ON THE ASYMPTOTIC BEHAVIOR OF SOME COUNTING FUNCTIONS

MACIEJ RADZIEJEWSKI AND WOLFGANG A. SCHMID

Abstract. The investigation of certain counting functions of elements with given factorization properties in the ring of integers of an algebraic number field gives rise to combinatorial problems in the class group. In this paper a constant arising from the investigation of the number of algebraic integers with factorizations of at most k different lengths is investigated. It is shown that this constant is positive if k is greater than 1 and that it is also positive if k equals 1 and the class group satisfies some additional conditions. These results imply that the corresponding counting function oscillates about its main term. Moreover, some new results on half-factorial sets are obtained.

1. Introduction

We study a combinatorial problem arising from the investigation of factorizations of distinct lengths in algebraic number fields and in some more general settings. Let K be an algebraic number field, $\mathcal{O}_K$ its ring of integers and G its ideal class group. If $a \in \mathcal{O}_K$ and $a = u_1 \cdot \ldots \cdot u_n$ is a factorization of a into atoms (irreducibles), then n is called the length of the factorization and $\mathsf{L}(a) = \{n \mid a \text{ has a factorization of length } n\}$ is called the set of lengths of a.

Let k be a positive integer and $|G| \geq 3$. Then $\mathbf{G}_k = \{(a) \bigm| |\mathsf{L}(a)| \leq k\}$ denotes the set of principal ideals generated by elements with factorizations of at most k different lengths and

$$\mathbf{G}_k(x) = |\{(a) \mid N(a) \leq x \text{ and } |\mathsf{L}(a)| \leq k\}|$$

the associated counting function. It is known (cf. [5]) that

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

for a $C > 0$ and non-negative integers $\mu(G)$ and $\psi_k(G)$ that depend on G (respectively G and k) alone. The invariants $\mu(G)$ and $\psi_k(G)$ are defined in combinatorial terms for any finite abelian group G (cf. Section 2 for the

2000 *Mathematics Subject Classification.* 11N64, 11R27, 20K01.

Key words and phrases. Factorizations of distinct lengths, zero-sum sequence, block monoid, half-factorial.

The first author is supported by the Foundation for Polish Science and partially supported by the Polish Research Committee (KBN grant No. 1P03A00826). The second author is supported by the Austrian Science Fund FWF (Project P16770-N12).

definitions). They remain meaningful in the more general case of arithmetical Krull monoids respectively formations (cf. [12]). There is considerable literature on $\mu(G)$ (cf. Section 5), but little is known about $\psi_k(G)$.

The aim of this paper is to show the positivity of $\psi_k(G)$ for various G and k. The study of this specific problem is motivated by analytic investigations of $\mathbf{G}_k(x)$ in [20]. There it was shown that $\psi_k(G) > 0$ implies the existence of oscillations of $\mathbf{G}_k(x)$ about its main term (cf. Section 3 for a detailed discussion).

We demonstrate that $\psi_k(G) > 0$ for all $k \geq 2$ and G with at least three elements (Theorem 6.1). For $k = 1$ we are able to prove the positivity for various types of groups (Section 7). Moreover, we will obtain some results on half-factorial sets (Propositions 5.2 and 5.4).

The investigation of the function $\mathbf{G}_k(x)$ was started by W. Narkiewicz (cf. [15, 16, 17, 19]) who also stated the problem of evaluating $\mu(G)$ (cf. [18, P 1142]). J. Śliwa (cf. [24, 25]) considered the counting functions associated to the sets $\overline{\mathbf{G}_k} = \mathbf{G}_k \setminus \mathbf{G}_{k-1}$ and demonstrated that

$$\overline{\mathbf{G}_k}(x) \sim C' x (\log x)^{-A(k,G)} (\log\log x)^{B(k,G)}$$

for some positive $C' = C'(k, K)$ and $A(k,G)$, and non-negative $B(k,G)$. Note that $\overline{\mathbf{G}_1} = \mathbf{G}_1$. J. Śliwa determined $B(k,G)$ for $|G| \leq 4$ and conjectured (cf. [25, P 1247]) that $A(k,G) = 1 - \frac{\mu(G)}{|G|}$ for all k and $(B(k,G))_{k=1}^{\infty}$ is an arithmetic progression. A. Geroldinger (cf. [5]) showed that $A(k,G) = 1 - \frac{\mu(G)}{|G|}$ for infinitely many k. It is relatively straightforward to see that

$$\psi_k(G) = \max_{l \leq k,\ A(l,G) = 1 - \frac{\mu(G)}{|G|}} B(l,G).$$

Thus the conjecture of J. Śliwa is equivalent to the statement that $(\psi_k(G))_{k=1}^{\infty}$ is an arithmetic progression. In general it is only known that $0 \leq \psi_1(G) \leq \psi_2(G) \leq \dots$ and $\lim_{k\to\infty} \psi_k(G) = +\infty$. See also J. Kaczorowski [13] for better asymptotic estimates of $\mathbf{G}_k(x)$, and F. Halter-Koch [10], A. Geroldinger and J. Kaczorowski [8], and A. Geroldinger, F. Halter-Koch and J. Kaczorowski [7] for investigations of the analogues of sets $\mathbf{G}_k$ in more general settings.

The first author would like to thank the Karl-Franzens-Universität for the support and excellent working conditions during his visit to Graz.

2. Preliminaries

Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{N}_0$ the non-negative integers and $\mathbb{P}$ the prime numbers. For $n \in \mathbb{N}$ let C_n denote a cyclic group with n elements. Throughout the paper, G will denote an, additively written, finite abelian group.

For $G_0 \subset G$ we denote by $\langle G_0 \rangle \subset G$ the subgroup generated by G_0 and we call G_0 a generating set if $\langle G_0 \rangle = G$. A subset $\{e_1, \dots, e_r\} \subset G \setminus \{0\}$, respectively its elements, is called independent, if $\sum_{i=1}^{r} m_i e_i = 0$ with $m_i \in$

$\mathbb{Z}$ implies $m_i e_i = 0$ for each $i \in \{1, \dots, r\}$. An independent generating subset of G is called a basis. By $\mathsf{r}(G)$ we denote the rank and by $\exp(G)$ the exponent of G.

We recall the definition of block monoids and several related notions, for a detailed description we refer to the survey articles [2, 11] in [1]. For a subset $G_0 \subset G$ we denote by $\mathcal{F}(G_0)$ the, multiplicatively written, free abelian monoid with basis G_0. An element $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G_0)$ with $l \in \mathbb{N}_0$ and $g_i \in G_0$ is called a sequence in G_0 and has a unique representation $S = \prod_{g \in G} g^{\mathsf{v}_g(S)}$ with $\mathsf{v}_g(S) \in \mathbb{N}_0$. By $1 \in \mathcal{F}(G_0)$ we denote the empty sequence, i.e., the identity element of $\mathcal{F}(G_0)$. If $T|S$ (in $\mathcal{F}(G_0)$), then we call T a subsequence of S and we denote by $T^{-1}S$ its co-divisor. We denote by $|S| = l$ the length, by $\mathsf{k}(S) = \sum_{i=1}^{l} \frac{1}{\operatorname{ord}(g_i)}$ the cross number and by $\sigma(S) = \sum_{i=1}^{l} g_i$ the sum of S. Further $\mathsf{K}(G) = \max\{\mathsf{k}(A) \mid A \in \mathcal{A}(G)\}$ denotes the cross number of G. Note that $\sigma(S)$ is used to denote the length of the sequence in several of the articles we quote. The length, cross number and sum define monoid homomorphisms from $\mathcal{F}(G_0)$ to $(\mathbb{N}_0, +), (\mathbb{Q}_{\geq 0}, +)$ and G, respectively.

