A realization theorem for sets of lengths

Wolfgang A. Schmid*
Institut für Mathematik und Wissenschaftliches Rechnen
Karl–Franzens–Universität Graz
Heinrichstraße 36
8010 Graz, Austria
wolfgang.schmid@uni-graz.at

*Supported by the FWF (P18779-N13).

Abstract

By a result of G. Freiman and A. Geroldinger [J. Number Theory 85, 2000] it is known that the set of lengths of factorizations of an algebraic integer (in the ring of integers of an algeraic number field), or more generally of an element of a Krull monoid with finite class group, has a certain structure: it is an almost arithmetical multiprogression for whose difference and bound only finitely many values are possible, and these depend just on the class group.

We establish a sort of converse to this result, showing that for each choice of finitely many differences and of a bound there exists some number field such that each almost arithmetical multiprogression with one of these difference and that bound is up to shift the set of lengths of an algebraic integer of that number field. Moreover, we give an explicit sufficient condition on the class group of the number field for this to happen.

Keywords: algebraic number field, almost arithmetical multiprogression, Krull monoid, zero-sum sequence

1 Introduction and main result

An atomic monoid is a commutative cancellative semigroup with identity element such that each non-invertible element has a factorization (i.e., a finite product decomposition) into irreducible elements. The multiplicative monoid of the ring of algebraic integers of a number field (or any noetherian domain) is an atomic monoid.

Let $a \in H$ be an element of an atomic monoid and let $a = u_1 \dots u_n$ be a factorization of a into irreducible elements $u_i \in H$. The integer n is called the lengths of this factorization of a. The set of lengths of a, denoted $\mathsf{L}_H(a)$, is defined as the set of all n such that a has a factorization of length n. The set of lengths of an invertible element is defined to be $\{0\}$. If H is v-noetherian, e.g., H is the multiplicative monoid of a noetherian domain, then the sets of lengths of its elements are finite sets. All monoids considered in this paper fulfil this condition.

The monoid H is called half-factorial if $|\mathsf{L}_H(a)| = 1$ for each $a \in H$. Obviously, factorial monoids are half-factorial and L. Carlitz [4] showed that the ring of integers of an algebraic number field is half-factorial if and only if its ideal class group has at most two elements. Since that time the investigation of half-factorial domains and monoids received much attention (see, e.g., the recent papers [6, 7, 15, 17]).

Suppose that H is not half-factorial. Then an easy argument shows that for every $k \in \mathbb{N}$ there is some $a \in H$ such that $|\mathsf{L}_H(a)| \ge k$. The investigation of the structure of sets of lengths is a central topic in the theory of non-unique factorizations (see, e.g., the proceedings [1, 5] or the recent paper [3] for, among others, results on elasticities and delta sets).

For many classes of monoids satisfying natural finiteness conditions, including Krull monoids with finite class group and orders in holomorphy rings of global fields, sets of lengths are almost arithmetical multiprogressions (AAMPs for short) with universal bounds on their parameters (see [10, Section 4.7] also cf. Theorem 1.2 below).

We recall the definition of AAMPs. In the present form it was introduced in [8] (also see [10, Definition 4.2.1]).

Definition 1.1. Let $d \in \mathbb{N}$ and $M \in \mathbb{N}_0$. Further, let $\{0, d\} \subset \mathcal{D} \subset [0, d]$, let $-L', L'' \subset \mathbb{N}$ be finite sets such that $-L', L'' \subset [1, M]$, and let $y \in \mathbb{Z}$, $l' \in \mathbb{N}_0$, and $L^* = [0, l'] \cap (\mathcal{D} + d\mathbb{Z})$. The set

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

is called an almost arithmetical multiprogression (AAMP for short) with difference d and bound M. Moreover, $\mathcal{D}$ and y are called period and shift of L, respectively, and the sets $y + L'$, $y + L^*$, and $y + l' + L''$ are called the initial part, the central part, and the end part of L, respectively.

We recall the structure theorem for sets of lengths for Krull monoids with finite class group (cf. [10, Theorems 4.6.6 and 2.9.12]). As usual $\mathcal{L}(H) = \{\mathsf{L}_H(a) \colon a \in H\}$ denotes the system of sets of lengths of H.

Theorem 1.2. *Let H be a Krull monoid with finite class group. Then there exists an $M \in \mathbb{N}_0$ and a finite non-empty set $\Delta^* \subset \mathbb{N}$, for which a precise description is known, such that the following holds: every $L \in \mathcal{L}(H)$ is an AAMP with difference $d \in \Delta^*$ and bound M.*

Let H be as above and suppose H is not half-factorial. As mentioned above, there exist elements with arbitrarily large sets of lengths, but by this theorem the initial and end part are universally bounded and only the highly structured central part can be arbitrarily large.

Krull monoids with finite class group are a basic class of monoids for which such a structure theorem holds true. The aim of this paper is to prove, for this class of monoids, the following realization theorem for sets of lengths.

