Restricted inverse zero-sum problems in groups of rank two

Wolfgang A. Schmid

Centre de Mathématiques Laurent Schwartz

UMR 7640 du CNRS

École polytechnique

91128 Palaiseau cedex

France

wolfgang.schmid@math.polytechnique.fr

Abstract

Let $(G, +)$ be a finite abelian group. Then, $\mathsf{s}(G)$ and $\eta(G)$ denote the smallest integer ℓ such that each sequence over G of length at least ℓ has a subsequence whose terms sum to 0 and whose length is equal to and at most, resp., the exponent of the group. For groups of rank two, we study the inverse problems associated to these constants, i.e., we investigate the structure of sequences of length $\mathsf{s}(G) - 1$ and $\eta(G) - 1$ that do not have such a subsequence. On the one hand, we show that the structure of these sequences is in general richer than expected. On the other hand, assuming a well-supported conjecture on this problem for groups of the form $C_m \oplus C_m$, we give a complete characterization of all these sequences for general finite abelian groups of rank two. In combination with partial results towards this conjecture, we get unconditional characterizations in special cases.

1 Introduction

The investigation of the following type of problem was initiated in the 1960's by the work of P. Erdős, A. Ginzburg, and A. Ziv [8]. Let G be an additive

finite abelian group. Determine the smallest integer ℓ such that each sequence over G of length at least ℓ has a subsequence the sum of whose terms equals $0 \in G$ and that fulfills some additional property; in particular, restrictions on the length of the subsequence were considered (see Section 2 for a more formal definition).

In the present paper, we are specifically interested in the constants $\mathsf{s}(G)$ and $\eta(G)$ that arise when imposing the condition that the subsequence has length equal to the exponent of the group and length at most the exponent of the group, respectively. Together, with the constant $\mathsf{ZS}(G)$ (subsequence of length equal to the order of the group) and the Davenport constant $\mathsf{D}(G)$ (no restriction on the length of the subsequence, besides the trivial one that the length is not zero, to exclude the empty sequence) these are the most classical constants of this form. The constant $\mathsf{s}(G)$ is a generalization (to general groups) of the original problem consider for cyclic groups in [8], first investigated in detail by H. Harborth [18]. The constant $\eta(G)$ was first investigated by P. van Emde Boas [30] and J.E. Olson [21], as a key-tool in the investigation of the Davenport constant for groups of rank two. Parallel to the direct problem of determining the value of these constants, the associated inverse problems, i.e., the problem of determining the structure of the longest sequences that do not have a subsequence of the above mentioned type, received considerable attention as well.

We refer to the recent paper of Y. Edel et al. [7] for a detailed exposition of the history and applications of these two constants, among others in discrete geometry and non-unique factorization theory. For various results on these constants and other related problems see the survey articles [4, 13] and the monograph [17], in particular Chapter 5.

Here, these inverse problems for general finite abelian groups of rank two are investigated. We give a short summary of the present state of knowledge on these invariants (in general), to illustrate that to consider this problem for groups of rank two is a natural choice. The direct problems for groups of rank at most two are solved (cf. Theorem 4.1 and the references there). Moreover, for cyclic groups, answers to the inverse problems are well-known (cf. Theorem 4.2), yet the refined problem of determining the structure of shorter sequences without subsequences of the respective form received considerable attention in the recent literature. We refer to, e.g., [31, 25, 26, 20, 2] for results of this form; note that for cyclic groups—and only in this case— the inverse problem associated to $\eta(G)$ is, for immediate reasons, identical to the one associated to $\mathsf{D}(G)$ (for recent investigations on the inverse problem

associated to the Davenport constant for groups of rank two see [23, 14, 27]). Whereas, for groups of rank at least three, both the direct and the inverse problem are in general wide open (see, e.g., [1, 7, 6, 28] for partial results and bounds), as is the problem of determining the Davenport constant (see, e.g., [3] for a recent contribution).

For groups of the form C_m^2, there is a well-known and well-supported conjecture regarding the answers to the inverse problems (see Section 3 for details). Yet, for general groups of rank two the situation was unclear. Some examples of extremal sequences have been established (see, e.g., [17, Proposition 5.7.8] and [7], in particular Lemma 3.2 and the remarks after Lemma 2.3, for constructions valid for more general groups as well). Our investigations show that these constructions are not exhaustive in an essential way; some expansion on the known constructions are immediate—the goal in the just mentioned work was not to give a complete list of examples—yet beyond these immediate modifications we exhibit aspects that were not noticed before. In particular for the problem associated to $\mathsf{s}(G)$, the structure of sequences can be richer than expected. More specifically, it was conjectured (see [13, Conjecture 7.1]) that, for G a finite abelian group, each sequence S over G of length $|S| = \mathsf{s}(G) - 1$ that has no zero-sum subsequence of length equal to $\exp(G)$ contains some element $\exp(G) - 1$ times. Our investigations yield an example showing that groups of rank two in general do not have this property (cf. Corollary 3.3).

Moreover, and this is the main part of the present work, we reduce the problem of solving the inverse problems for general finite abelian groups of rank two to the respective inverse problems for groups of the form C_m^2. Assuming that the above mentioned conjecture for the groups C_m^2 holds true, we get a complete solution for rank two groups (see Theorem 3.1). And, in combination with partial results towards this conjecture, we obtain unconditional results in special cases (see Corollary 3.2). In fact, due to a very recent result of Ch. Reiher [23], the result regarding the inverse problem associated to $\eta(G)$ becomes unconditional.

2   Preliminaries

We recall some notation and terminology (following [13] and [17]).

We denote by $\mathbb{Z}$ the set of integers, and by $\mathbb{N}$ and $\mathbb{N}_0$ the positive and non-negative integers, respectively. We denote by $[a, b] = \{z \in \mathbb{Z} \colon a \le z \le b\}$ the

interval of integers. For $k \in \mathbb{Z}$ and $m \in \mathbb{N}$, we denote by $[k]_m$ the smallest non-negative integer that is congruent to k modulo m.

