PERIODS OF SETS OF LENGTHS: A QUANTITATIVE RESULT AND AN ASSOCIATED INVERSE PROBLEM

WOLFGANG A. SCHMID

Abstract. The investigation of quantitative aspects of non-unique factorizations in the ring of integers of an algebraic number field gives rise to combinatorial problems in the class group of this number field. In this paper we investigate the combinatorial problems related to the function $\mathcal{P}(H, \mathcal{D}, M)(x)$, counting elements whose sets of lengths have period $\mathcal{D}$, for extreme choices of $\mathcal{D}$. If the class group fulfils certain conditions, we obtain the value of an exponent in the asymptotic formula of this function and results that imply oscillations of an error-term.

1. Introduction and main results

Let K be an algebraic number field, R its ring of integers, H the monoid of non-zero principal ideals of R and G the ideal class group. Then every non-zero element of R (or every element of H, respectively) is a product of finitely many irreducible elements (principal ideals, respectively), but such a factorization need not be unique (unless G is trivial). In the sixties W. Narkiewicz initiated the investigation of quantitative aspects of non-unique factorizations in algebraic number fields. That means one studies, for arithmetically interesting subsets $Z \subset H$, the asymptotic behavior of the associated counting function $Z(x) = |\{a \in Z \colon |a| \le x\}|$ for x tending to infinity. For an overview on known results see [20, Chapter 9] and [10, Chapter 9] and for recent contributions see, e.g., [1] and [24].

We start our discussion with a classical example, which is relevant for the investigations of this paper. Then, we turn to the problem actually considered in this paper and formulate the main results.

Suppose that $|G| \ge 3$ and let $a \in H$. If $a = u_1 \cdot \ldots \cdot u_l$ is a factorization of a into irreducible elements $u_1, \ldots, u_l \in H$, then l is called the length of the factorization and $\mathsf{L}(a) = \{l \in \mathbb{N}_0 \colon a \text{ has a factorization of length } l\} \subset \mathbb{N}_0$ denotes the set of lengths of a. Recall that $|G| \ge 3$ implies that for every $N \in \mathbb{N}$ there exists some $a \in H$ such that $|\mathsf{L}(a)| \ge N$. If $k \in \mathbb{N}$ and $\mathcal{G}_k = \mathcal{G}_k(H) = \{a \in H \colon |\mathsf{L}(a)| \le k\}$, then

$$\mathcal{G}_k(x) \sim Cx(\log x)^{-1+\mu(G)/|G|}(\log\log x)^{\psi_k(G)}$$

2000 *Mathematics Subject Classification.* 11R27 (11N64 20K01).

Key words and phrases. almost arithmetical multiprogression, block monoid, number field, set of lengths.

Supported by the Austrian Science Fund FWF (Project P18779-N13).

where C is a positive real constant, and $\mu(G) \in \mathbb{N}$ and $\psi_k(G) \in \mathbb{N}_0$ depend only on G and k (see Subsection 2.2 for the precise definition of $\mu(G)$ and $\psi_k(G)$).

The function $\mathcal{G}_k(x)$ was introduced by W. Narkiewicz (see [18, Theorem III]) and the above result (with the combinatorial description of the exponents) was given by A. Geroldinger [6]. Although $\mathcal{G}_k(x)$ received a lot of attention in recent years (for an overview see [10, Chapter 9]), there are still many open questions around it. Among others, even for cyclic groups the precise value of $\mu(G)$ is in general unknown (see [23]) and even less is known on $\psi_k(G)$ (see [25, 29]). Yet, since it is known that $\mu(G) < |G|$, for $|G| \geq 3$, a simple consequence of the above formula is that the density of all elements $a \in H$ with $|\,\mathsf{L}(a)| \leq k$ is zero.

In the present paper we study counting functions that deal with arbitrarily long sets of lengths. Such counting functions were considered initially in [5, Proposition 10] and [6, Satz 2], and more recently in [10, Chapter 9]. By a result of A. Geroldinger [5] (see [9] or [10] for generalizations and refinements) it is known that sets of lengths have a certain structure. Namely, there exists some bound $M_G \in \mathbb{N}$, just depending on G, such that every set of lengths in H is an almost arithmetical multiprogression (an AAMP for short) with some difference $d \in \Delta^*(G)$, period $\{0, d\} \subset \mathcal{D} \subset \{0, \dots, d\}$ and bound M_G (see Subsection 2.2 for a precise definition and see below and Subsection 2.1 for a definition of the set $\Delta^*(G)$).

Now fix some difference d, some period $\mathcal{D}$ and some bound M, and let $\mathcal{P}(H, \mathcal{D}, M)$ denote the set of all $a \in H$ for which the set of lengths $\mathsf{L}(a)$ is a long AAMP with difference d, period $\mathcal{D}$ and bound M (in Subsection 2.2 we make the term "long" precise).

The present paper is devoted to the counting functions $\mathcal{P}(H, \mathcal{D}, M)(x)$. Theorem 1.1 gives asymptotics and Theorems 1.2 and 1.3, which are the main results of the paper, deal with the exponents of $\log x$ and $\log\log x$ in the main term of the asymptotic formulas.

A weaker asymptotic formula, valid in the more general setting of abstract formations, for $\mathcal{P}(H, \mathcal{D}, M)(x)$ by A. Geroldinger and F. Halter-Koch can be found in [10, Theorem 9.4.10]. We restrict to the number field case. Thus, after showing that the sets $\mathcal{P}(H, \mathcal{D}, M)$ are arithmetical, we can directly apply the analytic results of of J. Kaczorowski [15] and M. Radziejewski [24], building on results of J. Kaczorowski, A. Perelli, and J. Pintz (see [16, 17]), to get the following result (for the short argument see Section 3).

Theorem 1.1. *Let R be the ring of integers of an algebraic number field K, H the set of all non-zero principal ideal and G the ideal class group with $|G| \geq 3$. Let $M \in \mathbb{N}$ sufficiently large, $d \in \Delta^*(G)$ and* $\{0, d\} \subset$

$\mathcal{D} \subset \{0, \dots, d\}$ be such that $\mathcal{P}(H, \mathcal{D}, M) \neq \emptyset$. There exist $\mathsf{a}_{\mathcal{D}}(G) \in \mathbb{N}$ and $\mathsf{b}_{\mathcal{D}}(G) \in \mathbb{N}_0$, just depending on G and $\mathcal{D}$, such that the following holds.

1. *For $x \ge e^e$,*

$$\mathcal{P}(H, \mathcal{D}, M)(x) = x(\log x)^{-1+\mathsf{a}_{\mathcal{D}}(G)/|G|}\big(V_{\mathcal{D}}(\log\log x) + O(\frac{(\log\log x)^m}{(\log x)^{\gamma}})\big)$$

   with $V_{\mathcal{D}}$ a polynomial with positive leading coefficient and degree $\mathsf{b}_{\mathcal{D}}(G)$, $\gamma = \frac{1}{|G|}\min\{1, 1 - \cos\frac{2\pi}{|G|}\}$ and $m \in \mathbb{N}$ depends on $\mathcal{D}$ and K.

2. *If $\mathsf{b}_{\mathcal{D}}(G) > 0$, then the following error-term is subject to oscillations of positive lower logarithmic frequency and size $x^{\frac{1}{2}-\varepsilon}$:*

$$\mathcal{P}(H, \mathcal{D}, M)(x) - \frac{1}{2\pi i}\int_{\mathcal{C}} \zeta(s, \mathcal{P}(H, \mathcal{D}, M))\frac{x^s}{s}\, ds,$$

   with $\zeta(s, \mathcal{P}(H, \mathcal{D}, M)) = \sum_{I \in \mathcal{P}(H,\mathcal{D},M)} (R : I)^{-s}$ for $\Re(s) > 1$, and the contour of integration $\mathcal{C}$ goes counterclockwise around the points $\frac{1}{2}$ and 1.

The condition that M is “sufficiently large” can be made more precise (see Subsection 2.2).

The main subject of this paper is the investigation of the constants $\mathsf{a}_{\mathcal{D}}(G)$ and $\mathsf{b}_{\mathcal{D}}(G)$ occurring in Theorem 1.1. In [10, Theorem 9.4.10] abstract combinatorial descriptions for $\mathsf{a}_{\mathcal{D}}(G)$ and $\mathsf{b}_{\mathcal{D}}(G)$ were obtained (see below and Subsection 2.2). Building on these descriptions, we derive explicit results in some special cases.

In [10, Theorem 9.4.10] the special case where $\mathcal{D} = \{0, 1\}$ has been considered. In that case $\mathcal{P}(H, \mathcal{D}, M)$ is the set of all $a \in H$ whose sets of lengths are almost arithmetical progressions with difference 1. It is proved that $\mathsf{a}_{\mathcal{D}}(G) = |G|$ and $\mathsf{b}_{\mathcal{D}}(G) = 0$. Indeed, it is even known that the set $\mathcal{P}(H, \mathcal{D}, M)$ has density 1 (cf. [10, Theorem 9.4.11]).

Here, we consider sets of lengths that are almost arithmetical progressions (that is the case where $\mathcal{D} = \{0, d\}$); for simplicity we set $\mathsf{a}_d(G) = \mathsf{a}_{\{0,d\}}(G)$ and $\mathsf{b}_d(G) = \mathsf{b}_{\{0,d\}}(G)$.

The starting point for all investigations of the invariants $\mathsf{a}_{\mathcal{D}}(G)$ and $\mathsf{b}_{\mathcal{D}}(G)$ is the set (see Subsection 2.1 for definitions of $\Delta(G_0)$ and the term “half-factorial”)

$$\Delta^*(G) = \{\min \Delta(G_0) \colon G_0 \subset G \text{ is not half-factorial } \}$$

which received a lot of attention in the recent literature (for an overview see [10, Section 6.8]). The structure of $\Delta^*(G)$ heavily depends on whether or not the exponent of G is large, in comparison with $|G|$ (see Section 4 for further discussion).

In [10, Theorem 9.4.10] it is proved that if $d \in \Delta^*(G)$ and no multiple of d is in $\Delta^*(G)$, then

$$\mathsf{a}_d(G) = \max\{|G_0| \colon G_0 \subset G, \min \Delta(G_0) = d\}.$$

Thus to determine $\mathsf{a}_d(G)$ we have to solve an inverse problem, in the sense of additive number theory. The combinatorial description of $\mathsf{b}_d(G)$ is more involved, we recall it in Subsection 2.2 after introducing more notation; to determine $\mathsf{b}_d(G)$ this inverse problem is relevant as well.

