ON INVARIANTS RELATED TO NON-UNIQUE FACTORIZATIONS IN BLOCK MONOIDS AND RINGS OF ALGEBRAIC INTEGERS

WOLFGANG A. SCHMID

ABSTRACT. Let K be a number field, R its ring of integers and H the set of non-zero principal ideals of R. For each positive integer k the set $\mathcal{B}_k(H) \subset H$ denotes the set of principal ideals for which the associated block has at most k different factorizations. For the counting functions associated to these sets asymptotic formulae are known. These formulae involve constants that just depend on the ideal class group G of R. Starting from a known combinatorial description for these constants, we use tools from additive group theory, in particular the notion of Davenport's constant and a classical addition theorem, to investigate them. We determine their precise value in case G is an elementary group or a cyclic group of prime power order. For arbitrary G we derive (explicit) lower bounds.

1. Introduction

Let R be the ring of integers of an algebraic number field K and G the ideal class group. If $|G| > 1$, then R respectively the monoid H of non-zero principal ideals of R is not factorial. Quantitative aspects of non-unique factorizations were first investigated by W. Narkiewicz and then by many authors (see [20, Chapter 9], [12], [9]). Among others, the following sets have been studied for every $k \in \mathbb{N}$:

- $\mathcal{F}_k(H)$, the set of all non-zero principal ideals aR where $a \in R$ has at most k distinct factorizations,
- $\mathcal{B}_k(H)$, the set of all non-zero principal ideals aR where $a \in R$ and the associated block $\boldsymbol{\beta}(aR)$ has at most k distinct factorizations,
- $\mathcal{G}_k(H)$, the set of all non-zero principal ideals aR where $a \in R$ has factorizations of at most k different lengths.

If Z is any of these sets and $x \in \mathbb{R}_{\ge 1}$, then let $Z(x)$ denote the number of principal ideals $aR \in Z$ with $(R\colon aR) \le x$. It has turned out that, for $x \to \infty$, $Z(x)$ has the following type of asymptotic behavior:

$$Z(x) \sim Cx(\log x)^{-A}(\log\log x)^{B}\,,$$

2000 *Mathematics Subject Classification.* 11N64, 11R27, 20D60, 20K01.

Key words and phrases. factorization, zero-sum sequence, block monoid.

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

where $C \in \mathbb{R}_{>0}$, $A \in \mathbb{R}_{\ge 0}$ and $B \in \mathbb{N}_0$. For the sets $\mathcal{F}_k(H)$ and $\mathcal{G}_k(H)$, the exponents A and B have received a lot of attention, but there are still many open questions around them (see [18, 19, 5, 10, 13, 4, 26, 28]). In this paper we concentrate on the set $\mathcal{B}_k(H)$. In [6] it was proved that

$$A = 1 - \frac{1 + \mathsf{r}^*(G)}{|G|} \quad \text{where } \mathsf{r}^*(G) \text{ is the total rank of } G\,,$$

and a (rather involved) combinatorial description of B was given (in terms of G and k). In Section 2 we first introduce the necessary terminology to give this description (Definition 2.1.2) and then we derive a result on the oscillatory behavior of the counting function associated to $\mathcal{B}_k(H)$, which is based on recent work of M. Radziejewski (Theorem 2.3.2). In the subsequent sections, we start from the combinatorial description of B and derive, for every $k \in \mathbb{N}$, an explicit lower bound for B (Theorem 7.1) and the precise value of B, in the case where G is an elementary group or a cyclic group of prime power order (Theorems 4.2, 5.4, and 6.1). For these investigations we use methods from additive group theory, in particular the notion of Davenport's constant and a classical addition theorem.

2. Preliminaries

Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers and we set $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $m, n \in \mathbb{Z}$ let

$$[m, n] = \{x \in \mathbb{Z} \mid m \le x \le n\}.$$

For $n \in \mathbb{N}$ let C_n denote a cyclic group with n elements. Let G be an additively written finite abelian group. A subset $G_0 = \{e_1, \ldots, e_r\} \subset G$ is called *independent* (resp. its elements are called independent), if $0 \notin G_0$, $e_1, \ldots, e_r$ are pairwise distinct and every equation of the form

$$\sum_{i=1}^{r} m_i e_i = 0 \quad \text{with } m_1, \ldots, m_r \in \mathbb{Z} \quad \text{implies } m_1 e_1 = \ldots = m_r e_r = 0.$$

The maximal cardinality of an independent set of elements having prime power order is called the *total rank of* G, which will be denoted by $\mathsf{r}^*(G)$. Then

$$\mathsf{r}^*(G) = \sum_{p \in \mathbb{P}} \mathsf{r}_p(G)$$

where, for every $p \in \mathbb{P}$, $\mathsf{r}_p(G)$ denotes the p-rank of G. Our terminology in factorization theory is consistent with that in [7] and with the survey articles in [2]. For convenience and to fix notations, we recall some key notions and some basic facts.

Monoids and factorizations. Throughout, a monoid is a multiplicatively written commutative cancellative semigroup with identity element. Let H be a monoid. We denote by $H^\times$ the group of invertible

elements of H and by $H_{\red} = \{aH^\times \mid a \in H\}$ the associated reduced monoid of H. We call H reduced if $H^\times = \{1\}$ (and then $H_{\red} = H$). An element $u \in H$ is called an *atom of H* (or an *irreducible element of H*), if $u \notin H^\times$, and for all $a, b \in H$, $u = ab$ implies that $a \in H^\times$ or $b \in H^\times$. We denote by $\mathcal{A}(H)$ the set of atoms of H, and H is called *atomic* if every $a \in H \setminus H^\times$ is a product of atoms. An element $p \in H$ is called a *prime of H*, if $p \notin H^\times$, and for all $a, b \in H$, $p \mid ab$ implies that $p \mid a$ or $p \mid b$. Then H is *factorial*, if it is atomic and every atom of H is a prime.

For a set P, we denote by $\mathcal{F}(P)$ the free abelian monoid with basis P. It is a reduced factorial monoid, and every $a \in \mathcal{F}(P)$ has a unique representation of the form

$$a = \prod_{p \in P} p^{\mathsf{v}_p(a)}, \quad \text{where } \mathsf{v}_p(a) \in \mathbb{N}_0 \text{ and } \mathsf{v}_p(a) = 0 \text{ for almost all } p \in P,$$

whence

$$|a| = \sum_{p \in P} \mathsf{v}_p(a) \in \mathbb{N}_0.$$

The monoid $\mathsf{Z}(H) = \mathcal{F}\big(\mathcal{A}(H_{\red})\big)$ is called the *factorization monoid* of H. The unique homomorphism $\pi \colon \mathsf{Z}(H) \to H_{\red}$ satisfying $\pi \mid \mathcal{A}(H_{\red}) = \id$ is called the *factorization homomorphism* of H. It is surjective if and only if H is atomic, and it is an isomorphism if and only if H is factorial. For $a \in H$, the elements in $\mathsf{Z}(a) = \pi^{-1}(aH^\times) \subset \mathsf{Z}(H)$ are called the *factorizations* of a, and $\mathsf{L}(a) = \{|z| \mid z \in \mathsf{Z}(a)\} \subset \mathbb{N}_0$ is called the *set of lengths* of a. For $k \in \mathbb{N}$ we set

$$\mathcal{F}_k(H) = \{a \in H \mid |\mathsf{Z}(a)| \le k\} \quad \text{and} \quad \mathcal{G}_k(H) = \{a \in H \mid |\mathsf{L}(a)| \le k\}.$$

Then $\mathcal{F}_k(H) \subset \mathcal{G}_k(H)$, and H is factorial if and only if it is atomic and $H = \mathcal{F}_1(H)$.