Theorem 1.3. *Let $M \in \mathbb{N}_0$ and let $\emptyset \neq \Delta^* \subset \mathbb{N}$ be a finite set. Then there exists a Krull monoid H with finite class group such that the following holds: for every AAMP L with difference $d \in \Delta^*$ and bound M there is some $y_{H,L}$ such that*

$$y + L \in \mathcal{L}(H) \text{ for all } y \geq y_{H,L}.$$

Indeed, there exists a number field such that the multiplicative monoid of its ring of algebraic integers has this property.

Our proof of Theorem 1.3 does not only yield the existence of a monoid H, but allows to extract a sufficient condition on the class group of H for $\mathcal{L}(H)$ to contain the relevant sets (see Remark 4.9); for these monoids we give an upper bound for the constants $y_{H,L}$ as well.

We note that a condition like $y \geq y_{H,L}$ is necessary: for an atomic monoid H, for each $L \in \mathcal{L}(H) \setminus \{\{0\}\}$ the ratio $\sup L / \min L$ does (by definition) not exceed $\rho(H)$ the elasticity of H, which for Krull monoids with finite class group is known to be finite (see [18] and [2] or [10, Theorem 3.4.1]).

First but weaker realization theorems for sets of lengths are obtained in [10, Section 4.8]. In locally tame, strongly primary monoids (e.g., in one-dimensional local noetherian domains) the structure theorem for sets is simpler than it is for Krull monoids (see [10, Theorem 4.3.6]), and a first realization theorem for sets of lengths for this class of monoids was recently given in [11].

If G is a an abelian group with $|G| \neq 2$, then the monoid of zero-sum sequences over G is a Krull monoid with class group (isomorphic to) G, and conversely the system of sets of lengths of a Krull monoid is equal to the system of sets of lengths of a monoid of zero-sum sequences, namely the block monoid associated to H, a notion introduced by W. Narkiewicz [16]. We outline this in more detail in Section 2. In Section 3 we formulate our main technical result (Theorem 3.1), which is a result on monoids of zero-sum sequences, and derive Theorem 1.3 from it. The proof of Theorem 3.1 is given in Section 4.

2 Preliminaries

We recall some further terminology and notation, which is consistent with [10] and [9].

For $m, n \in \mathbb{Z}$ let $[m, n] = \{z \in \mathbb{Z} \colon m \le z \le n\}$. For A, B subsets of an additive semigroup S and $n \in \mathbb{N}$ let $A + B = \{a + b \colon a \in A,\, b \in B\}$ and $n \cdot A = \{na \colon a \in A\}$; since no confusion is to be expected, we use the common notation $d\mathbb{Z}$ instead of $d \cdot \mathbb{Z}$. Moreover, if the elements of A are invertible we write $-A$ for $\{-a \colon a \in A\}$ and we write $a + A$ for $\{a\} + A$.

Let $(G, +)$ be a (finite) abelian group. Elements $e_1, \ldots, e_r \in G$ are called independent if $\sum_{i=1}^r m_i e_i = 0$ with $m_i \in \mathbb{Z}$ implies that $m_i e_i = 0$ for all $i \in [1, r]$. If $g = \sum_{i=1}^r m_i e_i$, then we refer to $m_i e_i$ as the i-coordinate of g.

Let $G_0 \subset G$. We denote by $\mathcal{F}(G_0)$ the multiplicatively written free abelian monoid over G_0. An element $S \in \mathcal{F}(G_0)$ is called a sequence over G_0. By definition there exist uniquely determined $v_g \in \mathbb{N}_0$ such that $S = \prod_{g \in G_0} g^{v_g}$ and up to order uniquely determined $g_1, \ldots, g_l \in G$ such that $S = g_1 \ldots g_l$. The sequence S is called a zero-sum sequence if its sum $\sigma(S) = \sum_{i=1}^l g_i$ is equal to $0 \in G$. The set of all zero-sum sequences over G_0 is denoted by $\mathcal{B}(G_0)$. This set is a submonoid of $\mathcal{F}(G_0)$ and it is called the block monoid over G_0.

Block monoids are Krull monoids and additionally are of great impor-

tance in the investigation of the arithmetic of Krull monoids. For a detailed discussion of Krull monoids and block monoids we refer to the monographs [13, 10, 12]. We recall some basic results (cf., e.g., Proposition 2.5.6, Theorem 3.4.10, and Proposition 7.3.1 in [10]).

Lemma 2.1. *Let G be an abelian group and $\emptyset \neq G_0 \subset G$.*

1. *$\mathcal{B}(G_0)$ is a Krull monoid and $\mathcal{L}(\mathcal{B}(G_0)) \subset \mathcal{L}(\mathcal{B}(G))$.*
2. *If $|G| \neq 2$, then the class group of $\mathcal{B}(G)$ is (isomorphic to) G and each class contains a prime divisor.*
3. *If $G = G_1 \oplus G_2$, then $\mathcal{L}(\mathcal{B}(G_1)) + \mathcal{L}(\mathcal{B}(G_2)) \subset \mathcal{L}(\mathcal{B}(G))$.*
4. *If $0 \in G_0$ and $L \in \mathcal{L}(\mathcal{B}(G_0))$, then $y + L \in \mathcal{L}(\mathcal{B}(G_0))$ for each $y \in \mathbb{N}_0$.*

For ease of notation we write $\mathcal{L}(G_0)$ instead of $\mathcal{L}(\mathcal{B}(G_0))$ and $\mathsf{L}(B)$ instead of $\mathsf{L}_{\mathcal{B}(G_0)}(B)$.

