Alfred GEROLDINGER et Qinghai ZHONG

A characterization of class groups via sets of lengths II


<http://jtnb.cedram.org/item?id=JTNB_2017__29_2_327_0>

© Société Arithmétique de Bordeaux, 2017, tous droits réservés.

L’accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/), implique l’accord avec les conditions générales d’utilisation (http://jtnb.cedram.org/legal/). Toute reproduction en tout ou partie de cet article sous quelque forme que ce soit pour tout usage autre que l’utilisation à fin strictement personnelle du copiste est constitutive d’une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.
A characterization of class groups
via sets of lengths II

par Alfred GEROLDINGER et Qinghai ZHONG

Résumé. Soit $H$ un monoïde de Krull avec un groupe des classes fini $G$, et supposons que chaque classe contient un diviseur premier. Si un élément $a \in H$ a une factorisation $a = u_1 \cdots u_k$ en éléments irréductibles $u_1, \ldots, u_k \in H$, alors nous appelons $k$ la longueur de la factorisation et l’ensemble $L(a)$ de toutes les longueurs de factorisation possibles l’ensemble des longueurs de $a$. C’est bien connu que le système $L(H) = \{L(a) \mid a \in H\}$ de tous les ensembles de longueurs ne dépend que du groupe des classes $G$, et c’est bien une conjecture de longue date que, inversement, le système $L(H)$ caractérise le groupe des classes. Nous vérifions la conjecture si le groupe des classes est isomorphe à $C_r^n$ avec $r, n \geq 2$ et $r \leq \max\{2, (n + 2) / 6\}$.

En effet, soit $H'$ un autre monoïde de Krull avec un groupe des classes $G'$ tel que chaque classe contient un diviseur premier, et supposons que $L(H) = L(H')$. Nous montrons que, si l’un des groupes $G$ et $G'$ est isomorphe à $C_r^n$ avec $r, n$ donnés comme ci-dessus, alors $G$ et $G'$ sont isomorphes (à part deux exceptions bien connues).

Abstract. Let $H$ be a Krull monoid with finite class group $G$ and suppose that every class contains a prime divisor. If an element $a \in H$ has a factorization $a = u_1 \cdots u_k$ into irreducible elements $u_1, \ldots, u_k \in H$, then $k$ is called the length of the factorization and the set $L(a)$ of all possible factorization lengths is the set of lengths of $a$. It is classical that the system $L(H) = \{L(a) \mid a \in H\}$ of all sets of lengths depends only on the class group $G$, and a standing conjecture states that conversely the system $L(H)$ is characteristic for the class group. We verify the conjecture if the class group is isomorphic to $C_r^n$ with $r, n \geq 2$ and $r \leq \max\{2, (n + 2) / 6\}$. Indeed, let $H'$ be a further Krull monoid with class group $G'$ such that every class contains a prime divisor and suppose that $L(H) = L(H')$. We prove that, if one of the
groups $G$ and $G'$ is isomorphic to $C_r^n$ with $r, n$ as above, then $G$ and $G'$ are isomorphic (apart from two well-known pairings).

1. Introduction and Main Result

Let $H$ be a Krull monoid with class group $G$ and suppose that every class contains a prime divisor (holomorphy rings in global fields are such Krull monoids and more examples will be given in Section 2). Then every nonunit $a \in H$ can be written as a product of irreducible elements, say $a = u_1 \cdot \ldots \cdot u_k$, and the number of factors $k$ is called the length of the factorization. The set $L(a)$ of all possible factorization lengths is the set of lengths of $a$, and $L(H) = \{L(a) \mid a \in H\}$ is called the system of sets of lengths of $H$ (for convenience we set $L(a) = \{0\}$ if $a$ is an invertible element of $H$). It is easy to check that all sets of lengths are finite and, by definition of the class group, we observe that $H$ is factorial if and only if $|G| = 1$.

By a result due to Carlitz in 1960, we know that $H$ is half-factorial (i.e., $|L| = 1$ for all $L \in L(H)$) if and only if $|G| \leq 2$.

Suppose that $|G| \geq 3$. Then there is some $a \in H$ with $|L(a)| > 1$. If $k, \ell \in L(a)$ with $k < \ell$ and $m \in \mathbb{N}$, then $L(a^m) \supset \{km + \nu(\ell - k) \mid \nu \in [0, m]\}$ which shows that sets of lengths can become arbitrarily large. The monoid $B(G)$ of zero-sum sequences over $G$ is again a Krull monoid with class group isomorphic to $G$, every class contains a prime divisors, and the systems of sets of lengths of $H$ and that of $B(G)$ coincide. Thus $L(H) = L(B(G))$, and it is usual to set $L(G) := L(B(G))$. In particular, the system of sets of lengths of $H$ depends only on the class group $G$. The associated inverse question asks whether or not sets of lengths are characteristic for the class group. More precisely, the Characterization Problem for class groups can be formulated as follows (see [8, Section 7.3], [11, p. 42], [22], and Proposition 2.1)):

Given two finite abelian groups $G$ and $G'$ such that $L(G) = L(G')$. Does it follow that $G \cong G'$?

The system of sets of lengths $L(G)$ is studied with methods from additive combinatorics. In particular, zero-sum theoretical invariants (such as the Davenport constant or the cross number) and the associated inverse problems play a crucial role. Most of these invariants are well-understood only in a very limited number of cases (e.g., for groups of rank two, the precise value of the Davenport constant $D(G)$ is known and the associated inverse problem is solved; however, if $n$ is not a prime power and $r \geq 3$, then the value of the Davenport constant $D(C_r^n)$ is unknown). Thus it is not surprising that affirmative answers to the Characterization Problem so far have been restricted to those groups where we have a good understanding of the Davenport constant. These groups include elementary 2-groups, cyclic
groups, and groups of rank two (the latter were recently handled in [13]; for a variety of partial results we refer to [20, 23, 21]).

The goal of the present note is to solve the Characterization Problem for groups of the form $C_n^r$ if the exponent is large with respect to the rank. Here is our main theorem.

**Theorem 1.1.** Let $G$ be an abelian group such that $\mathcal{L}(G) = \mathcal{L}(C_n^r)$ where $r, n \in \mathbb{N}$ with $n \geq 2$, $(n, r) \notin \{(2,1), (2,2), (3,1)\}$, and $r \leq \max\{2, (n + 2)/6\}$. Then $G \cong C_n^r$.

The groups $C_n^r$, where $r, n$ are as above, are the first groups at all for which the Characterization Problem is solved whereas the Davenport constant is unknown. This is made possible by a detailed study of the set of minimal distances

$$\Delta^*(G) = \{\min \Delta(G_0) \mid G_0 \subset G \text{ is a non-half-factorial subset}\}$$

and the associated minimal non-half-factorial subsets. Sets of minimal distances have been investigated by Chapman, Grynkiewicz, Hamidoune, Plagne, Schmid, Smith, and others (see [8, Section 6.8] for some basic information and [9, 19, 5, 21, 3, 15, 18] for recent progress). In Section 2 we repeat some key facts on Krull monoids and gather the required machinery, and in Section 3 we study structural properties of (large) minimal non-half-factorial sets. The proof of Theorem 1.1 will be provided in Section 4 where we also give a positive answer to the Characterization Problem for all groups $G$ with Davenport constant $D(G) \in [4, 11]$ (Proposition 4.1).

2. Background on Krull monoids and their sets of minimal distances

Our notation and terminology are consistent with [8, 12]. We denote by $\mathbb{N}$ the set of positive integers, and for $a, b \in \mathbb{Q}$, we denote by $[a, b] = \{x \in \mathbb{Q} \mid a \leq x \leq b\}$ the discrete, finite interval between $a$ and $b$. If $A, B \subset \mathbb{Z}$ are subsets of the integers, then $A + B = \{a + b \mid a \in A, b \in B\}$ denotes their sumset, and $\Delta(A)$ 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 $d, l \in \mathbb{N}$ 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 $L'' \subset \max L^* + [1, M]$.

By a monoid we mean a commutative semigroup with identity which satisfies the cancellation laws. A monoid $F$ is called free abelian with basis $P \subset F$, and we write $F = F(P)$, if every $a \in F$ has a unique representation
of the form
\[ a = \prod_{p \in P} p^{v_p(a)} \] with \( v_p(a) \in \mathbb{N}_0 \) and \( v_p(a) = 0 \) for almost all \( p \in P \).

A monoid \( H \) is said to be a Krull monoid if it satisfies one of the following two equivalent conditions (see [8, Theorem 2.4.8]).

