

On the index of sequences over cyclic groups

by

WEIDONG GAO (Tianjin), YUANLIN LI (St. Catharines),
JIANGTAO PENG (Tianjin), CHRIS PLYLEY (St. Catharines)
and GUOQING WANG (Tianjin)

1. Introduction and main results. Let G be an additively written, finite cyclic group and $g \in G$ with $\text{ord}(g) = |G|$. For a sequence

$$S = (n_1g) \cdot \dots \cdot (n_lg) \quad \text{over } G, \quad \text{where } l \in \mathbb{N}_0 \text{ and } n_1, \dots, n_l \in [1, n],$$

we set

$$\|S\|_g = \frac{n_1 + \dots + n_l}{n},$$

and then

$$\text{ind}(S) = \min\{\|S\|_h \mid h \in G \text{ with } \text{ord}(h) = |G|\} \in \mathbb{Q}_{\geq 0}$$

denotes the *index* of S . The index of a sequence is a crucial invariant in the investigation of (minimal) zero-sum sequences (resp. of zero-sum free sequences) over cyclic groups. It was first considered by Lemke and Kleitman ([11]), used as key tool by Geroldinger ([6, p. 736]), and then investigated by Gao [3] in a systematical way. Since then it has found a lot of attention in recent years (see [1, 2, 5, 8, 12–16]). We briefly discuss some key results.

If S is a minimal zero-sum sequence, then $|S| \leq 3$, as well as $|S| \geq \lfloor n/2 \rfloor + 2$, implies that $\text{ind}(S) = 1$ (see [1], [14], [16]). In contrast, it was shown that for every $k \in [5, \lfloor n/2 \rfloor + 1]$, there is a minimal zero-sum subsequence T of length $|T| = k$ and with $\text{ind}(T) \geq 2$, and that the same is true for $k = 4$ and $\text{gcd}(n, 6) \neq 1$. This leads to the conjecture that, in case $\text{gcd}(n, 6) = 1$, every minimal zero-sum sequence S over G of length $|S| = 4$ has $\text{ind}(S) = 1$. Li, Plyley, Yuan and Zeng [12] recently proved that this holds true if n is a prime power, but the general case is still open.

In 1989, Lemke and Kleitman [11, p. 344] stated the following conjecture, which we formulate in the present language.

2010 *Mathematics Subject Classification*: 11B30, 11B50, 20K01.

Key words and phrases: zero-sum sequences, index of sequences, cyclic groups.

CONJECTURE 1.1. *Let G be a cyclic group of order n , d a divisor of n , and S a sequence over G of length $|S| = n$. Then there exists a subsequence T of S and an element $g \in G$ with $\text{ord}(g) = n$ such that*

$$d \mid n \parallel T \parallel_g \mid n.$$

In the special case $d = n$, this is equivalent to the existence of a subsequence T with $\text{ind}(T) = 1$.

Indeed, the above is the third of three interesting conjectures stated by Lemke and Kleitman in [11]. Their first conjecture has turned out to be true for all finite abelian groups (see [7]), and the second one is still open. In this paper we demonstrate that the above conjecture fails in general (see Theorem 1.2), but that it holds true under an additional assumption on the highest multiplicity of an element occurring in the sequence. Here are the main results of the present paper (for any undefined terminology or notation the reader is referred to the beginning of Section 2).

THEOREM 1.2. *Let G be a cyclic group of order $n \geq 2$, where $n = 4k + 2$ for some $k \geq 5$, and let $g \in G$ with $\text{ord}(g) = n$. Then the sequence*

$$S = g^{n/2-3} \left(\frac{n}{2}g\right) \left(\left(\frac{n}{2} + 1\right)g\right)^{n/2-1} \left(\left(\frac{n}{2} + 2\right)g\right)^{\lfloor n/4 \rfloor - 2}$$

has no subsequence T with $\text{ind}(T) = 1$.

THEOREM 1.3. *Let G be a cyclic group of order $n \geq 2$ and S be a sequence over G of length $|S| = n$. If $\mathbf{h}(S) < 4$ or $\mathbf{h}(S) \geq n/2$, then S has a subsequence T with $\text{ind}(T) = 1$ and length $|T| \leq \mathbf{h}(S)$.*

THEOREM 1.4. *Let G be a cyclic group of prime order $p > 24318$ and S be a sequence over G of length $|S| = p$. If $\mathbf{h}(S) \geq (p - 2)/10$, then S has a subsequence T with $\text{ind}(T) = 1$.*

In Section 2 we summarize our notation and prove Theorem 1.2. In the following two sections we provide the proofs of Theorems 1.3 and 1.4. We end the paper with a further conjecture and some open problems (see Section 5).

2. Notation and proof of Theorem 1.2. Let \mathbb{N} denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers, and for rational numbers $a, b \in \mathbb{Q}$ we set $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$. Let G be an additively written abelian group and $G_0 \subset G$ a subset. We fix the notation concerning sequences over G_0 (which is consistent with [4] and [9]). Let $\mathcal{F}(G_0)$ be the free abelian monoid with basis G_0 . The elements of $\mathcal{F}(G_0)$ are called *sequences* over G_0 . We write sequences $S \in \mathcal{F}(G_0)$ in the form

$$S = g_1 \cdot \dots \cdot g_l = \prod_{g \in G} g^{\mathbf{v}_g(S)},$$

where $l \in \mathbb{N}_0$, $g_1, \dots, g_l \in G_0$, $\mathbf{v}_g(S) \in \mathbb{N}_0$ and $\mathbf{v}_g(S) = 0$ for almost all $g \in G_0$. We call $|S| = l$ the *length* of S , $\sigma(S) = g_1 + \dots + g_l$ the *sum* of S , $\mathbf{v}_g(S)$ the *multiplicity* of g in S , $\text{supp}(S) = \{g \in G \mid \mathbf{v}_g(S) > 0\}$ the *support* of S , and we denote by

