ON THE ASYMPTOTIC BEHAVIOR OF SOME COUNTING FUNCTIONS, II

WOLFGANG A. SCHMID

Abstract. The investigation of the counting function of the set of integral elements, in an algebraic number field, with factorizations of at most k different lengths gives rise to a combinatorial constant depending only on the class group of the number field and the integer k. In this paper the value of these constants, in case the class group in an elementary p-group, is estimated and under additional conditions determined. In particular, it is proved that for elementary 2-groups these constants are equivalent to constants that are investigated in extremal graph theory.

1. Introduction

In this paper we investigate a class of invariants of finite abelian groups, arising from investigations of the asymptotic behavior of counting functions.

Let K be a number field and $\mathcal{O}_K$ its ring of integers. For $a \in \mathcal{O}_K$ let $\mathsf{L}(a)$ denote its set of lengths, i.e., the set of $n \in \mathbb{N}_0$ such that $a = u_1 \cdot \ldots \cdot u_n$ with atoms (irreducibles) $u_1, \ldots, u_n \in \mathcal{O}_K$. Let k be a positive integer. The counting function

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

was initially considered in [13] and in the sequel by various authors (cf. [15, Chapter 9] and [17] for a recent result and further references). Note that this counting function is only interesting if G, the ideal class group of K, has at least three elements, since otherwise $\mathcal{O}_K$ is half-factorial, as proved in [1].

In [8] it was shown, applying and generalizing results obtained in [12, 21, 22], that

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

where C is a positive constant, $\mu(G)$ denotes the maximal cardinality of a half-factorial subset of G and $\psi_k(G)$ depends on the structure of half-factorial subsets with maximal cardinality of G (cf. Section 2 in particular Definition 2.1). In particular, $\mu(G)$ and $\psi_k(G)$ depend just on G and k and not the number field itself.

2000 *Mathematics Subject Classification.* 11N64, 11R27, 20K01, 05C35.

Key words and phrases. factorizations, zero-sum sequence, block monoid, half-factorial, edge disjoint cycles.

Supported by the Austrian Science Fund FWF (Project P16770-N12).

In this paper we will investigate $\psi_k(G)$. All our considerations will be carried out in the block monoid over G, a finite abelian group with $|G| \geq 3$, without making further use of the number field itself. The notion of block monoids was introduced in [14] to study combinatorial problems arising from the investigations of $\mathbf{G}_k(x)$ and other counting functions and is meanwhile a main tool for investigations of non-unique factorization in Krull monoids (cf. the references given in Section 2).

Not too much is known on the value of $\psi_k(G)$, in terms of invariants of G such as the rank or the exponent. In [21, 22] the value of $\psi_k(G)$ is obtained for $|G| \in \{3, 4\}$ and in [18] it was proved, motivated by investigations on the error term of $\mathbf{G}_k(x)$ in [17], that $\psi_k(G) > 0$ for $k \geq 2$ and $\psi_1(G) > 0$ for various types of groups. Moreover, in [22, P 1247] the problem to investigate whether $(\psi_k(G))_{k=1}^{\infty}$ is an arithmetic progression is posed. Note that $B(k, G)$, as defined in [22], is not identical with $\psi_k(G)$; however, they are closely related and the present statement is equivalent to [22, P 1247] (cf. the considerations following Theorem 5.7 and [18, Introduction]).

In this paper we obtain good bounds for $\psi_k(G)$ in case G is an elementary p-group, and under additional conditions even the precise value. More specifically, in Theorem 4.5 we determine $\psi_1(G)$ for elementary p-groups with $p \geq 3$ and even rank and we determine $\psi_k(G)$ for $k > 1$ under the additional condition that $p \geq \frac{\mathsf{r}(G)}{2}$. In particular, this result shows that in this case $(\psi_k(G))_{k=1}^{\infty}$ is an arithmetic progression (cf. Corollary 4.6). The case of odd rank, which we treat in Subsection 4.2, seems to be more complicated and we just obtain lower bounds. For elementary 2-groups we show that the problem of determining $\psi_k(G)$ is equivalent to a problem concerning edge disjoint cycles in graphs and we use this equivalence and results on the graph theoretic problem to prove $\psi_1(G) = \mathsf{r}(G) - 1$ and to determine $\psi_k(G)$ up to a constant that is independent of G (cf. Theorem 5.7). In particular, we show that these results imply that $(\psi_k(G))_{k=1}^{\infty}$ is not always an arithmetic progression. However, in the cases we consider, it seems it is at least eventually an arithmetic progression.

In our investigations we apply results on the structure of half-factorial sets with maximal cardinality in G; such results are known for elementary p-groups, but so far only for very few other groups (cf. [7] for various results on half-factorial sets).

2. Preliminaries

Let $\mathbb{Z}$ denote the integers, $\mathbb{N}$ the positive integers, $\mathbb{N}_0$ the non-negative integers and $\mathbb{P}$ the prime numbers. For $m, n \in \mathbb{Z}$ let $[m, n] = \{z \in \mathbb{Z} \mid m \leq z \leq n\}$ and let C_n denote a cyclic group with order n.

We summarize some notions and results concerning block monoids, for a detailed description and proofs we refer to the survey articles [3, 10]. Let G be a finite abelian group and $G_0 \subset G$ some subset. Then $\mathsf{r}(G)$ denotes the rank of G, $\langle G_0 \rangle$ denotes the group generated by G_0 and $\mathcal{F}(G_0)$ denotes the, multiplicatively written, free abelian monoid with basis G_0. An element

$S = \prod_{i=1}^{l} g_i = \prod_{g\in G} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G_0)$ with $l \in \mathbb{N}_0$ and $g_i \in G_0$ respectively $\mathsf{v}_g(S) \in \mathbb{N}_0$ is called a sequence in G (the identity element of $\mathcal{F}(G_0)$ is denoted by 1).

If $T|S$ (in $\mathcal{F}(G_0)$), then T is called a subsequence of S and $T^{-1}S$ denotes its co-divisor. Further $|S| = l$ is called the length, $\mathsf{k}(S) = \sum_{i=1}^{l} \frac{1}{\mathrm{ord}(g_i)}$ the cross number and $\sigma(S) = \sum_{i=1}^{l} g_i$ the sum of S.

A sequences S is called zero-sum sequence (a block), if $\sigma(S) = 0$ and it is called zero-sumfree, if $\sigma(T) \neq 0$ for all subsequences $1 \neq T|S$.

The set $\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ of zero-sum sequences in G_0 is called the block monoid over G_0. It is atomic (in fact 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 every proper subsequence is zero-sumfree. Davenport's constant, $\mathsf{D}(G)$, is defined as the maximal length of an atom in G. We only use the result that $\mathsf{D}(C_p) = p$ and $\mathsf{D}(C_p^2) = 2p-1$ where C_p denotes a cyclic group with $p \in \mathbb{P}$ elements (cf. [6, 16]).

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 n is called the length of the factorization and $\mathsf{L}(B) = \{n \mid n \text{ has a factorization of lengths n}\}$ is called the set of lengths of B. For $k \in \mathbb{N}_0$ we set $\mathcal{G}_k(G) = \{B \in \mathcal{B}(G) \bigm| |\mathsf{L}(B)| \le k\}$. Note that $\mathsf{L}(1) = \{0\}$ and $\mathcal{G}_0(G) = \emptyset$.

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 $B \in \mathcal{B}(G_0)$, and $\mu(G) = \max\{|G_0| \bigm| G_0 \subset G \text{ half-factorial}\}$ denotes the maximal cardinality of a half-factorial subset of G. A set G_0 is half-factorial if and only if $\mathsf{k}(A) = 1$ for each $A \in \mathcal{A}(G)$ (cf. [20, 21, 23]).

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

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

Next we recall the central definition of this paper (cf. [8]).

Definition 2.1. Let $k \in \mathbb{N}$ and G be a finite abelian group with $|G| \geq 3$. Then

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

Throughout, let G denote a finite ablian group with $|G| \geq 3$.

3. Some Basic Results

In this section we quote and establish some basic results on $\psi_k(G)$ and $\Omega(G_0, S)$. Parts of the results were initially obtained in [9, 21], however implicitly or in different notation. Proofs for all mentioned results can be found in [18, Section 4].

Let $G_0 \subset G$ be a half-factorial subset with maximal cardinality. It follows immediately from the definition that $\Omega(G_0, S) \cdot \Omega(G_0, S') \subset \Omega(G_0, SS')$

for $S, S' \in \mathcal{F}(G \setminus G_0)$. Moreover, $|\mathsf{L}(BB')| \ge |\mathsf{L}(B)| + |\mathsf{L}(B')| - 1$ for $B, B' \in \mathcal{B}(G)$ and therefore $\Omega(G_0, S) \not\subset \mathcal{G}_k(G)$ and $\Omega(G_0, S') \not\subset \mathcal{G}_l(G)$ implies $\Omega(G_0, SS') \not\subset \mathcal{G}_{k+l}(G)$ for $k, l \in \mathbb{N}_0$. This allows us to carry out investigations for special types of sequences and to transfer the obtained results to the general case. Of particular interest are sequences of length 1, i.e., elements of the group. It is easy to see that $\Omega(G_0, g) \cap \mathcal{A}(G) \ne \emptyset$ for every $g \in \langle G_0 \rangle \setminus G_0$. Moreover, if $k = |\mathsf{k}(\Omega(G_0, g) \cap \mathcal{A}(G))|$, then $\Omega(G_0, g) \subset \mathcal{G}_k(G)$ and there exists some $B \in \Omega(G_0, g)$ with $|\mathsf{L}(B)| = k$ (cf. [18, Lemma 4.1]).

