Journal de Théorie des Nombres
de Bordeaux **17** (2005), 323–345

Differences in sets of lengths of Krull monoids with finite class group

par Wolfgang A. SCHMID

Résumé. Soit H un monoïde de Krull dont le groupe de classes est fini. On suppose que chaque classe contient un diviseur premier. On sait que tout ensemble de longueurs est une presque multiprogression arithmétique. Nous étudions les nombres entiers qui apparaissent comme raison de ces progressions. Nous obtenons en particulier une borne supérieure sur la taille de ces raisons. En appliquant ces résultats, nous pouvons montrer que, sauf dans un cas particulier connu, deux p-groupes élémentaires ont le même système d'ensembles de longueurs si et seulement si ils sont isomorphes.

Abstract. Let H be a Krull monoid with finite class group where every class contains some prime divisor. It is known that every set of lengths is an almost arithmetical multiprogression. We investigate which integers occur as differences of these progressions. In particular, we obtain upper bounds for the size of these differences. Then, we apply these results to show that, apart from one known exception, two elementary p-groups have the same system of sets of lengths if and only if they are isomorphic.

1. Introduction

Let H be a Krull monoid with finite class group G where every class contains some prime divisor (for example the multiplicative monoid of a ring of integers in an algebraic number field). H is atomic, thus every non-unit $a \in H$ can be written as a product of irreducible elements. If $a \in H$ and $u_1, \dots, u_k \in H$ are irreducible elements such that $a = u_1 \cdot \ldots \cdot u_k$ is a factorization of a, then k is called the length of the factorization. The set $\mathsf{L}(a) \subset \mathbb{N}_0$ of all k such that a has a factorization into irreducibles of length k is a finite set and is called the set of lengths of a. The set $\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$ is called system of sets of lengths of H. It is well known that the system of sets of lengths of H just depends on the class group. More precisely, $\mathsf{L}(a)$ for some $a \in H$ is equal to the set of

This work was supported by the Austrian Science Fund FWF (Project P16770-N12).

length of some associated element in the block monoid $\mathcal{B}(G)$ over the class group (cf. Section 2 for the definition of a block monoid). Hence sets of lengths of Krull monoids can be studied in the associated block monoids. A detailed description of the construction and applications of the associated block monoids of Krull monoids can be found in the survey articles [17] and [4] in [1], for the algebraic theory of Krull monoids cf. [18, Chapter 22, Chapter 23].

In this article we are mainly interested in the set of differences $\Delta^*(G)$ which governs the structure of sets of length (cf. Definition 3.1). More precisely, every set of lengths is an almost arithmetical multiprogression (bounded by a constant just depending on G) with difference $d \in \Delta^*(G)$ (cf. [8, Satz 1], also cf. the survey articles, [7] and [12] for a generalization). The set $\Delta^*(G)$ was first investigated in [9] and recently in [7] and [13]. In Theorem 3.1 we give an upper bound for $\Delta^*(G)$. For an elementary p-group we explicitly determine $\max \Delta^*(G)$ and derive a criterion when $\Delta^*(G)$ is an interval (cf. Theorem 4.1).

It is an open question if, respectively to what extent, finite abelian groups (with Davenport's constant greater or equal 4) are characterized by their system of sets of lengths. This is a contribution to the problem due to W. Narkiewicz of arithmetical characterizations of the class group of a number field (cf. [20, Theorem 9.2, Notes to Chapter 9]). In [9] it was answered positively for cyclic groups, for elementary 2-groups and some other groups. In Section 5 we use Theorem 4.1 to prove that if an elementary p-group and an elementary q-group have the same system of sets of lengths, then they are, apart from one already known exception, isomorphic (cf. Theorem 5.1).

2. Preliminaries

In this section we fix notations and recall terminology and results that we will need, in particular for monoids, abelian groups and related notions. The notation will be mostly consistent with the usual one in factorization theory (cf. [17, 4], also cf. [7]).

For $m, n \in \mathbb{Z}$ we set $[m, n] = \{z \in \mathbb{Z} \mid m \le z \le n\}$ and we will call it an interval. For a set M we denote by $|M| \in \mathbb{N}_0 \cup \{\infty\}$ its cardinality. For a real number x let $\lceil x \rceil = \min\{z \in \mathbb{Z} \mid x \le z\}$ and $\lfloor x \rfloor = \max\{z \in \mathbb{Z} \mid x \ge z\}$.

A monoid is a commutative cancellative semigroup with identity element ($1_H = 1 \in H$) and we usually use multiplicative notation. Let H be a monoid. We denote by $H^\times$ the group of invertible elements of H. Let $H_1, H_2 \subset H$ be submonoids. Then we write $H = H_1 \times H_2$, if for each $a \in H$, there exist uniquely determined $b \in H_1$ and $c \in H_2$, such that $a = bc$. An element $u \in H \setminus H^\times$ is called irreducible (or an atom), if for all $a, b \in H$, $u = ab$ implies $a \in H^\times$ or $b \in H^\times$. By $\mathcal{A}(H) \subset H$ we denote the set of atoms. H is called atomic, if every $a \in H \setminus H^\times$ has a factorization into a product of atoms. Let $a \in H \setminus H^\times$ and $a = u_1 \cdot \ldots \cdot u_k$ a factorization of a into atoms $u_1, \ldots, u_k \in \mathcal{A}(H)$. Then k is called the length of the factorization and

$$\mathsf{L}(a) = \{k \in \mathbb{N} \mid a \text{ has a factorization of length } k\} \subset \mathbb{N}$$

denotes the set of lengths of a. We set $\mathsf{L}(a) = \{0\}$ for all $a \in H^\times$. The monoid H is called BF-monoid, if it is atomic and $|\mathsf{L}(a)| < \infty$ for all $a \in H$, and it is called half-factorial monoid, if it is atomic and $|\mathsf{L}(a)| = 1$ for all $a \in H$. Let H be an atomic monoid. Then $\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$ denotes the system of sets of lengths of H.

Let $L \subset \mathbb{N}_0$ with $L = \{l_1, l_2, l_3, \ldots\}$ and $l_i < l_{i+1}$ for each i. Then $\Delta(L) = \{l_2 - l_1, l_3 - l_2, l_4 - l_3, \ldots\}$ denotes the set of distances of L. For an atomic monoid H let $\Delta(H) = \bigcup_{L \in \mathcal{L}(H)} \Delta(L)$ denote the set of distances of H. Clearly, H is half-factorial if and only if $\Delta(H) = \emptyset$.

Throughout, let G be an additively written finite abelian group. By $\mathsf{r}(G)$ we denote its rank and by $\exp(G)$ its exponent. For $n \in \mathbb{N}$ let C_n denote a cyclic group with n elements. If $G_0 \subset G$ is a subset, then $\langle G_0 \rangle \subset G$ denotes the subgroup generated by G_0, where $\langle \emptyset \rangle = \{0\}$.

The set G_0 (respectively its elements) are said to be independent, if $0 \notin G_0$, $\emptyset \neq G_0$ and given distinct elements $e_1, \ldots, e_r \in G_0$ and $m_1, \ldots, m_r \in \mathbb{Z}$, then $\sum_{i=1}^r m_i e_i = 0$ implies that $m_1 e_1 = \cdots = m_r e_r = 0$. If we say that $\{e_1, \ldots, e_r\}$ is independent, then we will assume that the elements $e_1, \ldots, e_r$ are distinct.

Let $G_0 \subset G$. Then $\mathcal{F}(G_0)$ denotes the free abelian monoid with basis G_0. An element $S = \prod_{i=1}^l g_i \in \mathcal{F}(G_0)$ is called a sequence in G_0. It has a unique representation $S = \prod_{g \in G_0} g^{\mathsf{v}_g(S)}$ with $\mathsf{v}_g(S) \in \mathbb{N}_0$ for each $g \in G_0$. We denote the identity element of $\mathcal{F}(G_0)$, the empty sequence, by 1 and it will always be obvious from the context, whether we mean the empty sequence or the integer.

If $T \mid S$, then $T^{-1}S$ denotes the codivisor of T, i.e. the (unique) sequence such that $T(T^{-1}S) = S$. We denote by $|S| = l \in \mathbb{N}_0$ the length of S, by $\mathsf{k}(S) = \sum_{i=1}^l \frac{1}{\operatorname{ord}(g_i)}$ the cross number of S and by $\sigma(S) = \sum_{i=1}^l g_i \in G$ the sum of S. The support of S is the set of all $g \in G_0$ occurring in S, i.e. $\operatorname{supp}(S) = \{g_i \mid i \in [1, l]\} = \{g \in G_0 \mid \mathsf{v}_g(S) > 0\} \subset G_0$. The length and cross number of the empty sequence are 0 and the support is the empty set.

The sequence S is called a zero-sum sequence (a block), if $\sigma(S) = 0$, and S is called zero-sumfree, if $\sigma(T) \neq 0$ for all $1 \neq T \mid S$. A zero-sum sequence $1 \neq S$ is called minimal zero-sum sequence, if for each proper divisor $T \mid S$ (i.e. with $T \neq S$), T is zero-sumfree. The empty sequence is a zero-sum sequence and zero-sumfree.

The set $\mathcal{B}(G_0)$ consisting of all zero-sum sequences in G_0 is a submonoid of $\mathcal{F}(G_0)$, called the block monoid over G_0. $\mathcal{B}(G_0)$ is a BF-monoid and its atoms are just the minimal zero-sum sequences. If $G_1 \subset G_0$, then $\mathcal{B}(G_1) \subset \mathcal{B}(G_0)$ is a submonoid. For ease of notation, we denote by $\mathcal{A}(G_0)$ the set of atoms, by $\mathcal{L}(G_0)$ the system of sets of lengths and by $\Delta(G_0)$ the set of distances of $\mathcal{B}(G_0)$.