$$\mathbf{h}(S) = \max\{\mathbf{v}_g(S) \mid g \in G\} \in [0, |S|]$$

the *maximum of the multiplicities* of S . For every group homomorphism $\varphi: G \rightarrow H$, we set $\varphi(S) = \varphi(g_1) \cdot \dots \cdot \varphi(g_l) \in \mathcal{F}(H)$, and if φ is multiplication by some $m \in \mathbb{N}$, then we set $mS = \varphi(S)$. We say that S is a *zero-sum sequence* if $\sigma(S) = 0$, and it is called a *minimal zero-sum sequence* if $\sigma(S) = 0$ but $\sum_{i \in I} g_i \neq 0$ for all $\emptyset \neq I \subsetneq [1, l]$. Suppose that G is finite cyclic. Then a simple calculation (see [8, Lemma 5.1.2]) shows that

$$\begin{aligned} \text{ind}(S) &= \min\{\|S\|_h \mid h \in G \text{ with } \text{supp}(S) \subset \langle h \rangle\} \\ &= \min\{\|S\|_h \mid h \in G \text{ with } \langle \text{supp}(S) \rangle = \langle h \rangle\}. \end{aligned}$$

Proof of Theorem 1.2. Assume to the contrary that S has a subsequence T with $\text{ind}(T) = 1$. Then there exists an element $h \in G$ with $\text{ord}(h) = n$ such that $\|T\|_h = 1$. We set

$$g = jh \quad \text{and} \quad T = g^x \left(\frac{n}{2}g\right)^y \left(\left(\frac{n}{2} + 1\right)g\right)^z \left(\left(\frac{n}{2} + 2\right)g\right)^w$$

where $j \in [1, n - 1]$ with $\text{gcd}(j, n) = 1$, $x \in [0, n/2 - 3]$, $y \in [0, 1]$, $z \in [0, n/2 - 1]$ and $w \in [0, n/4 - 2]$. Then

$$(1) \quad n\|T\|_g = (x + z + 2w) + \frac{n}{2}(y + z + w) \equiv 0 \pmod{n}.$$

CASE 1: $j < n/4$. Then

$$T = (jh)^x \left(\frac{n}{2}h\right)^y \left(\left(\frac{n}{2} + j\right)h\right)^z \left(\left(\frac{n}{2} + 2j\right)h\right)^w.$$

Since $\|T\|_h = 1$, we infer that $y + z + w \leq 1$, which implies that $n\|T\|_g \leq x + (n/2 + 2) \leq n/2 - 3 + n/2 + 2 < n$, a contradiction.

CASE 2: $n/4 < j < n/2$. Then

$$T = (jh)^x \left(\frac{n}{2}h\right)^y \left(\left(\frac{n}{2} + j\right)h\right)^z \left(\left(2j - \frac{n}{2}\right)h\right)^w.$$

Since $\|T\|_h = 1$, we infer that $x \leq 3$ and $z \leq 1$, which implies that $x + z + 2w \leq 3 + 1 + 2(\lfloor n/4 \rfloor - 2) < n/2$. Since $x + z + 2w > 0$ and again by $\|T\|_h = 1$, we derive that $x + z + 2w \equiv 0 \pmod{n/2}$, a contradiction.

CASE 3: $n/2 < j < 3n/4$. Then

$$T = (jh)^x \left(\frac{n}{2}h\right)^y \left(\left(j - \frac{n}{2}\right)h\right)^z \left(\left(2j - \frac{n}{2}\right)h\right)^w.$$

Since $\|T\|_h = 1$, we infer that $x + y + w \leq 1$. We assert that

$$(2) \quad x + y + w = 1.$$

Otherwise, $x = y = w = 0$ and $n\|T\|_g = z + (n/2)z \not\equiv 0 \pmod{n/2}$, a contradiction to $n\|T\|_g \equiv 0 \pmod{n}$. Note that $0 < x + z + 2w < n$. By (1), we have

$$(3) \quad x + z + 2w = n/2,$$

$$(4) \quad y + z + w \equiv 1 \pmod{2}.$$

By (2) and (3), we have $y + z + w \equiv z + w - y = n/2 - 1 \equiv 0 \pmod{2}$, a contradiction to (4).

CASE 4: $3n/4 < j < n$. Then

$$T = (jh)^x \left(\frac{n}{2}h\right)^y \left(\left(j - \frac{n}{2}\right)h\right)^z \left(\left(2j - \frac{3n}{2}\right)h\right)^w.$$

Since $\|T\|_h = 1$, we infer that $x \leq 1$ and $z \leq 3$, which implies that $x + z + 2w \leq 1 + 3 + 2(\lfloor n/4 \rfloor - 2) < n/2$. Clearly, $x + z + 2w > 0$. From (1), we derive a contradiction. ■

3. Proof of Theorem 1.3. We need the following two results. A simple proof of the first one can be found in [8, Proposition 4.2.6] (for historical comments see [10]), and a proof of Lemma 3.2 is given in [13].

LEMMA 3.1. *Let G be a finite cyclic group and S be a sequence over G of length $|S| \geq |G|$. Then S has a zero-sum subsequence T of length $|T| \in [1, h(S)]$.*

LEMMA 3.2. *Let G be a finite cyclic group and S be a minimal zero-sum sequence over G of length $|S| \in [1, 3]$. Then $\text{ind}(S) = 1$.*

Proof of Theorem 1.3. We set $n = |G|$ and $h = h(S)$. If $h < 4$, then the assertion follows from Lemmas 3.1 and 3.2. Suppose that $h \geq n/2$. Let $g \in G$ with $v_g(S) = h$. If $\text{ord}(g) < n$, then $\text{ord}(g) \leq n/2 \leq h$, and $T = g^{\text{ord}(g)}$ has the required properties. If $0 \nmid S$, then $T = 0$ has the required properties.

Suppose that $\text{ord}(g) = n$ and that $0 \nmid S$. Then we can write S in the form

$$S = g^h(b_1g) \cdots (b_{n-h}g) \quad \text{where } b_1, \dots, b_{n-h} \in [2, n-1].$$

Assume to the contrary that S has no subsequence T with the required properties. We continue with the following assertion.