Lemma 3.1. *Let $k \in \mathbb{N}$ and $G = G' \oplus G''$ with $|G'|, |G''| \ge 2$. Let $G_0' \subset G'$, $G_0'' \subset G''$, $S' \in \mathcal{F}(G' \setminus G_0')$ and $S'' \in \mathcal{F}(G'' \setminus G_0'')$. Further let $G_0 = G_0' \cup G_0''$ and $S = S'S'' \in \mathcal{F}(G \setminus G_0)$.*

1. *$\Omega(G_0', S') \cdot \Omega(G_0'', S'') = \Omega(G_0, S)$.*
2. *If $\Omega(G_0', S') \subset \mathcal{G}_k(G')$ and $\Omega(G_0'', S'') \subset \mathcal{G}_l(G'')$ with $k, l \in \mathbb{N}_0$, then $\Omega(G_0, S) \subset \mathcal{G}_{kl}(G)$.*
3. *Suppose G_0' and G_0'' are half-factorial, $g' \in G_0' \setminus \{0\}$, $g'' \in G_0'' \setminus \{0\}$ and $g = g' + g''$. If $\emptyset \ne \Omega(G_0, S) \subset \mathcal{G}_k(G)$, then $\emptyset \ne \Omega(G_0, gS) \subset \mathcal{G}_k(G)$.*
4. *Suppose $\mu(G) = \mu(G') + \mu(G'') - 1$. Then*
   (a) *$\psi_k(G) \ge 1$.*
   (b) *$\psi_k(G) \ge \psi_k(G') + 1$, if $|G'| \ge 3$.*
   (c) *$\psi_k(G) \ge \psi_k(G') + \psi_1(G'') + 1$, if $|G'|, |G''| \ge 3$.*

Proof. 1. and 2. Clearly, $\Omega(G_0', S') \cdot \Omega(G_0'', S'') \subset \Omega(G_0, S)$. Let $B \in \Omega(G_0, S)$. By definition of G_0 and S we have $\mathsf{v}_g(B) = 0$ for every $g \in G \setminus (G' \cup G'')$. Thus $B = B'B''$ with $B' \in \mathcal{F}(G')$ and $B'' \in \mathcal{F}(G'')$. Since $G = G' \oplus G''$, it follows that B' and B'' are zero-sum sequences. Moreover, every factorization of B into atoms is the product of a factorization of B' and a factorization of B''. Thus $\mathsf{L}(B) = \mathsf{L}(B') + \mathsf{L}(B'')$ and $|\mathsf{L}(B)| \le |\mathsf{L}(B')| \cdot |\mathsf{L}(B'')|$.

3. Note that $g \notin G' \cup G''$. Let $C' \in \Omega(G_0, S)$. Then

$$C = gg'^{(\mathrm{ord}(g')-1)} g''^{(\mathrm{ord}(g'')-1)} C' \in \Omega(G_0, gS).$$

Thus it remains to prove the statement concerning the lengths of factorizations.

Let $B \in \Omega(G_0, gS)$ and let $B' = g^{-1}g'g''B \in \Omega(G_0, S)$. We assert that $1 + \mathsf{L}(B) \subset \mathsf{L}(B')$. Since $|\mathsf{L}(B')| \le k$, this proves the statement.

Let $B = \prod_{i=1}^n U_i$ a factorization into atoms. Without restriction let $g | U_1$. Since $S' \in \mathcal{F}(G')$ and $G_0' \subset G'$ respectively $S'' \in \mathcal{F}(G'')$ and $G_0'' \subset G''$, we have $U_1 = (g' + g'')F'F''$ with zero-sumfree sequences $F' \in \mathcal{F}(G')$ and $F'' \in \mathcal{F}(G'')$. Thus $\sigma(F') = -g'$, $\sigma(F'') = -g''$ and $(g' + g'')^{-1} g'g''U_1 = (g'F')(g''F'')$ (cf. [18, Lemma 4.2]). Since $g'F'$ and $g''F''$ are atoms, we get that $(g'F')(g''F'') \prod_{i=2}^n U_i$ is a factorization of B' into atoms and $1 + n \in \mathsf{L}(B')$.

4. Suppose G_0' and G_0'' are half-factorial with $|G_0'| = \mu(G')$ and $|G_0''| = \mu(G'')$. We have $|G_0| = \mu(G)$. Since $\mu(G'), \mu(G'') \ge 2$ there exist $g' \in$

$G_0' \setminus \{0\}$ and $g'' \in G_0'' \setminus \{0\}$. We set $g = g' + g''$. We note that $\emptyset \neq \Omega(G_0, 1) \subset \mathcal{G}_1(G)$ and apply (3) with $S = 1$. This implies $\emptyset \neq \Omega(G_0, g) \subset \mathcal{G}_1(G)$, which proves (a).

If $|G'| \geq 3$, then suppose there exists a sequence $S' \in \mathcal{F}(G' \setminus G_0')$ with $\emptyset \neq \Omega(G_0', S') \subset \mathcal{G}_k(G')$ and $|S'| = \psi_k(G')$. Since $\emptyset \neq \Omega(G_0'', 1) \subset \mathcal{G}_1(G'')$ we apply (1) with $S'' = 1$ and obtain $\emptyset \neq \Omega(G_0, S') \subset \mathcal{G}_k(G)$. Applying (3) we obtain $\emptyset \neq \Omega(G_0, gS') \subset \mathcal{G}_k(G)$. Thus $\psi_k(G) \geq |gS'| = 1 + \psi_k(G')$, which proves (b).

If in addition $|G''| \geq 3$, then suppose there exists a sequence $S'' \in \mathcal{F}(G'' \setminus G_0'')$ with $\emptyset \neq \Omega(G_0'', S'') \subset \mathcal{G}_1(G'')$ and $|S''| = \psi_1(G'')$. Again by (1) and (3) we obtain $\emptyset \neq \Omega(G_0, gS'S'') \subset \mathcal{G}_m(G)$, which proves (c). □

In [9, Proposition 5] it was proved that if $G = G' \oplus G''$, then $\mu(G) \geq \mu(G') + \mu(G'') - 1$. Moreover, there are known examples were equality holds as well as examples were equality does not hold (cf. the results quoted in Section 4). Thus $\mu(G) = \mu(G') + \mu(G'') - 1$ is a non-trivial condition. In particular, the statement of Lemma 3.1.4 is not true without this condition as Theorem 4.5 and Proposition 4.9 will show.

Lemma 3.2. *Let $k, l \in \mathbb{N}$. If each half-factorial set $G_0 \subset G$ with $|G_0| = \mu(G)$ generates G, then*

$$\psi_{k+l}(G) \leq \psi_k(G) + \psi_l(G) + 1.$$

Proof. Assume to the contrary, $\psi_{k+l}(G) \geq \psi_k(G) + \psi_l(G) + 2$. Let $G_0 \subset G$ half-factorial with $|G_0| = \mu(G)$ and $S \in \mathcal{F}(G \setminus G_0)$ such that $\emptyset \neq \Omega(G_0, S) \subset \mathcal{G}_{k+l}(G)$ and $|S| = \psi_{k+l}(G)$. By assumption there exist $S', S'' \in \mathcal{F}(G \setminus G_0)$ such that $S = S'S''$, $|S'| > \psi_k(G)$ and $|S''| > \psi_l(G)$. Since $\langle G_0 \rangle = G$, there exist blocks $B' \in \Omega(G_0, S')$ and $B'' \in \Omega(G_0, S'')$ such that $|\mathsf{L}(B')| > k$ and $|\mathsf{L}(B'')| > l$. Thus $B = B'B'' \in \Omega(G_0, S)$ and $|\mathsf{L}(B)| \geq |\mathsf{L}(B')| + |\mathsf{L}(B'')| - 1 \geq k + 1 + l + 1 - 1 > k + l$, a contradiction. □

In this paper we only deal with groups G where every half-factorial subset of maximal cardinality generates G, namely with elementary p-groups and cyclic groups with prime power order (in [7, Proposition 3.5] it is proved that this holds true for elementary and cyclic groups). Thus for the groups we consider the condition in Lemma 3.2 is always fulfilled and moreover we always have $\Omega(G_0, S) \neq \emptyset$, if $G_0 \subset G$ is half-factorial with maximal cardinality and $S \in \mathcal{F}(G \setminus G_0)$.

4. $\psi_k(G)$ for Elementary p-groups

4.1. **Groups with Even Rank.** For elementary p-groups with even rank the value of $\mu(G)$ and the structure of half-factorial sets with maximal cardinality are known. We use this to investigate $\psi_k(G)$ for these groups.