A sequence $S \in \mathcal{F}(G_0)$ is called a zero-sum sequence (a block) if $\sigma(S) = 0$ and it is called zero-sumfree if $\sigma(T) \neq 0$ for every $1 \neq T|S$. The set of all blocks, $\mathcal{B}(G_0)$, is called block monoid over G_0. It is a Krull monoid and its atoms, $\mathcal{A}(G_0)$, are the minimal zero-sum sequences, i.e., zero-sum sequences such that no proper subsequence has sum zero. Let $B \in \mathcal{B}(G_0)$ and $B = \prod_{i=1}^{n} U_i$ with $U_i \in \mathcal{A}(G_0)$ a factorization of B into atoms. Then we call n the length of the factorization. The set $\mathsf{L}(B) = \{n \mid B \text{ has a factorization of length } n\}$ is called the set of lengths of B and is a finite subset of $\mathbb{N}_0$ (for $B = 1$ we have $\mathsf{L}(B) = \{0\}$). For $k \in \mathbb{N}_0$ we set $\mathcal{G}_k(G) = \big\{B \in \mathcal{B}(G) \bigm| |\mathsf{L}(B)| \leq k\big\}$. Note that $\mathcal{G}_0(G) = \emptyset$.

A subset $G_0 \subset G$ is called half-factorial, if $\mathcal{B}(G_0)$ is a half-factorial monoid, i.e., $|\mathsf{L}(B)| = 1$ for every $B \in \mathcal{B}(G_0)$. Let

$$\mu(G) = \max\big\{|G_0| \bigm| G_0 \subset G \text{ half-factorial}\big\}$$

denote the maximal cardinality of a half-factorial subset of G, an invariant introduced in [24]. The main tool for investigations on half-factorial sets is the following characterization (cf. [23, 24, 26] and for example [2, Proposition 5.4]): A set $G_0 \subset G$ is half-factorial if and only if $\mathsf{k}(A) = 1$ for each $A \in \mathcal{A}(G_0)$. In Section 5 we provide several further results on half-factorial sets, which we will need in Section 7. A subset $G_0 \subset G$ is said to satisfy condition (C_0) if $\mathsf{k}(A) \in \mathbb{N}$ for each $A \in \mathcal{A}(G_0)$ (cf. [25] and [3, Section 4]).

Let $G_0 \subset G$ and $S \in \mathcal{F}(G \setminus G_0)$. Then

$$\begin{aligned}\Omega(G_0, S) &= S\mathcal{F}(G_0) \cap \mathcal{B}(G)\\ &= \{B \in \mathcal{B}(G) \mid \mathsf{v}_g(B) = \mathsf{v}_g(S) \text{ for each } g \in G \setminus G_0\}.\end{aligned}$$

Having these notations at hand we are ready to recall the central definition of this paper (cf. [5]).

Definition 2.1. Let G be a finite abelian group with at least three elements and let $k \in \mathbb{N}$. Then

$$\begin{aligned}\psi_k(G) = \max\bigl\{|S| \bigm| & G_0 \subset G \text{ half-factorial with } |G_0| = \mu(G) \text{ and} \\ & S \in \mathcal{F}(G \setminus G_0) \text{ with } \emptyset \neq \Omega(G_0, S) \subset \mathcal{G}_k(G)\bigr\}.\end{aligned}$$

3. The Counting Function $\mathbf{G}_k(x)$

In this section we state the main arithmetical results of this paper. We say that a real, piecewise continuous function $f(x)$ is subject to oscillations of lower logarithmic frequency γ and size $x^{\theta-\epsilon}$ (for $\gamma > 0$, θ real) if there exists an increasing sequence of positive real numbers $(x_n)_{n=1}^{\infty}$ with $\lim_{n\to\infty} x_n = +\infty$, such that:

(1) We have $f(x_n) \neq 0$ for each n and the signs of $f(x_n)$ alternate.
(2) If $V(Y)$ denotes the number of terms of (x_n) not exceeding Y, then
$$\liminf_{Y\to\infty} \frac{V(Y)}{\log Y} = \gamma.$$
(3) If $\varepsilon > 0$, then for any Y sufficiently large the segment $[Y^{1-\varepsilon}, Y]$ contains at least one element of (x_n).
(4) We have
$$\liminf_{n\to\infty} \frac{|f(x_n)|}{x_n^{\theta-\varepsilon}} = +\infty$$
for every $\varepsilon > 0$.

The function

$$\mathbf{M}_k(x) = \frac{1}{2\pi i}\int_{\mathcal{C}} \zeta(s, \mathbf{G}_k)\frac{x^s}{s}\, ds, \qquad x \geq 1,$$

where $\mathcal{C}$ is a contour starting at $\frac{1}{2}-\delta$, for a small $\delta > 0$, going closely around $[\frac{1}{2}, 1]$, counterclockwise, and back to $\frac{1}{2} - \delta$, and $\zeta(s, \mathbf{G}_k)$ is defined by

$$\zeta(s, \mathbf{G}_k) = \sum_{\mathfrak{a}\in\mathbf{G}_k} \frac{1}{\mathrm{N}(\mathfrak{a})^s}$$

for $\operatorname{Re} s > 1$ and by analytic continuation in a larger area, is called the main term of $\mathbf{G}_k(x)$ (cf. [13], [14, Theorem 3] and [20]) and the difference is called the error term. For $x < 1$ we set $\mathbf{M}_k(x) = 0$. In [20] it was proved that the positivity of $\psi_k(G) > 0$ implies the existence of oscillations of $\mathbf{G}_k(x) - \mathbf{M}_k(x)$.

Theorem 3.1 ([20])**.** *Let K be an algebraic number field with ideal class group G and let k be a positive integer. If $|G| \geq 3$ and $\psi_k(G) > 0$, then the error term $\mathbf{G}_k(x) - \mathbf{M}_k(x)$ is subject to oscillations of positive lower logarithmic frequency and size $x^{\frac{1}{2}-\epsilon}$.*

Theorem 3.1 together with Theorem 6.1 now implies:

Theorem 3.2. *Let K be an algebraic number field with ideal class group G and let $k \geq 2$ be a positive integer. If $|G| \geq 3$, then the error term $\mathbf{G}_k(x) - \mathbf{M}_k(x)$ is subject to oscillations of positive lower logarithmic frequency and size $x^{\frac{1}{2}-\epsilon}$.*

More precise results can be obtained for quadratic number fields.