Proposition 2.2. *Let H be a Krull monoid with class group G and let $G_0 \subset G$ denote the subset of classes containing prime divisors. Then $\mathcal{L}(H) = \mathcal{L}(G_0)$.*

3 A conditional proof of Theorem 1.3

In this section we formulate our main technical result (Theorem 3.1) and show that it implies Theorem 1.3. The proof of Theorem 3.1 is given in the following section.

Theorem 3.1. *Let $d, M \in \mathbb{N}$. Further, let $\{0, d\} \subset \mathcal{D} \subset [0, d]$ and let $L' \subset [-M, -1] \cap (\mathcal{D} + d\mathbb{Z})$ and $L'' \subset [1, M] \cap (\mathcal{D} + d\mathbb{Z})$. Let G be a finite abelian group and let $e_1, \ldots, e_r, f, e'_0 \ldots, e'_{\lceil M/d \rceil - 1} \in G$ be independent such that the following holds:*

- $r \ge |L'| + |L''| + \lceil M/d \rceil (|\mathcal{D}| - 1)$,
- $\operatorname{ord} e_1 \ge 3$ *and* $\operatorname{ord} e_i \ge 5$ *for* $i \in [2, r]$,
- $\operatorname{ord} f \ge 2(d\lceil M/d \rceil + \max L'' - \min L') + 1$ *(where* $\max \emptyset = \min \emptyset = 0$*)*,
- $\operatorname{ord} e'_i = d(\lceil M/d \rceil + i) + 2$ *for* $i \in [0, \lceil M/d \rceil - 1]$.

If $l \ge \frac{(3\lceil M/d\rceil+5)\lceil M/d\rceil}{2}$*, say* $l = \frac{(3\lceil M/d\rceil+5)\lceil M/d\rceil}{2} + t$ *with* $t \in \mathbb{N}_0$*, then, for*

$$y_l = 2 + M + 2\left(\lceil M/d\rceil + 1 + \left\lceil \frac{t + \lceil M/d\rceil}{2\lceil M/d\rceil - 1} \right\rceil\right),$$

and $y \ge y_l$*,*

$$y + \big(L' \cup ((\mathcal{D} + d\mathbb{Z}) \cap [0, ld]) \cup (dl + L'')\big) \in \mathcal{L}(G).$$

Moreover, if additionally $r \ge |L'| + |L''| + (|\mathcal{D}| - 1)\frac{(3\lceil M/d\rceil+5)\lceil M/d\rceil-2}{2}$ *and*

$$\operatorname{ord} f \ge 2\left(d\frac{(3\lceil M/d\rceil + 5)\lceil M/d\rceil - 2}{2} + \max L'' - \min L'\right) + 1,$$

then the condition on l *can be dropped and for* $l < \frac{(3\lceil M/d\rceil+5)\lceil M/d\rceil}{2}$ *we can set* $y_l = 2 + M$*.*

Using Theorem 3.1 we prove Theorem 1.3.

Proof of Theorem 1.3. First, we assert that it suffices to show that there exists a finite abelian group G such that $\mathcal{L}(G)$ contains the relevant sets. Except for the additional statement regarding number fields this is immediate, since by Lemma 2.1 $\mathcal{B}(G)$ is a Krull monoid. The result for number fields is obtained in the following way (cf. [10, Remark 4.8.9]): it suffices to recall that the multiplicative monoid of the ring of algebraic integers is a Krull monoid (its class group is equal to the usual ideal class group and each class contains a prime divisor, i.e., prime ideal) and that for each finite abelian group there exists a number field whose class group has a subgroup isomorphic to this group (see, e.g., [19, Corollary 3.9]). Thus, the claim follows by Proposition 2.2 and Lemma 2.1.

Now we proceed to show the existence of such a group. Let L be an AAMP with difference $d \in \Delta^*$ and bound M, i.e.,

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

where $L^* = [0, l'] \cap (\mathcal{D} + d\mathbb{Z})$, $L' \subset [-M, -1]$ and $L'' \subset [1, M]$ with $y \in \mathbb{Z}$, $l' \in \mathbb{N}_0$. Without restriction we may assume $M \ge 1$.

Let $l = \lfloor l'/d \rfloor$. Then

$$L = y + \big(L' \cup \big((\mathcal{D} + d\mathbb{Z}) \cap [0, ld]\big) \cup (ld + \overline{L''})\big) \subset y + \mathcal{D} + d\mathbb{Z}$$

where $\overline{L''} \subset [1, M+d-1]$ and necessarily $L', \overline{L''} \subset \mathcal{D} + d\mathbb{Z}$.

