-1} = g_1^2 Y_{n-1}$.

Since $\mathsf{k}(A_1^{\lfloor (n+2)/3 \rfloor} g_1^{-n}) = \lfloor (n+2)/3 \rfloor \mathsf{k}(A_1) - 1 = \lfloor (n+2)/3 \rfloor - 1 < \max\{3, n-2\}$, it follows that every atom X dividing $A_1^{\lfloor (n+2)/3 \rfloor} g_1^{-n}$ has $\mathsf{k}(X) = 1$ by (3.2). Let $C \in \mathcal{A}(G)$ divide $A_1^{\lfloor (n+2)/3 \rfloor} g_1^{-n}$. Then $\mathsf{k}(C) = 1$, $\operatorname{supp}(C) \subset \{g_1, \ldots, g_{n-2}\}$, and $|\operatorname{supp}(C)| \ge 2$, say $g_i, g_j \in \operatorname{supp}(C)$ where $1 \le i < j \le n-2$. Therefore $V_i V_j = g_i g_j Y_i Y_j \mid UC$ by (3.8). Arguing as in Case 1 we infer that UC is a product of $n-1$ atoms from W_1. By the choice of A_1, we obtain $|\operatorname{supp}(C)| = n-2$ and $\mathsf{h}(C) \ge 3$. This holds for all atoms dividing $A_1^{\lfloor (n+2)/3 \rfloor} g_1^{-n}$, contradicting the structure of $A_1^{\lfloor (n+2)/3 \rfloor}$. ∎

Proof of Theorem 1.1. Let H be a Krull monoid with class group G, and let $G_P \subset G$ denote the set of classes containing prime divisors. If $|G| \le 2$, then H is half-factorial by [13, Corollary 3.4.12], and thus $\Delta^*(H) \subset \Delta(H) = \emptyset$. If G is infinite and $G_P = G$, then $\Delta^*(H) = \mathbb{N}$ by [7, Theorem 1.1].

Suppose that $2 < |G| < \infty$. By Lemma 2.1, it suffices to prove the statements for the Krull monoid $\mathcal{B}(G_P)$. If G is finite, then $\Delta(G)$ is finite by [13, Corollary 3.4.13], hence $\Delta^*(G)$ is finite, and Lemma 2.3 shows that $\{\exp(G) - 2, \mathsf{r}(G) - 1\} \subset \Delta^*(G)$.

Since $\Delta^*(G_P) \subset \Delta^*(G)$, it remains to prove that

$$\max \Delta^*(G) \le \max\{\exp(G) - 2, \mathsf{r}(G) - 1\}.$$

Let $G_0 \subset G$ be a non-half-factorial subset, $n = \exp(G)$, and $r = \mathsf{r}(G)$. We need to prove that $\min \Delta(G_0) \le \max\{n-2, r-1\}$. If $G_1 \subset G_0$ is non-half-factorial, then $\min \Delta(G_0) = \gcd \Delta(G_0) \mid \gcd \Delta(G_1) = \min \Delta(G_1)$. Thus we may suppose that G_0 is minimal non-half-factorial. If there is an $U \in \mathcal{A}(G_0)$ with $\mathsf{k}(U) < 1$, then Lemma 2.3.3 implies that $\min \Delta(G_0) \le n-2$.

Suppose that $\mathsf{k}(U) \ge 1$ for all $U \in \mathcal{A}(G_0)$, i.e, G_0 is an LCN-set. Since G_0 is minimal non-half-factorial, it follows that G_0 is indecomposable by Lemma 2.5. By Lemma 2.6(2), we may suppose that $g \in \langle G_0 \setminus \{g\} \rangle$ for all $g \in G_0$.

Suppose that the order of each element of G_0 is a prime power. Since G_0 is indecomposable, Lemma 2.5 implies that each order is a power of a fixed prime $p \in \mathbb{P}$, and thus $\langle G_0 \rangle$ is a p-group. By Proposition 2.4 we infer that

$$\begin{aligned} \min \Delta(G_0) \le \max \Delta^*(\langle G_0 \rangle) &= \max\{\exp(\langle G_0 \rangle) - 2, \mathsf{r}(\langle G_0 \rangle) - 1\} \\ &\le \max\{n-2, r-1\}. \end{aligned}$$

From now on we suppose that there is a $g \in G_0$ whose order is not a prime power. Then $n \ge 6$. If $|G_0| \le r+1$, then $\min \Delta(G_0) \le |G_0| - 2 \le r-1$

by Lemma 2.3.3. Thus we may suppose that $|G_0| \ge r+2$ and we distinguish two cases.

CASE 1: *There exists a subset $G_2 \subset G_0$ such that $\langle G_2\rangle = \langle G_0\rangle$ and $|G_2| \le |G_0|-2$.* Then Lemma 3.2 implies that $\min \Delta(G_0) \le n-4 \le n-2$.

CASE 2: *Every subset $G_1 \subset G_0$ with $|G_1| = |G_0|-1$ is a minimal generating set of $\langle G_0\rangle$.* Then for each $h \in G_0$, $G_0 \setminus \{h\}$ is half-factorial and $h \notin \langle G_0 \setminus \{h,h'\}\rangle$ for any $h' \in G_0 \setminus \{h\}$. Thus Lemma 3.1 implies that $|G_0| \le n-2$, and hence $\min \Delta(G_0) \le |G_0|-2 \le n-4 \le n-2$ by Lemma 2.3(3). ∎

4. Inverse results on $\Delta^*(H)$. Let G be a finite abelian group. In this section we study the structure of minimal non-half-factorial subsets $G_0 \subset G$ with $\min \Delta(G_0) = \max \Delta^*(G)$. These structural investigations were started by Schmid who obtained a characterization in case $\exp(G)-2 > \mathsf{m}(G)$ (Lemma 4.1(1)). Our main result in this section is Theorem 4.5. All examples of minimal non-half-factorial subsets $G_0 \subset G$ with $\min \Delta(G_0) = \max \Delta^*(G)$ known so far are simple (in the sense of Remark 4.6), and it has been conjectured that all such sets are simple. We provide the first example of a set G_0 which is not simple (Remark 4.6).

