CHARACTERIZATION OF CLASS GROUPS OF KRULL MONOIDS VIA THEIR SYSTEMS OF SETS OF LENGTHS: A STATUS REPORT

WOLFGANG A. SCHMID

Abstract. This paper gives an overview of results on the systems of sets of lengths of Krull monoids, with a focus on monoids with finite class group where each class contains a prime divisor. There is an emphasis on results that allow to characterize (properties of) the class group via the system of sets of lengths. Moreover, it is shown for some further groups that the system of sets of lengths characterizes the class group.

1. Introduction

The Theory of Non-Unique Factorizations has its origins in Algebraic Number Theory. The ring of integers of an algebraic number field is factorial (a unique factorization domain) if and only if it is a principal ideal domain, i.e., its class group is trivial. Thus, if the class group contains at least two elements, there exist elements that have various essentially distinct factorizations into irreducible elements. A main subject of the Theory of Non-Unique Factorizations is to understand and describe the various types of non-uniqueness that can occur, both from a qualitative and quantitative point of view. A classical result due to L. Carlitz [8] yields the following: Let H be the ring of integers of an algebraic number field. For $a \in H$ let $\mathsf{L}(a)$ denote the set of all n such that a has a factorization into n irreducible elements. Then, $|\,\mathsf{L}(a)| = 1$ for each $a \in H$ if and only if the class group of H has at most two elements. The set $\mathsf{L}(a)$ is called the set of lengths of a, and the set of all $\mathsf{L}(a)$ for $a \in H$ is called the system of sets of lengths of H.

Subsequently, it turned out that all problems regarding sets of lengths in the ring of integers of an algebraic number field can be transferred to problems in the associated block monoid, i.e. the monoid of zero-sum

This paper partly consists of work done while the author was a visitor of the Harish-Chandra Research Institute. He would like to thank for hospitality and excellent working conditions. The author is supported by the Austrian Science Fund FWF (Project P18779-N13).

sequences over the class group, a notion introduced by W. Narkiewicz [42]. Moreover, this approach is not limited to the ring of integers of an algebraic number field, but still works for a more general class of monoids, namely Krull monoids; informally, these are the monoids for which the divisibilty relation is induced (in a natural way) by that of an associated free, and thus in particular factorial, monoid (in the number field case, it is the monoid of non-zero ideals). We refer to the monograph of W. Narkiewicz [43, Chapter 9] for an overview from a number theoretic point of view and to the monograph of A. Geroldinger and F. Halter-Koch [30] for a more abstract approach, which we adopt in this paper. Moreover, we refer to the conference proceedings [5, 10] and the recent survey articles [29, 35] for the history and development of the subject.

The purpose of this paper is mainly expository, though it contains some new results. Namely, we give an overview of, partly very recent, results on the system of sets of lengths of Krull monoids, focusing on the case that the class group is finite and each class contains a prime divisor, which is the case for the ring of integers of an algebraic number field. Moreover, we concentrate on those results that can be used to characterize (properties of) the class group via the system of sets of lengths; a classical example of such a result is the one, mentioned above, due to L. Carlitz. These results can be seen as contributions to the more general problem of finding arithmetical characterizations of the class group, which was posed by W. Narkiewicz (cf. [43]) and initially solved by J. Kaczorowski [38] and J.E. Rush [46] (see [30, Chapter 7] for a detailed discussion). Therefore, we mention certain closely related subjects, e.g., half-factorial domains and sets (see the survey article by S.T. Chapman and J. Coykendall [11]) only in passing and refer to the above mentioned publications for information on them. Moreover, we point out that questions of the type discussed in this paper for Krull monoids only are investigated for other classes of monoids as well, e.g., for numerical semigroups (see the recent paper by J. Amos, S.T. Chapman, N. Hine, and J. Paixão [4]).

The organization of the paper is as follows. In Section 2 and Section 3 we recall some results and terminology, which is fundamental for the subsequent discussion, in particular we recall the definition of Krull and block monoids. In Section 4 we recall some results on the Davenport constant and a related constant. In Section 5 we recall the Structure Theorem for Sets of Lengths, showing that all sets of lengths are almost arithmetical multiprogressions, and in Section 7 we discuss results that make this description more explicit. In Section 6 we recall what is known on the problem of characterizing the class group via the system of sets of lengths and formulate an extension of one of these results. In Section 8 we review (and partly extend) the results used to obtain the characterization results. Finally, in Section 9 we employ these results to prove the result formulated in Section 6.

2. Terminology and notation

In this section we fix some terminology and notation. We denote by $\mathbb{N}$ the set of positive integers and by $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. All intervals in this paper are intervals of integers, i.e., $[a, b] = \{z \in \mathbb{Z} \colon a \le z \le b\}$. For subsets A, B of an (additive) semigroup, we denote by $A + B = \{a + b \colon a \in A, b \in B\}$.

Let G be a finite abelian group. We use additive notation throughout and denote the identity element by 0. For $n \in \mathbb{N}$, let C_n denote a cyclic group of order n. A subset $E \subset G \setminus \{0\}$ is called independent if $\sum_{e \in E} m_e e = 0$ with $m_e \in \mathbb{Z}$ implies that $m_e e = 0$ for each $e \in E$. For $G_0 \subset G$, let $\langle G_0 \rangle$ denote the subgroup generated by G_0. Let $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r} \cong C_{q_1} \oplus \cdots \oplus C_{q_{r^*}}$ with $1 < n_1 \mid \cdots \mid n_r$ and prime powers q_i. Let $\exp(G) = n_r$ denote the exponent of G, $\mathsf{r}(G) = r$ the rank, and $\mathsf{r}^*(G) = r^*$ the total rank of G. The group G is called a p-group if the exponent is an (unspecified) prime power and an elementary p-group if it is an (unspecified) prime. Occasionally, we fix the prime and say, e.g., that a group is a 2-group to express that the exponent is a power of 2.

3. Basics of Non-unique Factorization Theory

In this section we briefly recall various results and definitions that are fundamental for many investigations in Non-Unique Factorization Theory, with an emphazise on Krull monoids and related notions. We refer to the monograph of A. Geroldinger and F. Halter-Koch [30] for a complete exposition.

3.1. **Monoids.** In this section we recall some basic notions on monoids. A monoid is a commutative cancellative semigroup with identity element; we use multiplicative notation for monoids and denoted the identity element by 1. We denote the subset of invertible elements of H by $H^\times$; if $H^\times = \{1\}$ then H is called reduced. The monoid $H_{\text{red}} = H/H^\times$ is reduced. Elements $a, b \in H$ are called associates, in symbols $a \simeq b$, if $a = \epsilon b$ for some $\epsilon \in H^\times$. We denote by $\mathsf{q}(H)$ the quotient group of H.

An element $u \in H \setminus H^\times$ is called irreducible, or an atom, if $u = ab$ implies that a or b is invertible. The set of atoms of H is denoted by

$\mathcal{A}(H)$. A monoid is called atomic if each (non-invertible) element can be written as finite product of atoms.

3.2. **Free monoids and block monoids.** A monoid F is called free (with basis $P \subset F$) if each $a \in F$ has a unique representation

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

For a set P we denote by $\mathcal{F}(P)$ the free monoid with basis P.

Let $F = \mathcal{F}(P)$ and let $a = \prod_{p \in P} p^{\mathsf{v}_p(a)} \in F$. Then, $\mathsf{v}_p(a)$ is called the multiplicity of p in a, $|a| = \sum_{p \in P} \mathsf{v}_p(a) \in \mathbb{N}_0$ the length of a, and $\operatorname{supp}(a) = \{p \in P \colon \mathsf{v}_p(a) \neq 0\}$ the support of a. The element a is called squarefree if $\mathsf{v}_p(a) \le 1$ for each $p \in P$. Frequently, we refer to the elements of $\mathcal{F}(P)$ as sequences over P and to divisors of an element as subsequences; moreover, we call the identity element the empty sequence.

Block monoids are a main tool in the investigation of Krull monoids. They were introduced by W. Narkiewicz [42].

Definition 3.1. Let G be an abelian group and $G_0 \subset G$ a subset. Let $S = \prod_{g \in G_0} g^{v_g} \in \mathcal{F}(G_0)$.

(1) $\sigma(S) = \sum_{g \in G_0} v_g g \in G$ is called the sum of S. If $\sigma(S) = 0$, then S is called a zero-sum sequence (or a block).
(2) If G_0 consists of torsion elements, then $\mathsf{k}(S) = \sum_{g \in G_0} v_g / \operatorname{ord} g$ is called the cross number of S.
(3) $\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \colon \sigma(S) = 0\}$ is called the block monoid, or the monoid of zero-sum sequences, over G_0.

The atoms of $\mathcal{B}(G_0)$ are those non-empty sequences that do not have a proper subsequence, i.e. one that is not equal to the sequence and non-empty, that is a zero-sum sequence; these are called minimal zero-sum sequences. We indentify the elements of G_0 with the sequences of length 1. In general, we denote sequences over subsets of abelian groups by upper case letters and a sequence over a subset of an abelian group that is denote by a lower case letter has always length 1, i.e., is an element of the group. Moreover, if $S = g_1 \dots g_l$ is a sequence over an abelian group, then $-S$ denotes the sequence $(-g_1) \dots (-g_l)$.

3.3. **Factorizations in monoids.** Typically, one wants to consider two factorizations of an element as equal if the irreducible factors are equal up to ordering and associates. This can be made precise in the following way. The monoid $\mathsf{Z}(H) = \mathcal{F}(\mathcal{A}(H_{\mathrm{red}}))$ is called the factorization monoid of H. The homomorphism given by $\pi_H : \mathcal{F}(\mathcal{A}(H_{\mathrm{red}})) \to H_{\mathrm{red}}$

that is constant on $\mathcal{A}(H_{\mathrm{red}})$ is called the factorization homomorphism. For $a \in H$, $\mathsf{Z}_H(a) = \pi_H^{-1}(aH^\times)$ is called the set of factorizations of a. And $\mathsf{L}_H(a) = \{|f| \colon f \in \mathsf{Z}_H(a)\}$ is called the set of lengths (of factorizations) of a. If the monoid H is clear from context, the subscript H is dropped. Moreover, $\mathcal{L}(H) = \{\mathsf{L}(a) \colon a \in H\}$ is called the system of sets of lengths of H.