In particular, under the assumption that the exponent of G is sufficiently large (this is made precise by supposing that the invariant $\mathsf{m}(G)$, see Definition 4.1, is small; for now we note that $4 \log |G| \le \exp(G)$ is sufficient) we consider an extreme case, namely $d = \max \Delta^*(G) = \exp(G) - 2$. In this case and the case $d = \exp(G) - 3$, we solve the inverse problem; and derive the following formulas for $\mathsf{a}_d(G)$. (Note that the invariant $\mu(\cdot)$ in the results below is the same as the one appearing in the asypmtotic formula for $\mathcal{G}_k(x)$.)

Theorem 1.2. *Let $G = G' \oplus C_n$ be a finite abelian group where $G' \subset G$ is a subgroup and $\exp(G) = n$.*

(1) *If $n > \mathsf{m}(G) + 2$, then*
$$\mathsf{a}_{n-2}(G) = \begin{cases} 3 + \mu(G') & \text{if } n \text{ is prime and } G \text{ has even rank,} \\ 2 + \mu(G') & \text{otherwise.} \end{cases}$$

(2) *If $G' = G'' \oplus C_n$ for some subgroup $G'' \subset G'$ and $n > \mathsf{m}(G) + 3$, then $\mathsf{a}_{n-3}(G) = 3 + \mu(G'')$.*

We note that the condition that the exponent is large is essential (cf. Section 4 for further discussion).

Then, we consider the question of positivity of $\mathsf{b}_d(G)$ and obtain the following result. (For the significance of this question cf. Theorem 1.1.2.)

Theorem 1.3. *Let G be a finite abelian group with $\exp(G) = n$.*

(1) *If $n > \mathsf{m}(G) + 2$, then $\mathsf{b}_{n-2}(G) = 0$ if and only if G is cyclic.*
(2) *If $n > \mathsf{m}(G) + 3$ and $n - 3 \in \Delta^*(G)$, then $\mathsf{b}_{n-3}(G) > 0$.*

The result that $\mathsf{b}_{n-2}(G) = 0$ for all cyclic G is quite surprising, since it is in contrast to results obtained for related counting functions (cf. [10, Chapter 9]). More precisely, for the counting functions $\mathcal{F}_k(x)$ and $\mathcal{B}_k(x)$, counting the number of elements with at most k distinct and block-distinct, respectively, factorizations, it is known that the constants analogous to $\mathsf{b}_d(G)$, i.e., the exponents of $\log \log x$ in the leading term of the asymptotic formulas, are positive for any group G, apart the exceptional cases $|G| = 1$ and $|G| \le 2$, respectively (see [19, Proposition 9] and [8, Corollary 1]); moreover, for

$\mathcal{G}_k(x)$ it was conjectured ([24, Conjecture]) that $\psi_k(G)$ is positive, apart the exceptional cases $|G| \le 2$, and this was proved for $k \ge 2$, and for $k = 1$ for various types of groups (see [25]).

Yet, all these exceptions as well as the fact $\mathsf{b}_{\{0,1\}}(G) = 0$, mentioned above, are in a certain sense "obvious" exceptions. All constants in discussion can be defined as the maximal length of sequences, in certain free monoids, fulfilling an additional condition (cf. the definition of $\mathsf{b}_d(G)$ and $\psi_k(G)$ in Subsection 2.2), and in all those exceptional cases, in contrast to our case, the free monoids just contain the empty-sequence, and the constants are 0 essentially by definition. Moreover, for $\mathcal{B}_k(x)$, $\mathcal{F}_k(x)$, and $\mathcal{G}_k(x)$ the exceptional cases coincide with the degenerate cases that either every or no ideal is counted according as $k = 1$ or $k > 1$.

2. Notations and basic results

Our terminology is consistent with the monograph [10] to which we refer for a detailed discussion of the notions we briefly mention.

We denote for integers a, b by $[a, b]$ the interval of integers. Let G denote an, additively written, finite abelian group; let $\mathsf{r}(G)$ denote its rank and $\exp(G)$ its exponent. By C_n we denote a cyclic group with n elements. A set $\{e_1, \dots, e_r\} \subset G$, where the e_i are distinct, is called independent if $\sum_{i=1}^{r} a_i e_i = 0$, with integers a_i, implies $a_i e_i = 0$ for each $i \in [1, r]$.

2.1. **Monoids.** For $G_0 \subset G$ we denote by $\mathcal{F}(G_0)$ the (multiplicatively written) free abelian monoid with basis G_0. An element $S = \prod_{i=1}^{l} g_i = \prod_{g \in G_0} g^{v_g} \in \mathcal{F}(G_0)$ is called a sequence. The identity element of $\mathcal{F}(G_0)$ is called the empty-sequence; it will be denoted by 1. Divisors of sequences are called subsequences. $|S| = l$ is called the length of S, $\sigma(S) = \sum_{i=1}^{l} g_i$ the sum, and $\mathsf{k}(S) = \sum_{i=1}^{l} 1/\operatorname{ord} g_i$ the cross number; the set $\operatorname{supp}(S) = \{g_1, \dots, g_l\}$ is called the support. If $\sigma(S) = 0 \in G$, then S is called a zero-sum sequence (or a block); the monoid $\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \colon \sigma(S) = 0\}$ is called the block monoid over G_0; the minimal zero-sum sequences, i.e., those without proper non-trivial zero-sum subsequence, are the irreducible elements (atoms) of $\mathcal{B}(G_0)$, denoted by $\mathcal{A}(G_0)$. If there exists no subsequence $1 \ne T \mid S$ with $\sigma(T) = 0$, then S is called zero-sumfree. For $G_0 \subset G$ and $S \in \mathcal{F}(G \setminus G_0)$ let $\Omega(G_0, S) = S \cdot \mathcal{F}(G_0) \cap \mathcal{B}(G)$ and $\Omega(G_0, S, l) = \{B \in \Omega(G_0, S) \colon \mathsf{v}_g(B) \ge l$ for each $g \in G_0\}$.

As already introduced in the Introduction for the monoid of principal ideals of the ring of integers, we denote for $a \in H$, where H is a Krull monoid (for instance, a block monoid), by $\mathsf{L}(a)$ the set of lengths of a.

For a set $L = \{l_1, l_2, \dots\} \subset \mathbb{N}$ with $l_i < l_{i+1}$, typically a set of lengths, let $\Delta(L) = \{l_2 - l_1, l_3 - l_2, \dots\}$ denote the set of (successive) distances. For

$G_0 \subset G$ let $\Delta(G_0) = \bigcup_{B \in \mathcal{B}(G_0)} \Delta(\mathsf{L}(B))$ the set of distances of G_0. Note that $\Delta(G_0) = \Delta(G_0 \cup \{0\})$ for every $G_0 \subset G$.

The set of differences of G is defined as

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

we will frequently make use of the fact that indeed $\min \Delta(G_0) = \gcd \Delta(G_0)$.

A set $G_0 \subset G$ with $\Delta(G_0) = \emptyset$ is called half-factorial, since in this case $\mathcal{B}(G_0)$ is a half-factorial monoid; a monoid is called half-factorial if for each element u of the monoid $|\mathsf{L}(u)| = 1$. It is a well known result, obtained by L. Skula [30] and A. Zaks [31], that G_0 is half-factorial if and only if

$$\mathsf{k}(A) = 1 \text{ for every } A \in \mathcal{A}(G_0); \tag{1}$$

moreover, $\mathcal{B}(G)$ is half-factorial if and only if $|G| \le 2$. Thus $\Delta^*(G) = \emptyset$ if and only if $|G| \le 2$. Moreover, for $|G| \ge 3$ one has $\min \Delta(G) = 1 \in \Delta^*(G)$.

Naturally, if $\Delta(G_0) \neq \emptyset$, then G_0 is referred to as non-half-factorial; if all proper subsets of G_0 are half-factorial, G_0 is called minimal non-half-factorial. For a non-half-factorial set G_0 some information on $\Delta(G_0)$ can as well be obtained from the cross numbers of atoms; more precisely the following holds: if n denotes the exponent of G, then for every $A \in \mathcal{A}(G_0)$ one has $\{n, n\,\mathsf{k}(A^n)\} \subset \mathsf{L}(A^n)$, in particular (see [4])

$$\min \Delta(G_0) \mid n(\mathsf{k}(A) - 1). \tag{2}$$

2.2. **AAMPs and related notions.** Now, we recall the central definitions for our investigations. Let $d, M \in \mathbb{N}$ and $\{0, d\} \subset \mathcal{D} \subset [0, d]$. A set $L \subset \mathbb{Z}$ is called an AAMP with difference d, period $\mathcal{D}$ and bound M if

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

for some integer y, $\emptyset \neq L^* = [0, \max L^*] \cap (\mathcal{D} + d\mathbb{Z})$, $L' \subset [-M, 1]$, and $L'' \subset \max L^* + [1, M]$. The sets L', L'', and L^* are called the initial, end, and central part, respectively.

Let H a Krull monoid with finite class group G and $|G| \ge 3$. Then there exists a constant M_G, just depending on G, such that for each $a \in H$ the set of lengths $\mathsf{L}(a)$ is an AAMP with bound M_G (see [10, Chapter 4] or [9] for even more general statements).

For $d \in \mathbb{N}$ and $\{0, d\} \subset \mathcal{D} \subset [0, d]$ let

$$\begin{aligned} \mathcal{P}(H, \mathcal{D}, M) = \{a \in H \colon\ & \mathsf{L}(a) \text{ is AAMP with period } \mathcal{D} \text{ bound } M, \\ & \max \mathsf{L} - \min \mathsf{L} \ge 3M + d_0^2\}, \end{aligned}$$

where $d_0 = \max \Delta(G)$ (the constant d_0 is indeed finite, for instance $d_0 \le |G| - 2$ and more precise results are known). For simplicity we write $\mathcal{P}(G, d, M)$ instead of $\mathcal{P}(\mathcal{B}(G), \{0, d\}, M)$.

