Journal of Combinatorics and Number Theory
JCNT 2009, Volume 1, Issue # 2, pp. 9-26
ISSN 1942-5600

ON THE STRUCTURE OF MINIMAL ZERO-SUM SEQUENCES WITH MAXIMAL CROSS NUMBER

Alfred Geroldinger[*] *and David J. Grynkiewicz*[†]
Institut für Mathematik und Wissenschaftliches Rechnen
Karl-Franzens-Universität Graz
Heinrichstraße 36
8010 Graz, Austria

Abstract

Let G be an additive finite abelian group, $S = g_1 \cdot \ldots \cdot g_l$ a sequence over G and $\mathsf{k}(S) = \mathrm{ord}(g_1)^{-1} + \ldots + \mathrm{ord}(g_l)^{-1}$ its cross number. Then the cross number $\mathsf{K}(G)$ of G is defined as the maximal cross number of all minimal zero-sum sequences over G. In the spirit of inverse additive number theory, we study the structure of those minimal zero-sum sequences S over G whose cross number equals $\mathsf{K}(G)$. These questions are motivated by applications in the theory of non-unique factorizations.

2000 Mathematics Subject Classification: 11P70, 11B50.

Key words and phrases: Inverse zero-sum problems, minimal zero-sum sequences, cross number.

1 Introduction

Let G be an additively written finite abelian group, $G = C_{q_1} \oplus \ldots \oplus C_{q_s}$ its direct decomposition into cyclic groups of prime power order, $\exp(G)$ its exponent, and set

$$\mathsf{k}^*(G) = \sum_{i=1}^{s} \frac{q_i - 1}{q_i} \quad \text{and} \quad \mathsf{K}^*(G) = \frac{1}{\exp(G)} + \mathsf{k}^*(G)\,.$$

Note $\mathsf{k}^*(G) = 0$ and $\mathsf{K}^*(G) = 1$ for G trivial. For a sequence $S = g_1 \cdot \ldots \cdot g_l$ over G,

$$\mathsf{k}(S) = \sum_{i=1}^{l} \frac{1}{\mathrm{ord}(g_i)} \in \mathbb{Q}$$

is the cross number of S, and

$$\mathsf{K}(G) = \max\{\mathsf{k}(S) \mid S \text{ is a minimal zero-sum sequence over } G\}$$

Received August 12, 2008; Revised November 14, 2008
[*]E-mail address: alfred.geroldinger@uni-graz.at
[†]E-mail address: diambri@hotmail.com

denotes the cross number of the group G. It was introduced by U. Krause in 1984 (see [18], [19]) and since that time was studied under various aspects (see [17, 6, 7, 10, 2, 11, 1, 4]). The cross number may be viewed as a special weighted version of the Davenport constant. Its relevance stems from the theory of non-unique factorizations (see [21, 22, 25] and [9, Chapter 6]).

We trivially have $\mathsf{K}^*(G) \le \mathsf{K}(G)$, and equality holds in particular for p-groups (see [9, Proposition 5.1.18 and Theorem 5.5.9]). Recently, B. Girard ([15]) established a new upper bound for the cross number, and his results support the conjecture that we always have equality.

In the present paper, we study the inverse problem associated to the cross number, that is we study the structure of minimal zero-sum sequences U over G with $\mathsf{k}(U) = \mathsf{K}(G)$. These investigations are motivated by questions from factorization theory (see recent work on $\Delta^*(G)$ performed in [23, 26, 3]), and they are part of inverse additive number theory (see [20] for general information, and [8, Section 7] for a recent survey on inverse zero-sum problems). This inverse question is simple for cyclic groups of prime power order (see [9, Theorem 5.1.10]). The case when G is a direct sum of an elementary p-group and an elementary q-group is studied in [12]. More recent progress is again due to B. Girard [15, 13]. The main results of the present paper (formulated in Theorems 3.7 and 3.9) give information on the order of elements contained in a minimal zero-sum sequence U with $\mathsf{k}(U) = \mathsf{K}(G)$. The results are sharp for p-groups and almost sharp in the general case (see the discussion following Theorem 3.9). Among other consequences, they give a structural characterization of the crucial equality $\mathsf{K}(G) = \mathsf{K}^*(G)$ (see Theorem 3.14).

Throughout this article, let G be an additively written, finite abelian group.

2 Preliminaries

Our notation and terminology are consistent with [5] and [9]. We briefly gather some key notions and fix the notation concerning sequences over finite abelian groups. Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers, and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$. For $n \in \mathbb{N}$ and $p \in \mathbb{P}$, let C_n denote a cyclic group with n elements, $nG = \{ng \mid g \in G\}$ and $\mathsf{v}_p(n) \in \mathbb{N}_0$ the p-adic valuation of n with $\mathsf{v}_p(p) = 1$. Throughout, all abelian groups will be written additively.

An s-tuple $(e_1, \ldots, e_s)$ of elements of G is said to be *independent* (or briefly, the elements $e_1, \ldots, e_s$ are said to be independent) if $e_i \neq 0$ for all $i \in [1, s]$ and, for every s-tuple $(m_1, \ldots, m_s) \in \mathbb{Z}^s$,

$$m_1 e_1 + \ldots + m_s e_s = 0 \qquad \text{implies} \qquad m_1 e_1 = \ldots = m_s e_s = 0 \,.$$

An s-tuple $(e_1, \ldots, e_s)$ of elements of G is called a *basis* if it is independent and $G = \langle e_1 \rangle \oplus \ldots \oplus \langle e_s \rangle$. For a prime $p \in \mathbb{P}$, we denote by $G_p = \{g \in G \mid \mathrm{ord}(g) \text{ is a power of } p\}$ the p-primary component of G, and by $\mathsf{r}_p(G)$, the p-rank of G (which is the rank of G_p).

Let $\mathcal{F}(G)$ be the free abelian monoid with basis G. The elements of $\mathcal{F}(G)$ are called *sequences* over G. We write sequences $S \in \mathcal{F}(G)$ in the form

$$S = \prod_{g \in G} g^{\mathsf{v}_g(S)}, \quad \text{with} \quad \mathsf{v}_g(S) \in \mathbb{N}_0 \quad \text{for all} \quad g \in G \,.$$

We call $\mathsf{v}_g(S)$ the *multiplicity* of g in S, and we say that S *contains* g if $\mathsf{v}_g(S) > 0$. A sequence S_1 is called a *subsequence* of S if $S_1 \,|\, S$ in $\mathcal{F}(G)$ (equivalently, $\mathsf{v}_g(S_1) \le \mathsf{v}_g(S)$ for all $g \in G$). If a sequence $S \in \mathcal{F}(G)$ is written in the form $S = g_1 \cdot \ldots \cdot g_l$, we tacitly assume that $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G$.

For a sequence

$$S \;=\; g_1 \cdot \ldots \cdot g_l \;=\; \prod_{g \in G} g^{\mathsf{v}_g(S)} \;\in \mathcal{F}(G)\,,$$

we call

$$|S| = l = \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0 \qquad \text{the } \textit{length} \text{ of } S\,,$$

$$\operatorname{supp}(S) = \{g \in G \,|\, \mathsf{v}_g(S) > 0\} \subset G \qquad \text{the } \textit{support} \text{ of } S \quad \text{and}$$

$$\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g \in G} \mathsf{v}_g(S) g \in G \qquad \text{the } \textit{sum} \text{ of } S\,.$$

The sequence S is called

- a *zero-sum sequence* if $\sigma(S) = 0$,
- *zero-sum free* if there is no nontrivial zero-sum subsequence,
- a *minimal zero-sum sequence* if $1 \neq S$, $\sigma(S) = 0$, and every $S' | S$ with $1 \le |S'| < |S|$ is zero-sum free.

We denote by $\mathcal{A}(G) \subset \mathcal{F}(G)$ the set of all minimal zero-sum sequences over G. Every map of abelian groups $\varphi\colon G \to H$ extends to a homomorphism $\varphi\colon \mathcal{F}(G) \to \mathcal{F}(H)$ where $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_l)$. If φ is a homomorphism, then $\varphi(S)$ is a zero-sum sequence if and only if $\sigma(S) \in \operatorname{Ker}(\varphi)$.

Let

- $\mathsf{D}(G)$ denote the smallest integer $l \in \mathbb{N}$ such that every sequence S over G of length $|S| \ge l$ has a nontrivial zero-sum subsequence.
- $\eta(G)$ denote the smallest integer $l \in \mathbb{N}$ such that every sequence S over G of length $|S| \ge l$ has a zero-sum subsequence T of length $|T| \in [1, \exp(G)]$.