By Theorem 3.1, with bound $M+d-1$, we know that there exists a finite abelian group $G_{\mathcal{D},L',\overline{L''}}$ such that for each $l \in \mathbb{N}_0$ there exists some y_l such that for $y \geq y_l$

$$y + \big(L' \cup \big((\mathcal{D} + d\mathbb{Z}) \cap [0, ld]\big) \cup (ld + \overline{L''})\big) \in \mathcal{L}(G_{\mathcal{D},L',\overline{L''}}).$$

Let G be a finite abelian group that has a subgroup isomorphic to $G_{\mathcal{D},L',\overline{L''}}$ as above for each of the admissible choice of $\mathcal{D}$, L', and $\overline{L''}$, i.e., $\{0, d\} \subset \mathcal{D} \subset [0, d]$ with $d \in \Delta^*$, $-L', \overline{L''} \subset [1, M+d-1]$ and moreover $L', \overline{L''} \subset \mathcal{D} + d\mathbb{Z}$. Since $d \leq \max \Delta^* < \infty$, there are only finitely many such choices. Then, $\mathcal{L}(G)$ contains all the required AAMPs. □

4 Proof of Theorem 3.1

The general approach is as in [10, Theorem 4.8.6]. However, various details are handled somewhat differently to get improved dependence on the constants and to make the condition on the class group explicit. First, we prove several auxiliary results, which we combine in Subsection 4.4 to prove Theorem 3.1.

4.1 An additive decomposition

We show that we can write an AAMP L with sufficiently large central part in the form $L = L_1 + L_2$ where L_1 is a small set, in the sense that $\max L_1 - \min L_1$ is bounded above by a constant that only depends on the the bound and differences of L, and L_2 is an AAMP of a special form.

Lemma 4.1. *Let $d \in \mathbb{N}$ and $s, s' \in \mathbb{N}$ and $M \in \mathbb{N}_0$ such that $s \leq s'$ and $M \leq ds$. Further, let $\{0, d\} \subset \mathcal{D} \subset [0, d]$ and $-L', L'' \subset [1, M]$ such that $L', L'' \subset \mathcal{D} + d\mathbb{Z}$. Then*

$$\begin{aligned} L' \cup \big((\mathcal{D} + d\mathbb{Z}) \cap [0, d(s'+2s)]\big) \cup (d(s'+2s) + L'') = \\ \big(L' \cup ((\mathcal{D} + d\mathbb{Z}) \cap [0, ds]) \cup (ds + L'')\big) + \big(\{0\} \cup d \cdot [s, s'] \cup \{d(s'+s)\}\big) \end{aligned}$$

Proof. Let $L = L' \cup ((\mathcal{D} + d\mathbb{Z}) \cap [0, d(s'+2s)]) \cup (d(s'+2s) + L'')$, $L_1 = L' \cup ((\mathcal{D} + d\mathbb{Z}) \cap [0, ds]) \cup (ds + L'')$, and $L_2 = \{0\} \cup d \cdot [s, s'] \cup \{d(s'+s)\}$. Clearly $L \subset L_1 + L_2$ and we only have to prove the reverse inclusion. Since

$L_1 \subset \mathcal{D} + d\mathbb{Z}$ and $L_2 \subset d\mathbb{Z}$, it follows that $L_1 + L_2 \subset \mathcal{D} + d\mathbb{Z}$. It remains to show that each element in $L_1 + L_2$ that is less than 0 or greater than $d(s'+2s)$ is contained in L' or $d(s'+2s) + L''$, respectively. Let $z = x + y \in L_1 + L_2$, where $x \in L_1$ and $y \in L_2$, be negative. It is clear that $x \in L'$ and it suffices to assert that $y = 0$. Assume not. Then $y \ge ds \ge M$ and since $x \ge -M$, we get $z \ge 0$, a contradiction. Similarly, if $z' > d(s'+2s)$ and $z' = x' + y' \in L_1 + L_2$, then since $\max L_2 = d(s'+s)$ we have $x' > ds$ and thus $x' \in ds + L''$ and since $\max L_1 \le 2ds$ we have $y' > ds'$ and thus $y' = d(s'+s)$. □

The point of this result is that by Lemma 2.1 it thus suffices to construct a group G_1 and a group G_2 whose system of sets of lengths contain the small sets and the special AAMPs, respectively. In the next two subsections we do this. We note that those AAMPs for which Lemma 4.1 is not applicable are already small sets in the above sense.

4.2 Realization of certain special AAMPs

We show how to obtain the AAMPs with period $\{0, d\}$ appearing in Lemma 4.1. Yet, we have to impose an additional restriction on the size of the central part. The sets not fulfilling this condition and, more importantly, the sets in the additive decomposition of which these sets arise are small sets in the sense of the preceding subsection.

We first show that one can write the AAMPs in question as the sum of simpler sets, namely arithmetical progressions. This means we prove that in fact they are multidimensional arithmetical progressions, and it is well-known how to obtain (multidimensional) arithmetical progressions as sets of lengths (see [10, Corollary 4.1.3] and Proposition 4.4). To do so, we first prove a simple lemma; a weaker version of this lemma would be a special case of a result on numerical monoids (cf. [10, Proposition 2.9.4], yet note that there is a minor flaw in that statement).