Proposition 3.3 ([21])**.** *Let K be a quadratic number field with ideal class group G, $|G| \geq 3$, and let k be a positive integer. If $\psi_k(G) > 0$ or there exists a half-factorial set $G_0 \subset G$ with $|G_0| = \mu(G)$ containing an element $g \in G_0$ of order other than $1, 2, 3, 4, 6$, then the error term $\mathbf{G}_k(x) - \mathbf{M}_k(x)$ is subject to oscillations of positive lower logarithmic frequency and size $x^{\frac{1}{2}-\epsilon}$.*

In this case using our Proposition 7.2.2 we obtain:

Corollary 3.4. *Let K be a quadratic number field with ideal class group G, $|G| \geq 3$, and suppose G is not isomorphic to $C_2^r \oplus C_4^s \oplus C_3^t$ for any non-negative integers $r, s, t \in \mathbb{N}$. Then the error term $\mathbf{G}_1(x) - \mathbf{M}_1(x)$ is subject to oscillations of positive lower logarithmic frequency and size $x^{\frac{1}{2}-\epsilon}$.*

Therefore the problem of oscillations of $\mathbf{G}_1(x) - \mathbf{M}_1(x)$ for quadratic fields is reduced to the study of $\psi_1(G)$ for some special types of groups. We further rule out some of the remaining cases in Theorem 7.1.

4. Auxiliary Results

In this section we prove several results that are needed in Section 6 and Section 7. Parts of the results of this section occurred (implicitly) already in other articles (cf. [8, 24]).

Lemma 4.1. *Let $\emptyset \neq G_0 \subset G$ and $S, S' \in \mathcal{F}(G \setminus G_0)$.*

1. *$\Omega(G_0, S) \neq \emptyset$ if and only if $\sigma(S) \in \langle G_0 \rangle$.*
2. *$\Omega(G_0, S) \cdot \Omega(G_0, S') \subset \Omega(G_0, SS')$.*
3. *Let $k, l \in \mathbb{N}_0$ such that $\Omega(G_0, S) \not\subset \mathcal{G}_k(G)$ and $\Omega(G_0, S') \not\subset \mathcal{G}_l(G)$. Then*
$$\Omega(G_0, SS') \not\subset \mathcal{G}_{k+l}(G).$$
4. *If $S|S'$ and $\emptyset \neq \Omega(G_0, S') \subset \mathcal{G}_k(G)$ for some $k \in \mathbb{N}_0$, then $\Omega(G_0, S) \subset \mathcal{G}_k(G)$.*

Proof. 1. and 2. follow immediately from the definition.

3. Let $B \in \Omega(G_0, S)$, $|\mathsf{L}(B)| \geq k+1$, and $B' \in \Omega(G_0, S')$, $|\mathsf{L}(B')| \geq l+1$. The assertion follows from the inequalities
$$|\mathsf{L}(BB')| \geq |\mathsf{L}(B) + \mathsf{L}(B')| \geq |\mathsf{L}(B)| + |\mathsf{L}(B')| - 1.$$

4. Suppose $\Omega(G_0, S) \not\subset \mathcal{G}_k(G)$. Then $\sigma(S) \in \langle G_0 \rangle$ and $\sigma(S^{-1}S') \in \langle G_0 \rangle$, so $\Omega(G_0, S^{-1}S') \not\subset \emptyset = \mathcal{G}_0(G)$ and we obtain a contradiction from (3) with $l = 0$. □

In the following lemma we investigate the effect of replacing an element $g_1 + g_2$ occurring in an atom by the sequence $g_1 g_2$.

Lemma 4.2. *Let $g_1, g_2 \in G$, $A \in \mathcal{A}(G)$ with $(g_1+g_2)|A$ and $B = (g_1+g_2)^{-1}g_1g_2A \in \mathcal{B}(G)$.*

(1) *Then $\mathsf{L}(B) \subset \{1,2\}$.*
(2) *If $G = G_1 \oplus G_2$, $g_i \in G_i \setminus \{0\}$, $A = (g_1+g_2)S_1S_2$ with $S_i \in \mathcal{F}(G_i)$ for $i \in \{1,2\}$, then $\mathsf{L}(B) = \{2\}$. In particular, $g_iS_i \in \mathcal{A}(G_i)$ for $i \in \{1,2\}$. Moreover, if $S_i' \in \mathcal{F}(G_i)$, $g_iS_i' \in \mathcal{A}(G_i)$ for $i \in \{1,2\}$, then $(g_1+g_2)S_1'S_2' \in \mathcal{A}(G)$.*

Proof. 1. Suppose $\mathsf{L}(B) \not\subset \{1,2\}$. Then there exist $B_1, B_2, B_3 \in \mathcal{B}(G) \setminus \{1\}$ with $B = B_1B_2B_3$. Without restriction let $g_1|B_1$ and $g_1g_2|B_1B_2$. Thus $(g_1g_2)^{-1}(g_1+g_2)B_1B_2|A$, a contradiction.

2. By (1) it suffices to show that $B \notin \mathcal{A}(G)$. We have

$$0 = \sigma(B) = g_1 + \sigma(S_1) + g_2 + \sigma(S_2).$$

Thus $g_i + \sigma(S_i) = 0$ and $g_iS_i \in \mathcal{B}(G)$ for $i \in \{1,2\}$. To prove the 'moreover'-part, it suffices to note that $S_1'S_2'$ is zero-sumfree. □

In the following lemma we investigate $\Omega(G_0, S)$ for sequences $S \in \mathcal{F}(G \setminus G_0) \setminus \{1\}$ that are minimal with the property $\emptyset \neq \Omega(G_0, S)$. By Lemma 4.1.2 this means $\sigma(S) \in \langle G_0 \rangle$ and $\sigma(S') \notin \langle G_0 \rangle$ for every proper subsequence $1 \neq S'|S$.

Lemma 4.3. *Let $G_0 \subset G$ half-factorial and $S \in \mathcal{F}(G \setminus G_0) \setminus \{1\}$ minimal such that $\Omega(G_0, S) \neq \emptyset$, and let $k = |\mathsf{k}(\Omega(G_0,S) \cap \mathcal{A}(G))|$. Then $\Omega(G_0, S) \subset \mathcal{G}_k(G)$ and there exists some $B_k \in \Omega(G_0, S)$ with $|\mathsf{L}(B_k)| = k$.*

Proof. Let $B \in \Omega(G_0, S)$. We need to show that $|\mathsf{L}(B)| \le k$. Let $B = \prod_{i=0}^{n} U_i$ be a factorization of B into atoms. Without restriction we assume $U_0 \notin \mathcal{A}(G_0)$. Thus there exists some $1 \neq S'|S$ such that $U_0 = S'F$ with $F \in \mathcal{F}(G_0)$. Due to the minimality of S we get $S' = S$. Consequently, $U_i \in \mathcal{A}(G_0)$ and $\mathsf{k}(U_i) = 1$ for each $i \in \{1, \ldots, n\}$. This implies that $n = \mathsf{k}(B) - \mathsf{k}(U_0)$ and

$$|\mathsf{L}(B)| \le |\{\mathsf{k}(A) \mid A \in \Omega(G_0, S) \cap \mathcal{A}(G)\}| = k.$$

Let $\{A_1, \ldots, A_k\} \subset \Omega(G_0, S) \cap \mathcal{A}(G)$ such that $|\mathsf{k}(\{A_1, \ldots, A_k\})| = k$. By definition of S we have $\sigma(S) \in \langle G_0 \rangle$ and therefore there exists some $F \in \mathcal{F}(G_0)$ such that $\sigma(F) = (k-1)\sigma(S)$. We set $B_k = S^{-(k-1)}F\prod_{i=1}^{k} A_i$. Clearly, $\sigma(B_k) = 0$ and $B_k \in \Omega(G_0, S)$. Moreover, $A_i|B_k$ for each $i \in \{1, \ldots, k\}$. Thus we get $\mathsf{k}(B_k) - \mathsf{k}(A_i) + 1 \in \mathsf{L}(B_k)$ for each $i \in \{1, \ldots, k\}$, and $|\mathsf{L}(B_k)| \ge k$. □

5. Results on half-factorial sets

In the proofs of our main results we will make use of several results on $\mu(G)$ and half-factorial subsets of finite abelian groups. In this section we summarize the known results we use and establish some new. Further results on half-factorial sets and proofs, in present terminology, of most results we quote can be found in [3].