Let $(G, +)$ denote a finite abelian group; throughout, we use additive notation for abelian groups. For a subset $G_0 \subset G$, we denote by $\langle G_0 \rangle$ the subgroup generated by G_0. We say that elements $e_1, \ldots, e_r \in G \setminus \{0\}$ are independent if $\sum_{i=1}^r m_i e_i = 0$ with $m_i \in \mathbb{Z}$ implies that $m_i e_i = 0$ for each $i \in [1, r]$. We say that a subset of G is a basis if it generates G and its elements are independent. For $n \in \mathbb{N}$, we denote by C_n a cyclic group of order n. For each finite abelian group G, there exist uniquely determined $1 < n_1 \mid \cdots \mid n_r$ such that $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$; then r is the rank of G and $\exp(G) = n_r$ the exponent of G.

We denote by $\mathcal{F}(G)$ the, multiplicatively written, free abelian monoid over G, that is, the monoid of all formal commutative products

$$S = \prod_{g \in G} g^{\mathsf{v}_g(S)}$$

with $\mathsf{v}_g(S) \in \mathbb{N}_0$. An element $S \in \mathcal{F}(G)$ is called a sequence over G; strictly speaking, this is not a finite sequence in the usual sense—as the ordering of the terms is disregarded—yet for the questions considered in our context the ordering is irrelevant anyway, while this formal framework has several advantages. We refer to $\mathsf{v}_g(S)$ as the multiplicity of g in S. Moreover, $\sigma(S) = \sum_{g \in G} \mathsf{v}_g(S) g \in G$ is called the sum of S, $|S| = \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0$ the length of S, and $\{g \in G : \mathsf{v}_g(S) > 0\} \subset G$ the support of S. We say that a sequence S (over G) is short if $|S| \in [1, \exp(G)]$.

We denote the unit element of $\mathcal{F}(G)$ by 1 and call it the empty sequence. If $T \in \mathcal{F}(G)$ and $T \mid S$ (in $\mathcal{F}(G)$), then we call T a subsequence of S. Moreover, we denote by $T^{-1}S$ the unique sequence R with $RT = S$. The sequence S is called zero-sum free, if $\sigma(T) \neq 0$ for each $1 \neq T \mid S$.

Having more notation at hand, we restate the definition of the invariants mentioned in the introduction in a more formal way, and mentioned a fourth one which we need in one of our arguments. For a finite abelian group G, let $\ell \in \mathbb{N}$ be minimal with the property that each $S \in \mathcal{F}(G)$ with $|S| \geq \ell$ has a subsequence $T \mid S$ such that $\sigma(T) = 0$ and

- $|T| = \exp(G)$; ℓ is denoted by $\mathsf{s}(G)$.

- $|T| \in [1, \exp(G)]$; ℓ is denoted by $\eta(G)$.

- $|T| \geq 1$; ℓ is denoted by $\mathsf{D}(G)$.

- $|T| = k \exp(G)$ for some $k \in \mathbb{N}$; ℓ is denoted by $\mathsf{s}_{\exp(G)\mathbb{N}}(G)$.

For each map $f : G \to G'$ between finite abelian groups, there exists a unique extension to a monoid homomorphism $\mathcal{F}(G) \to \mathcal{F}(G')$, which we denote by f as well. And, if f is group homomorphism, then $\sigma(f(S)) = f(\sigma(S))$ for each $S \in \mathcal{F}(G)$. Moreover, for $h \in G$ and $S \in \mathcal{F}(G)$, let $s_h : G \to G$ denote the map defined via $g \mapsto g + h$, and let $h + S$ denote $s_h(S)$.

3   Main result and Discussion

As mentioned in the Introduction, we reduce the inverse problem for general groups of rank two to the inverse problem for groups of the form C_m^2 for which these problems are well-understood.

We recall two related key-notions for C_m^2. Let $m \in \mathbb{N}$. The group $G = C_m^2$ is said to have

- Property **C** if each $S \in \mathcal{F}(G)$ of length $|S| = \eta(G) - 1$ that has no short zero-sum subsequence equals $T^{\exp(G)-1}$ for some $T \in \mathcal{F}(G)$.

- Property **D** if each $S \in \mathcal{F}(G)$ of length $|S| = \mathsf{s}(G) - 1$ that has no zero-sum subsequence of length $\exp(G)$ equals $T^{\exp(G)-1}$ for some $T \in \mathcal{F}(G)$.

Property **C** was first formulated and investigated by P. van Emde Boas [30]; to be precise, he considered a slightly weaker yet essentially equivalent property (cf. [10, Lemma 4.7] for details). And, Property **D** was introduced by W.D. Gao [9]. It is well-known that if C_m^2 has Property **D**, than it has Property **C** (see [12, Lemma 3.3]).

It is conjectured that for each $m \in \mathbb{N}$ the group C_m^2 has Property **D** and (thus) Property **C** (see the two just mentioned papers and, e.g., [13, Conjecture 7.2]). And, very recently Ch. Reiher [23] proved that C_m^2 has Property **C** for each $m \in \mathbb{N}$.

We recall some partial results on Property **D**. By a result of W.D. Gao [9], the property is multiplicative, i.e., if for $m, n \in \mathbb{N}$ both C_m^2 and C_n^2 have Property **D** so does C_{mn}^2; and an analogous assertion is known for Property **C** (also see [15, Theorem 3.2] for a version of this result for arbitrary rank), reducing the problem of establishing this property for C_m^2 to the case where m is prime. Moreover, it is known to hold true for small m, namely, for $m \leq 10$ (see [9, 29]).

We formulate our main result. In combination with the above mentioned results it yields unconditional answers to the inverse problems in certain cases, cf. Corollary 3.2 for a formal statement; indeed, by Ch. Reiher's result [23] the part regarding $\eta(G)$ holds unconditionally (yet, to highlight the parallelity of the two assertions and to reflect the actual content of this paper, we formulate the result in this way).

