ON A ZERO-SUM PROBLEM ARISING FROM FACTORIZATION THEORY

AQSA BASHIR AND ALFRED GEROLDINGER AND QINGHAI ZHONG

Abstract. We study a zero-sum problem dealing with minimal zero-sum sequences of maximal length over finite abelian groups. A positive answer to this problem yields a structural description of sets of lengths with maximal elasticity in transfer Krull monoids over finite abelian groups.

1. Introduction

Let G be an additively written, finite abelian group and $G_0 \subset G$ be a subset. By a sequence $S = g_1 \ldots g_\ell$ over G_0, we mean a finite sequence of terms from G_0, where the order is disregarded and repetition is allowed. We say that S has sum zero if $g_1 + \ldots + g_\ell = 0$ and that S is a minimal zero-sum sequence if no proper subsum equals zero (i.e., $\sum_{i \in I} g_i \ne 0$ for all $\emptyset \ne I \subsetneq [1, \ell]$). The set of all zero-sum sequences is a (multiplicative) monoid with concatenation of sequences as operation. The empty sequence is the identity element of this monoid and the minimal zero-sum sequences are the irreducible elements. The Davenport constant $\mathsf D(G)$ of G is the maximal length of a minimal zero-sum sequence over G (equivalently, $\mathsf D(G)$ is the smallest integer $\ell \in \mathbb N$ such that every sequence over G of length at least ℓ has a non-empty zero-sum subsequence).

In this note we study a conjecture stemming from factorization theory. We first formulate it in basic terms. Its background and significance will be discussed in Section 2, when we have more terminology at our disposal (Theorem 2.2 and Corollary 2.3).

Conjecture 1.1. *Let G be a finite abelian group, which is neither cyclic nor an elementary 2-group. Then, for every minimal zero-sum sequence $U = g_1 \ldots g_\ell$ of length $|U| = \ell = \mathsf D(G)$, there are $k \in \mathbb N$ and minimal zero-sum sequences $U_1, \ldots, U_k, V_1, \ldots, V_{k+1}$ with terms from $\{g_1, \ldots, g_\ell, -g_1, \ldots, -g_\ell\}$ such that $U_1 \ldots U_k = V_1 \ldots V_{k+1}$.*

Let G be a cyclic group of order $|G| = n \ge 3$. Then $\mathsf D(G) = n$ and every minimal zero-sum sequence over G of length n consists of an element g of order n repeated n times. Thus all distances $s-r$, occurring in equations $U_1 \ldots U_r = V_1 \ldots V_s$ over minimal zero-sum sequences with terms from $\{-g, g\}$, is a multiple of $n-2$. Similarly, if G is an elementary 2-group of rank $r \ge 2$, then $\mathsf D(G) = r+1$ and all distances $s-r$ are multiplies of $r-1$. Thus, the above conjecture neither holds for cyclic groups nor for elementary 2-groups with Davenport constant greater than or equal to four.

To describe the challenge of the above conjecture, suppose that $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$, where $r = \mathsf r(G) = \max\{\mathsf r_p(G) \colon p \in \mathbb P\}$ is the rank of G, $\mathsf r_p(G)$ is the p-rank of G for every prime p, and $1 < n_1 \mid \ldots \mid n_r$ are positive integers. Then

$$\mathsf D^*(G) := 1 + \sum_{i=1}^{r} (n_i - 1) \le \mathsf D(G)\,. \tag{1.1}$$

It is known since the 1960s that equality holds for p-groups and for groups of rank $\mathsf r(G) \le 2$. There are further sparse series of groups where equality holds and groups where equality does not hold (see

2010 *Mathematics Subject Classification.* 11B75, 11P70, 13A05, 20M13.

Key words and phrases. zero-sum sequences, sets of lengths, elasticity, transfer Krull monoids.

This work was supported by the Austrian Science Fund FWF, Project Numbers W1230 and P33499-N.

[1, 9, 10, 12] for recent progress). Even less is known for the associated inverse question asking for the structure of minimal zero-sum sequences of length $\mathsf{D}(G)$. However, the full structural description of minimal zero-sum sequences of length $\mathsf{D}(G)$ is not always needed in order to settle the Conjecture 1.1. We summarize what is known so far.

Conjecture 1.1 is settled for groups of rank two and for groups isomorphic to $C_2 \oplus C_2 \oplus C_{2n}$ with $n \ge 2$. These proofs heavily depend on the complete structural description of minimal zero-sum sequences of length $\mathsf{D}(G)$. Furthermore, the conjecture is proved for groups isomorphic to $C_{p^k}^r$, where p is a prime and $k, r \in \mathbb{N}$ such that $p^k > 2$, although for these groups there is not even a conjecture concerning the structure of minimal zero-sum sequences of maximal length (for all these results see [7]). We formulate a main result of the present paper.

Theorem 1.2. *Conjecture 1.1 holds true for the following non-cyclic finite abelian groups G.*

(a) *G is a p-group such that $\gcd(\exp(G) - 2, \mathsf{D}(G) - 2) = 1$.*
(b) *$G \cong C_{p^{s_1}}^{r_1} \oplus C_{p^{s_2}}^{r_2}$, where p is a prime and $r_1, r_2, s_1, s_2 \in \mathbb{N}$ such that s_1 divides s_2.*
(c) *G is a group with exponent $\exp(G) = pq$, where p, q are distinct primes satisfying one of the three properties.*
  (i) $\gcd(pq - 2, \mathsf{D}(G) - 2) = 1$.
  (ii) $\gcd(pq - 2, p + q - 3) = 1$.
  (iii) *$q = 2$ and $p - 1$ is a power of 2.*
  (iv) *$q = 2$ and $\mathsf{r}_p(G) = 1$.*
(d) *G is a group with exponent $\exp(G) \in [3, 11] \setminus \{8\}$.*

Since Conjecture 1.1 does not hold for groups G with $\exp(G) = 2$, groups that are sums of two elementary p-groups (as listed in (c)) and groups with small exponents, as listed in (d), are extremal cases for the validity of the conjecture. Statement (a) has a simple proof. However, since for p-groups we have $\mathsf{D}(G) = \mathsf{D}^*(G)$, it yields a variety of groups satisfying the conjecture. The precise value of the Davenport constant is not known in general for groups with exponent $\exp(G) = pq$, where p and q are distinct primes. To mention a few examples of what is known so far, let $G \cong C_2^r \oplus C_6$ with $r \in \mathbb{N}$. Then $\mathsf{D}(G) = \mathsf{D}^*(G)$ (i.e., equality holds in (1.1)) if and only if $r \in [1, 3]$ (see [6, Corollary 2] and [2]). Moreover, if a group G with $\exp(G) = 6$ has a subgroup isomorphic to $C_2^i \oplus C_6^{5-i}$ for some $i \in [1, 4]$, then $\mathsf{D}(G) > \mathsf{D}^*(G)$ by [4, Theorem 3.1].