In Theorem 1.1 we formulated a result on the counting functions of the sets $\mathcal{P}(H, \mathcal{D}, M)$ for all sufficiently large M. To get the result as stated, it turns out we only need to suppose that M is sufficiently large to ensure that every set of lengths of an element of $\mathcal{B}(G)$ is an AAMP with bound $M - d_0$, i.e., $M \ge M_G + d_0$. Yet, the combinatorial descriptions for $\mathsf{a}_{\mathcal{D}}(G)$ and $\mathsf{b}_{\mathcal{D}}(G)$ obtained in [10, Theorem 9.4.10] are only known to be valid, if M fulfils an additional condition. This condition is very technical and, since we do not need the precise condition, we only mention that there exists a constant $M(G)$ such that for $M \ge M(G)$ the statement of Theorem 1.1 holds, in particular $M(G) \ge M_G + d_0$, and the exponents $\mathsf{a}_{\mathcal{D}}(G)$ and $\mathsf{b}_{\mathcal{D}}(G)$ are given in the following way (we only formulate the special case we actually consider, the general case is similar but rather more technical): For $d \in \Delta^*(G)$ let $\mathsf{A}_d(G) = \{G_0 \subset G \colon \min \Delta(G_0) = d\}$. Then (see [10, Theorem 9.4.10])

$$\mathsf{a}_d(G) = \max\{|G_0| \colon G_0 \in \mathsf{A}_d(G)\}$$

and

$$\begin{aligned} \mathsf{b}_d(G) = \max\{|S| \colon G_0 \in \mathsf{A}_d(G), S \in \mathcal{F}(G \setminus G_0), \text{ for some } l \in \mathbb{N} \\ \emptyset \ne \Omega(G_0, S, l) \subset \mathcal{P}(G, d, M(G))\}. \end{aligned}$$

For $d \notin \Delta^*(G)$ we set $\mathsf{A}_d(G) = \emptyset$ and $\mathsf{a}_d(G) = \mathsf{b}_d(G) = 0$. Since we need it in the proof of Lemma 7.1, we finally mention that for $G' \subset G$ one has $M(G') \le M(G)$.

Now, we recall the combinatorial description for the invariants $\mu(G)$ and $\psi_k(G)$. We have $\mu(G) = \max\{G_0 \subset G \colon G_0 \text{ half-factorial}\}$ and

$$\begin{aligned} \psi_k(G) = \max\{|S| \colon G_0 \subset G \text{ half-factorial}, \mu(G) = |G_0|, S \in \mathcal{F}(G \setminus G_0) \\ \text{and } |\mathsf{L}(B)| \le k \text{ for every } B \in \Omega(G_0, S)\}. \end{aligned}$$

2.3. **Indecomposable sets.** We recall the definition of an indecomposable set and some related notions (see [27]). A subset $G_0 \subset G$ is called decomposable if $\mathcal{B}(G_0) = \mathcal{B}(G_1) \cdot \mathcal{B}(G_2)$ for non-empty and disjoint $G_1, G_2 \subset G_0$, equivalently $\langle G_0 \rangle = \langle G_1 \rangle \oplus \langle G_2 \rangle$ and $G_0 = G_1 \dot\cup G_2$; we call G_1, G_2 components of G_0 and speak of a decomposition of G_0. If $\mathcal{B}(G_0) = \mathcal{B}(G_1) \dots \mathcal{B}(G_s)$ with indecomposable and pairwise disjoint sets G_i, then we refer to this as a decomposition into indecomposables and call G_i the indecomposable components of G_0. Every set has an essentially (i.e., up to ordering) unique decomposition into indecomposables. We recall that a set is half-factorial if and only if all its components are half-factorial. Moreover, if G_0 is not half-factorial and $G_1, \dots, G_s$ are its indecomposable components, then $\min \Delta(G_0) = \gcd\{\min \Delta(G_i) \colon G_i \text{ non-half-factorial}\}$.

3. Proof of Theorem 1.1

In this section we present the proof of Theorem 1.1. We recall the definition of an arithmetical set (see [10, Definition 9.4.1] also cf. [14, Definition 5]) for subsets of the block monoid. Let G be a finite abelian group. A subset $\mathcal{Z} \subset \mathcal{B}(G)$ is called arithmetical if for all $B_1, B, B_2 \in \mathcal{B}(G)$ one has that $B_1, B_2 \in \mathcal{Z}$ and $B_1 \mid B \mid B_2$ implies that $B \in \mathcal{Z}$.

Next, we prove that the sets $\mathcal{P}(\mathcal{B}(G), \mathcal{D}, M)$ are arithmetical.

Lemma 3.1. *Let G, d, $\mathcal{D}$, and M as in Theorem 1.1. Then, $\mathcal{P}(G, \mathcal{D}, M)$ is an arithmetical set.*

In the proof of this result we make use of two facts on subsets of the integers (cf. [10, Lemma 4.2.4]): Let $d, d' \in \mathbb{N}$, $y \in \mathbb{Z}$, and $A, B \subset \mathbb{Z}$. If $y + A + d\mathbb{Z} \subset A + d\mathbb{Z}$, then $y + A + d\mathbb{Z} = A + d\mathbb{Z}$. If $(B + d\mathbb{Z}) \cap [y+1, y+\ell] \subset A + d'\mathbb{Z}$ and $\ell \geq \operatorname{lcm}\{d, d'\}$, then $B + d\mathbb{Z} \subset A + d'\mathbb{Z}$.

Proof of Lemma 3.1. Recall that we have $M \geq M_G + d_0$ (see Subsection 2.2). Let $B_1, B_2 \in \mathcal{P}(\mathcal{B}(G), \mathcal{D}, M)$ and let $B \in \mathcal{B}(G)$ such that $B_1 \mid B \mid B_2$. We have to show that $B \in \mathcal{P}(\mathcal{B}(G), \mathcal{D}, M)$. Let $C_1, C_2 \in \mathcal{B}(G)$ such that $C_1 B_1 = B$ and $B C_2 = B_2$. Let $c_i \in \mathsf{L}(C_i)$. Then $c_1 + \mathsf{L}(B_1) \subset \mathsf{L}(B) \subset -c_2 + \mathsf{L}(B_2)$. By definition of $\mathcal{P}(\mathcal{B}(G), \mathcal{D}, M)$ we know that $\mathsf{L}(B_1)$ and $\mathsf{L}(B_2)$ are AAMPs with difference d, period $\mathcal{D}$, bound M and $\max \mathsf{L}(B_i) - \min \mathsf{L}(B_i) \geq 3M + d_0^2$, where $d_0 = \max \Delta(G)$, i.e., $\mathsf{L}(B_i) = y_i + (L_i' \cup L_i^* \cup L_i'') \subset y_i + \mathcal{D} + d\mathbb{Z}$ for some integer y_i, $\emptyset \neq L_i^* = [0, \max L_i^*] \cap (\mathcal{D} + d\mathbb{Z})$, $L_i' \subset [-M, 1]$, and $L_i'' \subset \max L_i^* + [1, M]$ and we know that $\max L_i^* \geq M + d_0^2$. Moreover, we know that $\mathsf{L}(B)$ is an AAMP with some difference $d' \in \Delta^*(G)$, some period $\mathcal{D}'$ and bound $M - d_0$ (indeed, this is true for each element of $\mathcal{B}(G)$, cf. Subsection 2.2), i.e., $\mathsf{L}(B) = y + (L' \cup L^* \cup L'') \subset y + \mathcal{D}' + d'\mathbb{Z}$ for some integer y, $\emptyset \neq L^* = [0, \max L^*] \cap (\mathcal{D}' + d'\mathbb{Z})$, $L' \subset [-M + d_0, 1]$, and $L'' \subset \max L^* + [1, M - d_0]$. Additionally, since $\mathsf{L}(B)$ contains a shift of $\mathsf{L}(B_1)$, we know that $\max \mathsf{L}(B) - \min \mathsf{L}(B) \geq 3M + d_0^2$. Thus, we have $\max L^* \geq M + d_0^2$.

Since $c_1 + (y_1 + L_1^*) \subset c_1 + \mathsf{L}(B_1) \subset \mathsf{L}(B) \subset y + \mathcal{D}' + d'\mathbb{Z}$, we have

$$c_1 + y_1 + ([0, \max L^*] \cap (\mathcal{D} + d\mathbb{Z})) \subset y + \mathcal{D}' + d'\mathbb{Z}.$$

Since by definition $d, d' \leq d_0$ it follows (cf. above) that $c_1 + y_1 + \mathcal{D} + d\mathbb{Z} \subset y + \mathcal{D}' + d'\mathbb{Z}$. Considering $\mathsf{L}(B) \subset -c_2 + \mathsf{L}(B_2)$, we get in the same way that

$$y + \mathcal{D}' + d'\mathbb{Z} \subset -c_2 + y_2 + \mathcal{D} + d\mathbb{Z}.$$

Thus, we get (cf. above) $c_1 + y_1 + \mathcal{D} + d\mathbb{Z} = -c_2 + y_2 + \mathcal{D} + d\mathbb{Z} = y + \mathcal{D}' + d'\mathbb{Z}$. Thus, $L^* = [0, \max L^*] \cap (-c_2 + y_2 + \mathcal{D} + d\mathbb{Z})$. Let $\mathcal{D}'' = [0, d] \cap (-c_2 + y_2 + \mathcal{D} + d\mathbb{Z})$. Then, L is an AAMP with difference d, period $\mathcal{D}''$ and bound $M - d_0$.

Thus, “shifting” the central part possibly at the expense of increasing the bound (see [10, Lemma 4.2.6] for a precise statement), it follows that L is an AAMP with difference d, period $\mathcal{D}$ and bound M. We already noted that $\max \mathsf{L}(B) - \min \mathsf{L}(B) \ge 3M + d_0^2$. Thus, $B \in \mathcal{P}(\mathcal{B}(G), \mathcal{D}, M)$. □

Now, Theorem 1.1 follows quite directly from known results.