Block monoids. Let G be an additively written abelian group and $G_0 \subset G$ a subset. An element

$$S = \prod_{i=1}^{l} g_i = \prod_{g \in G_0} g^{\mathsf{v}_g(S)}$$

of the free abelian monoid $\mathcal{F}(G_0)$ is called a *sequence in G_0*. We denote by

- $|S| = l = \sum_{g \in G_0} \mathsf{v}_g(S) \in \mathbb{N}_0$ its *length*, by
- $\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g \in G_0} \mathsf{v}_g(S) g \in G$ its *sum*, and by
- $\Sigma(S) = \{\sum_{i \in I} g_i \mid \emptyset \ne I \subset [1, l]\} \subset G$ the *set of sums* of non-empty subsequences of S.

Then $\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \sigma(S) = 0\}$ is an atomic submonoid of $\mathcal{F}(G_0)$, called the *block monoid over G_0*. It is factorial if and only if $G_0 \setminus \{0\}$ is independent (see [6, Proposition 3]). Its elements are called *blocks* (or *zero-sum sequences*), its atoms are called *minimal zero-sum*

sequences and the identity element $1 \in \mathcal{B}(G_0)$ is also called the *empty sequence*. The sequence S is said to be *zero-sumfree*, if $0 \notin \Sigma(S)$. A sequence $T \in \mathcal{F}(G_0)$ is called a *subsequence of* S, if it is a divisor of S in the monoid $\mathcal{F}(G_0)$ (equivalently, $\mathsf{v}_g(T) \le \mathsf{v}_g(S)$ for all $g \in G_0$). Subsequences $T_1, \ldots, T_s$ of S are called *disjoint*, if their product is a divisor of S. For brevity, we set

$$\mathcal{A}(G_0) = \mathcal{A}\big(\mathcal{B}(G_0)\big), \ \mathcal{F}_k(G_0) = \mathcal{F}_k\big(\mathcal{B}(G_0)\big), \text{ and } \mathcal{G}_k(G_0) = \mathcal{G}_k\big(\mathcal{B}(G_0)\big).$$

Krull monoids. Let H be a reduced Krull monoid (see [14, Chapter 22]), $H \hookrightarrow D = \mathcal{F}(P)$ a divisor theory, $G = \{[a] \mid a \in D\}$ the class group of H and $G_0 = \{[p] \mid p \in P\} \subset G$ the set of classes containing primes. The block monoid $\mathcal{B}(G_0)$ is a reduced Krull monoid and the homomorphism $\boldsymbol{\beta}\colon H \to \mathcal{B}(G_0)$, defined by

$$\boldsymbol{\beta}(a) = \prod_{i=1}^{l} [p_i] \quad \text{for every} \quad a = \prod_{i=1}^{l} p_i \in H, \quad \text{where } p_1, \ldots, p_l \in P,$$

is called the *block homomorphism of* H. It is a transfer homomorphism (see [8]) and, among others, we have

$$\boldsymbol{\beta}\big(\mathcal{A}(H)\big) = \mathcal{A}(G_0) \quad \text{and} \quad \mathcal{G}_k(H) = \{a \in H \mid \boldsymbol{\beta}(a) \in \mathcal{G}_k(G)\}\,.$$

For every $k \in \mathbb{N}$ we define

$$\mathcal{B}_k(H) = \{a \in H \mid \boldsymbol{\beta}(a) \in \mathcal{F}_k(G)\}$$

and clearly

$$\mathcal{F}_k(H) \subset \mathcal{B}_k(H) \subset \mathcal{G}_k(H).$$

Let R be the ring of integers of an algebraic number field K, $\mathcal{I}^\bullet(R)$ the set of non-zero ideals of R and $H = \mathcal{H}(R)$ the set of non-zero principal ideals of R. Then H is a Krull monoid, the embedding $H \hookrightarrow \mathcal{I}^\bullet(R)$ is a divisor theory whose class group G is the usual ideal class group of R. Thus G is finite and every class contains a prime divisor. For $k \in \mathbb{N}$ and $x \in \mathbb{R}_{\ge 1}$, the functions

$$\begin{aligned} \mathcal{F}_k(x) &= |\{aR \in \mathcal{F}_k(H) \mid (R\colon aR) \le x\}|, \\ \mathcal{B}_k(x) &= |\{aR \in \mathcal{B}_k(H) \mid (R\colon aR) \le x\}| \quad \text{and} \\ \mathcal{G}_k(x) &= |\{aR \in \mathcal{G}_k(H) \mid (R\colon aR) \le x\}| \end{aligned}$$

are just the counting functions already discussed in the introduction. There is a general combinatorial machinery to tackle "block dependent" factorization properties. We introduce the necessary combinatorial terms (for a more general setting see [12, Section 4]).

Definition 2.1. Let G be a finite abelian group.

(1) For a subset $Q \subset G$ and a sequence $S \in \mathcal{F}(G \setminus Q)$, we set

$$\Omega(Q, S) = S\mathcal{F}(Q) \cap \mathcal{B}(G)\,,$$

and the pair (Q, S) is called a *k-system*, if $\emptyset \neq \Omega(Q, S) \subset \mathcal{F}_k(G)$.

(2) For every $k \in \mathbb{N}$, we define

$$\mathsf{b}_k(G) = \max\{|S| \,|\, Q \subset G \text{ with } Q \setminus \{0\} \text{ independent, } |Q| = 1 + \mathsf{r}^*(G), \text{ and } S \in \mathcal{F}(G \setminus Q) \text{ with } \emptyset \neq \Omega(Q, S) \subset \mathcal{F}_k(G)\}\,.$$

Note that for $|G| \le 2$ we have $\mathsf{b}_k(G) = 0$.