We proceed as follows. In Section 2, we present the background from factorization theory which motivates the above conjecture. We formulate a conjecture and a theorem in terms of factorization theory (Conjecture 2.1 and Theorem 2.2), associated to the ones given in the Introduction. In Corollary 2.3, we establish the significance of the two conjectures for the structure of sets of lengths having maximal elasticity. In Section 3, we prove Theorems 1.2 and 2.2.

2. Background on sets of lengths

For integers $a, b \in \mathbb{Z}$, we denote by $[a, b] = \{x \in \mathbb{Z} \colon a \le x \le b\}$ the discrete interval between a and b. Let $L = \{m_1, \ldots, m_k\} \subset \mathbb{Z}$ be a finite nonempty subset with $k \in \mathbb{N}$ and $m_1 < \ldots < m_k$. Then $\Delta(L) = \{m_i - m_{i-1} \colon i \in [2, k]\} \subset \mathbb{N}$ denotes the set of distances of L. If $L' \subset \mathbb{Z}$ is a finite subset, then $L + L' = \{a + a' \colon a \in L, a' \in L'\}$ is the sumset of L and L'. If $L \subset \mathbb{N}$ consists of positive integers, then $\rho(L) = \max L / \min L$ denotes the elasticity of L and for convenience we set $\rho(\{0\}) = 1$. Let G be an additively written finite abelian group. If $G_0 \subset G$ is a subset, then $\langle G_0 \rangle$ is the subgroup generated by G_0. Let $r \in \mathbb{N}$ and $(e_1, \ldots, e_r)$ be an r-tuple of elements of G. Then $(e_1, \ldots, e_r)$ is said to be independent if $e_i \ne 0$ for all $i \in [1, r]$ and if for all $m_1, \ldots, m_r \in \mathbb{Z}^r$ an equation $m_1 e_1 + \ldots + m_r e_r = 0$ implies that $m_i e_i = 0$ for all $i \in [1, r]$. Furthermore, $(e_1, \ldots, e_r)$ is a basis of G if it is independent and $G = \langle e_1 \rangle \oplus \ldots \oplus \langle e_r \rangle$. A subset $G_0 \subset G$ is independent if the tuple $(g)_{g \in G_0}$ is independent. We recall some basics of the arithmetic of monoids and of zero-sum sequences. Our notation and terminology are consistent with [5, 11].

Arithmetic of Monoids. By a monoid, we mean a commutative cancellative semigroup with identity element. Let H be a multiplicatively written monoid. We denote by $\mathcal{A}(H)$ the set of atoms (irreducible elements) of H and say that H is *atomic* if every non-invertible element can be written as a finite product of atoms. If $a = u_1 \ldots u_k$, where $k \in \mathbb{N}$ and $u_1, \ldots, u_k \in \mathcal{A}(H)$, then k is a factorization length of a, and

$$\mathsf{L}_H(a) = \mathsf{L}(a) = \{k \colon k \text{ is a factorization length of } a\} \subset \mathbb{N}$$

denotes the *set of lengths* of a. It is usual to set $\mathsf{L}(a) = \{0\}$ if $a \in H$ is invertible. The family

$$\mathcal{L}(H) = \{\mathsf{L}(a) \colon a \in H\}$$

is called the *system of sets of lengths* of H and

$$\rho(H) = \sup\{\rho(L) \colon L \in \mathcal{L}(H)\} \in \mathbb{R}_{\ge 1} \cup \{\infty\}$$

denotes the *elasticity* of H. Furthermore,

$$\Delta(H) = \bigcup_{L \in \mathcal{L}(H)} \Delta(L) \ \subset \mathbb{N}$$

is the *set of distances* of H. By definition, $\rho(H) = 1$ if and only if $\Delta(H) = \emptyset$, and otherwise we have $\min \Delta(H) = \gcd \Delta(H)$.

Zero-sum Sequences. Let G be an additively written finite abelian group and $G_0 \subset G$ be a subset. We denote by $\mathcal{F}(G_0)$ the (multiplicatively written) free abelian monoid with basis G_0, called the *monoid of sequences* over G_0. Let

$$S = g_1 \ldots g_\ell = \prod_{g \in G_0} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G_0)$$

be a sequence over G_0. Then, for every $g \in G_0$, $\mathsf{v}_g(S) \in \mathbb{N}_0$ is the multiplicity of g in S, $\operatorname{supp}(S) = \{g_1, \ldots, g_\ell\} \subset G_0$ is the support of S, $|S| = \ell = \sum_{g \in G_0} \mathsf{v}_g(S) \in \mathbb{N}_0$ is the length of S, $\Sigma(S) = \{\sum_{i \in I} g_i \colon \emptyset \ne I \subset [1, \ell]\}$ is the set of subsequence sums of S, and $\sigma(S) = g_1 + \ldots + g_\ell \in G$ is the sum of S. We say that S is zero-sum free if $0 \notin \Sigma(S)$. The set

$$\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \colon \sigma(S) = 0\} \subset \mathcal{F}(G_0)$$

is a submonoid of $\mathcal{F}(G_0)$, called the *monoid of zero-sum sequences* over G_0. We set

$$\mathcal{L}(G_0) := \mathcal{L}(\mathcal{B}(G_0)),\ \Delta(G_0) := \Delta(\mathcal{B}(G_0)),\ \rho(G_0) := \rho(\mathcal{B}(G_0))\,,$$

and so on.

Transfer Krull monoids. A monoid H (resp. a domain D) is said to be a *transfer Krull monoid* (resp. a transfer Krull domain) over a finite abelian group G if there exists a transfer homomorphism $\theta \colon H \to \mathcal{B}(G)$ (resp. $\theta \colon D \setminus \{0\} \to \mathcal{B}(G)$). The classical example of a transfer Krull domain is the ring of integers $\mathcal{O}_K$ of an algebraic number field K, and in this case G is the ideal class group of $\mathcal{O}_K$. We refer to the survey [8] for formal definitions and further examples. The crucial property of a transfer homomorphism $\theta \colon H \to \mathcal{B}(G)$ is that it preserves the system of sets of lengths. We have $\mathcal{L}(H) = \mathcal{L}(G)$, whence all invariants describing the structure of sets of length coincide. In particular, we have

$$\Delta(H) = \Delta(G) \subset [1, \mathsf{D}(G) - 2] \quad \text{and} \quad \rho(H) = \rho(G) = \mathsf{D}(G)/2\,. \tag{2.1}$$

We refer to the survey [14] for what is known on the system $\mathcal{L}(G)$ and on associated invariants. Let H be a transfer Krull monoid over G. It is classical that $|L| = 1$ for all $L \in \mathcal{L}(H)$ if and only if $|G| \le 2$. Suppose that $|G| \ge 3$. Then there is $a \in H$ such that $|\mathsf{L}(a)| > 1$. For every $n \in \mathbb{N}$, the n-fold sumset

$$\mathsf{L}(a) + \ldots + \mathsf{L}(a) \subset \mathsf{L}(a^n)\,,$$

whence $|\mathsf{L}(a^n)| > n$. Thus, sets of lengths in $\mathcal{L}(H)$ can be arbitrarily large.