A subset $G_0 \subset G$ is called half-factorial, if $\mathcal{B}(G_0)$ is a half-factorial monoid, and G_0 is called minimal non-half-factorial, if G_0 is not half-factorial and each $G_1 \subsetneq G_0$ is half-factorial.

$G_0 \subset G$ is half-factorial if and only if $\mathsf{k}(A) = 1$ for each $A \in \mathcal{A}(G_0)$ (cf. [24, 25, 27] and [4, Proposition 5.4] for a proof in present terminology). Note that G (and thus all subsets of G) is half-factorial if and only if $|G| \leq 2$ (cf. [3, 27, 24]). For further results and applications of half-factorial sets we refer to [6] and the references given there.

Let $G_0 \subset G$. Then $\mathsf{D}(G_0) = \max\{|A| \mid A \in \mathcal{A}(G_0)\}$ is called Davenport's constant of G_0 and $\mathsf{K}(G_0) = \max\{\mathsf{k}(A) \mid A \in \mathcal{A}(G_0)\}$ is called the cross number of G_0. If $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$ is a p-group, then $\mathsf{D}(G) = 1 + \sum_{i=1}^{r}(n_i - 1)$ and $\mathsf{K}(G) = \frac{1}{\exp(G)} + \sum_{i=1}^{r} \frac{n_i-1}{n_i}$ (cf. [5, 21] and [19, 11]).

3. An Upper Bound for $\Delta^*(G)$

Until the end of this section let G denote a finite abelian group with $|G| \geq 3$.

Definition 3.1. Let G be a finite abelian group.

(1) $\Delta^*(G) = \{\min \Delta(G_0) \mid \emptyset \neq G_0 \subset G \text{ and } G_0 \text{ non-half-factorial}\}$

(2) For $d \in \mathbb{N}$, we say $d \in \Delta_1(G)$, if for every $k \in \mathbb{N}$ there is some $L \in \mathcal{L}(G)$ with $L = L' \cup L^* \cup L''$ such that

$$\max L' < \min L^* \leq \max L^* < \min L'' \text{ and } L^* = \{y + id \mid i \in [0, l]\}$$

with some $y \in \mathbb{N}$ and $l \geq k$.

There is a close relation among $\Delta^*(G)$ and $\Delta_1(G)$ (cf. Lemma 3.1). Note that the definition of $\Delta^*(G)$ involves the group G itself, whereas the definition of $\Delta_1(G)$ just involves the system of sets of lengths $\mathcal{L}(G)$. This suggests that $\Delta^*(G)$ can be used to gather information on G from $\mathcal{L}(G)$ and in Section 5, as mentioned in the Introduction, we make use of this fact to distinguish elementary p-groups by their system of sets of lengths.

First we cite several fundamental results, that will be used in the proofs of our results.

Lemma 3.1. [10, Proposition 2] *$\Delta^*(G) \subset \Delta_1(G)$ and if $d \in \Delta_1(G)$, then there exists some $d' \in \Delta^*(G)$ such that $d \mid d'$. In particular,* $\max \Delta^*(G) = \max \Delta_1(G)$.

Lemma 3.2. [8, Proposition 3, Proposition 4] *Let $G_0 \subset G$ be a non-half-factorial set. Then* $\min \Delta(G_0) = \gcd(\Delta(G_0))$ *and* $\max \Delta(G_0) \le \mathsf{D}(G_0) - 2$.

The following Lemma summarizes several results that will we useful. Statements 1.,2. and 3. are immediate consequence of Lemma 3.2 and the definitions, the other statements are proved in [7, Lemma 5.4].

Lemma 3.3. *Let $G_0 \subset G_0' \subset G$ be non-half-factorial sets.*

(1) $\min \Delta(G_0') | \min \Delta(G_0)$.

(2) *Let G' be a finite abelian group such that $G \subset G'$ is a subgroup. Then* $\Delta^*(G) \subset \Delta^*(G')$.

(3) *Let $L \in \mathcal{L}(G_0)$ and $x, y \in L$. Then* $\min \Delta(G_0) \mid (x - y)$.

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

(5) *If there exists some $A \in \mathcal{A}(G_0)$ with $\mathsf{k}(A) < 1$, then* $\min \Delta(G_0) \le \exp(G) - 2$.

Next we give results on $\min \Delta(G_0)$ for special types of subsets $G_0 \subset G$ and results on $\Delta^*(G)$, which were obtained in [7, Proposition 5.2].

Lemma 3.4. [7, Proposition 5.2] *Let $G_1 = \{e_1, \ldots, e_r\} \subset G$ independent with* $\operatorname{ord}(e_1) = \cdots = \operatorname{ord}(e_r) = n$.

(1) *Let $g = -\sum_{i=1}^r e_i$ and $G_0 = \{g\} \cup G_1$. Then either $n = r + 1$ and G_0 is half-factorial or $\Delta(G_0) = \{|n - r - 1|\}$.*

(2) *Let $r \ge 2$ and $g' = \sum_{i=1}^r e_i$ and $G_0 = \{g'\} \cup G_1$. Then $\Delta(G_0) = \{r - 1\}$.*

(3) $[1, \mathsf{r}(G) - 1] \subset \Delta^*(G)$ *and for all $m \in \mathbb{N}$ with $m \ge 3$ and* $m | \exp(G)$
$$m - 2 \in \Delta^*(G).$$

This lemma gives immediately that
$$\max \Delta^*(G) \ge \max\{\exp(G) - 2, \mathsf{r}(G) - 1\}.$$
There are known several types of groups for which equality holds. For p-groups with large rank this was proved in [7, Theorem 1.5] and for cyclic groups even a more general result on $\Delta^*(G)$ is known (cf. [13, Theorem 4.4]). In Theorem 4.1 we will prove that equality holds for elementary p-groups. Moreover, there is known no group for which equality does not hold.

In Theorem 3.1 we obtain an upper bound, involving the cross number $\mathsf{K}(G)$, for the elements of $\Delta^*(G)$. Using this result we will treat several special cases (cf. Corollary 3.2 and Corollary 3.3).

Lemma 3.5. *Let $G_0 \subset G$ be a non-half-factorial set and $g \in G_0$ such that $G_0 \setminus \{g\}$ is half-factorial. Suppose there exists some $W \in \mathcal{A}(G_0)$ with $\mathsf{k}(W) = 1$, $g \in \operatorname{supp}(W)$ and*
$$\gcd(\{\mathsf{v}_g(W), \operatorname{ord}(g)\}) = 1.$$

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

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

Proof. Let $A \in \mathcal{A}(G_0)$. We need to prove, that $\mathsf{k}(A) \in \mathbb{N}$ and that

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

If $\mathsf{k}(A) = 1$, this is obvious, hence we assume $\mathsf{k}(A) \neq 1$. $G_0 \setminus \{g\}$ is half-factorial, thus $g \in \operatorname{supp}(A)$ and $\mathsf{v}_g(A) \in [1, \operatorname{ord}(g) - 1]$. Since

$$\gcd(\{\mathsf{v}_g(W), \operatorname{ord}(g)\}) = 1,$$

there exists some $x \in [1, \operatorname{ord}(g)]$ such that

$$x\mathsf{v}_g(W) \equiv -\mathsf{v}_g(A) \bmod \operatorname{ord}(g).$$

Thus $x\mathsf{v}_g(W) + \mathsf{v}_g(A) = y \operatorname{ord}(g)$ for some $y \in \mathbb{N}$. We consider the block $C = AW^x$. We get $C = g^{y\operatorname{ord}(g)}B$ with $B \in \mathcal{B}(G_0 \setminus \{g\})$. Since $G_0 \setminus \{g\}$ is half-factorial, we have $\mathsf{k}(B) \in \mathbb{N}$ and $\mathsf{L}(B) = \{\mathsf{k}(B)\}$. For $\mathsf{k}(A)$ we get

$$\mathsf{k}(C) = \mathsf{k}(A) + x = y + \mathsf{k}(B)$$

and consequently $\mathsf{k}(A) = \mathsf{k}(B) + y - x \in \mathbb{N}$, which proves the first part of the lemma. We know that each factorization of B has length $\mathsf{k}(B) = \mathsf{k}(A) + x - y$, hence there exists a factorization of C with length $y + \mathsf{k}(B) = \mathsf{k}(A) + x$. Since $C = AW^x$ is a factorization of length $1 + x$, we get, applying Lemma 3.3.3, that $\min \Delta(G_0) \mid (\mathsf{k}(A) - 1)$. □

Corollary 3.1. *Let $G_0 \subset G$ be a minimal non-half-factorial set. Suppose that G_0 has a proper subset $\emptyset \neq G_1 \subsetneq G_0$ which is not a minimal generating set (with respect to inclusion) for $\langle G_1 \rangle$. Then* $\mathsf{k}(\mathcal{A}(G_0)) \subset \mathbb{N}$ *and*

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

Proof. Let $G_1' \subsetneq G_1$ such that $\langle G_1' \rangle = \langle G_1 \rangle$ and $g \in G_1 \setminus G_1'$. Since G_0 is minimal non-half-factorial, we have $G_0 \setminus \{g\}$ is half-factorial. Since $-g \in \langle G_1' \rangle$, there is some $S \in \mathcal{F}(G_1')$ with $\sigma(S) = -g$, and consequently there exists some atom $W \in \mathcal{A}(G_1)$ with $\mathsf{v}_g(W) = 1$. Since G_0 is minimal non-half-factorial and $\operatorname{supp}(W) \subset G_1 \subsetneq G_0$, it follows that $\mathsf{k}(W) = 1$. Thus Lemma 3.5 implies the assertion. □

Now we are ready to prove the upper bound for $\Delta^*(G)$. In the proof it will be an important step to restrict our considerations to sets G_0 with convenient properties. To do so we will apply Lemma 3.3 and a result obtained in [22] that makes use of the notion of transfer homomorphisms (cf. [17, Section 5]).