Lemma 4.2. *Let $s \in \mathbb{N}$ and let $k_i \in \mathbb{N}$ for $i \in [0, s-1]$ and suppose $k_0 \ge 2$. Further, let $S = \sum_{i=0}^{s-1}(s+i)k_i$. Then*

$$L = \sum_{i=0}^{s-1}(s+i) \cdot [0, k_i] = \{0\} \cup [s, S-s] \cup \{S\}.$$

Proof. For $s = 1$ the assertion is trivial and we suppose $s \ge 2$. It is immediate that $\min L = 0$, $\max L = S$, $[1, s-1] \cap L = \emptyset$ and $[S-(s-1), S-1] \cap L = \emptyset$.

Thus, it remains to show that $[s, S-s] \subset L$. Assume this is not true and let $n = \min\{[s, S-s] \setminus L\}$. Since $[s, 2s-1] \subset L$, it follows that $n-1 \geq s$ and thus $n-1 \in L$. Let $h_i \in [0, k_i]$ such that $n-1 = \sum_{i=0}^{s-1}(s+i)h_i$. If $h_j \neq 0$ for some $j \in [0, s-2]$, it follows that $h_{j+1} = k_{j+1}$, since otherwise $n = (n-1) - (s+j) + (s+j+1) \in L$. And, if $h_{s-1} \neq 0$ it follows that $h_0 \geq k_0 - 1$, since otherwise $n = (n-1) - (2s-1) + 2s \in L$. Since $n-1 \neq 0$, not all of the h_is are equal to 0, and by the above reasoning it follows that $h_0 \geq k_0 - 1$ and $h_i = k_i$ for each $i \in [1, s-1]$. Thus $n-1 \geq S-s$, a contradiction. □

The following result is an almost immediate consequence of Lemma 4.2.

Proposition 4.3. *Let $s, s' \in \mathbb{N}$ such that $s' \geq (3s+1)s/2$ and let $t = s' - (3s+1)s/2$. There exist $k_i \in \mathbb{N}$ for $i \in [0, s-1]$ such that $\sum_{i=0}^{s-1} k_i = s + 1 + \lceil (t+s)/(2s-1) \rceil$ and*

$$\sum_{i=0}^{s-1} (s+i) \cdot [0, k_i] = \{0\} \cup [s, s'] \cup \{s + s'\}. \tag{1}$$

Proof. For each $n \in \mathbb{N}$ with $n \geq s$ there exist $h_i \in \mathbb{N}_0$ such that $\sum_{i=0}^{s-1} h_i(s+i) = n$; moreover, we can choose the h_is in such a way that $\sum_{i=0}^{s-1} h_i = \lceil n/(2s-1) \rceil$. Thus, for each $s' \geq 2s + \sum_{i=1}^{s-1}(s+i) = (3s+1)s/2$ there exist $k_i \in \mathbb{N}$ with $k_0 \geq 2$ such that $\sum_{i=0}^{s-1} k_i(s+i) = s' + s$ and we can choose the k_is in such a way that $\sum_{i=0}^{s-1} k_i = s + 1 + \lceil (t+s)/(2s-1) \rceil$. By Lemma 4.2 the result follows. □

Simply multiplying (1) by the difference d, our task is reduced to obtaining arithmetical progressions with difference $(s+i)d$ and prescribed lengths as sets of lengths. Several ways to achieve this are known. We recall two natural ways ([10, Propositions 4.1.2 and 6.8.1]):

- Let $g \in G$ be an element with $\operatorname{ord} g = n$. Then $\mathsf{L}\big(((-g)g)^{nk}\big) = \{2k + i(n-2) \colon i \in [0, k]\}$.
- Let $e_1, \ldots, e_r \in G$ be independent elements with $\operatorname{ord} e_i = n$, and $e_0 = \sum_{i=1}^{r} e_i$. Then $\mathsf{L}((e_0 \prod_{i=1}^{r} e_i^{n-1})^k) = \{k + i(r-1) \colon i \in [0, k - \lceil \frac{k}{n} \rceil]\}$.

We use the former construction in the proof of the following result, which summarizes the argument of this subsection. In Remark 4.5 we briefly discuss the other option.

Proposition 4.4. *Let $s, d \in \mathbb{N}$. Let $G = \oplus_{i=0}^{s-1} \langle e_i \rangle$ with $\operatorname{ord} e_i = d(s+i)+2$ for $i \in [0, s-1]$. For each $s' = t + ((3s+1)s/2)$, where $t \in \mathbb{N}_0$, and $y \geq 2(s+1+\lceil (t+s)/(2s-1) \rceil)$,*

$$y + (\{0\} \cup d \cdot [s, s'] \cup \{d(s'+s)\}) \in \mathcal{L}(G).$$

Proof. By Proposition 4.3, there exist $k_i \in \mathbb{N}$ with $\sum_{i=0}^{s-1} k_i = s + 1 + \lceil (t + s)/(2s-1) \rceil$ such that

$$y + (\{0\} \cup d \cdot [s, s'] \cup \{d(s'+s)\}) = y' + \sum_{i=0}^{s-1} (2k_i + d(s+i) \cdot [0, k_i])$$

and $y' = y - 2\sum_{i=0}^{s-1} k_i \geq 0$. Since $2k_i + d(s+i) \cdot [0, k_i] \in \mathcal{L}(\langle e_i \rangle)$ (cf. above) the claim follows by Lemma 2.1. □

Remark 4.5. Using the other construction to get the arithmetical progressions, we can obtain an analogous result. The condition on the group could be that its rank is at least $(d(3s^2 - s) + 2s)/2 = \sum_{i=0}^{s-1}((s+i)d + 1)$.