On $\Delta_\rho(H)$. Now we define the crucial invariant of the present paper (see [7, Definition 2.1]). Let $\Delta_\rho(H)$ denote the set of all $d \in \mathbb{N}$ with the following property: for every $k \in \mathbb{N}$, there is some $L_k \in \mathcal{L}(H)$ with $\rho(L_k) = \rho(H)$ and which has the form

$$L_k = y + (L' \cup \{0, d, \ldots, \ell d\} \cup L'') \subset y + d\mathbb{Z} \tag{2.2}$$

where $y \in \mathbb{Z}$, $\ell \ge k$, $\max L' < 0$, and $\min L'' > \ell D$. If H is a transfer Krull monoid over a finite abelian group G, then $\Delta_\rho(H) = \Delta_\rho(G)$ and there is a constant $M \in \mathbb{N}_0$ such that $L' \subset [-M, -1]$, and $L'' \subset \ell d + [1, M]$ ([7, Lemma 2.3]). The following conjecture was first formulated in [7, Conjecture 3.20].

Conjecture 2.1. *Let H be a transfer Krull monoid over a finite abelian group G with $|G| > 4$. Then $\Delta_\rho(H) = \{1\}$ if and only if G is neither cyclic nor an elementary 2-group.*

In the present note we study $\Delta_\rho(G)$ and obtain the following result.

Theorem 2.2. *Let H be a transfer Krull monoid over a finite abelian non-cyclic group G. Then $\Delta_\rho(H) = \{1\}$ for the following groups.*

(a) *G is a p-group such that $\gcd(\exp(G) - 2, \mathsf{D}(G) - 2) = 1$.*
(b) *$G \cong C_{p^{s_1}}^{r_1} \oplus C_{p^{s_2}}^{r_2}$, where p is a prime and $r_1, r_2, s_1, s_2 \in \mathbb{N}$ such that s_1 divides s_2.*
(c) *G is a group with exponent $\exp(G) = pq$, where p, q are distinct primes satisfying one of the three properties.*
   (i) *$\gcd(pq - 2, \mathsf{D}(G) - 2) = 1$.*
   (ii) *$\gcd(pq - 2, p + q - 3) = 1$.*
   (iii) *$q = 2$ and $p - 1$ is a power of 2.*
   (iv) *$q = 2$ and $\mathsf{r}_p(G) = 1$.*
(d) *G is a group with exponent $\exp(G) \in [3, 11] \setminus \{8\}$.*

The proof of Theorem 2.2 will be given in Section 3. We derive a corollary, which demonstrates the significance of the Conjecture 2.1 and of Theorem 2.2. It states that, if $\Delta_\rho(H) = \{1\}$, then all sets of lengths L with maximal elasticity $\rho(L) = \rho(H)$ are intervals, apart from their globally bounded initial and end parts.

Corollary 2.3. *Let H be a transfer Krull monoid over a finite abelian group G and suppose that $\Delta_\rho(H) = \{1\}$. Then there exists a constant $M^* \in \mathbb{N}_0$ such that every $L \in \mathcal{L}(H)$ with $\rho(L) = \rho(H)$ has the form*

$$L = y + (L' \cup [0, \ell] \cup L''),$$

where $y \in \mathbb{Z}$, $\ell \in \mathbb{N}_0$, $L' \subset [-M^*, -1]$, and $L'' \subset \ell + [1, M^*]$.

Proof. Since $\mathcal{L}(H) = \mathcal{L}(G)$, it is sufficient to prove the claim for the monoid $\mathcal{B}(G)$ of zero-sum sequences over G. If $\mathsf{D}(G) \le 3$, then $\Delta(G) \subset \{1\}$, whence all $L \in \mathcal{L}(G)$ are intervals and the claim holds with $M^* = 0$. Suppose that $\mathsf{D}(G) \ge 4$ and recall that $\Delta(G) \subset [1, \mathsf{D}(G) - 2]$ (see (2.1)). We proceed in four steps.

1. By [3, Section 4.7], there is a constant $M_1 \in \mathbb{N}_0$ such that every $L \in \mathcal{L}(G)$ has the form

$$L = y + (L' \cup L^* \cup L'') \subset y + (\mathcal{D} + d\mathbb{Z}), \tag{2.3}$$

where $y \in \mathbb{Z}$ is a shift parameter,

- $d \in \Delta(G) \subset [1, \mathsf{D}(G) - 2]$ and $\{0, d\} \subset \mathcal{D} \subset [0, d]$,
- L^* is finite nonempty with $\min L^* = 0$ and $L^* = (\mathcal{D} + d\mathbb{Z}) \cap [0, \max L^*]$,
- $L' \subset [-M_1, -1]$, and $L'' \subset \max L^* + [1, M_1]$.

As a side remark, we recall that the above description is best possible, as it was shown by a realization result of Schmid ([13]).

2. Let $G_0 \subset G$ be a subset with $\Delta(G_0) \ne \emptyset$. By [3, Theorem 4.3.6] (applied to the monoid $\mathcal{B}(G_0)$), there are constants $\psi(G_0)$ and $M_2(G_0) \in \mathbb{N}_0$ such that for every $A \in \mathcal{B}(G_0)$ with $\mathsf{v}_g(A) \ge \psi(G_0)$ for all $g \in G_0$,

$$\mathsf{L}(A) = y_A + (L'_A \cup \{0, d_A, 2d_A, \ldots, s_A d_A\} \cup L''_A) \subset y_A + d_A \mathbb{Z}\,, \tag{2.4}$$

where $y_A \in \mathbb{Z}$, $d_A = \min \Delta(G_0)$, $s_A \ge M_1 + \mathsf{D}(G)$, $L'_A \subset [-M_2(G_0), -1]$, and $L''_2 \subset s_A d_A + [1, M_2(G_0)]$. Since G has only finitely many subsets G_0 with $\Delta(G_0) \ne \emptyset$, we let ψ be the maximum over all $\psi(G_0)$ and let M_2 be the maximum over all $M_2(G_0)$. Then the structural statement (2.4) holds with constants ψ and M_2 for all subsets $G_0 \subset G$ with $\Delta(G_0) \ne \emptyset$.