Theorem 3.1. *Let G be a finite abelian group. Then*

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

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

$$\min \Delta(G_0) \le \max\left\{\exp(G) - 2, 2\mathsf{K}(G) - 1 - \frac{2}{\exp(G)}\right\}.$$

By Lemma 3.3.1 we may assume that G_0 is minimal non-half-factorial. Moreover, we may assume by [22, Theorem 3.17] that for each $g \in G_0$

$$g \in \langle G_0 \setminus \{g\}\rangle.$$

If there exists some atom $A \in \mathcal{A}(G_0)$ with $\mathsf{k}(A) < 1$, then by Lemma 3.3.5 $\min \Delta(G_0) \le \exp(G) - 2$, which gives the statement of the theorem.

Suppose $\mathsf{k}(A) \ge 1$ for each $A \in \mathcal{A}(G_0)$. Let $g \in G_0$ and $G_1 = G_0 \setminus \{g\}$. Since $-g \in \langle G_1\rangle$, there exists an atom $W \in \mathcal{A}(G_0)$ with $\mathsf{v}_g(W) = 1$. If $\mathsf{k}(W) = 1$, we apply Lemma 3.5 and obtain

$$\begin{aligned}\min \Delta(G_0) &\le \gcd(\{\mathsf{k}(A) - 1 \mid A \in \mathcal{A}(G_0)\}) \\ &\le \max\{\mathsf{k}(A) - 1 \mid A \in \mathcal{A}(G_0)\} \\ &\le \mathsf{K}(G) - 1 \le 2\mathsf{K}(G) - 1 - \frac{2}{\exp(G)}.\end{aligned}$$

Suppose $\mathsf{k}(W) > 1$. For every $j \in [1, \operatorname{ord}(g)]$ we consider the block W^j, and obviously we have $j \in \mathsf{L}(W^j)$. For every $j \in [1, \operatorname{ord}(g)]$ let $W_j \in \mathcal{B}(G_0)$ and $B_j \in \mathcal{B}(G_1)$, such that $W^j = W_j B_j$ and $\mathsf{k}(W_j)$ is minimal among all blocks $V_j \in \mathcal{B}(G_0)$ with $V_j \mid W^j$ and $\mathsf{v}_g(V_j) = j$. Since G_1 is half-factorial we obtain that $\mathsf{L}(B_j) = \{\mathsf{k}(B_j)\}$ for every $j \in [2, \operatorname{ord}(g)]$. For $j = 1$ we have $W_1 = W$, $B_1 = 1$ and

$$\{1\} = \mathsf{L}(W_1) = \mathsf{L}(W_1) + \mathsf{L}(B_1).$$

For $j = \operatorname{ord}(g)$ we have $W_{\operatorname{ord}(g)} = g^{\operatorname{ord}(g)}$ and

$$\operatorname{ord}(g)\mathsf{k}(W) = 1 + \mathsf{k}(B_{\operatorname{ord}(g)}) \in \mathsf{L}(W_{\operatorname{ord}(g)}) + \mathsf{L}(B_{\operatorname{ord}(g)}) \subset \mathsf{L}(W^{\operatorname{ord}(g)}).$$

In particular, since $\operatorname{ord}(g) \ne \operatorname{ord}(g)\mathsf{k}(W)$, we have $|\mathsf{L}(W^{\operatorname{ord}(g)})| > 1$.

We define

$$k = \min\{j \in [1, \operatorname{ord}(g)] \mid \mathsf{L}(W_j) + \mathsf{L}(B_j) \ne \{j\}\}.$$

Since $\operatorname{ord}(g)\mathsf{k}(W) \in \mathsf{L}(W_{\operatorname{ord}(g)}) + \mathsf{L}(B_{\operatorname{ord}(g)})$ and $\mathsf{L}(W_1) + \mathsf{L}(B_1) = \{1\}$ we obtain $k \in [2, \operatorname{ord}(g)]$.

We have $k \in \mathsf{L}(W^k)$ and there exists some $k' \in \mathsf{L}(W_k) + \mathsf{L}(B_k) \subset \mathsf{L}(W^k)$ such that $k' \ne k$. Since W^k is not an atom we have $k' > 1$.

By Lemma 3.3.3 it suffices to prove that

$$|k-k'| \le \max\left\{\exp(G)-2, 2\mathsf{K}(G)-1-\frac{2}{\exp(G)}\right\}.$$

If $k' < k$, then

$$k-k' \le \operatorname{ord}(g)-k' \le \operatorname{ord}(g)-2 \le \exp(G)-2.$$

Suppose $k < k'$. We estimate $\max \mathsf{L}(W^k)$. Since $\mathsf{k}(A) \ge 1$ for each $A \in \mathcal{A}(G_0)$, we have $\max \mathsf{L}(W^k) \le \mathsf{k}(W^k)$.

We will estimate $\mathsf{k}(W^{k-1})$, which leads to an estimate for $\mathsf{k}(W^k)$. By definition of k we have

$$\mathsf{L}(W_{k-1}) + \mathsf{L}(B_{k-1}) = \{k-1\}$$

and hence $\mathsf{L}(W_{k-1}) = \{l\}$ with some $l \in [1, k-1]$. We have $\mathsf{L}(B_{k-1}) = \{\mathsf{k}(B_{k-1})\}$, hence $\mathsf{k}(B_{k-1}) + l = k-1$ and

$$\mathsf{k}(B_{k-1}) = k-1-l \le k-2.$$

Let $W'_{k-1} \in \mathcal{F}(G_1)$ such that $W_{k-1} = g^{k-1}W'_{k-1}$. Since $\mathsf{k}(W_{k-1})$ is minimal, we know that W'_{k-1} is zero-sumfree. Thus $\mathsf{k}(W'_{k-1}) \le \mathsf{K}(G) - \frac{1}{\exp(G)}$ and $\mathsf{k}(W_{k-1}) \le \frac{k-1}{\operatorname{ord}(g)} + \mathsf{K}(G) - \frac{1}{\exp(G)} \le \mathsf{K}(G) + 1 - \frac{2}{\exp(G)}$. Combining these estimates we obtain

$$\begin{aligned}\mathsf{k}(W^k) &= \mathsf{k}(W) + \mathsf{k}(W_{k-1}) + \mathsf{k}(B_{k-1})\\ &\le \mathsf{K}(G) + \left(\mathsf{K}(G) + 1 - \frac{2}{\exp(G)}\right) + (k-2)\\ &= 2\mathsf{K}(G) + k - 1 - \frac{2}{\exp(G)}.\end{aligned}$$

Consequently, we have

$$k'-k \le \mathsf{k}(W^k) - k \le 2\mathsf{K}(G) - 1 - \frac{2}{\exp(G)}.$$

□

For p-groups the size of $\mathsf{K}(G)$ is known and using this we can bound $\max \Delta^*(G)$ by an expression just involving $\mathsf{r}(G)$ and $\exp(G)$. If $\exp(G) = 2$, then this upper bound yields $\max \Delta^*(G) = r-1$, which was initially proved in [9, Proposition 1].

Corollary 3.2. *If G is a p-group, then*

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

In particular, if $\exp(G) = 2$, *then* $\max \Delta^*(G) = r - 1$.

Proof. Suppose G is a p-group. Let $\mathsf{r}(G) = r$ and $k_1, \dots, k_r \in \mathbb{N}$ such that $G \cong \bigoplus_{i=1}^r C_{p^{k_i}}$. By [11, Theorem], as mentioned in Section 2, we have $K(G) = \frac{1}{\exp(G)} + \sum_{i=1}^r \frac{p^{k_i}-1}{p^{k_i}} \le \frac{1}{\exp(G)} + r\frac{\exp(G)-1}{\exp(G)}$. Therefore

$$2\mathsf{K}(G) - 1 - \frac{2}{\exp(G)} \le 2r\frac{\exp(G)-1}{\exp(G)} - 1,$$

and applying Theorem 3.1 the first statement follows.

Suppose $\exp(G) = 2$. Then $2\mathsf{r}(G)\frac{\exp(G)-1}{\exp(G)} - 1 = \mathsf{r}(G) - 1$. By Lemma 3.4.3 we have $\mathsf{r}(G) - 1 \le \max\Delta^*(G)$ and equality follows. □

For arbitrary finite abelian groups the size of $\mathsf{K}(G)$ is not known. However, there is known an upper bound for $\mathsf{K}(G)$. Using this result, we get an upper bound for $\max\Delta^*(G)$ just involving $\mathsf{r}(G)$ and $\exp(G)$ as-well. (By $\log(\cdot)$ we mean the natural logarithm.)

Corollary 3.3.

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

In particular, if $\frac{\exp(G)-2}{2\log(\exp(G))} \ge \mathsf{r}(G)$, *then*

$$\max\Delta^*(G) = \exp(G) - 2.$$

Proof. Let $n = \exp(G)$ and $r = \mathsf{r}(G)$. By [15, Theorem 2] we have $\mathsf{K}(G) \le \frac{1}{2} + \log(|G|)$. Therefore

$$\begin{aligned} 2\mathsf{K}(G) - 1 - \frac{2}{n} &\le 2\left(\frac{1}{2} + \log(|G|)\right) - 1 - \frac{2}{n} \\ &< 2\log(|G|) \le 2\log(n^r) = 2r\log(n), \end{aligned}$$

which proves, applying Theorem 3.1, the first statement.