(a) \( H \) is \( v \)-noetherian and completely integrally closed.

(b) There exists a monoid homomorphism \( \varphi: H \to F = F(P) \) into a free abelian monoid \( F \) such that \( a \mid b \) in \( H \) if and only if \( \varphi(a) \mid \varphi(b) \) in \( F \).

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 ([8, Section 2.11 and Examples 7.4.2]). Monoid domains and power series domains that are Krull are discussed in [17, 4], and note that every class of a Krull monoid domain contains a prime divisor. For monoids of modules that are Krull and their distribution of prime divisors, we refer the reader to [6, 1].

Sets of lengths in Krull monoids can be studied in the monoid of zero-sum sequences over its class group. Let \( G \) be an additively written abelian group and \( G_0 \subset G \) a subset. An element
\[ S = g_1 \cdot \ldots \cdot g_\ell = \prod_{g \in G_0} g^{v_g(S)} \in F(G_0) \]
is called a sequence over \( G_0 \), and we use all notations as in [16]. In particular, \( \sigma(S) = g_1 + \ldots + g_\ell \) denotes the sum, \( |S| = \ell \) the length, \( h(S) = \max \{ v_g(S) \mid g \in G_0 \} \) the maximal multiplicity, \( \text{supp}(S) = \{ g_1, \ldots, g_\ell \} \subset G_0 \) the support, and \( k(S) = \sum_{i=1}^\ell 1/\text{ord}(g_i) \) the cross number of \( S \). The monoid
\[ B(G_0) = \{ S \in F(G_0) \mid \sigma(S) = 0 \} \]
is the monoid of zero-sum sequences over \( G_0 \), and since the embedding \( B(G_0) \hookrightarrow F(G_0) \) satisfies Condition (b) above, \( B(G_0) \) is a Krull monoid. As usual, we write \( \mathcal{L}(G_0) = \mathcal{L}(B(G_0)) \) for the system of sets of lengths of \( B(G_0) \) and \( \mathcal{A}(G_0) = \mathcal{A}(B(G_0)) \) for the set of atoms (the set of irreducible elements) of \( B(G_0) \). Note that the atoms of \( B(G_0) \) are precisely the minimal zero-sum sequences over \( G_0 \), and
\[ D(G_0) = \sup\{ |U| \mid U \in \mathcal{A}(G_0) \} \in \mathbb{N} \cup \{ \infty \} \]
is the Davenport constant of \( G_0 \). The significance of the system of sets of lengths \( \mathcal{L}(G) \) (and hence of the Characterization Problem in the formulation given in the Introduction) stems from its universal role which can be seen from the following proposition.
Proposition 2.1.

(1) If $H$ is a Krull monoid with class group $G$ such that each class contains a prime divisor, then $\mathcal{L}(H) = \mathcal{L}(G)$.

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

(3) Let $H$ be a seminormal order in a holomorphy ring of a global field with principal order $\tilde{H}$ such that the natural map $\mathfrak{X}(\tilde{H}) \to \mathfrak{X}(H)$ is bijective and there is an isomorphism $\overline{\mathfrak{f}}: \mathfrak{C}_v(H) \to \mathfrak{C}_v(\tilde{H})$ between the $v$-class groups. Then $\mathcal{L}(H) = \mathcal{L}(G)$, where $G = \mathfrak{C}_v(H)$ is finite abelian.

Proof.

(1) See [8, Section 3.4].

(2) See [24, Theorem 1.1], and [2] for related results of this flavor.

(3) See [10, Theorem 5.8] for a more general result in the setting of weakly Krull monoids. □

Next we discuss sets of distances and minimal sets of distances. Let

$$
\Delta(G) = \bigcup_{L \in \mathcal{L}(G)} \Delta(L) \subset \mathbb{N}
$$

denote the set of distances of $G$. Then $G$ is called half-factorial if $\Delta(G) = \emptyset$. Otherwise, $G$ is called non-half-factorial and we have $\min \Delta(G) = \gcd \Delta(G)$. Note that $G$ is half-factorial if and only if $k(A) = 1$ for all $A \in \mathcal{A}(G)$. Furthermore, the set $G$ is called

- minimal non-half-factorial if it is half-factorial and every proper subset $G_1 \subsetneq G$ is half-factorial.
- an LCN-set if $k(A) \geq 1$ for all $A \in \mathcal{A}(G)$.

The set $\Delta(G)$ is an interval and its maximum is studied in [7]. The following two subsets of $\Delta(G)$, the set of minimal distances $\Delta^*(G)$ and the set $\Delta_1(G)$, play a crucial role in the present paper. We define

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

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

and we denote by $\Delta_1(G)$ 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 $l \geq k$.

Thus, by definition, if $G'$ is a further finite abelian group such that $\mathcal{L}(G) = \mathcal{L}(G')$, then $\Delta_1(G) = \Delta_1(G')$. The next proposition gathers the properties of $\Delta^*(G)$ and of $\Delta_1(G)$ which are needed in the sequel.
Proposition 2.2. Let $G$ be a finite abelian group with $|G| \geq 3$ and $\text{exp}(G) = n$.

1. $\Delta^*(G) \subset \Delta_1(G) \subset \{d_1 \in \Delta(G) \mid d_1 \text{ divides some } d \in \Delta^*(G)\}$. In particular, $\max \Delta^*(G) = \max \Delta_1(G)$.

2. $\max \Delta^*(G) = \max \{\exp(G) - 2, \text{m}(G)\} = \max \{\exp(G) - 2, \text{r}(G) - 1\}$. If $G$ is a $p$-group, then $\text{m}(G) = \text{r}(G) - 1$.

3. If $k \in \mathbb{N}$ is maximal such that $G$ has a subgroup isomorphic to $C_k^n$, then

$$\Delta_1(G) \subset [1, \max \{\text{m}(G), \lfloor \frac{n}{2} \rfloor - 1\} ] \cup [\max \{1, n - k - 1\}, n - 2].$$

and

$$[1, \text{r}(G) - 1] \cup [\max \{1, n - k - 1\}, n - 2] \subset \Delta_1(G).$$

Proof. (1) follows from [8, Corollary 4.3.16] and (2) from [15, Theorem 1.1 and Proposition 3.2].

Let us prove (3). In [21, Theorem 3.2], it is proved that $\Delta^*(G)$ is contained in the set given above. Since this set contains all its divisors, $\Delta_1(G)$ is contained in it by 1. The set $[1, \text{r}(G) - 1] \cup [\max \{1, n - k - 1\}, n - 2]$ is contained in $\Delta_1(G)$ by [8, Propositions 4.1.2 and 6.8.2].

3. Minimal non-half-factorial subsets

Throughout this section, let $G$ be an additive finite abelian group with $|G| \geq 3$, $\text{exp}(G) = n$, and $\text{r}(G) = r$.

The following two technical lemmas will be used throughout the manuscript.

Lemma 3.1. Let $G_0 \subset G$ be a subset.

1. For each $g \in G_0$,

$$\gcd \{v_g(B) \mid B \in \mathcal{B}(G_0)\} = \gcd \{v_g(A) \mid A \in \mathcal{A}(G_0)\}$$

$$= \min \{v_g(A) \mid v_g(A) > 0, A \in \mathcal{A}(G_0)\}$$

$$= \min \{v_g(B) \mid v_g(B) > 0, B \in \mathcal{B}(G_0)\}$$

$$= \min \{k \in \mathbb{N} \mid kg \in \langle G_0 \setminus \{g\} \rangle\}$$

$$= \gcd \{k \in \mathbb{N} \mid kg \in \langle G_0 \setminus \{g\} \rangle\}.$$  

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

2. Suppose that for each two distinct elements $h, h' \in G_0$ we have $h \not\in \langle G_0 \setminus \{h, h'\} \rangle$. Then for any atom $A$ with $\text{supp}(A) \subsetneq G_0$ and any $h \in \text{supp}(A)$, we have $\gcd(v_h(A), \text{ord}(h)) > 1$. 

(3) 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 $\theta: B(G_0) \to B(G_0^*)$ such that the following properties are satisfied:

(a) For each $g \in G_0^*$, we have $g \in \langle G_0^* \setminus \{g\} \rangle$.
(b) For each $B \in B(G_0)$, we have $k(B) = k(\theta(B))$.
(c) If $G_0^*$ has the property that for each $h \in G_0^*$, $h \notin \langle E \rangle$ for any $E \subset G_0^* \setminus \{h\}$, then $G_0$ also has the property.