The sets of factorizations and lengths of an element can be infinite. An atomic monoid H is called

- an FF-monoid (finite factorization) if $|\,\mathsf{Z}(a)| < \infty$ for each $a \in H$.
- a BF-monoid (bounded factorization) if $|\,\mathsf{L}(a)| < \infty$ for each $a \in H$.
- factorial if $|\,\mathsf{Z}(a)| = 1$ for each $a \in H$.
- half-factorial if $|\,\mathsf{L}(a)| = 1$ for each $a \in H$.

This definition of factorial is identical with the usual one of a factorial, or unique factorization, monoid/domain. All monoids that are investigated in this paper are FF-monoids. It is not difficult to see that a monoid is either factorial or contains elements for which $|\,\mathsf{Z}(a)|$ is arbitrarily large; and similarly it is either half-factorial or $|\,\mathsf{L}(a)|$ can be arbitrarily large.

The notion tameness plays an important role in Non-Unique Factorization Theory (it has its origins in [24], see [30] for a detailed account). To define it one introduces a metric on $\mathsf{Z}(H)$. For $x, y \in \mathsf{Z}(H)$, let $z = \gcd(x, y)$, since $\mathsf{Z}(H)$ is a free monoid this is well-defined, and we call

$$\mathsf{d}(x, y) = \max\{|z^{-1}x|, |z^{-1}y|\}$$

the distance of x and y.

Definition 3.2. Let H be a an atomic monoid.

(1) Let $a \in H$ and $x \in \mathsf{Z}(H)$. Then $\mathsf{t}(a, x)$ denotes the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property. If $\mathsf{Z}(a) \cap x\,\mathsf{Z}(H) \neq \emptyset$ and $z \in \mathsf{Z}(a)$, then there exists some $z' \in \mathsf{Z}(a) \cap x\,\mathsf{Z}(H)$ such that $\mathsf{d}(z, z') \le N$.
(2) For $H' \subset H$ and $X \subset \mathsf{Z}(H)$, let $\mathsf{t}(H', X) = \sup\{\mathsf{t}(a, x) \colon a \in H' \text{ and } x \in X\}$.
(3) H is called tame if $\mathsf{t}(H, \mathcal{A}(H_{\mathrm{red}})) < \infty$ and one calls $\mathsf{t}(H) = \mathsf{t}(H, \mathcal{A}(H_{\mathrm{red}}))$ the tame degree of H.

It is easy to see that for $a, b \in H$ one has $\mathsf{L}(a) + \mathsf{L}(b) \subset \mathsf{L}(ab)$, but in general these sets are not equal. The tame degree allows to establish a closer relation between $\mathsf{L}(a) + \mathsf{L}(b)$ and $\mathsf{L}(ab)$. We only mention one specific result that we need in the sequel (see [30, Section 4.3] for details).

Proposition 3.3. *Let H be BF-monoid and let $a, b \in H$. Then,*

$$\min \mathsf{L}(ab) \geq \max \mathsf{L}(a) + \min \mathsf{L}(b) - \mathsf{t}(\{ab\}, \mathsf{Z}(a))$$

and

$$\max \mathsf{L}(ab) \leq \min \mathsf{L}(a) + \max \mathsf{L}(b) + \mathsf{t}(\{ab\}, \mathsf{Z}(a)).$$

Note that $\mathsf{t}(\{ab\}, \mathsf{Z}(a)) \leq 2 \min \mathsf{L}(a)\, \mathsf{t}(H)$ and that the block monoid over subsets of finite abelian groups are tame.

We recall some more notions, widely used in the investigation of sets of lengths, which originated in [24, 15, 6]. Let H be an atomic monoid.

- For $L = \{l_1 < l_2 < l_3 < \dots\} \subset \mathbb{Z}$ let $\Delta(L) = \{l_2 - l_1, l_3 - l_2, \dots\}$ denote the set of successive distances. For $\emptyset \neq L \subset \mathbb{N}$ let $\rho(L) = \sup L / \min L$ denote the elasticity of L, and let $\rho(\{0\}) = 1$.
- Let $\Delta(H) = \bigcup_{a \in H} \Delta(\mathsf{L}(a))$ denote the set of distances of H and $\rho(H) = \sup\{\rho(\mathsf{L}(a)) \colon a \in H\}$ the elasticity of H. Moreover, for $a \in H$ let $\Delta(a) = \Delta(\mathsf{L}(a))$ and $\rho(a) = \rho(\mathsf{L}(a))$; these are called the set of distances and the elasticity, resp., of a.
- For $k \in \mathbb{N}$, let $\mathcal{V}_k(H) = \bigcup_{a \in H} \{\mathsf{L}(a) \colon a \in H,\, k \in \mathsf{L}(a)\}$. Moreover, let $\rho_k(H) = \sup \mathcal{V}_k(H)$ and $\lambda_k(H) = \min \mathcal{V}_k(H)$.

3.4. **Krull monoids.** We recall the definition of a Krull monoid; our exposition is very brief and we refer to the monographs [30], [34], [37] for a detailed expositions. Let H and D be monoids.

- A monoid homomorphism $\varphi : H \to D$ is called a divisor homomorphism if, for $a, b \in H$, $a \mid b$ if and only if $\varphi(a) \mid \varphi(b)$.
- A divisor homomorphism $\varphi : H \to D$ is called a divisor theory (for H) if $D = \mathcal{F}(P)$ is free and for each $p \in P$ there exists some finite subset $\emptyset \neq X_p \subset H$ such that $\gcd(\varphi(X_p)) = p$.

Definition 3.4. A monoid is called a Krull monoid if it has a divisor theory.

Note that a divisor theory of a Krull monoid is essentially unique. We point out that there are a variety of equivalent ways to define a Krull monoid; some of them are more reminiscent of common definitions of a Krull or Dedekind domain. In particular, the ring of non-zero algebraic integers of an algebraic number field is a Krull monoid (as is the multiplicative monoid of a Dedekind or Krull domain); a divisor theory can be obtained by mapping each element to the factorization of its principal ideal into prime ideals (or, for Krull domains, divisorial prime ideals). Moreover, note that block monoids are Krull monoids;

the embedding of $\mathcal{B}(G_0)$ in $\mathcal{F}(G_0)$ is a divisor homomorphism, though in general not a divisor theory.

3.5. **Transfer homomorphsims.** Next, we recall the definition of a transfer homomorphism and some of its properties. This notion was introduced by F. Halter-Koch (see [36], [28] or [30, Section 3.2]). It allows to transfer investigations from the (complicated) monoids of actual interest, e.g., orders in algebraic number fields, to simpler auxiliary monoids. A monoid homomorphism $\Theta : H \to B$ is called a transfer homomorphism if it has the following properties:

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

Let $\Theta : H \to B$ be a transfer homomorphism. Then, among others, the following holds.

- $\Theta(\mathcal{A}(H)) = \mathcal{A}(B)$.
- There exists a unique homomorphism $\overline{\Theta} : \mathsf{Z}(H) \to \mathsf{Z}(B)$ with $\overline{\Theta}(uH^\times) = \Theta(u)B^\times$ for each $u \in \mathcal{A}(H)$. Moreover $\overline{\Theta}(\mathsf{Z}(a)) = \mathsf{Z}(\Theta(a))$ and $\mathsf{L}(a) = \mathsf{L}(\Theta(a))$ for each $a \in H$. In particular, H is atomic if and only if B is atomic and $\mathcal{L}(H) = \mathcal{L}(B)$.

It will be of particular interest for us that transfer homomorphisms preserve lengths of factorizations. For Krull monoids, e.g., maximal orders in algebraic number fields, a transfer homomorphism to a block monoid over a subset of its class group exists (this result has its origins in [42] see [30, Chapter 3] for a detailed account):

Let H be a Krull monoid and $\varphi : H \to \mathcal{F}(P)$ the divisor theory. Then $G = \mathsf{q}(\mathcal{F}(P))/\,\mathsf{q}(\varphi(H))$ is called the class group of H. For $p \in P$, the class containing p is denoted by $[p]$ and $G_P = \{[p] \colon p \in P\}$ is called the subset of classes containing prime divisors. The class group can be infinite, however we almost exclusively consider the finite case in this paper. We use additive notation for the class group. Further, let $\tilde{\beta} : \mathcal{F}(P) \to \mathcal{F}(G_P)$ denote the homomorphism that maps each $p \in P$ to $[p]$. Then

$$\operatorname{im}(\tilde{\beta} \circ \varphi) = \mathcal{B}(G_P).$$

The homorphism $\beta = \tilde{\beta} \circ \varphi : H \to \mathcal{B}(G_p)$ is called the block homomorphism of H.

Theorem 3.5. *Let H be a Krull monoid. The block homomorphism is a transfer homomorphism.*

Thus, all questions regarding sets of lengths in Krull monoids can be investigated in the associated block monoid. If one is not just interested in lengths of factorizations, but also, say, in the number of (essentially) distinct factorizations, one can transfer to type monoids, informally these are colored versions of block monoids, instead (cf. [30, Section 3.5]).

As already indicated, the method of transferring the problems to suitable auxiliary monoids is not restricted to Krull monoids. For instance, see [27] for a method that allows to treat non-maximal orders as well.

4. Davenport constant and cross number

As explained in the preceding section problems on sets of lengths in Krull monoids (with finite class group) can be transferred to problems in the monoid of zero-sum sequences over a subset of a (finite) ablian group. The investigation of zero-sum problems in finite abelian groups has a long tradition; the Theorem of Erdős–Ginzburg–Ziv is one classical starting point for many investigations and the investigation of the Davenport constant is another.

In this section we discuss some results on the Davenport constant and the cross number, a related invariant introduced by U. Krause [40]. We restrict to recalling those results that are needed in this paper. We refer to the monographs [1] and [30], the recent survey article [20], and the recent papers [3, 2, 22, 33, 52] for more information on these and related invariants.

Let G be a finite abelian group. Then $\mathsf{D}(G) = \max\{|A| \colon A \in \mathcal{A}(G)\}$ is called the Davenport constant and $\mathsf{K}(G) = \max\{\mathsf{k}(A) \colon A \in \mathcal{A}(G)\}$ the cross number of G. The following result is classical; it was obtained by D. Kruyswijk and (independently) J.E. Olson [44, 45, 53].

