Shorter long minimal zero-sum sequences over finite cyclic groups

Fang Chen

Oxford College of Emory University

Joint work with Svetoslav Savchev

Combinatorial and Additive Number Theory 2016

Graz, Austria

Abstract

This is a presentation of a manuscript on an inverse zero-sum problem. It characterizes the minimal zero-sum sequences over the cyclic group C_n ($n \geq 10$) with lengths between $\lfloor n/3 \rfloor + 3$ and $\lfloor n/2 \rfloor + 1$. The result is a step beyond established analogous theorems about minimal zero-sum sequences over C_n of lengths at least $\lfloor n/2 \rfloor + 2$. The range of the obtained characterization is optimal.

Among the possible approaches we choose one with emphasis on unsplittable sequences—intriguing objects generalizing the longest minimal zero-sum sequences over an abelian group. They prove capable of capturing the essence of our setting and deserve an explicit description.

Henceforth G denotes an additively written finite abelian group;
C_n denotes the cyclic group of order n.

Terminology and notation

Let α be a sequence over G. We denote its length, sum and sumset by $|\alpha|$, $S(\alpha)$ and $\Sigma(\alpha)$ respectively. Denote $\Sigma^*(\alpha) = \Sigma(\alpha) \cup \{0\}$.

For a subsequence β of α we write $\beta|\alpha$. If β and γ are complementary subsequences we say that they form a *decomposition* of α and write $\alpha = \beta\gamma$. The notation $\gamma = \alpha\beta^{-1}$ is also used in this case.

The multiplicity of a term $a \in \alpha$ is denoted by m_a. The support $supp(\alpha)$ of α is $supp(\alpha) = \{a \in G \mid \alpha \text{ has a term equal to } a\}$. The set of nonzero elements of G is $G^\bullet = G \setminus \{0\}$.

A nonempty sequence over G is:

- a *minimal zero-sum sequence* if its sum is the zero element of G and all of its proper nonempty subsequences have nonzero sums;
- a *zero-sum-free sequence* if all of its nonempty subsequence sums are nonzero.

One-element basis

Let α be a sequence over $\langle a \rangle$ where $a \in G^\bullet$. For every term $t \in \alpha$ let $x_a(t)$ be the unique integer in $[1, \mathrm{ord}(a)]$ such that $t = x_a(t)a$.

We call $\{a\}$ a 1-*element basis* for α if $\sum_{t \in \alpha} x_a(t) = \mathrm{ord}(a)$.

Having a 1-element basis is a substantial property of all sufficiently long minimal zero-sum sequences over C_n.

Theorem 1. Every minimal zero-sum sequence over C_n, $n \geq 3$, of length at least $\lfloor n/2 \rfloor + 2$ has a 1-element basis (see [2], [4]).

Let α have a 1-element basis $\{a\}$. The very fact that it is a minimal zero-sum sequence is expressed by the equality $\sum_{t \in \alpha} x_a(t) = \mathrm{ord}(a)$.

We want a similar attribute in the characterization of the "shorter long" minimal zero-sum sequences, ones with lengths in $\left[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1\right]$.

Two-element basis

Let $u \neq 0$ and v be elements of G such that $2v = ru$ with $r \in \mathbb{Z}$ satisfying $0 < r \leq \text{ord}(u)$ and $v \notin \{u, \ldots, ru\}$. Call the ordered pair (u, v) a 2-*element basis* for a sequence α over G if each term $t \in \alpha$ can be written in the form $t = x_t v + y_t u$ with $x_t \in \{0, 1\}$, $y_t \in \mathbb{Z}$ so that:

(i) $y_t \geq 1$ for $x_t = 0$; $y_t \geq 0$ for $x_t = 1$ with at most one exception: There can be one term t such that $x_t = 1$ and $-r < y_t < 0$.

(ii) $\sum_{t \in \alpha} x_t$ is odd or even according as $v \in \langle u \rangle$ or $v \notin \langle u \rangle$.

(iii) $\sum_{t \in \alpha}(r x_t + 2 y_t) = |\,\langle u, v \rangle\,|$.

The quantity $r x_t + 2 y_t$ assumes the rôle of $x_a(t)$ in the definition of a 1-element basis.

Proposition 1. A sequence over G with a 2-element basis is a minimal zero-sum sequence.