3. Clearly, it is sufficient to prove the claim of the corollary for all $A \in \mathcal{B}(G)$ with $\rho(\mathsf{L}(A)) = \mathsf{D}(G)/2$, for which $\max \mathsf{L}(A) - \min \mathsf{L}(A)$ is sufficiently large. Indeed, suppose that there are constants $M_3, M_4 \in \mathbb{N}_0$ such that the claim holds for all A with $\mathsf{L}(A) \not\subset \min \mathsf{L}(A) + [0, M_3]$ and with bound M_4 for the initial and end parts of $\mathsf{L}(A)$. Then the claim holds for all A with bound $\max\{M_3, M_4\}$ for the initial and end parts of $\mathsf{L}(A)$.

4. Now let $A \in \mathcal{B}(G)$ with $\rho(\mathsf{L}(A)) = \mathsf{D}(G)/2$. By [7, Lemma 3.2.(a)], there are $k, \ell \in \mathbb{N}$ and $U_1, \ldots, U_k, V_1, \ldots, V_\ell \in \mathcal{A}(G)$ with $|U_1| = \ldots = |U_k| = \mathsf{D}(G)$ and $|V_1| = \ldots = |V_\ell| = 2$ such that $A = U_1 \ldots U_k = V_1 \ldots V_\ell$. Then $k = \min \mathsf{L}(A)$ and $\ell = \max \mathsf{L}(A) = k\mathsf{D}(G)/2$. By **3.**, we may suppose that $k \ge |\mathcal{A}(G)|\psi$. Then there is $i \in [1, k]$, say $U_i = U$, such that U^ψ divides A. This implies that $(-U)^\psi U^\psi$ divides A, say $A = (-U)^\psi U^\psi B_\psi$ for some $B_\psi \in \mathcal{B}(G)$. By **2.** (applied to the subset $\operatorname{supp}\big((-U)U\big)$),

$$\mathsf{L}((-U)^\psi U^\psi) = y_U + (L'_U \cup \{0, d_U, 2d_U, \ldots, s_U d_U\} \cup L''_U) \subset y_U + d_U \mathbb{Z}\,, \tag{2.5}$$

where $y_U \in \mathbb{Z}$, $s_U \in \mathbb{N}$ with $s_U \ge M_1 + \mathsf{D}(G)$, $d_U = \min \Delta(G_U)$, $L'_U \subset [-M_2, -1]$, and $L''_U \subset s_U d_U + [1, M_2]$. Since $\Delta_\rho(G) = \{1\}$, [7, Corollary 3.3] implies that $d_U = 1$. Since

$$\mathsf{L}(B_\psi) + \mathsf{L}((-U)^\psi U^\psi) \subset \mathsf{L}(A)\,,$$

$\mathsf{L}(A)$ contains an interval $[t, t + s_U]$ for some $t \in \mathbb{N}_0$. By **3.**, we may assume that $\mathsf{L}(A)$ is not contained in $\min \mathsf{L}(A) + [0, 2M_1 + \mathsf{D}(G)]$. Thus, by comparing the two representations (2.3) and (2.5), we infer that the period $\mathcal{D}$ in (2.3) is an interval. Thus, L^* is an interval, whence $\mathsf{L}(A)$ has the required form. $\square$

Remark 2.4. Let G be a finite abelian group. If $\Delta(G) = \{1\}$ (which, for example, holds if $G \cong C_3 \oplus C_3$), then all sets of lengths are intervals. In particular, Corollary 2.3 holds with $M^* = 0$. Suppose that $G = C_p^r$ is an elementary p-group with $p \ge 5$ and $r \ge 2$.

1. Let $(e_1, \ldots, e_r)$ be a basis of G and $e_0 = e_1 + \ldots + e_r$. Then $U = e_1^{p-1} \ldots e_r^{p-1} e_0 \in \mathcal{A}(G)$ with $|U| = \mathsf{D}(G)$. For every $k \in \mathbb{N}$, we set $A_k = (-U)^k U^k$. Then $\rho(\mathsf{L}(A_k)) = \mathsf{D}(G)/2$ and $\min \mathsf{L}(A_k) = 2k$. It is easy to see that $2k + 1 \notin \mathsf{L}(A_k)$, whence the constant M^*, occurring in Corollary 2.3, cannot be zero but is strictly positive.

2. Every nonzero element $g \in G$ can be extended to a basis. Thus, every nonzero element of G occurs in the support of a minimal zero-sum sequence of length $\mathsf{D}(G)$. Therefore, for every $k \in \mathbb{N}$, there is $B_k \in \mathcal{B}(G)$ with $\rho(\mathsf{L}(B_k)) = \mathsf{D}(G)/2$, $\operatorname{supp}(B_k) = G \setminus \{0\}$, and $\min \mathsf{L}(B_k) \ge k$. Since $\mathsf{L}(B)$ is an interval for all $B \in \mathcal{B}(G)$ with $\operatorname{supp}(B) = G \setminus \{0\}$ ([3, Theorem 7.6.9]), all sets $\mathsf{L}(B_k)$ are intervals with elasticity $\mathsf{D}(G)/2$.

3. Proof of Theorems 1.2 and 2.2

In this section, we prove Theorem 1.2 and Theorem 2.2. We start with two lemmas.

Lemma 3.1. *Let G be a finite abelian group with rank $\mathsf{r}(G) \ge 2$ and $\exp(G) \ge 3$, and let $U \in \mathcal{A}(G)$ with $|U| = \mathsf{D}(G)$. If there exist an independent tuple $(e_1, \ldots, e_t) \in G^t$ with $t \ge 2$ and an element g such that $\{e_1, \ldots, e_t, g\} \subset \operatorname{supp}(U)$ and $ag = k_1 e_1 + \ldots + k_t e_t$ for some $a \in [1, \operatorname{ord}(g) - 1] \setminus \{\frac{\operatorname{ord}(g)}{2}\}$ and with $k_i \in [1, \operatorname{ord}(e_i) - 1]$ for all $i \in [1, t]$, then $\min \Delta\big(\operatorname{supp}\big((-U)U\big)\big) = 1$. In particular, if $\operatorname{supp}(U)$ contains a basis of G, then $\min \Delta\big(\operatorname{supp}\big((-U)U\big)\big) = 1$.*

Proof. See [7, Lemma 3.10]. □

Lemma 3.2. *Let G be a finite abelian group such that $G \cong C_{p^{s_1}}^{r_1} \oplus C_{p^{s_2}}^{r_2}$, where p is a prime, $r_1, r_2, s_1, s_2 \in \mathbb{N}$ with $s_1 < s_2$, and let $G_0 \subset G$ be a subset with $\langle G_0 \rangle = G$. Then there is a subset $G_0' \subset G_0$ such that $\langle G_0' \rangle \cong C_{p^{s_2}}^{r_2}$ and G_0' is a basis of $\langle G_0' \rangle$.*