Now suppose $\frac{n-2}{2\log(n)} \ge r$. We get

$$\max\{n-2, 2r\log(n)\} = n - 2 \text{ and consequently } \max\Delta^*(G) \le n - 2.$$

By Lemma 3.4.3 we have $n - 2 \le \max\Delta^*(G)$ and equality follows. □

4. $\Delta^*(G)$ for Elementary p-groups

In this section we investigate $\Delta^*(G)$ for elementary p-groups. We proceed similarly to the previous section, but in elementary p-groups minimal generating sets are independent and thus certain sets are so-called simple sets. Using results on the set of atoms of block monoids over simple sets we will investigate $\min\Delta(G_0)$ for simple subsets of finite abelian groups (cf. Proposition 4.1). Having this at hand we will determine $\max\Delta^*(G)$ (and to some extent the structure of $\Delta^*(G)$) in case G is an elementary p-group.

We recall a definition of simple sets and some related notations. A subset $G_0 \subset G \setminus \{0\}$ is simple if there exists some $g \in G_0$ such that

$G_1 = G_0 \setminus \{g\} = \{e_1, \dots, e_r\}$ is independent with $\operatorname{ord}(e_i) = n_i$ for each $i \in [1, r]$ and $g = -\sum_{i=1}^r b_i e_i$ with $b_i \in [1, n_i - 1]$ for each $i \in [1, r]$. For $j \in \mathbb{N}$ let $W_j(G_1, g) = W_j \in \mathcal{B}(G_0)$ denote the unique block with $\mathsf{v}_g(W_j) = j$ and $\mathsf{v}_{e_i}(W_j) \in [0, n_i - 1]$ for each $i \in [1, r]$ (clearly, $\mathsf{v}_{e_i}(W_j) \equiv j b_i \bmod n_i$). Moreover, let $\mathsf{i}(G_1, g) = \{j \in \mathbb{N} \mid W_j \in \mathcal{A}(G_0)\}$.

Note that the sets considered in Lemma 3.4 are simple sets. In the following result we summarize some results on simple sets.

Lemma 4.1. [22, Theorem 4.7, Lemma 4.12] *Let G be an abelian group, $r \in \mathbb{N}$, $G_1 = \{e_1, \dots, e_r\}$ an independent set with $\operatorname{ord}(e_i) = n_i$ for each $i \in [1, r]$, $g = -\sum_{i=1}^r b_i e_i$ with $b_i \in [1, n_i - 1]$ for each $i \in [1, r]$ and $G_0 = G_1 \cup \{g\}$. Further let $j \in \mathbb{N}$.*

(1) *If $W \in \mathcal{B}(G_0)$ with $\mathsf{v}_g(W) = j$, then $W_j \mid W$.*
(2) *$\mathcal{A}(G_0) = \{e_i^{n_i} \mid i \in [1, r]\} \cup \{W_j \mid j \in \mathsf{i}(G_1, g)\}$.*
(3) $\mathsf{i}(G_1, g) = \{j \in [1, \operatorname{ord}(g)] \mid W_k \nmid W_j$ *for each* $k \in [1, j - 1]\}$. *In particular,* $\{1, \operatorname{ord}(g)\} \subset \mathsf{i}(G_1, g) \subset [1, \operatorname{ord}(g)]$.
(4) *If $W_j \notin \mathcal{A}(G_0)$, then there exists some $k \in [1, j - 1]$ such that $W_j = W_k W_{j-k}$.*
(5) $\min(\mathsf{i}(G_1, g) \setminus \{1\}) = \min\{\lceil \frac{n_i}{b_i} \rceil \mid i \in [1, r]\}$.
(6) $\mathsf{i}(G_1, g) = \{1, \operatorname{ord}(g)\}$ *if and only if* $\operatorname{ord}(g) \mid n_i$ *and* $b_i = \frac{n_i}{\operatorname{ord}(g)}$ *for each $i \in [1, r]$.*
(7) *If* $\mathsf{i}(G_1, g) \neq \{1, \operatorname{ord}(g)\}$, *then* $\min(\mathsf{i}(G_1, g) \setminus \{1\}) \le \left\lceil \frac{\operatorname{ord}(g)}{2} \right\rceil$.

Now we are ready to investigate $\min \Delta(G_0)$ for simple sets.

Proposition 4.1. *Let $G_0 = \{g, e_1, \dots, e_r\} \subset G$ be a simple and non-half-factorial set with $r \in \mathbb{N}$, $\{e_1, \dots, e_r\}$ independent,* $\operatorname{ord}(g) = n$ *and* $\operatorname{ord}(e_i) = n_i$ *for each $i \in [1, r]$. Then either*

$$\min \Delta(G_0) \le \max\{r - 1, \left\lfloor \frac{n}{2} \right\rfloor - 1\}$$

or

$$n \mid n_i \textit{ for every } i \in [1, r], g = -\sum_{i=1}^r \frac{n_i}{n} e_i \textit{ and } \min \Delta(G_0) = |n - r - 1|.$$

Proof. We set $G_1 = \{e_1, \dots, e_r\}$ and $g = -\sum_{i=1}^r b_i e_i$ with $b_i \in [1, n_i - 1]$ for every $i \in [1, r]$.

We use all notations introduced for simple sets and set $m = \min(\mathsf{i}(G_1, g) \setminus \{1\})$ hence $m \in [2, n]$

Suppose that $m = n$. Then, by definition of $\mathsf{i}(G_1, g)$, we have

$$\mathcal{A}(G_0) = \{e_1^{n_1}, \dots, e_r^{n_r}, W_n = g^n, W_1 = g \prod_{i=1}^r e_i^{b_i}\}$$

and Lemma 4.1.6 implies that $n \mid n_i$ and $b_i = \frac{n_i}{n}$ for every $i \in [1,r]$. Thus $W_1^n = W_n \prod_{i=1}^r e_i^{n_i}$ is the only non-cancellative relation among the atoms of G_0. Since G_0 is non-half-factorial, we get $n \neq r-1$ and $\Delta(G_0) = \{|n-r-1|\}$.

Suppose that $m \in [2, n-1]$.

If $\mathsf{k}(W_1) = 1$, then Lemma 3.5 implies $\min \Delta(G_0) \mid \gcd(\{\mathsf{k}(A) - 1 \mid A \in \mathcal{A}(G_0)\})$. Since G_0 is non-half-factorial, there exists an atom, say $A' \in \mathcal{A}(G_0)$, such that $\mathsf{k}(A') \neq 1$. We obtain

$$\mathsf{k}(A') = \frac{\mathsf{v}_g(A')}{n} + \sum_{i=1}^{r} \frac{\mathsf{v}_{e_i}(A')}{n_i} < 1 + r$$

and consequently $\min \Delta(G_0) < r$ hence $\min \Delta(G_0) \leq r-1$.

Suppose $\mathsf{k}(W_1) \neq 1$. For every $j \in [1,n]$ let $B_j = W_j^{-1} W_1^j \in \mathcal{B}(G_1)$. Since G_1 is half-factorial, it follows that $\mathsf{L}(B_j) = \{\mathsf{k}(B_j)\}$ for every $j \in [1,n]$. For $j=1$ we have

$$\{1\} = \mathsf{L}(W_1) = \mathsf{L}(W_1) + \{0\} = \mathsf{L}(W_1) + \mathsf{L}(B_1).$$

For $j = n$ we have $W_1^n = W_n B_n$, $W_n = g^n \in \mathcal{A}(G_0)$ and

$$n \neq n\mathsf{k}(W_1) = 1 + \mathsf{k}(B_n) \in \mathsf{L}(W_n) + \mathsf{L}(B_n).$$

We define

$$k = \min\{j \in [1,n] \mid \mathsf{L}(W_j) + \mathsf{L}(B_j) \neq \{j\}\}.$$

Clearly, we obtain that $k \in [2,n]$ and

$$\{j\} \cup (\mathsf{L}(W_j) + \mathsf{L}(B_j)) \subset \mathsf{L}(W_1^j)$$

for every $j \in [1,n]$.

Assertion: $W_k \in \mathcal{A}(G_0)$.

Proof of the Assertion: Assume to the contrary that $W_k \notin \mathcal{A}(G_0)$. We assert that

$$\mathsf{L}(W_k) + \mathsf{L}(B_k) \subset \bigcup_{j \in [1,k-1]} \mathsf{L}(W_j) + \mathsf{L}(W_{k-j}) + \mathsf{L}(B_j) + \mathsf{L}(B_{k-j}).$$

Suppose that this holds true. If $j \in [1,k-1]$, then $\mathsf{L}(W_j) + \mathsf{L}(B_j) = \{j\}$ and $\mathsf{L}(W_{k-j}) + \mathsf{L}(B_{k-j}) = \{k-j\}$. Thus $\mathsf{L}(W_k) + \mathsf{L}(B_k) \subset \{k\}$, a contradiction.

To verify the inclusion, let $l \in \mathsf{L}(W_k)$ and $U_1 \cdot \ldots \cdot U_l$ a factorization of W_k with length l. Then there is some $j \in [1,k-1]$ such that $U_1 = W_j$. By Lemma 4.1.4 we have $W_j^{-1} W_k = W_{k-j}$ hence $U_2 \cdot \ldots \cdot U_l$ is a factorization of W_{k-j} with length $l-1$. Since $(W_j B_j)^{-1} W_k B_k = W_1^{k-j} = W_{k-j} B_{k-j}$, we obtain that $W_k B_k = (W_j W_{k-j}) B_j B_{k-j}$ hence $B_k = B_j B_{k-j}$ and $\mathsf{k}(B_k) = \mathsf{k}(B_j) + \mathsf{k}(B_{k-j})$. Since $\mathsf{L}(B_\nu) = \{\mathsf{k}(B_\nu)\}$ for every $\nu \in [1,k]$ it follows that

$$l + \mathsf{L}(B_k) \subset \mathsf{L}(W_j) + \mathsf{L}(W_{k-j}) + \mathsf{L}(B_j) + \mathsf{L}(B_{k-j})$$

hence the inclusion is verified.

