A NONLINEAR BOUND FOR THE NUMBER OF SUBSEQUENCE SUMS

VSEVOLOD F. LEV

Abstract. We show that a finite zero-sum-free sequence α over an abelian group has at least $c|\alpha|^{4/3}$ distinct subsequence sums, unless α is "controlled" by a small number of its terms; here $|\alpha|$ denotes the number of terms of α, and $c > 0$ is an absolute constant.

1. Background and motivation

A classical object of study of the combinatorial number theory is the Davenport constant of a finite abelian group, defined to be the smallest integer n such that every n-term sequence of group elements is guaranteed to have a nonempty subsequence with the zero sum of its terms. According to Olson [O69a], the problem of finding this group invariant was raised by Davenport at the Midwestern Conference on Group Theory and Number Theory held in the Ohio State University in April 1966, in connection with the investigation of the class groups of the algebraic number fields. However, this exact problem has been considered three years earlier by Rogers [Ro63] who, in turn, refers to a personal communication with C. Sudler. Other early papers where this or related problems are studied include [EBK67, B68, EB69, O69b].

The precise value of the Davenport constant is still unknown in general, despite a large number of partial results. Eggleton and Erdős [EE72, Theorem 3] have shown that if the underlying group G is not cyclic, then its Davenport constant does not exceed $(|G| + 1)/2$; that is, if α is a finite sequence free of nonempty zero-sum subsequences, then its length satisfies $|\alpha| \le |G|/2$. This was improved by Olson and White [OW77] who proved that if α is free of nonempty zero-sum subsequences, then it has at least $2|\alpha|$ distinct subsequence sums provided that the subgroup generated by the elements of α is not cyclic; here the empty subsequence with the zero sum is counted, too. Indeed, the result of Olson-White applies to infinite and nonabelian groups as well.

Evidently, the reason for Eggleton-Erdős and Olson-White to ignore the cyclic groups is that for these groups the Davenport constant is easily seen to be equal to

2020 *Mathematics Subject Classification.* Primary 11P70; Secondary 11B13, 11B75.

Key words and phrases. Zero-sum-free sequences, Minimal zero-sum sequences, Subset sums, Inverse zero-sum problems, Hilbert cube.

the order of the group. This simple fact suggests, nevertheless, an interesting research avenue to explore: what is the structure of "long" sequences free of nonempty zero-sum subsequences in the finite cyclic groups?

We introduce some basic terminology to proceed.

A finite sequence of elements of an abelian group is called *zero-sum-free* if all of its nonempty subsequences have a nonzero sum of their terms; the sequence is *minimal zero-sum* if the sum of all of its terms is zero, while all of its nonempty proper subsequences have nonzero term sum. The two classes of sequences are actually quite close to each other due to the observation that removing any term from a minimal zero-sum sequence results in a zero-sum-free sequence, and conversely, any zero-sum-free sequence can be turned into a minimal zero-sum sequence by appending an appropriate group element to it.

Suppose that the underlying group G is cyclic of finite order. Addressing the above-mentioned problem, Gao [G00] characterized minimal zero-sum sequences α of length $n := |\alpha| > 2|G|/3 + O(1)$; specifically, for any such sequence there is a generating element $g \in G$ and positive integers $x_1, \dots, x_n$ with $x_1 + \dots + x_n = |G|$ such that the n terms of α are $x_1 g, \dots, x_n g$. Savchev and Chen [SC07] and, independently, Yuan [Y07] have shown that, indeed, Gao's characterization stays true for all zero-sum-free sequences of length $|\alpha| > |G|/2$. In [L], these results are extended the same way the theorem of Olson-White extends the result of Eggleton-Erdős; namely, [L, Theorem 2] shows that the assumption $|\alpha| > |G|/2$ can be relaxed to $|\alpha| > |\Sigma(\alpha)|/2$, where $\Sigma(\alpha)$ is the set of all subsequence sums of α, including the empty subsequence.

A significant further progress was made by Savchev and Chen [SC17] who have introduced a subtle and involved argument to classify minimal zero-sum sequences α in a finite cyclic group G, given that $|\alpha| \ge \lfloor |G|/3 \rfloor + 3$. As shown in [SC17], under this assumption there exist group elements $u \ne 0$ and v satisfying a number of conditions such that all terms or α are contained either in the subgroup $\langle u \rangle$ generated by u, or in the coset $v + \langle u \rangle$. We omit the (somewhat technical) exact statement of this result referring the interested reader to [SC17] instead.