LEMMA 4.1. *Let G be a finite abelian group with $|G| > 2$, $\exp(G) = n$, $\mathsf{r}(G) = r$, and let $G_0 \subset G$ be a subset with $\min \Delta(G_0) = \max \Delta^*(G)$.*

(1) *Suppose that $\mathsf{m}(G) < n-2$. Then G_0 is indecomposable if and only if $G_0 = \{g,-g\}$ for some $g \in G$ with $\mathrm{ord}(g) = n$.*
(2) *Suppose that $r \le n-1$. Then G_0 is minimal non-half-factorial but not an LCN-set if and only if $G_0 = \{g,-g\}$ for some $g \in G$ with $\mathrm{ord}(g) = n$.*

Proof. (1) See [30, Theorem 5.1].

(2) Since $n=2$ implies $r=1$ and $|G|=2$, it follows that $n \ge 3$. By Theorem 1.1, we have $\min \Delta(G_0) = n-2$. Obviously, the set $\{-g,g\}$, with $g \in G$ and $\mathrm{ord}(g) = n$, is a minimal non-half-factorial set with $\min \Delta(\{-g,g\}) = n-2$ but not an LCN-set.

Conversely, let G_0 be minimal non-half-factorial but not an LCN-set. Then there exists $A \in \mathcal{A}(G_0)$ with $\mathsf{k}(A) < 1$. Since $\{n, n\mathsf{k}(A)\} \subset \mathsf{L}(A^n)$, it follows that $n-2 \mid n(\mathsf{k}(A)-1)$, whence $\mathsf{k}(A) = 2/n$. Consequently, $A = (-g)g$ for some g with $\mathrm{ord}(g) = n$. Thus $\{-g,g\} \subset G_0$, and since G_0 is minimal non-half-factorial, equality follows. ∎

LEMMA 4.2. *Let G be a finite abelian group with $\exp(G) = n$ and $\mathsf{r}(G) = r$.*

(1) *Let* $G_0 \subset G$ *be a minimal non-half-factorial* LCN*-set with* $\min \Delta(G_0) = \max \Delta^*(G)$*. Then* $|G_0| = r+1$*,* $r \ge n-1$*, and for any distinct* $h, h' \in G_0$ *we have* $h \notin \langle G_0 \setminus \{h, h'\} \rangle$*.*
(2) *If* $r \le n-2$*, then* $\mathsf m(G) \le n-3$*.*
(3) *If* $n \ge 5$ *and* $r \le n-3$*, then* $\mathsf m(G) \le n-4$*.*

Proof. (1) We have $\min \Delta(G_0) \le |G_0| - 2$ by Lemma 2.3(3), and moreover $\min \Delta(G_0) = \max\{n-2, r-1\}$ by Theorem 1.1.

By Lemma 2.6(2) (properties (a) and (c)), we may assume that for each $g \in G_0$ we have $g \in \langle G_0 \setminus \{g\} \rangle$.

Case 1: *There is a subset* $G_2 \subset G_0$ *such that* $\langle G_2 \rangle = \langle G_0 \rangle$ *and* $|G_2| \le |G_0| - 2$*.* The existence of G_2 implies that G is isomorphic neither to C_3 nor to $C_2 \oplus C_2$ nor to $C_3 \oplus C_3$ (this is clear for the first two groups; to exclude the case $C_3 \oplus C_3$, use again [27, Corollary 3.1] which says that $\mathsf k(U) \in \mathbb N$ for each $U \in \mathcal A(G_0)$). By Lemma 3.2, we know that $\min \Delta(G_0) \le \max\{n-4, 1\} < \max\{n-2, r-1\} = \min \Delta(G_0)$, a contradiction.

Case 2: *Every subset* $G_1 \subset G_0$ *with* $|G_1| = |G_0| - 1$ *is a minimal generating set of* $\langle G_0 \rangle$*.* Then for any distinct $h, h' \in G_0$ we have $h \notin \langle G_0 \setminus \{h, h'\} \rangle$.

Assume to the contrary that $|G_0| \ge r+2$. Since $r+1 \le |G_0| - 1 \le \mathsf r^*(\langle G_0 \rangle)$, it follows by [13, Lemma A.6.2] that $\langle G_0 \rangle$ is not a p-group. Since G_0 is a minimal non-half-factorial subset, there exists an atom A with $\operatorname{supp}(A) = G_0$ and hence G_0 contains an element whose order is not a prime power. Thus, by Lemma 3.1 we infer that $|G_0| \le n-2$, and hence $\min \Delta(G_0) \le |G_0| - 2 \le n-4$, a contradiction.

Therefore $|G_0| \le r+1$. Then $\max\{n-2, r-1\} = \min \Delta(G_0) \le |G_0| - 2 \le r-1$, so we must have $|G_0| = r+1$ and $r \ge n-1$.

(2) Assume to the contrary that $r \le n-2$ and $\mathsf m(G) \ge n-2$. Then by Theorem 1.1, $\max \Delta^*(G) = \max\{r-1, n-2\} = n-2$. Since $\mathsf m(G) \ge n-2$, there is a minimal non-half-factorial LCN-set G_0 with $\min \Delta(G_0) = \max \Delta^*(G)$, and then (1) implies that $r \ge n-1$, a contradiction.

(3) Let $G_0 \subset G$ be a non-half-factorial LCN-subset. We need to prove that $\min \Delta(G_0) \le n-4$. Without restriction we may suppose that G_0 is minimal non-half-factorial, which implies that G_0 is indecomposable by Lemma 2.5. By Lemma 2.6(2) we may suppose that for each $g \in G_0$ we have $g \in \langle G_0 \setminus \{g\} \rangle$. Suppose that the order of each element of G_0 is a prime power. Since G_0 is indecomposable, Lemma 2.5 implies that each order is a power of a fixed prime $p \in \mathbb P$, and thus $\langle G_0 \rangle$ is a p-group. By Proposition 2.4, we infer that

$$\min \Delta(G_0) \le \mathsf m(\langle G_0 \rangle) = \mathsf r(\langle G_0 \rangle) - 1 \le \mathsf r(G) - 1 \le n-4.$$

From now on we suppose that there is a $g \in G_0$ whose order is not a prime power. If $|G_0| \le n-2$, then $\min \Delta(G_0) \le |G_0|-2 \le n-4$ by Lemma 2.3(3) Thus we may suppose that $|G_0| \ge n-1 \ge r+2$ and we distinguish two cases.