Theorem 3.1. *Let G be a finite abelian group of rank two, say, $G \cong C_m \oplus C_{mn}$ with $m, n \in \mathbb{N}$ and $m \geq 2$. Let $\{e_1, e_2\}$ be a basis of G with $\operatorname{ord} e_2 = mn$, and let $\{g_1, g_2\}$ be a generating set of G with $\operatorname{ord} g_2 = mn$.*

1. *The following sequences have length $\eta(G) - 1$ and no short zero-sum susbequence.*

   (a) $e_1^{m-1} e_2^{sm-1} (-xe_1 + e_2)^{(n+1-s)m-1}$ *with* $\gcd\{x, m\} = 1$ *and* $s \in [1, n]$.

   (b) $g_1^{m-1} g_2^{mn-1} (-g_1 + g_2)^{m-1}$.

   If C_m^2 has Property $\boldsymbol{C}$, then each sequence $S \in \mathcal{F}(G)$ with $|S| = \eta(G) - 1$ and no short zero-sum subsequence is of this form (for some basis or generating set, resp., with the above properties).

2. *The following sequences have length $\mathsf{s}(G) - 1$ and no zero-sum subsequence of length $\exp(G)$.*

   (a) $g^{tm-1}(e_1 + g)^{(n+1-t)m-1}(e_2 + g)^{sm-1}(-xe_1 + e_2 + g)^{(n+1-s)m-1}$ *where* $\gcd\{x, m\} = 1$, $s, t \in [1, n]$, *and* $g \in G$.

   (b) $g^{mn-1}(g_1 + g)^{m-1}(g_2 + g)^{mn-1}(-g_1 + g_2 + g)^{m-1}$ *where* $g \in G$.

   If C_m^2 has Property $\boldsymbol{D}$, then each sequence $S \in \mathcal{F}(G)$ with $|S| = \mathsf{s}(G) - 1$ and no zero-sum subsequence of length $\exp(G)$ is of this form (for some basis or generating set, resp., with the above properties).

We point out that to avoid technicalities Theorem 3.1 is formulated in such a way that neither the examples of sequences are mutually exclusive (e.g., we additionally could impose the condition $x \leq m/2$, cf. Lemma 4.4) nor cover all representations of sequences with respect to "natural" bases or generating sets (e.g., the sequence $e_1^{m-1} e_2^{m-1}(-xe_1 + xe_2)^{m-1}$ over C_m^2 with $\gcd\{x, m\} = 1$ has no short zero-sum subsequence and at first might seem to be of a different type, yet by considering it with respect to the basis $\{-xe_1 + xe_2, e_1\}$ it is readily seen that it is covered by our result). Moreover,

we note that (b), in both cases, is redundant for $n = 1$, since then there are no generating sets with two elements that are not a basis. Yet, also in this case, the assertion of our result is more precise than what is immediate by assuming Properties **C** and **D**, respectively.

We end this section by stating, in a formal way, two points that we informally mentioned before.

The following result summarizes the present state of knowledge regarding a full and unconditional solution of the inverse problems associated to $\eta(G)$ and $\mathsf{s}(G)$ for groups of rank two.

Corollary 3.2. *Let G be a finite abelian group of rank two, say, $G \cong C_m \oplus C_{mn}$ with $m, n \in \mathbb{N}$ and $m \geq 2$. Let $S \in \mathcal{F}(G)$.*

1. *The sequences S has length $\eta(G) - 1$ and no short zero-sum subsequence if and only if*

   - *there exist a basis $\{e_1, e_2\}$ of G with $\operatorname{ord} e_2 = mn$, $x \in \mathbb{N}$ with $\gcd\{x, m\} = 1$, and $s \in [1, n]$ such that $S = e_1^{m-1} e_2^{sm-1} (-xe_1 + e_2)^{(n+1-s)m-1}$, or*

   - *there exists a generating set $\{g_1, g_2\}$ of G with $\operatorname{ord} g_2 = mn$ such that $S = g_1^{m-1} g_2^{mn-1} (-g_1 + g_2)^{m-1}$.*

2. *Suppose m is not divisible by a prime strictly greater than 7. The sequences S has length $\mathsf{s}(G) - 1$ and no zero-sum subsequence of length $\exp(G)$ if and only if*

   - *there exist a basis $\{e_1, e_2\}$ of G with $\operatorname{ord} e_2 = mn$, $x \in \mathbb{N}$ with $\gcd\{x, m\} = 1$, $s, t \in [1, n]$, and $g \in G$ such that $S = g^{tm-1}(e_1 + g)^{(n+1-t)m-1}(e_2 + g)^{sm-1}(-xe_1 + e_2 + g)^{(n+1-s)m-1}$, or*

   - *there exists a generating set $\{g_1, g_2\}$ of G with $\operatorname{ord} g_2 = mn$ and $g \in G$ such that $S = g^{mn-1}(g_1+g)^{m-1}(g_2+g)^{mn-1}(-g_1+g_2+g)^{m-1}$.*

Proof. 1. By [23] we know that each $m \in \mathbb{N}$ has Property **C** (recall that Property **C** is implied by Property **B**, see [11, Theorem 10.7], and that Property **C** is multiplicative, see [9]). Thus, the condition in Theorem 3.1.1 is fulfilled and the claim follows.

2. By [9] and [29] we know that if m has no prime divisor strictly greater than 7, then m has Poperty **D**. Thus, the condition in Theorem 3.1.2 is fulfilled and the claim follows. $\square$

Moreover, as a consequence of Theorem 3.1.2, we get that, for groups of rank two, the structure of sequences of length $\mathsf{s}(G) - 1$ without zero-sum subsequence of length $\exp(G)$ can be more complicated than expected, though (provided Property $\mathbf{D}$ holds) for groups of rank two only slighly so. In particular, we can answer (negatively) [13, Conjecture 7.1].