If G is a cyclic group, say $G \cong C_n$, since every half-factorial set $G_0 \subset G$ must also satisfy condition (C_0), it follows that

$$G_0 \subset \{dg \mid 1 \le d \mid n\}$$

for some $g \in G$ with $\operatorname{ord}(g) = n$ ([3, Lemma 5.2]). Moreover, if $G_0 \subset G$ with $|G_0| = \mu(G)$, then $\langle G_0 \rangle = G$ (cf. [3, Proposition 3.5]). If n is a prime power, possibly 1, then the set on the righthand side is half-factorial. Thus, if G is a cyclic group with prime power order, say $|G| = p^m$, then $\mu(G) = m+1$ and if $G_0 \subset G$ is a half-factorial set with $|G_0| = m+1$, then $G_0 = \{p^i g \mid i \in \{0, \dots, m\}\}$ for some $g \in G$ with $\operatorname{ord}(g) = p^m$ (cf. [23, 24, 26]).

If G is an elementary p-group with rank $\mathsf{r}(G) = r$, then (cf. [8, Theorem 8])

$$1 + \left\lfloor \frac{r}{2} \right\rfloor p + 2\left(\frac{r}{2} - \left\lfloor \frac{r}{2} \right\rfloor\right) \le \mu(G) \le 1 + \left\lfloor \frac{r}{2} p \right\rfloor,$$

in particular if r is even, then $\mu(G) = 1 + \frac{r}{2}p$. Moreover, it is known that equality holds at the lower bound if $p \le 7$ (cf. [18, 22]) and there is known no example where equality does not hold.

The next lemma is essentially a reformulation of a result of L. Skula (cf. [23, Proposition 3.2]).

Lemma 5.1. *Let G be a finite abelian group and $G_0 \subset G$ a half-factorial set with $|G_0| = \mu(G)$. Then G_0 is a subgroup if and only if $|G| \le 2$.*

Proof. In [23, Proposition 3.2] it is proved that a finite abelian group G is a half-factorial set if and only if $|G| \le 2$. This proves the 'if'-part. To obtain the 'only if'-part, assume $G_0 \subset G$ is a subgroup and a half-factorial set with maximal cardinality as well. We have to show that $|G| \le 2$. Again by [23, Proposition 3.2], we get $|G_0| \le 2$, and $\mu(G) \le 2$. G cannot contain any two independent elements e_1 and e_2, since in this case $\{0, e_1, e_2\} \subset G$ would be a half-factorial subset of G with three elements, contradicting $\mu(G) \le 2$. Therefore, G is cyclic of prime power order. Since $\mu(C_{p^m}) = m+1$ (cf. above), we get either $\mu(G) = 1$ and $|G| = 1$, or $\mu(G) = 2$ and $|G| \in \mathbb{P}$. In the latter case a subset with two elements cannot be a subgroup unless $|G| = 2$. $\square$

The following proposition extends Corollary 6.4.3 in [3].

Proposition 5.2. *Let $p \in \mathbb{P}$, $m \in \mathbb{N}$ and $G \cong C_{p^m} \oplus C_{p^m}$. Further, let $\{e_1, e_2\}$ be a basis of G.*

(1) *$G_0 = \bigcup_{i=0}^{m} p^i(e_1 + \langle e_2 \rangle)$ is a half-factorial set with $|G_0| = \mu(G)$, in particular*

$$\mu(G) = \frac{p^{m+1} - 1}{p - 1}.$$

(2) *$\emptyset \ne \Omega(G_0, g) \subset \mathcal{G}_1(G)$, with G_0 as in (1), for every $g \in \langle e_2 \rangle \setminus \{0\}$.*

Proof. Let $G_0 = \bigcup_{i=0}^{m} p^i(e_1 + \langle e_2 \rangle)$. Further, let $\pi_1 : G \to \langle e_1 \rangle$ denote the projection on the first coordinate.

1. By [3, Corollary 6.4.3] we know that $\mu(G) \le \frac{p^{m+1}-1}{p-1} = |G_0|$ and thus it suffices to show that G_0 is half-factorial. Let $A \in \mathcal{A}(G_0)$ and we show that $\mathsf{k}(A) = 1$. For each $g \in G_0$ we have $\operatorname{ord}(g) = \operatorname{ord}(\pi_1(g))$. Therefore $\mathsf{k}(A) = \mathsf{k}(\pi_1(A))$ and, since $\pi_1(G_0) = \{p^i e_1 \mid i \in \{0, \ldots, m\}\} \subset \langle e_1 \rangle$ is half-factorial and $\pi_1(A)$ is a block, we have $\mathsf{k}(A) \in \mathbb{N}$. By the main result of [6] we have $\mathsf{k}(A) \le \mathsf{K}(G) = 2 - \frac{1}{p^m}$ and thus $\mathsf{k}(A) = 1$.

2. Let $g \in \langle e_2 \rangle \setminus \{0\}$. Since $\langle G_0 \rangle = G$, it suffices to verify that $\Omega(G_0, g) \subset \mathcal{G}_1(G)$. Let $A \in \Omega(G_0, g) \cap \mathcal{A}(G)$. Then $A = gF$ with $F \in \mathcal{F}(G_0)$ zero-sumfree and clearly $F \ne 1$. Since $\pi_1(F)$ is a zero-sum sequence, we obtain as in (1) that $\mathsf{k}(F) = 1$ and thus $\mathsf{k}(A) = \frac{1}{\operatorname{ord}(g)} + 1$. By Lemma 4.3 this implies the statement. □

In Proposition 5.4 we will determine the structure of generating half-factorial sets in C_4^r. First we recall two results, which we need in the proof of this proposition.

In [4, Lemma 2.1] it is proved that if $G \cong C_{p^m}^r$ with $p \in \mathbb{P}$ and $m, r \in \mathbb{N}$, then every generating subset $G_0 \subset G$ contains a basis $G_1 \subset G_0$.

The following lemma (cf. [3, Lemma 3.6]) provides results on half-factorial sets that consist of independent elements of equal order and at most two additional elements.