Proof of Theorem 1.1. By Lemma 3.1 we know that $\mathcal{P}(\mathcal{B}(G), \mathcal{D}, M)$ is an arithmetical set. Thus (see [10, Proposition 9.4.2]), there exist $G_1, \dots, G_n \subset G$, $S_i \in \mathcal{F}(G \setminus G_i)$ and $l_i \in \mathbb{N}_0$ such that

$$\mathcal{P}(\mathcal{B}(G), \mathcal{D}, M) = \bigcup_{i=1}^{n} \Omega(G_i, S_i, l_i). \tag{3}$$

We note that for $\Omega(G_i, S_i, l_i) \ne \emptyset$, we have $\Omega(G_i \cup \{0\}, S_i 0^{-\mathsf{v}_0(S_i)}, l_i) \subset \mathcal{P}(\mathcal{B}(G), \mathcal{D}, M)$. Thus, we have $\max\{|G_i| \colon i \in [1,n]\} > 0$. Now, using (3), the first statement follows by results of J. Kaczorowski [15] (see in particular the proof of Theorem 2 also see [14, Section 5]), with $\mathsf{a}_{\mathcal{D}}(G) = \max\{|G_i| \colon i \in [1,n]\}$ and $\mathsf{b}_{\mathcal{D}}(G) = \max\{|S_i| \colon |G_i| = \mathsf{a}_{\mathcal{D}}(G)\}$.

For the second statement we may assume that $\mathsf{a}_{\mathcal{D}}(G) < |G|$, since otherwise $\mathsf{b}_{\mathcal{D}}(G) = 0$ and it is vacuosly true. Now, again using (3) the statement follows from results of M. Radziejewski [24] (see in particular Theorem 6 and the proof of Theorem 5). □

4. The invariant $\mathsf{m}(G)$

We recall that the structure of $\Delta^*(G)$ depends on the size of $\exp(G)$ relative to $|G|$. To illustrate this, we recall some results: If G is cyclic of order n, then (see [11])

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

Yet, if G is a p-group of large rank, then $\Delta^*(G)$ is an interval (see [4]). However, much on $\Delta^*(G)$ is up to now unknown; for general G, even $\max \Delta^*(G)$ is only known if the exponent of G is sufficiently large, and in that case $\max \Delta^*(G) = \exp(G) - 2$ (see [28]).

In this section we introduce $\mathsf{m}(G)$, used in the formulations of Theorems 1.2 and 1.3 to give a precise meaning to to the informal statement that $\exp(G)$ is large. First, we introduce the notion LCN-set; the idea motivating this definition is well-know and present in several earlier investigations on $\Delta^*(G)$.

Definition 4.1. Let G be a finite abelian group.

(1) A subset $G_0 \subset G$ is called a set with large cross numbers (LCN-set for short) if $\mathsf{k}(A) \ge 1$ for each $A \in \mathcal{A}(G_0)$.

(2) We set

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

if there exists no non-half-factorial LCN-set, then $\mathsf{m}(G) = 0$.

We note that, since $g^{\operatorname{ord} g} \in \mathcal{A}(G_0)$ is an atom with cross number 1 for every $g \in G_0$, the value 1 is the largest possible value for which such a definition makes sense. Moreover, by (1) half-factorial sets are LCN-sets.

Next, we explain the significance of these notions for our investigations.

Proposition 4.2 ([4])**.** *Let G be a finite abelian group with exponent n. If $n > 2$, then*

$$\max\{\min \Delta(G_0) \colon G_0 \textit{ non-half-factorial and non-LCN }\} = n - 2;$$

in particular, $\max \Delta^*(G) = \max\{n - 2, \mathsf{m}(G)\}$.

Thus, the conditions on the exponent in Theorem 1.2 are just strong enough to assert that the sets in questions are not LCN-sets. We have to impose this condition, since for LCN-sets not even the basic direct problems, for instance to determine $\mathsf{m}(G)$, are solved in general. Thus, at present it does not seem (to the author) feasible to address the inverse problems. In any case, results on LCN-sets for (elementary) p-groups with large rank (cf. Proposition 4.4 and the subsequent remark) indicate that results (and proofs) for groups with "small" exponent should be quite different.

At the end of this section we give upper and lower bounds for $\mathsf{m}(G)$, which can be used to decide, for various types of groups, whether the conditions of Theorem 1.2 hold.

First, we recall the definition of the (little) cross number, $\mathsf{k}(G)$, of a finite abelian group G and some results. It is a well known, in the context of non-unique factorizations, invariant defined as

$$\mathsf{k}(G) = \max\{\mathsf{k}(S) \colon S \in \mathcal{F}(G) \text{ zero-sumfree}\}.$$

For $\mathsf{k}(G)$ a variety of results are known, though the precise value is unknown in general; we summarize those that we shall need in this paper.

Proposition 4.3. *Let G be a finite abelian group.*

(1) $\mathsf{k}(G) \le \log |G|$ *(see* [13]*).*
(2) *If $G = C_{n_1} \oplus \dots \oplus C_{n_r}$ is a p-group, then* $\mathsf{k}(G) = \sum_{i=1}^{r}(n_i - 1)/n_i$ *(see* [7]*).*
(3) *If $G = C_{p^m} \oplus C_{p^n} \oplus C_q^s$ with $m, n, s \in \mathbb{N}$ and distinct primes p and q, then* $\mathsf{k}(G) = (p^m - 1)/p^m + (p^n - 1)/p^n + s(q - 1)/q$ *(see* [12]*).*

In [26, Theorem 5.4] it is proved that

$$\mathsf{m}(G) \le 2\,\mathsf{k}(G) - 1; \tag{4}$$

clearly, using Proposition 4.3, more explicit bounds can derived from (4). The inequality (4) is sharp for elementary 2-groups, yet not in general, as can be seen from the following result.

Proposition 4.4. *Let G be a finite abelian group with $\mathsf{r}(G) \ge 2$. Then $\mathsf{m}(G) \ge \mathsf{r}(G) - 1$. If G is an elementary p-group, then equality holds.*

Moreover, [4, Theorem 1.5] yields that $\mathsf{m}(G) = \mathsf{r}(G) - 1$ for p-groups with sufficiently large rank (relative to the exponent) as well. We apply the following lemma, to prove the proposition.

Lemma 4.5. *Let $G_0 = \{g, e_1, \dots, e_r\}$ with independent e_i and $g \in G$. If G_0 is a non-half-factorial LCN-set, then* $\min \Delta(G_0) \le r - 1$.

In [28, Proposition 4.1] $\min \Delta(G_0)$ for "simple" sets has been investigated. This lemma strengthens that result under the additional condition that G_0 is a LCN-set; the proofs are very similar.

Proof of Lemma 4.5. By [27, Theorem 4.5] we may assume without restriction that $g = \sum_{i=1}^r a_i e_i$ with $a_i e_i \ne 0$ for each $i \in [1, r]$. Let $n = \operatorname{ord} g$ and $D = \min \Delta(G_0)$. For $j \in [1, n]$ let W_j denote the (unique) minimal block with $\mathsf{v}_g(W_j) = j$; let $B_j \in \mathcal{B}(\{e_1, \dots, e_r\})$ such that $W_j B_j = W_1^j$. Note that $\mathsf{L}(B_j) = \{\mathsf{k}(B_j)\}$ for every j. We know that W_1 and $W_n = g^n$ are atoms, and denote by $m = \min\{j \in [2, n] \colon W_j \in \mathcal{A}(G_0)\}$. If $m = n$, it follows (by [28]) that $\min \Delta(G_0) = |n - 1 - r|$; since $1 \le \mathsf{k}(W_1) = (r + 1)/n$, we have $|n - 1 - r| \le r - 1$. If $\mathsf{k}(W_1) = 1$, it follows (by [28]) that for any $A \in \mathcal{A}(G_0)$ with $\mathsf{k}(A) \ne 1$, $\min \Delta(G_0) \le \mathsf{k}(A) - 1 < r$. Thus assume $m < n$ and $\mathsf{k}(W_1) > 1$. Let $k = \min\{j \in [2, n] \colon \mathsf{L}(W_j) + \mathsf{L}(B_j) \ne \{j\}\}$. It follows (by [28]) that $W_k \in \mathcal{A}(G_0)$ and thus $\{1\} + \{\mathsf{k}(B_k)\} = \mathsf{L}(W_k) + \mathsf{L}(B_k)$. Consequently, $\min \Delta(G_0) \le |1 + \mathsf{k}(B_k) - k|$. If $1 + \mathsf{k}(B_k) > k$ it follows (by [28]) that $\min \Delta(G_0) \le r - 1$. Thus assume $1 + \mathsf{k}(B_k) < k$. By definition of k we have $\{k - 1\} = \mathsf{L}(W_{k-1}) + \mathsf{L}(B_{k-1})$; say $l \in \mathbb{N}$ such that $\{l\} = \mathsf{L}(W_{k-1})$.

We assert that $l \le r$. Note $W_{k-1} = g^{k-1} F$ with $F \in \mathcal{F}(\{e_1, \dots, e_r\})$ zero-sumfree, thus $\mathsf{k}(F) \le \sum_{i=1}^r (1 - 1/\operatorname{ord} e_i) < r$ and $\mathsf{k}(W_{k-1}) < r + 1$. Yet, since G_0 is a LCN-set, we have $\mathsf{k}(W_{k-1}) \ge l$ and the assertion is proved. Since W_k is an atom $B_k \ne B_{k-1}$ and thus $\mathsf{k}(B_k) \ge 1 + \mathsf{k}(B_{k-1})$. All this yields,

$$k - (1 + \mathsf{k}(B_k)) \le k - (2 + \mathsf{k}(B_{k-1})) = k - (2 + k - 1 - l) \le r - 1,$$

and finishes the proof. □

Now, we turn to the proof of Proposition 4.4.

Proof of Proposition 4.4. Let $\mathsf{r}(G) = r$. First, we show that $\mathsf{m}(G) \ge r - 1$. Let $\{e_1, \dots, e_r\} \subset G$ independent with $\operatorname{ord} e_1 = \dots = \operatorname{ord} e_r$, and $g =$

$\sum_{i=1}^{r} e_i$. By [4, Proposition 5.2], the set $G_0 = \{g, e_1, \dots, e_r\}$ is an LCN-set and $\min \Delta(G_0) = r - 1$.

Now, assume G is an elementary p-group and let $G_0 \subset G$ be a LCN-set. We have to show that $\min \Delta(G_0) \le r - 1$. Without restriction we assume that G_0 is minimal non-half-factorial. If G_0 fulfills the conditions of Lemma 4.5 the result is obvious, and if this is not the case it follows that $\min \Delta(G_0) \le 1/p + \mathsf{k}(G) - 1 < r - 1$, the first inequality by [28, Corollary 3.1] (also cf. Proof of Theorem 4.1 there) the second by Proposition 4.3. □

Finally, we prove a (weak) upper bound for $\mathsf{m}(C_n^2)$, which we will need in Section 6.