2. The main result

In this section we use the notation which will not be introduced formally until Section 3. We believe, however, that our notation is standard enough to not cause any discomfort to the reader. Nevertheless, it may be worth remarking that $\Sigma(\alpha)$ denotes the set of *all* subsequence sums of the sequence α, including the empty subsequence, while $\Sigma^\times(\alpha)$ is defined the same way, except that the empty subsequence is ignored; say, if α is the sequence of integers containing one term equal to -3 and two terms equal to 2, then $\Sigma(\alpha) = \{-3, -1, 0, 1, 2, 4\}$, while $\Sigma^\times(\alpha) = \{-3, -1, 1, 2, 4\}$. By

$\operatorname{supp}(\alpha)$ we denote the set of all terms of α, and by $|\alpha|$ the length (that is, the number of terms) of α.

The aim of the present paper is to go beyond the Savchev-Chen bound $|\alpha| \geq \lfloor |G|/3 \rfloor + 3$.

Theorem 1. *Suppose that $C \geq 2$ is an integer, and α is a zero-sum-free sequence of length $n := |\alpha| \geq (4C)^3$ over an abelian group. If $|\Sigma(\alpha)| < Cn - C^2\sqrt{6n}$, then there are an integer $h > n - C\sqrt{6n}$ and an element $a \in \operatorname{supp}(\alpha)$ of order $\operatorname{ord}(a) > h + 1$ such that, letting $P := \{a, 2a, , \dots, ha\}$, we have $\Sigma(\operatorname{supp}(\alpha)) + P \subseteq \Sigma^\times(\alpha)$.*

Moreover, there is a set $X \subseteq \Sigma(\operatorname{supp}(\alpha))$ with $0 \in X$ and $|X| \leq C - 1$ such that $\Sigma(\operatorname{supp}(\alpha)) \subseteq X + P - P$; in particular, each term of α can be written as $x + ta$ with an element $x \in X$ and an integer $t \in [-(h-1), h-1]$.

Remark 1. The arithmetic progression $P - P = \{-(h-1)a, \dots, (h-1)a\}$ can be considered as a "local approximation" to the subgroup $\langle a \rangle$ generated by a. The assertion of the theorem remains true, but becomes weaker with $P - P$ replaced by $\langle a \rangle$.

Remark 2. The translates $x + P - P$ with $x \in X$ are not guaranteed to be pairwise disjoint, but it is immediate from the proof that the translates $x + P$ are disjoint.

Remark 3. The bound $|X| \leq C - 1$ is best possible. To see this, fix a positive integer s, set $C := 2^s + 1$, choose linearly independent vectors $e_0, e_1, \dots, e_s$ in a vector space over a field of characteristic 0, and consider the sequence $\alpha = e_0^{n-s} e_1 \cdots e_s$. We have

$$\Sigma(\alpha) = \{x_1 e_1 + \cdots + x_s e_s + t e_0 \colon x_1, \dots, x_s \in \{0, 1\},\ 0 \leq t \leq n - s\}$$

whence

$$|\Sigma(\alpha)| = 2^s(n - s + 1) = (C-1)n - (C-1)(s-1) < Cn - C^2\sqrt{6n}$$

provided that n is sufficiently large. On the other hand, one cannot find an arithmetic progression P and a set X of size $|X| \leq C - 2 = 2^s - 1$ such that $\Sigma(\operatorname{supp}(\alpha)) \subseteq X + P$ since the right-hand side is contained in a system of $|X|$ lines, each of them covering at most two vertices of the $(s+1)$-dimensional cube $\Sigma(e_0 e_1 \cdots e_s) = \Sigma(\operatorname{supp}(\alpha))$.

Remark 4. The assumptions $n \geq (4C)^3$ and $|\Sigma(\alpha)| < Cn - C^2\sqrt{6n}$ essentially mean that our result applies to zero-sum-free sequences satisfying $|\Sigma(\alpha)| < \frac{1}{4}|\alpha|^{4/3}$. Conjecturally, the former assumption can be dropped or at least relaxed very significantly, and the latter can be replaced with the weaker $|\Sigma(\alpha)| \leq Cn - (C-1)^2$. If true, this is best possible as it follows by considering the sequence $\alpha := g_1^{n-C+1} g_2^{C-1}$, where g_1 and g_2 are independent group elements; in this example (originating from [L99, Examples 1 and 2]) we have $|\Sigma(\alpha)| = Cn - (C-1)^2 + 1$, while $\Sigma(\alpha)$ is not a union of $C - 1$ or less arithmetic progressions with the same difference.

Some minor adjustments of the constants can be obtained by fine-tuning our calculations, but we prefer instead to keep the argument clean and reasonably simple.

Remark 5. Theorem 1 markedly lacks the precision of the result of Savchev and Chen, the latter establishing a necessary and sufficient condition for α to be minimal zero-sum under the assumption $|\alpha| \ge \lfloor |G|/3 \rfloor + 3$, where G is the underlying group. On the other hand, Theorem 1 is not restricted to the coefficient $C = 3$, allowing C to be *any* positive integer. Also, the assumption $|\Sigma(\alpha)| < C(1 + o(1))|\alpha|$ is substantially weaker than the assumption $|\alpha| > (C^{-1} + o(1))|G|$. Finally, our result applies to any abelian group, not necessarily finite or cyclic. As explained in [SC17], the extension from the finite cyclic to arbitrary abelian groups is meaningless in the situation where $|\alpha| \ge \lfloor |G|/3 \rfloor + 3$; however, it makes perfect sense in the settings of Theorem 1.