Proposition 4.1 ([9, 19])**.** *Let G be an elementary p-group with even rank $\mathsf{r}(G) = 2r$. Then $\mu(G) = 1 + rp$ and $G_0 \subset G$ is half-factorial with $|G_0| =$*

$\mu(G)$ if and only if there exists a basis $\{e_1, e_1', \ldots, e_r, e_r'\}$ of G such that

$$G_0 = \{0\} \cup \bigcup_{i=1}^{r} \{je_i + e_i' \mid j \in [0, p-1]\}.$$

Proof. The result on $\mu(G)$ and the 'if'-part were proved in [9, Theorem 8], the 'only if'-part in [19, Theorem 3.1]. Note that in both papers the sets are described in a different basis, namely $\{e_1 + e_1', e_1', \ldots, e_r + e_r', e_r'\}$. □

For our purpose it is particularly interesting that for a given group all half-factorial subsets of maximal cardinality are equal up to automorphisms of the group. Thus it suffices to investigate $\Omega(G_0, \cdot)$ for one fixed half-factorial set $G_0 \subset G$ with maximal cardinality.

Note that for $p = 2$ the description of the half-factorial sets is not natural, since for $p = 2$ the set $G_0 \setminus \{0\}$ is independent. In Section 5 we will separately investigate elementary 2-groups (not necessarily with even rank). Thus whenever it is convenient we will assume $p \neq 2$.

Throughout the whole subsection we will use the following notations. Let G be an elementary p-group with rank $\mathsf{r}(G) = 2r$ and $\{e_1, e_1', \ldots, e_r, e_r'\} \subset G$ a basis of G. Further let

$$G_0 = \{0\} \cup \bigcup_{i=1}^{r} \{je_i + e_i' \mid j \in [0, p-1]\},$$

a half-factorial set with $|G_0| = \mu(G)$. For $i \in [1, r]$ let π_i denote the projection on $\langle e_i \rangle$, π_i' the projection on $\langle e_i' \rangle$ and $G_0^i = (\pi_i + \pi_i')(G_0) = \{0\} \cup \{je_i + e_i' \mid j \in [0, p-1]\}$.

We start with a technical lemma on cross numbers of certain atoms. It is of interest, since the number of different values of the cross numbers of the atoms in $\Omega(G_0, g)$ determines the maximal cardinality of the sets of lengths of the blocks in $\Omega(G_0, g)$ (cf. Section 3 and [18, Lemma 4.3]).

Lemma 4.2. *Let $g = \sum_{i=1}^{r} a_i e_i + b_i e_i' \notin G_0$ with $a_i, b_i \in [0, p-1]$ and $A \in \Omega(G_0, g) \cap \mathcal{A}(G)$. Then*

$$\mathsf{k}(A) = \frac{1}{p} + |I_1| \frac{p-1}{p} + |I_2| + |I_3| - \frac{c_g}{p} + m_A$$

where $I_1 = \{i \in [1, r] \mid b_i = 1\}$, $I_2 = \{i \in [1, r] \mid b_i = 0 \text{ and } a_i \neq 0\}$, $I_3 = \{i \in [1, r] \mid b_i \notin [0, 1]\}$, $c_g = \sum_{i \in I_3} b_i$ and $m_A \in [0, |I_3|]$. Moreover,

$$|\mathsf{k}(\Omega(G_0, g) \cap \mathcal{A}(G))| = 1 + |\{i \in [1, r] \mid b_i \notin [0, 1]\}|.$$

Proof. Let $B \in \Omega(G_0, g)$. Then $B = g0^v \prod_{i=1}^{r} S_i$ with uniquely determined $v \in \mathbb{N}_0$ and $S_i \in \mathcal{F}(G_0^i \setminus \{0\})$ for each $i \in [1, r]$. We note that $B \in \mathcal{A}(G)$ if and only if $v = 0$ and $(a_i e_i + b_i e_i') S_i$ is an atom for each $i \in [1, r]$. Thus it suffices to investigate each component separately.

For each $i \in [1, r]$ let $g_i = (\pi_i + \pi_i')(g) = a_i e_i + b_i e_i'$ and $F_i \in \mathcal{F}(G_0^i)$ such that $A = g \prod_{i=1}^{r} F_i$. Then $g_i F_i$ is an atom for each $i \in [1, r]$. If $b_i = 1$ or $a_i = b_i = 0$, then $\{g_i\} \cup G_0^i$ is half-factorial. Consequently,

$\mathsf{k}(g_iF_i) = 1$ and $\mathsf{k}(F_i) = \frac{p-1}{p}$ if $b_i = 1$ respectively $\mathsf{k}(F_i) = 0$ if $a_i = b_i = 0$. If $b_i = 0$ and $a_i \neq 0$, then $F_i \neq 1$ and $|F_i|e'_i = 0$. Since F_i is zero-sumfree and $\mathsf{D}(C_p^2) = 2p-1$, it follows that $|F_i| < 2p-1$ and therefore $|F_i| = p$ respectively $\mathsf{k}(F_i) = 1$.

Suppose $b_i \notin [0,1]$. Since $(b_i + |F_i|)e'_i = 0$ and $|F_i| \in [1, 2p-2]$, we get that $|F_i| \in \{p - b_1, 2p - b_1\}$.

Let I_1, I_2, I_3 and c_g as in the formulation of the lemma and $I_4 = \{i \in I_3 \mid \mathsf{k}(F_i) = 2p - b_i\}$.

Then

$$\mathsf{k}(A) = \frac{1}{\operatorname{ord}(g)} + \sum_{i=1}^{r} \mathsf{k}(F_i) = \frac{1}{p} + |I_1|\frac{p-1}{p} + |I_2| + |I_3| - \frac{c_g}{p} + |I_4|$$

and clearly $|I_4| \in [0, |I_3|]$, which proves the first part of the lemma and implies immediately that $|\mathsf{k}(\Omega(G_0,g) \cap \mathcal{A}(G))| \leq 1 + |\{i \in [1,r] \mid b_i \notin [0,1]\}|$.

To prove the remaining part, it suffices to verify that for each $i \in I_3$ there are sequences $F'_i, F''_i \in \mathcal{F}(G_0^i)$ such that $g_iF'_i, g_iF''_i \in \mathcal{A}(G)$, $\mathsf{k}(F'_i) = p - b_i$ and $\mathsf{k}(F''_i) = 2p - b_i$. The sequences $F'_i = (-a_ie_i + e'_i)e_i'^{p-b_i-1}$ and

$$F''_i = \begin{cases} (e_i + e'_i)^{p-b_i+1}((-b_i+1)e_i + e'_i)^{p-1} & \text{if } a_i = 0 \\ e_i'^{p-b_i+1}(a_ie_i + e'_i)^{p-1} & \text{if } a_i \neq 0 \end{cases}$$

have these properties. $\square$

In the following lemma we derive a lower bound for $\psi_k(G)$. In Theorem 4.5 we will see that equality holds in several cases.

Lemma 4.3. *Let $k \in \mathbb{N}$. Then $\psi_k(G) \geq (k-1+r)p - 1$.*

Proof. We proceed by induction on r. Let $r = 1$. We set $S = e_1^{kp-1}$ and show that $\Omega(G_0, S) \subset \mathcal{G}_k(G)$. We start with an investigation of the cross numbers of the atoms in $\{e_1\} \cup G_0$. For ease of notation we omit the subscript 1.

Let $A \in \mathcal{A}(\{e\} \cup G_0)$. If $\mathsf{v}_e(A) \in \{0, p\}$, then $\mathsf{k}(A) = 1$. Suppose $A = e^vF$ with $v \in [1, p-1]$ and $F \in \mathcal{F}(G_0)$. Clearly, $F \neq 1$ and F is zero-sumfree, thus $1 \leq |F| \leq 2p-2$ as in Lemma 4.2. Since $|F|e' = 0$, we obtain $|F| = p$ and $\mathsf{k}(A) = 1 + \frac{\mathsf{v}_e(A)}{p}$.

Let $B \in \Omega(G_0, S)$ and $B = (e^p)^m \prod_{i=1}^{l} U_i$ a factorization into atoms where $\mathsf{v}_e(U_i) < p$ for each $i \in [1, l]$. Clearly, $m \in [0, k-1]$. It follows that

$$\mathsf{k}(B) = m + \sum_{i=1}^{l} \frac{p + \mathsf{v}_e(U_i)}{p} = m + l + \frac{\mathsf{v}_e(B) - pm}{p} = l + \frac{kp-1}{p}.$$

Thus $l = \mathsf{k}(B) - k + \frac{1}{p}$ is determined by B, $\mathsf{L}(B) \subset l + [0, k-1]$ and $|\mathsf{L}(B)| \leq k$.

Let $r \geq 2$ and $G = G' \oplus G''$ with $\mathsf{r}(G') = 2(r-1)$ and $\mathsf{r}(G'') = 2$. By induction hypothesis we have $\psi_k(G') \geq (k-1+r-1)p-1$ and $\psi_1(G'') \geq p-1$. By Lemma 3.1.4 we get $\psi_k(G) \geq (k-1+r-1)p - 1 + p - 1 + 1 = (k-1+r)p-1$. $\square$

Next we prove a proposition that will be needed to establish an upper bound for $\psi_k(G)$. By $\sum_{i=1}^r G_0^i$ we denote, as usual, the set of elements $\sum_{i=1}^r g_i$ with $g_i \in G_0^i$ for each $i \in [1,r]$.