Then $\mathsf{D}(G)$ is called the *Davenport constant* of G, and we have $\mathsf{D}(G) = \max\{|U| \mid U \in \mathcal{A}(G)\}$. We use

$$\mathsf{k}(G) = \max\{\mathsf{k}(U) \mid U \in \mathcal{F}(G) \text{ zero-sum free}\} \in \mathbb{Q}$$

to denote the *little cross number* of G. We summarize the main properties of $\mathsf{k}(G)$, $\mathsf{D}(G)$ and $\eta(G)$ which will be used in the manuscript without further citing. Suppose that

$$G = C_{n_1} \oplus \ldots \oplus C_{n_r} \text{ with } 1 < n_1 \,|\, \ldots \,|\, n_r \quad \text{and set} \quad \mathsf{d}^*(G) = \sum_{i=1}^{r} (n_i - 1)\,.$$

Then we have trivially,

$$\mathsf{k}^*(G) \le \mathsf{k}(G), \;\; \mathsf{K}^*(G) \le \mathsf{K}(G) \quad \text{and} \quad 1 + \mathsf{d}^*(G) \le \mathsf{D}(G)\,.$$

Equality holds for p-groups ([9, Theorem 5.5.9]). Moreover, if $G = C_{n_1} \oplus C_{n_2}$ with $1 \le n_1 \mid n_2$, then (see [9, Theorem 5.8.3])

$$1 + \mathsf{d}^*(G) = \mathsf{D}(G) \quad \text{and} \quad \eta(G) = 2n_1 + n_2 - 2\,. \tag{1}$$

The result on $\eta(G)$ is based on the determination of the Erdős-Ginzburg-Ziv constant $\mathsf{s}(G)$, and thus on Reiher's solution ([24]) of the Kemnitz conjecture. For groups with rank $r \ge 3$, no such results are available (see [8, Section 7] for more information around that).

3 Structural results

We start with some lemmas which are elementary and combinatorial. The main results, Theorems 3.7, 3.9 and 3.14, are based on Equation (1) and use inductive techniques from zero-sum theory (cf. [9, Chapter 5.7]).

Proposition 3.1.

1. *There exists some $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$ such that $\max\{\mathsf{v}_p(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U)\} = \mathsf{v}_p(\exp(G))$ for all $p \in \mathbb{P}$.*

2. *Let $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$. Then $\langle \mathrm{supp}(U)\rangle = G$ if and only if $\max\{\mathsf{v}_p(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U)\} = \mathsf{v}_p(\exp(G))$ for all $p \in \mathbb{P}$.*

Proof. 1. This follows from [9, Proposition 5.1.12.2].

2. If $\langle \mathrm{supp}(U)\rangle = G$ and $p \in \mathbb{P}$, then

$$\mathsf{v}_p(\exp(G)) = \mathsf{v}_p\big(\exp(\langle \mathrm{supp}(U)\rangle)\big) = \max\{\mathsf{v}_p(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U)\}\,.$$

Conversely, set $H = \langle \mathrm{supp}(U)\rangle$ and assume to the contrary that $H \subsetneq G$. Clearly, the hypothesis implies that $\exp(H) = \exp(G)$. Since $H \ne G$, there exists $p \in \mathbb{P}$ such that $G_p \ne H_p$. Let $g \in \mathrm{supp}(U)$ with $\mathsf{v}_p(\mathrm{ord}(g)) = \mathsf{v}_p(\exp(H)) = \mathsf{v}_p(\exp(G))$, and let $g = h + g'$, where $g' \in H_p$, $h \in H$ and $p \nmid \mathrm{ord}(h)$. Then $\mathrm{ord}(g') = p^{\mathsf{v}_p(\exp(G))}$, and thus $\langle g'\rangle$ is a direct summand in G_p so that $G_p = G_p' \oplus \langle g'\rangle$, for some $G_p' < G_p$. Consequently, since $H_p \subsetneq G_p$ and $g' \in H_p$, there must exist some $e \in G_p' \setminus H$.

Let $g'' = g - (p-1)e$. Since $g = h + g'$ with $p \nmid \mathrm{ord}(h)$ and $\mathrm{ord}(g') = p^{\mathsf{v}_p(\exp(G))}$, since $G_p = G_p' \oplus \langle g'\rangle$, and since $e \in G_p'$, we see (by considering $\mathsf{v}_q(\mathrm{ord}(g''))$ for all $q \in \mathbb{P}$, with separate cases for $q = p$ and $q \ne p$) that $\mathrm{ord}(g'') = \mathrm{ord}(g)$. Thus, since $ne \notin H = \langle \mathrm{supp}(U)\rangle$ for $n \in [1, p-1]$ (in view of $e \notin H$), we have

$$U' = g''e^{p-1}Ug^{-1} \in \mathcal{A}(G) \quad \text{with} \quad \mathsf{k}(U') > \mathsf{k}(U) = \mathsf{K}(G)\,,$$

a contradiction. □

Proposition 3.2. *The following statements are equivalent*:

(a) $\mathsf{K}(G) > \mathsf{K}(H)$ *for all proper subgroups $H \subsetneq G$.*

(b) *For all* $U \in \mathcal{A}(G)$ *with* $\mathsf{k}(U) = \mathsf{K}(G)$, *we have* $\max\{\mathsf{v}_p(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U)\} = \mathsf{v}_p(\exp(G))$ *for all* $p \in \mathbb{P}$.

Proof. First we show (a) implies (b). Assume to the contrary that (b) fails. Then Proposition 3.1.2 implies that there exists $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$ and $H = \langle \mathrm{supp}(U) \rangle \subsetneq G$. Thus $U \in \mathcal{A}(H)$ and

$$\mathsf{K}(G) = \mathsf{k}(U) \le \mathsf{K}(H) \le \mathsf{K}(G),$$

contradicting (a).

Next we show (b) implies (a). Let $H \subsetneq G$ be a subgroup with $\mathsf{K}(H) = \mathsf{K}(G)$. Then there exists some $U \in \mathcal{A}(H)$ with $\mathsf{k}(U) = \mathsf{K}(H) = \mathsf{K}(G)$. Hence (b) and Proposition 3.1.2 imply that

$$G = \langle \mathrm{supp}(U) \rangle \le H,$$

contradicting that $H \subsetneq G$. □

We need the following basic result (see [16, Lemma 4.5]).

Lemma 3.3. *Let* $G = C_{m_1} \oplus \ldots \oplus C_{m_r}$, *with* $1 < m_1 \mid \ldots \mid m_r$, *and let* $H \le G$ *be a subgroup, say* $H \cong C_{m_1'} \oplus \ldots \oplus C_{m_r'}$, *with* $1 \le m_1' \mid \ldots \mid m_r'$. *If* $m_t' = m_t$ *for some* $t \in [1, r]$, *then there exists a subgroup* $K \le H$ *such that* $K \cong C_{m_t}$ *and* K *is a direct summand in both* H *and* G.

We will also use the following simple lemma.

Lemma 3.4. *If* $G = H \oplus K$, *with* H *and* K *nontrivial, then* $\mathsf{K}(G) > \mathsf{K}(H)$.

Proof. Let $U \in \mathcal{A}(H)$ with $\mathsf{k}(U) = \mathsf{K}(H)$ and $|U| > 1$ (possible in view of H nontrivial and Proposition 3.1.1), let $h \in \mathrm{supp}(U)$, let $g \in K \setminus \{0\}$, and let $h' = h - (\mathrm{ord}(g) - 1)g$. Set

$$U' = g^{\mathrm{ord}(g)-1} h' U h^{-1}.$$

Then $U' \in \mathcal{A}(G)$ with

$$\mathsf{k}(U') \ge \mathsf{k}(U) - \frac{1}{\mathrm{ord}(h)} + \frac{\mathrm{ord}(g) - 1}{\mathrm{ord}(g)} + \frac{1}{\mathrm{ord}(h')} \ge \mathsf{k}(U) - \frac{1}{2} + \frac{1}{2} + \frac{1}{\mathrm{ord}(h')} > \mathsf{k}(U) = \mathsf{K}(H),$$

whence $\mathsf{K}(G) > \mathsf{K}(H)$ follows. □

Proposition 3.5.

1. *For a proper subgroup* $H \subsetneq G$, *the following statements are equivalent*:

   (a) $\mathsf{K}^*(H) = \mathsf{K}^*(G)$.

   (b) G *is a* p*-group and* H *has a direct summand* A *such that* $H = A \oplus B$ *and* $G = A \oplus C$, *with* $B \cong C_{p^l}$ *and* $C \cong C_{p^m}$, *where* $p \in \mathbb{P}$, $l, m \in \mathbb{N}_0$, $l < m$ *and* $\exp(A) \mid p^l$.

2. *The following statements are equivalent*:

   (a) G *has a proper subgroup* $H \subsetneq G$ *with* $\mathsf{K}^*(H) = \mathsf{K}^*(G)$.

(b) $G = A \oplus C$ *with* $C \cong C_{p^m}$, *where* $p \in \mathbb{P}$, $m \in \mathbb{N}$ *and* $A \le G$ *is a subgroup with* $\exp(A) \mid p^{m-1}$.

Proof. 1. Let $H \subsetneq G$ be a proper subgroup.