Proposition 4.1. *Let $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $n_i \mid n_{i+1}$.*

(1) $\mathsf{D}(G) \ge 1 + \sum_{i=1}^{r}(n_i - 1)$.
(2) *If G is a p-group or if the rank of G is at most 2, then $\mathsf{D}(G)$ is equal to the above lower bound.*

There are a some further classes of groups for which it is known that $\mathsf{D}(G)$ is equal to the lower bound stated above (see [12, 7] for recent progress on this problem). Here, we only make use of the fact that this is true for the groups $C_3^2 \oplus C_6$ and $C_2^n \oplus C_6$ for $n \le 3$. However, it is known that equality does not always hold at this lower bound, in particular $\mathsf{D}(C_2^4 \oplus C_6) > 10$. These results are due to P.C. Baayen, P. van Emde Boas, and D. Kruyswijk (see [54] and the references there).

Now, we recall results on the cross number that are due to U. Krause, C. Zahlten [41] and A. Geroldinger and R. Schneider [26, 32].

Proposition 4.2. *Let $G \cong C_{q_1} \oplus \cdots \oplus C_{q_{r^*}}$ with prime powers q_i.*

(1) $\mathsf{K}(G) \ge \frac{1}{\exp(G)} + \sum_{i=1}^{r^*} \frac{q_i - 1}{q_i}$.
(2) *If G is a p-group, then $\mathsf{K}(G)$ is equal to the above lower bound.*
(3) *If $G \cong C_p^s \oplus H$ with $p \in \mathbb{P}$, $s \in \mathbb{N}_0$, $p \nmid |H|$ and $\mathsf{r}^*(H) \le 2$, then $\mathsf{K}(G)$ is equal to the above lower bound.*

In contrast to $\mathsf{D}(G)$, for $\mathsf{K}(G)$ no example is known where it exceeds the above lower bound.

5. The system of sets of lengths of Krull monoids

The investigation of sets of lengths of elements of Krull monoids is a main subject of Non-Unique-Factorization Theory. As explained in Section 3 it is equivalent to investigating sets of lengths of $\mathcal{B}(G_P)$ where G_P denotes the subset of the class group of classes containing prime divisors. Thus, we formulate all results for block monoids only. We focus on the case where every class contains a prime divisor and the class group is finite; e.g., this is the case for the multiplicative monoid of the ring of integers of an algebraic number field. For simplicity, it is common to replace $\mathcal{L}(\mathcal{B}(G))$ by $\mathcal{L}(G)$, and alike for all other quantities that are defined for monoids. In particular, we say that a subset G_0 of an abelian group is half-factorial if the monoid $\mathcal{B}(G_0)$ is half-factorial.

By a result of L. Carlitz [8], already mentioned in Section 1, the following is known.

Theorem 5.1. *Let G be a finite abelian group. $\mathcal{L}(G) = \{\{k\} \colon k \in \mathbb{N}_0\}$ if and only if $|G| \le 2$.*

In other words, a finite abelian group G is half-factorial if and only if $|G| \le 2$. As mentioned in Section 3, we thus know that if $|G| \ge 3$, then $\mathcal{L}(G)$ contains arbitrarily large sets. Still for some small groups an explicit description for $\mathcal{L}(G)$ is known (see [25]), namely

$$\mathcal{L}(C_3) = \mathcal{L}(C_2 \oplus C_2) = \{y + 2k + [0, k] \colon y, k \in \mathbb{N}_0\}$$

and similar but more complicated descriptions are known for C_4 and C_2^3. However, the complexity of this problem increases very rapidly. Thus, it seems (at present) rather infeasible to obtain explicit descriptions of $\mathcal{L}(G)$ even for groups of a moderate order or simple structure. Yet, by a result of A. Geroldinger [24], it is known that $\mathcal{L}(G)$ has some structure. The following definition is crucial to describe the structure of sets of lengths of Krull monoids (and other classes of monoids).

Definition 5.2. A finite subset $L \subset \mathbb{Z}$ is called an almost arithmetical multiprogression (AAMP) with bound M and difference d if

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

where $\{0, d\} \subset \mathcal{D} \subset [0, d]$, $\emptyset \neq L^* = [0, \max L^*] \cap (\mathcal{D} + d\mathbb{Z})$ and $L' \subset [-M, -1]$ and $L'' \subset \max L^* + [1, M]$.

The following result was obtained by A. Geroldinger [24]; meanwhile, results of this type are known for various other classes of monoids (see [30, Chapter 4]).

Theorem 5.3 (Structure Theorem for Sets of Lengths)**.** *Let G be a finite abelian group. There exists some $M_G \in \mathbb{N}$ and some finite set $\Delta_G^* \subset \mathbb{N}$ such that each element $L \in \mathcal{L}(G)$ is an AAMP with bound M_G and difference $d \in \Delta_G^*$.*

In Section 7 we discuss results on Δ_G^*. A recent result of the author [48], building on work of F. Halter-Koch and A. Geroldinger [30], indicates that the structure of $\mathcal{L}(G)$ indeed can be (depending on G) as complex as described by the Structure Theorem for Sets of Lengths. It might be interesting to note that the situation for infinite G is quite different. Namely, F. Kainrath [39] proved the following.

Theorem 5.4. *Let G be an infinite abelian group. Then, $\mathcal{L}(G)$ consists of all finite subsets of $\mathbb{N}_{\geq 2}$ and the sets $\{0\}$ and $\{1\}$.*

In other words, every set that possibly can be a set of lengths (recall that $\mathcal{B}(G)$ is a BF-monoid) is indeed a set of lengths.

6. Characterization via systems of sets of lengths

As discussed in the preceding section it seems very difficult to obtain explicit descriptions for $\mathcal{L}(G)$. Thus, as a more modest goal one seeks to understand the system of sets of lengths sufficiently well to decide whether the system of sets of lengths of a certain group is distinctive or whether there are other (non-isomorphic) groups with the same system of sets of lengths.

The following result summarizes for which types of groups it is known that they are indeed characterized by their system of sets of lengths. The first three parts are due to A. Geroldinger [25] the last due to the author [47]. We recall that by Theorem 5.1 and the subsequent discussion, the condition $\mathsf{D}(G) \geq 4$ below is necessary. In Section 8 we see that in fact $\mathsf{D}(G)$ is determined by $\mathcal{L}(G)$.

Theorem 6.1. *Let G, G' be finite abelian groups such that $\mathcal{L}(G) = \mathcal{L}(G')$. Suppose that $\mathsf{D}(G) \geq 4$ and one of the following statements holds:*

1. *G is cyclic.*
2. *G is an elementary 2-group.*

(3) *G is the direct sum of a cyclic group and a group of order* 2.
(4) *G is isomorphic to C_n^2 for some $n \ge 3$.*

Then, $G \cong G'$.

Though, we do not recall a proof of this result, we discuss the methods used in it in some detail in Sections 7 and 8. And, we indicate there in which way they are used in the proof. We point out that the proof of Theorem 6.1 is "constructive"; i.e., one could list properties of the systems of sets of lengths of the groups appearing in the theorem above, which are not shared by the system of sets of lengths of any other (up to isomorphy) finite abelian group.

Additionally, it can be shown that groups with small Davenport constant are characterized by their systems of sets of lengths. The following result extends a result of A. Geroldinger [25]; he proved the result for $4 \le \mathsf{D}(G) \le 7$. For completeness, we give a proof of the result for $4 \le \mathsf{D}(G) \le 7$ as well.

Theorem 6.2. *Let G, G' be finite abelian groups such that $\mathcal{L}(G) = \mathcal{L}(G')$. If $4 \le \mathsf{D}(G) \le 10$, then $G \cong G'$.*

The proof of this result makes ample use of Theorem 6.1 and the methods explained in Section 8; we give it in Section 9.

We end this section with a closely related result (see [49]) that shows that an elementary p-group is characterized by its system of sets of lengths among all elementary p-groups, apart from the already known exception.

Theorem 6.3. *Let p, q be primes and $r, s \in \mathbb{N}$. If $\mathcal{L}(C_p^r) = \mathcal{L}(C_q^s)$, then $(p, r) = (q, s)$ or $\{(p, r), (q, s)\} = \{(2, 2), (3, 1)\}$.*

7. The set of differences

A way to obtain more detailed information on the system of sets of lengths $\mathcal{L}(G)$ is to investigate the set

$$\Delta^*(G) = \{\min \Delta(G_0) \colon G_0 \subset G, \Delta(G_0) \ne \emptyset\}.$$

It is known that, for $|G| \ge 3$, Theorem 5.3 holds with $\Delta_G^* = \Delta^*(G)$. This set is also a main tool in results on characterizations via systems of sets of lengths, via its close connection to the set $\Delta_1(G)$ (see Section 8).

Though, many question on $\Delta^*(G)$, for general G, are still open there are a variety of results that give good or even complete descriptions of $\Delta^*(G)$ for special types of groups. We recall some of them below.

First, we recall some basic results on $\Delta(G_0)$. We note that for $G_1 \subset G_0$ one has $\Delta(G_1) \subset \Delta(G_0)$. And, one calls a set minimal non-half-factorial if each proper subset is half-factorial.

The first statement below is due to A. Zaks [55] and L. Skula [51] the others due to W.D. Gao and A. Geroldinger [24, 19].

Proposition 7.1. *Let G be a finite abelian group.*

(1) $\Delta(G_0) = \emptyset$ *if and only if* $\mathsf{k}(A) = 1$ *for each* $A \in \mathcal{A}(G_0)$.
(2) $\min \Delta(G_0) \mid \exp(G)(\mathsf{k}(A) - 1)$ *for each* $A \in \mathcal{A}(G_0)$.
(3) $\min \Delta(G_0) = \gcd \Delta(G_0)$.

The following result of W.D. Gao and A. Geroldinger [19] yields various elements that are contained in $\Delta^*(G)$.

Proposition 7.2. *Let G be a finite abelian group with $|G| \geq 3$. We have*

$$\{1, \dots, \mathsf{r}(G) - 1\} \subset \Delta^*(G)$$

and

$$\{d - 2 \colon 3 \leq d \mid \exp(G)\} \subset \Delta^*(G).$$

Moreover, $1 \in \Delta^*(G)$.