Now the main result in the manuscript can be stated as follows:

> *Each minimal zero-sum sequence over C_n, $n \geq 10$, with length in $[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1]$ has a 1-element or a 2-element basis.*

With an appropriate definition at hand it is not hard to reduce the proof to sequences of a rather special nature, the so-called *unsplittable sequences*.

These are minimal zero-sum sequences extremal in a well-defined sense; they enjoy certain properties of the longest minimal zero-sum sequences.

There are direct alternative ways to prove our main theorem, without reduction to sequences of a special kind. A common feature of all approaches known to us is the difficulty with the limit case of length exactly $\lfloor n/3 \rfloor + 3$.

Unsplittable sequences

A minimal zero-sum sequence α over G is *unsplittable* if replacing any term $t \in \alpha$ by any two elements of G with sum t yields a zero-sum sequence that is not minimal.

The basic properties of the unsplittable sequences are substantial enough to distinguish them among the general minimal zero-sum sequences.

Lemma 1. The following properties of a minimal zero-sum sequence α over G are equivalent:

(i) α is unsplittable.

(ii) For each $a \in supp(\alpha)$ one has $\Sigma(\alpha a^{-1}) = G^{\bullet}$.

(iii) For each $a \in \alpha$ and $g \in G$ there is a subsequence $\beta | \alpha$ that contains a and has sum g.

The general notion of an unsplittable sequence was introduced by Gao.

Work on nontrivial unsplittable sequences over C_n was started by Xia and Yuan [3] who determined all such sequences with maximum length $\lfloor n/2 \rfloor + 1$.

Recently Yuan and Li [5] solved the same problem for length $\geq \lfloor n/3 \rfloor + 8$, for sufficiently large n with least prime divisor greater than 13.

It is announced in [1] that Zeng, Yuan and Li [6] have extended this result, for odd $n > 50$, to sequences of lengths in $[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1]$.

Let us say that, apart from a couple of inevitable basic observations (see Lemma 1 above), our approach is entirely different in spirit and implementation from the ones in the articles [1], [3] and [5]. (The manuscript [6] is not available to us.)

In addition, our considerations are optimal in every relevant sense.

On the one hand, they are tight with respect to the sequence length $|\alpha|$, for which the range $[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1]$ is shown to be best possible. It is worth observing that the question becomes considerably more subtle and harder for values of $|\alpha|$ close to $\lfloor n/3 \rfloor + 3$.

On the other hand, the problem is solved for all admissible values of n, namely $n \geq 10$ (implied by the inequality $\lfloor n/3 \rfloor + 3 \leq \lfloor n/2 \rfloor + 1$).

Small terms

For a zero-sum-free sequence β over G and an element $u \in G$ define

$$I_\beta(u) = |\Sigma(\beta u)| - |\Sigma(\beta)| = |(u + \Sigma^*(\beta)) \setminus \Sigma(\beta)|.$$

Thus $I_\beta(u)$ denotes the increase of the sumset size $|\Sigma(\beta)|$ yielded by u if u is added to β as a term.

The elements $u \in G$ with $I_\beta(u) \in \{1, 2\}$ are particularly relevant. We call them *small terms* for β. More specifically u is a 1-term for β if $I_\beta(u) = 1$, and a 2-term for β if $I_\beta(u) = 2$.

Standard decompositions

A decomposition $\alpha = \beta\gamma$ of a zero-sum-free sequence α over G is *standard* if $|\beta| \geq 3$, $\gamma \neq \emptyset$ and each term of γ is a small term for β.

Both notions, a small term and a standard decomposition, are tailored to express the most the length condition $|\alpha| \geq \lfloor n/3 \rfloor + 3$ can provide.

The approach

Let α be a fixed "shorter long" unsplittable minimal zero-sum sequence over C_n without order-2 terms. We remove a term $t \in \alpha$ and consider the standard decompositions $\alpha t^{-1} = \beta\gamma$ of the zero-sum-free sequence αt^{-1}. It is fairly apparent that such a decomposition is meaningful if:

(1) the sequence γ (whose terms are small for β) is as long as possible;

(2) $|supp(\gamma)|$ is small, i. e., γ has as few distinct terms as possible.

The question is: To what extent can these demands be satisfied, and for what choices of β?

In search for an answer we start with observations on small terms in a general group, then go through a series of specific lemmas about the decompositions $\alpha t^{-1} = \beta\gamma$ defined above. As a result of the process we infer that a strong conclusion follows simply if, loosely speaking, β contains all occurrences in αt^{-1} of the removed term t.