Corollary 3.3. *Let $G = C_m \oplus C_{mn}$ with $m \geq 2$ and $n \geq 3$. There exists a sequence $S \in \mathcal{F}(G)$ of length $\mathsf{s}(G) - 1$ that has no zero-sum subsequence of length $\exp(G)$ yet $\mathsf{v}_g(S) < \exp(G) - 1$ for each $g \in G$.*

Proof. Clear, by Theorem 3.1.2.a with $s, t \in [2, n-1]$. $\qquad\square$

4 Proof of Theorem 3.1

In this section we prove Theorem 3.1. First, we recall and establish some auxiliary results and then turn to the actual details of the proof.

4.1 Auxiliary results

In the following theorem, we recall the answers to the direct problems for groups of rank at most two; in part, they are classical, yet the results on $\mathsf{s}(G)$ and $\mathsf{s}_{\exp(G)\mathbb{N}}(G)$ for groups of rank two were obtained only fairly recently (see [17, Theorem 5.8.3] building on crucial contributions by [22, 24], and [13, Theorem 6.5], respectively).

Theorem 4.1. *Let $m, n \in \mathbb{N}$ and $G = C_m \oplus C_{mn}$. Then $\mathsf{D}(G) = m + mn - 1$, $\eta(G) = 2m + mn - 2$, $\mathsf{s}_{\exp(G)\mathbb{N}}(G) = m + 2mn - 2$, and $\mathsf{s}(G) = 2m + 2mn - 3$.*

For cyclic groups, solutions to the inverse problems are well-known and as discussed in the Introduction meanwhile refined results—valid for shorter sequences—are known (cf., e.g., [13, Theorems 4.3 and 7.5] for results containing the result below and detailed references).

Theorem 4.2. *Let $n \in \mathbb{N}$ and $S \in \mathcal{F}(C_n)$.*

1. *Suppose $|S| = \eta(C_n) - 1 = \mathsf{D}(C_n) - 1$. Then S has no (short) non-empty zero-sum subsequence if and only if $S = e^{n-1}$ for some $e \in C_n$ with $\langle e \rangle = C_n$.*

8

2. *Suppose $|S| = \mathsf{s}(C_n) - 1$. Then S has no zero-sum subsequence of length n if and only if $S = g^{n-1}(g+e)^{n-1}$ for $g, e \in C_n$ with $\langle e \rangle = C_n$.*

In the following lemma, we collect some facts that we use and are essentially known (cf. [7, Lemma 2.2] and [16, Theorem 2]).

Lemma 4.3. *Let G be a finite abelian group, $g \in G$, and $S \in \mathcal{F}(G)$. Furthermore, let $n \in \mathbb{N}$ such that $\exp(G) \mid n$.*

1. *S has a zero-sum subsequence of length n if and only if $g + S$ has a zero-sum subsequence of length n.*

2. *If S has no short zero-sum subsequence, then, for $v \in [0, \exp(G) - 1]$, $g^v(g + S)$ has no zero-sum subsequence of length $\exp(G)$.*

3. *If $\mathsf{v}_g(S) \geq \lfloor (\exp(G) - 1)/2 \rfloor$ and S has no zero-sum subsequences of length $\exp(G)$, then S has a subsequence T of length at least $|S| - \exp(G) + 1$ such that $(-g) + T$ has no short zero-sum subsequence.*

The following lemma, which for prime m can be found in [30, Section 5], is needed in the proof of Theorem 3.1.1; it gives information on the sequence T appearing in the formulation of Property **C**.

Lemma 4.4. *Let $m \in \mathbb{N}$ with $m \geq 2$. Let $T^{m-1} \in \mathcal{F}(C_m^2)$ be a sequence of length $3m-3$ that has no short zero-sum subsequence. Then $T = f_1 f_2(-xf_1 + f_2)$ for a basis $\{f_1, f_2\}$ of C_m^2 and some $x \in [1, m-1]$ with $\gcd\{x, m\} = 1$; moreover, $x \leq m/2$. In particular, for each $f \in \mathrm{supp}(T)$, the sequence $(f^{-1}T)^{m-1}$ is zero-sum free.*

Proof. Obviously $|\mathrm{supp}(T)| = 3$. By [15, Lemma 4.4], the sequence T^{m-1} has a minimal zero-sum subsequence U of length $2m-1$. By [19, Theorem 1] and [12, Proposition 4.1.2], we know that $U = e_1^{m-1} \prod_{i=1}^m (a_i e_1 + e_2)$ for some basis $\{e_1, e_2\}$ of C_m^2. Thus, $T = e_1(ae_1 + e_2)(be_1 + e_2)$ with distinct $a, b \in [0, m-1]$, say $a > b$. Obviously both $\{e_1, ae_1 + e_2\}$ and $\{e_1, be_1 + e_2\}$ are a basis of C_m^2, and by [19, Corollary 1], $\{be_1 + e_2, ae_1 + e_2\}$ is a basis as well, which implies that $\gcd\{a - b, m\} = 1$. Furthermore, $be_1 + e_2 = -(a - b)e_1 + (ae_1 + e_2)$ and $ae_1 + e_2 = -(m + b - a)e_1 + (be_1 + e_2)$. Since $0 \leq \min\{a - b, (m + b - a)\} \leq m/2$, the claim follows. The "in particular"-statement is a direct consequence of the explicit description. $\square$

The following technical result is needed in the proof of Theorem 3.1.2.