Proposition 4.4. *Let $p \ge 3$. Then $\Omega(G_0, S) \not\subset \mathcal{G}_1(G)$ for each of the following choices of $S \in \mathcal{F}(G \setminus G_0)$:*

(1) *Let $S = g$ with $g \in G \setminus (\langle e_1, \dots, e_r \rangle + \sum_{i=1}^r G_0^i)$.*
(2) *Let $S \in \mathcal{F}((\langle e_1, \dots, e_r\rangle + \sum_{i=1}^r G_0^i) \setminus \sum_{i=1}^r G_0^i)$ such that $(\pi_m + \pi'_m)(S) \in \mathcal{A}(\langle e_m \rangle \setminus \{0\})$ for some $m \in [1,r]$.*
(3) *Let $S = gh$ with $g, h \in \langle e_1, \dots, e_r \rangle + \sum_{i=1}^r G_0^i$ such that $\pi'_j(g) = \pi'_j(h) = e'_j$ and $\pi'_m(g) = \pi'_m(h) = e'_m$ for distinct $j, m \in [1,r]$.*
(4) *Let $S = \prod_{j=1}^s g_j \in \mathcal{F}(\langle e_1, \dots, e_r \rangle + \sum_{i=1}^r G_0^i)$ with $s \ge 3$ and $I_j = \{i \in [1,r] \mid \pi'_i(g_j) = e'_i\}$ such that for every $J \subset [1,s]$ with $|J| \ge 2$*

$$|\bigcap_{j \in J} I_j| = \begin{cases} 1 & \textit{if } J = \{j, j'\} \textit{ and } j - j' \equiv \pm 1 \bmod s \\ 0 & \textit{otherwise} \end{cases}.$$

Proof. 1. By Lemma 4.2 we have

$$|\mathsf{k}(\Omega(G_0, g) \cap \mathcal{A}(G))| > 1,$$

since $\{g = \sum_{i=1}^r a_i e_i + b_i e'_i \mid b_i \in [0,1]\} = \langle e_1, \dots, e_r \rangle + \sum_{i=1}^r G_0^i$. This implies $\Omega(G_0, S) \not\subset \mathcal{G}_1(G)$.

2. Let $S = \prod_{j=1}^l g_j$. We have that for each $j \in [1,l]$ there exists some atom $A_j \in \Omega(G_0, g_j)$. By Lemma 4.2 respectively its proof we get $A_j = g_j F_j F'_j$ with $F_j \in \mathcal{F}(G_0^m)$, $F'_j \in \mathcal{F}(G_0 \setminus G_0^m)$ and $|F_j| = p$, since $\pi'_m(g_j) = 0$ and $\pi_m(g_j) \ne 0$. We consider the block $B = \prod_{j=1}^l A_j \in \Omega(G_0, S)$. Clearly, we have $l \in \mathsf{L}(B)$. Since $\sigma((\pi_m + \pi'_m)(S)) = 0$, we have $\sigma(\prod_{j=1}^l F_j) = 0$. Since $F_j \in \mathcal{F}(G_0^m)$ and G_0^m is half-factorial, we obtain $\{l\} = \mathsf{L}(\prod_{j=1}^l F_j)$. Consequently, $B = (\prod_{j=1}^l F_j)(\prod_{j=1}^l g_j F'_j)$ and $l + \mathsf{L}(\prod_{j=1}^l g_j F'_j) \subset \mathsf{L}(B)$. Clearly, $\prod_{j=1}^l g_j F'_j \ne 1$ and thus $\mathsf{L}(\prod_{j=1}^l g_j F'_j) \ne \{0\}$, which implies $|\mathsf{L}(B)| > 1$.

3. Suppose there exist $A, A' \in \Omega(G_0, S) \cap \mathcal{A}(G)$ with $\mathsf{k}(A) \ne \mathsf{k}(A')$. Then there exists some $B \in \Omega(G_0, S)$ such that $A | B$ and $A' | B$, for example $S^{-1} A A' T$ with $T \in \mathcal{F}(G_0)$ and $\sigma(T) = \sigma(S)$. This implies

$$\{1 + \mathsf{k}(B) - \mathsf{k}(A), 1 + \mathsf{k}(B) - \mathsf{k}(A')\} \subset \mathsf{L}(B)$$

and thus $|\mathsf{L}(B)| \ge 2$. Consequently, it suffices to show that there exist atoms $A, A' \in \Omega(G_0, S)$ with $\mathsf{k}(A) \ne \mathsf{k}(A')$.

Without restriction let $j = 1$ and $m = 2$. We have $g = a_1 e_1 + e'_1 + a_2 e_2 + e'_2 + g_1$ and $h = a'_1 e_1 + e'_1 + a'_2 e_2 + e'_2 + h_1$ with $a_1, a_2, a'_1, a'_2 \in [0, p-1]$ and $h_1, g_1 \in \langle e_3, \dots, e'_r \rangle$.

Let $F_2 = (-(a_2 + a'_2)e_2 + e'_2)e_2'^{p-3}$ and $F \in \mathcal{F}(G_0)$ zero-sumfree with $\sigma(F) = -g_1 - h_1$. Further let $F_1 = (-(a_1 + a'_1)e_1 + e'_1)e_1'^{p-3}$ and

$$F'_1 = \begin{cases} (e_1 + e'_1)^{p-1}(-e_1 + e'_1)^{p-1} & \text{if } a_1 + a'_1 \equiv 0 \bmod p \\ e_1'^{p-1}((a_1 + a'_1)e_1 + e'_1)^{p-1} & \text{if } a_1 + a'_1 \not\equiv 0 \bmod p. \end{cases}$$

Then $A = ghFF_2F_1$ and $A' = ghFF_2F'_1$ are atoms, elements of $\Omega(G_0, S)$ and $\mathsf{k}(A) \neq \mathsf{k}(A')$.

This construction is similar to the one used in Lemma 4.2. Note that $(a_1e_1 + e'_1)(a'_1e_1 + e'_1)F'_1$ is not an atom but the product of two atoms, where $(a_1e_1 + e'_1)$ divides the one and $(a'_1e_1 + e'_1)$ the other. However, due to the choice of F_2, we have that A' can not be factorized into two atoms, where g divides the one and h the other.

4. Let $\{i_1\} = I_s \cap I_1$ and $\{i_j\} = I_{j-1} \cap I_j$ for each $j \in [2, s]$. Clearly, $|\{i_1, \ldots, i_s\}| = s$ and without restriction we assume $i_j = j$ for each $j \in [1, s]$. Similarly to the construction in the proof of (3) we assert that there exist $A, A' \in \Omega(G_0, S) \cap \mathcal{A}(G)$ with $\mathsf{k}(A) \neq \mathsf{k}(A')$. For $j \in [1, s]$ let $c_j \in [0, p-1]$ such that $c_je_j = -\pi_j(\sigma(S))$ and $F_j = (c_je_j + e'_j)e_j'^{p-3}$. Further let

$$F'_1 = \begin{cases} (e_1 + e'_1)^{p-1}(-e_1 + e'_1)^{p-1} & \text{if } c_1 = 0 \\ e_1'^{p-1}(-c_1e_1 + e'_1)^{p-1} & \text{if } c_1 \neq 0 \end{cases}$$

and $F \in \mathcal{F}(G_0)$ be zero-sumfree with $\sigma(F) = -\sum_{m=s+1}^{r}(\pi_m + \pi'_m)(\sigma(S))$. Note that $F \in \mathcal{F}(\langle e_{s+1}, \ldots, e'_r\rangle)$. We verify that

$$A = F_1SF\prod_{j=2}^{l} F_j \text{ and } A' = F'_1SF\prod_{j=2}^{l} F_j$$

are atoms in $\Omega(G_0, S)$ with different cross numbers. That $\mathsf{k}(A) \neq \mathsf{k}(A')$ is obvious and that $\sigma(A) = \sigma(A') = 0$ can be checked easily, thus by construction $A, A' \in \Omega(G_0, S)$. It remains to show that A, A' are atoms. We do this just for A', since for A be can argue analogous. Suppose $A' = B_1B_2$ with $B_1, B_2 \in \mathcal{B}(G) \setminus \{1\}$. Without restriction let $g_1|B_1$. Since $\pi'_2(g_1) = e'_2$ and $\pi'_2(g) \neq 0$ if and only if $g|g_1g_2F_2$, we have $g_1g_2F_2|B_1$. The same way, since $\pi'_3(g_2) = e'_3$, we obtain $g_2g_3F_3|B_1$. Repeating this construction, respectively by an easy inductive argument, we get $g_j|B_1$ for each $j \in [1, s]$ and thus $\prod_{j=1}^{s} g_j|B_1$. Consequently, $B_2|F\prod_{j=1}^{s} F_j$. By construction $F\prod_{j=1}^{s} F_j$ is zero-sumfree, a contradiction. □

Note that (1), (2), and (3), (3) with a slightly different proof, hold for $p = 2$ as well. Moreover, in Lemma 5.4 we obtain a result similar to (4) for elementary 2-groups.

Theorem 4.5. *Let $p \geq 3$, $k \in \mathbb{N}$ and G be an elementary p-group with even rank $\mathsf{r}(G) = 2r$. Then*

$$(k - 1 + r)p - 1 \leq \psi_k(G) \leq rp - 1 + (k - 1)\max\{p, r\}.$$

In particular, $\psi_1(G) = rp - 1$ and if $p \geq r$, then $\psi_k(G) = (k - 1 + r)p - 1$.