CASE 1: *There exists a subset $G_2 \subset G_0$ such that $\langle G_2\rangle = \langle G_0\rangle$ and $|G_2| \le |G_0|-2$.* Then Lemma 3.2 implies that $\min \Delta(G_0) \le n-4$.

CASE 2: *Every subset $G_1 \subset G_0$ with $|G_1| = |G_0|-1$ is a minimal generating set of $\langle G_0\rangle$.* Then for each $h \in G_0$, $G_0 \setminus \{h\}$ is half-factorial and $h \notin \langle G_0 \setminus \{h,h'\}\rangle$ for any $h' \in G_0 \setminus \{h\}$. Thus Lemma 3.1 implies that $|G_0| \le n-2$, a contradiction. ∎

LEMMA 4.3. *Let G be a finite abelian group with $\exp(G) = n$ and $\mathsf r(G) = r$, and let $G_0 \subset G$ be a minimal non-half-factorial* LCN*-set with $\min \Delta(G_0) = \max \Delta^*(G)$.*

(1) *If $A \in \mathcal A(G_0)$ with $\mathsf k(A) = 1$, then $|\mathrm{supp}(A)| \le n/2$.*
(2) *If $A \in \mathcal A(G_0)$ with $\mathsf k(A) > 1$, then $\mathsf k(A) < r$ and SA^{-1} is also an atom where $S = \prod_{g\in G_0} g^{\mathrm{ord}(g)}$.*

Proof. By Lemma 4.2, we have $r \ge n-1$, $|G_0| = r+1$, and for each $h \in G_0$, $h \notin \langle G_0 \setminus \{h,h'\}\rangle$ for any $h' \in G_0 \setminus \{h\}$. Let $A \in \mathcal A(G_0)$.

(1) Since $\mathsf k(A) = 1$, it follows that $|\mathrm{supp}(A)| \le |A| \le n$. Assume that $|\mathrm{supp}(A)| = n$. Then $\mathsf v_g(A) = 1$ for each $g \in \mathrm{supp}(A)$. Since G_0 is a minimal non-half-factorial LCN-set, there is a $V \in \mathcal A(G_0)$ with $\mathsf k(V) > 1$ and $\mathrm{supp}(V) = G_0$. Therefore $A \,|\, V$, a contradiction.

Thus $|\mathrm{supp}(A)| \le n-1$, whence $\mathrm{supp}(A) \subsetneq G_0$. Therefore Lemma 2.6.1 implies that $\gcd(\mathsf v_g(A), \mathrm{ord}(g)) > 1$ for each $g \in \mathrm{supp}(A)$, and hence $|\mathrm{supp}(A)| \le |A|/2 \le n/2$.

(2) Let $A \in \mathcal A(G_0)$ with $\mathsf k(A) > 1$. Then $A \,|\, S$, $r+1 = |G_0| = \max \mathsf L(S)$, and $\mathsf L(S) \setminus \{r+1\} \ne \emptyset$. By Theorem 1.1, we have $\min \Delta(G_0) = r-1$, hence $\mathsf L(S) = \{2, r+1\}$, and thus SA^{-1} is an atom.

If $\mathsf k(SA^{-1}) = 1$, then (1) implies that $|\mathrm{supp}(SA^{-1})| \le n/2$, but on the other hand $|\mathrm{supp}(SA^{-1})| = |G_0| = r+1 \ge n$, a contradiction.

Therefore $\mathsf k(SA^{-1}) > 1$ and hence $r+1 = \mathsf k(S) = \mathsf k(A) + \mathsf k(SA^{-1})$ implies that $\mathsf k(A) < r$. ∎

LEMMA 4.4. *Let G be a finite abelian group with $\exp(G) = n$ and $\mathsf r(G) = r$, and let $G_0 \subset G$ be a minimal non-half-factorial* LCN*-set with $\min \Delta(G_0) = \max \Delta^*(G)$. Let $g \in G_0$ with $g \in \langle G_0 \setminus \{g\}\rangle$, and let $d \in [1, \mathrm{ord}(g)]$ be minimal such that $dg \in \langle E^*\rangle$, where the minimum is taken over all subsets $E^* \subsetneq G_0 \setminus \{g\}$. Then $d \,|\, \mathrm{ord}(g)$ and:*

(1) *Let $k \in [1, \mathrm{ord}(g)-1]$ with $d \nmid k$. Then there is an atom A with $\mathsf v_g(A) = k$ and $\mathsf k(A) > 1$. If $B \in \mathcal B(G_0)$ with $\mathsf v_g(B) = k$ and B divides $\prod_{g\in G_0} g^{\mathrm{ord}(g)}$, then B is an atom.*

(2) *If* A_1, A_2 *are atoms with* $\mathsf v_g(A_1) \equiv \mathsf v_g(A_2) \bmod d$, *then* $\mathsf k(A_1) = \mathsf k(A_2)$.

Proof. Lemma 4.2 yields $|G_0| = r+1$ and $r \ge n-1$. The minimality of d and (2.1) imply that $d \mid \operatorname{ord}(g)$. We set $S = \prod_{h \in G_0} h^{\operatorname{ord}(h)}$.

(1) Since $g \in \langle G_0 \setminus \{g\} \rangle$, there is a zero-sum sequence B such that $\mathsf v_g(B) = k$, and we choose B with minimal length $|B|$. Thus $B \mid S$, and it remains to prove that B is an atom with $\mathsf k(B) > 1$.