Since $W_k \in \mathcal{A}(G_0)$ we infer that $m \le k$ and

$$\{k\} \ne \mathsf{L}(W_k) + \mathsf{L}(B_k) = \{1\} + \{\mathsf{k}(B_k)\} = \{1 + \mathsf{k}(B_k)\}.$$

Note that since W^k is not an atom, $B_k \ne 1$ and hence $\mathsf{k}(B_k) \ne 0$.

Case 1: $1 + \mathsf{k}(B_k) > k$. Let $j \in [2, n]$ By definition we have

$$W_j^{-1} W_1 W_{j-1} \in \mathcal{B}(G_1),$$

and since G_1 is independent, it follows that $\mathsf{v}_{e_i}(W_j^{-1} W_1 W_{j-1}) \in n_i \mathbb{N}_0$ for every $i \in [1, r]$. Since $\mathsf{v}_{e_i}(W_l) \in [0, n_i - 1]$ for every $l \in \mathbb{N}$, it follows that $\mathsf{v}_{e_i}(W_j^{-1} W_1 W_{j-1}) \in \{0, n_1\}$ for every $i \in [1, r]$. Thus

$$W_j^{-1} W_1 W_{j-1} = \prod_{i \in I_j} e_i^{n_i}$$

for some $I_j \subset [1, r]$. Since $W_1 = W_{j-1}^{-1} B_{j-1}^{-1} W_j B_j$, we obtain that $B_{j-1}^{-1} B_j = \prod_{i \in I_j} e_i^{n_i}$ hence $\mathsf{k}(B_j) - \mathsf{k}(B_{j-1}) = |I_j| \in [0, r]$.

If $j \in [1, k-1]$, then $\{\mathsf{k}(B_j)\} + \mathsf{L}(W_j) = \mathsf{L}(B_j) + \mathsf{L}(W_j) = \{j\}$ hence $\mathsf{k}(B_j) \le j - 1$. Therefore we obtain that

$$\min \Delta(G_0) \le 1 + \mathsf{k}(B_k) - k \le 1 + (\mathsf{k}(B_{k-1}) + r) - k \le 1 + (k - 2 + r) - k = r - 1.$$

Case 2: $1 + \mathsf{k}(B_k) < k$. If $k = m$, Lemma 4.1.7 implies that

$$\min \Delta(G_0) \le k - (1 + \mathsf{k}(B_k)) = m - (1 + \mathsf{k}(B_k)) \le m - 2 \le \left\lceil \frac{n}{2} \right\rceil - 2 \le \left\lfloor \frac{n}{2} \right\rfloor - 1.$$

Suppose that $m < k$. Then we have

$$W_1^m = W_m B_m$$

and $\{1\} + \{\mathsf{k}(B_m)\} = \mathsf{L}(W_m) + \mathsf{L}(B_m) = \{m\}$ hence $\mathsf{k}(B_m) = m - 1$. We set $f = \lfloor \frac{k}{m} \rfloor$ and obtain that

$$W_k B_k = W_1^k = W_1^{k - mf} W_1^{mf} = W_1^{k - mf} W_m^f B_m^f.$$

Lemma 4.1.1 implies that $W_k \mid W_1^{k-mf} W_m^f$ but $W_1^{k-mf} W_m^f \notin \mathcal{A}(G_0)$ hence $W_k \ne W_1^{k-mf} W_m^f$. Thus $B_m^f \mid B_k$ but $B_m^f \ne B_k$ hence

$$\mathsf{k}(B_k) > \mathsf{k}(B_m^f) = f \mathsf{k}(B_m) = f(m-1).$$

Therefore we obtain that

$$\begin{aligned} \min \Delta(G_0) &\le k - (1 + \mathsf{k}(B_k)) \le k - (1 + fm - f + 1) \le m + f - 3 \\ &\le m + \frac{k}{m} - 3 \le \frac{n}{m} + m - 3. \end{aligned}$$

Recall that $m \in [2, \lceil \frac{n}{2} \rceil]$ and let $f : \mathbb{R}_{>0} \to \mathbb{R}$ be defined by $f(x) = \frac{n}{x} + x - 3$. Since $f''(x) > 0$ for every $x \in \mathbb{R}_{>0}$ (or by a direct argument cf. [23, Lemma 4.3]), we obtain that

$$\max\{f(x) \mid x \in [2, \left\lceil \frac{n}{2} \right\rceil]\} = \max\{f(2), f(\left\lceil \frac{n}{2} \right\rceil)\}$$

hence $\min \Delta(G_0) \le \lfloor \frac{n}{2} \rfloor - 1$. □

Theorem 4.1. *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,

(1) $\max \Delta^*(G) = \max\{p-2, r-1\}$.
(2) $\Delta^*(G)$ *is an interval if and only if* $p \le 2r+1$.

Proof. By Lemma 3.4 we know that

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

Let $G_0' \subset G$ be a non-half-factorial subset and $d' = \min \Delta(G_0')$. We have to prove that $d' \in [1, r-1] \cup [1, \frac{p-3}{2}] \cup [\max\{1, p-r-1\}, p-2]$. If $p = 2$, then $\min \Delta(G_0') \le \mathsf{D}(G_0') - 2 \le r-1$ by Lemma 3.2. Let $p \ge 3$ and $G_0 \subset G_0'$ a minimal non-half-factorial subset and $d = \min \Delta(G_0)$. Then Lemma 3.3.1 implies that $d' \mid d$. If $d \in [\max\{1, p-1-r\}, p-2]$, then either $d = d'$ or $d' \le \lfloor \frac{d}{2} \rfloor \le \frac{p-3}{2}$. Suppose that $d \notin [\max\{1, p-1-r\}, p-2]$. Let $g \in G_0$ and $G_1 = G_0 \setminus \{g\}$.

If G_1 is not a minimal generating set for $\langle G_1 \rangle$, then Corollary 3.1 implies that $d \le \mathsf{K}(G) - 1$. By [11, Theorem], as mentioned in Section 2, we have $\mathsf{K}(G) \le r$ and thus $d' \in [1, r-1]$.

Suppose that G_1 is a minimal generating set for $\langle G_1 \rangle$. G is an elementary p-group, consequently G_1 is independent. Since G_0 is minimal non-half-factorial, G_0 is not independent and it follows that G_0 is simple (also cf. [22, Lemma 4.4]).

Thus Proposition 4.1 implies that $d \le \max\{r-1, \frac{p-3}{2}\}$ hence $d' \in [1, r-1] \cup [1, \frac{p-3}{2}]$.
It remains to prove the additional statements: 1. is obvious.

2. If $p \le 2r+1$, then

$$[1, r-1] \cup [\max\{1, p-r-1\}, p-2] = [1, \max\{p-2, r-1\}]$$

and consequently $\Delta^*(G) = [1, \max\{p-2, r-1\}]$. If $p > 2r+1$, then $1 \in \Delta^*(G)$, $p-2 \in \Delta^*(G)$ but $p-r-2 \notin \Delta^*(G)$. □

5. Characterizing Elementary p-groups by $\mathcal{L}(G)$

As mentioned in the Introduction, it is an open question to what extent a finite abelian group is characterized by its system of sets of lengths. In Section 2 we mentioned that if $|G| \le 2$, then the block monoid $\mathcal{B}(G)$ is half-factorial, hence $\mathcal{L}(C_1) = \mathcal{L}(C_2)$ (cf. [24, Proposition 3.2]). In [9, Lemma 9, Lemma 10] it was proved, that $\mathcal{L}(C_3) = \mathcal{L}(C_2^2)$ and no group not isomorphic to C_3 or C_2^2 has the same system of sets of lengths as these groups.

Furthermore, it is known (cf. [9, Satz 4]) that for $n \in \mathbb{N}$ with $n \geq 4$ the following holds: If

$$\mathcal{L}(G) = \mathcal{L}(C_n), \text{ then } G \cong C_n$$

and if

$$\mathcal{L}(G) = \mathcal{L}(C_2^{n-1}), \text{ then } G \cong C_2^{n-1}.$$

In this section we will prove the following result.

Theorem 5.1. *Let p and q be primes, G be an elementary p-group and G' be an elementary q-group with $\mathsf{D}(G) \neq 3$. If $\mathcal{L}(G) = \mathcal{L}(G')$, then $G \cong G'$.*

Since we just investigate elementary p-groups, we will have, from Proposition 5.1 until the end of the paper, as general assumption that G is an elementary p-group and some additional notation introduced there.

In Theorem 5.1 but even more in its proof Davenport's constant is of importance. Recall that if G is an elementary p-group with $\mathsf{r}(G) = r$, then $\mathsf{D}(G) = 1 + (p-1)r$. Consequently, C_3 and C_2^2 are the only elementary p-groups and in fact the only abelian groups with Davenport's constant equal to 3. Thus the theorem gives, that apart from C_2^2 and C_3 any elementary p-group is characterized by its system of sets of lengths among all other groups that are elementary q-groups for some prime q.