Lemma 4.5. *Let $m \in \mathbb{N}$ with $m \geq 2$. Let $T^{m-1} \in \mathcal{F}(C_m^2)$ be a sequence of length $4m - 4$ that has no zero-sum subsequence of length m. Then for each $f \in \operatorname{supp}(T)$, the sequence $(f^{-1}T)^{m-1}$ has no zero-sum subsequence of length $2m$.*

Proof. Let $f \in \operatorname{supp}(T)$. By Lemma 4.3, the sequence $(-f + (f^{-1}T)^{m-1})$ has no short zero-sum subsequence. By Theorem 4.1, each zero-sum sequence over C_m^2 of length $2m$ is not minimal, implying it is the product of two non-empty zero-sum sequences, and at least one of them is short. Thus, $(-f + (f^{-1}T)^{m-1})$ has no zero-sum subsequence of length $2m$, which by Lemma 4.3 implies that $(f^{-1}T)^{m-1}$ has no zero-sum subsequence of length $2m$. $\square$

4.2 Details of the proof

First, we briefly indicate that the listed sequences indeed have the claimed properties.

Then, we solve the inverse problem associated to $\eta(G)$ conditional on Property **C**, and do likewise for the one associated to $\mathsf{s}(G)$ conditional on Property **D**.

4.2.1 Establishing the properties of the sequences

In both cases, the statements regarding the length of the sequences are immediate by Theorem 4.1.

Let S be a sequence as in the formulation of the respective result.
(1) We have to show that S has no short zero-sum subsequence. Let $1 \neq T \mid S$ be a zero-sum subsequence. Suppose S is of the form given in (a). It is clear that $\mathsf{v}_{e_2}(T) + \mathsf{v}_{-xe_1+e_2}(T)$ is not 0 and divisible by $\operatorname{ord} e_2 = mn$; thus, it is equal to mn. This implies that $m \nmid \mathsf{v}_{-xe_1+e_2}(T)$. Consequently, $\mathsf{v}_{e_1}(T) \neq 0$ and $|T| > mn$. Now, suppose S is of the form given in (b). Since $ag_1 \notin \langle g_2 \rangle$ for $|a| \in [1, m-1]$, we have $\mathsf{v}_{g_1}(T) = \mathsf{v}_{-g_1+g_2}(T)$. Thus, $\mathsf{v}_{-g_1+g_2}(T) + \mathsf{v}_{g_2}(T)$ is divisible by $\operatorname{ord} g_2 = mn$. So, we have $\mathsf{v}_{-g_1+g_2}(T) \neq 0$ and $|T| > mn$. Thus, S has no short zero-sum subsequence.
(2) By Lemma 4.3 we may assume that $g = 0$. If S is of the form given in (b), then we know by (1) that the sequence $g_1^{m-1}g_2^{mn-1}(-g_1 + g_2)^{m-1}$ has no short zero-sum subsequence. Similarly, if S is of the form given in (a), we note that by the argument in (1), each zero-sum subsequence T

of S with $\mathsf{v}_{e_2}(T) + \mathsf{v}_{-xe_1+e_2}(T) > 0$ is not short. Since neither 0^{mn-1} nor $0^{tm-1}e_1^{(n+1-t)m-1}$ has a zero-sum subsequence of length mn, it follows in both cases that S has no zero-sum subsequence of length mn.

4.2.2 Proof of Theorem 3.1.1

We start with some observations.

The case $n = 1$ is an immediate consequence of Lemma 4.4.

We thus assume $n \geq 2$, that is $G \cong C_m \oplus C_{mn}$ with $m \geq 2$ and $n \geq 2$. Furthermore, let $H = \{mg \colon g \in G\} \cong C_n$ and let $\varphi \colon G \to G/H$ be the canonical map; we have $G/H \cong C_m^2$. We apply the Inductive Method, as in [11, Section 8], with the exact sequence

$$0 \to H \hookrightarrow G \xrightarrow{\varphi} G/H \to 0,$$

partly using arguments similar to those in [9] and [15].

Now, let $S \in \mathcal{F}(G)$ be a sequence of length $\eta(G) - 1$ with no short zero-sum subsequence. We have to show that S is of the claimed form.

We start our argument by showing that $|\operatorname{supp}(S)| = 3$ and already obtain a somewhat more precise result on S in the process of doing so (see (4.1)). Since $\eta(G/H) = 3m - 2$ and $|S| = (n-1)m + 3m - 3$, we know that there exist subsequences $S_1, \ldots, S_{n-1}$ of S such that $\prod_{i=1}^{n-1} S_i \mid S$ and each $\varphi(S_i)$ is a short zero-sum sequence over G/H, i.e., $\sigma(\varphi(S_i)) = 0$ and $|\varphi(S_i)| \leq m$. Let $R \in \mathcal{F}(G)$ such that $S = R \prod_{i=1}^{n-1} S_i$. If $\sigma(S_1) \ldots \sigma(S_{n-1})$ has a (short) zero-sum subsequence, say $\sigma(\prod_{i \in I} \sigma(S_i)) = 0$ for some $\emptyset \neq I \subset [1, n-1]$, then $\sigma(\prod_{i \in I} S_i) = 0$ and $|\prod_{i \in I} S_i| \leq |I|m \leq mn$, a contradiction. Thus, this sequences has no zero-sum subsequence and consequently by Theorem 4.2 $\sigma(S_1) = \cdots = \sigma(S_{n-1}) = e$ where $\langle e \rangle = H$. Moreover, by the above reasoning it follows that $\varphi(R)$ does not have a short zero-sum subsequence. Thus, $|R| \leq 3m - 3$ and it follows that $|S_i| = m$ for each $i \in [1, n-1]$ and $|R| = 3m - 3$. Since C_m^2 has Property **C**, $\varphi(R) = T^{m-1}$ for some sequences $T \in \mathcal{F}(G/H)$ with $|T| = 3$.

We show that $\operatorname{supp}(\varphi(S)) = \operatorname{supp}(\varphi(R))$; more precisely, we show that each $\varphi(S_i)$ is equal to f^m for some $f \in \operatorname{supp}(T)$. Assume this is not the case, say $\varphi(S_1)$ is not of this form. We show that $\varphi(S_1 R)$ is divisible by the product of two short zero-sum sequences, which by the above argument yields a contradiction.