We set $B = A_1 \cdot \ldots \cdot A_s$ with $s \in \mathbb N$ and atoms $A_1, \ldots, A_s$. Then $\mathsf v_g(A_1) + \cdots + \mathsf v_g(A_s) = \mathsf v_g(B) = k$. Since $d \nmid k$, there is an $i \in [1, s]$ such that $d \nmid \mathsf v_g(A_i)$.

Assume to the contrary that $\mathsf k(A_i) = 1$. Then $|\operatorname{supp}(A_i)| \le n/2$ by Lemma 4.3(1). By the definition of d, there exists an atom A' such that $\mathsf v_g(A') = d$ and $\mathsf k(A') = 1$, which implies $|\operatorname{supp}(A')| \le n/2$ by Lemma 4.3(1). Hence $\gcd(d, \mathsf v_g(A_i)) < d$, $\gcd(d, \mathsf v_g(A_i))g \in \langle \operatorname{supp}(A_i) \cup \operatorname{supp}(A') \setminus \{g\} \rangle$, and $|\operatorname{supp}(A_i) \cup \operatorname{supp}(A') \setminus \{g\}| \le n-2 < r < |G_0|$, contradicting the choice of d.

Thus $\mathsf k(A_i) > 1$. Since $k \le \operatorname{ord}(g) - 1$, it follows that $SB^{-1} \ne 1$. Since $SA_i^{-1} = (SB^{-1})(BA_i^{-1})$ is an atom by Lemma 4.3(2), we infer that $B = A_i$ is an atom with $\mathsf k(B) > 1$.

2. Let $A_1 \in \mathcal A(G_0)$. We assert that $\mathsf k(A_1) = \mathsf k(A_2)$ for all $A_2 \in \mathcal A(G_0)$ with $\mathsf v_g(A_1) \equiv \mathsf v_g(A_2) \bmod d$. We distinguish two cases.

CASE 1: $d \mid \mathsf v_g(A_1)$. There is an $A \in \mathcal A(G_0)$ with $\mathsf v_g(A) = d$ and $\mathsf k(A) = 1$. It is sufficient to show that $\mathsf k(A_1) = 1$. There are $l \in \mathbb N$ and $V_1, \ldots, V_l \in \mathcal A(G_0 \setminus \{g\})$ (hence $\mathsf k(V_1) = \cdots = \mathsf k(V_l) = 1$) such that

$$A_1 A^{\frac{\operatorname{ord}(g) - \mathsf v_g(A_1)}{d}} = g^{\operatorname{ord}(g)} V_1 \cdot \ldots \cdot V_l, \quad \text{so} \quad \mathsf k(A_1) = 1 + l - \frac{\operatorname{ord}(g) - \mathsf v_g(A_1)}{d}.$$

Furthermore, $\min \Delta(G_0) = r-1$ divides

$$(l+1) - \left(1 + \frac{\operatorname{ord}(g) - \mathsf v_g(A_1)}{d}\right) = \mathsf k(A_1) - 1.$$

Since $\mathsf k(A_1) < r$ by Lemma 4.3, it follows that $\mathsf k(A_1) = 1$.

CASE 2: $d \nmid \mathsf v_g(A_1)$. Let $d_0 \in [1, d-1]$ be such that $\mathsf v_g(A_1) \equiv d_0 \bmod d$. By (1), there are atoms B_l such that $\mathsf v_g(B_l) = d_0 + ld$ for all $l \in \mathbb N_0$ with $d_0 + ld < \operatorname{ord}(g)$. Thus by an inductive argument it is sufficient to prove the assertion for those atoms A_2 with $\mathsf v_g(A_2) = \mathsf v_g(A_1)$, and those with $\mathsf v_g(A_2) = \mathsf v_g(A_1) + d$.

Suppose that $\mathsf v_g(A_1) = \mathsf v_g(A_2)$. By (1), there is an atom V such that $\mathsf v_g(V) = \operatorname{ord}(g) - \mathsf v_g(A_1)$ and $\mathsf k(V) > 1$. Then there are $l \in \mathbb N$ and $V_1, \ldots, V_l \in \mathcal A(G_0 \setminus \{g\})$ such that $A_1 V = g^{\operatorname{ord}(g)} V_1 \cdot \ldots \cdot V_l$, and hence $\mathsf k(A_1) + \mathsf k(V) = 1 + \sum_{i=1}^l \mathsf k(V_i) = l+1$. Since $\mathsf k(V) > 1$, we have $l > 1$. Since $\min \Delta(G_0) = r-1$ divides $l-1$, either $l = r$ or $l \ge 2r-1$. If $l \ge 2r-1$, then $\mathsf k(A_1) \ge r$ or

$\mathsf{k}(V) \ge r$, contrary to Lemma 4.3. Therefore $\mathsf{k}(A_1) + \mathsf{k}(V) = r + 1 = \mathsf{k}(A_2) + \mathsf{k}(V)$, and hence $\mathsf{k}(A_1) = \mathsf{k}(A_2)$.

Suppose that $\mathsf{v}_g(A_1) = \mathsf{v}_g(A_2) + d$. Let $E \subsetneq G_0 \setminus \{g\}$ be such that $dg \in \langle E\rangle$. Then there is an $A \in \mathcal{A}(E \cup \{g\})$ with $\mathsf{v}_g(A) = d$, and clearly $\mathsf{k}(A) = 1$. Let $V_1, \ldots, V_t$ be all the atoms with $V_\nu \mid A_2A$ and $|\mathrm{supp}(V_\nu)| = 1$ for all $\nu \in [1, t]$. Since $\mathsf{v}_g(A_2A) = \mathsf{v}_g(A_1) < \mathrm{ord}(g)$, it follows that $B = A_2A(V_1 \cdot \ldots \cdot V_t)^{-1}$ divides S and that $\mathsf{v}_g(B) = \mathsf{v}_g(A_1)$. Therefore (2) implies that B is an atom, and by Step 1 we obtain $\mathsf{k}(B) = \mathsf{k}(A_1)$.