We write G in the form $G \cong \bigoplus_{i=1}^{l} \left(\bigoplus_{j=1}^{r} C_{p_i^{k_{i,j}}} \right)$, with $l \in \mathbb{N}$, $p_1, \ldots, p_l$ distinct primes, $0 \le k_{i,1} \le \ldots \le k_{i,r}$ for all $i \in [1,l]$ and $k_{1,r}, \ldots, k_{l,r} \in \mathbb{N}$. Then H may be written in the form $H \cong \bigoplus_{i=1}^{l} \left(\bigoplus_{j=1}^{r} C_{p_i^{k'_{i,j}}} \right)$, with $0 \le k'_{i,1} \le \ldots \le k'_{i,r}$ and $k'_{i,j} \le k_{i,j}$, for all $i \in [1,l]$ and all $j \in [1,r]$ (see [9, Apendix A]). This shows that $\mathsf{k}^*(H) < \mathsf{k}^*(G)$, and thus $\mathsf{K}^*(H) = \mathsf{K}^*(G)$ implies that $\exp(H) < \exp(G)$. Therefore we get $k'_{i,r} < k_{i,r}$ for some $i \in [1,l]$, say w.l.o.g.

$$k'_{1,r} < k_{1,r}\,.$$

Suppose G is not a p-group (so $l \ge 2$). Further suppose that H is a p-group. Then H is nontrivial (else $1 = \mathsf{K}^*(H) = \mathsf{K}^*(G)$, which, in view of G not a p-group, contradicts Lemma 3.4) $\exp(H) \ge 2$, $G = G_p \oplus A$ for a direct summand A, and A has a direct summand isomorphic to C_q for some prime power q. Hence, since $H \le G_p$, it follows that

$$\begin{aligned} \mathsf{K}^*(G) - \mathsf{K}^*(H) &\ge \mathsf{k}^*(G_p) + \frac{q-1}{q} + \frac{1}{\exp(G)} - \mathsf{k}^*(H) - \frac{1}{\exp(H)} \\ &\ge \frac{q-1}{q} + \frac{1}{\exp(G)} - \frac{1}{\exp(H)} \ge \frac{1}{\exp(G)} > 0\,, \end{aligned}$$

a contradiction. So H is not a p-group and hence $p_1^{k'_{1,r}} \cdots p_l^{k'_{l,r}} \ge 2p_1^{k'_{1,r}}$. Thus we have

$$\begin{aligned} K^*(G) - K^*(H) &= \sum_{i=1}^{l}\sum_{j=1}^{r} \frac{p_i^{k_{i,j}-k'_{i,j}} - 1}{p_i^{k_{i,j}}} + \frac{1}{\exp(G)} - \frac{1}{\exp(H)} \\ &= \sum_{i=1}^{l}\sum_{j=1}^{r} \frac{p_i^{k_{i,j}-k'_{i,j}} - 1}{p_i^{k_{i,j}}} + \frac{1}{p_1^{k_{1,r}} \cdots p_l^{k_{l,r}}} - \frac{1}{p_1^{k'_{1,r}} \cdots p_l^{k'_{l,r}}} \\ &\ge \frac{p_1^{k_{1,r}-k'_{1,r}} - 1}{p_1^{k_{1,r}}} + \frac{1}{p_1^{k_{1,r}} \cdots p_l^{k_{l,r}}} - \frac{1}{p_1^{k'_{1,r}} \cdots p_l^{k'_{l,r}}} \\ &> \frac{p_1^{k_{1,r}-k'_{1,r}} - 1}{p_1^{k_{1,r}}} - \frac{1}{p_1^{k'_{1,r}} \cdots p_l^{k'_{l,r}}} \ge \frac{p_1^{k_{1,r}-k'_{1,r}} - 1}{p_1^{k_{1,r}}} - \frac{1}{2p_1^{k'_{1,r}}} \ge 0\,, \end{aligned}$$

a contradiction. So we may assume G is a p-group.

Consequently, $l = 1$, $\exp(H) = p_1^{k'_{1,r}}$ and $\exp(G) = p_1^{k_{1,r}}$. Hence

$$\sum_{i=1}^{r-1} \frac{p_1^{k'_{1,i}} - 1}{p_1^{k'_{1,i}}} + 1 = \mathsf{K}^*(H) = \mathsf{K}^*(G) = \sum_{i=1}^{r-1} \frac{p_1^{k_{1,i}} - 1}{p_1^{k_{1,i}}} + 1,$$

whence $k'_{1,i} = k_{1,i}$ for all $i \in [1, r-1]$. Thus $H = A \oplus B$ with $B \cong C_{p_1^{k'_{1,r}}}$, $A \cong \bigoplus_{j=1}^{r-1} C_{p_1^{k_{1,j}}}$ and $k'_{1,r} < k_{1,r}$. Thus, if $r = 1$, then the result is complete using A trivial. For $r \ge 2$, applying

Lemma 3.3 to $H \le G$, we see that there exists $A_1 \le H$ with $A_1 \cong C_{p_1^{k_{1,1}}}$ and A_1 a direct summand in both H and G. Moreover, we can choose the complimentary summands so that $H = A_1 \oplus H'$ and $G = A_1 \oplus G'$ with $H' \le G'$, and now by iterating this application of Lemma 3.3 (next to $H' \le G'$, and then so forth), we see that an appropriate isomorphic copy of A can be chosen that is a direct summand in both H and G, which establishes (b).

Next we show (b) implies (a). Since $\exp(H) = p^l$ and $\exp(G) = p^m$, the hypotheses of (b) further imply

$$\mathsf{K}^*(H) = \mathsf{k}^*(A) + 1 = \mathsf{K}^*(G),$$

as desired.

2. This follows immediately from 1 (to see (b) implies (a), take $H = A \oplus p^{m-l}C \cong A \oplus C_{p^l}$, where $l = \mathsf{v}_p(\exp(A))$). □

For the proof of Theorem 3.9 we will need the following lemma. A sequence $S \in \mathcal{F}(G)$ is called *short* (in G) if $1 \le |S| \le \exp(G)$.

Lemma 3.6. *Let $G = C_{n_1} \oplus C_{n_2}$ with $1 < n_1 \,|\, n_2$ and let $S \in \mathcal{F}(G)$ be a zero-sum sequence of length $|S| > \mathsf{D}(G) = n_1 + n_2 - 1$. Then S has a short zero-sum subsequence.*

Proof. Since $\eta(G) = 2n_1 + n_2 - 2$ and $\mathsf{D}(G) = n_1 + n_2 - 1$ (see Equation (1)), the assertion is clear for $|S| \ge 2n_1 + n_2 - 2$. Suppose that $|S| = n_1 + n_2 + k$ with $k \in [0, n_1 - 3]$. By [5, Theorem 6.7],

$$S_0 = 0^{n_2 - 2 - k} S$$

has a zero-sum subsequence $W = 0^l S'$ of length in $\{n_2, 2n_2\}$, where $l \in [0, n_2 - 2 - k]$ and $S' \in \mathcal{F}(G)$ is a zero-sum subsequence of S. If $|W| = n_2$, then S' is a short zero-sum subsequence of S. If $|W| = 2n_2$, then $S'^{-1}S$ is a zero-sum subsequence of S of length

$$|S| - |S'| = n_1 + n_2 + k - (2n_2 - l) \le n_1 + n_2 + k - 2n_2 + n_2 - 2 - k = n_1 - 2 \le n_2 \,. \quad \square$$

Theorem 3.7. *Let $G = C_{q_1} \oplus \ldots \oplus C_{q_s}$, where $1 < q_1 \le \ldots \le q_s = p^m$ are prime powers with $s, m \in \mathbb{N}$, $s \ge 2$ and $p \in \mathbb{P}$. Suppose that*

$$G_p = C_{p^{m_1}} \oplus \ldots \oplus C_{p^{m_r}}, \quad \text{where} \quad 1 \le m_1 \le \ldots \le m_r = m,$$

and, for every $i \in [1, s]$, let $H_i < G$ be such that $G = H_i \oplus C_{q_i}$. Let $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$ and $|U| = l$. For every $i \in [1, s]$, we set

$$U = (h_{i,1} + a_{i,1}) \cdot \ldots \cdot (h_{i,l} + a_{i,l}) \quad \text{where} \quad h_{i,\nu} \in H_i \text{ and } a_{i,\nu} \in C_{q_i} \text{ for all } \nu \in [1, l],$$

and let

$$\alpha_i = \max\{\mathrm{ord}(a_{i,\nu}) \mid \nu \in [1, l]\}.$$

1. *For all $i \in [1, s-1]$, we have $\alpha_i = q_i$. If $r = 1$, then $\alpha_s = q_s$, and if $r \ge 2$, then $\alpha_s \ge p^{m_{r-1}}$.*

2. *If $G \ne G_p$ and $\alpha_s < q_s$, then $r \ge 3$ and $2 \le m_{r-2} \le m_{r-1} < m_r$.*

Definition 3.8.