Proof. Let G_1 and G_2 be subgroups of G such that $G = G_1 \oplus G_2$, $G_1 \cong C_{p^{s_1}}^{r_1}$, and $G_2 \cong C_{p^{s_2}}^{r_2}$. Then every element $g \in G_0$ can be written uniquely as $g = u_g + v_g$, where $u_g \in G_1$ and $v_g \in G_2$. Hence $\langle v_g \colon g \in G_0 \rangle = G_2$ and $\{v_g \colon g \in G_0\}$ contains a basis of G_2 by [3, Lemma A.7.3]. We choose elements $g_1, \ldots, g_{r_2} \in G_0$ such that $(v_1 = v_{g_1}, \ldots, v_{r_2} = v_{g_{r_2}})$ is a basis of G_2. Note that $\mathrm{ord}(v_i) = \mathrm{ord}(g_i) = p^{s_2}$ for every $i \in [1, r_2]$. If $k_1, \ldots, k_{r_2} \in [0, p^{s_2} - 1]$ such that $k_1 g_1 + \ldots + k_{r_2} g_{r_2} = 0$, then $k_1 v_1 + \ldots + k_{r_2} v_{r_2} = 0$, whence the independence of $(v_1, \ldots, v_{r_2})$ implies that $k_1 = \ldots = k_{r_2} = 0$. It follows that $(g_1, \ldots, g_{r_2})$ is independent and hence $\langle g_1, \ldots, g_{r_2} \rangle \cong C_{p^{s_2}}^{r_2}$. □

Proof of Theorems 1.2 and 2.2. Let H be a monoid, G be a finite abelian non-cyclic group, and let $\theta \colon H \to \mathcal{B}(G)$ be a transfer homomorphism. Then $\Delta_\rho(H) = \Delta_\rho(G)$. In order to show that $\Delta_\rho(G) = \{1\}$, it is sufficient to show that

$$\min \Delta\big(\operatorname{supp}\big((-U)U\big)\big) = 1 \quad \text{for every minimal zero-sum sequence } U \text{ over } G \text{ with } |U| = \mathsf{D}(G) \tag{3.1}$$

(see [7, Corollary 3.3.2]). Note that (3.1) is precisely the statement of Conjecture 1.1. Let U be a minimal zero-sum sequence over G with $|U| = \mathsf{D}(G)$. We set $d = \min \Delta\big(\operatorname{supp}\big((-U)U\big)\big)$ and have to show that $d = 1$. Since $|U| = \mathsf{D}(G)$, we have $G = \langle \operatorname{supp}(U) \rangle$ by [3, Proposition 5.1.4].

Let $A \subset \operatorname{supp}(U)$ be a minimal subset such for every element $g \in \operatorname{supp}(U) \setminus A$, there exists $h \in A$ such that $g \in \langle h \rangle$. Thus, for any two elements $g_1, g_2 \in A$, we have $g_1 \notin \langle g_2 \rangle$ and $\langle A \rangle = \langle \operatorname{supp}(U) \rangle = G$ is not cyclic, whence $|A| \ge 2$. Assume to the contrary that A is independent. We set $A = \{g_1, \ldots, g_m\}$ and $W_i = \prod_{g \in \langle g_i \rangle} g^{\mathsf{v}_g(U)}$ for every $i \in [1, m]$, where $m = |A| \ge 2$. Then $U = \prod_{i \in [1,m]} W_i$ and $\sigma(W_i) \in \langle g_i \rangle$ for every $i \in [1, m]$. Since A is independent and U is a zero-sum sequence, we obtain that W_i are zero-sum sequences for all $i \in [1, m]$, a contradiction to the minimality of U. Thus A is not independent.

We start with two simple observations. Let V be a minimal zero-sum sequence over $\operatorname{supp}\big(U(-U)\big)$. Since $(-V)V$ has a factorization of length $|V|$, it follows that

$$d \quad \text{divides} \quad |V| - 2 \,. \quad \text{In particular,} \quad d \quad \text{divides} \quad \mathsf{D}(G) - 2 \,. \tag{3.2}$$

If $g \in \operatorname{supp}\big((-U)U\big)$ with $\mathrm{ord}(g) = n$, then $V = g^n$ is a minimal zero-sum sequence over $\operatorname{supp}\big(U(-U)\big)$, whence (3.2) implies that $d \mid (n-2)$. Thus we obtain that

$$d \quad \text{divides} \quad \mathrm{ord}(g) - 2 \quad \text{for all } g \in \operatorname{supp}\big((-U)U\big) \,. \tag{3.3}$$

We distinguish four cases. Whenever it is convenient, an elementary p-group will be considered as a vector space over the field with p elements.

CASE 1: G is a p-group such that $\gcd(\exp(G) - 2, \mathsf{D}(G) - 2) = 1$.

By [3, Corollary 5.1.13], $\operatorname{supp}(U)$ contains an element of order $\exp(G)$. Thus $d = 1$ by (3.3) and (3.2).

CASE 2: $G \cong C_{p^{s_1}}^{r_1} \oplus C_{p^{s_2}}^{r_2}$, where p is a prime and $r_1, r_2, s_1, s_2 \in \mathbb{N}$ such that s_1 divides s_2.

If $s_1 = s_2$, then the assertion follows from [7, Theorem 3.11]. Suppose that $s_1 < s_2$. Then $\exp(G) = p^{s_2} \ge 4$. By Lemma 3.2, there is a subset $A_2 \subset A$ such that $\langle A_2 \rangle \cong C_{p^{s_2}}^{r_2}$ and A_2 is a basis of $\langle A_2 \rangle$, say $A_2 = \{g_1, \ldots, g_{r_2}\}$. Since $\langle A_2 \rangle$ is a direct summand of G, there is a subgroup G_1 of G with $G = G_1 \oplus \langle A_2 \rangle$, whence $G_1 \cong C_{p^{s_1}}^{r_1}$. Every element g of A can be written uniquely as $g = u_g + v_g$, where $u_g \in G_1$ and $v_g \in \langle A_2 \rangle$. Hence $\langle u_g \colon g \in A \rangle = G_1$ and $\{u_g \colon g \in A\}$ contains a basis of G_1 by [3, Lemma A.7.3]. We choose $h_1, \ldots, h_{r_1} \in A$ such that $(u_1 = u_{h_1}, \ldots, u_{r_1} = u_{h_{r_1}})$ is a basis of G_1. We distinguish two cases.

Suppose $\mathrm{ord}(h_i) = p^{s_1}$ for every $i \in [1, r_1]$. Then the tuple $(h_1, \ldots, h_{r_1})$ is independent, whence the tuple $(h_1, \ldots, h_{r_1}, g_1, \ldots, g_{r_2})$ forms a basis of G. Then the assertion follows by Lemma 3.1.