We now briefly outline the idea behind the proof.

The crucial role is played by the transfer operation introduced in Section 5. The operation modifies a given sequence α so that, in particular, the subsequence sum set $\Sigma(\alpha)$ does not increase, while the length $|\alpha|$ either increases, or stays the same, but in the latter case the sequence α becomes, loosely speaking, "more concentrated". Moreover, the support $\operatorname{supp}(\alpha)$ stays unchanged, and the property of being zero-sum-free is preserved. Having applied the transfer operation sufficiently many times, we finally reach a zero-sum-free sequence which is stable under further applications of the operation. This resulting stable sequence turns out to contain a term of very large multiplicity, making it easier to analyze than a "generic" zero-sum-free sequence, and its relation to the original sequence α is strong enough to read off the properties of the latter from those of the former.

We introduce the notation used in the next section. Three basic results needed for the proof of Theorem 1 are quoted in Section 4. In Section 5 we define the transfer operation and study its properties. Theorem 1 is proved in the concluding Section 6.

3. Notation

From now on, by a *sequence* we mean a finite sequence of elements of an abelian group. Informally, a sequence is an unordered list of the group elements, with repetitions allowed. Formally, sequences are elements of the abelian monoid freely generated by the elements of the group. We use multiplicative notation for the monoid operation; thus, for instance, the "concatenation" of the sequences $\alpha_1, \dots, \alpha_k$ is the product sequence $\alpha_1 \cdots \alpha_k$.

Up to the order of the factors, every sequence α can be uniquely written in the form $\alpha = a_1^{m_1} \cdots a_s^{m_s}$ where $s \ge 0$ is an integer, $a_1, \dots, a_s$ are pairwise distinct group elements, and $m_1, \dots, m_s$ are positive integers. The elements a_i are called the *terms* of

α, and the integers m_i are the *multiplicities* of the corresponding terms. Alternatively, the terms of α are group elements dividing α, and the multiplicity of a group element a in α, denoted $\nu_\alpha(a)$ below, is the largest integer $m \geq 0$ such that $a^m \mid \alpha$.

For a nonempty sequence α, by $\mathsf{H}(\alpha)$ we denote the largest multiplicity of a term of α: that is, $\mathsf{H}(\alpha) = \max\{\nu_\alpha(a) \colon a \mid \alpha\}$. More generally, by $\mathsf{H}_k(\alpha)$ we denote the kth largest multiplicity of a term of α; thus, $\mathsf{H}(\alpha) = \mathsf{H}_1(\alpha)$. By convention, $\mathsf{H}_k(\varnothing) = 0$ for all $k \geq 1$.

The *length* of α is defined by $|\alpha| := m_1 + \cdots + m_s$. We also let $|\alpha|_2 := {m_1}^2 + \cdots + m_s^2$.

The set $\{a_1, \ldots, a_s\}$ is called the *support* of α and denoted $\operatorname{supp}(\alpha)$; therefore, $s = |\operatorname{supp}(\alpha)|$, and for a group element a, we have $a \mid \alpha$ if and only if $a \in \operatorname{supp}(\alpha)$, meaning that a is a term of α.

Subsequences of α are sequences α' with $\alpha' \mid \alpha$. Writing $\alpha = a_1^{m_1} \cdots a_s^{m_s}$ with s, a_i, and m_i as above, α' is a subsequence of α if and only if $\alpha' = a_1^{m_1'} \cdots a_s^{m_s'}$ where $0 \leq m_i' \leq m_i$ for all $i = 1, \ldots, s$.

We denote by $\sigma(\alpha)$ the sum of all terms of α with multiplicities counted: $\sigma(\alpha) = m_1 a_1 + \cdots + m_s a_s$.

The subsequence sum set of α is the set

$$\Sigma(\alpha) := \{\sigma(\alpha') \colon \alpha' \mid \alpha\}.$$

We also write

$$\Sigma^\times(\alpha) := \{\sigma(\alpha') \colon \alpha' \mid \alpha,\ \alpha' \neq \varnothing\};$$

thus, $\Sigma^\times(\varnothing) = \varnothing$ and $\Sigma(\alpha) = \Sigma^\times(\alpha) \cup \{0\}$. The sequence α is *zero-sum-free* if it does not have a nonempty zero-sum subsequence; that is, if $0 \notin \Sigma^\times(\alpha)$.