1. We say that G is *exceptional* if it has the form given in Proposition 3.5.2.

2. A sequence U satisfying the hypotheses of Theorem 3.7.2 will be called *anomalous* over G.

Theorem 3.9. *Let all notation be as in Theorem 3.7, and suppose $G \neq G_p$. Let q be a prime divisor of $\exp(G)$, V the subsequence of U consisting of all terms g with $\mathsf{v}_q(\mathrm{ord}(g)) = \gamma$ maximal, and suppose that $\langle \mathrm{supp}(V) \rangle = K$ is a q-group. Then $|V| \ge \mathsf{D}(q^{\gamma-1}K)$, and if $\mathsf{r}_q(qG) \le 2$, then even*

$$|V| \ge \mathsf{D}(q^{\gamma-1}K) + q. \tag{2}$$

Let all notations be as above. If G is a p-group, then $\alpha_s \ge p^{m_{r-1}}$ cannot be strengthened in general. This will be shown in Corollary 3.12. If $G = C_{p^m}$, then the structure of all zero-sum free $U \in \mathcal{F}(G)$ with $\mathsf{k}(U) = \mathsf{k}(G)$ is described in [9, Theorem 5.1.10]. Thus we may assume here that $s \ge 2$. Suppose that G is not a p-group. In that case we conjecture that $\alpha_s = p^{m_r}$, in other words, there are no anomalous sequences (in order to show this, it suffices to consider the case $\alpha_s = p^{m_{r-1}}$, as will be seen in the following proof). The fact that the conjecture holds for $\mathsf{r}_p(pG) \le 2$ is heavily based on Equation (1), and note that no similar results are available for the case $\mathsf{r}_p(pG) \ge 3$.

Proof of Theorems 3.7 *and* 3.9. We set $\exp(G) = n$ and first proceed with a series of assertions.

A1. Let q be a prime divisor of n and $\alpha = \max\{\mathsf{v}_q(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U)\}$. If there exists some $g \in \mathrm{supp}(U)$ with $\mathrm{ord}(g) > \sum_{\nu=\beta}^{\alpha} q^\nu = \frac{q^{\alpha+1}-q^\beta}{q-1}$, where $\beta = \mathsf{v}_q(\mathrm{ord}(g))$, then $\alpha = \mathsf{v}_q(n)$.

A2. There exists at most one prime divisor q of n such that $\max\{\mathsf{v}_q(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U)\} < \mathsf{v}_q(n)$.

A3. Let q be a prime divisor of n such that $\max\{\mathsf{v}_q(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U)\} = \mathsf{v}_q(n)$. Suppose that $G = H \oplus C_{q^\delta}$ and $U = (h_1 + a_1) \cdot \ldots \cdot (h_l + a_l)$, where $h_i \in H$ and $a_i \in C_{q^\delta}$ for all $i \in [1,l]$. Then $\max\{\mathrm{ord}(a_i) \mid i \in [1,l]\} = q^\delta$.

A4. Let q' and q be two prime divisors of n with $q^{\mathsf{v}_q(n)} > q'^{\mathsf{v}_{q'}(n)}$. Then $\max\{\mathsf{v}_{q'}(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U)\} = \mathsf{v}_{q'}(n)$.

Proof of **A1**. Assume to the contrary that $\alpha < \mathsf{v}_q(n)$. Hence there is some $e \in G$ with $\mathrm{ord}(e) = q^{\alpha+1}$. We set $\mathrm{ord}(g) = q^\beta t$ for some $t \in \mathbb{N}$ and $g' = g - (q-1)e$. Then $\mathrm{ord}(g') = q^{\alpha+1}t$ and

$$U' = g' e^{q-1} U g^{-1} \in \mathcal{A}(G)$$

with

$$\mathsf{k}(U') = \mathsf{k}(U) - \frac{1}{q^\beta t} + \frac{q-1}{q^{\alpha+1}} + \frac{1}{q^{\alpha+1}t} > \mathsf{k}(U) = \mathsf{K}(G),$$

a contradiction. □

Proof of **A2**. Assume to the contrary that there are two distinct primes q' and q such that

$$\alpha = \max\{\mathsf{v}_{q'}(\mathrm{ord}(g)) \mid g \in G\} < \mathsf{v}_{q'}(n) \quad \text{and} \quad \beta = \max\{\mathsf{v}_q(\mathrm{ord}(g)) \mid g \in G\} < \mathsf{v}_q(n)\,.$$

Without restriction we may suppose that $q'^{\alpha+1} > q^{\beta+1}$. Since $\alpha < \mathsf{v}_{q'}(n)$, **A1** implies that there exists some $g \in \mathrm{supp}(U)$ with $\mathrm{ord}(g) = q'^{\alpha}$ (any $g \in \mathrm{supp}(U)$ with $\mathsf{v}_{q'}(g) = \alpha$ will do).

Choose elements $e_1 \in G$ with $\mathrm{ord}(e_1) = q'^{\alpha+1}$, and $e_2 \in G$ with $\mathrm{ord}(e_2) = q^{\beta+1}$. Then we have $\mathrm{ord}(g-(q'-1)e_1-(q-1)e_2) = q'^{\alpha+1}q^{\beta+1}$ and

$$U' = (g-(q'-1)e_1-(q-1)e_2)e_1^{q'-1}e_2^{q-1}Ug^{-1} \in \mathcal{A}(G)$$

with

$$\mathsf{k}(U') = \mathsf{k}(U) - \frac{1}{q'^{\alpha}} + \frac{q'-1}{q'^{\alpha+1}} + \frac{q-1}{q^{\beta+1}} + \frac{1}{q'^{\alpha+1}q^{\beta+1}} > \mathsf{k}(U) = \mathsf{K}(G)\,,$$

a contradiction. □

Proof of **A3**. Assume to the contrary that $\max\{\mathrm{ord}(a_i) \mid i \in [1,l]\} = q^{\alpha} < q^{\delta}$. Since $\max\{\mathsf{v}_q(\mathrm{ord}(g) \mid g \in \mathrm{supp}(U)\} = \mathsf{v}_q(n)$, let $g \in \mathrm{supp}(U)$ with $\mathsf{v}_q(\mathrm{ord}(g)) = \mathsf{v}_q(n) \ge \delta > \alpha$. We pick some $a_0 \in C_{q^{\delta}}$ with $\mathrm{ord}(a_0) = q^{\alpha+1}$ and set $g' = g-(q-1)a_0$. Then $\mathrm{ord}(g') = \mathrm{ord}(g)$ and

$$U' = a_0^{q-1}g'Ug^{-1} \in \mathcal{A}(G)$$

with $\mathsf{k}(U') > \mathsf{k}(U) = \mathsf{K}(G)$, a contradiction. □

Proof of **A4**. Assume to the contrary that $\max\{\mathsf{v}_{q'}(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U)\} = \alpha < \mathsf{v}_{q'}(n)$. Then by **A2**, there exists some $g \in \mathrm{supp}(U)$ with

$$\mathrm{ord}(g) \ge q^{\mathsf{v}_q(n)} > q'^{\mathsf{v}_{q'}(n)} \ge q'^{\alpha+1} > \sum_{\nu=0}^{\alpha} q'^{\nu}\,,$$

and hence **A1** gives a contradiction. □

In view of **A4** and **A3**, we see that $\alpha_i = q_i$ for all q_i such that $p \nmid q_i$. Set

$$\alpha = \max\{\mathsf{v}_p(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U)\}.$$

We now proceed to show Theorem 3.7.1 holds. To that end, we can assume $\alpha < \mathsf{v}_p(n)$, else **A3** implies 3.7.1. Thus **A1** implies that all elements $g \in \mathrm{supp}(U)$ with $\mathsf{v}_p(\mathrm{ord}(g)) = \alpha$ have $\mathrm{ord}(g) = p^{\alpha}$.

We continue with the following assertion, which establishes the first part of Theorem 3.7.1.

A5. If $p \mid q_i$ and $i \in [1, s-1]$, then $\alpha_i = q_i$.