If $t \ge 2$, then $A_2A = BV_1 \cdot \ldots \cdot V_t$ implies $t \ge 1 + \min \Delta(G_0) = r$, and thus $\mathsf{k}(A_2) \ge r$, contradicting Lemma 4.3. Therefore $t = 1$, and thus $\mathsf{k}(A_2) + 1 = \mathsf{k}(B) + 1 = \mathsf{k}(A_1) + 1$. ■

THEOREM 4.5. *Let G be a finite abelian group with* $\exp(G) = n$ *and* $\mathsf{r}(G) = r$, *and let $G_0 \subset G$ be a minimal non-half-factorial set with* $\min \Delta(G_0) = \max \Delta^*(G)$.

(1) *If $r < n - 1$, then there exists $g \in G$ with* $\mathrm{ord}(g) = n$ *such that $G_0 = \{g, -g\}$.*
(2) *Let $r = n - 1$. If G_0 is not an* LCN-*set, then there exists $g \in G$ with* $\mathrm{ord}(g) = n$ *such that $G_0 = \{g, -g\}$. If G_0 is an* LCN-*set, then $|G_0| = r + 1$, and for any distinct $h, h' \in G_0$ we have $h \notin \langle G_0 \setminus \{h, h'\}\rangle$.*
(3) *If $r \ge n$, then G_0 is an* LCN-*set with $|G_0| = r + 1$, and for any distinct $h, h' \in G_0$ we have $h \notin \langle G_0 \setminus \{h, h'\}\rangle$.*
(4) *If $r \ge n-1$, G_0 is an* LCN-*set, and n is odd, then there exists $g \in G_0$ such that $G_0 \setminus \{g\}$ is independent.*

Proof. (1) Suppose that $r < n - 1$. Then Lemma 4.2 implies that G_0 is not an LCN-set. Thus Lemma 4.1(2) shows that G_0 has the asserted form.

(2) If G_0 is not an LCN-set, then the assertion follows from Lemma 4.1(2); otherwise it follows from Lemma 4.2(1).

(3) Suppose that $r \ge n$. Then Theorem 1.1 implies that $\min \Delta(G_0) = \max \Delta^*(G) = r - 1$. Thus Lemma 2.3(3)(a) shows that G_0 is an LCN-set. Hence the assertion follows from Lemma 4.2(1).

(4) Let $r \ge n - 1$, G_0 be an LCN-set, and suppose that n is odd. By Lemma 2.6(2) (properties (a) and (d)), we may suppose without restriction that $g \in \langle G_0 \setminus \{g\}\rangle$ for each $g \in G_0$. Lemma 4.2 implies that $|G_0| = r + 1$ and for each $g \in G_0$ we have $g \notin \langle E\rangle$ for any $E \subsetneq G_0 \setminus \{g\}$.

Assume to the contrary that $G_0 \setminus \{h\}$ is dependent for each $h \in G_0$. Then there exist $g \in G_0$, $d \in [2, \mathrm{ord}(g) - 1]$, and $E \subsetneq G_0 \setminus \{g\}$ such that $dg \in \langle E\rangle$. Now let $d \in \mathbb{N}$ be minimal over all configurations (g, E, d), and fix g, E corresponding to d. It follows that we have an atom A with $\mathrm{supp}(A) \subsetneq G_0$ and $\mathsf{v}_g(A) = d$. By Lemma 4.4, $d \mid \mathrm{ord}(g)$, and hence $d \ge 3$ because n is odd.

Since $G_0 \setminus \{g\}$ is dependent, there exists $U' \in \mathcal{A}(G_0 \setminus \{g\})$ with $|\mathrm{supp}(U')| > 1$. Thus, by (2.1), there exist $U \in \mathcal{A}(G_0 \setminus \{g\})$ and $h \in \mathrm{supp}(U)$ such that $\mathsf{v}_h(U) \le \mathrm{ord}(h)/2$ and $\mathsf{v}_h(U) \mid \mathrm{ord}(h)$.

By Lemma 4.4(1), there are atoms $A_1, \ldots, A_{d-1}$ with $\mathsf{v}_g(A_i) = i$ and $\mathsf{k}(A_i) > 1$ for each $i \in [1, d-1]$, and we choose each A_i with $\mathsf{v}_h(A_i)$ minimal. We prove the following assertion:

A. *For each $i \in [1, d-1]$, we have $\mathsf{v}_h(A_i) < \mathsf{v}_h(U) \le \mathrm{ord}(h)/2$.*

Proof of **A**. Assume to the contrary that there is an $i \in [1, d-1]$ such that $\mathsf{v}_h(A_i) \ge \mathsf{v}_h(U)$. Then

$$h \notin F = \{h' \in \mathrm{supp}(U) \mid \mathsf{v}_{h'}(A_i) < \mathsf{v}_{h'}(U)\} \quad \text{and} \quad U \mid A_i \prod_{h' \in F} h'^{\mathrm{ord}(h')}.$$

Hence $A_i \prod_{h' \in F} h'^{\mathrm{ord}(h')} = UB_i$ for some zero-sum sequence B_i. By Lemma 4.4 (items (1) and (2)), B_i is an atom with $i = \mathsf{v}_g(A_i) = \mathsf{v}_g(B_i)$ and with $\mathsf{k}(B_i) = \mathsf{k}(A_i) > 1$. Since $\mathsf{v}_h(A_i) > \mathsf{v}_h(B_i)$, this contradicts the choice of A_i. ■Proof of **A**

Let $j \in [1, d-1]$ be such that $\mathsf{k}(A_j) = \min\{\mathsf{k}(A_1), \ldots, \mathsf{k}(A_{d-1})\}$.