First, assume $f \mid \varphi(S_1)$ for some $f \in \operatorname{supp}(T)$. Then $f^m \mid \varphi(S_1 R)$ and $f^{-m}\varphi(S_1 R) = (f^{-1}\varphi(S_1))(f^{-1}T)^{m-1}$. Since by assumption $\varphi(S_1) \neq$

11

f^m, it follows that $|\operatorname{supp}(f^{-1}\varphi(S_1))| \geq 2$. Thus, $f^{-m}\varphi(S_1 R)$ contains an element with multiplicity at least m or its support contains at least 4 distinct elements; in both cases, in the latter using the fact that its length is $3m - 3$ and C_m^2 has Property **C**, it has a short zero-sum subsequence.

Second, assume $\operatorname{supp}(\varphi(S_1)) \cap \operatorname{supp}(\varphi(R)) = \emptyset$. Let $f' \mid \varphi(S_1)$. The sequence $f'\varphi(R)$ has a short zero-sum subsequence U. We know that $f' \mid U$ and thus, since $f' \notin \operatorname{supp}(T)$, we have $f^{m-1} \nmid U$ for each $f \in \operatorname{supp}(T)$. Therefore, $\operatorname{supp}(U^{-1}f'\varphi(R)) = \operatorname{supp}(\varphi(R))$ and $|\operatorname{supp}(U^{-1}\varphi(S_1 R))| \geq 4$. This implies the existence of a short zero-sum subsequence of $U^{-1}\varphi(S_1 R)$.

Now, we show that $|\varphi^{-1}(f) \cap \operatorname{supp}(S)| = 1$ for each $f \in \operatorname{supp}(\varphi(S))$. Assume not. Let $g, g' \in \operatorname{supp}(S)$ be distinct elements such that $\varphi(g) = \varphi(g') = f$.

First, suppose $f \in \operatorname{supp}(\varphi(\prod_{i=1}^{n-1} S_i))$. We may assume that $g' \mid R$ and, say, $g \mid S_1$. We have $\sigma(S_1) = e$. Let $S_1' = g^{-1}g'S_1$ and $R' = g'^{-1}gR$. As above, we know that $\sigma(S_1')\sigma(S_2)\ldots\sigma(S_{n-1})$ has no zero-sum subsequence. Thus, it follows that $\sigma(S_1') = e$ (for $n = 2$ this is the only generating element of H). Yet, $\sigma(S_1') = \sigma(S_1) + g' - g \neq \sigma(S_1)$, a contradiction.

Second, suppose $g, g' \in \operatorname{supp}(R)$. This implies $m \geq 3$. The sequence $g^{-1}R$ has a subsequence V such that $\varphi(V)$ is a minimal zero-sum sequence, thus in particular $|V| \leq 2m - 1$. Since $(f^{-1}T)^{m-1}$, for $f \in \operatorname{supp}(T)$, is zero-sum free (see Lemma 4.4), we have $\operatorname{supp}(\varphi(V)) = \operatorname{supp}(\varphi(R))$ and thus we may assume that $g' \mid V$. If $\sigma(U) \neq e$, then $\sigma(S_1)\ldots\sigma(S_{n-1})\sigma(U)$ has a zero-sum subsequence of length at most $n - 1$, yielding a zero-sum sequence of S of length at most $(n-2)m + 2m - 1 \leq mn$, a contradiction. Thus, we have $\sigma(V) = e$. Yet, the same is true for $\sigma(g'^{-1}gV)$, a contradiction.

So, we know that
$$S = g_1^{s_1 m - 1} g_2^{s_2 m - 1} g_3^{s_3 m - 1} \tag{4.1}$$
with $s_i \in [1, n]$ and $s_1 + s_2 + s_3 = n + 2$, in particular $|\operatorname{supp}(S)| = 3$.

We recall that by Lemma 4.4 $\operatorname{supp}(\varphi(S)) = \operatorname{supp}(\varphi(R)) = \{f_1, f_2, -xf_1 + f_2\}$ for a basis f_1, f_2 and some $x \in [1, m]$ with $\gcd(x, m) = 1$ and $x \leq m/2$. Say, $\varphi(g_i) = f_i$ for $i \in [1, 2]$. We note that if $s_i \geq 2$, then $mg_i = \sigma(g_i^m) = e$, in particular $\operatorname{ord} g_i = mn$.

For $a \in [1, m-1]$, let $R_a = g_1^{[xa]_m} g_2^{m-a} g_3^a$. Then $\varphi(R_a)$ is a zero-sum subsequence of $\varphi(R)$ of length at most $2m - 1$. Thus, as above, we conclude $\sigma(R_a) = e$ for each $a \in [1, m-1]$.

Considering $a = 1$ we have
$$xg_1 + (m-1)g_2 + g_3 = e \tag{4.2}$$

and considering $a = m - 1$ we have

$$(m - x)g_1 + g_2 + (m - 1)g_3 = e. \tag{4.3}$$

Now, we assume $m \geq 3$ and complete the argument. At the end we consider $m = 2$. Considering $a = 2$, we get

$$2xg_1 + (m - 2)g_2 + 2g_3 = e. \tag{4.4}$$

Thus, considering the difference of (4.4) and (4.2) we get

$$xg_1 - g_2 + g_3 = 0. \tag{4.5}$$

Moreover, considering the difference of (4.4) and two times (4.2) we get $mg_2 = e$, in particular $\operatorname{ord} g_2 = mn$, and combining this with the sum of (4.2) and (4.3) we get $mg_1 + mg_3 = e$. Note that $\{g_i, g_2\}$ for $i \in \{1, 3\}$ is a generating set of G, since $bg_i \notin \langle g_2 \rangle$ for $b \in [1, m - 1]$.