A. For every subset $I \subset [1, n-h]$ we have $\sum_{i \in I} b_i \leq n-h + |I| - 1$.

If **A** holds, then we apply it with $I = [1, n - h]$ and obtain

$$\sum_{i=1}^{n-h} b_i \leq 2(n - h) - 1,$$

a contradiction to $b_1, \dots, b_{n-h} \in [2, n - 1]$.

We prove **A** by induction on $|I|$. If there were an $i \in [1, n - h]$ such that $b_i \geq n - h + 1$, then $T = g^{n-b_i}(b_i g)$ would be a subsequence of S with $\text{ind}(T) = 1$ and length $|T| = n - b_i + 1 \leq h$, a contradiction. Let $I \subset [1, n - h]$ with $|I| = k + 1 \geq 2$, say $I = [1, k + 1]$, and suppose that **A** holds for all proper subsets of I . We set $\beta = b_1 + \dots + b_{k+1}$. By induction hypothesis we get $\beta - b_i \leq n - h + k - 1$ for every $i \in [1, k + 1]$, which implies that

$$\beta = \frac{1}{k}(k\beta) = \frac{1}{k} \sum_{i=1}^{k+1} (\beta - b_i) \leq \frac{(k + 1)(n - h + k - 1)}{k} \leq n$$

(to get the last inequality, use that $h \geq n/2$ and $k \leq n - h - 1$). Thus, if $\beta \geq n - h + k + 1$, then $T = g^{n-\beta}(b_1 g) \dots (b_{k+1} g)$ is a subsequence of S with $\text{ind}(T) = 1$ and length $|T| = n - \beta + k + 1 \leq h$. This is a contradiction, and thus **A** is proved. ■

Note that the sequence S given in Theorem 1.2 satisfies $\mathfrak{h}(S) = n/2 - 1$. Thus the assumption in Theorem 1.3, that $\mathfrak{h}(S) \geq n/2$, cannot be weakened for $n \equiv 2 \pmod{4}$.

4. Proof of Theorem 1.4. We fix our notation which remains valid throughout the whole section. Let G be a prime cyclic group of order $|G| = p > 24318$, $G^\bullet = G \setminus \{0\}$, and let S be a sequence over G^\bullet of length $|S| = p$. If $g \in G^\bullet$, $A \subset \mathbb{Z}$ and $S = (n_1 g) \dots (n_l g)$ with $n_1, \dots, n_l \in [1, p - 1]$, then we set

$$S(A, g) = \prod_{i \in [1, l], n_i \in A} (n_i g).$$

For an element $g \in G^\bullet$, we set

$$\Sigma_g(S) = \{p \parallel T \parallel_g \mid T \text{ is a subsequence of } S \text{ with } \|T\|_g \leq 1\},$$

and we denote by $\mathfrak{m}_g(S)$ the maximal $t \in [1, p]$ such that $\Sigma_g(T) = [1, t]$ for some subsequence T of S . We define

$$\mathfrak{m}(S) = \max\{\mathfrak{m}_g(S) \mid g \in G^\bullet\}.$$

From now on we fix an element $g \in G^\bullet$ such that $\mathfrak{m}_g(S) = \mathfrak{m}(S)$.

LEMMA 4.1. *Let T be a subsequence of S such that $\Sigma_g(T) = [1, \mathfrak{m}(S)]$. Then $|T| \leq \mathfrak{m}(S)$, and if $x \in [1, p - 1]$ is such that $(xg) \mid ST^{-1}$, then $x \geq \mathfrak{m}(S) + 2$. Furthermore, if $\mathfrak{m}(S) = p$, or if there exists an $x \in [1, p - 1]$ such that $(xg) \mid ST^{-1}$ and $x \geq p - \mathfrak{m}(S)$, then S has a subsequence with index 1.*

Proof. By definition, we have $|T| \leq p\|T\|_g = m(S)$. If there is some $x \in [1, p - 1]$ with $(xg) | ST^{-1}$ and $x \leq m(S) + 1$, then $\Sigma_g((xg)T) = [1, \min\{p, m(S) + x\}]$, a contradiction to the maximality of $m(S)$. The second part of this lemma is clear. ■

From now on we suppose that S has no subsequence with index 1.

Let $k \geq 2$ be a positive integer, and let $F[1/k, (k - 1)/k]$ be the set of all irreducible fractions between $1/k$ and $(k - 1)/k$ and with denominators in $[2, k]$, i.e.,

$$F\left[\frac{1}{k}, \frac{k-1}{k}\right] = \left\{ \frac{a}{b} \mid a \in \mathbb{N}, b \in [2, k] \text{ with } \gcd(a, b) = 1 \text{ and } \frac{1}{k} \leq \frac{a}{b} \leq \frac{k-1}{k} \right\}.$$

LEMMA 4.2. *Let a/b and c/d be two adjacent fractions in $F[1/k, (k-1)/k]$ with $a/b < c/d$. Then*

- (i) $b + d \geq k + 1$.
- (ii) $bc - ad = 1$.

Proof. (i) Note that $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$. Since a/b and c/d are adjacent, it follows that the irreducible fraction with value $\frac{a+c}{b+d}$ is not in $F[1/k, (k - 1)/k]$. This forces that $b + d \geq k + 1$.

(ii) Since $\gcd(a, b) = 1$, there are two integers u and v such that $bu + av = 1$. Note that $b(u + ma) + a(v - mb) = 1$ for any integer m . Let $x = u + ma$ and $y = mb - v$. Then $bx - ay = 1$. By choosing m suitably we may assume that $y \leq k$ and $y + b \geq k + 1$. It follows that $y \geq k + 1 - b > 0$ and $x > 0$. From $bx - ay = 1$ we get

$$\frac{x}{y} - \frac{a}{b} = \frac{1}{by}.$$

If $y > 1$, then x/y is a fraction in $F[1/k, (k - 1)/k]$. So, either $c/d = x/y$ and we are done, or $c/d < x/y$. For the latter case we have

$$\frac{1}{by} = \frac{x}{y} - \frac{a}{b} = \left(\frac{x}{y} - \frac{c}{d}\right) + \left(\frac{c}{d} - \frac{a}{b}\right) = \frac{b(dx - cy) + y(cb - ad)}{byd} \geq \frac{b + y}{byd}.$$

This implies that $d \geq b + y \geq k + 1$, a contradiction.