Proposition 2.2. *Let G be a finite abelian group with $|G| \ge 3$ and $k \in \mathbb{N}$.*

(1) *If (Q, S) is a k-system, then $Q \setminus \{0\}$ is independent.*
(2) *There exist finitely many k-systems (Q_i, S_i) with $i \in [1, m]$ such that*

$$\mathcal{F}_k(G) = \bigcup_{i=1}^{m} \Omega(Q_i, S_i).$$

(3) $\mathsf{b}_k(G) > 0$.

Proof. See [6], Proposition 3, Theorem 1 and Corollary 1. □

By Proposition 2.2.1 it is clear that

$$\mathsf{b}_k(G) = \max\{|S| \mid (Q, S) \text{ a } k\text{-system and } |Q| = 1 + \mathsf{r}^*(G)\}\,,$$

which is an alternative way to define $\mathsf{b}_k(G)$ (see [6, Definition 3]).

In the following theorem we summarize results on the asymptotic behavior of the functions $\mathcal{B}_k(x)$. The first part of the theorem is proved in [6, Theorem 2]. The second part is an immediate consequence of recent results obtained in [25, 24] building, among others, on results of [17, 16].

Theorem 2.3. *Let R be the ring of integers of an algebraic number field K, H the set of non-zero principal ideals, G the ideal class group with $|G| \ge 3$, and $k \in \mathbb{N}$.*

(1) *For $x \ge e^e$,*

$$\mathcal{B}_k(x) = x(\log x)^{-1+(1+\mathsf{r}^*(G))/|G|}\big(V_k(\log\log x) + O(\frac{(\log\log x)^M}{(\log x)^\gamma})\big)$$

with $V_k \in \mathbb{C}[X]$ a polynomial with positive leading coefficient and $\deg V_k = \mathsf{b}_k(G)$, $\gamma = \frac{1}{|G|}(1 - \cos\frac{2\pi}{|G|})$ and $M \in \mathbb{N}$ depends on k and K.

(2) *The error-term*

$$\mathcal{B}_k(x) - \frac{1}{2\pi i}\int_{\mathcal{C}} \zeta\big(s, \mathcal{B}_k(H)\big)\frac{x^s}{s}\,ds,$$

is subject to oscillations of positive lower logarithmic frequency and size $x^{\frac{1}{2}-\epsilon}$*, where*

$$\zeta\big(s, \mathcal{B}_k(H)\big) = \sum_{aR \in \mathcal{B}_k(H)} \frac{1}{(R\colon aR)^s} \quad \text{for} \quad \Re(s) > 1,$$

and the contour of integration $\mathcal{C}$ *goes counterclockwise around the points* $\frac{1}{2}$ *and* 1.

Proof. We briefly outline the argument.

1. By Proposition 2.2, $\mathcal{F}_k(G)$ is a finite union of k-systems. For a subset $Q \subset G$ and a sequence $S \in \mathcal{F}(G \setminus Q)$, the asymptotic behavior of the counting function

$$\Omega(Q,S)(x) = |\{aR \in H \mid \boldsymbol{\beta}(aR) \in \Omega(Q,S) \text{ and } (R\colon aR) \le x\}|$$

is studied in [15]. Combining these two results the assertion follows.

2. By [25, Theorem 1], it suffices to verify that the Mellin transform of the error-term fulfills certain conditions. (Note that in the terminology of [24] the result of [25, Theorem 1] can be expressed by saying, that the function is subject to oscillations of lower logarithmic frequency γ and size $x^{\theta-\epsilon}$.) Using again the decomposition of $\mathcal{F}_k(G)$, this can be done analogously as it was done in [24] for the functions $\mathcal{G}_k(x)$. Indeed, the technical results there, namely Theorem 6, Lemma 3 and Lemma 4, are formulated for counting functions $\Omega(Q,S)(x)$, and thus they can be applied immediately. Note that in order to apply [25, Theorem 6], we use that $\mathsf{b}_k(G)$ is positive. □

3. Auxiliary Results

In this section we recall respectively establish some auxiliary results.

Lemma 3.1. *Let* G *be a finite abelian group.*

1. *If* $G' \subset G$ *is a subgroup and* $k \in \mathbb{N}$*, then* $\mathsf{b}_k(G') \le \mathsf{b}_k(G)$.
2. *If* $G = G_1 \oplus G_2$ *and* $k_i \in \mathbb{N}$ *for* $i \in [1,2]$*, then* $\mathsf{b}_{k_1k_2}(G_1 \oplus G_2) \ge \mathsf{b}_{k_1}(G_1) + \mathsf{b}_{k_2}(G_2)$.

Proof. This is [6, Proposition 7], except for the cases $|G| \le 2$, and $|G_1| \le 2$ or $|G_2| \le 2$. However, the statements are obvious for $|G| \le 2$. And, if $|G_1| = 2$, say, then 2. follows from 1., since $G_2 \subset G$ and $\mathsf{b}_{k_1}(G_1) = 0$. □

In the following lemma we fix a subset $Q \subset G$ and compare factorization properties of the elements of $\Omega(Q,S)$ with those of $\Omega(Q,T)$ for a subsequence T of S.

Lemma 3.2. *Let* G *be a finite abelian group,* $Q \subset G$ *such that* $Q \setminus \{0\}$ *is independent,* $S_i \in \mathcal{F}(G \setminus Q)$ *and* $k_i \in \mathbb{N}$ *for* $i \in [1,2]$*. If* $\Omega(Q,S_i) \not\subset \mathcal{F}_{k_i}(G)$ *for* $i \in [1,2]$*, then*

$$\Omega(Q, S_1S_2) \not\subset \mathcal{F}_{k_1+k_2}(G).$$

In particular, if $S \in \mathcal{F}(G \setminus Q)$ *such that* $\Omega(Q,S) \neq \emptyset$ *and* T *a subsequence of* S *such that* $\Omega(Q,T) \not\subset \mathcal{F}_k(G)$ *for some* $k \in \mathbb{N}$, *then* $\Omega(Q,S) \not\subset \mathcal{F}_k(G)$.

Proof. If $\Omega(Q,S_i) \not\subset \mathcal{F}_{k_i}(G)$ for $i \in [1,2]$, then there exist blocks B_i with $|\mathsf{Z}(B_i)| \geq k_i + 1$ for $i \in [1,2]$. Since $B_1B_2 \in \Omega(Q,S_1S_2)$ and $|\mathsf{Z}(B_1B_2)| \geq |\mathsf{Z}(B_1)| + |\mathsf{Z}(B_2)| - 1 \geq k_1 + k_2 + 1$, the result follows. The 'in particular'-statement follows by noting that $\Omega(Q,S) \neq \emptyset$ is equivalent to $\Omega(Q,S) \not\subset \mathcal{F}_0(G)$, and $\Omega(Q,T^{-1}S) \neq \emptyset$ if both $\Omega(Q,S)$ and $\Omega(Q,T)$ are non-empty. □

4. Elementary Groups

A finite abelian group, G, is called *elementary* if every element in G has squarefree order, i.e., G is equal to a direct sum of cyclic groups of prime order. Also, elementary groups are characterized by the property that every subgroup is a direct summand. Thus for elementary groups maximal independent sets are necessarily generating. This fact simplifies the investigations considerably and allows us to determine the value of $\mathsf{b}_k(G)$ for elementary groups. Namely, we show (see Theorem 4.2) that equality holds at the lower bound (implicitly) obtained in [6].