For a term $a \in \alpha$ with multiplicity $m_a \geq 2$ consider a subsequence $\delta | \alpha a^{-1}$ such that $a^{m_a - 1} | \delta$ and $|\delta| \geq 3$. Let $\alpha a^{-1} = \beta\gamma$ be a standard decomposition of αa^{-1} such that δ is contained in β. Then:

a) $|supp(\gamma)| = 1$; moreover $supp(\gamma) = \{u\}$ where u is a 2-term for β.

b) $C_n^{\bullet} \backslash \Sigma(\beta) = \{-ku, \ldots, -2u, -u\} \cup \{-a-(k-1)u, \ldots, -a-u, -a\}$ where $k = |\gamma| \geq 1$.

Property (ii) from Lemma 1 plays a crucial rôle throughout this part of the work. Its impact can be seen in statement b) above, which shows that the structure of the complement $C_n^{\bullet} \backslash \Sigma(\beta)$ is simple and manageable.

Statement a) answers the demand (2) above in the best possible way. As for demand (1), applying statement a) to a special standard decomposition $\alpha a^{-1} = \beta\gamma$ yields the following key estimate:

$$|\gamma| \geq |\Sigma(\delta)| - 3|\delta| + 5. \tag{*}$$

It suggests to ensure $|\Sigma(\delta)|$ large with respect to $|\delta|$. This is where property (iii) from Lemma 1 comes into play.

Fix a term $a \in \alpha$ with highest multiplicity $m_a \geq 2$. Denote $\alpha_a = a^{m_a}$ and $P_a^* = \Sigma^*(\alpha_a) = \{0, a, \dots, m_a a\}$. From now on we consider decompositions of the zero-sum-free sequence αa^{-1}.

Call an a-*sum* a subsequence of $\alpha\alpha_a^{-1}$ with sum a. By property (iii) in Lemma 1 each $b \in supp(\alpha\alpha_a^{-1})$ is contained in an a-sum.

Moreover one can show that for every a-sum $b_1 \dots b_k$ the k translates $b_1 + P_a^*, b_1 + b_2 + P_a^*, \dots, b_1 + \cdots + b_k + P_a^*$ are disjoint.

This fact implies sufficiently strong lower bounds on $|\Sigma(\delta)|$ for appropriately chosen subsequences δ, so that the estimate (*) yields purposeful consequences.

Combined with the structural conclusion about $C_n^{\bullet} \setminus \Sigma(\beta)$ described in statement b), they complete the main argument.

The case of a “shorter long” sequence with an order-2 term over C_n is easy and considered separately.

To summarize, we identified all admissible “shorter long” sequences, i. e., unsplittable minimal zero-sum sequences α over C_n, $n \geq 10$, with length $|\alpha| \in [\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1]$.

Proposition 2. A necessary condition for a sequence to be admissible is that it has one of the following forms:

a) $\alpha = u^p v^q (v-u)$ where $\mathrm{ord}(v-u) = 2$ and $p, q \geq 1$, $p + q = n/2$.

b) $\alpha = a^{m_a} b^{m_b} (b - sa)$ where $m_a \geq m_b \geq 1$, $s \in [1, m_a]$ and $2b = (s+1)a$.

c) $\alpha = a^{m_a} b^{m_b} (b - a)$ where $m_a \geq m_b \geq 3$ and $3b = 2a$.

Instead of discussing sufficiency in each case we prefer a unified treatment.

A family of nontrivial unsplittable sequences

Apparently every admissible sequence a)–c) can be represented in the form $\alpha = u^p v^q (v - su)$, where $u, v \in C_n$ and $p, q, s \in \mathbb{Z}$ satisfy:

(i) $u \neq 0$, $v \notin \{u, 2u, \ldots, (p+1)u\}$ and $1 \leq s \leq p < \text{ord}(u)$, $q \geq 1$;

(ii) $2v = (s+1)u$ and $\langle u, v \rangle = C_n$.

The parameters p, q, s are far from independent; one needs to find out more for the sufficiency. A minimal zero-sum sequence α over C_n that has the above form satisfies the next conditions too:

(iii) q is even or odd according as $v \in \langle u \rangle$ or $v \notin \langle u \rangle$;

(iv) $2p + (q-1)(s+1) + 2 = n$.

It turns out that conditions (i)–(iv) are enough to ensure that α is an unsplittable minimal zero-sum sequence. Moreover they imply that (u, v) is a 2-element basis for α.