Proof. See [8, Proposition 6.8.2 and Lemmas 6.8.5 and 6.8.6].

Lemma 3.2.

(1) If $g \in G$ with $\text{ord}(g) \geq 3$, then $\text{ord}(g) - 2 \leq \Delta^*(G)$. In particular, $n - 2 \leq \Delta^*(G)$.
(2) If $r \geq 2$, then $[1, r - 1] \subset \Delta^*(G)$.
(3) Let $G_0 \subset G$ be a subset.

(a) If there exists an $U \in \mathcal{A}(G_0)$ with $k(U) < 1$, then min $\Delta(G_0) \leq \exp(G) - 2$.
(b) If $G_0$ is an LCN-set, then min $\Delta(G_0) \leq |G_0| - 2$.

Proof. See [8, Proposition 6.8.2 and Lemmas 6.8.5 and 6.8.6].

Lemma 3.3. Let $G_0 \subset G$ be a subset, $g \in G_0$, and $s$ the smallest integer such that $sg \in \langle G_0 \setminus \{g\} \rangle$, and suppose that $s < \text{ord}(g)$. Then $\text{ord}(sg) > 1$ and for each prime $p$ dividing $\text{ord}(sg)$, there exists an atom $A \in \mathcal{A}(G_0)$ with $2 \leq |\text{supp}(A)| \leq r(G) + 1$, $s \leq v_g(A) \leq \text{ord}(g)/2$, and $p \nmid \frac{v_g(A)}{s}$. In particular,

(1) If $|G_0| \geq r(G) + 2$, then there exist $s_0 < \text{ord}(g)$ and $E \subset G_0 \setminus \{g\}$ such that $s_0g \in \langle E \rangle$.
(2) If $s = 1$ and $\text{ord}(g)$ is a prime power, then there exists a subset $E \subset G_0 \setminus \{g\}$ with $|E| \leq r(G)$ such that $g \in \langle E \rangle$.

Proof. We set $\exp(G) = n = p_1^{k_1} \cdot \cdots \cdot p_t^{k_t}$, where $t, k_1, \ldots, k_t \in \mathbb{N}$ and $p_1, \ldots, p_t$ are distinct primes. Since $s < \text{ord}(g)$, we have that $\text{ord}(sg) > 1$. Let $\nu \in [1, t]$ with $p_\nu | \text{ord}(sg)$. Since $sg \in \langle G_0 \setminus \{g\} \rangle$, it follows that $0 \neq \frac{n}{p_\nu} sg \in G_\nu = \langle \frac{n}{p_\nu} h \mid h \in G_0 \setminus \{g\} \rangle$. Obviously, $G_\nu$ is a $p_\nu$-group. Let $E_\nu \subset G_0 \setminus \{g\}$ be minimal such that $\frac{n}{p_\nu} sg \in \langle \frac{n}{p_\nu} E_\nu \rangle$. Since $\langle \frac{n}{p_\nu} E_\nu \rangle \subset G_\nu$ and $G_\nu$ is a $p_\nu$-group, it follows that

$$1 \leq |E_\nu| = \left| \frac{n}{p_\nu} E_\nu \right| \leq r(G_\nu) \leq r(G).$$

Let $d_\nu \in \mathbb{N}$ be minimal such that $d_\nu g \in \langle E_\nu \rangle$. Since $0 \neq \frac{n}{p_\nu} sg \in \langle E_\nu \rangle$, it follows that $d_\nu < \text{ord}(g)$. By Lemma 3.1(1), $d_\nu | \text{gcd}(\frac{n}{p_\nu} s, \text{ord}(g))$ and there exists an atom $U_\nu$ such that $v_g(U_\nu) = d_\nu$ and $|\text{supp}(U_\nu) \setminus \{g\}| \leq |E_\nu| \leq r(G)$. 

A characterization of class groups via sets of lengths II 333
Since $\nu_g(U_\nu) = d_\nu < \operatorname{ord}(g)$, it follows that $|\operatorname{supp}(U_\nu)| \geq 2$. By the minimality of $s$ and $d_\nu \mid \frac{n}{p_\nu} s$, we have that $s \mid d_\nu$ and $p_\nu \nmid \frac{n}{s}$.

If $|G_0| \geq r(G) + 2$, then $|E_\nu| \leq r(G) < |G_0 \setminus \{g\}|$ implies that $E_\nu \subset G_0 \setminus \{g\}$, and the assertion holds with $E = E_\nu$ and $s_0 = d_\nu$.

If $s = 1$ and $\operatorname{ord}(g)$ is a prime power, then $\operatorname{ord}(g)$ is a power of $p_\nu$ which implies that $\gcd(\frac{n}{p_\nu} s, \operatorname{ord}(g)) = 1$ whence $d_\nu = 1$ and $g \in (E_\nu)$. □

**Lemma 3.4.** Let $G_0 \subset G$ be a minimal non-half-factorial LCN-set with $|G_0| \geq r + 2$. Suppose that for any $h \in G_0$, $h \not\in (G_0 \setminus \{h\})$ but $h \not\in (G_0 \setminus \{h, h'\})$ for any $h' \in G_0 \setminus \{h\}$. Then $|G_0| \leq r + \frac{n}{2}$. In particular, if each atom $A \in A(G_0)$ with $\operatorname{supp}(A) = G_0$ has cross number $k(A) > 1$, then $\min \Delta(G_0) \leq \frac{5n}{6} - 4$.

**Proof.** We choose an element $g \in G_0$. If $\operatorname{ord}(g)$ is a prime power, then there exists $E \subset G_0 \setminus \{g\}$ such that $g \in (E)$ and $|E| \leq r < |G_0| - 1$ by Lemma 3.3, a contradiction to the assumption on $G_0$. Thus $\operatorname{ord}(g)$ is not a prime power. Let $s \in \mathbb{N}$ be minimal such that there exists a subset $E \subset G_0 \setminus \{g\}$ with $sg \in (E)$, and by Lemma 3.3(1), we observe that $s < \operatorname{ord}(g)$.

Let $E \subset G_0 \setminus \{g\}$ be minimal such that $sg \in (E)$. By Lemma 3.1(1), there is an atom $V$ with $\nu_g(V) = s \mid \operatorname{ord}(g)$ and $\operatorname{supp}(V) = \{g\} \cup E \subset G_0$. By Lemma 3.1(2), for each $h \in \operatorname{supp}(V)$, $\nu_h(V) \geq 2$. Since $G_0$ is a minimal non-half-factorial LCN set, we obtain that

$$1 = k(V) \geq \frac{2}{n}(|E| + 1),$$

whence $|E| \leq \frac{n}{2} - 1$.

Since $s \geq 2$, there is a prime $p \in \mathbb{N}$ dividing $s$ and hence $p \mid s \mid \operatorname{ord}(g)$.

By Lemma 3.3, there exists an atom $U_1$ such that $|\operatorname{supp}(U_1)| \leq r + 1$ and $p \nmid \nu_g(U_1)$, and therefore $\operatorname{supp}(U_1) \subset G_0$.

Let $d = \gcd(s, \nu_g(U_1))$ and $E_1 = \operatorname{supp}(U_1) \setminus \{g\}$. Then $d < s$ and $dg \in (sg, \nu_g(U_1)g) \subset (E \cup E_1) \subset (G_0 \setminus \{g\})$. The minimality of $s$ implies that $E \cup E_1 = G_0 \setminus \{g\}$, and thus $|G_0| \leq 1 + |E| + |E_1| \leq 1 + r + \frac{n}{2} - 1 = r + \frac{n}{2}$.

Suppose that each atom $A \in A(G_0)$ with $\operatorname{supp}(A) = G_0$ has cross number $k(A) > 1$. There exist $x_1 \in [1, \frac{\operatorname{ord}(g)}{s} - 1]$ and $x_2 \in [1, \frac{\operatorname{ord}(g)}{\nu_g(U_1)} - 1]$ such that $dg = x_1 sg + x_2 \nu_g(U_1)g$. Thus $d + y \operatorname{ord}(g) = x_1 s + x_2 \nu_g(U_1)$ with some $y \in \mathbb{N}_0$. Let $V^{x_1 U_1^{x_2}} = (g^{\operatorname{ord}(g)})^y \cdot W$, where $W \in \mathcal{B}(G)$ with $\nu_g(W) = d$, and let $W_1$ be an atom dividing $W$ with $\nu_g(W_1) > 0$. Since $\nu_g(W_1) \leq d < s$, the minimality of $s$ implies that $\operatorname{supp}(W_1) = G_0$ and hence $k(W_1) > 1$. Since $G_0$ is minimal non-half-factorial, we have that $k(V) = k(U_1) = 1$. Therefore there exists $l \in \mathbb{N}$ with $2 \leq l < x_1 + x_2$ such that $\{l, x_1 + x_2\} \subset L(V^{x_1 U_1^{x_2}})$. Then

$$\min \Delta(G_0) \leq x_1 + x_2 - l \leq \frac{\operatorname{ord}(g)}{s} + \frac{\operatorname{ord}(g)}{\nu_g(U_1)} - 4 \leq \frac{5n}{6} - 4.$$

□
For our next result we need the following technical lemma.