To prove Theorem 5.1 we make use of the notion of elasticity one of the most investigated invariants in the theory of non-unique factorization (cf. the survey article [2] in [1]). For a non-empty, finite subset $L \subset \mathbb{N}$

$$\rho(L) = \frac{\max L}{\min L} \in \mathbb{Q}_{\geq 1}$$

is called the elasticity of L, and one sets $\rho(\{0\}) = 1$. Let H be a BF-monoid and $a \in H$. Then $\rho(a) = \rho(\mathsf{L}(a))$ is called the elasticity of a and

$$\rho(H) = \sup\{\rho(a) \mid a \in H\} \in \mathbb{R}_{\geq 1} \cup \{\infty\}$$

the elasticity of H.

By definition, a BF-monoid is half-factorial if and only if $\rho(H) = 1$. In the following lemma we summarize some facts on the elasticity, which we need in the proofs of Proposition 5.2 and 5.3. As usual, we write $\rho(G_0)$ instead of $\rho(\mathcal{B}(G_0))$.

Lemma 5.1. [16, 14] *Let H be a BF-monoid.*

(1) *If $H = \prod_{i=1}^{r} H_i$, then $\rho(H) = \sup\{\rho(H_i) \mid i \in [1, r]\}$.*
(2) *Let $H = \mathcal{B}(G_0)$ for a non-empty subset of an abelian group G. Then $\rho(G_0) \leq \frac{1}{2}\mathsf{D}(G_0)$. If $G_0 = \{-g \mid g \in G_0\}$, then $\rho(G_0) = \frac{1}{2}\mathsf{D}(G_0)$.*

Another concept we will use are decomposable and indecomposable sets. A non-empty subset $G_0 \subset G$ is decomposable, if G_0 has a partition $G_0 = G_1 \dot{\cup} G_2$ with non-empty sets G_1, G_2, such that $\mathcal{B}(G_0) = \mathcal{B}(G_1) \times \mathcal{B}(G_2)$ (equivalently $\langle G_0 \rangle = \langle G_1 \rangle \oplus \langle G_2 \rangle$). Otherwise G_0 is indecomposable. In the proof of Proposition 5.2 we will make use of the fact that every non-empty set $G_0 \subset G$ has a (up to order) uniquely determined decompositions into indecomposable sets (cf. [22, Section 3]). Note that minimal non-half-factorial sets are indecomposable.

An important tool to characterize groups is that $\mathsf{D}(G)$ is determined by $\mathcal{L}(G)$.

Lemma 5.2. [9, Lemma 7] *Let G be a finite abelian group with $|G| \geq 2$. Then*

$$\mathsf{D}(G) = \max\{\max L \mid L \in \mathcal{L}(G) \text{ with } 2 \in L\}.$$

From here until the end of this paper, although not explicitly stated in the exposition, all groups G will be elementary p-groups with $\mathsf{r}(G) = r$ and $\{e_1, \ldots, e_r\} \subset G$ an independent set.

The results established in Section 4 give information on $\Delta_1(G)$.

Proposition 5.1.

$$\max \Delta_1(G) = \max\{p-2, r-1\}$$

and $\Delta_1(G)$ is an interval if and only if $p \leq 2r+1$.

Proof. By Lemma 3.1 and Theorem 4.1 the statement on $\max \Delta_1(G)$ is obvious. Clearly, in case $\Delta^*(G)$ is an interval, we get by Lemma 3.1 $\Delta_1(G)$ is an interval as-well. Conversely, suppose that $\Delta^*(G)$ is not an interval. Then Theorem 4.1 implies that $p > 2r+1$ and $p-r-2 \notin \Delta^*(G)$. Since $p-r-2 > \frac{1}{2}\max \Delta^*(G)$, it follows that $p-r-2 \nmid d$ for any $d \in \Delta^*(G)$. Thus $p-r-2 \notin \Delta_1(G)$ hence $\Delta_1(G)$ is not an interval. □

Another result we will need to prove Theorem 5.1 is Proposition 5.3. In its proof we investigate properties of sets of lengths that are arithmetical progressions with maximal difference. We need some preparatory results, in particular on sets G_0 such that $\min \Delta(G_0)$ is maximal. Note that several of the occurring sets are just the sets considered in Lemma 3.4.

Lemma 5.3. *Let $g = \sum_{i=1}^{r} e_i$, $G_0 = \{g\} \cup \{e_1, \ldots, e_r\}$ and*

$$W_1 = g \prod_{i=1}^{r} e_i^{p-1}.$$

Then for every $n \in \mathbb{N}$ we have

$$\mathsf{L}(W_1^n) = \{n + i(r-1) \mid i \in [0, n - \left\lceil \frac{n}{p} \right\rceil]\}.$$

Proof. As usual we set $W_j = g^j \prod_{i=1}^p e_i^{p-j}$ for each $j \in [1,p]$. Then it follows, either by a simple direct argument or by Lemma 4.1.2 and 3., that

$$\mathcal{A}(G_0) = \{e_i^p \mid i \in [1,r]\} \cup \{W_j \mid j \in [1,p]\}.$$

Let $n \in \mathbb{N}$ and $s = n - \lceil \frac{n}{p} \rceil$. Suppose that

$$W_1^n = \prod_{\nu=1}^p W_\nu^{j_\nu} \prod_{\nu=1}^r (e_\nu^p)^{i_\nu}$$

with $j_1, \dots, j_p, i_1, \dots, i_r \in \mathbb{N}_0$. Clearly, we have $n = \mathsf{v}_g(W_1^n) = \sum_{\nu=1}^p \nu j_\nu$ hence $\sum_\nu^p j_\nu \in [n-s, n]$. Since

$$\mathsf{k}(\prod_{\nu=1}^p W_\nu^{j_\nu}) = \sum_{\nu=1}^p j_\nu \mathsf{k}(W_\nu) = \sum_{\nu=1}^p j_\nu (r - \frac{\nu(r-1)}{p}) = r\sum_{\nu=1}^p j_\nu - n\frac{(r-1)}{p}$$

and

$$n(r - \frac{r-1}{p}) = \mathsf{k}(W_1^n) = r\sum_{\nu=1}^p j_\nu - n\frac{r-1}{p} + \sum_{\nu=1}^r i_\nu,$$

it follows that

$$\begin{aligned}\sum_{\nu=1}^p j_\nu + \sum_{\nu=1}^r i_\nu &= \sum_{\nu=1}^p j_\nu + n(r - \frac{r-1}{p}) - r\sum_{\nu=1}^p j_\nu + n\frac{r-1}{p} \\ &= n + (n - \sum_{\nu=1}^p j_\nu)(r-1) \in \{n + i(r-1) \mid i \in [0,s]\}.\end{aligned}$$

Conversely, let $i \in [n-s, n]$. Then there exist $j_1, \dots, j_p \in \mathbb{N}_0$ with $\sum_{\nu=1}^p j_\nu = i$ and $\sum_{\nu=1}^p \nu j_\nu = n$, which implies that

$$W_1^n = \prod_{\nu=1}^p W_\nu^{j_\nu} \prod_{\nu=1}^r (e_i^p)^{n - \sum_{\nu=1}^p j_\nu}$$

and

$$\sum_{\nu=1}^p j_\nu + \sum_{\nu=1}^r (n - \sum_{\nu=1}^p j_\nu) = i + r(n-i) = n + (n-i)(r-1).$$

Therefore, we obtain that

$$\{n + i(r-1) \mid i \in [0,s]\} \subset \mathsf{L}(W_1^n).$$

□

In the following considerations we need a result on certain half-factorial sets. It was obtained in [25, Lemma 1] (cf. also [26, 5.]) and in [6, Lemma 3.6] a result is proved that contains it as a special case.

Lemma 5.4. *Let $g = -\sum_{i=1}^{r} b_i e_i$ with $b_i \in [0, p-1]$ for each $i \in [1, r]$. If $\{g, e_1, \ldots, e_r\}$ is half-factorial, then $\sum_{i=1}^{r} b_i = p - 1$.*

Lemma 5.5. *Let $p - 2 \geq r$ and $G_0 \subset G$. Then $G_0 \subset G$ is indecomposable with* $\min \Delta(G_0) = p - 2$ *if and only if $G_0 = \{-g, g\}$ for some $g \in G \setminus \{0\}$.*

Proof. If $G_0 = \{-g, g\}$ for some $g \in G \setminus \{0\}$, then obviously G_0 is indecomposable and Lemma 3.4 implies that $\min \Delta(G_0) = p - 2$.

Conversely, let $G_0 \subset G$ be indecomposable with $\min \Delta(G_0) = p - 2$. Then $|G_0| \geq 2$. Suppose that $\mathsf{r}(\langle G_0 \rangle) = 1$ and let $g \in G_0$. If $ag \in G_0$ for some $a \in [2, p-1]$, then [10, Theorem 1] (respectively Lemma 3.3.4 with $A = (ag)g^{p-a}$) implies that $\min \Delta(G_0) \mid a - 1$. Thus $a = p - 1$ and $G_0 = \{-g, g\}$.

Assume to the contrary that $\mathsf{r}(\langle G_0 \rangle) \geq 2$, and let $G_1 \subset G_0$ be a minimal non-half-factorial subset. Then $\min \Delta(G_0) \mid \min \Delta(G_1)$ by Lemma 3.3.1. Assume that G_1 has some proper subset G_2 which is not a minimal generating set for $\langle G_2 \rangle$. Then Corollary 3.1 implies that

$$\min \Delta(G_1) \mid \gcd(\{\mathsf{k}(A) - 1 \mid A \in \mathcal{A}(G_0)\})$$

hence

$$\begin{aligned} p - 2 =& \min \Delta(G_0) \leq \min \Delta(G_1) \leq \max\{\mathsf{k}(A) - 1 \mid A \in \mathcal{A}(G_1)\} \\ \leq& \mathsf{K}(G) - 1 = \frac{1}{p}(1 + r(p-1)) - 1 \leq \frac{1}{p}(1 + (p-2)(p-1)) - 1, \end{aligned}$$

a contradiction. Hence each proper subset of G_1 is independent. Since G_1 is minimal non-half-factorial and thus not independent, we get that G_1 is simple (also cf. [22, Lemma 4.4]). Since

$$\min \Delta(G_1) \geq p - 2 > \max\{r - 1, \left\lfloor \frac{p}{2} \right\rfloor - 1\},$$

Proposition 4.1 implies that $G_1 = \{-g, g\}$ for some $g \in G \setminus \{0\}$.