Suppose there exists $i \in [1, r_1]$ such that $\mathrm{ord}(h_i) \ne p^{s_1}$. Then $0 \ne p^{s_1} h_i$ and p^{s_1} is the minimal integer such that $p^{s_1} h_i \in \langle g_1, \ldots, g_{r_2} \rangle$. Set $h = h_i$. There exist $\emptyset \ne I \subset [1, r_2]$ and $k_i \in [1, p^{s_1} - 1]$ for every

$i \in I$ such that $p^{s_1}h = \sum_{i\in I} k_i g_i$. After renumbering if necessary, we may assume that $I = [1,t]$ for some $t \in [1, r_2]$.

If $t = 1$, then $(-h)^{p^{s_1}} g_1^{k_1}$ and $h^{p^{s_1}} g_1^{p^{s_2}-k_1}$ are both minimal zero-sum sequences. It follows by $\big(h^{p^{s_1}} g_1^{p^{s_2}-k_1}\big)\big((-h)^{p^{s_1}} g_1^{k_1}\big) = \big(h(-h)\big)^{p^{s_1}} g_1^{p^{s_2}}$ that d divides $p^{s_1} - 1$. Since d divides $p^{s_2} - 2$ by (3.3), it follows by the fact that s_1 divides s_2 that $d = 1$.

If $t \ge 2$ and $p^{s_1} \ne \frac{\mathrm{ord}(h)}{2}$, then $d = 1$ by Lemma 3.1.

If $t \ge 2$ and $\mathrm{ord}(h) = 2p^{s_1}$, then $p = 2$. Since $h^{2^{s_1}} g_1^{k_1} \ldots g_t^{k_t}$ is a minimal zero-sum sequence, we obtain that $g_1^{2k_1} \ldots g_t^{2k_t}$ is a zero-sum sequence, whence the independence of $(g_1, \ldots, g_t)$ implies that $k_i = 2^{s_2-1}$ for all $i \in [1,t]$. Since $(-h)^{2^{s_1}} g_1^{k_1} \ldots g_t^{k_t}$ is a minimal zero-sum sequence and

$$\big(h^{2^{s_1}} g_1^{k_1} \ldots g_t^{k_t}\big)^2 = h^{2^{s_1+1}} g_1^{2^{s_2}} \ldots g_t^{2^{s_2}} \text{ and } \big(h^{2^{s_1}} g_1^{k_1} \ldots g_t^{k_t}\big)\big((-h)^{2^{s_1}} g_1^{k_1} \ldots g_t^{k_t}\big) = \big(h(-h)\big)^{2^{s_1}} g_1^{2^{s_2}} \ldots g_t^{2^{s_2}},$$

we obtain that d divides $(t+1-2) - (2^{s_1} + t - 2) = 1 - 2^{s_1}$. Since d divides $2^{s_2} - 2$ by (3.3), it follows by the fact that s_1 divides s_2 that $d = 1$.

CASE 3: G is the sum of two elementary p-groups, say $G = C_p^r \oplus C_q^s$, where p, q are distinct primes and $r, s \in \mathbb{N}$.

We set $U = U_p U_q U_{pq}$, where $U_p \in \mathcal{F}(G)$ consists of elements of order p, $U_q \in \mathcal{F}(G)$ consists of elements of order q, and $U_{pq} \in \mathcal{F}(G)$ consists of elements of order pq. Since U is a minimal zero-sum sequence and $0 = \sigma(U) = \sigma(U_p) + \sigma(U_q) + \sigma(U_{pq})$, it follows that U_{pq} cannot be the empty sequence. Thus, $\mathrm{supp}(U)$ contains an element of order $pq = \exp(G)$ and hence by (3.3), we have

$$d \text{ divides } pq - 2\,. \tag{3.4}$$

CASE 3.(i): $\gcd(pq-2, \mathsf{D}(G)-2) = 1$.

Then $d = 1$ by (3.2) and (3.4).

CASE 3.(ii): $\gcd(pq-2, p+q-3) = 1$.

We first note that $\gcd(pq-2, p+q-3) = 1$ implies that p, q are both odd, $\gcd(pq-2, p-2) = 1$, $\gcd(pq-2, q-2) = 1$, and

$$\gcd(pq-2, p-1) = 1\,. \tag{3.5}$$

If there exists an element $h \in \mathrm{supp}(U)$ such that $\mathrm{ord}(h) \ne pq$, then d divides $p-2$ or $q-2$ by (3.3). In each case we infer that $d = 1$ by (3.4). Now, we assume that every element of $\mathrm{supp}(U)$ has order pq.

Let G_1 and G_2 be subgroups of G such that $G = G_1 \oplus G_2$, $G_1 \cong C_p^r$, and $G_2 \cong C_q^s$. Since G is not cyclic, we have $r \ge 2$ or $s \ge 2$. By symmetry, we may assume that $r \ge s$. Every element g of A can be written uniquely as $g = u_g + v_g$, where $u_g \in G_1$ and $v_g \in G_2$. Hence $\langle u_g \colon g \in A\rangle = G_1$ and $\{u_g \colon g \in A\}$ contains a basis of G_1. We choose $g_1, \ldots, g_r \in A$ such that $(u_1 = u_{g_1}, \ldots, u_r = u_{g_r})$ is a basis of G_1. We distinguish two cases.

First, suppose that $(v_1 = v_{g_1}, \ldots, v_r = v_{g_r}) \in G_2^r$ is independent. Since $r \ge s = \mathsf{r}(G_2) = s$, we infer that $r = s$. Therefore, $G \cong C_{pq}^r$ and $(g_1, \ldots, g_r)$ is a basis of G. The assertion follows by Lemma 3.1.

Now, suppose that $(v_1 = v_{g_1}, \ldots, v_r = v_{g_r})$ is not independent. Since $\langle v_1, \ldots, v_r\rangle$ is a q-group, there exists $I \subset [1,r]$ such that $(v_i)_{i\in I}$ is a basis of $\langle v_1, \ldots, v_r\rangle$. After renumbering if necessary, we may assume that $I = [1,y]$, where $y \in [1, r-1]$. Then $(g_1, \ldots, g_y)$ is independent and p is the minimal integer such that $pg_r \in \langle g_1, \ldots, g_y\rangle$. If there exists $i \in [1,y]$ such that $pg_r \in \langle g_i\rangle$, then there exists $k \in [1, pq-1]$ such that $g_r^p g_i^k$ and $(-g_r)^p g_i^{pq-k}$ are atoms, whence it follows by $(g_r^p g_i^k)\,((-g_r)^p g_i^{pq-k}) = (g_r(-g_r))^p\, g_i^{pq}$ that d divides $p-1$. The assertion follows by (3.5). Otherwise there exist $J \subset [1,y]$ with $|J| \ge 2$ and $k_j \in [1, pq-1]$ for every $j \in J$ such that $pg_r = \sum_{j\in J} k_j g_j$. Now the assertion follows by Lemma 3.1.