Suppose that $j \ge 2$. Let $V_1, \ldots, V_t$ be all the atoms with $V_s \mid A_1 A_{j-1}$ and $|\mathrm{supp}(V_s)| = 1$ for all $s \in [1, t]$. Then $B = A_1 A_{j-1} (V_1 \cdot \ldots \cdot V_t)^{-1}$ is an atom by Lemma 4.4(1). Since $\mathsf{v}_g(A_1 A_{j-1}) = j < \mathrm{ord}(g)$, $\mathsf{v}_h(A_1 A_{j-1}) < \mathrm{ord}(h)$, and $\mathsf{v}_f(A_1 A_{j-1}) < 2\,\mathrm{ord}(f)$ for all $f \in G_0 \setminus \{g, h\}$, it follows that $t \le |G_0| - 2 = r - 1$. Since $\min \Delta(G_0) = r - 1$ and $A_1 A_{j-1} = V_1 \cdot \ldots \cdot V_t B$, we must have $t = 1$. Therefore $\mathsf{k}(A_1) + \mathsf{k}(A_{j-1}) = 1 + \mathsf{k}(B)$, whence $\mathsf{k}(B) > \mathsf{k}(A_{j-1})$. Since

$$\mathsf{v}_g(B) = \mathsf{v}_g(V_1 B) = \mathsf{v}_g(A_1 A_{j-1}) = j = \mathsf{v}_g(A_j),$$

Lemma 4.4(2) implies that $\mathsf{k}(B) = \mathsf{k}(A_j) = \min\{\mathsf{k}(A_1), \ldots, \mathsf{k}(A_{d-1})\}$, a contradiction.

Suppose that $j = 1$. Let $V_1, \ldots, V_t$ be all the atoms with $V_s \mid A_2 A_{d-1}$ and $|\mathrm{supp}(V_s)| = 1$ for all $s \in [1, t]$. Then $B = A_2 A_{d-1} (V_1 \cdot \ldots \cdot V_t)^{-1}$ is an atom by Lemma 4.4(1). Since $\mathsf{v}_g(A_2 A_{d-1}) = d+1 < \mathrm{ord}(g)$, $\mathsf{v}_h(A_2 A_{d-1}) < \mathrm{ord}(h)$, and $\mathsf{v}_f(A_1 A_{j-1}) < 2\,\mathrm{ord}(f)$ for all $f \in G_0 \setminus \{g, h\}$, it follows that $t \le |G_0| - 2 \le r - 1$. Since $\min \Delta(G_0) = r - 1$ and $A_2 A_{d-1} = V_1 \cdot \ldots \cdot V_t B$, we must have $t = 1$. Therefore $\mathsf{k}(A_2) + \mathsf{k}(A_{d-1}) = 1 + \mathsf{k}(B)$, whence $\mathsf{k}(B) > \mathsf{k}(A_2)$. Since

$$\mathsf{v}_g(B) = \mathsf{v}_g(V_1 B) = \mathsf{v}_g(A_2 A_{d-1}) = d + 1 \equiv 1 = \mathsf{v}_g(A_1) \bmod d,$$

Lemma 4.4(2) implies that $\mathsf{k}(B) = \mathsf{k}(A_1) = \min\{\mathsf{k}(A_1), \ldots, \mathsf{k}(A_{d-1})\}$, a contradiction. ■

In the following remark we provide the first example of a minimal non-half-factorial subset G_0 with $\min \Delta(G_0) = \max \Delta^*(G)$ which is not simple. Furthermore, we provide an example showing that the structural statement given in Theorem 4.5(4) does not hold without the assumption that the exponent is odd.

REMARKS 4.6. Following Schmid, we say that a nonempty subset $G_0 \subset G \setminus \{0\}$ is *simple* if there exists $g \in G_0$ such that $G_0 \setminus \{g\}$ is independent and $g \in \langle G_0 \setminus \{g\} \rangle$, but $g \notin \langle E \rangle$ for any subset $E \subsetneq G_0 \setminus \{g\}$.

If G_0 is a simple subset, then $|G_0| \le \mathsf{r}^*(G)+1$ and G_0 is indecomposable. Moreover, if $G_1 \subset G$ is such that any proper subset of G_1 is independent, then there is a subset G_0 and a transfer homomorphism $\theta \colon \mathcal{B}(G_1) \to \mathcal{B}(G_0)$ where $G_0 \setminus \{0\}$ is simple or independent (for all this see [26, Section 4]). Furthermore, [26, Theorem 4.7] provides an intrinsic description of the sets of atoms of a simple set.

In elementary p-groups, every minimal non-half-factorial subset is simple [26, Lemma 4.4], and so far there are no examples of minimal non-half-factorial sets G_0 with $\min \Delta(G_0) = \max \Delta^*(G)$ which are not simple.

1. Let $G = C_9^{r-1} \oplus C_{27}$ with $r \ge 26$, and let $(e_1, \ldots, e_r)$ be a basis of G with $\mathrm{ord}(e_i) = 9$ for $i \in [1, r-1]$ and $\mathrm{ord}(e_r) = 27$. Then $\max \Delta^*(G) = r-1$ by Theorem 1.1. We set

$$G_0 = \{3e_1, \ldots, 3e_{r-1}, e_r, g\} \quad \text{with} \quad g = e_1 + \cdots + e_r.$$

Then (e_r, g) is not independent, $G_0 \setminus \{g\}$ and $G_0 \setminus \{e_r\}$ are independent, but $g \notin \langle G_0 \setminus \{g\} \rangle$ and $e_r \notin \langle G_0 \setminus \{e_r\} \rangle$. Therefore G_0 is not simple. It remains to show that $\min \Delta(G_0) \ge r-1$: then G_0 is minimal non-half-factorial (because every proper subset is half-factorial) and $\min \Delta(G_0) = r-1$ (because $\max \Delta^*(G) = r-1$).