**Lemma 3.5.** Let \( G_0 \subset G \) be a non-half-factorial subset satisfying the following two conditions:

1. There is some \( g \in G_0 \) such that \( \Delta(G_0 \setminus \{g\}) = \emptyset \).
2. There is some \( U \in \mathcal{A}(G_0) \) with \( k(U) = 1 \) and \( \gcd(v_g(U), \text{ord}(g)) = 1 \).

Then \( k(\mathcal{A}(G_0)) \subset \mathbb{N} \) and

\[
\min \Delta(G_0) \mid \gcd(k(A) - 1 \mid A \in \mathcal{A}(G_0)) = 0.
\]

Note that the conditions hold if \( \Delta(G_1) = \emptyset \) for each \( G_1 \subsetneq G_0 \) and there exists some \( G_2 \) such that \( \langle G_2 \rangle = \langle G_0 \rangle \) and \( |G_2| \leq |G_0| - 2 \).

**Proof.** The first statement follows from [8, Lemma 6.8.5]. If \( \Delta(G_1) = \emptyset \) for all \( G_1 \subsetneq G_0 \), then Condition (a) holds. Let \( G_2 \subsetneq G_1 \subsetneq G_0 \) with \( \langle G_2 \rangle = \langle G_0 \rangle \). If \( g \in G_1 \setminus G_2 \), then \( \langle G_2 \rangle = \langle G_0 \rangle \) implies that there is some \( U \in \mathcal{A}(G_1) \) with \( v_g(U) = 1 \), and since \( G_1 \subsetneq G_0 \), it follows that \( k(U) = 1 \). \( \square \)

**Lemma 3.6.** Suppose that \( \exp(G) = n \) is not a prime power. Let \( G_0 \subset G \) be a minimal non-half-factorial LCN-set with \( |G_0| \geq r + 2 \) such that \( h \in \langle G_0 \setminus \{h\} \rangle \) for every \( h \in G_0 \). Suppose that one of the following properties is satisfied:

1. For each two distinct elements \( h, h' \in G_0 \), we have \( h \not\in \langle G_0 \setminus \{h, h'\} \rangle \), and there is an atom \( A \in \mathcal{A}(G_0) \) with \( k(A) = 1 \) and \( \text{supp}(A) = G_0 \).
2. There is a subset \( G_2 \subset G_0 \) such that \( \langle G_2 \rangle = \langle G_0 \rangle \) and \( |G_2| \leq |G_0| - 2 \).

Then \( \min \Delta(G_0) \leq \frac{n+r-3}{2} \).

**Proof.** Assume to the contrary that \( \min \Delta(G_0) \geq \frac{n+r}{2} - 1 \). Then Lemma 3.2(3b) implies that \( |G_0| \geq \frac{n+r}{2} + 1 \). If Property (a) is satisfied, then there exists some \( g \in G_0 \) such that \( v_g(A) = 1 \). By Lemma 3.5, each of the two Properties (a) and (b) implies that \( k(U) \in \mathbb{N} \) for each \( U \in \mathcal{A}(G_0) \) and \( \min \Delta(G_0) \mid \gcd(\{k(U) - 1 \mid U \in \mathcal{A}(G_0)\}) \).

We set

\[
\Omega_{=1} = \{ A \in \mathcal{A}(G_0) \mid k(A) = 1 \} \quad \text{and} \quad \Omega_{>1} = \{ A \in \mathcal{A}(G_0) \mid k(A) > 1 \}.
\]

Thus for each \( U_1, U_2 \in \Omega_{>1} \) we have

\[
(3.1) \quad k(U_1) \geq \frac{n + r}{2} \quad \text{and} \quad \text{(either } k(U_1) = k(U_2) \text{ or } |k(U_1) - k(U_2)| \geq \frac{n + r}{2} - 1 \text{).}
\]

Furthermore, for each \( U \in \Omega_{=1} \) we have \( h(U) \geq 2 \) (otherwise, \( U \) would divide every atom \( U_1 \in \Omega_{>1} \)). We claim that
A1. For each \( U \in \Omega_{>1} \), there are \( A_1, \ldots, A_m \in \Omega_{=1} \), where \( m \leq \frac{n+1}{2} \), such that \( UA_1 \cdots A_m \) can be factorized into a product of atoms from \( \Omega_{=1} \).

Proof of A1. Suppose that Property (a) holds. As observed above there exists some \( g \in G_0 \) such that \( v_g(A) = 1 \). Lemma 3.3 implies that there is an atom \( X \) such that \( 2 \leq |\text{supp}(X)| \leq r(G) + 1 \) and \( 1 \leq v_g(X) \leq \text{ord}(g)/2 \). Since \( g \not\in \langle G_0 \setminus \{g, h\} \rangle \) for any \( h \in G_0 \setminus \{g\} \), it follows that \( v_g(X) \geq 2 \), and \(|G_0| \geq r + 2 \) implies supp\((X) \subsetneq G_0 \).

Suppose that Property (b) is satisfied. We choose an element \( g \in G_0 \setminus G_2 \). Then \( g \in (G_2) \) and by Lemma 3.1(1), there is an atom \( A' \) with \( v_g(A') = 1 \) and supp\((A') \subset G_2 \setminus \{g\} \subsetneq G_0 \). This implies that \( A' \in \Omega_{=1} \). Let \( h \in G_0 \) such that \( v_h(A') = h(A') \). Since \( h(A') \geq 2 \), we obtain that \( A'[\frac{\text{ord}(h)}{\text{ord}(A')} - 1] \) atoms and \( v_g(W) = \frac{\text{ord}(h)}{\text{ord}(A')} \). Thus there exists an atom \( X' \) with \( 2 \leq v_g(X') \leq \frac{\text{ord}(h)}{\text{ord}(A')} \leq \frac{n}{2} + 1 \).

Therefore both properties imply that there are \( A, X \in \mathcal{A}(G_0) \) and \( g \in G_0 \) such that \( k(A) = k(X) = 1 \), \( v_g(A) = 1 \), and \( 2 \leq v_g(X) \leq \frac{n}{2} + 1 \). Let \( U \in \Omega_{>1} \).

If \( \text{ord}(g) - v_g(U) < v_g(X) \leq \frac{n}{2} + 1 \), then
\[
UA^{\text{ord}(g) - v_g(U)} = g^{\text{ord}(g)} S,
\]
where \( S \in B(G_0) \) and \( \text{ord}(g) - v_g(U) \leq \frac{n}{2} \). Since supp\((S) \subsetneq G_0 \), \( S \) is a product of atoms from \( \Omega_{=1} \).

If \( \text{ord}(g) - v_g(U) \geq v_g(X) \), then
\[
UX^{\frac{\text{ord}(g) - v_g(U)}{v_g(X)}} A^{\text{ord}(g) - v_g(U) - v_g(X)} = g^{\text{ord}(g)} S,
\]
where \( S \) is a product of atoms from \( \Omega_{=1} \) (because supp\((S) \subsetneq G_0 \)) and
\[
\left[\frac{\text{ord}(g) - v_g(U)}{v_g(X)}\right] + \text{ord}(g) - v_g(U) - v_g(X) \cdot \left[\frac{\text{ord}(g) - v_g(U)}{v_g(X)}\right] \\
\leq \frac{(\text{ord}(g) - v_g(U)) - (v_g(X) - 1)}{v_g(X)} + v_g(X) - 1 \\
\leq \frac{\text{ord}(g) - v_g(U) + 1}{2} \leq \frac{n + 1}{2}.
\]

We set
\[
\Omega'_{>1} = \{ A \in \mathcal{A}(G_0) \mid k(A) = \min\{k(B) \mid B \in \Omega'_{>1}\} \} \subset \Omega_{>1},
\]
and we consider all tuples \((U, A_1, \ldots, A_m)\), where \( U \in \Omega'_{>1} \) and \( A_1, \ldots, A_m \in \Omega_{=1} \), such that \( UA_1 \cdots A_m \) can be factorized into a product of atoms from \( \Omega_{=1} \). We fix one such tuple \((U, A_1, \ldots, A_m)\) with the property that \( m \) is minimal possible. Let
\[ (3.2) \ UA_1 \cdots A_m = V_1 \cdots V_t \quad \text{with} \quad t \in \mathbb{N} \quad \text{and} \quad V_1, \ldots, V_t \in \Omega_{=1}. \]
We observe that \( k(U) = t - m \) and continue with the following assertion.