Proof. The lower bound was obtained in Lemma 4.3. It suffices to show $\psi_k(G) \le rp - 1 + (k-1)\max\{p, r\}$, since the other statements follow immediately. We will prove that (for $G_0 \subset G$ half-factorial with $|G_0| = \mu(G)$) if $S \in \mathcal{F}(G \setminus G_0)$ with $|S| \ge rp + (k-1)\max\{p, r\}$, then $\Omega(G_0, S) \not\subset \mathcal{G}_k(G)$.

We proceed by induction on k.

Let $k = 1$ and $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G \setminus G_0)$ with $l \ge rp$. We need to show that $\Omega(G_0, S) \not\subset \mathcal{G}_1(G)$. Since it will be needed in the sequel of the proof, we prove a slightly more general statement. We show that there exists a subsequence $R|S$ with $|R| \le \max\{p, r\}$ such that $\Omega(G_0, R) \not\subset \mathcal{G}_1(G)$.

This is done in four steps. In each step we use the according part of Proposition 4.4.

Step 1: Suppose there exists some $g|S$ with $g \in G \setminus (\langle e_1, \ldots, e_r\rangle + \sum_{i=1}^{r} G_0^i)$. Then we have by Proposition 4.4.1 that $\Omega(G_0, g) \not\subset \mathcal{G}_1(G)$. We set $R = g$ and are done. Thus we assume without restriction $S \in \mathcal{F}(\langle e_1, \ldots, e_r\rangle + \sum_{i=1}^{r} G_0^i)$.

Step 2: Let $S'|S$ denote the subsequence consisting of the elements $g|S$ for which there exists some $j_g \in [1, r]$ with $(\pi_{j_g} + \pi'_{j_g})(g) \in \langle e_j\rangle \setminus \{0\}$. Suppose $|S'| \ge r(p-1) + 1$. Then there exists some $m \in [1, r]$ and a sequence $S''|S'$ with $|S''| \ge p$ such that $(\pi_m + \pi'_m)(S'') \in \mathcal{F}(\langle e_m\rangle \setminus \{0\})$. Since $|S''| \ge |\langle e_m\rangle|$, we get that there exists some $A|S''$ with $(\pi_m + \pi'_m)(A) \in \mathcal{A}(\langle e_m\rangle \setminus \{0\})$. By Proposition 4.4.2 this implies $\Omega(G_0, A) \not\subset \mathcal{G}_1(G)$. Since $|A| \le p$, we set $R = A$. We assume that $|S'| \le r(p-1)$ respectively $|S'^{-1}S| \ge r$.

Step 3: Let $T = S'^{-1}S$ and for each $g|T$ let $I_g = \{i \in [1, r] \mid \pi'_i(g) = e'_i\}$. It follows that $|I_g| \ge 2$ for each $g|T$. Suppose there exists some $h \in G$ with $gh|T$ such that $|I_g \cap I_h| \ge 2$. Then we have by Proposition 4.4.3 that $\Omega(G_0, gh) \not\subset \mathcal{G}_1(G)$ and we set $R = gh$. Thus we assume if $gh|T$, then $|I_g \cap I_h| \le 1$. Note that this is only possible if $r \ge 3$. Thus in case $r \le 2$ the statement would be proved already. Moreover, it follows that T is squarefree, i.e., $\mathsf{v}_g(T) \le 1$ for each $g \in G$.

Step 4: We assert that there exists a subsequence $T' = (\prod_{j=1}^{s} g'_j)|T$ with $r \ge s \ge 3$ such that the sets $I'_j = I_{g'_j}$ fulfill the conditions of Proposition 4.4.4, i.e., for every $J \subset [1, s]$ with $|J| \ge 2$

$$|\bigcap_{j\in J} I'_j| = \begin{cases} 1 & \text{if } J = \{j, j'\} \text{ and } j - j' \equiv \pm 1 \bmod s \\ 0 & \text{otherwise} \end{cases}.$$

Then we have $\Omega(G_0, T') \not\subset \mathcal{G}_1(G)$ and we set $R = T'$.

We prove by induction on r that a sequence T with $|T| = r \ge 3$, where $|I_g \cap I_h| \le 1$ and $|I_g| \ge 2$ for each $gh|T$, has a subsequence with the claimed properties. For ease of notation we will write I_j instead of I_{g_j}.

Let $r = 3$. Since $|I_g \cap I_h| \le 1$ and $|I_g| \ge 2$ for $gh|T$, it follows that $|I_g| < 3$ for each $g|T$ and $|T| = 3$. Thus $T = g_1g_2g_3$ and $\{I_1, I_2, I_3\} = \{\{1, 2\}, \{2, 3\}, \{1, 3\}\}$. We set $T' = T$ and numerate the elements in a suitable way.

Let $r > 3$. For $j \in [1, r]$ let $T_j | T$ denote the subsequence of the elements $g | T$ with $j \in I_g$.

Case 1: There exists some $j \in [1, r]$ such that $|T_j| \le 1$. Without restriction let $j = r$. We apply the induction hypothesis to the sequence $T_r^{-1} T$ and obtain that there exists a subsequence $T' | T_r^{-1} T$ with $|T'| \le r - 1$ and the claimed properties.

Case 2: $|T_j| \ge 2$ for each $j \in [1, r]$. We define the sequence $T' | T$ by a recursive construction. Let $j_0 = 1$, $g_1 | T_{j_0}$ and $j_1 \in I_1 \setminus \{j_0\}$. Let $i \ge 1$ and suppose g_m and j_m are constructed for $m \in [1, i]$. Then let $g_{i+1} | g_i^{-1} T_{j_i}$. If $I_{i+1} \cap \bigcup_{m=1}^{i} I_m = \{j_i\}$, then let $j_{i+1} \in I_i \setminus \{j_i\}$ and we proceed with the construction.

If $|I_{i+1} \cap \bigcup_{m=1}^{i} I_m| \ge 2$, then let $m' = \max\{m \in [0, i-1] \mid I_m \cap I_{i+1} \ne \emptyset\}$ and we set $T' = \prod_{j=m'}^{i+1} g_j$. Note that $|\bigcup_{m=1}^{i} I_m| \ge i + 1$. Thus if $i = r - 1$, then we would have $\bigcup_{m=1}^{i} I_m = [1, r]$ and the construction would stop. Changing the indexset by setting $g_j' = g_{j+1-m'}$, we obtain the sequence T' as claimed. This proves the statement for $k = 1$.

Let $k \ge 2$ and suppose the statement holds for $k' < k$. Let $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G \setminus G_0)$ with $l \ge rp - 1 + (k-1)\max\{p, r\}$. Clearly, $l \ge rp - 1$ and we have that there exists a subsequence $R | S$ such that $\Omega(G_0, R) \not\subset \mathcal{G}_1(G)$ and $|R| \le \max\{p, r\}$. Since $|R^{-1} S| \ge rp - 1 + (k-2)\max\{p, r\}$, we get by induction hypothesis that $\Omega(G_0, R^{-1} S) \not\subset \mathcal{G}_{k-1}(G)$. This implies $\Omega(G_0, S) \not\subset \mathcal{G}_k(G)$. $\square$

Parts of the proof, in particular in Step 4, just depend on the system of sets (the hypergraph) $([1, r], (I_g)_{g|T})$. Thus the proof could be shortened by using results on hypergraphs (cf. for example [5] in particular 2.1). As mentioned in the Introduction we can solve the problem [22, P 1247] in the following special case.

Corollary 4.6. *Let $p \ge 3$ and G be an elementary p-group with even rank $\mathsf{r}(G) = 2r$. If $p \ge r$, then $(\psi_k(G))_{k=1}^{\infty}$ is an arithmetic progression.*

4.2. **Groups with Odd Rank.** In this section we investigate elementary p-groups with odd rank. The results we obtain are much weaker than the ones for groups with even rank, and we mainly establish lower bounds. We start with the investigation of groups with rank 1 and consider the more general situation of cyclic groups with prime power order.

The following characterization result on half-factorial sets in cyclic groups with prime power order was proved by various authors in slightly different formulations cf. [7, Corollary 5.4] for a proof and detailed references.

Proposition 4.7. *Let G be cyclic with $|G| = p^m$ for some $p \in \mathbb{P}$ and $m \in \mathbb{N}$. Then $\mu(G) = m + 1$ and $G_0 \subset G$ is half-factorial with $|G_0| = \mu(G)$ if and only if $G_0 = \{p^i g \mid i \in [0, m]\}$ for some $g \in G$ with $\mathrm{ord}(g) = p^m$.*

We apply this characterization to obtain a technical result and first lower bounds.

Proposition 4.8. *Let G be cyclic with $|G| = p^m$ for some $p \in \mathbb{P}$ and $m \in \mathbb{N}$.*

(1) *Let $G_0 = \{p^i e \mid i \in [0, m]\}$ with $e \in G$ and $\operatorname{ord}(e) = p^m$. Further let $g = ae \in G \setminus G_0$ with $a \in [2, p^m - 1]$ such that $p \nmid a$. If $l \in \mathbb{N}_0$ with $l(a-1) < p^m$, then $\emptyset \neq \Omega(G_0, g^l) \subset \mathcal{G}_1(G)$. In particular, $\mathsf{L}(C) = \{\mathsf{k}(C) + l\frac{a-1}{p^m}\}$ for each $C \in \Omega(G_0, g^l)$.*

(2) *If $p \geq 3$, then $\psi_1(G) \geq p^m - 1$.*

(3) *If $p = 2$, then $\psi_1(G) \geq 2^{m-1} - 1$.*

Proof. 1. By Proposition 4.7 we know that G_0 is half-factorial and $|G_0| = \mu(G)$. Clearly, $\langle G_0 \rangle = G$ and thus $\Omega(G_0, S) \neq \emptyset$ for every $S \in \mathcal{F}(G \setminus G_0)$. Let $l \in \mathbb{N}_0$ such that $l(a-1) < p^m$.