This condition seems rather more natural than the one given in Proposition 4.4, but it yields groups of much larger order.

4.3 Realization of small sets of lengths

We show how to obtain the small sets of lengths mentioned in Subsection 4.1. More precisely, for each $D \in \mathbb{N}$ we construct a finite abelian group whose system of sets of lengths contains all $L \subset \mathbb{N}_{\geq 2}$ for which $\max L - \min L \leq D$ (see Corollary 4.8). We emphasize that a result of this type is already known: it is implicit in [14, Proof of Proposition] and the existence of (but not an explicit construction for) such a group follows directly from [10, Proposition 4.8.3]. Nevertheless, we include a (different) proof of this fact, which, being designed for this specific purpose, is rather short, yields a group of a relatively small order, and is completely explicit. We start with a more technical result. In the following result $\delta_{i,j}$ is equal to 1 if $i = j$ and 0 otherwise. Furthermore, the set of factorizations of a zero-sum sequence B (over G) is the set of all essentially different (i.e., not only differing by the ordering of the factors) factorizations of B into minimal zero-sum sequences (over G); it is thus a subset of factorization monoid of $\mathcal{B}(G)$, the free abelian monoid over the set of minimal zero-sum sequences (cf. [10, Definition 1.2.6]).

Proposition 4.6. *Let $r, D \in \mathbb{N}$, and let $e_1, \ldots, e_r, f \in G$ be independent elements such that $\operatorname{ord} e_1 \ge 3$, $\operatorname{ord} e_i \ge 5$ for each $i \in [2, r]$ and $\operatorname{ord} f \ge 2D + 1$.*

1. *Let $d_1, \ldots, d_r \in \mathbb{N}$ such that $\sum_{i=1}^r d_i = D$. Let $g_1 = e_1 + \sum_{i=2}^r 3e_i + \sum_{i=1}^r d_i f$, $g_2 = \sum_{i=1}^r e_i$, $h_i = -e_i - 2e_{i+1} - d_i f$ for $i \in [1, r-1]$ and $h_r = -e_r - d_r f$. Furthermore, let*

$$B = g_1 g_2 \Big(\prod_{i=1}^{r} h_i\Big)(-e_1)\Big(\prod_{i=2}^{r} 2e_i(-3e_i)\Big)\big((-f)f\big)^{\sum_{i=1}^r d_i},$$

$$V_k = g_1 \Big(\prod_{i=1}^{k-1} h_i\Big)(-e_1)^{\delta_{1,k}}\Big(\prod_{i=\max\{2,k\}}^{r} -3e_i\Big)(2e_k)^{1-\delta_{r+1,k}}(-f)^{\sum_{i=k}^r d_i}, \text{ and}$$

$$W_k = g_2 \Big(\prod_{i=k}^{r} h_i\Big)(-e_1)^{1-\delta_{1,k}}\Big(\prod_{i=2}^{k-1} -3e_i\Big)\Big(\prod_{i\in[2,r]\setminus\{k\}} 2e_i\Big) f^{\sum_{i=k}^r d_i}$$

for $k \in [1, r+1]$. Then $B \in \mathcal{B}(G)$ and

$$\{V_k W_k \big((-f)f\big)^{\sum_{i=1}^{k-1} d_i} : k \in [1, r+1]\}$$

is the set of factorizations of B.

2. *Let $L \subset \mathbb{N}_{\ge 2}$ such that $\max L - \min L = D$ and $|L| = r + 1$. Then $L \in \mathcal{L}(G)$.*

Proof. 1. It is easy to see that B is a zero-sum sequence and thus an element of $\mathcal{B}(G)$. We have to show that each factorization of B into irreducible elements, i.e. minimal zero-sum sequences, is equal (as factorization) to $V_k W_k((-f)f)^{\sum_{i=1}^{k-1} d_i}$ for some $k \in [1, r+1]$. We observe that V_k, W_k for $k \in [1, r+1]$ and $(-f)f$ are minimal zero-sum sequences. Next, we show that no other minimal zero-sum sequence divides B. Let $W \mid B$ be a minimal zero-sum sequence.
Assertion 1: If $g_1 \nmid W$ and $g_2 \nmid W$, then $W = (-f)f$. If $h_i \nmid W$ for each $i \in [1, r]$, then this is obvious. Thus, suppose $h_j \mid W$ for some j and we assume j is minimal with this property. First, we suppose $j = 1$. The only elements in B with non-zero 1-coordinate are g_1, g_2, h_1, and $-e_1$. Thus, if $g_1 \nmid W$ and $g_2 \nmid W$, then the 1-coordinate of $\sigma(W)$ cannot equal 0, a contradiction. Now, we assume $j > 1$. By the minimality of j, we know that