Lemma 4.6. *Let $n \ge 5$. Then $\mathsf{m}(C_n^2) \le n - 4$.*

Since we make use of it in the proof of this result, we briefly recall the definition of Davenport's constant, $\mathsf{D}(G)$, of a finite abelian group G:

$$\mathsf{D}(G) = \max\{|A| \colon A \in \mathcal{A}(G)\}.$$

It is easy to see that $\mathsf{D}(G) = 1 + \max\{|S| \colon S \in \mathcal{F}(G) \text{ zero-sumfree}\}$. The value of Davenport's constant is known for various groups, but is in general unknown (cf. [10, Chapter 5] for a detailed discussion). We only use the fact that $\mathsf{D}(C_n^2) = 2n - 1$ for each $n \in \mathbb{N}$ (see [21]).

Proof of Lemma 4.6. By (4) we know $\mathsf{m}(C_n^2) \le 2\,\mathsf{k}(C_n^2) - 1$. This yields $\mathsf{m}(C_n^2) \le 4(\log n) - 1$, which is less than $n - 3$ for $n \ge 12$, and $\mathsf{m}(C_n^2) \le 3$ if n is a prime power, by Proposition 4.3 part 1. and 2., respectively. Moreover, by Proposition 4.4 we know that $\mathsf{m}(C_n^2) = 1$ if n is a prime. Thus, it remains to consider $n = 6$ and $n = 10$. Using Proposition 4.3.3, we get $\mathsf{m}(C_{10}^2) \le 21/5$ and $\mathsf{m}(C_6^2) \le 11/3$.

Consequently, it remains to show that $\mathsf{m}(C_6^2) \ne 3$. Seeking a contradiction, we assume that there exist some subset $G_0 \subset C_6^2$ that is an LCN-set with $\min \Delta(G_0) = 3$. Since we know that $\mathsf{m}(C_6^2) < 6$, we may assume without restriction that G_0 is minimal non-half-factorial. Let $A \in \mathcal{A}(G_0)$. By (2) we know that $6(\mathsf{k}(A) - 1)$ is a multiple of 3 and thus, by Proposition 4.3.3 and since G_0 is an LCN-set, $\mathsf{k}(A) \in \{1, 3/2, 2, 5/2\}$.

Let $W \in \mathcal{A}(G_0)$ with maximal cross number. We note that $\mathsf{k}(W) > 1$ and $\operatorname{supp}(W) = G_0$. We write $W = S_2 S_3 S_6$ where S_i denotes the subsequence of elements of order i. We recall that, for each $i \in [1, 3]$, $|S_i| \le \mathsf{D}(C_i^2)$, and equality can only hold if $W = S_i$.

Case 1: $\mathsf{k}(W) = 3/2$. Since $\mathsf{k}(W^2) = 3$, we have $\max \mathsf{L}(W^2) \le 3$. Since $\min \Delta(G_0) = 3$, this yields $\mathsf{L}(W^2) = \{2\}$. Consequently, every factorization of W^2 consists of two atoms each with cross number $3/2$. This implies that $S_2 = 1$, since otherwise W^2 would be divisible by an atom with cross number 1. Similarly, since $\mathsf{k}(W^3) = 9/2$ we have $S_3 = 1$ and $\mathsf{v}_g(W) = 1$ for each $g \in G_0$. Now, let $h \in G_0$ and we consider $(h^{-1}W)^2$. Since we know $|W| = 6\,\mathsf{k}(W) = 9$, we have $|(h^{-1}W)^2| > \mathsf{D}(C_6^2)$ and $(h^{-1}W)^2$ is not zero-sum free. Since $G_0 \setminus \{h\}$ is half-factorial, this implies that W^2 is divisible by an atom with cross number 1, a contradiction.

Case 2: $\mathsf{k}(W) = 2$. Again, we have $\mathsf{L}(W^2) = \{2\}$ and W^2 is not divisible by an atom with cross number less than 2, in particular $S_2 = 1$. Since $2|S_3| + |S_6| = 12$, we conclude that both S_3 and S_6 are non-empty. This implies that S_3^2 and S_6^2 are zero-sum free, since any minimal zero-sum subsequence of S_3 or S_6 would have cross number 1 and divide W^2. However, this implies $2|S_i| < \mathsf{D}(C_i^2)$ for $i \in \{3, 6\}$ and contradicts $2|S_3| + |S_6| = 12$.

Case 3: $\mathsf{k}(W) = 5/2$. It is easy to see that $S_6 \neq 1$. First we show that $S_3 = 1$. We assume $S_3 \neq 1$. Then $W^3 = S_3^3 \cdot (S_3^{-1}W)^{-1}$ is a factorization of W^3 into two blocks, each over a half-factorial set. This implies that $\mathsf{k}(W^3)$ is an integer, a contradiction.

Now, we have $3|S_2| + |S_6| = 15$, and $|S_2| < 3$ and $|S_6| \leq 11$. Consequently $|S_2| = 2$ and $|S_6| = 9$. Since $|S_6| > \mathsf{D}(C_3^2)$, the sequence S_6 has a non-trivial proper subsequence T_6 such that $\operatorname{ord} \sigma(T_6) = 2$. The sequence $\sigma(T_6)S_2$ has a non-trivial zero-sum subsequence and thus T_6S_2 as well. Consequently, $W = S_2S_6$ has a non-trivial proper zero-sum subsequence, a contradiction. □

5. Subsets with $\min \Delta(G_0) = \max \Delta^*(G)$

In this section we investigate the structure of subsets $G_0 \subset G$ such that $\min \Delta(G_0) = \max \Delta^*(G)$ for groups with "large" exponent, namely $\exp(G) > \mathsf{m}(G) + 2$; in particular, we prove Theorem 1.2.1.

As discussed in the preceding section, it is well-known that in this case $\max \Delta^*(G) = \exp(G) - 2$. Moreover, it is known that $\min \Delta(\{-g, g\}) = \operatorname{ord} g - 2$ for every $g \in G$ with $\operatorname{ord} g \geq 3$ (cf. [4, Proposition 5.2]) which provides examples for sets with minimal distance equal to $\max \Delta^*(G)$. In the following results we show that every indecomposable set with minimal distance equal to $\max \Delta^*(G)$ is of this form.

Theorem 5.1. *Let G be a finite abelian group with $\exp(G) > \mathsf{m}(G) + 2$ and let $G_0 \subset G$. Then G_0 is indecomposable with $\min \Delta(G_0) = \max \Delta^*(G)$ if and only if*

$$G_0 = \{-g, g\} \quad \textit{with } \operatorname{ord} g = \exp(G).$$

Proof. Let $\exp(G) = n$. By Proposition 4.2 we have $\min \Delta(G_0) = n - 2$. Since for $g \in G$ with $\operatorname{ord} g \geq 3$, by [4, Proposition 5.2], $\min \Delta(\{-g, g\}) = \operatorname{ord} g - 2$ one implication is obvious. It remains to prove the other one.

Thus, let $G_0 \subset G$ indecomposable with $\min \Delta(G_0) = n-2$ and assume to the contrary that G_0 is not of the claimed form; moreover assume that G_0 is minimal with this property. Clearly G_0 is not an LCN-set. Thus, there exists some $A \in \mathcal{A}(G_0)$ such that $\mathsf{k}(A) < 1$ and by (2) indeed $\mathsf{k}(A) = 2/n$. Consequently, $A = (-g)g$ for some g with $\operatorname{ord} g = n$, in particular $\{-g, g\} \subset G_0$. By assumption $G_0 \setminus \{-g, g\} \neq \emptyset$.

Since G_0 is indecomposable, there exists some $S \in \mathcal{A}(G_0 \setminus \{-g, g\})$ with $\sigma(S) \in \langle g \rangle \setminus \{0\}$, say $\sigma(S) = ag$ with $a \in [1, n-1]$. Assume S is minimal with this property, i.e., has no proper subsequence with this property. We consider the atoms $U = g^{n-a}S$ and $U' = (-g)^a S$. Note that $(-g)^n U = ((-g)g)^{n-a}U'$. Thus $(n-2) \mid (n-a+1-2)$ and therefore $a \in \{1, n-1\}$. Without restriction, else interchange the role of g and $-g$, assume $a = 1$.

Consequently, $|S| \geq 2$ and $\mathsf{k}(U) = (n-1)/n + \mathsf{k}(S) > 1$. Thus, the set $G_0 \setminus \{-g\}$ is not half-factorial. We have $n-2 = \min \Delta(G_0) \leq \min \Delta(G_0 \setminus \{-g\}) \leq n-2$. Since G_0 is indecomposable it follows that $G_0 \setminus \{-g\}$ is indecomposable as well and trivially $G_0 \setminus \{-g\}$ is not equal to $\{-h, h\}$ for any $h \in G$, a contradiction to the minimality of G_0. □

As discussed in Subsection 2.3 every set has a unique decomposition into indecomposables, thus Theorem 5.1 yields a description of all sets with minimal distance equal to $\max \Delta^*(G)$.

Corollary 5.2. *Let G be a finite abelian group with $\exp(G) > \mathsf{m}(G) + 2$, and let $G_0 \subset G$ with $\min \Delta(G_0) = \max \Delta^*(G)$. Further, let $G_0 = \bigcup_{i=1}^{s} G_i$ be the decomposition into indecomposable components. Then each component G_i is either half-factorial or equal to $\{-g_i, g_i\}$ for some $g_i \in G$ with $\operatorname{ord} g_i = \exp(G)$; and there exists at least one non-half-factorial component.*

Proof. At least one component has to be non-half-factorial and we have $\min \Delta(G_0) = \gcd\{\min \Delta(G_i) \colon G_i \text{ non-half-factorial}\}$ (see Subsection 2.3). We know that $\min \Delta(G_0)$ is maximal. Thus, if G_i is non-half-factorial, then $\min \Delta(G_i) = \min \Delta(G_0)$ and the result follows by Theorem 5.1. □

Before we prove Theorem 1.2.1, we derive a further auxiliary result.