Now assume that $y = 1$ and we must have $b = k$. It follows from $bx - ay = 1$ that $a = kx - 1$. Therefore, $x = 1$ and $a = k - 1$. So, $a/b = (k - 1)/k$ is the largest fraction in $F[1/k, (k - 1)/k]$, a contradiction. ■

We set

$$k = \left\lfloor \frac{p}{m(S)} \right\rfloor, \quad f = \left\lfloor F\left[\frac{1}{k}, \frac{k-1}{k}\right] \right\rfloor,$$

and we arrange all fractions in $F[1/k, (k - 1)/k]$ increasingly; so let

$$\frac{a_1}{b_1} < \dots < \frac{a_f}{b_f}$$

denote the elements of $F[1/k, (k - 1)/k]$. Furthermore, we set

$$S_1 = S([1, m(S)], g), \quad S_2 = S\left(\left[m(S) + 2, \frac{p-1}{b_1}\right], g\right)$$

and, for every $i \in [1, f]$, we set

$$S_{2i+1} = S\left(\left[\frac{a_i p + 1}{b_i}, \frac{a_i p + m(S)}{b_i}\right], g\right),$$

$$S_{2i+2} = S\left(\left[\frac{a_i p + m(S) + 1}{b_i}, \frac{a_{i+1} p - 1}{b_{i+1}}\right], g\right).$$

Furthermore, for every $i \in [2, k]$, we define

$$R_i = S(\{x \in [1, p] \mid \text{If } x_i \in [1, p] \text{ with } p \mid (x_i - ix), \\ \text{then } x_i \in [1, m(S)] \text{ and } \gcd(x_i, i) = 1\}, g).$$

LEMMA 4.3. We have $S = \prod_{j=1}^{2f+1} S_j$.

Proof. This is clear by construction. ■

LEMMA 4.4. Suppose that

$$4 \leq m(S) \leq \frac{p-3}{2} \quad \text{and} \quad \max\left\{\frac{p-m(S)-2}{m(S)}, \frac{p-m(S)}{m(S)+1}\right\} \leq k \leq \frac{p+1}{m(S)}.$$

- (i) $|S_{2i+2}| \leq b_{i+1} - 1$ for every $i \in [0, f - 1]$.
- (ii) $p = |S| \leq m(S) + \sum_{i=2}^k \sum_{j \in [1, i-1] \text{ with } \gcd(i, j) = 1} (i - 1) + \sum_{i=2}^k |R_i|$.

Proof. (i) Suppose that $i = 0$. Then $S_2 = S([m(S) + 2, (p - 1)/b_1], g)$ and $b_1 = k$. If $|S_2| \geq b_1 = k$, then we can take a k -term subsequence U of S_2 . Note that $p - 1 \geq p \|U\|_g \geq k(m(S) + 2) \geq p - m(S)$ and one can find a subsequence V of S_1 such that UV has index 1, a contradiction.

Now suppose that $i \in [1, f - 1]$, and assume to the contrary that $|S_{2i+2}| \geq b_{i+1}$. We choose an arbitrary b_{i+1} -term subsequence X of S_{2i+2} , and write $b_i S$ in the form

$$b_i S = (x_1 g) \cdot \dots \cdot (x_p g) \quad \text{with} \quad x_1, \dots, x_p \in [1, p - 1].$$

It follows from Lemma 4.2 that $a_{i+1} b_i - a_i b_{i+1} = 1$, and so

$$b_i \left(\frac{a_{i+1} p - 1}{b_{i+1}}\right) - a_i p = \frac{p - b_i}{b_{i+1}}.$$

Thus for every $\nu \in [1, p]$ with $(x_\nu g) \mid S_{2i+2}$, we infer that $x_\nu \in [m(S) + 1, (p - b_i)/b_{i+1}]$ and $x_\nu \equiv -a_i p \pmod{b_i}$. Therefore, since $b_i + b_{i+1} \geq k + 1$ by

Lemma 4.2, we get

$$p - b_i \geq p \|b_i X\|_g \geq b_{i+1}(\mathfrak{m}(S) + 1) \geq p - b_i \mathfrak{m}(S)$$

and

$$p \|b_i X\|_g \equiv -b_{i+1} a_i p = (1 - a_{i+1} b_i) p \equiv p \pmod{b_i}.$$

Therefore there exists a subsequence Y of S_1 such that $p \|b_i(XY)\|_g = p$, a contradiction.

(ii) For every $\ell \in [2, k]$, we have $R_\ell = \prod_{b_i=\ell} S_{2i+1}$, and hence

$$S = S_1 \prod_{i=0}^{f-1} S_{2i+2} \prod_{\ell=2}^k R_\ell.$$

Now (ii) follows from (i). ■

LEMMA 4.5. *Let $\ell \in \mathbb{N}_{\geq 2}$ and $S \in \mathcal{F}(\mathbb{Z})$ be a sequence of length $|S| = \ell$. Suppose that every element from S is coprime to ℓ . Then for every $m \in \mathbb{Z}$ there exists a subsequence S_m such that $\sigma(S_m) \equiv m \pmod{\ell}$. Moreover, if $m \notin \ell\mathbb{Z}$, then $S_m \neq S$.*

Proof. Let $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}/\ell\mathbb{Z}$ be the canonical epimorphism and $\varphi(S) = a_1 \cdot \dots \cdot a_\ell$. We denote by $A = \{a_1, 0\} + \dots + \{a_{\ell-1}, 0\} \subset \mathbb{Z}/\ell\mathbb{Z}$ the sumset, and by $H = \text{Stab}(A)$ the stabilizer of A . Clearly, it suffices to verify that $A = \mathbb{Z}/\ell\mathbb{Z}$. If H were a proper subgroup of $\mathbb{Z}/\ell\mathbb{Z}$, then Kneser's Theorem would imply that

$$|A| \geq \sum_{i=1}^{\ell-1} |\{a_i, 0\} + H| - (\ell - 2)|H| = (\ell - 1)2|H| - (\ell - 2)|H| \geq \ell,$$

whence $A = H = \mathbb{Z}/\ell\mathbb{Z}$. Thus $H = \mathbb{Z}/\ell\mathbb{Z}$, which implies that $A = \mathbb{Z}/\ell\mathbb{Z}$, and we are done. ■