$h_{j-1} \nmid W$. The only elements in B with non-zero j-coordinate are g_1, g_2, h_{j-1}, h_j, $2e_j$, and $(-3e_j)$. Again, if $g_1 \nmid W$ and $g_2 \nmid W$, then the j-coordinate of $\sigma(W)$ cannot equal 0, a contradiction.
Assertion 2: $g_1g_2 \nmid W$. Assume to the contrary that $g_1g_2 \mid W$. Let R the zero-sum sequence for which $B = WR$. By Assertion 1 it follows that $R = ((-f)f)^k$ for some $k \in \mathbb{N}_0$. Consequently the zero-sum sequence $g_2(-e_1)(\prod_{i=2}^{r} 2e_i(-3e_i))$ is a proper divisor of W and W is not a minimal zero-sum sequence, a contradiction.
Assertion 3: If $g_2 \mid W$, then $W = W_k$ for some $k \in [1, r+1]$. Suppose $g_2 \mid W$. We observe the following fact: If $h_j \mid W$ for some $j \in [1, r-1]$, then $h_{j+1} \mid W$. (This can be seen similarly to Assertion 1, considering the $(j+1)$-coordinate.) Now, let $k \in \mathbb{N}$ by minimal such that $h_i \mid W$ for each $i \geq k$. By the just established fact this implies that $h_i \nmid W$ for each $i < k$. Since $g_1 \nmid W$ and $(-f)f \nmid W$, it follows, considering each coordinate, that $W = W_k$.

Having these assertions at hand we finish our argument. Let $B = A_1 \cdot \ldots \cdot A_l$ be a factorization into minimal zero-sum sequences. Necessarily (exactly) one of the factors contains g_2, say A_1, and a different one contains g_1, say A_2. By Assertion 3 $A_1 = W_k$ for some $k \in [1, r+1]$ and by Assertion 1 $A_i = (-f)f$ for $i \in [3, l]$. Thus, $A_2 = V_k$ and $l = 2 + \sum_{i=1}^{k} d_i$.

2. By Lemma 2.1 we can assume that $\min L = 2$. Obviously there exist $d_1, \ldots, d_r \in \mathbb{N}$ such that $L = \{2 + \sum_{i=1}^{k-1} d_i \colon k \in [1, r+1]\}$. Applying 1. with these d_is the claim follows. □

We note that Proposition 4.6 and its proof can be generalized in the following way.

Remark 4.7. Instead of claiming the existence of the element f of order at least $2D+1$ one could make the (weaker) claim that independent elements f_j exist such that $\sum_j (\operatorname{ord} f_j - 1) \geq 2D$.

Yet, since our aim is a group with small order and a simple proof, we refrain from actually proving this slightly stronger result and also do not investigate further possible ramifications of the method used in the proof of Proposition 4.6.

We end this subsection with the announced result, which follows immediately from Proposition 4.6.

Corollary 4.8. *Let* $G = \big(\oplus_{i=1}^{D} \langle e_i \rangle\big) \oplus \langle f \rangle$ *with* $\operatorname{ord} e_i \geq 5$ *and* $\operatorname{ord} f \geq 2D+1$. *If* $\emptyset \neq L \subset \mathbb{N}_{\geq 2}$ *and* $\max L - \min L \leq D$, *then* $L \in \mathcal{L}(G)$.

Proof. For each non-empty set L of integers $|L| \le \max L - \min L + 1$. The claim is an immediate consequence of Proposition 4.6.2. □

4.4 Combination of the auxiliary results

In this subsection we combine the auxiliary results to prove Theorem 3.1.

Proof of Theorem 3.1. Suppose that the conditions on l and y_l hold and let $L = y + (L' \cup ((\mathcal{D} + d\mathbb{Z}) \cap [0, ld]) \cup (dl + L''))$ for some $y \ge y_l$. Further let $s = \lceil M/d \rceil$. Since $l \ge 3s$, we can apply Lemma 4.1 to get

$$L = \underbrace{\big(2 + M + (L' \cup ((\mathcal{D} + d\mathbb{Z}) \cap [0, ds]) \cup (ds + L''))\big)}_{L_1} + \underbrace{\big(y - M - 2 + (\{0\} \cup d \cdot [s, l-2s] \cup \{d(l-s)\})\big)}_{L_2}.$$

Since $l - 2s \ge (3s+1)s/2$ and $y - M - 2 \ge 2(s + 1 + \lceil \frac{t+s}{2s-1} \rceil)$, it follows by Proposition 4.4 that $L_2 \in \mathcal{L}(\oplus_{i=0}^{s-1} \langle e_i' \rangle)$. Since $|L_1| \le r + 1$ and $\operatorname{ord} f \ge 2(\max L_1 - \min L_1) + 1$, it follows by Proposition 4.6 that $L_1 \in \mathcal{L}(\oplus_{i=1}^{r} \langle e_i \rangle \oplus \langle f \rangle)$. Thus, $L = L_1 + L_2 \in \mathcal{L}\big((\oplus_{i=1}^{r} \langle e_i \rangle \oplus \langle f \rangle) \oplus (\oplus_{i=0}^{s-1} \langle e_i' \rangle)\big) \subset \mathcal{L}(G)$.