First we introduce some additional notation and recall basic facts. Let $E = \{e_1, \ldots, e_r\} \subset G$ be an independent generating set. For each $g \in G$ there exist uniquely determined coordinates $b_i \in [0, \mathrm{ord}(e_i) - 1]$ for $i \in [1,r]$ such that $g = -\sum_{i=1}^r b_i e_i$, and if $g \notin E$, there exists a uniquely determined atom $A_g \in \mathcal{A}(\{g\} \cup E)$ with $\mathsf{v}_g(A_g) = 1$, namely $A_g = g \prod_{i=1}^r e_i^{b_i}$ (see [27] for more general results of this type). For $i \in [1,r]$ let $\pi_i : G \to \langle e_i \rangle$ denote the projection, with respect to $\{e_1, \ldots, e_r\}$, on the i-th coordinate.

Proposition 4.1. *Let* G *be a finite abelian group with* $|G| \geq 3$. *Further, let* $\{e_1, \ldots, e_r\}$ *be an independent generating set,* $r_2 = \{i \in [1,r] \mid \mathrm{ord}(e_i) = 2\}$, *and* $Q = \{e_1, \ldots, e_r\} \cup \{0\}$. *If* $S \in \mathcal{F}(G \setminus Q)$ *and*

$$|S| > \sum_{i=1}^r (\mathrm{ord}(e_i) - 1) - \left\lceil \frac{r_2}{2} \right\rceil,$$

then there exists a subsequence T *of* S *with* $|T| \leq \max\{\mathrm{ord}(e_i) \mid i \in [1,r]\}$ *and* $\Omega(Q,T) \not\subset \mathcal{F}_1(G)$.

Proof. We start with the following immediate observations. For each $h \in G \setminus Q$, since $h \neq 0$, there exists some $i \in [1,r]$ with $\pi_i(h) \neq 0$. Moreover, if $j \in [1,r]$ and $\mathrm{ord}(e_j) = 2$, since $h \notin \{0, e_j\}$, there exists some $i \in [1,r] \setminus \{j\}$ with $\pi_i(h) \neq 0$.

Let $S \in \mathcal{F}(G \setminus Q)$ with $|S| > \sum_{i=1}^r (\mathrm{ord}(e_i) - 1) - \left\lceil \frac{r_2}{2} \right\rceil$. By our above considerations it follows that there exists some $\iota \in [1,r]$ and a subsequence T of S such that $\pi_\iota(g) \neq 0$ for each $g|T$ and $|T| \geq \mathrm{ord}(e_\iota)$. We consider the block $B = \prod_{g|T} A_g^{\mathsf{v}_g(T)}$. Clearly, $B \in \Omega(Q,T)$. For each

$g|T$ we have $e_\iota|A_g$, and $|T| \ge \mathrm{ord}(e_\iota)$. Thus it follows that $e_\iota^{\mathrm{ord}(e_\iota)}|B$. Consequently, B has at least two different factorizations into atoms and $\Omega(Q,T) \not\subset \mathcal{F}_1(G)$. □

Theorem 4.2. *Let $k \in \mathbb{N}$ and $G = \oplus_{i=1}^r C_{p_i}$ be an elementary group with $|G| \ge 3$. Then*

$$\mathsf{b}_k(G) = (k-1)\max\{p_i \mid i \in [1,r]\} + \sum_{i=1}^r (p_i - 1) - \left\lceil \frac{\mathsf{r}_2(G)}{2} \right\rceil .$$

Proof. Without restriction assume $p_1 \le \cdots \le p_r$. We set $s = \mathsf{r}_2(G)$.

First we prove that the expression on the right hand side is a lower bound for $\mathsf{b}_k(G)$. In case $s = r$, i.e., $G = C_2^r$, the statement is just [6, Proposition 9]. Thus assume $s < r$. By repeated application of Lemma 3.1.2 we have that

$$\mathsf{b}_k(G) \ge \mathsf{b}_1(C_2^s) + \sum_{j=s+1}^{r-1} \mathsf{b}_1(C_{p_j}) + \mathsf{b}_k(C_{p_r}).$$

The result follows since $\mathsf{r}_2(G) = s$ by definition, $\mathsf{b}_1(C_2^s) = \left\lfloor \frac{s}{2} \right\rfloor$ by [6, Proposition 9], and $\mathsf{b}_k(C_p) = kp - 1$ for $p \ge 3$ by [6, Proposition 8].

We proceed to prove that the expression is an upper bound. This is done by induction on k. Let $Q \subset G$ with $|Q| = 1 + \mathsf{r}^*(G)$ such that $Q \setminus \{0\}$ is independent. Note that since G is elementary, Q is a generating set and the orders of the elements of Q are uniquely determined.

Let $k = 1$ and $S \in \mathcal{F}(G \setminus Q)$ with $|S| > \sum_{i=1}^r (p_i - 1) - \left\lceil \frac{\mathsf{r}_2(G)}{2} \right\rceil$ such that $\Omega(Q,S) \ne \emptyset$. By Proposition 4.1 there exists a subsequence T of S with $|T| \le p_r$ and $\Omega(Q,T) \not\subset \mathcal{F}_1(G)$. The result follows by Lemma 3.2.

Let $k \ge 2$ and $S \in \mathcal{F}(G \setminus Q)$ with $|S| > (k-1)p_r + \sum_{i=1}^r (p_i - 1) - \left\lceil \frac{\mathsf{r}_2(G)}{2} \right\rceil$. Again by Proposition 4.1 there exists a subsequence $T|S$ with $|T| \le p_r$ and $\Omega(Q,T) \not\subset \mathcal{F}_1(G)$. By induction hypothesis $\Omega(Q, T^{-1}S) \not\subset \mathcal{F}_{k-1}(G)$ and the result follows by Lemma 3.2. □

5. Cyclic groups of prime power order

We start with a technical lemma. We use the following notations. For subsets $A_1, \ldots, A_s \subset G$ and $n \in \mathbb{N}$ we set $\sum_{i=1}^s A_i = \{\sum_{i=1}^s a_i \mid a_i \in A_i\}$, but $nA = \{na \mid a \in A\}$ and not the n-fold sum of A.