Proof of **A5**. Assume to the contrary that $\alpha_i = p^{\beta} < p^{\mathsf{v}_p(q_i)}$. We pick some $a_0 \in C_{p^{\mathsf{v}_p(q_i)}}$ with $\mathrm{ord}(a_0) = p^{\beta+1}$ and some $e \in C_{p^m} = C_{q_s}$ with $\mathrm{ord}(e) = p^m$ and set $g' = g-(p-1)a_0-$

$(p^{m-\alpha}-1)e$, where $g \in \operatorname{supp}(U)$ with $\operatorname{ord}(g) = p^\alpha$ (possible in view of the comment before the statement of **A5**). Then $\operatorname{ord}(g') = p^m$ and

$$a_0^{p-1} e^{p^{m-\alpha}-1} U g^{-1}$$

is zero-sum free. Thus

$$U' = g' a_0^{p-1} e^{p^{m-\alpha}-1} U g^{-1} \in \mathcal{A}(G)$$

and

$$\mathsf{k}(U') = \mathsf{k}(U) - \frac{1}{p^\alpha} + \frac{p^{m-\alpha}-1}{p^m} + \frac{1}{p^m} + \frac{p-1}{p^{\beta+1}} = \mathsf{k}(U) + \frac{p-1}{p^{\beta+1}} > \mathsf{k}(U) = \mathsf{K}(G)\,,$$

a contradiction. □

Now suppose $r = 1$. Then $s \ge 2$ implies $G \neq G_p$. Let S denote the subsequence of U consisting of all elements of order p^α. Since $\sigma(U) = 0$, it follows that $\operatorname{ord}(\sigma(S)) \le p^{\alpha-1}$. Since $G \neq G_p$, there is a prime divisor q of n distinct from p, and in view of **A3** and **A4**, there is some $h \in \operatorname{supp}(U)$ with $\mathsf{v}_q(h) = \mathsf{v}_q(n)$. Consequently, S is a proper subsequence of U. Thus, since $r = 1$, it follows that S has a subsequence T of length $|T| \le \mathsf{D}(p^{m-1}C_{p^m}) = p$ such that $\operatorname{ord}(\sigma(T)) \le p^{\alpha-1}$ and which is a *proper* subsequence of U. We consider the sequence

$$U' = T^{-1}\sigma(T)U \in \mathcal{A}(G)\,.$$

Then clearly $\mathsf{k}(U') \ge \mathsf{k}(U)$. Iterating this process, we either eventually obtain a sequence $W \in \mathcal{A}(G)$ with $\mathsf{k}(W) \ge \mathsf{k}(U) = \mathsf{K}(G)$ which satisfies the assumptions of **A1**, or else we find a *proper* zero-sum subsequence. In the second case, we contradict that $U \in \mathcal{A}(G)$, and in the first, **A1** implies that $\alpha = \mathsf{v}_p(n)$, a contradiction. So we may assume $r \ge 2$.

To conclude the proof of Theorem 3.7.1, suppose to the contrary that $\alpha_s < p^{m_{r-1}}$. Then $\alpha = m_{r-1}$ (in view of **A5**). Let $g \in \operatorname{supp}(U)$ with $\mathsf{v}_p(\operatorname{ord}(g)) = m_{r-1} = \alpha$ and pick some $a_0 \in C_{q_s}$ with $\operatorname{ord}(a_0) = p^\alpha$. We set $g' = g - (p-1)a_0$. Then, since $\alpha_s < p^\alpha = p^{m_{r-1}}$, $g \in \operatorname{supp}(U)$ and $a_0 \in C_{q_s}$, it follows that $\operatorname{ord}(g') = \operatorname{ord}(g)$ and

$$U' = a_0^{p-1} g' U g^{-1} \in \mathcal{A}(G),$$

with $\mathsf{k}(U') > \mathsf{k}(U) = \mathsf{K}(G)$, a contradiction. Thus Theorem 3.7.1 is established.

Next we proceed with the proof of Theorem 3.9. Thus, let q be a prime divisor of $\exp(G)$, V the subsequence of U consisting of all terms g with $\mathsf{v}_q(\operatorname{ord}(g)) = \gamma$ maximal, and suppose that $\langle \operatorname{supp}(V) \rangle = K$ is a q-group so that $q^{\gamma-1}K$ is an elementary q-group. Thus we have $\operatorname{ord}(g) = q^\gamma$ for all $g \in \operatorname{supp}(V)$. Since $\sigma(U) = 0$, it follows from the definition of V that $\mathsf{v}_q(\operatorname{ord}(\sigma(V))) < \gamma$. Let $\varphi\colon G \to G$ be the multiplication by $q^{\gamma-1}$ map. Then $\varphi(K) \cong C_q^\theta$, where θ is the rank of $q^{\gamma-1}K$, and $\mathsf{D}(q^{\gamma-1}K) = \theta(q-1)+1$.

Let $e_1, \ldots, e_\theta \in G$ be independent elements such that $(\varphi(e_1), \ldots, \varphi(e_\theta))$ is a basis of $\varphi(K)$ (and thus $\operatorname{ord}(e_i) = p^\gamma$ for all $i \in [1,\theta]$). Since $\mathsf{v}_q(\operatorname{ord}(\sigma(V))) < \gamma$ and K is a q-group, it follows that we can factor $V = V_1 V_2 \cdot \ldots \cdot V_w$ with $w \in \mathbb{N}$ and $\varphi(V_i) \in \mathcal{A}(\varphi(K))$ for all $i \in [1,w]$.

Let $U' \in \mathcal{F}(G)$ be the sequence obtained from U by replacing each subsequence V_i by the single term $\sigma(V_i)$ (i.e., $U' = \sigma(V_1) \cdot \ldots \cdot \sigma(V_w) U V^{-1}$), let

$$\beta = \max\{\mathsf{v}_q(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U')\},$$

and let $g \in \mathrm{supp}(U')$ be an element such that $\mathrm{ord}(g) = tq^\beta$ with t maximal. Note $U' \in \mathcal{A}(G)$ (since $U \in \mathcal{A}(G)$) and $\beta < \gamma$ (since $\mathsf{v}_q(\mathrm{ord}(\sigma(V))) < \gamma$). Let $g' = g - (q-1) \cdot \sum_{i=1}^{\theta} e_i$. Observe that $\mathrm{ord}(g') = tq^\gamma$. Define

$$U'' = e_1^{q-1} \cdot \ldots \cdot e_\theta^{q-1} g' U' g^{-1}.$$

Since $\mathsf{v}_q(e_i) = \gamma > \beta$, it follows that $U'' \in \mathcal{A}(G)$. Moreover, since $\mathrm{ord}(\sigma(V_i)) \mid q^\beta$ for all $i \in [1, w]$, it follows that

$$\mathsf{k}(U) = \mathsf{K}(G) \ge \mathsf{k}(U'') \ge \mathsf{k}(U) - \frac{|V|}{q^\gamma} - \frac{1}{tq^\beta} + \frac{w}{q^\beta} + \frac{\theta(q-1)}{q^\gamma} + \frac{1}{tq^\gamma},$$

which implies that

$$|V| \ge \theta(q-1) + \frac{1}{t} + q^{\gamma-\beta}\left(w - \frac{1}{t}\right). \tag{3}$$

Likewise, since $U' \in \mathcal{A}(G)$, we have

$$\mathsf{k}(U) = \mathsf{K}(G) \ge \mathsf{k}(U') \ge \mathsf{k}(U) - \frac{|V|}{q^\gamma} + \frac{w}{q^\beta}, \tag{4}$$

which implies

$$|V| \ge q^{\gamma-\beta} w. \tag{5}$$

Since $w, t \ge 1$, it follows from (3) that $|V| \ge \theta(q-1) + 1 = \mathsf{D}(\varphi(K))$, as claimed. Thus we now assume $\mathsf{r}_q(qG) \le 2$.

Suppose $w \ge 2$. Then $\gamma > \beta$ and $t \ge 1$ combined with (3) imply

$$|V| \ge \theta(q-1) + 1 + q(2-1) = \theta(q-1) + q + 1,$$

yielding (2) and so completing the proof of Theorem 3.9. So we may instead assume $w = 1$. Consequently (from the definitions of w and $\mathsf{D}(G)$), it follows that

$$|V| \le \mathsf{D}(\varphi(K)) = \theta(q-1) + 1. \tag{6}$$

Suppose $\theta = 1$. Then we must have equality in (5), and thus in (4) as well, with $\beta = \gamma - 1$, else (6) is contradicted. However, equality in (4) implies that U' is anomalous over G, whence Theorem 3.7.1 implies $q = p$. However, since Theorem 3.7.2 implies that there are no anomalous sequence over G with $\mathsf{r}_p(pG) \le 2$, we see that this case will be complete once we have proved Theorem 3.7.2 (whose proof will only use the case $\theta \ge 2$ in Theorem 3.9). So we may assume $\theta \ge 2$.

Suppose $\theta \ge 3$. Let W be the subsequence of U consisting of all terms h with $\mathsf{v}_q(\mathrm{ord}(h)) > 0$. Then, since $\mathsf{r}_q(qG) \le 2$ and $\theta \ge 3$, it follows that $\gamma = 1$, and thus all $h \in \mathrm{supp}(W)$ have $\mathrm{ord}(h) | q^\gamma$. As a result, since $\sigma(U) = 0$, it follows that $\sigma(W) = 0$.

Thus, since $U \in \mathcal{A}(G)$, it follows that either W is trivial or $W = U$. Since $G \neq G_p$ and $\mathsf{k}(U) = \mathsf{K}(G)$, either case contradicts Lemma 3.4. So we may assume $\theta = 2$.

Let $f_1^{(0)}, f_2^{(0)} \in \mathrm{supp}(V)$ be a basis for K. Let $\beta' \in [1, \gamma - 1]$ be the largest integer such that there is some $g \in \mathrm{supp}(U)$ with $\mathsf{v}_q(\mathrm{ord}(g)) = \beta'$ and $\mathrm{ord}(g) > q^{\beta'}$; note, since $G \neq G_p$, that β' must exist, else we obtain from Lemma 3.4 a contradiction to $\mathsf{k}(U) = \mathsf{K}(G)$, just as we did in the case $\theta \geq 3$. Furthermore, since $\mathsf{r}_q(qG) \leq 2$, it follows that there are no three independent elements of order q^x with $x > \beta'$.