**A2.** For each \( \nu \in [1, t] \), we have \( V_\nu \upharpoonright U A_1 \cdot \ldots \cdot A_{m-1} \).

**Proof of A2.** Assume to the contrary that there is such a \( \nu \in [1, t] \), say \( \nu = 1 \), with \( V_1 \upharpoonright U A_1 \cdot \ldots \cdot A_{m-1} \). Then there are \( l \in \mathbb{N} \) and \( T_1, \ldots, T_l \in \mathcal{A}(G_0) \) such that

\[ U A_1 \cdot \ldots \cdot A_{m-1} = V_1 T_1 \cdot \ldots \cdot T_l. \]

By the minimality of \( m \), there exists some \( \nu \in [1, l] \) such that \( T_\nu \in \Omega_{>1} \), say \( \nu = 1 \). Since

\[ \sum_{\nu=2}^{l} k(T_\nu) = k(U) + (m - 1) - 1 - k(T_1) \leq m - 2 \leq \frac{n - 3}{2}, \]

and \( k(T') \geq \frac{r + n}{2} \) for all \( T' \in \Omega_{>1} \), it follows that \( T_2, \ldots, T_l \in \Omega_{=1} \), whence \( l = 1 + \sum_{\nu=2}^{l} k(T_\nu) \leq m - 1 \). We obtain that

\[ V_1 T_1 \cdot \ldots \cdot T_l A_m = U A_1 \cdot \ldots \cdot A_m = V_1 \cdot \ldots \cdot V_l, \]

and thus

\[ T_1 \cdot \ldots \cdot T_l A_m = V_2 \cdot \ldots \cdot V_l. \]

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

\[ k(T_1) - k(U) = m - 1 - l \leq m - 2 \leq \frac{n - 3}{2} \leq \frac{r + n}{2} - 1 \leq k(T_1) - k(U), \]

a contradiction. \( \square \)

By Equation (3.2), there are \( X_1, Y_1, \ldots, X_t, Y_t \in \mathcal{F}(G) \) such that

\[ U A_1 \cdot \ldots \cdot A_{m-1} = X_1 \cdot \ldots \cdot X_t, \]

\[ A_m = Y_1 \cdot \ldots \cdot Y_t, \]

and \( V_i = X_i Y_i \) for each \( i \in [1, t] \).

Then A2 implies that \( |Y_i| \geq 1 \) for each \( i \in [1, t] \), and we set \( \alpha = \{|i \in [1, t] \mid |Y_i| = 1\}|. \) If \( \alpha \leq m + r \), then

\[ n \geq |A_m| = |Y_1| + \ldots + |Y_t| \geq \alpha + 2(t - \alpha) = 2t - \alpha \geq 2t - m - r, \]

and hence \( \min \Delta(G_0) \leq t - 1 - m \leq \frac{r + n - 3}{2} \), a contradiction. Thus \( \alpha \geq m + r + 1 \). After renumbering if necessary we assume that \( 1 = |Y_1| = \ldots = |Y_\alpha| < |Y_{\alpha+1}| \leq \ldots \leq |Y_t| \). Let \( Y_i = y_i \) for each \( i \in [1, \alpha] \) and

\[ S_0 = \{y_1, y_2, \ldots, y_\alpha\}. \]

For every \( i \in [1, \alpha] \), \( V_i \upharpoonright y_i U A_1 \cdot \ldots \cdot A_{m-1} \) whence \( v_{y_i}(V_i) \leq 1 + v_{y_i}(U A_1 \cdot \ldots \cdot A_{m-1}) \) and since \( V_1 \upharpoonright U A_1 \cdot \ldots \cdot A_{m-1} \), it follows that

\[ v_{y_i}(V_i) = v_{y_i}(U A_1 \cdot \ldots \cdot A_{m-1}) + 1. \]

Assume to the contrary that there are distinct \( i, j \in [1, \alpha] \) such that \( y_i = y_j \). Then

\[ v_{y_i}(U A_1 \cdot \ldots \cdot A_{m-1}) + 1 = v_{y_i}(V_i) = v_{y_i}(X_i) + 1 = v_{y_i}(V_j) = v_{y_i}(X_j) + 1. \]
Since $X_iX_j | UA_1 \cdots A_{m-1}$, we infer that

$$\nu_{g_i}(UA_1 \cdots A_{m-1}) \geq \nu_{g_i}(X_iX_j) = \nu_{g_i}(V_iV_j) - 2 = 2\nu_{g_i}(UA_1 \cdots A_{m-1}),$$

which implies that $\nu_{g_i}(UA_1 \cdots A_{m-1}) = 0$, a contradiction to $\operatorname{supp}(U) = G_0$. Thus $|S_0| = \alpha$ and

$$(3.5) \quad |\operatorname{supp}(A_m)| \geq |S_0| = \alpha \geq m + r + 1.$$  

We proceed by the following two assertions.

**A3.** There exist $g' \in G_0$ and $A' \in A(G_0)$ with $k(A') = 1$ satisfying the following three conditions:

1. $(C1)$ $\nu_{g'}(A') < \ord(g')$ is the smallest positive integer $\gamma$ such that $\gamma g' \in \langle \operatorname{supp}(A') \setminus \{g'\} \rangle$;
2. $(C2)$ $\nu_{g'}(A')g' \notin (E)$ for any $E \subset \operatorname{supp}(A') \setminus \{g'\}$.
3. $(C3)$ $UA_1 \cdots A_{m-1} \cdot A'$ can be factorized into a product of atoms from $\Omega_{=1}$.

**Proof of A3.** Suppose that Property (a) is satisfied. As observed at the beginning of the proof, there is a $g \in G_0$ such that $\nu_g(A) = 1$. We choose $A' = A$ and $g' = g$, and we need to prove that $UA_1 \cdots A_{m-1} \cdot A$ can be factorized into a product of atoms from $\Omega_{=1}$. Since $S_0 \subset \operatorname{supp}(A) = G_0$, then $V_1 \cdots V_\alpha | UA_1 \cdots A_{m-1} \cdot A$ and hence $k(UA_1 \cdots A_{m-1} \cdot A(V_1 \cdots V_\alpha)^{-1}) < k(U)$. The minimality of $k(U)$ implies that $UA_1 \cdots A_{m-1} \cdot A$ can be factorized into a product of atoms from $\Omega_{=1}$.

Suppose that Property (b) satisfied. We choose $g' = y_1$ (see Equation (3.3)) and distinguish two cases. First, suppose that there exists a subset $E \subset G_0 \setminus \{y_1\}$ such that $y_1 \in \langle E \rangle$. Choose a minimal subset $E$ with this property. By Lemma 3.1(1), there exists an atom $A'$ satisfying the two conditions (C1) and (C2) with $k(A') = 1$ and $\nu_{y_1}(A') = 1$. Since $\nu_{y_1}(V_1) = \nu_{y_1}(UA_1 \cdots A_{m-1}) + 1$ by Equation (3.4) and $V_1 | UA_1 \cdots A_{m-1} \cdot y_1$, we obtain that $|\operatorname{supp}(UA_1 \cdots A_{m-1} \cdot A'(V_1)^{-1})| < |G_0|$ and hence $UA_1 \cdots A_{m-1} \cdot A'$ can be factorized into a product of atoms from $\Omega_{=1}$.