CASE 3.(iii): $q = 2$ and $p-1$ is a power of 2.

If there is an element $g \in \mathrm{supp}(U)$ such that $\mathrm{ord}(g) = p$, then d divides $\gcd(p-2, 2p-2) = 1$ by (3.3) and (3.4), whence $d = 1$. Now, we suppose that $\mathrm{supp}(U)$ contains no element of order p. Since d divides $2(p-1)$ and $p-1$ is a power of 2, it suffices to prove that d divides an odd number.

Let G_1 and G_2 be subgroups of G such that $G = G_1 \oplus G_2$, $G_1 \cong C_p^r$, and $G_2 \cong C_2^s$. Then every element g of $\mathrm{supp}(U)$ can be written uniquely as $g = u_g + v_g$, where $u_g \in G_1$ and $v_g \in G_2$. Hence $\langle u_g \colon g \in \mathrm{supp}(U)\rangle = G_1$ and $\{u_g : g \in \mathrm{supp}(U)\}$ contains a basis of G_1. We choose $g_1, \ldots, g_r \in \mathrm{supp}(U)$ such that $(u_1 = u_{g_1}, \ldots, u_r = u_{g_r})$ is a basis of G_1. Since $\mathrm{supp}(U)$ has no element of order p, it follows that $\mathrm{ord}(g_i) = 2p$ for all $i \in [1, r]$.

We set

$$T_0 = \prod_{g \in \mathrm{supp}(U) \text{ with } \mathrm{ord}(g)=2} g \quad \text{and} \quad T_i = \prod_{g \in \langle g_i \rangle \text{ with } \mathrm{ord}(g)=2p} g^{\mathsf{v}_g(U)} \ \text{ for all } \ i \in [1, r] .$$

Assume to the contrary that $U = T_0 T_1 \ldots T_r$. Then $\sigma(T_i)$ has order 2 for every $i \in [1, r]$. If $|T_i| \ge p + 1 = \mathsf{D}(C_p) + 1$, then there exists a subsequence T_i' of T_i such that $1 \le |T_i'| \le p$ and $\sigma(T_i')$ has order 2, which implies that T_i' or $T_i T_i'^{-1}$ is a nonempty zero-sum sequence, a contradiction to the minimality of U. Thus $|T_i| \le p$ for every $i \in [1, r]$. Since T_0 is zero-sum free, we infer that $|T_0| \le r + s$. Hence $|U| \le pr + (r + s) = (p + 1)r + s < \mathsf{D}^*(G) \le \mathsf{D}(G)$, a contradiction.

Therefore, $U \ne T_0 T_1 \ldots T_r$, whence there is an element $h \in \mathrm{supp}(U) \setminus \{g_1, \ldots, g_r\}$ such that $\mathrm{ord}(h) = 2p$ and $h \notin \langle g_i \rangle$ for any $i \in [1, r]$. Let $I \subset [1, r]$ be a minimal subset such that $u_h \in \langle u_i \colon i \in I\rangle$. After renumbering if necessary, we may assume that $I = [1, x]$, where $x \in [1, r]$.

Suppose $x = 1$. Note that $h \notin \langle g_1 \rangle$ and $2h \in \langle g_1 \rangle$. Then there exists $k \in [1, 2p - 1]$ such that $h^2 g_1^k$ is a minimal zero-sum sequence, and then the same is true for $(-h)^2 g_1^{2p-k}$. Since $(h^2 g_1^k)((-h)^2 g_1^{2p-k}) = (h(-h))^2 g_1^{2p}$, we obtain $d = 1$.

Suppose $x \ge 2$ and $v_h \in \langle v_1, \ldots, v_x \rangle$, where $v_i = v_{g_i}$ for all $i \in [1, x]$. For all $i \in [1, x]$, let $k_i \in [1, p-1]$ be such that $u_h = k_1 u_1 + \ldots + k_x u_x$. The elements $v_h, v_1, \ldots, v_x$ have order 2. After renumbering if necessary, we may assume that $v_h v_1 \ldots v_y$ is a minimal zero-sum sequence over G_2 for some $y \in [1, x]$. Therefore, the tuple $(v_1, \ldots, v_y)$ is independent, whence $(g_1, \ldots, g_y)$ is independent. If $y = x$, then $h \in \langle g_1, \ldots, g_x \rangle$ and the assertion follows by Lemma 3.1. Suppose $y < x$. Then $h \notin \langle g_1, \ldots, g_y \rangle$ and p is the minimal integer such that $ph \in \langle g_1, \ldots, g_y \rangle$. If y is even, then $h^p g_1^p \ldots g_y^p$ is a minimal zero-sum sequence of odd length, whence d divides an odd number by (3.2). Suppose y is odd. We replace g_i by $-g_i$, u_i by $-u_i$, and k_i by $p - k_i$, if necessary, in order to make k_i to be odd for all $i \in [1, y]$ and k_j to be even for all $j \in [y + 1, x]$. Then

$$W = (-h) g_1^{k_1} \ldots g_x^{k_x} \quad \text{and} \quad V = h^{p-1} (-g_1)^{p-k_1} \ldots (-g_y)^{p-k_y} g_{y+1}^{k_{y+1}} \ldots g_x^{k_x}$$

are minimal zero-sum sequences over $\mathrm{supp}(U(-U))$, $T = g_{y+1}^{pk_{y+1}} \ldots g_x^{pk_x}$ is a zero-sum sequence,

$$W^p = T \ ((-h) g_1 \ldots g_y)^p \ \prod_{i=1}^{y} (g_i^{2p})^{\frac{k_i - 1}{2}} \quad \text{and} \quad V^p = T \ ((-h)^{2p})^{\frac{p-1}{2}} \prod_{i=1}^{y} ((-g_i)^{2p})^{\frac{p-k_i}{2}} .$$

If $\ell_0 \in \mathsf{L}(T)$, then d divides

$$\left(\ell_0 + \frac{p-1}{2} + \sum_{i \in [1,y]} \frac{p - k_i}{2} - p \right) - \left(\ell_0 + 1 + \sum_{i \in [1,y]} \frac{k_i - 1}{2} - p \right) = \frac{p-1}{2} + \frac{p+1}{2} y - \sum_{i=1}^{y} k_i - 1$$

Since y is odd and k_i are odd for all $i \in [1, y]$, it follows that $\frac{p-1}{2} + \frac{p+1}{2} y - \sum_{i=1}^{y} k_i - 1 \equiv 1 \pmod 2$, whence d divides an odd number.