We first prove the following statement on cross numbers of certain atoms: If $A \in \mathcal{A}(G_0 \cup \{g\})$ with $\mathsf{v}_g(A) = v \leq l$, then $\mathsf{k}(A) = 1 - \frac{v(a-1)}{p^m}$. Let $A \in \mathcal{A}(G_0 \cup \{g\})$ with $\mathsf{v}_g(A) = v \leq l$. By [11, Lemma 2] we know that $\mathsf{k}(A') \leq 1$ for every $A' \in \mathcal{A}(G)$. Let $B = g^{-v} e^{av} A \in \mathcal{B}(G_0)$. Since G_0 is half-factorial, we know $\mathsf{k}(B) \in \mathbb{N}$. Thus we have $1 \leq \mathsf{k}(B) = \mathsf{k}(A) + v\frac{a-1}{p^m} < 2$, consequently $\mathsf{k}(B) = 1$ and $\mathsf{k}(A) = 1 - \frac{v(a-1)}{p^m}$.

Let $C \in \Omega(G_0, g^l)$ and $C = \prod_{i=1}^n U_i$ be a factorization with $U_i \in \mathcal{A}(G)$ and $\mathsf{v}_g(A) = v_i$ for each $i \in [1, n]$. Then

$$\mathsf{k}(C) = \sum_{i=1}^n \mathsf{k}(U_i) = \sum_{i=1}^n \left(1 - \frac{v_i(a-1)}{p^m}\right) = n - \mathsf{v}_g(C)\frac{a-1}{p^m}$$

and $n = \mathsf{k}(C) + l\frac{a-1}{p^m}$ is determined by C. Consequently, $\mathsf{L}(C) = \{\mathsf{k}(C) + l\frac{a-1}{p^m}\}$ and $\Omega(G_0, g^l) \subset \mathcal{G}_1(G)$.

2. and 3. Note that if $p = 2$, then $m \geq 2$, since by our general assumption $|G| \geq 3$. Let $G_0 \subset G$ half-factorial with $|G_0| = \mu(G)$. By Proposition 4.7 we know that G_0 fulfills the conditions of (1). For $p \geq 3$, we set $g = 2e$. Since $(p^m - 1)(2 - 1) < p^m$, we obtain by Proposition 4.8 that $\psi_1(G) \geq p^m - 1$. For $p = 2$, we set $g = 3e$. Since $(2^{m-1} - 1)(3 - 1) < 2^m$, we obtain $\psi_1(G) \geq 2^{m-1} - 1$. □

This lower bound is in general not sharp as the following result shows. However, for $p^m = 4$ and $p^m = 3$ equality holds. As already mentioned in the Introduction, this was initially obtained in [21, 22]. For $p^m = 3$ we state this result (cf. [21, Corollary 2]) in the first part of the following lemma.

Proposition 4.9. *Let $|G| \in \mathbb{P}$ and $k \in \mathbb{N}$.*

(1) *If $|G| = 3$, then $\psi_k(G) = 3k - 1$.*

(2) *If $|G| \geq 5$, then $\psi_k(G) \geq pk - 1 + \frac{p-1}{2}$.*

Proof. Let $G_0 \subset G$ half-factorial with $|G_0| = \mu(G) = 2$. Then $G_0 = \{0, e\}$ with some $e \in G \setminus \{0\}$.

1. Let $|G| = 3$. We note that $\mathcal{A}(G) = \{0, e(2e), e^3, (2e)^3\}$. Since $(2e)^3 e^3 = ((2e)e)^3$, we have $\Omega(G_0, (2e)^3) \not\subset \mathcal{G}_1(G)$ and consequently $\psi_1(G) < 3$. Using Lemma 3.2 we obtain $\psi_k(G) \leq (k-1)(\psi_1(G) + 1) + \psi_1(G) \leq 3k - 1$.

It remains to show that $\Omega(G_0, (2e)^{3k-1}) \subset \mathcal{G}_k(G)$. Let $B \in \mathcal{B}(G)$ and

$$B = \prod_{i=1}^{n'} V_i = ((2e)e)^m \prod_{i=1}^{n} U_i$$

where $U_i \neq (2e)e$ for each $i \in [1, n]$. Since $\mathsf{k}(B) = m\frac{2}{3} + n$, we have that n is determined by m and $\mathsf{k}(B)$. Moreover, $m \equiv \mathsf{v}_{2e}(B) \bmod 3$. Thus for $C \in \Omega(G_0, (2e)^{3k-1})$ there are at most k possible values for m. This implies $|\mathsf{L}(C)| \le k$.

2. Let $|G| \ge 5$ and $S = (2e)^{kp-1}(-2e)^{\frac{p-1}{2}}$. We show $\emptyset \neq \Omega(G_0, S) \subset \mathcal{G}_k(G)$.

Note that if $A \in \mathcal{A}(\{0, e, 2e, -2e\})$ with $0 < \mathsf{v}_{-2e}(A) \le \frac{p-1}{2}$, then $A = (-2e)2e$ or $A = (-2e)e^2$. Let $C \in \Omega(G_0, S)$ and

$$C = \prod_{i=1}^{n'} V_i = ((2e)^p)^m \prod_{i=1}^{n} U_i$$

with $U_i \neq (2e)^p$ for each $i \in [1, r]$ be a factorization into atoms. Clearly, $m \in [0, k-1]$. We assert that n is determined by m and C. This implies, since there are at most k possible values for m, that $|\mathsf{L}(C)| \le k$.

Since $\mathsf{v}_{-2e}(C) = \frac{p-1}{2}$, there exists some subset $I \subset [1, n]$ with $|I| = \frac{p-1}{2}$ such that $U_i \in \{(-2e)2e, (-2e)e^2\}$ for each $i \in I$. Let $l = |\{i \in I \mid U_i = (-2e)e^2\}| \in [0, \frac{p-1}{2}]$. Then we have

$$C' = ((2e)^p)^m \prod_{i \in [1,n] \setminus I} U_i \in \Omega(G_0, (2e)^{kp-p+\frac{p-1}{2}+l}).$$

We have, cf. proof of Proposition 4.8, $\mathsf{k}(U_i) = 1 - \frac{\mathsf{v}_{2e}(U_i)}{p}$ for each $i \in [1, n] \setminus I$. Thus

$$\begin{aligned} \mathsf{k}(C') &= m + \sum_{i \in [1,n] \setminus I} \left(1 - \frac{\mathsf{v}_{2e}(U_i)}{p}\right) = m + n - \frac{p-1}{2} - \frac{\mathsf{v}_{2e}(C')}{p} \\ &= m + n - \frac{p-1}{2} - (k-1) - \frac{p-1+2l}{2p}. \end{aligned}$$

Since $\mathsf{k}(C') = \mathsf{k}(C) - \sum_{i \in I} \mathsf{k}(U_i) = \mathsf{k}(C) - \frac{p-1}{2}\frac{2}{p} - l\frac{1}{p}$, we obtain

$$\mathsf{k}(C) = m + n - \frac{p-1}{2} + k - 1 + \frac{3(p-1)}{2p}.$$

Thus n just depends on m and $\mathsf{k}(C)$. □

Next we combine the results on cyclic groups with the ones on elementary p-groups with even rank to establish lower bounds for elementary p-groups with odd rank. Again we neglect $p = 2$, since we will treat elementary 2-groups in the following section.

In [9, Theorem 8] it was proved that if G is an elementary p-group with odd rank $\mathsf{r}(G) = 2r+1$, then $2 + rp \le \mu(G) \le 1 + rp + \lfloor \frac{p}{2} \rfloor$. For $p \in \{2, 3\}$ this implies $\mu(G) = 2+rp$ and for $p \in \{5,7\}$ this was proved in [19, Theorem 3.2]. Note that if $G = G' \oplus G''$ and $\mu(G) = 2+rp$, then $\mu(G) = \mu(G') + \mu(G'') - 1$.

Corollary 4.10. *Let $r \in \mathbb{N}_0$, $k \in \mathbb{N}$ and G an elementary p-groups with* $\mathsf{r}(G) = 2r+1$.

1. *If $p = 3$, then $\psi_k(G) \ge 3(k+r) - 1$.*
2. *If $p \ge 5$ and $\mu(G) = 2+rp$, then $\psi_k(G) \ge p(k+r) - 1 + \frac{p-1}{2}$.*

Proof. Let $p \in \mathbb{P}$. For $r = 0$ the result is just Lemma 4.9. Let $r \ge 1$ and $G = G' \oplus G''$ with $\mathsf{r}(G') = 2r$ and $\mathsf{r}(G'') = 1$. Since $\mu(G) = \mu(G') + \mu(G'') - 1$, we can apply Lemma 3.1.4. We apply the lower bounds obtained in Lemma 4.3 for $\psi_k(G')$ and in Lemma 4.9 for $\psi_1(G'')$ and the statement follows. $\square$

Remark 4.11. Similarly as in [18, Theorem 7.1] we can obtain that for every $p \in \mathbb{P}$ there exists some $r_p \in \mathbb{N}$ such that $\psi_k(G) \ge (k - 1 + \frac{(r-r_p)}{2})p - 1$ for every elementary p-group G with $\mathsf{r}(G) \ge r_p$.