For subsets $A_1, \ldots, A_k$ of an abelian group, we let

$$A_1 + \cdots + A_k := \{a_1 + \cdots + a_k \colon a_1 \in A_1, \ldots, a_k \in A_k\}$$

and

$$A_i - A_j := \{a_i - a_j \colon a_i \in A_i,\ a_j \in A_j\}.$$

The subgroup generated by a group element g is denoted by $\langle g \rangle$, and the order of g by $\operatorname{ord}(g)$.

4. Basic Facts

We need the following, well-known, lower-bound estimates for the size of the subsequence sum set of a zero-sum-free sequence.

Lemma 1 ([SF01, Theorem 2.5]; see also [GH06, Proposition 5.3.5])**.** *If α is a finite zero-sum-free sequence over an abelian group, then*

$$|\Sigma(\alpha)| \geq 2|\alpha| - \mathsf{H}(\alpha) + 1 \geq |\alpha| + |\operatorname{supp}(\alpha)|.$$

Lemma 2 ([BEN75, Proof of Lemma 1]; see also [GH06, Theorem 5.3.1])**.** *Suppose that k is a positive integer, and $\alpha = \alpha_1 \cdots \alpha_k$ is a factorization of a finite, zero-sum-free sequence α over an abelian group. Then*

$$|\Sigma(\alpha)| \geq |\Sigma(\alpha_1)| + \cdots + |\Sigma(\alpha_k)| - (k-1).$$

Lemma 3 ([GHHLLP20, Theorem 1.1])**.** *If A is a finite, zero-sum-free* subset *of an abelian group (so that $\mathsf{H}(A) = 1$), then $|\Sigma(A)| \geq 1 + \frac{1}{6}|A|^2$.*

5. The transfer operation

A simple construction presented in Section 6 after the statement of Lemma 7 shows that a zero-sum-free sequence α with about $C|\alpha|$ subsequence sums may fail to contain a term of multiplicity larger than, roughly, $|\alpha|/C$. The machinery of transfer operation developed in this section supplies a sort of a poor man's compensation for the lack of high-multiplicity terms.

Throughout this section, α is a finite sequence of elements of an abelian group of length $n := |\alpha|$, written as $\alpha = a_1^{m_1} \dots a_s^{m_s}$ where $s \geq 2$, the terms $a_1, \dots, a_s$ are pairwise distinct, and the exponents $m_1, \dots, m_s$ are positive integers.

Lemma 4. *Suppose that $i, j \in [1, s]$, $i \neq j$, and $v < m_j$ is a positive integer. Consider the sequence $\alpha' = a_1^{m'_1} \cdots \alpha_s^{m'_s}$ defined by $m'_i = m_i + v$, $m'_j = m_j - v$, and $m'_k = m_k$ for $k \in [1, s] \setminus \{i, j\}$. Then $|\alpha'|_2 > |\alpha|_2$ if and only if $v > m_j - m_i$.*

Proof. It suffices to notice that the inequality $(m_i+v)^2 + (m_j-v)^2 > m_i^2 + m_j^2$ reduces to $v > m_j - m_i$. □

Fix indices $i, j \in [1, s]$ with $i \neq j$ and write $\alpha = a_i^{m_i} a_j^{m_j} \rho$ where ρ is a sequence with $a_i, a_j \notin \operatorname{supp}(\rho)$. If there exist positive integers $u \leq m_i + 1$ and $v \leq m_j - 1$ such that $ua_i = va_j$, and either $u > v$, or $u = v > m_j - m_i$, then we say that the sequence $a_i^{m_i+u} a_j^{m_j-v} \rho$ is obtained from the original sequence α by the transfer operation. We also say in this case that the (ordered) pair (i, j) is *unstable*. If u and v with the specified properties do not exist, then we say that (i, j) is *stable*. If both (i, j) and (j, i) are stable pairs, then we say that the set $\{i, j\}$ is stable. Finally, we say that the original sequence α is stable if all ordered pairs (i, j) are stable; equivalently, if all two-element subsets $\{i, j\} \subseteq [1, s]$ are stable.

We remark that the inequality $v \leq m_j - 1$ ensures that $\operatorname{supp}(\alpha)$ is not affected by the transfer operation, while the condition $u \leq m_i + 1$ is needed to guarantee that the set $\Sigma^\times(\alpha)$ of subsequence sums does not increase; see Lemma 6 below.

Lemma 5. *Suppose that $i, j \in [1, s]$, $i \neq j$.*

(i) *If* $m_i \geq m_j$, *then for the pair* (i,j) *to be unstable it is necessary and sufficient that there exist positive integers* $u \leq m_i+1$ *and* $v \leq m_j-1$ *such that* $ua_i = va_j$ *and* $u \geq v$.

(ii) *For the pair* (j,i) *to be unstable it is necessary and sufficient that there exist positive integers* $u \leq m_i - 1$ *and* $v \leq m_j + 1$ *such that* $ua_i = va_j$ *and either* $u < v$, *or* $u = v > m_i - m_j$.