Lemma 5.3. *Let $G \cong C_n^r$ with $n, r \in \mathbb{N}$, $\{e_1, \ldots, e_r\}$ a basis of G and $a = \sum_{i=1}^{r} a_i e_i$, $a' = \sum_{i=1}^{r} a_i' e_i \in G$ distinct elements with $\operatorname{ord}(a) = \operatorname{ord}(a')$ and $a_i, a_i' \in \{1, \ldots, n\}$ for each $i \in \{1, \ldots, r\}$.*

(1) *If $\{a, e_1, \ldots, e_r\}$ is a half-factorial set, then $\sum_{i=1}^{r}(n - a_i) = n - \gcd\{a_1, \ldots, a_r, n\}$.*

(2) *If $\{a, a', e_1, \ldots, e_r\}$ is a half-factorial set and $a_i = a_i'$ for some $i \in \{1, \ldots, r\}$, then $\operatorname{ord}(a_i e_i) < \operatorname{ord}(a)$.*

Proposition 5.4. *Let $G \cong C_4^r$ with $r \in \mathbb{N}$ and let $G_0 \subset G$ be a generating set. The set G_0 is half-factorial if and only if there exists a basis $G_1 = \{e_1, \ldots, e_r\}$, $s, t \in \mathbb{N}_0$ with $r = 3s + t$ and a map f from $\{1, \ldots, t\}$ to itself such that*

$$\begin{aligned} G_0 \subset \{0\} &\cup \bigcup_{j=1}^{t} \{e_j, 2e_j, 3e_j + 2e_{f(j)}\} \\ &\cup \bigcup_{i=0}^{s-1} \{e_{3i+t+1}, e_{3i+t+2}, e_{3i+t+3}, 3e_{3i+t+1} + 3e_{3i+t+2} + 3e_{3i+t+3}\}. \end{aligned}$$

Proof. First we prove the 'if'-part. Let $\{e_1, \ldots, e_r\} \subset G$ be a basis, $s, t \in \mathbb{N}_0$ with $3s + t = r$ and f a map from $\{1, \ldots, t\}$ to itself. For $i \in \{0, \ldots, s-1\}$ we set

$$H_i = \{e_{3i+t+1}, e_{3i+t+2}, e_{3i+t+3}, 3e_{3i+t+1} + 3e_{3i+t+2} + 3e_{3i+t+3}\}$$

and we set $F_0 = \bigcup_{j=1}^{t}\{e_j, 2e_j, 3e_j + 2e_{f(j)}\}$. We show that $G_0' = \{0\} \cup F_0 \cup \bigcup_{i=0}^{s-1} H_i$ is half-factorial. Since $\mathcal{A}(G_0') = \{0\} \cup \mathcal{A}(F_0) \cup \bigcup_{i=0}^{s-1} \mathcal{A}(H_i)$, it suffices to show that H_i is half-factorial for each $i \in \{0, \dots, s-1\}$ and that F_0 is half-factorial. For $i \in \{0, \dots, s-1\}$ we have that

$$\mathcal{A}(H_i) = \{h^4 \mid h \in H_i\} \cup \{(3e_{3i+t+1} + 3e_{3i+t+2} + 3e_{3i+t+3}) \prod_{l=1}^{3} e_{3i+t+l}\},$$

thus each atom has cross-number 1 and H_i is half-factorial.

Let $A \in \mathcal{A}(F_0)$ and we have to show that $\mathsf{k}(A) = 1$. If $(3e_j + 2e_{f(j)}) \nmid A$ for each $j \in \{1, \dots, t\}$ with $f(j) \neq j$, then $A \in \mathcal{A}(\{e_l, 2e_l\})$ for some $l \in \{1, \dots, t\}$ and it follows immediately that $\mathsf{k}(A) = 1$. Thus assume without restriction that $f(1) \neq 1$ and $g = (3e_1 + 2e_{f(1)})|A$. We set $n = f(1)$. Clearly, $\mathsf{v}_g(A) \leq 4$ and if $\mathsf{v}_g(A) = 4$, then $A = g^4$ and $\mathsf{k}(A) = 1$. We distinguish two cases.

Case 1: $\mathsf{v}_g(A) = 2$. If $e_1^2|A$ or $(2e_1)|A$, it follows that $A = e_1^2 g^2$ respectively $A = (2e_1)g^2$, and we are done. Thus assume $e_1^2 \nmid A$ and $(2e_1) \nmid A$. Since the sum of A is zero, this implies that there exists some $l \in \{2, \dots, t\}$ such that $f(l) = 1$ and $(3e_l + 2e_1)|A$ with odd multiplicity. Therefore we have $e_l|A$ and consequently $A = g^2(3e_l + 2e_1)e_l$ and $\mathsf{k}(A) = 1$.

Case 2: $\mathsf{v}_g(A) \in \{1, 3\}$. It follows that $e_1|A$. If $e_n^2|A$ or $(2e_n)|A$, we have $A = ge_1e_n^2$ respectively $A = ge_1(2e_n)$ and are done. Thus assume there exists some $m \in \{2, \dots, t\} \setminus \{n\}$ with $f(m) = n$ and $(3e_m + 2e_n)|A$ with odd multiplicity. This implies that $e_m|A$ and $A = g(3e_m + 2e_n)e_1e_m$.

Next we prove the 'only if'-part. Let $G_0 \subset G$ be a generating half-factorial set. Then there exists a basis $G_1 = \{e_1, \dots, e_r\} \subset G_0$. For $g \in G_0 \setminus G_1$ it follows by Lemma 5.3 that $g = 0$, $g = 2e_i$, $g = 3e_i + 2e_j$ or $g = 3e_i + 3e_j + 3e_l$ for distinct $i, j, l \in \{1, \dots, r\}$. Moreover, it follows that for each $i \in \{1, \dots, r\}$ there exists at most one element $g_i \in G_0$ such that $g_i = 3e_i + \sum_{j=1, j\neq i}^{r} b_j e_j$ with $b_j \in \{0, 1, 2, 3\}$. Thus it remains to show that if $g = 3e_i + 3e_j + 3e_l \in G_0$ with distinct $i, j, l \in \{1, \dots, r\}$, then there does not exist an element $h = 2e_i + \sum_{\nu=1, \nu\neq i}^{r} b_\nu' e_\nu \in G_0$ with $b_\nu' \in \{0, 3\}$. Assume to the contrary that such an element exists. We consider the atom $A = g^2 h \prod_{\nu=1, \nu\neq i}^{r} e_\nu^{c_\nu}$ with $c_\nu \in \{0, 1, 2, 3\}$ uniquely determined by independence. We have $c_j \equiv 2 - b_j' \pmod 4$ and $c_l \equiv 2 - b_l' \pmod 4$, hence the cross number of A is greater than 1, a contradiction. $\square$

In particular, this proposition shows that the maximal cardinality of a generating half-factorial set in C_4^r with $r \geq 2$ is $1 + 3r$. Thus for $p^m = 4$ and $r \geq 2$ the upper bound derived in [3, Proposition 3.7] for the cardinality of a generating half-factorial set in $C_{p^m}^r$ is sharp.

6. Positivity of $\psi_k(G)$ for $k \geq 2$.

In this section we show that the invariants $\psi_k(G)$ for $k \geq 2$ are all positive.