Lemma 5.1. *Let G be a cyclic group of prime power order p^m with $m \ge 2$. If $S \in \mathcal{F}(G \setminus \{0\})$ and $|S| \ge 2p - 1$, then there exists a zero-sumfree subsequence T of S with $|T| \le p$ such that $\sigma(T) \in p\,G \setminus \{0\}$.*

Proof. Let $S \in \mathcal{F}(G \setminus \{0\})$ and $|S| = 2p-1$. We assume $S \in \mathcal{F}(G \setminus p\,G)$, since otherwise the result follows by setting $T = g$ with $g \in p\,G \setminus \{0\}$. Further, let $\pi : G \to G/p\,G$ denote the canonical projection.

We note that it suffices to show that there exists a subsequence T of S such that $\sigma(T) \in p\,G \setminus \{0\}$. Suppose T is such a sequence. Then

$\pi(T) \in \mathcal{F}(G/pG)$, the sequence obtained by projecting each element of T, is a zero-sum sequence. We consider its factorization into atoms, say $U_1, \ldots, U_s$ are sequences such that $\prod_{i=1}^s U_i = T$ and $\pi(U_i)$ is an atom for each $i \in [1, s]$. It follows that U_i is zero-sumfree and $|U_i| \le p$ for each $i \in [1, s]$, and since $\sigma(T) \neq 0$, there exists some $j \in [1, s]$ such that $\sigma(U_j) \neq 0$.

We assert that for every $R \in \mathcal{F}(G \setminus pG)$ we have $|\Sigma(R) \cup \{0\}| \ge \min\{|R|+1, p^m\}$ and $|\Sigma(\pi(R)) \cup \{0\}| \ge \min\{|R|+1, p\}$. Let $R = \prod_{i=1}^r g_i$ and for each $j \in [1, r]$ we set $A_j = \sum_{i=1}^j \{0, g_i\}$. We have $|A_1| = |\pi(A_1)| = 2$. By I. Chowla's theorem (see for example [21, Theorem 2.1]) it follows for each $j \in [2, r]$ that $|A_j| \ge \min\{|A_{j-1}| + 1, p^m\}$ and $|\pi(A_j)| \ge \min\{|\pi(A_{j-1})| + 1, p\}$, thus $|A_j| \ge \min\{j+1, p^m\}$ and $|\pi(A_j)| \ge \min\{j+1, p\}$. Since $\Sigma(R) \cup \{0\} = A_r$ and $\Sigma(\pi(R)) \cup \{0\} = \pi(A_r)$, the assertion follows.

Let $S = S_1 S_2$ with $|S_1| = p$ and $|S_2| = p - 1$. Since $|\Sigma(S_1) \cup \{0\}| \ge p + 1 > |G/pG|$, there exist two, possibly empty and not necessarily disjoint, subsequences T_1, T_1' of S_1 such that $\pi(\sigma(T_1)) = \pi(\sigma(T_1'))$ but $\sigma(T_1) \neq \sigma(T_1')$. Moreover, since $\Sigma(\pi(S_2)) \cup \{0\} = G/pG$, there exists a subsequence T_2 of S_2, such that $\pi(\sigma(T_2)) = -\pi(\sigma(T_1))$. We have $\sigma(T_1T_2), \sigma(T_1'T_2) \in pG$ and $\sigma(T_1T_2) \neq \sigma(T_1'T_2)$, thus setting $T = T_1T_2$ or $T = T_1'T_2$ the result follows. □

As the following example shows the value $2p - 1$ in Lemma 5.1 is best possible.

Example 5.2. Let G be as in Lemma 5.1. The sequence $(-g)^{p-1}g^{p-1}$, for some generating element $g \in G$, has length $2p - 2$ and no subsequence with sum in $pG \setminus \{0\}$.

The following proposition will be the main tool in the proofs of Theorems 5.4 and 6.1.

Proposition 5.3. *Let G be cyclic of prime power order p^m with $m \ge 2$ and $S \in \mathcal{F}(G \setminus \{0\})$ with $|S| \ge p^m + p^{m-1} - 1$. For each $n \in [1, m-1]$, there exist $p^{m-n} + p^{m-n-1} - 1$ disjoint, zero-sumfree subsequences T of S with $|T| \le p^n$ and $\sigma(T) \in p^n G \setminus \{0\}$.*

Proof. Let $S \in \mathcal{F}(G \setminus \{0\})$ and $|S| \ge p^m + p^{m-1} - 1$. We prove the result by induction on n. Let $n = 1$. We note that

$$p^m + p^{m-1} - 1 = (p^{m-1} + p^{m-2} - 2)p + 2p - 1.$$

Thus the result follows be repeated application of Lemma 5.1. Let $n \ge 2$. By induction hypothesis we know that there exist disjoint zero-sumfree subsequences T_i of S with $|T_i| \le p^{n-1}$ and $\sigma(T_i) \in p^{n-1}G \setminus \{0\}$ for each $i \in [1, p^{m-n+1} + p^{m-n} - 1]$. Let S' denote the sequence formed by the $\sigma(T_i)$. The sequence S' is a sequence in $p^{n-1}G \setminus \{0\}$. Since $p^{n-1}G$ is a cyclic group with p^{m-n+1} elements and $|S'| = p^{m-n+1} + p^{m-n} - 1$,

we can apply the result for '$n = 1$' to the group $p^{n-1}G$ and obtain that there exists for $i \in [1, p^{m-n} + p^{m-n-1} - 1]$ disjoint subsets $J_i \subset [1, p^{m-n+1} + p^{m-n} - 1]$ such that $|J_i| \le p$, the sequence $\prod_{j \in J_i} \sigma(T_j)$ is zero-sumfree and $\sigma(\prod_{j \in J_i} \sigma(T_j)) \in p(p^{n-1}G) \setminus \{0\}$. We consider the sequences $\prod_{j \in J_i} T_j$ for $i \in [1, p^{m-n} + p^{m-n-1} - 1]$. Clearly, these are disjoint subsequences of S. For the length we have $|\prod_{j \in J_i} T_j| \le |J_i| p^{n-1} \le p^n$ and for the sum $\sigma(\prod_{j \in J_i} T_j) = \sigma(\prod_{j \in J_i} \sigma(T_j)) \in p^n G \setminus \{0\}$. We factorize $\prod_{j \in J_i} T_j = S_i B_i$ where B_i is a zero-sum sequence, possibly the empty sequence, and S_i is zero-sumfree. It follows immediately that $|S_i| \le p^n$ and $\sigma(S_i) \in p^n G \setminus \{0\}$ for each $i \in [1, p^{m-n} + p^{m-n-1} - 1]$. □

Now we are ready to prove the main result of this section.