Proof. The first assertion follows directly from the definition of a stable pair. The second assertion is the definition of an unstable pair in disguise, which is immediately seen by interchanging i and j and, simultaneously, u and v. □

Corollary 1. *Suppose that* $i,j \in [1,s]$, $i \neq j$, *and* $m_i \geq m_j$. *If there exist positive integers* $u \leq m_i + 1$ *and* $v \leq m_j - 1$ *such that* $ua_i = va_j$, *then* $\{i,j\}$ *is unstable.*

Proof. Suppose that $u \leq m_i + 1$ and $v \leq m_j - 1$ satisfy $ua_i = va_j$. If $u \geq v$, then (i,j) is unstable by Lemma 5 (i). If $u < v$ then $u < m_j - 1 \leq m_i - 1$ and (j,i) is unstable by Lemma 5 (ii). □

For $j \in [1,s]$, we write $P_j := \{0, a_j, 2a_j, \ldots, m_j a_j\}$ and $P'_j := \{0, a_j, 2a_j, \ldots, (m_j - 1)a_j\}$. Notice that if α is zero-sum-free, then $|P_j| = m_j$.

Corollary 2. *Suppose that* $i,j \in [1,s]$, $i \neq j$, *and* $m_i \geq m_j$. *If* $\{i,j\}$ *is stable, then* $P_i \cap P'_j = \{0\}$.

Proof. If P_i and P'_j share a common element $g \neq 0$, then there exist positive integers $u \leq m_i$ and $v \leq m_j - 1$ such that $g = ua_i$ and $g = va_j$. Therefore $ua_i = va_j$ and $\{i,j\}$ is unstable by Corollary 1. □

Corollary 3. *Suppose that* α *is zero-sum-free, and that* $i,j \in [1,s]$, $i \neq j$, *and* $m_i \geq m_j$. *If* $\{i,j\}$ *is stable, then* $|P_i + P'_j| = (m_i+1)m_j$ *and, consequently,* $|\Sigma(\alpha)| \geq (m_i+1)m_j$.

Proof. It suffices to show that all sums $ua_i + va_j$ with $u \in [0, m_i]$, $v \in [0, m_j - 1]$ are pairwise distinct. To this end, suppose that $u'a_i + v'a_j = u''a_i + v''a_j$ with $u', u'' \in [0, m_i]$ and $v', v'' \in [0, m_j - 1]$. Then, letting $u := u'' - u'$ and $v := v' - v''$, we have $ua_i = va_j$ where $|u| \leq m_i$ and $|v| \leq m_j - 1$. If u and v are distinct from 0, then they are of the same sign since α is zero-sum-free; without loss of generality, both are positive, and then the equality $ua_i = va_j$ contradicts Corollary 1. □

Corollary 4. *Suppose that* α *is zero-sum-free, and that* $i,j \in [1,s]$, $i \neq j$, $m_i = \mathsf{H}_1(\alpha)$, *and* $m_j = \mathsf{H}_2(\alpha)$. *If* $\{i,j\}$ *is stable, then* $|\Sigma(\alpha)| - 2n \geq (m_i - 2)(m_j - 2) - 2$.

Proof. Let ρ be the sequence defined by $\alpha = a_i^{m_i} a_j^{m_j-1}\rho$. By Corollary 3 and Lemmas 2 and 1, and in view of $\mathsf{H}(\rho) \le m_j$,

$$\begin{aligned}
|\Sigma(\alpha)| &\ge |\Sigma(a_i^{m_i} a_j^{m_j-1})| + |\Sigma(\rho)| - 1\\
&\ge |P_i + P_j'| + (2(n - m_i - (m_j - 1)) - m_j + 1) - 1\\
&= (m_i + 1)m_j + 2n - 2m_i - 3m_j + 2\\
&= m_i m_j - 2m_i - 2m_j + 2 + 2n\\
&= (m_i - 2)(m_j - 2) - 2 + 2n.
\end{aligned}$$

□

Lemma 6. *If α' is obtained from α by a series of subsequent transfer operations, then*

$$\Sigma^\times(\alpha') \subseteq \Sigma^\times(\alpha),\ \operatorname{supp}(\alpha') = \operatorname{supp}(\alpha),$$

and

$$\text{either } |\alpha'| > |\alpha|, \text{ or } |\alpha'| = |\alpha| \text{ and } |\alpha|_2 < |\alpha'|_2.$$

Proof. Without loss of generality, we assume that α' is obtained from α by just one transfer operation; say, $\alpha = a_i^{m_i} a_j^{m_j}\rho$ and $\alpha' = a_i^{m_i+u} a_j^{m_j-v}\rho$ where $i, j \in [1, s]$, $i \ne j$, $a_i, a_j \notin \operatorname{supp}(\rho)$, $u \in [1, m_i + 1]$, $v \in [1, m_j - 1]$, $ua_i = va_j$, and either $u > v$, or $u = v > m_j - m_i$. We prove the inclusion $\Sigma^\times(\alpha') \subseteq \Sigma^\times(\alpha)$; the rest follows in a straightforward way from Lemma 4.