We now iterate the arguments used to construct U' and U''. Let $S_0 = V$, $U_0 = U$ and $\gamma_0 = \gamma$. Assuming $S_{j-1}, U_{j-1}, \gamma_{j-1} > \beta'$, $f_1^{(j-1)}$ and $f_2^{(j-1)}$ have already been constructed, for $j \geq 1$, we define S_j, U_j, γ_j, $f_1^{(j)}$ and $f_2^{(j)}$ as follows. Since $\mathsf{v}_q(\mathrm{ord}(\sigma(S_{j-1}))) < \gamma_{j-1}$ and $\mathsf{v}_q(\mathrm{ord}(h)) \leq \gamma_{j-1}$ for all $h \in \mathrm{supp}(S_{j-1})$ (this holds for $j - 1 = 0$ and follows, for $j - 1 \geq 1$, from the subsequent definitions of S_j and γ_j), it follows from Lemma 3.6 (applied to S_{j-1} modulo the multiplication by the $p^{\gamma_{j-1}-1}$-homomorphism; we are allowed to apply it in view of $\gamma_{j-1} > \beta'$ and the conclusion of the previous paragraph) that we can factor $S_{j-1} = V_1^{(j-1)} \cdot \ldots \cdot V_{w_{j-1}}^{(j-1)}$ with $\sigma(V_i) \in q^{\mathsf{v}_q(n)-\gamma_{j-1}+1} G_q$ for all i and with $1 \leq |V_i| \leq q$ for $i \geq 2$. Let

$$U_j = \sigma(V_1^{(j-1)}) \cdot \ldots \cdot \sigma(V_{w_{j-1}}^{(j-1)}) U_{j-1} S_{j-1}^{-1},$$

let $\gamma_j = \max\{\mathsf{v}_q(\mathrm{ord}(g)) \mid g \in \mathrm{supp}(U_j)\}$, let S_j be the subsequence of U_j consisting of all terms h with $\mathsf{v}_q(\mathrm{ord}(h)) = \gamma_j$, and let $f_1^{(j)}$ and $f_2^{(j)}$ be two independent elements of order q^{γ_j}. If $\gamma_j = \beta'$, stop. Otherwise, every element $h \in \mathrm{supp}(U_j)$ with $\mathsf{v}_q(\mathrm{ord}(h)) = \gamma_j$ has $\mathrm{ord}(h) = q^{\gamma_j}$, whence $\sigma(U_j) = \sigma(U_{j-1}) = \ldots = \sigma(U_0) = \sigma(U) = 0$ implies $\mathsf{v}_q(\mathrm{ord}(\sigma(S_j))) < \gamma_j$, as claimed previously. Let k be the index such that $\gamma_k = \beta'$ (the process must terminate as γ_j decreases with each iteration and $\mathsf{v}_q(n)$ is finite).

By their construction, we have $U_j \in \mathcal{A}(G)$ for all j. Let $g \in \mathrm{supp}(U_k)$ with $\mathrm{ord}(g) = tq^{\gamma_k} = tq^{\beta'}$ and $t \geq 2$ (possible in view of the definition of β'). Then define

$$U''' = f \cdot \prod_{i=0}^{k-1} (f_1^{(i)} f_2^{(i)})^{q-1} \cdot U_k g^{-1},$$

where $f = g - (q-1) \sum_{i=0}^{k-1} (f_1^{(i)} + f_2^{(i)})$. Since $\beta' = \gamma_k < \gamma_{k-1} < \ldots < \gamma_1 < \gamma_0 = \gamma$, since $\mathsf{v}_q(\mathrm{ord}(h)) \leq \gamma_k$ for all $h \in \mathrm{supp}(U_k)$, and since $U_k \in \mathcal{A}(G)$, it follows that $U''' \in \mathcal{A}(G)$. Observe that $\mathrm{ord}(f) = tq^{\gamma_0}$. Thus, since $|V_i^{(j)}| \leq q$ for $i \in [2, w_j]$ and $|V_1^{(j)}| \leq \mathsf{D}(C_q \oplus C_q) = 2q - 1$, for all $j \in [0, k-1]$, since $\gamma_i - 1 \geq \gamma_{i+1}$, for $i \in [0, k-1]$, since $t \geq 2$, and since $k \geq 1$, it follows that

$$\begin{aligned}
\mathsf{K}(G) \geq \mathsf{k}(U''') &\geq \mathsf{k}(U) + \sum_{i=0}^{k-1} \Big(- \frac{|S_i|}{q^{\gamma_i}} + \frac{w_i}{q^{\gamma_{i+1}}} \Big) - \frac{1}{tq^{\gamma_k}} + \sum_{i=0}^{k-1} \frac{2q-2}{q^{\gamma_i}} + \frac{1}{tq^{\gamma_0}} \\
&\geq \mathsf{k}(U) + \sum_{i=0}^{k-1} \Big(- \frac{2q-1+(w_i-1)q}{q^{\gamma_i}} + \frac{w_i}{q^{\gamma_{i+1}}} \Big) - \frac{1}{tq^{\gamma_k}} + \sum_{i=0}^{k-1} \frac{2q-2}{q^{\gamma_i}} + \frac{1}{tq^{\gamma_0}} \\
&\geq \mathsf{k}(U) + \sum_{i=0}^{k-1} \Big(- \frac{2q-1}{q^{\gamma_i}} + \frac{1}{q^{\gamma_{i+1}}} \Big) - \frac{1}{tq^{\gamma_k}} + \sum_{i=0}^{k-1} \frac{2q-2}{q^{\gamma_i}} + \frac{1}{tq^{\gamma_0}}
\end{aligned}$$

$$\begin{aligned} &= \mathsf{k}(U)+\sum_{i=0}^{k-1}\left(-\frac{1}{q^{\gamma_i}}+\frac{1}{q^{\gamma_{i+1}}}\right)-\frac{1}{tq^{\gamma_k}}+\frac{1}{tq^{\gamma_0}} \\ &= \mathsf{k}(U)-\frac{1}{q^{\gamma_0}}+\frac{1}{q^{\gamma_k}}-\frac{1}{tq^{\gamma_k}}+\frac{1}{tq^{\gamma_0}} > \mathsf{k}(U)=\mathsf{K}(G), \end{aligned}$$

a contradiction. Thus it remains to prove Theorem 3.7.2.

To this end, assume $G \neq G_p$ and $\alpha_s < q_s$. We can assume $\alpha < \mathsf{v}_p(n)$, else **A3** contradicts the hypotheses of Theorem 3.7.2. Thus **A1** implies that all elements $g \in \mathrm{supp}(U)$ with $\mathsf{v}_p(\mathrm{ord}(g)) = \alpha$ have $\mathrm{ord}(g) = p^\alpha$. In view of Theorem 3.7.1, we may assume $r \geq 2$ as well, else the proof is complete. Furthermore, applying the argument used in the case $r = 1$, we may w.l.o.g. assume $\alpha_s = p^{m_{r-1}}$. Thus $\alpha = m_{r-1}$. Let V be as defined in the hypothesis of Theorem 3.9 with $q = p$, and let θ be as in the proof of Theorem 3.9. Note, in view of $r \geq 2$, $G \neq G_p$ and Theorem 3.7.1, that V is a nontrivial, proper subsequence of U.

Let $\theta' = \mathsf{r}_p(p^{m_{s-1}-1}G)$. Note $\theta \leq \theta'$ and $q_i = p^{m_{r-1}}$ for at least $\theta' - 1$ indices $i \in [1,s]$. Suppose $\theta < \theta'$. Then there exist $g_1, \ldots, g_\theta \in \mathrm{supp}(U)$ such that all elements $h \in \mathrm{supp}(U)$ with $\mathsf{v}_p(\mathrm{ord}(h)) = m_{r-1}$ (recall that we saw in the previous paragraph that all such elements are of order $p^{m_{r-1}}$) are contained in the subgroup $\langle g_1, \ldots, g_\theta \rangle$. If one of these g_i, say g_θ, has only its C_{q_s} coordinate being of order $p^{m_{r-1}}$, then the independence of the g_i implies g_θ is the unique such g_i, whence we can find a basis for G that includes $g_1, \ldots, g_{\theta-1}$ and a generator of C_{q_s}; applying Theorem 3.7.1 to U, using this basis to replace the representation of G given by $C_{q_1} \oplus \ldots \oplus C_{q_s}$, we obtain a contradiction to $\alpha_i = q_i$ for $i \leq s-1$ (since $\theta < \theta'$). Therefore we may instead assume every g_i has a coordinate other than C_{q_s} of order $p^{m_{r-1}}$. But now, since $q_i = m_{r-1}$ for at least $\theta' - 1 \geq \theta$ indices, we can find a basis for G that includes $g_1, \ldots, g_\theta$ and a generator of C_{q_s}, and then applying Theorem 3.7.1 to U, using this basis to replace the representation of G given by $C_{q_1} \oplus \ldots \oplus C_{q_s}$, we obtain a contradiction to $\alpha_s \geq p^{m_{r-1}}$. So we may assume $\theta = \theta'$. Consequently, $\theta = \theta' \geq 2$.