LEMMA 4.6. *Let $t, \ell \in [2, k - 1]$ with $t < \ell$ and $d = \gcd(t, \ell) < t$, and let $u \in [2, \mathfrak{m}(S)]$. If*

$$\frac{(t - d)p - \ell}{t\ell} \leq \mathfrak{m}(S) \leq \frac{dp}{\ell} - t(u - 1),$$

then

$$|R_t| = 0 \quad \text{or} \quad |R_\ell| \leq \frac{p - \ell \mathfrak{m}(S) - 2\ell + 1}{u} + 2\ell - 1.$$

Proof. Suppose that $|R_t| > 0$. Let $x \in [1, p - 1]$ be such that $(xg) | R_t$, and let $x_\ell \in [1, p - 1]$ be such that $p | (\ell x - x_\ell)$. By the definition of R_t , we get

$$x_\ell \in \bigcup_{i \in [1, t-1] \text{ with } \gcd(i, t)=1} \left[\frac{\ell ip + \ell}{t}, \frac{\ell ip + \ell \mathfrak{m}(S)}{t} \right],$$

and thus

$$x_\ell \in \bigcup_{i \in [1, t-1] \text{ with } d|i} \left[\frac{ip + \ell}{t}, \frac{ip + \ell m(S)}{t} \right] \subset \left[\frac{dp + \ell}{t}, \frac{(t-d)p + \ell m(S)}{t} \right] \\ \subset [p - \ell m(S), p - \ell(u-1)].$$

If $|(\ell R_\ell)([1, u-1], g)| \geq \ell$, then, by Lemma 4.5 and the definition of R_ℓ , we may choose a subsequence W of R_ℓ of length at most ℓ with $(\ell W)([1, u-1], g) = \ell W$ and $x_\ell + p\|\ell W\|_g \equiv p \pmod{\ell}$. Since $p\|\ell W\|_g \leq \ell(u-1)$, we have $x_\ell + p\|\ell W\|_g \in [p - \ell m(S), p]$. Thus, we can construct a subsequence of $(xg)WS_1$ of index 1, a contradiction. Therefore,

$$(5) \quad |(\ell R_\ell)([1, u-1], g)| \leq \ell - 1.$$

If $|R_\ell| < \ell$ then we are done. Otherwise, by Lemma 4.5, we get a subsequence R_0 of R_ℓ with $p\|\ell R_0\|_p \equiv p \pmod{\ell}$ and

$$(6) \quad |R_0| \geq |R_\ell| - \ell.$$

We assert that

$$(7) \quad p\|\ell R_0\|_p \leq p - \ell m(S) - \ell.$$

Assume to the contrary that $p\|\ell R_0\|_p \geq p - \ell m(S)$, and choose T to be the minimal subsequence of R_0 such that $p\|\ell T\|_g \geq p - \ell m(S)$ and $p\|\ell T\|_g \equiv p \pmod{\ell}$. If $p\|\ell T\|_g \leq p$, then we can construct a subsequence of TS_1 with index 1, a contradiction. Now suppose that $p\|\ell T\|_g > p$. If $y \in [1, p-1]$ is such that $(yg) | R_\ell$ and $y_\ell \in [1, p-1]$ such that $p | (\ell y - y_\ell)$, then $y_\ell \in [1, m(S)]$ and $\gcd(y_\ell, \ell) = 1$. By Lemma 4.5, by dropping at most ℓ terms from T , we get a proper subsequence \tilde{T} such that $p\|\ell \tilde{T}\|_g \geq p - \ell m(S)$ and $p\|\ell \tilde{T}\|_g \equiv p \pmod{\ell}$, a contradiction to the minimality of T . Therefore, (7) holds.

By (5), we have $p\|\ell R_0\|_g \geq (\ell - 1) + u(|R_0| - \ell + 1)$. This together with (7) gives

$$|R_0| \leq \frac{p - \ell m(S) - 2\ell + 1}{u} + \ell - 1.$$

Now the lemma follows from (6). ■

LEMMA 4.7. *Let $t \in [2, k]$, and let $1 = \alpha_1 < \alpha_2 < \dots$ denote all positive integers coprime to t . If*

$$m(S) \leq \frac{p - 2t + w\alpha_{u+1} + 2}{t + \sum_{i=2}^u \alpha_i} \quad \text{for some } w, u \in \mathbb{N}_0,$$

then

$$|R_t| \leq \frac{p - (t + \sum_{i=2}^u \alpha_i)m(S) - 2t + 2}{\alpha_{u+1}} + \delta_u(u-1)m(S) + 2t + w$$

where

$$\delta_u = \begin{cases} 0 & \text{for } u = 0, \\ 1 & \text{for } u \geq 1. \end{cases}$$

Proof. Assume to the contrary that $|R_t|$ is strictly larger than the above bound. Since

$$m(S) \leq \frac{p - 2t + w\alpha_{u+1} + 2}{t + \sum_{i=2}^u \alpha_i},$$

it follows that $|R_t| \geq 2t + 1$. By Lemma 4.5, there exists a nonempty subsequence R_0 of R_t with

$$(8) \quad p \|tR_0\|_g \equiv p \pmod{t} \quad \text{and} \quad |R_0| \geq |R_t| - t.$$

Similarly to Lemma 4.6, we can prove that

$$(9) \quad p \|tR_0\|_g \leq p - tm(S) - t.$$

Note that tR_0 contains $\alpha_1 g = g$ at most $t - 2$ times, because otherwise we would get

$$m(S) \geq m_g(tS) \geq tm_g(S) + t - 1 > m_g(S) = m(S),$$

a contradiction. Since $v_{\alpha_i g}(S) \leq h(S) \leq m(S)$ for all $i \geq 2$, it follows that

$$p \|tR_0\|_g \geq \alpha_1(t - 2) + \left(\sum_{i=2}^u \alpha_i \right) m(S) + \alpha_{u+1}(|R_0| - (u - 1)m(S) - (t - 2)).$$

By (9), we have

$$|R_0| \leq \frac{p - (t + \sum_{i=2}^u \alpha_i)m(S) - 2t + 2}{\alpha_{u+1}} + \delta(u - 1)m(S) + t - 2.$$

By (8), we derive a contradiction. ■

Proof of Theorem 1.4. We use the notation introduced at the beginning of this section. In particular, we assume to the contrary that there exists a sequence $S \in \mathcal{F}(G^\bullet)$ of length $|S| = p$ which has no subsequence with index 1. We have to derive a contradiction.