Now we suppose that $y_1 \notin \langle E \rangle$ for any $E \subset G_0 \setminus \{y_1\}$. Let $s_0 \in \mathbb{N}$ be minimal such that there exists a subset $E \subset G_0 \setminus \{y_1\}$ such that $s_0y_1 \in \langle E \rangle$, and by Lemma 3.3(1), we observe that $s_0 < \ord(g)$. Let $E$ be a minimal subset with this property. Thus, by Lemma 3.1(1), there exists an atom $A'$ with $\nu_{y_1}(A') = s_0$ satisfying the two conditions (C1) and (C2). Since $\operatorname{supp}(A') \subset G_0$, we have $k(A') = 1$. We distinguish two cases:

**Case 1:** $|S_0 \setminus \operatorname{supp}(A')| \geq r + 1$.

Since $s_0 \geq 2$, there is a prime $p$ dividing $s_0$. Since by assumption, $y_1 \in \langle G_0 \setminus \{y_1\} \rangle$, Lemma 3.3 implies that there exists an atom $A'_p$ such that $|\operatorname{supp}(A'_p)| \leq r + 1 < |G_0|$, $1 \leq \nu_{y_1}(A'_p) \leq \ord(y_1)/2$, and $p \nmid \nu_{y_1}(A'_p)$. 


Let $d = \gcd(s_0, \nu_{y_1}(A'_p))$. Then $d < s_0$ and $dy_1 \in \langle s_0y_1, \nu_{y_1}(A'_p)y_1 \rangle \subset \langle \text{supp}(A') \cup \text{supp}(A'_p) \rangle \setminus \{y_1\}$. By the minimality of $s_0$, we have $G_0 \setminus \{y_1\} = \langle \text{supp}(A') \cup \text{supp}(A'_p) \rangle \setminus \{y_1\}$. It follows that
\[
|\text{supp}(A')| + r \geq |\text{supp}(A')| + |\text{supp}(A'_p)| - 1 \geq |G_0| \geq |\text{supp}(A')| + r + 1,
\]
a contradiction.

**Case 2:** $|S_0 \setminus \text{supp}(A')| \leq r$.

Therefore $|\text{supp}(A') \cap S_0| \geq m + 1$ by Equation (3.5), and we may suppose that \{y_1, \ldots, y_{m+1}\} $\subseteq \text{supp}(A') \cap S_0$. Then $V_1 \cdot \ldots \cdot V_{m+1} | UA_1 \cdot \ldots \cdot A_{m-1} A'$ and $k(UA_1 \cdot \ldots \cdot A_{m-1} A'(V_1 \cdot \ldots \cdot V_{m+1})^{-1}) < k(U)$. By the minimality of $k(U)$, we have that $UA_1 \cdot \ldots \cdot A_{m-1} A'$ can be factorized into a product of atoms from $\Omega = 1$.

**A4.** Let $g' \in G_0$ and $A' \in \mathcal{A}(G_0)$ with $k(A') = 1$ satisfying the following three conditions:

(C4) $\nu_{g'}(A') < \text{ord}(g')$ is the smallest positive integer $\gamma$ such that $\gamma g' \not\in \langle \text{supp}(A') \setminus \{g'\} \rangle$;
(C5) $\nu_{g'}(A') g' \not\in \langle E \rangle$ for any $E \subset \supp(A') \setminus \{g'\}$.
(C6) $UA_1 \cdot \ldots \cdot A_{m-1} \cdot A'$ can be factorized into a product of atoms from $\Omega = 1$.

If $|\text{supp}(A')| \geq m + r + 1$, then there exists an atom $A'' \in \mathcal{A}(G_0)$ with $k(A'') = 1$ and $|\text{supp}(A'')| < |\text{supp}(A')|$ such that (C4), (C5), and (C6) hold.

Suppose that A4 holds. Iterating A4 we find an atom $A^* \in \mathcal{A}(G_0)$ with $|\text{supp}(A^*)| \leq m + r$ such that $UA_1 \cdot \ldots \cdot A_{m-1} \cdot A^*$ can be factorized into a product of atoms from $\Omega = 1$, a contradiction to Equation (3.5).

**Proof of A4.** For simplicity of notation, we suppose that $A' = A_m$.

Let $s_0 \in \mathbb{N}$ be minimal such that there exists a subset $E \subset \supp(A_m) \setminus \{g'\}$ such that $s_0 g' \in \langle E \rangle$. By (C4) and $|\text{supp}(A')| \geq m + r + 1 \geq r + 2$, Lemma 3.3 implies that $s_0 < \text{ord}(g')$. Let $E$ be a minimal subset with this property. Thus, by Lemma 3.1(1), there exists an atom $A''$ with $\nu_{g'}(A'') = s_0$ satisfying the two conditions (C4) and (C5). Since $\supp(A'') \subset G_0$, we have $k(A'') = 1$. We distinguish two cases:

**Case 1:** $|S_0 \setminus \text{supp}(A'')| \geq r + 1$.

We set $s' = \nu_{g'}(A_m) < \text{ord}(g')$. Since $A_m$ satisfies condition (C4), Lemma 3.1(1) implies that $s' | s_0$ and $\frac{s_0}{s'} > 1$. Let $p$ be a prime dividing $\frac{s_0}{s'}$. Since $s' | \text{ord}(g')$ and $s_0 | \text{ord}(g')$, it follows that $p | \frac{s_0}{s'} | \frac{\text{ord}(g')}{\text{ord}(g')} = \text{ord}(s' g')$.

Lemma 3.3 (applied to the subset \supp(A_m) \subset G) implies that there exists
an atom $A'_p \in \mathcal{A}(\text{supp}(A_m))$ such that $|\text{supp}(A'_p)| \leq r + 1 < |\text{supp}(A_m)|$, $s' \leq \nu g'(A'_p) \leq \text{ord}(g')/2$, and $p \nmid \frac{\nu g'(A'_p)}{s'}$.

Let $d = \gcd\left(\frac{s_0}{s'}, \frac{\nu g'(A'_p)}{s'}\right)$. Then $d < \frac{s_0}{s'}$ and

$$ds'g' \in (s_0g', \nu g'(A'_p)g') \subset \langle(supp(A'') \cup supp(A'_p)) \setminus \{g'\}\rangle.$$

Thus by minimality of $s_0$, we have $\text{supp}(A_m) \setminus \{g'\} = (\text{supp}(A'') \cup \text{supp}(A'_p)) \setminus \{g'\}$. It follows that

$$|\text{supp}(A'')| + r \geq |\text{supp}(A'')| + |\text{supp}(A'_p)| - 1 \geq |\text{supp}(A_m)|$$

$$\geq |\text{supp}(A'')| + |S_0 \setminus \text{supp}(A'')| \geq |\text{supp}(A'')| + r + 1,$$

a contradiction.

**Case 2:** $|S_0 \setminus \text{supp}(A'')| \leq r$.

Therefore $|\text{supp}(A'') \cap S_0| \geq m + 1$ by Equation (3.5), and we may suppose that $\{y_1, \ldots, y_{m+1}\} \subset \text{supp}(A'') \cap S_0$. Then $V_1 \cdots V_{m+1} | UA_1 \cdots A_{m-1}A''$ and $k(UA_1 \cdots A_{m-1}A''(V_1 \cdots V_{m+1})^{-1}) < k(U)$. By the minimality of $k(U)$, we have that $UA_1 \cdots A_{m-1}A''$ can be factorized into a product of atoms from $\Omega_{=1}$. This completes the proof of A4 and thus Lemma 3.6 is proved.

**Proposition 3.7.** We have

$$m(G) \leq \min\left\{ \frac{n}{2} + r - 2, \max\left\{ r - 1, \frac{5n}{6} - 4, \frac{n + r - 3}{2} \right\} \right\}.$$

**Proof.** Let $G_0 \subset G$ be a non-half-factorial LCN set. We have to prove that

$$\min \Delta(G_0) \leq \min\left\{ \frac{n}{2} + r - 2, \max\left\{ r - 1, \frac{5n}{6} - 4, \frac{n + r - 3}{2} \right\} \right\}.$$

If $G_1 \subset G_0$ is non-half-factorial, then $\min \Delta(G_0) = \gcd \Delta(G_0)$ divides $\gcd \Delta(G_1) = \min \Delta(G_1)$. Thus we may suppose that $G_0$ is minimal non-half-factorial. By Lemma 3.1(3a), we may suppose that $g \in \langle G_0 \setminus \{g\} \rangle$ for all $g \in G_0$.

If $n$ is a prime power, then $m(G) = r - 1$ by Proposition 2.2, and the assertion follows. Suppose that $n$ is not a prime power. If $|G_0| \leq r + 1$, then $\min \Delta(G_0) \leq |G_0| - 2 \leq r - 1$ by Lemma 3.2(3). Thus we may suppose that $|G_0| \geq r + 2$ 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 $|G_2| \leq |G_0| - 2$.

Then Lemma 3.6 implies that $\min \Delta(G_0) \leq \frac{n + r - 3}{2}.$
Case 2: Every subset \( G_1 \subset G_0 \) with \(|G_1| = |G_0| - 1\) is a minimal generating set of \((G_0)\).

Then for each \( h \in G_0, \ G_0 \setminus \{h\}\) is half-factorial and \( h \notin \langle G_0 \setminus \{h, h'\}\) for any \( h' \in G_0 \setminus \{h\}\). Thus Lemma 3.4 and Lemma 3.6 imply that \( \min \Delta(G_0) \leq \max\{\frac{5n}{6} - 4, \frac{n + r - 3}{2}\} \). By Lemma 3.4, we obtain that \(|G_0| \leq r + \frac{n}{2}\). Therefore Lemma 3.2(3) implies that \( \min \Delta(G_0) \leq \min\{r + \frac{n}{2} - 2, \max\{\frac{5n}{6} - 4, \frac{n + r - 3}{2}\}\} \). \(\square\)

**Proposition 3.8.** Let \( G' \) be a finite abelian group with \( \mathcal{L}(G) = \mathcal{L}(G') \). If \( r \in [2, (n - 2)/4] \), then \( n = \exp(G') > r(G') + 1 \).

**Proof.** Let \( k \in \mathbb{N} \) be maximal such that \( G \) has a subgroup isomorphic to \( C_n^k \). Then \( k \leq r \leq \frac{n - 2}{4} \). By Proposition 3.7, we obtain that

\[
m(G) \leq \frac{n}{2} + r - 2 \leq \frac{n}{2} + \frac{n - 2}{4} - 2 = n - \frac{n - 2}{4} - 3 \leq n - k - 3
\]

and hence

\[
\max\left\{ m(G), \left\lfloor \frac{n}{2} \right\rfloor - 1\right\} \leq n - k - 3.
\]

By Proposition 2.2(3), we have

\[
\Delta_1(G) \subset \left[ 1, \max\left\{ m(G), \left\lfloor \frac{n}{2} \right\rfloor - 1\right\} \right] \cup [n - k - 1, n - 2],
\]

and thus \( n - k - 2 \notin \Delta_1(G) \). Thus \( n - k - 2 \notin \Delta_1(G') \) and Proposition 2.2 implies that

\[
n - 2 = \max\{m(G), n - 2\} = \max \Delta_1(G) = \max \Delta_1(G') = \max\{r(G') - 1, \exp(G') - 2\}\]

If \( n - 2 = r(G') - 1 \), then \( \Delta_1(G') = [1, n - 2] \) by Lemma 3.2(2), a contradiction to \( n - k - 2 \notin \Delta_1(G') \). Therefore it follows that \( n = \exp(G') > r(G') + 1 \). \(\square\)

4. **Proof of the Main Result and groups with small Davenport constant**

**Proof of Theorem 1.1.** Let \( G \) be an abelian group such that \( \mathcal{L}(G) = \mathcal{L}(C_n^r) \) where \( r, n \in \mathbb{N} \) with \( n \geq 2 \), \( (n, r) \notin \{(2, 1), (2, 2), (3, 1)\} \), and \( r \leq \max\{2, (n + 2)/6\} \).

First we note that \( G \) has to be finite and that \( D(C_n^r) = D(G) \) and \( \Delta_1(C_n^r) = \Delta_1(G) \) (see [8, Proposition 7.3.1 and Theorem 7.4.1]). If \( r = 1 \), then the assertion follows from [8, Theorem 7.3.3]. If \( r = 2 \), then the assertion follows from [21], and hence we may suppose that \( r \in [3, (n + 2)/6] \).

Let \( k \in \mathbb{N} \) be maximal such that \( G \) has a subgroup isomorphic to \( C_n^k \). If \( k \geq r \), then \( D(C_n^r) = D(G) \geq D(C_n^k) \) implies that \( k = r \) and that \( G \cong C_n^r \). Suppose that \( k < r \). By Proposition 3.8, we obtain that \( n = \)
exp(G) > r(G) + 1. By Proposition 2.2(3) (applied to $C^r_n$) we infer that $[n - r - 1, n - 2] \subset \Delta_1(C^r_n) = \Delta_1(G)$. By Proposition 2.2(3) (applied to $G$), we obtain that

$$[1, r(G) - 1] \cup [n - r - 1, n - 2] \subset \Delta_1(G) \subset [1, \max \left\{ m(G), \left\lceil \frac{n}{2} \right\rceil - 1 \right\}] \cup [n - k - 1, n - 2],$$

which implies that $m(G) \geq n - r - 1$. By Proposition 3.7, we have that

$$n - r - 1 \leq m(G) \leq \max \left\{ r(G) - 1, \frac{5n}{6} - 4, \frac{n + r(G) - 3}{2} \right\}.$$ 

If $n - r - 1 \leq \frac{5n}{6} - 4$, then $r \geq \frac{n}{6} + 3$, a contradiction. Thus $n - r - 1 \leq \max \left\{ r(G) - 1, \frac{n + r(G) - 3}{2} \right\}$ which implies that $r(G) \geq n - 2r + 1$. Therefore

$$\tag{4.1} [1, n - 2r] \subset [1, r(G) - 1] \subset \Delta_1(G) = \Delta_1(C^r_n).$$

Since $r \leq \frac{n + 2}{6}$, we have that $n - 2r - 1 \geq \frac{n}{2} + r - 2 \geq \left\lfloor \frac{n}{2} \right\rfloor - 1$. By Proposition 3.7, we obtain that $m(C^r_n) \leq \frac{n}{2} + r - 2 \leq n - 2r - 1$. Therefore

$$\max \left\{ m(C^r_n), \left\lceil \frac{n}{2} \right\rceil - 1 \right\} < n - 2r < n - r - 1.$$ 

By Proposition 2.2(3), $n - 2r \notin \Delta_1(C^r_n)$, which is a contradiction to Equation (4.1). \hfill \Box

Our proof of Theorem 1.1, to characterize the groups $C^r_n$ with $r, n$ as above, uses only the Davenport constant and the set of minimal distances. Clearly, there are non-isomorphic groups $G$ and $G'$ with $D(G) = D(G')$, $\Delta^*(G) = \Delta^*(G')$, and $\Delta_1(G) = \Delta_1(G')$. We meet this phenomenon in Proposition 4.1. Indeed, since $\mathcal{L}(C_1) = \mathcal{L}(C_2)$ and $\mathcal{L}(C_3) = \mathcal{L}(C_2 \oplus C_2)$ ([8, Theorem 7.3.2]), small groups definitely deserve a special attention when studying the Characterization Problem. Clearly, the groups $C_1, C_2, C_3$, and $C_2 \oplus C_2$ are precisely the groups $G$ with $D(G) \leq 3$. In our final result we show that for all groups $G$ with $D(G) \in [4, 11]$ the answer to the Characterization Problem is positive.

Suppose that $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$ where $r \in \mathbb{N}_0$ and $1 < n_1 | \ldots | n_r$ and set $D^*(G) = 1 + \sum_{i=1}^r (n_i - 1)$. Then $D^*(G) \leq D(G)$. If $r(G) = r \leq 2$ or if $G$ is a $p$-group, then equality holds.

**Proposition 4.1.** Let $G$ be a finite abelian group with $D(G) \in [4, 11]$. If $G'$ is a finite abelian group with $\mathcal{L}(G) = \mathcal{L}(G')$, then $G \cong G'$. 

Proof. Suppose that $G'$ is a finite abelian group with $\mathcal{L}(G) = \mathcal{L}(G')$. Then $D(G) = D(G')$. If $D(G) \in [4, 10]$, then the assertion follows from [21, Theorem 6.2].

Suppose that $D(G) = D(G') = 11$. If $r(G) \leq 2$ or $r(G') \leq 2$, then the assertion follows from [12, Theorem 1.1]. If $G$ or $G'$ is an elementary 2-group, then the assertion follows from [8, Theorem 7.3.3].

Thus we suppose that $r(G) \geq 3$, $r(G') \geq 3$, $\exp(G) \in [3, 8]$, and $\exp(G') \in [3, 8]$. If $G \cong C_3^5$ or $G' \cong C_3^5$, then the assertion follows from [12, Theorem 4.1]. Thus we may suppose that all this is not the case. Since there is no finite abelian group $H$ with $D(H) = 11$ and $\exp(G) \in \{5, 7\}$, it remains to consider the following groups:

$$C_2^4 \oplus C_4^2, C_2^7 \oplus C_4, C_2^5 \oplus C_6, C_2^3 \oplus C_8, C_3^5$$

for some $r \in \mathbb{N}$.

By [14, Corollary 2], $D(C_2^4 \oplus C_6) = D^*(G) = r + 6$ if and only if $r \leq 3$. Thus $D(C_2^4 \oplus C_6) \geq 11$, and this is the only group for which $D(C_2^4 \oplus C_6) = 11$ is possible. Thus we have to consider

$$G_1 = C_2^4 \oplus C_4^2, \hspace{1em} G_2 = C_2^7 \oplus C_4, \hspace{1em} G_3 = C_2^4 \oplus C_6,$$

$$G_5 = C_2^3 \oplus C_8, \hspace{1em} G_6 = C_3^5.$$

Since $\max \Delta^*(G_1) = 5$, $\max \Delta^*(G_2) = 7$, $\max \Delta^*(G_4) = 4$, $\max \Delta^*(G_5) = 6$, and $\max \Delta^*(G_6) = 4$, it remains to show that $\mathcal{L}(C_2^4 \oplus C_6) \neq \mathcal{L}(C_3^5)$. Note that Proposition 2.2 implies that $\Delta^*(C_2^4 \oplus C_6) = [1, 4] = \Delta^*(C_3^5)$. By [8, Theorem 6.6.2], it follows that $\{2, 8\} \in \mathcal{L}(C_2^4 \oplus C_6)$, and we assert that $\{2, 8\} \notin \mathcal{L}(C_3^5)$.

Assume to the contrary that $\{2, 8\} \in \mathcal{L}(C_3^5)$. Then there exists $U, V \in \mathcal{A}(C_3^5)$ such that $\mathcal{L}(UV) = \{2, 8\}$. We choose the pair $(U, V)$ such that $|U|$ is maximal and observe that $11 \geq |U| \geq |V| \geq 8$. There exists an element $g \in G$ such that $g | U$ and $-g | V$. Then $v_g(U) \leq 2$ and $v_{-g}(V) \leq 2$. If $v_g(U) = v_{-g}(V) = 2$, then $gV(-g)^{-2}, (-g)Vg^{-2}$ and $g(-g)$ are atoms and hence $3 \in \mathcal{L}(UV)$, a contradiction. Therefore $v_g(U) + v_{-g}(V) \in [2, 3]$ and we set

$$(4.2) \{g \in \text{supp}(U) \mid v_g(U) + v_{-g}(V) = 3\} = \{g_1, \ldots , g_\ell\} \quad \text{where} \quad \ell \in \mathbb{N}_0.$$

We continue with the following assertion.

A5. For each $i \in [1, \ell]$ we have $v_{g_i}(U) = 2$.

Proof of A5. Assume to the contrary that there is an $i \in [1, \ell]$ with $v_{g_i}(U) = 1$. Then $g_iV((-g_i)^2)^{-1}$ is an atom and $(-g_i)^2Ug_i^{-1}$ is an atom or a product of two atoms. Since $3 \notin \mathcal{L}(UV)$, we obtain that $(-g_i)^2Ug_i^{-1}$ is an atom but $|(-g_i)^2Ug_i^{-1}| > |U|$, a contradiction to our choice of $|U|$. $\square$
Now we set
\[ U' = (-g_1) \cdots (-g_\ell) U (g_1^2 \cdots g_\ell^2)^{-1} \]
and \[ V' = g_1^2 \cdots g_\ell^2 V ((-g_1) \cdots (-g_\ell))^{-1}. \]

Using the above argument repeatedly we infer that \( U' \) and \( V' \) are atoms. Clearly, we have \( L(U'V') = L(UV) = \{2, 8\} \) whence \( |V| + \ell = |V'| \leq |U| \)
and thus \( \ell \leq 3 \). We consider a factorization
\[ UV = W_1 \cdots W_8, \]
where \( W_1, \ldots, W_8 \in \mathcal{A}(C_\mathbb{Z}_3^5) \) such that \(|\{i \in [1, 8] \mid |W_i| = 2\}| \) is maximal under all factorization of \( UV \) of length 8. We set \( U = U_1 \cdots U_8, \ V = V_1 \cdots V_8 \) such that \( W_i = U_iV_i \) for each \( i \in [1, 8] \), and we define \( W = \sigma(U_1) \cdots \sigma(U_8) \). We continue with a second assertion.

**A6.** There exist disjoint non-empty subsets \( I, J, K \subset [1, 8] \) such that
\[ I \cup J \cup K = [1, 8] \quad \text{and} \quad \sigma(\prod_{i \in I} U_i) = \sigma(\prod_{j \in J} U_j) = \sigma(\prod_{k \in K} U_k). \]

**Proof of A6.** First we suppose that \( h(W) \geq 2 \), say \( \sigma(U_1) = \sigma(U_2) \). Then \( I = \{1\}, \ J = \{2\}, \ K = [3, 8] \) have the required properties. Now suppose that \( h(W) = 1 \). Since the tuple \( (\sigma(U_1), \ldots, \sigma(U_7)) \) is not independent and the sequence \( \sigma(U_1) \cdots \sigma(U_7) \) is zero-sum free, there exist disjoint non-empty subset \( I, J \subset [1, 8] \), such that \( \sum_{i \in I} \sigma(U_i) = \sum_{j \in J} \sigma(U_j) \). Therefore, \( I, J, \) and \( K = [1, 8] \setminus (I \cup J) \) have the required properties. \( \Box \)

We define
\[ X_1 = \prod_{i \in I} U_i, \quad X_2 = \prod_{j \in J} U_j, \quad \text{and} \quad X_3 = \prod_{k \in K} U_k, \]
\[ Y_1 = \prod_{i \in I} V_i, \quad Y_2 = \prod_{j \in J} V_j, \quad \text{and} \quad Y_3 = \prod_{k \in K} V_k. \]

By construction, we have \( X_1Y_1 = \prod_{i \in I} W_i, \ X_2Y_2 = \prod_{j \in J} W_j, \ X_3Y_3 = \prod_{k \in K} W_k, \ \sigma(X_1) = \sigma(X_2) = \sigma(X_3), \ \sigma(Y_1) = \sigma(Y_2) = \sigma(Y_3), \) and hence \( X_iY_j \in \mathcal{B}(G) \) for all \( i, j \in [1, 3] \).

We choose a factorization of \( X_1Y_2 \), a factorization of \( X_2Y_3 \), and a factorization of \( X_3Y_1 \), and their product gives rise to a factorization of \( UV \), say \( UV = W_1 ' \cdots W_8 ' \), where all the \( W_i ' \) are atoms, and we denote by \( t_1 \) the number of \( W_i ' \) having length two. Similarly, we choose a factorization of \( X_1Y_3 \), a factorization of \( X_2Y_1 \), and a factorization of \( X_3Y_2 \), obtain a factorization of \( UV \), and we denote by \( t_2 \) the number of atoms of length 2 in this factorization. If \( g \in G \) and \( i, j \in [1, 3] \) are distinct with \( g(-g) | X_iY_j \) and \( g | X_i \), then the choice of the factorization \( UV = W_1 ' \cdots W_8 ' \) implies that \( g(-g) | X_iY_i \) or \( g(-g) | X_jY_j \) whence \( v_g(U) + v_{-g}(V) \geq 3 \). Therefore
Equation (4.2) implies that \( g \in \{ g_1, \ldots, g_\ell \} \) whence \( t_1 + t_2 \leq \ell \leq 3 \), and we may suppose that \( t_1 \leq 1 \). Therefore we infer that
\[
2 + 3 \times 7 \leq \sum_{i=1}^{8} |W_i'| = |UV| \leq 2D(C_3^5) = 22,
\]
a contradiction. \( \square \)

References


[22] ———, “Characterization of class groups of Krull monoids via their systems of sets of
lengths a status report”, in Number theory and applications. Proceedings of the interna-
tional conferences on number theory and cryptography, Allahabad, India, December 2006
[23] ———, “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.

Alfred Geroldinger
University of Graz, NAWI Graz
Institute for Mathematics and Scientific Computing
Heinrichstraße 36
8010 Graz, Austria
E-mail: alfred.geroldinger@uni-graz.at
URL: http://imsc.uni-graz.at/geroldinger/

Qinghai Zhong
University of Graz, NAWI Graz
Institute for Mathematics and Scientific Computing
Heinrichstraße 36
8010 Graz, Austria
E-mail: qinghai.zhong@uni-graz.at
URL: http://qinghai-zhong.weebly.com