Assuming that Theorem 3.7.2 fails, we have $\mathsf{r}_p(pG) \leq 2$, whence the hypotheses of Theorem 3.9 hold, and so in view of $\theta \geq 2$, we can apply the completed case of Theorem 3.9 to U with $p = q$ to conclude $|V| \geq 3p-1$. If there are three independent elements of order $p^{m_{r-1}}$, then $\mathsf{r}_p(pG) \leq 2$ implies $m_{r-1} = 1$, whence (in view of every $h \in \mathrm{supp}(V)$ having $\mathrm{ord}(h) | p^{m_{r-1}}$ and $\sigma(U) = 0$) V is a zero-sum subsequence, which contradicts that $U \in \mathcal{A}(G)$ (we noted in a previous paragraph that V is proper and nontrivial). Therefore we may assume there are no three independent elements of order $p^{m_{r-1}}$. Consequently, $|V| \geq 3p-1 > \eta(C_p^2)$ implies that we can find a subsequence $V_0 | V$ with $|V_0| \leq p$ and $\mathrm{ord}(\sigma(V_0)) \,|\, p^{m_{r-1}-1}$. Therefore the sequence

$$U' = \sigma(V_0) U V_0^{-1} \in \mathcal{A}(G)$$

satisfies

$$\mathsf{K}(G) \geq \mathsf{k}(U') \geq \mathsf{k}(U) - \frac{|V_0|}{p^{m_{r-1}}} + \frac{1}{p^{m_{r-1}-1}} \geq \mathsf{k}(U) = \mathsf{K}(G)$$

and hence $\mathsf{k}(U') = \mathsf{K}(G)$. Iterating this process, we see that we can w.l.o.g. assume

$$p < 2p-1 = (3p-1) - p \leq |V| < 3p-1,$$

which contradicts Theorem 3.9 applied to V one last time, completing the proof. □

Corollary 3.10. *Suppose that G is not a p-group and let $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$. Then for every prime divisor p of $\exp(G)$ with $\mathsf{r}_p(pG) \le 2$, there exists some $g \in \operatorname{supp}(U)$ with $\operatorname{ord}(g) = p^{\mathsf{v}_p(\exp(G))}t$ for some $t \ge 2$.*

Proof. Let V be the subsequence of U consisting of all $g \in \operatorname{supp}(U)$ with $\mathsf{v}_p(\operatorname{ord}(g)) = \mathsf{v}_p(\exp(G))$. By Theorem 3.7 and $\mathsf{r}_p(pG) \le 2$, we conclude that V is nontrivial and proper (since $G \neq G_p$). Thus, if the corollary is false, then we can apply Theorem 3.9 to U to conclude that

$$|V| \ge \theta(p-1) + p + 1,$$

where $\theta = \mathsf{r}_p(K)$ and $K = \langle \operatorname{supp}(V) \rangle$. If $\theta \ge 3$, then $\mathsf{r}_p(pG) \le 2$ implies that $\mathsf{v}_p(\exp(G)) = 1$, whence V is a zero-sum subsequence of U, contradicting that $U \in \mathcal{A}(G)$. Therefore $\theta \le 2$, and we see that $|V| > \eta(C_p^\theta)$ (recall $\eta(C_p^2) = 3p-2$ and $\eta(C_p) = p$ by (1)). Thus we can find $V_0 | V$ such that $\operatorname{ord}(\sigma(V_0)) \mid p^{\mathsf{v}_p(\exp(G))-1}$. Defining $U' = \sigma(V_0)UV_0^{-1} \in A(G)$, observe, as in the proof of Theorem 3.7.2, that $\mathsf{k}(U') = \mathsf{k}(U) = \mathsf{k}(G)$. Thus iterating this process, we can reduce the length of V until $|V| < \eta(C_p^\theta)$, which then contradicts Theorem 3.9 applied once more, completing the proof. □

The following corollary is thought to likely hold for all G. Here we show a very special case.

Corollary 3.11. *Suppose $\exp(G) = p^\alpha q$ and $\mathsf{r}_p(pG) \le 2$, where $p, q \in \mathbb{P}$ and $\alpha \ge 0$. Then*

$$\mathsf{K}(G) = \frac{1}{\exp(G)} + \mathsf{k}(G).$$

Proof. By the results mentioned at the end of Section 2, the result holds for p-groups. Therefore we may suppose that p and q are distinct and that $\alpha \ge 1$. Let $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$. Applying Corollary 3.10 to U, we find that there is some $g \in \operatorname{supp}(U)$ with $\operatorname{ord}(g) = \exp(G)$. Thus the assertion follows from [9, Proposition 5.1.8.6]. □

Corollary 3.12. *Let $G = C_{p^{m_1}} \oplus \ldots \oplus C_{p^{m_r}}$ be a p-group with $p \in \mathbb{P}$, $r \in \mathbb{N}$ and $1 \le m_1 \le \ldots \le m_r$.*

1. *For every $m \in [m_{r-1}, m_r]$, there exists some $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$ and $\max\{\operatorname{ord}(g) \mid g \in \operatorname{supp}(U)\} = p^m$.*

2. *G is not exceptional if and only if every $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$ contains some $g \in G$ with $\operatorname{ord}(g) = \exp(G)$.*

Proof. 1. Let $m \in [m_{r-1}, m_r]$ and let $(e_1, \ldots, e_r)$ be a basis of G with $\operatorname{ord}(e_\nu) = p^{m_\nu}$ for $\nu \in [1, r]$. We set $e_r' = p^{m_r - m} e_r$ and $e_0 = e_1 + \ldots + e_{r-1} + e_r'$. Then $\operatorname{ord}(e_r') = \operatorname{ord}(e_0) = p^m$ and

$$U \;=\; e_0 {e_r'}^{p^m - 1} \prod_{\nu=1}^{r-1} e_\nu^{p^{m_\nu}-1} \;\in \mathcal{A}(G)$$

with $\mathsf{k}(U) = 1 + \sum_{i=1}^{r-1} \frac{p^{m_i}-1}{p^{m_i}} = \mathsf{K}^*(G) = \mathsf{K}(G)$.

2. By definition, G is not exceptional if and only if $r \ge 2$ and $m_{r-1} = m_r$. In that case, Theorem 3.7 implies that every $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$ contains some element $g \in G$

with $\mathrm{ord}(g) = \exp(G)$. Conversely, if G is exceptional, then Corollary 3.12.1 shows, for $r \ge 2$, that there exists some $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$ and $\max\{\mathrm{ord}(g) \mid g \in \mathrm{supp}(U)\} < \exp(G)$. For $r = 1$, the sequence $U = 0$ has $\mathsf{k}(U) = 1 = \mathsf{K}^*(C_{p^{m_r}}) = \mathsf{K}(C_{p^{m_r}})$. □

Corollary 3.13. *Suppose that G is not exceptional and let $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$. If $g \in \mathrm{supp}(U)$ such that $\mathrm{ord}(h) \,|\, \mathrm{ord}(g)$ for all $h \in \mathrm{supp}(U)$, then $\mathrm{ord}(g) = \exp(G)$.*

Proof. If G is a p-group, then the assertion follows from Corollary 3.12. Therefore we may assume G is not a p-group, and we also assume to the contrary that $\mathrm{ord}(g) < \exp(G)$. Then there exists some $p \in \mathbb{P}$ such that $\alpha = \mathsf{v}_p(\mathrm{ord}(g)) < \mathsf{v}_p(\exp(G))$. Thus, since $\mathrm{ord}(h) \,|\, \mathrm{ord}(g)$, it follows that $\mathsf{v}_p(\mathrm{ord}(h)) \le \alpha$ for all $h \in \mathrm{supp}(U)$. By Theorem 3.7, $\langle \mathrm{supp}(U) \rangle$ is a p-group if and only if G is a p-group. Therefore $\langle \mathrm{supp}(U) \rangle$ is not a p-group, whence $\mathrm{ord}(g)$ is not a power of p. Thus $\mathrm{ord}(g) = p^\alpha t$ for some $t \ge 2$. We pick some $g_0 \in G$ with $\mathrm{ord}(g_0) = p^{\alpha+1}$ and set $g' = g - (p-1)g_0$. Then $\mathrm{ord}(g') = p^{\alpha+1}t$ and

$$U' = g_0^{p-1} g' U g^{-1} \in \mathcal{A}(G)$$

with

$$\mathsf{k}(U') - \mathsf{k}(U) = \frac{p-1}{p^{\alpha+1}} + \frac{1}{tp^{\alpha+1}} - \frac{1}{tp^\alpha} = \frac{(t-1)(p-1)}{tp^{\alpha+1}} > 0\,,$$

contradicting $\mathsf{k}(U) = \mathsf{K}(G)$. □

Theorem 3.14. *Let $G = G_1 \oplus \ldots \oplus G_s$, where $s \ge 2$ and $G_1, \ldots, G_s$ are the non-trivial primary components of G. For $V \in \mathcal{A}(G)$, we set $\theta(V) = |\{g \in \mathrm{supp}(V) \mid \mathrm{ord}(g)$ is not a prime power$\}|$. Then the following statements are equivalent*:

(a) $\mathsf{K}(G) = \mathsf{K}^*(G)$.