To get the "moreover"-statement, we note that for the remaining values of l and if r and $\operatorname{ord} f$ fulfil the additional conditions, the respective sets of lengths are elements of $\mathcal{L}((\oplus_{i=1}^{r} \langle e_i \rangle) \oplus \langle f \rangle)$ by Proposition 4.6. □

We conclude this paper with the explicit condition on the class group announced after Theorem 1.3, more precisely the subset of classes containing prime divisors. By Lemma 2.1 (and the proof of Theorem 1.3) it is clear that a condition for a finite abelian group G so that $\mathcal{L}(G)$ contains the relevant sets is sufficient. The proof of Theorem 1.3 and Theorem 3.1 immediately yield such a condition: G contains a subgroup isomorphic to the direct sum, over all $d \in \Delta^*$, all $\{0, d\} \subset \mathcal{D} \subset [0, d]$, and all (admissible) $-L', \overline{L''} \subset [1, M+d-1]$ of the groups $G_{\mathcal{D},L',\overline{L''}}$ occurring in the proof of Theorem 1.3, which are given explicitly by Theorem 3.1.

However, taking the proof of Theorem 3.1 into account an improvement to this condition is possible. The condition on the groups we use to construct the small sets depends on the parameters only in a weak way (cf. Corollary 4.8) and thus a single group for this purpose is sufficient (we only need to compute the maximal value that the lower bounds on r and $\operatorname{ord} f$ occurring

in Theorem 3.1 obtain for the range of parameters, see below). Apart this group for the small sets, we need a group to get the special AAMPs for each $d \in \Delta^*$ (see Proposition 4.4). Furthermore, with the same reasoning but using the variants of our results stated in Remarks 4.5 and 4.7, we obtain a different criterion (see below), which is simpler but typically (namely, if $\max \Delta^*$ is not much larger than the bound M) leads to a group of larger order.

Remark 4.9. Let $M \in \mathbb{N}$ and let $\emptyset \neq \Delta^* \subset \mathbb{N}$ and $D = \max \Delta^*$. Let G be a finite abelian group. If at least one of the following conditions holds, then $\mathcal{L}(G)$ contains each set L that is an AAMP with difference $d \in \Delta^*$ and bound M whose shift is sufficiently, e.g., $y \geq 5(M+D) + 2(\max L - \min L)$.

- G has a subgroup of the form

$$\Big(\bigoplus_{j=1}^{r} \langle e_j \rangle\Big) \oplus \langle f \rangle \oplus \bigoplus_{d \in \Delta^*} \Big(\oplus_{i=0}^{\lceil (M+d-1)/d \rceil} \langle e_i^d \rangle\Big),$$

  where $r \geq 12(M^2+D)$, $\operatorname{ord} f \geq 24(M^2+D)$ and $\operatorname{ord} e_i^d = d(\lceil (M+d-1)/d \rceil + i) + 2$.

- For some prime $p \geq 5$ the p-rank of G is at least $21(M^2+D)$.

Even with the present methods the conditions can be improved, in particular we estimated the complicated conditions on r and $\operatorname{ord} f$ that follow from our results only in a rough way. Yet, since the present construction will not yield anything close to a "necessary condition", we only state these relatively simple conditions that still make the dependence on the parameters transparent.

References

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

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

[3] C. Bowles, S. T. Chapman, N. Kaplan, and D. Reiser. On delta sets of numerical monoids. *J. Algebra Appl.*, 5(5):695–718, 2006.

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

[5] 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.

[6] 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.

[7] J. Coykendall. Extensions of half-factorial domains: A survey. In *Arithmetical Properties of Commutative Rings and Monoids*, volume 241 of *Lecture Notes in Pure and Appl. Math.*, pages 46–70. CRC Press (Taylor & Francis Group), Boca Raton, 2005.

[8] G. Freiman and A. Geroldinger. An addition theorem and its arithmetical application. *J. Number Theory*, 85(1):59–73, 2000.

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

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

[11] A. Geroldinger, W. Hassler, and G. Lettl. On the arithmetic of strongly primary monoids. *Semigroup Forum*, to appear.

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

[13] F. Halter-Koch. *Ideal systems*, volume 211 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 1998.

[14] F. Kainrath. Factorization in Krull monoids with infinite class group. *Colloq. Math.*, 80(1):23–30, 1999.

[15] F. Kainrath. On local half-factorial orders. In *Arithmetical properties of commutative rings and monoids*, volume 241 of *Lect. Notes Pure Appl. Math.*, pages 316–324. Chapman & Hall/CRC, Boca Raton, FL, 2005.

[16] W. Narkiewicz. Finite abelian groups and factorization problems. *Colloq. Math.*, 42:319–330, 1979.

[17] W. A. Schmid. Half-factorial sets in finite abelian groups: a survey. In D. Butković, D. Gronau, H. Kraljević, and O. Röschel, editors, *XI. Mathematikertreffen Zagreb-Graz*, volume 348 of *Grazer Math. Ber.*, pages 41–64. Karl-Franzens-Univ. Graz, Graz, 2005.

[18] R. J. Valenza. Elasticity of factorization in number fields. *J. Number Theory*, 36(2):212–218, 1990.

[19] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.