Theorem 5.4. *Let $k \in \mathbb{N}$ and G be a cyclic group of prime power order p^m. Then*

$$\mathsf{b}_k(G) = kp^m + p^{m-1} - 2.$$

Proof. For $m = 1$ the result is a special case of [6, Proposition 8] (or Theorem 4.2), thus we assume $m \ge 2$. Let $g \in G$ be a generating element, $Q = \{0, p^{m-1}g\}$ and $S = (-g)^{kp^m - 1} g^{p^{m-1} - 1}$. We assert that $\emptyset \ne \Omega(Q, S) \subset \mathcal{F}_k(G)$. This proves the lower bound. First we determine the atoms $A \in \mathcal{A}(\{0, g, -g, p^{m-1}g\})$ that satisfy $\mathsf{v}_g(A) \le p^{m-1} - 1$ and $\mathsf{v}_{-g}(A) \le kp^m - 1$, i.e., can occur in a factorization of a block in $\Omega(Q, S)$. If A is an atom with $\mathsf{v}_g(A) > 0$ and $\mathsf{v}_{-g}(A) > 0$, then clearly $A = (-g)g$. Since there cannot exist a zero-sum sequence $g^j (p^{m-1}g)^k$ with $0 < j < p^{m-1}$, it follows that 0, $(-g)^{p^{m-1}}(p^{m-1}g)$, $(-g)^{p^m}$, $(p^{m-1}g)^p$ and $(-g)g$ are the only atoms with the prescribed properties.

Since $\sigma(S) = p^{m-1}g$, it follows that $\Omega(Q, S)$ is non-empty. Let $B \in \Omega(Q, S)$ and let $B = \prod_{i=1}^{l} U_i$ be a factorization into atoms. It follows that exactly $p^{m-1} - 1$ of the atoms are equal to $(-g)g$. Thus it suffices to consider blocks in $\Omega(Q, (-g)^{kp^m - p^{m-1}})$. Let B' be such a block and $\prod_{i=1}^{n} V_i$ a factorization into atoms. We have that

$$V_i \in \{0, (-g)^{p^{m-1}}(p^{m-1}g), (-g)^{p^m}, (p^{m-1}g)^p\}$$

for each $i \in [1, n]$. Thus the factorization is determined by giving the number ν of $i \in [1, n]$ such that $V_i = (-g)^{p^m}$. Clearly, $\nu \in [0, k-1]$ and therefore $|\mathsf{Z}(B')| \le k$.

We prove the upper bound by induction on k. First we prove a preparatory assertion. Let $\{0\} \subset Q \subset G$ with $|Q| = 2$ and $S \in \mathcal{F}(G \setminus Q)$ with $|S| > p^m + p^{m-1} - 2$. Then there exists a subsequence T of S with $|T| \le p^m$ such that $\Omega(Q, T) \not\subset \mathcal{F}_1(G)$.

We have $Q = \{0, p^l g\}$ for some generating element $g \in G$ and $l \in [0, p-1]$. We apply Proposition 5.3 with $n = m - 1$ and obtain that there exist p disjoint subsequences $T_1, \ldots, T_p$ of S such that $|T_i| \le p^{m-1}$

and $\sigma(T_i) \in p^{m-1}G \setminus \{0\}$ for each $i \in [1,p]$. Let $b_i \in [1,p-1]$ such that $\sigma(T_i) = -b_i p^{m-1} g$ and we set

$$B_i = T_i (p^l g)^{b_i p^{m-1-l}}.$$

We set $T = \prod_{i=1}^p T_i$ and $B = \prod_{i=1}^p B_i$. Since $B \in \Omega(Q,T)$, it suffices to show that $|\mathsf{Z}(B)| > 1$. We have $\sum_{i=1}^p b_i \ge p$ and therefore $(p^l g)^{p^{m-l}} \mid B$. On the other hand we note that $(p^l g)^{p^{m-l}} \nmid B_i$. Thus there exists a factorization of B, in which the atom $(p^l g)^{p^{m-l}}$ does not occur. This implies that there exist at least two different factorizations of B and proves the assertion.

The inductive argument is a simple application of our assertion and Lemma 3.2. For $k = 1$ the statement is now obvious. Let $k \ge 2$ and further let $\{0\} \subset Q \subset G$ with $|Q| = 2$ and $S \in \mathcal{F}(G \setminus Q)$ with $|S| > kp^m + p^{m-1} - 2$ such that $\Omega(Q,S) \ne \emptyset$. By our assertion there exists a subsequence T of S with $|T| \le p^m$ and $\Omega(Q,T) \not\subset \mathcal{F}_1(G)$. It follows that $|T^{-1}S| > (k-1)p^m + p^{m-1} - 2$ and $\Omega(Q, T^{-1}S) \ne \emptyset$. Thus by induction hypothesis $\Omega(Q, T^{-1}S) \not\subset \mathcal{F}_{k-1}(G)$ and by Lemma 3.2 this implies $\Omega(Q,S) \not\subset \mathcal{F}_k(G)$. □

6. A Further Class of Groups

In the following theorem we show that a combination of Theorem 4.2 and Theorem 5.4, respectively the proofs, can be used to determine $\mathsf{b}_k(G)$ for groups that are direct sums of an elementary and a cyclic group of prime power order (with the restriction that the orders of the two direct summands have to be co-prime).

Theorem 6.1. *Let $k \in \mathbb{N}$, G' be an elementary group and $G = C_{p^m} \oplus G'$ with $p \nmid |G'|$. Then*

$$\mathsf{b}_k(G) = (k-1)\max\{p^m, p'\} + \mathsf{b}_1(C_{p^m}) + \mathsf{b}_1(G'),$$

where $p' = \max\{\overline{p} \in \mathbb{P} \mid \overline{p} \mid |G'|\}$.

Proof. By Lemma 3.1.2 we have

$$\mathsf{b}_k(G) \ge \max\{\mathsf{b}_k(C_{p^m}) + \mathsf{b}_1(G'), \mathsf{b}_1(C_{p^m}) + \mathsf{b}_k(G')\}$$

and thus by Theorem 4.2 and Theorem 5.4 we have $\mathsf{b}_k(G) \ge (k-1)\max\{p^m, p'\} + \mathsf{b}_1(C_{p^m}) + \mathsf{b}_1(G')$. Since for $m = 1$ the group G is elementary, we can assume $m \ge 2$.

Let $\{e_0, e_1, \ldots, e_r\}$ be an independent generating set of G with maximal cardinality and such that $\langle e_0 \rangle = C_{p^m}$ and $\langle \{e_1, \ldots, e_r\} \rangle = G'$. Let $\{0\} \subset Q \subset G$ such that $|Q| = 1 + \mathsf{r}^*(G)$ and $Q \setminus \{0\}$ is independent.

For each $g \in Q \setminus \{0\}$, since $\mathrm{ord}(g)$ is a prime power and $p \nmid |G'|$, we have $g = ae_0$ for some $a \in \mathbb{N}$ or $g \in G'$. Therefore we may assume, possibly after replacing e_0 by $a'e_0$ with $a' \in \mathbb{N}$ co-prime to p, that $Q = \{p^l e_0\} \cup Q'$ with $l \in [0, m-1]$ and $Q' \subset G'$. We have $Q' \setminus \{0\}$ is

independent with maximal cardinality $\mathsf r^*(G')$. Since G' is an elementary group, it follows that $\langle Q' \rangle = G'$.