Theorem 6.1. *Let G be a finite abelian group with $|G| \geq 3$ and let $k \geq 2$ be an integer. Then*

$$\psi_k(G) > 0.$$

Proof. From the definition of $\psi_k(G)$ it follows that $\psi_{k+1}(G) \geq \psi_k(G)$ for every $k \in \mathbb{N}$. Therefore it is enough to consider the case $k = 2$. Let $G_0 \subset G$ half-factorial with $|G_0| = \mu(G)$. By Lemma 5.1 we know that there exist $g_1, g_2 \in G_0$ (possibly $g_1 = g_2$) such that $g_1 + g_2 \notin G_0$. Clearly, $g_1 + g_2 \in \langle G_0 \rangle$ and by Lemma 4.1 it follows that $\Omega(G_0, g_1 + g_2) \neq \emptyset$. We assert that

$$\Omega(G_0, g_1 + g_2) \subset \mathcal{G}_2(G).$$

By Lemma 4.3 it suffices to prove that $|\mathsf{k}(\Omega(G_0, g_1 + g_2) \cap \mathcal{A}(G))| \leq 2$. Let $A \in \Omega(G_0, g_1 + g_2) \cap \mathcal{A}(G)$. We show that

$$\mathsf{k}(A) \in \left\{ j - \frac{1}{\operatorname{ord}(g_1)} - \frac{1}{\operatorname{ord}(g_2)} + \frac{1}{\operatorname{ord}(g_1 + g_2)} \mid j \in \{1, 2\} \right\}.$$

We consider the block $B = (g_1 + g_2)^{-1} g_1 g_2 A \in \mathcal{B}(G_0)$. Clearly,

$$\mathsf{k}(B) = \mathsf{k}(A) + \frac{1}{\operatorname{ord}(g_1)} + \frac{1}{\operatorname{ord}(g_2)} - \frac{1}{\operatorname{ord}(g_1 + g_2)}$$

and by Lemma 4.2 we have $\mathsf{L}(B) \subset \{1, 2\}$. Since G_0 is half-factorial, this implies $\mathsf{k}(B) \in \{1, 2\}$. Consequently, $\emptyset \neq \Omega(G_0, g_1 + g_2) \subset \mathcal{G}_2(G)$ and $\psi_2(G) > 0$. □

7. $\psi_1(G)$

In this section we establish results on the positivity of $\psi_1(G)$. If $\mu(G)$ and some half-factorial set $G_0 \subset G$ with $|G_0| = \mu(G)$ are known, then it is usually not difficult to give an example of a sequence $S \in \mathcal{F}(G \setminus G_0) \setminus \{1\}$ such that $\emptyset \neq \Omega(G_0, S) \subset \mathcal{G}_1(G)$, and thus to obtain $\psi_1(G) > 0$. Since for most groups $\mu(G)$ is not known, we are not able to prove $\psi_1(G) > 0$ in general. But we will prove the positivity in several special cases.

Theorem 7.1. *We have $\psi_1(G) > 0$ for every finite abelian group G with $|G| \geq 3$ satisfying at least one of the following conditions:*

1. *$G \cong C_{p^m}$ for $p \in \mathbb{P}$ and $m \in \mathbb{N}$.*
2. *$G \cong C_{p^m q^n}$ for $p, q \in \mathbb{P}$ and $m, n \in \mathbb{N}$.*
3. *$G \cong C_{p^m} \oplus C_{p^m}$ for $p \in \mathbb{P}$ and $m \in \mathbb{N}$.*
4. *G is an elementary p-group with even rank.*
5. *G is an elementary p-group with odd rank and $\mu(G) = 2 + \frac{\mathsf{r}(G)-1}{2} p$.*
6. *G is an elementary p-group and the rank $\mathsf{r}(G) > r_p$ for some $r_p \in \mathbb{N}_0$.*
7. *G is an elementary p-group with exponent $p \leq 7$.*
8. *$G \cong C_4^r$ for $r \in \mathbb{N}$.*
9. *$|G| \leq 95$.*

Before proving this theorem, we prove the positivity of $\psi_1(G)$ assuming different properties for some half-factorial set with maximal cardinality

(Proposition 7.2). Many groups for which $\mu(G)$ is known have some half-factorial subset with maximal cardinality satisfying one of the conditions considered in Proposition 7.2, and this will be used in the proof of Theorem 7.1.

Proposition 7.2. *Let $G_0 \subset G$ be a half-factorial set with $|G_0| = \mu(G)$.*

(1) *If there exist $\{0\} \subsetneq G_0', G_0'' \subset G_0$ such that $G_0 = G_0' \cup G_0''$ and $\langle G_0 \rangle = \langle G_0' \rangle \oplus \langle G_0'' \rangle$, then $\psi_1(G) > 0$.*

(2) *If there exists some $g \in G_0$ such that $\langle G_0 \setminus \{g\} \rangle \neq G$, then $\psi_1(G) > 0$. In particular, if $\langle G_0 \rangle \neq G$, then $\psi_1(G) > 0$.*

Proof. 1. Suppose $\{0\} \subsetneq G_0', G_0'' \subset G_0$ with $G_0 = G_0' \cup G_0''$ and $\langle G_0 \rangle = \langle G_0' \rangle \oplus \langle G_0'' \rangle$. Let $g' \in G_0' \setminus \{0\}$ and $g'' \in G_0'' \setminus \{0\}$. By Lemma 4.2.2 we have $\emptyset \neq \Omega(G_0, g' + g'') \subset \mathcal{G}_1(G)$ and the statement follows.

2. Suppose $g \in G_0$ with $\langle G_0 \setminus \{g\} \rangle \neq G$. We consider two cases.

Case 1: $g \in \langle G_0 \setminus \{g\} \rangle$. Since $\langle G_0 \rangle = \langle G_0 \setminus \{g\} \rangle \neq G$, there exists some $h \in G \setminus \langle G_0 \rangle$. We have $-h \in G \setminus \langle G_0 \rangle$ and, since $\sigma(-hh) = 0$, we have $-hh \in \Omega(G_0, -hh)$. Moreover, $\Omega(G_0, -hh) \cap \mathcal{A}(G) = \{-hh\}$ and applying Lemma 4.3 we get $\emptyset \neq \Omega(G_0, -hh) \subset \mathcal{G}_1(G)$ and $\psi_1(G) \geq |-hh| > 0$.

Case 2: $g \notin \langle G_0 \setminus \{g\} \rangle$. Clearly, we have $-g \notin \langle G_0 \setminus \{g\} \rangle$ and $-g = g$ if and only if $\mathrm{ord}(g) = 2$. If $-g = g$, then $\langle G_0 \rangle = \langle g \rangle \oplus \langle G_0 \setminus \{g\} \rangle$ and $\psi_1(G) > 0$ by (1). Thus we assume $-g \neq g$. Then $-g \notin G_0$ and $\Omega(G_0, -g) \cap \mathcal{A}(G) = \{-gg\}$. By Lemma 4.3 we have $\emptyset \neq \Omega(G_0, -g) \subset \mathcal{G}_1(G)$.