Clearly, $h(S) \leq m(S) \leq p - 1$. Lemma 4.1 implies that, for every $x \in [1, p - 1]$ with $(xg) | ST^{-1}$, we have $m(S) + 2 \leq x \leq p - m(S) - 1$. Thus it follows that

$$\frac{p - 2}{10} \leq h(S) \leq m(S) \leq \frac{p - 3}{2}.$$

We distinguish several cases.

CASE 1: $(p - 2)/3 \leq m(S) \leq (p - 3)/2$. With $k = 2$ in Lemma 4.4, we have

$$p \leq m(S) + 1 + |R_2|.$$

Applying Lemma 4.7 with $u = 0$ and $w = 6$, we infer that

$$|R_2| \leq p - 2m(S) + 8.$$

It follows that $p \leq m(S) + 1 + |R_2| = m(S) + 1 + p - 2m(S) + 8 < p$, a contradiction.

CASE 2: $(p+3)/4 \leq m(S) \leq (p-4)/3$. With $k=3$ in Lemma 4.4, we have

$$p \leq m(S) + 1 + 2 + 2 + |R_2| + |R_3|.$$

Applying Lemma 4.7 with $u=1$ and $w=6$, we infer that

$$|R_2| \leq \frac{p-2m(S)+28}{3}, \quad |R_3| \leq \frac{p-3m(S)+20}{2}.$$

It follows that

$$p \leq m(S) + 5 + \sum_{i=2}^3 |R_i| = m(S) + 5 + \frac{p-2m(S)+28}{3} + \frac{p-3m(S)+20}{2} < p,$$

a contradiction.

CASE 3: $(p-2)/5 \leq m(S) \leq (p+1)/4$. With $k=4$ in Lemma 4.4, we have

$$p \leq m(S) + 1 + 2 \cdot 2 + 3 \cdot 2 + |R_2| + |R_3| + |R_4|.$$

Applying Lemma 4.7 with $u=1$ and $w=6$, we infer that

$$|R_2| \leq \frac{p-2m(S)+28}{3}, \quad |R_3| \leq \frac{p-3m(S)+20}{2}, \quad |R_4| \leq \frac{p-4m(S)+36}{3}.$$

It follows that

$$p \leq m(S) + 11 + \frac{p-2m(S)+28}{3} + \frac{p-3m(S)+20}{2} + \frac{p-4m(S)+36}{3} < p,$$

a contradiction.

CASE 4: $(p-1)/6 \leq m(S) \leq (p-3)/5$. With $k=5$ in Lemma 4.4, we have

$$p \leq m(S) + 27 + \sum_{i=2}^5 |R_i|.$$

Applying Lemma 4.7 with $u=1$ and $w=6$, we infer that

$$\begin{aligned} |R_2| &\leq \frac{p-2m(S)+28}{3}, & |R_3| &\leq \frac{p-3m(S)+20}{2}, \\ |R_4| &\leq \frac{p-4m(S)+36}{3}, & |R_5| &\leq \frac{p-5m(S)+24}{2}. \end{aligned}$$

Applying Lemma 4.6 with $t=2, \ell=3$ and $u=12$, we obtain that either

$$|R_2| = 0 \quad \text{or} \quad |R_3| \leq \frac{p-3m(S)+55}{12},$$

and therefore

$$\begin{aligned} |R_2| + |R_3| &\leq \max \left\{ \frac{p-2m(S)+28}{3} + \frac{p-3m(S)+55}{12}, \frac{p-3m(S)+20}{2} \right\} \\ &= \frac{5p-11m(S)+167}{12}. \end{aligned}$$

Summing up we obtain

$$\begin{aligned} p &\leq m(S) + 27 + \sum_{i=2}^5 |R_i| = m(S) + 27 + (|R_2| + |R_3|) + |R_4| + |R_5| \\ &\leq \frac{5p - 11m(S) + 167}{12} + \frac{p - 4m(S) + 36}{3} + \frac{p - 5m(S) + 24}{2} + 27 < p, \end{aligned}$$

a contradiction.

CASE 5: $(p - 5)/7 \leq m(S) \leq (p - 5)/6$. With $k = 6$ in Lemma 4.4, we have

$$p \leq m(S) + 37 + \sum_{i=2}^6 |R_i|.$$

Applying Lemma 4.7 with $u = 2$ and $w = 0$, we infer that

$$|R_2| \leq \frac{p + 18}{5}, \quad |R_3| \leq \frac{p - m(S) + 20}{4}.$$

Applying Lemma 4.7 with $u = 1$ and $w = 6$, we infer that

$$|R_4| \leq \frac{p - 4m(S) + 36}{3}, \quad |R_5| \leq \frac{p - 5m(S) + 24}{2}, \quad |R_6| \leq \frac{p - 6m(S) + 80}{5}.$$

Summing up we obtain

$$\begin{aligned} p &\leq m(S) + 37 + \sum_{i=2}^6 |R_i| \\ &= m(S) + 37 + \frac{p + 18}{5} + \frac{p - m(S) + 20}{4} + \frac{p - 4m(S) + 36}{3} \\ &\quad + \frac{p - 5m(S) + 24}{2} + \frac{p - 6m(S) + 80}{5} < p, \end{aligned}$$

a contradiction.