Moreover, the considerations imply that every simple, non-half-factorial subset of G_0 is equal to $\{-g', g'\}$ for some $g' \in G_0$.

We set $e_1' = g$. Let $\{e_2', \ldots, e_{r'}'\} \subset G_0$ such that $\{e_1', \ldots, e_{r'}'\}$ is an independent generating set for $\langle G_0 \rangle$. Since G_0 is indecomposable, there exists some $h \in G_0$ such that $h = -\sum_{i=1}^{r'} b_i e_i'$ with $b_i \in [0, p-1]$, $b_1 \neq 0$ and $b_j \neq 0$ for some $j \in [2, r']$. Let $I = \{i \in [1, r'] \mid b_i \neq 0\}$. Then $\{h\} \cup \{e_i' \mid i \in I\}$ is simple and since $|I| \geq 2$ we obtain that $\{h\} \cup \{e_i' \mid i \in I\}$ is half-factorial. Thus by Lemma 5.4 we have $\sum_{i \in I} b_i = p - 1$. Clearly, $-e_1' \in G_0$, $\{-e_1'\} \cup \{e_2', \ldots, e_r'\}$ is independent, $h = -(p - b_1)(-e_1') - \sum_{i=2}^{r'} b_i e_i'$ and $\{h, -e_1'\} \cup \{e_i' \mid i \in I \setminus \{1\}\}$ is simple and has to be half-factorial. However, we have $(p - b_1) + \sum_{i \in I \setminus \{1\}} b_i = p - 2b_1 + \sum_{i \in I} b_i = p - 1 + p - 2b_1 \neq p - 1$, since $p \geq 3$. We obtain, again by Lemma 5.4, that $\{h, e_1'\} \cup \{e_i' \mid i \in I \setminus \{1\}\}$ is not half-factorial, a contradiction. Thus $\mathsf{r}(\langle G_0 \rangle) = 1$ and $G_0 = \{-g, g\}$. □

Proposition 5.2. *Let $p-2 \geq r$ and $G_0 \subset G$ a non-empty set. Then* $\min \Delta(G_0) = p-2$ *if and only if*

$$\mathcal{L}(G_0) = \{\{n+2k+i(p-2) \mid i \in [0,k]\} \mid n,k \in \mathbb{N}_0\}.$$

In particular, if $\min \Delta(G_0) = p-2$*, then* $\rho(G_0) = \frac{p}{2}$.

Proof. Let $\mathbb{L}$ denote the set on the right hand-side. If $\mathcal{L}(G_0) = \mathbb{L}$, then obviously $\min \Delta(G_0) = p-2$.

Conversely, suppose that $\min \Delta(G_0) = p-2$. By [22, Proposition 3.10] there exist uniquely determined non-empty subsets $G_1, \dots, G_d \subset G_0$ such that

$$\mathcal{B}(G_0) = \prod_{i=1}^{d} \mathcal{B}(G_i)$$

and consequently

$$\mathcal{L}(G_0) = \{\sum_{i=1}^{d} L_i \mid L_i \in \mathcal{L}(G_i)\}.$$

Clearly, there exists some $i \in [1,d]$ such that G_i is non-half-factorial. Then Theorem 4.1 implies that

$$p-2 = \min \Delta(G_0) \leq \min \Delta(G_i) \leq \max \Delta^*(G) = \max\{r-1, p-2\} = p-2$$

hence by Lemma 5.5 it follows that $G_i = \{-g, g\}$ with some $g \in G \setminus \{0\}$.

Thus it remains to verify the following three assertions:
A1: $\mathcal{L}(\{-g,g\}) = \mathbb{L}$ for every $g \in G \setminus \{0\}$.
A2: If $L, L' \in \mathbb{L}$, then $L + L' \in \mathbb{L}$.
A3: $\rho(G_0) = \frac{p}{2}$.
Proof of A1: Let $g \in G \setminus \{0\}$. For $n,k \in \mathbb{N}_0$ we set

$$B_{n,k} = -g^{kp} g^{(n+k)p} \in \mathcal{B}(\{-g,g\}).$$

Then $\mathsf{L}(B_{n,k}) = \{n+2k+i(p-2) \mid i \in [0,k]\}$, hence $\mathbb{L} \subset \mathcal{L}(\{-g,g\})$.

Let $B = -g^v g^w \in \mathcal{B}(\{-g,g\})$. We may suppose $w \geq v$. Clearly, $w \equiv v \bmod p$. Let $m \in [0,p-1]$ and $n', k' \in \mathbb{N}_0$, such that $v = m + n'p$ and $w = m + (n'+k')p$. Then $B = (-gg)^m B_{n',k'}$ and

$$\mathsf{L}(B) = m + \mathsf{L}(B_{n',k'}) = \{(m+n') + 2k' + i(p-2) \mid i \in [0,k']\} \in \mathbb{L}.$$

Proof of A2: Let $L, L' \in \mathbb{L}$ and $n, n', k, k' \in \mathbb{N}_0$ such that $L = \{n+2k+i(p-2) \mid i \in [0,k]\}$ and $L' = \{n'+2k'+i(p-2) \mid i \in [0,k']\}$. Then we have

$$\begin{aligned} L + L' =& \{n+2k+i(p-2) \mid i \in [0,k]\} + \{n'+2k'+i(p-2) \mid i \in [0,k']\} \\ =& \{n+n'+2(k+k')+i(p-2) \mid i \in [0,k+k']\} \in \mathbb{L}. \end{aligned}$$

Proof of A3: Let $g \in G\backslash\{0\}$ and set $G' = \{-g, g\}$. Since $\mathsf{D}(G') = p$, Lemma 5.1.2 implies that $\rho(G') = \frac{p}{2}$. Hence by Lemma 5.1.1 and the considerations of this proof, we obtain $\rho(G_0) = \frac{p}{2}$. □

Next we investigate blocks that have arithmetical progressions with difference $p-2$ as sets of lengths. We will show that such blocks can be factorized in a block for which the set of distances of the support is a subset of $\{p-2\}$ and a block with bounded length. Problems of this type were initially investigate in [8] to determine the structure of sets of lengths in block monoids.

Lemma 5.6. *Let $p-2 \geq r$. Then there exists a constant $N(G) \in \mathbb{N}$ such that for every $B \in \mathcal{B}(G_0)$ with $\Delta(\mathsf{L}(B)) = \{p-2\}$ the following statement holds: there exist $B_1, B_2 \in \mathcal{B}(G)$ with $|B_1| \leq N(G)$, $\Delta(\operatorname{supp}(B_2)) \subset \{p-2\}$ and $B = B_1B_2$.*

Proof. Let $B \in \mathcal{B}(G)$ with $\Delta(\mathsf{L}(B)) = \{p-2\}$. We construct blocks $B_1, B_2 \in \mathcal{B}(G)$ in such a way that $|B_1|$ is bounded above by a constant, not depending on B but only on G, and all remaining conditions are satisfied. We set $G_0 = \operatorname{supp}(B)$ and proceed in two steps.

1. We assert that there is some $N_1(G) \in \mathbb{N}$ and a partition $G_0 = G_1 \dot\cup G_2$ such that $B = F_1F_2$ with $F_i \in \mathcal{F}(G_i)$ for $i \in [1,2]$, $\Delta(G_2) \subset \{p-2\}$ and $|F_1| \leq N_1(G)$.

For every non-half-factorial set $G_0' \subset G$, let $B(G_0') \in \mathcal{B}(G_0')$ such that

$$\min\Delta(G_0') = \min\Delta(\mathsf{L}(B(G_0'))).$$

Let

$$N_1'(G) = \max\{\max\{\mathsf{v}_g(B(G_0')) \mid g \in G_0'\} \mid G_0' \subset G \text{ non-half-factorial}\},$$

$G_2 = \{g \in G_0 \mid \mathsf{v}_g(B) \geq N_1'(G)\}$ and $G_1 = G_0 \setminus G_2$.

If $G_2 = \emptyset$, we have $\Delta(G_2) = \emptyset$, $F_2 = 1$, $F_1 = B$ and $|F_1| = |B| \leq |G|N_1'(G)$.