Since $G_0 \neq \emptyset$, the 'in particular'-statement is obvious. □

There are known examples of groups that have a half-factorial subset with maximal cardinality that does not generate the group (cf. [3, Corollary 6.5]) and thus Proposition 7.2.2 can be used to obtain further examples of groups with $\psi_1(G) > 0$.

Proposition 7.2.1 implies $\psi_1(G) > 0$ for all groups $G = G' \oplus G''$ with $\mu(G) = \mu(G') + \mu(G'') - 1$, since $G_0 = G_0' \cup G_0''$ where $G_0' \subset G'$ is half-factorial with $|G_0'| = \mu(G')$ respectively $G_0'' \subset G''$ is half-factorial with $|G_0''| = \mu(G'')$ fulfills the conditions.

The following corollary provides equivalent conditions for $\psi_1(G) = 0$.

Corollary 7.3. *Let G be a finite abelian group. The following statements are equivalent:*

(1) $\psi_1(G) = 0$.

(2) *For every half-factorial $G_0 \subset G$ with $|G_0| = \mu(G)$ and for every $S \in \mathcal{F}(G \setminus G_0) \setminus \{1\}$ we have $\Omega(G_0, S) \not\subset \mathcal{G}_1(G)$.*

(3) *For every half-factorial $G_0 \subset G$ with $|G_0| = \mu(G)$ and for every $g \in G \setminus G_0$ we have $\Omega(G_0, g) \not\subset \mathcal{G}_1(G)$.*

(4) *For every half-factorial $G_0 \subset G$ with $|G_0| = \mu(G)$ and for every $g \in G \setminus G_0$ we have $|\mathsf{k}(\Omega(G_0, g) \cap \mathcal{A}(G))| > 1$.*

Proof. We can assume $\langle G_0 \rangle = G$ for every half-factorial $G_0 \subset G$ with $|G_0| = \mu(G)$, since otherwise statement (1) is false by Proposition 7.2 and (2)–(4) are obviously false as well.

Hence, $\Omega(G_0, S) \neq \emptyset$ for every $S \in \mathcal{F}(G \setminus G_0)$ by Lemma 4.1. Statements (1) and (2) are equivalent by definition of $\psi_1(G)$. (3) and (4) are equivalent by Lemma 4.3. Statement (3) is a special case of (2). Thus it remains to show that (3) implies (2). Let $G_0 \subset G$ half-factorial with $|G_0| = \mu(G)$. Further, let $S \in \mathcal{F}(G \setminus G_0) \setminus \{1\}$ and let $g|S$. By assumption we have $\Omega(G_0, g) \not\subset \mathcal{G}_1(G)$ and $\Omega(G_0, S) \neq \emptyset$, so $\Omega(G_0, S) \not\subset \mathcal{G}_1(G)$ by Lemma 4.1. □

We proceed to prove the main result of this section. We make use of the results on half-factorial sets given in Section 5 without further reference.

Proof of Theorem 7.1. 1. Let $G \cong C_{p^m}$ with $p \in \mathbb{P}$ and $m \in \mathbb{N}$. Further let $G_0 \subset G$ half-factorial with $|G_0| = \mu(G)$. Then $G_0 = \{p^i g \mid i \in \{0, \dots, m\}\}$ for some $g \in G$ with $\operatorname{ord}(g) = p^m$. Thus G_0 fulfills the conditions of Proposition 7.2.2 and we are done.

2. Let $G \cong C_{p^m q^n}$ with $p, q \in \mathbb{P}$, $p < q$ and $m, n \in \mathbb{N}$. Let $G_0 \subset G$ be half-factorial with $|G_0| = \mu(G)$. Then $\langle G_0 \rangle = G$ and there exists a generating element g of G such that

$$G_0 \subset \{dg \bigm| 1 \le d \mid p^m q^n\} = G_0'.$$

First we show that $|\mathsf{k}(\Omega(G_0', 2p^m g) \cap \mathcal{A}(G))| \le 1$. Let $A \in \Omega(G_0', 2p^m g)$ be an atom and $B = (p^m g)^2 (2p^m g)^{-1} A$. Since $B \in \mathcal{B}(G_0')$, $B \neq 1$, and G_0' satisfies condition (C_0), we have $\mathsf{k}(B) = l$ for a positive integer l. Hence $\mathsf{k}(A) = \mathsf{k}(B) - \frac{1}{q^m} = l - \frac{1}{q^n}$. On the other hand $\mathsf{k}(A) \le \mathsf{K}(G)$ and by [9, Theorem 2] we know

$$\mathsf{K}(G) = \frac{p^m - 1}{p^m} + \frac{q^n - 1}{q^n} + \frac{1}{p^m q^n}.$$

Thus it follows that $\mathsf{k}(A) = 1 - \frac{1}{q^n}$. Since $G_0 \subset G_0'$, it follows that $\Omega(G_0, S) \subset \Omega(G_0', S)$ and thus clearly $|\mathsf{k}(\Omega(G_0, 2p^m g) \cap \mathcal{A}(G))| \le 1$. This implies $\Omega(G_0, 2p^m g) \subset \mathcal{G}_1(G)$ by Lemma 4.3. Since $\langle G_0 \rangle = G$, we have $\Omega(G_0, 2p^m g) \neq \emptyset$ and the result follows.

3. Let $G \cong C_{p^m} \oplus C_{p^m}$ with $p \in \mathbb{P}$ and $m \in \mathbb{N}$. By Proposition 5.2 it follows that there exists a half-factorial subset $G_0 \subset G$ with maximal cardinality and an element $g \in G \setminus G_0$ such that $\emptyset \neq \Omega(G_0, g) \subset \mathcal{G}_1(G)$. Thus the statement follows immediately.

4. Let G be an elementary p-group with even rank. If $\mathsf{r}(G) = 2$, then the result follows by (3). Suppose $\mathsf{r}(G) \ge 4$. Then there exist subgroups G', G'' such that $G = G' \oplus G''$ and $\mu(G) = \mu(G') + \mu(G'') - 1$. Thus the statement follows by Proposition 7.2.1.

5. Let G be an elementary p-group with odd rank and $\mu(G) = 2 + \frac{\mathsf{r}(G)-1}{2} p$. If $\mathsf{r}(G) = 1$, then the statement follows by (1). Suppose $\mathsf{r}(G) \ge 3$. Then $G = G' \oplus G''$ with $\mathsf{r}(G') = 1$. By assumption $\mu(G) = \mu(G') + \mu(G'') - 1$ and the statement follows by Proposition 7.2.1.

6. For $s \in \mathbb{N}_0$ let $\delta(s) = \mu(C_p^{2s+1}) - 2 - sp \in \mathbb{Z}$. We know $\delta(s) \in \{0, \dots, \frac{p-1}{2}\}$ and $\delta(\cdot)$ is a non-decreasing function. Let $s_p \in \mathbb{N}$ such that

$\delta(s_p) = \max\{\delta(s) \mid s \in \mathbb{N}_0\}$, then $\delta(s) = \delta(s_p)$ for every $s \geq s_p$. We set $r_p = 2s_p + 1$. Let $\mathsf{r}(G) = r > r_p$. If r is even, the assertion is already proved in (4). Suppose r is odd. Let $G = G' \oplus G''$ with $\mathsf{r}(G') = r - r_p$ and $\mathsf{r}(G'') = r_p$. Then $\mu(G) = \mu(G') + \mu(G'') - 1$ and thus by Proposition 7.2.1 the statement follows.