5. $\psi_k(G)$ for Elementary 2-groups

Until the end of this section let G denote an elementary 2-group with rank $\mathsf{r}(G) = r \ge 2$. In [14, Problem II] it was proved that $\mu(G) = r+1$ and that $G_0 \subset G$ is half-factorial if and only if $G_0 \setminus \{0\}$ is independent. Thus again all half-factorial subsets with maximal cardinality are equal up to automorphisms. Throughout the whole section let $\{e_1, \ldots, e_r\} \subset G$ be a basis and $G_0 = \{0, e_1, \ldots, e_r\}$, a half-factorial set with $|G_0| = \mu(G)$. Further let π_i denote the projection on $\langle e_i \rangle$ for each $i \in [1,r]$.

We start with the following short lemma that provides a first lower bound.

Lemma 5.1. *Let $k \in \mathbb{N}$. Then $\psi_k(G) \ge 2(k-1) + r - 1$.*

Proof. If r is even, then this is just Lemma 4.3. Suppose r is odd and let $G = G' \oplus G''$ with $|G''| = 2$. Then $\psi_k(G) \ge \psi_k(G') + 1 \ge 2(k-1) + r - 2 + 1$ by Lemma 3.1.4 and Lemma 4.3. $\square$

As mentioned in the Introduction we will apply notions and results of extremal graph theory to determine $\psi_k(G)$ (in terms of constants introduced there). We will show (cf. Theorem 5.7) that to determine $\psi_k(G)$ is equivalent to determining the maximal number of edges in a graph on r vertices not containing k edge disjoint cycles. We use the convention that a graph may have multiple edges but no loops. Apart from that our terminology concerning (multi)graphs will follow [2].

We define for each $S \in \mathcal{F}(G \setminus G_0)$ an associated graph with vertex set $[1,r]$. In general this graph is not uniquely determined. Conversely, we define for each graph with vertex set $[1,r]$ its (uniquely determined) associated sequence $S \in \mathcal{F}(G \setminus G_0)$.

Definition 5.2. Let $l \in \mathbb{N}$.

1. Let $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G \setminus G_0)$. For $i \in [1,l]$ let $I_i = \{j \in [1,r] \mid \pi_j(g_i) = e_j\}$ and let $E_i \subset I_i$ be some subset with $|E_i| = 2$. The graph $([1,r], (E_i)_{i \in [1,l]})$ is called an associated graph of S.

(2) Let $([1,r],(E_i)_{i\in[1,l]})$ be a graph. For $i \in [1,l]$ let $g_i = \sum_{j\in E_i} e_j$. Then $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G \setminus G_0)$ is called the associated sequence of $([1,r],(E_i)_{i\in[1,l]})$.

Example 5.3. Let $S = (e_1+e_2)^{2(k-1)} \prod_{i=1}^{r-1}(e_i+e_{i+1})$. The sequence S is an example of a sequence with $|S| = 2(k-1)+r-1$ and $\Omega(G_0,S) \subset \mathcal{G}_k(G)$. Its associated graph, in this special case it is uniquely determined, is a path where one edge is a multiple edge with multiplicity $2k-1$. Note that this graph contains exactly $k-1$ edge disjoint cycles.

In the following two lemmata we prove that the number of edge disjoint cycles in an associated graphs of S and sets of lengths of $B \in \Omega(G_0,S)$ are closely related.

Lemma 5.4. *Let $k \in \mathbb{N}$, $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G \setminus G_0)$ and $([1,r],(E_i)_{i\in[1,l]})$ an associated graph that contains k edge disjoint cycles. Then $\Omega(G_0,S) \not\subset \mathcal{G}_k(G)$.*

Proof. Let $I_i = \{j \in [1,r] \mid \pi_j(g_i) = e_j\}$ for each $i \in [1,l]$. Then $A_i = g_i \prod_{j\in I_i} e_j \in \mathcal{A}(G)$ and $B = \prod_{i=1}^{l} A_i \in \Omega(G_0,S)$. It suffices to show $B \notin \mathcal{G}_k(G)$.

We proceed by induction on k. Let $k = 1$ and let $C \subset [1,l]$ such that $(E_i)_{i\in C}$ are the edges of a cycle and $V_C \subset [1,r]$ the set of vertices occurring in this cycle. We consider $B' = \prod_{i\in C} A_i$ and obtain $B' = (\prod_{i\in V_C} e_i^2)B''$ with $B'' \in \mathcal{B}(G) \setminus \{1\}$. Since $|C| = |V_C|$, we have $\mathsf{L}(B') \ge 2$ and $B \notin \mathcal{G}_1(G)$.

Let $k \ge 2$ and suppose the statement holds for $1 \le k' < k$. Again let $C \subset [1,l]$ such that $(E_i)_{i\in C}$ are the edges of a cycle and $([1,r],(E_i)_{i\in[1,l]\setminus C})$ has $k-1$ edge disjoint cycles. We have $B = B'B''$ with $B' = \prod_{i\in C} A_i$ and $B'' = \prod_{i\in[1,l]\setminus C} A_i$. By induction hypothesis we get $B' \notin \mathcal{G}_1(G)$ and $B'' \notin \mathcal{G}_{k-1}(G)$. Thus we obtain $B \notin \mathcal{G}_k(G)$. □

Lemma 5.5. *Let $([1,r],(E_i)_{i\in[1,l]})$ be a graph that does not contain k edge disjoint cycles and S its associated sequence. Then $\Omega(G_0,S) \subset \mathcal{G}_k(G)$.*

Proof. By definition we have $g = e_i + e_j$ for distinct $i,j \in [1,r]$ for every $g|S$, i.e., $S \in \mathcal{F}((G_0+G_0)\setminus G_0)$. Thus $\Omega(G_0,S) \subset \mathcal{B}(G_0+G_0)$. We start with an investigation of $\mathcal{A}(G_0+G_0)$. Let $A \in \mathcal{A}(G_0+G_0)\setminus\{0\}$.

1. Suppose $\mathsf{v}_{e_i}(A) = 0$ for every $i \in [1,r]$, i.e., $A|S$. We assert that the according edges are the edges of a cycle. Let $g_1 = e_{j_0} + e_{j_1}|A$. There exists some $g_2|g_1^{-1}A$ such that $g_2 = e_{j_1} + e_{j_2}$. If $j_2 \in \{j_0,j_1\}$, equivalently $j_2 = j_0$, then $\sigma(g_1g_2) = 0$ and $A = g_1g_2$. Otherwise we proceed with a recursive construction. Let $i \ge 2$ and $g_i = e_{j_{i-1}} + e_{j_i}$ such that $j_i \notin \{j_0,\dots,j_{i-1}\}$. Then there exists some $g_{i+1}|(\prod_{j=1}^{i} g_j)^{-1}A$ such that $g_{i+1} = e_{j_i} + e_{j_{i+1}}$. If $j_{i+1} \in \{j_0,\dots,j_i\}$, say $j_{i+1} = j_m$, then $\sigma(\prod_{j=m+1}^{i+1} g_j) = 0$. Thus it follows $m = 0$ and $A = \prod_{j=1}^{i+1} g_j$. For $i = r-1$ we would have $\{j_0,\dots,j_i\} = [1,r]$ and thus $j_{i+1} \in \{j_0,\dots,j_i\}$. Thus $A = \prod_{j=1}^{s} g_j$ for some $s \in [2,r]$ and the associated edges are the edges of a cycle with vertices $\{j_0,\dots,j_{s-1}\}$.

2. Suppose $e_{j_0}|A$ for some $j_0 \in [1, r]$. We set $g_0 = e_{j_0}$. If $e_{j_0}|(g_0^{-1}A)$, we set $g_1 = e_{j_0}$ and it follows that $A = g_0 g_1 = e_{j_0}^2$. Otherwise there exists some $j_1 \notin \{j_0\}$ such that $g_1 = (e_{j_0} + e_{j_1})|(g_0^{-1}A)$ and we proceed with a recursive construction. Let $i \geq 1$ and $g_i = e_{j_{i-1}} + e_{j_i}$ such that $j_i \notin \{j_0, \ldots, j_{i-1}\}$. If $e_{j_i}|(\prod_{j=0}^{i} g_j)^{-1}A$, we set $g_{i+1} = e_{j_i}$ and it follows that $A = \prod_{j=0}^{i+1} g_j$. Otherwise there exists some $g_{i+1}|(\prod_{j=0}^{i} g_j)^{-1}A$ such that $g_{i+1} = e_{j_i} + e_{j_{i+1}}$. It follows that $j_{i+1} \notin \{j_0, \ldots, j_i\}$, since otherwise A would have a proper zero-sum subsequence (cf. 1. for a detailed argument). Similarly to 1., if $i = r-1$ we have $\{j_0, \ldots, j_i\} = [1, r]$ and thus necessarily $e_{j_i}|(\prod_{j=0}^{i} g_j)^{-1}A$. Thus $A = \prod_{j=0}^{s} g_j$ for some $s \in [2, r]$. In particular, $A = \prod_{j=0}^{s} g_j = e_{j_0} e_{j_{s-1}} \prod_{j=1}^{s-1} g_j$ and the edges associated to g_j for $j \in [1, s-1]$ are the edges of a path from j_0 to j_{s-1}.