(b) *For every $V \in \mathcal{A}(G)$ with $\theta(V) > 1$, there exists some $U \in \mathcal{A}(G)$ with $\mathsf{k}(V) \le \mathsf{k}(U)$ and $\theta(U) < \theta(V)$.*

(c) *There exists some $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$ such that*

$$U = g \prod_{i=1}^{s} U_i, \quad \text{where} \quad U_i \in \mathcal{F}(G_i) \quad \text{for all} \quad i \in [1,s]\,.$$

Moreover, if U has the above form, then $\mathrm{ord}(g) = \exp(G)$ and $\mathsf{k}(U_i) = \mathsf{k}^*(G_i)$ for all $i \in [1,s]$.

Proof. First we show (a) implies (b). Let $(e_1, \ldots, e_s)$ be a basis of G with $\mathrm{ord}(e_i) = q_i$ a prime power for every $i \in [1,s]$. We set $g = e_1 + \ldots + e_s$. Then $\mathrm{ord}(g) = \exp(G)$ and

$$U = g \prod_{i=1}^{s} e_i^{q_i - 1} \in \mathcal{A}(G)$$

satisfies $\mathsf{k}(U) = \mathsf{K}^*(G) = \mathsf{K}(G)$ and $\theta(U) = 1$ (since $s \ge 2$).

Next we show (b) implies (c). Condition (b) implies (since $\theta(U) = 0$ is impossible for $U \in \mathcal{A}(G)$ with $\mathsf{k}(U) = \mathsf{K}(G)$, in view of Theorem 3.7 and $s \ge 2$) that

$$\mathsf{K}(G) = \max\{\mathsf{k}(U) \mid U \in \mathcal{A}(G) \text{ with } \theta(U) = 1\}\,.$$

Clearly, if $U \in \mathcal{A}(G)$ with $\theta(U) = 1$, then U has the form given in (c).

Finally, we show (c) implies both (a) and the moreover statement that follows (c). Let $\exp(G) = n$ and let $p_1, \ldots, p_s$ the distinct primes which divide n. For every $i \in [1,s]$, we set

$$\alpha_i = \max\{\mathsf{v}_{p_i}(\mathrm{ord}(h)) \mid h \in \mathrm{supp}(U_i)\} \quad \text{and} \quad \mathrm{ord}\big(\sigma(U_i)\big) = p_i^{\beta_i}.$$

Note that $\beta_i \le \alpha_i$ for every $i \in [1,s]$. We continue with the following assertion.

A6. For every $i \in [1,s]$, we have $\beta_i = \alpha_i$.

Proof of **A6**. Let $i \in [1,s]$. We set $a = g + \sigma(U_i)$ with $a \in G$, and let $\mathrm{ord}(a) = t$. Let $h \in \mathrm{supp}(U_i)$ with $\mathrm{ord}(h) = p_i^{\alpha_i}$ and let $g' = a + h$. Then we have $p_i \nmid t$ and $t \ge 2$ (because $s \ge 2$ and $\sigma(U) = 0$; else gU_i is a proper zero-sum subsequence, contradicting $U \in A(G)$), $\mathrm{ord}(g) = tp_i^{\beta_i}$ and $\mathrm{ord}(g') = tp_i^{\alpha_i}$. Thus we obtain

$$U' = g'(-\sigma(U_i))U(gh)^{-1} \in \mathcal{A}(G)$$

and

$$\begin{aligned} \mathsf{K}(G) &\ge \mathsf{k}(U') = \mathsf{k}(U) - \frac{1}{tp_i^{\beta_i}} - \frac{1}{p_i^{\alpha_i}} + \frac{1}{tp_i^{\alpha_i}} + \frac{1}{p_i^{\beta_i}} \\ &= \mathsf{K}(G) + \frac{(p_i^{\alpha_i - \beta_i} - 1)(t-1)}{tp_i^{\alpha_i}}. \end{aligned} \tag{7}$$

This implies that $\alpha_i = \beta_i$. □

Since $g = -(\sigma(U_1) + \ldots + \sigma(U_s))$, **A6** implies that $\mathrm{ord}(h) \,|\, \mathrm{ord}(g)$ for all $h \in \mathrm{supp}(U_i)$ and $i \in [1,s]$. Thus $\mathrm{ord}(g) = n$ by Corollary 3.13. Using the fact that $\mathsf{k}(G_i) = \mathsf{k}^*(G_i)$ for all $i \in [1,s]$, we obtain that

$$\begin{aligned} \mathsf{K}^*(G) = \frac{1}{n} + \mathsf{k}^*(G) &= \frac{1}{n} + \sum_{i=1}^s \mathsf{k}^*(G_i) = \frac{1}{n} + \sum_{i=1}^s \mathsf{k}(G_i) \\ &\le \mathsf{K}(G) = \mathsf{k}(U) = \frac{1}{n} + \sum_{i=1}^s \mathsf{k}(U_i) \le \frac{1}{n} + \sum_{i=1}^s \mathsf{k}(G_i) = \frac{1}{n} + \sum_{i=1}^s \mathsf{k}^*(G_i) \\ &= \frac{1}{n} + \mathsf{k}^*(G) = \mathsf{K}^*(G). \end{aligned}$$

Now all assertions follow. □

Acknowledgement

This work was supported by the Austrian Science Fund FWF (Project Number M1014-N13).

References

[1] P. Baginski, S.T. Chapman, K. McDonald, and L. Pudwell, *On cross numbers of minimal zero sequences in certain cyclic groups*, Ars Comb. **70** (2004), 47 – 60.

[2] S.T. Chapman and A. Geroldinger, *On cross numbers of minimal zero sequences*, Australas. J. Comb. **14** (1996), 85 – 92.

[3] S.T. Chapman, W.A. Schmid, and W.W. Smith, *On minimal distances in Krull monoids with infinite class group*, Bull. Lond. Math. Soc. **40** (2008), 613 – 618.

[4] S. Elledge and G.H. Hurlbert, *An application of graph pebbling to zero-sum sequences in abelian groups*, Integers **5(1)** (2005), Paper A17, 10p.

[5] W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups*: *a survey*, Expo. Math. **24** (2006), 337 – 369.

[6] A. Geroldinger, *On a conjecture of Kleitman and Lemke*, J. Number Theory **44** (1993), 60 – 65.

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

[8] _____, *Additive group theory and non-unique factorizations*, Combinatorial Number Theory and Additive Group Theory (A. Geroldinger and I. Ruzsa, eds.), Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, 2009, pp. 1 – 86.

[9] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

[10] A. Geroldinger and R. Schneider, *The cross number of finite abelian groups II*, Eur. J. Comb. **15** (1994), 399 – 405.

[11] _____, *The cross number of finite abelian groups III*, Discrete Math. **150** (1996), 123 – 130.

[12] _____, *On minimal zero sequences with large cross number*, Ars Comb. **46** (1997), 297 – 303.

[13] B. Girard, *Inverse zero-sum problems in finite abelian p-groups*, Colloq. Math., to appear.

[14] _____, *Inverse zero-sum problems and algebraic invariants*, Acta Arith. **135** (2008), 231 – 246.

[15] _____, *A new upper bound for the cross number of finite abelian groups*, Isr. J. Math. **172** (2009), 253 – 278.

[16] D.J. Grynkiewicz, E. Marchan, and O. Ordaz, *Representation of finite abelian group elements by subsequence sums*, J. Théor. Nombres Bordx., to appear.

[17] D. Kleitman and P. Lemke, *An addition theorem on the integers modulo n*, J. Number Theory **31** (1989), 335 – 345.

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

[19] U. Krause and C. Zahlten, *Arithmetic in Krull monoids and the cross number of divisor class groups*, Mitt. Math. Ges. Hamb. **12** (1991), 681 – 696.

[20] M.B. Nathanson, *Additive Number Theory : Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

[21] A. Plagne and W.A. Schmid, *On large half-factorial sets in elementary p-groups : maximal cardinality and structural characterization*, Isr. J. Math. **145** (2005), 285 – 310.

[22] _____, *On the maximal cardinality of half-factorial sets in cyclic groups*, Math. Ann. **333** (2005), 759 – 785.

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

[24] C. Reiher, *On Kemnitz' conjecture concerning lattice points in the plane*, Ramanujan J. **13** (2007), 333 – 337.

[25] W.A. Schmid, *Half-factorial sets in finite abelian groups : a survey*, Grazer Math. Ber. **348** (2005), 41 – 64.

[26] _____, *Periods of sets of lengths : a quantitative result and an associated inverse problem*, Colloq. Math. **113** (2008), 33 – 53.