Comparing the identities

$$\Sigma^\times(a_i^{m_i} a_j^{m_j}\rho) = (\Sigma^\times(a_i^{m_i} a_j^{m_j}) + \Sigma(\rho)) \cup \Sigma^\times(\rho)$$

and

$$\Sigma^\times(a_i^{m_i+u} a_j^{m_j-v}\rho) = (\Sigma^\times(a_i^{m_i+u} a_j^{m_j-v}) + \Sigma(\rho)) \cup \Sigma^\times(\rho),$$

it suffices to show that $\Sigma^\times(a_i^{m_i+u} a_j^{m_j-v}) \subseteq \Sigma^\times(a_i^{m_i} a_j^{m_j})$.

Suppose thus that $g \in \Sigma^\times(a_i^{m_i+u} a_j^{m_j-v})$ and write $g = xa_i + ya_j$ where $x \in [0, m_i + u]$ and $y \in [0, m_j - v]$ are not both equal to 0. We show that $g \in \Sigma^\times(a_i^{m_i} a_j^{m_j})$. Indeed, the case $x \le m_i$ is trivial, while if $x \ge m_i + 1$, then $x - u \in [0, m_i]$ and $y + v \in [1, m_j]$; consequently, $g = (x - u)a_i + (y + v)a_j \in \Sigma^\times(a_i^{m_i} a_j^{m_j})$, as wanted. □

If α and α' are as in Lemma 6 and α is zero-sum-free, then so is α' in view of $\Sigma^\times(\alpha') \subseteq \Sigma^\times(\alpha)$. On the other hand, from $|\alpha'| \le |\Sigma(\alpha')| \le |\Sigma(\alpha)|$ we conclude that the possible lengths $|\alpha'|$ are uniformly bounded; therefore, in view of the second assertion of the lemma, having applied a series of subsequent transfer operations to any given zero-sum-free sequence, we eventually obtain a stable zero-sum-free sequence.

6. Proof of Theorem 1

We start with a lemma establishing a number of relations between the length and the largest multiplicities of the terms of a zero-sum-free sequence α with a small number of subset sums; most importantly, the lemma shows that if α is stable, then it has a term of very large multiplicity, while all other terms have small multiplicities.

Lemma 7. *Suppose that $C \ge 2$ is an integer, and α is a zero-sum-free sequence over an abelian group with $n := |\alpha| \ge 2$. Let $h_1 := \mathsf{H}_1(\alpha)$ and $h_2 := \mathsf{H}_2(\alpha)$. If $|\Sigma(\alpha)| < Cn$, then*

$$h_1 > n^2/(6|\Sigma(\alpha)|) > n/(6C) \tag{1}$$

and

$$h_1 > n - \sqrt{6h_2|\Sigma(\alpha)|} + h_2 > n - \sqrt{6Cnh_2} + h_2. \tag{2}$$

If, moreover, α is stable, $n \ge (4C)^3$, and $|\Sigma(\alpha)| < Cn - C^2\sqrt{6n}$, then

$$h_2 \le C - 1 \tag{3}$$

and

$$h_1 > n - C\sqrt{6n} + 1. \tag{4}$$

We remark that only the last estimate of the lemma is used outside of the lemma itself; however, we believe that the first three estimates can be useful elsewhere, and for this reason we have included them into the statement.

Interestingly, the bound (1) is best possible save for the coefficient $1/6$. To see this, fix integer numbers $k, s \ge 1$ and consider the sequence $\alpha := (g \cdot 2g \cdots sg)^k$ where g is a group element of sufficiently large order. We have $n := |\alpha| = ks$, $\mathsf{H}(\alpha) = k$, and

$$|\Sigma(\alpha)| = 1 + \frac{1}{2}s(s+1)\,k = \frac{1}{2}(s+1)n + 1.$$

Choosing $s := 2(C-1)$ we therefore get $|\Sigma(\alpha)| < Cn$ while $\mathsf{H}(\alpha) = n/s = n/(2C-2)$.

Proof of Lemma 7. For an integer $k \in [1, h_1]$, let A_k be the set of all terms of α of multiplicity at least k:

$$A_k := \{a \in \operatorname{supp}(\alpha) \colon \nu_\alpha(a) \ge k\};$$

thus, $\operatorname{supp}(\alpha) = A_1 \supseteq A_2 \supseteq \cdots$. Observing that α factors as $\alpha = A_1 \cdots A_{h_1}$, by Lemma 2 we get

$$|\Sigma(\alpha)| \ge |\Sigma(A_1)| + \cdots + |\Sigma(A_{h_1})| - h_1 + 1.$$

Since each of $A_1, \dots, A_{h_1}$ has all its elements pairwise distinct, Lemma 3 applies to give $|\Sigma(A_i)| \ge \frac{1}{6}|A_i|^2 + 1$, $i \in [1, h_1]$. Hence,

$$|\Sigma(\alpha)| > \frac{1}{6}\left(|A_1|^2 + \dots + |A_{h_1}|^2\right) \ge \frac{1}{6h_1}(|A_1| + \dots + |A_{h_1}|)^2 = \frac{n^2}{6h_1},$$

which proves (1).