We summarize these results. Let $A \in \mathcal{A}(G_0 + G_0)$. If $A \notin \mathcal{A}((G_0 + G_0) \setminus G_0)$, then $\mathsf{k}(A) = 1 + \frac{1}{2} \sum_{g \in G \setminus G_0} \mathsf{v}_g(A)$. If $A \in \mathcal{A}((G_0 + G_0) \setminus G_0)$, then $\mathsf{k}(A) = \frac{1}{2} \sum_{g \in G \setminus G_0} \mathsf{v}_g(A)$ and the associated edges are the edges of a cycle in the associated graph.

Let $B \in \Omega(G_0, S)$ and $B = \prod_{i=1}^{n} U_i$ be a factorization of B into atoms. Further let $m = |\{i \mid U_i \in \mathcal{A}((G_0 + G_0) \setminus G_0)\}|$. Recall that each of these m atoms is associated to a cycle and thus $m \in [0, k-1]$. We have

$$\mathsf{k}(B) = \sum_{i=1}^{n} \mathsf{k}(U_i) = n - m + \frac{1}{2} \sum_{i=1}^{n} \sum_{g \in G \setminus G_0} \mathsf{v}_g(U_i) = n - m + \frac{|S|}{2}.$$

This implies $\mathsf{L}(B) \subset \mathsf{k}(B) - \frac{|S|}{2} + [0, k-1]$ and thus $\Omega(G_0, S) \subset \mathcal{G}_k(G)$. $\square$

The following constants are investigated in extremal graph theory (cf. [2, Chapter III.3] for detailed references and proofs of the results we mention).

Definition 5.6. Let $k, n \in \mathbb{N}$.

(1) $\mathsf{p}(k)$ denotes the smallest integer l with the property: every graph with v vertices, for some $v \in \mathbb{N}$, and $v + l$ edges contains at least k edge disjoint cycles.
(2) $\mathsf{p}(k, n)$ denotes the smallest integer l with the property: every graph with n vertices and $n + l$ edges contains at least k edge disjoint cycles.

By definition $\mathsf{p}(k, n) \leq \mathsf{p}(k)$ and $\mathsf{p}(k, n) \leq \mathsf{p}(k+1, n)$. Moreover, there exists some $n_k \in \mathbb{N}$ such that $\mathsf{p}(k, n) = \mathsf{p}(k)$ if $n \geq n_k$. It is well known that there exists a graph not containing a cycle with n vertices and $n-1$ edges, i.e., $\mathsf{p}(k, n) \geq 0$.

For $\mathsf{p}(\cdot)$ the following is known:

- $\mathsf{p}(k) + 4 \leq \mathsf{p}(k+1)$.
- $\mathsf{p}(1) = 0$, $\mathsf{p}(2) = 4$, $\mathsf{p}(3) = 10$, and $\mathsf{p}(4) = 18$.
- $\frac{1}{2} k \log_2 k < \mathsf{p}(k) \leq 2k(\log_2 k + \log_2 \log_2 k + 2)$ if $k \geq 2$.

The following theorem summarizes the results of Lemma 5.4 and 5.5.

Theorem 5.7. *Let $k \in \mathbb{N}$ and G and elementary 2-group with rank r. Then $\psi_k(G) = r - 1 + \mathsf{p}(k, r)$. In particular,*

(1) $\psi_1(G) = r - 1$.
(2) $2(k-1) + r - 1 \le \psi_k(G) \le r - 1 + \mathsf{p}(k)$.
(3) $\psi_k(G) = r - 1 + \mathsf{p}(k)$ *if* $r \ge r_k$ *for some* $r_k \in \mathbb{N}$.

Proof. Let $S \in \mathcal{F}(G \setminus G_0)$ with $|S| \ge r + \mathsf{p}(k, r)$. By definition every associated graph of S contains k edge disjoint cycles. By Lemma 5.4 this implies $\psi_k(G) < r + \mathsf{p}(k, r)$.

Conversely, by definition of $\mathsf{p}(k, r)$ there exists a graph with r vertices and $r - 1 + \mathsf{p}(k, r)$ edges that does not contain k edge disjoint vertices. Let S denote the associated sequence. By Lemma 5.5 we have $\Omega(G_0, S) \subset \mathcal{G}_k(G)$ and $\psi_k(G) \ge |S| = r - 1 + \mathsf{p}(k, r)$.

The additional statements follow, since $\mathsf{p}(1) = 0$, $\mathsf{p}(k, r) \ge 2(k - 1)$ (also cf. Lemma 5.1), $\mathsf{p}(k, r) \le \mathsf{p}(k)$, and $\mathsf{p}(k, r) = \mathsf{p}(k)$ for sufficiently large r. $\square$

Theorem 5.7 and $\mathsf{p}(k)+4 \le \mathsf{p}(k+1)$ imply that the lower bound in Lemma 5.1 is in general not sharp. For example, the graph $K^{3,3}$, the complete bipartite graph, is a graph with 6 vertices and $6 + \mathsf{p}(2) - 1 = 9$ edges not containing 2 edge disjoint cycles. Thus it follows $\psi_2(G) = r + 3 > 2 + r - 1$ for $r \ge 6$. However, if $r \in [2, 3]$, then $\mathsf{p}(k, r) = 2(k - 1)$ and thus $\psi_k(G) = 2(k-1)+r-1$, i.e., equality holds in Lemma 5.1 (for $r = 2$ cf. [22, Section 3]).

Moreover, the results on $\mathsf{p}(\cdot)$ show that $(\psi_k(G))_{k=1}^{\infty}$ is not an arithmetic progression if G is an elementary 2-group with sufficiently large rank. In order to be able to give an example of a number field with a class group having this property, we point out that $\mathsf{p}(1, 4) = 0$, $\mathsf{p}(2, 4) = 3$, where the complete graph K^4 serves as example, and $\mathsf{p}(3, 4) = 5$. Thus if G is an elementary 2-group with rank 4, then $(\psi_k(G))_{k=1}^{\infty}$ is not an arithmetic progression. Note that if $\psi_k(G) > \psi_{k-1}(G)$, then it follows that the maximum in the definition of $\psi_k(G)$ is realized by a block with $|\mathsf{L}(B)| = k$ (also cf. [8, Lemma 3]) and therefore in this case $\psi_k(G) = B(k, G)$ respectively $\psi_k(G) = \overline{\psi}_k(G)$ with $\overline{\psi}_k(G)$ as in [8]. Using the KANT database ([4]) we find that the class group of $\mathbb{Q}(\sqrt{-1365})$ is isomorphic to C_2^4.

Remark 5.8. For elementary p-groups with even rank $2r$, where $p \ge 3$, one can apply similar ideas as for $p = 2$ and obtain an alternative and thus an improved upper bound for $\psi_k(G)$. In particular, these bounds yield $\psi_k(G) \le (k - 1 + r)p - 1 + \mathsf{p}(k)$, which implies that for each $k \in \mathbb{N}$ the gap between lower and improved upper bound does not exceed $\mathsf{p}(k)$, whence is independent of G. However, for arbitrary p it seems that we cannot improve the lower bound in the way it was done for $p = 2$.

References

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

[2] B. Bollobás. *Extremal Graph Theory.* Academic Press, 1978.

[3] S. Chapman and A. Geroldinger. Krull domains and monoids, their sets of lengths and associated combinatorial problems. In *Factorization in integral domains*, Volume 189 of *Lecture Notes in Pure Appl. Math.*, Marcel Dekker, 1997, pages 73 – 112.

[4] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger. KANT V4. *J. Symbolic Comput.*, 24: 267–283, 1997.

[5] P. Duchet. Hypergraphs. In *Handbook of Combinatorics*, Volume 1, 381 – 433. Elsevier, 1995.

[6] P. van Emde Boas. A combinatorial Problem on finite abelian groups II. *Report ZW-1969-007, Math. Centre, Amsterdam.*

[7] W. Gao and A. Geroldinger. Half-factorial domains and half-factorial subsets in abelian groups. *Houston J. Math.*, 24: 593 – 611, 1998.

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

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

[10] F. Halter-Koch. Finitely generated monoids, finitely primary monoids and factorization properties of integral domains. In *Factorization in integral domains*, volume 189 of *Lecture Notes in Pure Appl. Math.*, Marcel Dekker, 1997, pages 31 – 72.

[11] U. Krause. A characterization of algebraic number fields with cyclic class group of prime power order. *Math. Z.*, 186: 143 – 148, 1984.

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

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

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

[15] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*, Third Edition. Springer-Verlag, Berlin, 2004.

[16] J.E. Olson. A combinatorial problem on finite abelian groups, I. *J. Number Theory*, 1: 8–10, 1969.

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

[18] M. Radziejewski and W.A. Schmid. On the asymptotic behavior of some counting functions. *Colloq. Math.*

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

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

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

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

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

Added note

Recently, A. Plagne and the author proved that $\mu(C_p^{2r+1}) = 2 + rp$ for $p \in \mathbb{P}$ and $r \in \mathbb{N}_0$. Thus, the condition in Corollary 4.10.2 is in fact always fulfilled.

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

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