We consider $k = 1$ and prove a slightly more general statement in order to be able to prove the general case with an inductive argument.

Let $S \in \mathcal F(G \setminus Q)$ with $|S| > \mathsf b_1(C_{p^m}) + \mathsf b_1(G')$ and $\Omega(Q, S) \neq \emptyset$. We show that there exists a subsequence $\overline{T}$ of S such that $\Omega(Q, \overline{T}) \not\subset \mathcal F_1(G)$ and $|\overline{T}| \le \max\{p^m, p'\}$.

Every $g \in G$ has a unique representation $g = c_g + h_g$ with $c_g = \pi_0(g) \in C_{p^m}$ and $h_g \in G'$. We consider the subsequence T of S of those elements $g|S$ with $\pi_0(g) = 0$. Note that if $|G'| = 2$, then, since $g \notin Q$, it follows that T is the empty sequence.

We distinguish two cases.

Case 1: $|T| > \mathsf b_1(G')$. Since $T \in \mathcal F(G' \setminus Q')$ with $|T| > \mathsf b_1(G')$, it follows by Proposition 4.1 and Theorem 4.2 that there exists a subsequence $\overline{T'}$ of T with $|\overline{T'}| \le p'$ such that $\emptyset \neq \Omega(Q', \overline{T'}) \not\subset \mathcal F_1(G')$. Since $\mathcal F_1(G') = \mathcal B(G') \cap \mathcal F_1(G)$ and $\Omega(Q', \overline{T'}) \subset \Omega(Q, \overline{T'})$, this implies, using Lemma 3.2, that $\Omega(Q, \overline{T}) \not\subset \mathcal F_1(G)$.

Case 2: $|T| \le \mathsf b_1(G')$. Then $|T^{-1}S| > \mathsf b_1(C_{p^m})$. We consider the projection $R = \pi_0(T^{-1}S)$, the sequence in C_{p^m} obtained by applying π_0 to each element of $T^{-1}S$. We note that if $\pi_0(g) = p^l e_0$, then $h_g \neq 0$. The argument is now almost the same as in the proof of Theorem 5.4. Note that in Proposition 5.3 the only condition on the sequence is that the elements are non-zero, thus the possible occurrence of $p^l e_0$ in R causes no problem. We obtain that there exist disjoint subsequences $T_1, \ldots, T_p$ of R such that $|T_i| \le p^{m-1}$ and $\sigma(T_i) \in p^{m-1} C_{p^m} \setminus \{0\}$ for each $i \in [1, p]$. Let $b_i \in [1, p-1]$ such that $\sigma(T_i) = -b_i p^{m-1} e_0$ and we set

$$B_i = T_i (p^l g)^{b_i p^{m-1-l}}.$$

Let $\overline{T_i}$ denote the subsequence of $T^{-1}S$ such that T_i is obtained by projection of $\overline{T_i}$. The sequence $\overline{T}_i (p^l g)^{b_i p^{m-1-l}}$ is in general no zero-sum sequence. However, there exists a uniquely determined zero-sumfree sequence $F_i \in \mathcal F(Q')$ such that $\overline{B_i} = F_i \overline{T}_i (p^l g)^{b_i p^{m-1-l}}$ is a zero-sum sequence. We set $\overline{T} = \prod_{i=1}^p \overline{T}_i$ and $B = \prod_{i=1}^p \overline{B}_i$. Clearly, we have $|\overline{T}| \le p^m$. Since $B \in \Omega(Q, \overline{T})$, it suffices to show that $|\mathsf Z(B)| > 1$. This follows since $(p^l g)^{p^{m-l}} \mid B$ but $(p^l g)^{p^{m-l}} \nmid \overline{B}_i$.

This proves the result for $k = 1$ and the result for general k follows by Lemma 3.2 and the usual inductive argument, as in the proofs of Theorem 4.2 and 5.4. □

7. Lower Bounds

In Theorem 7.1 we establish lower bounds for $\mathsf b_k(G)$ valid for arbitrary finite abelian groups. Then, in Example 7.2, we compare these bounds for cyclic groups.

First, we recall the definition of Davenport's constant and some results. For a finite abelian group G Davenport's constant, $\mathsf{D}(G)$, is defined as the maximal length of a minimal zero-sum sequence, i.e., $\mathsf{D}(G) = \max\{|A| \mid A \in \mathcal{A}(G)\}$.

Let $G \cong \oplus_{i=1}^r C_{n_i}$ with $1 < n_1 | \ldots | n_r$. Then

$$(\dagger) \qquad \mathsf{D}(G) \ge 1 + \sum_{i=1}^{r} (n_i - 1)$$

and it is known that equality holds if $r \le 2$ or n_r is a prime power (i.e., G is a p-group) (see [29, 22, 23]). However, it is also known that equality in Equation (†) does not hold in general. More precisely, for each $r \ge 4$ there are known infinitely many groups with rank r such that equality does not hold (see [11]) and the problem to determine $\mathsf{D}(G)$ in general is wide open. It is even open whether for groups with rank 3 equality holds in (†) or not (see [3, 1] for recent results).

Theorem 7.1. *Let $G = \oplus_{i=1}^r C_{p_i^{m_i}}$ with prime powers $p_i^{m_i}$ and $|G| \ge 3$.*

(1) *Let $k \in \mathbb{N}$ and $r_2 = |\{i \in [1,r] \mid p_i^{m_i} = 2\}|$. Then*

$$\mathsf{b}_k(G) \ge (k-1) \max\{p_i^{m_i} \mid i \in [1,r]\} + \sum_{i=1}^{r} (p_i^{m_i} + p_i^{m_i - 1} - 2) - \left\lceil \frac{r_2}{2} \right\rceil .$$

(2) $\mathsf{b}_1(G) \ge \mathsf{D}(\oplus_{i=1}^r C_{p_i^{m_i-1}})$.

Proof. 1. The result follows by Lemma 3.1.2, Theorem 4.2 and Theorem 5.4.

2. Let $\{e_1, \ldots, e_r\} \subset G$ be an independent generating set with $\mathrm{ord}(e_i) = p_i^{m_i}$ for each $i \in [1,r]$. Further, let $Q = \{0\} \cup \{p_i^{m_i-1} e_i \mid i \in [1,r]\}$ and $G' = \langle Q \rangle$. We note that $|Q| = 1 + \mathsf{r}^*(G)$ and $G/G' \cong \oplus_{i=1}^r C_{p_i^{m_i-1}}$.