Theorem 2. Let a sequence α over C_n have the form $\alpha = u^p v^q (v - su)$, where $u, v \in C_n$ and $p, q, s \in \mathbb{Z}$ satisfy conditions (i), (ii), (iii) and (iv). Then (u, v) is a 2-element basis for α.

The straightforward proof reveals the true nature of the inexpressive condition $2p + (q-1)(s+1) + 2 = n$. It is equivalent to the key identity $\sum_{t \in \alpha}(rx_t + 2y_t) = |\langle u, v \rangle|$ in the definition of a 2-element basis.

Corollary 1. Each sequence satisfying the assumptions of Theorem 2 is a minimal zero-sum sequence.

Proposition 3. Each sequence satisfying the assumptions of Theorem 2 is unsplittable.

A characterization of the unsplittable "shorter long" minimal zero-sum sequences over C_n, $n \geq 10$

Our first main result is a description of the longest nontrivial unsplittable minimal zero-sum sequences over C_n, $n \geq 10$.

Theorem 3. A sequence over the cyclic group C_n, $n \geq 10$, with length in $\left[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1\right]$ is an unsplittable minimal zero-sum sequence if and only if it has a representation of the form $u^p v^q (v - su)$, where $u, v \in C_n$ and $p, q, s \in \mathbb{Z}$ satisfy the following conditions:

(i) $u \neq 0$, $v \notin \{u, 2u, \ldots, (p+1)u\}$ and $1 \leq s \leq p < \text{ord}(u)$, $q \geq 1$;

(ii) $2v = (s+1)u$ and $\langle u, v \rangle = C_n$;

(iii) q is even or odd according as $v \in \langle u \rangle$ or $v \notin \langle u \rangle$;

(iv) $2p + (q-1)(s+1) + 2 = n$.

The range of characterization is optimal

The necessity part of the theorem states the substantial fact that *all* unsplittable "shorter long" minimal zero-sum sequences over C_n, $n \geq 10$, have the form described by Theorem 2. This is no longer so for shorter sequences, even for ones of length $\lfloor n/3 \rfloor + 2$.

Consider the following examples where g is a generator of C_n:

(1) $(3g)^{(n-7)/3}(4g)(5g)(-g)^2$ where $n \equiv 1 \pmod 3$, $n \geq 13$;

(2) $(3g)^{(n-8)/3}(5g)^2(-g)^2$ where $n \equiv 2 \pmod 3$, $n \geq 14$;

(3) $(3g)^{n/3-2}(4g)^2(-g)^2$ where $n \equiv 0 \pmod 3$, $n \geq 12$.

These are unsplittable minimal zero-sum sequences over C_n, all of length $\lfloor n/3 \rfloor + 2$. On the other hand apparently none of them can be expressed in the form in Theorem 2. Hence the length range $\left[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1\right]$ of our characterization is optimal.

A characterization of the general “shorter long” minimal zero-sum sequences over C_n, $n \geq 10$

The second main result is a description in terms of bases with one or two elements. It characterizes all minimal zero-sum sequences over C_n, $n \geq 10$, in the length range $\left[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1\right]$.

Theorem 4. A sequence over the cyclic group C_n, $n \geq 10$, with length in $\left[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1\right]$ is a minimal zero-sum sequence if and only if it has a 1-element or a 2-element basis.

The length range $\left[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1\right]$ of this second characterization theorem is also optimal. The sequences (1)–(3) above are minimal zero-sum sequences of length $\lfloor n/3 \rfloor + 2$; however none of them has a 1-element or a 2-element basis.

References

[1] W. D. Gao, Y. Li, P. Yuan and J. Zhuang, On the structure of long zero-sum free sequences and n-zero-sum free sequences over finite cyclic groups, *Archiv der Mathematik*, 105 (2015), 361–370.

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

[3] X. Xia and P. Yuan, Indexes of unsplittable minimal zero-sum sequences of length $\mathbb{I}(C_n) - 1$, *Discrete Mathematics* 310 (5) (2010), 1127–1133.

[4] P. Yuan, On the index of minimal zero-sum sequences over finite cyclic groups, *Journal of Combinatorial Theory, Series A* 114 (8) (2007), 1545–1551.

[5] P. Yuan and Y. Li, Long unsplittable zero-sum sequences over a finite cyclic group, *International Journal of Number Theory*, in press, doi:10.1142/S1793042116500615

[6] X. Zeng, P. Yuan and Y. Li, On the structure of long unsplittable minimal zero-sum sequences, submitted, 2015.