We have

$$\begin{aligned}
W_1 &= \{A \in \mathcal{A}(G_0) \mid \mathsf{k}(A) = 1\} = \{(3e_1)^3, \ldots, (3e_{r-1})^3, e_r^{27}, g^{27}, g^9 e_r^{18}, g^{18} e_r^9\}, \\
W_2 &= \{A \in \mathcal{A}(G_0) \mid \mathsf{k}(A) > 1\} \\
&= \{A_3 = g^3 e_r^{24} (3e_1)^2 \cdot \ldots \cdot (3e_{r-1})^2,\ A_6 = g^6 e_r^{21} (3e_1) \cdot \ldots \cdot (3e_{r-1}), \\
&\qquad A_{12} = g^{12} e_r^{15} (3e_1)^2 \cdot \ldots \cdot (3e_{r-1})^2,\ A_{15} = g^{15} e_r^{12} (3e_1) \cdot \ldots \cdot (3e_{r-1}), \\
&\qquad A_{21} = g^{21} e_r^{6} (3e_1)^2 \cdot \ldots \cdot (3e_{r-1})^2,\ A_{24} = g^{24} e_r^{3} (3e_1) \cdot \ldots \cdot (3e_{r-1})\},
\end{aligned}$$

and $\mathsf{k}(A_3) = \mathsf{k}(A_{12}) = \mathsf{k}(A_{21}) = (2r+1)/3$, $\mathsf{k}(A_6) = \mathsf{k}(A_{15}) = \mathsf{k}(A_{24}) = (r+2)/3$. For any $d \in \Delta(G_0)$, there exists $B \in \mathcal{B}(G_0)$ that has two such factorizations, say

$$B = U_1 \cdot \ldots \cdot U_s V_1 \cdot \ldots \cdot V_t W_1 \cdot \ldots \cdot W_u = X_1 \cdot \ldots \cdot X_{s'} Y_1 \cdot \ldots \cdot Y_{t'} Z_1 \cdot \ldots \cdot Z_{u'}$$

where all $U_i, V_j, W_k, X_{i'}, Y_{j'}, Z_{k'}$ are atoms, $s, t, u, s', t', u' \in \mathbb{N}_0$ with $d = (s+t+u) - (s'+t'+u')$, $\mathsf{k}(U_1) = \cdots = \mathsf{k}(U_s) = \mathsf{k}(X_1) = \cdots = \mathsf{k}(X_{s'}) = (2r+1)/3$, $\mathsf{k}(V_1) = \cdots = \mathsf{k}(V_t) = \mathsf{k}(Y_1) = \cdots = \mathsf{k}(Y_{t'}) = (r+2)/2$, and

$\mathsf{k}(W_1) = \cdots = \mathsf{k}(W_u) = \mathsf{k}(Z_1) = \cdots = \mathsf{k}(Z_{u'}) = 1$. This implies that

$$\mathsf{k}(B) = s\frac{2r+1}{3} + t\frac{r+2}{3} + u = s'\frac{2r+1}{3} + t'\frac{r+2}{3} + u'$$

and $\mathsf{v}_{3e_1}(B) \equiv 2s + t \equiv 2s' + t' \mod 3$. Since $d = (s+t+u) - (s'+t'+u') = \frac{r-1}{3}((t'-t) + 2(s'-s)) > 0$, we conclude that $(t'-t) + 2(s'-s) \ge 3$ and hence $d \ge r - 1$.

2. We provide an example of a minimal non-half-factorial LCN-set G_0 with $\min \Delta(G_0) = \max \Delta^*(G)$ in a group G of even exponent which has no element $g \in G_0$ such that $G_0 \setminus \{g\}$ is independent. In particular, G_0 is not simple and the assumption in Theorem 4.5(4) that the exponent of the group is odd cannot be cancelled.

Let $G = C_2^{r-2} \oplus C_4 \oplus C_4$ with $r \ge 3$, and let $(e_1, \ldots, e_r)$ be a basis of G with $\mathrm{ord}(e_i) = 2$ for $i \in [1, r-2]$ and $\mathrm{ord}(e_{r-1}) = \mathrm{ord}(e_r) = 4$. We set

$$G_0 = \{e_1, \ldots, e_{r-3}, e_{r-2} + e_{r-1}, e_{r-1}, e_r, g\}, \quad g = e_1 + \cdots + e_{r-2} + e_r.$$

Since $(e_{r-2} + e_{r-1}, e_{r-1})$ is dependent and (e_r, g) is dependent, there is no $h \in G_0$ such that $G_0 \setminus \{h\}$ is independent. We have

$$\begin{aligned}
W_1 &= \{A \in \mathcal{A}(G_0) \mid \mathsf{k}(A) = 1\} \\
&= \{e_1^2, \ldots, e_{r-3}^2, (e_{r-2} + e_{r-1})^4, e_{r-1}^4, \\
&\qquad\qquad\qquad e_r^4, g^4, (e_{r-2} + e_{r-1})^2 e_{r-1}^2, g^2 e_r^2\}, \\
W_2 &= \{A \in \mathcal{A}(G_0) \mid \mathsf{k}(A) > 1\} \\
&= \{A_1 = g e_r^3 (e_{r-2} + e_{r-1}) e_{r-1}^3 e_1 \cdot \ldots \cdot e_{r-3}, \\
&\qquad B_1 = g e_r^3 (e_{r-2} + e_{r-1})^3 e_{r-1} e_1 \cdot \ldots \cdot e_{r-3}, \\
&\qquad A_3 = g^3 e_r (e_{r-2} + e_{r-1}) e_{r-1}^3 e_1 \cdot \ldots \cdot e_{r-3}, \\
&\qquad B_3 = g^3 e_r (e_{r-2} + e_{r-1})^3 e_{r-1} e_1 \cdot \ldots \cdot e_{r-3}\},
\end{aligned}$$

and $\mathsf{k}(A_1) = \mathsf{k}(A_3) = \mathsf{k}(B_1) = \mathsf{k}(B_3) = (r+1)/2$. Theorem 1.1 implies that $\max \Delta^*(G) = r - 1$, and thus it remains to show that $\min \Delta(G_0) = r - 1$.

For any $d \in \Delta(G_0)$, there exists $B \in \mathcal{B}(G_0)$ with two such factorizations, say

$$B = U_1 \cdot \ldots \cdot U_s V_1 \cdot \ldots \cdot V_t = X_1 \cdot \ldots \cdot X_u Y_1 \cdot \ldots \cdot Y_v$$

where all U_i, V_j, X_k, Y_l are atoms, $s, t, u, v \in \mathbb{N}_0$ with $d = u + v - (s + t)$, $\mathsf{k}(U_1) = \cdots = \mathsf{k}(U_s) = \mathsf{k}(X_1) = \cdots = \mathsf{k}(X_u) = 1$, and $\mathsf{k}(V_1) = \cdots = \mathsf{k}(V_t) = \mathsf{k}(Y_1) = \cdots = \mathsf{k}(Y_v) = (r+1)/2$. This implies that

$$\mathsf{k}(B) = s + t\frac{r+1}{2} = u + v\frac{r+1}{2}$$

and $\mathsf{v}_g(B) \equiv t \equiv v \mod 2$. Since $d = (v+u) - (s+t) = (t-v)\frac{r-1}{2} > 0$, we infer that $t - v \ge 2$ and hence $d \ge r - 1$.