Suppose $x \ge 2$ and $v_h \notin \langle v_1, \ldots, v_x \rangle$. Then $h \notin \langle g_1, \ldots, g_x \rangle$ and $2h \in \langle g_1, \ldots, g_x \rangle$. Let $2u_h = k_1 u_1 + \ldots + k_x u_k$, where $k_i \in [1, p - 1]$. We replace g_i by $-g_i$, u_i by $-u_i$, and k_i by $p - k_i$, if necessary, in order to make k_i to be even for all $i \in [1, x]$. If $(g_1, \ldots, g_x)$ is independent, then the assertion follows by Lemma 3.1. Otherwise the tuple $(v_1 = v_{g_1}, \ldots, v_x = v_{g_x})$ is not independent. After renumbering if necessary, we may assume that $v_1 \ldots v_y$ is a minimal zero-sum sequence over G_2, where $y \in [2, x]$, whence $g_1^p \ldots g_y^p$ is a minimal zero-sum sequence. If y is odd, then d divides an odd number by (3.2). Suppose

y is even. Then $W = (-h)^2 g_1^{k_1} \dots g_x^{k_x}$ and $V = (-h)^2(-g_1)^{p-k_1} \dots (-g_y)^{p-k_y} g_{y+1}^{k_{y+1}} \dots g_x^{k_x}$ are minimal zero-sum sequences, $T = (-h)^{2p} g_{y+1}^{pk_{y+1}} \dots g_x^{pk_x}$ is a zero-sum sequence,

$$W^p = T \prod_{i=1}^{y} (g_i^{2p})^{\frac{k_i}{2}} \quad \text{and} \quad V^p = T\ ((-g_1)\dots(-g_y))^p \prod_{i=1}^{y}((-g_i)^{2p})^{\frac{p-k_i-1}{2}} .$$

If $\ell_0 \in \mathsf{L}(T)$, then d divides

$$\left(\ell_0 + 1 + \sum_{i\in[1,y]} \frac{p-k_i-1}{2} - p\right) - \left(\ell_0 + \sum_{i\in[1,y]} \frac{k_i}{2} - p\right) = 1 + \frac{p-1}{2}y - \sum_{i=1}^{y} k_i .$$

Since y is even and k_i are even for all $i \in [1, y]$, it follows that $1 + \frac{p-1}{2}y - \sum_{i=1}^{y} k_i \equiv 1 \pmod 2$, whence d divides an odd number.

CASE 3.(iv): $q = 2$ and $r = 1$.

Let $h \in \operatorname{supp}(U)$ such that $\operatorname{ord}(h) = 2p$. Since $\langle h \rangle$ is a direct summand of G, there is a subgroup G_1 of G with $G \cong G_1 \oplus \langle h \rangle$, whence $G_1 \cong C_2^s$. Every element g of $\operatorname{supp}(U)$ can be written uniquely as $g = u_g + v_g$, where $u_g \in G_1$ and $v_g \in \langle h \rangle$. Hence $\langle u_g \colon g \in \operatorname{supp}(U) \setminus \{h\} \rangle = G_1$ and $\{u_g \colon g \in \operatorname{supp}(U) \setminus \{h\}\}$ contains a basis of G_1. We choose $g_1, \dots, g_s \in \operatorname{supp}(U) \setminus \{h\}$ such that $(u_1 = u_{g_1}, \dots, u_s = u_{g_s})$ is a basis of G_1. We distinguish two cases.

Suppose $\operatorname{ord}(g_i) = 2$ for every $i \in [1, s]$. Then the tuple $(g_1, \dots, g_s)$ is independent, whence the tuple $(g_1, \dots, g_s, h)$ forms a basis of G. Then the assertion follows by Lemma 3.1.

Suppose there exists $i \in [1, s]$ such that $\operatorname{ord}(g_i) = 2p$. Then 2 is the minimal integer such that $2g_i \in \langle h \rangle$, whence there exists $k \in [1, 2p-1]$ such that both $g_i^2 h^k$ and $(-g_i)^2 h^{2p-k}$ are minimal zero-sum sequences. Then $d = 1$ because

$$\left(g_i^2 h^k\right) \left((-g_i)^2 h^{2p-k}\right) = \left(g_i(-g_i)\right)^2 h^{2p} .$$

CASE 4: G is a group with $\exp(G) \in [3, 11] \setminus \{8\}$.

If $\exp(G)$ is prime, then the claim follows from CASE 2 (with $s_1 = s_2 = 1$). The case, when $\exp(G) \in \{4, 9\}$, is also handled in CASE 2, and the case $\exp(G) \in \{6, 10\}$ is handled in CASE 3.(iii). □

References

[1] G. Bhowmik and J.-C. Schlage-Puchta, *Davenport's constant for groups of the form* $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$, Additive Combinatorics (A. Granville, M.B. Nathanson, and J. Solymosi, eds.), CRM Proceedings and Lecture Notes, vol. 43, American Mathematical Society, 2007, pp. 307 – 326.

[2] F. Chen and S. Savchev, *Long minimal zero-sum sequences in the groups* $C_2^{r-1} \oplus C_{2k}$, Integers **14** (2014), Paper A23.

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

[4] A. Geroldinger, M. Liebmann, and A. Philipp, *On the Davenport constant and on the structure of extremal sequences*, Period. Math. Hung. **64** (2012), 213 – 225.

[5] A. Geroldinger and I. Ruzsa, *Combinatorial Number Theory and Additive Group Theory*, Advanced Courses in Mathematics - CRM Barcelona, Birkhäuser, 2009.

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

[7] A. Geroldinger and Q. Zhong, *Long sets of lengths with maximal elasticity*, Can. J. Math. **70** (2018), 1284 – 1318.

[8] ______, *Factorization theory in commutative monoids*, Semigroup Forum **100** (2020), 22 – 51.

[9] B. Girard, *An asymptotically tight bound for the Davenport constant*, J. Ec. Polytech. Math. **5** (2018), 605 – 611.

[10] B. Girard and W.A. Schmid, *Direct zero-sum problems for certain groups of rank three*, J. Number Theory **197** (2019), 297 – 316.

[11] D.J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics 30, Springer, Cham, 2013.

[12] Chao Liu, *On the lower bounds of Davenport constant*, J. Comb. Theory, Ser. A **171** (2020), 105162, 15pp.

[13] W.A. Schmid, *A realization theorem for sets of lengths*, J. Number Theory **129** (2009), 990 – 999.

[14] ______, *Some recent results and open problems on sets of lengths of Krull monoids with finite class group*, in Multiplicative Ideal Theory and Factorization Theory, Springer, 2016, pp. 323 – 352.

Institut für Mathematik und wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, NAWI Graz, Heinrichstrasse 36, 8010 Graz, Austria

Email address: aqsa.bashir@uni-graz.at,alfred.geroldinger@uni-graz.at,qinghai.zhong@uni-graz.at

URL: https://imsc.uni-graz.at/geroldinger, https://imsc.uni-graz.at/zhong/