First, suppose $x \neq 1$. Then $1 \leq \lceil m/x \rceil < m$. Let $r = [\lceil m/x \rceil x]_m = \lceil m/x \rceil x - m$. Considering $a = \lceil m/x \rceil$, we get

$$rg_1 + (m - \lceil m/x \rceil)g_2 + \lceil m/x \rceil g_3 = e \tag{4.6}$$

and thus $rg_1 - \lceil m/x \rceil g_2 + \lceil m/x \rceil g_3 = 0$ and $(\lceil m/x \rceil x - m)g_1 - \lceil m/x \rceil g_2 + \lceil m/x \rceil g_3 = 0$. Using (4.5), we get $mg_1 = 0$ and thus $s_1 = 1$. Moreover, it follows that $\{g_1, g_2\}$ is a basis of G and by (4.5) the sequence is of the form given in (a).

Second, suppose $x = 1$. If $s_1 = s_3 = 1$, the sequence is of the form given in (b), since by (4.5) $g_3 = -g_1 + g_2$. If $s_3 \geq 2$, then $mg_3 = e$ and $mg_1 = 0$, implying that $\{g_1, g_2\}$ is a basis of G, completing the argument. Similarly, if $s_1 \geq 2$, then $mg_1 = e$ and $mg_3 = 0$. Now, $\{g_3, g_2\}$ is a basis of G and $g_1 = -g_3 + g_2$, again completing the argument.

Finally, we suppose $m = 2$. Then $x = 1$ and $g_1 + g_2 + g_3 = e$. Let $\{i, j, k\} = \{1, 2, 3\}$ such that $s_i \geq 2$. Then $2g_i = e$ and $-g_i + g_j + g_k = 0$. If $s_j \geq 2$, then $2g_j = e$, and $2g_k = 0$. It follows that $\{g_k, g_i\}$ is a basis of G and $g_j = -g_k + g_i$. If $s_j = s_k = 1$, we have $g_j = -g_k + g_i$ and $\{g_k, g_i\}$ is a generating set. This completes the proof of part 1.

4.2.3 Proof of Theorem 3.1.2

As for part 1, the case $n = 1$ is immediate, by Lemma 4.3 and part 1. We thus assume again $n \geq 2$, and use the same exact sequence as in the proof of

13

part 1. Also, other parts of the argument are similar to the one for part 1, we keep those parts brief.

Let $S \in \mathcal{F}(G)$ be a sequence of length $\mathsf{s}(G) - 1$ with no zero-sum subsequence of length $\exp(G)$. Again, we start by considering $\mathrm{supp}(S)$, this time showing that $|\mathrm{supp}(S)| = 4$. Since $\mathsf{s}(G/H) = 4m - 3$ and $|S| = (2n - 2)m + 4m - 4$. We know that there exist subsequences $S_1, \ldots, S_{2n-2}$ such that $\prod_{i=1}^{n-1} S_i \mid S$ and each $\varphi(S_i)$ is a zero-sum sequence of length m. Let $R \in \mathcal{F}(G)$ such that $S = R \prod_{i=1}^{2n-2} S_i$. We note that $\sigma(S_1) \ldots \sigma(S_{2n-2})$ has no zero-sum subsequence of length n. Thus, by Theorem 4.2 we know that it is equal to $(e'(e' + e))^{n-1}$ where $\langle e \rangle = H$, say $\sigma(S_i) = (e' + e)$ for $i \in [1, n-1]$.

Moreover, $\varphi(R)$ has no zero-sum subsequence of length m. Since $|R| = 4m - 4$ and C_m^2 has Property **D**, $\varphi(R) = T^{m-1}$ for some $T \in \mathcal{F}(G/H)$. Analogously to the proof of Theorem 3.1.1, using that C_m^2 has Property **D**, it can be seen that if, for some $i \in [1, 2n-2]$, $\varphi(S_i) \notin \{f^m \colon f \in \mathrm{supp}(T)\}$, then $\varphi(RS_i)$ is divisible by the product of two zero-sum sequences of length m, yielding a contradiction. Thus, $\mathrm{supp}(\varphi(S)) = \mathrm{supp}(\varphi(R))$ and each $\varphi(S_i)$ is equal to f^m for some $f \in \mathrm{supp}(T)$.

Now, we show that $|\varphi^{-1}(f) \cap \mathrm{supp}(S)| = 1$ for each $f \in \mathrm{supp}(\varphi(S))$. Assume not. If $f \in \mathrm{supp}(\varphi(\prod_{i=1}^{2n-2} S_i))$, then this can be seen similarly to the proof of Theorem 3.1.1. Suppose $g, g' \in \mathrm{supp}(R)$ are distinct but $\varphi(g) = \varphi(g') = f$. This implies $m \geq 3$. The sequence $g^{-1}R$ has a subsequence U of length $2m$ such that $\sigma(\varphi(U)) = 0$; this follows by Theorem 4.1, since in view of $\mathsf{s}_{m\mathbb{N}}(C_m^2) = 3m - 2$, we get a sequence of length m or $2m$, and by assumption it cannot have length m. By Lemma 4.5, we may assume that it contains g'. We show that $\sigma(U) = 2e' + e$. Assume not, say $\sigma(U) = 2e' - ae$ with $a \in [0, n-2]$. We consider $US_1 \ldots S_a S_n \ldots S_{2n-a-3}$. The sum of this sequence is $(2e' - ae) + a(e' + e) + (n - a - 2)e' = 0$ and its length is $2m + am + (n - a - 2)m = mn$, a contradiction. Yet, by the same argument $\sigma(g'^{-1}gU) = 2e' + e$, a contradiction.

Thus, we know $S = g^{s_0 m - 1} h_1^{s_1 m - 1} h_2^{s_2 m - 1} h_3^{s_3 m - 1}$ with $s_i \in [1, n]$ and $s_0 + s_1 + s_2 + s_3 = 2n + 2$.