Suppose that $G_2 \neq \emptyset$. Since $B(G_2) \mid B$, it follows that

$$p-2 = \min\Delta(\mathsf{L}(B)) \leq \min\Delta(\mathsf{L}(B(G_2))) = \min\Delta(G_2).$$

Theorem 4.1 implies that

$$\min\Delta(G_2) \leq \max\Delta^*(G) = \max\{p-2, r-1\} = p-2$$

hence $\min\Delta(G_2) = p-2$. By Proposition 5.2 we infer that $\Delta(G_2) = \{p-2\}$. By construction, we obtain that

$$|F_1| \leq |G_1|N_1'(G) \leq |G|N_1'(G).$$

2. Let $B_2 \in \mathcal{B}(G)$ be maximal (with respect to divisibility) such that $B_2|F_2$. Then $\Delta(\operatorname{supp}(B_2)) \subset \Delta(G_2) \subset \{p-2\}$ and $B_2^{-1}F_2$ is zero-sumfree

and therefore $|B_2^{-1}F_2| < \mathsf{D}(G)$. Setting $B_1 = F_1(B_2^{-1}F_2)$ we obtain that $B = B_1B_2$ and

$$|B_1| \le |G|N_1'(G) + \mathsf{D}(G).$$

□

Proposition 5.3. *Let p and q be primes with $p > q \ge 2$ and $(p-1)(q-1) \ge 3$. Then*

$$\mathcal{L}(C_p^{q-1}) \neq \mathcal{L}(C_q^{p-1}).$$

Proof. If $q = 2$, then $p \ge 5$ and by Proposition 5.1 we get that $\Delta_1(C_q^{p-1})$ is an interval and $\Delta_1(C_p^{q-1})$ is not an interval and consequently $\mathcal{L}(C_p^{q-1}) \neq \mathcal{L}(C_q^{p-1})$.

Suppose that $q \ge 3$. If $k \in \mathbb{N}$ with $q-1 \mid k$, then Lemma 5.3 (with $r = p-1$, $p = q$, $n = k + \frac{k}{q-1}$ and $s = n - \lceil \frac{n}{q} \rceil = k$) implies that

$$L_k = \{(k + \frac{k}{q-1}) + i(p-2) \mid i \in [0,k]\} \in \mathcal{L}(C_q^{p-1}).$$

Note that $\rho(L_k) = \frac{\max L_k}{\min L_k} = \frac{q+(q-1)(p-2)}{q}$.

We show that $L_k \notin \mathcal{L}(C_p^{q-1})$ for sufficiently large k. Let $k \in \mathbb{N}$ with $q-1 \mid k$ and assume to the contrary there is some $B_k \in \mathcal{B}(C_p^{q-1})$ such that $\mathsf{L}(B_k) = L_k$.

By Lemma 5.6 there exist some constant $N(C_p^{q-1}) \in \mathbb{N}$, not depending on k, and blocks $B_{k,1}, B_{k,2} \in \mathcal{B}(G)$ with $|B_{k,1}| \le N(C_p^{q-1})$ and $\Delta(G_k) \subset \{p-2\}$, where $G_k = \operatorname{supp}(B_{k,2})$, such that $B_k = B_{k,1}B_{k,2}$. If k is large enough, then $|\mathsf{L}(B_{k,2})| > 1$ hence $\Delta(G_k) = \{p-2\}$. Moreover, for any $l \in \mathbb{N}$ there exists some $k(l) \in \mathbb{N}$ such that $|\mathsf{L}(B_{k,2})| > l$ if $k \ge k(l)$.

By [8, Proposition 5] we obtain that there exists some constant $M \in \mathbb{N}$ not depending on k (for example $M = N(C_p^{q-1})\mathsf{D}(C_p^{q-1})$ is a possible choice) such that

$$\max \mathsf{L}(B_k) \le \max \mathsf{L}(B_{k,2}) + M$$

and

$$\min \mathsf{L}(B_k) \ge \min \mathsf{L}(B_{k,2}) - M.$$

Thus we obtain, if k is sufficiently large, that

$$\begin{aligned} \frac{q+(q-1)(p-2)}{q} &= \rho(L_k) = \rho(\mathsf{L}(B_k)) \\ &\le \frac{\max \mathsf{L}(B_{k,2}) + M}{\min \mathsf{L}(B_{k,2}) - M} = \frac{\rho(\mathsf{L}(B_{k,2})) + \frac{M}{\min \mathsf{L}(B_{k,2})}}{1 - \frac{M}{\min \mathsf{L}(B_{k,2})}}. \end{aligned}$$

Since by Lemma 5.1.2 and Proposition 5.2 $\rho(\mathsf{L}(B_{k,2})) \le \rho(G_k) = \frac{p}{2}$ and since $|\mathsf{L}(B_{k,2})|$ and hence $\min \mathsf{L}(B_{k,2})$ can be arbitrarily large, we obtain that for any $\epsilon > 0$

$$\frac{M}{\min(\mathsf{L}(B_{k,2}))} < \epsilon,$$

if k is sufficiently large. Hence

$$\frac{p}{2} < \frac{q + (q-1)(p-2)}{q} \le \frac{\frac{p}{2} + \epsilon}{1 - \epsilon},$$

for any ϵ with $0 < \epsilon < 1$, a contradiction. □

Proof of Theorem 5.1. Let G be an elementary p-group with $\mathsf{r}(G) = r$ and G' an elementary q-group with $\mathsf{r}(G') = s$ and $\mathsf{D}(G) \neq 3$. Suppose that $\mathcal{L}(G) = \mathcal{L}(G')$. We have to prove that $p = q$ and $r = s$. By definition of $\Delta_1(G)$ and by Lemma 5.2 it follows that

$$\mathsf{D}(G) = \mathsf{D}(G') \text{ and } \Delta_1(G) = \Delta_1(G').$$

Thus we obtain

$$r(p-1) = \mathsf{D}(G) - 1 = \mathsf{D}(G') - 1 = s(q-1)$$

and, by Proposition 5.1,

$$\max\{p-2, r-1\} = \Delta_1(G) = \Delta_1(G') = \max\{q-2, s-1\}.$$

If $\max\{p-2, r-1\} = p-2$, then either

$$p - 2 = q - 2 \text{ hence } p = q \text{ and } r = s$$

or

$$p - 2 = s - 1 \text{ hence } s = p - 1 \text{ and } r = q - 1.$$

If $\max\{p-2, r-1\} = r-1$, then either

$$r - 1 = s - 1 \text{ hence } r = s \text{ and } p = q$$

or

$$r - 1 = q - 2 \text{ hence } r = q - 1 \text{ and } s = p - 1.$$

Suppose that $s = p - 1$ and $r = q - 1$. If $\mathsf{D}(G) = 2$, then $p = q = 2$ and $r = s = 1$. If $\mathsf{D}(G) = (q-1)(p-1) + 1 \ge 4$, then Proposition 5.3 implies that $p = q$ and hence $r = s$. □

References

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

[2] D.F. ANDERSON, *Elasticity of factorizations in integral domains: a survey.* In [1], 1–29.

[3] L. CARLITZ, *A characterization of algebraic number fields with class number two.* Proc. Amer. Math. Soc. **11** (1960), 391–392.

[4] S. CHAPMAN, A. GEROLDINGER, *Krull domains and monoids, their sets of lengths and associated combinatorial problems.* In [1], 73–112.

[5] P. VAN EMDE BOAS, *A combinatorial problem on finite abelian groups II.* Report ZW-1969-007, Math. Centre, Amsterdam (1969), 60p.

[6] W. GAO, A. GEROLDINGER, *Half-factorial domains and half-factorial subsets in abelian groups.* Houston J. Math. **24** (1998), 593–611.

[7] W. GAO, A. GEROLDINGER, *Systems of sets of lengths II.* Abh. Math. Sem. Univ. Hamburg **70** (2000), 31–49.

[8] A. GEROLDINGER, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente.* Math. Z. **197** (1988), 505–529.

[9] A. GEROLDINGER, *Systeme von Längenmengen.* Abh. Math. Sem. Univ. Hamburg **60** (1990), 115–130.

[10] A. GEROLDINGER, *On nonunique factorizations into irreducible elements. II.* Colloq. Math. Soc. János Bolyai **51**, North-Holland, Amsterdam, 1990, 723–757.

[11] A. GEROLDINGER, *The cross number of finite abelian groups.* J. Number Theory **48** (1994), 219–223.

[12] A. GEROLDINGER, *A structure theorem for sets of lengths.* Colloq. Math. **78** (1998), 225–259.

[13] A. GEROLDINGER, Y. OULD HAMIDOUNE, *Zero-sumfree sequences in cyclic groups and some arithmetical application.* Journal Théor. Nombres Bordeaux **14** (2002), 221–239.

[14] A. GEROLDINGER, G. LETTL, *Factorization problems in semigroups.* Semigroup Forum **40** (1990), 23-38.

[15] A. GEROLDINGER, R. SCHNEIDER, *The cross number of finite abelian groups III.* Discrete Math. **150** (1996), 123–130.

[16] F. HALTER-KOCH, *Elasticity of factorizations in atomic monoids and integral domains.* J. Théor. Nombres Bordeaux **7** (1995), 367–385.

[17] F. HALTER-KOCH, *Finitely generated monoids, finitely primary monoids and factorization properties of integral domains.* In [1], 31–72.

[18] F. HALTER-KOCH, *Ideal Systems.* Marcel Dekker Inc., New York, 1998.

[19] U. KRAUSE, *A characterization of algebraic number fields with cyclic class group of prime power order.* Math. Z. **186** (1984), 143–148.

[20] W. NARKIEWICZ, *Elementary and analytic theory of algebraic numbers, second edition.* Springer-Verlag, Berlin, 1990.

[21] J.E. OLSON, *A combinatorial problem on finite abelian groups, I,.* J. Number Theory **1** (1969), 8–10.

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

[23] W.A. SCHMID, *Half-factorial sets in elementary p-groups.* Far East J. Math. Sci. (FJMS), to appear.

[24] L. SKULA, *On c-semigroups.* Acta Arith. **31** (1976), 247–257.

[25] J. ŚLIWA, *Factorizations of distinct length in algebraic number fields.* Acta Arith. **31** (1976), 399–417.

[26] J. ŚLIWA, *Remarks on factorizations in algebraic number fields.* Colloq. Math. **46** (1982), 123–130.

[27] A. ZAKS, *Half factorial domains.* Bull. Amer. Math. Soc. **82** (1976), 721–723.

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