First we show that there exists a sequence $S \in \mathcal{F}(G \setminus Q)$ with $|S| = \mathsf{D}(G/G')$ such that $\sigma(S) \in G'$ but $\sigma(T) \notin G'$ for every proper $1 \ne T | S$. If $\mathsf{D}(G/G') = 1$, we set $S = g$ for some $g \in G \setminus Q$. Thus we assume $\mathsf{D}(G/G') \ge 2$. By definition of $\mathsf{D}(G/G')$ there exists a minimal zero-sum sequence $\overline{S} = \prod_{i=1}^l \overline{g}_i \in \mathcal{F}(G/G')$ with $|\overline{S}| = \mathsf{D}(G/G')$. Let $S \in \mathcal{F}(G)$ such that $\overline{S}$ is the projection of S, i.e., $S = \prod_{i=1}^l g_i$ such that $g_i + G' = \overline{g}_i$ for each $i \in [1,l]$. Since $\sigma(\overline{S}) = 0 \in G/G'$, we have $\sigma(S) \in G'$, and since $\overline{S}$ is a minimal zero-sum sequence, we have $\sigma(T) \notin G'$ for each proper $1 \ne T | S$. Since $\mathsf{D}(G/G') \ge 2$, it follows that $S \in \mathcal{F}(G \setminus G') \subset \mathcal{F}(G \setminus Q)$.

It suffices to show that $\emptyset \ne \Omega(Q, S) \subset \mathcal{F}_1(G)$. The set $Q \setminus \{0\}$ is independent and generates G', thus there exists for every $h \in G'$ a uniquely determined zero-sumfree sequence $F \in \mathcal{F}(Q)$ with $\sigma(F) = h$ (for $h = 0$ this is the empty sequence). Since $\sigma(S) \in G'$, it is clear that $\Omega(Q, S) \ne \emptyset$. Let $B \in \Omega(Q, S)$ and $B = \prod_{i=0}^n U_i$ a factorization into atoms. Without restriction let $U_0 \notin \mathcal{A}(Q)$. Thus $U_0 = S'F'$ with

$1 \neq S' | S$ and $F' \in \mathcal{F}(Q)$. It follows that $\sigma(S') \in G'$ and therefore $S' = S$. Moreover, F' is zero-sumfree and thus uniquely determined. Since $U_0^{-1}B \in \mathcal{B}(Q)$ and $\mathcal{B}(Q)$ is factorial, the atoms $U_1, \ldots, U_n$ are uniquely determined as well and $|\mathsf{Z}(B)| = 1$. □

The following example shows that there exist groups for which the bound in 1. yields better estimates than the one in 2., and vice versa.

Example 7.2. Let $n = \prod_{i=1}^r p_i^{m_i}$ with $m_i \in \mathbb{N}$ and different primes p_i. First we note that if $p_i^{m_i} = 2$ for some $i \in [1, r]$, then the lower bounds for C_n are equal to those for $C_{\frac{n}{2}}$. Thus we assume that $p_i^{m_i} \neq 2$ for $i \in [1, r]$.

By Proposition 7.1.1 we get

$$\mathsf{b}_1(C_n) \geq \sum_{i=1}^r (p^{m_i} + p^{m_i - 1} - 2)$$

but 2. yields

$$\mathsf{b}_1(C_n) \geq \mathsf{D}(\oplus_{i=1}^r C_{p_i^{m_i-1}}) = \mathsf{D}(C_{\prod_{i=1}^r p_i^{m_i-1}}) = \prod_{i=1}^r p_i^{m_i-1}.$$

Thus depending on n either the former or the latter estimate is better.

References

[1] S.T. Chapman, M. Freeze, W.D. Gao, and W.W. Smith. On Davenport's constant of finite abelian groups. *Far East J. Math. Sci. (FJMS)*, 5(1):47–54, 2002.

[2] S.T. Chapman, editor. *Arithmetical Properties of Commutative Rings and Monoids*. Lecture Notes in Pure and Applied Mathematics, Marcel Dekker Inc., New York, to appear.

[3] W.D. Gao. On Davenport's constant of finite abelian groups with rank three. *Discrete Math.*, 222(1-3):111–124, 2000.

[4] W.D. Gao. On a combinatorial problem connected with factorizations. *Colloq. Math.*, 72(2):251–268, 1997.

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

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

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

[8] A. Geroldinger and F. Halter-Koch. Transfer principles in the theory of nonunique factorization, In [2].

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

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

[11] A. Geroldinger and R. Schneider. On Davenport's constant. *J. Combin. Theory Ser. A*, 61(1):147–152, 1992.

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

[13] F. Halter-Koch. Factorization problems in class number two. *Colloq. Math.*, 65(2):255–265, 1993.
[14] F. Halter-Koch. *Ideal systems*, volume 211 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 1998.
[15] J. Kaczorowski. Some remarks on factorization in algebraic number fields. *Acta Arith.*, 43(1):53–68, 1983.
[16] J. Kaczorowski and A. Perelli. Functional independence of the singularities of a class of Dirichlet series. *Amer. J. Math.*, 120(2):289–303, 1998.
[17] J. Kaczorowski and J. Pintz. Oscillatory properties of arithmetical functions. II. *Acta Math. Hungar.*, 49(3-4):441–453, 1987.
[18] W. Narkiewicz. Finite abelian groups and factorization problems. *Colloq. Math.*, 42:319–330, 1979.
[19] W. Narkiewicz and J. Śliwa. Finite abelian groups and factorization problems. II. *Colloq. Math.*, 46(1):115–122, 1982.
[20] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer-Verlag, Berlin, third edition, 2004.
[21] M.B. Nathanson. *Additive number theory*, volume 165 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.
[22] J.E. Olson. A combinatorial problem on finite Abelian groups. I. *J. Number Theory*, 1:8–10, 1969.
[23] J.E. Olson. A combinatorial problem on finite Abelian groups. II. *J. Number Theory*, 1:195–199, 1969.
[24] M. Radziejewski. On the distribution of algebraic numbers with prescribed factorization properties.
[25] M. Radziejewski. Oscillations of error terms associated with certain arithmetical functions. *Monatsh. Math.*, 2004.
[26] M. Radziejewski and W.A. Schmid. On the assymptotic behavior of some counting functions.
[27] W.A. Schmid. Arithmetic of block monoids. *Math. Slovaca*, to appear.
[28] W.A. Schmid. On the assymptotic behavior of some counting functions, II.
[29] P. van Emde Boas and D. Kruyswijk. A combinatorial problem on finite abelian groups. III. Technical report, Math. Centrum, Amsterdam, Afd. zuivere Wisk. ZW 1969-008, 34 p. , 1969.

Institute for Mathematics and Scientific Computing, University of Graz, Heinrichstrasse 36, 8010 Graz, Austria
E-mail address: wolfgang.schmid@uni-graz.at