Acknowledgements. The referee read the manuscript twice with utmost care. We would like to thank him/her for all the work which helped to improve the clarity of the arguments and the presentation of the paper. This work was supported by the Austrian Science Fund FWF, Project Number M1641-N26.

References

[1] N. R. Baeth and A. Geroldinger, *Monoids of modules and arithmetic of direct-sum decompositions*, Pacific J. Math. 271 (2014), 257–319.

[2] N. R. Baeth and D. Smertnig, *Factorization theory: From commutative to noncommutative settings*, J. Algebra 441 (2015), 475–551.

[3] N. R. Baeth and R. Wiegand, *Factorization theory and decomposition of modules*, Amer. Math. Monthly 120 (2013), 3–34.

[4] G. W. Chang, *Every divisor class of Krull monoid domains contains a prime ideal*, J. Algebra 336 (2011), 370–377.

[5] S. Chang, S. T. Chapman, and W. W. Smith, *On minimum delta set values in block monoids over cyclic groups*, Ramanujan J. 14 (2007), 155–171.

[6] S. T. Chapman, F. Gotti, and R. Pelayo, *On delta sets and their realizable subsets in Krull monoids with cyclic class groups*, Colloq. Math. 137 (2014), 137–146.

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

[8] W. Gao, Y. Li, J. Peng, C. Plyley, and G. Wang, *On the index of sequences over cyclic groups*, Acta Arith. 148 (2011), 119–134.

[9] W. Gao, J. Peng, and Q. Zhong, *A quantitative aspect of nonunique factorizations: the Narkiewicz constants III*, Acta Arith. 158 (2013), 271–285.

[10] A. Geroldinger, *Additive group theory and non-unique factorizations*, in: Combinatorial Number Theory and Additive Group Theory, A. Geroldinger and I. Ruzsa (eds.), Adv. Courses Math. CRM Barcelona, Birkhäuser, 2009, 1–86.

[11] A. Geroldinger and R. Göbel, *Half-factorial subsets in infinite abelian groups*, Houston J. Math. 29 (2003), 841–858.

[12] A. Geroldinger and F. Halter-Koch, *Congruence monoids*, Acta Arith. 112 (2004), 263–296.

[13] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. 278, Chapman & Hall/CRC, 2006.

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

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

[16] A. Geroldinger and W. A. Schmid, *A characterization of class groups via sets of lengths*, to appear.

[17] A. Geroldinger and W. A. Schmid, *The system of sets of lengths in Krull monoids under set addition*, Rev. Mat. Iberoamer., to appear.

[18] A. Geroldinger and P. Yuan, *The set of distances in Krull monoids*, Bull. London Math. Soc. 44 (2012), 1203–1208.

[19] B. Girard, *Inverse zero-sum problems and algebraic invariants*, Acta Arith. 135 (2008), 231–246.

[20] D. J. Grynkiewicz, *Structural Additive Theory*, Developments Math., Springer, 2013.

[21] Y. O. Hamidoune, *A structure theory for small sum subsets*, Acta Arith. 147 (2011), 303–327.

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

[23] A. Plagne and W. A. Schmid, *On congruence half-factorial Krull monoids with cyclic class group*, submitted.

[24] A. Plagne and W. A. Schmid, *On large half-factorial sets in elementary p-groups: maximal cardinality and structural characterization*, Israel J. Math. 145 (2005), 285–310.

[25] A. Plagne and W. A. Schmid, *On the maximal cardinality of half-factorial sets in cyclic groups*, Math. Ann. 333 (2005), 759–785.

[26] W. A. Schmid, *Arithmetic of block monoids*, Math. Slovaca 54 (2004), 503–526.

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

[28] W. A. Schmid, *Half-factorial sets in finite abelian groups: a survey*, Grazer Math. Ber. 348 (2005), 41–64.

[29] W. A. Schmid, *Half-factorial sets in elementary p-groups*, Far East J. Math. Sci. 22 (2006), 75–114.

[30] W. A. Schmid, *Periods of sets of lengths: a quantitative result and an associated inverse problem*, Colloq. Math. 113 (2008), 33–53.

[31] W. A. Schmid, *Arithmetical characterization of class groups of the form $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ via the system of sets of lengths*, Abh. Math. Sem. Univ. Hamburg 79 (2009), 25–35.

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

[33] D. Smertnig, *Sets of lengths in maximal orders in central simple algebras*, J. Algebra 390 (2013), 1–43.

[34] X. Zeng and P. Yuan, *Two conjectures on an addition theorem*, Acta Arith. 148 (2011), 395–411.

Alfred Geroldinger, Qinghai Zhong
Institute for Mathematics and Scientific Computing
University of Graz
NAWI Graz
Heinrichstrasse 36
8010 Graz, Austria
E-mail: alfred.geroldinger@uni-graz.at
qinghai.zhong@uni-graz.at

Abstract (will appear on the journal's web site only)

Let H be a Krull monoid with class group G. Then every nonunit $a \in H$ can be written as a finite product of atoms, say $a = u_1 \cdot \ldots \cdot u_k$. The set $\mathsf{L}(a)$ of all possible factorization lengths k is called the set of lengths of a. If G is finite, then there is a constant $M \in \mathbb{N}$ such that all sets of lengths are almost arithmetical multiprogressions with bound M and with difference $d \in \Delta^*(H)$, where $\Delta^*(H)$ denotes the set of minimal distances of H. We show that $\max \Delta^*(H) \le \max\{\exp(G) - 2, \mathsf{r}(G) - 1\}$ and that equality holds if every class of G contains a prime divisor, which holds true for holomorphy rings in global fields.