7. Let G be an elementary p-group with $p \leq 7$. If $\mathsf{r}(G)$ is even, then the statement follows by (4). If $\mathsf{r}(G)$ is odd, then $\mu(G) = 2 + \frac{r-1}{2}p$, which implies the assertion by (5).

8. Let $G \cong C_4^r$ with $r \in \mathbb{N}$. For $r = 1$ the statement follows by (1) and for $r = 2$ by (3). Suppose $r \geq 3$. If $\mu(G) > 1 + 3r$, it follows by Proposition 5.4 that a half-factorial set with maximal cardinality does not generate G, and the statement follows by 7.2.2.

Assume $\mu(G) = 1 + 3r$. If $r \geq 4$, there exist $s, t \geq 2$ and $G' \cong C_4^s$, $G'' \cong C_4^t$ two subgroups of G such that $G = G' \oplus G''$. It follows that

$$1 + 3r = \mu(G) \geq \mu(G') + \mu(G'') - 1 \geq 1 + 3(s + t) = 1 + 3r.$$

Thus the statement follows by 7.2.1. It remains to consider $r = 3$. Let $r = 3$ and $\{e_1, e_2, e_3\} \subset G$ a basis. Further let $G_0 = \{0, e_1, e_2, e_3, 2e_1, 2e_2, 2e_3, 3e_1 + 2e_2, 3e_2 + 2e_3, 3e_3 + 2e_1\}$. By Proposition 5.4 this set is half-factorial and by our assumption on $\mu(G)$ it has maximal cardinality. Let $g = 2e_1 + 2e_2 + 2e_3$. We assert that $\emptyset \neq \Omega(G_0, g) \subset \mathcal{G}_1(G)$, which implies the statement immediately. Clearly, the set is non-empty and by Lemma 4.3 it suffices to show that each atom in it has the same cross number. Let $A \in \Omega(G_0, g) \cap \mathcal{A}(G)$. We assert that $\mathsf{k}(A) = 2$. We observe that if $e_i^2 | A$, then $A' = (2e_i)e_i^{-2}A$ has the same cross number as A and is a zero-sum sequence. Since every factorization of A' yields a factorization of A, it follows that A' is an atom. Similarly, if $(3e_i + 2e_j)^2 | A$ or $e_i(3e_i + 2e_j) | A$, then $(2e_i)(3e_i + 2e_j)^{-2}A$ respectively $(2e_j)e_i^{-1}(3e_i + 2e_j)^{-1}A$ is an atom with the same cross number.

Note that $\mathsf{v}_{e_i}(A) \equiv \mathsf{v}_{3e_i+2e_j}(A) \pmod 2$ for each $i \in \{1, 2, 3\}$ and j such that $3e_i + 2e_j \in G_0$. Thus by repeated application of these replacements, we obtain an atom $A^* \in \Omega(G_0, g)$ such that $\mathsf{k}(A) = \mathsf{k}(A^*)$ and none of $\{e_1, e_2, e_3, 3e_1 + 2e_2, 3e_2 + 2e_3, 3e_3 + 2e_1\}$ divides A^*. Thus $A^* = g(2e_1)(2e_2)(2e_3)$ and $\mathsf{k}(A) = \mathsf{k}(A^*) = 2$.

9. The proof has been conducted using computational methods. First we determine all half-factorial subsets G_0 with maximal cardinality. This is done by examining the atoms in $\mathcal{F}(G_0')$ where $G_0' \subset G$ is a subset satisfying the condition (C_0). Then we pick one such subset G_0, find all the zero-sumfree sequences in $\mathcal{F}(G_0)$, and check if there exists a $g \in G \setminus G_0$ such that all zero-sumfree S with $\sigma(S) = -g$ have the same cross number. If we can find such a g for at least one G_0, the assertion $\psi_1(G) > 0$ is proved. Details can be found at `http://www.amu.edu.pl/~maciejr`. □

References

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

[2] S. Chapman and A. Geroldinger. Krull domains and monoids, their sets of lengths and associated combinatorial problems. In [1], pages 73 – 112.

[3] W. Gao and A. Geroldinger. Half-factorial domains and half-factorial subsets in abelian groups. *Houston J. Math.*, 24: 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. Ein quantitatives Resultat über Faktorisierungen verschiedener Länge in algebraischen Zahlkörpern. *Math. Z.*, 205: 159–162, 1990.

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

[7] A. Geroldinger, F. Halter-Koch, and J. Kaczorowski. Non-unique factorizations in orders of global fields. *J. Reine Angew. Math.*, 459: 89–118, 1995.

[8] A. Geroldinger and J. Kaczorowski. Analytic and arithmetic theory of semigroups with divisor theory. *Sém. Théor. Nombres Bordeaux (2)*, 4: 199 – 238, 1992.

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

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

[11] F. Halter-Koch. Finitely generated monoids, finitely primary monoids and factorization properties of integral domains. In [1], pages 31 – 72.

[12] F. Halter-Koch and W. Müller. Quantitative aspects of nonunique factorization: a general theory with applications to algebraic function fields. *J. Reine Angew. Math.*, 421:159–188, 1991.

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

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

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

[16] W. Narkiewicz. On algebraic number fields with non-unique factorization. II. *Colloq. Math.*, 15: 49–58, 1966.

[17] W. Narkiewicz. A note on numbers with good factorization properties. *Colloq. Math.*, 27: 275–276, 332, 1973.

[18] W. Narkiewicz. Finite abelian groups and factorization problems. *Colloq. Math.*, 17: 319 – 330, 1979.

[19] W. Narkiewicz. Numbers with all factorizations of the same length in a quadratic number field. *Colloq. Math.*, 45: 71–74, 1981.

[20] M. Radziejewski. On the distribution of algebraic numbers with prescribed factorization properties. *Acta Arith.*, to appear.

[21] M. Radziejewski. Independence of Hecke zeta functions of finite order over normal fields. (*submitted*)

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

[23] L. Skula. On c-semigroups. *Acta Arith.*, 31: 247 – 257, 1976.

[24] J. Śliwa. Factorizations of distinct length in algebraic number fields. *Acta Arith.*, 31: 399 –417, 1976.

[25] J. Śliwa. Remarks on factorizations in algebraic number fields. *Colloq. Math.*, 46: 123 – 130, 1982.

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

Added note

Recently, A. Plagne and the second author proved that $\mu(C_p^r) = 2 + \frac{r-1}{2}p$ for $p \in \mathbb{P}$ and r odd. Thus, every elementary p-group with odd rank fulfils condition (5) of Theorem 7.1, and consequently $\psi_1(G) > 0$ if G is an elementary p-group.

Faculty of Mathematics and Computer Science, Adam Mickiewicz University, ul. Umultowska 87, 61-614 Poznań, Poland

E-mail address: `maciejr@amu.edu.pl`

Institute for Mathematics and Scientific Computing, Karl-Franzens-Universität, Heinrichstrasse 36, 8010 Graz, Austria

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