CASE 6: $(p - 2)/8 \leq m(S) \leq (p - 3)/7$. With $k = 7$ in Lemma 4.4, we have

$$p \leq m(S) + 73 + \sum_{i=2}^7 |R_i|.$$

Applying Lemma 4.7 with $u = 2$ and $w = 0$, we infer that

$$|R_2| \leq \frac{p + 18}{5}, \quad |R_3| \leq \frac{p - m(S) + 20}{4}.$$

Applying Lemma 4.7 with $u = 1$ and $w = 6$, we infer that

$$\begin{aligned} |R_4| &\leq \frac{p - 4m(S) + 36}{3}, \quad |R_5| \leq \frac{p - 5m(S) + 24}{2}, \\ |R_6| &\leq \frac{p - 6m(S) + 80}{5}, \quad |R_7| \leq \frac{p - 7m(S) + 28}{2}. \end{aligned}$$

Applying Lemma 4.6 with $t = 2$, $\ell = 5$ and $u = 10$, we infer that

$$\begin{aligned} |R_2| + |R_5| &\leq \max \left\{ \frac{p - 5m(S) + 4}{2}, \frac{p + 18}{5} + \frac{p - 5m(S) - 9}{10} + 9 \right\} \\ &= \frac{3p - 5m(S) + 117}{10}. \end{aligned}$$

Summing up we obtain

$$\begin{aligned} p &\leq m(S) + 73 + \sum_{i=2}^7 |R_i| \\ &= m(S) + 73 + (|R_2| + |R_5|) + |R_3| + |R_4| + |R_6| + |R_7| \\ &\leq m(S) + 73 + \frac{3p - 5m(S) + 117}{10} + \frac{p - m(S) + 20}{4} + \frac{p - 4m(S) + 36}{3} \\ &\quad + \frac{p - 6m(S) + 80}{5} + \frac{p - 7m(S) + 28}{2} < p, \end{aligned}$$

a contradiction.

CASE 7: $(p - 2)/9 \leq m(S) \leq (p - 3)/8$. With $k = 8$ in Lemma 4.4, we have

$$p \leq m(S) + 111 + \sum_{i=2}^8 |R_i|.$$

Applying Lemma 4.7 with $u = 2$ and $w = 0$, we infer that

$$\begin{aligned} |R_2| &\leq \frac{p + 18}{5}, & |R_3| &\leq \frac{p - m(S) + 20}{4}, \\ |R_4| &\leq \frac{p - 2m(S) + 34}{5}, & |R_5| &\leq \frac{p - 4m(S) + 22}{3}. \end{aligned}$$

Applying Lemma 4.7 with $u = 1$ and $w = 6$, we infer that

$$|R_6| \leq \frac{p - 6m(S) + 80}{5}, \quad |R_7| \leq \frac{p - 7m(S) + 28}{2}, \quad |R_8| \leq \frac{p - 8m(S) + 52}{3}.$$

Applying Lemma 4.6 with $t = 2$, $\ell \in \{5, 7\}$ and $u = 20$, we can prove that either

$$|R_2| = 0 \quad \text{or} \quad |R_i| \leq \frac{p - im(S) - 2i + 1}{20} + 2i - 1 \quad \text{for } i \in \{5, 7\},$$

and therefore

$$\begin{aligned} |R_2| + |R_5| + |R_7| &\leq \max \left\{ \frac{p - 4m(S) + 22}{3} + \frac{p - 7m(S) + 28}{2}, \right. \\ &\quad \left. \frac{p - m(S) + 20}{4} + \frac{p - 5m(S) - 9}{20} + 9 + \frac{p - 7m(S) - 13}{20} + 13 \right\} \\ &= \frac{5p - 29m(S) + 128}{6}. \end{aligned}$$

Applying Lemma 4.6 with $t = 4$, $\ell = 6$ and $u = 10$, we find that either

$$|R_4| = 0 \quad \text{or} \quad |R_6| \leq \frac{p - 6m(S) - 11}{10} + 11,$$

and therefore

$$\begin{aligned} |R_4| + |R_6| &\leq \max \left\{ \frac{p - 2m(S) + 34}{5} + \frac{p - 6m(S) - 11}{10} + 11, \frac{p - 6m(S) + 80}{5} \right\} \\ &= \frac{3p - 10m(S) + 167}{10}. \end{aligned}$$

Summing up we obtain

$$\begin{aligned} p &\leq m(S) + 111 + \sum_{i=2}^8 |R_i| \\ &= m(S) + 111 + (|R_2| + |R_5| + |R_7|) + (|R_4| + |R_6|) + |R_3| + |R_8| \\ &\leq m(S) + 111 + \frac{5p - 29m(S) + 128}{6} + \frac{3p - 10m(S) + 167}{10} \\ &\quad + \frac{p - m(S) + 20}{4} + \frac{p - 8m(S) + 52}{3} < p, \end{aligned}$$

a contradiction.

CASE 8: $(p - 2)/10 \leq m(S) \leq (p - 4)/9$. With $k = 9$ in Lemma 4.4, we have

$$p \leq m(S) + 159 + \sum_{i=2}^9 |R_i|.$$

Applying Lemma 4.7 with $u = 2$ and $w = 0$, we infer that

$$\begin{aligned} |R_2| &\leq \frac{p + 18}{5}, & |R_3| &\leq \frac{p - m(S) + 20}{4}, \\ |R_4| &\leq \frac{p - 2m(S) + 34}{5}, & |R_5| &\leq \frac{p - 4m(S) + 22}{3}. \end{aligned}$$

Applying Lemma 4.7 with $u = 1$ and $w = 6$, we infer that

$$\begin{aligned} |R_6| &\leq \frac{p - 6m(S) + 80}{5}, & |R_7| &\leq \frac{p - 7m(S) + 28}{2}, \\ |R_8| &\leq \frac{p - 8m(S) + 52}{3}, & |R_9| &\leq \frac{p - 9m(S) + 32}{2}. \end{aligned}$$

Applying Lemma 4.6 with $t = 2$, $\ell \in \{5, 7\}$ and $u = 10$, we deduce that either

$$|R_2| = 0 \quad \text{or} \quad |R_i| \leq \frac{p - im(S) - 2i + 1}{10} + 2i - 1 \quad \text{for } i \in \{5, 7\},$$

and therefore

$$\begin{aligned} |R_2| + |R_5| + |R_7| &\leq \max \left\{ \frac{p - 4m(S) + 22}{3} + \frac{p - 7m(S) + 28}{2}, \right. \\ &\quad \left. \frac{p + 18}{5} + \frac{p - 5m(S) - 9}{10} + 9 + \frac{p - 7m(S) - 13}{10} + 13 \right\} \\ &= \frac{5p - 29m(S) + 128}{6}. \end{aligned}$$