Lemma 5.3. *Let $G = H_1 \oplus H_2$ and $d \in \Delta^*(G)$ such that $d\mathbb{N} \cap \Delta^*(G) = \{d\}$. If $d \in \Delta^*(H_1)$, then $\mathsf{a}_d(G) \geq \mathsf{a}_d(H_1) + \max\{\mu(H_2), \mathsf{a}_d(H_2)\} - 1$.*

Proof. Let $G_1 \in \mathsf{A}_d(H_1)$ with (maximal) cardinality $\mathsf{a}_d(H_1)$. Further let $H_0 \subset H_2$ half-factorial and, if such a set exists, $G_2 \in \mathsf{A}_d(H_2)$ with (maximal) cardinality $\mu(H_2)$ and $\mathsf{a}_d(H_2)$, respectively. Then $G_1 \cup G_2$ and $G_1 \cup H_0$ are elements of $\mathsf{A}_d(G)$. Since $G_1 \cap G_2 = G_1 \cap H_0 = \{0\}$, the result follows. □

Now the proof of Theorem 1.2.1 is almost straightforward, yet there is one exceptional case that requires the use of a recent result on half-factorial sets in elementary p-groups.

Proof of Theorem 1.2.1. Assume $n > \mathsf{m}(G) + 2$. By Theorem 5.1 it is obvious that $\mathsf{a}_{n-2}(C_n) = 3$. It follows by Lemma 5.3 that $\mathsf{a}_{n-2}(G) \ge 2 + \mu(G')$.

Let $G_0 \in \mathsf{A}_{n-2}(G)$ and let $G_0 = \bigcup_{i=1}^{s} G_i$ the decomposition into indecomposable components. By Theorem 5.1 each G_i is either half-factorial or equal to $\{-g_i, g_i\}$ for some $g_i \in G_0$ with $\operatorname{ord} g_i = n$; and there exists at least one $j \in [1, s]$ such that G_j is not half-factorial. Assume there exists more than one non-half-factorial component, say G_1 and G_2 are non-half-factorial. Now consider $G_0' = G_1' \cup \bigcup_{i=2}^{s} G_i$ where $G_1' \subset \langle g_1 \rangle \setminus \{0\}$ is half-factorial with maximal cardinality, $\mu(C_n) - 1$. We have $G_0' \in \mathsf{A}_{n-2}(G)$. Observe that $\mu(C_n) \ge 3$ unless $n \in \mathbb{P} \cup \{1\}$. Thus, if $n \notin \mathbb{P}$, then $|G_0'| \ge |G_0|$; consequently, in this case, there exists a set $G_0'' \in \mathsf{A}_{n-2}(G)$ with cardinality $\mathsf{a}_{n-2}(G)$ and exactly one non-half-factorial component, and the result follows.

So assume $n \in \mathbb{P}$, and set $r = \mathsf{r}(G)$. Repeated application of Lemma 5.3 yields $\mathsf{a}_{n-2}(G) \ge 2t + \mu(C_p^{r-t})$ for every $t \in [1, r]$. Conversely, let t denote the number of non-half-factorial components of G_0. We obtain

$$|G_0| \le 2t + \mu(C_p^{r-t}).$$

Recall (see [22]) that $\mu(C_p^r)$ equals $1 + rp/2$ for even r and $2 + (r-1)p/2 = 1 + \mu(C_p^{r-1})$ for odd r. Thus, $2t + \mu(C_p^{r-t})$ is maximal for odd r if $t = 1$, and for even r if $t = 2$, which implies the result. □

Since $\mu(C_n) = 3$ if and only if $n = p^2$ for some prime p, the proof of Theorem 1.2.1 yields that if n is not a prime or the square of a prime, then every $G_0 \in \mathsf{A}_{n-2}(G)$ with maximal cardinality, has exactly one non-half-factorial component. It might be interesting to note that for $G = C_{p^2}^2 = \langle e_1 \rangle \oplus \langle e_2 \rangle$ there actually exist sets in $\mathsf{A}_{p^2-2}(G)$ with cardinality $\mathsf{a}_{p^2-2}(G)$ both with one and two non-half-factorial components, e.g., $\{0, e_1, pe_1, e_2, -e_2\}$ and $\{0, e_1, -e_1, e_2, -e_2\}$.

6. Subsets with $\min \Delta(G_0) = \max \Delta^*(G) - 1$

Having dealt with sets where the minimal distance is maximal, we turn to the investigation of sets with minimal distance $\max \Delta^*(G) - 1$, again assuming that the exponent of G is sufficiently large (now we assume $\exp(G) > \mathsf{m}(G) + 3$). Of course, for $\max \Delta^*(G) - 1$ it is not granted by definition that sets with according minimal distance exist; indeed, as mentioned in Section 4 for cyclic groups (of order at least 5) this is not the case. However, if two independent elements $\{e_1, e_2\} \subset G$ each with order $\exp(G)$ exist, then the set $\{-e_1 - e_2, e_1, e_2\}$ has minimal distance $\exp(G) - 3$ (see [2, Example 4.11]). It turns out that, in case of "large" exponent, sets of this type are the only indecomposable ones with minimal distance $\exp(G) - 3$.

Theorem 6.1. *Let G be a finite abelian group with $\exp(G) > \mathsf{m}(G) + 3$ and let $G_0 \subset G$. Then G_0 is indecomposable with $\min \Delta(G_0) = \max \Delta^*(G) - 1$ if and only if*

$$G_0 = \{-e_1 - e_2, e_1, e_2\} \text{ with independent } \{e_1, e_2\} \text{ and } \operatorname{ord} e_i = \exp(G).$$

In particular, $\max \Delta^*(G) - 1 \in \Delta^*(G)$ if and only if there exist two independent elements each with order $\exp(G)$.

Again, we start with some auxiliary results.

Lemma 6.2. *Let $\exp(G) = n > \mathsf{m}(G) + 3$, and $G_0 \in \mathsf{A}_{n-3}(G)$. Then there exists an independent set $\{e_1, e_2\}$ with $\operatorname{ord} e_i = n$ such that $\{-e_1 - e_2, e_1, e_2\} \subset G_0$.*

Proof. Since $\mathsf{m}(G) < n - 3$ the set G_0 is not LCN. Thus there exists some $A \in \mathcal{A}(G_0)$ such that $\mathsf{k}(A) < 1$. By (2) we have $\mathsf{k}(A) = 3/n$, in particular $|A| \leq 3$. Since $|A| \leq 2$ yields a contradiction, we have $|A| = 3$, say $A = gh(-g-h)$, and each element in A has order n. It remains to show that g and h are independent. Suppose not. Then there exist $a, b \in [1, n-1]$ such that $g^a h^b$ is an atom. Again by (2) it follows that $a + b \in \{3, n, 2n - 3\}$; and in fact $a + b = 2n - 3$ is impossible, since in this case $g^{n-a}h^{n-b} \mid g^a h^b$, contradictory to $g^a h^b$ an atom. Assume $a + b = 3$, say $a = 2$ and $b = 1$. It follows that n is odd and $g^{(n+1)/2}h$ is an atom with cross number $(n+3)/2n$; a contradiction, since this would imply $(n-3) \mid (n-3)/2$. Now, assume $a + b = n$. Without restriction assume $a \leq b$. We consider the block

$$(g^a h^b) \cdot (-g-h)^n = ((-g-h)gh)^a \cdot ((-g-h)^{n-a}h^{b-a}).$$

If $B = (-g-h)^{n-a}h^{b-a}$ is an atom, it follows that $(n-3) \mid (a-1)$ and thus $a = 1$, which implies $b = n - 1$ and $g = h$, and is contradictory to B an atom. Thus B is not an atom. Since $\mathsf{k}(B) < 2$, there exist some atom A_1 such that $A_1 \mid B$ and $\mathsf{k}(A_1) < 1$. Using (2) again we infer that $\mathsf{k}(A_1) = 3/n$. As above, this yields an atom with cross number $(n+3)/2n$ and a contradiction. □

Lemma 6.3. *Let $n \geq 5$. Let $G_0 \in \mathsf{A}_{n-3}(C_n^2)$. Then $G_0 \setminus \{0\} = \{-e_1 - e_2, e_1, e_2\}$ with independent $\{e_1, e_2\}$ where $\operatorname{ord} e_i = n$.*

Proof. By Lemma 4.6 we know that $n > \mathsf{m}(C_n^2) + 3$. Consequently, by Lemma 6.2 we have $H_0 = \{-e_1 - e_2, e_1, e_2\} \subset G_0$ for suitable independent $\{e_1, e_2\}$ with $\operatorname{ord} e_i = n$. Thus it suffices to show that for $g \in C_n^2 \setminus (H_0 \cup \{0\})$

we have $\min \Delta(H_0 \cup \{g\}) \neq n-3$; say $g = -ae_1 - be_2$ with $a, b \in [0, n-1]$ and assume $a \geq b$.

In case $b > 0$, the identity

$$(5) \qquad (ge_1^a e_2^b) \cdot (-e_1 - e_2)^n = (g(-e_1 - e_2)^{n-b} e_1^{a-b}) \cdot ((-e_1 - e_2)e_1e_2)^b;$$

implies that $(n-3) \mid (b+1-2)$. Thus, we have $b \in \{0, 1, n-2\}$.

In case $a > b$, the identity

$$(6) \qquad (g(-e_1 - e_2)^{n-a} e_2^{b+n-a}) \cdot e_1^n = (ge_1^a e_2^b) \cdot ((-e_1 - e_2)e_1e_2)^{n-a}$$

implies that $(n-3) \mid (n-a+1-2)$. Thus, if $a > b$, then $a \in \{2, n-1\}$.

Consequently, it remains to consider the following cases (note that $(a, b) = (1, 1)$ and $(a, b) = (n-1, 0)$ are impossible):

Case 1: $(a, b) = (n-2, n-2)$. The relation

$$(ge_1^{n-2} e_2^{n-2})^2 = e_1^n e_2^n (g^2 e_1^{n-4} e_2^{n-4})$$

implies $(n-3) \mid 1$, a contradiction.

Case 2: $(a, b) \in \{(2, 1), (n-1, 1), (n-1, n-2)\}$. The atom $ge_1^a e_2^b$ has cross number $4/n$, $1 + 1/n$, or $(2 - 2/n)$, and thus $n-3$ divides $n-4$, 1, or $n-2$, respectively; a contradiction.

Case 3: $(a, b) = (2, 0)$. If n is even, then ge_1^2 has cross number $4/n$ and $(n-3) \mid (n-4)$, a contradiction. If n is odd, then the atom $g^{(n+1)/2} e_1$ has cross number $(n+3)/2n$ and $(n-3) \mid (n-3)/2$, a contradiction. □

Proof of Theorem 6.1. We set $\exp(G) = n$. By Proposition 4.2 we have $\max \Delta^*(G) - 1 = n - 3$. As recalled in the introduction of this section the set $\{-e_1 - e_2, e_1, e_2\}$ with independent $\{e_1, e_2\}$ and $\operatorname{ord} e_i = n$ has minimal distance $n-3$, and obviously the set is indecomposable.

To prove the converse, we assume to the contrary that there exist indecomposable sets in $\mathsf{A}_{n-3}(G)$ which do not have the asserted form. Let G_0 be such a set with minimal cardinality. By Lemma 6.2 it follows that $\{-e_1 - e_2, e_1, e_2\} \subset G_0$ with independent $\{e_1, e_2\}$ where $\operatorname{ord} e_i = n$. By assumption $H_0 = G_0 \setminus \{-e_1 - e_2, e_1, e_2\} \neq \emptyset$. Since G_0 is indecomposable, it follows that there exists some $S \in \mathcal{F}(H_0)$ such that $\sigma(S) \in \langle e_1, e_2 \rangle \setminus \{0\}$. Let S be minimal with this property. Note that by Lemma 6.3 $|S| \geq 2$. Further, let $a, b \in [0, n-1]$ such that $\sigma(S) = -ae_1 - be_1$, and we assume $a \geq b$

Since S is minimal with $\sigma(S) \in \langle e_1, e_2 \rangle \setminus \{0\}$, the same reasoning as in (5) and (6) applies. Thus, it suffices to consider the following cases; in each case we give an example of an atom with cross number not equal to 1 whose support is a proper subset of G_0.

Case 1: For $(a, b) \in \{(n-2, n-2), (n-1, 1), (n-1, n-2)\}$ the atom $A = Se_1^a e_2^b$ has cross number greater 1.

Case 2: For $(a, b) \in \{(2, 1), (2, 0)\}$ we consider the atom $A = S(-e_1 - e_2)^{n-2} e_2^{n-2+b}$.

Case 3: For $(a, b) = (1, 1)$ or $(a, b) = (n-1, 0)$, we consider $A = S(-e_1 - e_2)^{n-1}$ or $A = Se_1^{n-1}$, respectively; we recall $|S| \geq 2$.

We set $G_0' = \operatorname{supp}(A)$. Then $G_0' \subsetneq G_0$ is indecomposable, since it is the support of an atom, and non-half-factorial. Since $\min \Delta(G_0')$ has to be a multiple of $n-3$ and $\max \Delta^*(G) \leq n-2$ by Proposition 4.2, it follows that $\min \Delta(G_0') = n-3$. By the minimality condition on G_0, it follows that $G_0' = \{-f_1 - f_2, f_1, f_2\}$ with independent $\{f_1, f_2\}$ where $\operatorname{ord} f_i = n$. In any case, this yields a contradiction, since $\mathsf{k}(A') \leq 1$ for every $A' \in \mathcal{A}(G_0')$, yet $\mathsf{k}(A) > 1$. □

Clearly, Theorem 6.1 implies a result similar to Corollary 5.2, since no multiple of $\exp(G) - 3$ is contained in $\Delta^*(G)$. We do not formulate it explicitly. Now, Theorem 1.2.2 follows immediately.

Proof of Theorem 1.2.2. Assume $n > \mathsf{m}(G) + 3$. By Theorem 6.1 the result is obvious for C_n^2; and thus $\mathsf{a}_{n-3}(G) \geq 3 + \mu(G'')$ by Lemma 5.3. Since $\mu(C_n^2) \geq 1 + n > 5$ (cf. [3, Corollary 6.4]), it follows that a set $G_0 \in \mathsf{A}_{n-3}(G)$ with $|G_0| = \mathsf{a}_{n-3}(G)$ has exactly one non-half-factorial component; and the result follows. □

Moreover, the results of this section yield an (unconditional) result on $\Delta^*(G)$ for G with rank at most 2. For these groups it is known (unconditionally) that $\max \Delta^*(G) = \exp(G) - 2$ (see [4, Theorem 1.4] and [10, Corollary 6.8.11] for a different argument). Here, we answer for which G we have $\exp(G) - 3 \in \Delta^*(G)$. As mentioned in Section 4, for cyclic groups a stronger result is known.

Corollary 6.4. *Let G be a finite abelian group with $\exp(G) = n$ and $\mathsf{r}(G) \leq 2$. Then $n - 3 \in \Delta^*(G)$ if and only if $n = 4$ or $G \cong C_n^2$ with $n \geq 5$.*

7. Results on $\mathsf{b}_d(G)$

Now, we investigate $\mathsf{b}_d(G)$. Essentially, we restrict to prove Theorem 1.3. For a definition of the invariant $\psi_k(G)$, used below, see Subsection 2.2.

Lemma 7.1. *Let $G_0 \in \mathsf{A}_d(G)$ with $|G_0| = \mathsf{a}_d(G)$ where $d\mathbb{N} \cap \Delta^*(G) = \{d\}$; and let $G_0 = G_1 \cup G_2$ a decomposition where G_1 is non-half-factorial.*

(1) *If $G_2 \neq \{0\}$ is half-factorial, then $\mathsf{b}_d(G) \geq \mathsf{b}_d(\langle G_1 \rangle) + \psi_1(\langle G_2 \rangle) + 1$.*
(2) *If G_2 is non-half-factorial, then $\mathsf{b}_d(G) \geq \mathsf{b}_d(\langle G_1 \rangle) + \mathsf{b}_d(\langle G_2 \rangle) + 1$.*

Proof. Without restriction assume $0 \in G_2$. Note that G_1 and, in 2. G_2 as well, have minimal distance d.

1. By Lemma 5.3 we have $G_1 \in \mathsf{A}_d(\langle G_1\rangle)$ and $|G_1| = \mathsf{a}_d(\langle G_1\rangle) - 1$, moreover G_2 is half-factorial and $|G_2| = \mu(\langle G_2\rangle)$. Without restriction, else we consider suitable $G_1' \subset \langle G_1\rangle$ and $G_2' \subset \langle G_2\rangle$, we may assume that there exists a sequence $T_2 \in \mathcal{F}(\langle G_2\rangle \setminus G_2)$ with $|T_2| = \psi_1(\langle G_2\rangle)$ such that $|\mathsf{L}(C)| = 1$ for every $C \in \Omega(G_2, T_2)$. Further, we may assume that there exists a sequence $T_1 \in \mathcal{F}(\langle G_1\rangle \setminus G_1)$ with $|T_1| = \mathsf{b}_d(\langle G_1\rangle)$ such that $\Omega(G_1, T_1, l) \subset \mathcal{P}(\langle G_1\rangle, d, M(G))$ for some $l \in \mathbb{N}$. (Recall from Subsection 2.2 that $M(G) \geq M(\langle G_1\rangle)$ and since $\Omega(G_1, T_1, l') \subset \mathcal{P}(\langle G_1\rangle, d, M(\langle G_1\rangle))$ we have $\Omega(G_1, T_1, l) \subset \mathcal{P}(\langle G_1\rangle, d, M(G))$ for some $l \geq l'$.)

Now, let $g_1 \in G_1$ and $g_2 \in G_2 \setminus \{0\}$. We set $S = (g_1 + g_2)T_1T_2$ and assert that $\Omega(G_0, S, l) \subset \mathcal{P}(G, d, M(G))$. Let $B = SF_1F_2 \in \Omega(G_0, S, l)$ where $F_1 \in \mathcal{F}(G_1)$ and $F_2 \in \mathcal{F}(G_2)$. Consider $B' = (g_1 + g_2)^{-1}g_1g_2B = (g_1T_1F_1)(g_2T_2F_2)$.

We note that B' is a block over $\langle G_1\rangle \cup \langle G_2\rangle$ and thus $\mathsf{L}(B') = \mathsf{L}(g_1T_1F_1) + \mathsf{L}(g_2T_2F_2)$. Moreover, in each factorization of B there is an atom A containing $g_1 + g_2$, and $(g_1 + g_2)^{-1}g_1g_2A$ is a product of two atoms. Conversely, in each factorization of B' there are atoms A_1 and A_2 with $g_i \mid A_i$, and $(g_1g_2)^{-1}(g_1 + g_2)A_1A_2$ is an atom. Consequently $\mathsf{L}(B') = 1 + \mathsf{L}(B)$.

By definition of T_2, since $g_2F_2 \in \mathcal{F}(G_2)$, the set $\mathsf{L}(g_2T_2F_2)$ is a singleton, say equal to $\{L\}$; and $g_1T_1F_1 \in \Omega(G_1, T_1, l) \subset \mathcal{P}(\langle G_1\rangle, d, M(G))$. Thus $\mathsf{L}(B) = -1 + L + \mathsf{L}(g_1T_1F_1)$, $B \in \mathcal{P}(G, d, M(G))$, and $\mathsf{b}_d(G) \geq |S|$.

2. The argument is quite similar to 1. We have $|G_1| = \mathsf{a}_d(\langle G_1\rangle) - 1$ and $|G_2| = \mathsf{a}_d(\langle G_2\rangle)$; and we may assume that, for $i \in \{1, 2\}$, there exist a sequence $T_i \in \mathcal{F}(\langle G_i\rangle \setminus G_i)$ with $|T_i| = \mathsf{b}_d(\langle G_i\rangle)$ such that $\Omega(G_i, T_i, l_i) \subset \mathcal{P}(\langle G_i\rangle, d, M(G))$ for some $l_i \in \mathbb{N}$. Let $g_i \in G_i \setminus \{0\}$, $S = (g_1 + g_2)T_1T_2$ and $l = \max\{l_1, l_2\}$; we assert $\Omega(G_0, S, l) \subset \mathcal{P}(G, d, M(G))$. Again, for $B = SF_1F_2 \in \Omega(G_0, S, l)$ with $F_i \in \mathcal{F}(G_i)$ consider $B' = (g_1 + g_2)^{-1}g_1g_2B$. Then $\mathsf{L}(B) = -1 + \mathsf{L}(g_1T_1F_1) + \mathsf{L}(g_2T_2F_2)$. Thus, we have $\mathsf{L}(B)$ is an AAMP with period $\{0, d\}$ and it is not difficult to see that it is bounded by $M(G)$ (cf. [10, Section 4.2] for more general results of this form). Finally, since $\max \mathsf{L}(B) - \min \mathsf{L}(B) \geq \max \mathsf{L}(g_iT_iF_i) - \min \mathsf{L}(g_iT_iF_i)$ we have $B \in \mathcal{P}(G, d, M(G))$. □

Having the auxiliary results at hand the theorem follows easily.

Proof of Theorem 1.3. 1. We assume $n > \mathsf{m}(G) + 2$. First, we assume that G is cyclic, and we have to show that $\mathsf{b}_{n-2}(G) = 0$. The argument is similar to the proof of Theorem 5.1. Let $G_0 \in \mathsf{A}_{n-2}(G)$, say $G_0 = \{0, e, -e\}$ with $\operatorname{ord} e = n$. Further, let $S \in \mathcal{F}(G \setminus G_0)$. We may assume $|S| = 1$, say $S = g = ae$ with $a \in [2, n-2]$ Let $B = ge^{n-a}(-e)^n$. Then $\mathsf{L}(B) = \{2, n-a+1\}$. For every $l \in \mathbb{N}$, the set $\Omega(G_0, g, l)$ contains a block B_1 that is divisible by

B. Thus $n-a-1 \in \Delta(\mathsf{L}(B_1))$ and $\mathsf{L}(B_1)$ is not an AAMP with period $\{0, n-2\}$. Consequently $\mathsf{b}_{n-2}(G) = 0$ for cyclic G.

Conversely, we assume G is not cyclic, and show that $\mathsf{b}_{n-2}(G) > 0$. If G is an elementary p-group with rank 2, it follows by the proof of Theorem 1.2.1 that we can apply Lemma 7.1.2 which implies $\mathsf{b}_{n-2}(G) > 0$. In any other case, it follows by the proof of Theorem 1.2.1 that there exists some $G_0 \in \mathsf{A}_{n-2}(G)$ that allows a decomposition $G_0 = G_1 \cup G_2$ with $G_2 \neq \{0\}$ half-factorial. Now, $\mathsf{b}_{n-2}(G) > 0$ by Lemma 7.1.1.

2. We assume $n > \mathsf{m}(G) + 3$. By Theorem 1.2.2 and Lemma 7.1 it suffices to show that $\mathsf{b}_{n-3}(C_n^2) > 0$. Let $G_0 = \{0, e_1, e_2, -e_1 - e_2\}$ with independent $\{e_1, e_2\}$ and $\operatorname{ord} e_i = n$. We assert that $\Omega(G_0, 2e_1 + 2e_2, l) \subset \mathcal{P}(G, n-3, M)$ for sufficiently (depending on M) large l. The only atoms in $\Omega(G_0, 2e_1+2e_2)$ are $g^{\operatorname{ord} g}$ for $g \in G_0$, $e_1e_2(-e_1-e_2)$, $(2e_1+2e_2)e_1^{n-2}e_2^{n-2}$, and $(2e_1+2e_2)(-e_1-e_2)^2$. Thus, the only minimal relations are $(2e_1+2e_2)(-e_1-e_2)^2 \cdot e_1^n \cdot e_2^n = (2e_1+2e_2)e_1^{n-2}e_2^{n-2} \cdot ((-e_1-e_2)e_1e_2)^2$ and $(e_1e_2(-e_1-e_2))^n = e_1^n \cdot e_2^n \cdot (-e_1-e_2)^n$, thus the only possible distance is $n-3$, and the result follows. □

We end with two examples, showing that the lower bounds of Lemma 7.1 can be sharp.

Example 7.2.

1. Let $n \geq 6$ be even and $G = C_2 \oplus C_n = \langle e_1 \rangle \oplus \langle e_2 \rangle$. By Theorem 1.2, $\mathsf{a}_{n-2}(G) = 4$ and we need to consider $G_0 = \{0, e_1, e_2, -e_2\}$. Let $S \in \mathcal{F}(G \setminus G_0)$ such that $\Omega(G_0, S, l) \subset \mathcal{P}(G, n-2, M)$ for some $l \in \mathbb{N}$. From the argument for cyclic groups it follows that $\operatorname{supp}(S) \subset \{e_1+e_2, e_1-e_2\}$. Without restriction we assume $(e_1+e_2) \mid S$. Since each of the two blocks

$$(e_1+e_2)e_1(-e_2) \cdot (e_1-e_2)e_1e_2 = (e_1+e_2)(e_1-e_2) \cdot e_1^2 \cdot (-e_2)e_2,$$
$$(e_1+e_2)^2e_2^{n-2} \cdot (-e_2)^n = (e_1+e_2)^2(-e_2)^2 \cdot (-e_2e_2)^{n-2}$$

has $\{2,3\}$ as set of lengths, we have $\operatorname{supp}(S) = \{e_1+e_2\}$ and $\mathsf{v}_{e_1+e_2}(S) = 1$. This implies $\mathsf{b}_{n-2}(G) = 1$.

2. Let $p \geq 5$ a prime and $G = C_p^2 = \langle e_1 \rangle \oplus \langle e_2 \rangle$. By Theorem 1.2, $\mathsf{a}_{p-2}(C_p^2) = 5$ and we need to consider $G_0 = \{0, e_1, -e_1\} \cup \{e_2, -e_2\}$. Let $S \in \mathcal{F}(G \setminus G_0)$ such that $\Omega(G_0, S, l) \subset \mathcal{P}(G, p-2, M)$ for some $l \in \mathbb{N}$. From the argument for cyclic groups it follows that $\operatorname{supp}(S) \subset \{e_1+e_2, e_1-e_2, -e_1+e_2, -e_1-e_2\}$.

We assume $(e_1+e_2) \mid S$. Since each of the four blocks

$$\begin{aligned}&(e_1+e_2)(-e_1-e_2)(-e_1)e_1(-e_2)e_2,\\&(e_1+e_2)(e_1-e_2)(-e_2)e_2e_1^{2p-2},\\&(e_1+e_2)(-e_1+e_2)(-e_1)e_1e_2^{2p-2},\\&(e_1+e_2)^2e_1^{2p-2}e_2^{2p-2}\end{aligned}$$

has $\{2,3\}$ as set of lengths, we have $\operatorname{supp}(S)=\{e_1+e_2\}$ and $\mathsf{v}_{e_1+e_2}(S)=1$. This implies $\mathsf{b}_{p-2}(G)=1$.

Acknowledgement

The author would like to thank the anonymous referee for her/his detailed suggestions and comments; in particular, for pointing out a serious gap, and indicating how to close it, in an earlier version of the proof of Theorem 1.1.

References

[1] D. M. Bradley, A. E. Özlük, R. A. Rozario, and C. Snyder. The distribution of the irreducibles in an algebraic number field. *J. Aust. Math. Soc.*, 79(3):369–390, 2005.

[2] S. T. Chapman, M. Freeze, and W. W. Smith. On generalized lengths of factorizations in Dedekind and Krull domains. In *Non-Noetherian commutative ring theory*, volume 520 of *Math. Appl.*, pages 117–137. Kluwer Acad. Publ., Dordrecht, 2000.

[3] W. Gao and A. Geroldinger. Half-factorial domains and half-factorial subsets of abelian groups. *Houston J. Math.*, 24(4):593–611, 1998.

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

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

[6] A. Geroldinger. Ein quantitatives Resultat über Faktorisierungen verschiedener Länge in algebraischen Zahlkörpern. *Math. Z.*, 205(1):159–162, 1990.

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

[8] A. Geroldinger and F. Halter-Koch. Nonunique factorizations in block semigroups and arithmetical applications. *Math. Slovaca*, 42(5):641–661, 1992.

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

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

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

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

[13] A. Geroldinger and R. Schneider. The cross number of finite abelian groups. III. *Discrete Math.*, 150(1-3):123–130, 1996.

[14] F. Halter-Koch. Chebotarev formations and quantitative aspects of nonunique factorizations. *Acta Arith.*, 62(2):173–206, 1992.

[15] J. Kaczorowski. Some remarks on factorization in algebraic number fields. *Acta Arith.*, 43(1):53–68, 1983.

[16] J. Kaczorowski and A. Perelli. Functional independence of the singularities of a class of Dirichlet series. *Amer. J. Math.*, 120(2):289–303, 1998.

[17] J. Kaczorowski and J. Pintz. Oscillatory properties of arithmetical functions. II. *Acta Math. Hungar.*, 49(3-4):441–453, 1987.

[18] W. Narkiewicz. On algebraic number fields with non-unique factorization. *Colloq. Math.*, 12:59–68, 1964.

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

[20] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers.* Springer-Verlag, Berlin, third edition, 2004.

[21] J. E. Olson. A combinatorial problem on finite Abelian groups. II. *J. Number Theory*, 1:195–199, 1969.

[22] A. Plagne and W. A. Schmid. On large half-factorial sets in elementary p-groups: Maximal cardinality and structural characterization. *Isreal J. Math.*, 145:285–310, 2005.

[23] A. Plagne and W. A. Schmid. On the maximal cardinality of half-factorial sets in cyclic groups. *Math. Ann.*, 333(4):759–785, 2005.

[24] M. Radziejewski. On the distribution of algebraic numbers with prescribed factorization properties. *Acta. Arith.*, 116:153 – 171, 2005.

[25] M. Radziejewski and W. A. Schmid. On the asymptotic behavior of some counting functions. *Colloq. Math.*, 102(2):181–195, 2005.

[26] M. Radziejewski and W. A. Schmid. Weakly half-factorial sets in finite abelian groups. *Forum Math.*, 19:727–747, 2007.

[27] W. A. Schmid. Arithmetic of block monoids. *Math. Slovaca*, 54(5):503–526, 2004.

[28] W. A. Schmid. Differences in sets of lengths of Krull monoids with finite class group. *J. Théor. Nombres Bordeaux*, 17(1):323–345, 2005.

[29] W. A. Schmid. On the asymptotic behavior of some counting functions, II. *Colloq. Math.*, 102(2):197–216, 2005.

[30] L. Skula. On c-semigroups. *Acta Arith.*, 31(3):247–257, 1976.

[31] A. Zaks. Half factorial domains. *Bull. Amer. Math. Soc.*, 82(5):721–723, 1976.

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität, Heinrichstrasse 36, 8010 Graz, Austria

E-mail address: wolfgang.schmid@uni-graz.at