In the opposite direction various results are known as well. The following proposition summarizes result that are useful in investigations of $\min \Delta(G_0)$. The first two statements were obtained by W.D. Gao and A. Geroldinger (see [19]) and the last by the author (see [49]).

Proposition 7.3. *Let G be a finite abelian group and $G_0 \subset G$ a non-half-factorial set.*

(1) *If there exists an* $A \in \mathcal{A}(G_0)$ *with* $\mathsf{k}(A) < 1$, *then* $\min \Delta(G_0) \leq \exp(G) - 2$.
(2) *If* $\mathsf{k}(A) \geq 1$ *for each* $A \in \mathcal{A}(G_0)$, *then* $\min \Delta(G_0) \leq |G_0| - 2$.
(3) *If G_0 is minimal non-half-factorial and has a proper subset* $\emptyset \neq G_1 \subsetneq G_0$ *that is not a minimal generating set (with respect to inclusion) for* $\langle G_1 \rangle$. *Then,* $\min \Delta(G_0) \leq \mathsf{K}(G) - 1$ *and* $\mathsf{k}(A) \in \mathbb{N}$ *for each* $n \in \mathbb{N}$.

Motivated by results of this type the following terminology was introduced. A subset $G_0 \subset G$ of a finite abelian group is called an LCN-set if $\mathsf{k}(A) \geq 1$ for each $A \in \mathcal{A}(G_0)$. Moreover, let $\mathsf{m}(G) = \max\{\min \Delta(G_0) \colon G_0 \subset G \text{ non-half-factorial LCN}\}$ (if no such set G_0 exists, then $\mathsf{m}(G) = 0$).

The two propositions above are used in the proof of the following result, which was recently obtained by the author [47] and builds on results of [19].

Theorem 7.4. *Let G be a finite abelian group. Then,*

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

In particular, if G is a p-group, then

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

A key step in the proof of the above result is to show that

$$\mathsf{m}(G) \le \max\{\mathsf{K}(G) - 1, \mathsf{r}^*(G) - 1\}, \tag{1}$$

which together with Proposition 7.2 and Proposition 4.2 implies the result.

Proposition 7.2 and Theorem 7.4 show that $\Delta^*(G) = [1, \mathsf{r}(G) - 1]$ if G is a p-group with rank $\mathsf{r}(G) \ge \exp(G) - 1$. For groups with "large" exponent the situation is quite different. This is illustrated by the following results of A. Geroldinger and Y. ould Hamidoune [31] for cyclic groups and the author [49] for elementary p-groups.

Theorem 7.5. *Let G be a cyclic of order n. Then,*

$$\max \Delta^*(G) = n - 2 \quad \text{and} \quad \max\big(\Delta^*(G) \setminus \{n-2\}\big) = \left\lfloor \frac{n}{2} \right\rfloor - 1.$$

Further results on $\Delta^*(G)$ for cyclic groups can be found in a recent paper of S. Chang, S.T. Chapman, and W.W. Smith [9]. For a recent generalization of Theorem 7.5 see [47].

Theorem 7.6. *Let G be an elementary p-group with $\exp(G) = p$ and $\mathsf{r}(G) = r$. Then*

$$[1, r-1] \cup [\max\{1, p-r-1\}, p-2] \subset \Delta^*(G) \subset$$
$$[1, r-1] \cup [\max\{1, p-r-1\}, p-2] \cup [1, \frac{p-3}{2}].$$

In particular, $\Delta^*(G)$ is an interval if and only if $p \le 2r + 1$.

It is useful (see, e.g., Proposition 8.7) to not only know elements of $\Delta^*(G)$, but even to know the (precise) structure of subsets that yield these elements as their minimal distance, i.e., to solve the inverse problem. Some progress in this direction was made by the author [50].

Theorem 7.7. *Let G be a finite abelian group with $\exp(G) > \mathsf{m}(G) + 2 + \delta$ with $\delta \in \{0, 1\}$, and let $G_0 \subset G$ with $\min \Delta(G_0) = \max \Delta^*(G) - \delta$. Then $G_0 = \bigcup_{i=1}^s G_i$ where $\langle G_0 \rangle = \oplus_{i=1}^s \langle G_i \rangle$ and each G_i is either half-factorial or equal to,*

- *in case $\delta = 0$, $\{-g_i, g_i\}$ for some $g_i \in G$ with $\operatorname{ord} g_i = \exp(G)$,*
- *in case $\delta = 1$, $\{-g_i - h_i, g_i, h_i\}$ for independent $g_i, h_i \in G$ with order $\exp(G)$;*

and there exists at least one non-half-factorial G_i.

Note that the second statement implies that if $\exp(G) > \mathsf{m}(G) + 3$, then $\exp(G) - 3 \in \Delta^*(G)$ if and only if G has a subgroup isomorphic to $C_{\exp(G)}^2$.

In Section 9 we obtain a result that determines $\Delta^*(G)$ for some special groups of exponent 6, for which the result of this section do not (directly) yield a precise answer.

Finally, we remark that, as for $\mathcal{L}(G)$, for infinite abelian groups the problem of determining $\Delta^*(G)$ is solved. Recently, S.T. Chapman, W.W. Smith and the author [14] showed that for every infinite abelian group G one has $\Delta^*(G) = \mathbb{N}$.

8. Tools for characterization via systems of sets of lengths

In this section we collect results that can be used to characterize groups via their systems of sets of lengths. Vaguely, the idea is to express invariants of the group that by definition just depend on the system of sets of lengths by invariants whose definition uses the structure of the group in a more direct way.

8.1. **Elasticity and related notions.** The invariants $\rho(G)$ and $\rho_k(G)$, $k \in \mathbb{N}$, (see Section 3) obviously just depend on the system of sets of lengths. The following results (see [17, 13] and [30, Section 6.3]) show that some of these invariants can be expressed in terms of the Davenport constant.

Proposition 8.1. *Let G be a finite abelian group with $|G| \geq 2$.*

(1) $\rho(G) = \mathsf{D}(G)/2$.
(2) $\rho_{2k}(G) = k\,\mathsf{D}(G)$ *for each* $k \in \mathbb{N}$.
(3) $1 + k\,\mathsf{D}(G) \leq \rho_{2k+1}(G) \leq k\,\mathsf{D}(G) + \lfloor \mathsf{D}(G)/2 \rfloor$ *for each* $k \in \mathbb{N}$.

The value of $\rho_k(G)$ for odd k is unknown for most groups. Yet, it is known that depending on the structure of G equality can hold at either the upper or the lower bound: On the one hand, it is known that if $G = G_1 \oplus G_2$ with $|\,\mathsf{D}(G_1) - \mathsf{D}(G_2)| \leq 1$ and $\mathsf{D}(G) = \mathsf{D}(G_1) + \mathsf{D}(G_2) - 1$, then $\rho_{2k+1}(G) = k\,\mathsf{D}(G) + \lfloor \mathsf{D}(G)/2 \rfloor$ for each $k \in \mathbb{N}$. On the other hand, W.D. Gao and A. Geroldinger [21] recently proved that for cyclic G, $\rho_{2k+1}(G) = 1 + k|G|$ for each $k \in \mathbb{N}$. Moreover, M. Freeze and A. Geroldinger [18] showed that $\mathcal{V}_k(G)$ is an interval. Since we need it to apply Proposition 8.7 in the proof of Theorem 6.2, we recall (see

[16]) that for $G_0 \subset G$

$$\rho(G_0) \le \frac{\max\{\mathsf{k}(A) \colon A \in \mathcal{A}(G_0)\}}{\min\{\mathsf{k}(A) \colon A \in \mathcal{A}(G_0)\}}. \tag{2}$$

As a consequence of these results one gets the following (see [25]).

Proposition 8.2. *Let G, G' be finite abelian groups of order at least 2 such that $\mathcal{L}(G) = \mathcal{L}(G')$. Then $\mathsf{D}(G) = \mathsf{D}(G')$.*

Proposition 4.1 and 8.2 yield the following result (see [25]).

Theorem 8.3. *Let G be a finite abelian group. There exist at most finitely many (up to isomorphy) finite abelian groups G' with $\mathcal{L}(G) = \mathcal{L}(G')$.*

An improved understanding of the invariants $\rho_k(G)$ could lead to further progress on the problem of characterization of class groups via systems of sets of lengths. The same is true for the invariants $\lambda_k(G)$; yet by a recent result of A. Geroldinger [23] the invariants $\lambda_k(G)$ are determined in terms of the invariants $\rho_k(G)$.

The following result (see [25]) shows that a detailed analysis of sets of lengths containing 2, i.e. stemming from an element that is the product of two atoms, can be a powerful tool for this problem as well (see Section 9 for other investigations of this type).

Proposition 8.4. *Let G be a finite abelian group with $|G| \ge 3$. The following statements are equivalent.*

1. *G is an elementary 2-group or cyclic.*
2. *$\{2, \rho_2(G)\} \in \mathcal{L}(G)$.*
3. *If $L \in \mathcal{L}(G)$ and $\{2, \rho_2(G)\} \subset L$, then $L = \{2, \rho_2(G)\}$.*

8.2. **Long almost arithmetical (multi) progressions.** Above, we discussed methods building on the investigation of “small” sets of lengths. Now, we discuss methods based on the structure of long sets of lengths. The starting point for such methods is the Structure Theorem for Sets of Lengths (see Theorem 5.3) and related investigations.

In particular, we discuss that $\mathcal{L}(G) = \mathcal{L}(G')$ implies that $\Delta^*(G)$ is “almost equal” to $\Delta^*(G')$. To this end one considers the set $\Delta_1(G)$ that is defined as the set of all $d \in \mathbb{N}$ such that the following holds:

for each $k \in \mathbb{N}$ there exists some $L \in \mathcal{L}(G)$ such that,
for some $y \in \mathbb{N}_0$, $\{y + di \colon i \in [0, k]\} \subset L \subset y + d\mathbb{Z}$.

Since obviously $\Delta_1(G)$ just depends on $\mathcal{L}(G)$ it is clear that if $\mathcal{L}(G) = \mathcal{L}(G')$, then $\Delta_1(G) = \Delta_1(G')$. A result of W.D. Gao and A. Geroldinger [19] establishes a close connection between $\Delta_1(G)$ and $\Delta^*(G)$.