Applying Lemma 4.6 with $t = 3$, $\ell = 8$ and $u = 5$, we deduce that either

$$|R_3| = 0 \quad \text{or} \quad |R_8| \leq \frac{p - 8m(S) - 15}{8} + 15,$$

and therefore

$$\begin{aligned} |R_3| + |R_8| &\leq \max \left\{ \frac{p - m(S) + 20}{4} + \frac{p - 8m(S) - 15}{8} + 15, \frac{p - 8m(S) + 52}{3} \right\} \\ &= \frac{3p - 10m(S)}{8} + 20. \end{aligned}$$

Summing up we obtain

$$\begin{aligned} p &\leq m(S) + 159 + \sum_{i=2}^9 |R_i| \\ &= M + 159 + (|R_2| + |R_5| + |R_7|) + (|R_3| + |R_8|) + |R_4| + |R_6| + |R_9| \\ &\leq m(S) + 159 + \frac{5p - 29m(S) + 128}{6} + \left(\frac{3p - 10m(S)}{8} + 20 \right) \\ &\quad + \frac{p - 2m(S) + 34}{5} + \frac{p - 6m(S) + 80}{5} + \frac{p - 9m(S) + 32}{2} < p, \end{aligned}$$

a contradiction. ■

5. A conjecture and an open problem. In spite of Theorem 1.2 and in view of Lemma 3.1, we formulate a conjecture which sharpens the original Lemke–Kleitman Conjecture for prime cyclic groups.

CONJECTURE 5.1. *Let G be a cyclic group of prime order and S be a sequence over G of length $|S| = |G|$. Then S has a subsequence T with $\text{ind}(T) = 1$ and length $|T| \in [1, h(S)]$.*

Let G be a cyclic group of order $n \geq 2$. We denote by

- $\mathbf{t}(n)$ the smallest integer $\ell \in \mathbb{N}$ such that every sequence S over G of length $|S| \geq \ell$ has a subsequence T with $\text{ind}(T) = 1$,
- $\mathbf{T}(n)$ the smallest integer $\ell \in \mathbb{N}$ such that every squarefree sequence S over G of length $|S| \geq \ell$ has a subsequence T with $\text{ind}(T) = 1$.

By Theorem 1.2, it follows that $\mathbf{t}(n) \geq n + \lfloor n/4 \rfloor - 4$ for $n = 4k + 2 \geq 22$.

PROBLEM. *Determine $\mathbf{t}(n)$ and $\mathbf{T}(n)$ for all $n \geq 2$.*

Acknowledgements. We would like to thank the referees for their helpful suggestions. This work has been supported by NSFC within project no. 10971108.

References

- [1] S. T. Chapman, M. Freeze, and W. W. Smith, *Minimal zero sequences and the strong Davenport constant*, Discrete Math. 203 (1999), 271–277.
- [2] S. T. Chapman and W. W. Smith, *A characterization of minimal zero-sequences of index one in finite cyclic groups*, Integers 5 (2005), paper A27, 5 pp.
- [3] W. D. Gao, *Zero sums in finite cyclic groups*, Integers 0 (2000), paper A14, 9 pp.
- [4] W. D. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. 24 (2006), 337–369.
- [5] —, —, *On products of k atoms*, Monatsh. Math. 156 (2009), 141–157.
- [6] A. Geroldinger, *On non-unique factorizations into irreducible elements. II*, in: Number Theory, Vol. II (Budapest, 1987), Colloq. Math. Soc. János Bolyai 51, North-Holland, 1990, 723–757.
- [7] —, *On a conjecture of Kleitman and Lemke*, J. Number Theory 44 (1993), 60–65.
- [8] —, *Additive group theory and non-unique factorizations*, in: Combinatorial Number Theory and Additive Group Theory, A. Geroldinger and I. Ruzsa (eds.), Adv. Courses Math. CRM Barcelona, Birkhäuser, 2009, 1–86.
- [9] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. 278, Chapman & Hall/CRC, 2006.
- [10] Y. O. Hamidoune, *A weighted generalization of Gao's $n + D - 1$ theorem*, Combin. Probab. Comput. 17 (2008), 793–798.
- [11] P. Lemke and D. Kleitman, *An addition theorem on the integers modulo n* , J. Number Theory 31 (1989), 335–345.
- [12] Y. L. Li, C. Plyley, P. Z. Yuan, and X. Zeng, *Minimal zero-sum sequences of length four over finite cyclic groups*, *ibid.* 130 (2010), 2033–2048.
- [13] V. Ponomarenko, *Minimal zero sequences of finite cyclic groups*, Integers 4 (2004), paper A24, 6 pp.
- [14] S. Savchev and F. Chen, *Long zero-free sequences in finite cyclic groups*, Discrete Math. 307 (2007), 2671–2679.
- [15] X. W. Xia and P. Z. Yuan, *Indexes of insplitable minimal zero-sum sequences of length $l(C_n) - 1$* , *ibid.* 310 (2010), 1127–1133.
- [16] P. Z. Yuan, *On the index of minimal zero-sum sequences over finite cyclic groups*, J. Combin. Theory Ser. A 114 (2007), 1545–1551.

Weidong Gao, Jiangtao Peng, Guoqing Wang
 Center for Combinatorics
 LPMC-TJKLC
 Nankai University
 Tianjin 300071, P.R. China
 E-mail: wdgao1963@yahoo.com.cn
 jtpeing1982@yahoo.com.cn
 gqwang1979@yahoo.com.cn

Yuanlin Li, Chris Plyley
 Department of Mathematics
 Brock University
 St. Catharines, Ontario
 Canada L2S 3A1
 E-mail: yli@brocku.ca
 cp07rp@brocku.ca

Received on 6.9.2009
 and in revised form on 15.7.2010

(6139)