Without restriction we assume that s_0 is maximal. We have $s_0 m - 1 \geq m(n+1)/2 - 1 \geq \lfloor (mn - 1)/2 \rfloor$. Thus, by Lemma 4.3, $(S - g) = 0^{s_0 m - 1} RT$ where T is a sequence of length $mn + 2m - 3$ with no short zero-sum subsequence. By Theorem 3.1.1 we know all possible structures of T. It remains to determine s_0 and R. If $T = g_1^{m-1} g_2^{mn-1} (-g_1 + g_2)^{m-1}$ for some generating set $\{g_1, g_2\}$, we get, since s_0 is maximal, that $s_0 = n$ and consequently $R = 1$,

implying that S is of the form given in (b).

Thus, it remains to consider $T = e_1^{m-1} e_2^{km-1} (-xe_1 + e_2)^{(n-k)m-1}$ for a basis $\{e_1, e_2\}$. We note that if $\mathsf{v}_{e_2}(RT) + \mathsf{v}_{-xe_1+e_2}(RT) \geq mn + m - 1$, then $\lfloor \mathsf{v}_{e_2}(RT)/m \rfloor + \lfloor \mathsf{v}_{-xe_1+e_2}(RT)/m \rfloor \geq n$. Yet, if this is the case, then RT has a zero-sum subsequence of length mn, implying that $(g + RT) \mid S$ has a zero-sum subsequences of length mn. Consequently $\mathsf{v}_{e_2}(RT) + \mathsf{v}_{-xe_1+e_2}(RT) \leq mn + m - 2$ and thus $R = e_1^{(n-s_0)m}$, implying that S is of the form given in (a). This completes the proof of part 2.

Funding

References

[1] N. Alon and M. Dubiner. A lattice point problem and additive number theory. *Combinatorica*, 15(3):301–309, 1995.

[2] É. Balandraud. An addition theorem and maximal zero-sum free sets in $\mathbb{Z}/p\mathbb{Z}$, submitted.

[3] G. Bhowmik and J.-Ch. Schlage-Puchta. Davenport's constant for groups of the form $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$. In *Additive combinatorics*, volume 43 of *CRM Proc. Lecture Notes*, pages 307–326. Amer. Math. Soc., Providence, RI, 2007.

[4] Y. Caro. Zero-sum problems—a survey. *Discrete Math.*, 152(1-3):93–113, 1996.

[5] F. Chen and S. Savchev. Minimal zero-sum sequences of maximum length in the group $C_3 \oplus C_{3k}$. *Integers*, 7:A42, 6 pp. (electronic), 2007.

[6] Y. Edel. Sequences in abelian groups G of odd order without zero-sum subsequences of length $\exp(G)$. *Des. Codes Cryptogr.*, 47(1-3):125–134, 2008.

[7] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, and L. Rackham. Zero-sum problems in finite abelian groups and affine caps. *Q. J. Math.*, 58(2):159–186, 2007.

[8] P. Erdős, A. Ginzburg, and A. Ziv. Theorem in the additive number theory. *Bull. Res. Council Israel*, 10F:41–43, 1961.

[9] W. D. Gao. Two zero-sum problems and multiple properties. *J. Number Theory*, 81(2):254–265, 2000.

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

[11] W. D. Gao and A. Geroldinger. On long minimal zero sequences in finite abelian groups. *Period. Math. Hungar.*, 38(3):179–211, 1999.

[12] W. D. Gao and A. Geroldinger. On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$. *Integers*, 3:A8, 45 pp. (electronic), 2003.

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

[14] W. D. Gao, A. Geroldinger, and D. Grynkiewicz. Inverse zero-sum problems III. *Acta Arith.*, 141:103–152, 2010.

[15] W. D. Gao, A. Geroldinger, and W. A. Schmid. Inverse zero-sum problems. *Acta Arith.*, 128(3):245–279, 2007.

[16] W. D. Gao and R. Thangadurai. On the structure of sequences with forbidden zero-sum subsequences. *Colloq. Math.*, 98(2):213–222, 2003.

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

[18] H. Harborth. Ein Extremalproblem für Gitterpunkte. *J. Reine Angew. Math.*, 262/263:356–360, 1973.

[19] G. Lettl and W. A. Schmid. Minimal zero-sum sequences in $C_n \oplus C_n$. *European J. Combin.*, 28(3):742–753, 2007.

[20] H. H. Nguyen and V. H. Vu. Classification theorems for sumsets modulo a prime. *J. Combin. Theory Ser. A*, 116(4):936–959, 2009.

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

[22] Ch. Reiher. On Kemnitz' conjecture concerning lattice-points in the plane. *Ramanujan J.*, 13(1-3):333–337, 2007.

[23] Ch. Reiher. A proof of the theorem according to which every prime number possesses Property B, submitted.

[24] S. Savchev and F. Chen. Kemnitz' conjecture revisited. *Discrete Math.*, 297(1-3):196–201, 2005.

[25] S. Savchev and F. Chen. Long zero-free sequences in finite cyclic groups. *Discrete Math.*, 307(22):2671–2679, 2007.

[26] S. Savchev and F. Chen. Long n-zero-free sequences in finite cyclic groups. *Discrete Math.*, 308(1):1–8, 2008.

[27] W. A. Schmid. Inverse zero-sum problems II. *Acta Arith.*, to appear.

[28] W. A. Schmid and J. J. Zhuang. On short zero-sum subsequences over p-groups. *Ars Combin.*, to appear.

[29] B. Sury and R. Thangadurai. Gao's conjecture on zero-sum sequences. *Proc. Indian Acad. Sci. Math. Sci.*, 112(3):399–414, 2002.

[30] P. van Emde Boas. A combinatorial problem on finite abelian groups. II. *Math. Centrum Amsterdam Afd. Zuivere Wisk.*, 1969(ZW-007):60 pp., 1969.

[31] P. Yuan. On the index of minimal zero-sum sequences over finite cyclic groups. *J. Combin. Theory Ser. A*, 114(8):1545–1551, 2007.