To prove (2) we notice that if $h_2 = h_1$, then the first inequality of (2) is identical to the first inequality of (1), while otherwise there is a unique element $a \in \operatorname{supp}(\alpha)$ of multiplicity h_1, and we have $A_{h_2+1} = \dots = A_{h_1} = \{a\}$. Therefore, in the latter case, arguing as above,

$$\begin{aligned}|\Sigma(\alpha)| &> \frac{1}{6}\left(|A_1|^2 + \dots + |A_{h_2}|^2\right)\\ &\ge \frac{1}{6h_2}\left(|A_1| + \dots + |A_{h_2}|\right)^2\\ &= \frac{1}{6h_2}\left(n - h_1 + h_2\right)^2;\end{aligned}$$

this proves (2).

We now assume that α is stable and $n \ge (4C)^3$, and prove (3) and (4). We notice that, in view of (2), if (3) holds true, then so does (4), and we thus assume that (3) fails to hold; that is, $h_2 \ge C$.

By Corollaries 4 and 3 we have

$$|\Sigma(\alpha)| - 2n \ge (h_1 - 2)(h_2 - 2) - 2 \tag{5}$$

and

$$(h_1 + 1)h_2 \le |\Sigma(\alpha)| < Cn. \tag{6}$$

Combining (1) and (6) we obtain $h_2 < 6C^2$, and then

$$h_1 > n - \sqrt{36C^3 n} > \frac{1}{4}\,n$$

by (2) and the assumption $n \ge (4C)^3$. Reusing (6), we now get $h_2 < 4C$. On the other hand, from (5) and (2),

$$|\Sigma(\alpha)| - 2n \ge (n - \sqrt{6Cnh_2} + h_2 - 2)(h_2 - 2) - 2. \tag{7}$$

Considering h_2 as a variable ranging from C to $4C$, the right-hand side is a concave function of h_2 attaining at $h_2 = C$ the value

$$\begin{aligned}&(n - C\sqrt{6n} + C - 2)(C - 2) - 2\\ &\qquad \ge Cn - 2n - C(C-2)\sqrt{6n} - 2\\ &\qquad > Cn - C^2\sqrt{6n} - 2n,\\ &\qquad > |\Sigma(\alpha)| - 2n\end{aligned}$$

and at $h_2 = 4C$ the value

$$\begin{aligned}(n - 2C\sqrt{6n} + 4C - 2)&(4C - 2) - 2\\ &\geq 4Cn - 8C^2\sqrt{6n} - 2n\\ &> Cn - 2n\\ &> |\Sigma(\alpha)| - 2n.\end{aligned}$$

This shows that the right-hand side of (7) is larger than the left-hand side for all $C \leq h_2 \leq 4C$, a contradiction completing the proof of the lemma. □

We are eventually ready to prove Theorem 1.

Suppose that $C \geq 2$ is an integer, and α is a zero-sum-free sequence of length $n := |\alpha| \geq (4C)^3$ satisfying $|\Sigma(\alpha)| < Cn - C^2\sqrt{6n}$. We want to show that there are an integer $n - C\sqrt{6n} < h < n$, an element $a \in \operatorname{supp}(\alpha)$ of order $\operatorname{ord}(a) > h+1$, and a set $X \subseteq \Sigma(\operatorname{supp}(\alpha))$ with $0 \in X$ and $|X| \leq C-1$, such that $\Sigma(\operatorname{supp}(\alpha)) + P \subseteq \Sigma^\times(\alpha)$ and $\Sigma(\operatorname{supp}(\alpha)) \subseteq X + P - P$, where $P = \{a, 2a, \dots, ha\}$.

Consider a stable sequence α' obtained from α by a series of transfer operations. By Lemma 6 we have $\Sigma^\times(\alpha') \subseteq \Sigma^\times(\alpha)$, $\operatorname{supp}(\alpha') = \operatorname{supp}(\alpha)$, and $n' := |\alpha'| \geq n$; consequently, α' is zero-sum-free, and

$$|\Sigma(\alpha')| \leq |\Sigma(\alpha)| < Cn - C^2\sqrt{6n} \leq Cn' - C^2\sqrt{6n'}.$$

Notice also that $n' \geq n \geq (4C)^3$. Let $h' := \mathsf{H}(\alpha')$ be the largest multiplicity of a term of α'. We define $h := h' - 1$ and choose a to be a term of α' of multiplicity $\nu_{\alpha'}(a) = h'$. Thus, $h > n' - C\sqrt{6n'} \geq n - C\sqrt{6n}$ by (4), and $\operatorname{ord}(a) > h' = h + 1$ since α' is zero-sum-free.