Proposition 8.5. *Let G be a finite abelian group. Then,*

$$\Delta^*(G) \subset \Delta_1(G) \subset \{d \mid d' \colon d' \in \Delta^*(G)\}.$$

In particular, the following is true.

Proposition 8.6. *Let G, G' be finite abelian groups such that $\mathcal{L}(G) = \mathcal{L}(G')$. Then,*

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

The following result enables one to make use of results on the structure of subsets G_0 with given $\min \Delta(G_0)$ (see Theorem 7.7) when trying to characterize groups by their system of sets of lengths.

For $d \in \mathbb{N}$, $M \in \mathbb{N}_0$, and $\{0, d\} \subset \mathcal{D} \subset [0, d]$, let $\mathcal{P}_M(\mathcal{D}, G)$ denote the set of all $B \in \mathcal{B}(G)$ with $\mathsf{L}(B)$ an AAMP with period $\mathcal{D}$ and bound M; moreover let $\mathcal{P}(\mathcal{D}, G, M) \subset \mathcal{P}_M(\mathcal{D}, G)$ denote the subset of all B with $\max \mathsf{L}(B) - \mathsf{L}(B) \ge 3M + (\max \Delta(G))^2$ (see [30]). We say that a subset $\{0, d\} \subset \mathcal{D} \subset [0, d]$ is periodic if there exists some $d' \mid d$ and $\{0, d'\} \subset \mathcal{D}' \subset [0, d']$ with $\mathcal{D} = \mathcal{D}' + d' \cdot [0, d/d' - 1]$, i.e., the image of $\mathcal{D}$ in $\mathbb{Z}/d\mathbb{Z}$ is periodic; otherwise we call it aperiodic.

Proposition 8.7. *Let G be a finite abelian group. Let $d, M \in \mathbb{N}$ and $\{0, d\} \subset \mathcal{D} \subset [0, d]$ aperiodic. Then*

$$\limsup_{\substack{B \in \mathcal{P}_M(\mathcal{D}, G) \\ \min \mathsf{L}(B) \to \infty}} \rho(B) \le \max\{\rho(G_0) \colon G_0 \subset G, \ d \mid \min \Delta(G_0)\}$$

where $\min \emptyset = 0$ *and* $\rho(\emptyset) = 1$.

Proof. Let $M(G)$ be sufficiently large that [30, Theorem 9.4.10] holds and additionally $M(G) \ge M$. Since the righthand side is at least 1, we may restrict our consideration to those $B \in \mathcal{P}_M(\mathcal{D}, G)$ for which $\max \mathsf{L}(B) - \min \mathsf{L}(B) \ge C$ for some arbitrary but fixed C. We note that for $B \in \mathcal{P}_M(\mathcal{D}, G) \setminus \mathcal{P}(\mathcal{D}, G, M(G))$, $\max \mathsf{L}(B) - \min \mathsf{L}(B) < 3M(G) + (\max \Delta(G))^2$. Thus, we may assume that $\mathcal{P}(\mathcal{D}, G, M(G)) \ne \emptyset$ and can consider

$$\limsup_{\substack{B \in \mathcal{P}(\mathcal{D}, G, M(G)) \\ \min \mathsf{L}(B) \to \infty}} \rho(B)$$

instead. Let $B \in \mathcal{P}(\mathcal{D}, G, M(G))$. By the proof of Theorem 9.4.10 in [30] we know that $B = FS$ with $F \in \mathcal{F}(G_0)$ for some G_0 with $d \mid \min \Delta(G_0)$ and $|S| \le \mathsf{b}_{\mathcal{D}}(G)$. Thus, $B = B_1 B_2$ with $B_1 \in \mathcal{B}(G_0)$ and $|B_2| \le \mathsf{b}_{\mathcal{D}}(G) + \mathsf{D}(G) - 1$. By Proposition 3.3 we know that $\min \mathsf{L}(B) \ge \min \mathsf{L}(B_1) + \max \mathsf{L}(B_2) - t$ and and $\max \mathsf{L}(B) \le \max \mathsf{L}(B_1) + \min \mathsf{L}(B_2) + t$ with $t = \mathsf{t}(B, \mathsf{Z}(B_2)) \le 2 \min \mathsf{L}(B_2)\, \mathsf{t}(G) \le 2(\mathsf{b}_{\mathcal{D}}(G) + \mathsf{D}(G) - 1)\, \mathsf{t}(G) =$

t_0. And, note that $\max \mathsf{L}(B_2) \le |B_2| \le \mathsf{b}_{\mathcal{D}}(G) + \mathsf{D}(G) - 1$. Thus, if $\min \mathsf{L}(B)$ is sufficiently large and thus $\min \mathsf{L}(B_1)$ is large as well, in particular greater than t_0, then we have

$$\begin{aligned}\rho(B) = \frac{\max \mathsf{L}(B)}{\min \mathsf{L}(B)} &\le \frac{\max \mathsf{L}(B_1) + \min \mathsf{L}(B_2) + t_0}{\min \mathsf{L}(B_1) + \max \mathsf{L}(B_2) - t_0} \\ &\le \frac{\max \mathsf{L}(B_1) + (\mathsf{b}_{\mathcal{D}}(G) + \mathsf{D}(G) - 1) + t_0}{\min \mathsf{L}(B_1) - t_0}.\end{aligned}$$

Consequently, for $\varepsilon > 0$, there exists some L such that for $\min \mathsf{L}(B) \ge L$, we have $\rho(B) \le \frac{\max \mathsf{L}(B_1)}{\min \mathsf{L}(B_1)} + \varepsilon \le \rho(G_0) + \varepsilon$. The claim follows. $\square$

Finally, we briefly sketch how the above mentioned tools are used in the proof of Theorem 6.1. Propositions 8.4, 8.6, 7.2, 8.2 and (an earlier version of) Theorem 7.5 were used (and established) to prove the first two statements of Theorem 6.1. Moreover, Proposition 8.2 and (an earlier version of) Theorem 7.4 together with Proposition 4.1 reduced Theorem 6.3 to the problem of distinguishing $\mathcal{L}(C_p^q)$ and $\mathcal{L}(C_q^{p-1})$ for primes p and q. To achieve this a special case of Proposition 8.7 was established. Also, in the proofs of the two last statements of Theorem 6.1 it is crucial that one has a good understanding of the relation of the Davenport constant to the maximum of the Δ_1-set and that this relation is rather special.

9. Proof of Theorem 6.2

In this section we prove Theorem 6.2. Using the results stated in Sections 7 and 8, only few obstacles remain. These are addressed in the following two subsections.

9.1. **On $\Delta_1(G)$ for two groups of exponent 6.** In this subsection we determine $\Delta_1(G)$ and $\Delta^*(G)$ for two groups for which the results of Section 7 do not give a precise answer.

Proposition 9.1.

(1) $\Delta^*(C_2^2 \oplus C_6) = \Delta_1(C_2^2 \oplus C_6) = \{1, 2, 4\}$.
(2) $\Delta^*(C_3^2 \oplus C_6) = \Delta_1(C_3^2 \oplus C_6) = \{1, 2, 4\}$.

Proof. 1. By Theorem 7.4 and Propositions 7.2 and 8.5 it suffices to show that $3 \notin \Delta^*(C_2^2 \oplus C_6)$. By Theorem 7.7 it suffices to show that $\mathsf{m}(C_2^2 \oplus C_6) \le 2$. Assume to the contrary that $G_0 \subset \Delta_1(C_2^2 \oplus C_6)$ is an LCN-set with $\min \Delta(G_0) = 3$; we may assume it is minimal non-half-factorial.

By Proposition 7.3 we have $|G_0| \ge 5$. Let $A \in \mathcal{A}(G_0)$ with $\mathsf{k}(A) > 1$; then $\operatorname{supp} A = G_0$. Note that by Proposition 4.2 $\mathsf{k}(A) \le 7/3$. Let

$H_0 \subset G_0$ a minimal, with respect to inclusion, generating subset for $\langle G_0 \rangle$. By Proposition 7.3 we may assume that $|H_0| \ge 4$. Let $H_0 \supset \{h_1, h_2, h_3, h_4\}$. Since $\langle h_1 \rangle \subsetneq \langle h_1, h_2 \rangle \subsetneq \langle h_1, h_2, h_3 \rangle \subsetneq C_2^2 \oplus C_6$, it follows that $\operatorname{ord} h_1 < 6$. Thus H_0 does not contain an element of order 6, and consequently H_0 contains an element h of order 2. Thus, since $h^2 \mid A$ and $\operatorname{supp}(h^{-2}A)$ is half-factorial, it follows that A^2 has a factorization of length $\mathsf{k}(A^2)$. Therefore, $3 \mid (2\,\mathsf{k}(A) - 2)$ and $\mathsf{k}(A) \ge 5/2$, a contradiction.

2. The argument is very similar. It suffices to show that $3 \notin \Delta_1(C_3^2 \oplus C_6)$ and again we show that $\mathsf{m}(G) \le 2$. Assume to the contrary that $G_0 \subset C_3^2 \oplus C_6$ is an LCN-set such that $\min \Delta(G_0) = 3$; we may assume that it is minimal non-half-factorial, it generates G, and $|G_0| \ge 5$. Let $A \in \mathcal{A}(G_0)$ with $\mathsf{k}(A) > 1$. Note that $\mathsf{k}(A) \le 8/3$. Let $H_0 \subset G_0$ a minimal generating subset. We may assume that $|H_0| \ge 4$. Again, it follows that H_0 does not contain an element of order 6, and consequently contains elements of order 2 and 3. Thus, A^2 has a factorization of length $\mathsf{k}(A^2) \in \mathbb{N}$ and $3 \mid (2\,\mathsf{k}(A) - 2)$, which implies that and $\mathsf{k}(A) = 5/2$. Yet, A^3 has a factorization of length $\mathsf{k}(A^3) \in \mathbb{N}$, a contradiction. □

9.2. **Two specific groups.** For the groups $C_3 \oplus C_6$ and $C_2^2 \oplus C_6$ the Davenport constant and the Δ_1-set are equal and Proposition 8.7 seems to be not applicable to establish the differences of the systems of sets of lengths. However, in the following we show that considering the structure of sets of lengths that contain 2, similarly to Proposition 8.4, a difference can be established.

The following is a simple special case of [30, Lemma 6.6.4].

Lemma 9.2. $\{2, 3, 6, 7, 8\} \in \mathcal{L}(C_3 \oplus C_6)$.

Proof. Let $C_3 \oplus C_6 = \langle e_1 \rangle \oplus \langle e_2 \rangle$ with $\operatorname{ord} e_1 = 3$ and $\operatorname{ord} e_2 = 6$. Let $U = (e_1 + e_2)e_1^2 e_2^5$. Then $\mathsf{L}((-U)U) = \{2, 3, 6, 7, 8\}$. □

In the remainder of the subsection we show that $\{2, 3, 6, 7, 8\} \notin \mathcal{L}(C_2^2 \oplus C_6)$. To achieve this we need to understand the structure of atoms of maximal lengths of $C_2^2 \oplus C_6$.

Lemma 9.3. *Let $A \in \mathcal{A}(C_2^2 \oplus C_6)$ with $|A| = 8$ and let $g \mid A$. Then* $\operatorname{ord} g \in \{2, 6\}$.

Proof. It suffices to prove that $\operatorname{ord} g \ne 3$. Assume to the contrary that $\operatorname{ord} g = 3$. Then $C_2^2 \oplus C_6 \cong C_2^3 \oplus \langle g \rangle$. We denote by π_2 and π_3 the projection to C_2^3 and $\langle g \rangle$, respectively. We have $\pi_2(g^{-1}A) \in \mathcal{B}(C_2^3)$. Since A is an atom, this sequence is the product of two atoms. Thus $\operatorname{supp} \pi_2(g^{-1}A) = C_2^3 \setminus \{0\}$, in particular the sequence is squarefree.

There exists some $h \in \langle g \rangle$ such that $\mathrm{supp}(g^{-1}A) \cap \pi_3^{-1}(h)$ contains at least three elements. We denote these by g_1, g_2, g_3 and observe that $\pi_2(g_1), \pi_2(g_2), \pi_2(g_3)$ is independent. Let $g_4 \mid g^{-1}A$ such that $\pi_2(g_4) = \sum_{i=1}^{3} \pi_2(g_i)$. It follows that $\pi_3(g_4) = g$, since otherwise $\sigma(gg_1 \dots g_4) = 0$ or $\sigma(g_1 \dots g_4) = 0$. For $1 \le i < j \le 3$, let $g_{i,j} \mid g^{-1}A$ such that $\pi_2(g_{i,j}) = \pi_2(g_i) + \pi_2(g_j)$. As above, we get that, for $\{i, j, k\} = \{1, 2, 3\}$ and $i < j$, $\sigma(g_{i,j} g_k g_4) = g$. Thus, $\pi_3(g_{i,j}) = \pi_3(g_{i',j'})$ for each admissible choice of i, j, i', j'. Consequently $\sigma(g_{1,2} g_{1,3} g_{2,3}) = 0$, a contradiction. □

The following lemma can be found (the additional statement implicitly) in [25]. We make frequent use of it in the proof of Proposition 9.5.

Lemma 9.4. *Let G be a finite abelian group with $|G| \ge 3$. Let $B \in \mathcal{B}(G)$. If $\{2, \mathsf{D}(G)\} \subset \mathsf{L}(B)$, then there exists some $U \in \mathcal{A}(G)$ and $|U| = \mathsf{D}(G)$ such that $B = (-U)U$. If additionally $\mathsf{D}(G) \ge 4$ and $\mathsf{D}(G) - 1 \in \mathsf{L}(B)$, then there exist (possibly equal) $g, h \in G$ such that $gh(g + h) \mid U$.*

Proof. Suppose that $\{2, \mathsf{D}(G)\} \subset \mathsf{L}(B)$. Since $2 \in \mathsf{L}(B)$, there exist atoms $U_1, U_2 \in \mathcal{A}(G)$ such that $B = U_1 U_2$. If $U_i = 0$ for some i, then $\mathsf{L}(B) = \{2\}$. Thus, $0 \nmid B$. Now, let $V_1 \dots V_{\mathsf{D}(G)}$ be a factorization of B of length $\mathsf{D}(G)$. We have $|V_j| \ge 2$ for each j, and $\sum_{j=1}^{\mathsf{D}(G)} |V_j| = |B| \le 2\,\mathsf{D}(G)$. Thus, in fact $|V_j| = 2$, i.e., $V_j = (-g_j)g_j$ for some g_j, and $|U_i| = \mathsf{D}(G)$. We have $V_j \nmid U_i$. Thus, either $g_j \mid U_1$ or $(-g_j) \mid U_1$, whereas the other of the two elements divides U_2. Thus it follows that $-U_1 = U_2$, which proves the first claim.

Now, suppose $\mathsf{D}(G) \ge 4$ and there exists a factorization of lengths $d = \mathsf{D}(G) - 1$, say $W_1 \dots W_d$ and assume $|W_i| \le |W_{i+1}|$. It follows that either $|W_d| = 4$ and $|W_{d-1}| = 2$ or $|W_{d-1}| = |W_d| = 3$ and $|W_{d-2}| = 2$. Yet, the former is impossible since $W_i = (-h_i)h_i$ for $i < d$ and thus, by the first claim, W_d would have to equal $gh(-g)(-h)$, which is not an atom. Thus, $|W_{d-1}| = |W_d| = 3$. This means $W_{d-1} = gh(-g - h)$ and $W_d = (-g)(-h)(g + h)$ for possibly equal $g, h \in G$. We have $W_{d-1} \nmid U$ and $W_{d-1} \nmid (-U)$. We may assume that $gh \mid U$ and $(-g - h) \mid (-U)$. It follows that $(g + h) \mid U$, which proves the second claim. □

Proposition 9.5. $\{2, 3, 6, 7, 8\} \notin \mathcal{L}(C_2^2 \oplus C_6)$

Proof. Assume to the contrary that there exists some $B \in \mathcal{B}(C_2^2 \oplus C_6)$ such that $\mathsf{L}(B) = \{2, 3, 6, 7, 8\}$. By Lemma 9.4 we know that there exists some $U \in \mathcal{A}(C_2^2 \oplus C_6)$ with $|U| = 8$ and $g, h \in C_2^2 \oplus C_6$ such that $B = (-U)U$ and $gh(g + h) \mid U$.

By Lemma 9.3 we know that U does not contain an element of order 3. Let $e \mid U$ with $\mathrm{ord}\, e = 6$, obviously such an element exists, such that

$v = \mathsf{v}_e(U)$ is maximal. Let $U = e^v R$. We have $C_2^2 \oplus C_6 = \langle e_1\rangle \oplus \langle e_2\rangle \oplus \langle e\rangle$ with $\operatorname{ord} e_i = 2$. Let π denote the projection of $C_2^2 \oplus C_6$ to $\langle e_1\rangle \oplus \langle e_2\rangle \cong C_2^2$.

Suppose $v = 5$. Then $\sigma(R) = e$. Moreover, R has no proper subsequence $R' \mid R$ with $\sigma(\pi(R')) = 0$, since otherwise $R'e^w$ for some suitable w, is a proper zero-sum subsequence of R. Consequently, $\pi(R) = e_1e_2(e_1 + e_2)$. Thus by Lemma 9.4 $7 \notin \mathsf{L}(B)$, a contradiction.

Suppose $v = 4$. Then $\sigma(R) = 2e$ and for each proper subsequence $R' \mid R$ with $\sigma(\pi(R')) = 0$ we have $\sigma(R') = e$. Thus, $0 \nmid \pi(R)$ and $\pi(R) = e_i^2e_j^2$. We show that $i \neq j$. Assume not. Then $R = \prod_{k=1}^4(e_1 + a_ke)$ with $a_k \in [0, 5]$ and we have $a_k + a_{k'} \equiv 1 \pmod 6$ for all $k \neq k'$. This is clearly impossible: we get $a_k + a_{k''} \equiv a_{k'} + a_{k''} \pmod 6$ thus $a_k \equiv a_{k'} \pmod 6$ and $2a_k \equiv 1 \pmod 6$, a contradiction.

Consequently $R = (e_1 + a_1e)(e_1 + b_1e)(e_2 + a_2e)(e_2 + b_2e)$ for $a_i, b_i \in [0, 5]$ and we have $a_i + b_i \equiv 1 \pmod 6$. If $\{2, 5\} \notin \{\{a_1, b_1\}, \{a_2, b_2\}\}$, then $\mathsf{L}(B) = \{2, 6, 7, 8\}$. If, say, $\{a_1, b_1\} = \{2, 5\}$, then $(e_1 + 2e)(e_1 - 5e)e^3 \cdot (e_1 - 2e)(e_1 + 5e)(-e)^3 \cdot (e_2 + a_2e)(e_2 + b_2e)(-e) \cdot (e_2 - a_2e)(e_2 - b_2e)e$ is a factorization of B of length 4, a contradiction.

Suppose $v = 3$. Then $\sigma(R) = 3e$ and for each proper subsequence $R' \mid R$ with $\sigma(\pi(R')) = 0$ we have $\sigma(R') \in \{e, 2e\}$. Thus $0 \nmid \pi(R)$ and we may assume that $\pi(R) = e_1e_2(e_1 + e_2)^3$. We have $R = (e_1 + ae)(e_2 + be)\prod_{i=1}^3(e_1 + e_2 + c_ie)$ for $a, b, c_i \in [0, 5]$. Since $a + b + c_i$ is congruent to 1 or 2 modulo 6 for each i, it follows that, say, $c_1 = c_2$. Since $2c_1 = c_1 + c_2$ is congruent to 2 (it cannot be 1) modulo 6, it follows that c_1 equals 1 or 4. Thus one of the following has to hold:

(1) $c_i = 1$ and $a + b \equiv 0 \pmod 6$.
(2) $c_i = 4$ and $a + b \equiv 3 \pmod 6$.
(3) $c_1 = c_2 = 1$, $c_3 = 0$ and $a + b \equiv 1 \pmod 6$.
(4) $c_1 = c_2 = 4$, $c_3 = 3$ and $a + b \equiv 4 \pmod 6$.

In the first two cases, by Lemma 9.4 $7 \notin \mathsf{L}(B)$, a contradiction. In the two other cases we have that

$$(e_1 + e_2 + c_1e)(e_1 + ae)(e_2 + be)(-e)^2 \cdot$$
$$(e_1 + e_2 - c_1e)(e_1 - ae)(e_2 - be)e^2 \cdot (e_1 + e_2 + c_2e)(e_1 + e_2 - c_2e) \cdot$$
$$(e_1 + e_2 + c_3e)(e_1 + e_2 - c_3e) \cdot (-e)e$$

is a factorization of B of length 5, a contradiction.

Suppose $v = 2$. If $0 \mid \pi(R)$, i.e. $3e \mid R$, then $\pi(0^{-1}R) \in \mathcal{A}(C_2^2)$, which is impossible. Thus we have $0 \nmid \pi(R)$ and we may assume that $\pi(R)$ is equal to e_1^6, $e_1^4e_2^2$, or $e_1^2e_2^2(e_1 + e_2)^2$. We have $\sigma(R) = 4e$. Moreover for each proper subsequence $R' \mid R$ with $\sigma(\pi(R')) = 0$ we have $\sigma(R') \in \{e, 2e, 3e\}$. In particular, if $R = R_1R_2R_3$ such that

$\sigma(\pi(R_i)) = 0$ for each i, then it follows that, say, $\sigma(R_1) = \sigma(R_2) = 1$ and $\sigma(R_3) = 2e$.

Suppose that $\prod_{i=1}^{4}(e_1 + a_i e) \mid R$ for $a_i \in [0, 5]$, that is we are in the first or second case. We may assume that $a_1 + a_2 \equiv 1 \pmod 6$ and $a_3 + a_4 \equiv 2 \pmod 6$, since by the same argument as in the case $v = 4$ not both sums can be congruent to 1. Checking all possible combinations of a_is, we see that the only choice (up to ordering) of a_is for which the sum of any two is congruent to 1 or 2, is either $a_1 = 0$ and $a_1 = a_2 = a_3 = 1$ or $a_1 = 3$ and $a_1 = a_2 = a_3 = 4$. Yet, in this case $(e_1 + e)^3 \mid U$ or $(e_1 + 4e)^3 \mid U$, contradicting the maximality of $\mathsf{v}_e(U)$.

Consequently, we have $R = \prod_{i=1}^{2}(e_1+a_i e)(e_2+b_i e)(e_1+e_2+c_i e)$ with $a_i, b_i, c_i \in [0, 5]$. We may assume that $a_1 + a_2 \equiv b_1 + b_2 \equiv 1 \pmod 6$ and $c_1 + c_2 \equiv 2 \pmod 6$. Now, let $R = T_1 T_2$ with $\pi(T_i) = e_1 e_2 (e_1 + e_2)$. Then $\{\sigma(T_1), \sigma(T_2)\} = \{e, 3e\}$. Thus $\{a_1 e, a_2 e\} + \{b_1 e, b_2 e\} + \{c_1 e, c_2 e\} = \{e, 3e\}$. Checking all cases, we see that this condition together with the above congruence conditions can only (up to the obvious symmetries) be fulfilled if

(1) $a_1 = b_1 = 0$, $a_2 = b_2 = 1$, and $c_1 = c_2 = 1$.
(2) $a_1 = b_1 = 3$, $a_2 = b_2 = 4$, and $c_1 = c_2 = 1$.
(3) $a_1 = 0$, $b_1 = 3$, $a_2 = 1$, $b_2 = 4$, and $c_1 = c_2 = 4$.

Now, let $V_i = (e_1+a_i e)(e_2-b_i e)(e_1+e_2+c_i e)(-e)$ for $i \in [1, 2]$. Then V_i is an atom and $B = V_1 V_2 (-V_1)(-V_2)$. Thus, $4 \in \mathsf{L}(B)$, a contradiction.

Suppose $v = 1$. Note that this implies that U is squarefree. Then $\sigma(R) = 5e$. First we assume $0 \mid \pi(R)$, i.e, $3e \mid R$. Then $\sigma((3e)^{-1}R) = 2e$. Since $|(3e)^{-1}R| = 6$, it follows that $R = (3e)R_1R_2R_3$ such that $\sigma(\pi(R_i)) = 0$ for each i. Let $\sigma(R_i) = a_i e$. Since U is an atom it follows that $e(3e)\prod_{i=1}^{3}(a_i e)$ is an atom. However, this is impossible, a contradiction.

Thus, we suppose that $0 \nmid \pi(R)$. We may assume that $\pi(R)$ is equal to $e_1 e_2 (e_1 + e_2)^5$ or to $e_1^3 e_2^3 (e_1 + e_2)$. We show that both is impossible. In the former case we get $\prod_{i \in [0,5] \setminus \{j\}}(e_1+e_2+ie) \mid U$ for some $j \in [0, 5]$. Yet, this sequence has a zero-sum subsequence, a contradiction. In the latter case we get $R = (e_1+e_2+ce)\prod_{i=1}^{3}(e_1+a_i e)(e_2+b_i e)$ for $a_i, b_i, c \in [0, 5]$ with pairwise distinct a_i and b_i. And, we have $\{a_1 e, a_2 e, a_3 e\} + \{b_1 e, b_2 e, b_3 e\} + ce \subset \{e, 2e, 3e, 4e\}$, which is impossible. □

9.3. **Proof of theorem.** Combining the results of Sections 7 and 8 and the preceding two subsections, we prove Theorem 6.2.

Proof of Theorem 6.2. Suppose that $\mathcal{L}(G) = \mathcal{L}(G')$ and that $\mathsf{D}(G) \geq 4$. By Proposition 8.2 we know that $\mathsf{D}(G') = \mathsf{D}(G)$. By Theorem 6.1 the claim follows if G is an elementary 2-group or cyclic. Thus, we may assume that neither G nor G' is an elementary 2-group or cyclic.

Suppose $\mathsf{D}(G) = 4$. By Proposition 4.1 there is no group with Davenport constant 4 that is not an elementary 2-group or cyclic.

Suppose $\mathsf{D}(G) = 5$. By our assumption on G and G' it follows that their exponent is 3 or 4. Thus by Proposition 4.1 it follows that G and and G' are isomorphic to $C_2 \oplus C_4$ or C_3^2. The claim follows by Theorem 6.1, or by noting that by Theorem 7.4 and Proposition 8.5 $\Delta_1(C_2 \oplus C_4) = [1, 2]$ and $\Delta_1(C_3^2) = \{1\}$.

Suppose $\mathsf{D}(G) = 6$. By Proposition 4.1 and our assumption on G and G' it follows that G and and G' are isomorphic to $C_2^2 \oplus C_4$.

Suppose $\mathsf{D}(G) = 7$. It follows that G and G' are isomorphic to one of the following groups: $C_2^3 \oplus C_4$, C_4^2, C_3^3 or $C_2 \oplus C_6$. We note that by Theorem 7.4 and Propositions 7.2 and 8.5 $\Delta_1(C_2^3 \oplus C_4) = [1, 3]$, $\Delta_1(C_4^2) = [1, 2]$, $\Delta_1(C_3^3) = [1, 2]$, and $\Delta_1(C_2 \oplus C_6) = \{1, 2, 4\}$. Since $\Delta_1(G) = \Delta_1(G')$, we only have to consider the case that $G \cong C_4^2$ and $G' \cong C_3^3$ (or conversely). By Theorem 6.1 $\mathcal{L}(C_4^2) \neq \mathcal{L}(C_3^3)$, and the claim follows.

Suppose $\mathsf{D}(G) = 8$. By Proposition 4.1 and our assumption on G and G' it follows that their exponent is at least 3 and at most 7; moreover it can be seen easily that it is not in $\{3, 5, 7\}$. Thus, G and G' are isomorphic two one of the following groups: $C_2 \oplus C_4^2$, $C_2^4 \oplus C_4$, $C_3 \oplus C_6$, $C_2^2 \oplus C_6$. We note that by Theorem 7.4 and Propositions 7.2 and 9.1 $\Delta_1(C_2 \oplus C_4^2) = [1, 2]$, $\Delta_1(C_2^4 \oplus C_4) = [1, 4]$, $\Delta_1(C_3 \oplus C_6) = \{1, 2, 4\}$ and $\Delta_1(C_2^2 \oplus C_6) = \{1, 2, 4\}$.

Since $\Delta_1(G) = \Delta_1(G')$, we only have to consider the case that $G \cong C_2^2 \oplus C_6$ and $G' \cong C_3 \oplus C_6$ (or conversely). However, by Lemma 9.2 and Proposition 9.5, we know that in this case $\mathcal{L}(G) \neq \mathcal{L}(G')$, a contradiction.

Suppose $\mathsf{D}(G) = 9$. By Proposition 4.1 and our assumption G and G' are isomorphic to one of the following groups: C_3^4, $C_2^5 \oplus C_4$, $C_2^2 \oplus C_4^2$, C_5^2, $C_2^3 \oplus C_6$, or $C_2 \oplus C_8$. By Theorem 6.1 we can exclude $C_2 \oplus C_8$ and C_5^2 from our considerations.

We note that by Theorem 7.4 and Proposition 7.2 $\Delta_1(C_3^4) = [1, 3]$, $\Delta_1(C_2^5 \oplus C_4) = [1, 5]$, $\Delta_1(C_2^2 \oplus C_4^2) = [1, 3]$, and $\Delta_1(C_2^3 \oplus C_6) = [1, 4]$.

Since $\Delta_1(G) = \Delta_1(G')$, we only have to consider the case that $G \cong C_2^2 \oplus C_4^2$ and $G' \cong C_3^4$ (or conversely). Using Proposition 8.7, we show that in this case $\mathcal{L}(G) \neq \mathcal{L}(G')$. Let $G_0 \subset G$ with $\min \Delta(G_0) = 3$. By Proposition 7.3 we know that G_0 is an LCN-set. Thus by (2) we know that $\rho(G_0) \leq \mathsf{K}(G) = 11/4$. Thus, by Proposition 8.7 we have that $\limsup \rho(B)$ for $B \in \mathcal{P}_0(\{0, 3\}, G)$ and $\min \mathsf{L}(B) \to \infty$ is bounded above by $11/4$. Now, let $e_1, \dots, e_4 \in G'$ be independent, $e_0 = \sum_{i=1}^4 e_i$ and $A = e_0(e_1 \dots e_4)^2$. Then $\mathsf{L}(A^{3k})$ is an arithmetical progression with difference 3, minimum $3k$, and maximum $9k$. Thus, we have that $\limsup \rho(B)$ for $B \in \mathcal{P}_0(\{0,3\}, G')$ and $\min \mathsf{L}(B) \to \infty$ is bounded below by 3. Thus, $\mathcal{L}(G) \neq \mathcal{L}(G')$, a contradiction.

Suppose $\mathsf{D}(G) = 10$. We get that G and G' are isomorphic to one of the following groups: C_4^3, $C_2^3 \oplus C_4^2$, $C_2^6 \oplus C_4$, $C_3^2 \oplus C_6$, or $C_2^2 \oplus C_8$. Recall that (see the remark after Proposition 4.1) $\mathsf{D}(C_2^4 \oplus C_6) > 10$.

By Theorem 7.4 and Proposition 7.2 $\Delta_1(C_4^3) = [1,2]$, $\Delta_1(C_2^3 \oplus C_4^2) = [1,4]$, $\Delta_1(C_2^6 \oplus C_4) = [1,6]$, $\Delta_1(C_3^2 \oplus C_6) = \{1,2,4\}$, and $6 \in \Delta_1(C_2^2 \oplus C_8) \subset [1,4] \cup \{6\}$. Since $\Delta_1(G) = \Delta_1(G')$, the claim follows. □

References

[1] S. D. Adhikari. *Aspects of combinatorics and combinatorial number theory.* Narosa Publishing House, New Delhi, 2002.

[2] S. D. Adhikari, Y. G. Chen, J. B. Friedlander, S. V. Konyagin, and F. Pappalardi. Contributions to zero-sum problems. *Discrete Math.*, 306(1):1–10, 2006.

[3] S. D. Adhikari and P. Rath. Davenport constant with weights and some related questions. *Integers*, 6:A30, 6 pp. (electronic), 2006.

[4] J. Amos, S. Chapman, N. Hine, and J. Paixão. Sets of lengths and unions of sets of lengths do not characterize numerical monoids. *Integers*, 7:A50, 8 pp. (electronic), 2007.

[5] D. D. Anderson, editor. *Factorization in integral domains*, volume 189 of *Lecture Notes in Pure and Applied Mathematics*, New York, 1997. Marcel Dekker Inc.

[6] D. D. Anderson and D. F. Anderson. Elasticity of factorizations in integral domains. *J. Pure Appl. Algebra*, 80(3):217–235, 1992.

[7] G. Bhowmik and J.-C. Schlage-Puchta. Davenport's constant for groups of the form $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$. In *Additive combinatorics*, volume 43 of *CRM Proc. Lecture Notes*, pages 307–326. Amer. Math. Soc., Providence, RI, 2007.

[8] L. Carlitz. A characterization of algebraic number fields with class number two. *Proc. Amer. Math. Soc.*, 11:391–392, 1960.

[9] S. Chang, S. T. Chapman, and W. W. Smith. On minimum delta set values in block monoids over cyclic groups. *Ramanujan J.*, 14(1):155–171, 2007.

[10] S. T. Chapman, editor. *Arithmetical properties of commutative rings and monoids*, volume 241 of *Lecture Notes in Pure and Applied Mathematics.* Chapman & Hall/CRC, Boca Raton, FL, 2005.

[11] S. T. Chapman and J. Coykendall. Half-factorial domains, a survey. In *Non-Noetherian commutative ring theory*, volume 520 of *Math. Appl.*, pages 97–115. Kluwer Acad. Publ., Dordrecht, 2000.

[12] S. T. Chapman, M. Freeze, W. D. Gao, and W. W. Smith. On Davenport's constant of finite abelian groups. *Far East J. Math. Sci. (FJMS)*, 5(1):47–54, 2002.

[13] S. T. Chapman, M. Freeze, and W. W. Smith. On generalized lengths of factorizations in Dedekind and Krull domains. In *Non-Noetherian commutative*

ring theory, volume 520 of *Math. Appl.*, pages 117–137. Kluwer Acad. Publ., Dordrecht, 2000.

[14] S. T. Chapman, W. A. Schmid, and W. W. Smith. On minimal distances in Krull monoids with infinite class group. *Bull. London Math. Soc.*, to appear.

[15] S. T. Chapman and W. W. Smith. Factorization in Dedekind domains with finite class group. *Israel J. Math.*, 71(1):65–95, 1990.

[16] S. T. Chapman and W. W. Smith. An analysis using the Zaks-Skula constant of element factorizations in Dedekind domains. *J. Algebra*, 159(1):176–190, 1993.

[17] S. T. Chapman and W. W. Smith. Generalized sets of lengths. *J. Algebra*, 200(2):449–471, 1998.

[18] M. Freeze and A. Geroldinger. Unions of sets of lengths. *Funct. Approx. Comment. Math.*, to appear.

[19] W. Gao and A. Geroldinger. Systems of sets of lengths. II. *Abh. Math. Sem. Univ. Hamburg*, 70:31–49, 2000.

[20] W. Gao and A. Geroldinger. Zero-sum problems in finite abelian groups: a survey. *Expo. Math.*, 24:337–369, 2006.

[21] W. D. Gao and A. Geroldinger. On products of k atoms. *Monatsh. Math.*, to appear.

[22] W. D. Gao, I. Z. Ruzsa, and R. Thangadurai. Olson's constant for the group $\mathbb{Z}_p \oplus \mathbb{Z}_p$. *J. Combin. Theory Ser. A*, 107(1):49–67, 2004.

[23] A. Geroldinger. Additive group theory and non-unique factorizations. In *Advanced Courses in Mathematics CRM Barcelona*, to appear.

[24] A. Geroldinger. Über nicht-eindeutige Zerlegungen in irreduzible Elemente. *Math. Z.*, 197(4):505–529, 1988.

[25] A. Geroldinger. Systeme von Längenmengen. *Abh. Math. Sem. Univ. Hamburg*, 60:115–130, 1990.

[26] A. Geroldinger. The cross number of finite abelian groups. *J. Number Theory*, 48(2):219–223, 1994.

[27] A. Geroldinger and F. Halter-Koch. Congruence monoids. *Acta Arith.*, 112(3):263–296, 2004.

[28] A. Geroldinger and F. Halter-Koch. Transfer principles in the theory of non-unique factorizations. In *Arithmetical properties of commutative rings and monoids*, volume 241 of *Lect. Notes Pure Appl. Math.*, pages 114–141. Chapman & Hall/CRC, Boca Raton, FL, 2005.

[29] A. Geroldinger and F. Halter-Koch. Non-unique factorizations: a survey. In *Multiplicative ideal theory in commutative algebra*, pages 207–226. Springer, New York, 2006.

[30] A. Geroldinger and F. Halter-Koch. *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory.* Chapman & Hall/CRC, 2006.

[31] A. Geroldinger and Y. O. Hamidoune. Zero-sumfree sequences in cyclic groups and some arithmetical application. *J. Théor. Nombres Bordeaux*, 14(1):221–239, 2002.

[32] A. Geroldinger and R. Schneider. The cross number of finite abelian groups. II. *European J. Combin.*, 15(4):399–405, 1994.

[33] B. Girard. A new upper bound for the cross number of finite abelian groups. *Israel J. Math.*, to appear.

[34] P. A. Grillet. *Commutative semigroups*, volume 2 of *Advances in Mathematics (Dordrecht)*. Kluwer Academic Publishers, Dordrecht, 2001.

[35] F. Halter-Koch. Non-unique factorizations of algebraic integers. *Funct. Approx. Comment. Math.*, to appear.
[36] F. Halter-Koch. Finitely generated monoids, finitely primary monoids, and factorization properties of integral domains. In *Factorization in integral domains (Iowa City, IA, 1996)*, volume 189 of *Lecture Notes in Pure and Appl. Math.*, pages 31–72. Dekker, New York, 1997.
[37] F. Halter-Koch. *Ideal systems*, volume 211 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 1998.
[38] J. Kaczorowski. A pure arithmetical definition of the class group. *Colloq. Math.*, 48(2):265–267, 1984.
[39] F. Kainrath. Factorization in Krull monoids with infinite class group. *Colloq. Math.*, 80(1):23–30, 1999.
[40] U. Krause. A characterization of algebraic number fields with cyclic class group of prime power order. *Math. Z.*, 186(2):143–148, 1984.
[41] U. Krause and C. Zahlten. Arithmetic in Krull monoids and the cross number of divisor class groups. *Mitt. Math. Ges. Hamburg*, 12(3):681–696, 1991.
[42] W. Narkiewicz. Finite abelian groups and factorization problems. *Colloq. Math.*, 42:319–330, 1979.
[43] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.
[44] J. E. Olson. A combinatorial problem on finite Abelian groups. I. *J. Number Theory*, 1:8–10, 1969.
[45] J. E. Olson. A combinatorial problem on finite Abelian groups. II. *J. Number Theory*, 1:195–199, 1969.
[46] D. E. Rush. An arithmetic characterization of algebraic number fields with a given class group. *Math. Proc. Cambridge Philos. Soc.*, 94(1):23–28, 1983.
[47] 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, submitted.
[48] W. A. Schmid. A realization theorem for sets of lengths, submitted.
[49] W. A. Schmid. Differences in sets of lengths of Krull monoids with finite class group. *J. Théor. Nombres Bordeaux*, 17(1):323–345, 2005.
[50] W. A. Schmid. Periods of sets of lengths: a quantitative result and an associated inverse problem. *Colloq. Math.*, 113:33–53, 2008.
[51] L. Skula. On c-semigroups. *Acta Arith.*, 31(3):247–257, 1976.
[52] R. Thangadurai. A variant of Davenport's constant. *Proc. Indian Acad. Sci. Math. Sci.*, 117(2):147–158, 2007.
[53] P. van Emde Boas. A combinatorial problem on finite Abelian groups. II. Technical report, Math. Centrum, Amsterdam, Afd. Zuivere Wisk. ZW 1969-007, 60 p. , 1969.
[54] P. van Emde Boas and D. Kruyswijk. A combinatorial problem on finite abelian groups. III. Technical report, Math. Centrum, Amsterdam, Afd. zuivere Wisk. ZW 1969-008, 34 p. , 1969.
[55] A. Zaks. Half factorial domains. *Bull. Amer. Math. Soc.*, 82(5):721–723, 1976.

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität, Heinrichstrasse 36, 8010 Graz, Austria
E-mail address: `wolfgang.schmid@uni-graz.at`