The first assertion of the theorem is now immediate by observing that α' contains $a^h \cdot \operatorname{supp}(\alpha')$ as a subsequence, whence

$$\Sigma(\operatorname{supp}(\alpha)) + P = \Sigma(\operatorname{supp}(\alpha')) + P \subseteq \Sigma^\times(\alpha') \subseteq \Sigma^\times(\alpha).$$

To prove the second assertion we essentially apply the *Ruzsa covering lemma* ([Ru94], see also [TV06, Lemma 2.14]). Let X be a maximal subset of $\Sigma(\operatorname{supp}(\alpha)) = \Sigma(\operatorname{supp}(\alpha'))$ such that $0 \in X$ and the translates $x + P$ with $x \in X$ are pairwise disjoint. Then

$$|X||P| = |X + P| \leq |\Sigma(\alpha')| \leq |\Sigma(\alpha)| < Cn - C^2\sqrt{6n};$$

in view of $|P| = h > n - C\sqrt{6n}$, this gives $|X| \leq C - 1$.

On the other hand, by maximality of X, for any $g \in \Sigma(\operatorname{supp}(\alpha))$ there exists $x \in X$ such that $(x + P) \cap (g + P) \neq \varnothing$; that is, $g \in x + P - P$, showing that $\Sigma(\operatorname{supp}(\alpha)) \subseteq X + P - P$.

This completes the proof of Theorem 1.

References

[B68] P.C. Baayen, A combinatorial problem for finite abelian groups. (Dutch) *Colloquium on Discrete Mathematics, Math. Centrum, Amsterdam* (1968) 76–103, 107–108.

[BEN75] J. D. Bovey, P. Erdős, and I. Niven, Conditions for a zero sum modulo n, *Canad. Math. Bull.* **18** (1) (1975), 27–29.

[EB69] P. van Emde Boas, A combinatorial problem on finite abelian groups. II. *Math. Centrum Amsterdam Afd. Zuivere Wisk.* (1969), ZW-007, 60 pp.

[EBK67] P. van Emde Boas and D. Kruyswijk, A combinatorial problem on finite Abelian groups, *Math. Centrum Amsterdam Afd. Zuivere Wisk* (1967), ZW-009, 27pp.

[EE72] R.B. Eggleton and P. Erdős, Two combinatorial problems in group theory, *Acta Arith.* **21** (1972) 111–116.

[G00] W.D. Gao, Zero sums in finite cyclic groups, *Integers* **0** (2000), A12, 7 pp. (electronic).

[GH06] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations, Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics **278** (2006), Chapman & Hall/CRC, London, Boca Raton, FL.

[GHHLLP20] W. Gao, M. Huang, W. Hui, Y. Li, C. Liu, and J. Peng, Sums of sets of abelian group elements, *J. Number Theory* **208** (2020), 208–229.

[L99] V.F. Lev, The structure of multisets with a small number of subset sums, *Astèrisque* **258** (1999), 179–186.

[L] V.F. Lev, Zero-sum-free sequences with few subsequence sums, *Submitted.*

[O69a] J.E. Olson, A combinatorial problem on finite Abelian groups, I, *J. Number Theory* **1** (1969), 8–10.

[O69b] J.E. Olson, A combinatorial problem on finite Abelian groups, II., *J. Number Theory* **1** (1969), 195–199.

[OW77] J.E. Olson and E.T. White, Sums from a sequence of group elements, *Number theory and algebra* 215–222. Academic Press, New York, 1977.

[Ro63] K. Rogers, A combinatorial problem in abelian groups, *Proc. Camb. Phil. Soc.* **59** (1963), 559–562.

[Ru94] I. Ruzsa, Generalized arithmetical progressions and sumsets, *Acta Mathematica Hungarica* **65** (4) (1994), 379–388.

[SC07] S. Savchev and F. Chen, Long zero-free sequences in finite cyclic groups, *Discrete Math.* **307** (22) (2007), 2671–2679.

[SC17] S. Savchev and F. Chen, An inverse problem about minimal zero-sum sequences over finite cyclic groups, *J. Number Theory* **177** (2017), 381–427.

[SF01] W.W. Smith and M. Freeze, Sumsets of zerofree sequences, *Arab. J. Sci. Eng. Sect. C Theme Issues* **26** (1) (2001), 97–105.

[TV06] T. Tao and V.H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics, **105**. Cambridge University Press, Cambridge, 2006.

[Y07] P. Yuan, On the index of minimal zero-sum sequences over finite cyclic groups, *Journal of Combinatorial Theory, Series A* **114** (2007), 1545–1551.

Email address: `seva@math.haifa.ac.il`

Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel